Note

Before using this information and the product it supports, read the information in “Notices,” on page 671.
Chapter 6. Configuring the Community Services ............................................. 231

About the Community Services .......................................................... 231
Community Services configuration settings ........................................... 232
   General settings .................................................................................. 233
   Server Features settings ...................................................................... 233
   Sametime Connect for browsers settings ............................................. 233
   Community Services connectivity settings ........................................... 234
   Community Services server clusters .................................................. 234
   Number of entries on each page in dialog boxes that show names in the directory ......................................................... 234
   How often to poll for new names added to the Sametime Community directory ................................................................. 235
   How often to poll for new servers added to the Sametime Community ................................................................................... 235
   Maximum user and server connections to the Community server .......... 236
   Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf) ......................................................... 237
   Display the "Download Sametime Connect for the desktop" link .............. 237
   Allow users to transfer files to each other ............................................. 238
   Allow users to send announcements ................................................... 239
   Allow Connect users to save their user name, password, and proxy information (automatic login) ...................................................... 240
   Display the "Launch Sametime Connect for browsers" link ...................... 241
Anonymous Access Settings for Community Services ................................. 242
   Anonymous users can participate in meetings or enter virtual places ...... 243

Chapter 7. Enabling the SIP Gateway .................................................... 265

Using the SIP functionality with Sametime ............................................. 265
   Using the SIP functionality in a Windows, AIX, or Solaris environment ................................................................................. 265
Using the SIP functionality in an IBM i5/OS environment .......................... 266
   Overview of SIP components .............................................................. 267
Chapter 12. Logging Sametime

Activity ............................................ 383
Community Logins/Logouts  ........................................ 383
Community Login/Logout information .................................. 383
Community Statistics ............................................ 384
Community Statistics information .................................. 385
Community Events ............................................ 385
Community Events information .................................. 386
Place Login Failures ........................................... 386
Place Login Failure information .................................. 387
Meeting Login Failures ........................................... 388
Meeting Login Failures information .................................. 388
Meeting Connections ........................................... 389
Meeting Connections information .................................. 389
Server Connections ............................................ 390
Server Connections information .................................. 390
Meeting Statistics ............................................ 390
Meeting Statistics information .................................. 391
Meeting Events ............................................ 391
Meeting Events information .................................. 391
Capacity Warnings ............................................ 393
Capacity Warnings information .................................. 393
Usage Limits in the log ............................................ 394
Usage Limits and Denied Entries information ......................... 394
Domino log ............................................ 394
Content of the Domino log ............................................ 395
Views in the Domino log ............................................ 395
Sametime log settings ............................................ 396
General log settings ............................................ 396
Capacity Warnings log settings .................................. 399

Chapter 13. Managing Security .......................... 401
Getting started with Sametime security .......................... 401
The required fully qualified server name .......................... 401
Basic password authentication and authentication by token .......... 401
User requirements for basic password authentication .......... 402
Changing a user’s password ............................................ 405
Anonymous access and the Sametime Meeting Center .......... 406
Domino security and the Web browser connection ............ 408
Using database ACLs for identification and authentication .......... 409
Using database ACLs ............................................. 409
Maximum Internet name & password setting ......................... 410
Adding a name to a database Access Control List (ACL) .......... 410
Database ACL settings ............................................. 411
Anonymous access and database ACLs .................................. 415
Basic password authentication and database ACLs .......... 417
Authentication by token using LTPA and Sametime tokens .......... 419
Authentication by token using the Domino Single Sign-On (SSO) feature .................................. 420
Altering the Domino Web SSO configuration following the Sametime server installation .................................. 421
Manually enabling the Domino SSO feature .................................. 424
Using the Sametime custom logon form for SSO Authentication by token using Secrets and Tokens databases .................................. 428
Security recommendations for self-registration .................................. 430
Encryption and meeting passwords .................................. 431
Using SSL with Sametime ............................................ 432
Encrypting Web browser connections with SSL .................................. 432
Ensuring access to Sametime servlets when Domino requires SSL for all connections .................................. 432
Encrypting connections to an LDAP server .................................. 432
Setting up SSL for Sametime on Windows .................................. 433
Setting up SSL for Sametime on Solaris/AIX .................................. 436
Ensuring Sametime servlet access when Domino requires SSL for all connections .................................. 440
Obtaining the appropriate SSL trusted root or SSL server certificate .................................. 441
Import the SSL certificate into the STKeys.jks key database .................................. 444
Configure the Sametime.ini file on the Sametime server .................................. 446

Chapter 14. Deploying Multiple Lotus Sametime Servers .......................... 449
About Sametime server clusters .................................. 449
Advantages of using multiple Sametime servers .................................. 449
Advantages of multiple home Sametime servers .................................. 450
Advantages of a single meeting on multiple servers .................................. 450
Integrating a Sametime server into an existing Sametime community .................................. 451
Installing a Sametime server into an existing Sametime community .................................. 452
Configuring ports for server-to-server connections .................................. 455
Synchronizing the Sametime server with other Sametime servers .................................. 456
Extending Sametime to Internet users .................................. 463
Positioning a Sametime server in the network DMZ .................................. 464
Opening ports on the internal firewall .................................. 465
Opening ports on the external firewall .................................. 468
Screen-sharing security and Internet users .................................. 471
Extending a single Sametime community across multiple Domino domains .................................. 472
Example of extending a single Sametime community across two Domino domains .................................. 473

Chapter 15. Introduction to server clusters and the Enterprise Meeting Server .................................. 483
Creating Sametime server clusters .................................. 483
Clustering Community Services and Meeting Services .................................. 483
Clustering the Community Services without clustering the Meeting Services .................................. 484
Chapter 1. Introduction to Sametime

This chapter provides network administrators with an overview of the IBM® Lotus® Sametime® server. This chapter introduces Sametime collaborative features, clients, services, applications, administrative features, and the IBM Lotus Sametime Enterprise Meeting Server (EMS) application. The EMS application is an add-on product for a Sametime deployment that must be purchased separately from the Sametime server.

What is Sametime?

Sametime consists of client and server applications that enable a community of users to collaborate in real-time online meetings over an intranet or the Internet. Members of the Sametime community use collaborative activities such as presence, chat, screen sharing, a shared whiteboard, and real-time audio/video capabilities to meet, converse, and work together in instant or scheduled meetings.

Sametime "presence" technology enables members who have logged in to the Sametime server to see all other members who are online (logged in). The names of online users display in "presence lists" in Sametime applications. From these presence lists, members of the community can converse through instant messaging sessions or start instant meetings that include chat, screen-sharing, whiteboard, question and answer polls, the ability to send Web pages to other users, and audio/video capabilities.

While presence lists support instant awareness and instant collaboration with other online users, the Sametime Meeting Center on the Sametime server provides a central meeting place for members of the community. In the Meeting Center, users can schedule meetings to start at a particular time. Users access the Sametime Meeting Center with Web browsers at the scheduled meeting time to attend the meeting.

The two primary Sametime client applications are the IBM Lotus Sametime Connect client and the Sametime Meeting Room client. The Sametime Connect client is a Windows® application that contains a presence list that displays selected members of the community who are online. From Sametime Connect, a user can collaborate by sending instant messages or by starting an instant meeting with any other online member of the community.

The Sametime Meeting Room client is a Java™ applet that loads and runs in a user’s Web browser whenever the user attends an instant or scheduled meeting. The Sametime Meeting Room client contains components that support the full range of Sametime collaborative activities, including interactive audio and video.

Sametime supports a broadcast technology that enables a large number of view-only users (or audience members) to watch a small number of users (or presenters) interact in a meeting. The broadcast technology is especially useful for meetings in which one person, or a small group of people, make presentations to a large audience. Audience members watch a broadcast meeting using a separate receive-only Java client called the Sametime Broadcast client.

Each Sametime server contains an IBM Lotus Domino™ Directory that maintains information about all users and servers that comprise the Sametime community.
The Sametime server can also be configured to operate as a client to a Lightweight Directory Access Protocol (LDAP) server containing an LDAP directory.

Sametime works through the interaction of its client applications with services on the Sametime server. The Sametime services include the Community Services, Meeting Services, Broadcast Services, Domino/Web Application Services, and Audio/Video Services. Managing the directory, ensuring that Sametime clients can connect to the Sametime server, configuring the Sametime services, and monitoring the server are some of the primary administrative tasks associated with the Sametime server.

Sametime administrators use the Web-based Sametime Administration Tool. This tool runs in a Web browser and is available from the "Administer the Server" link on the Sametime server home page.

The Sametime 7.0 server includes the concept of server clustering. Sametime server clusters:

- Enhance server scalability and reliability to enable Sametime to meet the demands of large user populations.
- Provide load balancing and failover capabilities for Sametime Community Services and Meeting Services.

For more information about server clusters, see Sametime server clusters.

---

**Install Sametime on a Domino server**

A Sametime server must be installed on a Domino server. Sametime can be installed on a Domino server running on a Windows, IBM iSeries™, or IBM pSeries™ server. This documentation uses the term "Sametime server" to refer to the server that includes both Domino and Sametime.

**Note:** For detailed information about system requirements, installation procedures, and the version of Domino on which Sametime must be installed, see the Lotus Sametime Server 7.0 Installation Guide (stinstall.nsf or stinstall.pdf) that is shipped with the Sametime server. Separate installation guides are provided for each platform.

Sametime uses the Directory, security, and replication features of Domino servers. It is best if the Sametime server is dedicated to supporting the real-time, interactive communication services of Sametime. A Sametime server should not be used for other high-demand Domino services such as mail storage and routing, application and database storage, or centralized Directory and administration services.

**Note:** An IBM i5/OS or IBM pSeries server can run multiple partitioned servers on the same Domino system. While it is possible to add Sametime to an existing production Domino server, this configuration is not recommended. Instead, consider creating a new Domino server for running Sametime. The new Domino server can reside on the same system as your existing production server.

Users must access the Sametime server with a Web browser. IBM Lotus Notes® client access to the Sametime server home page (stcenter.nsf) or the Sametime Meeting Center database (stconf.nsf) is not supported. All other Sametime clients, including the Sametime Connect client, can be downloaded by end users from the Sametime server home page.
You can install more than one Sametime server in a Domino environment. Installing multiple Sametime servers provides several advantages related to load balancing and network usage and can enhance meeting and server performance. For more information, see "Advantages of using multiple Sametime servers".

If you install multiple Sametime servers, the administrator has the option of clustering the Sametime servers. Clustering Sametime servers provides failover and load balancing capabilities, and can increase the reliability and scalability of Sametime. For more information, see "Creating Sametime server clusters".

The Web-based Sametime Administration Tool is the recommended administration tool for the Sametime components of the Sametime server. The Sametime Administration Tool should be used for most administrative tasks. See "Sametime Administration Tool" for more information about tasks that are not performed with the Sametime Administration Tool.

**Sametime basics**

This section introduces Sametime administrators to basic Sametime terms, concepts, and features that appear throughout this administrator’s guide. The terms, concepts, and features are grouped into four basic categories:

- Collaborative activities and end-user features
- Administration terms and features
- Sametime clients
- Sametime services

**Collaborative activities and end-user features**

This section provides brief descriptions of Sametime collaborative activities and end-user features that are referred to throughout this administrator’s guide. Sametime administrators should be familiar with these terms. To learn more about these collaborative activities and features, you can experiment with the end-user features of Sametime. Online help for many of these features is also available from the Documentation link of the Sametime server home page.

The Sametime collaborative activities and end-user features include:

- Presence
- Chat
- Meetings
- Screen sharing
- Shared whiteboard
- Send Web Pages
- Polling
- Hand raise
- Transfer files
- Record and Playback (Recorded Meetings)
- IP audio
- IP video
- Sametime server home page
- Sametime Meeting Center
- Breakout sessions
Presence
Presence refers to the ability of a user to detect when other users are online. A user can view a presence list in a Sametime client or application that displays the names of other online users. Presence is sometimes called “awareness” or “online awareness.”

A presence list (or contact list) is a starting point for immediate or “instant” collaboration. Presence lists in Sametime clients display the names of online users in bold green text. Instant messaging sessions and instant meetings can be started immediately from a contact list. A user simply double-clicks or right-clicks an online user’s name to send an instant message or start an instant meeting.

Contact lists are found in all Sametime clients. The Sametime Connect client includes a contact list that can display the names of all users in the community who are online. The Sametime Meeting Room client contains a Participant List that displays the names of all users attending a particular meeting.

A user logs in to the Community Services on the Sametime server to become present in the community or an online place (such as a Sametime meeting or Web site enabled with Sametime technology). The Community Services on the Sametime server support all presence functionality in Sametime.

Chat
Sametime supports text-based chat and instant messaging. A chat session can consist of two (or more) users exchanging instant messages. Chat or instant messaging sessions can be initiated from any contact list in a Sametime client.

The Sametime Connect client includes a contact list from which instant messaging sessions can be started with any other member in the community who is online. Additional community members can be invited into instant messaging sessions to form group chat conferences.

The Sametime Meeting Room client contains a public chat area (called the “Meeting Room chat tool”) that enables all participants in a meeting to view and enter messages. All messages entered in the public chat area can be viewed by all participants in the meeting.

In addition to the Meeting Room chat tool, the Sametime Meeting Room client also includes a Participant List. The Participant List is a contact list from which one user can initiate a private chat session with another user in the meeting. The messages exchanged in the private chat session are seen by the users engaging in the chat session, but not by all participants in the meeting. The Meeting Room chat tool is the public chat tool in a meeting. The Participant List supports private chats in the meeting.

All instant messaging and chat activity is supported by Community Services on the Sametime server.

Meetings
Sametime meetings are either “instant” or “scheduled.”

An instant meeting is started immediately from a presence list in any Sametime client. Whiteboard files cannot be saved during instant meetings. Instant meetings cannot be recorded.
A scheduled meeting is scheduled to start at a particular time and date. Scheduled meetings are created in advance in the Sametime Meeting Center application (sconf.nsf) on the Sametime server. Users access the Sametime Meeting Center application on the Sametime server with a Web browser at the scheduled meeting time to attend the meeting.

**Note:** You can create a meeting in the Sametime Meeting Center and enable the meeting to "Start immediately." For clarity, such a meeting is considered a scheduled meeting. Any meeting started in the Sametime Meeting Center is a scheduled meeting. Any meeting started from a contact list is an instant meeting.

A collaborative session is a meeting if the Sametime Meeting Room client is launched. The Sametime Meeting Room client is launched for collaborative sessions that include any of the following activities: screen sharing, whiteboard, question and answer polling, send Web pages, Meeting Room chat, audio, and video. However, the Sametime Meeting Room client is not launched for chat-only sessions between users. A session that includes only instant messaging or a group chat conference does not require the use of the Sametime Meeting Room client.

The Meeting Services and the Community Services support the starting, stopping, and creation of meetings on the Sametime server. Components of the Sametime Meeting Room clients interact with the Meeting Services, Community Services, and Audio/Video Services when participating in Sametime meetings.

**Breakout sessions**

Users who are attending a meeting see a list of all meeting participants in the Participant List component of the Meeting Room client. While the meeting is in progress, a user can start a "breakout session" with any user displayed in the Participant List.

A breakout session is an instant meeting that is started from the Participant List of a meeting that is currently active. To start a breakout session, the user selects the name of another meeting participant (or participants) from the Participant List and starts an instant meeting with that user. Other users can also be invited to this breakout session.

Breakout sessions have the following characteristics:

- If a breakout session will include any collaborative activities other than chat (such as whiteboard or screen sharing), the user must have permission to edit/share from the Meeting Moderator to start a breakout session. If the breakout session will use chat only, no permissions are necessary to start the breakout session.
- When the user starts a breakout session, the original meeting remains open in a browser window, and the user is still a participant in the original meeting. To return to the original meeting, the user leaves the instant meeting and selects the browser window that contains the active meeting.
- When a breakout session begins, it does not contain any information (such as a chat transcript or whiteboard file) from the original meeting.
- If both the original meeting and the breakout session include IP audio, the user’s voice is heard in both meetings. Users should mute their microphones in either the original meeting or the breakout session so that their voices are heard in only one meeting at a time. Users should also mute their speakers in one of the meetings if they do not want to hear audio from both meetings at once.
• If the original meeting includes IP audio and the breakout session includes IP video, the user’s video image is not seen in the breakout session until his or her microphone is muted in the original meeting. If a user was the last person to speak in the original meeting, the user’s video image continues to appear in the original meeting until someone else in the original meeting speaks.

**Screen sharing**

Screen sharing is a Sametime collaborative activity that enables multiple users to work within a single application on one user’s computer. Geographically dispersed users in remote locations can collaborate within a single application to produce a document, spreadsheet, blueprint, or any other file generated from a Windows application. Screen sharing is sometimes also referred to as "application sharing."

In a meeting that includes screen sharing, one end user uses the screen-sharing tool in the Sametime Meeting Room client to share a screen or application on the user’s local computer with other meeting participants in remote locations. The other meeting participants also use the screen-sharing tools of the Sametime Meeting Room client on their local computers to view and make changes to the shared screen or application. It is not necessary for the remote users to have the application that is being shared installed on their local systems. (The remote users share a single instance of the application that is running on only one meeting participant’s computer.)

Only one user at a time can be in control of the shared screen. Most users see the initials of the user who controls the shared screen beside the cursor. The person who is sharing the screen does not see the initials when someone else controls the shared screen. The person who is sharing the screen must view the Participant List details to confirm who controls the shared screen.

The administrator controls whether this collaborative activity is available for meetings on the Sametime server from the Configuration - Meeting Services - General tab of the Sametime Administration Tool.

Screen sharing is supported by T.120 components of the Meeting Services on the Sametime server. For more information about using this collaborative activity in a meeting, see the Sametime end-user online help.

**Shared whiteboard**

The shared whiteboard is a Sametime collaborative activity that supports interactive presentations. A shared whiteboard presentation closely resembles a slide show.

In a whiteboard presentation, one participant presents images in the whiteboard tool of the Sametime Meeting Room client on the participant’s local computer. Remote meeting participants can view the images and annotate the images using the whiteboard tools in the Sametime Meeting Room clients running on their local computers.

Before images can be presented on the whiteboard, a file containing the images must be attached to the meeting. Users can attach files when creating meetings, and the Moderator can attach files before or during meetings. Files are automatically converted into the file type required for display in the whiteboard tool.

In some cases, the format of a file that is added to the Attachments dialog might not be properly preserved and the file might not display correctly during a
whiteboard meeting. In these cases, the IBM Lotus Sametime Print Capture utility provides an alternate method of creating a whiteboard file. The Sametime Print Capture operates much like a printer driver and enables end users to print output from any Windows application to the file format required by the whiteboard.

**Note:** Sametime servers that run on operating systems other than Windows only support whiteboard attachments created with the Sametime Print Capture utility. For more information on how to use the Sametime Print Capture utility, see the Sametime end-user help and the Sametime Print Capture help.

The shared whiteboard is supported by T.120 components of the Meeting Services on the Sametime server.

The administrator controls whether the shared whiteboard collaborative activity is available for meetings on the Sametime server by selecting a setting in the Configuration - Meeting Services - General tab of the Sametime Administration Tool. For more information about using the shared whiteboard collaborative activity in a meeting, see the Sametime end-user online help available from the Documentation link on the server home page.

**Saving the whiteboard:** During a meeting, the meeting Moderator can save a whiteboard file so that others can view it when the meeting is over. For example, if someone has presented a file on the whiteboard, and several participants have annotated the file, the Moderator can save the changed file.

The whiteboard file is saved on the Sametime server as an attachment to the Meeting Details document associated with the meeting. The whiteboard is saved in two file formats: RTF and SWB (Sametime whiteboard). The RTF file can be opened in most word processing or graphics applications for printing or viewing after the meeting has ended. The SWB file can be attached to future meetings and presented on the whiteboard during those meetings.

If the whiteboard is saved more than once during a meeting, only the most recently saved version is available from the Meeting Details document. The most recently saved version is available in both the RTF and SWB formats.

The administrator controls whether the Meeting Moderator is allowed to save the whiteboard from the Configuration - Meeting Services - General tab of the Sametime Administration Tool.

**Send Web Pages**
Send Web Pages is a Sametime collaborative activity that enables a Meeting Moderator to send a Web page URL to all participants in a meeting, including audience members in broadcast meetings. When the Moderator sends a Web page URL to the meeting participants, a browser window opens on each participant’s screen and displays the Web page. If the Moderator sends an additional Web page URL to the meeting participants, the new Web page replaces the previous Web page in the Web browser window.

The Send Web Pages feature enables the Moderator to ensure that all meeting participants are looking at the same Web page. However, if the Meeting Moderator or any meeting participant clicks a link or scrolls the Web page, the other meeting participants do not see this activity occurring in the Web browser window on their
local machines. Each participant can explore the Web page, go to a different Web page, or close the window without affecting what other participants see in their browser windows.

The administrator controls whether this collaborative activity is available for meetings on the Sametime server from the Configuration - Meeting Services - General settings of the Sametime Administration Tool.

For more information about using the Send Web Pages feature in a meeting, see the Sametime end-user online help available from the Documentation link on the Sametime server home page.

**Polling**
Polling is a Sametime collaborative activity that enables a Meeting Moderator to use polls (or ask questions) to gather feedback from meeting participants. For example, the Moderator might ask meeting participants to vote to approve or reject a proposal. Only the Moderator can send polls.

**Note:** During broadcast meetings, only presenters can respond to polls, but both presenters and audience members can view poll responses shared by the Moderator. During fully-interactive Sametime meetings, all meeting participants can respond to polls and view responses shared by the Moderator.

Participants’ responses to poll questions are tallied in the Moderator’s Poll Tab. The Moderator can keep the poll responses private, or share them with the other meeting participants.

When sending a poll, the Moderator can also:

• **Share the tallied responses with other participants** - Normally, the Moderator is the only person who sees poll responses. The Moderator can choose to share the tallied poll responses so that all participants see the responses in the Poll Tab of the Sametime Meeting Room client.

• **Allow anonymous responses** - By default, the Moderator can see each participant’s response to poll questions. (These individual responses cannot be shared with other meeting participants.) Because people often answer more freely when they know their identity will not be revealed, the Moderator can preserve participants’ privacy by allowing anonymous responses to poll questions. During Broadcast meetings, only presenters can respond to polls.

• **Mark correct answers** - The Moderator can specify correct answers for poll questions. When the Moderator shares the poll responses, participants can see if they answered the question correctly.

The administrator controls whether this collaborative activity is available for meetings on the Sametime server from the Configuration - Meeting Services - General tab of the Sametime Administration Tool.

For more information about using this collaborative activity in a meeting, see the Sametime end-user online help available from the Documentation link on the Sametime server home page.

**Hand raise**
Hand raise is a collaborative activity that allows users to raise a hand at any time during a meeting. When users raise their hands, a hand icon appears next to their names in the Participant List.
A user might raise a hand to:
- Ask for permission to edit/share or permission to speak.
- Respond to a question or speak during the meeting.
- Attract the Moderator’s attention.

The Moderator can lower raised hands at any time, or users can lower their own hands. Users do not need permission to edit/share or permission to speak to raise their hands.

**Transfer files**

Transferring files is a Sametime collaborative activity that enables users to send a file to another user via a contact list in the Sametime Meeting Room or the Sametime Connect client. Users must transfer one file at a time to one person at a time. File transfers are automatically encrypted.

The administrator can enable or disable this feature. When you enable this feature, both authenticated and anonymous users can transfer files.

**CAUTION:**

To protect against viruses that might be spread through file transfers, users should have current anti-virus software. The software’s real-time protection settings should be enabled and set to scan all files.

For more information about enabling, disabling, and setting size limits for file transfers, see [Allow users to transfer files to each other](#).

**Note:** The file transfer feature does not work with Sametime Links. For more information about Sametime Links, see the the Sametime Directory and Database Access Toolkit documentation available from IBM DeveloperWorks (http://www.ibm.com/developerworks/lotus/products/instantmessaging/). Follow the link for "Toolkits and Drivers."

**Record and Playback (Recorded Meetings)**

Sametime includes a Record and Playback feature that enables a user to record meetings. When scheduling a meeting, the user selects a check box labeled "Record this meeting so that others can replay it later" to record the meeting.

When a user records a meeting, a Sametime Record and Playback (.RAP) file that contains a recorded version of the meeting is automatically saved as an attachment to the Meeting Details document when the meeting ends. Anyone who has access to the meeting can click a "Replay the Meeting” button on the Meeting Details document in the Sametime Meeting Center to play the recorded version of the meeting.

When the user clicks "Replay the Meeting," a modified version of the Sametime Broadcast client Java applet starts in a Web browser window on the user’s machine and connects to the Broadcast Gateway component of the Sametime server. The Broadcast client is modified to include controls that enable the user to stop, pause, and resume the playback of recorded meeting files.

The following restrictions apply to recorded meetings:
- Users cannot choose to record a meeting after the meeting begins; they must select the "Record this meeting..." option when scheduling the meeting.
- Users can only record a scheduled meeting; it is not possible to record an instant meeting.
The administrator controls whether the Record and Playback feature is available for meetings on the Sametime server from the Configuration - Meeting Services - General tab of the Sametime Administration Tool.

If the administrator allows the Record and Playback feature to be available on the server, there are administrative tasks associated with managing the recorded meeting files. These tasks include:

- Exporting (or saving) a recorded meeting
- Deleting a recorded meeting
- Replacing a recorded meeting with another recorded meeting file
- Importing a recorded meeting file

See Managing recorded meetings (Record and Playback) for more information.

**IP audio**

Interactive IP Audio is a Sametime collaborative activity that enables multiple (two or more) users to transmit and receive audio over an IP network.

In a meeting that includes interactive IP audio, the audio can operate in either the "automatic microphone" or the "request microphone" mode. The request microphone mode is the more controlled mode. Only one user can speak at a time and a user must request the microphone before speaking. The automatic microphone mode enables two users to speak simultaneously. In the automatic microphone mode, the person speaking is automatically detected by the Audio/Video Services on the Sametime server (it is not necessary to request the microphone before speaking). Automatic microphone mode offers a more natural form of conversation but provides less control.

The end user uses the audio tool of the Sametime Meeting Room client when participating in a meeting that includes IP audio. This tool contains microphone and speaker volume controls and mute features, and a button that allows users to configure the audio and video preferences on their computers. For more information about the end-user aspects of the IP Audio collaborative activity, see the Sametime end-user online help.

The term "interactive" IP audio refers to the technology that enables all participants in a meeting to both transmit and receive IP audio packets on the network. In an interactive IP audio meeting, one user transmits a stream of audio packets to the server and the server disseminates this stream to all other meeting participants. This "one-to-many" form of communication is sometimes called "multipoint" audio.

The term "broadcast" IP audio refers to the streaming technology that enables a large group of users (or audience members) to receive the audio from a meeting but not transmit audio to other users in a meeting.

IP audio is supported by the Audio/Video Services on the Sametime server. Broadcast IP audio is supported by the Audio/Video Services and the Broadcast Services on the Sametime server.

**IP video**

Interactive IP video is a Sametime collaborative activity that enables multiple users to transmit and receive video packets over an IP network.

In a meeting that includes interactive IP video, the video follows the audio. The video component of the Sametime Meeting Room client includes a Remote and
Local video window. The Remote window displays images from the camera of the person who is speaking and the Local window displays the image from a user’s local camera.

Sametime does not support video-only meetings. A meeting that includes IP video must also include IP audio. For more information about the end-user aspects of this collaborative activity, see the Sametime end-user online help.

The term "interactive" IP video refers to the technology that enables all participants in a meeting to both transmit and receive IP video packets on the network. In an interactive IP video meeting, one user transmits a stream of video packets to the server and the server disseminates this stream to all other meeting participants. This "one-to-many" form of communication is sometimes called "multipoint" video.

The term "broadcast" IP video refers to the streaming technology that enables a large group of users (or audience members) to receive video but not transmit it.

Interactive IP video is supported by the Audio/Video Services on the Sametime server. Broadcast IP video is supported by the Audio/Video Services and the Broadcast Services on the Sametime server.

**Sametime server home page (stcenter.nsf)**
The Sametime server home page is an HTML page that exists in the Sametime Center database (stcenter.nsf). The Sametime server home page can only be accessed by a Web browser and is the end-user entry point to the Sametime server.

After installing the Sametime server on the Domino server, you must set stcenter.nsf as the Home URL for the server. To do this, open the Server document for the Domino server that includes Sametime, select the Internet Protocols tab, select the HTTP tab, and enter **stcenter.nsf** in the Home URL field of the Mapping section of the Server document.

As the user entry point to the Sametime server, the Sametime server home page contains links to the following important Sametime entities:

- [Sametime Meeting Center](#)
- [Sametime Connect client](#) (includes clients that can be downloaded)
- [Self-registration feature](#)
- [Sametime Administration Tool](#)
- End-user documentation
- Sametime Developers Web site

**Sametime Meeting Center (stconf.nsf)**
The Sametime Meeting Center is an application (a Lotus Notes database named stconf.nsf) on the Sametime server that is accessed by a Web browser. This application is a central meeting place for members of the Sametime community. From the Sametime Meeting Center, you can schedule a meeting, start a meeting immediately, attend a meeting, and view information about scheduled and finished meetings.

Users access the Sametime Meeting Center database by clicking "Attend a Meeting" or "Schedule a Meeting" on the Sametime server home page.

**Note:** All scheduled meetings in Sametime are created in the Sametime Meeting Center. A user who starts an instant meeting from a contact list does not access the Sametime Meeting Center.
Anonymous access is allowed to the Sametime Meeting Center database by default. With anonymous access, users are not required to authenticate when accessing the Sametime Meeting Center. For more information about the implications of anonymous access to the Sametime Meeting Center, see Anonymous Access Settings for Community Services.

**Sametime administration terms and features**

This section provides brief descriptions of general Sametime administration terms that appear throughout this administrator’s guide. Sametime administrators should be familiar with these terms and features. Issues and administrative procedures associated with these terms are discussed in greater detail in subsequent chapters and topics of this administrator’s guide.

Some basic Sametime administration terms and features include:

- **Sametime server**
- **Sametime Administration Tool**
- **Community**
- **Domino Directory**
- **LDAP directory**
- **Self-registration**
- **Connectivity (firewall and proxy support)**
- **Broadcast**
- **Monitoring and logging**
- **Security**
- **SIP Gateway and SIP Connector**
- **Reverse proxy and portal server support**
- **Chat logging**
- **Sametime server clusters**
- **Name Conversion Utility**
- **StdebugTool.exe Utility**

**Sametime server**

The term “Sametime server” is used throughout the documentation to refer to a server that has both Sametime and Domino installed.

**Sametime Administration Tool**

The Sametime Administration Tool is an HTML and XML based application that runs in a Web browser. You open the Sametime Administration Tool by clicking “Administer the Server” on the Sametime server home page. The Sametime Administration Tool is the primary administration tool for the Sametime server. For more information about the Sametime Administration Tool, see Overview of the Sametime Administration Tool features.

During the Sametime installation, one user is specified as the administrator of the Sametime server. This administrator has access to the Sametime Administration Tool and all of its administrative features. The administrator specified during the installation can provide other administrators with access to the Sametime Administration Tool as needed.

The Sametime Administration Tool should be used to perform all administrative procedures on the Sametime server with the following exceptions:
• **Replication and creation of new Lotus Notes databases** - If a Sametime procedure requires you to replicate a database or create a new database, you must use a Lotus Notes or Domino Administrator client. The Sametime Administration Tool does not provide the functionality required to create one-time replicas (replica stubs) or other new databases, or set up replication schedules.

• **Managing LDAP users** - If you have configured Sametime to operate as a client to an LDAP server, you cannot use the Sametime Administration Tool to add or delete users in the LDAP directory on the LDAP server. Use the software provided with the LDAP server for management of the LDAP directory.

  **Note:** Although you cannot use the Sametime Administration Tool to manage users in an LDAP directory on a third-party server, you must use the Sametime Administration Tool to configure the Sametime server to access the LDAP directory on the third-party LDAP server.

• **Setting up Secure Sockets Layer (SSL) on the Sametime server** - If you want to configure the Sametime server so that all Web browser clients use the SSL protocol when connecting to the Sametime server, you must use a Lotus Notes client or the Domino Administrator client to set up SSL on the server.

• **Enabling a SIP gateway and deploying a SIP Connector** - If you want to allow users in your Sametime community to communicate with users in other instant messaging communities that support the SIP/SIMPLE protocol, you must use a Lotus Notes client to enable the Session Initiation Protocol (SIP) Gateway.

• **Implementing chat logging** - The chat logging feature can capture all chat conversations that occur on the Sametime server, including instant messages, chat conferences (chats involving more than two people), and Meeting Room chats. For more information about chat logging, see the Sametime Directory and Database Access Toolkit documentation available from IBM DeveloperWorks (http://www.ibm.com/developerworks/lotus/products/instantmessaging/). Follow the link for ‘Toolkits and Drivers.’

• **Creating Community Services clusters** - A Community Services cluster consists of multiple Sametime servers configured to operate together, providing failover and load balancing for the Sametime instant messaging and presence functionality. For more information see Overview of Community Services clustering.

• **Starting or stopping Sametime services** - You must use the Services settings in the Windows NT Control Panel or Windows 2000 Administrative Tools to start or stop a Sametime service.

## Community

The Sametime community refers to all users that have Web browser access to a Sametime server (or servers) and all Sametime servers that support those users. The Sametime community can be maintained in the Domino Directory on the Sametime Server or in an LDAP Directory on a third-party LDAP-compliant server.

Specifically, the Sametime community can be described as follows:

- A shared directory, or set of directories, that lists the people and groups of the community
- One or more Sametime servers that each have access to the shared directory or set of directories

For information on integrating multiple Sametime servers into a single community, see Deploying multiple Sametime servers.
**Domino Directory**
The Sametime server uses the Domino Directory of the Domino server on which Sametime is installed.

The Domino Directory is a database that serves as a central repository for information about Sametime users (or members of the Sametime community). The Domino Directory contains a separate Person document for each Sametime user. The Person document contains the User Name and Internet password required for authentication with the Sametime server. The Person document also contains a “Sametime server” field that is used to specify a user’s home Sametime server. The home "Sametime server” is the Sametime server a user connects to when logging in to the Community Services for presence and chat activity.

The Domino Directory also contains Group documents that hold lists of users that perform similar tasks. Group documents also define the Public Groups that end users can add to the Sametime Connect client presence list.

Other information stored in the Domino Directory includes server configuration information in the Server document, database configuration settings, and Access Control Lists (ACLs).

Person and Group documents, and ACLs within the Domino Directory, can be accessed from the Sametime Administration Tool.

Sametime administrators have the option of using the Domino Directory for user management or configuring Sametime to connect to an LDAP directory on an LDAP server for user management.

To maintain current information about users, groups, and servers in the Sametime community, the Community Services must receive periodic updates from the Domino Directory.

For more information about the Domino Directory, see Managing the Domino Directory

**LDAP directory**
The administrator can configure the Sametime server to connect to a Lightweight Directory Access Protocol (LDAP) server. This capability enables an administrator to integrate Sametime into an environment in which LDAP servers and LDAP directories are already deployed.

When Sametime is configured to connect to an LDAP server, the Sametime server searches and authenticates user names against entries in the LDAP directory on the third-party LDAP server. The LDAP directory replaces the Domino Directory as the user repository in the community. The community is defined by the users in the LDAP directory.

Sametime can access LDAP directories on multiple LDAP servers.

For more information, see Using LDAP with the Sametime server

**Self-registration**
The Sametime server includes a self-registration feature. This feature allows an end user to create a Person document that contains a User Name and Internet password in the Domino Directory on the Sametime server.
The self-registration feature is available to end users from the Register link of the Sametime server home page.

The administrator has the option of allowing or not allowing self-registration. Self-registration can reduce the workload for the administrator because it enables users to add themselves to the Domino Directory (create a Person document in the directory containing a User Name and Internet password). Allowing self-registration can involve security risks because it enables anonymous users to create records in the Domino Directory. These records permit anonymous users to authenticate with databases on the server.

Self-registration is not allowed by default. Also, self-registration cannot be used if Sametime is configured to operate with an LDAP directory.

For more information, see Using Sametime self-registration.

**Connectivity (firewall and proxy support)**

To engage in collaborative activities, the Sametime clients must connect to various services on the Sametime server, as described below:

- Web browsers connect to the HTTP Services on the Sametime server.
- The Sametime Connect client connects to the Community Services on the Sametime server.
- The Sametime Meeting Room client contains components that connect to the Meeting Services, Community Services, and Audio/Video Services.
- The Sametime Broadcast client connects to the Broadcast Services on the Sametime server.

The HTTP Services, Community Services, Meeting Services, Broadcast Services, and Audio/Video Services on the Sametime server listen for connections from clients on different TCP/IP ports. Because of the number of ports required to support the full range of collaborative activities, Sametime includes specially-designed connectivity features that enable Sametime clients to establish connections through firewalls and proxy servers.

Generally, the Sametime connectivity features enable Sametime clients to establish connections through HTTP and SOCKS proxy servers, or by using the HTTP connection method. If necessary, Sametime can be configured to listen for HTTP connections from all clients on port 80 to enable Sametime clients behind restrictive firewalls to connect to the Sametime server.

**Note:** The Sametime Connect client can also establish connections to the Community Services through an HTTPS proxy server.

For more information about enabling Sametime clients to connect through firewalls and proxy servers, see Configuring Sametime Connectivity.

For information about enabling Sametime servers to operate behind a reverse proxy server, see Using reverse proxy or portal servers with the Sametime server.

**Broadcast**

Sametime includes streaming technology that enables the server to broadcast meetings on the Internet or corporate intranet. Broadcast meetings can scale to extremely large audiences.
A Sametime Broadcast meeting includes two types of users: presenters and audience members. Presenters use the Sametime Meeting Room client to engage in interactive collaborative activities in a meeting. "Audience members" watch the actions of the presenters in a special view-only Sametime Broadcast client. The audience members can watch the meeting, but do not interact in the collaborative activities. The meeting experience for audience members in a Broadcast meeting is similar to watching television.

Broadcast Services on the Sametime server transmit screen-sharing and whiteboard Real-Time Protocol (RTP) data streams to the special view-only Sametime Broadcast clients. Audio and video RTP data streams can also be broadcast on the network and received by the Broadcast clients. Audience members can watch the screen-sharing or whiteboard activity of the presenters, view poll responses shared by the Moderator, view Web pages sent by the Moderator, view Meeting Room chat entered by the presenters, hear audio discussions, and see video images from the camera of the person currently speaking. However, Audience Members cannot interact with the Presenters. The Broadcast client used by the audience members contains no interactive capabilities.

The Broadcast media streams travel in only one direction, from the server to the Broadcast clients. Scalability is enhanced primarily because the Sametime server is not required to handle any incoming data from Audience Members. Broadcast meetings are very effective for company-wide presentations or any type of meeting where one person, or a small number of people, lecture or make presentations to a large audience.

For more information, see [About the Broadcast Services](#)

**Monitoring and logging**

The Sametime server provides monitoring and logging features that enable you to monitor the current status of the server and record (or log) information about server events and activities.

**Monitoring:** The Sametime server includes charts that allow you to monitor current Sametime server statistics. The monitoring charts, which are presented as tables, provide up-to-the-second information about Community Services, Meeting Services, Broadcast Services, Audio/Video Services, Web statistics, and free disk space on the server.

For more information, see [Using the Monitoring charts](#)

**Logging:** The Sametime server logging tools include the Sametime log and the Domino log. The Sametime log records events in the Sametime log database (stlog.nsf). The Sametime Administration Tool includes logging settings that enable you to control whether activities are logged to a database or to text files and to determine which activities are logged. If you log Sametime information to a database, you can view the Sametime log from the Sametime Administration Tool.

The Sametime Administration Tool also allows an administrator to launch the Domino Web Administration Tool to view the Domino log. The Domino log includes information about available memory and disk space, server performance, and databases that need maintenance.

For more information, see [Viewing the Sametime log](#)
Security
The Sametime server uses the Internet and intranet security features that are available on the Domino server on which it is installed. Generally, you use the Access Control Lists (ACLs) of databases on the Sametime server to provide users with anonymous access or basic password authentication to individual databases on the server. For example, you might want to set the ACL of the Sametime Meeting Center database (sconf.nsf) to require basic password authentication so that only authenticated users can create and attend meetings on the Sametime server.

To authenticate with the Sametime server, users must have a Person document that contains a User Name and Internet password in the Domino Directory on the Sametime server. The user is prompted for these credentials when logging in to the Sametime Connect client or accessing a Sametime server database that requires basic password authentication.

Note: If you have configured Sametime to connect to an LDAP server, users are authenticated using names and passwords stored in LDAP directory entries.

In addition to the Domino Internet and intranet security features, the Sametime server requires “authentication by token” security mechanisms to ensure that Sametime clients that establish connections to the Sametime services are authenticated. These security mechanisms include the Sametime Secrets and Tokens authentication databases and the Domino Single Sign-On (SSO) authentication feature.

You can also use Secure Sockets Layer (SSL) to encrypt Sametime HTTP traffic.

For more information, see [Working with Sametime security](#).

SIP gateway and SIP connector
Enabling the Session Initiation Protocol (SIP) Gateway and deploying a SIP Connector are optional procedures that you can perform if you want users in your Sametime community to share presence and instant messaging capabilities with users in other SIP-enabled communities.

You can enable this functionality to allow users in your community to communicate with users in another Sametime community that contains a Sametime server with the SIP Gateway functionality enabled.

Enabling the SIP Gateway functionality requires the installation of a separate component, the SIP Connector. For more information see [Enabling the Session Initiation Protocol (SIP) Gateway](#).

Reverse proxy and portal server support
A Sametime server can be deployed behind a reverse proxy server or a portal server. When a Sametime server is deployed on an internal network behind a reverse proxy server, the reverse proxy server operates as an intermediary between the Sametime server and the Sametime clients. All Sametime data flowing between the Sametime server and its clients passes through the reverse proxy server.

To accomplish its security objectives, a reverse proxy server manipulates the data that passes through it. The manipulation of Sametime data by the reverse proxy server imposes specific requirements and limitations on the use of reverse proxy servers with the Sametime server.
These limitations and requirements are discussed in detail in Using reverse proxy or portal servers with the Sametime server.

**Sametime server clusters**
The Sametime server supports Sametime server clustering. Sametime server clusters:
- Enhance server scalability and reliability to enable Sametime to meet the demands of large user populations.
- Provide load balancing and failover capabilities for Sametime Community Services and Meeting Services.

Sametime server clustering enables you to cluster the Community Services separately from the Meeting Services. For example, if you have three Sametime servers, you can have two separate clusters: a Community Services cluster and a Meeting Services cluster.

The two cluster types operate independently. The Community Services cluster provides load balancing and failover for the instant messaging and presence functionality. The Meeting Services cluster provides load balancing and failover for the Meeting Services functionality.

Clustering each of the services separately provides the flexibility to manage the Sametime functionality according to the needs of your company. For example, some companies might have a greater need for Community Services functionality than Meeting Services functionality while other companies have more need for the Meeting Services functionality than the Community Services.

To support flexibility in the deployment of your Sametime servers, you have three options when creating Sametime server clusters:
- You can cluster the Community Services without clustering the Meeting Services.
- You can cluster the Meeting Services without clustering the Community Services.
- You can cluster both the Community Services and the Meeting Services.

For more information about server clusters, including detailed information about each option for clustering the servers, see Introduction to Sametime Server Clusters and the Enterprise Meeting Server.

**Name Conversion Utility**
The names that appear in Sametime Connect client buddy lists and privacy lists are stored in a Domino database (vpuserinfo.nsf) on the Sametime server. If you change the user or group names that appear in the Domino or LDAP directory accessed by the Sametime server, you must run the Name Conversion Utility to make these same user and group name changes in the vpuserinfo.nsf database on the Sametime server. Running this utility ensures that the names that appear in buddy lists and privacy lists stay synchronized with the latest changes made to the directory. For more information, see Using the Name Conversion Utility.

**StdebugTool.exe utility**
You can use the StdebugTool.exe utility to produce trace files and create new trace file sets for troubleshooting purposes. These trace files contain debug messages that aid IBM Technical Support in troubleshooting Sametime server problems. If you have never worked with Sametime trace files before, you should use the StdebugTool.exe utility only under the guidance of IBM Technical Support. For more information, see Using the StdebugTool.exe utility.
Sametime clients

The collaborative activities in Sametime are accomplished through the interactions of client applications installed on users’ local machines with services on the Sametime server.

Administrators should be familiar with the following Sametime client applications:

- Web browsers
- Lotus Notes clients
- Sametime Connect client
- Sametime Meeting Room client
- Sametime Broadcast client

Web browsers

For information about Web browsers supported by the Sametime 7.0 server, see the *Lotus Sametime Server 7.0 Installation Guide*.

Lotus Notes clients

Users cannot access the Sametime server home page (stcenter.nsf) or the Sametime Meeting Center (stconf.nsf) with a Lotus Notes client. These databases are designed for Web browser access only.

Sametime Connect client

Sametime includes three versions of the Sametime Connect client:

- Sametime Connect for the desktop
- Sametime Connect for browsers
- Macintosh Sametime Connect for the desktop

The Sametime Connect for the desktop client be downloaded and installed on client computers that run the Windows operating system. A user downloads Sametime Connect for the desktop from a link on the Sametime server Download page. After it is installed, Sametime Connect for the desktop runs as a Windows application in the Windows operating system.

The Sametime Connect for browsers client is a Java applet that is launched from a link on the Sametime server home page. The Sametime Connect for browsers client runs in the user’s Web browser instead of on the Windows operating system.

Both Sametime Connect for the desktop and Sametime Connect for browsers contain a presence list (or contact list) that provides an entry point to all collaborative activities in Sametime. This contact list can display the name of any user that is online in the Sametime community. From the presence list, a user can select another user’s name to initiate an instant messaging session, a file transfer, or an instant meeting. Other users can be invited to join the chat or instant meeting.

Initiating an instant meeting from the contact list launches the Sametime Meeting Room client on a user’s machine. The Sametime Meeting Room client contains collaborative components that support screen-sharing, whiteboard, send Web page, polling, chat, and audio/video collaborative activities.

The Sametime Connect client contains features that enable a user to browse or search the Domino Directory on the Sametime server to add users or groups of users to the presence list.
Sametime Connect also includes privacy features that can prevent selected users from seeing you or contacting you when you are online. Records for the Sametime Connect privacy features are maintained in the Privacy (vpuserinfo.nsf) database on the Sametime server.

The Sametime Connect client includes its own Sametime Connectivity settings. Sametime Connect connects to the Community Services using TCP/IP on the default port 1533. Sametime Connect can also establish connections with the Community Services through HTTP, HTTPS, or SOCKS proxy servers. Sametime Connect clients can also use connectivity settings defined in a user’s web browser to establish connections to the Community Services on the Sametime server.

To log in to Sametime Connect, a user must enter the User Name and Internet password that has been specified in the user’s Person document in the Domino Directory. A Sametime Connect user is always logged into the server specified as the "home" Sametime server.

The Sametime Connect presence, instant messaging, privacy, directory browsing, and connectivity features are supported by the Community Services on the Sametime server.

The Macintosh Sametime Connect for the desktop client is provided on a Sametime server CD and is designed to run on the Macintosh operating system. The Macintosh Sametime Connect for the desktop includes the same features as the Sametime Connect for browsers client but does not support instant meetings. The Macintosh Sametime Connect for the desktop client is not available to end users by default and must be manually deployed by the administrator. For more information, see Deploying the Macintosh Sametime Connect client for the desktop.

**Sametime Meeting Room client**

The Sametime Meeting Room client contains the collaborative components required to interact in Sametime instant or scheduled meetings. This client is downloaded to a user’s local machine the first time a user attends a Sametime meeting. The user should respond Yes when prompted to trust IBM during this initial download. The Meeting Room client is cached on the user’s machine to improve response times when attending subsequent meetings.

The Sametime Meeting Room client is a Java applet that contains several Java collaborative components used in meetings. These collaborative components include:

- Participant List
- Public chat
- Screen sharing
- Shared whiteboard
- Send Web Pages
- Polling
- Hand raise
- IP audio
- IP video

The Meeting Room client loads in a user’s Web browser when the user attends an instant or scheduled meeting. The Meeting Room client must establish connections
with the Meeting Services on the Sametime server (on default port 8081) and the Community Services on the Sametime server (on default port 1533).

Generally, the Meeting Room client first attempts to establish a direct TCP/IP connection with a Sametime service on the Sametime server. If the direct TCP/IP connection attempt fails, the Meeting Room client attempts to establish connections using information in the Web browser proxy (or connectivity) settings, or uses a direct HTTP connection to connect to the Sametime services. For more information, see About Sametime Connectivity.

**Sametime Broadcast client**
The Sametime Broadcast client is a Java applet that receives Real-Time Protocol (RTP) data streams from Broadcast Services on the Sametime server. The Sametime Broadcast client is a receive-only client with no interactive capabilities. This client enables users to watch and listen to activity occurring in a broadcast meeting, but not to interact in the meeting.

The Broadcast client is downloaded to a user’s local machine the first time a user attends a Sametime broadcast meeting. The user should respond Yes when prompted to trust Lotus during this initial download. The Broadcast client is cached on the user’s machine and launched from the cache when the user joins subsequent broadcast meetings.

Initially, the Broadcast client attempts a direct RTSP TCP/IP connection to the Broadcast Services on the Sametime server on default port 554. Over this connection, the Broadcast client negotiates with the server to receive the Broadcast streams. The Broadcast client can also connect to the Broadcast Services through an HTTP or SOCKS proxy server, or by using a direct HTTP connection.

The Broadcast client can receive broadcast meeting streams through unicast UDP or multicast UDP. If UDP is not available on the network, the broadcast UDP streams can be tunneled using the direct TCP/IP connection, tunneled through an HTTP or SOCKS proxy server, or tunneled through a direct HTTP connection.

For more information, see About the Broadcast Services and Broadcast client connection process using JVM 1.4.2.

**Sametime services**
End users can engage in real-time collaborative activities through the interactions of Sametime client applications with various services on the Sametime server. This section briefly describes the Domino and Sametime services that support the real-time collaborative activities.

The services include:
- **Domino Services**
- **Community Services**
- **Meeting Services**
- **Broadcast Services**
- **Audio/Video Services**

**Domino Services**
Sametime uses the infrastructure and services of the Domino server on which it is installed. The following are the primary Domino services used by a Sametime server:
• Web server
• Directory
• Security
• Replication
• Database storage

Note: For information about the version of Domino on which Sametime must be installed, see the Lotus Sametime Server 7.0 Installation Guide.

The Domino server on which Sametime is installed should not be used as a Domino mail or application server. If Sametime is installed on its own Domino server, the real-time, interactive communication services of Sametime will not compete for resources with other high-demand Domino services.

In this documentation, the term "Sametime server" refers to the server that includes both Domino and Sametime.

Community Services
The Sametime Community Services support all presence (or awareness), text chat, and file transfer activity in a Sametime community. Any Sametime client that contains a presence list must connect to the Community Services. The Community Services clients include the Sametime Connect client, Participant List and public chat components of the Sametime Meeting Room client, or presence and chat applications developed from the Sametime Software Development Kit.

Basic functionality supported by the Community Services includes:
• Handling client login requests.
• Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or through HTTP, HTTPS, or SOCKS proxy servers.
• Providing directory access for user name search and display purposes.
• Providing directory access to compile lists of all Sametime servers and users in the community.
• Dissemination of presence chat and file transfer data to all users connected to Community Services.
• Maintenance and storage of privacy information, user preference settings, and presence lists for online users.
• Interacting with the Meeting Services to create meetings in which collaborative activities supported by the Community Services, Meeting Services, and Audio/Video Services are simultaneously available.
• Handling connections from the Community Services on other Sametime servers when multiple servers are installed. Server-to-server connections for the Community Services occur on default TCP/IP port 1516.

Note: Port 1516 is also used by the Meeting Services. In a multiple server environment, port 1516 must be open between two Sametime servers to enable a single Sametime meeting to be simultaneously active on both Sametime servers. This functionality is sometimes called “invited servers.” For more information, see Advantages of a single meeting on multiple servers.

• Logging of Community Services events to the Sametime log (stlog.nsf).
• Enabling a name entry prompt to appear when the ACL settings of the Sametime Meeting Center database (or any other database that includes
Sametime technology) allow anonymous access. This name entry prompt ensures that the presence list in the Sametime database can be displayed for the user.

- Capturing chat conversations that occur on the Sametime server for later retrieval. Developers must implement a chat logging feature to capture and retrieve chat conversations.

### Meeting Services

The Meeting Services include the T.120 multipoint communications software that supports screen sharing and the shared whiteboard, and the starting, stopping, and deletion of meetings. Meeting Services also support connections for the interactive audio/video components of the Sametime Meeting Room client.

Basic functionality supported by the Meeting Services includes:

- Creating and destroying meeting objects.
- Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or through HTTP, or SOCKS proxy servers.
- Dissemination of T.120 screen-sharing and whiteboard data among multiple users in a meeting.
- Maintaining lists of active, scheduled, and completed meetings.
- Starting and stopping instant and scheduled meetings at the appropriate times.
- Interacting with the Community Services to create meetings in which collaborative activities supported by the Community Services, Meeting Services, and Audio/Video Services are simultaneously available.
- Allowing the administrator to control which collaborative activities are available to end users of the Sametime server.
- Handling connections from the Meeting Services of other Sametime servers when a community includes multiple Sametime servers. Meeting Services server-to-server connections occur on TCP/IP ports 1503 and 1516.

**Note:** In a multiple server environment, port 1516 must be open between two Sametime servers to enable a single Sametime meeting to be simultaneously active on both Sametime servers. This functionality is sometimes called "invited servers." For more information, see Advantages of a single meeting on multiple servers.

- Logging Meeting Services events to the Sametime log (stlog.nsf).
- Provide the ability to record Sametime meetings in Sametime Record and Playback (RAP) files so that users can replay meetings after the meetings have ended.

### Broadcast Services

The Broadcast Services support the conversion of the following data into individual RTP streams for transmission on the network:

- Screen-sharing
- Whiteboard
- Meeting Room chat
- Polling
- Send Web Pages
- Audio and video

The Sametime Broadcast client is the only client of the Broadcast Services.

Basic functionality supported by the Broadcast Services includes:
Handling connections from the Sametime Broadcast clients using the Real Time Streaming Protocol (RTSP)
Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or through HTTP, or SOCKS proxy servers
Negotiations with the Broadcast clients to ensure the clients can receive the meeting streams
Identifying and attaching to broadcast meetings on the Sametime server
Transcoding screen-sharing/whiteboard data, Meeting Room chat/poll/send Web page data, audio data, and video data into RTP streams
Transmission of RTP streams using User Datagram Protocol (UDP), or tunneling UDP data within TCP or HTTP packets to ensure clients operating in a variety of different network environments can receive the streams
Multicasting of data streams when transmitting on multicast-enabled networks
Simultaneous broadcast of multiple meetings
Handling the playback of recorded meetings

Audio/Video Services
The Audio/Video Services of Sametime support all IP audio/video capabilities of Sametime.

The Audio/Video Services clients include the IP audio and video components of the Sametime Meeting Room client.

Interactive audio/video meetings can be bandwidth intensive. Also, too many interactive audio/video users can tax the system resources of the server and degrade the audio/video quality. Sametime allows the administrator to set limits on audio/video usage to ensure a good quality of service.

Connection Speed Settings are also available for the Audio/Video Services to ensure audio and video data can be transmitted at speeds that are acceptable for users with modem connections and users with LAN/WAN connections.

Basic functionality supported by the Audio/Video Services includes:
• Handling connections from Sametime Meeting Room clients
• Negotiation of audio/video capabilities with clients
• Detecting the person currently speaking (or detecting the source of an audio stream)
• Performing audio and video switching operations as different people speak in meetings
• Sequencing and transmission of audio and video data streams to multiple clients
• Transmission of audio and video data streams using the UDP transport
• Multicasting of audio and video data streams when transmitting on multicast-enabled networks
• Tunneling of UDP streams through TCP when UDP is unavailable on a network
• Full-duplex operation (includes two-way mixing of audio that allows two participants to speak simultaneously and be heard by all meeting participants)
The Lotus Enterprise Meeting Server (EMS)

The Lotus Enterprise Meeting Server (EMS) is an optional add-on product for a Sametime deployment that supports a Meeting Services cluster. A Meeting Services cluster consists of a group of Sametime server that work together to increase Meeting Services reliability by providing load balancing and server failover for Sametime meetings.

Note: The EMS is a separate application from the Sametime server and must be purchased separately from IBM. The EMS is not included with the Sametime server.

The EMS is a central component of a Sametime Meeting Services cluster. The EMS provides the end user interface, administration tool, and meeting management functionality for all Sametime servers in the Meeting Services cluster.

The EMS is built using Java 2 Platform, Enterprise Edition (J2EE) technologies. These technologies include Java servlets, JavaServer Pages (JSPs), Java applications, and a relational database. The J2EE infrastructure must be in place before you can deploy the EMS. Specifically, this release of the EMS requires the following J2EE infrastructure:

- IBM Universal Database V8.2.
- WebSphere MQ 5.3.0.8
- IBM WebSphere Application Server V5.1.1.2.

For more information about the EMS, see Introduction to Sametime Server Clusters, and the Web Conference Management server, What is the Enterprise Meeting Server?, and Setting up the Enterprise Meeting Server and a Meeting Services cluster.

Starting and stopping the Sametime server

The Sametime server is configured as a set of Windows services that stop and start automatically when the Domino server is stopped or started.

The procedure for starting and stopping a Sametime server is slightly different depending on whether Sametime is running on a Windows NT or Windows 2000 server.

Note: For information about starting and stopping a Sametime server that is installed on an IBM eServer iSeries or IBM pSeries server, see the installation guide (stinstall.nsf or stinstall.pdf) that shipped with the Sametime server.

Sametime on a Windows NT server

Follow the instructions below to start and stop a Sametime server that is running on a Windows NT server.

Starting the Sametime server

To manually start and stop the server from the Windows NT desktop:

2. In the Services dialog box, select Sametime Server and click Start.
Stopping the Sametime server
To manually stop the Sametime server from the Windows NT desktop:
2. In the Services dialog box, select Sametime Server and click Stop.

Sametime on a Windows 2000 server
Follow the instructions below to start and stop a Sametime server that is running on a Windows 2000 server.

Starting the Sametime server
To manually start and stop the server from the Windows 2000 desktop:
2. In the Services dialog box, select Services (Local).
3. Right-click “Sametime server” and select start.

Stopping the Sametime server
To manually stop the Sametime server from the Windows 2000 desktop:
2. In the Services dialog box, select Services (Local).
3. Right-click “Sametime server” and select Stop.
Chapter 2. Using the Sametime Administration Tool

This chapter describes the administrative features available from the IBM Lotus Sametime server administration tool (or Sametime Administration Tool) and provides step-by-step instructions for giving others access to the Administration Tool.

Starting the Sametime Administration Tool

The Sametime Administration Tool is an HTML and XML based application that enables you to administer the Sametime server using a Web browser.

Start the Sametime Administration Tool from the "Administer the Server" link of the Sametime server home page. You must enable Java applets and JavaScript™ or ActiveX® Controls in your browser to use the Sametime Administration Tool.

To start the Sametime Administration Tool from the Sametime server home page:
1. Start your browser.
2. Enter the URL for the Sametime server:
   \[http://hostname\]
   where \(hostname\) is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime server you want to administer.
3. From the Sametime server home page (Sametime Welcome page), click "Administer the Server."
4. Enter the administrator name and password specified during the Sametime server installation. The Sametime Administration Tool opens in its own Web browser window.

User name and password requirements

To access the Sametime Administration Tool, an administrator enters the user name and the Internet password specified on the administrator’s Person document in the Domino Directory on the Sametime server. The installation automatically creates a Person document containing a user name and Internet password for the person specified as the administrator.

The administrator specified during the installation can provide other administrators with access to the Sametime Administration Tool. To allow other users to access the Sametime Administration Tool, see Adding a new Sametime administrator.

Details: Starting the Sametime Administration Tool

To run the Sametime Administration Tool in Microsoft Internet Explorer, make the following changes in your browser. You must make these changes regardless of whether Microsoft Internet Explorer is installed on a client or server computer.
1. Select Tools - Internet Options.
2. Select the Advanced tab.
3. Clear the check mark from the "Use HTTP 1.1" option.
Set the default font in your browser to a small font size to ensure that all Command Group and Command names display in the space provided in the Sametime Administration Tool.

To view multiple versions of the Sametime Administration Tool at the same time (for example, to simultaneously monitor Community Services and Meeting Services connections), start additional copies of the browser and open the Sametime Administration Tool in each copy of the browser. Arrange the windows so all copies display on the screen.

---

**Overview of the Sametime Administration Tool features**

The Sametime Administration Tool includes six command groups: Server Overview, Message From Administrator, Monitoring, Logging, Directory, and Configuration. You can use the command groups to perform a variety of administrative tasks. The basic command groups and their features are briefly described below.

**Server Overview**

Use the Server Overview feature to ensure that the Sametime services are functioning as expected. For more information, see [Server Overview feature](#).

**Message From Administrator**

The Message From Administrator command group enables the Sametime administrator to send a message to all users who are currently logged into the Community Services from a Sametime client. For more information, see [Message From Administrator feature](#).

**Monitoring**

The Sametime server includes charts that allow you to monitor current Sametime server statistics. The monitoring charts provide up-to-the-second information about Community Services, Meeting Services, Broadcast Services, Audio/Video Services, Web statistics, and free disk space on the server. For more information, see [Monitoring the Sametime server](#).

**Logging**

The Sametime logging command group enables the Sametime administrator to log information about Sametime activity to a database on the server or to a text file. The administrator can also configure logging parameters to determine the types of events and activities that are recorded in the Sametime log. For more information, see [Logging Sametime activity](#).

**Directory**

The available Directory group features depend on whether the Sametime server uses a Domino Directory or an LDAP directory on an LDAP server.

If the Sametime server is using a Domino Directory, the Directory features enable the administrator to manage users by creating, editing, and deleting Person and Group documents in the Domino Directory on the Sametime server. The administrator can also open the Access Control Lists (ACLs) of databases on the Sametime server from the Domino Directory settings of the Sametime Administration Tool. The ACLs are used to manage security for databases on the Sametime server. For more information about using the Domino Directory, see [Directory](#).
Managing Users and Domino Directories] For more information about ACLs and Sametime security, see [Managing Security.

If the Sametime server is operating in an LDAP environment, the administrator can use the LDAP Directory settings of the Sametime Administration Tool to configure the Sametime server to operate as a client to an LDAP server. In this environment, the Sametime users are managed in an LDAP directory on an LDAP server. The Sametime server establishes a connection to the LDAP server and accesses LDAP directory entries to perform search and authentication operations on behalf of Sametime clients. The administrator can also open the Access Control Lists (ACLs) of databases on the Sametime server from the LDAP Directory settings of the Sametime Administration Tool. For more information, see [Managing Users and LDAP Directories].

**Configuration**

The Configuration command group allows the Sametime administrator to control the operation of the Sametime services and the connection ports and processes of Sametime clients. The Configuration features include:

- **Connectivity** - The Connectivity configuration settings control the ports on which the Sametime services listen for connections from clients. The Connectivity settings also provide features that enable Sametime clients to connect to the Sametime server through restrictive firewalls and proxy servers. For more information, see [Configuring Sametime connectivity].

  The Connectivity configuration settings also include “Servers in this Community” settings. These settings are used when you install multiple Sametime servers. For more information, see [Advantages of using multiple Sametime servers].

- **Community Services** - The Community Services configuration settings enable the administrator to ensure that the Community Services receive timely updates from the Directory. These updates are necessary to ensure that Community Services have recent information concerning new users and servers that have been added to the Directory. The administrator can specify the time intervals in which the Community Services receive updates from the Directory.

  The Community Services settings also enable the administrator to control whether the Windows or Web browser version of Sametime Connect is available to end users and whether end users are allowed to use the automatic login feature of Sametime Connect.

  The administrator also uses the Community Services configuration settings to set the maximum number of connections to Community Services, to allow or prevent end users from using Sametime to transfer files to one another, to set the maximum size allowed for file transfers, and to allow or prevent users from sending announcements (one-way unencrypted instant messages).

  The Community Services Anonymous Access settings force a name entry dialog box to appear when anonymous access is allowed to a Sametime database by the database ACL. This name entry dialog box enables the user to enter a name so that the user can be individually identified in presence lists. (Normally, a name entry dialog box does not appear when the ACL settings of a database allow anonymous access.) The Community Services Anonymous Access settings also determine whether anonymous users can search and browse the Directory. For more information, see [Anonymous Access Settings for Community Services].

- **Meeting Services** - The Meeting Services configuration settings allow the administrator to enable meetings to extend past scheduled end times, record lists of meeting attendees on the Meeting Details document in the Sametime Meeting
Center, and control the collaborative activities and end-user security features that are available for all meetings on the Sametime server.

Connection Speed Settings control the rates at which broadcast meeting streams and interactive audio/video streams are transmitted on the network for modem and LAN/WAN users.

- **Audio/Video** - The Audio/Video configuration settings enable the administrator to turn the audio/video features on and off, set the switching time for audio and video, set the buffer time for broadcast meetings, set Connection Speed Settings for Audio/Video clients, and limit the number of audio and video users. You might want to limit the number of audio and video users if consistently high numbers of audio and video users degrade server performance or consume too much network bandwidth. For more information, see Configuring Audio/Video Services.

**Server Overview feature**

Use the Server Overview feature to ensure that the Sametime services are functioning as expected.

**Services Status**

The Services Status list includes all Sametime services and their current status: Running or Not Running. You cannot start or stop any Sametime service from the Sametime Administration Tool. Use the Services settings in the Windows Control Panel or Windows Administrative Tools to start or stop a Sametime service. The names of the services in the Control Panel or Administrative Tools are identical to the names of the services in the Sametime Administration Tool.

Refresh your browser to get current statistics. The Overview lists do not update until you click Refresh. The date and time of the last update are listed above the Services Status table.

To access the Server Overview feature, click Server Overview in the Sametime Administration Tool.

**Message From Administrator feature**

Use the Sametime Administration Tool to simultaneously send a single message to all users currently logged in to Community Services from any Sametime client.

To send a message to all users currently logged in to Community Services:
1. From the Sametime server home page, click "Administer the Server."
2. Select Message From Administrator.
3. Enter the message in the text box provided.
4. Click Send. You receive a confirmation that your message was sent.

**Monitoring the Sametime server**

Sametime includes a variety of monitoring tools that provide up-to-the-second information about server activity and statistics. The Sametime monitoring tools display information about:

- General Server Status
- Logins
- Meetings and Participants
- Tools in Meetings
Logging Sametime activity
Sametime provides a variety of logging capabilities that enable the administrator to record information about Sametime server activity and statistics. You can record the following information in the Sametime log:

- Community Logins/Logouts
- Community Statistics
- Community Events
- Place Login Failures
- Meeting Login Failures
- Meeting Connections
- Server Connections
- Meeting Statistics
- Meeting Events
- Capacity Warnings
- Usage Limits

You can also view the Domino log from the Sametime Administration Tool. Use the Domino log to monitor:

- Available server disk space
- Available server memory
- Server load
- Server performance
- Databases that need maintenance

You can determine the format for the Sametime log and the content of the log in the [logging settings]. For more information about the Sametime log, see [Using the Sametime logging features].

Managing users and Domino Directories
Sametime uses the Domino Directory of the Domino server on which it is installed. Sametime can also use Domino Directory Assistance or the Domino Extended Server Directory Catalog feature to access secondary Domino Directories in the Domino environment.

To ensure that Sametime can successfully access the Domino Directory or Directories and interoperate in the Domino domain, review the following topics:

- Managing the Domino Directory
- Managing users in the Domino Directory
- How Sametime uses Domino Directory information

Managing users and LDAP directories
Sametime can be configured to connect to a third-party LDAP server and access an LDAP directory on the LDAP server. This capability enables you to integrate Sametime into an environment in which LDAP servers are already operating.

The Sametime [LDAP Directory Settings] ensure that the Sametime server can access the LDAP directory (or directories) on behalf of Sametime clients.
For detailed information on the procedures required to configure Sametime to operate as a client to an LDAP server, see:

- [Using LDAP with the Sametime server](#)
- [Setting up an LDAP connection](#)

Note: For information on using LDAP with a Sametime server that operates on a platform other than Windows (such as the IBM i5/OS or IBM pSeries servers), see the installation guide (stinstall.nsf or stinstall.pdf) that shipped with the Sametime server.

Sametime Administration Tool and LDAP environments
If the Sametime server is configured to operate as a client to an LDAP server, Sametime administrators are authenticated using Person documents in the Domino Directory.

Note: In the LDAP environment, only Sametime administrators (or users that access the Sametime Administration Tool) are authenticated against the Domino Directory. All other users are authenticated against an LDAP directory on a third-party server.

If you have configured Sametime to operate in an LDAP environment, you must maintain Person documents in the Domino Directory on the Sametime server for the administrators. When accessing the Sametime Administration Tool, the administrator must enter the last name or user name and the Internet password from the administrator’s Person document in the Domino Directory. For information on adding administrators in the LDAP environment, see [Adding a new Sametime administrator](#).

When operating in an LDAP environment, administrators cannot use the Sametime Administration Tool to add or modify users and groups in the LDAP directory on the third-party server. User accounts must be added and modified using the software and procedures required by the LDAP directory on the third-party server.

Configuring ports and network connectivity
If you have installed the Sametime server behind a firewall and all clients that will access the server are also behind the firewall, configuring network ports and connectivity might not be an issue.

However, if clients are required to cross firewalls or access the Sametime server through proxy servers, you might need to make adjustments to the Sametime Networks and Ports settings available from the Configuration - Connectivity options of the Sametime Administration Tool.

Sametime provides a variety of features that enable clients to connect through restrictive firewalls and proxy servers. Some of these features include:

- HTTP tunneling of Community Services, Meeting Services, and Broadcast Services data on port 80
- TCP tunneling of audio and video streams on port 80
- HTTP, HTTPS, and SOCKS proxy support for Sametime Connect client connections
- HTTP and SOCKS proxy support for Sametime Meeting Room client connections

...
• Set the ports on which Community Services, Meeting Services, Broadcast Services, and Interactive Audio/Video Services listen for connections from clients

• Reverse HTTP proxy support for the Sametime server

For detailed information about the ports used by the Sametime server and how Sametime clients connect through firewalls and proxy servers, review the list of topics in About Sametime Connectivity.

For additional information about connectivity, see Extending Sametime to Internet users.

Configuring Community Services

The Sametime Administration Tool includes several features that enable the administrator to control the behavior of the Community Services.

The Community Services administration features enable the administrator to:

• Configure the number of user names that appear on a page when users search or browse the Directory.

• Configure the time intervals at which the Community Services receive updates from a Domino or LDAP Directory. The Community Services must receive updates from the Directory at periodic intervals to ensure that users recently added to the directory can be displayed in presence lists. The Community Services must also maintain an updated list of all Sametime servers operating in the community.

• Configure the maximum number of client and server connections to Community Services.

• Allow users to authenticate using either Lightweight Third Party Authentication (LTPA) or Sametime tokens.

• Determine whether the links that enable users to access the Java version of Sametime Connect (Sametime Connect for browsers) and the Windows version of Sametime Connect (Sametime Connect for the desktop) are available.

• Allow users to transfer files to each other and set a maximum file size for transfers.

• Allow users to send announcements (unencrypted one-way instant messages).

• Determine whether end users can use the automatic login feature of Sametime Connect.

• Configure Anonymous Access:
  – Allow anonymous users to participate in meetings and enter virtual places.
  – Force a name entry dialog box to appear when anonymous access is allowed to a Sametime database by the database ACL. This name entry dialog box enables the user to enter a name so that the user can be individually identified in presence lists.
  – Set the default name that appears for anonymous users who do not use the name entry dialog box.
  – Determine the level of access that anonymous users have to the Directory.

For more information about the Community Services configuration settings, see Community Services configuration settings.

For information about connecting to the Community Services, see Community Services Network settings.
Configuring Meeting Services

The Sametime Administration Tool includes features that enable the administrator to control the behavior of the Meeting Services.

The Meeting Services administration features enable the administrator to:

- Automatically extend meetings past their scheduled end times to ensure a meeting does not end before the meeting is concluded.
- Add the names of meeting participants to the meeting details document after a meeting ends.
- Specify the collaborative activities and security features that are available for all meetings on the Sametime server.
- Control whether users can record meetings, specify a location for storing the recordings, and specify that Sametime stop recording meetings when a certain amount of disk space is left.
- Automatically encrypt all Sametime meetings.
- Require that all scheduled meetings use a meeting password.
- Specify the default Connection Speed Settings for scheduled and instant meetings.
- Specify the Connection Speed Settings for the screen-sharing and whiteboard data stream that is transmitted on the network during a broadcast meeting. These settings control the speed (or bit rate) at which screen-sharing and whiteboard data is transmitted on the network. The administrator can specify different rates for users with modem connections and users with LAN/WAN connections.
- Capture chat conversations that occur on the Sametime server. The chat-logging feature can capture all chat conversations that occur on the Sametime server, including instant messages, chat conferences (chats involving more than two people), and Meeting Room chats. Administrators must use the Sametime Software Development Kit to implement chat logging. For more information, see the IMWC Directory and Database Access Toolkit documentation available from IBM DeveloperWorks (http://www.ibm.com/developerworks/lotus/products/instantmessaging/). Follow the link for "Toolkits and Drivers."

For more information about the Meeting Services configuration settings, see [Meeting Services configuration settings](#).

For information about connecting to the Meeting Services, see [Network settings](#).

Configuring Audio/Video Services

The Audio/Video Services administration features enable the administrator to:

- Specify whether IP audio and video is available for all meetings on the server.
- Control switching intervals for audio and video.
- Specify a time to buffer data, audio, and video during broadcast meetings.
- Specify the Connection Speed Settings for interactive audio/video and broadcast meetings. These settings control the speed (or bit rate) at which audio and video streams are transmitted on the network. The administrator can specify different rates for users with modem connections and users with LAN/WAN connections.
- Set the bit rate for screen-sharing and whiteboard data during broadcast meetings.
• Set the audio/video jitter buffer.
• Set the number of audio frames per packet.
• Set audio/video usage limits that limit the number of users simultaneously using audio/video. Too many audio/video users can adversely affect the performance of the server and significantly increase network bandwidth usage. Limiting the number of users enables the administrator to control network bandwidth usage and ensure an acceptable level of server performance.

For more information about configuring the Audio/Video Services, see Audio/Video Services configuration settings.

For information about connecting to the Audio/Video Services, see Interactive Audio/Video Network settings.

Additional administrative tasks

The following administrative tasks require you to use a combination of command groups in the Sametime Administration Tool or to use tools other than the Sametime Administration Tool.

• Configuring Broadcast Services
• Deploying multiple Sametime servers
• Managing users and LDAP Directories
• Managing Security
• Enabling the Session Initiation Protocol (SIP) Gateway
• Chat logging

Note: If a Sametime procedure requires you to replicate a database or create a new database, you must use a Lotus Notes or Domino Administrator client. The Sametime Administration Tool does not provide the functionality required to create one-time replicas (replica stubs) or other new databases or set up replication schedules.

Configuring Broadcast Services

The Sametime Administration Tool includes features that enable the administrator to control the behavior of the Broadcast Services.

The Broadcast Services administration features enable the administrator to:

• Specify the time to buffer broadcast data. Broadcast data can be held in a Sametime Broadcast client buffer for a brief period of time. Buffering data ensures that network congestion does not affect the playout of broadcast meeting streams in the Broadcast client.
• Enable the Broadcast Services to operate on a multicast-enabled network.
• Set Connection Speed Settings that control the amount and speed (or bit rate) of the data that the Broadcast Services transmit on the network. The administrator can specify different rates for users with modem connections and users with LAN/WAN connections.

For more information on the Broadcast Services configuration settings, see Configuring the Broadcast Services settings.

For information on connecting to the Broadcast Services, see Broadcast Services Network settings.
Deploying multiple Sametime servers

A Sametime community can include more than one Sametime server. If you have a large number of Sametime users, you can install multiple Sametime servers for load balancing and to reduce network bandwidth usage. You can also install multiple Sametime servers to securely allow Internet clients to attend meetings conducted on servers inside your firewall.

Before adding another Sametime server to your Sametime community, you should review the information in the Deploying multiple Sametime servers section of this documentation. This documentation contains information about:

• Installing multiple Sametime servers
• Synchronizing multiple Sametime servers to operate as a single community
• Enabling Internet clients to operate in meetings conducted on internal Sametime servers
• Techniques that can be used to extend a single Sametime community across multiple Domino domains

For more information, see Advantages of using multiple Sametime servers

Managing security

After you have installed and set up the Sametime server, you might want to review the available security features and default security settings of the Sametime server.

Sametime offers several features to enhance security. Some of the administrative tasks associated with enhancing security include:

• Turning off anonymous access to the Sametime Meeting Center - By default, the Sametime server allows anonymous access to the Sametime Meeting Center database (stconf.nsf). Anonymous access allows any unauthenticated user to create meetings in the Sametime Meeting Center. You can turn off anonymous access to the Sametime Meeting Center so that only authenticated users can create and attend meetings in the Sametime Meeting Center.

For information about anonymous access to the Meeting Center, see Anonymous and guest access to the Sametime Meeting Center

• Deciding whether to encrypt all meetings - Data that passes between the server and the Sametime Meeting Room clients can be encrypted using 128-bit RC2 encryption. For more information, see Encryption and meeting passwords.

• Requiring all Sametime meetings to have a password - The administrator can force users to specify a meeting-specific password for every new meeting that is created in the Sametime Meeting Center. For more information, see Requiring all scheduled meetings to have a password.

• Administering the Domino Single Sign-On (SSO) feature - The Domino SSO feature is enabled by default during a Sametime installation. The authentication tokens created by this feature are required to authenticate client connections to the Sametime services. In some cases, it may be necessary for the administrator to perform additional configurations following the Sametime server installation to ensure the Domino SSO feature is configured correctly. For more information, see Authentication by token using LTPA and Sametime tokens.

• Enabling the SametimeSecretsGenerator Agent - For added protection against hackers or other outside attacks, the administrator can enable the
Maintaining the Sametime Meeting Center

To ensure the Meeting Center operates efficiently, the administrator should prevent the number of Meeting Details documents in the IBM Lotus Sametime server Meeting Center database from growing too large.

The Sametime Meeting Center database (stconf.nsf) provides several different views (such as “Scheduled,” “Finished,” “Today,” and “All Meetings”) that enable an end user to quickly locate meetings in the Meeting Center. The user selects a specific view in the Meeting Center and then clicks on a meeting name to view the Meeting Details document for that meeting.

When a user selects a view in the Meeting Center, Sametime builds the view by parsing through the Meeting Details documents of active meetings, scheduled meetings, and finished meetings. If there is a large number of Meeting Details documents, the parsing process takes longer, and end users experience slower performance when using the Sametime Meeting Center.

To prevent this problem, the Sametime Meeting Center database includes a “PurgeMeetings” agent that automatically deletes Meeting Details documents from the Sametime Meeting Center when the documents reach a certain age. This agent is disabled by default.

To enable this agent and optimize Meeting Center performance, the administrator should:

- Archive the current Meeting Center database or Meeting Details documents (optional).
- Enable the PurgeMeetings agent in the Meeting Center database.
- Periodically compact the Meeting Center database.

Note: The size of the Sametime Meeting Center database is limited to 1GB, but you should keep it below 800 MB for optimal performance. For additional information on performance issues, visit the Web site www.lotus.com/sametime and click the About Sametime link. Lotus publishes white papers about performance issues on this Web site.

Archiving Meeting Details documents

Before enabling the PurgeMeetings agent, decide how to archive the Meeting Details documents so that back up copies are available after the documents are deleted from the Meeting Center. To archive Meeting Details documents:

- Lotus software recommends setting up a one-way replication of the Meeting Center database (stconf.nsf) from the Sametime server to a Domino server (preferably a Domino server that is reserved for database storage).
Setting up a one-way replication ensures that a backup replica of the Meeting Center database exists in case you need to get a copy of a Meeting Details document after the document has been deleted by the agent.

- You can also create an agent that moves the Meeting Details documents from the Sametime Meeting Center to a database on a different server after the documents reach a certain age. The standard IBM Lotus Notes Mail templates have archiving agents that provide examples for creating your own custom archiving agents.

**Enabling the PurgeMeetings agent (deleting Meeting Details documents)**

Enabling the PurgeMeetings agent to delete Meeting Details documents involves two tasks:

- Enabling the PurgeMeetings agent from the Notes client
- Setting the STPurgeMeetingPastDays Notes.ini parameter - This parameter specifies the age of documents the agent will delete.

**Enabling the PurgeMeetings agent from a Notes client**

Perform the following procedure to enable the PurgeMeetings agent.

1. From a Lotus Notes client, choose File - Database - Open:
   a. In the Server drop-down list, select the Sametime server.
   b. In the Filename text box, type `stconf.nsf`.
   c. Click Open.
2. From the Sametime Meeting Center database, select the View - Agents menu option.
3. Right click on the PurgeMeetings agent and select Enable or click the "Enable" button on the top of the agent view.
4. Close the Sametime Meeting Center database.
5. Set the STPurgeMeetingPastDays Notes.ini parameter, as described below.

The agent runs once each day. The agent deletes all Meeting Details documents that have a meeting state of "finished" or "failed" and have reached the age specified in the STPurgeMeetingPastDays parameter in the Notes.ini file.

**Setting the STPurgeMeetingPastDays Notes.ini parameter**

The STPurgeMeetingPastDays= parameter in the Notes.ini file on the Sametime server specifies the age (in days) of Meeting Details documents that are deleted from the Sametime Meeting Center by the PurgeMeetings agent.

**Note:** The PurgeMeetings agent does not run if you specify a setting of 0 (zero) for the STPurgeMeetingPastDays= Notes.ini setting.

To set the STPurgeMeetingPastDays parameter in the Notes.ini file:

1. Use a text editor to open the Notes.ini file in the C:\Lotus\Domino directory on the Sametime server.
2. In the Notes.ini file, locate the STPurgeMeetingPastDays= setting.
   - If the STPurgeMeetingPastDays= setting does not exist in the Notes.ini file, you must use a text editor to manually type the setting into the Notes.ini file.
3. For the STPurgeMeetingPastDays setting, specify the age in days of documents that you want the PurgeMeetings agent to delete from the Sametime Meeting Center.
For example, a setting of STPurgeMeetingPastDays=30 indicates that Meeting Details documents that are 30 days old are deleted from the Sametime Meeting Center.

4. Save and close the Notes.ini file.

**Compacting the Meeting Center database**

You should also compact the Sametime Meeting Center database periodically. Compacting a database ensures that space in the database is reused efficiently after documents are deleted from it.

Use the -B compact option when compacting the database. This option ensures that the space in the database is reused most efficiently and that the database is reduced in size.

It is not necessary to stop the Sametime server when compacting the Meeting Center database. However, users cannot access the Meeting Center database while it is compacting. You should compact the Meeting Center database when server usage is at its lowest.

**Note:** Avoid using the -D (Discard any built view indexes) and -R (Keep or revert database back to Release 4 format) options when compacting the Sametime Meeting Center. Also avoid using any of the Advanced compacting options.

For more information on compacting databases, see the *Domino Administration Help* database available from www.lotus.com/ldd or the help directory on a Domino server.

**Adding a new Sametime administrator**

A Sametime administrator name and password is specified during the Sametime installation and setup process. The administrator specified during the Sametime server installation and setup can access all features of the Sametime Administration Tool and can provide other administrators with access to the Sametime Administration Tool.

The recommended method for adding new administrators is to create an Administrators Group document. Add this Administrators Group to the ACLs of the appropriate Sametime databases and to the appropriate fields in the Server document of the Sametime server.

After you have added the Administrators Group document to the appropriate database ACLs and the appropriate fields on the Server document, you can add or remove an administrator by adding or removing a name from the Administrators Group document.

**Allowing others to access the Sametime Administration Tool**

To allow others to access the Sametime Administration Tool, perform the following tasks:

1. **Create a Person document for the administrator (if necessary)**
2. **Create an Administrators Group document**
3. **Add the Administrators Group document to Sametime database ACLs**

   Generally, you provide the Administrators Group with the Manager access level in the ACL of all Sametime databases, and provide the Administrators Group with all roles available in the database ACL.
4. **Modify the Server document of the Sametime server.** You must add the Administrators Group to the "Administrators" and "Run unrestricted methods and operations" fields in the Server document of the Sametime server.

5. **Edit the Administrators Group document** to allow or revoke access to the Sametime Administration Tool.

**Note:** If the new administrator uses Microsoft Internet Explorer to access the Sametime Administration Tool, the administrator must disable the "Use HTTP 1.1" setting in the Tools - Internet Options - Advanced tab of the Web browser.

**Using individual names instead of an Administrators Group**

You can also use the instructions in steps 1, 3 and 4 above to add individual user names to the database ACLs and the fields of the Server document.

**Note:** If the Sametime server is configured to use SSL for Web browser connections to the HTTP server, you must use the individual names of administrators in the database ACLs. If SSL is enabled, and the administrator is listed only as a member of a group in database ACLs, the administrator will be unable to log in to the Sametime Administration Tool.

If you use individual names instead of a Group document, you must repeat steps 1, 3, and 4 for each user. This is a more cumbersome method of providing access for administrators, but it allows you to use database roles to control the types of administrative tasks that each administrator can perform. If you use a Group document, every administrator entered in the Administrators Group document will have the same level of access to the Sametime Administration Tool.

**Create a Person document for the administrator**

This procedure is the first of five required when adding a new Sametime administrator. In this procedure, you create a Person document in the Domino Directory for the Sametime administrator. If the administrator whom you are adding already has a Person document that contains a last name, user name, and Internet password, skip this procedure.

To create a Person document from the Sametime Administration Tool:

1. From the Sametime server home page, click "Administer the Server."
2. From the Sametime Administration Tool:
   - If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino.
   - If you are using an LDAP directory with the Sametime server, select LDAP Directory.
3. Choose "Add Sametime Administrators - Create a record for each person who will be an administrator."
4. Choose Add Person.
5. In the Person document, select the Basics tab.
6. Enter the user’s first, middle, and last name in the appropriate fields. Only the last name is required.
7. Enter a name for the user in the User Name field. An entry in this field is required for the user to authenticate with the Sametime server.
You can use any of the following characters in a user name: A - Z, 0 - 9, ampersand (&), dash (-), period (.), underscore (_), apostrophe ('), and space. Using other characters can cause unexpected results.

8. Enter an Internet password for the person in the "Internet password" field. An entry in this field is required for the user to authenticate when accessing the Sametime Administration Tool. There are no restrictions on the number of characters used in the Internet password.

9. Click "Save & Close." The Person document is added to the Directory.

**Next step**

After creating the Person document for the administrator, create an Administrators Group document.

### Create an Administrators Group document

This procedure is the second of five required when adding a new Sametime administrator. In this procedure, you create a group document to hold the names of Sametime administrators.

To create an Administrators Group document:

1. From the Sametime server home page, click "Administer the Server."
2. From the Sametime Administration Tool:
   - If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino.
   - If you are using an LDAP directory with the Sametime server, select LDAP Directory.
3. Choose "Add Sametime Administrators -Create a group for the administrators."
4. Click Add Group.
5. Enter a name for the group in the "Group name" field (for example, "Administrators" or "Sametime Administrators").
6. For group type, select Multipurpose.
7. (Optional) Enter a description of the group in the Description field.
8. In the Members field, list the names of users you want to access the Sametime Administration Tool.
   Make sure to enter the name exactly as it is entered in the topmost entry of the "User name" field of a user’s Person document.
10. Enter the names of the group owners in the Owners field. Generally, the group owner is the administrator creating the group. Only the administrator listed in the Owners field can modify this Group document. If the Owners field is blank, any administrator can modify this Group document.
11. Click "Save & Close."

**Next step**

After creating the Administrators Group document, add the Administrators Group document to the ACLs of the appropriate Sametime databases.

### Add the Administrators Group document to Sametime database ACLs

This procedure is the third of five required when adding a new Sametime administrator. In this procedure, you add the Administrators Group document (or
the name of an individual user) to Sametime database Access Control Lists (ACLs) and provide the Manager access level to the Group (or individual user).

In addition to ACL access levels, you must also specify the ACL privileges and roles that the Administrators Group (or an individual user) has in each database. Generally, for an Administrators Group, select all ACL privileges and roles available when adding the Group to a Sametime database ACL. Selecting all ACL privileges and roles provides any administrator listed in the Administrators Group document with access to the full range of administrative features available from the Sametime Administration Tool.

**Note:** If you are adding individual user names to Sametime database ACLs instead of a group name, database roles can be used to prevent or allow access to specific features of the Sametime Administration Tool. For more information, see [Roles in Sametime database ACLs](#).

Add the Administrators Group to the ACLs of the following Sametime databases.

- **Sametime Configuration (stconfig.nsf)** - Stores the configuration parameters that are set from the Sametime Administration Tool.
- **Domino Directory or Address Book (names.nsf)** - Stores Person and Group documents, ACL settings, and other configuration information for the Domino/Web Application Services.
- **Sametime Online Meeting Center (stconf.nsf)** - Provides a central meeting place on the Sametime server.
- **Sametime Log (stlog.nsf)** - Stores logging information.
- **Sametime Self Registration (streg.nsf)** - Enables end users to add Person documents to the Domino Directory. These Person documents contain the credentials required to authenticate with the Sametime server.
- **Domino Web Administration (webadmin.nsf)** - Contains the Domino Web Administration client, which includes monitoring features for the HTTP Services and free disk space. This is the full Domino Web Administration client that is included with Domino servers.

Follow the instructions below to add the Administrators Group document (or an individual user’s name) to the ACLs of the Sametime databases and make the appropriate ACL settings in each database.

1. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
2. Choose "Add Sametime Administrators -Give the administrator group Manager access for all appropriate databases, such as stconf.nsf and stcenter.nsf." The Access Control options appear.
3. From the Databases list, select Sametime Configuration (stconfig.nsf).

**Note:** The database filename appears below the Databases list.

4. Click the Access button.
5. Click the Add button. Enter the Administrators Group document name in the dialog box (for example, "Administrators" or "Sametime Administrators").
If you are adding individual user names, enter the person’s user name in the
dialog box. Enter the name as it is entered in the top entry of the "User name" field on the user’s Person document.

6. Click OK.
7. Select the Administrators Group name (or individual person’s name) from the list in the Database Security window.
8. In the User Type drop-down list, select Group (or Person if you are adding an individual user’s name).
9. In the Access drop-down list, select Manager.
10. Make sure that all ACL privileges, such as "Create documents" and "Delete documents," are selected.
11. Click the Roles button.
12. If you want the Administrators Group to have access to the full range of administrative functions, select all roles. Click OK.
   The roles determine which administration tasks the members of the group can perform. If you are adding individual user names to the ACLs, you can use the roles to control the administrative features that are available to individual administrators. For more information, see Roles in Sametime databases ACLs.
13. Click Submit.
14. After adding the Administrators Group to the ACL of the Sametime Configuration database (stconfig.nsf), repeat steps 4 through 14 to add the Administrators Group to the ACL of each of the Sametime databases listed below:
   • Domino Address Book or Domino Directory (names.nsf)
   • Sametime Online Meeting Center (stconf.nsf)
   • Sametime Log (stlog.nsf)
   • Sametime Self Registration (streg.nsf)
   • Domino Web Administration (webadmin.nsf)
   If you are adding an Administrators Group document, for each of the databases above, be sure to select the Manager access level and all ACL privileges and roles as described in steps 9 through 12.
   If you are adding individual user names, you can specify different roles for each user.

Next step
After adding the Administrators Group document (or individual user names) to the database ACLs, you must modify the Server document of the Sametime server.

Modifying the Server document of the Sametime server
This procedure is the fourth of five required when adding a new Sametime administrator. In this procedure, you add the Administrators Group document (or the name of an individual user) to two fields on the Server document. The two fields are the "Administrators" field and "Run unrestricted methods and operations" field in the Security section of the Server document.

To add users to the fields on the Server document of the Sametime server:
1. From the Sametime Administration Tool:
   • If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   • If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
2. Choose "Add Sametime Administrators - Edit the Server document."
3. Click Security.
4. In the "Administrators" field of the Administrators section, type the name of the Administrators Group (or enter the name of an individual user).

   Note: Type a group name exactly as it appears in the Group document. If you are entering an individual user name in this field, type the user name exactly as it is entered in the topmost entry of the "User name" field on the Person document. Separate multiple entries in the "Administer the server from a browser" field with commas.
5. In the "Run unrestricted methods and operations" field of the Programmability Restrictions section, type the Administrators Group name (or an individual user's name). Separate multiple entries in this field with commas.
6. Click "Save & Close."

Next step
The fifth procedure explains how to edit the Administrators Group document (add or remove a user's name from the Group document) to allow or revoke access to the Sametime Administration Tool.

Adding and removing names from an Administrators Group document

This procedure is the last of five required when adding a new Sametime administrator. If you created an Administrators Group document to provide others with access to the Sametime Administration Tool, you can control access to the Sametime Administration Tool by editing the Group document. Adding a user's name to the Administrators Group document provides the user with access to the Sametime Administration Tool. Removing a user's name from the Group document revokes the user's access to the Sametime Administration Tool.

To add or remove a user's name from the Administrators Group document:
1. From the Sametime server home page, click "Administer the Server."
2. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
3. Choose "Add Sametime Administrators - Create a group for the administrators."
4. Double-click a group name.
5. Select Edit Group.
6. In the Members field, add or remove a user's name from the Group document. If you add a user's name, the user must have a Person document in the Domino Directory that contains a last name, user name, and Internet password. Make sure to enter the name exactly as it is entered in the top entry of the "User name" field of a user's Person document. The user must enter a last name or user name and the Internet password from the Person document to access the Sametime Administration Tool.
7. Click "Save & Close."
Roles in Sametime database ACLs

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool. For example, the Sametime Configuration database (stconfig.nsf) ACL contains three roles: ServerMonitor, ServerAdmin, or DatabaseAdmin. If you assign only the ServerMonitor role to an administrator, the administrator can monitor server memory, disk space, and other server statistics but cannot perform any other administrative functions. Assign all roles to an administrator if you want the administrator to have full access to all administrative functions.

Access Control List (ACL) roles are defined in the following Sametime databases:
- **Sametime Configuration database (stconfig.nsf)**
- **Domino Directory or Address Book (names.nsf)**
- **Sametime Meeting Center (stconf.nsf)**
- **Domino Web Administration (webadmin.nsf)**

### Roles in the Sametime Configuration database (stconfig.nsf)

The Sametime Configuration database (stconfig.nsf) stores the values for parameters that are available from the Sametime Administration Tool. The roles in this database affect the administrative tasks that an administrator can perform from the Sametime Administration Tool.

The following table lists the commands and features available with the Sametime Administration Tool and the roles that an administrator must be assigned in the stconfig.nsf database to use the Sametime Administration Tool commands and features. If an administrator does not have the appropriate roles, the Sametime Administration Tool does not display the command.

**Note:** The SametimeAdmin role allows the administrator to perform all tasks in the Sametime Administration Tool.

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Command or feature</th>
<th>Role required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message From Administrator</td>
<td>Sends message to all users logged into Community Services</td>
<td>None</td>
</tr>
<tr>
<td>Monitoring</td>
<td>All monitoring features</td>
<td>[ServerMonitor] or [SametimeAdmin]</td>
</tr>
<tr>
<td>Logging</td>
<td>All logging features</td>
<td>[ServerMonitor] or [SametimeAdmin]</td>
</tr>
<tr>
<td>Directory</td>
<td>Add Users, People, Groups</td>
<td>[SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Directory</td>
<td>Access Control Lists (ACL)</td>
<td>[DatabaseAdmin] or [SametimeAdmin]</td>
</tr>
<tr>
<td>Configuration</td>
<td>Connectivity, Community Services, Meeting Services, Audio/Video Services</td>
<td>[SametimeAdmin] or [ServerMonitor]</td>
</tr>
</tbody>
</table>

A user with the ServerMonitor role can view settings available from these commands but cannot change the settings.

| Help                         | Online help for administrators                                                    | No roles required                      |

Chapter 2. Using the Sametime Administration Tool 45
Roles in the Domino Directory (names.nsf)

The Domino Directory (or Address Book) contains the Person and Group documents that you create and edit when you use the Sametime Administration Tool. The roles in the Domino Directory determine who can create or edit a particular type of document in the Directory.

The Domino Directory also contains the Server document that you access to provide another user with administrative privileges to the Sametime Administration Tool.

Note: If you use Sametime in a Domino environment, the Domino Directory roles function the same as they do on Domino servers.

The Domino Directory contains eight roles. The privileges for each role are listed in this table:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserCreator</td>
<td>Allows an administrator to create Person documents in the Domino Directory</td>
</tr>
<tr>
<td>UserModifier</td>
<td>Allows an administrator to edit all Person documents in the Domino Directory</td>
</tr>
<tr>
<td>GroupCreator</td>
<td>Allows an administrator to create Group documents in the Domino Directory</td>
</tr>
<tr>
<td>GroupModifier</td>
<td>Allows an administrator to edit all Group documents in the Domino Directory</td>
</tr>
<tr>
<td>ServerCreator</td>
<td>Allows an administrator to create Server documents in the Domino Directory</td>
</tr>
<tr>
<td>ServerModifier</td>
<td>Allows an administrator to edit all Server documents in the Domino Directory</td>
</tr>
<tr>
<td>NetCreator</td>
<td>Not used by Sametime</td>
</tr>
<tr>
<td>NetModifier</td>
<td>Not used by Sametime</td>
</tr>
</tbody>
</table>

Roles in the Sametime Meeting Center (stconf.nsf)

The Sametime Meeting Center database contains only the Sametime Admin role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Admin</td>
<td>Allows an administrator to see hidden meetings displayed in the All Meetings view of the Meeting Center.</td>
</tr>
<tr>
<td></td>
<td>Allows an administrator to see the Hidden Meetings view in the Meeting Center. This view displays only hidden meetings.</td>
</tr>
<tr>
<td></td>
<td>Allows the administrator to alter the meeting details of any meeting. For example, the administrator can delete or change the end time of a meeting that the administrator did not create.</td>
</tr>
<tr>
<td></td>
<td>Allows an administrator to see and use the &quot;Delete the Recording,&quot; &quot;Export the Recording,&quot; &quot;Replace the Recording,&quot; and Import Recording options in the Meeting Center forms. These features enable the administrator to manage the recorded meeting files if the administrator makes the Record and Playback feature available on the Sametime server.</td>
</tr>
</tbody>
</table>
Roles in the Domino Web Administration database (webadmin.nsf)

The Domino Web Administration database is available on the Sametime server to enable administrators to monitor the HTTP server and access logging information about the Domino Application Services.

The following table defines the roles in the Domino Web Administration database:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerAdmin</td>
<td>A Sametime administrator requires this role to access the Server document when providing other users with access to the Sametime Administration Tool.</td>
</tr>
<tr>
<td>ServerMonitor</td>
<td>A Sametime administrator requires this role to access the Monitoring - Miscellaneous functions of the Sametime Administration Tool. These monitoring functions enable the administrator to monitor HTTP commands and requests, server memory usage, and free disk space. The Sametime administrator also requires this role to access the Logging - Domino Log functions of the Sametime Administration Tool, which report information about the Domino Application Services.</td>
</tr>
<tr>
<td>DatabaseAdmin</td>
<td>A Sametime administrator requires this role to change database ACLs from the Sametime Administration Tool.</td>
</tr>
<tr>
<td>FileRead</td>
<td>This feature provides access to the Configuration - System Files (read-only) command of the Domino Web Administration Tool. This feature is usually not used with Sametime.</td>
</tr>
<tr>
<td>FileModify</td>
<td>This feature provides access to the Configuration - System Files (read/write) command. This feature is usually not used with Sametime.</td>
</tr>
</tbody>
</table>
Chapter 3. Using Domino Directories

This chapter discusses issues pertaining to using Domino Directories with the IBM Lotus Sametime server.

If you have configured the Sametime server to operate as a client to an LDAP server, the Domino Directory is not used for user management. For information about using Sametime in an LDAP environment, see Chapter 4, "Using LDAP Directories with Sametime."

Managing the Domino Directory

The Sametime community consists of users and Sametime servers that are registered in the Domino Directory (or Directories) in use in the Domino domain in which Sametime is installed.

This section includes the following information concerning Domino Directory management:

- Basic Domino Directory requirements
- Managing multiple Directories with Sametime
- Directory security considerations
- Using an LDAP directory instead of a Domino Directory

Basic Domino Directory requirements

Every Domino server has a primary Directory in which the server is registered. When you install Sametime on a Domino server, Sametime uses the primary Directory of that Domino server. The primary Directory must always exist on the Sametime server.

Note: The primary Directory must exist on the Sametime server even if you set up Directory Assistance or an Extended Server Directory Catalog to access secondary Directories in the environment.

Sametime administrators should be aware of the following basic issues concerning Directory management:

- The Person document for each user in the Directory must contain entries in the "User name," "Internet password," and "Sametime server" fields. For more information, see Person documents.
- Group documents in the Directory can be used to simplify the process of adding users to the contact list in the Sametime Connect client. For more information, see Group documents.
- The Server document for the Sametime server requires specific values for the "Server name," "Is this a Sametime server," "Port," and "Net Address" fields to support online presence. For more information, see The Server document.
- You must ensure that Sametime agents can access the Domino Directory and run unrestricted methods and operations on the Sametime server. For more information, see Directory security considerations.

For more information, see How Sametime uses Domino Directory information.
Managing multiple Domino Directories with Sametime

Every Domino server has a primary Directory in which the server is registered. When you install Sametime on a Domino server, Sametime uses the primary Directory of that Domino server. The primary Directory must always exist on the Sametime server.

If the Sametime server is installed into a Domino environment that uses multiple Directories, the administrator should replicate the primary Directory to the Sametime server.

To access additional Domino Directories of interest in the environment, use either Directory Assistance or an Extended Directory Catalog. For more information, see either of the following topics:

- **Using Directory Assistance with the Sametime server**
- **Using Extended Server Directory Catalogs with the Sametime server**

**Note:** Multiple Directory environments generally indicate a large or geographically distributed user population. It might be necessary to install multiple Sametime servers to adequately support a large or distributed user population. For more information, see **Advantages of using multiple Sametime servers**.

**Using Directory Assistance with the Sametime server**

To access other Directories of interest in the Domino environment, the administrator can set up Directory Assistance on the Sametime server. The Sametime server can use Directory Assistance to obtain all needed Directory information in environments that include multiple Domino Directories. Ideally, the Directory Assistance database should point to a Directory server that is dedicated to providing Directory services. However, a Directory server is not required in a Sametime community that includes multiple Sametime servers.

For information about setting up Directory Assistance, see your Domino server administration documentation, that is provided with the Domino server. You can also access the Domino server administration documentation at http://www.lotus.com/ldd/doc.

**Using an Extended Server Directory Catalog on the Sametime server**

You can use an Extended Server Directory Catalog to share Directory information when the Sametime server operates in an environment that includes multiple Directories.

Follow the procedures in the *Lotus Domino 7 Administration* Help to set up an Extended Server Directory Catalog for the Sametime server. This documentation is available at http://www.lotus.com/ldd/doc and also provided with the Domino server.

When setting up the Extended Server Directory Catalog to use with Sametime, note the following:

- You must include specific fields in the “Additional fields to include” list on the Configuration document for the Extended Server Directory Catalog.
- If you only want to use the Directory documents that Sametime requires, you can include a selection formula in the Configuration document for the Extended Server Directory Catalog.
"Additional fields to include" list requirements: The Configuration document includes an "Additional fields to include" list in the Basics tab. The following field name entries must exist in the "Additional fields to include" list to ensure all information needed by Sametime is available in the Extended Server Directory Catalog:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerName</td>
<td>&quot;Server name&quot; field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>ServerTitle</td>
<td>&quot;Server title&quot; field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Domain</td>
<td>&quot;Domain name&quot; field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>ServerBuildNumber</td>
<td>&quot;Server build&quot; number field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Administrator</td>
<td>&quot;Administrator field&quot; in the Basics section of the Server document.</td>
</tr>
<tr>
<td>ServerPlatformDisplay</td>
<td>&quot;Operating system&quot; field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Sametime</td>
<td>&quot;Is this a Sametime server?&quot; field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Port_0 - Port_7</td>
<td>Ports fields in the Ports - Notes Network Ports section of the Server document. For completeness it is recommended that you list seven port fields (for example, Port_0, Port_1, Port_2, and so on).</td>
</tr>
<tr>
<td>Protocol_0 - Protocol_7</td>
<td>Protocol fields in the Ports - Notes Network Ports section of the Server document. For completeness, it is recommended that you list seven protocol fields (for example, Protocol_0, Protocol_1, Protocol_2 and so on).</td>
</tr>
<tr>
<td>NetName_0 - NetName_7</td>
<td>Notes Network fields in the Ports - Notes Network Ports section of the Server document. For completeness, it is recommended that you list seven Notes Network fields (for example, NetName_0, NetName_1, NetName_2, and so on).</td>
</tr>
<tr>
<td>NetAddr_0 - NetAddr_7</td>
<td>Net Address fields in the Ports - Notes Network Ports section of the Server document. The NetAddr_0 field is required. For completeness, it is recommended that you list seven Net Address fields.</td>
</tr>
<tr>
<td>Enabled_0 - Enabled_7</td>
<td>Enabled fields in the Ports - Notes Network Ports section of the Server document. The Enabled_0 field is required. For completeness, it is recommended that you list seven Enabled fields.</td>
</tr>
<tr>
<td>Sametime Server</td>
<td>&quot;Sametime server&quot; field in the Administration section of the Person document.</td>
</tr>
</tbody>
</table>

Selection formula: The Advanced tab of the Configuration document provides a "Selection formula (do not include form)" setting that enables you to specify a selection formula that ensures only the Directory documents required by Sametime are used when the Dircat task creates the Directory Catalog. The selection formula for selecting only the documents required by Sametime is (Type = "Person") | (Type = "Group") | (Type = "Server" and Sametime = "1").

Note: The (Type = "Server" and Sametime = "1") selection criteria select Server documents that have the "Is this a Sametime server?" field set to Yes.
Directory security considerations

Some Sametime databases contain agents that must access the Domino Directory to perform functions such as creating a new meeting. The signature of these agents must be allowed to:

- Access the primary Domino Directory. (Reader Access level is required.)
- Run unrestricted methods and operations on the Sametime server.

If the Default ACL setting of the Domino Directory is No Access, the Sametime agents cannot access the Domino Directory, and Sametime cannot function properly. Adjust the Domino Directory ACL and the "Run unrestricted methods and operations" setting in the Server document for the Sametime server as described below.

Agent access to the Domino Directory

The default Sametime agent signer is "Sametime Development/Lotus Notes Companion Products." If the Default entry in the Domino Directory ACL is set to No Access, you must:

1. Enter "Sametime Development/Lotus Notes Companion Products" in the Directory (names.nsf) ACL.
2. Provide the Sametime Development/Lotus Notes Companion Products ID with the Reader access level in the Directory ACL.

**Note:** If your organization re-signs databases with a different signer, such as an administrator or server signature, enter that signer in the Directory ACL and provide it with the Reader access level.

Run unrestricted methods and operations

The signature that is used to sign the Sametime agents must be allowed to run unrestricted methods and operations on the Sametime server.

To ensure that the Sametime agent signer can run unrestricted methods and operations on the Sametime server:

1. Open the Server document for the Sametime server.
2. Select the Security tab.
3. Enter the Sametime agent signer (for example, Sametime Development/Lotus Notes Companion Products) in the "Run unrestricted methods and operations" field.
4. Save the changes to the Server document.

Using an LDAP directory instead of a Domino Directory

Sametime can be configured to connect to an LDAP directory on a third-party server. When Sametime is configured to connect to an LDAP directory, Sametime users are managed in an LDAP directory on another server.

The Domino Directory must exist on the Sametime server to store Domino server configuration information. The Sametime administrator must also have a Person document in the Domino Directory to authenticate when accessing the Sametime Administration Tool. All other user information is maintained in the LDAP Directory. For information about using Sametime in an LDAP environment, see [Using LDAP with the Sametime server](#).
Managing users in the Domino Directory

This section discusses managing Sametime users in the Domino Directory. The topics discussed include:

- Adding users
- Using Sametime self-registration
- Managing Sametime users with the Sametime Administration Tool
  - Adding users (from the Sametime Administration Tool)
  - Deleting users
  - Changing a user’s password or editing a Person document
  - Creating a group
  - Deleting a group
  - Editing a group

Adding users

You can add users to the Domino Directory in any of three ways. You can:

- **Add users with a Domino Administrator client** - Follow the standard procedure for registering a new Lotus Notes user into a Domino Directory. Ensure that each user has an entry in the "User name" and "Internet password" fields on a Person document. For more information, see Adding users with a Domino Administrator client.

- **Add users from the Sametime Administration Tool** - This method enables you to create a Person document containing the credentials that provide Web browser and Sametime Connect client access to the Sametime server. This method does not create a Lotus Notes ID. Web browser access to Domino servers in the domain is also provided if the Domino Directory is replicated from the Sametime server to the Domino servers. For more information, see Adding users (from the Sametime Administration Tool) in the "Managing users with the Sametime Administration Tool" section of this documentation.

- **Use the Sametime server self-registration feature** - If you enable the Sametime self-registration feature, anonymous users can create Person documents in the Domino Directory. The Person documents contain the credentials required for Web browser access to the Sametime server. Lotus Notes IDs are not created by the Sametime self-registration feature.

  If the directory is replicated from the Sametime server to Domino servers in the domain, the self-registered user also has Web browser access to the Domino servers. For more information, see Using Sametime self-registration in a Domino environment.

Adding users with a Domino Administrator client

To add a Sametime user from the Domino Administrator client, follow the normal Domino procedure for adding a new user. Use a Domino Administrator client to register the user into the Directory. The Directory replication schedule should ensure that the user eventually appears in the Directory on each server (including the Sametime server) in the domain.

When you register a new user into the Domino Directory, you should ensure that the Person document for each user includes the information required to authenticate with and connect to a Sametime server. This information includes:

- A user name entered in the "User name" field in the Basics tab of the Person document.
• An Internet password entered in the "Internet password" field in the Basics tab of the Person document.

• A home Sametime server specified in the "Sametime server" field in the Basics tab of the Person document. This field is required when you have multiple Sametime servers in the Domino domain.

The "User name" and "Internet password" fields in a Person document are required to authenticate with the Sametime server with a Web browser and to log in to the Sametime Connect client. The Sametime server uses the same Internet and intranet authentication scheme provided by the Domino server on which it is installed. The Community Services also use this information to authenticate Sametime Connect users. The home Sametime server ensures that a client is connected to a specific Sametime server for presence and chat functionality. For more information, see Connecting to the Home Sametime server

**Using Sametime self-registration**

The Sametime server includes a self-registration feature. This feature allows any anonymous user who can access the server with a Web browser to create their own Person document containing a last name, user name, and Internet password in the Domino Directory on the Sametime server.

A self-registered user can use the Sametime Connect client and access protected databases on the Sametime server with a Web browser. If the Domino Directory is replicated from the Sametime server to Domino servers in the domain, the self-registered user might also be able to access the protected areas of the Domino servers in the domain with a Web browser.

**Note:** Generally, the Sametime self-registration feature provides an easy way to populate a Domino Directory with Sametime users. Because an existing Domino domain usually has a Directory populated with users, self-registration is disabled by default when Sametime is installed on the Domino server. Administrators should also consider the security implications of allowing anonymous users to create Person documents in the Domino Directory before allowing self-registration on the Sametime server.

To enable the self-registration feature on a Sametime server, perform the following three procedures. Each of these procedures is described in a separate topic.

1. **Enable self-registration from the Sametime Administration Tool**
2. **Add the Sametime signer ID to the Domino Directory (names.nsf) ACL**
3. **Review the security recommendations for the self-registration feature**

**Note:** If you have integrated multiple Sametime servers into a single community, and you are using the self-registration feature, self-registration should be enabled on only one of the Sametime servers. In multiple Sametime server environments, the Domino Directory is replicated among the Sametime servers. If self-registration is enabled on multiple Sametime servers, multiple groups named "Sametime Web Users" will be created in the Directory. For more information on multiple server environments, see Advantages of using multiple Sametime servers

**Enable self-registration from the Sametime Administration Tool**

This procedure is the first of three required to use the Sametime self-registration feature. To enable self-registration from the Sametime Administration Tool:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.


3. In the User Registration settings, place a check mark in the "Allow users to register themselves in the Domino Directory" check box.

4. You must click the Update button and restart the Sametime server for this change to take effect.

Next, ensure that the Sametime agent signer is added to the Domino Directory ACL and has the appropriate access level in the ACL.

Add the Sametime signer ID to the Domino Directory ACL

This procedure is the second of three required to use the Sametime self-registration feature. In this procedure you must add a signer ID to the Domino Directory ACL.

The Sametime self-registration feature is supported by a self-registration database (streg.nsf) on the Sametime server. Agents within the self-registration database must access the Domino Directory on the Sametime server to create and modify Person documents in the Directory. The default signature on these agents is "Sametime Development/Lotus Notes Companion Products." To ensure that the agents in the self-registration database can operate in the Domino Directory, do the following:

1. Add the "Sametime Development/Lotus Notes Companion Products" signer to the ACL of the Domino Directory.

2. Provide the Sametime Development/Lotus Notes Companion Products signer with the following Access level and Roles in the Domino Directory ACL:
   - Access level: Author
   - Roles: [Group Creator], [Group Modifier], [User Creator], [User Modifier]

3. Ensure that the "Create Documents" privilege is selected in the Domino Directory ACL.

Note: Administrators can also sign the self-registration database with another signer. Normally, an administrator uses the administrator signature or server signature for this purpose. If you use a different signer, you must add that signer to the Directory ACL and provide it with the Access level and Roles specified above.

Next, review the security recommendations for self-registration

Review the security recommendations for self-registration

This procedure is the last of three required to use the Sametime self-registration feature. If you are using the self-registration feature, you should review the security recommendations for self-registration.

The specific recommendations for securing your server when using self-registration are described in the Security recommendations for self-registration topic in the Security section of this documentation.

Managing Sametime users with the Sametime Administration Tool

The Sametime Administration Tool provides access to Person and Group documents in the Domino Directory on the Sametime server. You can use the
Sametime Administration Tool or a Lotus Notes client to delete and edit Person and Group documents in the Domino Directory on the Sametime server.

For information about using a Lotus Notes client to manage users in a Domino Directory, see your existing Domino documentation. If you use a Lotus Notes client or the Domino Administrator to manage Sametime users, you should review the topics in "How Sametime uses Domino Directory information".

For information about using the Sametime Administration Tool to manage users in the Domino Directory on the Sametime server, see the topics listed below.

- Adding users (from the Sametime Administration Tool)
- Deleting users
- Changing a user’s password or editing a Person document
- Creating a group
- Deleting a group
- Editing a group

**Adding users (from the Sametime Administration Tool)**

You can add users to the Directory using the Sametime Administration Tool. To add a user, you create a Person document for the user in the Directory and specify a last name, user name, and Internet password. A Lotus Notes user ID is not created by this process. The Sametime server is designed for Web browser access only.

When adding users with the Sametime Administration Tool, the new user might not be immediately visible in the Directory. A small refresh interval must pass before the user’s name is visible in the Directory. Also, a recently added user cannot appear in a Sametime presence list until the Community Services receive an updated list of users from the Domino Directory. For more information, see "How often to poll for new names added to the Sametime Community directory."

To add a user from the Sametime Administration Tool:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Choose Manage People.
4. Select Add Person. The Person document appears. If necessary, select the Basics section.
5. In the Basics section of the Person document, enter the user’s first, middle, and last name in the appropriate fields. Only the last name is required.
6. Enter a name for the user in the “User name” field. An entry in this field is required for the user to authenticate with the Sametime server.

   A user can enter this name when logging in to Sametime Connect or accessing a database on the Sametime server that requires basic password authentication. User names are case-sensitive.

   You can also enter multiple names in the "User name" field. If you enter multiple names, ensure that each name is separated by a carriage return. (Press the Enter key after entering each name.)

   **Note** The name that appears in the top line in the "User name" field is the name that displays in presence lists in Sametime clients.

7. Enter an Internet password for the person in the "Internet password" field. An entry in this field is required for the user to authenticate with the Sametime
server. The user is prompted for this password when logging in to Sametime Connect or accessing any database on the Sametime server that requires basic password authentication. Internet passwords are case-sensitive. Write down the Internet passwords as you assign them. After it is entered the first time, the Internet password is encrypted on the Person document and cannot be viewed.

8. Click "Save and Close." The Person document is added to the Directory.

Deleting users
You can use the Sametime Administration Tool to delete a user from the Domino Directory on the Sametime server. Deleting a user’s Person document removes the user from the Sametime community and prevents the user from accessing Sametime Connect or databases on the server that require basic password authentication.

To delete a user:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Choose Manage People.
4. Double-click the name of the user you want to delete. The user’s Person document opens.
5. Select Delete Person. The Person document is deleted from the Domino Directory.

Changing a user’s password or editing a Person document
You can use the Sametime Administration Tool to change a user’s Internet password. To change a user’s Internet password, you must edit the user’s Person document.

To change a password or edit the Person document:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Choose Manage People.
4. Double-click the name of a user.
5. Select Edit Person. The Person document changes to edit mode.
6. If necessary, select the Basics tab.
7. In the "Internet password" field, delete the existing Internet password and enter the new Internet password.
8. While the Person document is in edit mode, you can edit any other field of the Person document.
9. Click "Save and Close."

Creating a group
You can use the Sametime Administration Tool to create a group document. Each user that you add to a group document must have a Person document that contains information in the "Last name," "User name," and "Internet password" fields in the Domino Directory on the Sametime server.

Note: Groups larger than 400 members might not display correctly in Sametime presence lists. If you are creating a group that Sametime Connect users will
add to Sametime Connect contact lists, do not include more than 400 names in the group. For more information on how Sametime uses groups, see

**Group documents**

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Choose Manage Groups.
4. Click Add Group.
5. Enter a name for the group in the "Group name" field (for example, Administrators or Meeting Creators).
6. Select a group type (Multipurpose, Access Control List, Deny List, Mail Only, and Servers Only). Select Multipurpose if you are creating a Public Group that users will add to the Sametime Connect client presence list or a group that will serve more than one purpose.

**Note** You can also select the Mail Only group type when creating Public Groups that users will add to the Sametime Connect client presence list. Select Access Control List if the purpose of the group is to allow or deny access to databases on the Sametime server. Do not select the Access Control List, Deny List, or Servers Only group types when creating Public Groups for Sametime Connect users. The Sametime Connect client does not display the contents of groups that have a group type of Access Control List, Deny List, or Servers Only. Deny List groups are usually used only when you have integrated Sametime into a Domino environment.

7. (Optional) Enter a description of the group in the Description field.
8. List the members of the group in the Members field. Make sure to enter a name exactly as it is entered in the top line of the "User name" field of the user’s Person document.

For example, assume a person’s name is listed in the "User name" field of the Person document as:

**Tom Smith/West/Acme Tom Smith**

When adding the person’s name to the Members field of the Group document, you should enter the name as Tom Smith/West/Acme because this name appears in the top line in the "User name" field of the Person document. If the name entered in the Members field of the Group document is not identical to the name in the top line in the "User name" field of the Person document, the user will always appear to be off line when the Group document is opened in a Sametime client presence list. For example, the user will always appear off line in the group if you enter Tom Smith instead of Tom Smith/West/Acme.

9. Select the Administration link at the top of the Group document.
10. Enter the names of the group owners in the Owners field. Generally, the group owner is the administrator creating the group.
11. Click "Save and Close."

**Deleting a group**

You can use the Sametime Administration Tool to delete a group from the Domino Directory on the Sametime server.

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Choose Manage Groups.
4. Double-click the name of the group you want to delete.
5. When the Group document opens, select Delete Group. The Group document is deleted from the Domino Directory.

**Editing a group**
To add or delete users from a group or change any other fields in a Group document, you must use the Sametime Administration Tool to edit the Group document. To edit a Group document:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Choose Manage Groups.
4. Double-click the name of a group.
5. Select Edit Group and make the appropriate changes.
6. Click "Save and Close."

---

**How Sametime uses Domino Directory information**
This section discusses the Domino Directory information that is used by Sametime. The topics in this section include:

- Person documents
- Group documents
- The Server document
- Directory views used by Sametime features

**Person documents**
The Domino Directory maintains a Person document for each user in the Sametime community (or Domino domain). Each member of the Sametime community must have a Person document in the Directory to log into the Sametime Connect client or authenticate with the Sametime server.

A Person document includes many different fields that contain descriptive information about a user. Most of the fields are optional for Sametime users. The four most important fields on a Person document for a Sametime user are the "Last name," "User name," "Internet password," and "Sametime server" fields.

The "Last name," "User name," and "Internet password" fields in the Basics section of a Person document are required for authentication. For more information about how these fields are used by the authentication process, see [Person document, User names, and Internet passwords](#) in the Security section of this documentation.

**"Sametime server" field (home Sametime server)**
The "Sametime server" field in the Administration tab of a user’s Person document specifies a user’s "home" Sametime server. You must enter the name of a Sametime server in this field for every Sametime user when multiple Sametime servers are installed and integrated into a single community.

The home Sametime server stores a user’s Community Services preferences and other data. When a Sametime server is specified in the "Sametime server" field of a user’s Person document, Sametime ensures that the user always logs in to that Sametime server to receive the Community Services presence and chat functionality. For more information, see [Connecting to the Home Sametime server](#)
Group documents


Generally, a Group document contains a list of users who perform similar tasks. For example, all employees in the Marketing department might be listed in a "Marketing" Group document. All employees in the Engineering department might be listed in an "Engineering" Group document.

In the Sametime Connect client, groups that are defined by Group documents in the Directory are referred to as "Public Groups." Any Sametime Connect user can browse the Domino Directory to add these Public Groups to the Sametime Connect contact list. Public groups can greatly simplify the process of adding users to the Sametime Connect contact list. For example, the administrator can create a Group document called "Technical Support" that lists all 40 employees in the Technical Support department. With a single mouse click, a Sametime Connect user can add the Technical Support Public group to the Sametime Connect contact list to have presence (or online awareness) and chat capabilities with all 40 employees in the Technical Support Group document. Without the Group document, the user must add the 40 employees to the Sametime Connect contact list one at a time.

Note: Generally, Sametime Connect cannot use a Group document that contains more than 400 members. For a group that is larger than 400 members, create a Group document that contains other Group documents and add up to 400 members to each of the subgroups.

Using groups can also simplify administrative tasks. For example, if you create a group called "Administrators" that lists all users who can perform administrative tasks, you can add this group to the appropriate database Access Control Lists (ACLs) and fields on the Server document. If you want to add an administrator, you can edit the Administrators Group document. For more information about using Group documents to control access for administrators, see [Allowing others to access the Sametime Administration Tool](#).

If you modify the ACL of the Sametime Meeting Center (stconf.nsf) to require basic password authentication, you can create group documents to control access for meeting creators and attendees. For example:

1. Turn off anonymous access in the Sametime Meeting Center ACL. Set the Anonymous and -Default- entries in the ACL to No Access.
2. Create a Group document called "Meeting Creators" that lists all users who can create new meetings in the Sametime Meeting Center.
3. Add the Meeting Creators group to the ACL of the Meeting Center database (stconf.nsf).
4. Assign the Author access level to the Meeting Managers group and select the "Write public documents" check box. Users listed in the Meeting Creators group can create and attend meetings in the Meeting Center.
5. Create another group called "Attendees" that lists all users that you want to attend meetings but not create them.
6. Add the Attendees group to the ACL of the Sametime Meeting Center database and assign the Attendees group Reader access in the Sametime Meeting Center. Users listed in the Attendees group can attend meetings in the Sametime Meeting Center but cannot create them.
After setting up the Meeting Creators and Attendees groups as described above, you can add or remove user names from the Group documents to assign or revoke meeting creator and attendee privileges in the Sametime Meeting Center.

For more information about working with Group documents, see Creating a group, Deleting a group, or Editing a group.

The Server document

The following fields in the Server document are needed for each Sametime server to support online presence:

- **Server name** - This field in the Basics tab of the Server document must contain the name of the Sametime server.
- **Is this a Sametime server?** - This field in the Basics tab of the Server document must be set to Yes to indicate the Server document describes a Sametime server.
- **Port** - This field in the Ports-Notes Network Ports tab of the Server document must be set to TCPIP.
- **Net Address** - This field in the Ports-Notes Network Ports tab must contain the TCP/IP address of the Sametime server.

**Note:** The settings in the "Sametime" tab of the Server document are not used by Sametime. Configuration values for the settings available from the Sametime Administration Tool are stored in the Configuration database (stconfig.nsf) and the Sametime.ini file on the Sametime server. Changing settings in the Sametime tab of the Server document has no affect on the Sametime server.

Directory views used by Sametime features

Online presence for individual users and users listed in groups requires the use of specific views in the Domino Directory. Each Directory in the Sametime community must contain the views listed here according to Sametime feature:

<table>
<thead>
<tr>
<th>Sametime Feature</th>
<th>Views used</th>
</tr>
</thead>
</table>
| Expand a group to list all the unique members in the group | $People
|                                                      | $VIMGroups           |
| Determine which groups a user is a member of          | $MailGroups
|                                                      | $People
|                                                      | $ServerAccess        |
| Determine which servers are Sametime servers          | $Servers             |
| Authenticate a user                                   | $Users               |
| Browse the Directory for users and groups            | $PeopleGroupsFlat    |

Managing users in buddy lists and privacy lists

If you make changes to user names or group names in the Domino directory, you must run the Name Conversion Utility to ensure these same name changes are made in the buddy lists and privacy lists that display in the Sametime Connect client. The buddy list and privacy list names are stored in a Domino database (vpuserinfo.nsf) and must be managed separately from the names in the directory. For more information, see the appendix Using the Name Conversion Utility.
Chapter 4. Using LDAP Directories with Sametime

This chapter explains how the IBM Lotus Sametime server can be configured to connect to a Lightweight Directory Access Protocol (LDAP) server and access an LDAP directory. You can use this capability to integrate Sametime into an environment in which LDAP-compliant servers and directories are already deployed. This chapter discusses the following topics:

- Using LDAP with the Sametime server
- Setting up an LDAP connection
- LDAP Connectivity settings
- LDAP Basics settings
- LDAP Authentication settings
- LDAP Searching settings
- LDAP Group Contents settings
- Using SSL to encrypt connections between a Sametime and LDAP server
- Adding new administrators in the LDAP environment
- Access Control Lists and LDAP user names
- Setting up an LDAP connection after selecting the Domino directory during the server installation
- Customizing LDAP directory searches
- Solving token authentication problems in mixed server and multiple directory environments.

Using LDAP with the Sametime server

Using LDAP with the IBM Lotus Sametime server allows you to integrate Sametime into an environment in which other LDAP-compliant servers and directories are already deployed. Sametime can be used with LDAPv2 and LDAPv3.

Note: For information on using LDAP with a Sametime server that operates on a platform other than Windows (such as the IBM i5/OS and pSeries servers), see the installation guide (stinstall.nsf or stinstall.pdf) that shipped with the Sametime server.

Sametime users and groups can be maintained in an existing LDAP directory on an LDAP server. When Sametime users and groups are maintained in an existing LDAP directory, it is not necessary to populate the Domino Directory on the Sametime server with every user and group in the organization.

To use Sametime in an LDAP environment, you must configure the Sametime server to connect to an LDAP server. When connected to an LDAP server, Sametime can search and authenticate against the LDAP directory on the LDAP server on behalf of Sametime clients.

This section includes the following topics related to using Sametime with LDAP:

- How LDAP is used with Sametime - Provides basic information about using LDAP with Sametime.
• **Setting up an LDAP connection** - Describes the procedures required to set up a connection with an LDAP server.

• **LDAP Directory Settings** - Provides an overview of the LDAP configuration settings available in the Sametime Administration Tool and describes the level of LDAP knowledge required to configure the Sametime LDAP Directory settings. The administrator must configure the LDAP Connectivity, Basics, Authentication, Searching, and Group contents settings located within the LDAP Directory settings of the Sametime Administration Tool.

• **Configuring LDAP Connectivity settings** - Provides detailed information about the configuration settings that enable the Sametime server to connect to an LDAP server, including information on using SSL for authentication and encryption of the connection between the Sametime and LDAP server. This section also explains the configuration settings that enable a Sametime server to access multiple LDAP servers when searching for and authenticating users.

• **Configuring LDAP Basics settings** - Provides detailed information about the basic LDAP settings that support searching person and group entries in an LDAP directory. These settings ensure that user and group names maintained in an LDAP directory can be displayed in Sametime user interfaces.

• **Configuring LDAP Authentication settings** - Provides detailed information about the LDAP search filter required to enable users to authenticate against entries in an LDAP directory. Also explains how to specify a home Sametime server when Sametime is functioning in an LDAP environment.

• **Configuring LDAP Searching settings** - Provides detailed information on the LDAP search filters required to conduct searches for people and groups in an LDAP directory.

• **Configuring LDAP Group Contents settings** - Provides detailed information about the LDAP Group Contents setting required to enable Sametime to examine groups in an LDAP directory. Sametime uses these settings to resolve the names within a group entry to person or group entries in an LDAP directory.

• **Using SSL to encrypt connections between the Sametime and LDAP servers** - Provides information on how to encrypt all data transmitted between the Sametime and LDAP servers.

• **Access Control Lists and LDAP User Names** - Briefly describes rules for entering LDAP user names in database Access Control Lists (ACLs).

• **Adding new administrators in the LDAP environment** - Discusses adding new Sametime administrators when Sametime is configured to connect to an LDAP server.

• **Setting up an LDAP connection after selecting the Domino directory during the server installation** - Discusses how to set up a connection to an LDAP server if you did not choose the LDAP Directory option during the Sametime server installation.

• **Using Java classes to customize LDAP directory searches** - Explains how you can write a Java class to customize the way in which Sametime searches the LDAP directory for users and groups. You can also write a Java class that changes the format of user names returned from LDAP directory searches.

• **Solving token authentication problems in mixed server and multiple LDAP directory environments** - Explains how to solve token authentication problems that occur when a Sametime server operates in an environment that includes other application servers that issue authentication tokens (such as portal servers). These problems occur when Sametime connects to a different LDAP directory than the other application servers.
How LDAP is used with Sametime

The administrator can configure the Sametime server to connect to one or more LDAP servers. When Sametime connects to an LDAP server, the following support is provided for Authentication, Searches, Connectivity, Administration, and User Management.

Authentication

Sametime supports authentication against an LDAP directory in the following ways:

- Sametime Connect, Sametime Meeting Room, and Sametime Broadcast clients can authenticate using user names and passwords stored in an LDAP directory on an LDAP server.
- Only users that are entered in the LDAP directory on the LDAP server can authenticate with the Sametime server.
- The Sametime administrator is an exception. A Sametime administrator is always authenticated against the Domino Directory when accessing the Sametime Administration Tool. A Sametime administrator must have a Person document in the Domino Directory on the Sametime server to access the Sametime Administration Tool.
- End users use existing Sametime client interfaces when entering user names and passwords for authentication purposes. The end user does not know whether they are authenticating against an LDAP directory or a Domino directory.
- Authentication to individual databases on the Sametime server is still controlled by database ACLs. For information on entering names from an LDAP directory in a database ACL, see Access Control Lists and LDAP User Names.
- The Sametime server connects to the LDAP server to perform search and authentication procedures on behalf of Sametime clients. The Sametime administrator can specify whether the Sametime server binds to the LDAP server as an anonymous or authenticated user when making this connection. For more information, see Administrator distinguished name and password for authenticated binding.
- The Sametime server can be configured to use SSL for authentication and encryption when connecting to the LDAP server. For more information, see Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server.

Searches

Sametime supports searches of the LDAP directory in the following ways:

- Users can search the LDAP directory on an LDAP server to add people and groups to the Sametime Connect client presence list or privacy list. Users can also search the LDAP directory when adding users to the “Restrict To” list available from the New Meeting form in the Sametime Meeting Center.
- End users use existing Sametime client interfaces when searching for other users.
- Searches of the LDAP directory are conducted according to parameters specified in the Sametime LDAP Directory Settings in the Sametime Administration Tool. The administrator must configure the LDAP Directory Settings to ensure the searches are conducted using search filter and schema settings consistent with the schema of the LDAP directory to be searched.
- You can write Java classes to more precisely control the manner in which Sametime searches for users and groups and formats user names returned from LDAP directory searches.
Connectivity

Sametime supports connectivity with the LDAP server in the following ways:

- Sametime clients connect to the Sametime server. The Sametime server establishes a network connection to the LDAP server and performs searches and authentication on behalf of the Sametime clients. Sametime clients do not connect directly to the LDAP server.

  The Sametime server connects to the LDAP server using the LDAP protocol. By default, this connection occurs on TCP/IP port 389.

- The Sametime Administrator specifies whether the Sametime server binds to the LDAP server as an anonymous or authenticated user when connecting to the LDAP server. For more information, see Administrator distinguished name and password for authenticated binding.

- The Sametime server can be configured to access multiple LDAP servers when searching for and authenticating Sametime users. The Sametime server can access one LDAP directory per LDAP server.

- The Sametime server can be configured to use SSL when accessing the LDAP server.

Administration and user management

Sametime supports administration and user management with LDAP in the following ways:

- When using LDAP, Sametime server administrators are authenticated against the Domino Directory on the Sametime server when accessing the Sametime Administration Tool. All other users are authenticated against the LDAP directory on the LDAP server. For more information, see Sametime Administration Tool and LDAP environments.

- The person entries in the LDAP directory must contain a field to hold the name of a user’s home Sametime server. This field does not exist in the LDAP directory, so the administrator can either add a new field to the person entries in the LDAP directory or use an existing field such as the e-mail attribute. Once this field is added to the person entries in the LDAP directory, the administrator must enter the name of the user’s home Sametime server in the new field in each user’s person entry in the LDAP directory. The administrator must also specify the name of the field in the LDAP directory that contains the name of the Sametime server in the LDAP Authentication settings of the Sametime Administration Tool.

- Sametime server administrators cannot use the Sametime Administration Tool to add or modify users and groups in the LDAP directory on an LDAP server. User accounts must be added and modified using the software and procedures required by the LDAP directory on the LDAP server.

  The Sametime Administration Tool can be used to perform all other Sametime administrative procedures when Sametime is configured to connect to an LDAP server.

- If you make changes to user names or group names in the LDAP directory, you must run the Name Conversion Utility to ensure these same name changes are made in the buddy lists and privacy lists that display in the Sametime Connect client. The buddy list and privacy list names are stored in a Domino database (vpuserinfo.nsf) and must be managed separately from the names in the directory. For more information, see the appendix Using the Name Conversion Utility.
The Sametime self-registration feature cannot be used when Sametime connects to an LDAP server. The self-registration feature cannot access the LDAP directory to create person entries in the LDAP directory.

Note: Generally, Netscape servers contain LDAP-native directories, and it is not necessary to configure those servers for access by LDAP clients. In other cases, it might be necessary to configure the LDAP server to process LDAP requests from an LDAP client. Consult the documentation for the LDAP server for this information.

Setting up an LDAP connection

The three procedures associated with setting up an LDAP connection from Sametime to an LDAP server are:

1. Select the appropriate LDAP options during the server installation
2. Alter the Directory Assistance document for the LDAP directory
3. Configure the LDAP Directory settings in the LDAP document

You can use either a Lotus Notes client or the Sametime Administration Tool to configure these settings.

Selecting the appropriate LDAP options during the server installation

This procedure is the first of three associated with setting up an LDAP connection from Sametime to an LDAP server.

During the installation and setup of the Sametime server, you must provide information that is needed by Sametime to connect to the LDAP server. The Sametime installation prompts you with a “Select Directory type” dialog box. In the “Select Directory type” dialog box, you must select "LDAP Directory" from the drop-down list. After selecting the "LDAP Directory” option, the setup procedure prompts you for the following information:

- **LDAP Server Name** - Enter the fully-qualified DNS name or IP address of the LDAP server that contains the LDAP directory that Sametime will access.
- **Port Number for LDAP** - Specify the TCP/IP port number on which the LDAP server listens for LDAP connections. The default port number for LDAP connections is port 389.

Note: The *Lotus Sametime Server 7.0 Installation Guide* provides step-by-step instructions for selecting these options during a Sametime installation. If you did not select these options during the installation, you can either reinstall the Sametime server and select the appropriate LDAP options during the reinstallation or perform the procedures described in **Setting up an LDAP connection after selecting the Domino directory during the server installation**.

About selecting the LDAP directory during the server installation

When you select “LDAP Directory” as the directory type during a Sametime installation, the installation makes the configuration changes necessary to enable the Domino components used by Sametime to connect to the LDAP directory. Specifically, the following occurs when you select the "LDAP Directory” option during the Sametime installation:

- A Directory Assistance database (da.nsf) is created by the Sametime installation on the Domino server on which Sametime resides.
A Directory Assistance document is created in this da.nsf database. This document is configured by default to enable the Sametime server to connect to the LDAP directory. It may be necessary to alter the "Base DN for search" setting in the Directory Assistance document to ensure Sametime can connect to the LDAP server. This configuration is described in the next procedure.

- The filename da.nsf is written in the "Directory Assistance database name" field in the Server document of the Domino server on which Sametime is installed. This entry must exist in the Server document to enable the Domino server to use directory assistance.

**Note:** If an entry exists in the "Directory Assistance database name" field in the Server document of the Domino server at the time the Sametime server is installed, the Sametime server installation will create a Directory Assistance document in the database specified in the "Directory Assistance database name" field. This Directory Assistance document points to the LDAP server specified during the Sametime installation.

For example, if the "Directory Assistance database name" field in the Server document specifies the name "da.nsf" (or any other filename) when Sametime is installed, the Sametime installation creates a Directory Assistance document within the existing "da.nsf" database (or other database specified in the "Directory Assistance database name" field). This Directory Assistance document points to the LDAP server specified during the Sametime installation. The Sametime installation does not overwrite the existing da.nsf database or attempt to create a new directory assistance database if a directory assistance database is already specified in the "Directory Assistance database name" field of the Server document.

**Next step**

After specifying the correct LDAP options during the installation, you must alter the Directory Assistance document for the LDAP directory.

**Alter the Directory Assistance document for the LDAP directory**

This procedure is the second of three associated with setting up an LDAP connection from the Sametime server to an LDAP server.

The Sametime server installation creates a Directory Assistance database (da.nsf) on the Sametime server. This database contains a Directory Assistance document that enables Sametime to connect to the LDAP server to authenticate Web browser users.

You must ensure the "Base DN for search" setting in this Directory Assistance document is set appropriately for the LDAP directory used in your environment. To alter the "Base DN for search" setting in the Directory Assistance document:

   - Choose File - Database - Open.
   - Select the Local server.
   - Select the Directory Assistance database (da.nsf).
   - Click Open.
2. Double-click the name of the Directory Assistance document for the LDAP server to open the document.
3. Click the LDAP tab.
4. In the "Base DN for Search" field, make one of the following entries. The entry you make depends on the type of LDAP directory used in your environment.
   - **Domino directory** - An example value is "O=DomainName," where "DomainName" is the Lotus Notes domain (for example O=Acme).
   - **Microsoft Exchange 5.5 directory** - An example value is "CN= recipients, OU=ServerName, O=NTDomainName," where ServerName is the Windows server name and NTDomainName is the Windows NT Domain (for example, CN=recipients, OU=Acmeserver1, O=NTAcmedomain).
   - The Microsoft Exchange 5.5 example above assumes that the directory is using the default directory schema. If you have changed the schema of the Microsoft Exchange 5.5 directory, the entry in the "Base DN for Search" field must reflect the new schema.
   - **Microsoft Active Directory** - An example value is "CN=users, DC=DomainName, DC=com."
   - **Netscape LDAP directory** - Use the format O= followed by the organizational unit that was specified during the Netscape server setup. If you are uncertain about this entry, use the administrative features of the Netscape server to determine the appropriate entry.
   - **IBM SecureWay directory** - An example value is "DC=DomainName, DC=com."

5. Click Save and Close to save the Directory Assistance document.

**Next step**

After altering the Directory Assistance document, you must [configure the LDAP Directory settings](#).

**Configure the LDAP Directory settings**

This procedure is the last of three associated with setting up an LDAP connection from Sametime to an LDAP server.

You must configure the LDAP Directory settings on the LDAP document in the Configuration database to ensure that the Sametime server can search and authenticate against entries in the LDAP directory.

You can configure the LDAP Directory settings using either a Lotus Notes client or the Sametime Administration Tool.

If you use a Notes client, you enter the LDAP Directory settings directly into the fields in the LDAP document in the Configuration database.

If you use the Sametime Administration Tool, you complete the "LDAP Directory" settings available from the user interface of the Sametime Administration Tool. The administration tool writes the values to the LDAP document in the Configuration database.

Procedures for using either the [Sametime Administration Tool](#) or the [Lotus Notes client](#) to configure the LDAP Directory settings are included below. Refer to the help topics for either procedure in the [LDAP Directory Settings](#) section of this documentation for help on individual settings.

**Note:** Configuring the LDAP Directory settings requires previous experience with LDAP. For more information, see [LDAP knowledge required to configure the LDAP Directory settings](#).
Configuring LDAP Directory settings from the Sametime Administration Tool

To configure the LDAP settings using the Sametime Administration Tool:

1. Open the Sametime Administration Tool from the “Administer the Server” link of the Sametime server home page.
2. Select “LDAP Directory.”

The LDAP Directory options are listed below. The LDAP Directory options contain settings that must be consistent with your LDAP environment.

Connectivity - Includes settings that ensure the Sametime server can connect to the LDAP server. For more information, see Configuring the LDAP Connectivity settings.

Basics - Includes settings that ensure that the Sametime server can search person and group entries in the LDAP directory. For more information, see Configuring the LDAP Basics settings.

Authentication - Includes settings that ensure that users can authenticate against entries in an LDAP directory and provides settings that enable you to specify home Sametime servers when Sametime connects to an LDAP server. For more information, see Configuring LDAP Authentication settings.

Note: If you have deployed more than one Sametime server, you must add a “Sametime server” field to the Person entries in the LDAP directory and then specify the name of this field in the Authentication settings of the Sametime Administration Tool. For more information on this requirement, see Setting the Home Sametime Server setting for LDAP.

Searching - Includes search filter settings that resolve searches for person or group entries in the LDAP directory. For more information, see Configuring LDAP Searching settings.

Group Contents - Includes settings that resolve searches for person or group entries that are contained within another group entry. For more information, see Configuring LDAP Group Contents settings.

Configuring LDAP Directory settings using a Lotus Notes client

Use the instructions below to configure the LDAP Directory settings using a Lotus Notes client.

1. Use the Lotus Notes client on the Sametime server to open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
   • Choose File - Database - Open.
   • Select the Local server.
   • Select the Sametime Configuration database (stconfig.nsf).
   • Click Open.

2. Open the LDAP document in the Configuration database that is associated with the LDAP server. To open the LDAP document:
   • In the right pane of the Configuration database, locate the LDAP server entry in the Form Name column of the Configuration database.
   • Each LDAP Server document is listed to the right and beneath the LDAP Server entry under the Last Modified Date column. The date represents the last time the LDAP server document was modified.
   • To open an LDAP Server document, double-click the date in the Last Modified Date column that represents the document.
   • When the LDAP Server document opens, double-click the document to put it in edit mode.
3. To configure the LDAP Directory settings, you can enter values directly into the editable fields in the LDAP Server document.

The LDAP Directory settings that are available from the LDAP document in the Configuration database are the same LDAP settings that are available from the Sametime Administration Tool. However, some LDAP Directory settings in the LDAP document are worded differently and arranged in a different order from the LDAP Directory settings in the Sametime Administration Tool. This documentation assumes that the administrator is using the Sametime Administration Tool to configure these settings. Consult the lists below to locate the documentation in this chapter for individual LDAP Directory settings that appear in the LDAP document of the Configuration database.

**Connection settings**
The Connection settings in an LDAP document in the Configuration database include:

- **Network Address of LDAP Connection** - For more information, see [Host name or IP address of the LDAP server](#).
- **Port number for LDAP Connection** - For more information, see [Port](#).
- **Login Name for LDAP Connection** - For more information, see [Administrator distinguished name and password for authenticated binding](#). Note that if this field is left blank, the Sametime server binds to the LDAP server as an anonymous user.
- **Password for LDAP Connection** - For more information, see [Administrator distinguished name and password for authenticated binding](#).
- **SSL Enabled** - For more information, see [Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server](#).
- **SSL Port** - For more information, see [Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server](#).
- **Search Order** - For more information, see [Position of this server in the search order](#).

**Search Filter settings**
For information on any of the Search Filter settings below, see the topic later in this chapter that has the same name as the setting. The Search Filter settings and the help topic for each setting are:

- **Search filter for resolving person names**
- **Search filter to use when resolving a user name to a distinguished name**
- **Search filter for resolving group names**

**Search Base and Scope settings**
The Base Objects settings are worded differently in the LDAP document in the Configuration database than in the Sametime Administration Tool. The settings and the help topics for each setting are listed below:

- **Base object when searching for person entries** - For more information, see [Where to start searching for people](#).
- **Base object when searching for group entries** - For more information, see [Where to start searching for groups](#).

The Scope settings are worded the same in the LDAP document in the Configuration database as in the Sametime Administration Tool. The Scope settings and the help topics for each setting are:

- **Scope for searching for a person**
• Scope for searching for groups

Schema settings
The Schema settings are worded the same in the LDAP document in the Configuration database as in the Sametime Administration Tool. The Schema settings and the help topic for each setting are:
• The attribute of the person entry that defines the person’s name
• Attribute used to distinguish between two similar person names
• The person object class used to determine if an entry is a person
• Attribute of a person entry that defines a person’s e-mail address

The Groups settings are worded the same in the LDAP document in the Configuration database as in the Sametime Administration Tool. The Groups settings and the help topics for each are:
• Attribute used to distinguish between two similar group names
• Attribute in the group object class that has the names of the group members
• The group object class used to determine if an entry is a group

Home server
If you have deployed more than one Sametime server, you must add a "Sametime server” field to the Person entries in the LDAP directory and then specify the name of this field in the Home Server field in the LDAP document in the Configuration database. For more information on this setting, see Setting the Home Sametime Server setting for LDAP and Connecting to the Home Sametime server.

LDAP directory settings
The Sametime Administration Tool includes the LDAP Directory settings that enable the Sametime server to operate as a client to an LDAP server. These settings enable the Sametime server to search the LDAP directory on the LDAP server and authenticate Sametime users against entries in the LDAP directory.

The LDAP Directory configuration settings are available from the Directory - LDAP Directory Settings option of the Sametime Administration Tool.

Before configuring the LDAP Directory settings, the administrator must perform the procedures described in Setting up the LDAP connection.

Note: The administrator must have some experience with LDAP to properly configure the LDAP Directory settings. For more information on the LDAP knowledge required, see LDAP knowledge required to configure the LDAP Directory settings.

The available Sametime LDAP Directory configuration settings are:

Connectivity
The Connectivity settings enable the administrator to provide the IP address and ports the Sametime server uses when connecting to the LDAP server, and to specify whether the Sametime server binds to the LDAP server as an anonymous or authenticated user. These settings also enable the Sametime server to connect to multiple LDAP servers, and to use SSL when connecting to the LDAP server.
Basics

The Basics settings enable the administrator to specify the basic LDAP parameters required to conduct searches for people and group entries in an LDAP directory. Some of these parameters are also required to display the names of users in Sametime user interfaces. The Basics settings include parameters that specify the level of a directory from which a search begins, the scope of a search, and attributes of LDAP directory entries that define person and group names.

Authentication

The Authentication settings ensure that Sametime users can be authenticated against entries in an LDAP directory. The administrator must specify an LDAP search filter that can resolve a name provided by a user to a Distinguished Name (DN) in an LDAP directory.

The Authentication settings also enable the administrator to specify the field in the LDAP directory person entries that contains the name of each user’s home Sametime server.

Note: The administrator must add a field to the person entries in the LDAP directory to hold the name of each user’s home Sametime server or use an existing field in the person entries for this purpose.

Searching

The Searching setting enables the administrator to specify the search filters required to resolve the names of people and groups to specific entries in an LDAP directory.

Group Contents

The Group Contents setting enable the administrator to specify the attribute of a group entry that contains the names of group members.

Add Administrator

The Add Administrator settings are used to enable additional administrators to access the Sametime Administration Tool.

Access Control

The Access Control settings enable the administrator to work with Access Control Lists.

LDAP knowledge required to configure the LDAP Directory settings

Before configuring the LDAP Directory Settings for Sametime, the administrator should have experience with the Lightweight Directory Access Protocol (LDAP) and should be familiar with the following LDAP concepts and procedures:

- The structure (directory tree) of the LDAP directory the Sametime server will access
- The schema of Person and Group entries in the LDAP directory
- How to construct LDAP search filters to access the attributes of Person and Group entries in the LDAP directory
Note: LDAP defines a standard way to search for and manage entries in a directory. A detailed discussion of the LDAP standard is outside the scope of this documentation.

Configuring LDAP Connectivity settings
The LDAP Connectivity settings enable the Sametime server to connect to one or more LDAP servers. The Sametime server can be configured to search and authenticate against one LDAP directory on each LDAP server to which it connects.

Accessing LDAP Connectivity settings
To access the LDAP Connectivity settings, select LDAP Directory - Connectivity from the Sametime Administration Tool.

If you change a Connectivity setting, you must restart the server for the change to take effect.

LDAP Connectivity settings
The individual Connectivity settings are listed below. Detailed information on each setting is provided in subsequent topics. The LDAP Connectivity settings include:

- Host name or IP address of the LDAP server
- Position of this server in the search order
- Port
- Administrator distinguished name and password for authenticated binding
- Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server
- Adding or removing an LDAP server

Host name or IP address of the LDAP server
Use the "Host name or IP address of the LDAP server" setting to select the IP address (or fully qualified DNS name) of the LDAP server for which you want to change LDAP Connectivity settings. After selecting the Host name or IP address of the LDAP server, you can change any of the LDAP Connectivity settings listed below:

- Position of this server in the search order
- Port
- Administrator distinguished name and password for authenticated binding
- Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server
- Adding or removing an LDAP server

Position of this server in the search order
If you have configured the Sametime server to connect to multiple LDAP servers, use the "Position of this server in the search order" setting to specify the order in which Sametime will connect to the LDAP servers.

Note: To configure Sametime to connect to multiple servers, see Adding or removing an LDAP server

For example, if you select "1" for this setting, Sametime will search the LDAP directory on the specified LDAP server before searching any other LDAP directories available to Sametime.
Configuring the "Position of this server in the search order" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Host name or IP address of the LDAP server" drop-down list, select the name of the LDAP server for which you want to change the search order.
4. In the "Position of this server in the search order" text box, enter the search-order setting.
5. Click Update and restart the server for the change to take effect.

**Port**

Use the Port setting to specify the port over which the Sametime server connects to the LDAP server containing the LDAP directory. Set this port to the port number on which the LDAP server listens for TCP/IP connections. The default port for LDAP access and recommended setting is TCP/IP port 389.

Configuring the Port setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Host name or IP address of the LDAP server" drop-down list, select the name of the LDAP server for which you want to change the LDAP connection port.
4. In the Port setting, enter the port over which the Sametime server connects to the LDAP server. The default port number is 389.
5. Click Update and restart the server for the change to take effect.

**Administrator distinguished name and password for authenticated binding**

When the Sametime server connects to the LDAP server, the Sametime server can bind to the LDAP server as either an anonymous or authenticated user. The "Administrator distinguished name" and "Administrator password" settings determine whether the Sametime server binds to the LDAP server as an anonymous or authenticated user.

**Binding to the LDAP server as an anonymous user:** If the "Administrator distinguished name" and "Administrator password" settings do not contain entries, the Sametime server binds to the LDAP server as an anonymous user.

In this case, you must ensure the LDAP server is configured appropriately for anonymous access from a Sametime server. The LDAP server must allow anonymous binding and allow anonymous access to the attributes of the LDAP directory entries as described in [Required LDAP directory access](#).

**Note:** If you are using SSL to encrypt connections between the Sametime and LDAP servers, and you want to encrypt only the passwords transmitted between the Sametime and LDAP servers, you must allow Sametime to bind to the LDAP server as an anonymous user. For more information, see [Using SSL to encrypt connections between the Sametime and LDAP servers](#).

**Binding to the LDAP server as an authenticated user:** If you want the Sametime server to bind to the LDAP server as an authenticated user, you must enter an appropriate user name and password in the "Administrator distinguished name" and "Administrator password" fields. The Sametime server will transmit this user...
name and password to the LDAP server when making its initial connection to the
LDAP server. The LDAP server verifies this user name and password against an
entry in the LDAP directory to authenticate the connection from the Sametime
server. Some notes about the "Administrator distinguished name" and
"Administrator password" settings are included below:

- **Administrator distinguished name** - Use this setting to specify the
  Distinguished name of an LDAP directory entry that the Sametime server uses
  when binding to the LDAP directory.

  IBM Lotus software recommends that you create a unique directory entry that is
  used only for the purpose of authenticating connections from the Sametime
  server to the LDAP server.

  After creating the directory entry, you must ensure this directory entry has the
  appropriate access rights on the LDAP server. This directory entry must have at
  least read access to the attributes of the LDAP directory entries. For more
  information on the level of LDAP directory access required for the Administrator
distinguished name directory entry, see "Required LDAP directory access" below.

- **Administrator password** - Use this setting to specify the password associated
  with the "Administrator distinguished name" directory entry described above.

**Required LDAP directory access**: When accessing the LDAP directory, the
Sametime server must have access to specific attributes of the LDAP directory
entries. If you leave the "Administrator distinguished name" and "Administrator
password" settings blank to allow anonymous binding to the LDAP directory, the
Sametime server must be able to access the LDAP directory entry attributes listed
below as an anonymous user.

If you place entries in the "Administrator distinguished name" and "Administrator
password" fields to enable authenticated binding to the LDAP server, the
"Administrator distinguished name" directory entry you specify must be able to
access LDAP directory entry attributes as described below.

For Person and Group entries, the Sametime server must have access to the
following LDAP directory attribute entries:

- **ObjectClass**

- Any LDAP directory entry attribute that is specified in any search filter defined
  in the LDAP Directory Settings in the Sametime Administration Tool (or on the
  LDAP document in the Configuration database on the Sametime server)

For Person entries, the Sametime server must have access to the following
attributes:

- The attribute used as the person name
- The attribute used as the person description
- The attribute used to define the home Sametime server

For Group entries, the Sametime server must have access to the following
attributes:

- The attribute used as the group name
- The attribute used as the group description (if this setting is not empty)
- The attribute used to hold names of the group’s members

Enabling authenticated or anonymous binding to the LDAP server:

1. From the Sametime server home page, click the "Administer the Server" link to
   open the Sametime Administration Tool.

3. In the "Host name or IP address of the LDAP server" drop-down list, select the LDAP server for which you want to enable authenticated or anonymous binding.

4. To enable authenticated binding to the LDAP server:
   - Enter a user name in the "Administrator distinguished name" field.
     
     **Note** This user name must meet the requirements discussed in the "Binding to the LDAP server as an authenticated user" and "Required LDAP directory access" sections of this topic.
   - Enter the password associated with the administrator distinguished name in the "Administrator password" field.

To enable anonymous binding to the LDAP server, delete any entries that appear in the "Administrator distinguished name" or "Administrator password" fields. If these fields are blank, the Sametime server binds to the LDAP server as an anonymous user.

If you allow anonymous binding, review the information in the "Binding to the LDAP server as an anonymous user" and "Required LDAP directory access" sections of this topic.

5. Click Update and restart the server for the change to take effect.

**Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server**

For tighter security, the Sametime administrator can use SSL to encrypt the connections between the Sametime and LDAP servers.

The administrator selects the "Use SSL to authenticate and encrypt the connections between the Sametime server and the LDAP server" setting to encrypt the connections between the Sametime server and the LDAP server. For more information, see the section "Using SSL to encrypt connections between the Sametime and LDAP servers" later in this chapter.

If this setting is not selected, the directory information and passwords transmitted between the Sametime and LDAP servers are not encrypted.

**Adding or removing an LDAP server**

Sametime can connect to multiple LDAP servers. Use the "Adding another LDAP server" setting to enable the Sametime server to connect to a new LDAP server. Sametime can access one LDAP directory on each LDAP server to which it connects.

If you no longer want the Sametime server to access an LDAP server, you can remove the LDAP server from the list of available servers.

When adding an LDAP directory server, you must also specify a position for the server in the search order.

**To remove an LDAP server:** To remove the LDAP server from the list of available servers:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Host name or IP address of the LDAP server" drop-down list, select the name of the LDAP server you want to remove.
4. Click the Remove button.
5. Restart the Sametime server.

To add a new LDAP server: To enable the Sametime server to connect to a new LDAP server, you must perform two procedures:
1. Add the new LDAP server in the Sametime Administration Tool
2. Create a Directory Assistance document for the new LDAP server

Instructions for each of these procedures are included below.

Adding a new LDAP server in the Sametime Administration Tool: To add a new LDAP server in the Sametime Administration Tool:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. Below the "Adding an LDAP Server" heading, type the host name or IP address of the new LDAP server.
4. In the Port field below the "Adding an LDAP Server" heading, specify the port on which you want to connect to the new LDAP server.
5. Configure the LDAP Directory Settings (Connectivity, Basics, Authentication, Searching, and Group Contents) that enable Sametime to search and authenticate against the LDAP directory on the new LDAP server.
6. After you have set and updated all Sametime LDAP configuration options, restart the Sametime server.

Create a Directory Assistance document for the new LDAP server: The Directory Assistance database on the Sametime server must contain a Directory Assistance document that enables the Sametime server to access the LDAP server. To create the Directory Assistance document, use the procedure described in Create a Directory Assistance document that enables the Sametime server to access the LDAP server later in this chapter.

Configuring the LDAP Basics settings
The LDAP Basics settings enable the administrator to specify the basic LDAP parameters required to conduct searches for people and group entries in an LDAP directory. The administrator specifies one set of parameters for people searches and a separate set of parameters for group searches.

Accessing the LDAP Basics settings
To access the LDAP Basics settings, select LDAP Directory - Basics from the Sametime Administration Tool.

Configuring LDAP Basics settings for People
The LDAP Basics settings for People are listed below. Detailed information on each setting is provided in subsequent topics. The LDAP Basics settings for People are:

- Where to start searching for people
- Scope for searching for a person
- The attribute of the person entry that defines the person’s name
- Attribute used to distinguish between two similar person names
- The object class used to determine if an entry is a person
- Attribute of a person entry that defines the person’s e-mail address
Configuring LDAP Basics settings for Groups

The LDAP Basics settings for Groups are listed below. The LDAP Basics settings for Groups are:

- **Where to start searching for groups**
- **Scope for searching for groups**
- **Attribute used to distinguish between two similar group names**
- **The group object class used to determine if an entry is a group**

Where to start searching for people

The Sametime client user interfaces allow a user to search for individual users in the LDAP directory.

Use the "Where to start searching for people" setting to specify the base object of the directory (or level of the directory) from which to start a search for person entries in the LDAP directory.

The default setting of "" begins the search from the root of the directory.

**Note:** Before accepting the default setting (""), be aware that some LDAP directory servers allow the "" value only for searching the LDAP directory root DSE (Directory Server Entry, or entry with directory server properties) and only when the search scope is confined to "One level" below the "Where to start searching for people" setting. Also, searching from the root of an LDAP directory generally results in a less efficient search than specifying a specific base object such as **ou=west, o=acme**.

The setting you specify for the "Where to start searching for people" setting is entirely dependent on the directory schema of the LDAP directory the Sametime server is accessing. Example settings are:

- **ou=west, o=acme**
  
  or

- **o=acme**

In the first example, the search for the person entry begins from the LDAP directory base object **ou=west, o=acme**. In the second example, the search for the person entry begins from the base object **o=acme**.

The extent of the search for person entries is further controlled by the **Scope for searching for a person** setting.

Suggested values for this setting are:

- **Microsoft Active Directory** - **cn=users, dc=domain, dc=com**
- **Netscape Directory** - **o=organizational unit/(i.e. computer name)**
- **Microsoft Exchange 5.5 Directory** - **cn=Recipients, ou=computername, o=domain**
- **Domino Directory** - **o=organizational unit**
- **SecureWay Directory** - **dc=domain, dc=com**

Configuring the "Where to start searching for people" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Where to start searching for people" setting.

4. In the "Where to start searching for people" setting, enter the base object of the LDAP directory from which to start the search for a person entry (for example, ou=west, o=acme).

5. Click Update and restart the server for the change to take effect.

Scope for searching for a person

Use the "Scope for searching for a person" setting to specify how many LDAP directory levels below the "Where to start searching for people" setting to search when resolving a search for a person entry.

The two available settings are Recursive and One level. Recursive is the default value.

Recursive: Type recursive to search the entire subtree of directory entries beneath the "Where to start searching for people" setting (or the base object of the search).

For example, assume the "Where to start searching for people" setting has the value "ou=west, o=acme" and the "Scope for searching for a person" setting has the value "recursive."

Now assume the user searches on the name "John Smith." The search begins at the ou=west, o=acme directory level and searches the entire subtree of the directory beneath that level.

Such a search might return the following names, depending on the organization of the directory:
• cn=John Smith, ou=managers, ou=marketing, ou=west, o=acme
• cn=John Smith, ou=engineering, ou=west, o=acme
• cn=John Smith, ou=west, o=acme

The search would fail to turn up the following directory entries because the "Where to start searching for people" setting in this example begins the search at the ou=west, o=acme level of the directory:
• cn=John Smith, o=acme
• cn=John Smith, ou=engineering, ou=east, o=acme

Note: The Search filter for resolving person names setting provides the search filter that resolves the user’s input (John Smith) to a specific person entry in the LDAP directory.

One level: Type one level to search only the level immediately below the "Where to start searching for people" setting.

For example, assume the "Where to start searching for people" setting has the value ou=west, o=acme and the "Scope for searching for a person" setting has the value "one level."

Now assume the user searches on the name "John Smith." The search begins at the ou=west, o=acme level and searches only one directory level beneath that level.
Such a search might return the following names, depending on the organization of the directory:

- cn=John Smith, ou=west, o=acme
- cn=John Smithson, ou=west, o=acme

The search would fail to find the following directory entries because the entries are more than one level below the "Where to start searching for people" setting or are not found beneath the "Where to start searching for people" setting:

- cn=John Smith, ou=marketing, ou=west, o=acme
- cn=John Smith, ou=engineering, ou=east, o=acme.

To configure the "Scope for searching for a person" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to set the "Scope for searching for a person" setting.
4. In the "Scope for searching for a person" setting, type recursive or one level. Recursive is the default setting.
5. Click Update and restart the server for the change to take effect.

The attribute of the person entry that defines the person’s name

The "The attribute of the person entry that defines the person’s name" setting specifies the attribute of an LDAP directory person entry that is used to display a user’s name in the Sametime end-user interfaces (as the result of a search or in a privacy or presence list).

The value of this setting can be any attribute of the LDAP directory person entry, such as cn (common name), sn (surname), givenname, or mail (e-mail address).

For example, consider an LDAP person entry containing the following attributes:

- cn - James Lock
- givenname - James
- sn - Lock
- mail - jlock@acme.com

In this example, if the "The attribute of the person entry that defines the person’s name" setting is "cn," the search result displays the user’s name as James Lock. If the "The attribute of the person entry that defines the person’s name" setting is mail, the user’s name displays as jlock@acme.com.

The suggested value for Microsoft Exchange 5.5 Directory, Microsoft Active Directory, Netscape Directory, Domino Directory servers, and SecureWay servers is "cn."

Note: You can also write a Java class to control the format of user names returned from LDAP directory searches. This capability is useful if you want user names to display in a format that is not specified by an LDAP directory entry attribute. For more information, see Using a custom Java class to control the format of user names returned in LDAP directory searches later in this chapter.
To configure the "The attribute of the person entry that defines the person’s name" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "The attribute of the person entry that defines the person’s name" setting.
4. In the "The attribute of the person entry that defines the person’s name" setting, enter the appropriate attribute.
5. Click Update and restart the server for the change to take effect.

Attribute used to distinguish between two similar person names
Use the "Attribute used to distinguish between two similar person names" setting to specify the attribute of a person entry that is used to differentiate between two users that have the same common name (cn) attribute.

This setting can specify any attribute of a person entry that can differentiate one person from another person that has the same name. An example value for this setting is the mail attribute. The mail attribute contains the e-mail address of an LDAP directory person entry.

To illustrate, assume that a search on the name John Smith returns two person entries with the common name (cn) John Smith. Since the two John Smiths will have different e-mail addresses, the mail attribute can be displayed to enable the user to determine which John Smith is the correct one.

Suggested values for this setting are:
- Microsoft Exchange 5.5 Directory, Netscape Directory, Domino Directory, SecureWay Directory: mail
- Microsoft Active Directory: user principal name

To configure the "Attribute used to distinguish between two similar person names" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Attribute used to distinguish between two similar person names" setting.
4. In the "Attribute used to distinguish between two similar person names" setting, enter the appropriate attribute.
5. Click Update and restart the server for the change to take effect.

The object class used to determine if an entry is a person
In some situations, Sametime must determine whether a person entry returned by a search is a person or group entry. Use the "The object class used to determine if an entry is a person" setting to specify the attribute of a directory entry that identifies the entry as a person.
Sametime assumes that individual users are represented by entries with a unique objectclass. Sametime compares the name of the objectclass specified in this setting to the objectclass values of each entry to decide whether the entry is a person or a group.

Enter the objectclass attribute used for people in the LDAP schema of the LDAP directory in your environment.

The suggested value for Microsoft Exchange 5.5 Directory, Microsoft Active Directory, Netscape Directory, Domino Directory, and SecureWay Directory is "organizationalPerson."

**To change this setting:** To set the "The object class used to determine if an entry is a person" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basic settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "The object class used to determine if an entry is a person" setting.
4. In the "The object class used to determine if an entry is a person" setting, enter the objectclass value that identifies a directory entry as a person (for example, "organizationalPerson").
5. Click Update and restart the server for the change to take effect.

**Attribute of a person entry that defines a person’s e-mail address**

Use the "Attribute of a person entry that defines a person’s e-mail address" setting to specify the attribute of a person entry that contains the user’s e-mail address.

This setting is required by components of the Sametime server that use the Session Initiation Protocol (SIP), such as the SIP Gateway. SIP entities are identified by their e-mail addresses.

Suggested values for this setting are:
- **Microsoft Exchange 5.5 Directory, Netscape Directory, Domino Directory, SecureWay Directory**: mail
- **Microsoft Active Directory**: user principal name

**To configure the "Attribute of a person entry that defines a person’s e-mail address" setting:**
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basic settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Attribute of a person entry that defines a person’s e-mail address" setting.
4. In the "Attribute of a person entry that defines a person’s e-mail address" setting, enter the appropriate attribute.
5. Click Update and restart the server for the change to take effect.
**Where to start searching for groups**

The Sametime client user interfaces allow a user to search for groups in the LDAP directory.

Use the "Where to start searching for groups" setting to specify the base object of the directory (or level of the directory) from which to start a search for group entries in the LDAP directory.

The default setting of "" begins the search from the root of the directory.

**Note:** Before accepting the default setting (""), be aware that some LDAP Directory servers allow the "" value only for searching the LDAP directory root DSE (Directory Server Entry, or entry with directory server properties) and only when the search scope is confined to "One level" below the "Where to start searching for groups" setting. Also, searching from the root of an LDAP directory generally results in a less efficient search than setting a specific base object (such as ou=west, o=acme) for the search.

The setting you specify in the "Where to start searching for groups" setting is entirely dependent on the directory schema of the LDAP directory in your environment. Example settings are:

- **ou=west, o=acme**
  - or
  - **o=acme**

In the first example, the search for the group entry begins from the LDAP directory base object ou=west, o=acme. In the second example, the search for the group entry begins from the base object o=acme.

The extent of the search for group entries is further controlled by the **Scope for searching for groups** setting.

Suggested values for this setting are:

- **Microsoft Active Directory** - cn=users, dc=domain, dc=com
- **Netscape Directory** - o=organizational unit/(i.e. computer name)
- **Microsoft Exchange 5.5 Directory** - cn=Recipients, ou=computername, o=domain
- **Domino Directory** - o=organizational unit.
- **SecureWay Directory** - dc=domain, dc=com

**To configure the "Where to start searching for groups" setting:**

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Where to start searching for groups" setting.
4. In the "Where to start searching for groups" setting, enter the base object of the LDAP directory from which to start the search for a group entry (for example, ou=west, o=acme).
5. Click Update and restart the server for the change to take effect.
**Scope for searching for groups**

Use the "Scope for searching for groups" setting to specify how many levels below the "Where to start searching for groups" setting to search when resolving a search for a group entry in the LDAP directory.

The two available settings are Recursive and One level. Recursive is the default value.

**Recursive:** Type recursive to search the entire subtree of directory entries beneath the "Where to start searching for groups" setting.

For example, assume the "Where to start searching for groups" setting has the value ou=west, o=acme, and the "Scope for searching for groups" setting has the value "recursive."

Now assume the user searches on the name "Marketing." The search begins at the ou=west, o=acme level and searches the entire subtree of the directory beneath that level. Such a search might return the following group names, depending on the organization of the directory:

- cn=Marketing, ou=Los Angeles, ou=west, o=acme
- cn=Marketing, ou=San Diego, ou=west, o=acme
- cn=Marketing, ou=west, o=acme

The search would fail to turn up directory entries such as:

- cn=Marketing, o=acme
- cn=Marketing, ou=Pittsburgh, ou=west, o=acme

**Note:** The [Search filter for resolving group names](#) setting provides the search filter that resolves the user’s input (Marketing) to a specific group entry in the LDAP directory.

**One level:** Type one level to search only the level of directory entries immediately below the "Where to start searching for groups" setting.

For example, assume the "Where to start searching for groups" setting has the value ou=west, o=acme, and the "Scope for searching for groups" setting has the value "one level."

Now assume the user searches on the name Marketing. The search begins at the ou=west, o=acme level and searches only one level beneath that level.

Such a search might locate a group entry such as:

- cn=Marketing, ou=west, o=acme

The search would fail to turn up a directory entry such as:

- cn=Marketing, ou=Los Angeles, ou=west, o=acme

**To configure the "Scope for searching for groups" setting:**

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Scope for searching for groups" setting.
4. In the "Scope for searching for groups" setting, type **recursive** or **one level**. Recursive is the default setting.
5. Click Update and restart the server for the change to take effect.

**Attribute used to distinguish between two similar group names**
Use the "Attribute used to distinguish between two similar group names" setting to specify the attribute of a group entry that is used to differentiate between two groups that have the same common name (cn) attribute.

An example of a value for this setting is the "info" attribute of an LDAP group entry. In many LDAP directories, the "info" attribute contains descriptive information about a group.

For example, assume that a search on the name "Marketing" returns two group entries with the common name Marketing. The information contained in the info attribute (such as "West region" or "East region") of the group entry can be used to distinguish between the two groups.

Suggested values for this setting are:
- Microsoft Exchange 5.5 Directory - info

**To configure the "Attribute used to distinguish between two similar group names" setting:**
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basics settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Attribute used to distinguish between two similar group names" setting.
4. In the "Attribute used to distinguish between two similar group names" setting, enter the appropriate attribute.
5. Click Update and restart the server for the change to take effect.

**The group object class used to determine if an entry is a group**
In some situations, Sametime must determine whether a directory entry returned by a search is a person or group entry. Use the "The group object class used to determine if an entry is a group" setting to specify the attribute of a directory entry that identifies the entry as a group.

Sametime assumes that groups are represented by entries with a unique objectclass. Sametime compares the name of the objectclass specified in this setting to the objectclass values of each entry to decide whether the entry is a group or a person.

Enter the objectclass attribute used for groups in the LDAP schema of the LDAP directory in your environment.

Suggested values for the setting are:
- Microsoft Active Directory - group
- Netscape Directory - groupOfUniqueNames
- Microsoft Exchange 5.5 and Domino Directories - groupOfNames
SecureWay Directory - groupOfUniqueNames

To change "The group object class used to determine if an entry is a group" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Basic settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "The group object class used to determine if an entry is a group" setting.
4. In the "The group object class used to determine if an entry is a group" setting, enter the objectclass value that identifies a directory entry as a group (for example, "groupOfNames" or "groupOfUniqueNames").
5. Click Update and restart the server for the change to take effect.

Configuring LDAP Authentication settings

The LDAP Authentication settings are listed below. Detailed information on each setting is provided in subsequent topics. The LDAP Authentication settings are:

- Search filter to use when resolving a user name to a distinguished name
- Home Sametime Server

Search filter to use when resolving a user name to a distinguished name

To authenticate a user, Sametime must know the Distinguished Name (DN) of the user’s person entry in the LDAP directory. The “Search filter to use when resolving a user name to a distinguished name” resolves the name (or text string) provided by a user to a DN for authentication purposes.

To illustrate, consider the following default search filter in which the value "%s" is substituted for the string provided by the user when logging in:

```
(&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s*)))
```

Note: You can find detailed information on the syntax and formatting of search filters at the following Web site:

The default search filter above first performs a search for all entries of the type (or objectclass) organizationalPerson. The search filter then looks for an exact match with either the common name (cn), given name, or surname (sn) attribute of the person entry. If the search locates a person entry with an attribute value that matches the text string provided by the user, the Sametime server accesses the person entry with that DN when authenticating the user.

The specific search filter used for this setting must be based on the schema of the LDAP directory the Sametime server is accessing.

The default value is the suggested value for Microsoft Exchange 5.5, Microsoft Active Directory, Netscape Directory, Domino Directory, and SecureWay Directory servers.

Note: In some cases, for Microsoft Active Directory it may be necessary to substitute (user principal name=%s*) for (mail=%s*) in the default search filter shown above.
To configure the "Search filter to use when resolving a user name to a distinguished name" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Authentication for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Search filter to use when resolving a user name to a distinguished name" setting.
4. In the "Search filter to use when resolving a user name to a distinguished name" setting, enter the search filter appropriate for the LDAP directory schema.
5. Click Update and restart the server for the change to take effect.

Setting the Home Sametime Server setting for LDAP

The home Sametime server is the Sametime server on which the preferences and data of a Community Services user are saved. Users connect to the home Sametime server for presence and chat functionality. If you have installed multiple Sametime servers, each user’s person entry in an LDAP directory must contain a field in which a user’s home Sametime server can be specified.

Note: For more information on the purpose of the home Sametime server, see Connecting to the Home Sametime server

To support the Home Sametime Server setting requirement in an LDAP environment, the administrator must do one of the following:

- Manually add a field to the LDAP directory to hold the name of each user’s home Sametime server. This added field must appear in the person entry of every Sametime user in the LDAP directory.
- Use a field that already exists in the person entries of each Sametime user (such as the e-mail address) for this purpose.

Use the LDAP Home Sametime Server setting in the Sametime Administration Tool to enter the name of the field that the administrator uses to hold the name of each Sametime server. This entry can specify a the name of the field that the administrator has added to the LDAP directory or the name of an existing field in the LDAP directory person entries that the administrator chooses for this purpose.

To set the home Sametime server setting for LDAP:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Authentication for server" drop-down list, select the appropriate LDAP server.
4. In the "Home Sametime server" setting, enter the name of the field in each user’s LDAP person entry that contains the name of the user’s home Sametime server.
5. Click Update and restart the server for the change to take effect.

After the administrator has added the home "Sametime server" field to the person entries in the LDAP directory, and specified the name of this field in the LDAP Directory - Authentication settings of the Sametime Administration Tool, the administrator must populate the home "Sametime server" field in each person entry in the LDAP directory.
For each person entry in the LDAP directory, enter the name of a Sametime server in the home "Sametime server" field. Use the full canonical name of the Sametime server (for example, cn=sametime.acme.com/ou=west/o=acme) when entering the server name in the "Sametime server" field in the LDAP directory.

Note: The server name in the LDAP directory is matched to the server name in the Servers view ($Servers) of the Domino Directory. The name entered in the "Sametime server" field in the person entries of the LDAP directory should match the name of the Sametime server as it appears in the Servers view of the Domino Directory.

The user connects to this server for presence and chat functionality. You should try to assign an equal number of users to each Sametime server to spread the load evenly among multiple servers. For more information about working with multiple Sametime servers, see Advantages of using multiple Sametime servers.

Configuring the LDAP Searching setting

The LDAP Searching settings are listed below. Detailed information on these settings are provided in subsequent topics. The LDAP Searching setting is:

- **Search filter for resolving person names**
- **Search filter for resolving group names**

Search filter for resolving person names

To search for a user name, a Sametime end user enters a text string in the user interface of a Sametime client. The "Search filter for resolving person names" setting defines the LDAP search filter responsible for selecting a user name from the LDAP directory. This search filter matches the text string provided by the user to information contained within the attributes of LDAP directory person entries.

To illustrate, consider the following default search filter in which the value "%%s" represents the text string provided by the user:

\[
(&(objectclass=organizationalPerson)\%(cn=%%s)\%(givenname=%%s)\%(sn=%%s)\%(mail=%%s)\%))
\]

Note: You can find detailed information on the syntax and formatting of search filters at the following Web site:

The default search filter first looks for entries whose type (or object class) is organizationalPerson. The search filter looks for a prefix match ("%%s") with an entry’s common name, a complete match with an entry’s given name, or a complete match with the entry’s surname attribute.

Using the default search filter, a search on the person name “James” might return the following directory entries (provided that each directory entry is of the objectclass organizationalPerson).

- Jameson Sanders
- James Lock
- James Clark
- Henry James

Note: The "Where to start searching for people" and "Scope for searching for a person" settings in the Basics - People settings of the Sametime Administration Tool define the level of the directory tree from which the search begins and how much of the directory is searched.
The suggested value for this setting for Microsoft Exchange 5.5, Microsoft Active Directory, Netscape Directory, Domino Directory, and SecureWay Directory servers is:

```c
(&(objectclass=organizationalPerson)(|(cn=%s*)(givenname=%s*)(sn=%s*)(mail=%s*))
```

In some cases, Microsoft Active Directory may require you to substitute (user principal name=%s*) for (mail=%s*) in the search filter shown above.

**Note:** If a single search filter is not adequate to resolve user searches in your environment, you can create a custom Java class that refines the user search capabilities. This capability is useful in environments with complex LDAP directory schemas. For more information, see [Using a custom Java class to control LDAP directory searches for people and groups](http://developer.netscape.com/docs/manuals/directory/41/ag/find.htm#1046960) later in this chapter.

**To configure the “Search filter for resolving person names” setting:**
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Search settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Search filter for resolving person names" setting.
4. In the "Search filter for resolving person names" setting, enter the search filter appropriate for the LDAP directory schema.
5. Click Update and restart the server for the change to take effect.

**Search filter for resolving group names**

To search for a group name, a Sametime end user enters a text string in the user interface of a Sametime client. The "Search filter for resolving group names" defines the LDAP search filter responsible for selecting the group name from an LDAP directory. This search filter matches the text string provided by the user to values listed for the attributes of the LDAP directory group entries.

To illustrate, consider the following default search filter in which the value "%s" is substituted for the text string supplied by the user:

```c
(&(objectclass=groupOfNames)(cn=%s*))
```

**Note:** You can find detailed information on the syntax and formatting of search filters at the following Web site:


The default search filter first looks for directory entries of the type (or object class) groupOfNames. The search filter then looks for a prefix match (%s*) with the common name (cn) attribute of the groupOfNames entries.

Using the search filter above, a search on the name "Market" might return the following group entries from the directory (provided that each entry also has the groupOfNames objectClass attribute):

- Marketing
- Marketers
- Markets

**Note:** The "Where to start searching for groups" and "Scope for searching for groups" settings in the Basics - Groups settings of the Sametime...
Administration Tool define the level of the directory tree from which the search begins and how much of the directory is searched.

The search filter used for resolving group names must be based on the schema of your LDAP directory. The suggested value for Microsoft Exchange 5.5 and Domino directory servers is the default value discussed above.

The other suggested values for this setting are:

- **Microsoft Active Directory:**
  
  `(&(objectClass=group)(cn=%s*))`

- **Netscape Directory and SecureWay Directory:**
  
  `(&(objectClass=groupOfUniqueNames)(cn=%s*))`

**Note:** If a single search filter is not adequate to resolve group searches in your environment, you can create a custom Java class that refines the group search capabilities. This capability is useful in environments with complex LDAP directory schemas. For more information, see Using a custom Java class to control LDAP directory searches for people and groups later in this chapter.

To configure the "Search filter for resolving group names" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Search settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Search filter for resolving group names" setting.
4. In the "Search filter for resolving group names" setting, enter the search filter appropriate for the LDAP directory schema.
5. Click Update and restart the server for the change to take effect.

### Configuring the LDAP Group Contents setting

The LDAP Group Contents setting is listed below. Detailed information on this setting is provided in a subsequent topic. The LDAP Group Contents settings is:

- Attribute in the group object class that has the names of the group members

**Attribute in the group object class that has the names of the group members**

If an end user adds a group to a presence list, privacy list, or a list that restricts meeting attendance, Sametime must obtain the list of members within the group so that individual members of the group can be displayed. The "Attribute in the group object class that has the names of the group members" setting defines the attribute within an LDAP directory group entry that holds the names of all members of the group.

Suggested values for this setting are:

- **Microsoft Active Directory, Microsoft Exchange 5.5 Directory, and Domino Directory:** member
- **Netscape Directory and IBM Secureway Directory:** UniqueMember

This setting assumes that the LDAP directory schema uses a single directory entry to represent a group, and that names of group members are held in one attribute.
that contains multiple values. This assumption is true for Microsoft Exchange 5.5, Microsoft Active Directory, Netscape Directory, and Domino 5 environments.

To configure the "Attribute in the group object class that has the names of the group members" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Settings for determining the content of groups for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Attribute in the group object class that has the names of the group members" setting.
4. In the "Attribute in the group object class that has the names of the group members" setting, enter the appropriate group entry attribute.
5. Click Update and restart the server for the change to take effect.

Using SSL to encrypt connections between the Sametime and LDAP servers

When Sametime is configured to connect to an LDAP server, the Sametime server makes five separate connections to the LDAP server. Sametime makes a separate connection to the LDAP server to perform each of these five tasks:

- Authenticate users
- Resolve a user name to a distinguished name as part of the login procedure
- Resolve user and group names (for example, as a response to an "Add Person or Group" request from a Sametime Connect client)
- Browse the directory
- Get the content of public groups

The Sametime and LDAP servers exchange directory information, including user names and passwords, over these connections. To ensure this information is secure, the administrator can use SSL to encrypt the data that passes over these connections. The administrator should consider the level of protection required before enabling SSL. Using SSL to encrypt these connections can slow the server performance. The administrator has the following options when using SSL to encrypt the data transmitted between the Sametime and LDAP servers:

- **Encrypt all data** - This option encrypts all directory information (both user names and passwords) that is transmitted between the Sametime server and the LDAP server. If you encrypt all data, all five connections between the Sametime server and LDAP server are encrypted with SSL. This option provides the most security but also has the greatest effect on server performance.

- **Encrypt only user passwords** - This option encrypts passwords but not other directory information (such as user names) passing over the connections between the Sametime and LDAP servers. If you encrypt only user passwords, only the "authenticating users" connection between the Sametime server and the LDAP server is encrypted with SSL. This option provides an intermediate level of security and has less affect on server performance than encrypting all of the data.

- **Encrypt no data** - This option allows all directory information and passwords to pass unencrypted between the Sametime and LDAP servers. This option does not affect server performance and should be used if the administrator feels there
is no chance that an unauthorized user can intercept information transmitted over the connections between the Sametime and LDAP servers.

**Note:** If you are encrypting connections between an AIX version of the Sametime server and an LDAP directory, xlC.aix50.rte must be 6.0.0.3 (or higher).

### Using SSL to encrypt all data transmitted between the Sametime and LDAP servers

The administrator can use SSL to authenticate and encrypt all data passing over all five connections between the Sametime and LDAP servers. Encrypting all data passing between the Sametime and LDAP servers provides the highest level of security but can slow the performance of the Sametime server.

Encrypting all data transmitted between the Sametime and LDAP servers involves three basic procedures:

- Enabling the "Use SSL to authenticate and encrypt the connection between the Sametime and the LDAP server" setting in the Sametime Administration Tool.
- Modifying the Directory Assistance document of the LDAP server to encrypt the connection between the servers.
- Ensuring that the Sametime server trusts the server certificate of the LDAP server.

To encrypt all data passing between the Sametime and LDAP servers, follow the steps below.

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Host name or IP address of the LDAP server" drop-down list, select the name of the LDAP server to which you want to connect using SSL.
4. Select the "Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server" option.
5. In the "LDAP SSL port" field, specify the port on which the LDAP server is listening for SSL LDAP connections. The default port for this setting is port 636.
6. Click Update and close the Sametime Administration Tool.
7. Perform the procedure described in the Directory Assistance document of the LDAP server to encrypt the connection between the servers later in this chapter.
8. Ensure the Sametime server trusts the LDAP server certificate by performing the procedure below that is appropriate for your platform. Each of these procedures is described later in this chapter.
   - Ensuring that the Sametime server trusts the LDAP server certificate (Windows and AIX/Solaris servers)
   - Ensuring that the Sametime server trusts the LDAP server certificate (i5/OS servers)
9. Stop and restart the Sametime server.

### Using SSL to encrypt only user passwords passing between the Sametime and LDAP servers

The administrator can use SSL to encrypt passwords but not directory information (such as user names) passing over the connection between the Sametime and
LDAP servers. This option provides an intermediate level of security and affects server performance less than encrypting all data that is transmitted between the Sametime and LDAP servers.

When Sametime is configured in this way, only one connection between the Sametime and LDAP server is encrypted with SSL; the encrypted connection is the "authenticating users" connection. Data passing over the other four connections between the Sametime and LDAP servers is not encrypted. In this scenario, the Sametime server must bind to the LDAP server as an anonymous user.

**Note:** Data that passes over the "authenticating users" connection includes the user names and passwords that all users enter to authenticate when creating or attending meetings, or logging in to Sametime Connect. User names and passwords are never sent over the other four connections between a Sametime and LDAP server unless the Sametime server is required to authenticate when binding to the LDAP server. If the Sametime server is required to authenticate when binding to the LDAP server, instead of binding as an anonymous user, the user name and password the Sametime server uses to authenticate with the LDAP server is transmitted on all five connections between the Sametime server and the LDAP server. If you perform the configurations described here to encrypt only the "authenticating users" connection, and simultaneously require the Sametime server to bind to the LDAP server as an authenticated user, the user name and password Sametime uses to bind to the LDAP directory is passed in the clear on four connections between the Sametime and LDAP server. To prevent the Sametime server from transmitting this user name and password on four unencrypted connections, the Sametime server must bind to the LDAP server as an anonymous user.

For more information about anonymous binding to the LDAP server, see [Administrator distinguished name and password for authenticated binding](#). For more information about connections to an LDAP server, see [Using SSL to encrypt connections between the Sametime and LDAP servers](#).

Encrypting user passwords passing between the Sametime and LDAP servers involves five basic procedures:

- Enabling the Sametime server to bind to the LDAP server as an anonymous user. To enable the Sametime server to bind to the LDAP server as an anonymous user, you must ensure that the "Administrator distinguished name" and "Administrator password" settings in the Sametime Administration Tool LDAP Directory-Connectivity settings do not contain entries. For more information, see [Administrator distinguished name and password for authenticated binding](#).
- Enabling the "Use SSL to authenticate and encrypt the connection between the Sametime and the LDAP server" setting in the Sametime Administration Tool.
- Modifying the ST_DB_LDAP_SSL_ONLY_FOR_PASSWORDS setting in the Sametime.ini file on the Sametime server.
- Modifying the Directory Assistance document of the LDAP server to encrypt the connection between the servers.
- Ensuring that the Sametime server trusts the certificate of the LDAP server.

To encrypt only user passwords passing between the Sametime and LDAP servers, follow the steps below.
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.


3. In the "Host name or IP address of the LDAP server" drop-down list, select the name of the LDAP server to which you want to connect using SSL.

4. Make sure that both the "Administrator distinguished name" and "Administrator password" fields are blank. If either of these fields contains an entry, remove the entry from the field. 

   Note: Clearing the entries from these fields ensures that the Sametime server will bind to the LDAP server as an anonymous user. For more information, see Administrator distinguished name and password for authenticated binding.

5. Select the "Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server" option.

6. In the "LDAP SSL port" field, specify the port on which the LDAP server is listening for SSL LDAP connections. The default port for this setting is port 636.

7. Click the Update button and close the Sametime Administration Tool.

8. Use a text editor to open the Sametime.ini file located in the C:\Lotus\Domino directory on the Sametime server.

9. In the Sametime.ini file, set the following parameter to "1."

   [Directory] ST_DB_LDAP_SSL_ONLY_FOR_PASSWORDS=1

   If set to 1, the ST_DB_LDAP_SSL_ONLY_FOR_PASSWORDS setting encrypts one of the five connections to the LDAP server. (Sametime uses SSL to encrypt the connection to the LDAP server over which users are authenticated.)

10. Save and close the Sametime.ini file.

11. Perform the procedure described in "Modifying the Directory Assistance document of the LDAP server to encrypt the connection between the servers" later in this chapter.

12. Ensure the Sametime server trusts the LDAP server certificate by performing the procedure below that is appropriate for your platform. Each of these procedures is described later in this chapter.

   • Ensuring that the Sametime server trusts the LDAP server certificate (Windows and AIX/Solaris servers)

   • Ensuring that the Sametime server trusts the LDAP server certificate (i5/OS servers)

13. Restart the Sametime server.

Allowing all data to pass unencrypted between the Sametime and LDAP servers

If the administrator is not concerned with unauthorized users intercepting transmissions between the Sametime and LDAP servers, the administrator should disable the "Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server" option in the LDAP Directory - Connectivity settings of the Sametime Administration Tool.

When this option is disabled, none of the connections between the Sametime and LDAP servers are encrypted with SSL and all directory information and passwords pass unencrypted between the two Sametime servers.
To disable the "Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server" option:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Host name or IP address of the LDAP server" drop-down list, select the name of the LDAP server to which Sametime connects.
4. Verify that the "Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server" option is not selected. If this option is selected, deselect it.
5. If you deselected the "Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server" option, click Update and restart the server for the change to take effect.

Note: If you had previously set the ST_DB_LDAP_SSL_ONLY_FOR_PASSWORDS parameter in the Sametime.ini file to 1 to encrypt only passwords, you should also set that parameter to "0" or remove it from the Sametime.ini file to prevent the encryption of the server-to-server connection that authenticates users.

Modifying the Directory Assistance document of the LDAP server to encrypt the connection between the Sametime server and the LDAP servers

This procedure is required when you use SSL to encrypt all data transmitted between the Sametime and LDAP server or use SSL to encrypt only user passwords that are transmitted between the Sametime and LDAP servers. For more information, see Using SSL to encrypt all data transmitted between the Sametime and LDAP servers or Using SSL to encrypt only user passwords passing between the Sametime and LDAP servers.

In this procedure, you modify the Directory Assistance document for the LDAP server to ensure that the connection between the Sametime server and the LDAP server is encrypted using SSL.

   - Choose File - Database - Open.
   - For Server, select Local.
   - Select the Directory Assistance database (da.nsf).
   - Click Open.
2. Double-click the Directory Assistance document for the LDAP server to open the document. (The Directory Assistance documents are displayed in the right pane of the Directory Assistance database.)
3. Click Edit Directory Assistance.
4. Click the LDAP tab.
5. In the "Perform LDAP search for" field, select the "Notes Clients/Web Authentication" option.
6. In the "Channel encryption" field, select SSL.
7. In the Port field, specify the same port that was specified in the "LDAP SSL port" field of the LDAP Directory - Connectivity options of the Sametime Administration Tool. (This port is the one on which the LDAP server listens for SSL connections. The default port for SSL connections is port 636.)
8. In the "Accept expired SSL certificates" field, select Yes (the default setting) to accept a certificate from the LDAP directory server, even if the certificate has expired. For tighter security, select No. If No is selected, the Sametime server checks the certificate expiration dates. If the certificate presented by the LDAP server has expired, the connection is terminated.

9. In the "SSL protocol version" field, select the version number of the SSL protocol to use. The choices are:
   - **V2.0 only** - This setting allows only SSL 2.0 connections.
   - **V3.0 handshake** - This setting attempts an SSL 3.0 connection. If this connection attempt fails but Sametime detects that SSL 2.0 is available on the LDAP server, Sametime attempts the connection using SSL 2.0.
   - **V3.0 only** - This setting allows only SSL 3.0 connections.
   - **V3.0 and V2.0 handshake** - This setting attempts an SSL 3.0 connection, but starts with an SSL 2.0 handshake that displays relevant error messages. This setting is used to receive V2.0 error messages when trying to connect to the LDAP server. These error messages might provide information about any compatibility problems found during the connection.
   - **Negotiated** - This setting allows SSL to determine the handshake and protocol version required.

10. In the "Verify server name with remote server’s certificate" field, select Enabled (the default setting) to verify the server name with the remote server’s certificate. If Enabled is selected, the Sametime server verifies the name of the LDAP server with the remote server’s certificate. If the names do not match, the connection is terminated. For more relaxed security, select Disabled (the server name is not verified with the certificate).

11. Click Save and Close to close the Directory Assistance document.


**Next step**

After modifying the Directory Assistance document of the LDAP server to encrypt the connection between the Sametime server and the LDAP servers, you must **Ensuring that the Sametime server trusts the LDAP server certificate (Windows and AIX/Solaris servers)**

This procedure is required when you use SSL to encrypt all data transmitted between the Sametime and LDAP server or use SSL to encrypt only user passwords that are transmitted between the Sametime and LDAP servers. For more information, see [Using SSL to encrypt all data transmitted between the Sametime and LDAP servers](#) or [Using SSL to encrypt only user passwords passing between the Sametime and LDAP servers](#)

Ensuring that the Sametime server trusts the LDAP server certificate (Windows and AIX/Solaris servers)

This procedure enables a Sametime server that operates on a Windows or AIX/Solaris platform to trust the SSL server certificate of the LDAP server. To ensure the Sametime server trusts the certificate of the LDAP server, the administrator must perform the following procedures:

- Install the IKeyMan program on the Sametime server.
- Create a key database on the Sametime server named "key.kdb" and store this database in the root Sametime directory.
- Ensure that the key.kdb database on the Sametime server contains the SSL trusted root certificate that enables the Sametime server to trust the SSL server certificate of the LDAP server.
These procedures are described below:

**Install the IKeyMan program on the Sametime server**

The Sametime server must have access to an SSL trusted root certificate to complete the SSL handshake when making an SSL connection to the LDAP server. This certificate is stored in an SSL key database. The tool provided with a Sametime 7.0 server to create the key database and manage SSL certificates for Sametime server to LDAP server connections is the IBM IKeyMan utility.

You must install the IBM IKeyMan utility on the Sametime server so that you can manage the SSL certificates required to encrypt connections between the Sametime server and LDAP server with SSL. Follow the instructions below to install IKeyMan on either a Windows or AIX/Solaris Sametime server.

**Installing IKeyMan on a Windows Sametime server**

To install IKeyMan onto the Windows Sametime server, the administrator must run the setup.exe file located on Sametime CD2 in the GSKit directory. For example, to install IKeyMan:

1. Insert the Sametime 7.0 server CD 2 into the Sametime server machine.
2. Open a command prompt on the Sametime server machine.
3. In the command prompt window, change to the CD drive.
4. In the command prompt window, change to the "GSKit" folder on the Sametime 7.0 server CD 2. (For example, enter "cd GSKit" at the command prompt.)
5. From the <CD drive>\GSKit directory, enter the following command: setup.exe GSKit <Sametime installation directory> -s f1setup.iss. For example, your command string might look like this:
   
   D:\GSKit>setup.exe GSKit C:\Lotus\Domino -s f1setup.iss
   
   This command performs a silent installation of the IKeyMan program into the Sametime installation directory on the Sametime server. If your Sametime server is installed into a directory other than C:\Lotus\Domino, use the installation directory that is appropriate for your environment in the command string.
6. To verify that the installation is successful, do the following:
   - Check that the C:\Lotus\Domino\IBM\GSK6 folder exists on the Sametime server.
   - Verify that the HKLM\Software\IBM\GSK6 registry key has been created on the Sametime server machine.
7. After installing the IBM IKeyMan utility, you must define the Java environment on the Sametime server machine. Follow the steps below:
   a. From the Windows desktop, right click on the My Computer icon and select "System Properties."
   b. Select the "Advanced" tab.
   c. Click the "Environment Variables" button.
   d. For "System Variables," select "New."
   e. Enter the following in the Variable Name and Variable Value fields:
      
      **Variable Name:** JAVA_HOME
      
      **Variable Value:** C:\Lotus\Domino\ibm-jre\jre
   8. Use a text editor to add "com.ibm.spi.IMCMSProvider" to the list of providers in the C:\Lotus\Domino\ibm-jre\jre\lib\security\java.security file. Follow the steps below:
a. Use a text editor to open the java.security file located in the directory path shown above on the Sametime server.

b. Type the following line into the list of security providers in the java.security file: security.provider.3=com.ibm.spi.IBMCMSProvider. The example below illustrates this line added to the java.security file.

```
# List of providers and their preference orders (see above)
#
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.spi.IBMCMSProvider
```

9. Delete the file "gskikm.jar" from the following location:
C:\Lotus\Domino\ibm-jre\jre\lib\ext\gskikm.jar.

### Installing IKeyMan on an AIX/Solaris Sametime server

To install IKeyMan on an AIX/Solaris Sametime server, follow the instructions below:

1. Insert the Sametime 7.0 server CD 2 into the Sametime server machine.
2. Open a command prompt on the Sametime server machine.
3. Login to the AIX/Solaris server as root.
4. From the command prompt, change to the GSKit directory on Sametime 7.0 server CD 2.

**On AIX**, use one of these procedures to perform the installation:

- Use the System Management Interface Tool (SMIT) utility to install the gskak.rte package. The package name is "6.0.7.4 AIX Certificate and SSL Base ACME Runtime Toolkit".
- Use the installp command. For example:
```
installp -acgqw /var/spool/pkg gskak.rte
```

**On Solaris**, uncompress and untar the gsk6bas.tar.Z file, and then use one of these procedures to perform the installation:

- Use the admintool application to install the package.
- Use the pkgadd command. For example:
```
pkgadd -d /var/spool/pkg gsk6bas
```

5. Use a text editor to open the java.security file.

**On AIX**:
- Open the java.security file located at
```
/opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre/lib/security/java.security
```

**On Solaris**:
- Open the java.security file located at
```
/opt/ibm/lotus/notes/latest/sunspa/ibm-jre/jre/lib/security/java.security
```

6. In the java.security file, type this line into the list of security providers:

```
security.provider.3=com.ibm.spi.IBMCMSProvider
```

The example below illustrates this line added to the java.security file:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.spi.IBMCMSProvider
security.provider.4=com.ibm.crypto.provider.IBMJCA
```

7. Delete the file "gskikm.jar" from the system.

**On AIX**:
- Delete gskikm.jar from this location:
```
/opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre/lib/ext
```
On Solaris:
- Delete gskikm.jar from this location:
  /opt/ibm/lotus/notes/latest/sunspa/ibm-jre/jre/lib/ext

8. Set the JAVA_HOME environment variable to the java VM installed under the sametime binaries directory:

On AIX:
JAVA_HOME=/opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre

On Solaris:
JAVA_HOME=/opt/ibm/lotus/notes/latest/sunspa/ibm-jre/jre export JAVA_HOME

Create a key database on the Sametime server named "key.kdb" and store this database in the root Sametime directory

Use the IKeyMan utility you have just installed to create an SSL key database named key.kdb on the Sametime server. When creating this database, store the database in the directory in which Sametime is installed.

Note: Sametime 7.0 installs on a Domino server in the same directory in which Domino is installed. The Domino server installs to the C:\Lotus\Domino directory by default. If the Domino server is installed in this default directory, the Sametime server also installs to the C:\Lotus\Domino directory.

To create the key.kdb database, follow the instructions below:

1. Start the IBM IKeyMan utility.
   On Windows:
   - Run the gsk6ikm.exe file located in the C:\Lotus\Domino\IBM\gsk6\bin directory on the Sametime server.
   On AIX:
   - Run the gsk6ikm file located in the /usr/opt/ibm/gskak/bin directory on the Sametime server.
   On Solaris:
   - Run the gsk6ikm file located in the /opt/ibm/gsk6/bin directory on the Sametime server.

2. From the IBM IKeyMan menu bar, select Key Database File-New.

3. In the New window, do the following:
   a. For Key database type, select "CMS key database file."
   b. For File Name, enter "key.kdb."
   c. For Location, enter the Sametime server Data directory. For example, on Windows enter C:\Lotus\Domino\Data.
   d. Click OK.

4. In the Password prompt window, do the following:
   a. Type a password and confirm the password used to access the key database. The password is at your discretion.
   b. Select the "Stash the password to a file?" Check box.
   c. Click OK.

   An information window appears indicating the password is encrypted and saved in the location C:\Lotus\Domino\Data\key.sth (or <Sametime install directory>\key.sth).
After creating the key.kdb database, ensure the key.kdb database contains the appropriate trusted root certificate.

**Ensuring the key.kdb database on the Sametime server contains the appropriate trusted root certificate**

If the LDAP server is set up to listen for SSL connections, the LDAP server will include an SSL key database that contains (at minimum) two certificates.

These certificates are:

- A trusted root (or "signer") certificate signed by a specific Certificate Authority (CA), such as VeriSign.
- A server certificate signed by the same CA as a trusted root certificate.

The LDAP server presents its SSL server certificate to the Sametime server during the SSL connection handshake. The key database on the Sametime server ("key.kdb" created above) must contain one of the following:

- A copy of the SSL server certificate used by the LDAP server. This certificate can be exported from the key database on the LDAP server and imported into the key.kdb database on the Sametime server as a signer certificate.
- A trusted root (or "signer") certificate that matches the trusted root certificate for the CA that signed the LDAP server certificate.

For example, if the key database on the LDAP server contains a "VeriSign Class 4 Public Primary Certification Authority" trusted root certificate and the LDAP SSL server certificate is signed by VeriSign, the key database on the Sametime server must also contain a "VeriSign Class 4 Public Primary Certification Authority" trusted root certificate.

When the key.kdb database is created, the database contains several trusted root (or "signer") certificates by default. If the appropriate trusted root certificate exists in the key.kdb database by default, no other procedures are required to ensure that the Sametime server trusts the LDAP server certificate. The procedure required to ensure the Sametime server trusts the SSL certificate of the LDAP server is complete.

**Ensuring that the Sametime server trusts the LDAP server certificate (i5/OS servers)**

This procedure is required when you use SSL to encrypt all data transmitted between the Sametime and LDAP server or use SSL to encrypt only user passwords that are transmitted between the Sametime and LDAP servers. For more information, see [Using SSL to encrypt all data transmitted between the Sametime and LDAP servers](#) or [Using SSL to encrypt only user passwords passing between the Sametime and LDAP servers](#).

This procedure enables a Sametime server that operates on the i5/OS platform to trust the SSL server certificate of the LDAP server. To ensure the Sametime for i5/OS server trusts the certificate of the LDAP server, the administrator must perform the following procedures:

- Install and setup the software required to use the integrated Digital Certificate Manager (DCM) on the i5/OS server where the Sametime server is located
- Ensure that the i5/OS LDAP client on the Sametime server system trusts the Certificate Authority (CA) that signed the SSL server certificate of the LDAP server.
• Ensure that Sametime has appropriate access to the system certificate store on the i5/OS server.

Install and setup required DCM software on i5/OS server
For i5/OS servers, certificates are managed using the integrated Digital Certificate Manger (DCM), rather than IKeyMan. You must install and setup the DCM software so that you can manage the SSL certificates required to encrypt connections between the Sametime server and LDAP server with SSL. All of the following software must be installed on the i5/OS server where your Sametime server is located:

• 5722-SS1 Option 34, Digital Certificate Manager
• 5722-DG1, IBM HTTP Server
• 5722-AC3, Crypto Access Provider 128-bit

If you need more detailed information about setting up and using DCM in order to complete the steps in this section, see the iSeries Information Center at http://www.ibm.com/as400/inforcenter. After selecting the i5/OS release and your preferred language, select the “Digital Certificate Manager” topic in the “Security” section.

If you do not already have a *SYSTEM certificate store, use DCM to create it.

Ensure that i5/OS LDAP client trusts the server certificate of the LDAP server
Sametime for i5/OS uses the LDAP client included with the IBM Directory Server which is installed as part of the i5/OS operating system.

In order for the Sametime server to communicate with the LDAP server using SSL, the IBM Directory Server LDAP client must trust the Certificate Authority (CA) that signed the LDAP directory server’s server certificate.

Note: As an alternative to the method described here, you may choose instead to ensure that the i5/OS LDAP client trusts the server certificate of the LDAP server. Only one of these methods is necessary. The LDAP client must trust the Certificate Authority (CA) that signed the LDAP directory server’s server certificate OR it must trust the server certificate of the LDAP server.

1. Use the Digital Certificate Manager (DCM) to ensure that the CA Certificate that signed the LDAP directory server’s server certificate has been imported to the DCM *SYSTEM certificate store on the i5/OS server where you are running Sametime.
   Well-known public Internet Certificate Authorities (CA) that most web browsers can recognize readily, such as VeriSign, are included in the DCM. If you are using a private certificate authority, you must import the CA’s certificate into the DCM *SYSTEM certificate store.

2. Import the LDAP directory server’s server certificate to the DCM *SYSTEM certificate store on the i5/OS server.

3. Then use DCM to add that CA Certificate to the trust list of the IBM Directory Server LDAP client application. The application id is QIBM_GLD_DIRSRV_CLIENT.

Ensure Sametime has access to the system certificate store
Sametime must be able to access certificates located in the DCM *SYSTEM certificate store when connecting to an LDAP server using SSL.
The DCM *SYSTEM certificate store is located in the /qibm/userdata/icss/cert/server directory on an i5/OS server. Run the following command from any i5/OS command line to view the contents of this directory:
WRKLNK '/QIBM/USERDATA/ICSS/CERT/Server/*'

By default, the certificate store is named default.kdb, but it may have another name.

QNOTES is an i5/OS user profile created by Domino and used by Sametime when it is running. By default, the QNOTES user profile does not have access to the DCM *SYSTEM certificate store or the /qibm/userdata/icss/cert/server directory. The higher level directories usually have *PUBLIC *RX authority which allows QNOTES to access those directories.

For example, run the following commands from any i5/OS command line to ensure QNOTES has the necessary authority to the DCM *SYSTEM certificate store and associated directory:
CHGAUT OBJ('/QIBM/USERDATA/ICSS/CERT/Server') USER(QNOTES) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.RDB') USER(QNOTES) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.KDB') USER(QNOTES) DTAAUT(*RX)

Adding a new administrator in the LDAP environment

When using LDAP, an administrator uses the Sametime Administration Tool for Sametime server administration. The administrator is authenticated against the Domino Directory on the Sametime server when accessing the Sametime Administration Tool.

One Sametime administrator is specified during the Sametime server installation procedure. To allow other administrators to access the Sametime Administration Tool, follow the instructions in [Adding a new Sametime administrator](#).

Note: In the LDAP environment, you can use the Sametime Administration Tool to perform LDAP configuration procedures. You cannot modify entries in the LDAP directory using the Sametime Administration Tool. Person and group entries in the LDAP directory must be modified using the software and procedures required by the LDAP server. See the documentation for your LDAP server for more information.

Access Control Lists and LDAP User Names

When using LDAP, authentication to individual databases on the Sametime server is controlled by database ACLs.

To access the database ACLs when Sametime is configured to operate as a client to an LDAP server:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.

Administrators should be aware of the following when entering names from an LDAP directory in the ACL of a database on the Sametime server:
When entering the names of users or groups registered in an LDAP directory to a database ACL, use the fully-qualified Distinguished Name (DN), but use forward slashes (/) as delimiters instead of commas (,). For example, if the DN for the user in the LDAP directory is:

```
uid = Joe Waters, ou=West, o=Acme
```

enter this name in the database ACL:

```
uid = Joe Waters/ou=West/o=Acme
```

You can also use an asterisk as a wildcard character when entering names from an LDAP directory in an ACL. For example, entering */ou=West/o=Acme is equivalent to entering all users in the ou=West, o=Acme branch of the directory to the ACL.

With the exceptions noted above, the ACL settings of Sametime databases should operate as they do when Sametime is configured to operate with a Domino Directory. For more information about working with database ACLs, see Using database ACLs for identification and authentication.

### Setting up an LDAP connection after selecting the Domino directory during the server installation

During the Sametime server installation, you must specify the directory type (either Domino or LDAP) used in your Sametime community. If you select the Domino directory during the installation, and later decide you want to configure Sametime to connect to an LDAP server, use the procedure below to set up the LDAP connection to the LDAP server.

**Note:** Using this procedure prevents you from having to reinstall the Sametime server and specify the LDAP directory type during the server installation to connect to the LDAP server.

There are six procedures associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation:

1. Shut down the Sametime services but keep the Domino services active.
2. Set up a Directory Assistance database on the Sametime server.
4. Create a Directory Assistance document in the Directory Assistance database that enables the Sametime server to access the LDAP server.
6. Copy and rename .DLL files, edit the Notes.ini file, or edit the Sametime.ini file.
7. Run the Lotus Sametime Name Conversion Utility.
8. Configure the LDAP Directory settings in the LDAP document (You can use either a Lotus Notes client or the Sametime Administration Tool to configure these settings.)
9. Restart the Sametime services on your Domino server.
Shut down the Sametime services but keep the Domino services active

This procedure is the first of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

In this procedure, you must shut down the Sametime services while you make configuration changes on the Sametime server. You must leave the Domino server running so you can access Domino databases on the server.

To shut down the Sametime services:
1. Open the Domino server console on the Sametime/Domino server.
2. In the Domino server console, type the following command:
   For Windows, AIX, and Solaris servers:
   Tell STADDIN Quit
   For IBM i5/OS servers:
   Tell STADDIN2 Quit

Next step
Set up a Directory Assistance database

Set up a Directory Assistance database

This procedure is the second of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

Because Sametime uses Directory Assistance to access an LDAP server, you must ensure that a Directory Assistance database exists on the Sametime server. Setting up Directory Assistance enables Web browser users to authenticate against entries in the LDAP directory when accessing databases on the Sametime server that require basic password authentication.

Note: The Sametime Connect client does not require Directory Assistance to authenticate against the LDAP directory or perform name and group lookups in the LDAP directory.

You can either create a new Directory Assistance database on the Sametime server or replicate an existing Directory Assistance database to the Sametime server.

Use the same process to set up Directory Assistance for a Sametime server as you would for a Domino server without Sametime. If you have already created a Directory Assistance database for the Domino environment in which Sametime is installed, you can replicate the existing Directory Assistance database to the Sametime server instead of creating a new Directory Assistance database.

Creating a new Directory Assistance database

To create a new Directory Assistance database:
1. Open a Lotus Notes client.
2. Choose File - Database - New.
3. Select the Sametime server (or select the Local server if you are running Sametime on a Windows server and you opened the Notes client on the server).
4. Create the Directory Assistance database on the server using the template DA50.NTF. Provide a database name and file name (for example, da.nsf) for the Directory Assistance database.

**Replicating an existing Directory Assistance database**

To replicate an existing Directory Assistance database, follow the normal Domino procedure for replicating a database. First create a new replica of the Directory Assistance database on the Sametime server, and then create a Connection document to schedule replication of the database. See your Domino server administration documentation for information on these procedures.

**Next step**

After you have ensured that a Directory Assistance database exists on the Sametime server, you must **identify the Directory Assistance database on the Sametime server**.

**Identify the Directory Assistance database on the Sametime server**

This procedure is the third of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

After you have ensured that a Directory Assistance database exists on the Sametime server, you must identify the Directory Assistance database on the Sametime server. Enter the database filename in the "Directory Assistance database name" field in the Basics section of the Sametime server Document.

1. From a Notes client, choose File - Database - Open.
2. Select the Sametime server (or select the Local server if you are running Sametime on a Windows server and you opened the Notes client on the server).
3. Select the Domino directory (names.nsf) and click Open.
4. Select Server - Servers to open the Servers view.
5. Double-click the name of the Sametime server to open the Server Document.
6. If necessary, select the Basics tab of the Server Document.
7. Click Edit Server.
8. In the "Directory Assistance database name" field, enter the filename (for example, da.nsf) of the Directory Assistance database.
9. Click Save and Close.

**Next step**

After you have identified the Directory Assistance database on the Sametime server, create a Directory Assistance document that enables the Sametime server to access the LDAP server.

**Create a Directory Assistance document that enables the Sametime server to access the LDAP server**

This procedure is the fourth of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

The Directory Assistance database on the Sametime server must contain a Directory Assistance document that enables the Sametime server to access the
LDAP server. The procedure below explains how to create the Directory Assistance document for the LDAP server and provides suggested values for the fields in the Directory Assistance document. You can change the suggested values as required by your environment.

To create the Directory Assistance document:
1. From the Notes client open the Directory Assistance database (usually named da.nsf) on the Sametime server.
2. Click "Add Directory Assistance".
3. In the Basics tab, make these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type</td>
<td>Select LDAP.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Enter any descriptive name; the name must be different from any other in Directory Assistance. Do not use the Domino domain name.</td>
</tr>
<tr>
<td>Company name</td>
<td>Enter the name of your company.</td>
</tr>
<tr>
<td>Search order</td>
<td>The suggested value is 1. The search order specifies the order this directory is searched relative to other directories in Directory Assistance.</td>
</tr>
<tr>
<td>Group expansion</td>
<td>The suggested setting is Yes. This setting enables Directory Assistance to examine the contents of groups in the LDAP directory. This capability is necessary if you enter the name of a group defined in the LDAP directory in the ACL of a database on the Sametime server.</td>
</tr>
<tr>
<td>Nested group expansion</td>
<td>The suggested setting is Yes. This setting enables Directory Assistance to examine the content of an LDAP directory group that is a member of another LDAP directory group. This capability is also used when an LDAP directory group name is entered in the ACL of a database on the Sametime server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Set to Yes to enable Directory Assistance for the LDAP Directory.</td>
</tr>
</tbody>
</table>

4. Select the Rules tab. Configure Rule 1 as needed for your Domino environment. The suggested values for Rule 1 are as follows:
   - The OrgUnit1, OrgUnit2, OrgUnit3, OrgUnit4, Organization, and Country fields should all contain an asterisk. Using all asterisks in this setting ensures that all entries in the LDAP directory can be searched and authenticated.
   - Note The Rules setting indicates the names in the directory that can be authenticated. You can modify the Rules setting as needed according to the structure of the LDAP Directory the Sametime server is accessing. For more information on using naming rules in Directory Assistance, see the Domino server administration documentation. (Domino documentation is available from www.lotus.com/ldd/doc and also provided with the Domino server.)
   - The "Enabled” and "Trusted for Credentials” fields should both be set to "Yes.”

5. Select the LDAP tab. The LDAP tab contains the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The host name for the LDAP server (for example, ldap.acme.com).</td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Optional Authentication</td>
<td>Binding parameters to the LDAP server. For more information, see [Administrator distinguished name and password for authenticated binding][1]. If entries exist in the &quot;Administrator distinguished name&quot; and &quot;Administrator password&quot; fields in the LDAP Directory-Connectivity settings of the Sametime Administration Tool, the Sametime server binds to the LDAP server as an authenticated user. If there are no entries in the &quot;Administrator distinguished name&quot; or &quot;Administrator password&quot; fields, the Sametime server binds to the LDAP server as an anonymous user.</td>
</tr>
<tr>
<td>Username</td>
<td>Complete this field if you want your Sametime server to bind to the LDAP server as an authenticated user. Otherwise, leave this field empty. Suggested values for Microsoft Active Directory server are: cn=qadmin, cn=users, dc=ubq-qa, dc=com.</td>
</tr>
<tr>
<td>Password</td>
<td>Complete this field if you want your Sametime server to bind to the LDAP server as an authenticated user. Otherwise, leave this field empty. Enter the password for the Username specified above.</td>
</tr>
</tbody>
</table>
| Base DN for search            | Specify a search base. A search base defines where in the directory tree a search should start. Suggestions for this setting are:  
   **Domino directory** - An example value is "O=DomainName," where "DomainName" is the Lotus Notes domain (for example O=Acme).  
   **Microsoft Exchange 5.5 directory** - An example value is "CN=recipients, OU=ServerName, O=NTDomainName," where ServerName is the Windows server name and NTDomainName is the Windows NT Domain (for example, CN=recipients,OU=Acmeserver1,O=NTAcmedomain).  
   The Microsoft Exchange 5.5 example above assumes that the directory is using the default directory schema. If you have changed the schema of the Microsoft Exchange 5.5 directory, the entry in the Base DN for search field must reflect the new schema.  
   **Microsoft Active Directory** - An example value is "CN=users, DC=DomainName, DC=com."  
   **Netscape LDAP directory** - Use the format O= followed by the organizational unit that was specified during the Netscape server setup. If you are uncertain about this entry, use the administrative features of the Netscape server to determine the appropriate entry. |
| Perform LDAP search for       | Select Notes clients/Web Authentication. |
| Channel encryption            | Select None. For information on using Secure Sockets Layer (SSL) to encrypt the connection between the Sametime server and the LDAP server, see [Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server][1]. |
| Port                          | Enter the port number used to connect to the LDAP server. The default setting is port 389. |

[1]: #108 Sametime Administrator’s Guide
### Table

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>The suggested setting is 60 seconds. This setting specifies the maximum number of seconds allowed for a search of the LDAP directory.</td>
</tr>
<tr>
<td>Maximum number of entries returned</td>
<td>The suggested setting is 100. This setting specifies the maximum number of names the LDAP server will return for the name searched. If the LDAP server also has a maximum setting, the lower setting takes precedence.</td>
</tr>
</tbody>
</table>

6. Click "Save and Close." The warning message notifies you that your connection does not include SSL settings; you can ignore the warning and continue with the procedure. For more information on the SSL configuration, see [Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server](#).

**Next step**

After you create the Directory Assistance document that enables the Sametime server to access the LDAP server, you must [create an LDAP document in the Configuration database on the Sametime server](#).

### Create an LDAP document in the Configuration database

This procedure is the fifth of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

The Configuration database (stconfig.nsf) stores administration settings made from the Sametime Administration Tool. These administration settings are stored on individual documents within the Configuration database. You must use a Lotus Notes client to create an LDAP document in the Configuration database on the Sametime server. The LDAP document you create will hold the LDAP Directory settings that enable Sametime to search and authenticate against entries in the LDAP directory.

To create an LDAP document in the Configuration database:

1. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
2. Select Create - LDAPServer.
   
   A document opens that contains the LDAP administration settings. You can configure these settings using either the Sametime Administration Tool or a Lotus Notes client. If you want to use the Lotus Notes client, leave the document open and continue to the next procedure (see "Next step" below).

   If you want to use the Sametime Administration Tool to configure the LDAP settings, choose File - Save to save the LDAP document. Close the LDAP document and close the Lotus Notes client.

**Next step**

After you have created an LDAP document in the Configuration database, you must [copy and rename the .DLL files or edit the Notes.ini file](#).
Copy and rename the .DLL files, edit the Notes.ini file, or edit the Sametime.ini file

This procedure is the sixth of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

The procedure you perform at this point depends on whether your Sametime server runs on the Windows, AIX/Solaris, or IBM i5/OS operating system.

- If your Sametime server runs on the Windows operating system, you must copy and rename some .DLL files from the C:\Sametime\DirectoryBB\Ldap directory to the C:\Sametime directory.
- If your Sametime server runs on the AIX/Solaris operating system, you must edit the Sametime.ini file.
- If your Sametime server runs on the IBM i5/OS operating system, you must edit the Notes.ini file.

Follow the procedure below that is appropriate for your environment.

Copying and renaming the DLL files (Windows only)

If your Sametime server runs on the Windows operating system, perform this procedure:

1. On the Sametime server, create a working directory to copy files to so that you can rename them.
2. Copy the "STAuthenticationLdap.dll" from the directory C:\Sametime\DirectoryBB\Ldap to the working directory.
3. In the working directory, rename the "STAuthenticationLdap.dll" file to "STAuthentication.dll."
4. Copy the renamed "STAuthentication.dll" file to the C:\Sametime directory.
   **Note** Copying the "STAuthentication.dll" file to the C:\Sametime directory will overwrite an existing file of the same name.
5. Copy the file "STGroupsLdap.dll" from the directory C:\Sametime\DirectoryBB\Ldap to the working directory.
6. Rename the "STGroupsLdap.dll" file to "STGroups.dll."
7. Copy the renamed STGroups.dll file to the C:\Sametime directory.
   **Note** Copying the "STGroups.dll" file to the C:\Sametime directory will overwrite an existing file of the same name.
8. Copy the file "STResolveLdap.dll" from the directory C:\Sametime\DirectoryBB\Ldap to the working directory.
9. Rename the "STResolveLdap.dll" file to "STResolve.dll."
10. Copy the renamed "STResolve.dll" file to the C:\Sametime directory.
    **Note** Copying the "STResolve.dll" file to the C:\Sametime directory will overwrite an existing file of the same name.
11. Copy the "StBrowseLdap.dll" from the directory C:\Sametime\DirectoryBB\Ldap to the working directory.
12. Rename the "StBrowseLdap.dll" file to "StBrowse.dll."
13. Copy the renamed STBrowse.dll file to the C:\Sametime directory.
Editing the Sametime.ini file (AIX/Solaris only)

If your Sametime server runs on the AIX/Solaris operating system, perform this procedure to edit the Sametime.ini file in the Sametime server installation directory. You must change the DirectoryType parameter from "Domino" to "LDAP" in the Sametime.ini file.

1. Use a text editor to open the Sametime.ini file located in the Sametime server installation directory (for example, <root>/lotus/domino).
2. In the [CONFIG] section of the Sametime.ini file edit the DirectoryType= parameter so that it specifies LDAP as shown below:
   
   
   DirectoryType=LDAP
3. Save and close the Sametime.ini file.

Editing the Notes.ini file (IBM i5/OS only)

If your Sametime server runs on the IBM i5/OS operating system, perform this procedure to edit the Notes.ini file. You must change the SametimeDirectoryType parameter from "Domino" to "LDAP" in the Notes.ini file:

1. To edit the notes.ini file, run the WRKDOMSVR command and then enter option 13 next to your Sametime server.
2. Change the line that reads "SametimeDirectoryType=DOMINO" to "SametimeDirectoryType=LDAP".
3. Press F3 twice to close the file and save the changes.

Next step

After you have copied and renamed the .DLL files, you must run the Lotus Sametime Name Conversion Utility.

Run the Lotus Sametime Name Conversion Utility

This procedure is the seventh of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

You must run the Lotus Sametime Name Conversion Utility to ensure that the user and group names that are stored in the vpuserinfo.nsf database on the Sametime server are converted from the native Domino directory name format to the LDAP directory format.

Users create buddy lists and privacy lists from the Sametime Connect client by selecting user names and group names from the directory accessed by the Sametime server.

If the Sametime Connect client users in your environment have created buddy lists and privacy lists by selecting names from the Domino directory, the user and group names in these lists are stored in the vpuserinfo.nsf database on the Sametime server in the native Domino directory format. You must run the Sametime Name Conversion Utility to convert the names in the vpuserinfo.nsf database to the LDAP directory format.

The Name Conversion Utility is provided with the Sametime 7.0 server. For more information, see the appendix on using the Name Conversion Utility later in this documentation.

Next step

After you have run the Sametime Name Conversion Utility, you must configure the LDAP directory settings.
Configuring the LDAP directory settings

This procedure is the eighth of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

This procedure is described in Configure the LDAP Directory settings earlier in this chapter.

Next step

After you have run the Sametime Name Conversion Utility, you must restart the Sametime services on your Domino server.

Restart the Sametime services on your Domino server

This procedure is the last of nine associated with enabling Sametime to connect to an LDAP server if you have selected the Domino directory during the server installation.

In this procedure, you restart the Sametime services on the Domino server. You can either stop the server and restart it, or just restart the Sametime services by following these steps:

1. Open the Domino server console on the Sametime/Domino server.
2. In the Domino server console, type the following command:
   For Windows, AIX, and Solaris servers:
   Load STADD1N
   For IBM i5/OS servers:
   Load STADD1N2

Using Java classes to customizing LDAP directory searches

This section explains how you can write Java classes that provide greater control over how the Sametime server conducts user name and group name searches of an LDAP directory. You can also write a Java class that controls how user names returned from LDAP directory searches are formatted. This section includes these topics:

- Using a Java class to control directory searches for people and groups
- Using a Java class to control the format of user names returned by directory searches

Using a Java class to control directory searches for people and groups

The "Search filter for resolving person names" and the "Search filter for resolving group names" settings in the LDAP directory settings of the Sametime Administration Tool define the LDAP directory search filters responsible for selecting user and group names from the LDAP directory.

In some LDAP directory environments, the LDAP directory schema may be too complex to use a single search filter to select user names (or group names) from the LDAP directory.

If a single search filter is not adequate to resolve user name (or group name) searches, you can write a Java class containing a method that specifies exactly how directory searches are conducted. This Java class can invoke different LDAP seach
filters depending on the search criteria entered by the end user. Writing a Java class can ensure that the search capability functions exactly as needed for a particular directory schema.

The following example illustrates the extent to which you can control searching behavior when you use a Java class for this purpose. This example assumes that three different users want to add the user Victor Lazlow to their Sametime Connect buddy lists. Each of the three users searches for Victor Lazlow in a different way. The logic of the Java class dictates the results of these three user searches.

- User 1 enters "Victor L*" into the Sametime client user interface to add Victor Lazlow to the buddy list. This search attempt returns an error because the Java class is programmed to return an error when the user enters a text string that includes an asterisk.
- User 2 enters "Victor_Lazlow@acme.com" into the Sametime client interface. This search attempt succeeds and returns the value "Victor_Lazlow@acme.com" (Victor Lazlow’s e-mail address) from the LDAP directory. The search attempt succeeds in this way because the Java class is programmed to return an LDAP search filter that can resolve an LDAP directory search to a user’s e-mail address. The Java class returns this e-mail address search filter if the search text string entered by the end user includes the "at" character (@).
- User 3 enters "Victor L" into the Sametime client interface. This search attempt succeeds and returns the common name (cn) directory attribute of "Victor Lazlow." The search attempt succeeds in this way because the Java class is programmed to return an LDAP search filter that can resolve an LDAP directory search to a user’s common name (cn). The Java class returns this common name search filter if the search text string entered by the end user does not include either an asterisk or "at" (@) character.

When using a Java class to control the directory searching behavior, you write the Java class so that it provides the searching behavior desired for your particular LDAP directory schema. The search behavior is not limited to the behavior described in the example above; the behavior is controlled by the code you write.

To use a custom Java class to control the LDAP directory searching behavior, you must perform the following procedures:

1. Write a Java source code file containing the Java class and method that defines the searching behavior.
2. Compile the source code file and copy the resulting Java class file to the Sametime server computer.
3. Update the Sametime.ini file parameters.
4. Enter the Java class and method name in the Sametime Administration Tool.

Each of these procedures is described below.

**Writing a Java source code file containing the Java class and method that defines the searching behavior**

Writing a Java source code file containing the Java class and method that defines the searching behavior is the first of four steps required to use a Java class to control LDAP directory searches for people and groups.

The specific source code that you write to support customized LDAP searches is entirely dependent on your environment. This section provides a code sample to help you understand how to write the Java class appropriate for your environment.
Note: The Java code that you write must be compatible with the Java Run-Time Environment (JRE 1.4.2).

In this example, you write a Java class consisting of a Java method that invokes different LDAP directory search filters based on the text string that is entered into the Sametime user interface by an end user. The search filters invoked by the method are dependent on the directory schema and the search behavior needed for the environment.

The code sample below shows the Java source code that produces the search behavior described in the example of the three different user searches discussed earlier in this section. This code creates a Java class named "StLdapCustomized" that includes the "peopleResolveFilter" method. The if statements in the peopleResolveFilter method examine the text string entered by the user in the Sametime client user interface and return the appropriate LDAP search filter based on this text string. The comments in the source code explain the purpose of each if statement.

```java
public class StLdapCustomized {

    /*
     * Generates a search filter for finding a user, given the user's * name. *
     * The user's name as provided by the Sametime client.
     */

    @param String peopleResolveFilter (String name) {
        // prevent users from adding their own wildcards
        if (name.indexOf("*") != -1) return null;

        // if name looks like e-mail, do not search with wildcards
        if (name.indexOf('@') != -1)
            return "(&(objectclass=person)(mail=\"+ name + ")") ";

        // otherwise, search as CN with wildcard
        return "(&(objectclass=person) (cn=\"+ name + ")")";
    }
}
```

If you also want to customize searches for groups, you must write a similar java source code file that contains the logic you want to employ for group searches.

Note: You do not have to write Java classes to control the search behavior for both users and groups. You can use a Java class to control the search behavior for users while using a single LDAP search filter to control the search behavior for groups, or vice versa.
Compiling the source file and copying the Java class file to the Sametime server computer

Compiling the source file and copying the Java class file to the Sametime server computer is the second of four steps required to use a custom Java class to control LDAP directory searches for people and groups.

To complete this step, perform these procedures:
1. Compile the Java source code file to produce the Java class file.
   This example assumes that you compile the sample source code from the previous step to produce a Java class file named "StLdapCustomized.class."
2. Copy the compiled class file (StLdapCustomized.class) to the "java" subdirectory of the Sametime server installation directory. In a default Sametime server installation, the correct directory path for the class file is:
   c:\Lotus\Domino\java.

   **Note:** You should copy the Java class file to the C:\Lotus\Domino\java location because this is the default class path specified for the Meeting Services in the Windows registry settings. Copying the class file to this location ensures that LDAP directory searches conducted from both Meeting Services clients and Community Services clients will return user names in the programmed format.

Update the Sametime.ini file parameters

Updating the Sametime.ini file Java parameters is the third of four steps required to use a custom Java class to control LDAP directory searches for people and groups.

In this procedure, you update the ST_JAVA_CLASS_PATH parameter and the ST_JAVA_JVM_PATH parameters in the Sametime.ini file on the Sametime server. This step ensures that the Sametime Community Services class path and JVM location settings are configured appropriately for the environment.

The ST_JAVA_CLASS_PATH parameter must specify the location of the Java class file copied in the previous step (c:\Lotus\Domino\java\StLdapCustomized.class in this example).

The ST_JAVA_JVM_PATH parameter should specify the location of the jvm.dll file used by the Sametime Meeting Services. By default, the Meeting Services use the jvm.dll file located at c:\Lotus\Domino\wsc-jre\jre\bin\classic\jvm.dll.

To update the Sametime.ini file:
1. Use a text editor to open the Sametime.ini file located in the C:\Lotus\Domino directory.
2. In the [Config] section of the Sametime.ini file, ensure that the ST_JAVA_CLASS_PATH parameter specifies the "java" subdirectory of the Sametime server installation directory (default C:\Lotus\Domino\java), as shown in the example below.
   
   ```
   ST_JAVA_CLASS_PATH=C:\Lotus\Domino\StConfig.jar;C:\Lotus\Domino\StConfigXml.jar;C:\Lotus\Domino\java
   ```

3. In the [Config] section of the Sametime.ini file, ensure that the ST_JAVA_JVM_PATH parameter specifies the directory path to the jvm.dll file on the Sametime server that is used by the Meeting Services. The recommended setting for the ST_JAVA_JVM_PATH parameter is:
   
   ```
   ST_JAVA_JVM_PATH=C:\Lotus\Domino\wsc-jre\jre\bin\classic\jvm.dll
   ```
Note The Community Services loads the JVM specified by the ST_JAVA_JVM_PATH parameter in the Sametime.ini file. In some circumstances, the Meeting Services may load the JVM before the Community Services does. Specifying the same JVM for both of these services ensures consistent searching behavior for both Community Services and Meeting Services clients, regardless of which service loads the JVM.

4. Save and close the Sametime.ini file.

Enter the Java class and method name in the Sametime Administration Tool

Entering the Java class and method name in the Sametime Administration Tool is the last of four steps required to use a custom Java class to control LDAP directory searches for people and groups.

In this procedure, you enter the Java class name and method name into the "Search filter for resolving person names" setting in the LDAP directory settings of the Sametime Administration Tool.

Use the format "Classname.methodname()" when entering the java class name and method name into the "Search filter for resolving person names" setting. Following our earlier example, you would enter "StLdapCustomized.peopleResolveFilter()" in the "Search filter for resolving person names" setting.

Follow the instructions below:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
3. In the "Search settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "Search filter for resolving person names" setting.
4. In the "Search filter for resolving person names" setting, enter the class name and method name in the format "Classname.methodname()."

Following our earlier example, you would enter StLdapCustomized.peopleResolveFilter() in the "Search filter for resolving person names" setting.
5. If you have also created a Java class to define the group search behavior, enter the "Classname.methodname()" for group searches in the "Search filter for resolving group names" setting.
6. Click Update and restart the server for the changes to take effect.

Using a Java class to control the format of user names returned in LDAP directory searches

You can write a Java class to control the format of user names returned in LDAP directory searches. In a typical Sametime deployment, the "The attribute of the person entry that defines the user’s name" setting in the LDAP Directory settings of the Sametime Administration Tool controls the format of the user name that is returned by an LDAP directory search.

In most environments, the value of the "The attribute of the person entry that defines the user’s name" setting can specify a common LDAP directory attribute, such as cn (common name) or mail (e-mail address). When configured in this way, the search returns the value assigned to a user’s cn or mail directory attribute and displays this value in the Sametime client user interface.
Some environments may require LDAP directory searches to return a user name in a format that is not available in an LDAP directory entry attribute. In this case, you can write a Java class that manipulates existing information in the LDAP directory to produce the user name in the desired format. For example, you might write a Java class that combines the values of two LDAP directory attributes to produce the user name in a desired format. Or, you can write a Java class that edits the information in a single LDAP directory attribute to produce the user name in a format that is different than the value specified by the attribute.

To illustrate this feature, consider an example environment in which all of the following are true:

- LDAP searches must return a user name in the format LastName, FirstName (for example: Smith, John)
- None of the LDAP directory attributes specify the user name in the LastName, FirstName format.
- The LDAP directory attribute sn specifies each user’s last name.
- The LDAP directory attribute givenName specifies each user’s first name.

In this example, you can write a Java class that takes values from the sn and givenName directory attributes and combines these values into a single display name in the format of LastName, FirstName.

You can then configure the Sametime server to use this Java class to return the names in that format when the LDAP directory is searched.

To use a custom Java class to control the LDAP directory searching behavior, you must perform the following procedures.

**Note:** These procedures are very similar to the procedures discussed in the Using a custom Java class to control LDAP directory searches for people and groups topic earlier in this chapter.

1. **Write the Java source code file that returns the user name**
2. **Compile the source code file and copy the resulting Java class file to the Sametime server**
3. **Update the Sametime.ini file**
4. **Enter the Java class and method name in the Sametime Administration Tool LDAP directory settings**

Each of these procedures is described below.

**Writing the Java source code file that returns the user name**

Writing the Java source code file that returns the user name is the first of four steps required to use a custom Java class to control the format of user names returned in LDAP directory searches.

The specific source code that you write to support customized LDAP searches is entirely dependent on the user name requirements of your environment. This section provides a code sample to help you understand how to write the Java class appropriate for your environment.

**Note:** The Java code that you write must be compatible with the Java Run-Time Environment (JRE 1.4.2).
This code sample below shows the code you might use to combine values stored in the sn and givenName LDAP directory entry attributes into a single display name in the format of LastName, FirstName.

```java
public class StLdapCustomizedAttributes {
    public static String displayName (String givenName, String sn) {
        String result = sn + ", " + givenName;
        return result;
    }
}
```

Compiling the source file and copying the Java class file to the Sametime server

Compiling the source file and copying the Java class file to the Sametime server is the second of four steps required to use a Java class to control the format of user names returned in LDAP directory searches.

To complete this step, perform these procedures:
1. Compile the Java source code file to produce the Java class file.
   This example assumes you compile the source code file example from the previous procedure to produce a Java class file named "StLdapCustomizedAttributes.class."
2. Copy the compiled class file (StLdapCustomizedAttributes.class) to the "java" subdirectory of the Sametime server installation directory. In a default Sametime server installation, the correct directory path for the class file is: c:\Lotus\Domino\java.

Note: You should copy the Java class file to the C:\Lotus\Domino\java location because this is the default class path specified for the Meeting Services in the Windows registry settings. Copying the class file to this location ensures that LDAP directory searches conducted from both Meeting Services clients and Community Services clients will return user names in the programmed format.

Update the Sametime.ini file

Updating the Sametime.ini file is the third of four steps required to use a custom Java class to control the format of user names returned in LDAP directory searches.

In this procedure, you update the ST_JAVA_CLASS_PATH and the ST_JAVA_JVM_PATH parameters in the Sametime.ini file on the Sametime server. This step ensures that the Sametime Community Services class path and JVM location settings are configured appropriately for the environment.

The ST_JAVA_CLASS_PATH parameter must specify the location of the Java class file copied in the previous step (c:\Lotus\Domino\java\StLdapCustomizedAttributes.class in this example).
The ST_JAVA_JVM_PATH parameter should specify the location of the jvm.dll file used by the Sametime Meeting Services. By default, the Meeting Services use the jvm.dll file located at C:\Lotus\Domino\wsc-jre\jre\bin\classic\jvm.dll.

To update the Sametime.ini file:

1. Use a text editor to open the Sametime.ini file located in the C:\Lotus\Domino directory.

2. In the [Config] section of the Sametime.ini file, ensure that the ST_JAVA_CLASS_PATH parameter specifies the subdirectory of the Sametime server installation directory (default C:\Lotus\Domino\java), as shown in the example below:

   ST_JAVA_CLASS_PATH=C:\Lotus\Domino\StConfig.jar;C:\Lotus\Domino\StConfigXml.jar;C:\Lotus\Domino

3. In the [Config] section of the Sametime.ini file, ensure that the ST_JAVA_JVM_PATH parameter specifies the directory path to the jvm.dll file on the Sametime server that is used by the Meeting Services. The recommended setting for the ST_JAVA_JVM_PATH parameter is:

   ST_JAVA_JVM_PATH=C:\Lotus\Domino\wsc-jre\jre\bin\classic\jvm.dll

   Note: The ST_JAVA_JVM_PATH parameter specifies the JVM loaded by the Community Services. Either the Community Services or the Meeting Services can load the JVM. Specifying the same JVM for both of these services ensures consistent searching behavior for both Community Services and Meeting Services clients, regardless of which of these services loads the JVM.

4. Save and close the Sametime.ini file.

**Enter the Java class and method name in the Sametime Administration Tool LDAP Directory settings**

Entering the Java class and method name in the Sametime Administration Tool LDAP Directory settings is the last of four steps required to use a Java class to control the format of user names returned in LDAP directory searches.

In this procedure, you enter the Java class and method name into "The attribute of the person entry that defines the user’s name" setting in the LDAP Directory settings of the Sametime Administration Tool.

Use the format "Classname.methodname()" when entering the Java class name and method name in the Sametime Administration Tool setting. Following our earlier example, you would enter the class name and method name as "StLdapCustomizedAttributes.displayName(givenName, sn)."

Follow the instructions below:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.


3. In the "Search settings for server" drop-down list, select the LDAP server that contains the LDAP directory for which you want to modify the "The attribute of the person entry that defines the user’s name" setting.

4. In the "The attribute of the person entry that defines the user’s name" setting, type the class name and method name in the format classname.methodname(). For example:

   StLdapCustomizedAttributes.displayName(givenName, sn)

5. Click Update and restart the server for the change to take effect.
Solving token authentication problems in mixed server and multiple LDAP directory environments

A token authentication problem may occur when a Sametime server is deployed in the same environment as a portal server (or any other application server that issues authentication tokens). This problem occurs when the Sametime server and the portal server access different LDAP directories to authenticate users.

Several Sametime Java applet clients present an authentication token to the Sametime server when connecting to the server. These clients include the Sametime Connect for browsers client, the Sametime Meeting Room client, and Sametime Links clients.

If a Web browser user first authenticates to a portal server, and then later attempts to connect to the Sametime server using one of the Sametime Java applet clients, the Sametime client connection may fail.

This problem occurs because the Sametime client sends the authentication token it received from the portal server to authenticate the connection to the Sametime server. The portal server creates this authentication token by gathering user credentials from the LDAP directory that it accesses. When the Sametime server receives this token, it extracts these user credentials and compares them to user credentials in the different LDAP directory that it accesses. The authentication fails because the user credentials do not match.

To further illustrate this token authentication problem, consider an example environment in which all of the following are true:

- A portal server is deployed and connected to a Netscape LDAP directory. In the Netscape LDAP directory, the user Victor Lazlow has a distinguished name entry of cn=Victor Lazlow,ou=People,dc=Acme,dc=com.
- A Sametime server is deployed and connected to a Domino LDAP directory. In the Domino LDAP directory, the user Victor Lazlow has a distinguished name entry of cn=Victor Lazlow,ou=Acme.
- An application using Sametime Links is deployed on the portal server.

The sequence of events below illustrates the token authentication problem.

1. Victor Lazlow accesses the portal server with a Web browser and enters his user name and password. The portal server authenticates this user name and password against Victor’s person entry in the Netscape LDAP directory.
2. The portal server sends a Lightweight Third Party Access (LTPA) token to Victor’s Web browser. This LTPA token contains Victor’s user name as specified in the Netscape LDAP directory (cn=Victor Lazlow,ou=People,dc=Acme,dc=com).
3. Victor Lazlow accesses the Sametime Links application on the portal server.
4. The Sametime Links client applet loads to Victor’s Web browser and connects to the Sametime server. To authenticate this connection, the client transmits the LTPA token obtained from the portal server to the Sametime server.
5. The Sametime server extracts the user name from the LTPA token (cn=Victor Lazlow,ou=People,dc=Acme,dc=com) and compares the user name to Victor’s person entry in the Domino LDAP directory (cn=Victor Lazlow,ou=Acme).
6. Since the name extracted from the token is not an identical match with the name obtained from the LDAP directory, the authentication fails and Victor cannot use the Sametime Links application.
Solving the token authentication problem

Sametime 7.0 contains logic designed to solve the token authentication problem. This solution, and its configuration, is discussed below.

When the user accesses Sametime Links on the portal server, the Sametime client sends an authentication by token request to the Sametime server. This authentication by token request contains two parameters:

- The Sametime user name (cn=Victor Lazlow, o=acme in this example). This name is known by the portal server and passed to the client from the portal server.
- The LTPA token containing the user name from the directory accessed by the portal server (cn=Victor Lazlow, ou=People, dc=Acme, dc=com in this example).

Upon receiving the authentication by token request, the Sametime 7.0 server can do the following:

1. Extract the text string "Victor Lazlow" from the cn=Victor Lazlow, ou=People, dc=Acme, dc=com user name provided in the LTPA token.
2. Search the Domino directory accessed by the Sametime server to locate a directory entry containing the same user name text string (Victor Lazlow).
3. Sametime then takes the Domino user ID from the Domino directory entry it locates (cn=Victor Lazlow, o=acme in this example) and compares this user ID with the Sametime user name that was received as a parameter in the authentication by token request from the client. If this comparison produces a match, the authentication by token is successful.

To configure this logic, the administrator must add two parameters to the Notes.ini file on the Sametime/Domino server. These two parameters are used by the Sametime logic to extract the user name text string ("Victor Lazlow" in this example) from the full canonical user name provided in the LTPA token.

The two Notes.ini parameters are:

- ST_UID_PREFIX=
- ST_UID_POSTFIX=

Sametime uses the value of the ST_UID_PREFIX= parameter to strip out the characters that precede the user name text string that you want to extract. In this example, those characters are "cn=".

Sametime uses the value of the ST_UID_POSTFIX= parameter to identify the first character that follows the user name text string that you want to extract. In this example, that character is a comma (,).

The correct configuration for the Notes.ini parameters in the example scenario described earlier is shown below:

- ST_UID_PREFIX=cn=
- ST_UID_POSTFIX=,

When configured in this way, Sametime extracts the user name by first stripping the prefix of cn= from the cn=Victor Lazlow, ou=People, dc=Acme, dc=com user name to produce the text string Victor Lazlow, ou=People, dc=Acme, dc=com.

Sametime then locates the postfix character (,) and strips that character and all characters that follow it from the user name string. In this example, Sametime
would strip the text string `ou=People, dc=Acme, dc=com` from the user name to produce the text string of "Victor Lazlow."

Sametime then searches the directory it accesses and performs the authentication by token as discussed earlier.

**Notes**

- If the ST_UID_PREFIX= and ST_UID_POSTFIX= parameters do not exist in the Notes.ini file, Sametime compares the user name taken from the LTPA token (cn=Victor Lazlow, ou=People, dc=Acme, dc=com in this example) to the user name it receives as a parameter in the authentication by token request (cn=Victor Lazlow, o=Acme in this example).
- In some complex directory environments, or in environments in which the token authentication logic is customized, the out-of-the-box solution provided with Sametime 7.0 may not be adequate for the authentication to succeed as discussed above. In these environments, it is possible to create a custom DLL to compare the name received in an LTPA authentication token to the name received as a parameter in the authentication by token request.

**Managing users in buddy lists and privacy lists in an LDAP environment**

If you make changes to user names or group names in the LDAP directory, you must run the Name Conversion Utility to ensure these same name changes are made in the buddy lists and privacy lists that display in the Sametime Connect client. The buddy list and privacy list names are stored in a Domino database (vpuserinfo.nsf) and must be managed separately from the names in the LDAP directory. For more information, see the appendix Using the Name Conversion Utility later in this documentation.
Chapter 5. Configuring Ports and Network Connectivity

This chapter discusses the connectivity settings available from the administration tool and the connection processes of IBM Lotus Sametime server clients.

This chapter discusses:
- Ports used by the Sametime server
- Forward proxy support for Sametime clients
- Configuring Sametime Networks and Ports administration settings
- Sametime client connection processes
- Changing the default connectivity settings of the Sametime Connect for browsers client
- HTTP tunneling
- TCP tunneling of audio/video streams
- Reverse proxy support for the Sametime server

## Ports used by the Sametime server

The tables below list the default ports used by all Sametime services, including:

- **HTTP Services, Domino Services, LDAP Services, and Sametime intraserver ports**
- **Community Services ports**
- **Meeting Services ports**
- **Broadcast Services ports**
- **Audio/Video Services ports**

You can use the Sametime Administration Tool to configure the ports on which the Sametime services listen for connections from clients.

The port settings for all services can be accessed from the Configuration-Connectivity—“Networks and Ports” options of the Sametime Administration Tool.

### HTTP Services, Domino Services, LDAP Services, and Sametime intraserver ports

The following ports are used by the Sametime HTTP Services, Domino Application Services, and LDAP Services.

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 80</td>
<td>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Community Services multiplexer on the Sametime server listens for HTTP connections from Web browsers, Sametime Connect clients, Sametime Meeting Room clients, and Sametime Broadcast clients on port 80. If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server listens for HTTP connections on this port.</td>
</tr>
</tbody>
</table>
### Community Services ports

The following ports are used by the Sametime Community Services. Most of these ports are configurable.

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 1516</td>
<td>The Community Services listen for direct TCP/IP connections from the Community Services of other Sametime servers on this port. If you have installed multiple Sametime servers, this port must be open for presence, chat, and other Community Services data to pass between the servers. The communications that occur on port 1516 also enable one Sametime server to start a meeting on another server (or “invite” the other server to the meeting).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Alternate HTTP port (8088) | If the administrator allows HTTP tunneling on port 80 during the Sametime installation (or afterward), the Domino HTTP server on which Sametime is installed must listen for HTTP connections on a port other than port 80. The Sametime installation changes the Domino HTTP port from port 80 to port 8088 if the administrator allows HTTP tunneling on port 80 during a Sametime server installation.

**Note:** If the administrator allows HTTP tunneling on port 80 during the Sametime installation, Web browsers make HTTP connections to the Community Services multiplexer on port 80, and the Community Services multiplexer makes an intraserver connection to the Sametime HTTP server on port 8088 on behalf of the Web browser.

This configuration enables the Sametime server to support HTTP tunneling on port 80 by default following the server installation. For more information, see [About HTTP tunneling](#).

| Port 389 | If you configure the Sametime server to connect to an LDAP server, the Sametime server connects to the LDAP server on this port. For more information, see [Using LDAP with the Sametime server](#). |

| Port 443 | The Domino HTTP server listens for HTTPS connections on this port by default.

This port is used only if you have set up the Domino HTTP server to use Secure Sockets Layer (SSL) for Web browser connections. To configure the Sametime HTTP server to use SSL for Web browser connections, see [About SSL and Sametime](#).

| Port 1352 | The Domino server on which Sametime is installed listens for connections from Notes clients and Domino servers on this port. |

| Port 9092 | The Event Server port on the Sametime server is used for intraserver connections between Sametime components. Make sure that this port is not used by other applications on the server. |

<p>| Port 9094 | The Token Server port on the Sametime server is used for intraserver connections between Sametime components. Make sure that this port is not used by other applications on the server. |</p>
<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 1533</td>
<td>The Community Services listen for direct TCP/IP connections and HTTP-tunneled connections from the Community Services clients (such as Sametime Connect and Sametime Meeting Room clients) on this port. <strong>Note:</strong> The term &quot;direct&quot; TCP/IP connection means that the Sametime client uses a unique Sametime protocol over TCP/IP to establish a connection with the Community Services. The Community Services also listen for HTTPS connections from the Community Services clients on this port by default. The Community Services clients attempt HTTPS connections when accessing the Sametime server through an HTTPS proxy server. If a Community Services client connects to the Sametime server using HTTPS, the HTTPS connection method is used, but the data passed on this connection is not encrypted. If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Community Services clients attempt HTTP-tunneled connections to the Community Services on port 1533 by default. For more information, see <a href="#">About HTTP tunneling</a>.</td>
</tr>
<tr>
<td>Port 80</td>
<td>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 80. For more information, see <a href="#">About HTTP tunneling</a>. <strong>Note:</strong> When HTTP tunneling on port 80 is allowed during the Sametime installation, the Community Services multiplexer listens for HTTP-tunneled connections on both port 80 and port 1533. The Community Services multiplexer simultaneously listens for direct TCP/IP connections on port 1533.</td>
</tr>
<tr>
<td>Port 8082</td>
<td>When HTTP tunneling support is enabled, the Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 8082 by default. Community Services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default. Port 8082 ensures backward compatibility with previous Sametime releases. In previous releases, Sametime clients made HTTP-tunneled connections to the Community Services only on port 8082. If a Sametime Connect client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime 7.0 server, the client might attempt this connection on port 8082.</td>
</tr>
</tbody>
</table>

**Meeting Services ports**

The following default ports are used by the Sametime Meeting Services. These ports are configurable.
<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 8081</td>
<td>The Meeting Services listen for Sametime protocol over TCP/IP connections from the Sametime Meeting Room client on this port. The screen-sharing, whiteboard, send Web page, and question-and-answer polling components of the Sametime Meeting Room client exchange data with the server over this connection. The Meeting Room client can make the TCP/IP connection directly to the Meeting Services or through a SOCKS proxy server. The interactive audio and video components of the Sametime Meeting Room client also exchange control information over a direct TCP/IP connection on this port. Nota: The term &quot;direct&quot; TCP/IP connection means that the Sametime client uses a unique Sametime protocol operating over TCP/IP to establish a connection with the Meeting Services. If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Meeting Services clients attempt HTTP-tunneled connections to the Meeting Services on port 8081 by default. For more information, see <a href="#">About HTTP tunneling</a>.</td>
</tr>
<tr>
<td>Port 80</td>
<td>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Meeting Room client can make HTTP-tunneled connections to the Community Services multiplexer on port 80. When the Meeting Room client makes an HTTP-tunneled connection to the Community Services multiplexer, the Community Services multiplexer makes an intraserver connection to the Meeting Services on behalf of the Meeting Room client. The intraserver connection occurs on port 8081 by default. The Meeting Room client attempts the Sametime protocol over TCP/IP connection (or &quot;direct TCP/IP connection&quot;) on port 8081 before attempting an HTTP-tunneled connection on port 80.</td>
</tr>
<tr>
<td>Port 1503</td>
<td>The Meeting Services listen for T.120 connections from the Meeting Services of other Sametime servers on this port. If you have installed multiple Sametime servers, this port must be open between the two servers for the servers to exchange screen-sharing, whiteboard, and other Meeting Services data.</td>
</tr>
<tr>
<td>Port 1516</td>
<td>In a multiple Sametime server environment, a single Sametime meeting can be simultaneously active on multiple Sametime servers. This functionality is sometimes called “invited servers.” Port 1516 must be open between two Sametime servers to enable one server to extend a meeting invitation to another server in support of the invited servers functionality. For more information, see <a href="#">Advantages of a single meeting on multiple servers</a>.</td>
</tr>
</tbody>
</table>

### Broadcast Services ports

The following default ports are used by the Sametime Broadcast Services. These ports are configurable.
<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 554</td>
<td>The Broadcast Services listen for Real-Time Streaming Protocol (RTSP) call-control connections over TCP/IP on this TCP/IP port. (RTSP uses TCP as the transport service.) The Broadcast client can make the RTSP TCP/IP connection directly to the Broadcast Services or through a SOCKS proxy server. If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Broadcast Services clients attempt HTTP-tunneled connections to the Broadcast Services on port 554 by default. For more information, see <a href="#">About HTTP tunneling</a>.</td>
</tr>
<tr>
<td>Port 80</td>
<td>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Broadcast clients can make HTTP-tunneled connections to the Community Services multiplexer on port 80. When the Broadcast client makes an HTTP-tunneled connection to the Community Services multiplexer, the Community Services multiplexer makes an intraserver connection to the Broadcast Gateway on behalf of the Broadcast client. The intraserver connection occurs on port 554 by default. For more information, see <a href="#">About HTTP tunneling</a>. The Broadcast client attempts the RTSP TCP/IP connection on port 554 before attempting an HTTP-tunneled connection on port 80.</td>
</tr>
<tr>
<td>Dynamic UDP Ports</td>
<td>The Broadcast Services stream meeting data in RTP format from the server to the client over UDP ports. The specific UDP ports are chosen randomly by the Broadcast client and cannot be controlled by the administrator. <strong>Note:</strong> The Broadcast Services can also stream audio and video data to Sametime Broadcast clients. A meeting might include three separate streams (one each for audio, video, and screen-sharing/whiteboard data). If the client or server network, or any network between the Sametime server and the client, does not allow UDP traffic, the Sametime Broadcast Services will tunnel the streamed data over the initial RTSP TCP/IP control connection that occurs on port 554. If the call-control connection was established using HTTP-tunneling on port 80, the client attempts to tunnel the UDP data through the HTTP-tunneled connection on port 80 or other port specified by the administrator. For more information, see <a href="#">Broadcast client connection process using JVM 1.4.2</a>.</td>
</tr>
<tr>
<td>Port 8083</td>
<td>Broadcast Services use this port for internal control connections between Broadcast Services components. You should change this port only if another application on the Sametime server is using port 8083.</td>
</tr>
<tr>
<td>1 - 65535 (UDP ports for multicast)</td>
<td>The Broadcast Services can take advantage of the bandwidth efficiency provided by multicast-enabled networks. If your network supports multicast, the Broadcast Services transmit multicast data over UDP ports within the 1 to 65535 range. <strong>Note:</strong> Multicast uses multicast IP addresses, not the IP address of the Sametime server.</td>
</tr>
</tbody>
</table>

**Audio/Video Services ports**

The following default ports are used by the Audio/Video Services. These ports are configurable.
Proxy support for Sametime clients

The table below shows the client-side proxy types through which clients can connect to the Sametime server.

**Note:** The term “client-side” proxy refers to a proxy server that is deployed in the client’s network. To access other machines on the Internet, the client connects to the client-side proxy and the proxy sends requests to the Internet on behalf of the client. Before sending these requests, the client-side proxy substitutes its IP address for the address of client. This substitution hides the IP addresses of internal clients and makes it appear as if all outbound network traffic originates from a single address (the proxy server). Hiding internal addresses in this way makes it more difficult for attackers to gain knowledge of your internal networks. A client-side proxy is sometimes called a “forward” proxy. A Sametime server can be deployed behind a reverse HTTP proxy server (or “server-side” proxy). For more information about using a Sametime server with a reverse proxy server, see [”Using reverse proxy servers with the Sametime server”](#).

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 801</td>
<td>The Sametime Meeting Room client establishes a TCP/IP connection with the Sametime server Meeting Services on this port. The Audio/Video Services and audio/video components of the Sametime Meeting Room client use this connection to the Meeting Services for call-control functions.</td>
</tr>
<tr>
<td>49252 - 65535 (Dynamic UDP port range)</td>
<td>The Sametime Audio/Video Services listen for inbound audio and video streams from Sametime Meeting Room clients on a range of UDP ports specified by the administrator. The UDP ports are selected by the Sametime Audio/Video Services dynamically from within the range of ports specified by the administrator. The administrator can configure the range of available UDP ports from the MMP UDP port numbers start at/end at settings available from the Interactive Audio/Video Services “Networks and Ports” settings of the Sametime Administration Tool.</td>
</tr>
<tr>
<td>Port 804</td>
<td>If UDP is unavailable between a Sametime Meeting Room client and a Sametime server, Sametime uses this TCP port when attempting to tunnel the RTP audio and video streams using the TCP transport.</td>
</tr>
<tr>
<td>Port 9093</td>
<td>The Interactive Audio/Video Services use this port for internal control connections between Interactive Audio/Video Services components. You should change this port only if another application on the Sametime server is using port 9093.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sametime client</th>
<th>SOCKS 4 proxy</th>
<th>SOCKS 5 proxy</th>
<th>HTTP proxy</th>
<th>HTTPS proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Connect</td>
<td>supported</td>
<td>supported</td>
<td>supported</td>
<td>supported</td>
</tr>
<tr>
<td>Sametime Meeting Room screen-sharing/whiteboard components</td>
<td>supported</td>
<td>not supported</td>
<td>supported</td>
<td>not supported*</td>
</tr>
<tr>
<td>Sametime Meeting Room participant list/chat components</td>
<td>supported</td>
<td>not supported</td>
<td>supported</td>
<td>not supported</td>
</tr>
</tbody>
</table>

*Not supported in some configurations.
<table>
<thead>
<tr>
<th>Sametime client</th>
<th>SOCKS 4 proxy</th>
<th>SOCKS 5 proxy</th>
<th>HTTP proxy</th>
<th>HTTPS proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Meeting Room interactive audio/video components</td>
<td>supported</td>
<td>not supported</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>Sametime Broadcast client</td>
<td>supported</td>
<td>not supported</td>
<td>supported</td>
<td>not supported</td>
</tr>
</tbody>
</table>

* Sametime Meeting Room clients can make HTTP connections through an HTTPS proxy. However, Sametime Meeting Room clients cannot make HTTPS connections through the HTTPS proxy. Sametime Connect supports a special feature of HTTPS proxies (called CONNECT) that enables the Sametime Connect client to maintain a persistent, asynchronous connection through an HTTPS proxy. The Meeting Room client does not support CONNECT.

### Overview of Sametime client connectivity

This section includes descriptions of the connectivity settings available from the Configuration-Connectivity-"Networks and Ports" tab of the Sametime Administration Tool. These settings control the ports on which the Sametime server listens for connections from clients and can affect the connection processes of the clients. For information about the connectivity settings in the Sametime Administration Tool, see Configuring Sametime "Networks and Ports" settings.

This section also describes the connection processes of each client to illustrate how the connectivity settings on the "Networks and Ports" tabs affect the connection processes of Sametime clients. The connection processes also explain the client behavior in relation to proxy servers and Proxy Auto-Configuration (PAC) files. For more information about client connection processes, including direct TCP/IP connections and HTTP-tunneled connections, see:

- Sametime Connect client connection processes
- Meeting Room and Broadcast client connection processes

### Configuring Sametime "Networks and Ports" settings

Sametime connectivity settings are available from the "Networks and Ports" tab of the Sametime Administration Tool. To access the "Networks and Ports" tab, open the Sametime Administration Tool and select Configuration-Connectivity-"Networks and Ports."

The settings on the "Networks and Ports" tab define the host names and ports on which the Sametime services listen for connections from clients and control other aspects of connectivity, such as HTTP-tunneling functionality. Changing these settings can affect the connection processes of clients.

The connectivity options available from the "Networks and Ports" tab include:

- **HTTP Services settings** - These settings specify the ports on which the Domino HTTP server listens for HTTP connections from Web browsers. If the administrator allows HTTP tunneling on port 80, the Sametime Community Services multiplexer listens for HTTP connections on port 80, and the Domino HTTP server must listen on a different port to prevent a port conflict. For more information, see HTTP Services settings.
• **Community Services Network settings** - These settings specify the Community Services host names and ports and affect the connection processes of Community Services clients, including the client HTTP-tunneling functionality.

The Community Services support all presence and chat features of Sametime. The Community Services clients include Sametime Connect, the Sametime Meeting Room client (participant list and chat components), and the Community Services of other Sametime servers. For more information, see [Community Services Network settings](#).

• **Meeting Services Network settings** - These settings specify the Meeting Services host name and ports and affect the connection processes of Meeting Services clients, including the client HTTP-tunneling functionality.

The Meeting Services support the starting and stopping of meetings, screen-sharing, whiteboard, polling, send Web page, and other T.120 activity. The Meeting Services clients include the Sametime Meeting Room client (screen-sharing, whiteboard, polling, and send Web page components) and the Meeting Services of other Sametime servers. For more information, see [Meeting services Network settings](#).

• **Broadcast Services Network settings** - These settings specify the Broadcast Services host name and ports and affect the connection processes of the Sametime Broadcast clients, including the client HTTP-tunneling functionality.

The Broadcast Services support all broadcast meetings. Broadcast meetings can also include audio and video. When a broadcast meeting includes audio/video, the Broadcast Services are responsible for transmitting the audio/video streams to the Broadcast clients. For more information, see [Broadcast Services network settings](#) and [About the Broadcast Services](#).

• **Interactive Audio/Video settings** - These settings specify the Audio/Video Services ports and affect the connection processes of the Sametime Meeting Room client to the Audio/Video Services. The Audio/Video Services support all interactive IP audio and video activity on the Sametime server. For more information, see [Interactive Audio/Video network settings](#).

• **Reverse Proxy Support** - These settings enable a Sametime server to be deployed behind a reverse proxy server. The administrator must configure these settings to ensure that Sametime clients can communicate with a Sametime server through the reverse proxy server. For more information see [Using reverse proxy or portal servers with the Sametime server](#) and [Configuring a Sametime server to operate with a reverse proxy server](#).

• **About HTTP Tunneling** - During installation, the administrator can allow HTTP tunneling on port 80 for all clients except audio/video clients. This capability enables the Sametime Connect client, Sametime Meeting Room client, and Sametime Broadcast clients to connect to the Sametime server using HTTP over port 80. The Sametime 7.0 server can support HTTP tunneling on port 80 for all clients when only one IP address is assigned to the server.

The administrator can also manually assign separate IP addresses to each of the Sametime services to accommodate the HTTP tunneling on port 80 functionality. Using multiple IP addresses to support the HTTP tunneling on port 80 functionality is more efficient than using a single IP address to support this functionality. For more information, see [About HTTP tunneling](#).

• **Assigning IP addresses to multiple Sametime servers installed on a single server machine** - If you are operating Sametime on an IBM i5/OS or IBM pSeries server, you can install multiple Sametime servers on a single server machine. In this scenario, each instance of a Sametime server operates in a separate partition of the single physical server. When multiple servers are operating in separate partitions of a single machine, it is important for each
HTTP Services settings

Sametime installs on a Domino server and uses the HTTP server provided with the Domino server.

During a Sametime installation, the administrator can allow HTTP tunneling on port 80. To support the HTTP tunneling on port 80 functionality, the Community Services multiplexer on the server listens for HTTP connections from clients (including Web browsers) on port 80. A Web browser connects to the Community Services multiplexer on port 80, and the Community Services multiplexer makes an intraserver connection to the Domino HTTP server on behalf of the Web browser.

If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server must listen for HTTP connections on a port other than port 80. In this scenario, the Sametime server installation programmaticaly changes the HTTP port of the Domino HTTP server to port 8088 during the Sametime installation process. It is not necessary to manually change the setting.

If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server listens for HTTP connections on port 80 by default.

For more information about the HTTP tunneling functionality supported by Sametime, see [About HTTP tunneling].

On some platforms, you can configure Sametime to operate using a Microsoft IIS HTTP server or IBM WebSphere HTTP server. For information on setting up Sametime to use a different HTTP Web server, see the installation guide that shipped with the Sametime software.

Follow these instructions if you need to change the HTTP port of the Domino HTTP server:

1. Open the Sametime Administration Tool.
2. Select Configuraton-Connectivity-"Networks and Ports."
3. Select "Configure HTTP Services on a Web page in its own window."
4. Select Ports.
5. Select Internet Ports.
   If the Domino server is set up for HTTP connections from Web browsers, you can change the "TCP/IP port number" setting.
   The "TCP/IP port number" for the HTTP server is located under the "Web (HTTP/HTTPS)" column of the settings. To change the port used by the HTTP server, change the port associated with the "TCP/IP port number" field. (For example, if you are enabling HTTP tunneling on port 80 on a Sametime server that includes a single IP address, you may want to change the HTTP port from port 80 to 8088.)
6. Select "Internet Protocols."
7. Select "Domino Web Engine."
8. Under the "Generating References to this server" section, make the following changes:
If the HTTP server uses HTTP for Web browser connections:

- In the Protocol setting, select "http."
- In the "Port number" setting, enter the same port entered in the "TCP/IP port number" setting in Step 5.

9. Click "Save and Close" to save the Server document.
10. Restart the Domino server for the change to take effect.

Community Services Network settings

The Community Services Network settings control the host names and ports on which the Sametime Community Services multiplexer listens for connections from clients. The administrator can also enable or disable the HTTP tunneling functionality from the Community Services Network settings.

Access the Community Services Network settings from the Sametime Administration Tool by selecting Configuration-Connectivity-"Networks and Ports."

The Community Services multiplexer (or "mux") is the component of the Community Services that handles connections from clients. The Community Services multiplexer handles TCP/IP connections to the Community Services.

The Community Services multiplexer is particularly important to connectivity. In addition to handling TCP/IP connections to the Community Services, the Community Services multiplexer can also handle HTTP-tunneled connections to the Community Services, Meeting Services, and Broadcast Services. For more information, see [Sametime Connect client connection processes](http://www.ibm.com/support/docview.wss?uid=swg27023290) [Meeting Room and Broadcast client connection processes](http://www.ibm.com/support/docview.wss?uid=swg27024340) and About [HTTP tunneling](http://www.ibm.com/support/docview.wss?uid=swg27026907).

The Community Services Network settings include:

- Address for server connections
- Address for client connections
- Address for HTTPS-tunneled client connections
- Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options
- Address for HTTP-tunneled client connections (Community Services)

Address for server connections (Community Services)

The Community Services Network "Address for server connections" settings control the IP addresses or DNS names and the ports on which the Community Services listen for connections from the Community Services of other Sametime servers.

The "Address for server connections" setting includes these fields:

- Host name
- Port number

**Host name:** The "Host name" field allows an administrator to specify the IP addresses or DNS names (for example, www.sametime.com) on which the Community Services multiplexer listens for connections from the Community Services of other Sametime servers.

If this field is blank, the Community Services multiplexer listens for the Community Services server-to-server connections on all IP addresses or DNS names assigned to the machine on which the server is installed.
If only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.

If you enter one or more IP addresses or DNS names in the "Host name" field, the Community Services multiplexer listens for server-to-server connections only on the IP addresses or DNS names specified in the "Host name" field. When entering multiple IP addresses or DNS names in this field, separate each entry with a comma.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple servers is assigned a separate IP address. For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

If you change this setting, click the Update button and restart the server for the changes to take effect.

**Port number:** The "Port number" setting specifies the TCP/IP port (default 1516) on which the Community Services multiplexer listens for connections from the Community Services of other Sametime servers. Community Services server-to-server connections are direct TCP/IP connections that cannot occur through a proxy server.

This port is also used by the Community Services for intraserver connections to other components of the Community Services. For example, the Community Services multiplexer can listen for connections from Community Services clients on port 1533 and port 80. The Community Services multiplexer connects to other components of the Community Services on port 1516.

For more information about working with multiple Sametime servers, see:
- [Integrating a Sametime server into an existing Sametime community](#)
- [Extending Sametime to Internet users](#)

If you change this setting, click the Update button and restart the server for the changes to take effect.

**Address for client connections (Community Services)**

The Community Services Network "Address for client connections" settings control the IP addresses or DNS names and the ports on which the Community Services multiplexer listens for TCP/IP connections, HTTP-tunneled connections, and HTTPS-tunneled connections from clients.

**Note:** The Community Services multiplexer contains a connectivity agent that enables the multiplexer to simultaneously listen for connections that use different protocols (HTTP, HTTPS, or TCP/IP) on a single port. This feature enables Community Services clients to establish connections to the Sametime server in a wide variety of network environments.

These clients include Sametime Connect clients and Sametime Meeting Room clients. For information on the connection processes of these clients, see Sametime Connect client connection processes and Meeting Room and Broadcast client connection processes.

**Note:** The term "TCP/IP connection" means that the clients and server use a unique Sametime protocol operating over TCP/IP to establish a connection.
The client can make this TCP/IP connection directly to the Community Services on the Sametime server or through a SOCKS proxy. A direct TCP/IP connection provides the best performance. The direct TCP/IP connection is also called a "Direct connection using Sametime standard protocol" in the Sametime Connect client Sametime Connectivity settings.

The "Address for client connections" setting includes these fields:

- **Host name**
- **Port number**

**Host name:** The "Host name" field allows an administrator to specify the IP addresses or DNS names (for example, www.sametime.com) on which the Community Services multiplexer listens for TCP/IP connections, HTTP-tunneled connections, and HTTPS-tunneled connections from clients.

If the "Host name" field is blank, the Community Services multiplexer listens for these connections on all IP addresses or DNS names assigned to the machine on which the Sametime server is installed.

If only one IP address or DNS name is assigned to the server, Lotus software recommends leaving the "Host name" field blank.

If you enter one or more IP addresses or DNS names in the "Host name" field, the Community Services multiplexer listens for TCP/IP connections only on the IP addresses or DNS names specified in the "Host name" field. When entering multiple IP addresses or DNS names in this field, separate each entry with a comma.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple servers is assigned a separate IP address. For more information, see [Assigning IP addresses to multiple Sametime servers installed on a single server machine](#).

The "Host name" field can also be used if you decide to use multiple IP addresses to support the HTTP tunneling functionality. For more information, see [Configuring HTTP tunneling on a machine that uses multiple IP addresses](#).

If you change the "Host name" setting, click the Update button and restart the server for the change to take effect.

**Port number:** The "Port number" setting allows an administrator to specify the ports (default 1533) on which the Community Services multiplexer listens for TCP/IP connections, HTTP-tunneled connections, and HTTPS-tunneled connections from Community Services clients, such as the Sametime Connect client and the Sametime Meeting Room client.

If multiple ports exist in the "Port number" field, the Community Services multiplexer listens for these connections on all ports specified in the field. For example, if the administrator enters ports 1533 and 1522 in this field, the Community Services multiplexer listens for TCP/IP, HTTP-tunneled, and HTTPS-tunneled connections on both ports 1533 and 1522. When entering multiple ports in this field, separate each entry with a comma.
The Meeting Room client automatically attempts a direct TCP/IP connection to the Community Services multiplexer on these ports after loading in the user’s Web browser.

**Note:** The Meeting Room client will not attempt an HTTP-tunneled connection to the Community Services on this port. For more information about the Meeting Room client connection processes, see Meeting Room and Broadcast client connection processes.

The Sametime Connect client can attempt a TCP/IP connection, an HTTP-tunneled connection, or an HTTPS-tunneled connection to the Community Services on this port. The type of connection the Sametime Connect client attempts is dependent on the connectivity setting that is specified in the Options-Preferences-Sametime Connectivity tab of the Sametime Connect client. For more information about this connection process, see:

- Basic Sametime Connect client connection process
- Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings

If you change the "Port number" setting, click the Update button and restart the server for the change to take effect.

**Address for HTTPS-tunneled client connections (Community Services)**

The Community Services Network "Address for HTTPS-tunneled client connections" settings control the IP addresses or DNS names and the ports on which the Community Services multiplexer listens for HTTPS-tunneled connections from the Sametime Connect client. Only the Sametime Connect client can attempt HTTPS-tunneled connections to the Community Services. For information about this connection process, see Sametime Connect client connection process.

The "Address for HTTPS-tunneled client connections" setting includes these fields:

- **Host name**
- **Port number**

**Host name:** The "Host name" field allows an administrator to specify the IP addresses or DNS names (for example, www.sametime.com) on which the Community Services multiplexer listens for HTTPS-tunneled connections from Sametime Connect clients.

If the "Host name" field is blank, the Community Services multiplexer listens for HTTPS-tunneled connections on all IP addresses or DNS names assigned to the machine on which the Sametime server is installed.

If only one IP address or DNS name is assigned to the server, Lotus software recommends leaving the "Host name" field blank.

If you enter one or more IP addresses or DNS names in the "Host name" field, the Community Services multiplexer listens for HTTPS-tunneled connections only on the IP addresses or DNS names specified in the "Host name" field. When entering multiple IP addresses or DNS names in this field, separate each entry with a comma.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the
"Host name" field to ensure that each of the multiple servers is assigned a separate IP address. For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

If you change the "Host name" setting, click the Update button and restart the server for the changes to take effect.

**Port number:** The "Port number" setting allows an administrator to specify the ports (default 1533) on which the Community Services multiplexer listens for HTTPS-tunneled connections from Sametime Connect clients. If multiple ports exist in the "Port number" field, the Community Services multiplexer listens for HTTPS-tunneled connections on all ports specified. For example, if the administrator enters ports 1533 and 443 in this field, the Community Services multiplexer listens for HTTPS-tunneled connections on both ports 1533 and 443. When entering multiple ports in this field, separate each entry with a comma.

The Sametime Connect client attempts HTTPS-tunneled connections through an HTTPS proxy when the Use Proxy and "Use HTTPS proxy" options are selected in the Sametime Connect client Sametime Connectivity settings. For more information, see Basic Sametime Connect client connection process.

Many organizations have firewall or network configurations that prevent HTTPS connections on the default port of 1533. For the Sametime Connect clients to connect to the Community Services multiplexer, you might need to specify port 443 as the "Address for HTTPS client connections" port. If you specify port 443 as a Community Services HTTPS-tunneled client connection port, note the following:

- The Sametime Connect clients must have the "Use proxy" and "Use HTTPS proxy" options selected in the Sametime Connectivity settings.
- The "Community port" setting in the Sametime Connect client Sametime Connectivity settings must match the Community Services Network-Address for HTTPS client connections "Port number" setting in the Sametime Administration Tool. If you specify port 443 as the Community Services Network-Address for HTTPS client connections "Port number" setting, the "Community port" setting in the Sametime Connect clients must also specify port 443.
- Sametime Connect client establishes an HTTPS connection but this HTTPS connection is not encrypted with SSL. To secure chat messages, users should select the "Secure messages I start" option in the Options-Preferences-Messages settings of the Sametime Connect client.

**Note:** The HTTPS connection method is implemented to enable the Sametime Connect client to pass data through the HTTPS proxy. However, the data passing over this HTTPS connection is not encrypted.

- If you have configured the Domino HTTP server to use SSL for Web browser connections, the Domino HTTP server listens for HTTPS connections on port 443. In this case, you cannot specify port 443 as the Community Services Network-Address for HTTPS client connections "Port number" setting unless you assign multiple IP addresses to the Sametime server machine. This configuration would cause both the Community Services multiplexer and the Domino HTTP server to listen for HTTPS connections on the same port number and IP address. For more information on this issue, see the "Things you need to know" section of the Sametime 7.0 Release Notes (strn70.nsf or strn70.pdf on the Sametime CD).

If you change the HTTPS Tunneded Client Connections Port setting, click the Update button and restart the server for the changes to take effect.
Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options

The Community Services Network "Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options" setting enables the Sametime Meeting Room client to use HTTP to establish connections with the Community Services multiplexer.

When this setting is enabled, the Sametime Meeting Room client attempts an HTTP-tunneled connection to the Community Services multiplexer if the following settings match:

- The "Host name" and "Port number" settings under "Address for HTTP tunneled client connections" in the Meeting Services Network settings.
- The "Host name" and "Port number" settings under "Address for HTTP tunneled client connections" in the Community Services Network settings.

The Meeting Room client attempts the HTTP-tunneled connection on the matching port number.

Note the following about this setting:

- If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the following settings both specify port 80:
  - The "Port number" setting under "Address for HTTP tunneled client connections" in the Meeting Services Network settings.
  - The "Port number" setting under "Address for HTTP tunneled client connections" in the Community Services Network settings.

This configuration enables the Sametime server to support HTTP tunneling on port 80 on a Sametime server that uses a single IP address. For more information, see [About HTTP tunneling](#).

- The Meeting Room client attempts a TCP/IP connection to the Community Services before attempting an HTTP-tunneled connection to the Community Services multiplexer. For more information about the Meeting Room client connection process, see [Meeting Room and Broadcast client connection processes](#).

- If the "Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options" setting is disabled, the Meeting Room client will not attempt HTTP-tunneled connections to the Community Services multiplexer.

The Meeting Room client might attempt HTTP-tunneled connections to the Meeting Services (instead of the Community Services multiplexer) if the Meeting Services "Enable the Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options" setting is enabled. For more information, see [Enable Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options](#).

Address for HTTP-tunneled client connections (Community Services)

The Community Services Network "Address for HTTP tunneled client connections" settings control the IP addresses or DNS names and the ports on which the Community Services multiplexer listens for HTTP-tunneled connections from clients.

The fields included with this setting are:

- Host name
• Port number

**Host name:** The "Host name" field allows an administrator to specify the IP addresses or DNS names (for example, www.sametime.com) on which the Community Services multiplexer listens for HTTP-tunneled connections from clients.

If the "Host name" field is blank, the Community Services multiplexer listens for HTTP-tunneled connections on all IP addresses or DNS names assigned to the machine on which the Sametime server is installed.

If only one IP address or DNS name is assigned to the server, Lotus software recommends leaving the "Host name" field blank.

If you enter one or more IP addresses or DNS names in the "Host name" field, the Community Services multiplexer listens for HTTP-tunneled connections only on the IP addresses or DNS names specified in the "Host name" field. When entering multiple IP addresses or DNS names in this field, separate each entry with a comma.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple servers is assigned a separate IP address. For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

The "Host name" field can also be used if you decide to use multiple IP addresses to support the HTTP tunneling functionality. For more information, see Configuring HTTP tunneling on a machine that uses multiple IP addresses.

If you change the Address for HTTP-tunneled connections "Host name" setting, click the Update button and restart the server for the changes to take effect.

**Port number:** The "Port number" field allows an administrator to specify the ports on which the Community Services multiplexer listens for HTTP-tunneled connections from Sametime clients.

The default port numbers are dependent on the "Allow HTTP tunneling on port 80" option available to the Sametime administrator during the Sametime server installation.

• If the administrator chooses the "Allow HTTP tunneling on port 80" option during the Sametime server installation, the default port number is port 80.
• If the administrator does not choose the "Allow HTTP tunneling on port 80" option during the Sametime server installation, the default port numbers are ports 1533 and 8082.

If multiple ports exist in this "Port number" field, the Community Services multiplexer listens for HTTP-tunneled connections on all ports specified. For example, when ports 80 and 8082 are entered in this field, the Community Services multiplexer simultaneously listens for HTTP-tunneled connections on both ports 80 and 8082. When entering multiple ports in this field, separate each entry with a comma.

**Note:** The Community Services multiplexer will also listen for HTTP-tunneled connections on the Community Services Network-Address for client connections-Port number (default 1533).
The Sametime Meeting Room client, the Sametime Connect client, and the
Sametime Broadcast client can make HTTP-tunneled connections to the
Community Services multiplexer. These HTTP-tunneled connections are discussed
below.

**Meeting Room client connection to Community Services:** When joining a
meeting, the Meeting Room client must make separate connections to the
Community Services and the Meeting Services. The Meeting Room client attempts
a TCP/IP connection to the Meeting Services (on default port 8081) and a separate
TCP/IP connection to the Community Services (on default port 1533). If the
network security configuration prevents these TCP/IP connections, the Meeting
Room client resorts to HTTP tunneling, as described below:

- To establish a Community Services connection, the Meeting Room client
  attempts an HTTP-tunneled connection to the Community Services multiplexer
  using the Port number specified in the "Port number" field under "Address for
  HTTP tunneled client connections" in the Community Services Network settings.
The Community Services multiplexer handles all connections (TCP/IP or
HTTP-tunneled) to the Community Services.

- To establish the Meeting Services connection, the Meeting Room client attempts
  an HTTP-tunneled connection to the Community Services multiplexer if both of
  the following conditions exist:

  - The "Enable the Meeting Room client to try HTTP tunneling to the
    Community Server after trying other options" setting is enabled.

  - A port specified in the "Port number" field under "Address for HTTP
tunneled client connections" in the Meeting Services Network settings
  matches a port number specified in the "Port number" field under "Address
  for HTTP tunneled client connections" in the Community Services Network
  settings. The connection attempt to the Community Services multiplexer
  occurs on the matching port number. (If none of the port settings in these two
  "Port number" fields match, the HTTP-tunneled Meeting Services connection
  occurs to the Meeting Services instead of the Community Services
  multiplexer.)

If the administrator allows HTTP tunneling on port 80 during the Sametime
server installation, both the Community Services and Meeting Services HTTP
tunneling ports default to port 80. The Meeting Room client attempts the
HTTP-tunneled Meeting Services connection to the Community Services
multiplexer on port 80 (the matching port number). The Community Services
multiplexer handles the HTTP-tunneled connection from the client and
forwards the data to the Meeting Services.

For more information, see the following:

- [Meeting Room client connection process using JVM 1.4.2 (Community
  Services and Meeting Services)]
- Configuring HTTP tunneling settings

**Sametime Connect client connection:** The Sametime Connect client can attempt
an HTTP-tunneled connection to the Community Services multiplexer when any of
the following options are selected in the Sametime Connectivity tab of the
Sametime Connect client:

- Use my Internet Explorer HTTP settings (Sametime Connect for the desktop
  only)
- Direct connection using HTTP protocol
- Use Proxy and Use HTTP proxy
• Use my Java Plug-in settings is selected and an HTTP proxy server is specified in the Java Plug-in settings

The Sametime Connect client will use the port specified as the “Community port” (default 1533) in the Options-Preferences-Sametime Connectivity tab of the Sametime Connect client to establish an HTTP-tunneled connection with the Community Services multiplexer. To enable the Sametime Connect client to successfully establish an HTTP-tunneled connection to the Community Services, the “Community port” setting in the Sametime Connect client must match one of the port numbers on which the Community Services multiplexer listens for HTTP-tunneled connections. Note that the Community Services multiplexer will listen for HTTP-tunneled connections on these ports:

• The “Port number” setting under ”Address for client connections” in the Community Services Network settings of the Sametime Administration Tool

• The “Port number” setting under ”Address for HTTP tunneled client connections” in the Community Services Network settings of the Sametime Administration Tool

**Note:** If the Sametime Connect client must connect to the Sametime server through a firewall that allows only HTTP connections on port 80, the “Community port” setting on the Sametime Connect client must specify port 80 and one of the Community Services Network administrations settings listed above must also specify port 80 to enable the client to establish an HTTP-tunneled connection to the server.

For more information about the Sametime Connect client connection processes, see the following:

• [Basic Sametime Connect client connection process](#)

• [Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings](#)

• Configuring HTTP tunneling [settings](#)

**Note:** The port 8082 setting in the ”Port number” field under ”Address for HTTP tunneled client connections” in the Community Services Network settings ensures backward compatibility with previous Sametime releases. In previous releases, Sametime clients made direct TCP/IP connections to the Community Services on port 1533 and HTTP connections on port 8082. If a Sametime Connect client or Sametime Meeting Room client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime 7.0 server, the client might attempt this connection on port 8082 by default. Listing port 8082 in the HTTP Tunneling port setting ensures that these clients can establish HTTP-tunneled connections with the Community Services on the Sametime 7.0 server.

If you change the ”Port number” setting, click the Update button and restart the server for the changes to take effect.

**Meeting Services Network settings**

The Meeting Services Network settings control the host names and ports on which the Meeting Services listen for connections from the Sametime Meeting Room client. The administrator can also enable or disable the HTTP tunneling functionality for connections to the Meeting Services from these settings. Access these settings from the Sametime Administration Tool by selecting Configuration-Connectivity-"Networks and Ports."
The Meeting Services Network settings include:

- Address for server connections
- Address for client connections
- Enable the Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options
- Event Server port
- Token Server port

**Address for server connections (Meeting Services)**

The Meeting Services Network "Address for server connections" settings control the IP address or DNS name and the port on which the Meeting Services listen for T.120 connections from the Meeting Services of other Sametime servers.

The fields in the "Address for client connections" setting include:

- Host name
- Port number

**Host name:** The Host name field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Meeting Services listen for T.120 connections from the Meeting Services of other Sametime servers.

When only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.

The "Host name" field can also be used if you decide to use multiple IP addresses to support the HTTP tunneling functionality. For more information, see [Configuring HTTP tunneling on a machine that uses multiple IP addresses](#).

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple Sametime servers is assigned a separate IP address. For more information, see [Assigning IP addresses to multiple Sametime servers installed on a single server machine](#).

If you change the "Host name" field, click the Update button and restart the server for the changes to take effect.

**Port number:** The "Port number" field specifies the port (default 1503) on which the Meeting Services listen for T.120 connections from the Meeting Services of other Sametime servers. T.120 connections are direct TCP/IP connections that cannot occur through a proxy server.

**Note:** Port 1503, the default setting, is the registered port for T.120 connections.

A Sametime server connects to another Sametime server on this port when multiple Sametime servers are installed and integrated into the same community. For more information, see [Advantages of using multiple Sametime servers](#), [Integrating a Sametime server into an existing Sametime community](#), and [Extending Sametime to Internet users](#).

If you change the "Port number" field, click the Update button and restart the server for the changes to take effect.
Address for client connections (Meeting Services)
The Meeting Services network "Address for client connections" settings control the IP address or DNS name and the port on which the Meeting Services listen for TCP/IP connections from Sametime Meeting Room clients. For information on this connection process, see [Meeting Room client connection process using JVM 1.4.2](http://www.ibm.com/support/docview.wss?uid=swg21428621) (Community Services and Meeting Services).

**Note:** The term "TCP/IP connection" means that the clients and server use a unique Sametime protocol operating over TCP/IP to establish a connection. The client can make this TCP/IP connection directly to the server or make the TCP/IP connection to the server through a SOCKS proxy. A direct TCP/IP connection to the Meeting Services results in more efficient performance than a TCP/IP connection through a SOCKS proxy or an HTTP-tunneled connection.

The "Address for client connections" settings include these fields:
- Host name
- Port number

**Host name:** The "Host name" field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Meeting Services listen for direct TCP/IP connections from Sametime clients.

When only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.

The "Host name" field can also be used if you decide to use multiple IP addresses to support the HTTP tunneling functionality. For more information, see [Configuring HTTP tunneling on a machine that uses multiple IP addresses](http://www.ibm.com/support/docview.wss?uid=swg21428621).

If you change the "Host name" setting, click the Update button and restart the server for the changes to take effect.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple servers is assigned a separate IP address. For more information, see [Assigning IP addresses to multiple Sametime servers installed on a single server machine](http://www.ibm.com/support/docview.wss?uid=swg21428621).

**Port number:** The "Port number" field allows an administrator to specify the port (default 8081) on which the Meeting Services listen for TCP/IP connections from the Sametime Meeting Room client. The Sametime Meeting Room client exchanges screen-sharing, whiteboard, send Web page, question and answer polling, and other Meeting Services data with the Sametime server on this port.

The Meeting Room client automatically attempts a direct TCP/IP connection to the Meeting Services on this port after loading in the user's Web browser. For more information on the Meeting Room client connection processes, see the [Meeting Room and Broadcast client connection processes](http://www.ibm.com/support/docview.wss?uid=swg21428621) section later in this chapter.

The audio/video components of the Sametime Meeting Room client also use the connection on this port to exchange call-control data. For more information, see [Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)](http://www.ibm.com/support/docview.wss?uid=swg21428621).
If you change the Address for client connections "Port number" setting, click the Update button and restart the server for the changes to take effect.

**Enable Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options**

The Meeting Services Network "Enable Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options" setting enables the Sametime Meeting Room client to use HTTP to establish connections with the Meeting Services when a TCP/IP connection attempt fails. This option is selected by default.

The Sametime Meeting Room client can attempt two different kinds of connections to the Meeting Services:

- A connection using a unique Sametime protocol over TCP/IP
- An HTTP-tunneled connection (The unique Sametime protocol data is encased within an HTTP request)

**Note:** The Sametime Meeting Room client can make HTTP-tunneled Meeting Services connections to either the Community Services multiplexer or the Meeting Services. The "Port number" setting under "Address for HTTP tunneled client connections" in the Meeting Services Network settings determines whether this connection occurs to the Community Services multiplexer or the Meeting Services. For more information, see the "Port number" heading later in this topic.

For more information on the Meeting Room connection processes, see the section later in this chapter.

**Address for HTTP tunneled client connections (Meeting Services):** The Meeting Services network "Enable Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options" setting must be selected for the "Address for HTTP tunneled client connections" settings to take effect.

The Meeting Services network "Address for HTTP-tunneled client connections" settings control the IP addresses or DNS names and the port on which the Meeting Services listen for HTTP-tunneled connections from the Sametime Meeting Room client.

**Note:** Sametime uses a unique Sametime protocol over TCP/IP to establish connections with the Meeting Services. The Sametime protocol data can be encased within an HTTP request to enable Sametime clients to connect using HTTP. This capability is referred to as "HTTP tunneling."

**Host name:** The Address for client connections "Host name" field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Meeting Services listen for HTTP-tunneled connections from the Sametime Meeting Room client.

When only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple servers is assigned a separate IP address. For more information, see the section on assigning IP addresses to multiple Sametime servers installed on a single server machine.
If you change the Address HTTP-tunneled client connections "Host name" setting, click the Update button and restart the server for the changes to take effect.

**Port number:** The Address for HTTP tunneled client connections "Port number" setting allows an administrator to specify the port on which the Meeting Services listen for HTTP-tunneled connections from Sametime Meeting Room clients.

The default port numbers are dependent on the "Allow HTTP tunneling on port 80" option available to the Sametime administrator during the Sametime server installation.

- If the administrator chooses the "Allow HTTP tunneling on port 80" option during the Sametime server installation, the default port number is port 80.
- If the administrator does not choose the "Allow HTTP tunneling on port 80" option during the Sametime server installation, the default port number is 8081.

To establish an HTTP-tunneled connection to the Meeting Services, the Meeting Room client can either connect to the Meeting Services or to the Community Services multiplexer. This "Port number" setting determines whether the Meeting Room client establishes an HTTP-tunneled connection to the Community Services multiplexer or the Meeting Services. Note the following:

- The Meeting Services "Enable Web client to try HTTP tunneling after trying other options" setting must be selected to enable the Meeting Room client to make an HTTP-tunneled connection to either the Community Services multiplexer or the Meeting Services.

- If a port number in the "Port number" field under "Address for HTTP tunneled client connections" in the Meeting Services Network settings matches a port number specified in the "Port number" field under "HTTP tunneled client connections" in the Community Services Network settings, the Meeting Room client makes the HTTP-tunneled connection to the Community Services multiplexer. This connection occurs using the matching port number.

If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, both the Community Services and Meeting Services HTTP tunneling ports default to port 80. The Meeting Room client attempts the HTTP-tunneled Meeting Services connections to the Community Services multiplexer. The Community Services multiplexer handles the HTTP-tunneled connection from the client and makes an intraserver TCP/IP connection to the Meeting Services on behalf of the client.

**Note:** The Community Services network-"Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options" setting must also be enabled to allow the Meeting Room client to make HTTP-tunneled connections to the Community Services multiplexer.

- If none of the port numbers specified in the "Port number" field under "Address for HTTP tunneled client connections" in the Meeting Services Network settings match a port number specified in the "Port number" field under "HTTP tunneled client connections" in the Community Services Network settings, the Meeting Room client makes the HTTP-tunneled connection to the Meeting Services and does not use the Community Services multiplexer. This connection occurs using the port number specified in the "Port number" field under "Address for HTTP tunneled client connections" in the Meeting Services Network settings.

For example, if the "Port number" field under "Address for HTTP tunneled client connections" in the Community Services Network settings specifies port 80 and the "Port number" field under "Address for HTTP tunneled client connections" in the Meeting Services Network settings specifies port 85, the
Meeting Room client makes one HTTP-tunneled connection to the Community Services multiplexer on port 80 and a separate HTTP-tunneled connection to the Meeting Services on port 85.

- The “Host name” settings can also affect whether the Meeting Room client HTTP-tunneled connection occurs to the Community Services multiplexer or the Meeting Services. The "Host name" setting can affect the connection process only if multiple IP addresses or DNS host names are assigned to the Sametime server.

  If the "Host name" field under "Address for HTTP tunneled client connections" in the Meeting Services Network settings specifies a different host name than the “Host name” field under "Address for HTTP tunneled client connections" in the Community Services Network settings, the Meeting Room client makes the HTTP-tunneled connection to the Meeting Services regardless of the "Port number" settings. If these two settings specify different host names, the client does not try an HTTP-tunneled connection to the Community Services multiplexer.

  For more information about configuring the HTTP tunneling settings, see:
  - Configuring HTTP tunneling settings
  - Configuring HTTP tunneling on a machine that uses multiple IP addresses

If you change the "Port number" setting, click the Update button and restart the server for the changes to take effect.

**Event server port**

The “Event server” port (default 9092) is used for intraserver connections between components of the Sametime server.

Generally, it is only necessary to change this port if you have installed multiple Sametime servers on a single server machine or if another application on the server uses port 9092.

**Note:** If you run Sametime on an IBM i5/OS or IBM pSeries machine, you can install multiple Sametime servers on a single machine, within the same logical partition. Each Sametime server instance runs on a separate partitioned Domino server. If you run Sametime on Windows 2000 or Windows NT, you can only install one server on each Windows machine.

If multiple Sametime servers are running on the same machine, you must ensure that each Sametime server specifies a different port as the "Event server” port. For example, if Sametime server 1 and Sametime server 2 are running in separate partitions of an IBM i5/OS machine, you can specify port 9092 as the “Event server” port for Sametime server 1 and port 9095 as the "Event server" port for Sametime server 2. Sametime for IBM i5/OS provides an option to specify the Event server port at the time you configure your Sametime server.

  For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine

**Token server port**

The “Token server” port (default 9094) is used for intraserver connections between components of the Sametime server.

Generally, it is only necessary to change this port if you have installed multiple Sametime servers on a single server machine or if another application on the server uses port 9094.
Note: If you run Sametime on an IBM i5/OS or IBM pSeries machine, you can install multiple Sametime servers on a single machine within the same logical partition. Each Sametime server instance runs on a separate partition of the Domino server. If you run Sametime on Windows 2000 or Windows NT, you can only install one server on each Windows machine.

If multiple Sametime servers are running on the same machine, you must ensure that each Sametime server specifies a different port as the “Token server” port. For example, if Sametime server 1 and Sametime server 2 are running in separate partitions of an IBM i5/OS machine, you might want to specify port 9094 as the "Token server” port for Sametime server 1 and port 9096 as the "Token server” port for Sametime server 2. Sametime for IBM i5/OS provides an option to specify the Token server port at the time you configure your Sametime server.

For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

Broadcast Services Network settings

The Broadcast Services Network settings control the host names and ports on which the Broadcast Services listen for connections from Sametime Broadcast clients. The settings also enable the Broadcast Services on the Sametime server to operate on multicast-enabled networks. Access these settings from the Sametime Administration Tool by selecting Configuration-Connectivity-"Networks and Ports."

For more information about the operations of the Broadcast Services, see Broadcast Services components and clients.

The Broadcast Services Network settings include:
- Broadcast gateway address for client connections
- Broadcast gateway address for control connections
- IP address of Small Group Multicast (SGM) router
- Enable Web client to try HTTP tunneling after trying other options
- Use multicast

Broadcast gateway address for client connections

The Broadcast Services network "Broadcast gateway address for client connections" settings control the IP address or DNS name and the port on which the Broadcast Services listen for Real-Time Streaming Protocol (RTSP) TCP/IP call-control connections from Broadcast clients. For more information on the Broadcast client connection process, see the Meeting Room and Broadcast client connection processes section later in this chapter.

The "Broadcast gateway address for client connections” settings include the following fields:
- Host name
- Port number

Host name: The "Host name" field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Broadcast gateway listens for RTSP TCP/IP connections from Broadcast clients.

When only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.
The "Host name" field can also be used if you decide to use multiple IP addresses to support the HTTP tunneling functionality. For more information, see Configuring HTTP tunneling on a machine that uses multiple IP addresses.

If you change the "Host name" setting, click the Update button and restart the server for the changes to take effect.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple Sametime servers is assigned a separate IP address. For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

**Port number:** The Sametime server Broadcast gateway address for client connections "Port number" setting allows an administrator to specify the port (default 554) on which the Broadcast Services gateway listens for RTSP over TCP/IP call-control connections from the Sametime Broadcast client.

The Broadcast gateway component of the Sametime server provides the Broadcast client with descriptions of the media streams available for the broadcast meeting over the connection that occurs on this port. These descriptions include information concerning the audio codecs and bit rates of the broadcast media streams. The description also provides the IP address of the Broadcast Gateway and indicates if multicast is available for transmission of the broadcast streams.

The Broadcast client attempts a RTSP TCP/IP connection to the Broadcast Gateway on this port after loading in a Web browser. For more information on the Broadcast client connection processes, see the Meeting Room and Broadcast client connection processes section later in this chapter.

If you change the "Port number" setting, click Update and restart the Sametime server for the change to take effect.

**Broadcast gateway address for control connections**

The Broadcast Services network "Broadcast gateway address for control connections" settings control the IP addresses or DNS names and the port on which the Sametime Broadcast gateway listens for TCP/IP connections from the Sametime Broadcast gateway controller. The connection between the Broadcast gateway controller and the Broadcast gateway is an intraserver connection unless Sametime is customized so that the Broadcast gateway operates on a different machine than the Sametime server.

**Note:** For more information about the Broadcast gateway and the Broadcast gateway controller, see Broadcast Services server components.

The "Broadcast gateway address for control connections" setting includes these fields:

- Host name
- Port number

**Host name:** The Sametime server "Host name" field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Broadcast gateway listens for the TCP/IP connection from the Broadcast gateway controller. (The Broadcast gateway controller uses this "Host name" when establishing the connection with the Broadcast gateway.)
Note: If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple Sametime servers is assigned a separate IP address. For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

When only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.

Note: By default, the Broadcast gateway and the Broadcast gateway controller are both installed on the Sametime server machine. If Sametime is customized so that the Broadcast gateway operates on a separate machine, enter the IP address or DNS name of the machine on which the Broadcast gateway is installed.

If you change the "Host name" setting, click Update and restart the Sametime server for the change to take effect.

**Port number:** The Sametime server "Port number" setting allows an administrator to specify the port (default 8083) on which the Broadcast Services gateway listens for connections from the Broadcast gateway controller. (The Broadcast gateway controller uses this port when calling the Broadcast gateway.)

Generally, it is only necessary to change this port if another application on the server uses port 8083.

If you change the "Port number" setting, click Update and restart the Sametime server for the change to take effect.

**IP address of Small Group Multicast (SGM) router**
The Broadcast Services gateway component is compatible with the Small Group Multicast (SGM) technology developed by IBM. If the SGM protocol is used in your network, the broadcast gateway component of the Broadcast Services can route all unicast data through the local SGM router.

If you want the Broadcast Services to use SGM when transmitting broadcast meeting streams on the network, you must enter the DNS name or IP address of the SGM router in the "IP address of Small Group Multicast (SGM) router" field. If this field is blank, the SGM protocol is not used when transmitting the broadcast meeting streams.

The broadcast gateway routes unicast streams through the SGM router. Using SGM does not affect the multicast functionality provided with the Broadcast Services. If the "Use multicast" option is selected in the Broadcast Services Network settings, the Broadcast Services will still attempt to multicast the broadcast streams. For more information, see Using multicast.

**Enable broadcast client to try HTTP tunneling after trying other options (Broadcast Services)**
The Broadcast Services Network "Enable broadcast client to try HTTP tunneling after trying other options" setting enables Sametime Broadcast clients to use HTTP to establish a call-control connection with the Broadcast Services gateway if a connection over TCP/IP fails.

The Sametime Broadcast client can attempt two different kinds of connections to the Broadcast Services:
• A connection using RTSP over TCP/IP
• An HTTP-tunneled connection (The RTSP data is encased within an HTTP request.)

Note: For more information about the Broadcast client connection process, see the [Meeting Room and Broadcast client connection processes](#) later in this chapter.

The Broadcast client can attempt the HTTP-tunneled connection to either the Community Services multiplexer or the Broadcast Services gateway. The Broadcast Services "Port number” setting determines whether this connection occurs to the Community Services multiplexer or the Broadcast Services gateway. For more information, see the "Port number” heading below.

**Broadcast Gateway address for HTTP-tunneled client connections:** The Broadcast Services Network "Enable broadcast client to try HTTP tunneling after trying other options” setting must be selected for the "Broadcast Gateway address for HTTP-tunneled client connections” settings to take effect.

The Broadcast Services network "Broadcast Gateway address for HTTP-tunneled client connections” settings control the IP address or DNS name and the port on which the Broadcast Services gateway listens for HTTP-tunneled connections from the Sametime Broadcast client.

Note: Sametime Broadcast clients use RTSP over TCP/IP to establish connections with the Broadcast Services. The RTSP data can be encased within an HTTP request to enable Sametime Broadcast clients to connect using HTTP. This capability is referred to as "HTTP tunneling.”

**Host name:** The Broadcast Gateway address for HTTP-tunneled client connections "Host name” field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Broadcast Services gateway listens for HTTP-tunneled connections from the Sametime Broadcast client.

Note: If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name” field to ensure that each of the multiple Sametime servers is assigned a separate IP address. For more information, see [Assigning IP addresses to multiple Sametime servers installed on a single server machine](#).

When only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name” field blank.

The "Host name” field can also be used if you decide to use multiple IP addresses to support the HTTP tunneling functionality. For more information, see [Configuring HTTP tunneling on a machine that uses multiple IP addresses](#).

If you change the Address for HTTP-tunneled connections "Host name” setting, click the Update button and restart the server for the changes to take effect.

**Port number:** The Broadcast Gateway address for HTTP-tunneled client connections "Port number” setting allows an administrator to specify the port on which the Broadcast Services gateway listens for HTTP-tunneled connections from Sametime Broadcast clients.
The default port numbers are dependent on the "Allow HTTP tunneling on port 80" option available to the Sametime administrator during the Sametime server installation.

- If the administrator chooses the "Allow HTTP tunneling on port 80" option during the Sametime server installation, the default port number is port 80.
- If the administrator does not choose the "Allow HTTP tunneling on port 80" option during the Sametime server installation, the default port number is 554.

To establish an HTTP-tunneled connection to the Broadcast Services, the Broadcast client can either connect to the Broadcast Services or connect to the Community Services multiplexer. This "Port number" setting determines whether the Broadcast client attempts an HTTP-tunneled connection to the Community Services multiplexer or the Broadcast Services. The "Host name" settings can also affect how this connection occurs. Note the following:

- The Broadcast Services "Enable Web client to try HTTP tunneling after trying other options" setting must be selected to enable the Broadcast client to make an HTTP-tunneled connection to either the Community Services multiplexer or the Broadcast Services.
- If the port number in the "Port number" field under "Broadcast Gateway address for HTTP-tunneled client connections" in the Broadcast Services Network settings matches a port number specified in the "Port number" field under "Address for HTTP-tunneled client connections" in the Community Services Network settings, the Broadcast client makes the HTTP-tunneled connection to the Community Services multiplexer. This connection occurs using the matching port number.

If none of the ports specified in these two settings match, the Broadcast client makes the HTTP-tunneled connection to the Broadcast Services (without using the Community Services multiplexer). This connection occurs using the port number specified in the "Port number" field under "Broadcast Gateway address for HTTP-tunneled client connections" in the Broadcast Services Network settings.

If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, both the Community Services and Broadcast Services HTTP tunneling ports default to port 80. The Broadcast client attempts the HTTP-tunneled Broadcast Services connections to the Community Services multiplexer. The Community Services multiplexer handles the HTTP-tunneled connection from the client and forwards this data to the Broadcast Services.

- The "Host name" settings can also affect whether the Broadcast client HTTP-tunneled connection occurs to the Community Services multiplexer or the Broadcast Services. The "Host name" setting can affect the connection process only if multiple IP addresses or DNS host names are assigned to the Sametime server.

If the following fields specify different host names, the Broadcast client makes the HTTP-tunneled connection to the Broadcast Services, regardless of the Broadcast client "Port number" settings:
- The "Host name" field under "Broadcast Gateway address for HTTP-tunneled client connections" in the Broadcast Services Network settings
- The "Host name" field under "Address for HTTP tunneled client connections" in the Community Services Network settings

If these two settings specify different Host names, the client does not try an HTTP-tunneled connection to the Community Services multiplexer.

For more information about configuring the HTTP tunneling settings, see:

- [About HTTP tunneling](#)
- [Configuring HTTP tunneling settings](#)
– Configuring HTTP tunneling on a machine that uses multiple IP addresses

If you change the "Port number" setting, click the Update button and restart the server for the changes to take effect.

**Use multicast**

Enable this option if your network environment supports multicast technology and you want the Broadcast Services to use multicast when transmitting media streams to Broadcast clients. To support multicast, the UDP transport must be available on the network, and the network routers must be multicast-enabled. For more information, see [Using multicast](#). If you change any of the multicast settings, click Update and restart the Sametime server for the change to take effect.

**Specifying a range of multicast addresses for the Broadcast Services:** When the Broadcast Services Network "Use multicast" option is selected, you can enter a range of Class D multicast IP addresses in the "Multicast addresses start at IP address" and "Multicast addresses end at IP address" fields. When a meeting begins, the Broadcast Services randomly select a multicast address from this range, and begin transmitting data to the selected address. The Broadcast clients associate themselves with this multicast address when forming a multicast group.

**Note:** If your environment includes a multicast address allocation server that supports the Multicast Address Dynamic Client Allocation Protocol (MADCAP), you can configure Sametime to query that server to obtain a multicast address instead of allowing Sametime to randomly select one from a range of addresses. For more information, see "Assign multicast addresses using MADCAP" below.

Generally, a multicast-enabled application randomly selects an IP address from the range of Class D IP addresses reserved for multicast use. There are no network layer protocols that prevent two (or more) different multicast-enabled applications from selecting the same multicast address. If two applications select the same multicast address, this "collision" of addresses can disrupt the transmission of multicast data for both applications.

You should ensure that the Broadcast Services Network multicast address settings specify a different range of addresses than the Interactive Audio/Video Network multicast address settings to prevent multicast address collisions with the Sametime Audio/Video Services.

If the other multicast-enabled applications in your environment also allow you to specify a range of multicast addresses, be sure to specify a range of addresses for these applications that is different from the address range specified for either the Sametime Broadcast Services or Audio/Video Services.

**Note:** When specifying either the "Multicast addresses start at IP address" or "Multicast addresses end at IP address" values, you must enter an IP address that contains four octets (for example, 239.254.254.254). Do not enter an IP address in which the lowest octet is zero. For example, 224.1.1.1 is acceptable, but 224.1.1.0 is not. If the lowest octet has a value of zero, the multicast address range settings do not take effect.

With some multicast environments, you can also associate the range of multicast addresses you select with a geographically close high-end router that is designated as a multicast Rendezvous Point (RP) router. This configuration ensures that the
nearby router is chosen as the RP router. If this is not done, a distant, slow router might be chosen as the RP router, resulting in poor meeting performance.

**Assign multicast addresses using MADCAP:** Select the "Assign multicast addresses using MADCAP" setting to enable Sametime to query a server that supports the Multicast Address Dynamic Client Allocation Protocol (MADCAP) to obtain a multicast address for the meeting.

**Note:** MADCAP is an emerging standard that enables hosts to request multicast address allocation services from multicast allocation servers (such as the Windows 2000 DHCP server). This protocol can prevent multicast address conflicts if you have other applications deployed on your network that require multicast addresses.

If the "Assign multicast addresses using MADCAP" setting is selected, you must specify the DNS name or IP address of the MADCAP-enabled server that you want Sametime to query in the "Host name or IP address of the MADCAP server" setting.

If the "Assign multicast addresses using MADCAP" setting is not selected or Sametime cannot connect to the MADCAP-enabled server, the Sametime server randomly selects an IP address from the range specified by the administrator, as described in "Specifying a range of multicast addresses" above.

**Specifying the Broadcast Services multicast time-to-live (TTL):** When multicast is enabled, the administrator can control how far the multicast traffic will propagate on the network before the multicast traffic is discarded by network routers. The administrator can specify a Time-To-Live (TTL) for the multicast UDP packets. This TTL setting can limit either the number of router hops the packets make before they are discarded or the number of seconds the packets are alive on the network.

The TTL setting measures both time and the number of router hops. The TTL decrements by one for each second it is alive on the network and also decrements by one when it passes through a router. If a packet waits in a router queue for two seconds, the TTL of that packet decrements by three when it passes through the router. The packets TTL decrements twice for the two-second wait and once for passing through the router.

On a typical network packets spend much less than a second in the router queue; the TTL decrements only when passing through the router. In this case, the TTL measures the number of router hops the packet will make. However, long delays at the router queues on a busy network can cause the TTL to expire before making the number of router hops equal to the TTL setting.

The following table provides general guidelines regarding how far multicast data will propagate on the network with specific TTL settings.

<table>
<thead>
<tr>
<th>TTL Setting</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>Restricted to the same subnet</td>
</tr>
<tr>
<td>16.00</td>
<td>Restricted to the same site</td>
</tr>
<tr>
<td>32.00</td>
<td>Restricted to the same region</td>
</tr>
<tr>
<td>64.00</td>
<td>Restricted to the same continent</td>
</tr>
<tr>
<td>128.00</td>
<td>Unrestricted in scope</td>
</tr>
</tbody>
</table>
Interactive Audio/Video Network settings

The Interactive Audio/Video Network settings control the host names and ports on which the Interactive Audio/Video Services listen for connections from Sametime Meeting Room clients.

These settings also enable the Interactive Audio/Video Services on the Sametime server to operate with multicast-enabled networks. Access these settings from the Sametime Administration Tool by selecting Configuration-Connectivity-“Networks and Ports.”

Note: For more information about the operations of the Audio/Video Services, see About the Audio/Video Services and Audio/Video Services server components.

The Interactive Audio/Video Network settings include:

- **TCP tunneling address for client connections**
- **Multimedia Processor (MMP) start at/end at**
- **Multimedia control address**

TCP tunneling address for client connections

When connecting to an interactive audio/video meeting, the Sametime Meeting Room client makes a connection to the Sametime Meeting Services and exchanges interactive audio/video call-control information using the Meeting Services connection. If the call-control connection is successful, the Meeting Room client and server attempt to receive and transmit the audio and video streams using the User Datagram Protocol (UDP) transport.

If UDP is unavailable, the RTP and RTCP audio and video streams are transmitted between the client and server using a TCP connection. This capability is referred to as “TCP tunneling” and ensures that clients operating in network environments that do not allow UDP traffic can participate in interactive audio/video meetings.

Use the “TCP tunneling address for client connections” settings to control the IP address or DNS name and the port on which the Audio/Video Services listen for TCP-tunneled connections from the interactive audio/video components of the Sametime Meeting Room client.

For more information about the Meeting Room client connection processes, see the Meeting Room and Broadcast client connection processes section later in this chapter.

Note: You can use the TCP tunneling address for client connections settings to enable TCP tunneling of interactive audio/video streams on port 80. This capability enables a Sametime Meeting Room client that operates behind a firewall that only allows connections on port 80 to receive all of the data required to participate in an interactive audio/video meeting over port 80. This capability is very useful in circumventing the connectivity restrictions imposed by corporate firewalls. For more information, see TCP tunneling of interactive audio/video streams on port 80.

The “TCP tunneling address for client connections” settings include these fields:

- **Host name**
- **Port number**
**Host name:** The "Host name" field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) on which the Audio/Video Services listen for TCP-tunneled connections from Sametime Meeting Room clients. The specified IP address or DNS name is used to transmit the interactive audio and video streams.

If only one IP address or DNS name is assigned to the Sametime server, Lotus software recommends leaving the "Host name" field blank.

If you change the "Host name" setting, click Update and restart the Sametime server for the change to take effect.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, use the "Host name" field to ensure that each of the multiple Sametime servers is assigned a separate IP address. For more information, see [Assigning IP addresses to multiple Sametime servers installed on a single server machine](#).

**Port number:** The "Port number" setting allows an administrator to specify the port (default 8084) on which the Audio/Video Services listen for TCP-tunneled connections from Sametime Meeting Room clients. The specified port is used to tunnel UDP audio and video streams through a TCP connection.

For a complete description of the connection process associated with this port, see [Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)](#).

If you change the "Port number" setting, click Update and restart the Sametime server for the change to take effect.

**Multimedia Processor (MMP) UDP port numbers start at/end at**
If the UDP transport is available on all networks between the client and server, the Audio/Video Services dynamically select the UDP ports on which to receive audio and video data streams from a range of UDP ports specified by the Sametime administrator. Use the "Multimedia Processor (MMP) UDP..." settings to define the range of UDP ports that are available for the transmission of audio and video data from the clients to the Audio/Video Services. The default range includes UDP ports 49252 through 65535.

For a complete description of this connection process, see [Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)](#).

If you change these settings, click Update and restart the server for the change to take effect.

**Multimedia control address**
The Interactive Audio/Video Network "Multimedia Control Address" settings control the IP address or DNS name and the port on which the Sametime Multimedia Processor (MMP) listens for TCP/IP connections from the Multimedia Multipoint Control Unit (MMCU). The connection from the MMCU to the MMP is an intraserver connection.

For more information about the MMCU and the MMP, see [Audio/Video Services server components](#).

The "Multimedia control address" setting includes these fields:

- Host name
• Port number

**Host name:** The Sametime server "Host name" field allows an administrator to specify the IP address or DNS name (for example, www.sametime.com) the Sametime MMCU uses when establishing a TCP/IP connection with the MMP.

**Note:** If you are running Sametime on an IBM i5/OS or IBM pSeries server, you can run multiple Sametime servers on a single machine. In this case, multiple MMCUs and MMPs might operate on the same physical machine. Use the "Host name" field to ensure that the MMCU connects to the MMP with the same IP address as the MMCU. For more information, see [Assigning IP addresses to multiple Sametime servers installed on a single server machine](#).

If you change the "Host name" setting, click Update and restart the server for the change to take effect.

**Port number:** The Sametime server "Port number" setting allows an administrator to specify the port (default 9093) on which the MMP listens for connections from the MMCU. The MMCU uses this port number when calling the MMP.

Change this port only if another application on the server uses port 9093.

If you change the "Port number" setting, click Update and restart the Sametime server for the change to take effect.

---

**Community Services connectivity and the home Sametime server**

Sametime includes the concept of a home Sametime server. The home Sametime server plays an important part in client connectivity to the Community Services. The Sametime Connect client, Sametime Meeting Room client, and Sametime Links all connect to the Community Services.

If your environment includes multiple Sametime servers or you have deployed other applications enabled with Sametime technology on Domino servers, it is mandatory that every user be assigned to a "home" Sametime server. To assign a user to a home Sametime server, you must enter the name of the Sametime server in the "Sametime server" field of the user’s Person document in the Domino Directory. For more information, see [Assigning users to a home Sametime server](#).

**Note:** Sametime 7.0 supports Community Services server clustering that enables users to receive Community Services functionality from any of a group of clustered Sametime servers. In this scenario, each user can be assigned to a home Sametime server cluster instead of a home Sametime server. For more information, see [Creating Community Services server clusters](#).

The concept of the home Sametime server is important to Community Services connectivity for the following reasons:

• **Users need a single place to store their Community Services preferences** - The home server is the Sametime server to which each user logs in to appear in a presence list in a Sametime client or a database enabled with Sametime technology. The home Sametime server stores a user’s Community Services preferences settings, contact lists, privacy information, and information about the availability of audio/video hardware on the user’s computer. This information is stored in the Notes database vpuserinfo.nsf on the user’s home Sametime server. The client must retrieve this information each time the user logs in to the
Community Services. In multiple server environments, this information must be stored on a single server. If this information were stored on multiple servers and the user changed the Community Services preferences settings while logged in to one Sametime server, the user could receive different Community preferences settings when logging in to a different Sametime server. For this reason, the user is always required to log in to the same home Sametime server.

- **Users can only log in to one Sametime server at a time** - A user’s presence can only be registered to the Community Services on one Sametime server at a time. When multiple Sametime servers are integrated into a single community, the Community Services will not allow a single user to simultaneously log in to the Community Services on two separate Sametime servers. If a user attempts to do so, the first connection to the Community Services is disconnected.

The home Sametime server setting ensures that a user always connects to a single Sametime server to receive the Community Services functionality. For example, assume a user’s home Sametime server setting on the Person document is set to Sametime server A. The user starts the Sametime Connect client and connects to Sametime server A. The user then attends a meeting on Sametime server B that includes presence, chat, and whiteboard functionality. The Meeting Room client launches on the user’s machine and receives the whiteboard data from Sametime server B but is directed to Sametime server A for presence and chat functionality. The home Sametime server setting ensures that the user is always directed to Sametime server A for the Community Services functionality regardless of how many different Sametime clients they are using. If no home Sametime server is specified for a user and the user attempts to connect to the Community Services on two different Sametime servers, all connections to the Community Services are disconnected.

**Note:** Another characteristic of the Community Services is that a user’s presence can originate from only one machine (or IP address) at a time. A user who has two machines can only log in to the Community Services from one of the machines. If the user attempts to log in to the Community Services from Sametime clients on two separate machines, the client that logged in to the Community Services first is disconnected. Although the home Sametime server concept does not solve this issue, the administrator should be aware of this Community Services characteristic if the user population includes many users with multiple machines.

**Sametime Connect and the home Sametime server**

The Sametime Connect client includes settings that enable any user to specify the Sametime server to which the Sametime Connect client will connect. The user specifies a particular Sametime server from the Options - Preferences - Sametime Connectivity settings on the Sametime Connect client.

**Note:** By default, the Sametime Connect client Sametime Connectivity settings specify the server from which it was downloaded as the server to which it should connect. The Sametime Client Packager allows the administrator to change the default settings of any Sametime Connect client downloaded from the server. For more information on the Sametime Client Packager application, see the *Lotus Sametime Server 7.0 Installation Guide* (stinstall.nsf or stinstall.pdf).

Lotus software recommends that the Sametime Connectivity settings of the Sametime Connect client and the "Sametime server" setting on a user’s Person document specify the same Sametime server.
If the Sametime Connectivity settings of a user’s Sametime Connect client specify a different Sametime server than the "Sametime server” field of the user’s Person document, the client first connects to the server specified in the Sametime Connectivity settings of the client, but the connection is redirected to the server specified in the "Sametime server” field of the Person document. Logging in to Community Services occurs on the Sametime server specified in the user’s Person document.

Connectivity functions more efficiently if the Sametime Connectivity settings of the Sametime Connect client specify the same Sametime server as the “Sametime server” setting in a user’s Person document because it is not necessary to redirect the connection to a different Sametime server.

For more information on Community Services connection processes, see:

- Sametime Connect client connection process
- Meeting Room client connection process using JVM 1.4.2 (Community Services and Meeting Services)

**Assigning users to a home Sametime server**

To assign a user to a home Sametime server, enter the Sametime server name in the "Sametime server” field in the Administration section of a user’s Person document in the Domino Directory.

In the "Sametime server” field on the Person document, you can enter the name of the Sametime server in the Domino hierarchical name format (for example, sametime.acme.com/west/acme). The “Sametime server” field automatically converts the name to the full canonical name format. For example, if you enter sametime.acme.com/west/acme in the "Sametime server” field, the name is stored as cn=sametime.acme.com/ou=west/o=acme. You can also use the full canonical format when entering the server name in the "Sametime server” field.

**Note:** Community Services reads the server name from the Servers view ($Servers) of the Domino Directory. The name entered in the "Sametime server” field on the Person document must match the name of the Sametime server as it appears in the Servers view of the Domino Directory. If you are using an agent to populate the home "Sametime server” field for several different users, ensure that the agent specifies the full canonical name of the server.

For information about assigning users to a home Sametime server when Sametime is configured to access an LDAP directory, see Setting the Home Sametime Server setting for LDAP

**Home Sametime servers and self-registration**

If you are allowing self-registration, the "Sametime server” field on the Person document is automatically populated when the user self-registers. The field is populated with the name of the Sametime server on which the user self-registered.

For more information about self-registration, see Using Sametime self-registration

**Home Sametime servers and instant meetings**

When a user starts an instant meeting, the instant meeting is created on the user’s home Sametime server. If a user starts an "n-way chat” (a chat involving more than two people), the chat meeting is also created on the user’s home Sametime server.
Sametime Connect client connection processes

This section discusses the connection processes of the Sametime Connect clients. Read this section to gain a better understanding of how the Sametime Connect clients connect to the server and the configuration settings that affect the connection processes. These configuration settings include both settings on the Sametime Connect client and the “Networks and Ports” settings in the Sametime Administration Tool.

This section discusses the connection processes of both the "Sametime Connect for the desktop" and "Sametime Connect for browsers" clients. The Sametime Connect clients connect to the Community Services on the Sametime server. The Community Services support all Sametime presence and chat capabilities. Sametime Connect clients can establish connections with the Community Services using either direct TCP/IP connections or through HTTP-tunneled connections. The Sametime Connect client can also connect to the Community Services through an HTTPS proxy.

Sametime is designed to enable Sametime Connect clients that operate behind restrictive firewalls to connect to the Sametime services using HTTP over port 80. For detailed information on this capability, see the connection process topics below for the individual clients and [About HTTP tunneling](#).

The Sametime Connect clients offer a variety of different connectivity options to ensure connectivity can be established in any network environment. Because there are many different connectivity options, the discussion of Sametime Connect client connection processes is divided into two topics: Basic Sametime Connect client connection process and Sametime Connect client connection process using the Web browser or Java Plug-in settings.

Basic Sametime Connect client connection process

The "Basic Sametime Connect client connection process” topic discusses the basic connection process used by both the Sametime Connect for browser client and the Sametime Connect for the desktop client. The basic connection processes of both these clients are very similar and are discussed in a single topic.

The "Basic Sametime Connect client connection process” topic discusses all connectivity processes with the exception of the connectivity processes that occur when the user’s Web browser or Java Plug-in settings are used to establish connections with the server.

Sametime Connect client connection process using the Web browser or Java Plug-in settings

The "Sametime Connect client connection process using the Web browser or Java Plug-in settings” topic discusses the connection processes that can occur when the Sametime Connect client is configured to establish a connection using connectivity settings defined in a Web browser or Java Plug-in.

The Sametime Connect for the desktop client and the Sametime Connect for browsers client have different capabilities when using connectivity settings defined in a Web browser or Java Plug-in.

- **Sametime Connect for the desktop** - This client can establish an HTTP connection to the Community Services using the connectivity settings defined in
Basic Sametime Connect client connection process

The Sametime Connect client connects to the Community Services on the Sametime server. The Community Services support all Sametime presence and chat capabilities.

This topic discusses the basic connection processes of both the "Sametime Connect for the desktop" and "Sametime Connect for browsers" clients.

Note: This topic describes all Sametime Connect client connection scenarios with the exception of the connection processes that occur when either the "Use my Internet Explorer HTTP settings," or "Use my Java Plug-in settings" option is selected in the Sametime Connect client Sametime Connectivity settings. For information on these connection processes, see Sametime Connect client connection processes using the Web browser or Java Plug-in settings.

Settings that affect the connection process

The Sametime Connect client connection process is controlled by two groups of settings: the Sametime Connect client Sametime Connectivity settings (available on the client) and the Community Services Network settings (available on the server).

- The Sametime Connect client Sametime Connectivity settings are available from the Options - Preferences - Sametime Connectivity menu in the Sametime Connect client. These settings are stored in the Connect.ini file on the user's local computer; the Connect.ini file is stored in the directory in which the Sametime Connect client is installed.

  The Sametime Connectivity settings enable the Sametime Connect client to make a direct TCP/IP connection (also called a "Direct connection using standard Sametime protocol") or a direct HTTP-tunneled connection to the Community Services. The Sametime Connectivity settings also enable Sametime Connect clients that access the Internet or intranet through HTTP, HTTPS, or SOCKS proxy servers to connect to the Community Services. Sametime Connect uses the port specified in the "Community port" setting of the Sametime Connectivity settings when attempting connections to the Community Services.

  Sametime Connect for the desktop includes a Client Packager application that enables the administrator to pre-configure the Sametime Connect client with the Sametime Connectivity settings appropriate for your network environment. If you use the Client Packager, end users will not have to adjust the connectivity settings of the client to accommodate your network environment. For more information about the Client Packager, see the Lotus Sametime Server 7.0 Installation Guide (stinstall.nsf and stinstall.pdf) on the Sametime product CD. This guide is also available from the Documentation library on the www-10.lotus.com Web site.

- The Community Services Network settings are available from the Configuration-Connectivity-"Networks and Ports" settings of the Sametime Administration Tool. The Community Services Network settings include the "Address for client connections," the "Address for HTTPS client connections,"
and the "Address for HTTP tunneled client connections." These server-side settings control the IP addresses or DNS names and the ports on which the Sametime server Community Services multiplexer listens for Sametime Connect client connections.

**Connection process**

The basic connection process of the Sametime Connect client is described below. The connection process depends on the Connection, "Proxy type," and Port settings that are selected in the Sametime Connect client Sametime Connectivity settings.

1. The user starts the Sametime Connect client. (Sametime Connect for the desktop runs on the Windows operating system. Sametime Connect for browsers loads in the user’s Web browser).

2. The Sametime Connect client examines the values in the "Host" field and the "Community Port" field (default 1533) of the Sametime Connect client Sametime Connectivity settings.

   The Sametime Connect client uses the "Host" and "Community Port" values to determine the Host name and port it should use when attempting a connection to the Sametime server.

   **Note** For the most efficient connectivity, the Host field of the Sametime Connect client Sametime Connectivity settings and the "Sametime server" field of a user’s Person document should specify the same Sametime server (the user’s home Sametime server). For more information, see Connecting to the Home Sametime server.

3. The Sametime Connect client uses the "Connection" setting in its Sametime Connectivity settings to determine how to make the connection to the Host machine specified in the Sametime Connectivity settings. The possible Connection settings are:

   - Use my Internet Explorer HTTP settings (This setting appears in Sametime Connect for the desktop only)
   - Use my Java Plug-in settings (This setting appears in Sametime Connect for browsers only)
   - Direct connection using standard Sametime protocol
   - Direct connection using HTTP protocol
   - Use Proxy

   **Note:** The order in which these settings appear varies for the Sametime Connect client for the desktop and the Sametime Connect client for browsers.

**Using the Internet Explorer HTTP settings or the Java Plug-in settings** - The connection process that occurs when either the “Use my Internet Explorer HTTP settings” or "Use my Java Plug-in settings" is selected is described in a separate section. For more information about these connection processes, see Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings later in this chapter.

"Direct connection using standard Sametime protocol" - Select this setting if the Sametime Connect client can make a direct TCP/IP connection to the Sametime server. Generally, this setting is used when the connection does not occur through a proxy server, and the network does not block TCP/IP connections on the port used by the Sametime Connect client.

When "Direct connection using standard Sametime protocol" is selected as the Connection type, the Sametime Connect client attempts a connection to the Community Services multiplexer on the Sametime server using a unique
Sametime protocol over TCP/IP. The client attempts this connection on the "Community port" (default port 1533) specified in the Sametime Connect client Sametime Connectivity settings.

The Community Services on the Sametime server listen for direct Sametime protocol over TCP/IP connections on the host name and port specified in the "Community Services Network-Address for client connections-Host name and Port" settings of the Sametime Administration Tool. By default, the Community Services listen for this connection on port 1533.

For this connection to succeed, the port setting specified in the Sametime Connect client Sametime Connectivity settings must match one of the ports specified in the "Community Services Network-Address for client connections-Port number" setting on the Sametime server. (By default, both of these settings specify port 1533.)

This connection can fail if the connection must pass through a proxy server or network that prevents direct TCP/IP connections on port 1533 (or other port specified in both the Sametime Connectivity settings of the Sametime Connect client and the "Community Services Network-Address for client connections-Port number" setting in the Sametime Administration Tool). For more information about connecting through firewalls, see About HTTP tunneling and Extending Sametime to Internet users.

"Direct connection using HTTP protocol" setting -Select this option if you want the Sametime Connect client to use HTTP to establish a connection with the Community Services, but you do not want this connection to occur through an HTTP proxy server.

When "Direct connection using HTTP protocol" is selected, the client encases the standard Sametime protocol connection information within an HTTP request. The Sametime Connect client then attempts to establish an HTTP connection directly with the Community Services multiplexer on the Sametime server. The Sametime Connect client attempts this connection on the "Community port" specified in its Sametime Connectivity settings.

The Community Services multiplexer can listen for HTTP-tunneled connections on multiple ports. The Community Services multiplexer listens for HTTP-tunneled connections on the host name and port specified in the "Community Services Network-Address for client connections-Host name and Port" settings of the Sametime Administration Tool and the host name and port specified in the "Community Services Network-Address for HTTP tunneled client connections-Host name and Port number" settings of the Sametime Administration Tool.

Note: If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the Community Services multiplexer listens for HTTP-tunneled connections on port 80 by default on the Community Services Network-Address for HTTP tunneled client connections-Port number. In this scenario, the Community Services multiplexer also listens for HTTP-tunneled connections on port 1533 (the Community Services Network-Address for client connections-Port number).

This setting is used most frequently to enable Sametime Connect clients that operate behind restrictive firewalls without HTTP proxy servers to connect to a Sametime server available to Internet users.

The "Direct connection using HTTP protocol" connectivity option is intended primarily to support the HTTP tunneling on port 80 functionality available with the Sametime 7.0 server. For more information about HTTP tunneling on port 80, see About HTTP tunneling.
If a Sametime Connect client operates behind a firewall that allows only HTTP connections on port 80 and the client’s firewall or network environment does not include an HTTP proxy server, select the "Direct connection using HTTP protocol" setting and change the "Community port" setting in the Sametime Connect client Sametime Connectivity settings from the default of 1533 to port 80.

The administrator must also ensure that the "Port number" setting under "Address for HTTP tunneled client connections" in the Community Services Network settings specified in the Sametime Administration Tool also specifies port 80. Such a configuration should enable a Sametime Connect client operating behind a restrictive firewall to establish a connection with an Internet Sametime server using HTTP tunneling over port 80.

**Use proxy** - Selecting the "Use proxy" option enables the Sametime Connect client to connect through a SOCKS, HTTP, or HTTPS proxy server when establishing a connection to the Community Services. After selecting the "Use proxy" connection type, select the appropriate "Proxy type" in the Sametime Connect client Sametime Connectivity options. The available "Proxy type" settings are:

- Use SOCKS4 proxy
- Use SOCKS5 proxy
- Use HTTPS proxy
- Use HTTP proxy

**Note:** You can also select "Use my Internet Explorer HTTP settings," "Use my Internet Explorer browser settings," or "Use my Java Plug-in settings" to establish connections through HTTP and SOCKS proxy servers. For more information, see [Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings](#).

**Use SOCKS4 proxy and Use SOCKS5 proxy** - If the Sametime Connect client connects to a SOCKS proxy server to access the Internet or intranet, you must select the appropriate SOCKS proxy option (either Use SOCKS4 proxy or Use SOCKS5 proxy) as the "Proxy type" in the Sametime Connect client Sametime Connectivity settings.

If you select "Use SOCKS4 proxy" or "Use SOCKS5 proxy," you must also specify the "Host name" (DNS name or IP address) of the SOCKS proxy server and the port required to connect to the SOCKS proxy server in the "Proxy server" options of the Sametime Connect client Sametime Connectivity settings.

For SOCKS5 proxies, you must also specify the user name and password required for SOCKS5 authentication.

Sametime Connect connects to the SOCKS proxy, and the proxy server connects to the Community Services on the Sametime server on behalf of the Sametime Connect client. The client uses the "standard Sametime protocol" over TCP/IP for this connection. The connection from the SOCKS proxy to the Community Services occurs on the "Community port" (default 1533) specified in the Sametime Connect client Sametime Connectivity settings.

The "Resolve server name locally" setting determines whether the Sametime server host name is resolved by the Sametime Connect client or the SOCKS4 or SOCKS5 proxy server.

When the "Resolve server name locally" setting is selected, the Sametime Connect client calls a local DNS server to resolve the Sametime server name. The Sametime Connect client passes the IP address to the SOCKS proxy; the SOCKS proxy does not resolve the IP address.
When "Resolve server name locally" is not selected, Sametime Connect does not resolve the DNS name of the Sametime server. Sametime Connect passes the DNS name of the Sametime server to the SOCKS proxy, and the SOCKS proxy server calls a DNS server to resolve the server name.

Some organizations do not allow their internal DNS servers to resolve the names of external servers for security reasons. If the DNS server is configured in this way, users should clear the check mark from the "Resolve server name locally" field. The SOCKS proxy resolves the external server name by calling a different DNS server (which is not available on the internal network).

For a connection through a SOCKS proxy to succeed, the port specified in the "Community port" field of the Sametime Connect client Sametime Connectivity settings must match one of the ports listed in the "Community Services Network-Address for client connections-Port number" setting in the Sametime Administration Tool or one of the ports specified in the "Community Services Network-Address for HTTP tunneled client connections-Host name and Port number" setting in the Sametime Administration Tool.

**Use HTTP proxy** - If the Sametime Connect client connects to an HTTP proxy to access the Internet or intranet, you can select "Use HTTP proxy" as the "Proxy type" in the Sametime Connect client Sametime Connectivity settings. If "Use HTTP proxy" is selected as the Proxy type, you must also specify the "Host name" (DNS name or IP address) of the HTTP proxy server and the port required to connect to the HTTP proxy server in the "Proxy server" options of the Sametime Connect client Sametime Connectivity settings.

**Note:** If the HTTP proxy server requires authentication, the user name and password required for authentication to the HTTP proxy server must also be entered in the "Proxy server" options of the Sametime Connect client Sametime Connectivity settings.

When "Use HTTP proxy" is selected, the client encases the standard Sametime protocol connection information within an HTTP request. Sametime Connect connects to the HTTP proxy, and the HTTP proxy server connects to the Community Services multiplexer on the Sametime server on behalf of the Sametime Connect client. The HTTP connection to the Community Services multiplexer occurs on the "Community port" (default 1533) specified in the Sametime Connect client Sametime Connectivity settings.

The Community Services multiplexer on the Sametime server listens for HTTP connections on all ports specified in the "Port number" field under "Address for client connections" in the Community Services Network settings of the Sametime Administration Tool and "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool.

For this connection to succeed, the port specified as the "Community port" setting in the Sametime Connect client Sametime Connectivity settings must match a port number specified in one of these settings in the Sametime Administration Tool:

- The "Port number" field under "Address for client connections" in the Community Services Network settings of the Sametime Administration Tool.
- The "Port number" field under "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool.

**Note:** If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the "Community Services Network-Address for client connections-Port number" setting default
to port 1533, and the “Community Services Network-Address for HTTP tunneled client connections-Port number” settings are ports 80 and 8082. In this configuration, the Sametime Connect client can complete an HTTP-tunneled connection to the Community Services multiplexer using either port 1533, 80, or 8082.

For more information about HTTP tunneling on port 80, see [About HTTP tunneling](#).

**Use HTTPS proxy** - If the Sametime Connect client must connect to an HTTPS proxy to access the Internet or intranet, select the “Use HTTPS proxy” option in the “Proxy type” settings. If “Use HTTPS proxy” is selected as the proxy type, you must also specify:

- The "Host name" (DNS name or IP address) of the HTTPS proxy server
- The port required to connect to the HTTPS proxy server in the "Proxy server" options of the Sametime Connect client Sametime Connectivity settings

When "Use HTTPS proxy" is selected, the client encases the standard Sametime protocol information within an HTTPS request. Sametime Connect connects to the HTTPS proxy, and the HTTPS proxy server connects to the Community Services multiplexer on the Sametime server on behalf of the Sametime Connect client. The HTTPS connection to the Community Services multiplexer occurs on the port (default 1533) specified in the Sametime Connect client Sametime Connectivity settings.

The Community Services multiplexer on the Sametime server listens for HTTPS connections on all ports specified in the "Community Services Network-Address for HTTPS tunneled client connections-Port number" setting in the Configuration-Connectivity options of the Sametime Administration Tool. For this connection to succeed, the port specified as the "Community port" setting in the Sametime Connect client Sametime Connectivity settings must match the port listed in the "Community Services Network-Address for HTTPS tunneled client connections-Port number" setting.

The "Community port” setting in the Sametime Connect client Sametime Connectivity settings and the Community Services Network-Address for HTTPS tunneled client connections-"Port number” setting in the Sametime Administration Tool both specify port 1533 by default.

Many organizations have firewall or network configurations that prevent HTTPS connections on the default port of 1533. For the HTTPS connection to succeed in your network environment, you might need to specify port 443 for HTTPS connections in both of the following settings:

- The "Community port” setting of the Sametime Connect client Sametime Connectivity settings
- The "Port number” field under "Address for HTTPS tunneled client connections” in the Community Services Network settings of the Sametime Administration Tool

If you have configured the Domino HTTP server to listen for HTTPS connections from Web browsers on port 443, the Community Services multiplexer cannot also listen for HTTPS connections on port 443 unless you assign multiple IP addresses to the Sametime server. For more information on this issue, see the "Things you need to know” section of the Sametime 7.0 Release Notes (strn70.nsf or strn70.pdf on the Sametime CD).
Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings

The Sametime Connect clients available with Sametime include connectivity options that enable the clients to use connectivity settings defined in a Web browser or the connectivity settings defined in the Java Plug-in for the Sun or IBM Java Virtual Machine (JVM) 1.4.2 to establish connections with the Community Services on the Sametime server. These connectivity options are discussed below:

- **Use my Internet Explorer HTTP settings** - The “Use my Internet Explorer HTTP settings” option appears only in the Sametime Connectivity tab of the Sametime Connect for the desktop client. This option enables the Sametime Connect for the desktop client to use the connectivity settings defined in a user’s Internet Explorer Web browser to establish connections with the Sametime server. This connection process is described in **Sametime Connect for the desktop - Use my Internet Explorer HTTP settings**. The “Use my Internet Explorer HTTP settings” option does not appear in the Sametime Connect for browsers client.

- **Use my Java Plug-in settings** - The “Use my Java Plug-in settings” option appears in the Sametime Connectivity tab of the Sametime Connect for browsers client when the client loads in a Web browser that runs under the Sun or IBM JVM 1.4.2. The **connection process that occurs when this option is selected** is described in **Sametime Connect for browsers - Use my Java Plug-in settings**. The “Use my Java Plug-in settings” option does not appear in the Sametime Connect for the desktop client.

**Sametime Connect for the desktop - Use my Internet Explorer HTTP settings**

The “Use my Internet Explorer HTTP settings” option appears only in the Sametime Connectivity tab of the Sametime for the desktop client.

When the “Use my Internet Explorer HTTP settings” option is selected in the Sametime Connectivity settings, Sametime Connect for the desktop uses the proxy connectivity settings defined in the user’s Internet Explorer Web browser to attempt an HTTP-tunneled connection to the Sametime server.

The connection process for the “Use my Microsoft Internet Explorer browser settings” option is:

1. The Sametime Connect for browsers client examines the values in the "Host" field and the "Community Port" field (default 1533) of the Sametime Connectivity settings available on the client.

   The Sametime Connect client uses the "Host" and "Community Port" values to determine the Host name and port it should use when attempting a connection to the Sametime server.

   **Note** For the most efficient connectivity, the Host field of the Sametime Connect client Sametime Connectivity settings and the "Sametime server" field of a user’s Person document should specify the same Sametime server. For more information, see **Connecting to the Home Sametime server**.

2. The Sametime Connect client uses the Web connectivity (or proxy) settings of the Web browser to establish a connection with the Community Services as noted in the subsequent steps.

3. The Sametime Connect client encases the standard Sametime protocol data within an HTTP request and attempts to connect to the Community Services multiplexer using HTTP. Encasing this connection protocol data within an HTTP request is called "HTTP-tunneling."
4. Sametime Connect examines the Internet Explorer Web browser connectivity settings to attempt the HTTP-tunneled connection to the Community Services multiplexer. If the Web browser settings:

- **Do not specify a proxy server** - The HTTP request is sent directly to the Community Services multiplexer on the Sametime server. This connection is called a "direct HTTP connection."

- **Specify a SOCKS proxy server** - The HTTP request is sent to the Community Services multiplexer through the SOCKS proxy server.

- **Specify an HTTP proxy server** - The HTTP request is sent to the Community Services multiplexer through the HTTP proxy server.

In all three cases above, the Host name and "Community port" settings (default port 1533) specified in the Sametime Connect client are used to establish the connection to the Community Services multiplexer.

For the HTTP-tunneled connection to succeed, the following must be true:

- The port specified as the "Community port" setting in the Sametime Connect client Sametime Connectivity settings must match a port number specified in one of these settings in the Sametime Administration Tool: the "Port number" field under "Address for client connections" in the Community Services Network settings of the Sametime Administration Tool or the "Port number" field under "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool.

- All networks between the Sametime Connect client and the Sametime server must allow HTTP connections on the port specified as the "Community Port" in the Sametime Connect client.

- The IP address or DNS name specified in the Host setting in the Sametime Connect client Sametime Connectivity settings must correspond to any IP address or DNS name specified in the "Host name" field under "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool. If the Community Services Network-Address for HTTP tunneled client connections-"Host name" field is blank, the entry in the Host setting of the Sametime Connect client can correspond to any IP address or DNS name assigned to the Sametime server.

**Note:** The "Enable Web client to try HTTP tunneling after trying other options" setting must be enabled in the Community Server Network settings on the "Networks and Ports" tab of the Sametime Administration Tool for the connection to occur using the port specified as the "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool.

5. If the HTTP-tunneled connection does not succeed, an error message displays to the user.

**Sametime Connect for browsers - Use my Java Plug-in settings (Sun Microsystems or IBM JVM 1.4.2 only)**

The "Use my Java Plug-in settings" option appears only in the Sametime Connectivity tab of a Sametime Connect for browsers client that loads in a Web browser that operates with the Sun Microsystems JVM 1.4.2 or the IBM JVM 1.4.2.

**Note:** For information about accessing the connectivity settings of the Java Plug-in 1.4.2, see "Notes on the connection process" below.

Sametime Connect for browsers follows this connection process when the "Use my Java Plug-in settings" connectivity option is selected in the Sametime Connectivity tab of the Sametime Connect for browsers client.
1. The Sametime Connect for browsers client examines the values in the "Host" field and the "Port" field (default 1533) of the Sametime Connect client Sametime Connectivity settings.

Sametime Connect for browsers uses the "Host" and "Port" values to determine the Host name and port it should use when attempting a connection to the Sametime server.

**Note** For the most efficient connectivity, the Host field of the Sametime Connect client Sametime Connectivity settings and the "Sametime server" field of a user’s Person document should specify the same Sametime server. For more information, see [Connecting to the Home Sametime server](#).

2. Sametime Connect for browsers attempts a direct Sametime protocol over TCP/IP connection to the Community Services on the port specified as the "Community port" in the Sametime Connectivity settings (default port 1533) of the Sametime Connect client.

The Community Services multiplexer on the Sametime server listens for this connection on the host names and ports specified in the [Community Services Network-Address for client connections-Host name and Port number](#) settings (default port 1533) in the Connectivity settings of the Sametime Administration Tool.

Sametime Connect for browsers attempts a direct TCP/IP connection first regardless of how the connectivity settings are configured in the Java Plug-in Control Panel. The client attempts a direct TCP/IP connection first because this type of connection provides the best performance of all possible connection types. For the TCP/IP connection to succeed, both of the following must be true:

- The host name specified in the Host setting in the Sametime Connect client Sametime Connectivity settings must correspond to any IP address or DNS name specified in the "Host name" field under "Address for client connections" in the Community Services Network settings of the Sametime Administration Tool. If the Community Services Network-Address for client connections-"Host name" field is blank, the entry in the Host setting of the Sametime Connect for browsers client can correspond to any IP address or DNS name assigned to the Sametime server.
- The "Port" setting specified in the Sametime Connect client Sametime Connectivity settings must match one of the ports specified in the Community Services Network-Address for client connections-"Port number" setting on the Sametime server. By default, both of these settings specify port 1533.

This Sametime protocol over a TCP/IP connection can fail if the connection must pass through a proxy server or if the network configuration prevents direct TCP/IP connections on port 1533 (or other port specified in both the Sametime Connectivity settings of the Sametime Connect client and the Community Services Network-Address for client connections- "Port number" setting in the Sametime Administration Tool).

If the Sametime protocol over a TCP/IP connection attempt is not successful, Sametime Connect continues with the connection process as described below.

3. The Sametime Connect for browsers client examines the connectivity settings specified in the Proxies tab of the Java Plug-in Control Panel to establish the connection with the Community Services on the Sametime server. The possible settings in the Proxies tab of the Java Plug-in Control Panel include:

- Use Browser Settings
- HTTP
- Secure
• Socks
• FTP (Not applicable for Sametime)
• Gopher (Not applicable for Sametime)

The connection processes associated with these settings are described below.

Use my browser settings is not selected and no proxies are specified - If the “Use my browser settings” is not selected and no proxy servers are specified in the Java Plug-in connectivity settings, Sametime Connect for browsers attempts a direct HTTP connection to the Community Services on the Sametime server.

Direct HTTP-tunneled connections are used most frequently to enable Sametime Connect clients that operate behind restrictive firewalls without HTTP proxy servers to connect to a Sametime server available to Internet users. This connection process is identical to the connection process that occurs when the “Direct connection using HTTP protocol” option is selected in the Sametime Connectivity tab of the Sametime Connect client. For details on this connection process, see the “Direct connection using HTTP protocol” description in the Basic Sametime Connect client connection process topic earlier in this chapter.

Note: The Sametime Connect for browsers client will also try a direct HTTP-tunneled connection if the client attempts to connect through a proxy server but the connection attempt through the proxy fails. For more information, see "Notes about the connection process" below.

Use my browser settings is selected - When "Use my browser settings" is specified in the Java Plug-in connectivity settings, Sametime Connect for browsers will attempt to use the proxy settings of the Web browser to connect to the Sametime server. In this case, the Sametime Connect client follows the connection process that is described in Sametime Connect for the desktop - Use my Internet Explorer HTTP settings earlier in this chapter.

An HTTP proxy is specified - If the "HTTP" fields in the Proxies tab of the Java Plug-in Control Panel specify an HTTP server address and port, the Sametime Connect for browsers client attempts to connect to the Community Services through the specified HTTP proxy server.

In this scenario, the client encases the standard Sametime protocol connection information within an HTTP request. Sametime Connect for browsers connects to the HTTP proxy, and the HTTP proxy server connects to the Community Services multiplexer on the Sametime server on behalf of the Sametime Connect client.

The HTTP connection from the Sametime Connect client to the HTTP proxy server uses the port specified for the HTTP proxy server in the Proxies tab of the Java Plug-in Control Panel. The HTTP connection from the HTTP proxy server to the Community Services multiplexer occurs on the port (default 1533) specified in the Sametime Connect for browsers client Sametime Connectivity settings.

The Community Services multiplexer on the Sametime server listens for HTTP connections on all ports specified in the "Port number" field under "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool.

For this connection to succeed, the ports specified as the "Port" setting in the Sametime Connect for browsers client must match one of these ports specified in the Sametime Administration Tool:

• The "Port number" field under "Address for client connections" in the Community Services Network settings of the Sametime Administration Tool.
• The "Port number" field under "Address for HTTP tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool.

If the HTTP-tunneled connection attempt through the HTTP proxy server fails, the client attempts a direct HTTP-tunneled connection to the Community Services on the Sametime server. For details on this connection process, see the "Direct connection using HTTP protocol" description in the Basic Sametime Connect client connection process topic earlier in this chapter.

For more information about HTTP tunneling on port 80, see About HTTP tunneling.

A Secure proxy is specified - If the "Secure" fields in the Proxies tab of the Java Plug-in Control panel specify an address and port, the Sametime Connect client attempts to connect to the Community Services through the specified HTTPS proxy server.

In this scenario, the client encases the standard Sametime protocol information within an HTTPS request. Sametime Connect for browsers connects to the HTTPS proxy, and the HTTPS proxy server connects to the Community Services multiplexer on the Sametime server on behalf of the Sametime Connect for browsers client.

The HTTPS connection from the Sametime Connect client to the HTTPS proxy server occurs on the port specified in the Proxies tab of the Java Plug-in. The HTTPS connection from the HTTPS proxy server to the Community Services multiplexer occurs on the port (default 1533) specified in the Sametime Connect for browsers client Sametime Connectivity settings.

The Community Services multiplexer on the Sametime server listens for HTTPS connections on all ports specified in the Community Services Network-Address for HTTPS tunneled client connections-Port number setting in the Configuration-Connectivity options of the Sametime Administration Tool.

For this connection to succeed, the port specified as the "Port" setting in the Sametime Connect for browsers client Sametime Connectivity settings must match the port listed in the "Community Services Network-Address for HTTPS tunneled client connections-Port number" setting.

The "Port" setting in the Sametime Connect for browsers client Sametime Connectivity settings and the Community Services Network-Address for HTTPS tunneled client connections "Port number" setting in the Sametime Administration Tool both specify port 1533 by default.

Many organizations have firewall or network configurations that prevent HTTPS connections on the default port of 1533. For the HTTPS connection to succeed in your network environment, you might need to specify port 443 for HTTPS connections in both of the following settings:

• The "Port" setting of the Sametime Connect for browsers client Sametime Connectivity settings

• The "Port number" field under "Address for HTTPS tunneled client connections" in the Community Services Network settings of the Sametime Administration Tool

If you have configured the Domino HTTP server to listen for HTTPS connections from Web browsers on port 443, the Community Services multiplexer cannot also listen for HTTPS connections on port 443 unless you assign multiple IP addresses to the Sametime server. For more information on this issue, see the “Things you need to know" section of the Sametime 7.0 Release Notes (strn70.nsf or strn70.pdf on the Sametime CD).
If the HTTP-tunneled connection attempt through the HTTPS proxy server fails, the client attempts a direct HTTP-tunneled connection to the Community Services on the Sametime server.

**A Socks proxy is specified** - If the "Socks" fields in the Proxies tab of the Java Plug-in Control panel specify an address and port, the Sametime Connect for browsers client attempts to connect to the Community Services through the SOCKS proxy server at the specified address.

In this scenario, Sametime Connect for browsers connects to the SOCKS proxy, and the proxy server connects to the Community Services on the Sametime server on behalf of the Sametime Connect client. The client uses the "standard Sametime protocol" over TCP/IP for this connection.

The connection from the Sametime Connect for browsers client to the SOCKS proxy server occurs on the port specified in the Proxies tab of the Java Plug-in Control Panel. The connection from the SOCKS proxy server to the Community Services occurs on the "Port" (default 1533) specified in the Sametime Connect for browsers client Sametime Connectivity settings.

For this connection to succeed, the port specified in the "Community port" field of the Sametime Connect client Sametime Connectivity settings must match one of the ports listed in the **Community Services Network-Address for client connections-Port number** setting in the Sametime Administration Tool or one of the ports listed in the **Community Services Network-Address for HTTPS tunneled client connections-Port number** setting in the Sametime Administration Tool.

This connection can fail if it must pass through a firewall or network that blocks the port specified in the "Community port" field of the Sametime Connect client. For more information about connecting through firewalls, see [Extending Sametime to Internet users](#) and [About HTTP tunneling](#).

If the connection attempt through the SOCKS proxy server fails, the client attempts a direct HTTP-tunneled connection to the Community Services on the Sametime server.

**Notes about the connection process:** Note the following about the connection process described above:

- The Java Plug-in connectivity settings used by the client are defined in the Java Plug-in 1.4.2 Control Panel on a user’s machine. The Java Plug-in Control Panel is usually accessed from the Windows Control Panel on the user’s machine.

To view or change the connectivity settings defined in the Java Plug-in Control Panel:

1. Open the Windows Control Panel from the Windows desktop (Start-Settings-Control Panel).
2. Double-click the "Java Plug-in 1.4.2" icon to open the Java Plug-in Control Panel.
3. Select the Proxies tab to view or change the Java Plug-in connectivity settings.

- It is possible to have both the "Use my browser settings" option selected and a proxy server specified in the Java Plug-in connectivity settings. In this case, the Sametime Connect for browsers client will exhaust all possible options to successfully establish a connection. The client will try to connect using the proxy settings of the Web browser and if that fails the client will try to connect using the proxy server (HTTP, Secure, or SOCKS) that is specified in the Java Plug-in connectivity settings.

The order in which these connection attempts occur is determined by internal operations of the client code and is not within the control of the connectivity
design. The client may attempt to connect using the Web browser settings first and then attempt to connect through the proxy defined in the Java Plug-in connectivity options or vice versa.

- The Sametime Connect for browsers client attempts to make a direct HTTP-tunneled connection to the Community Services if a connection attempt through a proxy server fails.
  - If the "Use my browser settings" option is selected and all connection attempts using the proxy settings of the Web browser fail, the client will attempt a direct HTTP-tunneled connection to the Community Services in a final effort to establish a successful connection.
  - If a proxy server is specified in the Java Plug-in connectivity settings and the connection attempt through the proxy server fails, the client will attempt a direct HTTP-tunneled connection to the Community Services in a final effort to establish a successful connection.

For details on direct HTTP-tunneled connections, see the "Direct connection using HTTP protocol" description in the Basic Sametime Connect client connection process topic earlier in this chapter.

- For information about Sametime Connect for browsers client connectivity and reverse proxy servers, see Sametime client connectivity and reverse proxy servers.

### Changing the default connectivity settings of the Sametime Connect for browsers client

Following a Sametime server installation, the Sametime Connect for browsers client will load to a user's web browser with one of the following connectivity settings selected by default in the Options-Preferences-Sametime Connectivity tab of the Sametime Connect client:

- Use my Internet Explorer browser settings - This setting is selected by default if the client loads in a web browser that operates with the Microsoft Virtual Machine (VM).
- Use my Java Plug-in settings - This setting is selected by default if the client loads in a web browser that operates with the Sun or IBM Java Virtual Machine (JVM) 1.4.2.

**Note:** For detailed information about the connectivity process that the Sametime Connect client follows for each connectivity configuration, see Basic Sametime Connect client connection process and Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings earlier in this chapter.

The administrator can alter the default connectivity settings of the Sametime Connect for browsers client. For example, the administrator can alter the connectivity settings so that the Sametime Connect for browsers client is configured by default to connect to the Sametime server through a SOCKS proxy. Performing this configuration ensures that the Sametime Connect for browsers client loads in a user's web browser with connectivity settings that are appropriate for the network environment.

Specifying the default connectivity settings of the Sametime Connect for browsers client prevents end users from having to modify the connectivity settings. Note that an end user can still manually modify the connectivity settings from the administrator-specified defaults if necessary.
**Note:** This capability is also very useful for Sametime Connect for browsers clients that operate in the kiosk mode. Note also that if a user alters the default connectivity settings when the Sametime Connect for browsers client operates in kiosk mode, the new connectivity settings will be valid only for the duration of that instant messaging session. The next time the user starts the client on that machine, the client will load with the administrator-defined default connectivity settings. For more information, see [Enabling Sametime Connect for browsers to function in kiosk mode](#).

### Specifying the default configuration settings of the Sametime Connect for browsers client

To specify the default configuration settings of the Sametime Connect for browsers client, the administrator must add an applet parameter to the HTML code on the Sametime server that loads the Sametime Connect for browsers client.

On a standard Sametime server deployment, the applet code that loads the Sametime Connect for browsers client is located in the Sametime Resources database (STSrc.nsf) on the Sametime server. You can use the Domino Designer client to open the STSrc.nsf database and add the applet parameter to the existing applet code. For instructions, see the following topics:

- [Creating the ConnectivityMethod applet parameter](#)
- [Adding the ConnectivityMethod parameter to the STSrc.nsf database](#)

If you have deployed a customized user interface to launch the Sametime Connect for browsers client, a complete example of the applet code required to launch the client with a specific default connectivity configuration is provided in the [Example of custom HTML code required to launch the Sametime Connect for browsers client](#) topic.

**Note:** To accommodate the kiosk mode, some organizations may choose to create a custom user interface to launch the Sametime Connect for browsers client. For more information, see [Enabling Sametime Connect for browsers to function in kiosk mode](#).

### Creating the ConnectivityMethod applet parameter

To specify the connectivity setting that is selected by default when the Sametime Connect for browsers client loads in a user’s Web browser, the administrator must add a new ConnectivityMethod applet parameter to the HTML code that loads the Sametime Connect client.

One example of this applet parameter is provided below:

```html
<PARAM NAME="ConnectivityMethod" VALUE="directST://sametime.ibm.com:1533">
```

This example applet parameter instructs the Sametime Connect for browsers client to attempt a "Direct connection using standard Sametime protocol" to the Sametime server named sametime.ibm.com on port 1533 by default when the client loads to the user’s web browser.

The ConnectivityMethod applet parameter can be constructed to enable the Sametime Connect client to attempt any supported connection type by default. The syntax of the ConnectivityMethod applet parameter is discussed below. Specific examples of the ConnectivityMethod applet parameters required to support the different connection types are also included.
Syntax of the ConnectivityMethod applet parameter

The complete syntax of the ConnectivityMethod applet parameter is shown below.

```xml
<PARAM NAME="ConnectivityMethod" VALUE=methodName://serverName:port/proxyType=type&proxyName=name&proxyPort=port&proxyAuthUser=username&proxyAuthPwd=password>
```

When constructing the ConnectivityMethod applet parameter, note that applet parameter will always begin with this text string:

```
<PARAM NAME="ConnectivityMethod"
```

The `VALUE=` component of the text string determines which connectivity option the client tries by default. The syntax of the `VALUE=` component is shown below. Note that the values of this component are shown in **bold**:

```
VALUE=methodName://serverName:port/proxyType=type&proxyName=name&proxyPort=port
```

Each of the variable values in this parameter string is discussed below.

- **methodName** - The `methodName` variable can have any of these values:
  - **DirectST** - This value indicates the client will default to the "Direct connection using standard Sametime protocol" connection type.
  - **DirectHTTP** - This value indicates the client will default to the "Direct connection using HTTP protocol" connection type.
  - **IESettings** - This value indicates the client will default to the "Use my Internet Explorer browser settings" connection type.
  - **Proxy** - This value indicates the client will default to one of the "Use proxy" connection types. The specific proxy type is determined by subsequent values in the parameter string as discussed below.

  **Note:** For detailed information on each of these connection types, see [Basic Sametime Connect client connection process](#) and [Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings](#) earlier in this chapter.

- **servername:port** - The `servername:port` variable specifies the name of the Sametime server to which the Sametime Connect client connects and the port to use for the connection. If the Sametime server name is `sametime.ibm.com`, some sample values include:
  - `sametime.ibm.com:1533`
  - `sametime.ibm.com:8082`

  The port specified must correspond to the port on which the Sametime server listens for each specific connection type (as determined by the `methodName` variable). For detailed information on the default ports used for each of the connection types, see [Basic Sametime Connect client connection process](#) and [Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings](#) earlier in this chapter.

- **type** - The `type` variable specifies a specific proxy type and is valid only when "proxy" is used as the `methodName`. The `type` variable can have any of these values:
  - **HTTP**
  - **HTTPS**
  - **SOCKS4**
  - **SOCKS5**
• **name** - The name variable specifies the DNS name of the proxy server and is valid only when "proxy" is used as the methodName. An example value is HTTPproxy.ibm.com.

• **port** - The port variable specifies the port on which the proxy server listens for connections and is valid only when "proxy" is used as the methodName. The value depends on the configuration of the proxy server.

• **username** - The username variable specifies the user name required to authenticate with the proxy server. This variable is required only when "proxy" is used as the methodName and the proxy server requires authentication.

• **password** - The password variable specifies the password associated with the username required to authenticate with the proxy server. This variable is required only when "proxy" is used as the methodName and the proxy server requires authentication.

**Complete examples of the ConnectivityMethod applet parameter**

Listed below are some complete examples of the ConnectivityMethod applet parameter that is used to specify a default connectivity configuration for the Sametime Connect for browsers client. In each of these examples the Sametime server to which the client must connect is named "sametime.ibm.com."

The applet parameter below enables the Sametime Connect for browsers client to make a direct HTTP connection to a Sametime server on port 8082:

```xml
<PARAM NAME="ConnectivityMethod" VALUE="directHTTP://sametime.ibm.com:8082"/>
```

The applet parameter below enables the Sametime Connect for browsers client to make a connection to a Sametime server on port 8082 using the connectivity settings specified in an Internet Explorer web browser:

```xml
<PARAM NAME="ConnectivityMethod" VALUE="IESettings://sametime.ibm.com:8082"/>
```

The applet parameter below enables the Sametime Connect for browsers client to make a connection to a Sametime server through an HTTP proxy server named "HTTPproxy.ibm.com." The HTTP proxy server listens for connections on port 8080 and requires authentication. The user name required to authenticate with the proxy is "Dawn_Ortiz" and the password associated with this user name is "sametime."

```xml
```

The applet parameter below enables the Sametime Connect for browsers client to make a connection to a Sametime server through SOCKS4 proxy server named "SOCKS4proxy.ibm.com." The SOCKS proxy server listens for connections on port 8080 and does not require authentication.

```xml
<PARAM NAME="ConnectivityMethod" VALUE="proxy://sametime.ibm.com:8082/proxyType=SOCKS4&proxyName=SOCKS4proxy.ibm.com&proxyPort=8080">
```

The applet parameter below enables the Sametime Connect for browsers client to make a connection to a Sametime server through SOCKS5 proxy server named "SOCKS5.ibm.com." The SOCKS proxy server listens for connections on port 8080 and requires authentication. The user name required to authenticate with the proxy is "Dawn_Ortiz" and the password associated with this user name is "sametime."

```xml
```
Adding the ConnectivityMethod parameter to the STSrc.nsf database

To specify the default connectivity setting for the Sametime Connect for browsers client, you must add the appropriate ConnectivityMethod applet parameter to the HTML code on the Sametime server.

In a standard Sametime server deployment, this applet code exists in two subforms of the Sametime Resources (STSrc.nsf) database on the Sametime server. To ensure the default connectivity settings go into effect for all browser types, you must add the ConnectivityMethod applet parameter to the HTML code in each of these two subforms.

- **WebConnect-IE** (This subform applies to the Microsoft Internet Explorer browsers.)
- **WebConnect-Moz** (This subform applies to Mozilla browsers.)

**Note:** A WebConnect-N4 subform may appear in the STSrc.nsf database, but this subform applies to the Netscape 4 browsers and is not used with Sametime 7.0.

To add the applet parameter to the HTML code in these subforms:

1. Use the Domino Designer client to open the STSrc.nsf database on the Sametime server.
2. In Domino Designer expand the "Recent Databases" icon and ensure that the STSrc.nsf database is selected.
3. Expand "Resources" and click "Subforms."
4. In the Subforms list, double-click on the WebConnect-IE subform.
5. In the work pane at the top of the Domino Designer client, scroll down until you see the HTML code containing the applet parameters.
   **Note** An applet parameter begins with the text string `<paramname=...`.
6. Add the applet parameter to the list of parameters.
   **Note** Use the information provided in "Creating the ConnectivityMethod applet parameter" above to determine the correct syntax for the applet parameter.
7. Save the subform.
8. Repeat steps 4 through 7 for the WebConnect-Moz subform.

Example of custom HTML code required to launch the Sametime Connect for browsers client

Some organizations may choose to create a custom user interface to launch the Sametime Connect for browsers client. The example below illustrates the applet code that might be used in a custom HTML page or Domino application to launch the Sametime Connect for browsers client with a specific default connectivity configuration. If you create a custom interface for this purpose, ensure the code includes all necessary parameters as shown below:

```html
<APPLET>
code=com.lotus.sametime.connectapplet.ConnectApplet.class
height=100% name=ConnectApplet
style="BACKGROUND-COLOR: gray; LEFT: 0px; TOP: 0px" width=100% MAYSCRIPT=TRUE>
<PARAM NAME="cabinets" VALUE="connect.cab">
<PARAM NAME="SametimeServer" VALUE=""/>
<PARAM NAME="SametimePort" VALUE=""/>
</APPLET>
```
Meeting Room and Broadcast client connection processes

This section discusses the connection processes of the Sametime Meeting Room and Broadcast clients. Read this section to gain a better understanding of how the Meeting Room and Broadcast clients connect to the server and how the "Networks and Ports" settings in the Sametime Administration Tool are used in these connection processes.

This section discusses the connection processes of both the Sametime Meeting Room and Broadcast clients. The Sametime Meeting Room client can connect to Community Services, Meeting Services, and Audio/Video Services.

The Sametime Broadcast client connects to the Meeting Services for call control purposes and receives streamed meeting data from the Broadcast Services.

Both the Meeting Room client and the Broadcast client can connect to the Sametime server:

- Using either direct TCP/IP connections or HTTP-tunneled connections
- Through an HTTP proxy server, a SOCKS proxy server, or a reverse HTTP proxy server.

Sametime is designed to enable Sametime Meeting Room and Broadcast clients that operate behind restrictive firewalls to connect to the Sametime services using HTTP over port 80. For detailed information on this capability, see the connection process topics below for the individual clients and the About HTTP tunneling.

For detailed information about these client connection processes, see Meeting Room and Broadcast client connection processes using the Sun or IBM JVM 1.4.2.

Meeting Room and Broadcast client connection processes using the Sun or IBM JVM 1.4.2

This section discusses the client connection processes and issues associated with Sametime Meeting Room or Broadcast clients that run in a Web browser that operates with the Sun or IBM Java Virtual Machine 1.4.2 and Java Plug-in 1.4.2.

When operating with the Sun or IBM JVM 1.4.2, the Meeting Room and Broadcast clients are unable to detect proxy connectivity settings that are configured in the user’s Web browser and cannot use the proxy connectivity settings specified in the Web browser to establish connections with the Sametime server.

The Meeting Room and Broadcast clients are able to detect proxy connectivity settings that are configured in the Java Plug-in 1.4.2 Control Panel on each user’s machine, and can use these proxy connectivity settings to establish connections with the Sametime server.
Because the Meeting Room and Broadcast clients use the Java Plug-in Control Panel settings, it may be necessary for the administrator to ensure that each user’s machine has these settings configured appropriately for the network environment in which the client operates.

This section includes the following topics related to the Meeting Room and Broadcast client connection processes when running in a Web browser that operates with the Sun or IBM JVM 1.4.2:

- Accessing proxy connectivity settings in the Java Plug-in Control Panel
- Suggested Java Plug-in configurations for specific network environments
- Meeting Room client connection process using JVM 1.4.2 (Community Services and Meeting Services)
- Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)
- Broadcast client connection process using JVM 1.4.2

**Accessing proxy connectivity settings in the Java Plug-in Control Panel**

When the Sun Microsystems or IBM JVM 1.4.2 is installed on a user’s machine, the Java Plug-in 1.4.2 Control Panel is accessible from the Windows Control Panel on the user’s machine. The proxy connectivity settings are defined in the Proxies tab of the Java Plug-in 1.4.2 Control Panel.

Use the following instructions to view or change the connectivity settings defined in the Java Plug-in on the user’s machine:

1. Open the Control Panel from the Windows desktop (Start-Settings-Control Panel).
2. Double-click the "Java Plug-in 1.4.2" icon to open the Java Plug-in Control Panel.
3. Select the Proxies tab to view or change the Java Plug-in connectivity settings.

   **Note** The possible settings in the Proxies tab of the Java Plug-in Control Panel include:
   - Use my browser settings
   - HTTP
   - Secure (Not applicable for the Meeting Room and Broadcast client)
   - Socks
   - FTP (Not applicable to any Sametime clients)
   - Gopher (Not applicable to any Sametime clients)

**Suggested Java Plug-in configurations for specific network environments**

The Sametime Meeting Room and Broadcast clients cannot access proxy connectivity settings specified in a Web browser when running in a Web browser that operates with the Sun or IBM JVM 1.4.2. The Meeting Room and Broadcast clients can access the proxy connectivity settings specified in the Java Plug-in 1.4.2 Control Panel and use these settings to establish a connection with the Sametime server.

Because of this limitation, IBM Lotus software recommends the following configurations to ensure the Sametime Meeting Room and Broadcast clients can connect to the Sametime server directly or connect to the Sametime server through an HTTP or SOCKS proxy server. For information about connectivity issues that
occur when connecting to a Sametime server deployed behind a reverse proxy server, see Using reverse proxy or portal servers with the Sametime server.

**Note:** If you are already familiar with Sametime client connection processes, the section below provides a summary of the connectivity behavior that occurs when the Proxies tab of the Java Plug-in Control Panel is configured in a particular way. If you are not familiar with the Sametime client connection processes, see either Meeting Room client connection process using JVM 1.4.2 (Community Services and Meeting Services), Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services), or Broadcast client connection process using JVM 1.4.2 later in this chapter.

- **No proxies exist between the client and the Sametime server** - If a Sametime client can make a direct connection to the Sametime server, make the following settings in the Proxies tab of the Java Plug-in Control Panel:
  1. Make sure that no proxy servers are specified in the Proxies tab. (The address and port fields for each type of proxy server must be blank in the Proxies tab.)
  2. The "Use my browser settings" option in the Proxies tab can be selected or not selected. The Sametime clients cannot access proxy settings in the user's Web browser when operating with the Sun or IBM JVM 1.4.2 so it does not matter if the "Use my browser settings" is selected or not selected. Even if the "Use my browser settings" option is selected, the Sametime clients will not use the browser settings to establish connections with a Sametime server.

When configured in the manner shown above, the client behaves as follows:
- The client attempts a direct TCP/IP connection to the Sametime server.
- If the direct TCP/IP connection fails, the client attempts a direct HTTP-tunneled connection to the Sametime server.

**Note:** The term "direct" connection means that the client can connect directly to the Sametime server. In this case, the network environment must not require connections to occur through an HTTP or SOCKS proxy server.

- **The client must connect to the Sametime server through an HTTP proxy server** - If a Sametime client must connect to an HTTP proxy server to establish a connection with the Sametime server, make the following settings in the Proxies tab of the Java Plug-in Control Panel:
  - Clear the check mark from the "Use my browser settings" option
  - Specify the address of the HTTP proxy server and the port required to connect to the HTTP proxy server.

When configured in the manner shown above, the client behaves as follows:
- The client attempts a direct TCP/IP connection to the Sametime server.
- If the direct TCP/IP connection fails, the client attempts an HTTP-tunneled connection to the Sametime server through the HTTP proxy server.

- **The client must connect to the Sametime server through a SOCKS proxy server** - If a Sametime client must connect to SOCKS proxy server to establish a connection with the Sametime server, make the following settings in the Proxies tab of the Java Plug-in Control Panel:
  - Clear the check mark from the "Use my browser settings" option
  - Specify the address of the SOCKS proxy server and the port required to connect to the SOCKS proxy server.

When configured in the manner shown above, the client behaves as follows:
- The client attempts a direct TCP/IP connection to the Sametime server.
– If the direct TCP/IP connection fails, the client attempts a TCP/IP connection through the SOCKS proxy server.
– If the TCP/IP connection through the SOCKS proxy fails, the client attempts an HTTP-tunneled connection to the Sametime server through the SOCKS proxy server.

**Meeting Room client connection process using JVM 1.4.2 (Community Services and Meeting Services)**

This topic describes the connection process the Meeting Room client uses to connect to the Community Services and Meeting Services when the Meeting Room client runs in a Web browser that operates with the Sun or IBM JVM 1.4.2.

**Note:** For information about connecting to meetings that include interactive audio/video, see [Audio/Video Services](#). For information about connecting to broadcast meetings, see [Broadcast client connection process using JVM 1.4.2](#).

The Sametime Meeting Room client is a signed Java applet that is loaded in a user’s Web browser when a user attends an instant or scheduled meeting. The user is prompted to accept the Meeting Room client applet when it is loaded in the Web browser.

The Meeting Room client contains several Java components. During a meeting, different Java components contained within the Sametime Meeting Room client might require connections to the Community Services and Meeting Services on the Sametime server.

The Meeting Room Java components that require connections to the Sametime Community Services and Meeting Services include:

- Participant List and Chat - These Meeting Room client components require a connection to the Community Services.
- Screen sharing, whiteboard, send Web page, and question and answer polls - These Meeting Room components require a connection to the Meeting Services.

The steps below describe the connection process the Meeting Room client uses to connect to the Community Services and Meeting Services when the Meeting Room client runs in a Web browser that operates with the Sun or IBM JVM 1.4.2.

1. The Sametime Meeting Room client loads in the user’s Web browser when the user attends an instant or scheduled Sametime meeting.
   The host names and port numbers on which the Community Services and Meeting Services are listening for connections are passed from the server to the Meeting Room client. (These host names and port numbers are specified in the Configuration-Connectivity-“Networks and Ports” tab of the Sametime Administration Tool.)

2. Regardless of how the connectivity settings are configured in the Proxies tab of the Java Plug-in Control Panel, the Sametime Meeting Room client first attempts to make separate direct TCP/IP connections to the Community Services and Meeting Services on the Sametime server.
   **Note** For the “direct TCP/IP connections,” the Meeting Room client uses unique Sametime protocols over TCP/IP to connect to the Community Services and Meeting Services; these connections do not occur through a proxy server. Direct TCP/IP connections result in optimum meeting performance. For this reason, the client always attempts direct TCP/IP connections first before resorting to other connectivity options.
• The Meeting Room client attempts the direct TCP/IP connection to the Community Services multiplexer using the host names and ports (default port 1533) specified in the Connections-Host name and Port number settings of the Sametime Administration Tool.

• The Meeting Room client attempts the direct TCP/IP connection to the Meeting Services using the Host names and ports (default 8081) specified in the Meeting Services Network-Address for client connections-Host name and Port number settings of the Sametime Administration Tool.

These direct TCP/IP connections can fail if the connections must occur through a proxy server or if any network between the client and server prevents TCP/IP connections on the ports described above (default ports 1533 and 8081).

3. If the direct TCP/IP connection attempts described in step 2 fail, the configuration of the settings in the Proxies tab of the Java Plug-in Control Panel determines how the connections to the Sametime server are established. The possible configurations are discussed below.

An HTTP proxy server is specified in the Proxies tab of the Java Plug-in Control Panel

If the Meeting Room client must connect to the Sametime server through an HTTP proxy server, you should disable the “Use my browser settings” option in the Java Plug-in Control Panel and enter the HTTP proxy server address and port in the Proxies tab of the Java Plug-in Control Panel.

When configured in this way, the Sametime Meeting Room client encases the Sametime connectivity protocol data in HTTP requests and sends these requests to the HTTP proxy server. (This capability is referred to as HTTP-tunneling.) The HTTP proxy server forwards these requests to the Sametime server on behalf of the clients. The client will attempt to establish and maintain an HTTP-tunneled connection to the Sametime services.

Refer to step 4 in this procedure for a more detailed description of how these HTTP-tunneled connections are handled by the Sametime server.

A SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel

If the Meeting Room client must connect to the Sametime server through a SOCKS proxy server, you should disable the “Use my browser settings” option in the Java Plug-in Control Panel and enter the SOCKS proxy server address and port in the Proxies tab of the Java Plug-in Control Panel.

If a SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel, the Sametime Meeting Room client will make the following connection attempts:

a. The Sametime Meeting Room client attempts to make separate TCP/IP connections to the Community Services and Meeting Services on the Sametime server through the SOCKS proxy server.

The connections through a SOCKS proxy server use the same protocols (unique Sametime protocols over TCP/IP) that were used in the direct TCP/IP connection attempt discussed in step 2 above. The same host names and ports (1533 and 8081) defined in the Sametime Administration Tool are also used for these connection attempts.

The connections through the SOCKS proxy server can fail if the connections must occur through an HTTP proxy server or any network between the client and server prevents TCP/IP connections on the ports described above (default ports 1533 and 8081).
Note The default ports are configurable from the "Networks and Ports" tab of the Sametime Administration Tool.

b. If the connection attempts using the standard Sametime protocols over TCP/IP through the SOCKS proxy are not successful, the Meeting Room client attempts to make HTTP-tunneled connections to the Community Services and Meeting Services through the SOCKS proxy server. In this case, the Meeting Room client encases the Sametime Connectivity protocol data in HTTP requests and sends these requests to the SOCKS proxy. The SOCKS proxy server sends these HTTP-tunneled requests to the Sametime server on behalf of the Meeting Room client. The client will then attempt to establish and maintain an HTTP-tunneled connection to the Sametime services through the SOCKS proxy server.

Refer to step 4 in this procedure for a more detailed description of how these HTTP-tunneled connections are handled by the Sametime server.

No proxies are specified the Proxies tab
If no proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel, the Sametime Meeting Room client can establish direct HTTP-tunneled connections with the Community Services and the Meeting Services on the Sametime server.

Direct HTTP-tunneled connections occur directly from the Meeting Room client to the services on the Sametime server and are not established through a proxy server.

Refer to step 4 in this procedure for a more detailed description of how these HTTP-tunneled connections are handled by the Sametime server.

Notes about this connectivity configuration:
• No proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel if the address and port fields associated with the proxy server fields of the Proxies tab are blank.
• The Java Plug-in Control Panel includes a "Use my browser settings" option. This setting has no affect on this connection process. If no proxy servers are specified in the Proxies tab, the client attempts to establish direct HTTP-tunneled connections with the Community Services and the Meeting Services regardless of whether the "Use my browser settings" option is on or not selected. A Sametime client cannot access the proxy settings specified in the Web browser when operating with the Sun or IBM JVM 1.4.2.
• Direct HTTP-tunneled connections may be useful if a Sametime client must make a connection to a Sametime server through a client-side firewall that allows outbound HTTP traffic, but the firewall does not include an HTTP proxy server.

4. As noted in the previous steps, the client will eventually resort to HTTP-tunneling to establish connections with the Community Services and Meeting Services if other connections attempts fail or are not possible.

This step discusses the way in which HTTP-tunneled connections are established with the Sametime server.

The HTTP tunneling capabilities work differently depending on whether the administrator allows or does not allow HTTP tunneling on port 80. The administrator has the option of allowing or not allowing HTTP tunneling on port 80 during the server installation.

If HTTP tunneling on port 80 is allowed - If HTTP tunneling on port 80 is allowed during the Sametime server installation, the Meeting Room client sends the HTTP requests containing Community Services and Meeting Services connection data to the Sametime Community Services multiplexer.
The "Host name" and "Port number" settings (default port 80) specified in the "Community Server Network Address for HTTP-tunneled client connections" settings of the Sametime Administration Tool are used to establish the connections to the Community Services multiplexer.

The Community Services multiplexer can differentiate between the HTTP requests intended for the Community Services and the Meeting Services by examining code that is appended to each URL by Sametime clients. Upon receiving these requests, the Community Services multiplexer:

- Creates an intraserver connection to other Community Services components and sends the Community Services data to the Community Services.
- Creates an intraserver connection to the Meeting Services and sends the Meeting Services data to the Meeting Services.

The ability of the Community Services multiplexer to receive both Community Services and Meeting Services requests on a single port (port 80) enables the Sametime server to support HTTP tunneling over port 80 even if the Sametime server machine uses only a single IP address. This connectivity capability is sometimes referred to as "single-port mode."

**If HTTP tunneling on port 80 is not allowed** - If the administrator does not allow HTTP tunneling on port 80 during the Sametime server installation, the Meeting Room client attempts to establish an HTTP-tunneled connection to the Community Services and a separate HTTP-tunneled connection to the Meeting Services.

The Meeting Room client attempts an HTTP-tunneled connection to the Community Services using the "Host name" and "Port number" settings (default port 1533) specified in the "Community Server Network Address for HTTP-tunneled client connections" settings.

The Meeting Room client attempts a separate HTTP-tunneled connection to the Meeting Services using the "Host name" and "Port number" settings (default port 8081) specified in the "Meeting Server Network-Address for HTTP-tunneled client connections" settings.

If the Meeting Room client is successful in establishing connections with the Community Services and Meeting Services using either a single port (port 80) or two separate ports (1533 and 8081), the Meeting Room client and Sametime server maintain either a persistent or polled HTTP-tunneled connection as noted below.

**Maintaining a persistent HTTP-tunneled connection** - When establishing a connection using HTTP-tunneling, the Meeting Room client first attempts to maintain a persistent HTTP-tunneled connection. (The persistent HTTP-tunneled connection is sometimes called "hybrid polling" or "master/slave HTTP tunneling.")

With this connection, data trickles continuously between the client and the Sametime server. This persistent connection provides the client with an event-driven, real-time connection to the server.

**Note** The persistent HTTP-tunneled connection provides better performance and uses fewer system and network resources than the polled HTTP-tunneled connections described below.

A persistent HTTP-tunneled connection might fail in the following circumstances:

- The client connects to the Sametime server through a proxy that buffers or caches data.
- Multiple Java applets running within a single instance of the Web browser attempt to create additional connections, and exceed the connection limits.
imposed by the Web browser. Web browsers limit the number of HTTP connections the browser can make to a single server.

- The client is unable to access the Web browser connectivity settings or authenticate with an HTTP proxy.

**Maintaining a polled HTTP tunneled connection** - If a persistent HTTP connection fails or is not possible, the client uses a continuous polling functionality to maintain the HTTP-tunneled connections.

In this type of tunneling, the client and server enter a mode in which the client continuously makes and breaks HTTP connections to post data to and receive data from the server.

The polling functionality overcomes most of the limitations that cause persistent HTTP-tunneled connections to fail.

The polling functionality enables the Sametime Meeting Room client to maintain connections in almost any network environment as long as the client can connect to the server using HTTP. The polling functionality can increase network traffic. Polling might also affect the scalability of the server as more system resources are required to continuously make and break the connections. The polling activity might be noticeable to the end user but should not prevent the user from interacting in the meeting or viewing meeting presentations.

**Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)**

The interactive audio/video components of the Sametime Meeting Room client must communicate with the Audio/Video Services on the Sametime server to receive and transmit audio and video streams. This topic describes the connection process the Meeting Room client uses to connect to the Audio/Video Services when the Meeting Room client runs in a Web browser that operates with the Sun or IBM JVM 1.4.2.

To interact in an audio/video meeting, the interactive audio/video components of the Sametime Meeting Room client and the Sametime server engage in a connection process. This connection process is discussed in two parts:

- **Call-control connection** - First, the Meeting Room client makes a TCP/IP control connection to the Audio/Video Services on the Sametime server. The interactive audio/video components of the Meeting Room client exchange call setup and control data with the Audio/Video Services over this connection.

- **Transmitting Audio/Video streams** - If the call control connection is successful, the audio/video streams are transmitted between the server and client using either unicast UDP or TCP tunneling.

**Note:** The call-control connection is a connection from the Sametime Meeting Room client to the Meeting Services. This is the same Meeting Services connection that is described in [Meeting Room client connection process using JVM 1.4.2 (Community Services and Meeting Services)]. Sametime uses the Meeting Services connection that supports the Meeting Services functionality to transmit audio/video call-control information.

**Call-control connection:** The process for the call control connection for the Meeting Room audio/video components occurs as follows:

1. The Meeting Room client loads in a Web browser when a user attends a meeting. The interactive audio and video Java applets are components of the Sametime Meeting Room client.

The host names and ports on which the Sametime server listens for connections from clients are passed from the server to the client. These host names and port
numbers are specified in the Configuration-Connectivity-Networks and Ports tab of the Sametime Administration Tool.

2. Regardless of how the connectivity settings are configured in the Proxies tab of the Java Plug-in Control Panel, the Sametime Meeting Room client first attempts a direct TCP/IP connection to the Meeting Services using the host name and port (default 8081) specified in the Meeting Services Network-Address for client connections-"Host name" and "Port number settings of the Sametime Administration Tool.

If this direct TCP/IP connection is successful, the connection to the Meeting Services is used for the exchange of call setup and control information between the Meeting Room client and the Audio/Video Services on the Sametime server. The audio and video streams are transmitted between the server and the client as described in "Transmitting audio and video streams" below.

If the direct TCP/IP connection attempt is not successful, the Meeting Room client continues with the connection process as documented in step 3.

3. Audio/video connectivity can only be successful if the call control connection occurs in one of these ways:
   • Using a direct TCP/IP connection (as described in step 2 above).
   • Using a TCP/IP connection or an HTTP tunneled connection that occurs through a SOCKS proxy server
   • Using a direct HTTP-tunneled connection

   **Note:** The call control connection cannot occur through an HTTP proxy server. Interactive audio and video streams cannot be transmitted between the client and server if the call control connection occurs through an HTTP proxy server.

If the direct TCP/IP connection attempt described in step 2 fails, the configuration settings in the Proxies tab of the Java Plug-in Control Panel determine how the connection process proceeds. To enable a call control connection to be successfully established for the purpose of transmitting audio and video streams, the Java Plug-in Control Panel must be configured in one of these two ways:
   • A SOCKS proxy server is specified
   • No proxies are specified

   Each of these possibilities is discussed below:

   **A SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel**

   If the Meeting Room client must connect to the Sametime server through a SOCKS proxy server, you should disable the "Use my browser settings" option in the Java Plug-in Control Panel and enter the SOCKS proxy server address and port in the Proxies tab of the Java Plug-in Control Panel.

   If a SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel, the Sametime Meeting Room client will make the following connection attempts:

   **a.** The Sametime Meeting Room client attempts to make a TCP/IP connection to the Meeting Services on the Sametime server through the SOCKS proxy server.

   The connection through the SOCKS proxy server uses the same protocol (unique Sametime protocol over TCP/IP) that was used in the direct TCP/IP connection attempt discussed in step 2 above. The same host name and port (default 8081) defined in the Sametime Administration Tool are also used for this connection attempt.
If the TCP/IP connection through the SOCKS proxy is successful, the connection to the Meeting Services is used for the exchange of call setup and control information between the Meeting Room client and the Audio/Video Services on the Sametime server. The audio and video streams are transmitted between the server and the client as described in “Transmitting audio and video streams” below.

The connections through the SOCKS proxy server can fail if the connections must occur through an HTTP proxy server or any network between the client and server prevents TCP/IP connections on the ports described above (8081).

**Note** The default ports are configurable from the "Networks and Ports" tab of the Sametime Administration Tool.

b. If the connection attempt using the standard Sametime protocol over TCP/IP through the SOCKS proxy is not successful, the Meeting Room client attempts to make an HTTP-tunneled connection to the Meeting Services through the SOCKS proxy server.

In this case, the Meeting Room client encases the Sametime Connectivity protocol data in an HTTP request and sends this request to the SOCKS proxy. The SOCKS proxy server sends this HTTP-tunneled request to the Sametime server on behalf of the Meeting Room client.

The client will attempt this connection to the Sametime server using the port specified as the Community Services Network-Address for HTTP-tunneled client connections-Port number (default 1533) in the Sametime Administration Tool.

Although this HTTP-tunneled connection occurs by default on port 1533, it is likely the administrator will need to enable the Sametime server to support HTTP-tunneling on port 80 to enable the audio/video connectivity to succeed.

There are several important issues pertaining to audio/video connectivity when the call control connection is established using HTTP tunneling. To maintain clarity in this discussion, these issues are discussed in step 4 below.

**No proxies are specified the Proxies tab**

If no proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel, the Sametime Meeting Room client can establish direct HTTP-tunneled connections with the Meeting Services on the Sametime server.

A direct HTTP-tunneled connection is a connection that occurs directly from the Meeting Room client to the Meeting Services on the Sametime server and does not pass through a proxy server.

The client will attempt this connection to the Sametime server using the ports specified in the Community Services Network-Address for HTTP-tunneled client connections-Port number setting (default 1533) in the Networks and Ports tab of the Sametime Administration Tool.

**Notes on this connectivity configuration:**

- No proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel if the address and port fields associated with the proxy servers are blank.

- The Java Plug-in Control Panel includes a "Use my browser settings" option. This setting has no affect on this connection process. If no proxy servers are specified in the Proxies tab, the client attempts to establish direct HTTP-tunneled connections with the Community Services and the Meeting Services regardless of whether the "Use my browser settings” option is or is
not selected. A Sametime client cannot access the proxy settings specified in
the Web browser when operating with the Sun JVM 1.4.2.

• Direct HTTP-tunneled connections may be useful if a Sametime client must
make a connection to a Sametime server through a client-side firewall that
allows outbound HTTP traffic, but the firewall does not include an HTTP
proxy server.

Although this HTTP-tunneled connection occurs by default on port 1533, it is
likely the administrator will need to enable the Sametime server to support
HTTP-tunneling on port 80 to enable the audio/video connectivity to
succeed.

There are several important issues pertaining to audio/video connectivity
when the call control connection is established using HTTP tunneling. To
maintain clarity in this discussion, these issues are discussed in step 4 below.

4. The information in step 4 is not relevant if a Sametime Meeting Room client
establishes a call control connection with the Sametime server using a direct
TCP/IP connection or a TCP/IP connection through a SOCKS proxy.

However, if the Meeting Room client establishes a call control connection using
a direct HTTP-tunneled connection or an HTTP-tunneled connection the
administrator should review the information provided in this step to
understand the issues associated with establishing audio/video call control
connections using HTTP tunneling.

Interactive audio/video streams can be successfully transmitted when the call
control connection is established using HTTP-tunneling only if the Sametime
server is also configured to support TCP-tunneling of the interactive
audio/video streams on a port that is open through all networks between the
client and server.

The most common configuration for this connectivity is as follows:

• The Sametime server is configured to support HTTP tunneling over port 80
for connections to the Community Services, Meeting Services, and Broadcast
Services. The administrator can specify this configuration during the
Sametime server installation. The administrator also has the option of
enabling HTTP tunneling over port 80 using multiple IP addresses. For more
information about configuring a Sametime server to support HTTP-tunneling
over port 80, see [About HTTP tunneling](#).

• If the Sametime server is configured to support HTTP tunneling over port 80,
the administrator can also configure the Sametime server to support
TCP-tunneling of interactive audio/video streams on port 80. When
configured in this way all Sametime meeting data, including interactive
audio/video streams, can be transmitted using port 80. To configure the
Sametime server to support TCP tunneling of audio/video streams, see [TCP
[4] tunneling of interactive audio/video streams on port 80](#).

Although port 80 is the port most likely port to use for both the
HTTP-tunneled call control connection and the TCP tunneling of the audio and
video streams, you can configure this connectivity to occur on a different port.
To do this, you must configure the Sametime server to support HTTP tunneling
on a port other than port 80. For instructions, see [Changing the
HTTP-tunneling port](#). Next, you must configure the TCP tunneling of
audio/video streams to occur on the same port as the HTTP-tunneled
connection. For instructions, see [TCP tunneling of interactive audio/video
streams on port 80](#).

Although these are the most common configurations, practically any
configuration is possible using the Networks and Ports tab of the Sametime
Administration Tool. For example, it is possible for the HTTP-tunneled call
control connection to occur on port 1533 (or any other port) while the TCP tunneling of the audio/video streams occurs on port 80 (or any other port). The administrator must determine the appropriate configuration for the network environment.

Note also that the call control connection must be established using a direct HTTP-tunneled connection between the client and the server, or an HTTP-tunneled connection through a SOCKS proxy server. Interactive audio and video is not supported if the client connects to the Sametime server through an HTTP proxy server. It is not possible to use TCP tunneling to transmit audio/video streams through an HTTP proxy server.

**Transmitting audio and video streams:** The manner in which audio and video streams are transmitted depend on how the call control connection was established:

- If the Meeting Room client direct TCP/IP connection described in Step 2 above is successful, the Audio/Video Services dynamically select the UDP ports on which to receive audio and video streams from the clients. These dynamic UDP ports are selected from the range of ports the administrator specifies in the "Interactive Audio/Video Network - Multimedia Processor (MMP) UDP port numbers start/end at" settings in the Sametime Administration Tool "Networks and Ports" settings. If any network between the client and the server blocks UDP traffic, the audio and video streams can be tunneled over a single TCP/IP port.

The administrator can specify the TCP port over which the streams will be tunneled in the "Interactive Audio/Video Network-TCP tunneling port" (default 8084) setting in the Sametime Administration Tool. The port specified as the "TCP tunneling port" must be open through all firewalls between the client and the server for the client to transmit and receive TCP-tunneled audio and video streams.

- If the Meeting Room client TCP/IP connection occurs through a SOCKS proxy server (as discussed in Step 3 above), the audio and video streams cannot be transmitted through the SOCKS server using UDP. The client and server transmit the audio and video streams through the SOCKS proxy server using TCP over the "TCP tunneling port" (port 8084) as described above. The TCP Tunneling option must be enabled on the "Networks and Ports" tab of the Sametime Administration Tool, and the "TCP tunneling port" must be open through all networks between the client and the server for the transmission through the SOCKS proxy to succeed.

If necessary, the administrator can change the default TCP Tunneling port from 8084 to an administrator-specified port. The administrator can change this port from the "Networks and Ports" tab of the Sametime Administration Tool.

- If the Meeting Room client call control connection occurs using a direct HTTP-tunneled connection on port 80, or an HTTP connection through a SOCKS proxy server on port 80, the Sametime server must also be configured to support TCP tunneling of interactive audio/video streams on port 80. If the Sametime server is configured in this way, the audio and video streams can be transmitted between the Sametime client and server (either directly or through the SOCKS proxy server) using a TCP connection on port 80. This configuration enables a Sametime server and the Meeting Room client to exchange all meeting data, including interactive audio and video streams using port 80. For more information, see [TCP tunneling of interactive audio/video streams on port 80](#). The Meeting Room client can use a port other than port 80 to support HTTP tunneling and TCP tunneling of the Sametime data, as noted in Step 4 above.
**Note:** If the client transmits and receives audio and video streams through the TCP Tunneling port, up to four separate TCP sockets can be created to accommodate the audio and video streams. Two sockets are created for the RTP audio and video streams, and two sockets are created for the associated RTCP streams. Having four separate TCP sockets might affect audio/video performance because of the system resources required to maintain the sockets. Transmitting the streams over UDP results in better meeting performance than the TCP-tunneling method.

**Broadcast client connection process using JVM 1.4.2**

The Broadcast client must connect to the Broadcast Services on the Sametime server to receive the broadcast meeting streams. This topic describes the connection process the Broadcast client uses to receive broadcast meeting streams when the Broadcast client runs in a Web browser that operates with the Sun or IBM JVM 1.4.2.

**Note:** The following meeting streams can be sent during a broadcast meeting:
- Screen-sharing/whiteboard
- Chat
- Send Web page
- Question and answer polling
- Audio
- Video

To receive broadcast meeting streams, the Broadcast client and the Sametime server engage in a connection process. This connection process includes:

- **Call-control connection** - First, the Broadcast client makes a Real-Time Streaming Protocol (RTSP) connection to the Broadcast Services on the Sametime server. The Broadcast client and Broadcast Services exchange call-control data over this connection.

- **Receiving Broadcast streams** - If the call-control connection is successful, the Broadcast streams are transmitted from the server to the client using UDP or are tunneled through the call-control connection. If the client successfully establishes the call-control connection to the Broadcast Services, the Broadcast client should also receive the Broadcast meeting streams successfully.

The broadcast streams can also be transmitted using multicast.

**Call-control connection:** The steps below describe the connection process the Broadcast client uses to establish a call-control connection to the Broadcast Services.

1. The Sametime Broadcast client loads in the user’s Web browser when the user attends an instant or scheduled Sametime meeting.
   The host names and port numbers on which the Sametime server listens for connections are passed from the server to the Broadcast client. These host names and port numbers are specified in the Configuration-Connectivity-"Networks and Ports" tab of the Sametime Administration Tool.

2. Regardless of how the connectivity settings are configured in the Proxies tab of the Java Plug-in Control Panel, the Sametime Broadcast client first attempts to make a direct RTSP over TCP/IP connection to the Broadcast gateway component of the Broadcast Services on the Sametime server. The Broadcast client attempts this connection using the host names and ports specified in the "Broadcast Services Network-Broadcast gateway address for client
connections-Host name and Port number” setting (default port 554) in the Broadcast services network settings of the Sametime Administration Tool. Generally, a direct RTSP TCP/IP connection results in optimum performance for the Broadcast client. This connection fails if the connections must occur through a proxy server or any network between the client and server blocks TCP/IP connections on the specified port (default 554).

If the direct RTSP over TCP/IP connection is successful, the client can begin receiving the broadcast meeting streams as described in “Receiving broadcast meeting streams” below.

If the direct RTSP over TCP/IP connection is not successful, the Broadcast client continues with the call-control connection process, as described in the steps below.

3. If the direct RTSP over TCP/IP connection attempts described in step 2 fail, the configuration of the settings in the Proxies tab of the Java Plug-in Control Panel determines how the connections to the Sametime server are established. The possible configurations are discussed below.

**An HTTP proxy server is specified in the Proxies tab of the Java Plug-in Control Panel**

If the Broadcast client must connect to the Sametime server through an HTTP proxy server, you should disable the “Use my browser settings” option in the Java Plug-in Control Panel and enter the HTTP proxy server address and port in the Proxies tab of the Java Plug-in Control Panel.

When configured in this way, the Sametime Broadcast client encases the Sametime connectivity protocol data in HTTP requests and sends these requests to the HTTP proxy server. (This capability is referred to as HTTP-tunneling.) The HTTP proxy server forwards these requests to the Sametime server on behalf of the clients. The client will then attempt to establish and maintain an HTTP-tunneled connection to the Broadcast services.

Refer to step 4 in this procedure for a description of how these HTTP-tunneled connections are handled by the Sametime server.

**A SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel**

If the Broadcast client must connect to the Sametime server through a SOCKS proxy server, you should disable the “Use my browser settings” option in the Java Plug-in Control Panel and enter the SOCKS proxy server address and port in the Proxies tab of the Java Plug-in Control Panel.

If a SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel, the Broadcast client will make the following connection attempts:

a. The Broadcast client attempts to make TCP/IP connection to the Broadcast Services on the Sametime server through the SOCKS proxy server.

   This connection through a SOCKS proxy server uses the same protocols (RTSP over TCP/IP) that was used in the direct TCP/IP connection attempt discussed in step 2 above. The same host name and port (554) defined in the Sametime Administration Tool are also used for this connection attempt. This connection through the SOCKS proxy server can fail if the connection must occur through an HTTP proxy server or any network between the client and server prevents TCP/IP connections on the port described above (default port 554).

   **Note** The default ports are configurable from the “Networks and Ports” tab of the Sametime Administration Tool.
b. If the connection attempts using RTSP over TCP/IP through the SOCKS proxy is not successful, the Broadcast client attempts to make HTTP-tunneled connections to the Broadcast Services through the SOCKS proxy server. In this case, the Broadcast client encases the Sametime connectivity data in HTTP requests and sends these requests to the SOCKS proxy. The SOCKS proxy server sends these HTTP-tunneled requests to the Sametime server on behalf of the Broadcast client. The client will then attempt to establish and maintain an HTTP-tunneled connection to the Broadcast Services through the SOCKS proxy server.

Refer to step 4 in this procedure for a description of these how HTTP-tunneled connections are handled by the Sametime server.

**No proxies are specified the Proxies tab**

If no proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel, the Broadcast client can establish direct HTTP-tunneled connections with the Broadcast Services on the Sametime server. Direct HTTP-tunneled connections occur directly from the Broadcast client to the services on the Sametime server and are not established through a proxy server.

Refer to step 4 in this procedure for a description of how these HTTP-tunneled connections are handled by the Sametime server.

**Notes:**

- No proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel if the address and port fields associated with the proxy servers are blank.
- The Java Plug-in Control Panel includes a “Use my browser settings” option. It does not matter if the “Use my browser settings” option is or is not selected in the Java Plug-in Control Panel. When a Sametime client runs in a Web browser that operates with the Sun Microsystems JVM 1.4.2, the Sametime client cannot access the proxy settings specified in the Web browser even if the “Use my browser settings” option is selected in the Java Plug-in Control Panel.
- Direct HTTP-tunneled connections may be useful if a Sametime client must make a connection to a Sametime server through a client-side firewall that allows outbound HTTP traffic, but the firewall does not include an HTTP proxy server.

4. This step discusses the way in which HTTP-tunneled connections are established with the Sametime server.

When the direct TCP/IP connection attempt described in step 2 above fails, the Broadcast client will attempt to make an HTTP-tunneled connection to the Broadcast Services in the following scenarios:

- An HTTP proxy server is specified in the Proxies tab of the Java Plug-in Control Panel. In this case, the Broadcast client will attempt an HTTP-tunneled connection to the Broadcast Services through the HTTP proxy server.
- A SOCKS proxy server is specified in the Proxies tab of the Java Plug-in Control Panel and the Sametime protocol over TCP/IP connection attempts through the SOCKS proxy server to the Broadcast Services fails. In this case, the Broadcast client will attempt HTTP-tunneled connections to the Broadcast Services through the SOCKS proxy server.
- No proxy servers are specified in the Proxies tab of the Java Plug-in Control Panel. In this case, the Broadcast client will attempt direct HTTP-tunneled
The circumstances:

connections to the Sametime server. No attempt is made to establish an HTTP-tunneled connection to the Sametime server through a proxy server. The HTTP tunneling capabilities work differently depending on whether the administrator allows or does not allow HTTP tunneling on port 80. The administrator has the option of allowing or not allowing HTTP tunneling on port 80 during the server installation.

**If HTTP tunneling on port 80 is allowed** - If HTTP tunneling on port 80 is allowed during the Sametime server installation, the Broadcast client sends the HTTP requests containing Broadcast Services connection data to the Sametime Community Services multiplexer.

The "Host name" and "Port number" settings (default port 80) specified in the "Community Server Network Address for HTTP-tunneled client connections" settings of the Sametime Administration Tool are used to establish the connections to the Community Services multiplexer.

The Community Services multiplexer can differentiate between the HTTP requests intended for the Community Services, Meeting Services, and Broadcast Services by examining code that is appended to each URL by Sametime clients.

Upon receiving a Broadcast Services request, the Community Services multiplexer creates an intraserver connection to the Broadcast Services and sends the Broadcast Services data to the Broadcast Services.

The ability of the Community Services multiplexer to receive Community Services, Meeting Services, and Broadcast Services requests on a single port (port 80) enables the Sametime server to support HTTP tunneling over port 80 even if the Sametime server machine uses only a single IP address. This connectivity capability is sometimes referred to as "single-port mode."

**If HTTP tunneling on port 80 is not allowed** - If the administrator does not allow HTTP tunneling on port 80 during the Sametime server installation, the Broadcast client attempts to establish an HTTP-tunneled connection to the Broadcast Services (instead of the Community Services multiplexer).

The Meeting Room client attempts an HTTP-tunneled connection to the Broadcast Services using the "Host name" and "Port number" settings (default port 554) specified in the "Broadcast Services Network-Address for HTTP-tunneled client connections" settings.

If the Broadcast client is successful in establishing an HTTP-tunneled connections with the Broadcast Services using either port 80 or port 554, the Broadcast client maintains either a persistent or polled HTTP-tunneled connection as noted below.

**Maintaining a persistent HTTP-tunneled connection** - When establishing a connection using HTTP-tunneling, the Broadcast client first attempts to maintain a persistent HTTP-tunneled connection. (The persistent HTTP-tunneled connection is sometimes called "hybrid polling" or "master/slave HTTP tunneling.")

With this connection, data trickles continuously between the client and the Sametime server. This persistent connection provides the client with an event-driven, real-time connection to the server.

**Note** The persistent HTTP-tunneled connection provides better performance and uses fewer system and network resources than the polled HTTP-tunneled connections described below.

A persistent HTTP-tunneled connection might fail in the following circumstances:

- The client connects to the Sametime server through a proxy that buffers or caches data.
• Multiple Java applets running within a single instance of the Web browser attempt to create additional connections, and exceed the connection limits imposed by the Web browser. Web browsers limit the number of HTTP connections the browser can make to a single server.
• The client is unable to access the Web browser connectivity settings or authenticate with an HTTP proxy.

**Maintaining a polled HTTP tunneled connection** - If a persistent HTTP connection fails or is not possible, the client uses a continuous polling functionality to maintain the HTTP-tunneled connections.

In this type of tunneling, the client and server enter a mode in which the client continuously makes and breaks HTTP connections to post data to and receive data from the server.

The polling functionality overcomes most of the limitations that cause persistent HTTP-tunneled connections to fail.

The polling functionality enables the Sametime Broadcast client to maintain connections in almost any network environment as long as the client can connect to the server using HTTP. The polling functionality can increase network traffic. Polling might also affect the scalability of the server as more system resources are required to continuously make and break the connections.

**Receiving broadcast meeting streams:** If the initial call control connection described in "Call-control connection" above is successful, the client and server determine how to transmit and receive the broadcast meeting RTP streams.

Using the initial call-control connection described in "Call-control connection" above, the Broadcast Services send data to the client that describes the available broadcast meeting streams.

The manner in which the client receives the broadcast streams is determined by two variables:
• The way in which the call control connection was established
• The availability of the UDP transport between the client and the server

**Most efficient method for transmitting broadcast streams:** The most efficient transmission of the broadcast meeting media streams occurs when both of the following are true:
• The Broadcast client established a direct RTSP TCP/IP call control connection with the Sametime server. The term "direct" indicates that the client established a TCP/IP connection and did not establish this connection through a proxy server.
• The UDP transport is available on all networks between the client and the server.

If both of the above are true, the Broadcast client can subscribe to the broadcast meeting streams in either of two ways. The manner in which the client subscribes to the broadcast streams depends on whether multicast is available on the user’s network.
• **The Broadcast client can subscribe to unicast UDP streams** - The Broadcast client dynamically selects UDP ports on which to receive the streams. For this method to succeed, UDP traffic must be allowed to pass through all networks between the Sametime server (Broadcast Gateway component) and the Broadcast client.
• **The Broadcast client can subscribe to multicast UDP streams** - In this scenario, the Broadcast Gateway component of the Broadcast Services dynamically selects the UDP ports on which to send the data. These ports are randomly generated. The client subscribes to a multicast address on a multicast-enabled router and receives the meeting streams from the router. This method requires a multicast-enabled network that allows UDP traffic to pass through all networks between the Sametime server and the Broadcast client. For more information, see [Using multicast](#).

**Note:** Transmitting the streams over UDP results in better meeting performance than the TCP or HTTP tunneling method described in "Tunneling of broadcast streams" below.

**Tunneling of broadcast streams:** If UDP is not available on any network between the client and the server, the broadcast meeting streams are sent to a client using a tunneled connection. The streams are tunneled over the call-control connection port and can be tunneled over a direct RTSP TCP/IP connection, an RTSP TCP/IP connection through a SOCKS proxy server, or an HTTP-tunneled connection. These tunneling capabilities ensure that any client that can establish a call-control connection with the Broadcast Services can also receive the meeting data streams. The possible tunneling scenarios are described below:

- The Broadcast client establishes a direct RTSP TCP/IP call-control connection (on default port 554), but UDP is not available between the client and server - In this scenario, the RTP broadcast streams are tunneled to the client using TCP over the RTSP TCP/IP control connection between the client and server.
- The Broadcast client establishes an RTSP TCP/IP call-control connection through a SOCKS proxy server (on default port 554) - In this scenario, the RTP broadcast streams are also tunneled using RTSP TCP/IP over the control connection through the SOCKS proxy server.
- The Broadcast client established a call-control connection using HTTP-tunneling - In this scenario, the broadcast meeting RTP streams are tunneled through the HTTP-tunneled connection between the client and the server on the "Community Server Network-Address for HTTP-tunneled client connections" port (default port 80).

If the client established the call-control connection through an HTTP proxy server, the RTP streams are transmitted through the HTTP proxy on port 80. If the client established a call-control connection using HTTP through a SOCKS proxy server, the RTP streams are transmitted using HTTP through the SOCKS proxy on port 80. If the Broadcast client established a call-control connection through a direct HTTP connection, the RTP streams are transmitted directly to the client using HTTP on port 80.

### About HTTP tunneling

Many corporate networks restrict all connections to machines outside of the corporate network with the exception of HTTP connections on port 80.

Sametime provides HTTP tunneling functionality that enables Sametime clients to make all necessary connections to the Sametime server using HTTP over port 80 (with the exception of interactive audio/video connections). This functionality is especially useful if you deploy a Sametime server for Internet users or in situations where Sametime users operate behind a firewall and the Sametime server is not located in the network protected by that firewall.
Sametime supports HTTP tunneling on port 80 when the Sametime server uses only a single IP address. If you allow HTTP tunneling on port 80 during the Sametime server installation, you do not need to adjust any connectivity settings in the Sametime Administration Tool or add IP addresses to the Sametime server machine to enable the HTTP tunneling on port 80 functionality.

The HTTP-tunneling settings in the Sametime Administration Tool provide the administrator with the flexibility to configure the HTTP-tunneling functionality to accommodate a variety of different network environments. For example, Sametime can be configured to support HTTP tunneling on ports other than port 80 on a machine that includes a single IP address. Sametime can also be set up so that HTTP-tunneled connections are handled by the individual services instead of the Community Services multiplexer. As with previous Sametime releases, you can also assign multiple IP addresses to the Sametime server to support HTTP tunneling on port 80.

Read the following topics for a better understanding of the HTTP-tunneling functionality and the administrative settings that control it:

- **What is HTTP tunneling on port 80?** - Briefly elaborates on the purpose of HTTP tunneling on port 80 and provides a connection scenario to illustrate its advantages.

- **Configuring HTTP tunneling settings on a server that uses a single IP address** - Discusses the administration settings that control the HTTP tunneling functionality. This section explains how to change the HTTP-tunneling port on a server that includes a single IP address.

- **HTTP tunneling on port 80 using multiple IP addresses (optional)** - If your Sametime server is used heavily, you can improve server performance by assigning multiple IP addresses to the Sametime server to support the HTTP tunneling on port 80 functionality. This section discusses how the administrator can bind separate host names or IP addresses to each Sametime service to support HTTP tunneling on port 80. Using multiple IP addresses lessens the number of connection sockets required to maintain connectivity and might improve the I/O performance of the server.

- **Sametime Connect client 2.5 and 7.0 compatibility issues with HTTP tunneling on port 80** - Discusses compatibility issues that occur when a Sametime 2.5 connect client connects to a Sametime 7.0 server that supports HTTP tunneling on port 80 or a Sametime 7.0 Connect client connects to a Sametime 2.5 server that supports HTTP tunneling on port 80.

**What is HTTP tunneling on port 80?**

If you have extended a Sametime server to Internet users, the configuration of a remote client’s firewall might prevent the client from connecting to the Sametime server. For example, to exchange presence and chat data with other clients in a meeting, a Sametime client connects to the Community Services on a Sametime server using TCP/IP port 1533 (by default). To exchange screen-sharing and whiteboard data, a Sametime client connects to the Meeting Services using TCP/IP port 8081 (by default).

Many firewalls allow only HTTP connections on port 80 and will block the connection attempts that occur on ports 1533 and 8081. To establish connections in these environments, Sametime clients can automatically attempt a connection using HTTP tunneling over port 80. Using this tunneled connection, Sametime clients are able to communicate with the Community Services, Meeting Services, or Broadcast Services.
The example connection scenario below illustrates the advantages of the HTTP-tunneling functionality.

**Connection scenario**

In this scenario, a user (“Gina”) is operating behind a corporate firewall and attempting to attend a meeting on a Sametime server that is available to Internet users. Gina’s firewall allows HTTP connections to the Internet over port 80 but blocks all other connections.

1. A Sametime Administrator (“Ted”) employed by Meetings Incorporated in Los Angeles deploys a Sametime server for access by Internet users.

2. An Internet user in Denver (“Gina”) employed by the Acme corporation, and unknown to Ted, accesses the Sametime server in Los Angeles with a Web browser using HTTP over port 80. Gina clicks on the name of a meeting in the Sametime Meeting Center to attend the meeting.

3. The Sametime Meeting Room client loads from the Sametime server to the Web browser on Gina’s computer.

4. The Meeting Room client on Gina’s machine attempts to establish connections to the Community Services on the Sametime server on the default TCP/IP port 1533 and to the Meeting Services on the default TCP/IP port 8081. The Acme corporation’s firewall, which allows outbound connections only on HTTP port 80, blocks the outbound Sametime connections on both ports 1533 and 8081.

5. The Sametime Meeting Room client automatically attempts HTTP-tunneled connections for both Community Services and the Meeting Services to the Community Services multiplexer using port 80.

   The Community Services multiplexer can differentiate between HTTP connection requests intended for the Community Services and Meeting Services. The Community Services multiplexer creates intraserver connections to the Community Services and Meeting Services and passes the Community Services and Meeting Services data over these connections.

   **Note** The Broadcast client can also make HTTP-tunneled connections to the Community Services multiplexer using port 80. The Community Services multiplexer also forwards the Broadcast Services data to the Broadcast Services over an intraserver connection.

6. The HTTP-tunneled connection to the Community Services multiplexer on port 80 is successful because Gina’s firewall allows HTTP connections on that port.

As many corporate networks allow only HTTP connections on port 80, this functionality increases the possibility that users in restrictive network environments can attend meetings on a Sametime server that is extended to the Internet.

**Configuring HTTP-tunneling settings on a server that uses a single IP address**

This section discusses the settings in the Sametime Administration Tool that control the HTTP-tunneling functionality and how these settings are used when a Sametime server uses a single IP address.

If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the Community Services multiplexer handles all HTTP-tunneled connections, including connections to the Community Services, Meeting Services, and Broadcast Services. The ability of the Community Services multiplexer to
handle HTTP connections for three different services on a single port enables the Sametime server to support HTTP tunneling on port 80 when the server uses a single IP address.

To illustrate how the settings in the Sametime Administration Tool affect the connectivity, three examples are provided. The three examples assume you have installed Sametime on a machine that uses a single IP address. These examples illustrate how to:
- Allow HTTP tunneling on port 80 after the server installation
- Change the HTTP-tunneling port from port 80 to a different port
- Make HTTP-tunneled connections to individual services instead of the Community Services multiplexer

**Allowing HTTP tunneling on port 80 after the server installation**

If your Sametime server uses a single IP address and you did not allow HTTP tunneling on port 80 during the Sametime server installation, follow the example below to enable HTTP tunneling on port 80.

1. Open the Sametime Administration Tool.
2. Select Configuration-Connectivity-“Networks and Ports.”
3. Ensure that the “Community Services Network-Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options” setting is enabled.
4. In the “Community Services Network-Address for HTTP tunneled client connections” settings:
   - If your Sametime server operates on a Windows server, you can leave the “Host name” field blank.
     - If your Sametime server operates on an IBM i5/OS server, you must specify the fully-qualified host name of the Sametime server in the “Host name” field.
   - In the “Port number” field, delete port 1533 and enter port 80.
5. In the “Meeting Services Network-Address for HTTP tunneled client connections” settings:
   - If your Sametime server operates on a Windows server, you can leave the “Host name” field blank.
     - If your Sametime server operates on an IBM i5/OS server, you must specify the fully-qualified host name of the Sametime server in the “Host name” field.
   - In the “Port number” field, delete port 8081 and enter port 80.
6. In the “Broadcast Services Network-Broadcast Gateway address for HTTP-tunneled client connections” settings:
   - If your Sametime server operates on a Windows server, you can leave the “Host name” field blank.
     - If your Sametime server operates on an IBM i5/OS server, you must specify the fully-qualified host name of the Sametime server in the “Host name” field.
   - In the “Port number” field, delete port 554 and enter port 80.
7. Change the HTTP port used by the Domino server to a port other than port 80.
   - For more information, see [HTTP Services settings](#).
8. Click Update and restart the server for the change to take effect.
For more detailed information on how the HTTP-tunneling settings function, see Explanation of HTTP-tunneling settings.

**Changing the HTTP-tunneling port**

If your Sametime server uses a single IP address and you want to change the HTTP-tunneling port from port 80 to a different port, follow the procedure below. The example below assumes you are changing the HTTP tunneling port from port 80 to port 85.

1. Open the Sametime Administration Tool.
2. Select Configuration-Connectivity-“Networks and Ports.”
3. Ensure that the “Community Services Network-Enable Meeting Room client to try HTTP tunneling to the Community Server after trying other options” setting is enabled.
4. In the “Community Services Network-Address for HTTP tunneled client connections” settings:
   - Leave the “Host name” field blank. This setting is only used if the Sametime server machine uses multiple IP addresses or host names. For more information, see Configuring HTTP tunneling on a machine that uses multiple IP addresses.
   - In the “Port number” field, delete port 80 and enter port 85.
5. In the “Meeting Services Network-Address for HTTP tunneled client connections” settings:
   - Leave the “Host name” field blank.
   - In the “Port number” field, delete port 80 and enter port 85.
6. Ensure that the “Broadcast Services Network-Enable Web client to try HTTP tunneling after trying other options” setting is enabled.
7. In the “Broadcast Services Network-Broadcast Gateway address for HTTP-tunneled client connections” settings:
   - Leave the “Host name” field blank.
   - In the “Port number” field, delete port 80 and enter port 85.
8. Click Update and restart the server for the change to take effect.

For more detailed information on how the HTTP-tunneling settings function, see Explanation of HTTP tunneling settings.

**Connecting to individual services instead of the Community Services multiplexer**

If the Sametime server uses a single IP address, you can configure each Sametime service so that clients make separate HTTP-tunneled connections to the individual services instead of connecting to the Community Services multiplexer and relying on the Community Services multiplexer to forward the data to the Sametime services.

However, if the Sametime server uses a single IP address, each service must be assigned a different port number if you want clients to connect to individual services instead of the Community Services multiplexer. If you configure the Sametime server in this way, clients cannot make HTTP-tunneled connections to all services over port 80.

For example, assume you make the following settings in the "Networks and Ports" tab of the Sametime Administration Tool:
• In the "Community Services Network-Address for HTTP tunneled client connections-Port number" field, delete port 80 and enter port 1533. In the "Meeting Services Network-Address for HTTP tunneled client connections-Port number" field, delete port 80 and enter port 8081.
• In the "Broadcast Services Network-Broadcast Gateway address for HTTP-tunneled client connections-Port number" field, delete port 80 and enter port 554.

In this configuration, a Sametime client would make HTTP-tunneled connections to the Community Services using port 1533, the Meeting Services using port 8081, and the Broadcast Services using port 554. The Community Services connections occur to the Community Services multiplexer. The Meeting Services connections occur to the Meeting Services and the Broadcast Services connections occur to the Broadcast Services. Neither the Meeting Services connection nor the Broadcast Services connection is handled by the Community Services multiplexer.

Note: The port settings described above are the default port settings for HTTP-tunneled connections if the administrator does not allow HTTP tunneling on port 80 during the Sametime server installation.

If all users in your network environment must use HTTP to access the Sametime server, but users are not required to access the server via port 80, the configuration described above might improve server performance by lessening the connectivity load of the Community Services multiplexer. Fewer connection sockets are created when clients connect to each service individually instead of connecting to the Community Services multiplexer and relying on the multiplexer to forward data to the services.

**Explanation of HTTP tunneling settings**
The configuration settings that determine whether the HTTP-tunneled connection occurs to the individual service or the Community Services multiplexer are:
• Community Services Network-Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options
• Community Services Network-Address for HTTP tunneled client connections-Host name and Port number
• Meeting Services Network-Enable the Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options
• Meeting Services Network-Address for HTTP tunneled client connections-Host name and Port number
• Broadcast Services Network-Enable Web client to try HTTP tunneling after trying other options
• Broadcast Services Network-Broadcast Gateway address for HTTP-tunneled client connections-Host name and Port number

For Meeting Room and Broadcast client connectivity, these settings operate as follows:
• If the "Community Services Network-Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options" is selected, the Meeting Room client can attempt an HTTP-tunneled connection to the Community Services multiplexer.

The Meeting Room client attempts the connection to the Community Services multiplexer only when the following settings match:
  – The "Host name" and "Port number" settings under "Address for HTTP tunneled client connections" in the Meeting Services Network settings.
– The “Host name” and “Port number” settings under "Address for HTTP tunneled client connections" in the Community Services Network settings.

Upon receiving the HTTP-tunneling connection request, the Community Services multiplexer forwards the data to the Meeting Services.

If the "Community Services Network-Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options" setting is not selected, the Meeting Room client cannot attempt an HTTP-tunneled connection to the Community Services multiplexer.

• If the "Meeting Services Network-Enable the Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options" setting is selected, the Meeting Room client can attempt an HTTP-tunneled connection to the Meeting Services (instead of the Community Services multiplexer).

The primary purpose of this setting is to enable Meeting Room clients to make the HTTP-tunneled connection to the Meeting Services without requiring the clients to access the Meeting Services through the Community Services multiplexer. Connecting to the Meeting Services without using the Community Services multiplexer might improve server performance.

The Meeting Room client attempts the connection to the Meeting Services only when the "Meeting Services Network-Address for HTTP tunneled client connections-Host name and Port number" settings do not match the "Community Services Network Address for HTTP tunneled client connections-Host name and Port number" settings.

If the "Meeting Services Network-Enable the Meeting Room client to try HTTP tunneling to the Meeting Server after trying other options" setting is not selected, the Meeting Room client cannot attempt an HTTP-tunneled connection to the Meeting Services.

• If the "Broadcast Services Network-Enable Web client to try HTTP tunneling after trying other options" setting is selected, the Broadcast client can attempt an HTTP-tunneled connection to either the Community Services multiplexer or the Broadcast Services.

The Broadcast client attempts the connection to the Community Services multiplexer only when the "Broadcast Services Network-Broadcast Gateway address for HTTP-tunneled client connections-Host name and Port number" setting match the "Community Services Network Address for HTTP tunneled client connections-Host name and Port number" setting.

The Broadcast client attempts the connection to the Broadcast Services only when the "Broadcast Services Network-Broadcast Gateway address for HTTP-tunneled client connections-Host name and Port number" settings do not match the "Community Services Network Address for HTTP tunneled client connections-Host name and Port number" settings. Connecting to the Broadcast Services without using the Community Services multiplexer might improve server performance.

If the "Broadcast Services Network-Enable Web client to try HTTP tunneling after trying other options" setting is not selected, the Broadcast client cannot attempt an HTTP-tunneled connection to either the Community Services multiplexer or the Broadcast Services.

For Sametime Connect client connectivity, note the following:
• The Sametime Connect client attempts (or does not attempt) HTTP-tunneled connections based on the Sametime Connectivity settings in the Sametime Connect client. You cannot enable or disable HTTP-tunneling functionality for the Sametime Connect client from the Configuration-Connectivity-"Networks and Ports" tab of the Sametime Administration Tool. For more information, see:
- Basic Sametime Connect client connection process
- Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings

- The "Community Port" setting in the Sametime Connect client must match the port setting in the Community Services Network settings on the Sametime server for the connection to be successful. For more information, see:
  - Basic Sametime Connect client connection process
  - Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings

- There are compatibility issues with the Sametime Connect 2.5 and Sametime Connect 7.0 clients when connecting to servers configured to support HTTP tunneling on port 80. For more information, see Sametime Connect client 2.5 and 7.0 compatibility issues with HTTP tunneling on port 80

**Configuring HTTP tunneling on a server that uses multiple IP addresses**

Assigning multiple IP addresses to support HTTP tunneling on port 80 is an optional procedure the administrator can perform to improve the I/O performance of the Sametime server. Lotus software recommends this approach if a large number of users connect to your Sametime server using HTTP tunneling over port 80.

The administrator has the option of assigning a separate IP address to each of the Sametime services. In this configuration, the Community Services, Meeting Services, and Broadcast Services are bound to separate IP addresses and each service listens as a separate entity for HTTP connections on port 80. This configuration might result in more efficient I/O performance on the server but requires the administrator to perform the configuration procedures described below.

**Note:** The Sametime 7.0 server can be configured to support TCP tunneling of audio/video streams on port 80. The procedures in this section are focused primarily on setting up HTTP tunneling on port 80 for the Community Services, Meeting Services, and Audio/Video Services. However, if you want to set up both HTTP tunneling of Community Services, Meeting Services, and Broadcast Services data and TCP tunneling of Audio/Video Services streams, notes have been added to the procedures in this section that explain all additional procedures needed to set up TCP tunneling of audio/video streams on port 80. For more detailed information about TCP tunneling of audio/video streams, see TCP tunneling of interactive audio/video streams on port 80 later in this chapter.

**Configuration procedures required**

To assign multiple IP addresses to support HTTP tunneling on port 80, the administrator must perform the procedures listed below. Each procedure is described separately.

1. **Use the Sametime Administration Tool to bind the base DNS name for the Sametime server to the Sametime HTTP server**
2. **Add three new IP addresses to the Sametime server machine**
3. **Set up your DNS server to map the new IP addresses to required DNS names**
4. **Configure the HTTP-tunneling settings in the Sametime Administration Tool**
Bind the base DNS name for the Sametime server to the Sametime HTTP server

This procedure is the first of four required when using multiple IP addresses to support HTTP tunneling over port 80.

In this procedure, you use the Sametime Administration Tool to bind the Sametime HTTP server to the base DNS name currently used for the Sametime server. Before performing this procedure, ensure that your DNS server already has one DNS name mapped to the IP address of the Sametime server machine (for example, www.sametime1.com). To bind the base DNS name for the Sametime server to the Sametime HTTP server:

1. From the Sametime server home page, select "Administer the server" to open the Sametime Administration Tool.
2. Select Configuration.
3. Select Connectivity.
4. Select "Networks and Ports."
5. Select "Configure HTTP services on a Web page in its own window." The HTTP section of the Server document in the Domino Directory opens and displays in a separate window on the computer.
6. Under the Basics heading in the "Host name" field, enter the base DNS name for the Sametime HTTP server (for example, www.sametime1.com). In the "Host name" field, also enter 127.0.0.1. This entry is required for the Sametime Administration Tool to operate in this configuration. Place a comma between the DNS name of the HTTP server and the 127.0.0.1 entry (for example: www.sametime1.com, 127.0.0.1).
7. In the "Bind to Host name" field, select Enabled.
8. Click "Save & Close." (This button is located at the top of the Server document.) When the document closes, the Server - Servers view of the Domino Directory displays in the window.

Next, **Add three new IP addresses to the Sametime server machine**

Add three new IP addresses to the Sametime server machine

This procedure is the second of four required when using multiple IP addresses to support HTTP-tunneling over port 80.

To ensure that each Sametime service has its own IP address, the Sametime server machine requires four IP addresses. One IP address was mapped to the base DNS name in the previous procedure. You must add three additional IP addresses to the Sametime server machine so that the Community Services, Meeting Services, and Broadcast Services can be associated with individual IP addresses.

**Note:** If you also want to support TCP tunneling of audio/video streams on port 80, you must add one more IP address. In this scenario, the Sametime server requires five IP addresses because the Audio/Video Services must also be associated with an individual IP address.

To add additional IP addresses to the Sametime server, you can either add additional Network Interface Cards (NICs) to the Sametime server machine or assign multiple IP addresses to a single NIC.
Adding additional NICs: You can add three new NIC cards (one each for Community Services, Meeting Services, and Broadcast Services) and assign an IP address to each NIC. The computer’s I/O might operate more efficiently if you add a separate NIC for each of the services.

Note: If you want to support TCP tunneling of audio/video streams on port 80, add a fourth NIC to support the Audio/Video Services and assign an IP address to the NIC.

Assigning multiple IP addresses to a single NIC: To assign multiple IP addresses to a single NIC on a Windows machine:
2. Right click on the "Local Area Connection" icon to which you would add the IP address. Select Properties.
3. In the "Local Area Connection Properties" dialog ensure the "General" tab is selected.
   • In the "This connection uses the following items:" area, select "Internet Protocol (TCP/IP)."
   • Select the "Properties" button.
4. In the "Internet Protocol (TCP/IP) Properties" dialog box, select "Use the following IP address" and enter the primary (currently assigned) IP address of the system in the "IP address:" field.
5. Click the "Advanced" button in the lower-right corner of the "Internet Protocol (TCP/IP) Properties" dialog box.
6. In the "Advanced TCP/IP Settings" dialog ensure the "IP Settings" tab is selected.
7. In the "IP Settings" section of the "IP Settings" tab, click the Add button.
8. In the "TCP/IP Address" dialog, enter the IP address and Subnet mask settings and click Add.
9. At this point, the new IP address is added. If necessary, use the "Default gateways" section of the "Advanced TCP/IP Settings" dialog to add a new gateway for the system.

Next, set up your DNS server to map the IP addresses to required DNS names

Set up your DNS server to map the IP addresses to required DNS names

This procedure is the third of four required when using multiple IP addresses to support HTTP-tunneling over port 80.

After you have added three new IP addresses to the Sametime server machine, set up your DNS server to map the three new IP addresses to the following DNS names, where xxx.xxx.xxx is the base DNS name that is bound to the Sametime HTTP server:
   • community-xxx.xxx.xxx
   • meeting-xxx.xxx.xxx
   • broadcast-xxx.xxx.xxx For example, if the base DNS name to which you have bound the Sametime HTTP server is www.sametime1.com, map the three new IP addresses to the following names:
   • community-www.sametime1.com
   • meeting-www.sametime1.com
- broadcast-www.sametime1.com

The Community Server prepends "community-" to the base DNS name of the server to provide the Community Server with a unique DNS name. The Community Server multiplexer listens on port 80 for connections to the Community Services on this name. This name is passed from the server to the client when the client attends a meeting.

The Meeting Server prepends "meeting-" to the base DNS name of the server to provide the Meeting Server with a unique DNS name. The Meeting Server listens on port 80 for connections on this name.

The Broadcast server prepends "broadcast-" to the base DNS name and listens on port 80 for connections on this name.

Note: If you want to support TCP tunneling of audio/video streams on port 80, you must also map the IP address associated with the Audio/Video Services to a DNS name. The DNS name that you associate with the IP address of the Audio/Video Services is at your discretion. It is not necessary to adhere to any specific naming convention for the Audio/Video Services DNS name. In this example, we assume you map the DNS name "av-www.sametime1.com" to the Audio/Video Services.

Next, configure the HTTP tunneling settings in the Sametime Administration Tool.

Configure the HTTP-tunneling settings in the Sametime Administration Tool

This procedure is the last of four required when using multiple IP addresses to support HTTP tunneling over port 80.

In this procedure, you use the Sametime Administration Tool to bind the Community Services, Meeting Services, and Broadcast Services to the DNS names that were mapped to the three new IP addresses in the previous procedure.

1. From the Sametime server home page, select "Administer the server" to open the Sametime Administration Tool.
2. Select Configuration.
3. Select Connectivity.
4. Select "Networks and Ports."
5. In the Community Services Network settings, make the following settings:
   - Ensure the "Enable Web client to try HTTP-tunneling after trying other options" setting is selected.
   - In the "Address for HTTP tunneled client connections-Host name" setting, enter the Community Services DNS name that you mapped to an IP address in the previous procedure. The Community Services DNS name has the format community-xxx.xxx.xxx, where xxx.xxx.xxx is the DNS name that is bound to the HTTP server (for example, community-www.sametime1.com).
   - In the "Address for HTTP tunneled client connections-Port number" setting, enter 80 if it is not already listed.
6. In the Meeting Services Network settings, make the following settings:
   - Ensure the "Enable Web client to try HTTP-tunneling after trying other options" setting is selected.
   - In the "Address for HTTP tunneled client connections-Host name" setting, enter the Meeting Services DNS name that you mapped to an IP address in
the previous procedure. The Meeting Services DNS name has the format meeting-xxx.xxx.xxx, where xxx.xxx.xxx is the DNS name that is bound to the HTTP server (for example, meeting-www.sametime1.com).

- In the "Address for HTTP tunneled client connections-Port number" setting, enter 80 if it is not already listed.

7. In the Broadcast Services Network settings, select the following settings:
- Ensure the "Enable Web client to try HTTP-tunneling after trying other options" setting is selected.
- In the "Broadcast Gateway address for HTTP-tunneled client connections-Host name" setting, enter the Broadcast Services DNS name that you mapped to an IP address in the previous procedure. The Broadcast Services DNS name has the format broadcast-xxx.xxx.xxx, where xxx.xxx.xxx is the DNS name that is bound to the HTTP server (for example, broadcast-www.sametime1.com).
- In the "Broadcast Gateway address for HTTP-tunneled client connections-Port number" setting, enter 80 if it is not already listed.

8. Click update and restart the Sametime server for the changes to take effect.

Additional configurations required for Sametime on IBM i5/OS servers: When configuring a Sametime server to use multiple IP addresses to support HTTP tunneling over port 80 on an IBM i5/OS server, you must perform these additional configurations:

- In the Community Services Network settings of the Sametime Administration Tool, you must also enter the Community Services DNS name in the "Address for Client Connections-Host Name" field. Following the examples provided above, you must enter community-www.sametime1.com in the "Address for Client Connections-Host Name" field.
- Each of your users who are using the Sametime Connect for the desktop client must have it configured to connect to the Community Services DNS name (for example, community-www.sametime1.com).

Additional configurations required to support TCP tunneling of audio/video streams on port 80: If you want to support the TCP tunneling of audio/video streams on port 80, you must use the Sametime Administration Tool to perform these additional configurations:

1. In the Configuration-Connectivity-Networks and Ports tab of the Sametime Administration Tool, configure the Audio/Video Network settings as follows:
   - In the "TCP tunneling address for client connections-Host name" setting, enter the DNS name for the Audio/Video Services (av-www.sametime1.com in this example).
   - In the "TCP tunneling address for client connections-Port number" setting, delete the port 8084 entry and enter 80.

2. In the Configuration-Audio/Video-Connection Speed Settings tab of the Sametime Administration Tool, configure the settings as follows:
   - a. In the drop-down list immediately below the "Audio/Video and Broadcast Connection Speeds" heading, select the "Meetings with modem users" setting.
      - For "Audio bit rate," select 6.3 Kbps
      - For "Video bit rate," select 16 Kbps
      - For "Screen sharing and whiteboard bit rate for broadcast meeting only," select 16 Kbps
b. In the drop-down list immediately below the "Audio/Video and Broadcast Connection Speeds" heading, select the "Meetings with LAN/WAN users" setting.
   For "Audio bit rate," select 6.3 Kbps
   For "Video bit rate," select 16 Kbps
   For "Screen sharing and whiteboard bit rate for broadcast meeting only," select 16 Kbps

   **Note:** To support TCP tunneling of audio/video streams, the lowest possible bit rates must be selected for the streaming data to ensure acceptable performance for the end users. For more information, see [TCP tunneling of interactive audio/video streams on port 80](#).

### Notes about client connection processes using HTTP tunneling on port 80

Administrators should be aware of the following issues concerning clients that connect to the Sametime server using HTTP-tunneled connections. These issues apply regardless of whether the server uses a single IP address or multiple IP addresses to support the HTTP-tunneling functionality.

- **Clients that do not operate behind restrictive firewalls can still make direct TCP/IP connections to Sametime services on the Meeting Services Network-Address for client connections-Port number (default 8081), Community Services Network-Address for client connections-Port number (default 1533), and Broadcast Services Network-Broadcast gateway address for client connections-Port number (default 554).** Direct TCP/IP connections operate more efficiently than HTTP-tunneled connections, and clients automatically attempt these connections before attempting HTTP-tunneled connections. Only clients that cannot establish direct TCP/IP connections will attempt the HTTP-tunneled connection. For more information about client connection processes, see [Sametime Connect client connection processes](#) and [Meeting Room and Broadcast client connection processes](#).

- **A Sametime Connect client that operates behind a firewall that only allows outbound connections on port 80 can connect to the Community Services using HTTP over port 80.** The following configurations are required in the Sametime Connect client Sametime Connectivity settings for the connection to succeed:
  - Change the "Community port" setting to port 80.
  - If the client does not access the Internet through an HTTP proxy, select "Direct connection using HTTP protocol" for the Connection type.
  - If the client accesses the Internet through an HTTP proxy server, select "Use proxy" as the Connection type. For proxy type, select "Use HTTP proxy" and specify the DNS name or IP address of the HTTP proxy and the port on which to connect to the proxy.

   **Note:** You can also select "Use my Internet Explorer HTTP settings," "Use my Internet Explorer Web browser settings," or "Use my Java Plug-in settings" to establish connections to the Community Services through HTTP tunneling on port 80. If you select one of these settings, you must also ensure that the "Community port" setting in the Sametime Connectivity settings is set to port 80. For more information, see [Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings](#).

- **No end-user configurations are required for the end user to connect to the Sametime server using the Sametime Meeting Room or Sametime Broadcast**
clients. These clients receive all connection information from the server dynamically when a user attends a meeting.

**Sametime Connect client 2.5 and 7.0 compatibility issues with HTTP tunneling on port 80**

A Sametime 2.5 server does not support HTTP tunneling on port 80 when using a single IP address. With Sametime 2.5, HTTP tunneling on port 80 is supported only if the administrator assigned multiple IP addresses to the Sametime server.

A Sametime 7.0 server supports HTTP tunneling on port 80 when using a single IP address. This difference in HTTP tunneling support creates some compatibility issues regarding Sametime Connect client connectivity in the following scenarios:

- A Sametime Connect 2.5 client connecting to a Sametime 7.0 server configured to support HTTP tunneling on port 80 using a single IP address.
- A Sametime Connect 7.0 client connecting to a Sametime 2.5 server configured to support HTTP tunneling on port 80.

These compatibility issues are discussed below.

**Note:** For information about connectivity issues that occur when a Sametime Connect client attempts connections on port 443 or 563 to a Sametime server, see the “Things you need to know” section of the Sametime 7.0 Release Notes (strn70.nsf or strn70.pdf on the Sametime CD).

**Sametime 2.5 Connect clients connecting to a Sametime 7.0 server configured to support HTTP tunneling on a single IP address**

The Sametime 2.5 Connect client is designed to connect using HTTP tunneling on port 80 to a server that uses multiple IP addresses.

When a Sametime 2.5 server is configured to listen for HTTP-tunneled client connections on port 80, the server listens for Community Services connections on the server name “Community-hostname.” For example, if your Sametime 2.5 server is named sametimeserver.acme.com, the server listens for HTTP-tunneled Community Services connections on the name "Community-sametimeserver.acme.com."

**Note:** On a Sametime server that listens for HTTP-tunneled connections on multiple IP addresses, the Meeting Services listen for HTTP-tunneled connections on the server name "Meeting-hostname," the Broadcast Services listen for HTTP-tunneled connections on the server name "Broadcast-hostname," and the Community Services listen for HTTP-tunneled connections on the server name "Community-hostname." Each of those distinct host names are associated with a separate IP address. This configuration is described in Configuring HTTP tunneling on a server that uses multiple IP addresses.

When the Sametime 2.5 Connect client starts, the client connects to the Sametime server that is specified in the "Host" field of the Sametime Connect client Sametime Connectivity tab.

If port 80 is entered in the "Community port" field of the Sametime 2.5 Connect client Sametime Connectivity tab, the client automatically prepends the string "Community-" to the host name specified in the "Host" field of the Sametime Connect client Sametime Connectivity tab.
For example, if the host name "sametimeserver.acme.com" is specified in the "Host" field and port 80 is specified in the "Community port" field of the Sametime Connect client Sametime Connectivity tab, the Sametime 2.5 Connect client attempts an HTTP-tunneled connection to the "Community-sametimeserver.acme.com" host name. The prepending of the "Community-" string to the host name is hard-coded in the client and cannot be changed or deleted by the administrator.

When a Sametime 7.0 server is configured to listen for HTTP-tunneled connections on port 80 on a single IP address, the Sametime 7.0 server listens for all HTTP-tunneled connections on a single DNS name. For example, the Sametime 7.0 server might listen for the HTTP-tunneled connections on port 80 on the "sametimeserver.acme.com" host name.

**Note:** The Community Services multiplexer on a Sametime 7.0 server is designed to listen for all HTTP-tunneled Community Services, Broadcast Services, and Community Services connections on a single DNS name (associated with a single IP address). The Community Services multiplexer handles the connection for each service, makes an intraserver connection to the service, and forwards the data to the service.

As a result, when port 80 is specified in the "Community port" setting in the Sametime 2.5 Connect client, the client attempts a Community Services connection to the host name "Community-sametimeserver.acme.com," while a Sametime 7.0 server listens for this connection on the host name "sametimeserver.acme.com." As the client attempts the connection to a different host name than the server listens on, the connection cannot succeed.

If your Sametime community includes Sametime 2.5 Connect clients, and these clients must connect to a Sametime 7.0 server configured to listen for HTTP-tunneled client connections on a single IP address, the administrator can perform the following configurations to enable the Sametime 2.5 Connect client to connect to the Sametime 7.0 server:

1. Add the name "Community-hostname" ("Community-sametimeserver.acme.com" in the example) to the DNS server and associate "Community-sametimeserver.acme.com" to the same IP address as the sametimeserver.acme.com server name. This configuration ensures that both the "Community-sametimeserver.acme.com" and "sametimeserver.acme.com" server address resolve to the IP address of the Sametime server.

2. Open the Sametime Administration Tool on the Sametime 7.0 server. In the Sametime Administration Tool:
   a. Select Configuration-Connectivity.
   b. In the Community Services Network-Address for HTTP-tunneled client connections-Host Name field, make sure that both of these host names are entered:
      - Community-host name (Community-sametimeserver.acme.com in the example.)
      - Host name (Sametimeserver.acme.com in the example.)
      **Note:** Separate multiple entries in the Host Name field with a comma. For example, enter community-sametimeserver.acme.com, sametimeserver.acme.com.
   c. Ensure that the Community Services Network-Address for HTTP-tunneled client connections-Port Number setting specifies port 80.
Configuring the Sametime 7.0 server in this way ensures that the Sametime 2.5 Connect clients can make HTTP-tunneled connections on port 80 to the Sametime 7.0 server. Note also that the Sametime 2.5 Connect clients must specify port 80 in the "Port" setting of the Sametime Connect client Sametime Connectivity tab when making these connections.

**Sametime Connect 7.0 client connecting to a Sametime 2.5 server configured to support HTTP tunneling on port 80**

The following compatibility issue can occur if a Sametime 7.0 client attempts an HTTP-tunneled connection to a Sametime 2.5 server on port 80.

When a Sametime 2.5 server is configured to listen for connections on port 80, the server listens for Community Service connections on the server name "Community-hostname."

If the "Host" field in the Sametime Connectivity tab of a Sametime Connect 7.0 client specifies a Sametime 2.5 server, and the "Community port" setting of the Sametime Connect 7.0 client specifies port 80, the Sametime 7.0 client will attempt a connection to a Sametime 2.5 server on port 80.

When the Sametime Connect 7.0 client attempts this connection to the Sametime 2.5 server, the Sametime Connect 7.0 client attempts the connection to the host name specified in the "Host" field of the Sametime Connectivity tab. Unlike the Sametime 2.5 Connect client, the Sametime Connect 7.0 client does not prepend "Community-" to the host name specified in the "Host" field of the Sametime Connectivity tab when attempting connections on port 80.

For example, if the "Host" field of a Sametime Connect 7.0 client specifies "sametimeserver.acme.com," the Sametime Connect 7.0 client attempts the connection to the "sametimeserver.acme.com" host name. A Sametime 2.5 server listens for this connection on the "Community-sametimeserver.acme.com" address. Since the client and server specify different host names for this connection, the connection cannot succeed.

In this scenario, the user of the Sametime Connect 7.0 client must enter the host name "Community-sametimeserver.acme.com" in the "Host" field of the Sametime Connect 7.0 client Sametime Connectivity tab to connect to the Sametime 2.5 server.

**TCP tunneling of interactive audio/video streams on port 80**

The information in this section assumes the reader is familiar with the HTTP tunneling functionality supported by the Sametime server. If you are not familiar with the Sametime HTTP-tunneling functionality, see "About HTTP tunneling" earlier in this chapter.

During a Sametime server installation, a Sametime 7.0 server can be configured to support HTTP-tunneling on port 80 for Community Services, Meeting Services, and Broadcast Services data. This configuration enables all meeting activity supported by these services to transmit between a Sametime client and the Sametime server using HTTP over port 80.

When a Sametime server is configured to support HTTP tunneling on port 80 for the Community Services, Meeting Services, and Broadcast Services data, the administrator can also configure the Sametime server to support TCP tunneling of interactive audio/video streams on port 80.
Configuring a Sametime server in this way enables a Meeting Room client that connects to the Sametime server using HTTP tunneling on port 80 to also receive interactive audio/video streams over a TCP/IP connection on port 80.

**Note:** In previous Sametime releases, Meeting Room clients that connected to the Sametime server using HTTP tunneling could not receive the interactive audio and video streams. This limitation prevented these clients from participating in interactive audio/video meetings. With Sametime 7.0, the TCP tunneling of interactive audio/video streams enables a client that can access the Sametime server only over port 80 to participate in the full range of meeting activities supported by Sametime, including interactive audio and video.

This section includes the following topics pertaining to TCP tunneling of interactive audio/video streams on port 80:

- **Issues associated with TCP tunneling of interactive audio/video streams** - The administrator should be familiar with these issues before enabling TCP tunneling of audio/video streams on port 80.
- **Enabling TCP tunneling of interactive audio/video streams on port 80** - This topic includes the step-by-step instructions for enabling TCP tunneling of audio/video streams.

**Issues associated with TCP tunneling of interactive audio/video streams**

Before enabling TCP tunneling of interactive audio/video streams on port 80, the administrator should be aware of the following issues associated with using TCP connections to transmit interactive audio/video streams:

- A Sametime server can also transmit the audio and video streams using RTP over UDP. Using UDP to transmit audio/video streams consumes less network bandwidth and is more efficient than TCP. Also, additional processing is required at the server to handle TCP connections. TCP tunneling of the audio/video streams does not scale as well as transmitting audio/video streams using UDP.

    If it is possible to configure the network environment to support the transmission of audio/video streams between client and server using UDP, you should do so. Use TCP tunneling only when transmitting audio/video streams over UDP is not possible.

**Note:** To understand the client connection process that determines whether audio/video streams are transmitted via UDP or TCP, see [Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)](http://www.example.com).

- Audio and video latency (or delay) increases when tunneling audio and video streams over TCP. (Latency refers to the amount of time that elapses from the time a sender transmits data until this data arrives at the receiver.)
- The lowest bandwidth audio and video codecs must be used to compress the audio and video streams to get reasonable performance for end users.
- If a user must communicate with the Sametime server through a firewall that allows only HTTP on port 80, the user will be unable to receive the interactive audio/video streams from the Sametime server on port 80. The firewall must be configured so that both HTTP and TCP data can pass through the firewall on port 80.
- TCP tunneling of audio/video streams through an HTTP proxy server is not possible. A Sametime Meeting Room client that establishes an HTTP-tunneled
audio/video call control connection to the Sametime server through an HTTP proxy server cannot participate in an interactive audio/video meeting.

To receive the TCP-tunneled interactive audio and video streams, the HTTP-tunneled audio/video call control connection must be established either:

- Directly between the client and the server (the connection is not routed through any type of proxy server)
- Through a SOCKS proxy server.

For detailed information about the audio/video call control connection and the way in which the Meeting Room client establishes connections with the Audio/Video Services, see [Meeting Room client connection process using JVM 1.4.2](https://www.ibm.com/support/docview.wss?uid=swg21433111).

For step-by-step instructions to enable the TCP-tunneling of interactive audio/video streams on port 80, see [Enabling TCP tunneling of interactive audio/video streams on port 80](https://www.ibm.com/support/docview.wss?uid=swg21433111).

### Enabling TCP tunneling of interactive audio/video streams on port 80

During the Sametime server installation, the administrator can select an option to enable HTTP tunneling on port 80 for Community Services, Meeting Services, and Broadcast Services data. The HTTP tunneling on port 80 option provided during the Sametime server installation enables a Sametime server to support HTTP tunneling on port 80 for these services on a single IP address. The instructions in this section assume the administrator has selected the HTTP tunneling option during the Sametime server installation, and the Sametime server is currently supporting HTTP tunneling on port 80 on a single IP address.

**Note:** If you did not enable the HTTP tunneling on port 80 functionality during the Sametime server installation, you can manually enable it using the procedures described in [Configuring HTTP-tunneling settings on a server that uses a single IP address](https://www.ibm.com/support/docview.wss?uid=swg21433111) earlier in this chapter.

If you have enabled the HTTP tunneling on port 80 functionality, you can follow the steps below to enable TCP tunneling of audio/video streams on port 80.

1. **Add a new IP address to the Sametime server for the Audio/Video Services**
2. **Map the new IP address to a DNS name on your DNS server**
3. **Configure the Networks and Ports settings in the Sametime Administration Tool**
4. **Configure the Connection Speed Settings in the Sametime Administration Tool**

**Add a new IP address to the Sametime server for the Audio/Video Services**

This procedure is the first of four required to enable TCP tunneling of interactive audio/video streams on port 80.

To enable TCP tunneling of interactive audio/video streams on port 80, the Audio/Video Services must be assigned an individual IP address (separate from the IP address already assigned to the Sametime server). To make this possible, you must add an additional IP address to the Network Interface Card (NIC) on the Sametime server.

**Note:** It is not possible for a Sametime server that uses a single IP address to support TCP tunneling of interactive audio/video streams on port 80.
Assigning an additional IP address to a single NIC: An example of how to assign an additional IP address to a NIC on a Windows XP computer is provided below:

2. Click "My Network Places" in the "Other Places" panel.
3. Click "View network connections" in the "Network Tasks" panel.
4. Right click on the "Local Area Connection" icon to which you would add the IP address. Select Properties.
5. In the "Local Area Connection Properties" dialog ensure the "General" tab is selected.
   - In the "This connection uses the following items:" area, select "Internet Protocol (TCP/IP)."
   - Select the "Properties" button.
6. In the "Internet Protocol (TCP/IP) Properties" dialog box, select "Use the following IP address" and enter the primary (currently assigned) IP address of the system in the "IP address:" field.
7. Click the "Advanced" button in the lower-right corner of the "Internet Protocol (TCP/IP) Properties" dialog box.
8. In the "Advanced TCP/IP Settings" dialog ensure the "IP Settings" tab is selected.
9. In the "IP Addresses" section of the "IP Settings" tab, click the Add button.
10. In the "TCP/IP Address" dialog, enter the IP address and Subnet mask settings and click Add.
11. At this point, the new IP address is added. If necessary, use the "Default gateways" section of the "Advanced TCP/IP Settings" dialog to add a new gateway for the system.

Next: Map the new IP address to a DNS name on your DNS server

Map the new IP address to a DNS name on your DNS server
This procedure is the second of four required to enable TCP tunneling of interactive audio/video streams on port 80.

After adding the new IP address to the Sametime server, make sure you map the IP address to a DNS name for the Audio/Video Services on your DNS server.

The example provided in this documentation assumes that you map the new IP address to the DNS name "av-sametime.ibm.com.”

Next: Configure the Networks and Ports settings in the Sametime Administration Tool

Configure the Networks and Ports settings in the Sametime Administration Tool
This procedure is the third of four required to enable TCP tunneling of interactive audio/video streams on port 80.

In this procedure, you use the Sametime Administration Tool to assign the new host name (or DNS name) to the Audio/Video Services and specify port 80 as the port to use for TCP-tunneling of the audio/video streams.
In addition, you must also specify a host name for HTTP-tunneled connections to the Community Services, Meeting Services, and Broadcast Services in the Networks and Ports tab of the Sametime Administration Tool.

The example provided below assumes the following:

- The primary DNS name assigned to the Sametime server is sametime.ibm.com
- The DNS name you have added to the Sametime server for the Audio/Video Services is av-sametime.ibm.com

When a Sametime server is configured to support HTTP tunneling on port 80 on one IP address for the Community Services, Meeting Services, and Broadcast Services and TCP tunneling on port 80 on a separate IP address for the Audio/Video Services, you must specify the primary DNS name of the Sametime server (sametime.ibm.com) as the host name on which the Community Services, Meeting Services, and Broadcast Services will listen for HTTP-tunneled connections. You must assign the newly-added DNS name (av-sametime.ibm.com) to the Audio/Video Services. Follow the instructions below.

1. From the Sametime Administration Tool, select Configure - Connectivity.
2. Select the Networks and Ports tab (if necessary).
3. In the Community Services Network settings, make the following settings:
   - Ensure the "Enable Web client to try HTTP-tunneling after trying other options" setting is selected.
   - In the "Address for HTTP tunneled client connections-Host name" setting, enter the primary DNS name of the Sametime server (sametime.ibm.com).
   - In the "Address for HTTP tunneled client connections-Port number" setting, enter 80 if it is not already listed.
4. In the Meeting Services Network settings, make the following settings:
   - Ensure the "Enable Web client to try HTTP-tunneling after trying other options" setting is selected.
   - In the "Address for HTTP tunneled client connections-Host name" setting, enter the primary DNS name of the Sametime server (sametime.ibm.com).
   - In the "Address for HTTP tunneled client connections-Port number" setting, enter 80 if it is not already listed.
5. In the Broadcast Services Network settings, make the following settings:
   - Ensure the "Enable Web client to try HTTP-tunneling after trying other options" setting is selected.
   - In the "Broadcast Gateway address for HTTP tunneled client connections-Host name" setting, enter the primary DNS name of the Sametime server (sametime.ibm.com).
   - In the "Broadcast Gateway address for HTTP tunneled client connections-Port number" setting, enter 80 if it is not already listed.
6. In the Interactive Audio/Video Network settings, make the following settings:
   - In the "TCP tunneling address for client connections-Host name" setting, enter the DNS name for the Audio/Video Services (av-sametime.ibm.com).
   - In the "TCP tunneling address for client connections-Port number" setting, delete the port 8084 entry and enter 80.
7. Click update.
8. Leave the Sametime Administration Tool open. You must use the Sametime Administration Tool in the next procedure.
Additional configurations required for Sametime on IBM i5/OS servers: To enable TCP tunneling of audio/video streams over port 80 on an IBM i5/OS server, you must perform these additional configurations:

In the Community Services Network settings of the Sametime Administration Tool, you must also enter the Sametime server primary DNS name in the "Address for Client Connections-Host Name" field. Following the examples provided above, you must enter sametime.ibm.com in the "Address for Client Connections-Host Name" field.

Each user of the Sametime Connect for the desktop client must have the client configured to connect to the Community Services DNS name (for example, sametime.ibm.com).

Next: Configure the Audio/Video connection speed settings in the Sametime Administration Tool

Configure the Audio/Video connection speed settings in the Sametime Administration Tool
This procedure is the last of four required to enable TCP tunneling of interactive audio/video streams on port 80.

In this procedure, you use the Sametime Administration Tool to set the Audio/Video Connection Speed Settings on the Sametime server to support the TCP-tunneling of audio/video streams.

To support the TCP-tunneling of audio/video streams, the administrator must select the lowest possible bit rate settings as the “Audio/Video and Broadcast Connection Speeds” values to limit the amount of data that comprises the streams. Limiting the amount of data transmitted in these streams ensures acceptable performance for the end user.

Notes:
• When the administrator selects a low bite rate setting, the administrator invokes a low-bandwidth codec to handle the compression of the data streams. The TCP connection sockets over which the audio and video streams are tunneled cannot handle the amount of data generated by the high-bandwidth codecs. Using high bandwidth codec to compress the data stream results in poor performance for the end user.
• The instructions below indicate that you should set the low bit rate settings for both “Meetings with modem users” and “Meetings with LAN/WAN users.” Setting low bit rate settings for both of these options prevents end users from accidentally invoking the high bandwidth codecs when creating a meeting. For detailed information about the Connection Speed Settings, see the topics in the Connection Speed Settings for Audio/Video Services section.

To ensure that the low-bandwidth codecs are used to compress the streaming data:
1. From the Sametime Administration Tool, select Configurator-Audio/Video Services-Connection Speed Settings.
2. In the drop-down list immediately below the "Audio/Video and Broadcast Connection Speeds" heading, select the "Meetings with modem users" setting.
   • For Audio bit rate, select 6.3 Kbps
   • For Video bit rate, select 16 Kbps
• For Screen sharing and whiteboard bit rate for broadcast meeting only, select
16 Kbps
3. In the drop-down list immediately below the "Audio/Video and Broadcast
Connection Speeds" heading, select the "Meetings with LAN/WAN users" setting.
• For Audio bit rate, select 6.3 Kbps
• For Video bit rate, select 16 Kbps
• For Screen sharing and whiteboard bit rate for broadcast meeting only, select
16 Kbps
4. Click Update and restart the server for the change to take effect.

Note: This concludes the procedure required to enable TCP tunneling of
interactive audio/video streams on port 80. Note also that in some cases
you can improve the audio/video performance by adjusting the
"Audio/Video jitter buffer" setting available from the Configuration-
Audio/Video Services-Connection Speed Settings tab of the Sametime
Administration Tool. The optimal value for this setting depends on the
characteristics of the network on which Sametime is deployed. You should
experiment with settings that fall in the 100 to 500 millisecond range to find
the optimal value for this setting in your environment. For more
information, see [Audio/Video jitter buffer](#).

Assigning IP addresses to multiple Sametime servers installed on a
single server machine

If you are operating Sametime on an IBM i5/OS server, you can install multiple
Sametime servers on a single server machine, within the same logical partition. In
this scenario, each Sametime server instance runs on a separate partitioned
Domino server.

Note: Do not install multiple Sametime servers on a Windows NT or Windows
2000 server. You can install only one Sametime server on each Windows
server.

When multiple Sametime servers are running on separate Domino partitions
within the same logical partition of an IBM i5/OS server, it is important for each
Sametime server to be assigned a separate IP address. If you are also running any
other Domino servers or HTTP servers within the same logical partition, you must
also be certain that those servers are assigned a separate IP address to avoid port
conflicts.

For detailed instructions on properly preparing your IBM i5/OS TCP/IP
environment for Sametime and configuring multiple Sametime servers within
the same logical partition, see the Installation Guide (stinstall.nsf or stinstall.pdf) that
was shipped with Sametime for IBM i5/OS.

Connecting to other Sametime servers

If you install multiple Sametime servers, the services of the Sametime servers must
establish connections with each other to ensure that:
• A meeting started on one Sametime server can be simultaneously active on
another Sametime server.
• Users with different home Sametime servers have presence and chat capabilities
with all users in the community.
For more information about working with multiple servers and server-to-server connections, see:

- Advantages of using multiple Sametime servers
- Configuring ports for server-to-server connections

## Connecting Meeting Servers

The Connecting Meeting Servers option available from the "Configuration-Connectivity-Servers in this Community" settings of the Sametime Administration Tool is used only if you have installed multiple Sametime servers.

The administrator creates Connection Records to connect Meeting Servers as part of the process of integrating a new Sametime server into an environment in which other Sametime servers are already operating. These Connection Records are required for the invited servers to operate correctly. For more information about this process, see:

- Advantages of using multiple Sametime servers
- Integrating a Sametime server into an existing Sametime community
- Creating Connection Records to connect Sametime servers

## Using the Servers in this Community settings

The "Servers in this Community" settings available from the Configuration-Connectivity settings of the Sametime Administration Tool are used only if you have installed multiple Sametime servers.

The administrator configures the "Servers in this Community" settings as part of the process of integrating a new Sametime server into an environment in which other Sametime servers are already operating. For more information about this process, see the following topics:

- Advantages of using multiple Sametime servers
- Integrating a Sametime server into an existing Sametime community
- Configuring the "Servers in this Community" settings for the Sametime server

## Extending a Sametime server to the Internet

Many organizations need to conduct Sametime meetings that can be attended both by users on the corporate intranet and users from the Internet.

Because of the number and complexity of connections that can be required to connect to a Sametime server, it might be unacceptable for many organizations to open ports through the firewall to enable Internet clients to connect to a Sametime server on the corporate intranet.

The recommended solution for extending Sametime meetings to Internet users involves a multiple Sametime server deployment. This solution enables users on the corporate intranet and users from the Internet to attend the same Sametime meetings without jeopardizing the security of the corporate intranet. This solution requires you to:

- Install a Sametime server on the corporate intranet.
- Install a Sametime server in the network DMZ.
- Connect the two Sametime servers.
• Configure the firewalls to enable the servers and clients to establish the appropriate connections with the servers.

For more information, see Extending Sametime to Internet users.

Using reverse proxy or portal servers with the Sametime server

A Sametime 7.0 server can be deployed behind a reverse proxy server or a portal server. This section discusses issues related to using reverse HTTP proxy servers with a Sametime server. The issues discussed in this section also apply to deploying a Sametime server behind a portal server.

When a Sametime 7.0 server is deployed on an internal network behind a reverse proxy server, the reverse proxy server operates as an intermediary between the Sametime server and the Sametime clients. All Sametime data flowing between the Sametime server and its clients passes through the reverse proxy server.

To accomplish its security objectives, a reverse proxy server manipulates the data that passes through it. The manipulation of Sametime data by the reverse proxy server imposes specific requirements and limitations on the use of reverse proxy servers with the Sametime server.

This section includes the following topics related to the use of reverse HTTP proxy servers with the Sametime server:

• What is a reverse proxy server?
• Requirements and limitations associated with using a reverse proxy server with the Sametime server
• Configuring mapping rules on a reverse proxy server
• Configuring a Sametime server to operate with a reverse proxy server
• Sametime client connectivity and reverse proxy servers

Note: If you are configuring the Sametime 7.0 server to operate behind a Tivoli Access Manager WebSEAL reverse proxy server, refer to the Lotus Sametime Server 7.0 Release Notes for additional configuration information.

What is a reverse proxy server?

A reverse proxy server is a security device that is usually deployed in a network DMZ to protect HTTP servers (or Sametime servers) on a corporate intranet. The reverse proxy server performs security functions that protect the internal servers from attacks by users on the Internet.

The reverse proxy server protects internal HTTP servers by providing a single point of access to the internal network. Providing a single point of access to all HTTP servers on an internal network offers these specific security advantages and network access characteristics:

• The administrator can use the authentication and access control features of the reverse proxy server to control who can access the internal servers and control which servers each individual user can access. When a reverse proxy is deployed, the authentication process and access rights to multiple internal servers can be controlled from a single machine, which simplifies the security configuration.
• All traffic to your intranet servers appears to be destined for a single network address (the address of the reverse proxy server).
When a reverse proxy server is deployed, only URLs that are associated with the reverse proxy server are made public to Web browser users. Users from the Internet use these URLs to access the reverse proxy server. The reverse proxy server handles these requests from Internet users and redirects these requests to the appropriate internal HTTP server.

The administrator performs URL mapping configurations on the reverse proxy server that make this redirection possible. When configuring the reverse proxy server, the administrator maps the URLs that are used to access the reverse proxy server to the real URLs of the internal HTTP servers. When an Internet user sends a URL to the reverse proxy server, the reverse proxy server examines the URL and uses these mapping configurations (or rules) to rewrite the URL.

The reverse proxy server rewrites the URL by replacing the server address provided by the Internet user (a reverse proxy address) with the real address of the internal server. The HTTP request is then sent on the internal network from the reverse proxy server to the internal server.

- All traffic sent to Internet users from your internal servers appears to originate from a single network address.

When an internal HTTP server (or Sametime server) responds to a request from an Internet user, the internal server sends the response to the reverse proxy server and the reverse proxy server sends the response to the Internet user. The response sent on the Internet to the Internet user contains the address of the reverse proxy server, not the address of the internal HTTP server.

Unlike previous Sametime releases, Sametime 7.0 is designed to enable Sametime clients to establish and maintain connectivity with a Sametime server when these clients connect to the Sametime server through a reverse proxy server.

The security functionality of reverse proxy servers described above imposes specific requirements and limitations on the use of reverse proxy servers with Sametime. See any of the following topics for specific information about using reverse proxy servers with a Sametime server.

- Requirements and limitations associated with using a reverse proxy server with the Sametime server
- Configuring mapping rules on a reverse proxy server to support Sametime
- Configuring a Sametime server to operate with a reverse proxy server
- Sametime client connectivity and reverse proxy servers

Requirements and limitations of Sametime 7.0 reverse proxy support

The requirements and limitations associated with using a reverse proxy server with Sametime include:

- Reverse proxy server requirements
- Sametime client limitations and requirements
- Sametime server limitations
- Secure Sockets Layer (SSL) issues and requirements
- Client certificate authentication issues
- Lotus Enterprise Meeting Server (WCMS) restrictions

Each of these topics is discussed under a separate heading below.
Reverse proxy server requirements
This section lists the requirements and issues that are specific to the reverse proxy server.

- **URL specification requirement (affinity-id requirement)** - Only reverse proxy servers that use the following URL specification to access protected internal servers can be used with Sametime:

  Http[s]://hostname:port/affinity-id/

  The "affinity-id" is an administrator-defined alias for an internal Sametime server. This affinity-id must be present in the URLs sent from Web browsers to the reverse proxy server to enable Web browser users to access the Sametime server through the reverse proxy. For detailed information on this mandatory requirement of the reverse proxy server, see [Configuring mapping rules on a reverse proxy server](#).

- **Multiple reverse proxy servers must use the same DNS name and mapping configurations** - If you have deployed multiple reverse proxy servers in your network environment, and you expect users to access your Sametime server(s) through multiple reverse proxy servers, each of the reverse proxy servers must have the same DNS name and the same mapping configurations as noted below:

  - **DNS name** - All reverse proxy servers must use the same DNS name. For example, if one reverse proxy server is named reverseproxy.ibm.com all other reverse proxy servers must be named reverseproxy.ibm.com. If the reverse proxy servers have different DNS names, the Sametime clients will be unable to maintain communications with a Sametime server deployed behind the reverse proxy servers.

    **Note** If a network environment includes multiple reverse proxy servers that have the same DNS names, a connection dispatching device (such as an IBM WebSphere EdgeServer) is usually used to distribute connections from Web browsers to the multiple reverse proxy servers. These devices are frequently used to load balance connections to multiple machines.

  - **Mapping configurations** - Each reverse proxy server must use identical mapping rules and configurations to govern the translation of URLs sent by Web browsers to the reverse proxy server for the purpose of accessing an internal Sametime server. If the translation of these URLs to the URLs of the internal Sametime servers does not occur in exactly the same way on each of the reverse proxy servers, the Sametime clients will be unable to maintain communications with a Sametime server deployed behind the reverse proxy server.

    **Note** Each Sametime server must be represented by the same "affinity-id" in the mapping rules on each of the reverse proxy servers.

    For more information about the affinity-id and mapping rules, see [Configuring mapping rules on a reverse proxy server](#).

- **The reverse proxy server must use cookies for authentication** - When an end user uses a Web browser to access and authenticate with the reverse proxy server, the reverse proxy server must send an authentication cookie to the Web browser. All subsequent HTTP requests from a Sametime client will then pick up this cookie and use it for automatic authentication with the reverse proxy server. Reverse proxy servers that rewrite URLs for authentication purposes are not supported. Some reverse proxy servers append authentication and session information to the end of URLs embedded in HTML that passes through the proxy back to the client. The client will include this appended data on subsequent requests to the reverse proxy server. When the reverse proxy server receives these subsequent requests from the client, the reverse proxy server strips the authentication data and rewrites the URL to accomplish the internal
routing of requests. A Sametime server cannot operate behind a reverse proxy server that handles authentication data in this way.

- A lengthy timeout value should be specified for the authentication cookies - The administrator should specify a lengthy timeout value for authentication cookies generated by the reverse proxy server.

If the authentication cookie expires when the user is attending a meeting, the user is disconnected from the meeting. To re-enter the meeting, the user must go through the inconvenient process of reconnecting to the reverse proxy, reauthenticating with the reverse proxy, and waiting for the Java applets to be reloaded to the Web browser.

Setting a lengthy timeout value for authentication cookies can prevent unexpected user disconnections due to an authentication cookie expiration. Generally, the authentication cookie should be valid for the entire length of the longest meetings that are routinely conducted on the Sametime server deployed behind the reverse proxy server.

**Sametime client/Web browser limitations and JVM requirements**

The following Sametime clients can communicate with Sametime servers through a reverse proxy server:

- Sametime Meeting Room client
- Sametime Broadcast client
- Sametime Connect for browsers (the Java version of Sametime Connect)
- Sametime Links applications built with Sametime developer toolkits

**Note:** Sametime Connect for the desktop (the Windows version of Sametime Connect) cannot be used with a Sametime server that is deployed behind a reverse proxy server.

The Sametime Meeting Room client and the Sametime Broadcast client can communicate with a Sametime server through a reverse proxy server when running with the following Web browsers and Java Virtual Machines (JVMs):

- An Internet Explorer 6 browser that operates with the Microsoft native VM or the Sun Microsystems JVM 1.4.2 (and associated Java Plug-in).
- A Netscape 7 browser that operates with the Sun Microsystems JVM 1.4.2 (and associated Java Plug-in).

The Sametime Connect for browsers client and Sametime Links applications can communicate with a Sametime server through a reverse proxy server when running in an Internet Explorer 6 or Netscape 7 browser that operates with the Sun Microsystems JVM 1.4.2. These clients may not function appropriately with other JVMs, including the native Microsoft VM provided for Internet Explorer.

**Sametime server limitations**

The following limitations apply to Sametime server features when the Sametime server is deployed behind a reverse proxy server.

- **Audio/video is not available** - Audio/video streams cannot be transmitted to Sametime clients that access the Sametime server through a reverse proxy server.

- **Access to the Sametime Administration Tool is not available** - A user that connects to the Sametime server through a reverse proxy server cannot access the Sametime Administration Tool. The user can open a Web browser that is installed on the Sametime server to access the Sametime Administration Tool. The user can also connect to the Sametime server from an internal network.
location that does not route HTTP traffic through the reverse proxy server to access the Sametime Administration Tool.

**Secure Sockets Layer (SSL) issues and requirements**
Note the following about SSL and Sametime in a reverse proxy environment:

- Secure Sockets Layer (SSL) can be used to encrypt data transmitted between the Sametime clients and the reverse proxy server.
- SSL cannot be used to encrypt data transmitted between the Sametime servers and the reverse proxy server.

If SSL is used to encrypt data transmitted between Web browsers and the reverse proxy server, the administrator must perform the mapping configurations on the Sametime server necessary to map the HTTPS data received from the Web browser to the HTTP required by the Sametime server.

The reverse proxy must also be configured to translate the HTTP data received from the Sametime server to the HTTPS data required by the client.

When a reverse proxy server is configured to support SSL, the reverse proxy server sends an SSL server certificate to the Web browser during the SSL connection handshake. The Java 1.4.2 Plug-in used by the Web browser must have access to a Signer certificate that is signed by the same Certificate Authority (CA) as the server certificate that is sent by the reverse proxy.

By default, the Java Plug-in has access to several different Signer certificates that can be used for this purpose. To view the Signer certificates that are available to the Java Plug-in 1.4.2, use the Java Plug-in Control Panel as noted below:

1. From the Windows desktop, open the Control Panel (Select Start-Settings-Control Panel).
2. Double-click on the Java Plug-in 1.4.2 icon to open the Java Plug-in Control Panel.
3. Click the Certificates tab.
4. Select the Signer CA radio button.
   
   The server certificate sent by the reverse proxy server to the client Web browser must be signed by one of the CAs that appears in the signer CA list for the SSL connection handshake to succeed.

**Client certificate authentication issues**

If the reverse proxy server is configured to require client certificate authentication, the client certificate for an individual user must be imported into the Java Plug-in 1.4.2 Control Panel on that user’s machine. You can use the Certificates tab of the Java Plug-in Control Panel to import the client certificate into the Java Plug-in key store. For example:

1. From the Windows desktop on a user’s machine, open the Control Panel (Select Start-Settings-Control Panel).
2. Double-click on the Java Plug-in 1.4.2 icon to open the Java Plug-in Control Panel.
3. Click the Certificates tab.
4. In the Certificates column, select "Secure Site."
5. Click the Import button to import the client certificate.
Lotus Enterprise Meeting Server restrictions
The Enterprise Meeting Server that operates with Sametime 7.0 servers cannot be deployed behind a reverse proxy server.

Configuring mapping rules on a reverse proxy server to support Sametime

When a Sametime server is deployed behind a reverse proxy server, the administrator must configure mapping rules on the reverse proxy server. These mapping rules enable the reverse proxy server to translate (or rewrite) a URL associated with the reverse proxy server to the URL of an internal Sametime server.

This section discusses how mapping rules are configured on a reverse proxy server to accomplish the translation (or rewriting) of URLs when the reverse proxy operates with Sametime. This section includes the following topics:

- Affinity-id (server alias) requirement of the reverse proxy server
- Example of URL mapping configurations on the reverse proxy server

Affinity-id (server alias) requirement of the reverse proxy server

Only reverse proxy servers that support the use of an affinity-id (or server alias) in the URLs that are associated with internal servers can be used with Sametime. Specifically, the reverse proxy server must support this URL specification to access protected internal servers:

```
Http[s]://hostname:port/affinity-id/
```

In this example, the "hostname" represents the DNS name of the reverse proxy server and the affinity-id is an alias for an internal server that is protected by the reverse proxy server. A specific example of this URL format is:

```
Http[s]://reverseproxy.ibm.com/st01/stcenter.nsf
```

In the example above, the text sting "st01" is the affinity-id. The affinity-id is an alias for a specific Sametime server (such as sametime.ibm.com) that is protected by the reverse proxy server. The affinity-id is used by the reverse proxy server to direct incoming requests to the specific internal Sametime server.

For example, if the incoming URL from the Web browser is:

```
Http[s]://reverseproxy.ibm.com/st01/stcenter.nsf
```

And the mapping rules on the reverse proxy server map the "st01" affinity-id to the Sametime server named "sametime.ibm.com," the affinity-id ensures the reverse proxy server rewrites the incoming URL to:

```
Http[s]://sametime.ibm.com/stcenter.nsf
```

Essentially, the affinity-id is an administrator-defined alias for an internal Sametime server. The affinity-id is defined in the mapping rules of the reverse proxy server. If you have multiple Sametime servers deployed behind a reverse proxy server, each Sametime server must have an individual affinity-id as indicated below:

<table>
<thead>
<tr>
<th>Mapping rule for client-provided URL:</th>
<th>Routed to internal server:</th>
</tr>
</thead>
<tbody>
<tr>
<td>/st01/*</td>
<td><a href="http://sametime1.ibm.com/">http://sametime1.ibm.com/</a>*</td>
</tr>
<tr>
<td>/st02/*</td>
<td><a href="http://sametime2.ibm.com/">http://sametime2.ibm.com/</a>*</td>
</tr>
</tbody>
</table>

It is mandatory that any reverse proxy server that operates with a Sametime server support the affinity-id (or server alias) in URLs.
For additional information about configuring mapping rules on reverse proxy server, see Example of URL mapping configurations on the reverse proxy server below.

**Important:** The Sametime Administration Tool on a Sametime server contains a “Server Alias” setting. This Server Alias setting must specify the same affinity-id that is used to represent the Sametime server in the mapping rules on the reverse proxy server. For more information, see Configuring a Sametime server to operate with a reverse proxy server.

**Example of URL mapping configurations on the reverse proxy server**

This section provides basic examples of how an administrator might configure URL mapping configurations for a reverse proxy server deployed in front of a Sametime server.

When a user connects to a Sametime server through a reverse proxy server, the reverse proxy server must be configured to support the following actions that enable Sametime users to attend meetings and participate in chat sessions:

- The user must be able to click on links in the Sametime server home page and navigate to the various HTML pages of the UI. This capability requires the reverse proxy server to rewrite the URLs of the HTML pages that comprise the Sametime UI.
- The Sametime Java applet clients that load in a user’s Web browser must be able to connect to the services on the Sametime server. Since these connections must occur through the reverse proxy server, the reverse proxy server must also be able to rewrite the URLs required to establish these connections to the services on the Sametime server.

The following sections provide examples of the mapping configurations required to accomplish the two tasks above.

**Reverse proxy mapping configurations that enable a Web browser user to navigate the Sametime user interface:** The example below illustrates how an administrator can configure the reverse proxy server to enable users to navigate the HTML pages of the Sametime user interface. This example assumes the following:

- The Sametime server name is "sametime.ibm.com."
- The URL required to access the reverse proxy server is "reverseproxy.ibm.com."
- The affinity-id chosen by the administrator for the Sametime server is "st01."

Listed below are two entities of the Sametime server user interface and the URLs required to access these entities on a Sametime server with the server name "sametime.ibm.com."

- **Active Meeting page** - The Sametime server URL for the Active Meeting page is http://sametime.ibm.com/stconf.nsf/vwWebActiveMeetings?OpenView.

**Example 1 - Translating the URL of the server home page:** To access the Sametime server home page through a reverse proxy server, the Web browser would send the following URL to the reverse proxy server:

http[s]://reverseproxy.ibm.com/st01/stcenter.nsf
The reverse proxy server must contain a mapping rule that translates this URL into the following URL required to access the Sametime server home page:
http[s]://sametime.ibm.com/stcenter.nsf

Example 2 - Translating the URL of the Active Meeting page: If the user selects the Attend a Meeting link in the Sametime user interface to view the list of active meetings, the Web browser would send the following URL to the reverse proxy server:
http[s]://reverseproxy.ibm.com/st01/stconf.nsf/vwWebActiveMeetings?OpenView

The reverse proxy server must contain a mapping rule that translates this URL into the following URL required to access the Sametime server Active Meetings page:
http[s]://sametime.ibm.com/stconf.nsf/vwWebActiveMeetings?OpenView

A single mapping rule can be used to translate all URLs associated with the Sametime server user interface: Through the use of wildcards, the administrator can create a single mapping rule on the reverse proxy server to translate all URLs associated with the Sametime server interface. Following the examples above, the administrator can create a mapping rule that translates the following URL from the Web browser:
http[s]://reverseproxy.ibm.com/st01/*

To this Sametime server URL:
http[s]://sametime.ibm.com/*

A single mapping rule that accomplishes this type of URL translation should enable users to access all entities of the Sametime user interface through a reverse proxy server.

Note: It is not mandatory to configure the mapping rules as described above. The actual configuration of the mapping rules on the reverse proxy server is at the discretion of the administrator. When configuring the mapping rules note that the URL for any entity of the Sametime server user interface will begin with the Sametime server name (sametime.ibm.com in this example).

Reverse proxy mapping configurations that enable Sametime Java applet connectivity through the reverse proxy server: The following example URL mappings enable the Sametime Java applet clients running in a user’s Web browser to connect to the Community Services, Meeting Services, and Broadcast Services on the Sametime server through the reverse proxy server:

Example 1 - Mapping configuration for Community Services connectivity

This example illustrates the mapping configurations that enable a Java applet client to connect to the Community Services:

If the incoming URLs from the Java applet are:
http[s]://proxy.ibm.com/st01/communityCBR/
http[s]://proxy.ibm.com/st01/CommunityCBR/

The mapping rules on the reverse proxy must translate these URLs to:
http://sametime.ibm.com:8082/communityCBR
http://sametime.ibm.com:8082/CommunityCBR
Note: The mapping configuration for the Community Services connectivity should contain two case-sensitive mapping rules as indicated above. Some pieces of the Java code contain the lowercase "c" in "communityCBR" and some pieces of the Java code use the uppercase "C" in "CommunityCBR." This difference may prevent connections if the proxy is case-sensitive.

Example 2 - Mapping configuration for Meeting Services connectivity

This example illustrates the mapping configurations that enable a Java applet client to connect to the Meeting Services:

If the incoming URL from the Java applet is:
Http[s]://proxy.ibm.com/st01/MeetingCBR

The mapping rule on the reverse proxy must translate this URL to:
Http://sametime.ibm.com:8081/MeetingCBR

Example 3 - Mapping configuration for Broadcast Services connectivity

This example illustrates the mapping configurations that enable a Java applet client to connect to the Broadcast Services:

If the incoming URL from the Java applet is:
Http[s]://proxy.ibm.com/st01/BroadcastCBR

The mapping rule on the reverse proxy must translate this URL to:
Http://sametime.ibm.com:554/BroadcastCBR

Notes about the Java applet connectivity mapping rule examples: During a Sametime server installation, the administrator has the option of allowing or not allowing HTTP tunneling on port 80.

If the administrator does not allow HTTP tunneling on port 80 during the Sametime server installation, it is necessary to configure separate mapping rules for each of the three Sametime services (Community Services, Meeting Services, and Broadcast Services).

Note: Four mapping rules are required: two for the Community Services, one for the Meeting Services, and one for the Broadcast Services as shown in the three examples above.

When the administrator does not allow HTTP tunneling on port 80, each of the Sametime services listens for HTTP connections on a different port:

- The Community Services listen for HTTP connections on port 8082. Port 8082 is reflected in the mapping rule for Community Services connections above. You can view or change this port setting from the Community Services Network - Address for HTTP-tunneled client connections option in the Networks and Ports tab of the Sametime Administration Tool.

- The Meeting Services listen for HTTP connections on port 8081. Port 8081 is reflected in the mapping rule for Meeting Services connections above. You can view or change this port setting from the Meeting Services Network - Address for HTTP-tunneled client connections option in the Networks and Ports tab of the Sametime Administration Tool.

- The Broadcast Services listen for HTTP connections on port 554. Port 554 is reflected in the mapping rule for Broadcast Services connections above. You can
view or change this port setting from the Broadcast Services Network - Address for HTTP-tunneled client connections option in the Networks and Ports tab of the Sametime Administration Tool.

Because each of these Sametime services listens for a connection on a separate port, separate mapping rules must be established for each of the services. The mapping rule must specify the port on which each of the services is listening for connections.

**Note:** If you change the HTTP-tunneling port number for a specific service in the Sametime Administration Tool, the mapping rules you configure on the reverse proxy server must reflect the new port number.

If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the Sametime clients connect to all of the services on a single port. With this configuration, the single mapping rule that enables users to navigate the Sametime server user interface will also enable the Sametime clients to make connections to the Sametime services.

When HTTP tunneling on port 80 is allowed, the Community Services multiplexer on the Sametime server listens for HTTP connections on behalf of the HTTP Services, Community Services, Meeting Services, and Broadcast Services on the Sametime server. The Community Services multiplexer listens for connections to all of these services on a single port (port 80).

**Note:** When operating in this mode, the Community Services multiplexer on the Sametime server can distinguish between HTTP requests destined for the HTTP Services, Community Services, Meeting Services, and Broadcast Services and establish intraserver connections to each of the services. For example, if the Community Services multiplexer receives an HTTP request for the Meeting Services on port 80, the Community Services handles the request and creates an intraserver connection to the Meeting Services. The Community Services multiplexer then forwards the request to the Meeting Services. The ability of the Community Services multiplexer to handle requests for multiple services in this way is sometimes referred to as "single port mode."

When the administrator allows HTTP tunneling on port 80 (that is, when the Sametime server is operating in single port mode), the mapping rules for Java applet connectivity are much simpler. Since all connections from the Sametime Java applet clients occur on the same port, it is not necessary to specify individual ports for each service in the mapping rules.

In this scenario, the administrator would only need to ensure that this incoming URL from the Sametime Java applets:

```text
Http[s]://proxy.ibm.com/st01/*
```

Is translated to this URL by the mapping rules on the reverse proxy server:

```text
Http://sametime.ibm.com/*
```

Note that server performance is not as efficient when the Sametime server is configured to support HTTP tunneling on port 80 because of the connectivity burden placed on the Community Services multiplexer. For more information, see [About HTTP tunneling](#).
Configuring a Sametime server to operate with a reverse proxy server

The administrator must use the Sametime Administration Tool on the Sametime server to configure the Sametime server to operate with a reverse proxy server.

There are two settings the administrator must configure in the Configuration-Connectivity-Networks and Ports tab of the Sametime Administration Tool to enable a Sametime server to operate with a reverse proxy server. These settings include:

- **Enable Reverse Proxy Discovery on the client** - Selecting this setting allows the administrator to enable or disable the reverse proxy support. This setting enables the logic in the Sametime clients that enables them to connect to a Sametime server through the reverse proxy server. This setting is disabled by default.

**Note:** Enabling this setting does not require that all users on your corporate intranet access the Sametime server through the reverse proxy server. Users on your corporate intranet that are not required to route connections through the reverse proxy servers can still establish connections with the Sametime server using the standard Sametime client connection processes. For more information, see [Connecting to a Sametime server without going through the reverse proxy server](#).

- **Server Alias** - The Server Alias setting must specify the affinity-id that the administrator uses to represent this Sametime server in the mapping rules on the reverse proxy server.

**Note:** The term “Server Alias” is synonymous with affinity-id.

For example, if the administrator uses the text string “st01” as the affinity-id that represents the Sametime server in the mapping rules on the reverse proxy server, the administrator must also enter “st01” as the value for the Server Alias setting in the Sametime Administration Tool.

Following a Sametime server installation, the Server Alias setting defaults to the Sametime server name that is extracted from the fully-qualified DNS name of the Sametime server. For example, if the fully-qualified DNS name of the Sametime server is “sametime.ibm.com,” the default value for the Server Alias is “sametime.”

**Note:** An administrator may want to change the default Server Alias setting to avoid using the real Sametime server name as the affinity-id in the mapping rules on the reverse proxy server. If the real Sametime server name is used as the affinity-id on the reverse proxy server, the real server name will appear in URLs transmitted on the Internet.

For more information about the affinity-id, see [Configuring mapping rules on a reverse proxy server to support Sametime](#).

Enabling reverse proxy support on a Sametime server

To enable reverse proxy support on a Sametime server:

1. From the Sametime server home page, click the “Administer the Server” link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Connectivity.
4. If necessary, select the Networks and Ports tab.
5. At the bottom of the Networks and Ports tab, select “Enable Reverse Proxy Discovery on the client.”
6. In the "Server Alias" text box, type the text string that is used as the affinity-id that represents this Sametime server in the mapping configurations on the reverse proxy server (for example, type st01).

7. Click Update and restart the Sametime server for the changes to take effect.

Sametime client connectivity and reverse proxy servers

This section briefly discusses Sametime client connectivity issues when the Sametime Meeting Room client, Sametime Broadcast client, and Sametime Connect for browsers client operate with a reverse proxy server.

These connectivity issues are discussed in the following topics:

- Connecting to the Sametime server without using the reverse proxy server
- Notes about Sametime client connectivity through a reverse proxy server

Connecting to a Sametime server without using the reverse proxy server

When a Sametime server is configured to operate with a reverse proxy server, users on the corporate intranet that are not required to route connections through the reverse proxy server can still connect to the Sametime server using the standard Sametime client connection processes.

Note: In this scenario, both intranet and Internet users connect to the same Sametime server. Connections from Internet users are routed through the reverse proxy server while connections from intranet users are not routed through the reverse proxy server.

To configure a Sametime server to operate with a reverse proxy server, the administrator must select the "Enable Reverse Proxy Discovery on the client" setting in the Sametime Administration Tool. Selecting this setting:

- Enables the additional logic in the Meeting Room client, Broadcast client, and Sametime Connect for browsers client that the clients use to connect to a Sametime server through a reverse proxy server.
- Does not disable the existing connectivity logic in these Sametime clients.

Enabling the "Enable Reverse Proxy Discovery on the client" setting enhances the existing logic in the Sametime clients by adding the reverse proxy connection logic to the existing logic. The existing logic is still present and operable within the clients. This design enables clients that do not connect to the Sametime server through the reverse proxy server to follow the standard Sametime client connection processes when connecting to the Sametime server.

Note: For detailed information about the standard Sametime client connection processes, see the Meeting Room and Broadcast client connection processes section earlier in this chapter.

To illustrate this point, the Meeting Room client connection process that occurs when the "Enable Reverse Proxy Discovery on the client" setting is selected is summarized below.

1. Upon loading in a user’s Web browser, the Sametime Meeting Room client attempts a direct TCP/IP connection to the Sametime server.

   If the direct TCP/IP connection attempt fails, the Meeting Room client continues with the connection process as described below.

   Note Step 1 is part of the standard Sametime client connection process.
2. If the user's Web browser detects the existence of a forward SOCKS proxy server, the Meeting Room client will attempt the TCP/IP connection through the forward SOCKS proxy server to the Sametime server.

If the TCP/IP connection through the SOCKS proxy server is not successful, the Meeting Room client continues with the connection process as described below.

**Note** Step 2 is part of the standard Sametime client connection process.

3. If the TCP/IP connection attempt is not successful, the Meeting Room client attempts to detect the reverse proxy server.

If the reverse proxy server is detected, the Meeting Room client attempts to connect to the Sametime server through the reverse proxy server using HTTP tunneling. The client programationally detects the address of the reverse proxy server. No client-side configurations are required to enable the Sametime client to detect the reverse proxy server.

**Note** Step 3 represents the major difference in the connection process that occurs when the "Enable Reverse Proxy Discovery on the client” setting is selected.

4. If the reverse proxy server is not detected, the Sametime clients will still attempt to connect to the Sametime server using HTTP tunneling but the connection attempts will not be made to the reverse proxy server.

**Note:** These HTTP-tunneled connection attempts are part of the standard Sametime client connection processes as discussed in the meeting Room and Broadcast client connection processes section earlier in this chapter.

These connection attempts enable Sametime clients that do not connect to the Sametime server through the reverse proxy server to establish HTTP-tunneled connections to the Sametime server.

**Notes about Sametime client connectivity through a reverse proxy server**

This section provides additional notes about Sametime client connectivity through a reverse proxy server.

Generally, there are no client-side configurations required to enable a Sametime Meeting Room client, Sametime Broadcast client, or Sametime Connect for browsers client to connect to a Sametime server through a reverse proxy server.

If the administrator has selected the "Enable reverse proxy discovery on client" setting and specified the "Affinity ID" setting in the Sametime Administration Tool on the Sametime server, the Sametime clients should be able to programationally detect the presence of the reverse proxy server and connect to the Sametime server through the reverse proxy server.

If these clients must connect to the reverse proxy server through a forward (or client-side) HTTP or SOCKS proxy server, the connectivity settings (address and port) of the forward proxy server should be specified the locations noted below:

- If the Sametime client runs in a Web browser that operates with the Sun Microsystems Java Virtual Machine (1.4.2), the forward proxy server address and port are specified in the Sun Microsystems Java Plug-in Control Panel on the user’s machine. (The Java Plug-in Control Panel is available from the user’s Windows Control Panel).

- If the Sametime client runs in a Web browser that operates with the native Microsoft Virtual Machine (VM), the forward proxy server address and port are specified in the proxy configuration settings of the Web browser.
Note the following about using Sametime Connect for browsers with a reverse proxy server:

- The Sametime Connect for browsers client loads in the user’s Web browser with either the "Use my Java Plug-in settings" option or the "Use my Internet Explorer Browser settings" option selected by default in the Options-Preferences-Sametime Connectivity tab. User’s should not change this default setting when operating with a reverse proxy server. These connectivity settings ensure the client will make either a direct connection to the Sametime server or connect through a forward proxy server if one is defined in the Web browser connectivity settings or Java Plug-in as noted above.

- The Sametime Connect for browsers client includes a "Host name" and "Port" setting in the Options-Preferences-Sametime Connectivity tab. The values in these settings are ignored when the Sametime server is configured to operate with a reverse proxy server. (In a normal Sametime deployment, these settings specify the Host name of the Sametime server to which the client should connect and the port number on which the Sametime server listens for connections from Sametime Connect clients).
Chapter 6. Configuring the Community Services

This chapter describes the Community Services administration settings and features.

The Community Services administration settings:
• Control the number of user names that appear on a page in the “add to contact list” feature in the Sametime Connect client user interface.
• Control the time intervals in which Community Services receive updates from the Directory to maintain current lists of users and servers in the Sametime Community.
• Control the maximum number of connections to Community Services.
• Show or hide the links in the IBM Lotus Sametime server user interface that enable users to download the Windows or Java versions of Sametime Connect. The Java version of Sametime Connect is referred to as “Sametime Connect for browsers” and the Windows version of Sametime Connect is referred to as “Sametime Connect for the desktop.”
• Enable or disable the following features in Sametime Connect:
  – File transfer (If this feature is enabled, the administrator can set a maximum file size for transferred files)
  – The send announcements feature
  – Automatic login
• Force a name entry prompt to appear when the ACL settings of the Sametime Meeting Center database allow anonymous access. This name entry prompt allows each user to enter a name that is displayed in the presence list available in the Sametime Meeting Center or other database enabled with Sametime technology. The administrator can also specify whether anonymous users can search or browse entries in the directory.
• Enable or disable the Sametime server’s ability to accept authentication tokens generated by the Secrets and Tokens databases. You can disable this feature if all of the servers in your environment are Sametime 3.0 or higher servers.

This chapter also discusses:
• Enabling the Sametime Connect for browsers client to operate in kiosk mode if multiple users must access this client from a single Sametime server.
• Deploying a Community Services multiplexer on a separate machine to improve the performance of the Community Services.
• Deploying the Macintosh Sametime Connect client for the desktop client.

About the Community Services

The IBM Lotus Sametime server Community Services support all presence (or awareness) and text chat activity in a Sametime community. Any Sametime client that contains a presence list must connect to the Community Services. The Community Services clients include the Sametime Connect client and the Participant List and chat components of the Sametime Meeting Room client.

Basic functionality supported by the Community Services includes:
• Handling client login requests.
• Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or a HTTP, HTTPS, or SOCKS proxy server. Community Services clients connect to the Community Services multiplexer component, which can be deployed on a separate machine from the core Sametime server.

• Providing directory access for user name search and display purposes.

• Providing directory access to compile lists of all Sametime servers and users in the community.

• Dissemination of presence and chat data to all users connected to Community Services.

• Maintenance of privacy information for online users.

• Interacting with the Meeting Services to create meetings in which collaborative activities supported by the Community Services, Meeting Services, and Audio/Video Services are available.

• Handling connections from the Community Services on other Sametime servers when multiple servers are installed. Server-to-server connections for the Community Services occur on default TCP/IP port 1516.

Note: Port 1516 is also used by the Meeting Services. In a multiple server environment, port 1516 must be open between two Sametime servers to enable a single Sametime meeting to be simultaneously active on both Sametime servers. This functionality is sometimes called “invited servers.” For more information, see Advantages of a single meeting on multiple servers.

• Logging of Community Services events to the Sametime log (stlog.nsf).

• Enabling the administrator to force a name entry prompt to appear when the ACL settings of the Sametime Meeting Center database (or any other database that includes Sametime technology) allow anonymous access. This name entry prompt ensures that the presence list in the Sametime database can display a unique name for the user.

• Capturing transcripts of chat conversations that occur on the Sametime server for later retrieval. Developers must implement a chat logging feature to capture and retrieve transcripts of chat conversations.

**Community Services configuration settings**

Community Services support all online presence (or awareness), instant messaging, and chat features and activities available with Sametime. Presence, instant messaging, and chat features exist in the Sametime Connect client and the Sametime Meeting Room client Participant List. Developers can also use the Sametime toolkits to implement presence and chat features in custom applications.

The Community Services configuration settings control the interaction of the Community Services with a Domino or LDAP directory and the maximum number of Community Services users allowed on the server.

The Community Services configuration settings also enable the administrator to control whether the Java or Windows version of Sametime Connect is available to end users. The Java version of Sametime Connect is called "Sametime Connect for browsers" in the end user interface while the Windows version is called "Sametime Connect for the desktop." The administrator also controls whether the automatic login feature of Sametime Connect for browsers is available to end users.
**Note:** You can also create a Community Services server cluster to support failover and load balancing for the Community Services or enable the Session Initiation Protocol (SIP) Gateway functionality to support instant messaging between two different SIP-enabled communities. For more information, see [Creating Sametime server clusters](#) or [Enabling the Session Initiation Protocol (SIP) Gateway](#).

You can access the Community Services configuration settings from the Sametime Administration Tool by selecting Configuration - Community Services.

The three types of Community Services configuration settings are:

### General settings

The General settings allow the administrator to:

- Control the number of entries on each page in the dialog boxes that show names in the directory.
- Control how often to poll for new names added to the Sametime Community directory.
- Control how often to poll for new servers added to the Sametime Community.
- Control the maximum number of user and server connections to the Community services.
- Allow users to authenticate using either LTPA or Sametime Tokens.
- Display the "Download Sametime Connect for the Desktop" link.

### Server Features settings

The Server Features settings allow the end user to determine which Community Services options are available for end users. The administrator can:

- Enable or disable the end-user ability to transfer files.
- Enable or disable the end-user ability to send announcements.

### Sametime Connect for browsers settings

The administrator can use the Community Services configuration settings to determine which options are available in the Java version of Sametime Connect ("Sametime Connect for browsers"). These settings do not affect the Windows version of Sametime Connect ("Sametime Connect for the desktop"). To change the settings for "Sametime Connect for the desktop," you must use the Sametime Client Packager.

The Community Services configuration settings for "Sametime Connect for browsers" allow you to:

- Enable or disable the end-user ability to save the user name, password, and proxy information when logging in to the Community Services from Sametime Connect. This capability controls whether users can use the automatic login feature of Sametime Connect.
- Display the "Launch Sametime Connect for browsers" link.

The Sametime Administration Tool also allows you to send a Message from the administrator to all users logged in to the Community Services.
Community Services connectivity settings

For information about the ports used by the Community Services and the available connectivity options, see [Community Services Network settings].

Community Services server clusters

You can create a Community Services server cluster to support failover and load balancing for a large community of Community Services users. For more information on creating a Community Services cluster, see [Overview of Community Services clustering].

Number of entries on each page in dialog boxes that show names in the directory

The "Number of entries on each page in dialog boxes that show names in the directory" setting controls the number of user and group names that display when a user browses the Domino Directory on the Sametime server.

Note: If you have configured the Sametime server to connect to an LDAP server, see [Using LDAP with the Sametime server] for information about using directory browsing features with an LDAP directory.

An end user can browse the names and groups listed in the Domino Directory on the Sametime server (or Domino Directories available through Directory Assistance) when performing the following operations:

- Adding users or groups to the contact list (or presence list) in the Sametime Connect client
- Adding users or groups to a privacy list (or Who Can See If I Am Online list) in the Sametime Connect client
- Restricting meeting attendance when creating a meeting in the Sametime Meeting Center

When an end user browses the names and groups in the directory, the directory entries (names and groups) are listed on "pages" in a dialog box. The "Number of entries on each page in dialog boxes that show names in the directory" setting controls the number of entries that appear on each of these pages in the dialog box. The end user can select entries from these pages when adding users to the contact list, a Privacy list, or meeting attendance Restrictions list. The default is 100 entries per page, the minimum is five entries, and the maximum is 1440 entries. It is best to use a setting between 100 and 200 entries. Higher settings cause more data to be transmitted on the network when a user browses the Domino Directory.

To change the number of directory entries that appear on each page in the end-user dialog boxes:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. In the "Number of entries on each page in dialog boxes that show names in the directory" field, enter the number of entries that you want to appear on each page.
5. Click the Update button and restart the server for the change to take effect.
How often to poll for new names added to the Sametime Community directory

The Sametime Community Services maintain a cache that contains information about the users and groups in the community. The user information that is stored in this cache is gathered from the Domino or LDAP directory. This cache must be updated (or refreshed) periodically to ensure that users who have recently been added to a directory can be displayed in the presence lists of all Sametime clients.

The "How often to poll for new names added to the Sametime Community directory" setting controls how frequently the cache of user names maintained by Community Services is updated with new information from the Domino or LDAP directory. The update occurs only if changes are made to the directory during the update interval. The default setting is 60 minutes, the minimum setting is 5 minutes, and the maximum setting is 1440 minutes.

Note: Low settings result in frequent updates from the directory and can adversely affect the performance of the server. Lower settings also cause more data to be transmitted on the network.

To change how frequently the Domino or LDAP directory is polled for new user names (and how often the cache is updated):
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. In the "How often to poll for new names added to the Sametime Community directory" field, specify a new number to control the time interval (in minutes) in which polling (and updates, if necessary) will occur.
5. Click the Update button and restart the server for the change to take effect.

How often to poll for new servers added to the Sametime Community

If you have installed more than one Sametime server, the Community Services on each Sametime server must maintain a list of all other Sametime servers in the Sametime Community. Community Services uses this list to ensure that users who have different home Sametime servers or different home clusters can see each other in presence lists and communicate through instant messaging and chat.

Note: For more information on multiple Sametime server environments, see Advantages of using multiple Sametime servers. For more information about Community Services clusters, see Overview of Community Services clustering.

Before installing a Domino server, you must register the Domino server by creating a Server document for it in the Domino directory. Each Server document includes an "Is this a Sametime server?" field that identifies the server as a Sametime server. Community Services uses these fields to build a list of Sametime servers in the domain (or community). The Sametime Administration Tool includes a setting that allows the administrator to control the time interval in which the Community Server receives an updated list of all Sametime servers from the Domino Directory. The default setting is 60 minutes, the minimum setting is five minutes, and the maximum setting is 1440 minutes.
To change how frequently the Domino Directory is polled to detect a new Sametime server:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. In the "How often to poll for new servers added to the Sametime Community" field, specify the time interval in minutes in which polling (and updates, if necessary) will occur.
5. Click the Update button and restart the server for the change to take effect.

**Maximum user and server connections to the Community server**

The administrator can specify the maximum number of connections allowed to Community Services. The connections include both Sametime client connections and Sametime server-to-server connections.

A client connection (or Community Services login) occurs when a user starts the Sametime Connect client or joins a meeting with the Sametime Meeting Room client.

The limit is 20,000 connections. Generally, a server that meets the minimum system requirements can support 8,000 TCP/IP connections. To support limits higher than 8,000 connections, use servers with high-level processing capabilities of at least 512 MB of RAM, a 10 MB or 100 MB network card, and dual processors.

**Note:** You can deploy a Community Services multiplexer on a separate machine from the Sametime server. In this scenario, you cannot use the "Maximum user and server connections to the Community server" field in the Sametime Administration Tool to specify the maximum number of connections to the Community Services. When a Community Services multiplexer is deployed on a different machine than the Sametime server, you must use the VPMX_CAPACITY= setting in the Sametime.ini file on the multiplexer machine to specify the maximum number of connections. For more information, see [Deploying a Community Services multiplexer on a separate machine](#).

Server-to-server connections occur when the administrator has installed multiple Sametime servers and different home Sametime servers are specified for users. When users have different home Sametime servers, two users can be connected to Community Services on two different Sametime servers. A server-to-server connection must be established to enable these users to see each other in presence lists and chat with each other.

To change the maximum user and server connections to the Community Services:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. In the "Maximum user and server connections to the Community server" field, specify the maximum number of connections allowed to the Community Server.
5. Click the Update button and restart the server for the change to take effect.
Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)

When the "Allow users to authenticate using either LTPA or Sametime Tokens" option is selected in the Community Services-Configuration settings of the Sametime Administration Tool, the Sametime server accepts authentication tokens generated by both the Domino Single-Sign On (SSO) feature and the Secrets and Tokens databases on the Sametime server. This option is selected by default.

When the "Allow users to authenticate using either LTPA or Sametime Tokens" option is not selected, the Sametime server accepts authentication tokens generated only by the Domino SSO feature (LTPA tokens).

The "Allow users to authenticate using either LTPA or Sametime Tokens" option must be selected when you require basic password authentication to the Sametime Meeting Center and the Sametime 7.0 server and Sametime 2.0 or 2.5 servers function as part of a single Sametime community.

The "Allow users to authenticate using either LTPA or Sametime Tokens" option can be disabled when you require basic password authentication to the Sametime Meeting Center and all Sametime servers in your environment are Sametime 3.0 servers or higher.

Note: By default, anonymous access is allowed to the Sametime Meeting Center and authentication by token is not enforced on the Sametime server.

For more information, see Authentication by token using LTPA and Sametime Tokens and Turning off anonymous access to the Sametime Meeting Center

Display the "Download Sametime Connect for the desktop" link

Sametime includes two versions of the Sametime Connect client: a standalone Windows application and a signed Java applet that runs in a user's Web browser. The standalone Windows application is called "Sametime Connect for the desktop." Use the "Display the 'Launch Sametime Connect for the desktop' link" setting to make the Windows version of Sametime Connect available or unavailable to end users.

Note: The Java version of Sametime Connect is called "Sametime Connect for browsers." The availability of this client is controlled from the Display the "Launch Sametime Connect for browsers" link setting. By default, both Sametime Connect for browsers and Sametime Connect for the desktop clients are available to end users. A Macintosh version of the Sametime Connect client is provided with the Sametime server, but not available by default. For more information, see Deploying the Macintosh Sametime Connect client for the desktop.

End users download and install Sametime Connect for the desktop by accessing the Sametime server home page with a Web browser, selecting the "Download" link, and selecting the "Download the Sametime Connect client" link from the Download page.

The administrator uses the "Display the 'Download Sametime Connect for the Desktop' link" setting to show or hide the "Download the Sametime Connect client" link on the Download page.
If the administrator disables the "Display the 'Download Sametime Connect for the desktop' link" setting, the "Download the Sametime Connect client" link is hidden on the Download page and end users are unable to download and install Sametime Connect for the desktop. All other references to "Sametime Connect for the desktop" are also hidden in the user interface when the administrator disables this setting.

To allow or prevent users from downloading and installing Sametime Connect for the desktop (the Windows version of Sametime Connect):

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. To allow end users to download and install Sametime Connect on their Windows desktops, place a check mark in the "Display the ‘Download Sametime Connect for the Desktop’ link" check box. Selecting this check box causes the "Download the Sametime Connect client" link to appear on the Download page on the Sametime server.

To prevent end users from downloading and installing Sametime Connect on their Windows desktops, clear the check mark from the "Display the ‘Download Sametime Connect for the Desktop’ link" check box. When this setting is disabled, the "Download the Sametime Connect client" link is hidden from the end users.

5. Click the Update button and restart the server for the change to take effect.

**Allow users to transfer files to each other**

Community Services allow end users to transfer files to each other over the network while using Sametime Connect or attending a Sametime meeting. The administrator can enable or disable this feature. When you enable this feature, both authenticated and anonymous users can transfer files.

The file transfer feature does not work with Sametime Links. For more information about Sametime Links, see the IMWC Directory and Database Access Toolkit documentation available from IBM DeveloperWorks (http://www.ibm.com/developerworks/lotus/products/instantmessaging/). Follow the link for "Toolkits and Drivers."

**Caution** Computer viruses can be spread through transferred files. To protect against this possibility, users should have current anti-virus software installed. The anti-virus software real-time protection settings should be enabled and set to scan all files.

**Enabling file transfer**

To enable the file transfer feature:

1. Select the "Allow users to transfer files to each other" check box on the Configuration - Community Services tab in the Sametime Administration Tool. Enabling this feature might increase the amount of network bandwidth consumed by Sametime users. This functionality is similar to allowing users to attach files to an e-mail and transmit these files on the network.

2. Enter a maximum file size for transferred files, in KB. The default maximum size is 1000 KB. Keep in mind that the larger this number, the more network bandwidth it is possible for Sametime users to consume with file transfers.
When you select this check box, a user who is sending a file can:

- Send a file to anyone who is online (with active or away status) in Sametime Connect or in an online meeting. Users cannot send files to people whose status is offline or “do not disturb,” and audience members in a broadcast meeting cannot send or receive files. The transferred file must be within the size limit set by the administrator in step 2 above.
- Send a file to only one person at a time.
- Enter a description of the file.
- Receive notification that the file has been sent.
- Receive notification that the other user has accepted or rejected the file.

Note: Users must send files to other users in the Sametime Community. It is not possible to send a file to someone in an external community using the SIP Gateway functionality.

The person receiving the file can:

- Accept or reject the file.
- See how large the file is before sending it.
- Save and open the file on his or her computer.

Disabling file transfer
To disable the file transfer feature for authenticated users, clear the "Allow authenticated users to transfer files to each other" check box on the Configuration - Community Services tab in the Sametime Administration Tool. When you disable this feature, all references to file transfer are hidden from users in the end user interface.

Allow users to send announcements
Community Services allow end users to send unencrypted announcements to others who are online in the Sametime Community. The administrator can enable or disable this feature.

Note: Users of Sametime Links can also receive and respond to announcements. For more information about Sametime Links, refer to the Sametime Software Development Kit documentation.

Allowing users to send announcements
To allow users to send announcements, select the "Allow users to send announcements" check box in the Configuration - Community Services settings of the Sametime Administration Tool.

When you enable this feature end users can:

- Send unencrypted announcements to anyone who is online in Sametime Connect or in an online meeting. (To receive an announcement, a user must be online, and in either active or away status. Users who are offline or have a status of "do not disturb" do not receive announcements.)

Note: Users must send announcements to other users in the Sametime Community. It is not possible to someone in an external community using the SIP Gateway functionality.
- Allow the recipients of the announcement to respond to the announcement, or prevent them from responding.
**Note:** If a user who is receiving the announcement is logged in from more than one Community Services application (for example, if a user is in an online meeting and logged in with Sametime Connect), the announcement will only be sent to that user once.

**Preventing users from sending announcements**

To prevent users from sending announcements, clear the "Allow users to send announcements" check box in the Configuration - Community Services settings of the Sametime Administration Tool. When you disable this feature, all menu items and toolbar buttons for sending announcements are removed from the end user interfaces of both versions of Sametime Connect ("Sametime Connect for the desktop" and "Sametime Connect for browsers.")

**Allow Connect users to save their user name, password, and proxy information (automatic login)**

Sametime Connect includes a feature that saves a user’s login information and logs that user into the Connect client automatically. The administrator can enable or disable this setting in the Java version of Sametime Connect ("Sametime Connect for browsers") in the Community Services configuration settings of the Sametime Administration Tool.

**Note:** You must use the Sametime Client Packager to enable or disable this feature in "Sametime Connect for the desktop.” For more information about the Sametime Client Packager, see the Lotus Sametime Installation Guide (stinstall.nsf or stinstall.pdf).

**Enabling automatic login**

To enable automatic login for "Sametime Connect for browsers,” select the "Allow Connect users to save their user name, password, and proxy information (automatic login)” check box in the Configuration - Community Services options of the Sametime Administration Tool.

When you enable the automatic login feature, a user can select an "Automatically log me on” option when starting Sametime Connect. If the user selects this option, the user name, password, and connectivity information for the user are stored on the Sametime server. The next time the user starts Sametime Connect, this information is automatically retrieved from the server. This feature prevents users from having to enter the user name and password each time Sametime Connect is started.

**Disabling automatic login**

Organizations that require strict security might have policies that prevent storing user names and passwords on the server. If you do not want the user names and passwords stored on the server, you should disable the automatic login feature of Sametime Connect. When automatic login is disabled, all automatic login features are hidden in the user interface of the Sametime Connect client and automatic login is unavailable to the end users.

To disable the automatic login feature for "Sametime Connect for browsers,” clear the "Allow Connect users to save their user name, password, and proxy information (automatic login)” check box in the Configuration - Community Services options of the Sametime Administration Tool.
Display the "Launch Sametime Connect for browsers" link

Sametime includes two versions of the Sametime Connect client: a standalone Windows application and a signed Java applet that runs in a user's Web browser. The Java version of Sametime Connect is called "Sametime Connect for browsers." Use the "Display the 'Launch Sametime Connect for browsers' link" setting to make the Java version of Sametime Connect available or unavailable to end users.

**Note:** The version of Sametime Connect that runs as a standalone Windows application is called "Sametime Connect for the desktop." The availability of this client is controlled from the "Display the 'Download Sametime Connect for the desktop' link" setting. By default, both Sametime Connect for browsers and Sametime Connect for the desktop clients are available to end users. A Macintosh version of the Sametime Connect client is provided with the Macintosh server, but not available by default. For more information, see Deploying the Macintosh Sametime Connect client for the desktop.

End users start Sametime Connect for browsers by accessing the Sametime server home page with a Web browser, dragging the cursor over the "Launch Sametime Connect" option and selecting the "Launch Sametime Connect for browsers" link. The Web page containing Sametime Connect for browsers is loaded to the user's Web browser. Sametime Connect for browsers establishes connections with the Community Services using the process described in the Sametime Connect client connection process.

The administrator uses the "Display the 'Launch Sametime Connect for browsers' link" setting to show or hide the "Launch Sametime Connect for browsers" link on the Sametime home page. If the administrator disables this setting, the "Launch Sametime Connect for browsers" link is hidden on the Sametime server home page and end users cannot use Sametime Connect for browsers. All other references to Sametime Connect for browsers are also hidden in the end user interface when this setting is disabled.

**Note:** When both versions of the Sametime Connect client are available to end users, the link on the server home page that launches the Java version of Sametime Connect reads "Launch Sametime Connect for browsers." If the administrator makes only Sametime Connect for browsers available to end users, the link reads "Launch Sametime Connect."

To allow or prevent user access to Sametime Connect for browsers:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. To allow end users to use the Java version of Sametime Connect, place a check mark in the "Display the 'Launch Sametime Connect for browsers' link" check box. Selecting this check box causes the "Launch Sametime Connect for browsers" link to appear on the Sametime server home page.

To prevent end users from using the Java version of Sametime Connect, clear the check mark from the "Display the 'Launch Sametime Connect for browsers' link" check box. When the check mark is cleared from this setting, the "Launch Sametime Connect for browsers" link is hidden from the end users.

5. Click the Update button and restart the server for the change to take effect.
Anonymous Access Settings for Community Services

Anonymous access is allowed to the Sametime Meeting Center database (stconf.nsf) on the Sametime server by the default Access Control List (ACL) settings of the database. When the ACL settings of a database allow anonymous access, a user is not authenticated and is not required to enter a user name and Internet password when accessing the database.

**Note:** The "Anonymous users can participate in meetings or enter virtual places" setting in the Configuration - Community Services - Anonymous Access settings of the Sametime Administration Tool must also be selected to allow an anonymous user to enter the Sametime Meeting Center. This setting is selected by default.

The Community Services Anonymous Access Settings in the Sametime Administration Tool allow the administrator to force a name entry dialog box to appear when anonymous access is allowed by the ACL settings of the Sametime Meeting Center (or any other database that includes Sametime technology). The name entry dialog box accepts any name the user provides and has no security functions. The name entered by the user is for presence list display purposes only. The display name serves to uniquely identify the user in any presence list in the Sametime Meeting Center or other database enabled with Sametime technology.

If you allow anonymous access to the Sametime Meeting Center (or other Sametime database that includes a presence list), and you do not force this name entry dialog box to appear, every user present in the meeting or database is listed as "Anonymous" in the presence list.

**Note:** To force users to authenticate (enter a user name and password that is verified against entries in a directory) when accessing a database, change the database ACL settings. For more information, see Using database ACLs for identification and authentication and Basic password authentication and database ACLs.

The administrator can also specify the level of access that anonymous users have to the directory. These administrative settings control an anonymous user’s ability to search for entries in a directory or browse a list of all entries in the directory.

The Anonymous Access settings include:

- **Anonymous users can participate in meetings or enter virtual places**
- **Users of Sametime applications (databases such as stconf.nsf or Web sites) can specify a display name so that they do not appear online as "Anonymous."**
  - Default domain for anonymous users
  - Default name
- **Directory Searching and Browsing options.**
  - Users cannot search or browse the Directory
  - Users can type names (resolve users and groups) to add them to an awareness list
  - Users can browse the directory (see a list of names) or type names (resolve users and groups)
  - Users can browse the directory to see group content and names, or type names (resolve users and groups)
Anonymous users can participate in meetings or enter virtual places

The "Anonymous users can participate in meetings or enter virtual places" setting must be selected to enable an anonymous user to attend a meeting in the Sametime Meeting Center (stconf.nsf) or access any other database that includes Sametime functionality (such as a presence list).

Note: The ACL settings of the Sametime Meeting Center (stconf.nsf) must also allow anonymous access to enable anonymous users to attend meetings in the Sametime Meeting Center.

When the "Anonymous users can participate in meetings or enter virtual places" setting is selected, the administrator can use the following settings in the Configuration - Community Services - Anonymous Access tab of the Sametime Administration Tool to control how the anonymous users enter display names when accessing the Sametime Meeting Center.

- Users of Sametime applications (databases such as stconf.nsf or Web sites) can specify a display name so that they do not appear online as anonymous.
- Default domain name for anonymous users
- Default name

Note: The settings listed above do not take effect unless the "Anonymous users can participate in meetings or enter virtual places" setting is selected.

About "virtual places"

A "virtual place" is a programming concept. An example of a virtual place is an online meeting.

Users can enter a virtual place and have awareness of other users in the same virtual place. For example, a user can enter a Sametime meeting and use the Participant List of the Meeting Room client to have awareness of other users who are attending the same meeting (or who are in the same "virtual place"). This capability is sometimes called "Place-based awareness."

Place-based awareness differs from "Community-wide awareness." In the example above, the Participant List in the Sametime Meeting Room client displays the names of users who are attending the meeting, but does not display members of the Sametime community who are online, but not attending the meeting. With Community-wide awareness, users can have awareness of any user in the Community (any user entered in the directory) who is online. Sametime Connect provides users with Community-wide awareness functionality. Anonymous users are not allowed to have Community-wide awareness in any Sametime clients.

The Sametime Software Development Kit provides developers with the capability to build programs that create virtual places. The "Anonymous users can participate in meetings or enter virtual places" setting also controls the ability of anonymous users to enter virtual places created by custom-built applications created with the Sametime Software Development Kit.

For more information on virtual places, see the the IMWC Directory and Database Access Toolkit documentation available from IBM DeveloperWorks (http://www.ibm.com/developerworks/lotus/products/instantmessaging/). Follow the link for "Toolkits and Drivers."
Users of Sametime applications can specify a display name so that they do not appear online as "anonymous."

The "Users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting enables an anonymous user to enter a unique display name when accessing a database or application (such as the Sametime Meeting Center) that includes a Sametime presence list. This display name allows the anonymous user to be individually identified in any presence lists in the Sametime application.

The following conditions are required to allow anonymous users to access a Sametime application or database. Both of these conditions exist by default following a Sametime server installation:

- The **ACL settings of the database** (for example, the Sametime Meeting Center) must allow anonymous access.
- The **"Anonymous users can participate in meetings or enter virtual places"** setting in the Configuration - Community Services - Anonymous Access settings of the Sametime Administration Tool must be selected.

When both of the above conditions are true, you can select the "Anonymous users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting to force a name entry dialog box to appear when an anonymous user enters the Sametime Meeting Center (or other Sametime database that includes a presence list).

The name entry dialog box that appears enables a user to enter a name so that the user can be individually displayed in the Sametime Meeting Room Participant List (or any other presence list in a Sametime database). The name entry dialog box accepts any name that the user enters; the name is for display purposes only in the presence list. The user is not authenticated.

If the ACL settings of a Sametime database allow anonymous access and the "Anonymous users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting is not selected, users are not required to enter a user name when attending a meeting. Every meeting participant is displayed as "Anonymous" in the Sametime Meeting Room Participant List (or other presence list). Meeting participants will be unable to distinguish one participant from another in the presence list.

**Note:** For information on the ACL settings required to prevent anonymous users from accessing a Sametime database, see "Anonymous access and the Sametime Meeting Center".

If the "Users of Sametime applications can specify a display name..." setting is selected, you can also edit the "Default domain for anonymous users" and "Default name" settings described below.

**Default domain for anonymous users**

If the "Users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting is selected, you are forcing a name entry dialog box to appear when a user accesses a Sametime database (such as stconf.nsf) that has ACL settings that allow anonymous access.

The "Default domain for anonymous users" setting enables a domain name to be automatically appended to the name entered by the user at the name entry dialog box.
For example, if the "Default domain for anonymous users" setting contains the entry "/Guest," and a user enters "John Smith" at the name entry dialog box, the user’s name appears as "John Smith/Guest" in the Meeting Room Participant List.

**Default name**

If the "Users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting is selected, you are forcing a name entry dialog box to appear when a user accesses a Sametime database (such as stconf.nsf) that has ACL settings that allow anonymous access.

The "Default name" setting enables you to specify a name to appear by default in the name entry dialog box.

For example, if the "Default name" setting contains the entry "User," the first person entering a meeting sees "User" displayed by default in the user name field of the name entry dialog box. If the person accepts the default and enters the meeting, the person is identified as "User 1" in any Participant List or presence list in the database.

For each person who accepts the default name, the number that follows the default name is incremented by one. For example, the next two users who accept the default name setting in the name entry dialog box are identified as "User 2" and "User 3" in any Participant List or presence list in the database.

**Directory Searching and Browsing options**

In some cases, the administrator might need to specify the level of access that an anonymous user of a database enabled with Sametime technology has to the directory.

For security purposes, the administrator can limit an anonymous user’s ability to view names in the directory. The "Directory Searching and Browsing" options might be used to prevent anonymous users from browsing all names in a directory or searching for names in the directory. Also, applications that are custom-built by Sametime developers using the Sametime Software Development Kit might require specific Community Services "Directory Searching and Browsing" settings configurations to enable the custom applications to function properly.

**Note:** The term "anonymous user" refers to a user who is not authenticated when accessing a database enabled with Sametime technology. The ACL settings of the database determine whether a user is authenticated or allowed to access the database anonymously.

The four "Directory Searching and Browsing" options are described below.

**Users cannot search or browse the directory**

If this option is selected, anonymous users cannot search or browse the directory.

**Users can type names (resolve users and groups) to add them to an awareness list**

If this option is selected, anonymous users can type text in an end-user search interface to search for person or group entries in the directory. However, users cannot view (or browse) a list containing all entries in the directory. Users might perform such searches to add users to a presence list.
Users can still browse the directory when scheduling meetings in the Sametime Meeting Center. This setting does not affect a user’s ability to browse the directory when creating a meeting in the Sametime Meeting Center.

**Users can browse the directory (see a list of names) or type names (resolve users and groups)**

If this option is selected, anonymous users can type text in an end-user search interface and search for group or person entries in the directory. Anonymous users can also browse lists that contain all entries in the directory. When this option is selected, anonymous users can see all group and name entries in the directory, but cannot see the content of a group entry (the list of names within a group entry).

**Note:** If Sametime is configured to connect to an LDAP server, users cannot browse the LDAP directory on the LDAP server.

Users can browse the directory when scheduling meetings in the Sametime Meeting Center. This setting does not affect a user’s ability to browse the directory when creating a meeting in the Sametime Meeting Center.

**Users can browse the directory to see group content and names, or type names (resolve users and groups)**

If this option is selected, anonymous users have all searching and browsing privileges described for the "Users can browse the directory (see a list of names) or type names (resolve users and groups)” setting above. In addition, users can search and browse within group entries in the directory and access the user and group names that are specified within group entries in the directory.

Users can browse the directory and examine the contents of groups in the directory when scheduling meetings in the Sametime Meeting Center. This setting does not affect a user’s ability to browse the contents of groups when creating a meeting in the Sametime Meeting Center.

---

### Allowing users to control the default screen location and size of chat windows

When a Sametime server is in its default state, end users cannot control the default screen location or screen size of chat windows. For example, when a Sametime Connect user initiates a chat session with another user, the chat window always pops up immediately to the left of the Sametime Connect window.

The administrator can configure a Sametime server so that users can determine the screen location and size that a chat window will have when the window first pops up on the user’s screen.

**Note:** This configuration must be performed on a user’s "home" Sametime server for the user to have access to this feature. For more information about the home Sametime server, see [Community Services connectivity and the home Sametime server](#).

When the administrator has configured a user’s home Sametime server in this way, the end user can perform the following actions to control the default screen location and size of chat windows:

1. An end user initiates a chat session with another user from the Sametime Connect client. The chat window pops up immediately to the left of the Sametime Connect client.
2. The end user moves the chat window to the upper-left corner of the screen (or any other desired screen location) and resizes the chat window.

3. The end user selects the "Set dialog as default" item from the "Options" menu in the chat window.

After the user has performed these actions, the chat window will always pop up at the screen location and size that it has at the time the user selects the "Set dialog as default" menu item. The chat window pops up at this location and size any time the user initiates a chat session with another user or another user initiates a chat session with this user.

After the user sets a default screen location and size for the chat window, the user has the following options for controlling chat window behavior:

• The user can move the chat window from the selected default location without changing the default location. For example, the user can move the chat window from the upper-left corner of the screen to the lower-right corner of the screen. The chat window will remain positioned in the lower right corner of the screen for the remainder of the chat session (unless the user moves it again).

  When the user starts a new chat session with a different user, the initial chat window for the new chat session will pop up at the user-defined default location (the upper-left corner of the screen), not the location to which the screen was moved in the previous chat.

• The user can move the chat window from the selected default location and specify a new default location. For example, the user can move the chat window from the upper-left corner of the screen to the lower-right corner and select the "Set dialog as default" menu item. The lower-right corner of the screen becomes the new default screen location. The initial chat window for all subsequent chat sessions will pop up in the lower-right corner of the screen.

One-to-one chat windows and n-way chat windows

There are two different chat windows launched from Sametime clients: "one-to-one" chat windows and "n-way" chat windows. The default locations of these windows must be set separately.

A "one-to-one chat window" launches when one user engages one other user in a chat session. An "n-way chat window" launches when one user invites more than one other user to a chat session (an "n-way" chat session is any chat session consisting of three or more users).

A user must specify individual default locations for each of these chat windows. For example, if the user selects the "Set dialog as default" menu item while engaged in a one-to-one chat, this setting will only apply to the one-to-one chat window. The user must also select the "Set dialog as default" menu item while engaged in an n-way chat to set the default location of the n-way chat window. The default setting for the one-to-one chat window can be different than the default setting of the n-way chat window.

Note: This feature does not control the default location and size of the Meeting Room client window that appears when a user starts an instant meeting from Sametime Connect. This feature applies only to chat windows.
Enabling users to select the default location and size of chat windows

To enable users to select the default location and size of chat windows, the administrator must add an ST_FIXED_CHAT_SUPPORTED setting to the [Client] section of the Sametime.ini file on the Sametime server.

To enable users to select the default location and size of chat windows:

1. Use a text editor to open the Sametime.ini file on the Sametime server. The Sametime.ini file is located in the Sametime installation directory.
   
   **Note** Sametime installs into the same directory as the Domino server. The default Sametime installation directory is C:\Lotus\Domino.

2. The Sametime.ini file contains a [Client] section. At the bottom of the [Client] section, manually add the following setting by typing it into the Sametime.ini file:

   ST_FIXED_CHAT_SUPPORTED=1

   **Note** You can change the value of the setting above to zero to disable this feature. For example, ST_FIXED_CHAT_SUPPORTED=0 disables the feature.

3. Save and close the Sametime.ini file and restart the Sametime server.

After the administrator enables the feature and restarts the server, end users can use the 'Set dialog as default' setting in the Sametime Connect client to set the default locations of chat windows.

---

Prohibiting logins from insecure clients to the server

Earlier versions of the Sametime client contain security vulnerabilities which could result in exposure of user credentials or message data. To ensure that information exchanged between Sametime clients and the server remain confidential, the server requires clients connecting to the server to be running the security level of a minimum client version. The server prevents logins from clients running Sametime versions earlier than the minimum version. By default, this minimum client version is set to Sametime 2.5. You can retain this default behavior, or change the security level to match a different client version.

In most cases it is best to prohibit earlier client versions from logging in to the server. If all clients connecting to the server are running Sametime 6.5.1 or higher, increasing the default security level to 6510 ensures that all information exchanged between client and server after the handshake is encrypted. By prohibiting logins from earlier versions of the Sametime client you ensure that all connections are encrypted.

However, if you must support older versions of the client, decrease the security level to enable logins from these earlier client versions. Setting a security level less than 6510 allows the server to accept non-encrypted connections.

To control how servers respond to login requests from different client versions, the sametime.ini and STsecurity.ini files provides settings that enable you to perform the following tasks:

- **Specify the security level (minimum client version) for the server**
- **Enable or disable logins from clients running versions that do not conform to the security level**
- **Configure the server to generate instant messages automatically in response to login requests from clients that do not conform to the security level**
Specifying the security level (minimum allowed client version)

Each server is configured to allow logins from a minimum client version, which defines the security level of the server. By default, the server allows logins from Sametime 2.5 and later clients. To specify a different security level, you must change the value of the VP_SECURITY_LEVEL setting in the sametime.ini file. You can specify a minimum client version of 3.1 or later, 3.0 or later, 2.5 or later, and so forth. After you specify a minimum version, you can then specify other settings to control how the server responds to login requests from client versions earlier than the specified minimum version.

To specify the security level for the server

1. Open the sametime.ini file in a text editor. By default the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\Sametime.ini.
2. In the [Config] section of the sametime.ini file, specify the minimum Sametime client version that can log in to the server by providing one of the following values for the VP_SECURITY_LEVEL setting:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0&lt;no zeros&gt;</td>
<td>Select this option to disable security filtering and allow logins from all clients regardless of version level.</td>
</tr>
<tr>
<td>20&lt;no zeros&gt;</td>
<td>Select this option to set the minimum client level to Sametime 2.0 clients and later. To determine the client level, the server detects whether the client uses the Diffie-Hellman public key agreement protocol to encrypt the user’s password. Any client that does not authenticate using the Diffie-Hellman method is determined to be a 1.5 client.</td>
</tr>
<tr>
<td>25&lt;no zeros&gt;</td>
<td>(Default) Select this option to set the minimum client level to Sametime 2.5. To determine the client level, after the client logs in using the Diffie-Hellman method, the server attempts to create a chat channel to the client. If the server successfully creates the chat channel, the client version is determined to be 2.5 or later.</td>
</tr>
<tr>
<td>30&lt;no zeros&gt;</td>
<td>Select this option to set the minimum client level to Sametime 3.0. The server determines the client version from information that the client sends during the handshake.</td>
</tr>
<tr>
<td>31&lt;no zeros&gt;</td>
<td>Select this option to set the minimum client level to Sametime 3.1. The server determines the client version from information that the client sends during the handshake.</td>
</tr>
<tr>
<td>6510&lt;no zeros&gt;</td>
<td>Select this option to set the minimum client level to Sametime 6.5.1. The server determines the client version from information that the client sends during the handshake.</td>
</tr>
<tr>
<td>70&lt;no zeros&gt;</td>
<td>Select this option to set the minimum client level to Sametime 7.0. The server determines the client version from information that the client sends during the handshake.</td>
</tr>
</tbody>
</table>

3. Save and close the file.

Effect of security level settings on server connections

The security level that you set on the server also determines the server versions from which the server accepts connections. When a Sametime server receives a connection request from another server, it uses information sent as part of the
server handshake to determine the security level of the requesting server. To prevent older clients from logging in to a Sametime 7.0 server by way of less secure servers running earlier versions of Sametime, the server blocks incoming connections from Sametime servers running versions earlier than the defined security level, and from Sametime servers that do not have a defined security level. By default, there is no security level defined for Sametime servers earlier than version 3.1.

To ensure interconnectivity with Sametime 3.0 and earlier servers, install the Sametime CF1 patch on these servers and configure the security level on all servers to a value consistent with the earliest version server in the community. For example, if the environment includes Sametime 2.0 servers, after you apply the CF1 patch on all version 3.0 and earlier servers, set the value of the VP_SECURITY_LEVEL setting on all servers to 20. Later, if you upgrade the 2.0 servers to a later version, increase the value of the setting to match the version of the upgraded servers.

If you choose not to apply the CF1 patch on Sametime 3.0 and earlier servers and want to allow earlier versions of the Sametime server to connect to a Sametime 7.0 server, disable security level checking on the 7.0 server by setting the value of VP_SECURITY_LEVEL to 0.

**Allowing logins from clients that do not conform to the security level**

By default, the server automatically logs out users who attempt to connect from clients of versions earlier than the specified minimum. To allow users with earlier clients to continue to access the server during the transition to the new server version, you can configure the server to allow logins from client versions earlier than the specified minimum.

Maintaining a flexible login policy is especially important in environments that include a large number of older Sametime clients. In such an environment, immediately enforcing a minimum client version can result in a high volume of help desk calls. To avoid locking users out of Sametime, give users several weeks to upgrade and use the VP_SECURITY_ALLOW_USER setting to enable servers to continue to accept logins from earlier client versions. After the deadline for upgrading passes, change the value of the setting to block logins from clients that do not meet the minimum security level.

**To specify whether the server allows logins from clients that do not conform to the security level**

1. Open the sametime.ini file in a text editor. By default the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\Sametime.ini.
2. In the [Config] section of the sametime.ini file, specify whether to allow logins from clients earlier than the minimum allowed version by providing one of the following values for the VP_SECURITY_ALLOW_USER setting:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(Default) Reject login attempts from clients of versions earlier than allowed by the VP_SECURITY_LEVEL setting.</td>
</tr>
<tr>
<td>1</td>
<td>Allow logins from all clients, regardless of version.</td>
</tr>
</tbody>
</table>
3. Save and close the file.
Configuring the server to send instant messages to clients that do not conform to the security level

You can use the VP_SECURITY_MESSAGE setting in the STSecurity.ini file to provide additional information to users who attempt to log in to the server from Sametime clients running versions earlier than what is allowed by the specified security level. This setting configures the server to automatically respond to login requests from clients that do not conform to the server’s security level by sending an instant message containing specified text. The message you specify functions as either a warning message or a disconnection notification, depending on whether the value of the VP_SECURITY_LEVEL setting allows logins from earlier clients. If the VP_SECURITY_LEVEL setting allows logins, use the text of the message to warn users that they need to upgrade and to explain how to obtain and install the client upgrade. If the VP_SECURITY_LEVEL setting does not allows logins, use the text of the message to explain why login was denied.

Note the following before you configure the settings in the STSecurity.ini file:

• All platforms - Double-byte characters are not allowed in the message text or sender name.

• All platforms - If you want to use accented characters (for example, Æ,é,ä,ñ) in the message text or sender name, you should use Notepad on a Windows client or server to edit the file. When you finish making your changes with Notepad, save the STSecurity.ini file as a UTF-8 file (select File-Save As And specify UTF-8 as the Encoding option, then save the file).

• IBM i5/OS platform only - It is recommended that you map a network drive to make the STSecurity.ini file on the server accessible from your workstation. Then you can run Notepad from your workstation and update the file directly on your ibm i5/OS server. (By default, the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\STSecurity.ini).

Alternatively, you can copy the file from the ibm i5/OS server to your client workstation using any convenient means (for example, dragging and dropping from ibm i5/os Navigator or FTP), edit the file on your workstation using Notepad, and then copy the updated file back to the server.

• IBM i5/OS platform only - When you have updated the file on your IBM i5/OS server, ensure that the file is owned by QNOTES. To update the file ownership, run the following command:
  CHGOWN OBJ('server_data_directory/stsecurity.ini') NEWOWN(QNOTES)

Use the following procedure to configure the server to send an instant message to users who attempt to log in from client versions earlier than the specified minimum.

To configure the server to send messages to clients that do not conform to the security level

1. Use a text editor to open the STSecurity.ini file. By default the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\STSecurity.ini.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>(Default) Do not send an instant message.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>text</td>
<td>Specifies the text of the instant message that is sent in response to login requests from clients that do not conform to the server's security level. If the VP_SECURITY_ALLOW_USER setting is set to 0 (reject logins from client versions earlier than the specified minimum), the text you provide serves as a disconnection notification. The server sends the specified text to the client as an instant message and then disconnects the client. If the VP_SECURITY_ALLOW_USER setting is set to 1 (allow logins from client versions earlier than the specified minimum), and you provide a value for VP_SECURITY_MESSAGE, the text you provide serves as a warning message. The server allows the login and then sends the specified text. You can use the message to provide users with information on upgrading. For example, you can include an address that specifies the location of a download site. After receiving the instant message with the address link, users can click the address link to open the link location. To include non-ASCII characters in the message text, save the STSecurity.ini file in UTF-8 format.</td>
</tr>
</tbody>
</table>

2. Save and close the file.

**Specifying the name to display in the title bar of instant messages sent by the server**

By default, when the server generates an instant message in response to a login from a client older than the minimum defined version, the instant message window does not identify the sender. Use the following procedure to specify the name to display in the title bar of the instant message window.

**To specify the name to display in the title bar of the instant message window**

1. Use a text editor to open the STSecurity.ini file. By default the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\STSecurity.ini.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>(Default) When the server sends an instant message in response to a login request from an older client, the title bar of the instant message window does not display a user name.</td>
</tr>
<tr>
<td>name</td>
<td>Specifies the user name to display in the title bar of the instant message window when the server sends an instant message in response to a login request from a client that does not conform to the server's security level.</td>
</tr>
</tbody>
</table>

2. Save and close the file.

**Chat Logging**

Programming tools are available to implement chat logging on a Sametime server. The chat logging feature can capture all chat conversations that occur on the Sametime server, including instant messages, chat conferences (chats involving more than two people), and Meeting Room chats. The text of these conversations is stored on the server and retrievable through the chat logging feature.

For more information on chat logging, see the the IMWC Directory and Database Access Toolkit documentation available from IBM DeveloperWorks.
Deploying a Community Services multiplexer on a separate machine

This section discusses the performance advantages and procedures associated with deploying a Community Services multiplexer on a separate machine from the Sametime server.

**Note:** This section discusses deploying a separate multiplexer in front of a Sametime server machine (or machines) that does not operate as part of a Community Services cluster. If you want to deploy a separate Community Services multiplexer to handle connections for a Community Services cluster, do not use the procedures in this section. To deploy a separate Community Services multiplexer in front of a Community Services cluster, see [Deploying separate Community Services multiplexers (optional)](http://www.ibm.com/developerworks/lotus/products/instantmessaging/) in the [Setting up a Community Services cluster without clustering the Meeting Services](http://www.ibm.com/developerworks/lotus/products/instantmessaging/) chapter of this documentation.

Each Sametime server contains a Community Services multiplexer (or MUX) component. The function of the Community Services multiplexer is to handle and maintain connections from Sametime clients to the Community Services on the Sametime server.

During a normal Sametime server installation, the Community Services multiplexer is installed with all other Sametime components on the Sametime server machine. The Sametime server CD provides an option to install only the Community Services multiplexer component. This option enables the administrator to install the Community Services multiplexer on a different machine than the Sametime server.

When the Sametime Community Services multiplexer is installed on a different machine than the Sametime server:

- The Sametime Connect clients connect to the Community Services multiplexer machine, not the Sametime server. This configuration frees the Sametime server from the burden of managing the live client connections; the multiplexer machine is dedicated to this task.
- The Community Services multiplexer maintains a single IP connection to the Sametime server. The data for all Community Services clients is transmitted over this single IP connection to the Community Services on the Sametime server.

In this scenario, the Community Services connection-handling load is removed from the Sametime server. The Sametime server does not need to employ system resources to maintain thousands of client connections. Removing the connection-handling load from the Sametime server ensures these system resources can be dedicated to other Community Services processing tasks.

The Community Services multiplexer machine dedicates its system resources to handling client connections but does not perform other Community Services processing. Distributing the Community Services workload between multiple servers in this way enables the Community Services on the Sametime server to handle a larger number of connections (users) and to function more efficiently.
Performance improvements with a separate multiplexer

If the Community Services multiplexer operates on the same machine as the Sametime server, the Sametime server can handle approximately 8,000 to 10,000 Community Services connections and also perform other Community Services processing tasks adequately.

However, if the Sametime server is not required to expend system resources to maintain client connections, the server can service approximately 100,000 connections. (The Sametime server is capable of processing the Community Services data that is passed over 100,000 connections if it does not have to maintain the connections themselves.)

Note: This estimate of 100,000 connections assumes that the Meeting Services and Broadcast Services are not in use. If the Sametime server is simultaneously supporting interactive meetings and broadcast meetings, it will support fewer Community Services users.

When a Sametime Community Services multiplexer is installed on a separate machine, the Community Services multiplexer can support approximately 20,000 live IP port connections. You can also deploy multiple Community Services multiplexers in front of a Sametime server.

To summarize the performance benefits of a separate multiplexer deployment, consider the following example:

- You can install three separate Community Services multiplexers in front of a single Sametime server. If each Community Services multiplexer handles 20,000 connections, as many as 60,000 users can be connected to a single Sametime server at one time.
- If the Sametime server is capable of servicing 100,000 connections, the server performance will not degrade under the load produced by 60,000 connections.
- If the multiplexer operates on the Sametime server instead of being deployed separately, the Sametime server can service a maximum of 10,000 users. By deploying three separate multiplexers in front of a single Sametime server, you can service 50,000 more users (assuming one connection per user) than if the multiplexer operates on the same machine as the Sametime server.
- If you deploy separate multiplexers in the manner described above, you can also implement a rotating DNS system, or IBM WebSphere Edge Server, in front of the multiplexers to load balance connections to the separate multiplexers.

To deploy separate Community Services multiplexers in your Sametime environment, see Installing and setting up a separate Community Services multiplexer.

Installing and setting up a separate Community Services multiplexer

Installing and setting up a separate Community Services multiplexer involves the following considerations and procedures:

1. Community Services multiplexer preinstallation considerations
2. Install the Community Services multiplexer
3. Configure security settings in the Configuration database on the Sametime server
4. Configure settings in the Sametime.ini file on the multiplexer machine
Community Services multiplexer preinstallation considerations

Considering the requirements of the Community Services multiplexer machine is the first of six procedures associated with installing and setting up a separate Community Services multiplexer.

Consider the following before installing a Community Services multiplexer on a separate machine:

- The minimum system requirements for the Community Services multiplexer machine are the same as the system requirements for the core Sametime server. For more information, see the *Sametime Installation Guide* (stinstall.nsf or stinstall.pdf).

  A machine that meets the minimum system requirements should be able to handle approximately 20,000 simultaneous client connections.

  Testing indicates that machines with dual 1133 MHz CPUs and 2 GB of RAM can handle approximately 30,000 simultaneous client connections.

- TCP/IP connectivity must be available between the Community Services multiplexer machine and the Sametime server. Port 1516 is the default port for the connection from the Community Services multiplexer machine to the Sametime server.

Next step: Install the Community Services multiplexer machine

Install the Community Services multiplexer

Installing the Community Services multiplexer machine is the second of six procedures associated with installing and setting up a separate Community Services multiplexer.

To install the Community Services multiplexer:

1. Insert the Sametime CD into the Community Services multiplexer machine and choose the option to install the Community Services multiplexer (or MUX).

2. Follow the instructions on the installation screens. Ensure that you enter the DNS name or IP address of the Sametime server to which the multiplexer will connect. The DNS name or IP address of the Sametime server is the only significant parameter you must enter during the Community Services multiplexer installation.

3. You can repeat these steps to install additional Community Services multiplexers on other machines.

Next step: Configure security settings in the Configuration database on the Sametime server

Configure security settings in the Configuration database on the Sametime server

Configuring security settings in the Configuration database is the third of six procedures associated with installing and setting up a separate Community Services multiplexer.
After you have installed the Community Services multiplexer on a separate machine, you must configure the Sametime server to accept connections from the Community Services multiplexer.

A Sametime server only accepts connections from a Community Services multiplexer that is listed in the stconfig.nsf database on the Sametime server. Specifically, the Community Services multiplexer machine must be listed in the "CommunityTrustedIps" field of a "CommunityConnectivity" document in the stconfig.nsf database. This security setting prevents a Community Services multiplexer from unauthorized machines from connecting to the Sametime server.

To enable the Sametime server to accept connections from the Community Services multiplexer(s):

1. Use a Lotus Notes client to open the stconfig.nsf database on the Sametime server.
2. Open the CommunityConnectivity document in the stconfig.nsf database by double-clicking on the date associated with the document. If the CommunityConnectivity document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnectivity document, choose Create-CommunityConnectivity from the menu bar in the stconfig.nsf database.
3. In the "CommunityTrustedIps" field, enter the IP addresses of the Community Services multiplexer machine(s). If you enter multiple addresses, separate each address with a comma. Note The IP addresses of SIP Connector machines associated with a Sametime community are also entered in this field.
4. Save and close the CommunityConnectivity document.

**Next step:**
Configure settings in the Sametime.ini file on the multiplexer machine

**Configure settings in the Sametime.ini file on the multiplexer machine**

Configuring settings in the Sametime.ini file is the fourth of six procedures associated with installing and setting up a separate Community Services multiplexer.

When the multiplexer is installed on a separate machine, the configuration of the multiplexer is controlled by the settings in the Sametime.ini file on the multiplexer machine. In most cases, it is not necessary to change any of the settings in the Sametime.ini file but you should review the information below to be sure.

The configuration parameters in the Sametime.ini file include:

- The host name of the Sametime server to which the Community Services multiplexer connects (specified during the Community Services multiplexer installation and in the stconfig.nsf database as discussed in the previous procedure).
- The port the Community Services multiplexer uses to establish the connection with the Sametime server (default port 1516).
- The maximum number of simultaneous connections allowed to the multiplexer.

To specify a maximum number of simultaneous connections, use the VPMX_CAPACITY= parameter of the Sametime.ini file. The default value is 20,000 connections (for example, VPMX_CAPACITY=20000).
Notes about the VPMX_CAPACITY= setting:

- The Sametime Administration Tool contains a Configuration-Community Services-Maximum user and server connections to the Community Server setting that controls the maximum number of Community Services connections allowed to the Sametime server. When the Community Services multiplexer is installed on a separate machine, Community Services users do not connect to the Sametime server and the "Maximum user and server connections to the Community Server” setting cannot be used to control the maximum number of connections allowed. Use the VPMX_CAPACITY= parameter in the Sametime.ini file to control the maximum number of connections instead of the setting in the Sametime Administration Tool.

- Multiplexer machines that meet the minimum system requirements can successfully handle 20,000 connections. This value may vary depending on the processing capabilities of the multiplexer machine. Multiplexer machines that have dual 1133 MHz CPUs and 2GB of RAM can successfully handle as many as 30000 connections.

If it is necessary to modify the settings above, open the Sametime.ini file on the Community Services multiplexer machine with a text editor, alter the setting, and save the Sametime.ini file.

**Next step:**
Configuring client connectivity to the Community Services multiplexer machine

**Configuring client connectivity to the Community Services multiplexer machine**

Configuring client connectivity to the Community Services multiplexer machine is the fifth of six procedures associated with installing and setting up a separate Community Services multiplexer.

After you have installed and configured the Community Services multiplexer, you must ensure that Sametime Connect clients are configured to connect to the Community Services multiplexer instead of the Sametime server.

A Sametime Connect client attempts to connect to the network address specified in the Options-Preferences-Sametime Connectivity-Host setting available on the Sametime Connect client.

To ensure that Sametime Connect clients connect to the Community Services multiplexer machine instead of the Sametime server machine, each user in the Sametime community must enter the DNS name or IP address of the Community Services multiplexer machine in the "Host" field of the Sametime Connect clients. For example, each user may need to perform this procedure:

1. Open Sametime Connect.
2. Choose Options-Preferences-Sametime Connectivity.
3. In the Host field enter the DNS name of the Community Services multiplexer machine.

If you have deployed multiple Community Services multiplexers, your user community should connect to these multiplexers in a balanced fashion. For example, if you have deployed two Community Services multiplexers, half of your users should configure the Sametime Connect client to connect to multiplexer 1 and the other half of the users should configure Sametime Connect to connect to multiplexer 2.
Notes about configuring client connectivity:

- If users have not yet downloaded the Sametime Connect clients from the Sametime server, you can run the Sametime client packager application on a Sametime server to ensure that each Sametime Connect client downloaded from a Sametime server is pre-configured with the appropriate connectivity settings for your environment. Using the client packager prevents end users from having to manually change the connectivity settings. For more information, see the Sametime Installation Guide (stinstall.nsf or stinstall.pdf).

- The next topic discusses an optional configuration you can employ to provide a more dynamic form of connection load balancing across multiple Community Services multiplexer machines than is discussed above. If you dynamically load balance connections to the multiplexers, the Host field in the Sametime Connect client must contain the DNS name or IP address of the load balancing mechanism, not the multiplexer machine as described above.

Next step:

(Optional) Dynamically load balancing client connection to the multiplexers

(Optional) Dynamically load balancing client connection to the multiplexers

Dynamically load balancing connections to multiple Community Services multiplexers is the last of six procedures associated with installing and setting up a separate Community Services multiplexer.

Dynamically load balancing connections is an optional procedure. Also, this procedure is only valid when you have installed multiple Community Services multiplexers.

To dynamically load balance client connections to multiple Community Services multiplexers, you can do one of the following:

- Set up a rotating DNS system to accomplish load balancing. Use rotating DNS to associate the IP addresses of the Community Services multiplexer machines to a single DNS name.

For example, associate the IP address of Community Services multiplexer machine 1 (11.22.33.44) and Community Services multiplexer machine 2 (11.22.33.55) to the DNS name cscluster.sametime.com.

- Set up an IBM WebSphere Edge Server (Network Dispatcher) in front of the Sametime servers that you intend to cluster. Use the WebSphere Edge Server Network Dispatcher to distribute connections to the Community Services multiplexer machines. See the documentation for the IBM WebSphere Edge Server for more information.

Notes about dynamically load balancing client connections to the multiplexers:

- The topic Set up the load-balancing mechanism (rotating DNS or Network Dispatcher) in the “Setting up a Community Services cluster without clustering the Meeting Services” chapter of this documentation illustrates a rotating DNS system set up in front of a separate multiplexer deployment. Note that the deployment shown in that topic illustrates multiple multiplexers in front of a Community Services server cluster instead of a single, non-clustered Sametime server.

- For information about rotating DNS limitations, see Rotating DNS Limitations with cached DNS resolve requests.
Enabling Sametime Connect for browsers to function in kiosk mode

In some Sametime deployments, it may be necessary for multiple users to access the Sametime Connect for browsers client on a Sametime server from the same client machine. For example, several different users may access the Sametime Connect client from the same public computer in an airport. In situations where it is necessary for multiple users to access the Sametime Connect for browsers client from the same client machine, you can enable the Sametime Connect for browsers client to function in kiosk mode.

When the Sametime Connect for browsers client loads on a computer, a JavaConnect.ini file is created on that computer. The JavaConnect.ini file stores many of the client preference settings that a user selects from the menus in the Sametime Connect for browsers client.

When different users access the Sametime Connect for browsers client from the same machine, each user will start a different instance of the Sametime Connect for browsers client on that machine. These different instances of the Sametime Connect for browsers client will modify the single JavaConnect.ini file on that machine. In this scenario, it is possible for a current user to gain access to the preferences settings of a previous user because the JavaConnect.ini file will contain the values specified by the most recent user. This possibility may pose some security risks and may also cause the Sametime Connect for browsers client to operate in unexpected ways for the end users.

To prevent these problems, you can configure the Sametime Connect for browsers client to operate in kiosk mode.

When the Sametime Connect for browsers client operates in kiosk mode, the client preference settings are not stored on the client machine (the JavaConnect.ini file is not created on the client machine). The client preference settings are stored in memory and the settings a user makes are valid only for the duration of the current instant messaging session. When the user closes the Sametime Connect for browsers client, the settings are lost and cannot be picked up by a subsequent instance of the Sametime Connect client that loads on that machine.

When the Sametime Connect for browsers client operates in kiosk mode, the administrator can also set the default connectivity configuration of the Sametime Connect for browsers client. Specifying the default connectivity configuration ensures that the client loads with the default connectivity settings required to successfully connect to the Sametime server from the client machine. For more information about specifying the default connectivity configuration, see Changing the default connectivity settings of the Sametime Connect for browsers client.

Note: If you enable the Sametime Connect for browsers client to operate in kiosk mode, it is not mandatory to also specify the default connectivity configuration of the Sametime Connect for browsers client. Specifying the default connectivity configuration is a separate optional procedure from enabling the client to function in kiosk mode.

Enabling the kiosk mode

To enable kiosk mode, the administrator must add the following applet parameter to the HTML code on the Sametime server that loads the Sametime Connect for browsers client.

<PARAM NAME="KioskMode" VALUE="1">
**Note:** If this parameter specifies any value other than 1, the Sametime Connect for browsers client will not operate in kiosk mode. The client will operate in its default mode and the preferences settings will be saved in the JavaConnect.ini file on the client machine.

On a standard Sametime server deployment, the applet code that loads the Sametime Connect for browsers client is located in the Sametime Resources database (STSrc.nsf) on the Sametime server. You can use the Domino Designer client to open the STSrc.nsf database and add the applet parameter to the existing applet code. For instructions, see "**Enabling the kiosk mode by altering the HTML in the STSrc.nsf database**".

**Note:** If you enable the kiosk mode by adding the applet parameter to the HTML in the STSrc.nsf database, the Sametime Connect for browsers client will operate in kiosk mode for all users of this Sametime server. If some of those users access the Sametime server from private workstations, those users will not be able to specify permanent preferences settings for the Sametime Connect for browsers client.

To accommodate the kiosk mode, some organizations may choose to customize the user interface of the Sametime server by creating a custom HTML page or Domino application specifically to launch the Sametime Connect for browsers client. This custom interface would be accessible only from those client machines that must operate in the kiosk mode. This possibility is briefly discussed in "**Example of custom HTML code that enables the kiosk mode**".

### Enabling the kiosk mode by adding an applet parameter to the HTML in the STSrc.nsf database

To enable the kiosk mode on a standard deployment of the Sametime server, you must add the required applet parameter to the HTML code in the Sametime Resources (STSrc.nsf) database on the Sametime server.

This applet code exists in three subforms of the Sametime Resources (STSrc.nsf) database on the Sametime server. To ensure the default connectivity settings go into effect for all browser types, you must add the ConnectivityMethod applet parameter to the HTML code in each of these two subforms.

- **WebConnect-IE** (This subform applies to the Microsoft Internet Explorer browsers.)
- **WebConnect-Moz** (This subform applies to Mozilla browsers.)

**Note:** A WebConnect-N4 subform may appear in the STSrc.nsf database, but this subform applies to the Netscape 4 browsers and is not used with Sametime 7.0.

To add the applet parameter to the HTML code in the STSrc.nsf database:

1. Use the Domino Designer client to open the STSrc.nsf database on the Sametime server.
2. In Domino Designer expand the "Recent Databases" icon and ensure that the STSrc.nsf database is selected.
3. Expand "Resources" and click "Subforms."
4. In the Subforms list, double-click on the WebConnect-IE subform.
5. In the work pane at the top of the Domino Designer client, scroll down until you see the HTML code containing the applet parameters.
Note: The applet parameters begin with the text string "<paramname=".

6. Add the applet parameter below to the list of applet parameters in the WebConnect-IE subform:
   <paramname="KioskMode" value="1">

7. Save the subform.
8. Repeat steps 4 through 7 for the WebConnect-Moz subform.

Note: When enabling the kiosk mode, you may also want to add an applet parameter that specifies the default connectivity configuration of the Sametime Connect for browsers client. For more information, see Changing the default connectivity setting of the Sametime Connect for browsers client.

Example of custom HTML code that loads the Sametime Connect for browsers client

The example below illustrates the applet code that might be used in a custom HTML page or Domino application to launch the Sametime Connect for browsers client in the kiosk mode. If you create a custom interface for this purpose, ensure the code includes the kiosk mode applet parameter as shown below:

```html
<APPLET>
code=com.lotus.sametime.connectapplet.ConnectApplet.class
height=100% name=ConnectApplet
style="BACKGROUND-COLOR: gray; LEFT: 0px; TOP: 0px" width=100% MAYSCRIPT=TRUE>
<PARAM NAME="cabinets" VALUE="connect.cab">
<PARAM NAME="SametimeServer" VALUE="">
<PARAM NAME="SametimePort" VALUE="">
<PARAM NAME="TokenUserId" VALUE="">
<PARAM NAME="TokenValue" VALUE="">
<PARAM NAME="KioskMode" VALUE="1">
</APPLET>

Note: When enabling the kiosk mode, you may also want to add an applet parameter that specifies the default connectivity configuration of the Sametime Connect for browsers client. For more information, see Changing the default connectivity setting of the Sametime Connect for browsers client.

Deploying the Macintosh Sametime Connect client for the desktop

The Sametime 7.0 release includes a new version of the Sametime Connect client application that is designed to run on Macintosh operating systems. This version of Sametime Connect is called "Macintosh Sametime Connect for the desktop."

The Macintosh Sametime Connect for the desktop client can install and run on the following Macintosh operating systems:
- Mac OS X 10.3.x (with JVM 1.4.2 for Mac OS X)
- Mac OS X 10.4.x (with JVM 1.4.2 for Mac OS X)

The Macintosh Sametime Connect client does not support and includes no user interface options for the following features that are supported on other versions of Sametime Connect:
- Instant meetings
• The "Automatically change my status" feature (available from the Options-Preferences-Status tab on other versions of Sametime Connect)
• The "Launch at startup" option (available from the Options menu on other versions of Sametime Connect)

Aside from these differences, the Macintosh Sametime Connect for the desktop client provides the same functionality as the Sametime Connect for browsers client available from the user interface of the Sametime server.

Authentication
As with the other versions of the Sametime Connect client, the Macintosh Sametime Connect for the desktop client uses basic password authentication to authenticate end users. Users enter their authentication credentials at a log in screen when starting the client.

The requirements for end user authentication to the Macintosh Sametime Connect for the desktop client are the same as for other versions of the Sametime Connect client. For more information, see [User requirements for basic password authentication](#).

Deploying the client
The Macintosh Sametime Connect for the desktop client runs as a standalone java application on the Macintosh operating system. This client is not a java applet that runs in a Web browser.

The Macintosh Sametime Connect client is not available for download from the user interface of the Sametime server. The Macintosh Sametime Connect client is available in the Client directory on Sametime server CD 2 (it is the setupMac.command file).

To deploy this client, the administrator must distribute the setupMac.command file to the end users. The manner in which the administrator distributes the file to end users is at the discretion of the administrator. A user double-clicks the setupMac.command file on the Macintosh computer to install the client.

The Macintosh Sametime Connect client must be manually installed on each end user system. After installing the client, the user must manually configure the connectivity options to enable the client to connect to the Sametime server.

Follow the instructions below to install the Macintosh Sametime Connect client on a client computer:
1. Double-click the setupMac.command file.
2. At the Welcome screen, click Next.
3. At the Directory Name screen, accept the default location or select a specific directory into which you want to install the Sametime Connect client.
4. At the Summary information screen, click Install.
5. When the message appears indicating the installation was successful, click Finish.
6. Follow the instructions below to configure the client to connect to the Sametime server.
Configuring the client to connect to the Sametime server

After installing the Macintosh Sametime Connect for the desktop client on a computer, you must configure the connectivity settings in the client to enable it to connect to the Sametime server. To configure these settings:

1. Open the Macintosh Sametime Connect for the desktop client.
2. Click the Connectivity button on the log in screen.
3. In the Sametime server section of the Sametime Connectivity tab, complete these fields:
   - **Host** - Enter the fully-qualified DNS name of the Sametime server.
   - **Port** - This port must match the port number on which the Sametime server listens for Community Services connections. The default setting is port 1533. For more information, see [Sametime Connect client connection processes](#) and [Community Services Network settings](#).
4. Select the connection type below that is appropriate for your environment. For more information about these settings, see [Sametime Connect client connection processes](#):
   - Use my Java Plug-in Settings
   - Direct connection using Sametime protocol
   - Direct connection using HTTP protocol
   - Use proxy
5. Click OK.
Chapter 7. Enabling the SIP Gateway

The Session Initiation Protocol (SIP) Gateway uses SIP to enable instant messaging and audio/video collaboration between an IBM Lotus Sametime server and another online collaboration community that supports SIP.

This chapter discusses the following topics concerning the SIP Gateway:

- Using SIP functionality with Sametime
- Overview of Sametime SIP components
- Setting up the SIP Gateway functionality
- Disabling the SIP Gateway functionality
- Encrypting SIP traffic with Transport Layer Security (TLS)
- Requiring client certificate authentication for SIP connections
- Audio/Video connectivity with SIP
- End user experience with the SIP Gateway

Using the SIP functionality with Sametime

The Sametime SIP functionality is designed primarily to support instant messaging and audio/video communications between two Sametime communities. The SIP functionality can also be used to enable users in your Sametime community to communicate using instant messaging or audio/video with users in any other online collaboration community that supports SIP, including other Sametime communities.

You can enable the SIP functionality for a Sametime server that is installed on any of these operating systems: Windows, AIX, Solaris, or IBM i5/OS. You can use the same procedure to set up the SIP functionality if your Sametime servers operate in a Windows, AIX, or Solaris environment. You must use a different procedure to set up the SIP functionality if your Sametime servers operate in an IBM i5/OS environment.

For more information about using SIP functionality with Sametime, see the topic below that is appropriate for your environment:

- Using the SIP functionality in a Windows, AIX, or Solaris environment
- Using the SIP functionality in an IBM i5/OS environment

Using the SIP functionality in a Windows, AIX, or Solaris environment

This topic provides an overview of using the SIP functionality with Sametime servers installed on Windows, AIX, or Solaris operating systems.

To use the SIP functionality with Sametime servers that operate in a Windows environment, the Sametime community must be "SIP-enabled." A Sametime community is "SIP-enabled" if the following three conditions are true:

- The "SIP Connector" is installed and connected to the "SIP Gateway" on the Sametime 7.0 server.
A "SIP Gateway" is the Sametime server component that supports the SIP functionality. The SIP Gateway installs automatically with all other Sametime server components during a Sametime 7.0 installation.

A "SIP Connector" is a separate SIP component that installs on a different machine than the SIP Gateway. The SIP Connector connects to the SIP Gateway on the Sametime server and handles connections to and from other SIP-enabled communities on behalf of the SIP Gateway.

The SIP Connector component must be installed from the Sametime 7.0 server CD.

• The SIP Gateway functionality is enabled on the Sametime server.
  The administrator enables the SIP Gateway functionality by configuring settings on documents in the Sametime Configuration database (stconfig.nsf) on the Sametime server.

For step-by-step instructions on enabling the SIP functionality for a Sametime community in a Windows environment, see [Setting up the SIP Gateway functionality (Windows, AIX, or Solaris environment)](link).

After enabling the SIP functionality, the administrator also has the option of using Transport Layer Security (TLS) to encrypt SIP data transmitted between the SIP-enabled communities or requiring client certificate authentication for connections between SIP Connectors in two separate communities. For information about encrypting data transmitted between different communities with Transport Layer Security (TLS), see [Encrypting SIP traffic with Transport Layer Security (TLS)](link).

### Using the SIP functionality in an IBM i5/OS environment

This topic provides an overview of using the SIP functionality in an environment in which the Sametime servers are installed on IBM i5/OS servers.

To use the SIP functionality with Sametime servers that operate in an IBM i5/OS environment, the Sametime community must be "SIP-enabled." A Sametime community is "SIP-enabled" if the following conditions are true:

• The SIP Gateway functionality is enabled on a Sametime 7.0 server. The administrator enables the SIP Gateway functionality by configuring settings on documents in the Sametime Configuration database (stconfig.nsf) on the Sametime server.

• A "SIP Connector" is installed and connected to the SIP Gateway on the Sametime 7.0 for IBM i5/OS server.

A SIP Connector is a separate component that connects to the SIP Gateway on the Sametime server and handles connections to and from other SIP-enabled communities on behalf of the SIP Gateway.

In an IBM i5/OS environment, you have two options regarding the SIP Connector installation.

- You can use the "integrated SIP Connector" that installs with the Sametime 7.0 server. The integrated SIP Connector installs automatically as part of the Sametime 7.0 i5/OS installation, but must be manually enabled by the administrator following the installation.
  The integrated SIP Connector is most useful if two communities can communicate over a corporate intranet and do not need to establish connections over the Internet.

- You can install a "standalone SIP Connector" on a separate machine. In this scenario, the SIP Connector installs on a separate machine running a
Windows NT or 2000 server. The standalone SIP Connector handles connections to and from the SIP Gateway that is installed on the Sametime 7.0 i5/OS server.

The standalone SIP Connector is useful if two Sametime communities must establish connections over the Internet.

If you prefer to install the standalone SIP Connector on a Windows system, you can install the SIP Connector from a Sametime 7.0 for IBM i5/OS CD.

For step-by-step instructions on enabling the SIP functionality for a Sametime community in an IBM i5/OS environment, see Setting up the SIP Gateway functionality (IBM i5/OS environment).

After enabling the SIP functionality, the administrator also has the option of using Transport Layer Security (TLS) to encrypt SIP data transmitted between the SIP-enabled communities or requiring client certificate authentication for connections between SIP Connectors in two separate communities. Unlike previous Sametime i5/OS releases, TLS encryption is supported for both integrated SIP Connector and standalone SIP Connector deployments. For information about encrypting data transmitted between different communities with Transport Layer Security (TLS), see Encrypting SIP traffic with Transport Layer Security (TLS).

---

**Overview of SIP components**

This topic provides the following basic information about SIP, the Sametime SIP Gateway, and the Sametime SIP Connector.

- What are SIP and SIMPLE
- SIP Gateway overview
- SIP Connector overview
- SIP proxies and connections

**What are SIP and SIMPLE**

Session Initiation Protocol (SIP) is a general-purpose application-layer signaling protocol that can establish, modify, or terminate real-time calls and multimedia sessions over IP networks. Extensions to SIP enable it to establish sessions that include audio, video, or instant messaging and presence data.

SIP for Instant Messaging and Presence Leveraging (SIMPLE) is an extension to the SIP protocol that supports instant messaging and presence functionality.

Detailed discussions of SIP and SIMPLE are outside the scope of this documentation. For more detailed information about these protocols, see the following Internet Engineering Task Force (IETF) documents:

- SIP - IETF RFC 3261
- SIMPLE - draft-ietf-simple-im-01; draft-ietf-simple-presence-06
- CPIM (Common Presence and Instant Messaging) - draft-ietf-impp-cpim-msgfmt-06; draft-ietf-impp-cpim-pidf-03

**Sametime SIP Gateway overview**

The Sametime SIP Gateway component is installed on a Sametime 7.0 server during the Sametime 7.0 server installation. Once installed, the SIP Gateway operates as a server application on the Sametime server.

The Sametime SIP Gateway provides the following functionality:
• Users in your SIP-enabled community can add a user from another SIP-enabled community to the contact list in Sametime Connect. Users in the other community can also add users in your community to the buddy lists of their clients.

In the SIP environment, a user enters the Internet e-mail address of another user when adding a user to the contact list or buddy list. For one user to successfully add another user to a contact list or buddy list, both users must have an Internet e-mail address defined in the directory. (E-mail addresses are usually defined in a user’s person entry in the directory accessed by the Sametime server.)

Note: SIP defines users and other entities by their Internet e-mail addresses.

• Users in your community have awareness of the online/offline status (or "presence") of users in the other SIP-enabled community. Users in the other community can also see the online/offline status of users in your community.

• Users in either community can initiate instant messaging sessions or instant audio/video sessions with users in the other community. Only one-to-one instant messaging sessions or audio/video sessions are supported. Instant messaging sessions or audio/video sessions involving more than two users (also called "n-way" meetings) are not supported between users in different communities.

An instant messaging session between two users cannot include audio/video as an additional meeting activity. Similarly, an audio/video meeting cannot include chat as an additional meeting activity. Collaboration sessions that use the SIP Gateway functionality must be "instant messaging only" or "audio/video only" sessions; a single session cannot include both instant messaging and audio/video.

• A user in your community can use the privacy features of Sametime Connect to prevent a user in another community from seeing the online status of the user in your community.

Note: Privacy is not symmetrical between communities. For example, assume Susan operates in your community and Juan operates in a remote SIP-enabled community. Susan can use the privacy features of Sametime Connect to prevent Juan from detecting her online status. Even though Susan has concealed her online status from Juan, Susan can still detect Juan’s online status. (This type of non-symmetrical presence in which Susan can see Juan but Juan cannot see Susan is referred to as "lurking,"

Similarly, assuming Juan’s instant messaging client includes privacy features, Juan can conceal his online status from Susan. Even though Juan has concealed his online status from Susan, Juan can still detect Susan’s online status if Susan does not use the privacy features of Sametime Connect to conceal her status. If Susan conceals her online status from Juan and Juan conceals his online status from Susan, neither user can detect the online status of the other user.

Sametime SIP Connector overview

A separate software component, called the SIP Connector, must be installed and operational before the SIP Gateway functionality is available to users in your community.

When using the SIP functionality with Sametime servers that run on the Windows, AIX, or Solaris operating systems, the SIP Connector software must be installed on a separate, dedicated machine running the Windows operating system. You specify the Sametime server to which the SIP Connector connects during the SIP Connector installation.
When using the SIP functionality with the Sametime servers that run on the IBM i5/OS operating system, you have the option of using an integrated SIP Connector which installs and runs on the IBM i5/OS machine with all other components of the Sametime server or a standalone SIP Connector which installs on a separate, dedicated machine running the Windows operating system.

Note: Generally, in the IBM i5/OS environment, you install a standalone SIP Connector if it is necessary for two Sametime communities to establish connections using the Internet. For more information, see the topic Review the SIP Connector planning considerations (IBM i5/OS environment) later in this chapter.

The SIP Connector handles connections with the external community. The SIP Connector handles both inbound and outbound connections. Specifically, the SIP Connector:

- Receives outbound SIP data from the local SIP Gateway.
- Constructs outbound SIP messages.
- Creates connections to a SIP-enabled component in the other community (for example, another SIP Connector that supports a different Sametime community, or a SIP proxy server that supports the community).
- Receives connections from a SIP-enabled component in another community.
- Parses inbound SIP messages.
- Forwards the inbound messages to the SIP Gateway on the Sametime server.

The administrator must configure a SIP Connector to accept connections from and create connections to a specific SIP-enabled community (or communities).

A single SIP Connector may be configured to support connections to one or more external communities. Multiple SIP Connectors can also be deployed to support connections to multiple external communities. For example, if you want users in your community to communicate with users in Sametime communities A and B, you can install one SIP Connector to support connections with Sametime community A and a separate SIP Connector to support connections with Sametime community B. Both of these SIP Connectors can connect to the same SIP Gateway in your community.

You can also install multiple SIP Connectors and configure them to support connections to the same external community to ensure continuity of service in case of a server failure. If one SIP Connector machine becomes unavailable, the other machine can continue handling the connections.

**SIP proxies and connections**

A SIP proxy server is an intermediate component usually located between a SIP-enabled community and the Internet. The SIP proxy is responsible for routing and delivering all calls to a SIP-enabled community. With the Sametime SIP functionality, the SIP Connector component and SIP Gateway together act as a SIP proxy server.

When allowing connections to SIP-enabled communities in other DNS domains (for example, acme.com), the administrator can specify the DNS name of the SIP proxy associated with the other domain. All calls from your community to the external community are routed through that SIP proxy.
If the administrator does not specify the name of a specific SIP proxy, Sametime performs a DNS lookup to determine if a SIP proxy exists for that DNS domain. If Sametime is unable to locate a SIP proxy using DNS, Sametime attempts a SIP connection to the domain using port 5060 (the default SIP connection port).

**Setting up the SIP Gateway functionality**

This section explains how to set up the SIP Gateway functionality in the following environments:

- **Windows, AIX, and Solaris** - You can use the same set of instructions to set up the SIP Gateway functionality in a Windows, AIX, or Solaris environment.
- **IBM i5/OS** - You must use a separate set of instructions to set up the SIP Gateway functionality in an IBM i5/OS server environment.

Follow the procedure below that is appropriate for your environment:

- [Setting up the SIP Gateway functionality (Windows, AIX, or Solaris server environment)](#)
- [Setting up the SIP Gateway functionality (IBM i5/OS server environment)](#)

**Setting up the SIP Gateway functionality (Windows, AIX, or Solaris environment)**

Use the instructions in this section to set up the SIP Gateway functionality if your Sametime servers run on the Windows, AIX, or Solaris operating system.

To set up the SIP Gateway functionality and SIP-enable your Sametime community in a Windows, AIX, or Solaris environment, perform the procedures below.

1. [Review the SIP Connector planning considerations (Windows/AIX/Solaris environment)](#)
2. [Install the SIP Connector (Windows/AIX/Solaris environment)](#)
3. [Configure the SIP Gateway and SIP Connector parameters (Windows/AIX/Solaris environment)](#)

Detailed instructions for each of these procedures are provided in subsequent topics.

**Review the SIP Connector planning considerations (Windows/AIX/Solaris environment)**

Reviewing the SIP Connector planning considerations is the first of three procedures required to set up the SIP Gateway functionality in a Windows, AIX, or Solaris environment.

If your Sametime 7.0 server runs on a Windows, AIX, or Solaris operating system, you must install the SIP Connector on a separate, dedicated Windows machine. Do not install the SIP Connector on the same machine as a Sametime server.

**Important**: You cannot install the SIP connector on a computer that runs either the AIX or Solaris operating system. The SIP Connector must be installed on one of the Windows operating systems listed below. A SIP Connector installed on one of these Window operating systems can communicate with a Sametime server running on either Windows, AIX, or Solaris. However, the SIP Connector can only be installed on a Windows machine.
SIP Connector system requirements

The system requirements for the SIP Connector machine are the same as the system requirements for a Sametime server. These requirements include:

  
  **Note:** The SIP Connector must be installed on a server that runs the Windows operating systems. A SIP Connector cannot be installed on an AIX or Solaris operating system.

- **Processor** - Pentium II with 400 MHz minimum
- **RAM** - 1 GB recommended; 500 MB minimum
- **Disk space** - 500 MB minimum
- **Disk swap space** - 64 MB
- **Network software** - TCP/IP network software installed

SIP Connector planning considerations

Before installing the SIP Connector, consider the following:

- If the users in your community do not need to use the Internet to communicate with users in another community, you can install the SIP Connector on any intranet machine that has a LAN or WAN connection to the Sametime server containing the SIP Gateway. The SIP Connector machine must be able to establish a TCP/IP connection to the Sametime server on port 1516. The SIP Connector must be able to receive connections from other SIP-enabled communities on TCP/IP port 5060 (the default SIP port).

  If you intend to encrypt connections to your SIP-enabled community with the Transport Layer Security (TLS) protocol, the SIP Connector must be able to receive connections from other SIP-enabled communities on TCP/IP port 5061 (the default TLS/SIP port). For more information, see [Encrypting SIP traffic with Transport Layer Security (TLS)] later in this chapter.

- If the SIP Connector must connect to other SIP-enabled communities using the Internet, you can install the SIP Connector on a machine outside your corporate firewall (in the network DMZ). The SIP Connector machine must be available for connections from Internet users on port 5060 (or 5061 if TLS is used for encryption).

  If you position the SIP Connector outside the firewall in the network DMZ, the SIP Connector machine must be able to initiate connections to the Sametime server machine inside the firewall that contains the SIP Gateway. (The default port for these connections is port 1516.)

  It may be necessary to configure the firewall with a set of access rules that establish trust between the Sametime server on your intranet and the SIP Connector machine in the network DMZ. (For example, the access rules might allow those machines to make SIP connections to each other through the firewall on port 5060 but prevent other machines from connecting to them).

- Optionally, you can install multiple SIP connectors. For example, if you want users in your community to connect to two separate external SIP-enabled communities, you may want to install two separate SIP Connectors. Installing multiple SIP Connectors can spread the connection handling load among multiple machines; each SIP Connector handles the incoming and outgoing connections for only one of the external communities.

  You can also install two SIP connectors and configure both SIP Connectors to handle connections for the same external SIP-enabled community. This configuration ensures that a SIP Connector is available if one SIP Connector machine fails.
Next step:
Install the SIP Connector (Windows/AIX/Solaris environment)

Install the SIP Connector (Windows/AIX/Solaris environment)
Installing the SIP Connector is the second of three procedures required to set up the SIP Gateway functionality in either a Windows, AIX, or Solaris environment.

Note: The SIP Connector must always be installed on a computer running a Windows operating system. For more information, see Review the SIP Connector planning considerations (Windows/AIX/Solaris environment)

To install a SIP Connector:
1. You can install the SIP Connector from the Sametime 7.0 CD or download the SIP Connector from the Web.
2. During the installation, you must enter the following:
   • The IP address or DNS name of a Sametime 7.0 server. This address enables the SIP Connector to locate and establish a connection with the SIP Gateway on the Sametime server.
   • A SIP Connector name. SIP Connector configuration data is organized under this name. The SIP Connector requires this name to get its configuration parameters. You can use the DNS name of the SIP Connector machine as the SIP Connector name.

The Sametime server address and SIP Connector name are the only significant parameters required by the SIP Connector installation.

Note: The SIP Connector configuration parameters are stored in a CommunityConnector document in the stconfig.nsf database on the Sametime server. You create this document later in this process.

Next step:
Configure the SIP Gateway and SIP Connector parameters (Windows/AIX/Solaris environment)

Configuring the SIP Gateway and SIP Connector parameters (Windows/AIX/Solaris environment)
Configuring the SIP Gateway and SIP Connector parameters is the last of three procedures required to set up the SIP Gateway functionality in a Windows, AIX, or Solaris environment.

Configuring the SIP Gateway and SIP Connector parameters is accomplished in four steps. These steps include:
1. Enabling connections to other communities and enabling e-mail address translation (Windows/AIX/Solaris environment)
2. Configuring the community connectivity parameters (Windows/AIX/Solaris environment)
3. Configuring the SIP Connector parameters (Windows/AIX/Solaris environment)
4. Enabling the SIP Connector to authenticate when connecting to the Sametime server (Windows/AIX/Solaris environment)

Each of these steps is described in detail in a subsequent topic.
Enabling connections to other communities and enabling e-mail address translation (Windows/AIX/Solaris environment)

Enabling connections to other communities and enabling e-mail address translation is the first of four steps required to configure the SIP Gateway and SIP Connector parameters.

In this step you perform two separate configurations; you enable connections to other communities and enable e-mail address translation:

- Enabling connections to other communities allows the SIP Gateway to initiate connections to and receive connections from another SIP-enabled community.
- Enabling e-mail address translation ensures that users in your Sametime community can be identified by their Internet e-mail addresses. Users from another community must specify the Internet e-mail addresses of the users in your community when adding them to contact lists or buddy lists. Enabling e-mail address translation ensures the internal user IDs used by Sametime can be translated to the appropriate Internet e-mail addresses.

**Note:** SIP entities are identified by e-mail address. For one user to successfully add another user to a contact list or buddy list, both users must have an Internet e-mail address defined in the directory. (E-mail addresses are usually defined in a user’s person entry in the directory accessed by the Sametime server.) A user that does not have an e-mail address defined in the directory can add other users to a contact list or buddy list, but will not be able to communicate with those users or detect their online status.

To enable connections to other communities and enable e-mail address translation, you must alter settings in the "CommunityGateway" document of the Configuration database (stconfig.nsf):

1. Use a Lotus Notes client to open the stconfig.nsf database on the Sametime server on which you have installed the SIP Gateway (which is installed automatically with Sametime Service Pack 1).
2. Open the CommunityGateway document by double-clicking on the date associated with the document.
   If the CommunityGateway document does not exist in the stconfig.nsf database, you must create it. To create the CommunityGateway document, choose Create-CommunityGateway from the menu bar in the stconfig.nsf database.
3. In the "Support external communities" field, select "True."
   Selecting "True" in this field enables the SIP Connector to initiate connections to and receive connections from other SIP-enabled communities.
   **Note:** To disable connections to other communities, set the "Support external communities" value to "False." Setting this value to "False" is the quickest way to disable all SIP functionality for the community.
4. In the "ConvertID" field, select "True."
   Selecting "True" in this field enables e-mail address translation.
   **Note:** To disable e-mail address translation, set the "ConvertID" field to "False."
5. Save the CommunityGateway document.
6. Leave the stconfig.nsf database open. The next step involves creating and modifying a document in this database.
Important You must enable e-mail address translation on every Sametime server in the community. Repeat all of the steps above in the Configuration database of every Sametime server in the community.

Next step: Configuring community connectivity parameters (Windows/AIX/Solaris environment)

Configuring community connectivity parameters (Windows/AIX/Solaris environment)
Configuring community connectivity parameters is the second of four steps required to configure the SIP Gateway and SIP Connector parameters.

In this procedure, the administrator creates an ExternCommunity document in the Sametime Configuration database (stconfig.nsf). The administrator uses the settings in this ExternCommunity document to specify the parameters that enable the SIP Gateway to connect to another SIP-enabled community.

The connectivity parameters specified in this procedure include:
- A name for the external community
- The DNS domains that comprise the external community
- The DNS name of the SIP proxy (or SIP Connector) for the external community
- The port to use when connecting to the SIP proxy that handles connections for the external community.

To configure the community connectivity parameters:
1. Open the ExternCommunity document in the stconfig.nsf database by double-clicking on the date associated with the document.
   If the ExternCommunity document does not exist in the stconfig.nsf database, you must create it. To create the ExternCommunity document, choose Create-Other-ExternCommunity from the menu bar in the Configuration database (stconfig.nsf).
2. In the "Community Name" field, enter a name for the external community. The name is at your discretion. You might want to choose a name that represents the organization associated with this community. (For example, IBM).
3. In the "Domains" field, enter the domain names associated with the instant messaging community of the organization specified above. This entry can consist of one domain name, or a group of domain names. You can also use wildcards when specifying domain names. For example, *.ibm.com, lotus.com, tivoli.com, ubique.com.
4. In the "DNS" field, enter the fully-qualified DNS name of the SIP proxy that handles connections for the other SIP-enabled community. The SIP Connector attempts to connect to this SIP proxy (or SIP Connector for another Sametime community).
   Note If you leave the "DNS" field blank, Sametime performs a DNS lookup to locate the SIP proxy associated with the domain(s) specified above. If Sametime is unable to locate a SIP proxy, Sametime attempts a SIP connection to the domain(s) using the port specified below.
5. In the "Port" field, enter the port the SIP Connector uses when attempting SIP connections to the SIP proxy or domain(s) specified above. The default port for SIP connections is port 5060.
6. Set the "Encryption" field to "Disabled" unless you intend to encrypt SIP connections between communities with Transport Layer Security (TLS). For more information, see [Encrypting SIP traffic with Transport Layer Security (TLS)](chapter) later in this chapter.

7. Leave the "Certificate distinguished” name field blank unless you intend to require client certificate authentication for connections between SIP Connectors. For more information, see [Enabling client certificate authentication](chapter) later in this chapter.

8. Leave the stconfig.nsf database open. The next step involves creating and modifying a document in this database.

**Next step:** Configuring SIP Connector parameters (Windows/AIX/Solaris environment)

### Configuring SIP Connector parameters (Windows/AIX/Solaris environment)

Configuring SIP Connector parameters is the third of four steps required to configure the SIP Gateway and the SIP Connector parameters.

In this procedure, the administrator creates a CommunityConnector document in the Sametime Configuration database (stconfig.nsf). The administrator uses the settings in this CommunityConnector document to specify the parameters that control the functioning of the SIP Connector.

The SIP Connector parameters include:
- The name of the SIP Connector machine
- The IP address of the SIP Connector machine
- The port on which the SIP Connector listens for connections
- The names of the communities for which the SIP Connector handles connections (these names are defined in the ExternCommunity document created in the previous procedure).

To configure the SIP Connector parameters:

1. Open the CommunityConnector document in the stconfig.nsf database by double-clicking on the date associated with the document.

   If the CommunityConnector document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnector document, choose Create-CommunityConnector from the menu bar in the Configuration database (stconfig.nsf).

2. In the "Connector Name" field, enter a name for the SIP Connector. If you specified a SIP Connector name during the SIP Connector installation, this field should contain the name specified for the SIP Connector during the installation. (Generally, the DNS name of the machine on which the SIP Connector is installed is used as the Connector Name.)

3. In the "IP" field, enter the IP address of the machine on which the SIP Connector is installed. The SIP Connector listens for SIP connections on this IP address.

   If this field is left blank, the SIP Connector listens for SIP connections on all IP addresses assigned to the SIP Connector machine.

4. In the "Port" field, enter 5060. The SIP Connector listens for SIP connections from the SIP Gateway or another SIP-enabled community on this port. Port 5060 is the default port for SIP connections.
Note that if the "IP" field is blank, and the "Port" field specifies 0 (zero), the SIP Connector will not listen for clear text (or unencrypted) SIP connections. A SIP Connector in another community cannot make an unencrypted SIP connection to the SIP Connector. If you configure the SIP Connector parameters in this way, you must encrypt SIP traffic with Transport Layer Security (TLS).

5. (Optional) In the "TLS IP" field, enter the IP address of the machine on which the SIP Connector is installed. The SIP Connector listens for TLS-encrypted SIP connections on this IP address.

If this field is left blank, the SIP Connector listens for TLS-encrypted SIP connections on all IP addresses assigned to the SIP Connector machine.

Note The "TLS IP" field is only relevant if you use TLS to encrypt connections between the SIP-enabled communities. For more information, see Encrypting SIP traffic with Transport Layer Security (TLS) later in this chapter.

6. (Optional) In the "TLS Port" field, enter the port number on which the SIP Connector will listen for TLS-encrypted connections. The default port number for these connections is port 5061.

Note that if the "TLS IP" field is blank, and the "TLS Port" field specifies 0 (zero), the SIP Connector will not listen for TLS-encrypted SIP connections.

Note The "TLS Port" field is only relevant if you use TLS to encrypt connections between the SIP-enabled communities. For more information, see Encrypting SIP traffic with Transport Layer Security (TLS) later in this chapter.

7. In the "Supported Communities" field, enter the names of the communities for which this SIP Connector will handle connections. These are the "Community Names" as defined in the ExternCommunities documents created when you configured the community connectivity parameters in the previous procedure.

8. Choose File - Save to save the CommunityConnector document.

9. Leave the stconfig.nsf database open. The next step involves creating and modifying a document in this database.

Next step: Enabling the SIP Connector to authenticate when connecting to the Sametime server (Windows/AIX/Solaris environment)

Enabling the SIP Connector to authenticate when connecting to the Sametime server is the last of four steps required to configure the SIP Gateway and the SIP Connector.

A Sametime server will only accept connections from SIP Connectors that are listed in its stconfig.nsf database. Specifically, the IP addresses of all SIP Connectors that connect to a Sametime server must be listed in the "CommunityTrustedIps" field of the "CommunityConnectivity" document in the stconfig.nsf database on the Sametime server.

Sametime uses the IP address of the SIP Connector machine to authenticate connections from the SIP Connector (or verify that the SIP Connector is known to the Sametime server). Using the IP address for authentication prevents a SIP Connector on an unauthorized machine from connecting to the Sametime server.

To enable the SIP Connector to authenticate when connecting to the Sametime server:

1. Open the CommunityConnectivity document in the stconfig.nsf database by double-clicking on the date associated with the document.
If the CommunityConnectivity document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnectivity document, choose Create-CommunityConnectivity from the menu bar in the stconfig.nsf database.

2. In the "CommunityTrustedIps" field, enter the IP address(es) of the SIP Connector machine(s).
   
   **Note:** The IP addresses of Community Services multiplexer machines associated with a Community Services cluster are also entered in this field.

3. Save and close the CommunityConnectivity document.

   **Note:** Sametime SIP Connectors can also be deployed with Sametime servers that operate as part of a Community Services cluster.

After you enable the SIP Connector to authenticate, you have completed all procedures required to set up the SIP Gateway functionality in a Windows environment. Your Sametime community is now SIP-enabled and users in your community can communicate with users in a different SIP-enabled community. Note that the other Windows-based Sametime community must also be "SIP-enabled" by completing the procedures described in this section.

---

### Setting up the SIP Gateway functionality (IBM i5/OS environment)

Use the instructions in this section to set up the SIP Gateway functionality if your Sametime servers run on IBM i5/OS servers.

To set up the SIP Gateway functionality and SIP-enable your Sametime community in an IBM i5/OS server environment, perform the procedures below.

1. **Review the SIP Connector planning considerations (IBM i5/OS environment)**
2. **Installing or enabling the SIP Connector (IBM i5/OS environment)**
3. **Configure the SIP Gateway and SIP Connector parameters (IBM i5/OS environment)**

Detailed instructions for each of these procedures are provided in subsequent topics.

### Review the SIP Connector planning considerations (IBM i5/OS environment)

Reviewing the SIP Connector planning considerations is the first of three procedures required to set up the SIP Gateway functionality in an IBM i5/OS environment.

When using the SIP functionality with Sametime servers that run on IBM i5/OS servers, you have three options for deploying the SIP Connector. You can:

- **Use a standalone SIP Connector** - This option requires you to install a SIP Connector on a separate, dedicated Windows system. Generally, you install a standalone SIP Connector if two communities must communicate by transmitting data over the Internet. Standalone SIP Connectors can also be used to ensure load balancing and continuity of service.

- **Use an integrated SIP Connector** - This option requires you to enable a SIP Connector that resides on the same machine as the Sametime server. Generally, you enable the integrated SIP Connector if two communities can communicate using a corporate intranet and do not need to use the Internet to establish connections.
• **Use both a standalone and integrated SIP Connector** - In cases where a community must communicate with more than one other external community, it may be possible to use both a standalone SIP Connector and an integrated SIP Connector. The standalone SIP Connector can be installed to handle connections for an external community that can be accessed only over the Internet. An integrated SIP Connector can be used to handle connections to a different community that is accessible over the corporate intranet.

These options are discussed in more detail below.

**Using the standalone SIP Connector**

You can install a standalone SIP Connector on a separate machine from the Sametime server. In this scenario, the SIP Connector installs on a separate, dedicated Windows server. The standalone SIP Connector maintains a connection to the SIP Gateway on the Sametime server that resides on the IBM i5/OS machine. The SIP Connector handles connections to and from another SIP-enabled community (or communities) for the SIP Gateway.

Deploying a standalone SIP Connector(s) can provide any or all of the following advantages. You can:

• **Overcome firewall restrictions** - You can deploy a separate SIP Connector to overcome firewall restrictions when two communities must use the Internet to make connections and transmit data.

  For example, you can install the SIP Connector on a machine outside your corporate firewall (in the network DMZ) and install the Sametime server on a machine inside your corporate firewall.

  If the SIP Connector machine is deployed outside the firewall in the network DMZ, the SIP Connector machine must be able to initiate connections to the Sametime server machine inside the firewall. (The default port for these connections is port 1516.)

  To ensure the two machines can communicate through the firewall, you must configure the firewall with a set of access rules that establish trust between the Sametime server and SIP Connector machines. (For example, the access rules might allow those machines to connect to each other through the firewall but prevent other machines from connecting to them). This deployment enables SIP communication to occur between two communities over the Internet while protecting your local Sametime server behind the corporate firewall.

• **Balance the connection handling load for multiple communities** - If you want users in your community to connect to two separate SIP-enabled communities, you have the option of installing two separate SIP Connectors. Installing multiple SIP Connectors can spread the connection handling load among multiple machines. You can configure the SIP Connectors so that each SIP Connector handles the incoming and outgoing connections for only one of the external communities.

• **Ensure continuity of service** - You can also install two SIP Connectors and configure both SIP Connectors to handle connections for the same SIP-enabled community. This configuration ensures that a SIP Connector is available if one SIP Connector machine fails.

  The SIP Connector must be able to receive connections from other SIP-enabled communities on the TCP/IP port 5060 (the default SIP port).

  If you intend to encrypt connections to your SIP-enabled community with the Transport Layer Security (TLS) protocol, the SIP Connector must be able to receive
connections from other SIP-enabled communities on TCP/IP port 5061 (the default TLS/SIP port). For more information, see Encrypting SIP traffic with Transport Layer Security (TLS) later in this chapter.

**Using the integrated SIP Connector**

You can use the integrated SIP Connector that is available on the Sametime 7.0 server following the Sametime 7.0 installation. You can use the integrated SIP Connector if you can establish connections with another community using the corporate intranet (or in any situation in which you do not need the SIP Connector to reside outside the firewall).

You can have one instance of the integrated SIP Connector for each Sametime server on your IBM i5/OS system. If the Sametime servers reside in the same community, each one can be configured to access any of the integrated SIP Connectors associated with the other servers in the community. If the Sametime servers are in different communities, then each server can only access its own integrated SIP Connector.

The integrated SIP Connector must be able to receive connections from other SIP-enabled communities on the TCP/IP port 5060 (the default SIP port).

**Using both a standalone and integrated SIP Connector**

In some multiple community environments, you can use both a standalone and integrated SIP Connector. Using both a standalone and integrated SIP Connector can provide any or all of the following advantages. You can:

- **Connect to communities using both an intranet and the Internet** - You can use an integrated SIP Connector to establish connections with a community using the corporate intranet and a standalone SIP Connector to establish connections with a different community over the Internet.

  For example, assume that Community A must communicate with Community B and Community C. Community A can communicate with Community B using the corporate intranet. However, Community A can only communicate with Community C over the Internet.

  In this case, an integrated SIP Connector can be configured to handle connections between Community A and B. You can deploy a standalone SIP Connector to handle connections between Community A and Community C. The standalone SIP Connector can be used to overcome any Internet firewall restrictions as noted in the "Using the standalone SIP Connector" section above.

- **Balance the connection handling load for multiple communities** - If you want users in your community to connect to two separate SIP-enabled communities, you can use the integrated SIP Connector to connect to one community and install a standalone SIP Connector to connect to the other community. Using multiple SIP Connectors can spread the connection handling load among multiple machines. You can configure the SIP Connectors so that each SIP Connector handles the incoming and outgoing connections for only one of the external communities.

  **Note:** In this deployment, the standalone SIP Connector can handle connections for a community that is accessed using the corporate intranet or a community that is accessed using the Internet.

- **Ensure continuity of service** - You can use both the integrated SIP Connector and the standalone SIP Connector to handle connections for the same SIP-enabled community. This configuration ensures that a SIP Connector is available if one SIP Connector fails.

Chapter 7. Enabling the SIP Gateway 279
Next step: Install or enable the SIP Connector (IBM i5/OS environment)

Installing or enabling the SIP Connector (IBM i5/OS environment)

Installing or enabling a SIP Connector is the second of three procedures required to set up the SIP Gateway functionality in an IBM i5/OS environment.

This topic discusses the following:

- Enabling the integrated SIP Connector on Sametime for iSeries
- Installing the standalone SIP Connector on a Windows system in an IBM i5/OS environment

Each of these procedures is described in detail in a subsequent topic. You can choose to complete one or both procedures, depending on your requirements.

Enabling the SIP Connector on IBM i5/OS

The IBM i5/OS integrated SIP Connector was installed on your system when you installed Sametime 7.0 for i5/OS. If you plan to use the integrated SIP Connector, you must enable it.

To enable the integrated SIP Connector for a particular Sametime server, complete these steps:

1. From any OS/400 command line, type the following command:
   WRKDOMSVR (and press the Enter key)
2. Type option 12 (Work object links) next to the Sametime server and press Enter to display a list of the files and directories in the server data directory.
3. Page down until you find this file: STCommLaunch.dep
4. Type option 2 (Edit) next to the file and press Enter.
5. Remove the "#" from the last line in the file (the line containing "StSIPCon").
6. Press F3 twice to save and exit.
7. Restart your server.

Next step: If you also want to install a separate SIP Connector to support connections to an external community over the Internet, or for load balancing purposes, perform the procedure described in Installing the SIP Connector on a Windows system.

If you do not want to install a separate SIP Connector on a Windows system, continue with the procedure titled Configure the SIP Gateway and SIP Connector parameters (IBM i5/OS environment).

Installing the SIP Connector on a Windows system (IBM i5/OS environment)

To install a SIP Connector on a separate Windows system, follow the instructions in this topic.

SIP Connector system requirements: The system requirements for the SIP Connector on a Windows system are:

- **Processor** - Pentium II with 400 MHz minimum
- **RAM** - 1 GB recommended; 500 MB minimum
- Disk space - 500 MB minimum
- Disk swap space - 64 MB
- Network software - TCP/IP network software installed

**Windows SIP Connector installation procedure:** To install a SIP Connector:

1. You can install the SIP Connector on your Windows system from the Sametime 7.0 for IBM i5/OS CD. Install the SIP Connector from the \SIPConnector directory of the Sametime 7.0 for IBM i5/OS CD.

2. During the installation, you must enter the following:
   a. The IP address or DNS name of a Sametime 7.0 server. This address enables the SIP Connector to locate and connect to the SIP Gateway on the Sametime server.
   b. A SIP Connector name. SIP Connector configuration data is organized under this name. The SIP Connector requires this name to get its configuration parameters. You can use the DNS name of the SIP Connector machine as the SIP Connector name.

The SIP Connector configuration parameters are stored in a CommunityConnector document in the stconfig.nsf database on the Sametime server. You create this document later in this process. These are the only significant parameters required by the SIP Connector installation.

**Next step:** Configure the SIP Gateway and SIP Connector parameters (IBM i5/OS environment)

**Configuring the SIP Gateway and SIP Connector parameters (IBM i5/OS environment)**

Configuring the SIP Gateway and SIP Connector parameters is the last of three procedures required to set up the SIP Gateway functionality in an IBM i5/OS environment.

Configuring the SIP Gateway and SIP Connector parameters is accomplished in four steps. These steps include:

1. **Enabling connections to other communities and enabling e-mail address translation (IBM i5/OS environment)**
2. **Configuring the Community Connectivity parameters (IBM i5/OS environment)**
3. **Configuring the SIP Connector parameters (IBM i5/OS environment)**
4. **Enabling the SIP Connector to authenticate when connecting to the SIP Gateway (IBM i5/OS environment)**

Each of these steps is described in detail in a subsequent topic.

**Enabling connections to other communities and enabling e-mail address translation (IBM i5/OS environment)**

Enabling connections to other communities and enabling e-mail address translation is the first of four steps required to configure the SIP Gateway and SIP Connector parameters in an IBM i5/OS environment.

In this step you perform two separate configurations; you enable connections to other communities and enable e-mail address translation:

- Enabling connections to other communities allows the SIP Gateway to initiate connections to and receive connections from another SIP-enabled community.
• Enabling e-mail address translation ensures that users in your Sametime community can be identified by their Internet e-mail addresses.

Users from another community must specify the Internet e-mail addresses of the users in your community when adding them to contact lists or buddy lists. Enabling e-mail address translation ensures the internal user IDs used by Sametime can be translated to the appropriate Internet e-mail addresses.

**Note:** SIP entities are identified by e-mail address.

To enable connections to other communities and enable e-mail address translation, you must alter settings in the "CommunityGateway" document of the Configuration database (stconfig.nsf). Follow the instructions below:

1. Use a Lotus Notes client to open the stconfig.nsf database on the Sametime 7.0 server.

2. Open the CommunityGateway document by double-clicking on the date associated with the document.

If the CommunityGateway document does not exist in the stconfig.nsf database, you must create it. To create the CommunityGateway document, choose Create-CommunityGateway from the menu bar in the stconfig.nsf database.

3. In the "Support external communities" field, select "True."

Selecting "True" in this field enables the SIP Connector to initiate connections to and receive connections from other SIP-enabled communities.

**Note** To disable connections to other communities, set the "Support external communities" value to "False." Setting this value to "False" is the quickest way to disable all SIP functionality for the community.

4. In the "ConvertID" field, select "True."

Selecting "True" in this field enables e-mail address translation.

**Note** To disable e-mail address translation, set the "ConvertID" field to "False."

5. Save the CommunityGateway document.

6. Leave the stconfig.nsf database open. The next step involves creating and modifying a document in this database.

**Note** You must enable e-mail address translation on every Sametime server in the community. Repeat the procedure above in the Configuration database of every Sametime server in the community.

**Next step:** Configuring Community Connectivity parameters (IBM i5/OS environment)

**Configuring the Community Connectivity parameters (IBM i5/OS environment)**

Configuring community connectivity parameters is the second of four steps required to configure the SIP Gateway and SIP Connector parameters.

In this procedure, the administrator creates an ExternCommunity document in the Sametime Configuration database (stconfig.nsf). The administrator uses the settings in this ExternCommunity document to specify the parameters that enable the SIP Gateway to connect to another SIP-enabled community.

The connectivity parameters specified in this procedure include:

• A name for the external community

• The DNS domains that comprise the external community
• The DNS name of the SIP proxy (or SIP Connector) for the external community
• The port used to connect to the SIP proxy that handles connections for the external community

To configure the community connectivity parameters:
1. Open the ExternCommunity document in the stconfig.nsf database by double-clicking on the date associated with the document.
   If the ExternCommunity document does not exist in the stconfig.nsf database, you must create it. To create the ExternCommunity document, choose Create-Other-ExternCommunity from the menu bar in the Configuration database (stconfig.nsf).
2. In the "Community Name" field, enter a name for the community. The name is at your discretion. You might want to choose a name that represents the organization associated with this community. (For example, IBM).
3. In the "Domains" field, enter the domain names associated with the instant messaging community of the organization specified above. This entry can consist of one domain name, or a group of domain names. You can also use wildcards when specifying domain names. For example, *.ibm.com, lotus.com, tivoli.com, ubique.com.
4. In the "DNS" field, enter the fully-qualified DNS name of the SIP proxy that handles connections for the other SIP-enabled community. The SIP Connector attempts to connect to this SIP proxy (or SIP Connector for another Sametime community).
   If you leave the "DNS" field blank, Sametime performs a DNS lookup to locate the SIP proxy associated with the domain(s) specified above. If Sametime is unable to locate a SIP proxy, Sametime attempts a SIP connection to the domain(s) using the port specified below.
5. In the "Port" field, enter the port the SIP Connector uses when attempting SIP connections to the SIP proxy or domain(s) specified above. The default port for SIP connections is port 5060.
6. Set the "Encryption" field to "Disabled" unless you intend to encrypt SIP connections between communities with Transport Layer Security (TLS). For more information, see "Encrypting SIP traffic with Transport Layer Security (TLS)" later in this chapter.
7. Leave the "Certificate distinguished" name field blank unless you intend to require client certificate authentication for connections between SIP Connectors. For more information, see "Enabling client certificate authentication" later in this chapter.
8. Leave the stconfig.nsf database open. The next step involves creating and modifying a document in this database.

Next step: Configuring SIP Connector parameters (IBM i5/OS environment)

Configuring the SIP Connector parameters is the third of four steps required to configure the SIP Gateway and the SIP Connector parameters.

In this procedure, the administrator creates a CommunityConnector document in the Sametime Configuration database (stconfig.nsf). The administrator uses the settings in this CommunityConnector document to specify the parameters that control the functioning of the SIP Connector.
The SIP Connector parameters include:

- The name of the SIP Connector machine
- The IP address of the SIP Connector machine
- The port on which the SIP Connector listens for connections
- The names of the communities for which the SIP Connector handles connections (these names are defined in the ExternCommunity document created in the previous procedure).

Note that if you are using multiple SIP Connectors, you must create a separate CommunityConnector document for each SIP Connector. Repeat the steps below for each SIP Connector.

To configure the SIP Connector parameters:

1. Open the CommunityConnector document in the stconfig.nsf database by double-clicking on the date associated with the document.

   If the CommunityConnector document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnector document, choose Create-CommunityConnector from the menu bar in the Configuration database (stconfig.nsf).

2. In the "Connector Name" field, enter a name for the SIP Connector.

   Generally, the DNS name of the machine on which the SIP Connector is installed is used as the Connector Name. If you are using the IBM i5/OS integrated SIP Connector, specify the fully qualified host name of the Sametime server associated with the integrated SIP Connector.

   If you installed a standalone SIP Connector, you specified a SIP Connector name during the SIP Connector installation. The "Connector Name" field should contain the name specified for the SIP Connector during the SIP Connector installation.

3. In the "IP" field, enter the IP address of the machine on which the SIP Connector is installed. The SIP Connector listens for SIP connections on this IP address.

   If you are using the IBM i5/OS integrated SIP Connector, specify the fully qualified host name of the Sametime server associated with the integrated SIP Connector. Do not leave this field blank on an IBM i5/OS server.

   If you are using a standalone SIP Connector, specify the fully qualified host name of the machine on which the SIP Connector is installed.

4. In the "Port" field, enter 5060. The SIP Connector listens for SIP connections from the SIP Gateway or another SIP-enabled community on this port. Port 5060 is the default port for SIP connections.

   Note that if the "IP" field is blank, and the "Port" field specifies 0 (zero), the SIP Connector will not listen for clear text (or unencrypted) SIP connections. A SIP Connector in another community cannot make an unencrypted SIP connection to the SIP Connector.

5. (Optional) In the "TLS IP" field, enter the IP address of the machine on which the SIP Connector is installed. The SIP Connector listens for TLS-encrypted SIP connections on this IP address.

   If this field is left blank, the SIP Connector listens for TLS-encrypted SIP connections on all IP addresses assigned to the SIP Connector machine.

   The "TLS IP" field is only relevant if you use TLS to encrypt connections between the SIP-enabled communities. For more information, see "Encrypting SIP traffic with Transport Layer Security (TLS)" later in this chapter.
6. (Optional) In the "TLS Port" field, enter the port number on which the SIP Connector will listen for TLS-encrypted connections. The default port number for these connections is port 5061.

Note that if the "TLS IP" field is blank, and the "TLS Port" field specifies 0 (zero), the SIP Connector will not listen for TLS-encrypted SIP connections. The "TLS Port" field is only relevant if you use TLS to encrypt connections between the SIP-enabled communities. For more information, see "Encrypting SIP traffic with Transport Layer Security (TLS)" later in this chapter.

7. In the "Supported Communities" field, enter the names of the communities for which this SIP Connector will handle connections. These are the "Community Names" as defined in the ExternCommunities documents created when you configured the community connectivity parameters in the previous procedure.

8. Choose File - Save to save the CommunityConnector document.

9. Leave the stconfig.nsf database open. The next step involves creating and modifying a document in this database.

Next step: Enabling the SIP Connector to authenticate when connecting to the Sametime server (IBM i5/OS environment)

Enabling the SIP Connector to authenticate when connecting to the SIP Gateway (IBM i5/OS environment)

Enabling the SIP Connector to authenticate when connecting to the SIP Gateway on the Sametime server is the last of four steps required to configure the SIP Gateway and the SIP Connector.

A SIP Gateway on Sametime server will only accept connections from SIP Connectors that are listed in its stconfig.nsf database on the Sametime server. Specifically, the IP addresses of all SIP Connectors that connect to a SIP Gateway on a Sametime server must be listed in the "Community/TrustedIps" field of the "CommunityConnectivity" document in the stconfig.nsf database.

Sametime uses the IP address of the SIP Connector machine to authenticate connections from the SIP Connector (or verify that the SIP Connector is known to the Sametime server/SIP Gateway). Using the IP address for authentication prevents a SIP Connector on an unauthorized machine from connecting to the SIP Gateway on a Sametime server.

If you are using the IBM i5/OS integrated SIP Connector associated with your Sametime server, the IP address of the SIP connector is the same as the IP address of your Sametime server. Therefore, you do not need to add anything to the trusted IP field. Only SIP connectors that run on an IP address that is different from your Sametime server need to be added to the trusted IP field. That is, you must update the trusted IP field if your Sametime server communicates with a SIP Connector installed on a Windows system or an IBM i5/OS integrated SIP Connector associated with a different Sametime server in the same community.

To enable the SIP Connector to authenticate when connecting to the Sametime server:

1. Open the CommunityConnectivity document in the stconfig.nsf database by double-clicking on the date associated with the document.

If the CommunityConnectivity document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnectivity document, choose Create-CommunityConnectivity from the menu bar in the stconfig.nsf database.
2. In the "CommunityTrustedIps" field, enter the IP address(es) of the SIP Connector machine(s).
   
   **Note** The IP addresses of Community Services multiplexer machines associated with a Community Services cluster are also entered in this field.

3. Save and close the CommunityConnectivity document.
   
   **Note** Sametime SIP Connectors can also be deployed with Sametime servers that operate as part of a Community Services cluster.

After you enable the SIP Connector to authenticate you have completed all procedures required to set up the SIP Gateway in an IBM i5/OS environment. Your Sametime community is now SIP-enabled and users in your community can communicate with users in a different SIP-enabled community.

---

**Disabling the SIP Gateway functionality**

You can disable the SIP Gateway functionality if you want to prevent users in your community from using SIP to communicate with users in a different community.

The easiest way to disable the SIP Gateway functionality is to prevent the SIP Gateway from making connections to or receiving connections from another community. To disable this functionality, follow the instructions below.

1. Use a Lotus Notes client to open the Configuration database (stconfig.nsf) on the Sametime server machine.
2. Open the CommunityGateway document by clicking on the date associated with it.
3. In the "Support external communities" field, select "False."
4. Choose File - Save to save the CommunityGateway document.

---

**Encrypting SIP traffic with Transport Layer Security (TLS)**

Encrypting SIP traffic with Transport Layer Security (TLS) is an optional procedure that provides the highest level of security for the SIP Gateway functionality. The administrator can use TLS to encrypt sensitive information (such as user e-mail addresses and chat text) that is transmitted between two SIP-enabled communities. Audio/video data cannot be encrypted.

In addition to encrypting SIP traffic with TLS, the administrator can also configure the SIP Connector to support client certificate authentication. Client certificate authentication is an optional security configuration that requires a SIP Connector in another community to present a client certificate when connecting to the SIP Connector in your community. This client certificate is used to authenticate the remote SIP Connector.

**Note:** All of the procedures in this section apply to all SIP Connectors in every environment (Windows, AIX, Solaris, and IBM i5/OS) with the exception of procedure 3. In procedure 3, the certificate management procedures you must perform depend on whether you are encrypting traffic for an integrated SIP Connector on an IBM i5/OS machine or a standalone SIP Connector installed on a Windows machine.

To encrypt SIP traffic with TLS, you must perform the procedures below.

1. **Specify the host name and port for TLS-encrypted connections**
2. **Set the TLS encryption mode**
3. Depending on your environment see:
   - Managing the certificates required for TLS connections (integrated SIP Connector on IBM i5/OS)
   - Managing the certificates required for TLS connections (standalone SIP Connector on Windows)

4. Enabling client certificate authentication for a standalone SIP Connector on a Windows machine (optional)

**Specify the host name and port for TLS connections**

Specifying the host name and port number for TLS-encrypted connections is the first of three procedures required to encrypt SIP traffic between two SIP-enabled communities.

In this procedure, you specify the host name and port number on which a SIP Connector will listen for TLS-encrypted connections from another SIP-enabled community.

The SIP Connector will also use the port number specified in this procedure to attempt TLS-encrypted connections to the other community.

These host name and port settings are specified in the CommunityConnector document in the Configuration database (stconfig.nsf) on the Sametime server.

To specify the host name and port for TLS connections, follow the steps below:

1. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime 7.0 server on which you have enabled the SIP Gateway functionality.

2. Open the CommunityConnector document by double-clicking on the "Last modified date" associated with the document.

3. Enter values in the "TLS IP" and the "TLS Port" fields in the CommunityConnector document as described below:

   - **TLS IP** - This field specifies the IP address on which the SIP Connector listens for TLS-encrypted SIP connections from another SIP-enabled community (or communities).
     
     If you leave the TLS IP field blank, the SIP Connector listens for TLS-encrypted connections on all IP addresses assigned to the SIP Connector machine. By default, this setting is blank and the SIP Connector machine listens for connections on all IP addresses.

   - **TLS Port** - This field specifies the port on which the SIP Connector listens for TLS-encrypted SIP connections from the external community (or communities) supported by this SIP Connector. The default setting is port 5061.

     **Note:** The SIP Connector initiates connections to another community using the port number specified in the ExternCommunity document.

     If the fields above do not contain the appropriate values, double-click on the CommunityConnector document to put the document in edit mode. Edit the fields as needed and save the CommunityConnector document.


5. Leave the stconfig.nsf database open. The next step requires you to modify a document in this database.
Next step:

Set the TLS encryption mode

Set the TLS encryption mode

Setting the TLS encryption mode is the second of three procedures required to encrypt SIP traffic between two SIP-enabled communities.

In this procedure, you specify the way in which the SIP Connector attempts TLS-encrypted SIP connections to another community. Your options for the TLS encryption mode include "enabled," "mandatory," or "disabled." Each of these options is discussed below.

- **Enabled** - If you select the "enabled" encryption mode, the SIP Connector first attempts a TLS-encrypted connection to the other community on the TLS port specified in the CommunityConnector document (default port 5061). If the TLS-encrypted connection fails, the SIP Connector attempts an unencrypted SIP connection to the other community. The unencrypted SIP connection is attempted on the SIP port specified in the CommunityConnector document (default port 5060).

- **Mandatory** - If you select the "mandatory" encryption mode, the SIP Connector attempts a TLS-encrypted connection to the other community on the TLS port specified in the CommunityConnector document (default port 5061). If the TLS-encrypted connection fails, the SIP Connector does not attempt an unencrypted connection.

- **Disabled** - If you select "disabled" as the encryption mode, the SIP Connector attempts an unencrypted SIP Connection to the other community on the SIP port specified in the CommunityConnector document (default port 5060). The SIP Connector does not attempt a TLS-encrypted connection.

To set the TLS encryption mode:

1. Open the ExternCommunity document by double-clicking on the "Last modified date" associated with the document.
2. From the Encryption drop-down list, select either "Enabled," "Mandatory," or "Disabled."
3. The Certificate distinguished name field should be left blank unless you intend to support client certificate authentication. For more information, see [Enabling client certificate authentication (optional)] later in this document.
4. Save and close the ExternCommunity document.

Next step:

See the topic that is appropriate for your environment:

- Managing the certificates required for TLS connections (integrated SIP Connector on IBM i5/OS)
- Managing the certificates required for TLS connections (standalone SIP Connector on Windows)

Managing the certificates required for TLS connections (integrated SIP Connector on IBM i5/OS)

Follow the procedures in this topic only if you are using TLS to encrypt connections to an integrated SIP Connector on an IBM i5/OS machine. The procedures in this topic can also be used to enable client authentication for the integrated SIP Connector.
Note: For instructions on managing certificates for a standalone SIP Connector installed on a Windows machine, see Managing the certificates required for TLS connections (standalone SIP Connector on Windows).

Certificates are required for both TLS encryption and for client authentication. You can choose to enable TLS encryption alone or you can enable TLS encryption with client authentication. You cannot implement client authentication without TLS encryption.

On IBM i5/OS systems, certificates are managed using the integrated Digital Certificate Manager (DCM), rather than IKeyMan. To use the Digital Certificate Manager, you must install the following software products on the IBM i5/OS server where you are running the integrated SIP connector:

- 5722-SS1 Option 34, Digital Certificate Manager
- 5722-DG1, IBM HTTP Server for IBM i5/OS
- 5722-AC2, Crypto Access Provider 56-bit for AS/400 or 5722-AC3, Crypto Access Provider 128-bit for AS/400

The remainder of this topic outlines the tasks required to implement TLS encryption on an IBM i5/OS integrated SIP connector. If you need more detailed information about using DCM in order to complete the steps, see the IBM i5/OS Information Center at http://www.ibm.com/as400/infocenter. Select the "Digital Certificate Manager" topic in the "Security" section.

To enable TLS encryption, complete the following steps on the IBM i5/OS system where you are running the integrated SIP connector:

1. Define the Server Certificate in the Digital Certificate Manager (DCM)

   - The server certificate for your integrated SIP Connector must be imported into the DCM *SYSTEM certificate store and it must be signed by a certificate authority (CA) that is trusted by the external community’s SIP connector.
   - Well-known public Internet Certificate Authorities (CA) that most web browsers can recognize readily, such as VeriSign, are included in the DCM. If you are using a private certificate authority, you must import the CA’s certificate into the DCM *SYSTEM certificate store.
   - If you are implementing client authentication, you must also have a certificate for the CA that signed the server certificate for the external community’s SIP connector. Again, this can either be a public Internet Certificate Authority (CA) that is already included in the DCM or you can import the certificate for a private certificate authority.
   - The following public Internet Certificate Authorities (CA) are included in the DCM:
     - Microsoft Root Authority
     - Thawte Personal Premium CA
     - Thawte Personal Freemail CA
     - Thawte Personal Basic CA
     - Thawte Premium Server CA
     - Thawte Server CA
     - RSA Secure Server Certification Authority
     - VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
     - VeriSign Class 2 CA Individual Subscriber-Persona Not Validated
     - VeriSign Class 3 CA Individual Subscriber-Persona Not Validated

Chapter 7. Enabling the SIP Gateway 289
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority

2. Define the DCM Server Application in the Digital Certificate Manager (DCM)
This is a DCM Application Definition that is used when the integrated SIP Connector accepts incoming connections from an external community. That is, the integrated SIP Connector is acting as a server in the context of the TLS connection handshake.

Specify the following when creating the DCM Server Application:
- Type="Server"
- A unique identifier for the Application ID, such as
  SAMETIME_SERVER_MyServerName
- If you are not implementing client authentication, specify "Client authentication supported" = no
- If you are implementing client authentication, also specify:
  "Define the CA trust list" = yes
  "Client authentication supported" = yes
  "Client authentication required" = yes

Select "Update certificate assignment" to specify the server certificate for your integrated SIP Connector. This is the server certificate described in Step 1.
If you are implementing client authentication, select "Define CA Trust List" to specify a Certificate Authority (CA) trust list that includes the certificate authority that signed the server certificate used by the external community.

3. Define the DCM Client Application in the Digital Certificate Manager (DCM)
This is a DCM Application Definition that is used when the integrated SIP Connector is initiating a connection to an external community. That is, the integrated SIP Connector is acting as a client in the context of the TLS connection handshake.

Specify the following when creating the DCM Client Application:
- Type="Client"
- A unique identifier for the Application ID, such as
  SAMETIME_CLIENT_MyServerName
- "Define the CA trust list" = yes

Select "Define CA Trust List" to specify a Certificate Authority (CA) trust list that includes the certificate authority that signed the server certificate used by the external community.
If you are implementing client authentication, select "Update certificate assignment" to specify the server certificate for your integrated SIP Connector. This is the server certificate described in Step 1.

4. Add entries to the [External Community] section of thesametime.ini file to specify the DCM application IDs. For example:
  ConnectorServerApplicationId=SAMETIME_SERVER_MyServerName
  ConnectorClientApplicationId=SAMETIME_CLIENT_MyServerName

5. Ensure that the QNOTES user profile has the proper authority to the DCM certificate store by running the following commands from any OS/400 command line:

CHGAUT OBJ('QIBM/USERDATA/ICSS/CERT/Server') USER(QNOTES) RTAAUT(*RX)
CHGAUT OBJ('QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.RDB') USER(QNOTES) RTAAUT(*RX)
CHGAUT OBJ('QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.KDB') USER(QNOTES) RTAAUT(*RX)
Note that these procedures must be performed both on the SIP Connector in your community and the SIP Connector on the community to which you are connecting.

**Managing the certificates required for TLS connections**  
(standalone SIP Connector on Windows)

Follow the procedures in this section only if you are using TLS to encrypt connections to a standalone SIP Connector on a Windows machine.

**Note:** For instructions on managing certificates for an integrated SIP Connector on an IBM i5/OS machine, see [Managing the certificates required for TLS connections (integrated SIP Connector on IBM i5/OS)](chapter7.html).

Managing the certificates required for Transport Layer Security (TLS) connections is the last of three procedures required to encrypt SIP traffic between two SIP-enabled communities.

Similar to the Secure Sockets Layer (SSL) protocol, the TLS protocol relies on certificates for authentication and encryption. This section discusses the certificate management issues and procedures associated with encrypting SIP traffic between two SIP-enabled communities.

When your SIP-enabled Sametime community is configured to communicate with another SIP-enabled community, either community can initiate a connection with the other community. Essentially, this means that the SIP Connector in each community can operate as either the server or the client in a TLS connection handshake. To support TLS, you must ensure that the SIP Connector has access to the certificates that enable the SIP Connector to operate as either a server or a client in a TLS connection handshake.

To manage the certificates required for TLS connections for a standalone SIP Connector on a Windows machine, you must perform both of the following procedures:

1. Ensure the SIP Connector can operate as a server in a TLS handshake
   This procedure includes the following steps:
   a. Install the IKeyMan program on the SIP Connector machine
   b. Use the IKeyMan program to create a key database on the SIP Connector machine
   c. Identify the signer (or "trusted root") certificate you will use
   d. Create and submit a server certificate request
   e. Import the server certificate into the key database

2. Ensure the SIP Connector can operate as a client in a TLS connection handshake

Each of these procedures is described in subsequent topics. Note that these procedures must be performed both on the SIP Connector in your community and the SIP Connector on the community to which you are connecting.

**Ensure the SIP Connector can operate as a server in a TLS handshake**

Ensuring the SIP Connector can operate as a server in a TLS handshake is the first of two procedures associated with managing the certificates required encrypt connections to a standalone SIP Connector on a Windows machine.
When a SIP Connector in another SIP-enabled community initiates a TLS-encrypted SIP connection to the SIP Connector in your community, the SIP Connector in your community must operate as the server in the TLS connection handshake.

To operate as a server in a TLS handshake, the SIP Connector must have all of the following:
- A key database (this database is created by the IKeyMan program).
- The key database must contain a signer (or “trusted root”) certificate.
- The key database must also contain a separate server certificate signed by the same Certificate Authority (CA) as the signer certificate.

To ensure that the SIP Connector meets all of these requirements, you must perform these five steps:
1. **Install the IKeyMan program on the SIP Connector machine**
2. **Use the IKeyMan program to create a key database on the SIP Connector machine**
3. **Identify the signer (or “trusted root”) certificate you will use**
4. **Create and submit a server certificate request**
5. **Import the server certificate into the key database**

Each of these procedures is described in a subsequent topic.

**Install the IKeyMan program on the SIP Connector machine:** Installing the IKeyMan program on the SIP Connector machine is the first of five steps required to ensure that a SIP Connector on a Windows machine can operate as a server in a TLS connection handshake.

To Install the IKeyMan program on the SIP Connector machine.
1. Create a directory named “GSKit” on the SIP Connector machine.
2. Insert the Sametime 7.0 server CD 2 into the CD drive on the SIP Connector machine.
3. Copy the contents of the GSKit directory on the Sametime 7.0 server CD 2 to the GSKit directory on the SIP Connector machine.
4. Open a command prompt on the SIP Connector machine.
5. In the command prompt window, change to the drive and "GSKit” directory to which you have copied the GSKit contents.
   (For example, enter “cd GSKit” at the command prompt to change to the directory containing the GSKit setup.exe file.)
6. Enter the following command in the command prompt:
   ```
   setup.exe GSKit <SIP Connector installation directory> -s flsetup.iss
   ```
   In the command string above, <SIP Connector installation directory> is the directory path in which the SIP Connector is installed. For example, if the SIP Connector is installed in a directory named SIP, your command string would look like this:
   ```
   C:\GSKit>setup.exe GSKit C:\SIP -s flsetup.iss
   ```
   This command line performs a silent installation of the IKeyMan program into the SIP Connector installation directory.
7. To verify that the installation is successful, do the following:
   - Check that the C:\<SIP Connector installation directory>\IBM\GSK6 folder exists on the SIP Connector computer.
• Verify that the HKLM\Software\IBM\GSK6 registry key has been created on the SIP Connector computer.

8. After installing the IBM IKeyMan utility, you must define the Java environment on the SIP Connector machine. Follow the steps below:
   a. Copy the ibm-jre directory from the Sametime server to the SIP Connector machine. The ibm-jre directory is located in the <root>\lotus\domino directory on the Sametime server. Copy the ibm-jre directory (including its subdirectories) to the SIP Connector installation directory on the SIP Connector machine. When you have completed this operation, the following directory structure should exist on the SIP Connector machine:
      C:\<SIP Connector installation directory>\ibm-jre\jre
   b. From the Windows desktop, right click on the My Computer icon and select "System Properties."
   c. Select the "Advanced" tab.
   d. Click the "Environment Variables" button.
   e. For "System Variables," select "New."
   f. Enter the following in the Variable Name and Variable Value fields:
      **Variable Name:** JAVA_HOME
      **Variable Value:** C:\<SIP Connector installation directory>\ibm-jre\jre

9. Use a text editor to add "com.ibm.spi.IBMCMSPProvider" to the list of providers in the C:\<SIP Connector installation directory>\ibm-jre\jre\lib\security\java.security file. Follow the steps below:
   a. Use a text editor to open the java.security file located in the directory path shown above on the SIP Connector machine.
   b. Type the following line into the list of security providers:
      security.provider.3=com.ibm.spi.IBMCMSPProvider. The example below illustrates this line added to the java.security file:
      ```
      #
      # List of providers and their preference orders (see above)
      #
      security.provider.1=sun.security.provider.Sun
      security.provider.2=com.ibm.crypto.provider.IBMJCE
      security.provider.3=com.ibm.spi.IBMCMSPProvider
      ```
   c. In this procedure, you use IKeyMan to create the key database that is used to store the trusted root and server certificates required by the TLS handshake.

Next step: Use the IKeyMan program to create a key database on the SIP Connector machine

Use the IKeyMan program to create a key database on the SIP Connector machine: Using the IKeyMan program to create a key database on the SIP Connector machine is the second of five steps required to ensure the a SIP Connector on a Windows machine can operate as a server in a TLS connection handshake.

In this procedure, you use IKeyMan to create the key database that is used to store the trusted root and server certificates required by the TLS handshake.

To create the key database:

1. Start the IKeyMan program on the SIP Connector machine. To start the program, run the gsk6km.exe file located in the C:\<SIP Connector installation directory>\IBM\gsk6\bin directory on the SIP Connector machine.
   **Note:** You can also start IKeyMan from the Windows Start-Programs button.
2. From the menu bar, select Key Database File - New....

3. In the New window, complete these fields:
   - **Key database type** - Select "CMS key database file."
   - **File Name** - Enter "key.kdb" as the file name for the key database. The key database must have the filename of key.kdb.
   - **Location** - The location must specify the directory in which the SIP Connector is installed.

   Click OK.

4. In the Password prompt window, do the following:
   - Type a password and confirm the password. The password is at your discretion. You will be required to enter this password when you open the key database to add or remove a certificate, or create a certificate request.
   - Select the "Stash the password to a file?" Check box.

   Click OK.

   An information window appears indicating the password is encrypted and saved in the location:

   `<SIP Connector installation path>\key.kdb`

   **Next step:** [Identify the signer (or "trusted root") certificate you will use](#)

**Identify the signer (or trusted root) certificate you will use:** Identifying the signer (or "trusted root") certificate you will use is the third of five steps required to ensure that a SIP Connector on a Windows machine can operate as a server in a TLS connection handshake.

To operate as a server in a TLS connection handshake, the SIP Connector must have access to two certificates:

- An SSL signer (or "trusted root") certificate signed by a specific Certification Authority (CA), such as VeriSign
- An SSL server certificate signed by the same CA as the signer certificate.

**Note:** Both SSL and TLS connections use SSL certificates. A TLS connection does not require a TLS certificate.

In this procedure, you identify the signer certificate that you want to use as the trusted root certificate. In a subsequent procedure, you must request a server certificate from the same Certification Authority (CA) that created the signer certificate.

The key database created in the previous procedure contains several signer certificates by default. Use the procedure below to view the available signer certificates that are provided by default in the key database.

1. If necessary, start the IKeyMan program by running the gsk6ikm.exe file located in the `<SIP Connector installation directory>\IBM\GSK6` directory on the SIP Connector machine.

2. Select Key Database File-Open to open the SIP Connector key database ("key.kdb" in this example).

3. In the Key database content drop-down list, select "Signer Certificates" to display the list of CA trusted root certificates provided by default. This list includes:
   - RSA Secure Server Certification Authority
   - Thawte Personal Basic CA
4. Identify the Signer Certificate you want to use as the trusted Certificate Authority (CA). In the next procedure, you must request a server certificate from the same CA.

**Note:** If you do not want to use one of the default signer certificates, you can also request a signer certificate from another CA. Generally, you must browse to the Cas web site and follow the instructions on the web site to request a signer certificate from another CA. When you receive the signer certificate from the CA, you must add the signer certificate to the key.kdb database as a Signer certificate. You use the “Import” feature of the IKeyMan key.kdb database to add the certificate.

Note also that Domino servers include Certificate Authority applications. Using a Domino Certificate Authority application can prevent you from having to pay for certificates. For information on using a Domino server Certificate Authority application, see the Domino server administration documentation.

**Next step:** [Create and submit a server certificate request](#)

**Create and submit a server certificate request:** Creating and submitting a server certificate request is the fourth of five steps required to ensure that a SIP Connector on a Windows machine can operate as a server in a TLS connection handshake.

After you have chosen the CA that will provide the signer (or "trusted root") certificate, you must request a separate server certificate from that CA. For example, if you elect to use the "VeriSign Class 1 Public Primary Certification Authority” certificate as the signer certificate, you must request a separate server certificate from VeriSign.

To request a server certificate, you use the IKeyMan program to create a certificate request. After creating this request, you must submit it to a CA.

To create a server certificate request:
1. If necessary, start the IKeyMan program by running the gsk6ikm.exe file located on the SIP Connector machine.
2. Select Key Database File-Open and open the "key.kdb" database created earlier.
3. In the "Key database content" drop-down list, select "Personal Certificate Requests.”
4. On the right-hand side of the "Key database content" box, click the "New..." button.
5. In the "Create New Key and Certificate Request" window, complete the following fields.
   • **Key Label** - The Key Label is at your discretion. The key label identifies the server certificate in IKeyMan lists. You should provide a Key Label that indicates the certificate is a server certificate (for example, "VeriSignServerCert.")
   • **Key Size** - Select "1024."
   • **Common name** - Enter the fully-qualified DNS name of the machine that contains the SIP Connector (for example, sipconnector1.ibm.com).
   • **Organization** - Enter the organization with which the server is associated. For example, "IBM."
   • **Country** - Select the country in which your server is located.
   • **Enter the name of a file in which to store the certificate request** - Specify a directory path and file name in which to store the certificate request. In this example, the certificate request will be stored in the file "TLScertreq.arm."

6. Click OK. The certificate request is stored as a text file.
7. Submit the certificate request to the CA (see the notes below).

**Notes on submitting a server certificate request to a CA:** The procedure to submit a server certificate request can vary for each CA. Usually, you submit the request by providing the CA with the certificate request file ("TLScertreq.arm" in this example) or by copying the contents of the certificate request file to your Windows clipboard and pasting these contents into a field in a web page on the CA's web site.

After you request the server certificate, the CA will notify you when the signed certificate is available and explain how to pick up the certificate.

Note also that Cas charge a fee for these certificates. If you use the Domino server Certificate Authority application as your CA, you can request the CA server certificate from the Domino CA application and avoid this fee. For more information on using the Domino CA application, see the Domino server administration documentation.

**Next step:** Import the server certificate into the key database

**Import the server certificate into the key database:** Importing the server certificate into the key database is the last of five steps required to ensure that a SIP Connector on a Windows machine can operate as a server in a TLS connection handshake.

To import the server certificate into the key database:
1. Use IKeyMan to open the "key.kdb" database created earlier in this procedure.
2. On the right-hand side of the "Key database content" box, click the "Receive..." button.
3. In the "Receive Certificate from a file" window, complete the following fields:
   • **Data type** - Accept the default of "Base64-encoded ASCII data."
   • **Certificate file name** - Browse to and select the signed server certificate you received from the CA (as described in the previous procedure titled "Create and submit a server certificate request.")
   • **Location** - Ensure the location field specifies the directory path to which the signed certificate was saved after you received it from the CA.
4. Click OK.

You should now see the server certificate name displayed in the Personal Certificates list in IKeyMan.

_next step:_ This concludes the procedures required to ensure that a SIP Connector on a Windows machine can operate as a server in a TLS connection handshake. Next, you must perform the procedures required to ensure the SIP Connector can operate as a client in a TLS handshake.

**Ensure the SIP Connector can operate as a client in a TLS handshake**

Ensuring the SIP Connector can operate as a client in a TLS handshake is the last of two procedures associated with managing the certificates required to encrypt SIP connections to a standalone SIP Connector installed on a Windows machine.

To ensure the SIP Connector meets all requirements to operate as a client in a TLS handshake, you must ensure the SIP Connector has access to the appropriate SSL certificate.

When the SIP Connector in your community initiates a TLS-encrypted connection to a SIP Connector in another community, the SIP Connector in the other community will send its SSL server certificate to your SIP Connector. The SIP Connector in your community requires this server certificate to negotiate encryption levels and ensure the data exchanged with the other SIP Connector is encrypted.

To ensure the server certificate of the SIP Connector from the other community can be used to accomplish encryption, the key database on the SIP Connector in your community must contain one of the following certificates:

- A signer (or "trusted root") certificate signed by the same CA as the server certificate sent to your SIP Connector by the SIP Connector in the other community.

  For example, if the SIP Connector in the other community sends a server certificate signed by VeriSign, the SIP Connector in your community must have access to a signer (or "trusted root") certificate signed by VeriSign to establish trust with the other SIP Connector.

- A copy of the signed server certificate that is sent by the SIP Connector in the other community. The SIP Connector in your community can also establish trust with the other SIP Connector if the SIP Connector in your community has access to a copy of the server certificate sent by the other SIP Connector.

In many cases, the key databases on both SIP Connectors will have the appropriate trusted root certificates by default and no procedures will be necessary to ensure that the SIP Connector in one community can operate as a client to the SIP Connector in the other community.

If it is necessary to obtain a copy of the server certificate of the other SIP Connector, the IKeyMan program on the SIP Connector in the other community can be used to export (or extract) the server certificate from the key database.

The server certificate must then be sent in some secure way (for example, on a floppy disk using registered mail) to your location. The IBM IKeyMan program on your SIP Connector can then be used to import the server certificate into the key database on your SIP Connector.
After you ensure the SIP Connector can operate as a client in a TLS handshake, you have completed all procedures required to encrypt SIP traffic with TLS.

Note that all procedures described in this section must be performed for the SIP Connector in your community and the SIP Connector in the other community to ensure data transmitted between the SIP Connectors is encrypted.

### Enabling client certificate authentication for a standalone SIP Connector on a Windows machine (optional)

Enabling client certificate authentication is an optional procedure that requires a SIP Connector to authenticate when connecting to a SIP Connector in another community.

**Note:** The procedures in this section explain how to enable client certificate authentication for a standalone SIP Connector on a Windows machine. To enable client certificate authentication for an integrated SIP Connector on an IBM i5/OS machine, see Managing the certificates required for TLS connections (integrated SIP Connector on IBM i5/OS).

Client certificate authentication requires a SIP Connector to present a separate client certificate when initiating a connection (or operating as a client) to a SIP Connector in another community. The SIP Connector in the other community uses this client certificate to verify the identity of the client SIP Connector.

Client certificate authentication is a separate security process from encrypting SIP connections with TLS (described earlier in this chapter). Client certificate authentication verifies the identity of the connecting server while encryption protects the data from being read by an unauthorized user or attacker.

To illustrate client certificate authentication, consider the following basic example in which SIP Connector A operates in one community while SIP Connector B operates in a separate community.

1. SIP Connector A initiates a connection (or operates as a client) to SIP Connector B.
2. SIP Connector B requests a client certificate from SIP Connector A.
3. SIP Connector B authenticates SIP Connector A based on the data provided on this client certificate.

For client certificate authentication to be accomplished in this scenario, SIP Connector A must be configured to operate as the client to SIP Connector B in the connection handshake. Similarly, SIP Connector B must be configured to operate as a server in the connection handshake to validate the identity of SIP Connector A based on the client certificate presented by SIP Connector A. Instructions for each of these procedures are provided in the following topics:

- [Enabling a SIP Connector to operate as a client when client certificate authentication is required](#)
- [Enabling a SIP Connector to require client certificate authentication](#)
Enabling a SIP Connector to operate as a client when client certificate authentication is required

Enabling the SIP Connector to operate as a client when client authentication is required is the first of two procedures associated with enabling client certificate authentication for a standalone SIP Connector on a Windows machine.

In this procedure, you must request a client certificate (or "Personal" certificate) from a Certificate Authority (CA) and merge this certificate into the key database on the SIP Connector.

The procedures required to request a client (or "Personal" certificate) from a Certificate Authority (CA) are identical to the procedures discussed earlier in this document in the section titled "Ensure the SIP Connector can operate as a server in a TLS handshake." These procedures are summarized below:

1. Install the IKeyMan program on the SIP Connector machine
2. Use the IKeyMan program to create a key database on the SIP Connector machine
3. Identify the signer (or "trusted root") certificate you will use
4. Create and submit a server certificate request (See the notes below.)
5. Import the server certificate into the key database

If you have already performed these procedures, you have completed all steps necessary to enable a SIP Connector to operate as a client when client authentication is required by the SIP Connector in another community. If you have not performed these procedures, you can follow the procedures described in "Ensure the SIP Connector can operate as a server in a TLS handshake" to enable a SIP Connector to operate as a client when client authentication is required.

Notes concerning "server" and "client" certificates

In step 4 above, the term "server" certificate request is used. A "client" certificate is identical to a "server" certificate except the certificates are used for different purposes. For client certificate authentication, the certificate name is used to verify the identity of the client. For TLS encryption, the public key on the certificate is required to begin the encryption process. When importing this certificate into the IKeyMan database, you designate it as a "Personal" certificate. IKeyMan does not distinguish between "client" and "server" certificates and regards them both as "Personal" certificates. The five steps above can be followed exactly as written to import the client certificate into the key database. However, when performing these procedures the administrator should be aware that the terms "server certificate" and "client certificate" are synonymous.

Next step:

Enabling a SIP Connector to require client certificate authentication

Enabling a SIP Connector to require client certificate authentication is the last of two procedures associated with enabling client certificate authentication for a standalone SIP Connector on a Windows machine.

This procedure enables the SIP Connector to operate as a server in the client certificate authentication process.
To require client certificate authentication (or enable the SIP Connector to operate as a server in the client authentication process), you must perform two steps:

1. **Enter the client certificate name in the ExternCommunity document in the Configuration database**

2. **Ensure the SIP Connector has access to the certificates necessary to trust the client certificate**

Each of these procedures is described in detail in a subsequent topic.

**Enter the client certificate name in the ExternCommunity document in the Configuration database**

Entering the client certificate name in the ExternCommunity document in the Configuration database is the first of two steps required to enable a SIP Connector to require client certificate authentication.

When client certificate authentication is required, a SIP Connector in another community must send its client (or "Personal") certificate to the SIP Connector in your community. The SIP Connector in your community must verify that the name on this certificate is a certificate name it knows to accomplish the authentication.

To ensure that your SIP Connector knows the name of the client certificate provided by the SIP Connector in the other community, you must enter this certificate name in the ExternCommunity document in the Configuration database (stconfig.nsf) of the Sametime server to which your SIP Connector connects.

To enter the name of the client certificate in the ExternCommunity document:

1. Use a Lotus Notes client to open the Configuration database (stconfig.nsf) on the Sametime server.
2. Open the ExternCommunity document in the stconfig.nsf database by double-clicking on the date associated with the document.
3. In the "Certificate distinguished name" field, enter the name associated with the client certificate (or "Personal" certificate) sent by the SIP Connector in the other community to the SIP Connector in your community.
   The name of this certificate is usually entered in canonical format, including both the name, organizational unit (if applicable), and organization. For example, cn=servername, ou=organization, o=organization.
   The name of this certificate is specified when the certificate request is created. If you do not know the name of this certificate, it may be necessary to contact the administrator for the other community to get this certificate name.
4. Save and close the ExternCommunity document.

**Next step:** **Ensure the SIP Connector has access to the certificates necessary to trust the client certificate**

**Ensure the SIP Connector has access to the certificates necessary to trust the client certificate**

Ensuring the SIP Connector has access to the certificates necessary to trust the client certificate sent by a SIP Connector in another community is the last of two steps required to enable client certificate authentication on a standalone SIP Connector installed on a Windows machine.

This procedure ensures that the client certificate (or "Personal" certificate) sent by a SIP Connector in another community is signed by a Certificate Authority (CA) that is trusted by the SIP Connector in your community.
To ensure the SIP Connector in your community trusts the CA of the client certificate, the SIP Connector in your community must have access to one of the following certificates:

- A signer (or “trusted root”) certificate signed by the same CA as the client certificate sent by the SIP Connector in the other community.
- A copy of the signed client certificate that is sent by the SIP Connector in the other community. The SIP Connector in your community can also establish trust of the client certificate if your SIP Connector has access to a copy of the client certificate that is sent by the other SIP Connector.

In many cases, the key databases on each SIP Connector will have the appropriate trusted root certificates by default and no procedures will be necessary to ensure that the SIP Connector in one community has the trusted root certificate necessary to trust the client certificate sent by the SIP Connector in the other community.

If it is necessary to obtain a copy of the client certificate of the other SIP Connector, the IKeyMan program on the other SIP Connector can be used to export (or extract) the certificate from the key database on that SIP Connector. This certificate must then be sent in some secure fashion (for example, on a floppy disk sent by registered mail) to your organization. You can use the IBM IKeyMan program on your SIP Connector to import the certificate into the key database on your SIP Connector.

If you have not yet created a key database on the SIP Connector to store these certificates, you can follow the steps described in these two topics to create the key database. These two topics appear earlier in this chapter.

- Install the IKeyMan program on the SIP Connector machine
- Use the IKeyMan program to create a key database on the SIP Connector machine

If it is necessary to import the client certificate of the other SIP Connector machine into the key database, follow the instructions in the “Import the server certificate into the key database” earlier in this chapter to import the certificate.

---

**Audio/Video connectivity with SIP**

When a user in your community invites another user to an instant audio/video meeting, the meeting is created on a Sametime server in your community. The call control and signaling aspect of this connection is handled by SIP. If both communities are configured to support SIP, as described earlier in this chapter, the user from the other community should be able to participate in the audio/video meeting.

Note however that the audio/video streams for the meeting are sourced from the Multimedia Processor (MMP) on the Sametime server hosting the meeting. This aspect of audio/video connectivity functions as follows:

- The Audio/Video streams are transmitted using UDP. The Sametime server Audio/Video Services dynamically select the UDP ports on which to transmit the audio and video streams. These ports are chosen from the “Interactive Audio/Video Network - Multimedia Processor (MMP) UDP port numbers start/end at” settings in the Sametime Administration Tool on the Sametime server.
• If any network between the client and the server blocks UDP traffic, the audio/video streams cannot be transmitted to the client in the other community. In this case, the audio and video streams can be tunneled over a single TCP/IP port.

The administrator can specify the TCP port over which the streams will be tunneled in the "Interactive Audio/Video Network-TCP tunneling port" (default 8084) setting in the Sametime Administration Tool on the Sametime server. The port specified as the "TCP tunneling port" must be open through all networks between the client and the server for the client to transmit and receive TCP-tunneled audio and video streams.

Note: If the audio/video streams must be routed through an HTTP or SOCKS proxy server on any network between the user in the external community and the Sametime server in your community, the user cannot participate in an instant audio/video meeting with a user in your community.

For more information about the MMP on the Sametime server, see Audio/Video Services components and clients

End user experience with the SIP Gateway

The Sametime User’s Guide refers to users in other SIP-enabled communities as “external users.” External users cannot access Sametime features, but they can communicate with Sametime users through instant messages and audio/video sessions.

Sametime Connect identifies external users by Internet e-mail address (Jane_Doe@acme.com) rather than hierarchical names (Jane Doe/East/Acme or short names (Jane Doe). External users also identify Sametime users by e-mail addresses. For example, when adding a Sametime user to an awareness list, external users enter the Sametime user’s e-mail address.

For the most part, Sametime users interact with external users just as they do with other Sametime users. For more information, refer to the topics listed below in "Chapter 2: Using Sametime Connect" of the Sametime 7.0 online end user help (available from the "Documentation" link on the Sametime server home page). This help is also available in PDF format at www.lotus.com/1dd. Click the Documentation Library link to search for the Sametime User’s Guide.

Sametime users can:
• Add and remove external users from the contact list. See "Adding an Individual Name to the Contact List" for more information.
• Add and remove external users from the Who Can See If I Am Online List. See "Determining Who Sees You Online" for more information.
• Send and receive instant messages with external users. See "Chatting with People" for more information.
• Create specific alerts for external users. See "Setting Specific Alerts" for more information.
• Display external users in the contact list in two ways: only when external users are online or all the time. See "Displaying Online People or All People" for more information.
Sametime users can also invite external users to instant audio/video sessions and attend instant audio/video sessions started by external users. These sessions are different from Sametime meetings because they do not include any other Sametime tools, such as whiteboard or chat.

To invite an external user to an instant audio/video session:
1. Select the external user in the contact list.
2. Right-click the external user and select either Audio (for an audio-only session) or Video (for a session that includes both audio and video).
3. The Start Instant Meeting dialog box appears. Edit the Topic and Message fields if necessary and click Send. (You cannot add tools or add invitees to the session. Even if “Secure Meeting is checked, your session might not be encrypted because the external user’s community might not enable encryption.)
4. Click OK if the confirmation dialog box appears.

The following Sametime features do not work with external users:
• External users cannot attend scheduled or instant Sametime meetings.
• External users do not appear in the local directory. These users must added individually to the Sametime Connect contact list using the Internet e-mail address.
• You cannot send announcements to external users.
• You cannot transfer files to external users or receive files from external users.
• External users appear either online or offline in the contact list. They do not have the full range of online statuses that are available to regular Sametime users. Sametime online statuses are not visible to external users, either. To external users, Sametime users appear only as online or offline. If an external user is part of another Sametime community, then the full range of Sametime online statuses is available.
• You cannot include multiple external users in a single chat or audio/video session.
• You cannot invite other people to a chat or an audio/video session with an external user.
• You cannot add tools to chats or audio/video sessions with external users.
• Audio/video sessions with external users do not include chat.
• External users are not listed in your company’s directory. You cannot use the directory to search for the names of external users when you add them to your contact list, add them to the Who Can See If I Am Online List, or invite them to chat or audio/video sessions.
• Privacy features work slightly differently between Sametime users and external users. Normally, if you use the Who Can See If I Am Online List to prevent Jane Doe from seeing you online, you also cannot see Jane online. She always appears offline in your contact list. However, if you use the Who Can See If I Am Online list to prevent an external user from seeing you online, you can still see the external user online (unless she uses the privacy features of her own instant messaging client to prevent you from viewing her online status).
• The Sametime Connect settings for displaying full names or short names do not affect external users’ names.
Chapter 8. Configuring the Meeting Services

This chapter describes the Meeting Room maintenance procedures and the Meeting Services configuration options available from the Sametime Administration Tool. This chapter includes information on:

- Maintaining the Sametime Meeting Center
- Automatically extending meetings past their scheduled end times
- Adding the names of meeting participants to the Meeting Details document after a meeting ends
- Specifying the collaborative activities that are available for all meetings on the IBM Lotus Sametime server
- Forcing the screen sharing tool to use an 8-bit color depth to enhance screen sharing performance
- Encrypting meeting data and requiring passwords for all scheduled meetings
- Specifying different Connection Speed Settings for modem and LAN/WAN connections to the Broadcast Services. The Connection Speed Settings determine the rate that streams are transmitted on the network for broadcast meetings with no audio/video activity
- Controlling the bandwidth usage of the Meeting Services

About the Meeting Services

The Meeting Services include the T.120 software that supports real-time collaboration through screen sharing and a shared whiteboard. The Meeting Services also provide a variety of other types of support for the meeting activity occurring on the Sametime server.

Functions of the Meeting Services are to:

- Support a direct TCP/IP connection, a SOCKS proxy connection, and an HTTP proxy connection between the Sametime Meeting Room client and the Sametime server. The default port for this connection is port 8081. This connection is used by all screen-sharing and whiteboard components of the Meeting Room client. The interactive audio and video components of the Sametime Meeting Room client also use this connection for call setup and control purposes. For more information, see [Meeting Services Network settings](#).
- Maintain multiple connections and distribute screen-sharing, whiteboard, and other T.120 data to all participants in a Sametime meeting.
- Maintain lists of active, scheduled, finished, and recorded meetings in the Sametime Meeting Center.
- Start and stop meetings at the appropriate time.
- Interact with components of the Community Services to create meetings in which collaborative activities supported by the Community Services, Meeting Services, and Audio/Video Services are simultaneously available.
- Enforce administrator-specified restrictions on the collaborative activities available for meetings on the Sametime server.
- Support encryption of meeting data and password protection for individual meetings.
- Log Meeting Services events to the Sametime log (stlog.nsf).
• Write the names of meeting attendees to the Meeting Details document.
• Provide the ability to record Sametime meetings in Sametime Record and Playback (RAP) files so that users can replay meetings after the meetings have ended.
• Support different Connection Speed Settings for modem and LAN/WAN connections to the Broadcast Services.
• Handling connections from the Meeting Services of other Sametime servers when a community includes multiple Sametime servers. Meeting Services server-to-server connections occur on TCP/IP ports 1503 and 1516.

**Note:** In a multiple server environment, port 1516 must be open between two Sametime servers to enable a single Sametime meeting to be simultaneously active on both Sametime servers. This functionality is sometimes called “invited servers.” For more information, see [Advantages of a single meeting on multiple servers](#).

### Meeting Services configuration settings

The Sametime Administration Tool includes configuration settings that allow the administrator to control the Meeting Services. The available settings are:

#### General

The **General** settings enable the administrator to extend meetings, include participant names in the Meeting Details document, allow users to schedule meetings from Microsoft Outlook, and control the collaborative activities and security features (encryption and meeting password) that are available for all meetings on the Sametime server. The administrator also uses the General settings to allow scheduled meetings to be recorded and stored on the server so that they can be replayed after the meeting has ended.

#### Connection Speed Settings

The **Connection Speed Settings** enable the administrator to specify data transmission speeds (bit rates) for the Real-Time Protocol (RTP) streams that are transmitted by the Broadcast Services on the Sametime server to Sametime Broadcast clients. These Connection Speed Settings control the transmission rates for broadcast meetings without audio/video. Different transmission speeds are specified for modem and LAN/WAN connections to the Sametime Broadcast Services.

#### Meeting Services connectivity settings

For information about the ports used by the Meeting Services and the available connectivity options, see [Meeting Services Network settings](#).

#### Meeting Services bandwidth control

If the bandwidth usage of the screen sharing and whiteboard tools is too high, users may be unexpectedly disconnected from Sametime meetings. For information about controlling the network bandwidth usage of the screen sharing and whiteboard tools, see [Controlling the bandwidth usage of the Meeting Services](#).

#### Accessing the Meeting Services configuration settings

To access the Meeting Services configuration settings:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.

2. Choose Configuration.

3. Choose Meeting Services. The available settings are:
   - General
   - Connection Speed Settings

**General Settings for Meeting Services**

The General settings for Meeting Services allow you to configure settings for instant and scheduled meetings on the Sametime server.

The available settings are:

**General**

- Automatically extend meetings past their scheduled end times - Extends any meeting past its scheduled end time when people are still attending the meeting.
- After a meeting, add the names of participants to the meeting document - Adds the names of participants to the meeting details after the meeting ends.

**When people start an instant meeting or schedule a meeting**

- Allow people to choose the screen-sharing tool in meetings - Allows end users to select the screen-sharing tool for instant and scheduled meetings.
- Force screen sharing to use 8-bit color - Allows the administrator to force all images displayed in the screen sharing tool to use the 8-bit color depth. This feature can improve screen sharing performance and decrease network bandwidth usage.
- Allow people to choose the whiteboard tool in meetings - Allows end users to select the whiteboard tool for instant and scheduled meetings. When you allow users to choose the whiteboard, you can also control whether the Meeting Moderator can save whiteboard annotations as attachments in the meeting.
- Allow people to choose the "Send Web Page" tool in meetings - Allows end users to select the Send Web Page tool for instant and scheduled meetings.
- Allow people to choose the "Polling tool" in meetings - Allows end users to select the Polling tool in meetings.
- Allow people to record meetings for later playback - Allows a user to record a scheduled meeting so the meeting can be replayed after the meeting has ended. When you allow users to record meetings, you must also specify the directory on the Sametime server in which recorded meeting files will be stored and the amount of free disk space on the server that must be available for a meeting to be recorded. For more information about allowing users to record meetings and the administrative tasks associated with recorded meetings, see Managing recorded meetings (Record and Playback).
- Allow people to schedule Broadcast meetings - Allows end users to schedule broadcast meetings. If this option is not selected, broadcast meetings are not available on the Sametime server.

**Security**

- Encrypt all Sametime meetings - Encrypts the T.120 screen-sharing and whiteboard data, streaming audio/video data, and chat data that passes between clients and the Sametime server during all Sametime meetings.
- Require all scheduled meetings to have a password - Ensures that every meeting scheduled in the Sametime Meeting Center has a password. This password is
meeting-specific and is different from the Internet password specified on each user’s Person document that enables users to authenticate with the server.

**Automatically extending meetings beyond the scheduled end time**

When scheduling a meeting in the Meeting Center, an end user chooses a duration for the meeting. To ensure that meetings do not end before participants have concluded their business, you can allow any online meeting to extend past its scheduled end time if people are still in the meeting. You can also specify the number of minutes that the meeting should be extended. By default, all online meetings are extended by 15 minutes.

If the "Automatically extending meetings beyond the scheduled end times when there are still people in the meeting" setting is not selected, all meetings will end after the specified duration regardless of whether participants are still in attendance. Participants receive a warning message approximately three minutes before a meeting ends. Do not select this setting if a consistently high number of active meetings is affecting server performance.

To allow an online meeting to extend past its scheduled end time:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. Select the "Automatically extend meetings beyond scheduled end times when there are still people in the meeting" check box in the General settings for Meeting Services. (This check box is selected by default.)
6. Specify the number of minutes you want the meetings to extend in the "Meeting extension length (minutes)" box.
7. Click Update and restart the server for the change to take effect.

**Adding the names of participants to the meeting document**

Every meeting that is scheduled in the Sametime Meeting Center includes a Meeting Details document. This document records information such as the name of the meeting, the date and time of the meeting, and any files for the meeting. Meeting details documents are available before, during, and after a meeting. These documents are not available for instant meetings.

You can record the names of meeting participants on the Meeting Details document after a meeting is over. When participant names are included in the details, end users can determine who attended a particular meeting and contact other meeting participants.

To record the names of meeting participants on the Meeting Details document after a meeting ends:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. Select the "After a meeting, add the names of participants to the meeting document" check box in the General settings for Meeting Services.
6. Click Update and restart the server for the change to take effect.

To view the names in the Meeting Details document after the meeting has ended, click Finished on the left side of the Meeting Center and then click the meeting name.

**Allowing or preventing use of the screen-sharing tool in meetings**

The administrator selects the "Allow people to choose the screen sharing tool in meetings" setting to allow people to choose screen sharing as a collaborative activity when creating an instant or scheduled meeting.

When this setting is selected, the administrator can also determine the screen-sharing tasks that meeting participants can perform. By default, people are allowed to choose screen sharing in meetings, and all participants are allowed to use all screen-sharing features.

When you allow people to choose screen sharing, it is automatically included in all scheduled meetings on the Sametime server. An end user can remove the screen-sharing tool from a scheduled meeting by using the Tools tab on the New Meeting page in the Meeting Center. An end user can also select screen sharing as a tool when starting an instant meeting.

When this setting is not selected, the screen-sharing tool and all screen-sharing features and options are hidden in the Sametime end-user interface. Essentially, the screen-sharing collaborative activity is unavailable for all instant and scheduled meetings.

**Note:** For more information about screen sharing, see the *Lotus Sametime User’s Guide* available from the Documentation link on the Sametime server home page.

To allow or prevent the use of the screen-sharing tool in meetings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To prevent the use of screen sharing, clear the check mark from the check box labeled "Allow people to choose the screen sharing tool in meetings." Skip to Step 7.
   To allow the use of screen sharing, select the check box labeled "Allow people to choose screen sharing tool in meetings" in the General settings for Meeting Services. (This check box is selected by default.)
6. Select an option for allowing participants to use screen sharing:
   - Select "Participants can share their screen, view a shared screen, or control a shared screen if the Moderator permits" to allow participants to use all aspects of screen sharing. (This option is selected by default.) This option allows all meeting participants to share their screens if screen sharing is allowed in the meeting by the Moderator.
   - Select "Participants can share their screen if the Moderator permits or view a shared screen" to allow participants to share information and to view shared information, but to prevent them from controlling information that someone else is sharing. Select this option to ensure a high level of security for screen
sharing. This option allows only specific users selected by the Moderator to share screens on their computers. All other meeting participants can view the shared screens.

- The "Participants can view the shared screen only" option is provided for security purposes when you have used a multiple Sametime server deployment and connected Sametime servers across a firewall to extend Sametime to Internet users. For more information on this setting, see Extending Sametime to Internet users and Screen sharing security and Internet users.

7. Click Update and restart the server for the change to take effect.

**Forcing Screen Sharing to use 8-bit color**

The administrator selects the "Force Screen Sharing to use 8-bit color" setting to force all applications shared in the screen sharing tool to be shared at the 8-bit color depth.

This setting can improve the screen sharing performance in Sametime meetings. When a user displays an application in the screen sharing tool, an image of that application is sent on the network from that user’s computer to all other users in the meeting. If the image of the application has a high color depth (more than 8-bit), it can negatively affect screen sharing performance. High color-depth images negatively affect screen sharing performance because these images:

- Require more CPU usage on the user’s computer to process than low color-depth images.
- Consume more network bandwidth than low color-depth images.

When this setting is selected, all applications displayed in the screen sharing tool display at the 8-bit color depth. Selecting this setting can enhance the screen sharing performance but decreases the quality of the image viewed by the end users.

When this setting is not selected, the end user uses settings on the Preferences tab of the Sametime Meeting Room client to control the color depth of the shared images. The settings on the Preferences tab include an "Optimize for Image Quality" setting and an "Optimize for Performance" setting.

If the end user selects the "Optimize for Image Quality" setting, the application is shared at the color depth that is specified in the Windows Control Panel on that user’s machine. This option enables the end user to share applications at higher color depths if the quality of the 8-bit images is not sufficient.

If the end user selects the "Optimize for Performance" setting, the application is shared at an 8-bit color depth regardless of the color depth specified on the user’s machine.

**Note:** The "Optimize for Image Quality" and "Optimize for Performance" settings in the Preferences tab of the Meeting Room client are grayed out when the administrator selects the "Force Screen Sharing to use 8-bit color" setting; the end user cannot alter the color depth at which an application displays in the screen sharing tool.

Only the user who is using the screen sharing tool to share the application can control the color depth at which the image displays. If a user in a meeting shares a screen at a 32-bit color depth, other users in the meeting must view this screen image at the 32-bit color depth. The user viewing the image cannot use the settings
in the Preferences tab of the Meeting Room client to view the image at a different color depth than the color depth specified by the user sharing the screen.

If you select this setting, you may want to experiment with the screen sharing tool to ensure that the image quality is adequate at the 8-bit color depth.

**Note:** Generally, applications displayed at 16-bit color require up to twice as much processing on the user computer as 8-bit color settings. The 32-bit color settings could require up to four times as much processing as 8-bit color settings. The additional processing occurs because the amount of data required to represent each pixel of an image increases with the higher color settings.

To configure the "Force Screen Sharing to use 8-bit color" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To require end users to share all applications in all meetings at the 8-bit color depth, select the check box labeled "Force Screen Sharing to use 8-bit color."
   To allow end users to control the color depth at which applications are shared, clear the check box labeled "Force Screen Sharing to use 8-bit color."
6. Click Update and restart the server for the change to take effect.

**Allowing or preventing use of the whiteboard tool in meetings**
The "Allow people to choose the whiteboard tool in meetings" setting enables the administrator to allow or prevent users from selecting the whiteboard as a collaborative activity when creating instant or scheduled meetings. By default, users can select the whiteboard collaborative activity in all instant and scheduled meetings created on the Sametime server.

When this setting is selected, the whiteboard is automatically included in all scheduled meetings on the Sametime server. An end user can remove the whiteboard tool from a scheduled meeting by using the Tools tab on the New Meeting page in the Meeting Center.

**Note:** To include the whiteboard in an instant meeting, the user must select the "Collaborate..." option from the presence list or Sametime Connect client when starting the instant meeting.

If the administrator disables the "Allow people to choose the whiteboard tool in meetings" setting, all whiteboard features and options are hidden from the end user in the Sametime end-user interface. The whiteboard cannot be selected as a collaborative activity for instant or scheduled meetings.

**Allow people to save whiteboard annotations as attachments to the meeting:**
When the "Allow people to choose the whiteboard tool in meetings" setting is selected, the administrator has the option of allowing the Meeting Moderator to save whiteboard annotations as attachments to the meeting.

During a whiteboard meeting, end users can use various whiteboard drawing or text tools to mark (or annotate) the image that is being presented on the whiteboard. If the administrator enables this setting, the Meeting Moderator can
save the whiteboard at any time during the meeting. When the Meeting Moderator saves the whiteboard, it is saved in its current state with all annotations included in the saved file. This feature enables the Moderator to capture the contents of the whiteboard at any time during the meeting. The saved whiteboard file can be used for later viewing or for presentation during a subsequent whiteboard meeting.

If the Meeting Moderator saves a whiteboard file more than once in a meeting, only the most recently saved version of the whiteboard file is saved on the server.

The whiteboard file is saved on the Sametime server as an attachment to the meeting’s Meeting Details document in the Sametime Meeting Center. The whiteboard is saved in two file formats: RTF and SWB (Sametime Whiteboard). The RTF file can be opened in most word processing or graphics applications for printing or viewing after the meeting has ended. The SWB file can be attached to future meetings and presented on the whiteboard during those meetings.

Note: The Moderator saves the whiteboard by selecting the menu option Meeting - Save Whiteboard in the Whiteboard tool in the Sametime Meeting Room client. The Save Whiteboard option is hidden if the administrator does not allow the Meeting Moderator to save the whiteboard.

To allow or prevent the use of the whiteboard tool in Sametime meetings:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To allow whiteboard activity on the server, select the check box labeled "Allow people to choose the whiteboard tool in meetings." (This check box is selected by default.) To prevent whiteboard activity on the server, remove the check mark from the check box labeled "Allow people to choose the whiteboard tool in meetings." Skip to Step 7.
6. Perform this step only if you selected the "Allow people to choose the whiteboard tool in meetings" in Step 5. To allow people to save the whiteboard and annotations to it at any time during a meeting, select the check box labeled "Allow people to save whiteboard annotations as attachments to the meeting." To prevent people from saving the whiteboard during meetings, remove the check mark from the check box labeled "Allow people to save the whiteboard annotations as attachments to the meeting."
7. Click Update and restart the server for the change to take effect.

Allowing or preventing use of the Send Web Page tool in meetings
The "Allow people to choose the ‘Send Web Page’ tool in meetings” setting enables the administrator to allow or prevent users from selecting Send Web Page as a collaborative activity when creating instant or scheduled meetings. By default, users can select the Send Web Page collaborative activity in all instant and scheduled meetings created on the Sametime server.
When this setting is selected, the Send Web Page tool is automatically included in all scheduled meetings on the Sametime server. An end user can remove the Send Web Page tool from a scheduled meeting by using the Tools tab on the New Meeting page in the Meeting Center.

**Note:** To include the Send Web Page tool in an instant meeting, the user must select the "Collaborate..." option from the presence list or Sametime Connect client when starting the instant meeting.

If the administrator disables this setting, all Send Web Page features and options are hidden from the end user in the Sametime end-user interface. The Send Web Page tool cannot be selected as a collaborative activity for instant or scheduled meetings.

To allow or prevent the use of the Send Web Page tool in Sametime meetings:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To allow Send Web Page activity on the server, select the "Allow people to choose the Send Web Page tool in meetings" check box. This check box is selected by default.
   To prevent Send Web Page activity on the server, remove the check mark from the "Allow people to choose the Send Web Page tool in meetings" check box.
6. Click Update and restart the server for the change to take effect.

**Allowing or preventing the use of the Polling tool in meetings**

The "Allow people to choose the Polling tool in meetings" setting enables the administrator to allow or prevent users from selecting polling as a collaborative activity when creating instant or scheduled meetings. By default, users can select the polling collaborative activity in all instant and scheduled meetings created on the Sametime server.

When this setting is selected, polling is automatically included in all scheduled meetings on the Sametime server. An end user can remove the polling tool from a scheduled meeting by using the Tools tab on the New Meeting page in the Meeting Center.

**Note:** To include the polling tool in an instant meeting, the user must select the "Collaborate..." option from the presence list or Sametime Connect client when starting the instant meeting.

If the administrator disables this setting, all polling features and options are hidden from the end user in the Sametime end-user interface. Polling cannot be selected as a collaborative activity for instant or scheduled meetings.

To allow or prevent the use of the polling tool in Sametime meetings:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To allow Polling activity on the server, select the check box labeled "Allow people to choose the Polling tool in meetings." (This check box is selected by default.)

To prevent Polling activity on the server, remove the check mark from the "Allow people to choose the Polling tool in meetings" check box.

6. Click Update and restart the server for the change to take effect.

Allow people to record meetings for later playback (scheduled meetings)
The administrator uses this setting to allow or prevent users from recording scheduled meetings on the Sametime server. For more information on allowing users to record meetings and the administrative tasks associated with recorded meetings, see Managing recorded meetings.

Note: The whiteboard tool pointer tool is not available in a recorded meeting.

Allowing or preventing broadcast meetings
The "Allow people to schedule Broadcast meetings" setting allows or prevents end users from scheduling broadcast meetings on the Sametime server. Disabling this setting prevents the end users from using the broadcast capabilities supported by the Broadcast Services on the Sametime server. By default, users are allowed to schedule broadcast meetings on the Sametime server.

When this setting is selected, the end user can select the "Broadcast Presentation or Demo” meeting type when scheduling meetings in the Sametime Meeting Center. (The end user selects this meeting type to schedule a broadcast meeting.)

Note: For more information on broadcast meetings and the Sametime Broadcast Services, see About the Broadcast Services.

When this setting is not selected, the "Broadcast Presentation or Demo” meeting type is hidden from the end user on the New Meeting page of the Sametime Meeting Center. Since a broadcast meeting must always be a scheduled meeting, disabling this setting prevents users from creating broadcast meetings on the Sametime server.

Note: Broadcast meetings are always scheduled meetings. An end user cannot start an instant broadcast meeting from a presence list.

To allow or prevent broadcast meetings on the Sametime server:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To allow users to schedule broadcast meetings, select the "Allow people to schedule Broadcast meetings" check box.

To prevent users from scheduling broadcast meetings, remove the check mark from the check box.

6. Click Update and restart the server for the change to take effect.

Encrypting all Sametime meetings
The administrator can encrypt the T.120 screen-sharing and whiteboard data and audio/video data that passes between clients and the Sametime server during all
Managing activities: the files and recorded Sametime 6.

When you encrypt all meetings, an end user cannot remove encryption for an individual meeting. If you do not select this option, an end user can choose whether to encrypt the screen-sharing, whiteboard, and audio/video data when creating the meeting. (Chat encryption is handled as described in the note above.)

To encrypt all meetings on the Sametime server:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. Select the "Encrypt all meetings" check box in the General settings for Meeting Services.
6. Click Update and restart the server for the change to take effect.

**Requiring all scheduled meetings to have a password**
You can require every meeting scheduled in the Sametime Meeting Center to have a password. (Instant meetings cannot have passwords.) When you select this option, an end user must enter a password when scheduling a meeting. When a scheduled meeting includes a password, all participants must enter the password to attend the meeting or view the Meeting Details document for the meeting.

**Note:** The meeting password is an additional security feature that provides password protection for individual meetings. The meeting password is different from the Internet password that is specified on each user’s Person document. The Internet password is used to authenticate a user when the user accesses any protected database on the server or logs in to the Community Services from Sametime Connect.

To require all scheduled meetings to have a password:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. Select the check box labeled "Require all scheduled meetings to have a password."
6. Click Update and restart the server for the change to take effect.

**Managing recorded meetings (Record and Playback)**
Sametime provides the ability to record a scheduled meeting and store the recorded meeting on the Sametime server. The recorded meeting can be accessed and replayed by any Sametime user at any time. Users access the recorded meeting files from Meeting Details documents in either the Finished or Recorded view of the Sametime Meeting Center. Sametime can record the following meeting activities:
- Chat
- Send Web page
• Question and answer polls
• Audio
• Video
• Screen sharing
• Whiteboard

**Note:** The whiteboard tool pointer tool is not available in a recorded meeting. If
a user selects the whiteboard pointer tool while a meeting is being
recorded, the following message appears and the user is unable to use the
pointer tool:

"Pointer Tool Disabled Not All Participants Support This Tool."

The administrator controls whether end users have the ability to record meetings
on the Sametime server from the "Allow people to record meetings for later
playback" setting in the Configuration-Meeting Services settings of the Sametime
Administration Tool. If the administrator allows users to record meetings, a
"Record this meeting so that others can replay it later" option appears on the
Essentials tab of the New Meeting page in the Sametime Meeting Center. If an end
user selects this option when creating a scheduled meeting, the meeting is recorded
in a Sametime Record and Playback (RAP) file and stored on the Sametime server
in a location specified by the administrator. The default RAP filename includes a
unique meeting identifier followed by the RAP file extension.

After a meeting has been recorded, a "Replay the Meeting" button appears in the
Meeting Details document associated with the meeting in the Sametime Meeting
Center. A user can open the Meeting Details document and select this button to
replay the meeting.

When the user selects the "Replay the Meeting" button, a modified version of the
Sametime Broadcast client Java applet loads in the Web browser on the user’s
machine and connects to the Broadcast Gateway component of the Sametime
server. The Broadcast client is modified to include controls that enable the user to
stop, pause, resume, rewind, and forward the playback of the recorded meeting
file.

To replay a meeting, the Sametime server locates the RAP file that contains the
recorded meeting, and the Broadcast Gateway streams the meeting content to the
modified Broadcast client. The connection process and streaming of the recorded
meeting content operate exactly as if the user is attending a broadcast meeting. The
Broadcast components of the Sametime server handle the connection process and
playback of recorded meeting files. For more information, see [Broadcast client
connection process using JVM 1.4.2](#) and [Working with the Broadcast Services](#)

If you allow users to record Sametime meetings, you should also be familiar with
the administrative features provided for exporting, importing, deleting, and
replacing recorded meeting files on the Sametime server. The remaining topics in
this section describe the administrative tasks related to recorded meetings:

• [Allowing or preventing recorded meetings](#) - Describes how to allow or prevent
users from recording meetings on the Sametime server. If you allow recorded
meetings, you must specify the directory on the Sametime server in which
recorded meeting files are stored and the minimum amount of free disk space
that must be available for the recording of a meeting to continue.

• [Managing recorded meeting files](#) - Discusses the administrative features
provided to export, import, delete, and replace recorded meeting files on the
Sametime server. These features are available from the user interface of the Sametime Meeting Center; they are not available from the Sametime Administration Tool.

Notes:

- A user cannot access a recording of a meeting until approximately one hour after the meeting ends. The recording is not available while the meeting is in progress. This delay period occurs because time is required for the server to convert the meeting data into the RAP file format. The length of this delay period varies depending on the length of the meeting and the complexity of the activities that occur in the meeting.
- The Sametime log does not log information related to the playback of recorded meetings. Information is logged only for the original meeting.

Allowing or preventing recorded meetings on the Sametime server

The "Allow people to record meetings for later playback" setting in the Configuration - Meeting Services settings of the Sametime Administration Tool enables the administrator to allow or prevent users from recording scheduled meetings on the Sametime server.

Note: The Sametime log does not record information related to the playback of recorded meetings. Information is recorded only for the original meeting.

If you want to allow users to record meetings on the Sametime server, you must select the "Allow people to record meetings for later playback" setting and specify the following:

- The directory on the Sametime server where the recorded meeting files will be stored
- The number of megabytes of free disk space that must exist for recording to continue

Each of these settings are discussed in detail below.

The directory on the Sametime server where the recorded meeting files will be stored.: By default, the recorded meeting files are stored in the following location:

- <sametime server install directory>\MeetingArchive\ on a Windows system (for example C:\Sametime\MeetingArchive).
- <sametime server data directory>\MeetingArchive\ on an IBM i5/OS system.

Note the following if you change the default location for recorded meetings:

- If you specify a directory that does not currently exist on the Sametime server, the directory is created when the next meeting is recorded. If, for any reason, the directory cannot be created, meetings are not recorded. If meetings are not recorded, verify that the directory was created or create the directory if necessary.

Note: You do not receive any notification if the directory cannot be created.

- If meetings were recorded previously and stored in the C:\Sametime\MeetingArchive directory (or Data/MeetingArchive directory on IBM i5/OS), the Sametime server cannot locate those recorded meeting files if a user attempts to play them. You must export the files from the C:\Sametime\MeetingArchive directory and import them into the new directory to enable users to play the recorded meetings.
• If you change the default directory setting and attempt to import recorded meeting files to the new directory before you have recorded the first meeting, the import will fail because the directory is not created until a meeting is recorded. You should either record a meeting or manually create the directory before importing meetings.

The number of megabytes of free disk space that must exist for recording to continue.: The recording of meetings stops when the number of megabytes of free disk space falls below the threshold specified by the administrator. The default setting is 300MB of free disk space. If a meeting is in the process of being recorded when this threshold is reached, recording is stopped and an error is written to the Sametime log.

To check available disk space on the Sametime server from the Sametime Administration Tool:
2. Select the "You can view the Domino Web Administration pages in a new browser window" link. Selecting this link opens the Domino Web Administration client.
3. Enter your administrator name and password to access the Domino Web Administration client.
4. In the Domino Web Administration client, select Analysis - Disk Space to view the available disk space on the Sametime server. If you are using Microsoft Internet Explorer, make sure the "Use HTTP 1.1" setting in the Tools-Internet Options-Advanced options of the browser is disabled to use the graphical monitoring tools of the Domino Web Administration client.

Note: If recording is stopped because of a shortage of disk space, a RAP file that contains a partial recording of the meeting is stored on the Sametime server and a message is written on the Meeting Details document for the meeting indicating that the meeting could not be recorded. The administrator must make more disk space available on the server before recording can continue. If necessary, you can make more disk space available by deleting old recorded meeting files. For more information, see Deleting recorded meetings.

If the administrator disables the "Allow people to record meetings for later playback" setting, scheduled meetings cannot be recorded on the Sametime server.

Follow the instructions below to allow or prevent users from recording scheduled meetings on the Sametime server:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. To allow users to record scheduled meetings on the server, select the check box labeled "Allow people to record meetings for later playback." This check box is selected by default.

To prevent users from recording scheduled meetings on the Sametime server, remove the check mark from the "Allow people to record meetings for later playback" check box. If you disable this setting, skip to Step 8.
6. In the "Save recorded meetings in the following location" field, accept the default directory or type a new path to the directory in which you want the recorded meeting files (or RAP files) to be stored. The default path is <sametime server install directory>\MeetingArchive\ on a Windows system and <sametime server data directory>/MeetingArchive on an IBM i5/OS system.

The Sametime server uses the entry in this field to locate the recorded meeting files when a user selects the "Replay the Meeting" button from the Meeting Details document associated with the recorded meeting.

7. In the "Stop recording when this much disk space is left (MBytes)" setting, type the number of megabytes of free disk space that must exist on the Sametime server hard drive for a meeting to be recorded. If the number of megabytes of free disk space falls below the specified level, recording is stopped and a message is written on the Meeting Details page indicating that the recording did not complete. The default setting is 300MB.

**Note**: If your Sametime server runs on the AIX or Solaris operating system, the "Stop recording when this much disk space is left (MBytes)" option is not supported. This setting will not go into effect even if you enter a number for this setting.

8. Click Update and restart the server for the change to take effect.

**Note**: A Recorded view is available from the Sametime Meeting Center that enables an end user to see a list of all recorded meetings on the Sametime server. Users can also access the Meeting Details documents of recorded meetings from the Finished view of the Sametime Meeting Center. If the "Allow people to record meetings for later playback" setting is disabled, the Recorded view is still visible in the Sametime Meeting Center. A user selecting the Recorded view sees a message indicating that there are no recorded meetings. All other recorded meeting features and options are hidden from the end user in the Sametime end-user interfaces.

### Managing recorded meeting files

If the administrator allows users to record Sametime meetings, the meetings are recorded in Sametime Record and Playback (RAP) files. These files are stored on the Sametime server in the directory the administrator specifies in the "Save recorded meetings in the following location" setting available from the Configuration-Meeting Services settings of the Sametime Administration Tool.

Recorded meeting files are managed from the Meeting Details documents associated with recorded meetings in the Sametime Meeting Center (stconf.nsf) and from the Import Recording link available from the Sametime Meeting Center.

An administrator can perform the following procedures to manage recorded meeting files:

- **Delete the Recording** - To delete a recorded meeting file, select this option on the Meeting Details document associated with the recorded meeting. You might want to periodically delete recorded meetings from the server to conserve disk space. For more information, see [Deleting recorded meetings](#).

- **Export the Recording** - To export (copy) a recorded meeting file, select this option on the Meeting Details document associated with the recorded meeting. You can use this option to make backup copies of meetings or move a meeting to a different Sametime server. For more information, see [Exporting recorded meetings](#).
• **Replace the Recording** - To replace a recorded meeting file, select this option on the Meeting Details document associated with the recorded meeting. For more information, see [Replacing recorded meetings](#).

• **Import Recording** - To add a recorded meeting file to the Sametime server, select this option from the list of links on the left side of the Sametime Meeting Center. The administrator can add a recorded meeting file even if the meeting did not occur on this Sametime server. In multiple server environments, this feature can be used to distribute a copy of a recorded meeting to multiple Sametime servers. For more information, see [Importing recorded meetings](#).

**Note:** The "Delete the Recording," "Export the Recording," and "Replace the Recording" options on the Meeting Details document are only visible to the meeting creator, the Meeting Moderator, and the administrator. The meeting creator and Meeting Moderator only see these options for meetings for which they have creator or moderator status.

An administrator must have the Sametime Admin role selected in the ACL of the Sametime Meeting Center to see the "Delete the Recording," "Export the Recording," "Replace the Recording," and "Import Recording" options in the Meeting Center forms. The administrator sees these options in the Meeting Details documents of all recorded meetings on the server.

**Recorded meetings and invited servers:** If you have set up a multiple Sametime server environment, a single meeting can be simultaneously active on two or more Sametime servers. This scenario is often referred to as "invited servers." For more information on invited servers, see [Deploying multiple Sametime servers](#).

If a meeting includes invited Sametime servers and the meeting is recorded, the recorded meeting file for the meeting is only available from the Meeting Details document on the source Sametime server (the Sametime server on which the meeting was created). The recorded meeting file is not available on the invited servers. The administrator can make the recorded meeting file available on an invited server by exporting the recorded meeting file from the source Sametime server and importing the file to the invited Sametime server.

**Deleting recorded meetings:** You might want to periodically delete recorded meeting files to conserve disk space on the Sametime server. Before deleting a file, you might want to use the "Export the Recording" feature to make a copy of the recorded meeting file before deleting it. For more information, see [Exporting recorded meetings](#).

To delete a recorded meeting file from the Sametime server:

1. Use a Web browser to browse to the Sametime server home page.
2. Click the "Attend a Meeting" link.
3. Click the Recorded link to see a list of all recorded meetings on the Sametime server.
4. Click the name of the recorded meeting that you want to delete.
5. Click the "Delete the Recording" button on the Meeting Details document to delete the recorded meeting file from the Sametime server.

**Note:** If the "Delete the Recording" link is not visible in the Meeting Details document, click the "Log on to Sametime" link beneath the date and time and log on as the administrator. You must have the Sametime Admin role assigned in the ACL of the Sametime Meeting Center to see the "Delete the Recording" option in the Sametime Meeting Center.
After you select the “Delete the Recording” button to delete the meeting, the Meeting Details document remains available from the Finished view of the Sametime Meeting Center. It no longer exists in the Recorded view of the Sametime Meeting Center.

You can also delete a recorded meeting by selecting the “Delete the Meeting” button on the Meeting Details document. Selecting the “Delete the Meeting” button deletes the Meeting Details document, any attachments to the Meeting Details document, and the recorded meeting file associated with the meeting.

**Exporting recorded meetings:** Use the “Export recorded meetings” option on the Meeting Details document associated with the recorded meeting to rename the recorded meeting file and export (or copy) it to a different local or network directory.

You might want to export a recorded meeting file before deleting it so that the file is safely stored on a different machine in case the file is needed later.

**Note:** Recorded meeting files have default file names that include a unique meeting identifier. When exporting a file, Lotus software recommends renaming the file to a more easily identifiable name. (For example, you might want to rename "A1BC3235348F_recorded.rap" to "November2001BenefitsMeeting.rap").

You also use the "Export recorded meetings" option to copy a recorded meeting file from one Sametime server to another. Use the export procedure below to rename the file and copy the file to a different local or network directory. On the Sametime server to which you want to copy the meeting file, use the **[Import recorded meeting]** feature to add the recorded meeting to that server.

When you export a meeting, a copy of the meeting is created in the local or network directory you specify. The original recorded meeting file is not removed from the server. To remove a recorded meeting file from the server, you must delete the file. For more information, see **Deletings recorded meetings**.

To export (or copy) a recorded meeting:

1. Use a Web browser to browse to the Sametime server home page.
2. Click the "Attend a Meeting" link.
3. Click the Recorded link to see a list of all recorded meetings on the Sametime server.
4. Click the name of the recorded meeting that you want to export to open the Meeting Details document.
5. Click the "Export the Recording" button.

   **Note** If the "Export the Recording" link is not visible in the Meeting Details document, click the "Log on to Sametime" link beneath the date and time and log on as the administrator. You must have the Sametime Admin role assigned in the ACL of the Sametime Meeting Center to see the "Export the Recording" option in the Sametime Meeting Center.

6. Do one of the following:

   - If you are using Microsoft Internet Explorer as your browser, choose “Save this file to disk” in the File Download dialog box. Click OK.
   - If you are using Netscape Communicator as your browser, click Save File in the Unknown File Type dialog box.
7. In the Save As dialog box, locate or create the folder you want to use to store
the recorded meeting.

The name of the recorded meeting file contains a unique meeting identifier
followed by the RAP extension. When exporting the file, Lotus software
recommends that you change the filename to a name that is more easily
identifiable. For example, you might want to change a meeting file name from
"A1BC3235348F_recorded.rap" to "November2001BenefitsMeeting.rap."

8. Click the Save button.

Replacing recorded meetings: Use the "Replace recorded meetings" option to
replace an existing recorded meeting file with a different recorded meeting file.
This option is available from the Meeting Details document associated with the
recorded meeting.

This feature allows an administrator to:
• Replace a Sametime RAP file with a backup version if a RAP file is damaged.
• Replace a RAP file with an edited version of the file.

When you replace an existing recorded meeting file with another recorded meeting
file, the existing recorded meeting file is deleted. The existing file is deleted even if
the file that you replace it with has a different name. Before you replace a recorded
meeting file, you might want to use the Exporting recorded meetings feature to
make a backup copy of the file.

To replace a recorded meeting file:
1. Use a Web browser to browse to the Sametime server home page.
2. Click the "Attend a Meeting" link.
3. Click the Recorded link to see a list of all recorded meetings on the Sametime
server.
4. Click the name of the recorded meeting that you want to replace to open the
Meeting Details document.
5. Click the "Replace the Recording" button.
6. In the Replace Recorded Meeting dialog, type the path (or browse) to the
recorded meeting file that will replace the existing recorded meeting file.
   **Note** The existing file will be deleted and replaced with the file specified in the
Replace Recorded Meeting dialog box.
7. Click OK.

Importing recorded meetings: The "Import recording" feature enables an
administrator to add a recorded meeting to a Sametime server on which the
meeting did not previously exist. In a multiple server environment, an
administrator can use this feature to distribute recorded meetings to multiple
servers or to move recorded meetings from one server to another. Only Sametime
RAP files can be imported using this feature.

When importing a recorded meeting file, you can accept or change the following
meeting details for the recorded meeting:
• Meeting name
• Restrict the meeting to the following people
• Meeting password
• Secure this meeting using encryption
• Secure this meeting by not listing it in the Sametime Online Meeting Center
After you accept or change the meeting details, a Meeting Details document appears on the Sametime server for the imported meeting. The Meeting Details document includes the specifications you made while importing the meeting. Users access this new Meeting Details document from the "Recorded" view of the Sametime Meeting Center to play the recording of the meeting.

**Note:** You must export a meeting before you can import it. Exporting the meeting allows you to save a copy of the meeting on a network drive. You can also change the recorded meeting file name to an easily identifiable name when exporting a meeting. For more information, see [Exporting recorded meetings](#).

To import a recorded meeting to a Sametime server:

1. Use a Web browser to browse to the home page of the Sametime server to which you want to import the recorded meeting file.
2. Click the "Attend a Meeting" link.
3. Click the Import Recording link.
   
   **Note** If the Import Recording link is not visible, click the "Log on to Sametime" link beneath the date and time, and log on as the administrator. The administrator must be assigned the Sametime Admin role in the ACL of the Sametime Meeting Center (stconf.nsf) to see the Import Recording link.
4. On the "Import a Recorded Meeting" dialog box, browse to and select the recorded meeting file (RAP file) that you want to import.
   
   **Note** Browsing to the directory that holds all RAP files on the other Sametime server is not recommended because the RAP files do not have easily identifiable file names by default. The files are named according to unique numerical identifiers assigned to each meeting. Lotus software recommends that you use the [Export the meeting](#) feature to rename and copy the RAP file to a different directory before importing the meeting to a different Sametime server.
5. Click OK.
   
   **Note** It might take several seconds for the file to be imported to the server. The meeting creation screen appears when the import process concludes.
6. The meeting creation screen displays the values specified by the original creator of the meeting. The administrator can change or accept the following values in the meeting creation screen. All values specified in this screen will be reflected in the Meeting Details document for the recorded meeting in the Sametime Meeting Center.
   
   - **Meeting name** - The administrator can change the meeting name.
   - **Meeting start date, time, and duration** - These fields contain read-only information that cannot be changed.
   - **Restrict the meeting to the following people** - The administrator can remove or add names to the restriction list. If the restriction list contains any user names, only those users can replay the recorded meeting. If you want to allow any user to replay the meeting, remove all names from the restrictions list.
   - **Meeting password** - If a series of asterisks (***** ) displays in the "Meeting password" field, the original meeting was password-protected. If you leave the asterisks in the "Meeting password" field, the recorded version of the meeting will be password-protected by the password that was specified by the original creator of the meeting.
If you delete these asterisks and leave the "Meeting password" field blank, the recorded meeting will not be password-protected.

To change the password, delete the asterisks and enter a new password in the "Meeting password" field. The recorded version of the meeting will be password-protected by the new meeting password that you enter.

- Secure this meeting using encryption - Select this option if you want the recorded version of the meeting to be encrypted when it is streamed from the server to the Broadcast client. The meeting stream is encrypted using RC2 encryption with a 128-bit encryption key. Clear the check mark from this option if you do not want the recorded version of the meeting to be encrypted.

- Secure this meeting by not listing it in the Sametime Online Meeting Center - If the administrator selects this option, the recorded version of the meeting is not listed in the Meeting Center and can only be accessed from the View Unlisted link in the Meeting Center. If this option is not selected, the recorded meeting is listed in the Recorded view in the Meeting Center.

Note Attachments can also be added to the meeting by the person who is importing the recorded meeting file. These attachments can be downloaded by any user with permission to play the recorded meeting.

7. Click Save. Users can now access the Meeting Details document from the Recorded view of the Sametime Meeting Center to replay the recorded version of the meeting.

Recorded meeting performance issues: A recorded meeting is streamed onto a network by the Broadcast Services components in the same manner as a Broadcast meeting. Network congestion can affect the quality of the recorded meeting for the end user. Users viewing a recorded meeting that is streamed onto a congested network might see any of the following problems:

- The audio might cut out for a couple seconds.
- The video might pause for up to 15 seconds.
- The whiteboard or screen-sharing presentation might appear to pause for up to 45 seconds; after that time, you will begin receiving information again. If the Broadcast client stays in this state for up to 45 seconds, the user can try pausing the video. Pausing the video frees up network bandwidth for the other broadcast streams.
- You might not receive 100 percent of the chat text, sent Web pages, or polls in a meeting.

For more information on these issues, see Broadcast Services performance issues.

Connection Speed Settings for Meeting Services

The Connection Speed Settings for Meeting Services allow the administrator to set the speeds (bit rates) at which data streams are sent on the network for broadcast meetings without audio/video.

A screen-sharing/whiteboard Real-Time Protocol (RTP) data stream is sent on the network by the Sametime Broadcast Services during a broadcast meeting. This stream is received and played out by the Sametime Broadcast clients. For this data stream, the Sametime administrator can set one transmission speed for users with modem connections and a separate transmission speed for users with LAN/WAN connections.
The administrator also specifies whether the Connection Speed Settings for modem users or LAN/WAN users are used by default for all broadcast meetings created on the Sametime server. The end user can change this default setting for an individual meeting when creating a new broadcast meeting.

Note: To set Connection Speed Settings for broadcast meetings with audio/video, see Connection Speed Settings for Audio/Video Services.

For more information on Connection Speed Settings for Meeting Services, see the following topics:

- How the Connection Speed Settings are used
- Connection Speed Settings (Meeting Services)
- Type of connection speed setting to use for the default in scheduled and instant meetings
- Screen-sharing and whiteboard bit rate for broadcast meetings
- Connection Speed Settings and bandwidth usage
- Connection Speed Settings for Broadcast Services
- Broadcast Services performance issues

How Connection Speed Settings are used
This topic explains how the administrator sets the Connection Speed Setting defaults and how the end user can override these default settings.

Note: These settings are used to transmit meeting streams only in broadcast meetings without audio/video. These settings do not affect the transmission of data in interactive meetings.

To set the Connection Speed Settings, the administrator:
1. Sets the bit rate for the screen-sharing and whiteboard data stream for users with modem connections
2. Sets a separate bit rate for the screen-sharing and whiteboard data stream for users with LAN/WAN connections

During a Sametime broadcast meeting, the data streams are transmitted either at the connection speeds (or bit rates) that the administrator has specified for modem users or at the connection speeds that the administrator has specified for LAN/WAN users. Only one set of Connection Speed Settings is used in a meeting. It is not possible for modem users and LAN/WAN users connected to the same meeting to send and receive data at different rates.

The administrator can use the Type of connection speed setting to use for the default in scheduled and instant meetings setting to determine whether the Connection Speed Settings for modem users or for LAN/WAN users are used by default in all Sametime meetings. End users can change this default setting for scheduled meetings but cannot change it for instant meetings.

Note: At installation, the "Type of Connection speed settings to use for the default in scheduled and instant meetings" setting is set so that instant and scheduled meetings use the LAN/WAN connection speeds. The LAN/WAN connection speed settings can prevent modem users from participating in audio/video meetings.

End users can override the administrator-specified default and determine whether an individual scheduled meeting uses the LAN/WAN settings or the modem
settings. If the administrator determines that all Sametime meetings use the modem settings by default, the “People are attending this meeting using a modem” option on the Locations tab of the New Meeting page in the Meeting Center is selected by default, and the meeting data streams are transmitted using the Connection Speed Settings that are specified for modem users. If the end user clears the check mark from the “People are attending this meeting using a modem” check box, the meeting data streams are transmitted using the Connection Speed Settings that are specified for LAN/WAN users.

Note: If a meeting includes both modem users and LAN/WAN users, the “People are attending this meeting using a modem” option must be selected in the end-user interface for all users to receive the meeting streams. In this case, users attending over LAN/WAN connections will receive the data at the slower rate specified for modem users. For more information, see Connection Speed Settings for Broadcast Services and Broadcast Services performance issues.

Connection Speed Settings (Meeting Services)
The Connection Speed Settings for Meeting Services are used by the Sametime Broadcast Services when transmitting RTP streams for broadcast meetings without audio/video. The screen-sharing or whiteboard data stream requires most of the bandwidth needed for these meetings. Chat, Send Web Page, and Question and Answer Polling data streams might also be transmitted. However, the bandwidth requirements of these streams are so small that they do not require separate connection speed settings.

Note: To set Connection Speed Settings for broadcast meetings with audio/video, use the Configuration-Audio/Video Services-Connection Speed Settings of the Sametime Administration Tool. For more information, see Connection Speed Settings for Audio/Video Services.

The Connection Speed Settings include:

- **Type of connection speed settings to use for the default in scheduled and instant meetings** - Allows the administrator to specify whether the Connection Speed Settings for modem users or LAN/WAN users are used by default in all Sametime meetings. For more information, see How Connection Speed Settings are used.

- **Meetings with modem or LAN/WAN users** - The administrator selects “Meetings with modem users” from a drop-down list and then specifies the bit rates to be used for modem connections. The administrator then selects “Meetings with LAN/WAN users” and specifies the bit rates to be used for LAN/WAN connections. For more information, see Screen-sharing and whiteboard bit rate for broadcast meetings.

- **Screen-sharing and whiteboard bit rate for broadcast meetings** - Allows the administrator to specify the bit rate for the meeting streams that are sent by the Broadcast Services to Sametime Broadcast clients during a broadcast meeting without audio/video. The administrator can set one bit rate for modem connections and a separate bit rate for LAN/WAN connections.

**Type of connection speed setting to use for the default in scheduled and instant meetings:** The administrator can use the “Type of Connection speed settings to use for the default in scheduled and instant meetings” setting to determine whether the Connection Speed Settings for modem users or for LAN/WAN users are used by default in all Sametime broadcast meetings. End users cannot change this default setting for instant meetings.
**Note:** At installation, this setting is set so that instant and scheduled meetings use the LAN/WAN connection speeds. Broadcast meeting performance is best over the high-speed settings.

For scheduled meetings, the end user can override the default specified by the administrator and determine whether the Connection Speed Settings for modem connections or for LAN/WAN connections are used in a particular meeting. The end user selects or deselects the "People are attending this meeting using a modem" option when creating the meeting in the Sametime end-user interface to override the default.

The "People are attending this meeting using a modem" option is selected by default in the end-user interface if the administrator chooses "Meetings with modem users" as the default Connection Speed Settings for Sametime meetings. The end user can clear the check mark from this setting to have the meeting use the Connection Speed Settings specified by the administrator for LAN/WAN connections.

The "People are attending this meeting using a modem" option is not selected by default in the end-user interface when the administrator chooses "Meetings with LAN/WAN users" as the default Connection Speed settings for Sametime meetings. If the end user selects the modem option, the meeting uses the Connection Speed Settings specified by the administrator for modem connections.

To set the "Type of Connection Speed Settings to use for the default in scheduled and instant meetings" option:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
4. Choose Connection Speed Settings.
5. In the "Type of Connection Speed Settings to use for the default" option, make one of the following selections:

   - **Meetings with modem users** - If you select this option, the "People are attending this meeting using a modem" option is selected by default in the end-user interface when a user schedules a meeting in the Sametime Meeting Center. Any broadcast meeting started on the Sametime server uses the Connection Speed Settings the administrator specified for modem users unless the end user changes the default when creating the meeting. End users cannot change the default setting for instant meetings; all instant meetings use the Connection Speed Settings the administrator has specified for modem users if you select this option.

   - **Meetings with LAN/WAN users (default)** - If you select this option, the "People are attending this meeting using a modem" option is not selected by default in the end-user interface when a user schedules a meeting in the Sametime Meeting Center. Any broadcast meeting started on the Sametime server uses the Connection Speed Settings the administrator has specified for LAN/WAN users unless the end user changes the default when creating the meeting. End users cannot change the default setting for instant meetings; all instant meetings use the Connection Speed Settings the administrator has specified for LAN/WAN users if you select this option.

6. Click Update and restart the server for the change to take effect.
Screen sharing and whiteboard bit rate for broadcast meetings: The screen-sharing and whiteboard bit rate settings specify the bit rate for the screen-sharing and whiteboard broadcast data stream transmitted on the network by the Broadcast Services in Kilobits per second (Kbps). Different bit rates can be selected for the "Meetings with modem users" and "Meetings with LAN/WAN users" connection types.

The available screen-sharing and whiteboard bit rate settings are 16, 32, 64, and 128Kbps. The 16Kbps setting is recommended for modem connections. The higher settings provide better broadcast meeting performance. The higher settings consume more network bandwidth and use fewer CPU cycles to compress and decompress the data. For LAN/WAN connections, select the highest bit rate that the bandwidth capabilities of your network and the connection speeds of your clients will support. For information about the bandwidth implications of these settings, see Connection Speed Settings for Broadcast Services and Connection Speed Settings and bandwidth usage.

Note: This setting affects only the screen-sharing or whiteboard data stream sent by the Broadcast Services to the Sametime Broadcast clients during a broadcast meeting without audio/video. This setting has no effect on data transmission speeds in interactive meetings or broadcast meetings with audio/video.

To set the screen-sharing and whiteboard bit rates for broadcast meetings without audio/video:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
4. Choose Connection Speed Settings.
5. Select the "Meetings with modem users" setting.
6. Specify a screen-sharing and whiteboard bit rate for modem connections to broadcast meetings (16, 32, 64, and 128Kbps). 16Kbps is recommended for modem users.
7. Select the "Meetings with LAN/WAN users" setting.
8. Specify a screen-sharing and whiteboard bit rate for LAN/WAN connections to broadcast meetings (16, 32, 64, and 128Kbps).
9. Click Update and restart the server for the changes to take effect.

Controlling the bandwidth usage of the Meeting Services

Sametime includes a feature that enables you to control the network bandwidth used by the Sametime servers. This feature is useful if users are being disconnected from Sametime meetings because the network routers are being overwhelmed by the data surges that occur in large Sametime meetings (meetings of 20 users or more).

The following example illustrates how data surges may cause users to unexpectedly disconnect from the Sametime server during a meeting. In this example, assume that 50 users are attending a whiteboard meeting. During the meeting, the meeting moderator changes to a whiteboard slide that contains 100K of data. This 100K is pushed from the server to all 50 meeting attendees which results in a 5000K data surge on the network. The 5000K of data is sent as fast as the network will accept it.
If the network router closest to the Sametime server is capable of handling a data surge of this size, the meeting will proceed with no problems. However, if the router cannot handle the data surge, it will begin discarding packets. The discarding of packets may break some user TCP connections.

If users are unexpectedly disconnecting from Sametime meetings, you should check the router logs, or run diagnostics on the router that is closest to the Sametime server to determine if the router is discarding packets. If you determine that the router is discarding packets, you can enable the Sametime server Bandwidth Control feature. You can use this feature to ensure that the server transmits data at a rate that the router can handle. For example, you can configure the feature so that the maximum data surge sent on the network by the Sametime server is 1000K.

Before enabling this feature, consider the following:

- There are several highly dynamic variables involved in determining the appropriate Bandwidth Control feature setting. The number of users in a meeting, the size of the files that are shared or presented in a meeting, the level of other network activity occurring during the meeting, and the bandwidth handling capabilities of the routers all have a role in determining the appropriate setting for this feature. There is no specific formula that can be applied to determine the appropriate setting. The administrator must be familiar with the network equipment and network topology, and may need to study the Sametime usage and network usage statistics to arrive at the appropriate setting. Some experimentation may be required.

- Enabling the Bandwidth Control feature may slow the meeting performance. Higher settings for the MaxBandwidthAvailable parameter result in better performance, so it is beneficial to determine the highest possible setting for this parameter that the network can handle.

- This feature controls the amount of screen sharing and whiteboard data sent on the network by the Sametime Meeting Services. This feature does not control the amount of audio/video, broadcast, chat, and presence data sent on the network by other Sametime services.

### Enabling the Bandwidth Control feature

To enable the Bandwidth Control feature, you must configure three Windows registry settings. The three registry settings are listed and described below:

[HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Sametime\MeetingServer\MCAT\MCS\HTTP]
- "MaxBandwidthAvailable"="0"
- "BandwidthUpdateInterval"="10"
- "BandwidthReportInterval"="300"

### MaxBandwidthAvailable

When MaxBandwidthAvailable is set to 0 the feature is turned off.

When the MaxBandwidthAvailable has a non-zero number, this setting specifies the amount of meeting data in kilobits per second that the Sametime server can transmit on the network. If you want the server to transmit data at a rate of 1000Kbps, set the MaxBandwidth available setting as shown below:

- "MaxBandwidthAvailable"="1000"
**Note**: Providing a value for this setting that is too low may cause the server to operate at a speed that is too slow to use.

**BandwidthUpdateInterval**

The BandwidthUpdateInterval specifies the interval in milliseconds in which the server updates its internal bandwidth counters. The server counts the kilobits of data sent on the network and updates the internal counters at the interval specified by this setting. The server must periodically check the internal counters to ensure it is sending data at the appropriate rate (as determined by the MaxBandwidthAvailable value above).

The recommended setting for this interval is ten milliseconds, as shown below.

- "BandwidthUpdateInterval"="10"

**BandwidthReportInterval**

The BandwidthReportInterval specifies the interval in seconds in which the server reports bandwidth usage to the diagnostics window. This capability enables the administrator to monitor the bandwidth usage for diagnostics purposes.

The example below shows the BandwidthReportInterval set to 300 seconds.

- "BandwidthReportInterval"="300"

The minimum value for this setting is 1 second.

**Note**: The bandwidth usage is reported to the stddiagviewer window, under the MEDIA T120 MCSNC module.
Chapter 9. Configuring the Broadcast Services

This chapter describes the Broadcast Services and the administrative features associated with these services. This chapter discusses:

- Broadcast Services server components and clients
- Broadcast Services configuration settings and administrative tasks
- Broadcast Services Connection Speed Settings
- Broadcast Services performance issues

Broadcast Services components and clients

The Broadcast Services enable one-way RTP meeting data streams to be transmitted from the Sametime server to Sametime Broadcast clients on an intranet or the Internet.

Presenters in a broadcast meeting use the Sametime Meeting Room client to interact with each other and make presentations. The Broadcast Services on the Sametime server access the meeting data passing between the presenters and transmit this meeting data on the network as an RTP stream. The Broadcast Services can transmit up to six separate streams for a single meeting (separate streams are transmitted for chat, screen sharing/whiteboard, send Web page, polling, audio, and video data). Audience members receive these meeting data streams in the non-interactive, receive-only Sametime Broadcast client.

For information about the operation of the server and client components, see:

- Broadcast Services server components
- Broadcast Services client

Broadcast Services server components

The two server components that provide the Broadcast Services are the:

- Broadcast Gateway Controller
- Broadcast Gateway

The Broadcast Gateway Controller interacts with the Meeting Services, Community Services, and Audio/video Services on the Sametime server and passes control information to the Broadcast Gateway. The Broadcast Gateway handles client connections. The Broadcast Gateway also accesses meeting data and transmits RTP streams containing this data to the Broadcast clients.

Broadcast Gateway Controller

The Broadcast Gateway Controller resides on a Sametime server and monitors an event system within the Sametime server. The event system informs the Broadcast Gateway Controller when a broadcast meeting becomes active and provides the Broadcast Gateway Controller with information about the meeting. The Broadcast Gateway Controller passes this information to the Broadcast Gateway.

When a broadcast meeting becomes active, the Broadcast Gateway Controller sends a command to the Broadcast Gateway component of the Broadcast Services instructing the Broadcast Gateway to join the meeting and make the broadcast RTP streams available to the Sametime Broadcast clients.
The command to join the meeting is sent over a control connection that the Broadcast Gateway Controller establishes with the Broadcast Gateway. This connection occurs over the "Broadcast gateway control port" (default TCP port 8083) specified in the Broadcast Services Configuration-Connectivity-Networks and Ports settings of the Sametime Administration Tool.

**Broadcast Gateway**
The Broadcast Gateway Controller instructs the Broadcast Gateway to join a specific meeting on the Sametime server, as described in the previous section.

When the Broadcast Gateway joins a meeting, it connects to the Sametime Meeting Services, Community Services, and Audio/Video Services. The Broadcast Gateway connects to these services to:

- Gain access to the meeting data exchanged during the meeting
- Transcode the meeting data into RTP streams
- Transmit the RTP stream to the Broadcast clients

The administrator controls the rate at which the meeting RTP streams are transmitted using Connection Speed Settings in the Sametime Administration Tool. The administrator must set separate Connection Speed Settings for meetings that include audio/video and meetings that do not include audio/video (broadcast meetings that do not include audio/video are called "data-only" meetings).

- The administrator sets the Connection Speed Settings for broadcast meetings that do not include audio/video from the Configuration-Meeting Services-Connection Speed Settings option in the Sametime Administration Tool.
- The administrator sets the Connection Speed Settings for broadcast meetings that include audio/video from the Configuration-Audio/Video Services-Connection Speed Settings option in the Sametime Administration Tool.

The Connection Speed Settings selected by the administrator can have a significant impact on the Broadcast Meeting performance for the end users. For more information, see [Connection Speed Settings for Broadcast Services](#).

**Note:** To access audio/video streams, the Broadcast Gateway connects to the Multimedia Multipoint Control Unit (MMCU) component of the Audio/Video Services. The Broadcast Gateway communicates with the MMU to access the audio and video streams handled by the Audio/Video Services Multimedia Processor (MMP). The Broadcast Gateway transmits the audio and video streams to the Broadcast clients. The Sametime administrator can control the rate at which the audio and video streams are transmitted to clients from the "Audio bit rate" and "Video bit rate" options available from the Configuration-Audio/Video-Connection Speed Settings of the Sametime Administration Tool.

The Broadcast Services can transmit the RTP streams using the UDP transport, or tunnel the streams through a TCP/IP connection, a SOCKS 4 proxy server, or an HTTP proxy server. For more information on the transmission of the Broadcast streams to the Broadcast clients, see [Broadcast client connection process using JVM 1.4.2](#).

**Broadcast Services client**
The Sametime Broadcast client is a separate Java client that is loaded from the Sametime server to a user’s Web browser the first time a user attends a broadcast
meeting as an audience member. When attending the broadcast meeting, end users must respond “Yes” when prompted to trust the signer of the Sametime Broadcast client.

A meeting audience member uses the Broadcast client to watch and listen to any meeting activity that is taking place among the presenters in the meeting. The Broadcast client includes no interactive features.

**Connecting to the Broadcast Gateway**
The Broadcast clients connect to the Broadcast Gateway on the Sametime server to receive RTP streams containing meeting data. This connection process occurs in two parts. In the first part of the process, the Broadcast client makes a Real Time Streaming Protocol (RTSP) call control connection using the “Broadcast gateway port” (default TCP port 554).

The second part of the connection process involves the transmission of the RTP media streams. The manner in which the Broadcast client receives the RTP streams depends on:

- Whether the User Datagram Protocol (UDP) is available through all networks (routers and firewalls) between the Broadcast client and the Broadcast Gateway
- Whether the initial call control connection was a direct TCP/IP connection, a direct HTTP connection, or a connection through an HTTP or SOCKS 4 proxy server

For more information on this connection process, see [Broadcast client connection process using JVM 1.4.2](#).

**Buffering the broadcast data streams**
When the Broadcast client begins receiving the media streams, the client buffers the streams for a period of time before it begins to play them. The administrator can specify this buffering period from the “Time to buffer broadcast data” option in the Broadcast Services network settings of the Sametime Administration Tool.

This buffering period prevents network congestion from affecting the playback of the media streams. For example, if you buffer 10 seconds of data, you can tolerate up to 10 seconds of network congestion and packet delay before the end user notices any jitter effects (intermittent audio and video or garbled speech) in the playback of the media streams. If the network congestion clears in less than 10 seconds, the Broadcast client buffer refills, and the streams continue to play without the user noticing a problem. This buffering causes a slight delay (or latency) in the broadcast of the meeting between the sender and the receiver but ensures that the media streams play smoothly for the end user.

**Using multicast**
One of the primary purposes of the Broadcast Services is to enable meetings to scale to large audiences. The one-way transmission of RTP streams over the network-efficient UDP transport enables a meeting to scale to a large audience. Scalability can also be enhanced by the use of multicast technology.

If your network environment supports multicast technology, you can configure the Broadcast Services to take advantage of the multicast functionality to conserve network bandwidth usage. To support multicast for the Broadcast Services, the UDP transport must be available on the network and the routers in the network must be multicast enabled.
Note: Detailed discussion of the operation of multicast technology is outside the scope of this documentation. Multicast technology is discussed in IETF RFC 1112. There are also many Web sites and publications that discuss multicast.

To enable multicast for the Broadcast Services, select the Use multicast option available from the Configuration-Connectivity-Broadcast Services Network options of the Sametime Administration Tool.

When multicast is enabled and a broadcast meeting begins, the Broadcast Services randomly select a multicast address for the meeting from a range of available Class D multicast addresses. The administrator specifies the range of available addresses in the "Multicast addresses start at IP address" and "Multicast addresses end at IP address" fields in the Broadcast Services Network options of the Sametime Administration Tool.

Sametime can also be configured to query a server that supports the Multicast Address Dynamic Client Allocation Protocol (MADCAP) to obtain a multicast address for the meeting. MADCAP is an emerging standard that enables hosts to request multicast address allocation services from multicast allocation servers (some Windows DHCP servers support MADCAP). This protocol can prevent multicast address conflicts if you have other applications deployed on your network that require multicast addresses. For more information, see Assign multicast addresses using MADCAP.

The Broadcast Services transmit data to the selected multicast address. The Broadcast clients "join" the multicast address. When the Broadcast client joins a multicast address, a message is sent to the local multicast-enabled router that indicates the client is interested in receiving information on this address. The routers disseminate multicast information among themselves using their own protocols.

Note: To preserve the resources of multicast-enabled routers, all meeting streams associated with a broadcast meeting are sent to a single multicast address. Although up to six streams might be sent to the router, the router is only required to maintain information for a single multicast address. Each meeting stream is sent on a different UDP port to this multicast address.

For a client to receive the multicast broadcast meeting streams, the Broadcast client makes an RTSP TCP/IP call control connection to the Sametime server Broadcast Gateway on the port specified as the "Broadcast gateway control port" (default port 554) in the Broadcast Services Network and Ports options of the Sametime Administration Tool. Over this call control connection, the server informs the client that multicast is available for the meeting.

The Broadcast Services begin sending broadcast meeting streams to the client using the unicast UDP transmission method. When multicast is available, the Broadcast client also joins the multicast address. If the client begins to receive the broadcast meeting streams from the multicast address, the client halts the unicast transmission of the streams and receives all meeting content through the multicast streams.

When multicast is enabled, the administrator can control how far the multicast traffic will propagate on the network before the multicast traffic is discarded by network routers. The administrator can specify a Time-To-Live (TTL) for the multicast UDP packets. This TTL setting can limit the number of router hops the
packets make before they are discarded. For more information on this setting, see Specifying the multicast time to live (TTL).

Configuring the Broadcast Services settings

To access the configuration options for the Broadcast Services, open the Sametime Administration Tool and select Configuration-Connectivity-Network and Ports-Broadcast Services Network.

Note: To configure Connection Speed Settings for the Broadcast Services, see Broadcast Services Connection Speed Settings and meeting performance.

Before changing these configuration settings, the administrator should be familiar with the operations of the Broadcast Services and the connection process of the broadcast client.

Broadcast configuration settings

These settings are described in the Broadcast Services network settings topic in the “Configuring ports and network connectivity” section of this documentation.

The Broadcast Services configuration options include:

- Broadcast gateway address for client connections
- Broadcast gateway address for control connections
- Enable Web client to try HTTP tunneling after trying other options (Broadcast Services)
- Use multicast
- Time to buffer broadcast, audio, and video data (This setting is located in the Configuration-Audio/Video Services-Interactive Audio/Video Services tab of the Sametime Administration Tool.)
- Connection Speed Settings (Broadcast Services Connection Speed Settings are discussed later in this chapter.)

Broadcast Services Connection Speed Settings and meeting performance

The Connection Speed Settings allow the administrator to set the speeds (bit rates) at which audio, video, and data (screen sharing/whiteboard) streams are sent on the network to the Sametime Broadcast clients. The administrator must set separate Connection Speed Settings for meetings that include audio and video and meetings that do not include audio/video (broadcast meetings that do not include audio/video are called "data-only" meetings).

- The administrator sets the Connection Speed Settings for broadcast meetings that do not include audio/video from the Configuration-Meeting Services-Connection Speed Settings option in the Sametime Administration Tool. For information on using these Connection Speed Settings, see Connection Speed Settings for Meeting Services.
- The administrator sets the Connection Speed Settings for broadcast meetings that include audio/video from the Configuration-Audio/Video Services-Connection Speed Settings option in the Sametime Administration Tool. For information on using these Connection Speed Settings, see Connection Speed Settings for Audio/Video Services

The Connection Speed Settings can affect the broadcast meeting performance for the end user. This section discusses some issues to consider when setting
Connection Speed Settings for broadcast meetings. These issues can affect the broadcast meeting performance of the Sametime server.

**Setting Connection Speed Settings for broadcast meetings that do not include audio/video**

The Sametime Administration Tool includes separate Connection Speed Settings for broadcast meetings that do not include audio/video. These Broadcast meetings might include screen sharing, whiteboard, chat, send Web page, and question and answer polling activity.

If a user schedules a broadcast meeting, and the user does not include the audio/video tools in the meeting, the meeting streams are transmitted at the rates defined in the Configuration-Meeting Services-Connection Speed Settings of the Sametime Administration Tool.

Separate meeting stream transmission rates can be specified for users that have modem connections to the server and users that have LAN/WAN connections to the server. The available transmission rates are 16K (Kilobits per second), 32K, 64K, and 128K. For example, the administrator can specify 32K as the transmission rates for modem users and 128K as the transmission rate for users with LAN/WAN connections to the server.

Only one transmission rate can be used in a meeting (either the transmission rate specified for LAN/WAN connections or the transmission rate specified for modem connections). The default settings of a Sametime server invoke the LAN/WAN connection speed settings for all broadcast meetings. To use the slower modem Connection Speed Settings in a broadcast meeting, the end user must override the default by selecting the “People are attending using a modem” option in the Tools tab of the New Meeting page when creating the meeting.

Meeting performance can improve significantly with the higher bit-rate settings. However, the administrator must also consider the slowest speed at which users will connect when specifying the bit rates for broadcast meetings that do not include audio and video. For example, if the bit rate setting specified for the meeting is 64K, and a user connects to the server using a 56K modem, the user cannot attend the meeting.

For more information, see **Connection Speed Settings for Meeting Services** and **Broadcast Services performance issues**.

**Setting Connection Speed Settings for broadcast meetings that include audio/video**

The administrator uses the Configuration-Audio/Video Services-Connection Speed Settings to specify the meeting stream transmission rates for broadcast meetings that include audio/video.

When setting Connection Speed Settings for broadcast meetings that include audio/video, the administrator should consider the slowest speeds at which users will connect and the cumulative bandwidth required to transmit all meeting streams in the broadcast meeting. These factors can greatly affect meeting performance for the end users.

As an example, consider a broadcast meeting that has the following characteristics:

* Audio is used so an audio stream is transmitted to all clients
* Video is used so a video stream is transmitted to all clients
• Whiteboard is used so a whiteboard stream is transmitted to all clients
• The end user selects the "People are attending using a modem" option when creating the meeting.

When the "People are attending using a modem" option is selected, the "Meetings with modem users" connection speed settings are invoked for the meeting. The "Meetings with modem users" settings are defined by the administrator (from the Configuration-Audio/Video Services-Connection Speed Settings of the Sametime Administration Tool). In this example, we assume the administrator has defined the following parameters for "Meetings with modem users:"
  • Audio bit rate - 6.3Kbps (The G.723 audio codec is invoked.)
  • Video bit rate - 16Kbps
  • Screen sharing and whiteboard bit rate - 16Kbps

During the meeting, the meeting data streams are transmitted at the following rates:
  • The audio stream transmits audio at 17Kbps

  Note: The G.723 codec usually transmits at 6.3 Kbps. However, transmission overhead causes the G.723 codec to transmit at 17Kbps.
  • The video stream transmits at 20Kbps (16Kbps + 4Kbps of packet overhead).
  • The whiteboard stream transmits at 20Kbps (16Kbps + 4Kbps of packet overhead).

The cumulative bit rate of all streams in this meeting is 57Kbps (17Kbps + 20Kbps + 20Kbps). Clients connecting to this meeting must have a connection speed faster than 57Kbps. Users connecting to this meeting at 56Kbps will either be unable to participate in the meeting or experience severe performance problems.

Generally, to experience good meeting performance when attending a broadcast meeting that includes audio, video, and screen sharing/whiteboard activities, a user requires a DSL or cable modem or a LAN/WAN connection to the Sametime server.

The example above assumes that the end user selected the "People are attending using a modem" option when creating the meeting. As an alternate example, consider the same audio, video, and whiteboard meeting except assume the end user does not select the "People are attending using a modem" option when creating the meeting.

When the "People are attending using a modem" option is not selected, the "Meetings with LAN/WAN users" connection speed settings are invoked for the meeting. The "Meetings with LAN/WAN users" settings are defined by the administrator (from the Configuration-Audio/Video Services-Connection Speed Settings of the Sametime Administration Tool). Also assume the administrator has defined the following parameters for "Meetings with LAN/WAN users:"
  • Audio bit rate - 64Kbps (The G.711 audio codec is invoked.)
  • Video bit rate - 64Kbps
  • Screen sharing and whiteboard bit rate - 64Kbps

In this configuration, the cumulative bit rate used by the meeting is 192 Kbps (64 Kbps + 64 Kbps + 64 Kbps). An individual user connecting to a broadcast meeting that uses the "Meetings with LAN/WAN users" Connection Speed Settings must
have a connection capable of handling this cumulative bit rate to experience satisfactory performance in the broadcast meeting.

If your environment requires users to consistently access broadcast meetings over 56Kbps connections, the person creating the meeting should consider eliminating video from the meetings when creating them. If only the whiteboard and audio are available in the meeting, a connection speed of greater than 37Kbps (17Kbps + 20Kbps) is required to view and hear the meeting. Most users with 56Kbps modems should experience adequate meeting performance with these bandwidth requirements.

If broadcast meeting performance is still not acceptable after making these changes, it might be necessary to use a telephone conferencing solution for the audio in broadcast meetings to accommodate users with slow connections to the Sametime server. When the audio stream is removed from the broadcast meeting, the Connection Speed Settings defined for meetings that do not include audio/video are used to transmit the streams, which can significantly enhance the screen sharing or whiteboard presentations.

The end user controls the Connection Speed Settings that are used in a meeting

The end user controls whether the "Meetings with LAN/WAN users" connection speed settings or the "Meetings with modem users" connection speed settings are used for a broadcast meeting when the end user creates the meeting.

If the end user selects the "People are attending using a modem" option in the Tools tab of the New Meeting page when creating a meeting, the "Meetings with modem users" Connection Speed Settings are used for the meeting. If the end user clears the check mark from the "People are attending using a modem" setting the "Meetings with LAN/WAN users" Connection Speed Settings are used in the meeting.

If all users attending the meeting have LAN/WAN connections, but the end user mistakenly selects the "People are attending using a modem" option, the users might experience poor meeting performance unnecessarily (meeting streams are transmitted at much slower rates than the users can handle).

To minimize mistakes of this kind, the administrator can specify the default setting for the "People are using a modem" option. Use the "Type of connection speed settings to use for the default in instant and scheduled meetings" setting on the Connection Speed Settings tab of the Sametime Administration Tool to specify the default.

If the administrator selects the "Meetings with LAN/WAN users" value for the "Type of connection speed settings to use for the default in instant and scheduled meetings" setting, the check mark is cleared from the "People are attending using a modem" setting in the end-user interface by default. All broadcast meetings transmit streams using the "Meeting with LAN/WAN users" connection speed settings unless the end user manually changes the default.

The administrator should ensure that the default state (selected or not selected) for the "People are attending using a modem" setting is appropriate for the environment. The "People are attending using a modem" setting is not selected by default following a Sametime server installation.
Broadcast Services performance issues

During a broadcast meeting, end users might notice any of the following conditions:

- The audio might cut out for a couple seconds.
- The video might pause for up to 15 seconds.
- The whiteboard or screen sharing presentation might appear to pause for up to 45 seconds; after that time, the user receives information again. If the Broadcast client stays in this state for up to 45 seconds, the user can try pausing the video. Pausing the video frees up network bandwidth for the other broadcast streams.
- The user might not receive 100 per cent of the chat text, sent Web pages, or polls in a meeting.

The problems described above are caused by network congestion. The Sametime broadcast system transmits network packets using the User Datagram Protocol (UDP) network transport. Generally, UDP packets are considered “low priority” by network components (such as routers, bridges, or gateways). Because of their low priority status, UDP packets are frequently the first to be discarded when a network approaches its capacity limits.

When packets are discarded on a congested network, the end users might experience the audio, video, and screen sharing or whiteboard “dropouts” or pause intervals described above.

**Note:** The network key frame cycles used for audio, video, and screen sharing/whiteboard data determine the length of the stream “dropout” or pause interval. When significant packet loss occurs, the Broadcast client appears to pause or drop the stream, and the stream does not play out until the next key frame cycle for that stream. Generally, these cycles result in the different dropout or pause periods for audio, video, and screen sharing/whiteboard delays described above.

There is little the administrator can do concerning packet loss on a congested network. However, Sametime does include some administrative settings that the administrator can use to minimize the problems caused by packet loss and improve broadcast performance. For more information, see the following topics:

- **Time to buffer broadcast, audio, and video data** in the “Configuring Audio/Video Services” chapter.
- **Audio frames per packet** in the “Configuring Audio/Video Services” chapter.
- **Connection Speed Settings for Broadcast Services** in this chapter.

**Note:** Muting the audio stream during a broadcast meeting stops audio transmission from the server. Muting the audio lessens bandwidth consumption for broadcast meetings. If you mute the audio, the audio/video jitter buffers must refill with audio data when you play the audio. There may be an audio delay in the broadcast meeting of up to 10 seconds while the buffers refill. Pausing and then playing the video during a broadcast meeting has the same effect as muting the audio stream.

For additional information on broadcast performance issues, see **Broadcast Services Connection Speed Settings and meeting performance**.
Chapter 10. Configuring the Audio/Video Services

This chapter describes Audio/Video Services and the administrative features associated with these services. This chapter discusses:

• Client system requirements for the Audio/Video Services
• IP Audio/Video terminology and concepts
• Audio/Video Services components and clients
• Audio/Video Services configuration settings and administrative tasks
• Usage Limits and Denied Entry settings
• Audio/Video Services Connection Speed Settings
• Using a 360-degree video camera

About the Audio/Video Services

The Audio/Video Services support interactive IP audio and video capabilities and enable clients with the appropriate hardware (sound card, microphone, speakers, and camera) to transmit and receive real-time audio and video during a Sametime meeting.

Audio/video components of the Sametime Meeting Room client connect to the interactive Audio/Video Services. Audio/video components in the Sametime Meeting Room client include local and remote video windows, microphone and speaker volume controls, audio mute, and video pause controls.

In an interactive audio/video meeting, any meeting participant can speak and be heard by all other meeting participants. The video from the camera of the speaking person is displayed to all other meeting participants in a video window on each participant’s local machine. A participant also sees the video from the participant’s local camera in a separate video window in the Meeting Room client.

Sametime audio/video meetings can include audio only or both audio and video. Video-only meetings are not supported. In an interactive audio/video meeting, a camera is optional. Users without a camera can receive video images from the server but cannot transmit video.

The Sametime Audio/Video Services can also operate with the Sametime Broadcast Services so that audio/video meetings can be broadcast on the network and received by the Sametime Broadcast clients. For more information, see the Sametime Broadcast Services.

The Audio/Video Services are enabled by default following a Sametime server installation. The administrator can enable and disable the Audio/Video Services from the Configuration-Audio/Video-Interactive Audio/Video Services tab of the Sametime Administration Tool.

You can use a BeHere TotalView High Res 360-degree video camera with the Sametime 7.0 server. A Sametime client system can capture a 360-degree video stream and transmit it through the Audio/Video Services to the other Meeting participants. Both the Meeting Room client and Broadcast client can receive and play this 360-degree video stream.
See the following topics pertaining to the Audio/Video Services:

- **Client system requirements for the Audio/Video Services** - Provides information about the system requirements for client computers, including information about sound cards, microphones, and cameras.
- **IP Audio/Video terminology and concepts** - Provides a brief glossary of IP audio and video terminology.
- **Audio/Video Services components and clients** - Provides information about the operation of the Audio/Video Services server components and clients.
- **Audio/Video Services configuration settings** - Describes the configuration settings for the Audio/Video Services available from the Sametime Administration Tool. These settings include:
  - Interactive Audio/Video Services
  - Usage Limits and Denied Entry
  - Connection Speed Settings
  - Interactive Audio/Video Network and Ports settings
- **Using a 360-degree video camera with Sametime** - Provides information about using a 360-degree video camera in Sametime interactive and broadcast audio/video meetings.
- **Tips for using audio/video** - Provides tips to assist end users in conducting successful audio/video meetings on the Sametime server.

**Audio/Video Services Connectivity settings**

For information about the ports used by the Audio/Video Services and the available connectivity options, see **Interactive Audio/Video Network settings** and **Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)**

### Client system requirements for the Audio/Video Services

<table>
<thead>
<tr>
<th>CPU:</th>
<th>Pentium II 233 MHz or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory:</td>
<td>128MB RAM for Windows 2000 Professional or Windows XP</td>
</tr>
<tr>
<td>Browsers:</td>
<td>For information about Web browser supported by the Sametime 7.0 server, see the Lotus Sametime Server 7.0 Installation Guide.</td>
</tr>
<tr>
<td>Sound card:</td>
<td>A full-duplex sound card is required to participate in interactive audio/video meetings.</td>
</tr>
<tr>
<td></td>
<td>A half-duplex sound card is required to enable a user to listen to a recorded meeting or to an audio/video meeting that is broadcast by the Sametime Broadcast Services.</td>
</tr>
<tr>
<td></td>
<td>A list of supported sound cards is provided below.</td>
</tr>
<tr>
<td>Microphone and speakers:</td>
<td>Lotus software recommends a microphone and speakers that are of good quality. Avoid microphones with on and off switches unless they are of high quality. A headset that contains a boom microphone performs best. If a desktop microphone is used, a unidirectional dynamic microphone that uses batteries is preferred.</td>
</tr>
<tr>
<td>Video capturing software:</td>
<td>Video for Windows.</td>
</tr>
<tr>
<td>Camera:</td>
<td>A high-quality USB camera. (Do not use parallel port cameras.) A camera is optional. Users who do not have a camera can participate in an audio/video meeting. When a user without a camera speaks, no video is displayed to other users in the meeting. A list of supported cameras is provided below.</td>
</tr>
</tbody>
</table>
Supported sound cards and cameras

The following tables identify sound cards and cameras that you can use with Sametime.

Sound cards

Any correctly installed full-duplex sound card should work with Sametime. The list below includes all sound cards that have been tested with Sametime to date. If a specific sound card is not listed, check the Sametime Release Notes (strn70.nsf or strn70.pdf) for more up-to-date information.

These sound cards have been tested with Sametime:

- CrystalWare (integrated)
- Montego A3D Xstream
- SoundBlaster Live Value
- ALS120
- Aureal Vortex A3D SQ1500
- Aureal SB Audio PCI 64V
- ES1887 (integrated)
- Montego II A3D
- Montego II Quadzilla
- Rockwell WaveArtist
- SoundBlaster PCI 128
- SoundBlaster PCI 512
- SoundBlaster 32 AWE
- SIIG SoundWave Pro PCI
- Yamaha DS-XG (integrated)
- Creative Crystal PnP Es 1868
- Creative Sound Blaster Creative 16 Plug & Play
- Creative AWE64
- Creative SoundBlaster PCI
- Addonic (PCI)
- Crystal Audio (Dell onboard sound card)
- Crystal SoundFusion PCI Audio Accelerator (IBM ThinkPad® default)

Cameras

A high-quality USB camera that is compatible with Video for Windows and Windows sound cards is recommended.

Note: Sametime supports the TotalView High Res 360-degree video camera from BeHere Technologies. For more information about this camera, such as required hardware and software, see the camera documentation.
IP audio/video terminology and concepts

This section defines common audio/video terminology and discusses some of the concepts and issues associated with the use of audio/video over IP networks.

Codec

A codec compresses streaming data, such as audio or video, on the transmitting side and decompresses it for playback on the receiving side. Codecs reduce the amount of bandwidth required to send streaming data. Generally, higher compression conserves more bandwidth. Higher compression also results in poorer audio or video quality and requires more CPU cycles to compress and decompress the data streams.

The Sametime Audio/Video Services support audio codecs (G.711 and G.723) and one video codec (H.263+).

- **G.711** - This audio codec contains more frequencies and produces a better sound quality than G.723. G.711 data is less compressed and consumes more bandwidth and fewer CPU cycles than G.723. G.711 requires a 64Kbps connection and cannot be used with a 56K modem.
- **G.723** - This audio codec compresses data by removing all frequencies except those that support voice. This codec uses less network bandwidth but consumes more CPU cycles than G.711. This codec is recommended for voice transmissions but not for music.
- **H.263+** - This video codec is used by the Audio/Video Services to compress and decompress the video data. The "+" extensions of this codec are not used by Sametime 7.0.

Bandwidth

Bandwidth refers to the amount of data that can flow through a network connection. Typical throughputs for network connections are:

- **28.8K modem** - 28Kbps (Kilobits per second)
- **56K modem** - 56Kbps
- **ISDN** - 64Kbps
- **LAN** - LAN connection speeds vary. Typical connection speeds fall between 10 and 100Mbps (Megabits per second). Data collisions affect the connection speed. For example, a 10Mbps LAN connection might peak at 2Mbps under heavy traffic conditions.

If you are planning bandwidth consumption for a 56K modem, plan for a maximum rate of 48K. Generally, the G.723 audio codec uses approximately 6.3Kbps in one direction. With overhead, this codec might use 10Kbps, depending on other factors. The available bandwidth of a 56K modem is generally adequate for voice, screen-sharing, and whiteboard data, assuming that data is not flowing simultaneously in both directions. Audio quality degrades temporarily if throughput is too high. The H.263+ video codec consumes a minimum of 16Kbps. Video is not recommended when operating over a 28.8K modem.

Duplex modes

Duplex refers to the mode in which audio is transmitted and received during a meeting. The two duplex modes are full-duplex and half-duplex.
• **Full duplex** - With full-duplex mode, you can simultaneously transmit and receive. For example, while you are speaking you can also hear another person speaking to you. The full-duplex mode is similar to talking to someone on the telephone because you can begin speaking immediately when the other person stops speaking or you can interrupt the other person.

  To participate in an interactive audio/video meeting, the end user should have a sound card that supports full-duplex mode.

• **Half duplex** - With half-duplex mode, you can transmit and receive, but you cannot do both at the same time. In this mode only one person can speak at a time. You must stop speaking before you can hear anyone else speak.

  Users that have half-duplex sound cards installed can listen to audio/video meetings that are using the Sametime Broadcast Services. Users must have a full-duplex sound card to participate in interactive audio/video meetings.

Echo cancellation

A feature that eliminates any echo caused by audio coming out of your speakers and going back into your microphone. This type of echo can occur when your speakers and microphone are too close together (for example, if you are using a laptop with speakers and microphone set close together or if you move your microphone too close to your desktop speakers). To eliminate echoes in meetings, a user can use headphones or a speakerphone with echo cancellation or select the echo cancellation check box in the audio preferences of Sametime.

Jitter buffer management

Jitter buffer management occurs on the receiving side of a conversation. This technology compensates for delays in the delivery of real-time data caused by network congestion or disruption. Audio packets are streamed from a sender at a consistent rate. However, varying network conditions make the arrival of packets unpredictable. Packets might take longer than expected to arrive, arrive out of order, or be lost. A jitter buffer saves several packets before playback of the packets begins.

For example, assume each packet contains 30 milliseconds (ms) of audio. The jitter buffer can save up to 10 packets. This process adds 300 ms of delay (or latency) to the playback but significantly increases overall quality. The delay period enables slowed or out-of-order packets to arrive and be properly sorted for playback before playback begins.

Latency

When two audio clients are connected and one person speaks, a substantial amount of time might pass before the other person hears what was said. This delay is called latency. Latency is caused by:

• Processor performance at the sending, receiving, and server computers
• Network bandwidth usage
• Jitter buffer management

Before audio data from the microphone can be transmitted on the network, the data must be encoded into the proper codec form. Encoding audio data can consume 15 to 30 times more CPU cycles than decoding the same audio. Fast processors with multimedia extensions (MMX™) reduce the amount of time required to encode the data and allow the data to be transmitted faster.
On the receiving end, the data must be decoded before being played out through the speakers. This delay is much less than the delay that occurs at the sender.

Available network bandwidth is usually the primary contributor to latency. Heavy network traffic can cause packets to be delayed or discarded. Delayed or discarded packets can result in increased latency or garbled speech. For these reasons, it is best to avoid using slow modems when connecting to Sametime meetings.

MMX

MMX is a set of multimedia extensions that enhance the ability of a processor to handle streaming data. MMX provides a codec with a significant performance improvement in encoding and decoding streaming data.

H.323

The H.323 standard, which is a recommendation from the International Telecommunications Union (ITU), provides a foundation for audio and video communications across IP-based networks, including the Internet. H.323 sets standards for multimedia communications over local area networks (LANs) that do not provide a guaranteed quality of service (QoS).

You can find basic information about H.323 at www.webproforum.com/h323/index.html. You can also visit www.ietf.org to research Requests for Comments (RFCs) related to H.323.

Real-Time Protocol (RTP)

The RTP is designed to transmit packets containing audio or video data. Each packet contains a payload type, a sequence number, a time stamp, codec data, and other information.

Real-Time Control Protocol (RTCP)

The RTCP sends time stamps to synchronize the data streams and reports about the number of RTP packets received and lost. RTCP also communicates transmission statistics from the sender and canonical names associated with data stream sources.

User Datagram Protocol (UDP)

UDP is a transport level protocol that operates on top of IP at the same network level as TCP. UDP is an unreliable and connectionless transport. Unreliable means that packets are not guaranteed to arrive at their destination in order and might not arrive at all. Connectionless means that an active connection between two systems is not maintained. If one system shuts down, the other system is not notified.

UDP is generally more efficient than TCP at handling real-time data, and is the preferred transport method for real-time data.

Audio/Video Services components and clients

The Audio/Video Services support interactive IP audio-only and interactive IP audio/video meetings that include two or more meeting participants. Video-only meetings are not supported.
Two server components provide the Audio/Video Services: the Multimedia Multipoint Control Unit (MMCU) and the Multimedia Processor (MMP).

The Audio/Video Services support the Sametime Meeting Room client.

For information about the operation of the server and client components, see:
- Audio/Video Services server components
- Audio/Video Services clients

**Audio/Video Services server components**

The Audio/Video Services server components include the:
- **Multimedia Multipoint Control Unit (MMCU)** - Manages client connections
- **Multimedia Processor (MMP)** - Manages the audio and video streams

**Multimedia Multipoint Control Unit (MMCU)**

The MMCU manages client connections and passes audio/video call setup and control information between the server and the clients joining the meeting.

The Sametime administrator controls much of the call setup and control information that is passed to the clients through the settings available in the Connection Speed Settings of the Sametime Administration Tool. Some of the more significant attributes that are passed from the MMCU to the client during the call setup and control process include:
- Audio codec (G.711 or G.723)
- Video codec (H.263+)
- Video bit rate (16Kbps to 128Kbps)
- Encryption (enabled or disabled)
- UDP and TCP tunneling ports for the audio and video streams

**Note:** For more information on the audio/video attributes that are specified by the administrator, see [Connection Speed Settings for Audio/Video Services](#) and [Encrypting all meetings](#).

The MMCU is also responsible for setting up the call in the MMP. In addition to setting up the call, the MMCU interacts with the MMP to coordinate the video source with the audio source as described in "Multimedia Processor (MMP)" below.

**Note:** The MMCU uses the host name and port specified in the Configuration-Connectivity-Interactive Audio/Video Network-Multimedia control address settings of the Sametime Administration Tool to establish a connection with the MMP.

**Multimedia Processor (MMP)**

The MMP component of the Audio/Video Services manages the audio and video Real Time Protocol (RTP) streams. The MMP scans the meeting participants who have connected to the MMCU and locates the person currently speaking (transmitting audio packets). The MMP performs switching operations as different people speak during a meeting.

When a meeting participant speaks, the MMP locks onto that client’s audio stream and distributes that stream to all other clients in the meeting. When a participant stops speaking, the MMP waits for a brief period of time, and then begins scanning for the other active audio clients.
The time interval that the MMP waits before scanning for other active clients is specified by the administrator in the Time to wait for silence before switching to next speaker setting available in the Audio/Video Services settings of the Sametime Administration Tool. This time interval prevents the MMP from switching during normal pauses in conversation. Rapid audio switching can unnecessarily tax the system CPU and consume network bandwidth.

The video follows the audio. When the MMP switches to a new audio source (speaking person), the MMP sends an event to the MMCU. The MMCU, through its connections to the clients, ensures that the icon indicating the current speaker is properly updated for all clients. After this update, the MMCU instructs the MMP to set the video source to the person currently speaking.

It is important to ensure that the video does not switch too quickly. Rapid video switching reduces usability and can consume considerable network bandwidth. The administrator can control the time interval that must pass before the video switches to the new speaking person. This time interval is specified in the Time to wait before switching to the next video (ms) setting in the Audio/Video Services settings.

Note: If the current speaker does not have video capabilities or has the video window paused, the MMCU ensures that all client video windows are also paused.

The MMP can lock onto and broadcast a maximum of two audio streams at the same time. In a Sametime meeting, if two people speak at the same time, it is possible for all meeting participants to simultaneously hear both people speaking. However, if three people speak simultaneously, only two of the people will be heard. The MMP designates the audio stream that has been transmitting the longest (generally, the person who started speaking first) as the primary audio stream. The source of the primary audio stream is also the source of the video stream.

Note: Sametime can also transmit a 360-degree video stream to meeting participants. For more information, see Using a 360-degree video camera with Sametime.

**Automatic Microphone and Request Microphone modes**

End users use two types, or modes, of audio: Automatic Microphone mode and Request Microphone mode. All meetings begin in Automatic Microphone mode, but an end user can switch to Request Microphone mode during the meeting. Full-duplex sound cards are required to participate in either an Automatic Microphone or Request Microphone meeting.

- **Automatic Microphone Mode** - Sametime Meeting Room clients perform a two-way mixing process that enables two voices to be played out simultaneously. The Sametime end-user interface refers to this two-way mixing mode as "Automatic Microphone."

  In Automatic Microphone mode, any meeting participant can speak at any time. Unlike Request Microphone mode, Automatic Microphone mode does not require the user to request the microphone before speaking. Two people speaking simultaneously can both be heard by all meeting participants. (However, a third person speaking will not be heard.) Automatic Microphone mode provides a more natural and less controlled conversational experience in meetings.
Note: The Automatic Microphone mode consumes more network bandwidth than the Request Microphone mode.

- **Request Microphone Mode** - In Request Microphone mode, only one user can speak at a time. Before speaking, a user must request the microphone. If the microphone is owned by another participant, the participant currently speaking must release the microphone before another user can speak. Request Microphone mode is a more controlled audio environment than Automatic Microphone mode.

Note: Mixing modes that enable more than two participants to speak simultaneously and be heard by all other meeting participants are not supported in Sametime 7.0. (These higher mixing modes are sometimes referred to as “n-way mixing.”)

### Audio/Video Services client

The Audio/Video Services support connections from the **Sametime Meeting Room client**.

### Sametime Meeting Room client

When a user attends a meeting that includes interactive audio/video capabilities, the Sametime Meeting Room client includes audio and video controls.

The audio component of the Sametime Meeting Room includes microphone and speaker volume controls and audio mute features. The video component includes:

- A local video window that displays the image from the user’s local camera
- A remote video window that displays the image from the camera of the user who is speaking

End users should test their audio and video equipment to ensure that their local systems are optimally configured to interact with the Sametime Audio/Video Services. Users can test their audio and video equipment from a Test Audio/Video link in the Sametime Online Meeting Center.

**Connecting to the MMCU:** The Sametime Meeting Room client makes a connection to the Meeting Services on the Sametime server as described in **Meeting Room client connection process using JVM 1.4.2 (Community Services and Meeting Services)** in the Connectivity chapter of this documentation. Over this connection, the Multimedia Multipoint Control Unit (MMCU) exchanges call-signaling and call-control information with the audio/video components of the Sametime Meeting Room client.

For detailed information on the network settings and the connection process of the Sametime Meeting Room client audio/video components, see:

- **Interactive Audio/Video Services network settings**
- **Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)**

**Buffering audio and video data streams**: When the Meeting Room client begins receiving the audio and video data streams during an interactive audio/video meeting, the client buffers the streams for a brief period of time before it begins to play them. The administrator can specify the amount of audio and video data that is held in the buffer from the **Audio/Video jitter buffer** setting in the Audio/Video Services Connection Speed Settings of the Sametime Administration Tool.
This buffer setting can minimize the effect of network congestion on the quality of
the audio and video data streams that are played out for the end user. Network
congestion can delay the delivery of some audio and video packets, which might
result in intermittent audio and video or garbled speech. Buffering a small amount
of the data can result in smoother audio and video performance for the end user.
The buffering of audio and video also causes a slight delay (or latency) between
the time a meeting participant speaks and the time that the sounds and images
originating from that meeting participant’s computer are played out to the other
remote meeting participants.

For more information, see Connection Speed Settings for Audio/Video Services

Adjusting audio frames per packet and video bit rate: Network packet loss can
also affect the quality of the audio played out by the client. The administrator can
minimize the effect of network packet loss by adjusting the Audio frames per
packet setting. This setting enables the administrator to control the amount of
audio information that is contained within each audio RTP packet.

High "Audio frames per packet" settings reduce network bandwidth usage but
increase the chances for audio problems due to network packet loss. Higher audio
frames per packet settings are recommended for modem connections. Conversely,
low "Audio frames per packet" settings increase network bandwidth usage but
decrease the chances for audio problems due to packet loss. Lower settings are
recommended for LAN/WAN connections.

For more information, see Connection Speed Settings for Audio/Video Services

You can also improve the video quality by setting higher video bit-rate settings. A
higher video bit rate can result in a smoother video playout for the end users but
might increase network bandwidth usage. For more information, see Video bit rate

Audio/Video Services configuration settings

The Sametime Administration Tool includes Audio/Video Services configuration
settings that allow the administrator to enable and disable the audio and video
functionality and control the operation of the Audio/Video Services. The
audio/video functionality is enabled by default.

Interactive Audio/Video Services settings

The Interactive Audio/Video Services settings enable the administrator to:

• Turn IP audio and video functionality on or off.
• Control switching intervals for audio and video.
• Control jitter buffer settings for the Sametime Broadcast client.

Connection Speed Settings

The Connection Speed Settings for the Audio/Video Services determine the rate at
which audio and video streams are transmitted by clients and server components
in an interactive audio/video meeting. Connection speed parameters are passed
from the MMCU component on the server to the Sametime Meeting Room client
during the call-setup phase of a connection to the Audio/Video Services.
The Sametime Broadcast Services also use the audio and video Connection Speed Settings when transmitting meeting streams for Broadcast meetings that include audio and video. For more information, see [Connection Speed Settings for Audio/Video Services](#).

**Usage Limits and Denied Entry settings**

The [Usage Limits and Denied Entry](#) settings enable the administrator to limit the number of users simultaneously using audio/video. Such limits prevent a large number of users from overwhelming the system resources of the server computer or the bandwidth capabilities of the network. When the number of users reaches the limit specified by the administrator, all other users are unable to use Sametime audio/video features in meetings. The Usage Limits and Denied Entry settings enable the administrator to ensure that server and network performance remain at optimum levels for a specified number of users. The administrator can set separate limits to restrict the number of users attending instant meetings, scheduled meetings, and broadcast meetings.

**Interactive Audio/Video Network and Ports settings**

The Interactive Audio/Video Network and Ports settings enable the administrator to:

- Specify the ports and TCP tunneling options for Audio/Video Services.

**Accessing the Audio/Video Services configuration settings**

To access the Audio/Video Services configuration settings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video. The available settings are:
   - [Interactive Audio/Video Services](#)
   - [Connection Speed Settings](#)
   - [Usage Limits and Denied Entry](#)

To access Network and Port settings for the Audio/Video Services:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Connectivity.
4. Choose Networks and Ports.

   For information about the Network and Ports settings for the Interactive Audio/Video Services, see:
   - [Interactive Audio/Video Network settings](#)
   - [Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)](#)

**Interactive Audio/Video Services settings**

The Audio/Video Services settings allow you to configure whether IP audio and video are available, the time intervals for audio and video switching, and the size of the Sametime Broadcast client jitter buffer.

The available settings are:
When people schedule a meeting

- **Allow people to choose Sametime IP Audio in meetings** - Enables or disables IP audio on the Sametime server. Disabling IP audio also disables IP video.
- **Allow people to choose Sametime IP video in meetings** - Enables or disables IP video on the Sametime server. Disabling IP audio also disables IP video. Video-only meetings are not supported.

Switching

- **Time to wait for silence before switching to next speaker (ms)** - Controls the amount of time (in milliseconds) a person that was speaking must be silent before the Audio/Video Services begin scanning for a new audio source.
- **Time to wait before switching to next video (ms)** - Controls the amount of time to wait (in milliseconds) before switching the video from the previous speaker to the person currently speaking.

Broadcast meetings

- **Time to buffer broadcast data, audio, and video (in seconds)** - Controls the amount of audio/video data held in the buffer by the Sametime Broadcast clients before the client begins playing out the data.

Allow or prevent the use of Sametime IP Audio in meetings

The "Allow people to choose Sametime IP Audio in meetings" setting determines whether an end user can select audio as a collaborative activity for instant or scheduled meetings conducted with the Sametime Meeting Room client. This setting enables and disables the audio/video functionality on the Sametime server.

This option is enabled by default. When this option is enabled:

- End users can include IP audio in scheduled Sametime meetings by selecting audio as a tool on the Tools tab of the New Meeting page in the Sametime Meeting Center.
- End users can include IP audio in instant Sametime meetings by selecting audio as a tool when starting the meeting or by adding audio to a meeting that is in progress.

If you disable this option, end users cannot include the audio collaborative activity in an instant or scheduled meeting. Video is also not available. (Video meetings without audio are not supported.) Disabling this option causes all audio and video options to disappear from the Sametime end-user interface. Audio settings in the Sametime Administration Tool are also disabled.

You might want to disable this option if heavy audio usage is taxing the bandwidth capabilities of your network or if audio is not needed in your Sametime community.

To change the "Allow people to choose IP Audio in meetings" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
5. To prevent the use of Sametime IP Audio in meetings, clear the check mark from the check box labeled "Allow people to choose Sametime IP Audio in meetings."
To allow the use of Sametime IP Audio in meetings, select the check box labeled "Allow people to choose Sametime IP Audio in meetings."

6. Click Update and restart the server for the change to take effect.

**Allow or prevent the use of Sametime IP Video in meetings**

The "Allow people to choose Sametime IP Video in meetings" setting determines whether an end user can select video as a collaborative activity for instant or scheduled meetings conducted with the Sametime Meeting Room client.

**Note:** This setting must be enabled before this setting can be used. Video-only meetings are not supported.

If this option is enabled, end users with Sametime Meeting Room clients can include the video collaborative activity in instant or scheduled meetings that also include audio. This option is enabled by default. When this option is enabled, video is automatically included in all scheduled meetings on the Sametime server. An end user can remove IP video from a scheduled meeting by using the Tools tab on the Create Meeting page in the Meeting Center. An end user can also select video as a collaborative activity when starting an instant meeting.

If you disable this option, end users cannot include the video collaborative activity in an instant or scheduled meeting. Disabling this option causes all video options to disappear from the Sametime end-user interface. Video settings in the Sametime Administration Tool are also disabled.

You might want to disable this option if video usage is taxing the bandwidth capabilities of your network or if video is not needed in your Sametime community.

To change the "Allow people to choose IP Video in meetings" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
5. To prevent the use of Sametime IP video in meetings, clear the check mark from the check box labeled "Allow people to choose Sametime IP Video in meetings."

To allow the use of Sametime IP video in meetings, select the check box labeled "Allow people to choose Sametime IP Video in meetings."

6. Click Update and restart the server for the change to take effect.

**Time to wait for silence before switching to next speaker (ms)**

The Multimedia Processor (MMP) component of the Audio/Video Services listens for incoming audio packets to determine when a person is speaking. When a person stops speaking, the MMP waits for a brief period of time before scanning for another active client (a client transmitting audio packets). This setting controls the time interval (in milliseconds) that the MMP waits before scanning for other active audio clients.

The purpose of this setting is to prevent rapid switching of the audio source during normal pauses in conversation. Rapid audio switching consumes additional CPU cycles and network resources. The valid range for this setting is 100 to 500 milliseconds (ms). The default setting is 250 ms (.25 seconds). By default, the MMP...
can tolerate .25 seconds of silence before it begins to scan for a new audio source (person speaking or system transmitting audio packets).

For more information on the MMP, see Multimedia Processor (MMP)

To change the "Time to wait for silence before switching to next speaker (ms)" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
5. In the "Time to wait for silence before switching to next speaker (ms)" field, enter the new time interval in milliseconds. For example, entering 500 changes the time interval to 500 milliseconds or .5 seconds. (The valid range for this setting is from 100 to 500 milliseconds.)
6. Click Update and restart the server for the change to take effect.

**Time to wait before switching to the next video (ms)**
The Multimedia Processor (MMP) component of the Audio/Video Services controls the process of switching from one audio source to another. In an audio/video meeting, the video follows the audio. After the MMP switches to a new audio source (person speaking or system transmitting audio packets), the MMP also switches the video to the same source. Use the "Time to wait before switching to the next video" setting to specify the minimum amount of time (in milliseconds) that must pass before the video switches from the person who just finished speaking to the new person speaking. The valid range for this setting is from 500 to 4000 milliseconds (ms). The default setting is 4000 ms (or four seconds).

This setting reduces rapid video switching, which can reduce usability and unnecessarily consume CPU and network resources. For example, assume the "Time to wait before switching to the next video" setting is four seconds. If the first presenter talks for 10 seconds, and a second presenter briefly interrupts for two seconds, then the first presenter resumes speaking, the video remains locked on the original presenter. The "Time to wait before switching to the next video" setting of four seconds prevents the video from switching unnecessarily to a person who makes only a brief comment.

For more information on the MMP, see Multimedia Processor (MMP)

To change the "Time to wait before switching to next video (ms)" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
5. In the "Time to wait before switching to next video (ms)" field, enter the new time interval in milliseconds. For example, entering 3000 changes the time interval to 3000 milliseconds, or three seconds. The valid range for this setting is from 500 to 4000 milliseconds.
6. Click Update and restart the server for the change to take effect.
**Time to buffer broadcast, audio, and video data**

Use this setting to specify the amount of streamed data that the Broadcast client will hold in its buffer before playing the data for the end user. This feature is designed to ensure a smooth playout of broadcast meeting data streams for the end user. This setting is specified in milliseconds. The default setting is 10,000 milliseconds, which is equivalent to 10 seconds.

This setting prevents network congestion from affecting the playout of broadcast media streams. The Broadcast meeting streams are transmitted at a consistent rate. However, network congestion and busy router queues can cause some packets to be delayed or some packets to arrive out of order. If packets are played immediately as they arrive, end users might experience jitter effects caused by network congestion, such as intermittent audio and video or garbled speech.

To prevent these jitter effects, the Sametime Broadcast client accumulates 10,000 milliseconds (or 10 seconds) of audio and video data in its buffer before it begins to play the data. As a result, the client can tolerate up to 10 seconds of network congestion before the end user notices any jitter effects in the playback of the media streams. If the network congestion clears in less than 10 seconds, the buffer refills, and the streams continue to play smoothly for the end user. Buffering the meeting streams causes a slight delay in the broadcast of the meeting but ensures the meeting plays smoothly for the end users.

You can adjust this setting as needed. To ensure that broadcast meetings play uninterrupted for the end users, change the "Time to buffer broadcast, audio, and video data" setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
5. In the "Time to buffer broadcast, audio, and video data (sec)" setting, enter the new time interval in milliseconds. For example, entering 20,000 indicates that 20,000 milliseconds (or 20 seconds) of data is stored in the buffer before it is played.
6. Click Update and restart the server for the change to take effect.

**Connection Speed Settings for Audio/Video Services**

The Connection Speed Settings for the Audio/Video Services allow the administrator to set the speeds (bit rates) at which streaming audio and video data is sent on the network between the Sametime Audio/Video Services and the Sametime Meeting Room clients.

**Note:** If a broadcast meeting includes audio and video, the *Broadcast Services* also use the Audio/Video Services connection speed settings to transmit the Broadcast Meeting streams to the Broadcast clients.

The Audio/Video Services (and clients) use Connection Speed Settings when transmitting Real-Time Protocol (RTP) audio and video streams. These settings control the speeds at which audio and video data is transmitted on the network. The Sametime administrator can specify one set of transmission speeds for users with modem connections and a separate (faster) set of transmission speeds for users with LAN/WAN connections.
The administrator can determine whether the settings for modem users or LAN/WAN users are used by default in all Sametime meetings. End users cannot change the default setting for instant meetings. However, end users can change the default and choose whether the modem or the LAN/WAN connection speeds are used in a scheduled meeting. At installation, the default settings of the Sametime Administration Tool cause all instant and scheduled meetings to use the LAN/WAN connection speed settings.

**Note:** In a broadcast meeting, the Broadcast Services on the Sametime server attach to the Audio/Video Services and Meeting Services to gain access to the audio, video, and screen-sharing/whiteboard or other data being transmitted among meeting presenters. The Broadcast Services transmit the audio, video, and data streams on the network to Sametime Broadcast clients. In an interactive audio/video meeting, the audio, video, and data streams are transmitted and played out by the Audio/Video Services on the server and by the Sametime Meeting Room clients.

For more information on Connection Speed Settings for Audio/Video Services, see:
- How Connection Speed Settings are used for audio and video
- Type of Connection Speed Setting to use for the default in instant and scheduled meetings
- Audio bit rate
- Video bit rate
- Screen-sharing and whiteboard bit rate (Broadcast meetings only)
- Audio/Video jitter buffer
- Audio frames per packet

**Configuring the Connection Speed Settings for audio and video**

This topic describes how the administrator sets Connection Speed Settings and how these settings are chosen by the end user when creating a scheduled meeting.

To set the Connection Speed Settings for audio and video streams, the administrator performs the following actions:

1. The administrator sets the following settings for users with modem connections. These settings apply to both interactive audio and video meetings with the exception of the screen-sharing/whiteboard bit rate. The screen-sharing/whiteboard bit rate applies only to broadcast meetings and has no effect on screen-sharing and whiteboard data transmitted in interactive meetings.
   - Audio stream bit rate
   - Video stream bit rate
   - Screen-sharing and whiteboard bit rate for broadcast meetings
   - Audio/video jitter buffer
   - Audio frames per packet

2. The administrator then specifies these settings for LAN/WAN connections:
   - Audio, video, and screen-sharing/whiteboard bit-rate settings
   - Audio/video jitter buffer
   - Audio frames per packet settings

During a Sametime meeting, all data streams are transmitted either at the connection speeds (or bit rates) that the administrator has specified for modem users or at the connection speeds that the administrator has specified for
LAN/WAN users. Only one set of Connection Speed Settings is used in a meeting. It is not possible for modem users and LAN/WAN users connected to the same meeting to send and receive data at different rates.

The administrator can use the "Type of Connection speed settings to use for the default in scheduled and instant meetings" setting to determine whether the Connection Speed Settings for modem users or LAN/WAN users are used by default in all Sametime meetings. End users cannot change this default setting for instant meetings.

**Note:** At installation, the "Type of Connection speed settings to use for the default in scheduled and instant meetings" setting is set so that instant and scheduled meetings use the LAN/WAN connection speeds. The default settings prevent modem users from participating in audio/video meetings.

End users can override the administrator-specified default and determine whether an individual scheduled meeting uses the LAN/WAN settings or the modem settings. If the administrator determines that all Sametime meetings use the LAN/WAN settings by default, the "People are attending this meeting using a modem" option on the Locations tab of the New Meeting page in the Meeting Center is not selected by default, and the meeting data streams are transmitted using the Connection Speed Settings that are specified for LAN/WAN users. If the end user selects the "People are attending this meeting using a modem" check box, the meeting data streams are transmitted using the Connection Speed Settings specified for modem users. This speed is generally slower and results in less efficient meeting performance.

**Note:** If a meeting includes both modem users and LAN/WAN users, the "People are attending this meeting using a modem" setting should always be selected for the meeting. In this case, users attending over LAN/WAN connections will receive the data at the slower rate specified for modem users. It is not possible for modem users and LAN/WAN users connected to the same meeting to send and receive data at different rates.

**Type of Connection Speed Setting to use for the default**

The administrator can use the "Type of Connection speed settings to use for the default in scheduled and instant meetings" setting to determine whether the Connection Speed Settings for modem users or for LAN/WAN users are used by default in all Sametime meetings. End users cannot change this default setting for instant meetings.

**Note:** At installation, this setting is set so that instant and scheduled meetings use the LAN/WAN connection speeds. The default setting prevents modem users from participating in interactive audio/video meetings or broadcast meetings that include audio/video.

For scheduled meetings, the end user can override the default specified by the administrator and determine whether the Connection Speed Settings for modem or LAN/WAN connections are used in a particular meeting. The end user can override the default by selecting or not selecting the "People are attending this meeting using a modem" option in the Sametime end-user interface when creating a meeting.

The "People are attending this meeting using a modem" option is not selected by default in the end-user interface when the administrator chooses "Meetings with LAN/WAN users” as the default connection speed settings for Sametime meetings.

Chapter 10. Configuring the Audio/Video Services  357
If the end user selects the "People are attending this meeting using a modem" setting, the meeting uses the Connection Speed Settings specified by the administrator for modem connections. This connection speed is generally slower and results in less efficient meeting performance.

The "People are attending this meeting using a modem" option is selected by default in the end-user interface when the administrator chooses "Meetings with modem users" as the default connection speed settings for Sametime meetings. If the end user clears the check mark from the "People are attending this meeting using a modem" option, the meeting uses the Connection Speed Settings specified by the administrator for LAN/WAN connections.

To set the "Type of Connection Speed Setting to use for the default in scheduled and instant meetings" option:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Connection Speed Settings.
5. In the "Type of Connection Speed Setting to use for the default in scheduled and instant meetings" option, make one of the following selections:
   • **Meetings with Modem users** - If you select this option, the "People are attending this meeting using a modem" option is selected by default in the end-user interface when a user schedules a meeting in the Sametime Meeting Center. Any broadcast or interactive audio/video meeting started on the Sametime server uses the Connection Speed Settings the administrator has specified for modem users unless the end user changes the default when creating the meeting. End users cannot change the default setting for instant meetings; all instant meetings use the Connection Speed Settings specified by the administrator for modem users if you select this option.
   • **Meetings with LAN/WAN users (default)** - If you select this option, the "People are attending this meeting using a modem" option is not selected by default in the end-user interface when a user schedules a meeting in the Sametime Meeting Center. Any broadcast or interactive audio/video meeting started on the Sametime server uses the Connection Speed Settings specified by the administrator for LAN/WAN users unless the end user changes the default when creating the meeting.
   • End users cannot change the default setting for instant meetings; all instant meetings use the Connection Speed Settings specified by the administrator for LAN/WAN users if you select this option.
6. Click Update and restart the server for the change to take effect.

**Audio bit rate**
The Audio bit rate settings specify the audio codec that is used for the modem and LAN/WAN connection types. The audio codec that you select determines the transmission speed (or bit rate) for the audio stream transmission in Kilobits per second (Kbps). Different audio codecs can be selected for the "Meetings with modem users" and "Meetings with LAN/WAN users" connection types.

The two available bandwidth (or audio codec) settings are:
• **6.3 Kbps - Less network intensive, lower quality** - This setting is the default for modem connections. With this option selected, the G.723 codec is used to
compress the audio data stream. The G.723 codec compresses data by removing all frequencies except those that support voice. This codec uses less network bandwidth but consumes more CPU cycles than the G.711 codec. Generally, the frequency range provided by this codec is not adequate for music.

Note: If your network environment does not support User Datagram Protocol (UDP), users will receive audio streams through TCP-tunneled connections. When users receive audio streams through TCP-tunneled connections, Lotus software recommends using the G.723 codec in audio meetings. For more information about audio/video connectivity, see Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services).

- **64Kbps - More network intensive, higher quality** - This is the default setting for LAN/WAN connections. With this option selected, the G.711 codec is used to compress the audio data stream. The G.711 codec produces a less-compressed audio stream that has better sound quality. The G.711 codec also requires less CPU cycles when decompressing the stream. The G.711 codec uses more network bandwidth and requires a 64Kbps connection. This codec will not work with a 56K modem.

For information about the bandwidth implications of these settings, see Connection Speed Settings and bandwidth usage.

To change a bandwidth (audio codec) setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Connection Speed Settings.
5. Select the "Meetings with modem users" setting.
6. Select the 6.3Kbps (G.723) or the 64Kbps (G.711) setting.
   Note: This setting should be set to 6.3Kbps for modem users unless all users who attend meetings over modem connections have modems capable of receiving data at rates faster than 64Kbps.
7. Select the "Meetings with LAN/WAN users" setting.
8. Select either the 6.3Kbps (G.723) or the 64Kbps (G.711) setting.
9. Click Update and restart the server for the change to take effect.

**Video bit rate**

The video bit rate settings specify the transmission speed (or bit rate) of the video stream in Kilobits per second (Kbps). Different video bit rates can be selected for the "Meetings with modem users" and "Meetings with LAN/WAN users" connection types.

The available video bit-rate settings are 16, 32, 64, 128, 256, 384, and 512 Kbps. For modem connections, the 16Kbps setting is recommended. For LAN/WAN connections, select the highest video bit rate that the bandwidth capabilities of your network will support.

Generally, higher bit-rate settings produce smoother video and consume more network bandwidth than lower settings. The amount of movement that occurs within the camera’s field of view also affects the amount of data that must be transmitted. If a lot of movement occurs in the camera’s field of view, a high...
bit-rate setting can result in smoother video for the end user and reduce the halting quality sometimes seen in the video images.

If you are using a 360-degree video camera, a setting of 128 Kbps or higher is recommended to ensure that video with a lot of movement plays smoothly for the end user. For more information, see [Using a 360-degree video camera with Sametime](#).

**Note:** If your network environment does not support UDP, users will receive video streams through TCP-tunneled connections. When users receive video streams through TCP-tunneled connections, Lotus software recommends using the lower video bit-rate settings of 16 or 32Kbps to ensure adequate meeting performance. For more information about audio/video connectivity, see [Meeting Room client connection process using JVM 1.4.2 (Audio/Video Services)](#).

For more information about the bandwidth implications of these settings, see [Connection Speed Settings and bandwidth usage](#).

To change the video bit-rate setting:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Connection Speed Settings.
5. Select the "Meetings with modem users" setting.
6. Select either the 16, 32, 64, 128, 256, 384, and 512Kbps setting. (16Kbps is recommended for modem users. The higher settings are used for LAN/WAN connections unless all users accessing the server have high-speed modems.)
7. Select the "Meetings with LAN/WAN users" setting.
8. Select either the 16, 32, 64, 128, 256, 384, and 512Kbps setting.
9. Click Update and restart the server for the change to take effect.

**Screen-sharing and whiteboard bit rate (Broadcast meetings only)**

The "Screen-sharing and whiteboard bit rate for broadcast only" settings specify the bit rate for the screen-sharing and whiteboard broadcast data stream transmitted on the network by the Broadcast Services for broadcast meetings with audio/video and screen-sharing/whiteboard activity. Different bit rates can be selected for the "Meetings with modem users" and "Meetings with LAN/WAN users" connection types.

The available screen-sharing and whiteboard bit rate settings are 16, 32, 64, and 128Kbps (Kilobits per second). The 16Kbps setting is recommended for modem connections. The higher settings provide better broadcast meeting performance. The higher settings consume more network bandwidth and use fewer CPU cycles to compress and decompress the data. For LAN/WAN connections, select the highest bit rate that the bandwidth capabilities of your network and the connection speeds of your clients will support.

When specifying this setting, note that the audio, video, and screen-sharing/whiteboard bit rates for broadcast meetings are cumulative. For example, if the administrator specifies an audio bit rate of 64Kbps, a video bit rate of 64Kbps, and a screen-sharing/whiteboard bit rate of 64Kbps, the meeting streams...
for that meeting use a total of 192Kbps (64Kbps + 64 Kbps + 64Kbps). To attend a meeting that uses these settings, a user must have a connection to the server that can receive data at the 192Kbps rate.

**Note:** These settings that you select from the Configuration-Audio/Video-Connection Speed Settings tab are used only for broadcast meetings with audio, video, and screen-sharing/whiteboard activity. If the broadcast meeting includes screen-sharing/whiteboard activity but not audio or video, the settings defined in the Configuration-Meetings Services-Connection Speed Settings of the Sametime Administration Tool are used to transmit the screen-sharing/whiteboard broadcast meeting stream. This arrangement allows for a more efficient use of connection bandwidth for broadcast meetings without audio/video. For information about the bandwidth implications of these settings, see Connection Speed Settings for Broadcast Services, Connection Speed Settings and bandwidth usage and Connection Speed Settings for Meeting Services.

To set the screen-sharing and whiteboard bit rates for broadcast meetings with audio/video:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
4. Choose Connection Speed Settings.
5. Select the "Meetings with modem users" setting.
6. Specify a screen-sharing and whiteboard bit rate for modem connections to broadcast meetings (16, 32, 64, and 128Kbps). 16Kbps is recommended for modem users.
7. Select the "Meetings with LAN/WAN users" setting.
8. Specify a screen-sharing and whiteboard bit rate for LAN/WAN connections to broadcast meetings (16, 32, 64, and 128Kbps).
9. Click Update and restart the server for the changes to take effect.

**Audio/Video jitter buffer**

The Audio/Video jitter buffer setting specifies the amount of audio and video data that the Sametime Meeting Room client will hold in its buffer before playing the audio and video data for the end user. This setting is specified in milliseconds (ms). The default setting is 200 ms.

**Note:** This setting affects the amount of audio and video data buffered by the Sametime Meeting Room client. If a broadcast meeting includes audio and video, this setting does not affect the amount of data buffered by the Broadcast client. To set the buffer size for the Broadcast client, see Time to buffer broadcast, audio, and video data.

This setting minimizes the effect of network congestion on the quality of the audio and video RTP streams that are played out for the end user in the Sametime Meeting Room client. Network congestion can delay the delivery of audio and video packets or cause packets to arrive out of order at the client. Delayed or out-of-order packets produce jitter effects for the end user such as intermittent audio and video or garbled speech. Briefly buffering packets before playing them provides time for missing packets that have been delayed by network congestion to arrive at the client and minimizes these jitter effects.
The Sametime Meeting Room client buffers audio and video data for 200 ms (by default) before it plays the packets for the end user. As a result, the client can tolerate up to 200 ms of network congestion before the end user notices any jitter effects in the media streams. If the network congestion clears in less than 200 ms, the buffer refills and the packets continue to play smoothly for the end user.

Higher settings are more effective at reducing jitter effects. With higher settings, more data is buffered, which allows more time for delayed packets to arrive at the client. However, higher settings also result in more delay (or latency) in the meeting. A user who is speaking will not be heard immediately by the other meeting participants. The delay in the meeting increases with the amount of time that data is held in the buffer.

Lower settings cause less delay in the meeting, but meetings with lower settings are more susceptible to jitter effects caused by network congestion. Less data is buffered, increasing the likelihood that delayed or lost packets will produce a jitter effect in the media stream.

Adjust this setting to accommodate the amount of network congestion occurring on your network. Generally, a setting of 200 ms is adequate for a clean network with little congestion. Busier, more congested networks might require settings around 250 ms while the most efficient high-end networks might require settings in the 100 to 150 ms range.

To change the "Audio/Video jitter buffer" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Connection Speed Settings.
5. Select the "Meetings with modem users" setting.
6. In the "Audio/Video jitter buffer" setting, enter the new time interval in milliseconds. The recommended setting for modem users is 200 ms.
7. Select the "Meetings with LAN/WAN users" setting.
8. In the "Audio/Video jitter buffer" setting, enter the new time interval in milliseconds. The default setting for LAN/WAN users is 200 ms. For high-end networks with little data congestion, 100 to 150 ms settings are recommended.
9. Click Update and restart the server for the change to take effect.

**Audio frames per packet**
The "Audio frames per packet" setting specifies the number of audio frames sent in every RTP packet in the audio stream. Each G.723 audio frame equals 30 milliseconds (ms) of audio data, and each G.711 frame equals 20 ms of audio data. You can specify settings of one, two, or three audio frames per packet.

This setting can minimize the effect of network packet loss on the audio quality. When packet loss occurs, end users can experience garbled speech, intermittent audio, or unexpected silence. This setting also affects network bandwidth usage.

Increasing the "Audio frame per packet" settings:
• **Reduces network bandwidth usage** - With higher settings, each packet contains more audio data. Fewer packets are sent on the network to transmit the audio data, which results in less packet header overhead.
• **Increases the possibility of poor audio quality due to packet loss** - If your network is susceptible to packet loss, audio quality can degrade more easily with higher "Audio frame per packet" settings. Since each packet contains more audio data, each lost packet creates a bigger gap in the audio stream, resulting in more disruption in the audio for the end user.

• **Increases latency** - Higher settings might increase the audio delay in the meeting.

Decreasing the "Audio frame per packet" settings:

• **Increases network bandwidth usage** - With lower settings, less audio data is contained within each packet. More packets must be sent on the network to transmit the audio information.

• **Decreases the possibility of poor audio quality due to packet loss** - With lower settings, each packet contains less audio data. A lost packet creates a smaller gap in the audio stream and less disruption for the end user.

**Note:** When network packet loss is affecting the audio quality, the administrator should lower the "Audio frames per packet" setting and increase the "Audio/Video jitter buffer" setting to minimize the impact of lost packets on the audio quality. These adjustments increase the amount of delay (or latency) in the meeting but improve the audio quality.

Generally, users with LAN/WAN connections can use lower "Audio frames per packet" settings. Although these settings increase network bandwidth consumption, lower settings result in higher audio quality. LAN/WAN connections are usually capable of handling the increased bandwidth required by the lower settings. If necessary, the administrator can increase the "Audio frames per packet" setting to conserve network bandwidth consumption for users with LAN/WAN connections.

Users with modem connections might require higher "Audio frames per packet" settings to ensure the audio data can be transmitted over modem connections with limited bandwidth-handling capabilities.

**Note:** If audio data bandwidth consumption routinely strains the network, the administrator should set Usage Limits and Denied Entry settings for the server.

To change the "Audio frames per packet" setting:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Connection Speed Settings.
5. Select the "Meetings with modem users" setting.
6. In the "Audio frames per packet" setting, enter the new number of audio frames per packet. The recommended setting for modem users is three frames per packet.
7. Select the "Meetings with LAN/WAN users" setting.
8. In the "Audio frames per packet" setting, enter the new number of audio frames per packet. The recommended setting for LAN/WAN users is one frame per packet.
9. Click Update and restart the server for the change to take effect.
Connection Speed Settings and bandwidth usage

The Connection Speed Settings affect the network bandwidth usage of the Sametime server. However, the primary purpose of these settings is not to control bandwidth usage, but to ensure a high quality of service. The primary functions of the Connection Speed Settings are to:

- Ensure that meeting data can be transmitted at higher speeds when only LAN/WAN users (no modem users) are connected to the meeting. The faster transmission speeds generally result in better meeting performance for the end user.
- Ensure that transmission speeds can be adjusted to accommodate users with modem connections.

While the primary purposes of these settings do not involve bandwidth control, adjustments to these settings can have beneficial effects on bandwidth usage in some situations.

**Note:** The primary administrative features for controlling server bandwidth usage are the Usage Limits and Denied Entry settings. For more information, see [Usage Limits and Denied Entry](#).

Administrators should consider the following when selecting the Connection Speed Settings:

- If a meeting is attended only by LAN/WAN users, higher bit-rate settings generally produce better meeting results. High bit-rate settings require less data compression when transmitting on the network. Audio and video quality improve as data compression diminishes. Uncompressed data is less taxing for the CPUs of the server and its clients because fewer CPU cycles are required to compress and decompress the data when transmitting and receiving. The higher bit-rate settings increase the network bandwidth consumption of the Sametime server and its users.
- In some cases, large numbers of users connected to a meeting with high bit-rate connections might tax the bandwidth capabilities of your network. For these meetings, it can be beneficial to use the modem settings even though all users are connected through LAN/WAN connections. Using the modem connection settings reduces network bandwidth usage but can degrade the audio and video quality and require more CPU cycles for compression and decompression of the data streams.
- If the User Datagram Protocol (UDP) is unavailable on your network, the audio and video data streams are tunneled to clients through the TCP transport. If users must make TCP-tunneled connections to the Sametime server to receive the audio/video streams, lower audio and video bit-rate settings produce the best meeting performance for end users. Use an audio bit-rate setting of 6.3 Kbps (G.723 Codec) and a video bit-rate setting of 16Kbps if your network environment requires users to establish TCP-tunneled connections for audio/video.
- If quality of meeting performance is your priority, control the bandwidth usage by setting limits on the number of audio and video users that can be connected to the Audio/Video Services. The Usage Limits and Denied Entry settings in the Configuration - Audio/Video settings of the Sametime Administration Tool limit the number of people who can attend meetings that use audio and video. Limiting the number of users can prevent some users from attending meetings but ensures a high quality of service for the users that are in the meetings. This method is recommended for controlling the bandwidth usage of the Sametime server. For more information, see [Usage Limits and Denied Entry](#).


- The bit rates of all streams are cumulative. For example, consider a broadcast meeting that involves the transmission of a whiteboard stream, an audio stream, and a video stream. If the G.723 audio codec transmits at approximately 17Kbps, the video transmits at 16Kbps, and the whiteboard stream transmits at 16Kbps, each client must have a connection speed faster than 49Kbps (17Kbps + 16Kbps + 16Kbps) to receive the audio, video, and whiteboard data streams. For more information, see [Connection Speed Settings for Broadcast Services](#).

**Note:** The G.723 audio codec transmits at 6.3Kbps. However, transmission overhead can cause the G.723 codec to use up to 17.1Kbps during a transmission.

### Usage Limits and Denied Entry

The Audio/Video Usage Limits and Denied Entry settings restrict the number of users who can connect to the Audio/Video Services and the Broadcast Services. Essentially, these settings limit the number of users who can simultaneously participate in interactive audio/video meetings or broadcast meetings on the server. If you set limits, some people might be able to attend a meeting while others are rejected when the limit is reached.

The administrator should set limits to prevent a large number of users from affecting the performance of the Sametime server or taxing the bandwidth capabilities of the network. To support a large community of Sametime users, it is usually necessary to install multiple Sametime servers. For more information, see [Advantages of using multiple Sametime servers](#).

**Note:** The recommended tool for monitoring the bandwidth usage of the Sametime server is the Windows Performance Monitor. To access this tool from the Windows desktop, select Start - Programs - Administrative Tools - Performance. For more information, see the online help for the Performance Monitor. If your Sametime server runs on an IBM i5/OS or IBM pSeries server, you cannot use the Windows Performance Monitor to monitor the bandwidth usage of the Sametime server.

You set separate limits for instant and scheduled meetings. The available settings are:

#### Usage Limits and Denied Entry for Instant Meetings
- **Set a maximum number of interactive audio connections for all instant meetings on this server**
- **Set a maximum number of interactive video connections for all instant meetings on this server**

#### Usage Limits and Denied Entry for Scheduled Meetings
- **Set a maximum number of interactive audio connections for all scheduled meetings on this server**
- **Set a maximum number of interactive video connections for all scheduled meetings on this server**

#### Usage Limits and Denied Entry for Broadcast Meetings
- **Set a maximum number of data connections for all broadcast meetings**
- **Set a maximum number of audio connections for all broadcast meetings**
- **Set a maximum number of video connections for all broadcast meetings**
Setting a maximum number of interactive audio connections for all instant meetings

The administrator can set a limit for the maximum number of interactive audio connections in all instant meetings. This limit assumes that one connection equals one IP audio client (or one user).

The administrator can set limits to prevent a large number of users from affecting the performance of the Sametime server or taxing the bandwidth capabilities of the network. To support a large community of Sametime users, it is usually necessary to install multiple Sametime servers. For more information, see Advantages of using multiple Sametime servers.

Notes:

- You can also set a maximum number of interactive video connections for all instant meetings. Generally, the maximum number of interactive video connections for all instant meetings should not exceed the maximum number of audio connections.
- If a user starts an instant meeting that includes both audio and video, and either the audio or video limit is reached, users who join the meeting after either of the limits is reached will not be able to use either audio or video in the meeting. If the video limit is set lower than the audio limit, the administrator should recommend that users select the audio-only option when starting large instant meetings.

To set a maximum number of interactive audio connections for all instant meetings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled "Set a maximum number of interactive audio connections for all instant meetings on this server."
6. Enter the maximum number of interactive audio connections. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

Setting a maximum number of interactive video connections for all instant meetings

The administrator can set a limit for the maximum number of interactive video connections in all instant meetings. This limit assumes that one connection equals one IP video client (or one user). When you set a limit on the maximum number of video connections, some users might not be able to receive or transmit video when the limit is reached.

The administrator can set limits to prevent a large number of users from affecting the performance of the Sametime server or taxing the bandwidth capabilities of the network.

Notes:
• **Ensure that the maximum number of video connections does not exceed the maximum number of audio connections for instant meetings**. An audio connection is required for the video to function.

• If a user starts an instant meeting that includes both audio and video, and either the audio or video limit is reached, users who join the meeting after either of the limits is reached will not be able to use either audio or video in the meeting. If the video limit is set lower than the audio limit, the administrator should recommend that users select the audio-only option when starting large instant meetings.

To set a maximum number of interactive video connections for all instant meetings:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled "Set a maximum number of interactive video connections for all instant meetings on this server."
6. Enter the maximum number of interactive video connections. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

**Setting a maximum number of interactive audio connections for all scheduled meetings**
The administrator can set a limit for the maximum number of interactive audio connections in all scheduled meetings. When you set a limit on the maximum number of audio connections, it is possible that some users might not be able to attend an instant meeting when the limit is reached. Limits are useful because they can prevent a large number of users from affecting Sametime server performance or taxing network bandwidth capabilities.

This limit assumes that one connection equals one IP audio client (or one user). An IP audio client may be:
• A Sametime Meeting Room client
• The Broadcast Gateway component of the Sametime Broadcast Services.

**Broadcast Services and Audio Limits:** As noted above, the Broadcast Gateway component of the Sametime Broadcast Services can be an audio client. If a broadcast meeting includes audio, the Broadcast Services must connect to the Sametime Audio/Video Services to access the audio stream associated with the meeting. The Broadcast Services then transmit the audio stream to all Sametime Broadcast clients attending the broadcast meeting. This connection between the Broadcast Services and the Audio/Video Services counts as one audio connection.

When specifying the maximum number of interactive audio connections for all scheduled meetings, remember to account for broadcast meetings. For example, if there are 15 active broadcast meetings that include audio, there are 15 connections from the Sametime Broadcast Services to the Sametime Audio/Video Services to support these meetings. If you allow a maximum of 100 interactive audio connections for all scheduled meetings, and there are 15 active broadcast meetings, only 85 connections are available for individual Sametime Meeting Room clients.

**Notes:**
• You can also set [maximum number of interactive video connections for all scheduled meetings]. Ensure that the maximum number of video connections does not exceed the maximum number of audio connections. An audio connection is required for the video to function.

• If a user schedules a meeting that includes both audio and video, and either the audio or video limit is reached, users who join the meeting after either of the limits is reached will not be able to use either audio or video in the meeting. If the video limit is set lower than the audio limit, the administrator should recommend that users select the audio-only option when scheduling large meetings.

**Setting a Maximum Number of Audio Connections:** To set a maximum number of interactive audio connections for all scheduled meetings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled “Set a maximum number of interactive audio connections for all scheduled meetings on this server.”
6. Enter the maximum number of interactive audio connections. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

**Setting a maximum number of interactive video connections for all scheduled meetings**

The administrator can set a limit for the maximum number of interactive video connections in all scheduled meetings. When you set a limit on the maximum number of video connections, it is possible that some users might not be able to attend an instant meeting when the limit is reached. Limits are useful because they can prevent a large number of users from affecting Sametime server performance or taxing network bandwidth capabilities.

This limit assumes that one connection equals one IP video client (or one user). An IP video client may be:

- A Sametime Meeting Room client
- The Broadcast Gateway component of the Sametime Broadcast Services.

**Broadcast Services and Video Limits:** As noted above, the Broadcast Gateway component of the Sametime Broadcast Services can be a video client. If a broadcast meeting includes video, the Broadcast Services must connect to the Sametime Audio/Video Services to access the video stream associated with the meeting. The Broadcast Services then transmit the video stream to all Sametime Broadcast clients attending the broadcast meeting. This connection between the Broadcast Services and the Audio/Video Services counts as one video connection.

When specifying the maximum number of interactive video connections for all scheduled meetings, remember to account for broadcast meetings. For example, if there are 15 active broadcast meetings that include video, there are 15 connections from the Sametime Broadcast Services to the Sametime Audio/Video Services to support these meetings. If you allow a maximum of 100 interactive video connections for all scheduled meetings, and there are 15 active broadcast meetings, only 85 connections are available for individual Meeting Room clients.
Notes:

- Ensure that the maximum number of video connections does not exceed the maximum number of audio connections. An audio connection is required for the video to function.
- If a user schedules a meeting that includes both audio and video, and either the audio or video limit is reached, users who join the meeting after either of the limits is reached will not be able to use either audio or video in the meeting. If the video limit is set lower than the audio limit, the administrator should recommend that users select the audio-only option when scheduling large meetings.

Setting a Maximum Number of Video Connections: To set a maximum number of interactive video connections for all scheduled meetings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled "Set a maximum number of interactive video connections for all scheduled meetings on this server."
6. Enter the maximum number of interactive video connections. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

Setting a maximum number of data connections for all broadcast meetings

The administrator can set a limit for the number of data connections to all broadcast meetings on the server. This limit assumes that one connection equals one Broadcast client (or one user). A Broadcast client makes a "data" connection to the Broadcast Services to receive the Real Time Protocol (RTP) streams containing the whiteboard and screen-sharing meeting data. When you set a limit on the maximum number of broadcast connections, some users might not be able to attend a meeting after the limit is reached.

The administrator sets limits to prevent a large number of users from affecting the performance of the Sametime server or taxing the bandwidth capabilities of the network.

You can also set a maximum number of audio and video connections for broadcast meetings. The limits for broadcast meetings can be adjusted to accommodate the types of broadcast meetings conducted in your organization. For example, if audio and data connections are important for broadcast meetings but video is not needed, you can set the video connection limit to zero and set limits of 100 users for the data and audio connections.

Note: If a broadcast meeting includes audio or video, users are rejected from the meeting once the lowest limit is reached. If a broadcast meeting includes audio, video, and screen-sharing/whiteboard (data) activities, the users receiving the data portion of the meeting are rejected when the audio/video limits for broadcast meetings are reached. For example, assume a meeting includes audio, video, and screen-sharing activities, and the "Usage Limits for Denied Entry for Broadcast Meetings" setting specifies limits of 10 users for video, 10 users for audio, and 20 users for data. The 11th user that
attempts to enter this meeting is rejected; the user will not receive the data portions of the meeting even though that setting is set to allow 20 users. However, if the person who creates the broadcast meeting does not include the audio and video activities as part of the meeting and the same limits are in effect, 20 users can join the meeting and the 21st user will be rejected.

To set a maximum number of data connections for all broadcast meetings:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled "Set a maximum number of data connections for all broadcast meetings."
6. Enter the maximum number of data connections. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

**Setting a maximum number of audio connections for all broadcast meetings**
The administrator can set a limit for the maximum number of audio connections to all broadcast meetings active on the server. This limit assumes that one connection equals one Broadcast client (or one user). When you set a limit on the maximum number of broadcast connections, some users might not be able to attend a meeting after the limit is reached.

The administrator sets limits to prevent a large number of users from affecting the performance of the Sametime server or taxing the bandwidth capabilities of the network. If your network is not multicast-enabled, a large number of Broadcast clients connected to a broadcast meeting with audio can consume considerable network bandwidth.

You can also set a maximum number of data and video connections for broadcast meetings. The limits for broadcast meetings can be adjusted to accommodate the types of broadcast meetings conducted in your organization. For example, if audio and data connections are important for broadcast meetings but video is not needed, you can set the video connection limit to zero and set limits of 100 users for the data and audio connections.

**Note:** If a broadcast meeting includes audio or video, users are rejected from the meeting once the lowest limit is reached. If a broadcast meeting includes audio, video, and screen-sharing/whiteboard (data) activities, the users receiving the data portion of the meeting are rejected when the audio/video limits for broadcast meetings are reached. For example, assume a meeting includes audio, video, and screen-sharing activities and the "Usage Limits for Denied Entry for Broadcast Meetings" setting specifies limits of 10 users for video, 10 users for audio, and 20 users for data. The 11th user that attempts to enter this meeting is rejected; the user will not receive the data portions of the meeting even though that setting is set to allow 20 users. However, if the person who creates the broadcast meeting does not include the audio and video activities as part of the meeting, and the same limits are in effect, 20 users can join the meeting and the 21st user will be rejected.
To set a maximum number of audio connections for all broadcast meetings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled "Set a maximum number of audio connections for all broadcast meetings."
6. Enter the maximum number of audio connections for broadcast meetings. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

**Setting a maximum number of video connections for all broadcast meetings**

The administrator can set a limit for the maximum number of video connections to all broadcast meetings active on the server. This limit assumes that one connection equals one Broadcast client (or one user). When you set a limit on the maximum number of broadcast connections, some users might not be able to attend a meeting after the limit is reached.

The administrator sets limits to prevent a large number of users from affecting the performance of the Sametime server or taxing the bandwidth capabilities of the network. If your network is not multicast-enabled, a large number of Broadcast clients connected to a broadcast meeting with audio can consume considerable network bandwidth.

You can also set a maximum number of data and audio connections for broadcast meetings. Generally, the maximum number of video connections should be equal to or less than the number specified for the maximum number of audio connections for all broadcast meetings. You can also use a setting of zero for the maximum number of video connections for all broadcast meetings settings to prevent users from receiving video streams for broadcast meetings. Preventing the transmission of video streams for broadcast meetings can conserve network bandwidth usage.

**Note:** If a broadcast meeting includes audio or video, users are rejected from the meeting once the lowest limit is reached. If a broadcast meeting includes audio, video, and screen-sharing/whiteboard (data) activities, the users receiving the data portion of the meeting are rejected when the audio/video limits for broadcast meetings are reached. For example, assume a meeting includes audio, video, and screen-sharing activities and the "Usage Limits for Denied Entry for Broadcast Meetings" setting specifies limits of 10 users for video, 10 users for audio, and 20 users for data. The 11th user that attempts to enter this meeting is rejected; the user will not receive the data portions of the meeting even though that setting is set to allow 20 users. However, if the person who creates the broadcast meeting does not include the audio and video activities as part of the meeting, and the same limits are in effect, 20 users can join the meeting and the 21st user will be rejected.

To set a maximum number of video connections for all broadcast meetings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Audio/Video.
4. Choose Usage Limits and Denied Entry.
5. Select the check box labeled “Set a maximum number of video connections for all broadcast meetings.”
6. Enter the maximum number of video connections for broadcast meetings. The default is 100 connections. You might need to experiment with this setting to determine the limits of your server and network.
7. Click Update and restart the server for this setting to take effect.

---

**Prioritizing audio/video UDP data (TOS values)**

Large organizations with multiple Sametime servers connected through WAN (Wide-Area Network) connections might require a way to prioritize the Sametime audio and video User Datagram Protocol (UDP) data streams transmitted on the network. If the audio and video data are not prioritized in some manner, users participating in audio and video meetings on congested networks or through WAN connections might experience audio and video interruptions during the meeting.

**Note:** For more information about the issues associated with transmitting UDP streams on congested networks, see [Broadcast Services performance issues](http://www.iwet.org).

Sametime provides the ability to use the IP TOS (Type-of-Service) facility to prioritize UDP packets transmitted by the server on the network. The TOS parameter exists in all IP packets and helps the underlying network route the packet through the network based on an application’s need.

If you set TOS values for the UDP IP audio and video packets, it might be necessary for your network administrator to make adjustments to the network routers and infrastructure to take full advantage of the TOS facility. To fully understand the advantages of the TOS facility, the administrator should review RFC 1349 available at the [http://www.iwet.org](http://www.iwet.org) Web site.

The administrator can make certain configuration changes to the Windows registry to enable Windows to support TOS. For more information about using TOS with Windows 2000, see the following Web page:

http://support.microsoft.com/support/kb/articles/Q248/6/11.ASP.

To set the TOS values for the UDP IP audio and video packets, the administrator must modify the registry settings on the Windows NT server as follows:

1. Go to the registry setting

   "HKEY_LOCAL_MACHINE/SOFTWARE/Lotus/Sametime/BroadcastGateway/DBNL/TOSValues"

2. Select one of the values below for the TOS value. The default setting is 0.

   - 0 - Normal Service
   - 2 - Minimize Monetary Cost
   - 4 - Maximize Reliability
   - 8 - Maximize Throughput
   - 16 - Minimize Delay

**Note:** For more information on the settings above, see RFC 1349 available on the [www.iwet.org](http://www.iwet.org) Web site.
Using a 360-degree video camera with Sametime

A meeting participant can connect a BeHere TotalView High Res 360-degree video camera to a computer system and transmit a 360-degree video stream to other users in a Sametime meeting. This functionality is useful when several meeting participants are gathered in a single conference room while other meeting participants attend the meeting from remote locations.

To use this functionality effectively, a user can place the TotalView High Res 360-degree camera at the center of a conference table. The user should also place an omnidirectional microphone connected to the same system as the 360-degree camera in a central location in the conference room. The microphone should be placed so that it can easily pick up the voices of all meeting participants in the conference room. This system is then used to attend a Sametime meeting.

When any person in the conference room speaks, the audio stream and 360-degree video stream are transmitted to the Sametime server. The Sametime server transmits the audio stream and 360-degree video stream to all other Sametime Broadcast clients or Sametime Meeting Room clients connected to the meeting. When a Broadcast client or Meeting Room client detects a 360-degree video stream, the end user has two options for viewing this video stream. The end user can:

- **Leave the video window docked to the Meeting Room or Broadcast client.** In this case, the end user can scroll the video window by clicking on it with a mouse. The end user can click and hold the mouse button down on the left or right sides of the video window to scroll the window left or right.

- **Float the video window (undock it from the Meeting Room or Broadcast client).** In this case, the video window increases its horizontal size and displays the entire 360-degree video stream.

When viewing a 360-degree video stream, each Broadcast client or Meeting Room client user can scroll the video window independently. For example, if one user scrolls the video window to the right, the other users do not see their video windows scroll to the right.

The administrator should be aware of the following issues when using a 360-degree video camera with Sametime:

- The Configuration-Audio/Video-Connection Speed Settings-Video bit-rate setting in the Sametime Administration Tool should have a minimum setting of 128 Kbps to transmit a 360-degree video stream that includes a lot of movement within the camera’s field of view.

  Higher video bit-rate settings increase the network bandwidth required to transmit the video stream. Also, all users connecting to a meeting must have connection speeds greater than 128Kbps to view the 360-degree meeting stream in the Broadcast client or Meeting Room client. Only LAN connections or the most advanced modems support these connection speeds. For more information about these settings, see [Connection Speed Settings for Broadcast Services](#).

- If any user with a conventional camera connects to the meeting and speaks, the video window reverts to its normal functioning while the user with the conventional camera is speaking. (The video window cannot be scrolled with a mouse and does not display a 360-degree image when undocked.) The video window returns to the 360-degree behavior when the Audio/Video Services detect that the system with the TotalView High Res 360-degree camera is transmitting audio packets.
Tips for using audio/video

End users should be aware of the following to ensure good sound and video quality when using audio/video features in an audio/video meeting:

- Use a good quality microphone. When the microphone connection wire is moved, you should not hear static or hissing, and the sound should not cut out. Excess noise such as static or hissing generates audio packets which can inadvertently cause the Multimedia Processor (MMP) to lock onto a client even though the user is not speaking. If the unwanted noise is continuous, the MMP does not switch from that client. All meeting participants hear only noise from that user’s microphone and no one else can speak.
- Do not lay the microphone on the table. (Laying the microphone down amplifies noise.) The microphone might pick up unwanted noise which causes the MMP to remain locked on a client when no one is speaking.
- Do not place the microphone near your speakers. Output from the speakers might feed back into the microphone, creating an echo or a feedback loop. A feedback loop can result in a high-pitched squeal.
- If possible, use a headset that contains a boom microphone. If you are using a boom microphone, do not touch the microphone with your face or hands. Also, breathing loudly can generate noise and cause the MMP to lock onto the client.
- If you are using a desktop microphone, use a unidirectional dynamic microphone with batteries.
- Avoid microphones with on and off switches unless they are of high quality. Poor-quality switches are frequently the source of static or hissing.
- Be aware that large video windows consume more network bandwidth than smaller ones.
- Ensure that end users test their audio and video equipment by using the link that is available in the Sametime Online Meeting Center. Testing audio and video equipment optimizes an end user’s system for the best audio/video quality when attending Sametime meetings.
- For information about using a 360-degree video camera with Sametime, see Using a 360-degree video camera with Sametime.

374 Sametime Administrator’s Guide
Chapter 11. Monitoring the Sametime Server

The IBM Lotus Sametime server includes charts that allow you to monitor current Sametime server statistics. The monitoring charts, which are presented as tables, provide up-to-the-second information about Community Services, Meeting Services, Broadcast Services, Audio/Video Services, Web statistics, and free disk space on the server.

Accessing the Monitoring charts

To access the monitoring charts:
1. Open the Sametime Administration Tool.
2. Select Monitoring.
3. Select the appropriate chart for monitoring:
   - General Server Status
   - Logins
   - Meetings and Participants
   - Tools in Meetings
   - Miscellaneous

General Server Status

The tables in the General Server Status monitoring chart allow you to see the status of the Sametime server at a glance. Use this chart to keep track of the types of meetings on the server, the types of connections to the server, and the Community Services logins to the server at a particular moment.

Total Active Meetings

The Total Active Meetings chart displays:
- The total number of active meetings
- The number of active meetings that were scheduled in the Sametime Meeting Center (rather than started as instant meetings)
- The number of scheduled meetings that are broadcast meetings
- The number of instant meetings
- The number of active meetings that do not have any participants in attendance

Use this chart to determine the types of meetings that occur on the server. You might want to monitor this chart before setting usage limits and denied entries in the Configuration - Audio/Video Services settings of the Sametime Administration Tool. For example, if you notice that a consistently high number of people attend instant meetings, but a lower number of people attend scheduled meetings, you might set the audio/video limits for instant meetings at a higher number than the limits for scheduled meetings.

Tip: If you notice several active meetings that do not have any participants, you might want to delete those meetings to create more room on the server.

You can also use this chart to determine how many broadcast meetings are being scheduled. A consistently high number of broadcast meetings indicates a potential
performance problem and might indicate the need for an additional Sametime server. See [Advantages of using multiple Sametime servers](#) for more information.

**Total Meeting Room Connections**

The Total Meeting Room Connections chart displays the number of connections from the Sametime Meeting Room client to the Sametime server for each of three connection types:

- **Direct Connections** - The number of direct TCP/IP connections to the Sametime server. The Meeting Room client attempts a direct connection when first connecting to the Sametime server. A direct connection results in the most efficient meeting performance.

  **Note:** Clients that connect through a SOCKS proxy are also recorded as Direct connections.

- **HTTP Tunneled Connections** - The number of tunneled HTTP connections from the Meeting Room client to the Sametime server. The Meeting Room client attempts a tunneled HTTP connection when a direct connection fails.

  **Note:** The number of connections does not always equal the number of users. For example, the same user could log in to multiple meetings.

See [About Sametime Connectivity](#) for more information about the connection processes for the Meeting Room.

**Total Community Logins**

Community Services clients include the Sametime Connect and the Participant List component of the Sametime Meeting Room. A user can be logged in to the Community Services from more than one client.

The Total Community Logins chart displays current information about:

- **Total Community Logins** - The total number of logins to Community Services on the Sametime server that you are monitoring. The Total Community Logins chart includes multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user.

- **Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, the Total Unique Logins chart records only one login for that user. A user logged in from multiple clients is considered a single “unique” login. Use this chart to determine the current number of Community Services users.

- **Total 2-way Chats** - The total number of 2-person chats taking place on the Sametime server. This chart only includes chats that were started from the Sametime server you are monitoring. For example, if you are monitoring Sametime server A and a user who has specified Sametime server A as her home server starts a chat with another user, that chat will be counted in the “Total 2-way Chats” chart. You will not see chats that were started by users who have specified a server other than Sametime server A as their home server.

- **Total n-way Chats** - The total number of multi-person chats taking place on the Sametime server. This chart only includes chats that were started from the Sametime server you are monitoring. For example, if you are monitoring Sametime server A and a user who has specified Sametime server A as her home server starts a chat with two other users, that chat will be counted in the “Total
n-way Chats” chart. You will not see chats that were started by users who have
specified a server other than Sametime server A as their home server.
• **Total Number of Active Places** - The "Total Number of Active Places” chart lists
the combined number of n-way Chats and active meetings. Both n-way Chats
and online meetings are counted as “Active Places;” 2-way Chats are not counted
in this chart.

**Note:** Use the Total Community Logins portion of the General Server Status
Monitoring chart to determine current login information. For detailed
information about logins over a longer period of time (such as several
minutes) choose Monitoring - Total Logins.

### Total Broadcast Connections

The Total Broadcast Connections chart displays the number of connections to the
Broadcast Gateway on the Sametime server using a Broadcast client. The chart
includes users who are receiving unicast broadcast streams via the User Datagram
Protocol (UDP) transport, but it does not include users who are receiving broadcast
data via multicast.

The chart displays the number of broadcast connections for each of two connection
types:

- **Direct Connections** - The number of direct TCP/IP connections to the Sametime
  server. The Broadcast client attempts a direct connection when first connecting to
  the Sametime server.

  **Note:** Clients that connect through a SOCKS proxy are also recorded as Direct
  connections.

- **HTTP Tunneled Connections** - The number of tunneled HTTP connections to
  the Sametime server. The Broadcast client attempts a tunneled HTTP connection
  when a direct connection fails.

  **Note:** The number of connections does not always equal the number of users. For
  example, the same user could log in to multiple meetings.

See the [Broadcast client connection process using JVM 1.4.2](#) topic for more
information.

### Total Broadcast Streams

The Total Broadcast Streams chart displays the aggregate number of unicast UDP
streams, the number of multicast UDP streams, and TCP-tunneled UDP streams
that are being transmitted on the network from the Sametime server. Use this chart
to determine network bandwidth usage of the Broadcast Services. A high number
of streams indicates significant network bandwidth usage by the Sametime server.
If a consistently high number of unicast connections taxes the bandwidth
capabilities of your network, you might want to limit the number of connections to
the Broadcast Services. For more information, see [Usage Limits and Denied Entries](#)

The General Server Status chart updates at the time interval specified in the
Polling Interval field (in seconds). Enter a new interval to change the rate at which
the chart updates. To update the chart immediately, click Refresh.

To access the General Server Status chart, open the Sametime Administration Tool
and select Monitoring - General Server Status.
Logins

Sametime Community Services clients include the Sametime Connect client and the Participant List component of the Sametime Meeting Room. A user can be logged in to the Community Services from more than one client.

The Logins chart displays:

- **Community Server Total Logins** - The total number of logins to Community Services, including multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user. Internal components of the Community Services also log in to the Community Services. These are intraserver connections between Community Services components that occur as part of the normal operations of the Community Services. These logins are also counted in the total logins chart.

- **Community Server Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, this chart records only one login for that user. A user logged in from multiple clients is considered a single "unique" login. Use this chart to determine the current number of Community Services users.

**Note:** Use the Logins chart to determine detailed information about logins over a longer period of time (such as several minutes). For up-to-the-second login information, choose Monitoring - General Server Status and view the Total Community Logins chart.

The Logins chart updates at the time interval specified in the Polling Interval field (in seconds). Enter a new interval to change the rate at which the chart updates. To update the chart immediately, click Refresh.

To access the Logins chart, open the Sametime Administration Tool and select Monitoring - Logins.

Meetings and Participants

The "Meetings and Participants" chart displays the names of active meetings and the number of participants in each meeting. The total number of active meetings and the total number of participants appear above the "Meetings and Participants" chart.

**Note:** All participants in Sametime meetings are counted in this chart, including users in broadcast meetings that use unicast. Broadcast users who are receiving multicast streams are not counted in this chart.

Use this chart to identify potential performance problems for the Sametime server. The following situations indicate a potential performance problem and might indicate the need for an additional Sametime server:

- Many active meetings with high numbers of attendees
- A consistently high number of active meetings
- A consistently high number of participants
To sort the meetings by the number of participants, click the Sort By Participants button. The meeting with the highest number of participants appears at the bottom of the chart. Click the Sort By Meeting button to sort the meeting names alphabetically.

The “Meetings and Participants” chart updates at the time interval specified in the Polling Interval field (in seconds). Enter a new interval to change the rate at which the chart updates. To update the chart immediately, click Refresh.

To access the "Meetings and Participants" chart, open the Sametime Administration Tool and select Monitoring - “Meetings and Participants.”

### Tools in Meetings

The "Tools in Meetings" chart displays the number of instant and scheduled meetings that use each tool and the number of people in meetings that use each tool. The chart might count some meetings more than once; for example, if an instant meeting includes both interactive audio and interactive video, the meeting is counted twice in the chart. Total numbers for instant meetings, scheduled meetings, and participants in each type of meeting are listed above the table.

The chart displays meetings and participants for the following tools:

- Whiteboard
- Screen sharing
- Polling
- Send Web Page
- Meeting Room chat (the public chat tool that is a component of the Meeting Room client)
- Interactive audio
- Interactive video

Monitor this chart to determine:

- **The tools that are currently being used in meetings** - This information is useful for tracking performance problems or determining the reasons for excess bandwidth usage. For example, too many simultaneously active video meetings can cause a high level of overall bandwidth usage. You can alleviate bandwidth bottlenecks at a single Sametime server by installing multiple Sametime servers and connecting the servers. For more information, see [Advantages of using multiple Sametime servers](#).

- **The tools that are seldom or never used** - If a tool is not being used in meetings on the server, you might want to remove it from the server. See [General Settings for Meeting Services](#) for more information.

- **The proximity of server usage to server limits** - If you have entered limits on the number of audio connections in instant or scheduled meetings or on the number of video connections in instant or scheduled meetings, use this chart to determine if the number of people using audio or video is approaching the server limit.

- **The number of people who are currently in meetings that use each tool** - This information can be useful in identifying potential performance problems. For example, a consistently high number of people in meetings with interactive audio and video indicates a potential performance problem and might indicate the need for an additional Sametime server. For more information, see [Advantages of using multiple Sametime servers](#).
The “Tools in Meetings” chart updates at the time interval specified in the Polling Interval field (in seconds). Enter a new interval to change the rate at which the chart updates. To update the chart immediately, click Refresh.

To access the “Tools in Meetings” chart, open the Sametime Administration Tool and select Monitoring - “Tools in Meetings.”

**Miscellaneous**

The Miscellaneous charts are part of the Lotus Domino Web Administration pages. To access the Domino Web Administration pages, choose Monitoring - Miscellaneous in the Sametime Administration Tool, and then click the link that appears on the right. The Domino Web Administration pages launch in a new browser window. The three charts that are useful for Sametime administrators are Memory, Disk Space, and Web Statistics.

**Memory**

To access the Memory chart, click Analysis in the Domino Web Administration Tool, and then click Memory. A pie chart that depicts free memory on the server appears. Use this information to troubleshoot memory problems. In addition to the pie chart, the memory status is displayed as Painful, Normal, or Plentiful. If the value is Painful, consider adding more memory.

**Disk Space**

To access the Disk Space chart, click Analysis in the Domino Web Administration Tool, and then click Diskspace. A pie chart of each hard disk on the server appears. Use this information to free disk space before users receive out-of-disk-space errors when trying to create Discussion databases or save data (such as whiteboard files) to the server.

You can also use the information in the Disk Space chart to check the free disk space when setting logging parameters for the Sametime log. Small logging intervals in the logging parameters can rapidly increase the size of the Sametime log database.

**Web Statistics**

To access the Web Statistics chart, click Analysis in the Domino Web Administration Tool and then click Web Statistics. This monitor tracks HTTP requests and commands. An option at the bottom of this monitor allows you to select either Domino HTTP Requests or Domino HTTP Commands. Each of these charts is explained below. These charts are refreshed automatically every 60 seconds.

**Domino HTTP Requests**

When you select Domino HTTP Requests, a bar chart of server request statistics for the current server session (the period from when the server was last started to the current time) appears. A server request occurs when a user or another server asks your server to perform a task. The bar chart shows the average and peak numbers of requests per minute, per every five minutes, per hour, and per day. It also shows the total number of requests during the current session.
Monitor this chart to determine whether the rate of requests to the server is rising or whether the server is constantly at peak load. A rise in server requests indicates a potential performance problem and might indicate the need for a server upgrade or an additional server.

**Domino HTTP Commands**

When you click Domino HTTP Commands at the bottom of the screen, the Sametime Administration Tool displays a bar chart for server command statistics for the current server session. Use this information to analyze the type and number of tasks your server must handle, which can help you monitor and manage server performance. The Sametime Administration Tool also displays statistics for HTTP commands such as OpenDatabase and EditDocument.
Chapter 12. Logging Sametime Activity

IBM Lotus Sametime server activity is recorded in the Sametime log. The Sametime Administration Tool includes log settings that allow the administrator to control whether Sametime information is logged to a database or a text file. The log settings also enable the administrator to specify the information recorded in the log and to control the size of the log. If the administrator logs Sametime information to a database, the administrator can view the log from the Sametime Administration Tool. For more information about log settings, see "Sametime log settings" in this chapter.

The Sametime Administration Tool also allows an administrator to launch the Domino Web Administration Tool to view the Domino log. The Domino log includes information about available memory and disk space, server performance, and databases that need maintenance. For more information, see “Domino log” in this chapter.

Community Logins/Logouts

The Community Logins/Logouts section of the Sametime log displays successful user logins to Community Services and failed user attempts to log in to Community Services. If a single user is logged in to Community Services from more than one client, each login for that user is recorded in the log. A user can be logged in to Community Services from Sametime Connect and from the Participant List component of the Sametime Meeting Room.

You can view login and logout information in the following ways:

- **Login/Logout by Time**: Login and logout times for each user who logged in to Community Services, sorted by time. This option only appears if the [Successful logins] option in the Community Server Events to Log settings is selected.
- **Login/Logout by User**: Login and logout times for each user who logged in to Community Services, sorted by user name. This option only appears if the [Successful logins] option in the Community Server Events to Log settings is selected.
- **Failed Logins by Time**: Failed attempts to log in to Community Services, sorted by time. This option only appears if the [Failed logins] option in the Community Server Events to Log settings is selected.

Community Login/Logout Information

Each of the options listed above contains some or all of the following information about user attempts to log in to a Sametime community:

- **User ID** - A Lotus Notes User ID (canonical name, such as cn=John Smith, ou=West, o=Acme), a User Name as specified in the Person document of the Sametime directory, or a Distinguished Name from an LDAP directory. Anonymous users are identified by numbers.
- **Time** - The date and time that a user logged in or logged out.
- **Event Type** - The type of event being logged: Community Login, Community Logout, or Failed Login.
- **IP Address** - The IP address of the user’s computer.
- **Application Type** - The type of application from which a user logged in:
- **Connect**: Sametime Connect for the desktop. Indicates a user is authenticated.
- **Connect for browser**: Sametime Connect for browsers. Indicates a user is authenticated.
- **Web**: The Sametime Meeting Room, the Sametime Meeting Center, the Sametime Administration Tool, or an application created with the Sametime Java Software Development Kit.
- **Sametime links**: An application created with the Sametime Links Software Development Kit.
- **DB**: An application created with the C++ Software Development Kit.
- **Unknown type**: Appears when the Application Type cannot be determined.

- **Client Version** - The user's client version. If "Pre V3.1" or "Post 3.1" appears in this field, then the precise version of the client could not be detected.
- **Connectivity** - The connectivity method used by the client:
  - Direct
  - HTTP polling
  - HTTP tunneling

  **Note** For more information about these connectivity methods, see [Sametime Connect client connection processes](#) and [Meeting Room and Broadcast client connection processes](#).

- **Failure Reason** - The reason a login failed.
- **Reason** - The reason a login failed. Also indicates if a user was able to log out normally.

The administrator can use the [Successful logins](#) and [Failed logins](#) options in the Community Server Events to Log settings to record information in the Community Logins/Logouts section of the log.

To access the Community Logins/Logouts section of the Sametime log, select Logging - Community Logins/Logouts in the Sametime Administration Tool.

---

**Community Statistics**

The Community Statistics section of the Sametime log displays information about the peak and total number of Community Services users and logins, as well as the peak and total number of chats and places created on the server. If a user is logged in to Community Services from more than one client, each login for that user is recorded in the Total Logins category. A user can log in to Community Services from Sametime Connect and from the Participant List component of the Sametime Meeting Room.

You can view Community Statistics in the following ways:

- **Users and Logins by Day**
- **Users and Logins by Week**
- **Users and Logins by Month**
- **Users and Logins by Year**
- **Chats and Places by Day**
- **Chats and Places by Week**
- **Chats and Places by Month**
- **Chats and Places by Year**
Community Statistics information

Each of the options listed above contains some or all of the following information:

• Date/Week Beginning/Month Beginning/Year Beginning - The heading depends upon the Community Statistics view chosen from the drop-down menu. The date that users accessed Community Services.

• Peak Users - The number of users accessing Community Services when server usage is at its highest.

• Peak User Time - The time when the peak number of users occurs.

• Total Users - The number of new users that accessed Community Services during the selected date range. Users who accessed Community Services prior to the selected date range are not included in this number.

• Peak Logins - The number of logins to Community Services when server usage is at its highest.

• Peak Login Time - The time when the peak number of logins occurs.

• Total Logins - The number of new Community Services logins during the selected date range. Users who logged in prior to the selected date range are not included in this number.

• Peak 2-Way Chats - The maximum number of 2-way chats that existed during the selected date range, regardless of when the chats were started.

• Peak 2-Way Chat Time - The time when the peak number of 2-way chats occurs.

• Total 2-Way Chats - The number of new 2-way chats created during the selected date range. Chats that were started prior to the selected date range are not included in this number.

• Peak n-Way Chats - The maximum number of n-way chats that existed during the selected date range, regardless of when the chats were started.

• Peak n-Way Chat Time - The time when the peak number of n-way chats occurs.

• Total n-Way Chats - The number of new n-way chats created during the selected date range. Chats that were started prior to the selected date range are not included in this number.

• Peak Places - The maximum number of places that existed during the selected date range, regardless of when the places were created.

• Peak Place Time - The time when the peak number of places occurs.

• Total Places - The number of new places that were created during the selected date range. Places that were created prior to the selected date range are not included in this number.

The administrator can use the [Sametime Statistics] settings to record information in the Community Statistics section of the Sametime log.

To view information about Community Services statistics, select Logging - Community Statistics in the Sametime Administration Tool.

Community Events

The administrator can use the Community Events section of the Sametime log to view information about Community Services on the Sametime server. For example, you can view the name and status (started or stopped) of the service.

You can view community events in the following ways:

• Community Server Events by Date - Community Services events listed by date
• **Community Server Events by Name** - Community Services events listed by event name

**Community Events information**

Each of the options above contains some or all of the following information:

- **Date** - The date the service was started or stopped
- **Time** - The time the service was started or stopped
- **Application Name** - The name of the Community Service
- **Description** - The status of the service (Started or Stopped)
- **Reason** - The reason that the Community Service was stopped

The administrator can use the **Community server events and activities** option in the Community Server Events to Log settings to record Community server events in the Community Events section of the log.

To access information about Community events, select Logging - Community Events in the SameTime Administration Tool.

**Place Login Failures**

Use the Place Login Failures option to view failed user attempts to authenticate when accessing a SameTime "place." You can also use this option to view password failures that occur when users attempt to access password-protected SameTime meetings or places. SameTime does not log password failures that occur when users attempt to view recorded meetings or the meeting details of password-protected meetings.

For information about how users are authenticated when accessing the SameTime server, see [**Working with SameTime security**](#).

**Note:** A SameTime "place" or "virtual place" is a programming concept that is generally synonymous with an online meeting. Each SameTime meeting occurs in a virtual place. Users are authenticated in the virtual place through the "login by token" or "login by password" processes described in [**About SameTime security**](#). The Place Login Failure option records information about user authentication and password failures to online meetings started from the SameTime Meeting Center. Programmers can also use the SameTime Software Development Kit to build other applications that create different types of online places. If such applications exist on the SameTime server, login failures to those places are also recorded in the Place Login Failure option. Some Place Login Failure information is recorded only for places that are created with the SameTime Software Development Kit. For more information, see [**About "virtual places."**](#)

You can view Place Login Failure information in the following ways:

- **Global Error** - Contains authentication failure information for places in which authentication fails for unknown reasons.
- **Bad Encryption Level** - Records failures that occur when the encryption level required by the place is higher than the encryption level supported by the client. For example, if a SameTime 1.5 client that supports RC2 40-bit encryption attempts to access a place that requires RC2 128-bit encryption, the client will be unable to log in.
• **Login Already Participating** - Records authentication failures that occur when a user has already authenticated to a place and attempts to authenticate to the same place a second time using the same client. Recorded only for places that are created with the Sametime Software Development Kit.

• **Meeting Password Failures** - Records failures that occur when users enter incorrect meeting passwords for password-protected Sametime meetings.

**Note:** Sametime does not log password failures that occur when users attempt to view recorded meetings or the meeting details of password-protected meetings.

• **Missing Mandatory Activity** - Records failures that occur when a place that is missing a required activity (such as chat, screen sharing, whiteboard, or audio/video) is created. Recorded only for places that are created with the Sametime Software Development Kit.

• **Place Already Exists** - Records failures that occur when the name of a newly-created place is identical to the name of an already existing place. Recorded only for places that are created with the Sametime Software Development Kit.

• **Place is Full** - Records failures that occur when the place is limited to a specific number of users and that number is exceeded. Recorded only for places that are created with the Sametime Software Development Kit.

• **Place Not Found** - Records failures that occur when a user attempts to log in to a place that doesn’t exist. For example, if a user attempts to join an instant meeting after all other participants have already left the meeting.

• **User Authentication Failures** - Records authentication failures that occur when a specific user attempts to enter a specific online place.

• **User Has No Permissions** - Records failures that occur when a place is restricted to specific users and a user without permission to enter the place attempts to enter it.

• **Wrong Place Type** - Records failures that occur when the wrong place type is used to enter to enter a place. For example, if a user attempts to use the "published" type to enter a place of the "private" type, a Wrong Place Type failure is recorded. Conversely, if a user attempts to use the "private" type to enter a place of the "published" type, a Wrong Place Type failure is also recorded. Users can enter either both private and published places by using the "Don’t care" place type. This type of login failure is recorded only for places that are created with the Sametime Software Development Kit.

**Place Login Failure information**

The options listed above contain the following information. The Global Error event type might not include data for each of these fields.

• **Severity** - All events on the server have a severity from 0 to 4, which indicates the impact of the event on the server (4 is the highest severity, indicating a critical problem on the server). Authentication failures and meeting password failures are considered high severity events because they might indicate attempts by unauthorized people to gain illegal access to a place. These failures also indicate that users were unable to access meetings or other Sametime places.

• **Place Login Failure Event Type** - The Place Login Failure Event Type is either Global Error, Login already participating, Meeting Password Failure, or User Authentication Failure. Each event type is described above.

• **Date and Time** - The date and time that the authentication failure or meeting password failure occurred.
• **Place ID** - A unique identifier of the place in which the authentication failure or meeting password failure occurred. The Sametime server assigns a unique ID to each place. A client must obtain this ID during the connection process to connect to a specific place or meeting on the server.

• **User Name** - The User Name of the person for whom the authentication failure or meeting password failure occurred.

The administrator can use the **Failed meeting authentications** option in the Meeting Server Events to Log settings and the **Failed logins** option in the Community Server Events to Log settings to record information in the Place Login Failures section of the Sametime log.

To access information about failed logins to places, select **Logging - Place Login Failures** in the Sametime Administration Tool.

---

### Meeting Login Failures

Meeting Login Failures includes failed attempts by the Sametime Meeting Room client to authenticate when connecting to the Meeting Services on the Sametime server.

You can view failed authentication attempts from the "Meeting Room Client Authentication Failures" option.

To authenticate with the Meeting Services, the Meeting Room client passes an authentication token to the Meeting Services. If this token is not valid, the Meeting Room Client cannot authenticate and the user is not allowed to attend the meeting. A failed Meeting Room Client Authentication Failure might indicate an attempt by an unauthorized person to gain illegal entry to a meeting (or hack into a meeting).

**Note:** If a user enters an incorrect password when attempting to attend a password-protected meeting, the meeting password failure is logged in the **Logging - Place Login Failures** section of the Sametime Administration Tool. Sametime does not log password failures that occur when users attempt to view recorded meetings or the meeting details of password-protected meetings.

### Meeting Login Failures information

The following information is recorded for Meeting Login Failures:

• **User Name** - A Lotus Notes User ID (canonical name, such as cn=John Smith, ou=West, o=Acme), a User Name as specified in the Person document of the Sametime directory, or a Distinguished Name from an LDAP directory. Anonymous users are identified by numbers.

• **Date** - The date of the failure

• **Time** - The time of the failure

• **Network Address** - The IP address or host name of the user’s computer

Click the time of a particular failure to view the following information:

• **Severity** - All events on the server have a severity from 0 to 4, which indicates the impact of the event on the server (4 is the highest severity, indicating a critical problem on the server). Authentication failures are considered high severity events because they might indicate attempts by unauthorized people to
gain illegal access to a meeting. These failures also indicate that users were unable to access meetings or other Sametime places.

- **Meeting Login Failure Event Type** - The Event Type is Meeting Room Client Authentication Failure, as described above.
- **Date and Time** - The date and time of the failed authentication.
- **Network Address** - The IP address or host name of the user’s computer.
- **Meeting ID** - A unique identifier for the meeting in which the failure occurred. The Sametime server assigns a unique meeting ID to each meeting. A client must obtain this ID during the connection process to connect to a specific meeting on the server.
- **User Name** - A Lotus Notes User ID (canonical name, such as cn=John Smith, ou=West, o=Acme), a User Name as specified in the Person document of the Sametime directory, or a Distinguished Name from an LDAP directory. Anonymous users are identified by numbers.

The administrator can use the **[failed meeting authentications]** option in the Meeting Server Events to Log settings to record information in the Meeting Login Failures section of the Sametime log.

To access information about failed logins to Meeting Services, select Logging - Failed Meeting Logins in the Sametime Administration Tool.

### Meeting Connections

You can view meeting connections in the following ways:

- **Sametime Meeting Room Client Connections** - The Sametime Meeting Room client connects to both Meeting Services and Community Services when a user attends a meeting. See [Meeting Room client connection process using JVM 1.4.2](Audio/Video Services) for more information.

- **Broadcast Control Connections** - The Broadcast client connects to the Broadcast Services on the Sametime server to receive the broadcast meeting streams. See [Broadcast client connection process using JVM 1.4.2](Audio/Video Services) for more information.

### Meeting Connections information

Each of the options above contains some or all of the following information:

- **User Name** - A Lotus Notes User ID (canonical name, such as cn=John Smith, ou=West, o=Acme), a User Name as specified in the Person document of the Sametime directory, or a Distinguished Name from an LDAP directory. Anonymous users are identified by numbers.

- **Meeting ID** - A unique identifier for the meeting the user attended or left. The Sametime server assigns a unique meeting ID to each meeting. A client must obtain this ID during the connection process to connect to a specific meeting on the server.

- **Date** - The date the user attended or left a meeting.

- **Time** - The time the user attended or left a meeting.

- **Connection Type** - Indicates whether a connection was a direct TCP/IP connection or tunneled through an HTTP proxy server.

**Note:** Connections through SOCKS servers are recorded as direct TCP/IP connections.

- **Connection Status** - Indicates whether the client was connecting to the Sametime server or disconnecting from the Sametime server.
The administrator can use the Meeting client connections option in the Meeting Server Events to Log settings to record information in the Meeting connections section of the log.

To access information about meeting connections, select Logging - Meeting Connections in the Sametime Administration Tool.

**Server Connections**

When multiple Sametime servers are installed in a community, a meeting started on one Sametime server can be simultaneously active on other Sametime servers. The Meeting Server component of one Sametime server must establish a connection with the Meeting Server component of another Sametime server to enable a meeting to be simultaneously active on both Sametime servers. You can view information about connections between Meeting Servers in the Server Connections section of the Sametime log. For more information, see Advantages of using multiple Sametime servers.

**Server Connections information**

The Server Connections section of the Sametime log includes the following information:

- **Meeting ID** - A unique identifier for the meeting during which the servers were connected or disconnected. The Sametime server assigns a unique meeting ID to each meeting. A client must obtain this ID during the connection process to connect to a specific meeting on the server.
- **Date** - The date of the connection or disconnection between the servers.
- **Time** - The time of the connection or disconnection between the servers.
- **Server Name** - The fully qualified Domino name of the Sametime server. (For example, cn=Sametime.acme.com/ou=West/o=acme.)
- **Encrypted** - Whether the meeting was encrypted.
- **Connect or Disconnect** - Whether there was a connection or a disconnection between the Meeting Server components of the Sametime servers.

The administrator can use the Connections to other meeting servers in this community option in the Meeting Server Events to Log settings to record information in the Server Connections section of the Sametime log.

To access information about server connections, select Logging - Server Connections in the Sametime Administration Tool.

**Meeting Statistics**

The Meeting Statistics section of the Sametime log displays information about number and duration of meetings on the Sametime server, as well as the average number of participants per meeting.

You can view meeting statistics in the following ways:

- **Statistics by Day**
- **Statistics by Week**
- **Statistics by Month**
- **Statistics by Year**
Note: The Sametime log does not record information related to playback of recorded meetings. Meeting Statistics are logged for the initial meeting only, not for subsequent playbacks.

Meeting Statistics information
Each of the options listed above contains some or all of the following information:

- **Date/Week Beginning/Month Beginning/Year Beginning** - The heading depends upon the Meeting Statistics view chosen in the drop-down menu. The date that Meeting Services were accessed.
- **Peak Meetings** - The number of active meetings when server usage is at its highest.
- **Peak Meeting Time** - The time when the peak number of active meetings occurs.
- **Total Meetings** - The number of new meetings that become active during the selected date range. Meetings that started prior to the selected date range are not included in this number.
- **Average Participants/Meeting** - The average number of participants in meetings which end during the selected date range, regardless of when the meetings started.
- **Average Meeting Duration** - The average duration of meetings which end within the selected date range, regardless of when the meetings started.
- **Total Meeting Hours** - The cumulative duration of all meetings which end within the selected date range.

The administrator can use the Sametime Statistics settings in the General tab of the log settings to record information about Meeting Statistics.

To view information about Meeting Statistics, select Logging - Meeting Statistics in the Sametime Administration Tool.

Meeting Events
You can use the Meeting Events section of the Sametime log to view detailed information about meetings on the Sametime server. You can also view the status of Meeting Services applications.

You can view meetings on the Sametime server in the following ways:

- **All Meetings** - All scheduled and instant meetings on the Sametime server, sorted by date
- **Meeting Server Events** - Meeting Services events, sorted by date

Note: The Sametime log does not record information related to playback of recorded meetings. Meeting Events are logged for the initial meeting only, not for subsequent playbacks.

Meeting Events information
Each of the options above contains some or all of the following information:

- **Date** - The date the meeting or service was started or stopped.
- **Time** - The time the meeting or service was started or stopped.
- **Application Name** - The name of the Meeting Services application that was started or stopped.
- **Description** - The status of the service (Started or Stopped).
• **Meeting Name** - The name of the meeting. Generally, instant meetings do not have names.

• **Moderator** - The name of the Meeting Moderator. The Moderator of an instant meeting is the person who starts the meeting. If "Anonymous" appears in this field, the meeting does not have a Moderator. This situation occurs when the administrator allows anonymous access to the Sametime server and an unauthenticated user schedules a meeting without designating a specific Moderator. If the Moderator switched during the meeting, only the initial Moderator's name appears.

• **Start or Stop** - Whether the meeting was started or stopped.

• **Meeting ID** - A unique identifier for the meeting. The Sametime server assigns a unique meeting ID to each meeting. A client must obtain this ID during the connection process to connect to a specific meeting on the server.

When viewing the information listed above, click on a meeting date to view some or all of the following information about the meeting:

• **Severity** - The severity of the meeting server event. All events on the server have a severity from 0 to 4, which indicates the impact of the event on the server (4 is the highest severity, indicating a critical problem on the server). Meeting events have a low severity.

• **Meeting Server Event Type** - Whether the Meeting Services application was started or stopped.

• **Meeting Started and Stopped Event Type** - Whether the meeting was started or stopped.

• **Date and Time** - The date and time the meeting was started and stopped.

• **Application Name** - The name of the Meeting Services application that was started or stopped.

• **Version** - The version of the Sametime server on which the meeting occurred.

• **Meeting ID** - A unique identifier for the meeting. The Sametime server assigns a unique meeting ID to each meeting. A client must obtain this ID during the connection process to connect to a specific meeting on the server.

• **Meeting Name** - The name of the meeting. Generally, instant meetings do not have names.

• **Moderator** - The name of the Meeting Moderator. The Moderator of an instant meeting is the person who starts the meeting. If "Anonymous" appears in this field, the meeting does not have a Moderator. This situation occurs when the administrator allows anonymous access to the Sametime server and an unauthenticated user schedules a meeting without designating a specific Moderator. If the Moderator switched during the meeting, only the initial Moderator's name appears.

• **Has Attached Data** - Whether the meeting included attached data. Attached data must be used with the whiteboard. Users can attach data before or during scheduled meetings. Data cannot be attached to instant meetings.

• **Instant** - Whether the meeting was an instant meeting. If it was not an instant meeting, the meeting was scheduled in the Sametime Meeting Center.

• **Meeting Type** - The meeting type (for scheduled meetings only): Collaboration, Moderated Presentation or Demo, or Broadcast Presentation or Demo.

• **Screen Sharing** - Whether the meeting included screen sharing.

• **Whiteboard** - Whether the meeting included the whiteboard.

• **Meeting Room Client Chat** - Whether the meeting included Meeting Room chat.

• **Audio** - Whether the meeting included audio.
• **Video** - Whether the meeting included video.
• **Send Web Pages** - Whether the meeting included the Send Web Page tool.
• **Polling** - Whether the meeting included polling (question and answer).
• **Broadcast** - Whether the meeting was a broadcast meeting.
• **Encrypted** - Whether the meeting was encrypted.
• **Password Protected** - Whether the meeting was protected with a password.
• **Attendee List** - The name of each meeting participant. If anonymous access to the server is permitted, the number of anonymous participants is displayed, but their names do not appear. Not available for broadcast meetings.

The administrator can use the **Meeting Events** and **Meeting server events and activities** options in the Meeting Server Events to Log settings to record information in the Meeting Events section of the Sametime log.

To access information about meetings and meeting server events, select **Logging** - **Meeting Events in the Sametime Administration Tool**.

---

**Capacity Warnings**

Capacity warnings inform you when meetings have reached a number that you define in the log settings. You can set the following types of capacity warnings for both instant and scheduled meetings:

- The number of active screen-sharing/whiteboard meetings
- The number of people in all screen-sharing/whiteboard meetings
- The number of people in one screen-sharing/whiteboard meeting

Warnings are only meant to notify the administrator about server usage; they do not prevent people from attending meetings when a limit is reached. For information about preventing people from attending meetings when a limit is reached, see **Usage Limits in the log**.

You can view capacity warnings in the following ways:

- **Instant Meetings** - Capacity warnings for instant meetings
- **Scheduled Meetings** - Capacity warnings for scheduled meetings

**Capacity Warnings information**

Each of the options above contains some or all of the following information:

- **Type of Capacity Warning** - One of the three capacity warnings listed above
- **Meeting Name** - The name of the meeting in which the capacity was exceeded
- **User Name** - The name of the person who reached the capacity
- **Date** - The date that the capacity was exceeded
- **Time** - The time that the capacity was exceeded

**Tip:** Click a capacity warning to see more information about it, such as the capacity (the limit that the administrator set in the Capacity Warnings log settings) and the current count (the current number of people or meetings).

The administrator can use the **Capacity Warnings** settings to record information in the Capacity Warnings section of the Sametime log.
To access information about capacity warnings, select Logging - Capacity Warnings in the Sametime Administration Tool.

**Usage Limits in the log**

The administrator can use the **Usage Limits and Denied Entries settings** (available from the Configuration - Audio/Video Services option in the Sametime Administration Tool) to restrict the number of users who can connect to the Audio/Video Services and the Broadcast Services. These settings limit the number of users who can simultaneously participate in interactive audio/video meetings or broadcast meetings on the server. If you set limits, some people might be able to attend a meeting while others are rejected when the limit is reached. When a limit is reached, it is recorded in the Sametime log. You can set separate limits for instant and scheduled meetings.

You can view usage limits and denied entries in the following ways:

- **Instant Meetings** - Usage limits and denied entries for instant meetings
- **Scheduled Meetings** - Usage limits and denied entries for scheduled meetings

**Usage Limits and Denied Entries information**

Each of the options above contains some or all of the following information:

- **Type of Usage Limit or Denied Entry** - The type of limit: Audio, Video, Broadcast Audio, Broadcast Video, or Broadcast Data. You can set limits for each of these categories in the Configuration - Audio/Video Services options in the Sametime Administration Tool.

- **Meeting Name** - The name of the meeting in which someone exceeded the usage limit.

- **User Name** - The name of the person who exceeded the usage limit and was denied entry to the meeting.

- **Date** - The date that the person who exceeded the limit was denied entry to the meeting.

- **Time** - The time that the person who exceeded the limit was denied entry to the meeting.

**Tip:** Click a usage limit to see more information about it, such as the current limit (the limit that the administrator set in the Usage Limits and Denied Entries settings).

To access information about usage limits and denied entries, select Logging - Usage Limits in the Sametime Administration Tool.

**Domino log**

An administrator can view additional information about the Sametime server in the Domino log database (log.nsf). The Domino log database records server activity information related to the Domino server and Domino databases, including databases used by the Sametime server (such as the Sametime Meeting Center). During setup, the Domino log database is automatically created and the server is assigned Manager access in the database’s Access Control List (ACL). The default access for all other users is Reader.

The Domino log database records information about all server activities, such as database size and usage, server events, calls made to and from the server, and billing for server services. Check the Domino log to monitor:
Available server disk space
Available server memory
Server load
Server performance
Databases that need maintenance

**Note:** The Domino log is only available from the Sametime Administration Tool. If you record Sametime log information in a text file, the text file does not include information about the Domino log.

**Content of the Domino log**

The administrator cannot use the Sametime log settings or the Sametime Administration Tool options to determine what appears in the Domino log. The Domino log records information about the activities of the Domino server on which Sametime is installed. Generally, the default settings should provide an adequate record of server activity. However, you can record additional information in this log file by altering settings in the Notes.ini file. Recording this additional information might be necessary to troubleshoot a specific system problem.

For more information, see the Maintenance section of the Domino R5 Administration documentation.

**Views in the Domino log**

The Domino log includes many views that do not apply to Sametime. Use the table below to determine which views are relevant for Sametime.

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database-Sizes</td>
<td>Lists the size of the database, the percentage of the database’s disk space in use, and the weekly usage for all databases on the server.</td>
</tr>
<tr>
<td></td>
<td>Use this view to check unused views, database size, and unused space in a database.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The stconf.nsf database grows in size depending on the number of meetings that have been created. You can archive this database frequently to prevent it from growing too large.</td>
</tr>
<tr>
<td>Database-Usage</td>
<td>Lists the date and time the database was accessed, the type of access, and the name of the user accessing the database for all databases on the server.</td>
</tr>
<tr>
<td></td>
<td>Use this view to check unused views and unused space in a database.</td>
</tr>
<tr>
<td>Mail Routing Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Miscellaneous Events</td>
<td>Shows Sametime events and error messages not contained in other views. Messages are sorted in order of occurrence.</td>
</tr>
<tr>
<td></td>
<td>Use this view to check for Sametime error messages, server crashes, and corrupted databases.</td>
</tr>
<tr>
<td>NNTP Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Object Store Usage</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Passthru Connections</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By Date</td>
<td>Not used by the Sametime server.</td>
</tr>
</tbody>
</table>
### Sametime log settings

Sametime uses two types of log settings:

- **General settings** - Allow you to specify the format and content of the Sametime log.
- **Capacity Warnings** - Allow you to set server usage parameters. When these parameters are exceeded, warning messages are written to the Sametime log. These messages help you monitor server usage and determine the cause of slow server performance.

To access the log settings, choose Logging - Settings in the Sametime Administration Tool.

### General log settings

The General log settings allow you to specify the format for the Sametime log and to control the information that the log records. The four types of General log settings are:

- **Database or text file settings** - Allow you to specify the format for the log and to automatically remove information from the log.
- **Sametime Statistics settings** - Allow you to control whether to log statistics related to chats, meetings, and users.
• Community Server Events to Log settings - Allow you to control which Community Services events are recorded in the Sametime log.

• Meeting Server Events to Log settings - Allow you to control which Meeting Services events are recorded in the Sametime log.

Database or text file settings
The "database or text file" settings allow you to specify the format for the log and to automatically remove old information from the log.

Enable logging to a Domino database (STLog.nsf): Select this setting to record Sametime Meeting Services and Community Services data in the Sametime log database (stlog.nsf). During setup of the Sametime server, the Sametime Log database is automatically created, and the administrator specified during setup is assigned Manager access in the database Access Control List (ACL). The server is also assigned Manager access to the database so that it can write information to the log. The default access for all other users is Reader.

When this option is selected, a Sametime administrator can view all of the information in the Sametime log by opening the Sametime Administration Tool and selecting Logging. The links available from the Logging menu display different views of the Sametime log database. For more information, see Viewing the Sametime log.

When this option is selected, you can use the Remove history after (days) setting to prevent the Sametime log from growing too large.

If the "Enable logging to a Domino database" option is not selected, Sametime activity is not recorded in the Sametime database, and the links beneath the logging option in the Sametime Administration Tool do not appear.

If you select this option, you cannot select the "Enable logging to a text file" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

Remove history after (days): Select this setting to automatically remove old information from the Sametime log database (stlog.nsf). In the field provided, specify the age (in days) of information that is automatically removed from the database. The default setting is 60 days.

This setting only applies to the Sametime log database; it does not remove Sametime log information stored in text files. You must manually delete old text files.

After selecting this option, click Update and restart the server for the setting to take effect.

Enable logging to a text file: Select this setting to record Sametime log information in a text file. When this option is selected, a new Sametime log text file is created every day. By default, the name of each text file contains the date on which the file was created (for example, log_23_Mar_2002.txt). After you select this option, specify a directory for the text files in the "Path to log text file" field. To view the file, open it in your preferred text editor. You cannot view the text file log from the Sametime Administration Tool.
If you log Sametime activity to a text file:

- Sametime activity is not recorded in the Sametime log database, and the links beneath the logging option in the Sametime Administration Tool do not appear. You cannot access the Domino log when you log to a text file.
- You must manually delete the text files from the server hard drive periodically to conserve hard disk space.

If you select this option, you cannot simultaneously select the "Enable logging to a Domino database" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and **restart the server** for the setting to take effect.

To access the "Database or text file" settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

**Sametime Statistics**

The Sametime Statistics log settings allow you to record statistics related to chats, meetings, and users. These statistics appear in the **Community Statistics** and **Meeting Statistics** sections of the Sametime log.

To record these statistics, select the Sametime Statistics option. Sametime statistics are recorded every 60 minutes.

After selecting this option, click Update and **restart the server** for the settings to take effect.

To access the Sametime Statistics settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

**Community Server Events to Log**

The Community Server Events to Log settings allow you to control which Community Services events are recorded in the Sametime log. After selecting any of these options, click Update for the settings to take effect.

**Note:** The settings take effect within a reasonable time period. The longest time period you will wait for these settings to take effect is the time interval specified for the "How often to poll for new servers added to the Sametime community" setting in the Configuration - Community Services settings of the Sametime Administration Tool. The default time interval for that setting is 60 minutes.

**Successful logins:** Select this setting to record information about successful Community Services logins and logouts in the **Community Logins/Logouts** section of the Sametime log. This option is selected by default.

**Failed logins:** Select this setting to record information about failed logins to Community Services in the **Place Login Failures**, **Meeting Login Failures**, and **Community Logins/Logouts** sections of the Sametime log.

**Community server events and activities:** Select this setting to record information about Community Services events in the **Community Events** section of the Sametime log. For example, you can view the name and status of each service.
To access the Community Server Events to Log settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

**Meeting Server Events to Log**

The Meeting Server Events to Log settings allow you to control which Meeting Services events are recorded in the Sametime log. After selecting any of these settings, click Update and **restart the server** for the settings to take effect. The Meeting Server Events to Log options are listed below.

**Failed meeting authentications:** Select this setting to record information about failed authentication attempts in the `Meeting Login Failures` section of the Sametime log and failed meeting password entries in the `Place Login Failures` section of the Sametime log. This setting enables the log to record the following failures:

- When the Meeting Room client cannot authenticate with the Meeting Services
- When a user enters an incorrect password while attempting to attend a password-protected meeting or place

**Meeting client connections:** Select this setting to record information about the following types of meeting client connections in the `Meeting Connections` section of the log:

- Sametime Meeting Room client connections
- Broadcast control connections

**Connections to other meeting servers in this community:** Select this setting to record information about connections and disconnections between meeting servers in the `Server Connections` section of the log.

**Meeting Events:** Select this setting to record information about Sametime meetings in the `Meeting Events` section of the log. For example, you can view meeting names and times and whether meetings were instant or scheduled. Click a meeting name to view additional information about the meeting, such as the collaborative activities used in the meeting.

**Meeting server events and activities:** Select this setting to record information about Meeting Services events in the `Meeting Events` section of the Sametime log. For example, you can view the name and status (started or stopped) of each service.

To access the Meeting Server Events to Log settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

**Capacity Warnings log settings**

Server performance can slow when many users are simultaneously accessing the server or when data-intensive applications or files are being shared in many meetings. The Sametime log settings include Capacity Warnings settings that enable you to set server usage parameters. When these parameters are exceeded, warning messages are written to the `Capacity Warnings` section of the Sametime log. The capacity warnings assist you in monitoring server usage and determining the cause of slow server performance.

If you have a consistently high level of server usage or many users who share data-intensive applications and files (such as CAD programs and files), you might need to install an additional Sametime server. For more information, see `Advantages of using multiple Sametime servers`.
The Sametime log settings allow you to make separate Capacity Warnings settings for instant and scheduled meetings. The settings for both instant and scheduled meetings are:

**Number of active screen sharing/whiteboard meetings exceeds**
Select this option to write a capacity warning message in the Sametime log when the number of meetings that include screen sharing and the whiteboard exceeds the specified number. The default setting is 100.

**Number of people in all screen sharing/whiteboard meetings exceeds**
Select this option to write a capacity warning message in the Sametime log when the number of people in all active screen-sharing/whiteboard meetings exceeds the specified number. The default setting is 200.

**Number of people in one active screen sharing/whiteboard meeting exceeds**
Select this option to write a capacity warning message in the Sametime log when the number of people in one active meeting that includes screen sharing or the whiteboard exceeds the specified number. The default setting is 50.

**Note:** Although Capacity Warnings settings record a message in the log, they do not prevent users from attending meetings when a limit is reached. The administrator can set **usage limits and denied entries** in the Configuration - Audio/Video Services settings of the Sametime Administration Tool to prevent users from attending meetings when certain limits are reached. Usage limits and denied entries are recorded in the **Usage Limits** section of the Sametime log. Usage limits and denied entries apply to audio connections, video connections, and broadcast data connections only. There are no usage limits or denied entries settings to control the screen sharing and whiteboard activities.

After selecting any of the Capacity Warnings settings, click Update and **restart the server** for the settings to take effect.

To access the Capacity Warnings settings, open the Sametime Administration Tool, select Logging - Settings, and click the Capacity Warnings tab.
Chapter 13. Managing Security

This chapter discusses:

- Authentication of Web browser and IBM Lotus Sametime server client connections
- Database Access Control Lists (ACLs)
- Self-registration security issues
- Encryption
- Using SSL with Sametime
- Ensuring Sametime servlet access when Domino requires SSL for all connections

Getting started with Sametime security

This section includes basic security information to help you get started with Sametime security. This section discusses:

- The required fully qualified server name
- Basic password authentication and authentication by token
- User requirements for basic password authentication
- Changing a user’s password
- Anonymous access and the Sametime Meeting Center
- Turning off anonymous access to the Sametime Meeting Center

The required fully qualified server name

The end user must enter the fully qualified DNS name of the Sametime server (for example, sametimeserver.meetings.acme.com) in the Web browser URL locator when accessing the Sametime server to authenticate with a Sametime 7.0 server.

The Domino Single Sign-On (SSO) feature must be enabled on the Sametime 7.0 server. The Domino SSO feature requires the user to enter the fully qualified DNS name of the server for a successful authentication. For more information, see Authentication by token using LTPA and Sametime tokens.

Basic password authentication and authentication by token

Sametime uses two types of authentication:

- Basic password authentication
- Authentication by token

Basic password authentication

Sametime uses basic password authentication to authenticate Web browser connections and Sametime Connect client connections. Sametime uses the same Internet and intranet security features as a Domino server to authenticate the Web browser connections. These features include Domino database Access Control Lists (ACLs) and security settings in the Server document of the Domino server on which Sametime is installed.

The Domino security features also allow you to configure databases for anonymous access. When a database is configured for anonymous access, the user is not authenticated when accessing the database.
Note: By default, the ACL settings of the Sametime Meeting Center database (stconf.nsf) allow anonymous access, and users can start and attend meetings without authenticating. You can turn off anonymous access to the Sametime Meeting Center by altering the ACL settings of the database. For more information, see [Turning off anonymous access to the Sametime Meeting Center](#).

The following topics in this section discuss basic password authentication:
- User requirements for basic password authentication
- Using database ACLs for identification and authentication
- Basic password authentication and database ACLs
- Setting up basic password authentication in a database Access Control List (ACL)

### Authentication by token

After a Web browser user authenticates using basic password authentication, Sametime Java applet clients (such as the Meeting Room client, Broadcast client, and Sametime Connect for browsers client) load in a user’s Web browser. These Sametime clients make connections to the Community Services, Meeting Services, and Broadcast Services when a user attends a meeting. Sametime uses "authentication by token" to authenticate the connections from these Sametime clients to the Sametime services.

Note: Connections from the Sametime clients to the Community Services, Meeting Services, and Broadcast Services are authenticated only if the Sametime Meeting Center database (stconf.nsf) requires basic password authentication. If the Sametime Meeting Center allows anonymous access, these connections are not authenticated.

When the Sametime Meeting Center requires basic password authentication, authentication by token is supported on the Sametime 7.0 server using the Domino Single Sign-On (SSO) authentication feature.

If your environment includes only Sametime 3.0 (or higher) servers, it is only necessary to enable the Domino SSO feature on the Sametime servers.

Note: Sametime TeamRoom and Discussion databases were available with previous Sametime releases but are no longer included in the Sametime product.

The Sametime 7.0 server must support both the Domino SSO feature and the Secrets and Tokens database authentication system if your environment includes Sametime 3.0 (or higher) servers that interoperate with Sametime servers from releases earlier than Sametime 3.0.

The following topics discuss authentication by token:
- Authentication by token
- Authentication by token using the Domino Single Sign-On (SSO) feature
- Authentication by token using Secrets and Tokens databases

### User requirements for basic password authentication

When accessing the Sametime server with a Web browser, a user must enter a user name and Internet password to access any protected database on the Sametime server. A protected database is a database that has its Access Control List (ACL) set
to require **basic** password authentication. If the ACL settings of a database allow anonymous access, the user is not authenticated (prompted for a user name and Internet password) when accessing the database.

**Note:** It is important for a user to enter a name when accessing a Sametime database so that the user’s name can be displayed in any presence list within the database. If the ACL settings of a database allow anonymous access, a user is not prompted for a name unless the "Users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting is selected in the Configuration-Community Services-Aononymous Access settings of the Sametime Administration Tool. When this option is selected, it forces a name entry prompt to appear when an anonymous user attends a scheduled meeting. From this name entry prompt, the user can enter a name for display purposes in a presence list. The server accepts any name entered by the user at the name entry prompt; the user is not authenticated. For more information, see [Users of Sametime applications can specify a display name](#).

A Sametime Connect user must also be authenticated each time the user starts the Sametime Connect client and connects to the Community Services on the Sametime server. Sametime Connect users must enter the user name and Internet password from the Person document in the Domino Directory when logging on to Sametime Connect.

**Note:** If you have configured Sametime to operate with an LDAP directory, Sametime authenticates users based on the user names and passwords stored in the person entries of the LDAP directory.

**Person document, User names, and Internet passwords in the Domino Directory**

This section discusses the requirements for basic password authentication when Sametime is installed to operate with a Domino Directory. You must choose either the Domino Directory or an LDAP directory during the Sametime installation.

Each member of the Sametime community must have a Person document in the Domino Directory to authenticate with the Sametime server. The names and password that a user can enter when accessing a Sametime server are maintained in the Basics tab of a Person document in the Domino Directory.

To access a Person document, open the Sametime Administration Tool and select Domino Directory-Domino-Manage People. Double-click a person’s name to open that user’s Person document.

The table below shows a sample entry in the Basics section of a user’s Person document. The text that follows the table explains how these entries are used in the Web browser and Sametime Connect client password authentication processes.

**Sample settings in the Basics section of a Person document**

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>Gary</td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Middle initial</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Last name</td>
<td>Ollerman</td>
<td>This field is required.</td>
</tr>
</tbody>
</table>
### Table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Gary Ollerman/CommunityГОllerman</td>
<td>This field is required.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Community (or domain) name is appended to the first entry in the user name field by default.</td>
<td></td>
</tr>
<tr>
<td>Alternate name</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Short name/UserID</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Generational qualifier</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Internet password</td>
<td>(FCF5F3960B0A289D3)</td>
<td>This field is required.</td>
</tr>
</tbody>
</table>

The following fields on the Person document are used by the authentication process:

- **First name** - This field is optional.

  *Web browser* - If an entry exists in the "First name" field in the Basics tab of the Person document, the user can enter just this name at the User Name prompt that appears when accessing a protected database on the Sametime server with a Web browser. The user must also enter the Internet password to access the database. (A protected database is a database that has its ACL set to require **basic password authentication**.)

  *Sametime Connect* - The first name is not a valid entry at the User Name prompt that appears when logging on to the Sametime Connect client.

- **Last name** - This field is required. An entry must exist in the "Last name" field of the Basics tab of a Person document.

  The last name can be entered in the User Name prompt that appears when accessing a protected database on the Sametime server with a Web browser. The last name can also be used when logging on from the Sametime Connect client. A user must also enter the Internet password to complete the authentication process.

  **Note:** If both the "First name" and "Last name" fields contain entries, the user can enter the first and last names at the User Name prompt that appears when accessing the Sametime server.

- **User name** - This field is required. An entry must exist in the "User name" field in the Basics tab of a Person document.

  Generally, it is good practice to use a user’s first and last name in the "User name" field. The "User name" field can contain multiple entries. In our example, the User name field contains both Gary Ollerman/Community and GOllerman. (Each entry must be separated by a semicolon or a carriage return in the "User name" field of the Person document.)

  A user can enter any name that appears in the "User name" field of the Person document when logging on to the Sametime server from the Sametime Connect client or a Web browser. For example, the user could enter Gary Ollerman/Community or GOllerman at a Sametime Connect or Web browser User Name prompt. The name entered by the user is resolved to the topmost
name (Gary Ollerman/Community in the example) in the "User name" field. The topmost name in the "User name" field is the name that is displayed in the presence lists of all Sametime clients.

Note: If you want a user’s e-mail address to display in presence lists, enter the user’s e-mail address as the topmost name in the "User name" field of the Person document. If the e-mail address is included in the User name field, the user can also enter the e-mail address at the "User name" prompt when logging in from a Sametime Connect client or Web browser.

Sametime uses the topmost name in the "User name" field to validate a user in a database ACL. If you require basic password authentication for a database and you enter the names of individual users in the ACL of a database, enter the topmost name that appears in the "User name" field of the Person document in the database ACL. Although the user can enter "GOllerman" when logging on, Sametime uses "Gary Ollerman/Community" to validate the user in the database ACL. Therefore, "Gary Ollerman/Community" must be the name that appears for this user in database ACLs.

- **Internet password** - This field is required. Users must enter the Internet password to authenticate with the Sametime server using a Web browser or the Sametime Connect client. In the example, the Internet password is "sametime." The password displays as a series of random characters because Internet passwords are encrypted on the Person document.

**Self-registration**

If you are using the self-registration feature of the Sametime server, a Person document containing a last name, user name, and Internet password is automatically created for a user in the Domino Directory on the Sametime server at the time the user self registers. Agents in the Self-Registration database (streg.nsf) access the Domino Directory to create these Person documents. The signers of these agents must have the proper access levels and permissions in the Domino Directory for self-registration to work properly. If you allow self registration, you might need to add these signers to the Domino Directory ACL. For more information, see [Using Sametime self-registration in a Domino environment](#).

The Sametime self-registration feature cannot be used if you have configured the Sametime server to operate with an LDAP directory on a third-party server (such as a Microsoft Exchange or Netscape Directory Server).

**LDAP**

If you have configured the Sametime server to operate with an LDAP directory on a third-party server, the authentication process uses the user names and passwords stored in the LDAP directory. It is not necessary to create Person documents containing separate user names and passwords in the Domino Directory on the Sametime server.

For more information, see [Using LDAP with the Sametime server](#).

**Changing a user’s password**

When accessing the Sametime server from any Sametime client, the user might be prompted for a user name and password. The password is specified in the Internet password field on the user’s Person document in the Domino Directory on the Sametime server. To change a user’s password, open the user’s Person document and enter a new password in the “Internet password” field.
Note: If you have configured the Sametime server to operate with an LDAP directory on an LDAP server, the authentication process uses the passwords specified in the LDAP directory. Use the administrative tools provided with the third-party LDAP server to access the LDAP directory and make password changes for individual users. You cannot change passwords stored in an LDAP directory from the Sametime Administration Tool.

To change a user's Internet password in the Domino Directory on the Sametime server:
1. From the Sametime server home page, open the Sametime Administration Tool.
2. Select Domino Directory.
3. Select Domino.
4. Select Manage People.
5. Double-click the name of the user whose password you want to change.
6. Click Edit Person.
7. Enter the new password in the "Internet password" field of the Person document. You might want to write the new password down before closing and saving the Person document. After you close and save the Person document, the Internet password is encrypted and you cannot view it.
8. Select "Save and Close."

Anonymous access and the Sametime Meeting Center

The default Access Control List (ACL) settings of the Sametime Meeting Center database (sconf.nsf) allow anonymous users to access the database. When the ACL settings of the Sametime Meeting Center allow anonymous access, a user is not authenticated and is not required to enter a user name and Internet password when accessing the database.

If a user does not enter a name when accessing the Sametime Meeting Center, the presence list (Participant List) component of the Sametime Meeting Room client displays that user’s name as "anonymous." If several users access the database without entering a name, all users are listed in the presence list as "anonymous," which can be confusing. (The end users cannot distinguish one anonymous user from another.)

To avoid the "anonymous" display name problem, the Sametime Administration Tool includes "Anonymous Access Settings" that force a name entry prompt to appear when the ACL settings allow anonymous users to access the database. This prompt accepts any name provided by the user and ensures that all users are individually identified in the Participant List of the Sametime Meeting Room client. The name entered at this prompt is for Participant List display purposes only. These Anonymous Access Settings are available from the Configuration-Community Services-Anonymous Access Settings tab of the Sametime Administration Tool. For more information, see Anonymous Access Settings for Community Services.

For tighter security, you can use the database ACL settings to require basic password authentication to the Sametime Meeting Center. When the database ACL settings require basic password authentication, users are required to enter a user name and Internet password when accessing the database. The user name and Internet password entered by the user are authenticated against entries in the user's Person document in the Domino Directory. The Sametime presence lists represent the authenticated user by displaying the topmost entry in the "User
name” field of the user’s Person document. The Anonymous Access Settings in the Sametime Administration Tool are not used when the ACL settings of a database require basic password authentication. For more information, see Turning off anonymous access to the Sametime Meeting Center.

Note: Sametime Connect client users cannot access the Sametime Connect client as anonymous users. Sametime Connect users must provide a user name and password to log in to the Community Services from Sametime Connect.

**Turning off anonymous access to the Sametime Meeting Center**

The default Sametime security settings allow Web browser users to access the Sametime Meeting Center database (stconf.nsf) anonymously.

To increase security for the Meeting Center, you can turn off anonymous access and require basic password authentication to the Sametime Meeting Center. All users are then required to authenticate when accessing the Sametime Meeting Center to schedule or attend a meeting. When basic password authentication is required, Web browser users must enter the user name and Internet password from their Person documents when selecting the “Attend a meeting” or “Schedule a meeting” link from the Sametime server home page. The name and password entered by the user is verified against information in the Directory to verify that users are who they claim to be.

Note: It is mandatory that you enable the Domino SSO feature on the Sametime 7.0 server. Tokens generated by the SSO feature are required to authenticate connections from Sametime clients to the Meeting Services, Community Services, and Broadcast Services. For more information, see Authentication by token using the Domino Single Sign-On (SSO) feature.

Use the following procedure to turn off anonymous access to the Sametime Meeting Center (stconf.nsf):

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino.
   If you are using an LDAP directory with the Sametime server, select LDAP Directory.
3. Select Set Access Control.
4. From the Databases list, select Sametime Online Meeting Center (the filename of the database is stconf.nsf).
5. Click the Access button.
6. Select the Anonymous entry.
7. In the Access Box, select the "No access" level for the Anonymous entry (or delete the "Anonymous" entry from the Access Box).
8. Click Submit.

After you complete this procedure, users will receive the Default access level in the Access Control List (ACL) of the Meeting Center. The Default access level is Author with the Write Public Documents privilege selected. These ACL settings provide meeting creator privileges (the ability to create and modify meetings) to any user who enters the correct user name and Internet password when accessing the Meeting Center.
If you want to further control security by specifying which users have meeting creator privileges and which users have attendee-only privileges, you must enter individual names or group names in the ACL of the Meeting Center. Assign the access levels and privileges as follows:

- **Meeting Creators** - Assign the Author access level with the Write Public Documents privilege to the individual user names or group names that you are allowing to create and modify meetings on the server.
- **Reader (attendee-only)** - Assign the Reader access level to the individual user names or group names that you want to have attendee-only access to the Sametime Meeting Center. These users can attend meetings but cannot create them.

**Note:** To enable a user with the Reader access level to attend unlisted meetings, you must also select the Write Public Documents privilege for the user.

In addition to adding individual user or group names to the ACL, you must also ensure that the Anonymous and Default entries are set to No Access in the database ACL. For more information, see **[Setting up basic password authentication in a database Access Control List (ACL)](https://www.ibm.com/support/docview.wss?uid=swg21139516)**

---

### Domino security and the Web browser connection

To attend a meeting on the Sametime server, a user first connects to the Sametime HTTP server with a Web browser. By default, the user is not authenticated when accessing the Sametime server over this port and is able to access the Sametime server home page database (stcenter.nsf) without entering a user name and password.

By using the Access Control List (ACL) settings of individual databases, the Sametime administrator can force users to authenticate using basic password authentication when they attempt to access the databases on the server.

Generally, the first database that a user accesses when connecting to the Sametime server is the Domino database that contains the Sametime server home page (stcenter.nsf). By default, the ACL settings of the stcenter.nsf database allow anonymous access so users can access the Sametime server home page without being authenticated (entering a user name and password that is verified against entries in a directory).

After accessing the home page, a user selects links to access other databases on the Sametime server. Most users will access the Sametime Meeting Center (stconf.nsf). The Sametime Administrator can alter the ACLs of these databases to force users to authenticate at the time they select the link that accesses the database.

The databases on the Sametime server that are accessible from the Sametime server home page include:

- **Sametime Meeting Center (stconf.nsf)** - An end user accesses the Sametime Meeting Center database when selecting the "Attend a Meeting" or "Schedule a Meeting" link from the Sametime server home page. The ACL settings of the Sametime Meeting Center database (stconf.nsf) allow anonymous access by default. Any anonymous user who accesses the Sametime server home page can select the "Attend a Meeting" or "Schedule a Meeting" link and access the Sametime Meeting Center database. These anonymous users can create meetings and attend any meeting on the server.
Although the ACL settings of the Sametime Meeting Center allow anonymous access, users are still prompted for a display name when attending a scheduled meeting. This display name appears in the Participant List of the Sametime Meeting Room client. For more information, see Anonymous access and Sametime databases.

If you change the ACL of the Meeting Center to require basic name and password authentication, users are required to enter a user name and Internet password when selecting the "Attend a Meeting" or "Schedule a Meeting" link.

**Note:** The Domino SSO authentication feature must be enabled on the Sametime server. For more information, see Authentication by token using the Domino Single Sign-On (SSO) feature.

- **Self-Registration (streg.nsf)** - An administrator controls whether self-registration is available on the server. The administrator controls self-registration by selecting or clearing the "Allow people to register themselves in the Directory" check box available from the Domino Directory - Domino option in the Sametime Administration Tool. The self-registration database (streg.nsf) should always allow anonymous access to enable anonymous users to self register when the administrator allows self-registration. For more information about the security considerations associated with self-registration, see Security recommendations for self-registration.

- **Server Administration** - You must add users to the ACLs of several Sametime databases when allowing other users to have administrative privileges on the Sametime server. For more information about controlling access to the Sametime Administration Tool, see Adding a new Sametime administrator.

**Note:** By default, the connection from a Web browser to the Sametime server is neither authenticated nor encrypted. The authentication occurs at the time a user accesses an individual database on the Sametime server. You can configure Sametime so that all HTTP traffic (including passwords and authentication tokens) that passes over the connection between the Web browser and the HTTP server is encrypted using the Secure Sockets Layer (SSL). For more information, see About SSL and Sametime.

### Using database ACLs for identification and authentication

Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server. For each database on the server, you can set the ACL to allow:

- **Anonymous access**

  or

- **Basic password authentication**

The settings in the database ACLs work together with the "Maximum Internet name & password" setting for each database to control the level of access that Web browser users have to a database on the Sametime server.

### Using database ACLs

The database ACL defines user access to the content of the database. Before you set up basic password authentication or anonymous access to a database, you should be familiar with how to add users to a database ACL and the available settings within the ACL. For more information, see:

- **Adding a name to a database ACL**
• **Database ACL settings**

**Maximum Internet name & password setting**

The "Maximum Internet name & password" setting on the Advanced panel of each database ACL specifies the maximum level of access to the database that is allowed for Web browser clients. This setting overrides individual levels set in the ACL.

Generally, administrators should not need to change the "Maximum Internet name & password" settings for databases on the Sametime server. The default settings should function adequately in most cases.

**Adding a name to a database Access Control List (ACL)**

To add a name to a database Access Control List:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select LDAP Directory.
4. Select a database from the list.
5. Click the Access button. The database ACL displays.
6. Click Add.
7. In the dialog box, type the exact user name from a Person document or the group name from a Group document. Click OK.

When entering a user name for a user with a Person document in the Domino Directory on the Sametime server, type the name exactly as it appears in the topmost entry of the "User name" field in the user's Person document.

When entering the names of users or groups registered in an LDAP directory in a Sametime database ACL, use the fully qualified Distinguished Name, but use forward slashes (/) as delimiters instead of commas. For example, if the Distinguished Name for the user in the LDAP directory is:

- uid = Joe Waters, ou=West, o=Acme

enter the name in the Sametime database ACL as follows:

- uid = Joe Waters/ou=West/o=Acme

You can also use asterisks for wildcards when entering names from an LDAP directory or a Domino Directory in an ACL. For example, entering */ou=West/o=Acme is equivalent to entering all users in the ou=West/o=Acme branch of the directory to the ACL.

**Note** It is possible to enter entities other than user and group names in an ACL. For more information about the types of entries that can exist in an ACL, see [User type - ACL settings](#).

8. Click the name entered in the previous step so that the name is selected (highlighted).

9. In the User Type box, select the type of user (Unspecified, Person, Server, Person Group, Server Group, or Mixed Group). For more information, see [User type - ACL settings](#).

10. In the Access Box, assign an access level for the user (Manager, Designer, Editor, Author, Reader, Depositor, or No Access). For more information, see [Access level - ACL settings](#).
11. Edit the privileges if necessary. For more information, see Privileges - ACL settings.

12. Click Submit.

Database ACL settings

A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database. For each user in the database ACL, you can specify the following ACL settings:

- User Type
- Access Level
- Privileges
- Roles

User type - ACL settings

When you add a user or group to an ACL, you specify a user type for the entry in the ACL. A user type identifies whether a name in the ACL is for a person, server, group, or other entity. You assign a user type to a name to specify the type of ID required for accessing the database with that name.

You can designate an entry in the ACL as any of the following user types:

Unspecified

Select the Unspecified user type if you want to enable the name you are entering to access the database with any type of ID (Person, Server, or Group). The Default entry in an ACL is always assigned the Unspecified user type. IDs used to sign agents, such as Sametime Development/Lotus Notes Companion Products, are also assigned the Unspecified user type when entered in a database ACL.

Person

Select the Person user type if the name you are entering belongs to a user who has a Person document containing a user name and Internet password in the Directory on the Sametime server or if the user has a Person entry in an LDAP directory on a third-party server.

Server

Select the Server user type if the name you are entering belongs to another server in the Domino domain. When multiple servers are installed in a Domino environment, it might be necessary for a server to access data within the database or to replicate a database. Server names are frequently added to the pre-existing LocalDomainServers and OtherDomainServers server groups. The Server user type is generally used only if you have installed Sametime in a Domino environment. This user type performs the same function as it does on a Domino server.

Mixed Group

Select the Mixed Group user type if the name you are entering belongs to a group that consists of both Server and Person names.

Person Group
Select the Person Group user type if you are entering the name of a group that contains only people. You can enter a group from the Directory on the Sametime server, or you can enter a group stored in an LDAP directory on a third-party server in the ACL of a database.

Server Group

Select the Server Group user type if the name you are entering belongs to a group that consists of only servers.

**Access level - ACL settings**

Access levels are the database ACL settings that control the type of actions a user can perform on the contents of a database and on the database itself. Access levels range from No Access, which prevents a user from opening a database, to Manager, which lets a user read, create, and edit the ACL and all documents in the database.

Users that are listed both individually and in one or more groups in the ACL might be assigned different levels of access. The access level granted in an individual entry takes precedence over the access level granted through a group entry. If a user is in multiple groups, the user is granted the access level of the group with the highest level of access.

If a user or group has one level of access in the ACL and another level of access in a database component (such as a Read or View access list), the database component access level takes precedence over the user or group access level.

The following access levels are listed from lowest to highest. A higher access level has all the privileges granted to lower access levels. For example, Authors can perform all of the functions of a Depositor and a Reader.

**No Access**

No Access prevents a user from accessing the database. For example, if you assign No Access as the Default access for a database, only a user who has a Person document in the Address Book and is listed in the ACL can access the database.

**Depositor**

Depositor access allows a user to create documents but not view any documents in the database, including the documents created by the user. This access level is not generally used for Sametime databases. This ACL type is most frequently used for automatic agents to write documents into a database for Domino workflow applications.

**Reader**

Reader access allows a user to read documents in a database, but not create or edit documents. For example, you can assign Reader access in the Meeting Center (stconf.nsf) ACL to users who are allowed to attend but not start meetings.

**Note:** If you assign a user the Reader access level in the Meeting Center (stconf.nsf), the user can attend listed meetings but cannot attend unlisted meetings in the Meeting Center. To enable a user with Reader access to also attend unlisted meetings, you must select the "Write public documents" check box for that user in the ACL.
Author

Author access allows a user to create and edit documents. Users with Author access can edit documents they have created themselves, but they cannot edit documents created by other users.

Assign Author access in the Meeting Center ACL to allow users to create meetings in the Sametime Meeting Center. Meeting Center users with Author access can modify the meetings they create, but they cannot modify meetings created by other users. To create a meeting, the user must have Author access and the Write Public Documents privilege selected.

Editor

Editor access allows users to read, create, and edit all documents in the database, including those created by other users.

Assign Editor access in the Meeting Center ACL to users who are allowed to modify meetings they create and meetings that are created by other users. Editors can also start meetings in the Meeting Center. To create meetings, the user must also have the Write Public Documents privilege selected.

Designer

Designer access allows a user to create full-text indexes, modify all database design elements, and read, create, and edit all documents in the database. This access level is primarily for programmers and database developers.

Manager

Manager access allows a user to read, create, and edit the ACL and all documents in a database, modify ACL settings, and delete the database. Modifying the ACL and deleting databases are tasks permitted by no other access level. This access level is usually assigned to Sametime administrators and is not recommended for general users.

Each database must have at least one Manager. Generally, the Manager access level is provided in each database to the person specified as the administrator during the Sametime installation and setup procedure. You should assign Manager access to two people in case one manager is unavailable. For information about granting other users administrative privileges, see [Allowing others to use the Sametime Administration Tool](#).

Privileges - ACL settings

The database Access Control List (ACL) defines privileges for users. Depending on the access level assigned to a user, some ACL permissions are granted, denied, or optional. Privileges listed in the ACL are:

Create documents

This privilege allows users to create documents in a database. This privilege is:
- Permanently granted to Managers, Designers, Editors, and Depositors
- Permanently denied to Readers
- Optionally granted to Authors
Delete documents

This privilege allows users to delete documents from a database. This privilege is:

- Permanently denied to Readers and Depositors
- Optionally granted to Managers, Designers, Editors, and Authors

Create personal agents

This privilege allows an Lotus Notes developer or user to create agents that perform automated procedures in a database. This privilege is:

- Permanently granted to Managers and Designers
- Optionally granted to Editors, Authors, and Readers

Clear this option on server databases to prevent certain users from creating personal agents that take up server disk space and processing time. Use the Agent Restrictions settings in the Security tab of the Server document in the Directory to prevent users from running personal agents on a server, even if the “Create personal agents” permission in a server database ACL is selected.

Create personal folders/views

This privilege is:

- Permanently granted to Managers and Designers
- Permanently denied to Depositors
- Optionally granted to Editors, Authors, and Readers

Personal folders and views created on a server are more secure and are available on multiple servers. Also, administrative agents can operate only on folders and views stored on a server. If this permission is not selected, users can still create personal folders and views that are stored on their local workstations. Clear this option to save disk space on a server.

Create shared folders/views

This privilege is:

- Permanently granted to Managers and Designers
- Permanently denied to Authors, Readers, and Depositors
- Optionally granted to Editors

Deny this privilege to Editors to save disk space on a server and maintain tighter control over database design.

Create LotusScript

This privilege is:

- Permanently granted to Managers
- Permanently denied to Depositors
- Optionally granted to Designers, Editors, Authors, and Readers

Clear this option on server databases to prevent certain users from running restricted and unrestricted LotusScript agents that take up server disk space and processing time. Use the Agent Restrictions settings in the Security tab of the Server document in the Directory to prevent users from running restricted and
unrestricted LotusScript agents on a server, even if the “Create personal agents” permission in a server database ACL is selected.

Read Public Documents

This privilege is:
- Permanently granted to Managers, Designers, Editors, Authors, and Readers
- Optionally granted to Depositors

Write Public Documents

This privilege is:
- Permanently granted to Managers, Designers, and Editors
- Optionally granted to Authors, Readers, and Depositors

Public documents, such as the meeting details document in the Sametime Meeting Center, are designed to be accessed by a wide audience. Users with the Write Public Documents permission can read, create, edit, and delete public documents from a database. To create a meeting in the Sametime Meeting Center, a user must have the Author access level with the Write Public Documents privilege selected.

A user must also have the Write Public Documents privilege selected to attend unlisted meetings on the Sametime server.

Users without the Write Public Documents privilege are prompted for a password when accessing a database with public documents. After entering the user name and Internet password, the user is given the Default access level to the database.

Roles - ACL settings

Database Access Control List (ACL) roles grant access to individual database components, such as forms or views. You can use ACL roles to delegate authority for managing specific documents in a database. For example, you can assign the roles of UserCreator and UserModifier in the Directory (Address Book) ACL to the administrator who has the responsibility for creating and maintaining Person documents.

ACL roles are optional in most databases. You can choose to rely on a broader access level and not use roles.

For more information on roles available in important Sametime databases, see Roles in Sametime databases ACLs

Note: You can create up to 75 roles in a database.

Anonymous access and database ACLs

You can set a database ACL to allow anonymous access. Anonymous access has the following characteristics:
- Users are not identified or authenticated when they access databases and applications on the server.
- Data sent between the user and the Sametime server is not encrypted.
- Anonymous users are not identified in the maintenance log files. All anonymous user activity is recorded under the name “Anonymous.”
The anonymous access level requires the least maintenance from the administrator, but it is the least secure. You should only allow anonymous access when you do not need to know the identity of users accessing your server. For example, use anonymous access if the Sametime server is behind your firewall and you plan to only allow trusted intranet users to access it.

**Setting up anonymous access in a database Access Control List (ACL)**

To allow anonymous access to a database, you can add the Anonymous entry to the ACL and assign an access level to the Anonymous entry.

**Note:** Alternatively, you can remove the Anonymous entry from the ACL and assign an access level to the Default entry in the ACL. When the Anonymous entry is removed from the ACL, anonymous users receive the access level and privileges assigned to the Default entry in the database ACL.

Use the following procedure to allow anonymous users to access a database:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select LDAP Directory.
4. Select a database from the list.
5. Click the Advanced button.
6. Set the "Maximum Internet name & password" access to Manager, which is the maximum access level.

**Note:** The "Maximum Internet name & password" setting on the advanced panel of each database Access Control List (ACL) specifies the maximum database access level granted to Web browser clients. This setting overrides higher individual access levels set in the ACL. For example, if you set the "Maximum Internet name & password" to Author, and assign Editor access to the Anonymous entry in the database ACL, anonymous users will only have Author access to the database. Alternatively, if you set the "Maximum Internet name & password" to Manager, and assign Reader access to the Anonymous entry in the database ACL, anonymous users will only have Reader access to the database.

7. Click the Access button.

   If the Anonymous entry exists in the ACL, select the Anonymous entry and assign an access level (for example, Author). Edit the default privileges if necessary.

   If the Anonymous entry does not exist in the ACL, users who access the database anonymously receive the access level and privileges assigned to the Default entry in the ACL.

   **Note:** If the Anonymous entry does not exist in the ACL, the administrator also has the option to create an Anonymous entry and assign an access level and privileges. In this case, users receive the access level associated with the Anonymous entry instead of the Default entry.

8. Click Submit.

**Note:** If you set the ACL of the Sametime Meeting Center database to allow anonymous access, you should ensure that users are required to enter a
display name when accessing the database. To ensure that users will be
required to enter a display name to appear in the Participant List of the
Sametime Meeting Room during a scheduled meeting, make sure that the
"Users of Sametime or Sametime applications can specify a display name so
that they do not appear online as ‘anonymous’” setting is selected in the
Configuration-Community Services-Anonymous Access settings of the
Sametime Administration Tool. For more information, see Anonymous
Access settings for Community Services.

Basic password authentication and database ACLs

You can set a database ACL to require basic password authentication. Basic
password authentication has the following characteristics:

- Users are identified or authenticated when they access databases and
  applications on the server.
- A Web browser user must have a user name and an Internet password stored in
  the user’s Person document to access databases. Only users with these
  credentials can access a database that requires basic password authentication.
- Data transmitted between the user and the Sametime server (including the name
  and password) is not encrypted.
- Users are identified in the maintenance log files.

Basic password authentication identifies users, but it does not prevent
unauthorized users from listening to network transmissions or gaining server
access by guessing passwords. For information on using Secure Sockets Layer
(SSL) to encrypt the data that passes over the Web browser connection to the
Sametime server, see About SSL and Sametime.

Using the Default entry or individual names in database ACLs

When basic password authentication is enabled for a database, browser clients are
authenticated when they attempt to open a database. For example, a Web browser
user might be authenticated when selecting the “Attend a Meeting” link from the
Sametime server home page to access the Sametime Meeting Center database
(stconf.nsf).

The Sametime server challenges the user to supply a valid name and password
and then verifies that the user’s response matches the information stored in the
user’s Person document in the Domino Directory (or LDAP directory if you have
configured Sametime to operate with an LDAP directory). Authentication succeeds
if the user name and password provided by the user matches the user name and
password in the directory and:

- The user is listed individually or as a member of a group in the database ACL.
  or
- The Anonymous entry is set to No Access while an access level is specified for
  the Default entry in the ACL. Using this method allows you to require users to
  authenticate but prevents you from having to add individual entries for every
  user and group in the ACL.

When the Anonymous entry in the database ACL is set to No Access, users are
presented with a logon prompt when they attempt to access the database.

Users must enter the user name and Internet password at the logon prompt. Users
that are successfully authenticated are then provided with the access level that is
specified for the Default entry in the database ACL.
If both the Anonymous entry and the Default entry in the database ACL are set to No Access, a user must be listed in the ACL individually or as part of a group to access the database. Setting the Anonymous and Default entries to No Access provides the strictest control over access to the database because only users and groups that are listed in the ACL are allowed to access the database.

An individual name receives precedence over the Default entry. If a user’s name is entered in a database ACL and provided with an access level, the user receives the access level assigned to the user name entry in the database. Only users who are not listed individually in the database ACL receive the Default access level.

**Note:** If the Anonymous entry does not exist in the database ACL, the Default entry in the ACL must be set to “No access” to require basic password authentication to the database. When the Anonymous entry does not exist in the database ACL, anonymous users can access the database and receive the access level assigned to the Default entry in the database. If the Anonymous entry exists in the ACL and is assigned the "No access" access level, users are authenticated when accessing the database and receive the access level specified for the Default entry in the ACL.

**Setting up basic password authentication in a database Access Control List (ACL)**

To require users to specify a valid name and password when accessing a database on the Sametime server:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select LDAP Directory.
4. Select a database from the list.
5. Click the Advanced button.
6. Set the "Maximum Internet name & password" access to Manager, which is the maximum access level.
   
   **Note** The "Maximum Internet name & password" setting on the advanced panel of each database Access Control List (ACL) specifies the maximum database access level granted to Web browser clients. This setting overrides higher individual access levels set in the ACL. For example, if you set the "Maximum Internet name & password" to Author and assign Manager access to the Anonymous entry in the database ACL, anonymous users will only have Author access to the database. Alternatively, if you set the "Maximum Internet name & password" to Manager and assign Reader access to the Anonymous entry in the database ACL, anonymous users will only have Reader access to the database.
7. Click the Access button.
8. Select the Anonymous entry, and then select No Access in the Access box.
   
   If the Anonymous entry does not exist, you must create it. Use the following procedure to create an Anonymous entry and assign the No Access level to the entry:
   
   • Click Add.
   • Type Anonymous in the dialog box and click OK.
   • Select the Anonymous entry, and then select No Access in the Access box.
9. Select the Default entry. You can either set an access level for the Default entry, or set the Default entry to No Access.
   - If you specify an access level for the Default entry other than No Access, all users are required to authenticate when accessing the database. Each authenticated user receives the access level you have specified for the Default entry. It is not necessary to enter individual names or groups in the ACL. After selecting an access level for the Default entry, click Submit. You have finished the procedure required to set up basic password authentication in a database ACL. Skip the remaining steps.
   - If you select No Access for the Default entry, you must enter individual user names or group names in the ACL. Only the names and groups you enter can access the database. Complete steps 10 and 11 to add users to the ACL.

10. Click the Add button to add user names or group names to the ACL. Click OK after adding each name.

11. Click Submit.

---

**Authentication by token using LTPA and Sametime tokens**

Sametime uses authentication by token to authenticate connections that occur after a user has authenticated to Domino once using password authentication. Authentication by token prevents a user from having to re-enter authentication credentials when accessing different servers or using Sametime Web clients or Domino applications that connect to a Sametime server.

The Sametime server includes two separate security features capable of generating the authentication token used by Sametime:

- **Domino Single Sign-On (SSO) authentication feature** - The Domino SSO feature must be enabled on a Sametime 7.0 server.
  
  If the Domino SSO feature is not enabled on the Domino server when you install Sametime, the Sametime installation automatically enables and configures the Domino SSO feature. In some environments, you might need to alter the default SSO configuration provided by the Sametime installation. For more information, see [Altering the Domino Web SSO configuration following the Sametime server installation](#).

  The end user must enter the fully qualified domain name of the Sametime server (for example, sametimeserver.meetings.acme.com) in the Web browser URL locator when accessing the Sametime server to authenticate successfully using SSO.

  If your Sametime environment includes only Sametime 3.0 (or higher) servers, and you do not use Sametime TeamRoom or Discussion databases that were available with earlier Sametime server releases, only the Domino SSO feature is required to support authentication by token.

  If your Sametime environment includes Sametime 3.0 (or higher) servers that interoperate with Sametime servers from releases earlier than Sametime 3.0, both the Domino SSO feature and the Secrets and Tokens databases must be supported on the Sametime 7.0 server to enforce authentication by token.

  Sametime includes a custom logon form for the SSO feature. This custom logon form can be used in place of the default SSO logon form. The custom logon form is presented to the user the first time the user accesses a database on the server that requires basic password authentication.

- **Secrets and Tokens authentication databases** - Sametime server releases earlier than Sametime 3.0 used only the Secrets and Tokens authentication databases to
create authentication tokens. When Sametime 7.0 operates in environments that include servers from Sametime releases earlier than Sametime 3.0, the Sametime 7.0 server supports both the Domino SSO feature and the Secrets and Tokens authentication databases.

A Sametime 7.0 server supports Secrets and Tokens authentication by default. The following are required to support Secrets and Tokens authentication:

- The Secrets and Tokens databases must be present on the server following a Sametime 7.0 server installation.
- The "Allow users to authenticate using either LTPA token or Sametime Token (stauths.nsf and stautht.nsf)" option must be selected in the Configuration-Community Services-General settings of the Sametime Administration Tool.

Both conditions above exist on a Sametime 7.0 server following the server installation, so no additional procedures are required to support Secrets and Tokens authentication following the installation. However, if you have enhanced security by enabling the SametimeSecretsGenerator agent in one Secrets database on one Sametime server in your community, you must ensure that this Secrets database is replicated to all Sametime servers in the community. For more information, see [Replicating the Secrets database (optional)]

**Authentication by token using the Domino Single Sign-On (SSO) feature**

The Domino Single Sign-On (SSO) feature must be enabled on the Sametime 7.0 server. This feature creates Lightweight Third Party Authentication (LTPA) tokens that enable Web browser users to log in a single time to access multiple Sametime, Domino, or IBM WebSphere® servers that are in the same DNS domain. This capability is called "single sign-on."

Sametime also uses LTPA tokens to authenticate connections from Sametime clients to the Community Services, Meeting Services, and Broadcast Services on the Sametime server. These clients are Java applets and include the Meeting Room client, and Broadcast client.

**Note:** Sametime also requires users to present an authentication token when attending an instant meeting. Client applications generate this token from the user’s home Sametime server. Users with Sametime 2.5 (or earlier) home Sametime servers will present Sametime tokens (generated from the Secrets and Tokens databases) when connecting to instant meetings started on a Sametime 7.0 server. For this reason, Sametime 7.0 servers operating in Sametime environments that include Sametime servers from previous releases must also support the Secrets and Tokens databases for authentication by token.

Authentication by LTPA token occurs after a user has already authenticated once using password authentication. For example, authentication by token on a Sametime server might occur as follows:

1. A user accesses a Sametime Meeting Center database that requires authentication or clicks the "Log onto Sametime" link in the Sametime Meeting Center.

**Note** To successfully authenticate, the end user must enter the fully qualified domain name of the Sametime server (for example, sametimeserver.meeting.acme.com) in the Web browser URL locator when accessing the Sametime server.
2. An SSO logon form appears, and the user enters a valid user name and password from the Domino Directory (or LDAP directory) to authenticate. **Note** Sametime provides a custom Sametime SSO logon form that can be enabled by the administrator. If the custom logon form is not enabled, the standard Domino SSO logon form displays to the user.

3. After a successful authentication, the Domino Single Sign-On (SSO) feature generates an LTPA token containing the user’s authentication information and passes the token to the user’s Web browser in a cookie. The user’s Web browser must have cookies enabled to accept the LTPA token.

4. The user attends a meeting, and the Meeting Room client loads in the user’s Web browser.

5. The Meeting Room client connects to the Meeting Services and Community Services and passes the LTPA token to Sametime. The Meeting Services and Community Services connections are authenticated using the LTPA token. The user is not required to re-enter authentication credentials to authenticate these connections.

The same LTPA token described above can be used to authenticate the user when the user accesses other Sametime, Domino, or WebSphere servers in the same DNS domain during a single Web browser session. The other Sametime, Domino, or WebSphere servers must also support the SSO feature (that is, the servers must accept LTPA tokens).

If the Domino SSO feature is not enabled when you install Sametime, the Sametime installation automatically enables and configures the Domino SSO feature. In some environments, it may be necessary to alter the SSO configuration following the Sametime server installation. For more information, see **Altering the Domino Web SSO configuration following the Sametime server installation**.

### Altering the Domino Web SSO configuration following the Sametime server installation

The Sametime installation automatically enables and configures the Domino SSO feature on the Domino server. In some cases, it may be necessary to alter the default configuration of the Domino SSO feature following the Sametime server installation.

This topic discusses the following issues pertaining to the Sametime installation and the Domino SSO feature:

- **SSO configurations performed by the Sametime server** - This section explains how the Sametime installation configures the Domino Web SSO feature. You can use this information to determine if it is necessary to alter the default SSO configuration following a Sametime server installation.

- **Altering the SSO configuration** - This section explains the most common reasons for altering the SSO configuration following the Sametime server installation. In multiple Sametime server environments, it is frequently necessary to add the Domino server names of Sametime servers to the Domino Web SSO Configuration document.

- **Viewing and editing the Domino Web SSO configuration document** - This section explains how to edit the Domino Web SSO configuration document in the Domino Directory. This document contains the parameters for the Web SSO configuration that you may need to change.
• **Sametime includes** a custom SSO logon form. See [Using the Sametime custom logon form for SSO](#) for information about enabling this form following the Sametime server installation.

**Note:** If for some reason it is necessary to manually enable the Domino SSO feature, you can use the procedures described in [Manually enabling the Domino SSO feature](#). You can also review these procedures to understand all configurations that are required to support SSO for the Sametime server.

## SSO configurations performed by the Sametime installation

The Sametime installation enables the Domino SSO feature and performs the SSO configurations described below. The Sametime installation:

• Generates an LTPA token named LtpaToken. This token (or cookie) is used to authenticate Web browser and Sametime client connections to the Sametime server.

• Creates a Web SSO Configuration document and populates the following fields in the Web SSO Configuration document:
  - DNS Domain - To populate the DNS Domain field, the installation determines the fully-qualified domain name of the Sametime server machine and then subtracts the hostname value from the fully-qualified domain name. For example, if the installation determines the fully qualified name of the Sametime server is "Sametimeserver.east.acme.com," the installation writes ".east.acme.com" in the DNS Domain field. The LTPA token is then valid for the servers that belong to the DNS domain specified in the DNS Domain field.
  - Expiration (minutes) - This field specifies the length of time for which the LTPA token is valid. This value is 30 minutes by default. You may want to provide a longer value for the token expiration. Lotus software recommends a setting of 120 minutes.
  - Domino Server Names: Each Domino/Sametime server that can accept the SSO token must be listed in the Domino Server Names field. By default, the installation writes only the name of the Domino server on which Sametime is installed in this field. It may be necessary to add the names of all other Domino/Sametime servers in the community to this field. For more information, see [Altering the SSO configuration](#).
  - Alters the Sametime/Domino server Server document. The installation changes the Internet Protocols-Domino Web Engine-Session authentication field in the Server document to the value "Multiple servers (SSO)." The Server authentication field must have the "Multiple servers (SSO)" value even if your Sametime community uses only one Sametime server. If the "Multiple server (SSO)" value is not selected, the SSO feature will not function properly for Sametime.
  - Automatically configures the Sametime server to use the Sametime custom logon form for SSO. To enable the custom logon form, the Sametime installation:
    - Creates a Domino Configuration database named domcfg.nsf in the root data directory of the Domino server.
      **Note:** If a domcfg.nsf database already exists on the Domino server when Sametime is installed, the Sametime installation overwrites the existing domcfg.nsf database.
    - Creates a "Mapping a Login Form" document in the domcfg.nsf database.
    - Populates the following fields in the Mapping a Login Form document:
      - Target database filename - This field is set to the value "stcenter.nsf."
Target form name - This field is set to STLogonForm.nsf.

The configurations described above ensure that the custom logon form named “STLogonForm.nsf” displays to users when users authenticate with the server.

**Altering the SSO configuration**

The default configuration outlined above meets the basic requirements necessary for a Sametime server to support SSO. In some cases, it may be necessary for the administrator to alter the "DNS Domain" field or the "Domino Server Names" field of the Domino Web SSO Configuration document following the Sametime server installation.

- **Altering the DNS Domain field** - The Sametime installation may not always accurately detect the fully-qualified domain name of the Sametime server machine. If this problem occurs, the DNS Domain field may not specify the appropriate DNS domain. The administrator might need to manually edit the Domino Web SSO Configuration document to add the appropriate entry in the DNS Domain field of the Domino Web SSO Configuration document. Follow the instructions in "Viewing and editing the Domino Web SSO Configuration document" below to manually edit the document.

- **Altering the Domino Server Names field** - If the Sametime community consists of multiple Sametime/Domino servers, the Domino server names of all of the Sametime/Domino servers in the Sametime community must exist in the "Domino Server Names" field of the Domino Web SSO Configuration document. By default, the installation writes only the name of the Domino server on which Sametime is installed to this field. If you have multiple Sametime servers, it may be necessary to manually open the Domino Web SSO configuration document and enter the names of the Domino/Sametime servers in the "Domino Server Names" field.

For example, if you have Sametimeserver1/East/Acme and Sametimeserver2/East/Acme in your Sametime community, and you install Sametimeserver3/East/Acme, only Sametimeserver3/East/Acme is written to the Domino Server Names field during the Sametime installation. The administrator may need to open the Domino Web SSO Configuration document and manually enter the names Sametimeserver1/East/Acme and Sametimeserver2/East/Acme in the "Domino Server Names" field on the Domino Web SSO Configuration document on Sametimeserver3/East/Acme to ensure that all servers in the community are entered in this field. To manually open the Domino Web SSO Configuration document, see "Viewing and editing the Domino Web SSO Configuration document" below.

Note that in multiple server environments, the Domino Directory may already be replicated to the Domino server at the time the Sametime server is installed. If the Domino Directory already exists on the server and contains a Domino Web SSO configuration document, the Sametime installation will not attempt to alter the existing configuration in any way. In this case, the existing Domino Web SSO configuration document may already contain the names of the existing servers in the community and it may be necessary to add the name of the newly installed Sametime server to the Domino Web SSO configuration document.

For example, the names Sametimeserver1/East/Acme and Sametimeserver2/East/Acme may already exist in the Domino Web SSO configuration document in the Domino Directory on the server reserved for the Sametimeserver3/East/Acme installation. Since the Sametimeserver3/East/Acme installation does not alter an existing SSO configuration, that server name will not appear in the Domino Web SSO Configuration document following the Sametime server installation. In this scenario, it is necessary to open the Domino Web SSO configuration document in the Domino Directory on Sametimeserver3/East/Acme and manually enter
"Sametimeserver3/East/Acme" in the "Domino Server Names" field. All other parameters in the existing Web SSO Configuration document should be valid for the newly-added server.

**Viewing and editing the Domino Web SSO Configuration document**

To view or edit the Web SSO configuration document that is created by the Sametime installation, do the following:

1. From a Lotus Notes client, open the Domino Directory on the Sametime server.
2. Choose the Configuration - Web - Web Configurations view.
3. In the right-hand pane, select the twistie to display the document under "Web SSO Configurations."
5. Click the Edit button to put the document in edit mode.
6. Edit the appropriate field (for example, the DNS Domain or Domino Server Names field).
7. Click Save and Close after editing the document.

**Manually enabling the Domino SSO feature**

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature. This procedure is identical to the procedure used to enable the SSO feature on a Domino server. After manually enabling the feature, you can configure the server to use the Sametime custom SSO logon form.

Generally, the Domino SSO feature will be enabled by default during the Sametime installation and it is not necessary to manually enable the feature. For more information, see [Altering the Domino Web SSO feature following the Sametime server installation](#).

To enable the Domino SSO feature on the Sametime 7.0 server:

1. **Create a Web SSO Configuration document in the Domino Directory**
2. **Enable SSO and Name & Password authentication in the Server document**
3. **Start the HTTP task on the SSO-enabled server**

**Using the custom Sametime SSO logon page**

After enabling the Domino SSO feature, follow the procedure described in [Using the custom Sametime SSO logon page](#) to use the custom Sametime SSO logon form.

**Create the Web SSO Configuration document in the Domino Directory**

This procedure is the first of three required to manually enable the Domino SSO authentication feature on a Sametime 7.0 server.

In this procedure you create a Web SSO document that specifies the servers participating in the shared authentication, the time-out value for the cookie containing the LTPA access token, and the encrypted secret used to create the cookie.

2. Select Configuration - Servers - All Server Documents.
3. Select the Web pull-down menu button from the task bar.
4. Select Create Web SSO Configuration.
5. In the document, select the Keys pull-down menu button.
6. Select Create Domino SSO Key.
   
   **Note** The Import WebSphere LTPA Keys option is usually used to enable a WebSphere server to communicate with a Domino server. To enable a WebSphere server to communicate with a Domino server, you must export the LTPA keys from the WebSphere server and import the LTPA keys to the Domino server. See the WebSphere Information Center documentation for details.

7. Configure the Token Expiration field. Note that a token does not expire based on inactivity; it is valid only for the number of minutes specified from the time of issue. The token is also valid only for a single browser session. Lotus software recommends an expiration value of 120 minutes.
   
   **Note** Generally, the expiration value should reflect the average length of a Sametime meeting in your environment. Setting a high value may create a security risk. If the LTPA token is intercepted by an attacker, the attacker may use the token to illegally gain access to the Sametime server until the token expires. Setting up the Domino server to support SSL for Web browser connections makes provides the highest level of security against attempts to intercept LTPA tokens.

8. In the DNS Domain field, enter the DNS domain (for example, lotus.com or meetings.acme.com) for which the tokens will be generated. The servers enabled for SSO must all belong to the same DNS domain. This field is required.

   When users access the Sametime 7.0 server, they must enter the fully qualified domain name of the Sametime server for authentication to be successful (for example, sametimeserver.meetings.acme.com).

9. In the Server Names field, enter the servers that will be participating in SSO. Generally, this field should contain the Domino hierarchical names of all Sametime servers in your environment. You can browse and select the server names from the Domino Directory.

   **Note** Groups and wildcards are not allowed in the field.

10. Select "Save and Close" to save the Web SSO Configuration document. The document will appear in the Web Configurations view. This document will be encrypted for the creator of the document, the members of the Owners and Administrators fields, and the servers specified in the Server Names field.

**Next step**

Next, **enable SSO and "Name & Password" authentication** in the Server document.

**Enable SSO and “Name & Password” authentication in the Server document**

This procedure is the second of three required to manually enable the Domino SSO authentication feature on a Sametime 7.0 server. Use this procedure to enable SSO and “Name & Password” authentication in the Server document of the Sametime server for which you are enabling the Domino SSO feature.

1. In the Configuration - Servers - All Server Documents view of the Domino Directory, double-click the name of the Sametime server to open the Server document.
2. Select Edit Server to put the Server document in edit mode.
3. Select the Ports tab.
4. Select the Internet Ports tab.
5. Select the Web tab (if it is not displayed by default).
6. For the HTTP TCP/IP port Authentication Options, select Yes in the "Name & Password" field.
7. Select the Internet Protocols tab.
8. Select the Domino Web Engine tab.
9. In the "HTTP Sessions" section, select "Multiple server (SSO)" in the "Session authentication" field.
   
   **Note** You must select the "Multiple server (SSO)" value even if your environment includes only a single Sametime server.
10. Click "Save and Close" to save the Server document.

**Next step**

Next, [start (or restart) the HTTP task on the SSO-enabled server](#)

**Start (or restart) the HTTP task on the SSO-enabled server**

This procedure is the last of three required to manually enable the Domino SSO authentication feature on a Sametime 7.0 server.

To start the HTTP task on the SSO-enabled server:

1. Open the Domino console.
2. Start the HTTP server, or stop and restart the HTTP server if it is already running.
   - Use the Tell HTTP Quit command to stop the HTTP server.
   - Use the Load HTTP command to start the HTTP server.
3. On the Domino console, the following message should appear:
   HTTP: Successfully loaded Web SSO Configuration
4. If a server enabled for SSO cannot find a Web SSO Configuration document or is not included in the Server Names field (and thus cannot decrypt the document), then the following message should appear on your server’s console.
   HTTP: Error Loading Web SSO configuration. Reverting to single server session authentication.

**Next step**

Next, Lotus software recommends using the custom Sametime SSO logon form. If you do not use this logon form, users will see the default Domino SSO logon form the first time they access a database on the server that requires authentication.

**Note:** Authentication by token does not occur if you allow anonymous access to the Sametime server and all its databases.

To configure the Sametime server to use the custom Sametime SSO logon form, see [Using the Sametime custom logon form for SSO](#)
Using the Sametime custom logon form for SSO

The Sametime installation automatically configures the Sametime server to use the Sametime custom logon form for SSO. The Sametime installation performs the following configurations to enable the custom logon form. The Sametime installation:

1. Creates a Domino Configuration database named domcfg.nsf in the root data directory of the Domino server on which Sametime is installed. This database is created from the domcfg5.ntf template available with the Domino server.
2. Creates a "Mapping a Login Form” document in the domcfg.nsf database.
3. Populates the following fields in the Mapping a Login Form document:
   - Target database filename - This field is set to the value “stcenter.nsf.”
   - Target form name - This field is set to STLogonForm.nsf.

The configurations described above ensure that the custom logon form named “STLogonForm.nsf” displays to users when users authenticate with the server.

If a database named domcfg.nsf exists on the Sametime server when Sametime is installed, the administrator must manually enable the custom logon form. This procedure is described below.

Manually enabling the custom logon form.

Follow the procedure below to manually enable the Sametime custom logon form for SSO. The custom logon form displays when the user accesses the first database on the server that requires authentication or selects the “Log on to Sametime” link in the Sametime Meeting Center.

**Note:** The custom logon form exists in the Sametime server home page database (stcenter.nsf). If you want to require users to authenticate when accessing the server, you should allow anonymous access to the Sametime server home page (stcenter.nsf) and require authentication to the Sametime Meeting Center database (stconf.nsf). With this arrangement, users access the server home page anonymously and are presented with the SSO logon form when attempting to create or attend a meeting.

To use the Sametime custom logon form for SSO, you must configure settings in the Domino Configuration database (domcfg.nsf) provided with the Domino server on which Sametime is installed.

To use the Sametime custom logon form for SSO:

1. Verify that the Sametime server has a Domino Configuration database named domcfg.nsf.
   **Note** If your server includes an existing domcfg.nsf database, but you do not want to use that database you can delete the existing domcfg.nsf database and create a new one. To create a new domcfg.nsf database, use the Domino Configuration (R5) template (domcfg5.ntf) available with a Domino server. When creating the new database, you must select the "Show advanced templates" option to access the domcfg5.ntf template.
2. If necessary, copy the domcfg.nsf Domino Configuration database to the root data directory of the Domino server on which Sametime is installed (for example C:\Lotus\Domino\Data directory).
3. From a Lotus Notes client, open the Domino Configuration database.
5. Under Site Information, accept the default of All Web Sites/Entire Server.

Chapter 13. Managing Security 427
6. In the "Target database filename" field, enter stcenter.nsf.
7. In the "Target form name" field, enter STLogonForm.

Required ACL settings for the Sametime Center database (stcenter.nsf)
The Sametime Center database (stcenter.nsf) must meet the following ACL requirements for the custom logon form to operate properly.

- In the Advanced options of the stcenter.nsf ACL settings, the "Maximum Internet name & password" field must allow at least Reader access. If either Depositor or No Access are selected, the logon form will not appear.
- In the Basics options of the stcenter.nsf ACL settings, anonymous users must have an access level of Reader or higher. If the access level provided for anonymous users is less than Reader, the logon form will not appear. The "Write public documents" and "Read public documents" options should also be selected.

Authentication by token using Secrets and Tokens databases
To authenticate by token, the Sametime 7.0 server can accept an authentication token created by the Secrets and Tokens authentication databases, the Domino Single Sign-On (SSO) feature, or both. The Sametime 7.0 server can also generate tokens using the Secrets and Tokens authentication databases or the Domino SSO feature.

If the Sametime 7.0 server is operating in an environment that includes Sametime servers from releases earlier than Sametime 3.0, or if Domino databases enabled with Sametime technology (such as the Sametime Discussion and TeamRoom databases that were available with earlier releases) are used in your environment, the Sametime server must support both the Secrets and Tokens authentication databases and the Domino SSO authentication feature.

The Sametime 7.0 server is set up to support Secrets and Tokens authentication by default. The basic requirements for this authentication system are:

- The Secrets (stauths.nsf) and Tokens (stautht.nsf) databases must exist on the Sametime server. These databases are created during the Sametime server installation.
- The "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" option must be selected in the Sametime Administration Tool. (This option is selected by default.)

Note that previous releases of Sametime allowed an administrator to enhance the level of security provided by the Secrets and Tokens databases by enabling the SametimeSecretsGenerator agent in one Sametime Secrets database (stauths.nsf) on one Sametime server in the Sametime community. If you enable the SametimeSecretsGenerator agent on one Secrets database on one Sametime server, that Secrets database must be replicated to all Sametime servers in the community. If your environment includes Sametime servers from previous releases and you are currently replicating a Secrets database to all of the servers in your environment, you must also replicate that Secrets database to the Sametime 7.0 servers.

There are two procedures associated with ensuring the Secrets and Tokens authentication databases on the Sametime 7.0 server are functioning properly:

1. If necessary, select the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" option in the Sametime Administration Tool. (This option is selected by default.)
2. **Replicating the Secrets and Tokens databases** (optional) - This step is necessary only if you have deployed Domino databases enabled with Sametime technology (such as Sametime TeamRoom and Discussion databases) or if you have enhanced security by enabling the SametimeSecretsGenerator agent in the Secrets database.

**Selecting the “Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)” option**

This procedure is the first of two associated with setting up the Secrets and Tokens authentication system on a Sametime 7.0 server.

**Note:** This procedure might not be necessary as the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)” setting is enabled by default following the server installation.

The “Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)” setting must be enabled in the Sametime Administration Tool to enable the Sametime server to accept both the LTPA and Sametime Tokens. This setting must be set consistently on all Sametime 7.0, 6.5.1, 3.1 and 3.0 servers in your environment; if you enable this setting on one Sametime server, you must enable it on all Sametime servers in your environment. If you disable it on one Sametime server, you must disable it on all Sametime servers in the environment.

To enable this setting:
1. From the Sametime server home page, click the "Administer the Server” link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Community Services.
4. Select the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)” option.
5. Click the Update button and restart the server for the change to take effect.

**Next step**

You have the option of **replicating the Secrets database** to enhance security.

**Replicating the Secrets and Tokens databases (optional)**

This topic discusses the second of two procedures associated with setting up the Secrets and Tokens authentication system on a Sametime server.

The Secrets and Tokens databases exist on every Sametime server. If you have installed multiple Sametime servers, you can enable the SametimeSecretsGenerator agent in the Secrets database. Enabling the SametimeSecretsGenerator agent is an optional procedure that increases security against outside attacks.

If you enable the SametimeSecretsGenerator agent, only one Secrets database should be used for all Sametime servers in the environment. You should replicate the Sametime Secrets database in which you have enabled the SametimeSecretsGenerator agent to all Sametime servers in the environment. Create a replication schedule for the Secrets database in which you have enabled the SametimeSecretsGenerator agent to ensure it replicates at regular intervals. Delete all other copies of the Secrets database from all Sametime servers in the environment. For more information, see **Integrating a Sametime server into an existing Sametime community**.
Do not replicate the Tokens database to the other Sametime servers. The replicated Secrets database can work with the Tokens database that exists on each Sametime server by default following the server installation.

If you do not enable the SametimeSecretsGenerator agent in any Secrets database on any Sametime server, it is not necessary to replicate the Secrets database. If you do not enable the SametimeSecretsGenerator agent, administration is simpler because no replications or replication schedules are required, but the security level is not as high.

**Security recommendations for self-registration**

The Sametime server includes a self-registration feature available from the Register link on the Sametime server home page. From the Register link, any anonymous Web browser user can create a Person document that contains a user name and Internet password in the Directory on the Sametime server. These credentials on the Person document enable a Web browser user to authenticate with the Sametime server.

**Note:** Self-registration is not available if you have configured the Sametime server to access an LDAP directory on a third-party server. Users cannot register themselves in an LDAP directory on another server.

The administrator has the option of allowing or not allowing self-registration. To turn self-registration on or off, use the "Allow people to register themselves in the Domino Directory" setting in the Directory options available from the Sametime Administration Tool.

Allowing self-registration enables any anonymous user to access Sametime Connect to chat or conduct instant meetings with other members of the Sametime Community. A self-registered user can also authenticate to access protected areas of the server with a Web browser (including the Sametime Meeting Center).

Follow these recommendations to secure your server if you allow users to self register:

- In the ACL of the Directory (names.nsf) on the Sametime server, set the Anonymous entry to No Access. This setting prevents anyone who has not authenticated from accessing the Directory. Some activities of authenticated users are recorded in the Notes Log.
- In the ACL of the Directory on the Sametime server, set the Default entry to No Access. This setting protects privacy, which might be a concern if your Sametime server is accessible by the general public. The initial setting for the Default entry in the Directory ACL is Reader. Setting the Default entry to No Access prevents users from browsing the Directory and viewing the user names in the Directory.
- Verify that the Sametime Development/Lotus Notes Companion Products ID has the appropriate settings in the ACL of the Directory on the Sametime server.

Self-registration is supported by the Self-Registration database (streg.nsf) on the Sametime server. When a user clicks the Register link from the Sametime server home page, the user is accessing the Self-Registration database. This database contains agents that access the Directory (names.nsf) on the Sametime server to create a Person document for the user who self registers. These agents also access the Directory for password changes. The Directory must have the file name names.nsf for these agents to access the Directory.

The agents in the Self-Registration database are signed by the Sametime Development/Lotus Notes Companion Products ID. For self-registration to work
Encryption and meeting passwords

The Configuration - Meeting Services options of the Sametime Administration tool include two options that the administrator can select to enhance the security of meetings:

- **Encrypt all Sametime meetings** - When this option is selected, all T.120 screen-sharing and whiteboard data and audio/video data that passes between the Sametime Meeting Room or Sametime Broadcast client and the Sametime server during any meeting is encrypted. The meeting data is encrypted using RC2 128-bit encryption. Encrypted meeting data might be transmitted more slowly than unencrypted meeting data.

  If this option is not selected, the end user has the option of encrypting or not encrypting meeting data when creating a new meeting. For more information on this setting, see [Encrypting all Sametime meetings](#).

**Note:** When any Sametime 2.5 or higher client accesses a Sametime 7.0 server, all chat data is encrypted regardless of whether the "Encrypt all meetings" setting is selected. All chat activity between Sametime 2.5 or higher clients and the Sametime 7.0 server is always encrypted. Sametime clients from releases earlier than 2.5 contain settings that enable users to conduct unencrypted chats. If a Sametime client from a release earlier than 2.5 connects to a Sametime 7.0 server, the chat is either encrypted or unencrypted depending on the client settings.

For information on using Secure Sockets Layer (SSL) to encrypt information passing between the Web browser and the Sametime server when the Web browser makes the initial connection to the server, see [About SSL and Sametime](#).

- **Require all scheduled meetings to have a password** - This option forces the end user to specify a meeting password for a meeting when creating a new meeting. A meeting password is valid only for one meeting and applies only to
the meeting. The user creating the meeting password must notify other participants about the meeting password before the meeting starts. The meeting password is unrelated to the Internet password required to authenticate with databases on the Sametime server. For more information on this setting, see Requiring all scheduled meetings to have a password.

Note: An end user can also restrict access to a meeting by entering the names of users in a Restrictions list when creating a meeting. Only users who are selected in the Restrictions list are allowed to access the meeting. This level of meeting security is controlled by the end user creating the meeting.

**Using SSL with Sametime**

The Secure Sockets Layer (SSL) protocol can be used to encrypt Web browser connections to Sametime or to encrypt connections between Sametime and an LDAP server.

**Encrypting Web browser connections with SSL**

Sametime installs on a Domino server and uses the HTTP server provided with the Domino server. To encrypt Web browser connections to the Sametime server with SSL, you must configure the Domino HTTP server to support SSL. If the Domino HTTP server supports SSL, Web browser connections to Sametime are also encrypted with SSL.

To encrypt Web browser connections to the Sametime server, you must configure the Domino HTTP server to support SSL. The procedure required to configure the Domino HTTP server to support SSL varies depending on the operating system on which Sametime runs. To encrypt Web browser connections to the Sametime server, perform the procedure below that is appropriate for your environment:

- Setting up SSL for Sametime on Windows
- Setting up SSL for Sametime on Solaris/AIX

**Ensuring access to Sametime servlets when Domino requires SSL for all connections**

When setting up a Domino server to support SSL, the administrator has the option of forcing all HTTP connections to the server to use SSL. If a Domino server is configured in this way, you must configure the Sametime server to support SSL for HTTP connections to servlets on the Sametime server. If you do not configure the Sametime server to support SSL access to its servlets, the Sametime server will not function properly and users will be unable to access the server.

For more information about this procedure, see Ensuring Sametime servlet access when Domino requires SSL for all connections.

**Encrypting connections to an LDAP server**

If you have configured Sametime to connect to an LDAP directory on an LDAP server, you can also use SSL to encrypt the connections between Sametime and the LDAP server. For more information, see Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server.
Setting up SSL for Sametime on Windows

Use these instructions to encrypt Web browser connections to the Domino HTTP server if your Sametime server operates on the Windows operating system:

1. Set up the Domino HTTP server to support SSL (Windows)
2. Use IKeyMan to create a key store file on the Sametime server
3. Import the SSL trusted root or SSL server certificate into the key store database on the Sametime server
4. Modify the Sametime.ini file

Set up the Domino HTTP server to support SSL (Windows)

Setting up the Domino HTTP server to support SSL is the first of four procedures required to set up SSL for a Sametime server on Windows.

Use the procedures described in the Security chapter of the Domino server administration documentation to set up a Domino server to support SSL for HTTP connections. These procedures are summarized below.

To set up SSL on a Domino server:

1. Set up the Server Certificate Admin application (CERTSRV.NSF), which Domino creates automatically during server setup.
2. Create a server key ring file to store the server certificate.
3. Request an SSL server certificate from the CA.
4. Merge the CA certificate as a trusted root into the server key ring file.
5. The CA approves the request for a server certificate and sends notification that you can pick up the certificate.
6. Merge the approved server certificate into the key ring file.
7. Configure the port for SSL.

The Domino administration documentation that describes these procedures in detail is available both on the Domino server and from the IBM Lotus documentation library at www.lotus.com/ldd/doc.

When you perform the procedures above, be sure to save and have available a copy of one of these two SSL certificates:

- The trusted root certificate that is merged into the server key ring file in step 4.
- The server certificate that is merged into the key ring file in step 6.

In a subsequent procedure, you must add one of these certificates to a key store database used by the Sametime server.

Next step:

Use IKeyMan to create a key file on the Sametime server

Use IKeyMan to create a key store file on the Sametime server (Windows)

Creating the IBM IKeyMan key store file is the second of four procedures required to set up SSL for a Sametime server on Windows.

In this procedure, you use the IKeyMan program provided on the Sametime server to create a key store file named "stkeys.jks and store this file in the Sametime
installation directory. In this example, the Sametime installation directory is the default installation directory of C:\Program Files\Lotus\Domino.

To create a key database on the Sametime server:

1. Start the IKeyMan program from a command prompt on the Sametime server. The IKeyMan program resides in the "jvm" sub-directory of the Sametime server installation directory (default C:\Program Files\Lotus\Domino). Use the command "java com.ibm.gsk.ikeyman.Ikeyman" to start the IKeyMan program. For example, the command string to start IkeyMan might look like this: C:\Program Files\Lotus\Domino\jvm>java com.ibm.gsk.ikeyman.Ikeyman

2. From the menu bar, select Key Database File - New....

3. In the New window, complete these fields:
   - **Key database type:** - Accept the default of "JKS."
   - **File name:** - Enter the file name for the key database. The file name is at your discretion. This example assumes that you name the key database "stkeys.jks."
   - **Location:** - Enter the directory in which the "stkeys.jks" key database will be stored. The Location is at your discretion. This example assumes the key database is stored in the C:\Program Files\Lotus\Domino\jvm directory. Click OK after completing the fields in the New window.

4. In the Password prompt window, do the following:
   a. Type and confirm the password that will be used to access the stkeys.jks key database. The password is at your discretion.
   b. Check "Set expiration time?" And specify the number of days for which the password will be valid before it must be changed. If no expiration date is required, you can leave the "Set expiration time?" Field blank.
      In a production environment, it is recommended that you set an expiration date for the password for the highest level of security.
   c. Click OK.

5. Close the stkeys.jks key database file.

Next step:

**Import the SSL trusted root or SSL server certificate into the key store database on the Sametime server**

**Import the SSL trusted root or SSL server certificate into the key store database on the Sametime server (Windows)**

Importing the SSL trusted root certificate or SSL server certificates used by the Domino HTTP server is the third of four procedures required to set up SSL for a Sametime server on Windows.

Before beginning this step, make sure you have one of these certificates available. You were instructed to save one of these certificates earlier in this procedure

In this procedure, you must do one of the following:

- The SSL trusted root certificate imported into the Domino HTTP server key ring file
- The SSL server certificate imported into the Domino HTTP server key ring file

**Note:** In this procedure, you must import one of these certificates into the stkeys.jks database you have just created. Import the certificate as a signer certificate.
To import an SSL certificate to the IKeyMan key store file (stkeys.jks):

1. Start the IKeyMan program from a command prompt on the Sametime server. The IKeyMan program resides in the "jvm" sub-directory of the Sametime server installation directory (default C:\Program Files\Lotus\Domino). Use the command "java com.ibm.gsk.ikeyman.Ikeyman" to start the IKeyMan program. For example, the command string to start IkeyMan might look like this: C:\Program Files\Lotus\Domino\jvm> java com.ibm.gsk.ikeyman.Ikeyman

2. Choose Key Database File - Open.
   Browse to and select the "stkeys.jks" key database (or other database you have created to manage the SSL certificates on the WebSphere server).

3. Enter the password required to access the Stkeys.jks file.

4. In the Key database content area, select "Signer certificates."

5. Click the "Add" button.

6. In the "Add Cas certificate from a File" dialog box:
   • Verify that "Base64-encoded ASCII data" is selected as the Data type.
   • Browse to and select the SSL certificate you want to import.
     Click OK.

7. In the "Enter a Label" dialog box, provide a label for the certificate. This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program. Click OK.
   The certificate label will display in the Signer Certificates list.

Next step:

Modify the Sametime.ini file

Modify the Sametime.ini file (Windows)
Modifying the Sametime.ini file is the last of four procedures required to set up SSL for a Sametime server on Windows.

The Sametime.ini file on the Sametime server must contain the parameters that enable the Sametime servers to connect to the Domino HTTP server using SSL. You must use a text editor to edit the Sametime.ini file.

Follow these instructions to edit the Sametime.ini file in the Sametime installation directory on the Sametime/Domino server.

1. Open a text editor on the Sametime server.

2. Open the Sametime.ini file located in the Sametime server installation directory (the default directory is C:\program files\lotus\domino).

3. Locate the "ConfigurationPort=" setting. Make sure that the "ConfigurationPort=" setting, specifies the port on which the Domino HTTP server listens for SSL connections (default port 443). You may need to alter the ConfigurationPort setting to specify the Domino HTTP server SSL port. For example:
   ConfigurationPort=443

4. The following settings must exist in the Sametime.ini file. If necessary, manually add the following settings to the [Config] section of the Sametime.ini file. (At the bottom of the Config section, manually type these settings into the file):
[Config] ConfigurationSSLEnabled=javax.net.ssl.keyStore=
javax.net.ssl.trustStore=javax.net.ssl.keyStorePassword=
javax.net.ssl.trustStorePassword=

Use the instructions below to populate each of the fields in the Sametime.ini file:

- **ConfigurationSSLEnabled** - This setting should be set to true. An example value is:
  ConfigurationSSLEnabled=true.
- **javax.net.ssl.keyStore** - This setting must specify the complete file path, including the filename, of the IKeyMan database you have created on the Sametime server. For example:
  javax.net.ssl.keyStore=C:\program files\lotus\domino\stkeys.jks
- **javax.net.ssl.trustStore** - This setting must also specify the complete file path, including the filename, of the IKeyMan database you have created on the Sametime server. For example:
  javax.net.ssl.trustStore=C:\program files\lotus\domino\stkeys.jks
- **javax.net.ssl.keyStorePassword** - This setting must specify the password you provided for the IKeyMan database when you created the database. The example shown here assumes the password is "sametime." Alter the setting to reflect your password.
  javax.net.ssl.keyStorePassword=sametime
- **javax.net.ssl.trustStorePassword** - This setting must also specify the password you provided for the IKeyMan database when you created the database. The example shown here assumes the password is "sametime." Alter the setting to reflect your password.
  javax.net.ssl.trustStorePassword=sametime

5. Save the Sametime.ini file.
6. Restart the Domino server.

**Setting up SSL for Sametime on Solaris/AIX**

Use these instructions to encrypt Web browser connections to the Domino HTTP server if your Sametime server operates on the Solaris or AIX operating system:

1. **Create a certificate authority database**
2. **Enable SSL on the Domino server**
3. **Copy the text of the certificate stored in the Certificate Authority Key Ring**
4. **Transfer files to the server**
5. **Use IKeyMan to create a store key file**
6. **Modify the Sametime.ini file**

**Create a certificate authority database (Solaris/AIX)**

Creating a certificate authority database is the first of six procedures required to use SSL to encrypt Web browser connections to a Sametime server that runs on the Solaris or AIX operating system. In this procedure, you create a certificate authority database and use this database to create a certificate authority key ring and a server authority key ring. You also create a certificate for each of these key rings.

To create a certificate authority database:

1. Open a Lotus Notes client and use the advanced template named "Domino R5 Certificate Authority" to create a certificate authority database named "CA.nsf."
2. Open the CA.nsf database in the Notes client.
3. Click on "1. Create Certificate Authority Key Ring & Certificate." If you receive an error, close the CA.nsf database, reopen it, and then try this step again.
   Complete the following steps:
   a. Accept the default Key Ring file name - [CAKey.kyr].
   b. Enter the Key Ring Password and verify it.
   c. Set the "Key Size" to [1024].
   d. Enter the common name (a descriptive name such as "Servername CA"), organization, state/province and country.
   e. Click on the "Create Certificate Authority Key Ring" button.
4. Click on "2. Configure Certificate Authority Profile." Accept all defaults and click on "Save and Close."
5. Click on "3. Create Server Key Ring & Certificate" and complete the following steps:
   a. Accept the default key ring file name - [keyfile.kyr].
   b. Enter the Key Ring Password and verify it.
   c. Accept the default key size.
   d. Enter the CA Certificate Label; for example, "servername CA."
   e. Enter the common name (the fully-qualified DNS name of the server), organization, state/province and country.
   f. Click on the "Create Server Key Ring" button.
   g. Enter the password for the authority that you entered when you clicked on "1. Create Certificate Authority Key Ring and Certificate."

Next step:

Enable SSL on the Domino server (Solaris/AIX)

Enable SSL on the Domino server (Solaris/AIX)
Enabling SSL on the Domino server is the second of six procedures required to use SSL to encrypt Web browser connections to a Sametime server that runs on the Solaris or AIX operating system.

In this procedure, you configure settings on the Domino server Server document to enable SSL.
1. Using a Notes client, open the Domino directory (names.nsf).
2. Open the Server document for the Sametime server and follow the steps below.
   a. Go to Ports-Internet Ports.
   b. Ensure that the "SSL key file name" matches the default server key ring file name (keyfile.kyr) you created in the previous procedure.
   c. Set the "TCP/IP Port Status" to Disabled.
   d. Set the "SSL Port Status" to Enabled.
3. Click on "Save and Close."

Next step:

Copy the text of the certificate stored in the Certificate Authority Key Ring (Solaris/AIX)
Copy the text of the certificate stored in the Certificate Authority Key Ring (Solaris/AIX)

Copying the text of the certificate stored in the Certificate Authority Key Ring is the third of six procedures required to use SSL to encrypt Web browser connections to a Sametime server that runs on the Solaris or AIX operating system.

In this procedure, you copy the text of the SSL certificate stored in the Certificate Authority Key Ring file and paste it into a text document to create a copy of the certificate.

1. Open a Web browser and browse to http://servername/CA.nsf. (This URL is case sensitive.)
2. On the left, click on "Accept This Authority In Your Server." The certificate text appears on the right.
3. Copy the certificate text, including the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.
4. Use a text editor to create a new text file and paste the certificate text into the text file.
5. Insert a new line (carriage return) in the text file after the "END CERTIFICATE" line.
6. Save the text file as CA.txt.

Next step:

Transfer files to the server (Solaris/AIX)

Transferring files to the server is the fourth of six procedures required to use SSL to encrypt Web browser connections to a Sametime server that runs on the Solaris or AIX operating system.

In this procedure you use FTP to transfer files from their current locations to the Domino server data directory.

• Use FTP to transfer the keyfile.kyr and keyfile.sth files from the data directory of your Notes client to the data directory of your Domino server (for example, the /local/notesdata directory).
• Use FTP to transfer the CA.txt file you created in the previous procedure from its current location to the Domino server data directory.

Next step:

Use IKeyMan to create a key store file on the server (Solaris/AIX)

Using IKeyMan to create a key file on the server is the fifth of six procedures required to use SSL to encrypt Web browser connections to a Sametime server that runs on the Solaris or AIX operating system.

In this procedure, you use IKeyMan to create a key store file on the server and then import the CA.txt file you created earlier into this key store file. This procedure involves two steps:

• Verify that the SAMETIME_HOME variable is set correctly
• Creating the key file
Verify that the SAMETIME_HOME variable is set correctly: Before you run the ikeyman.sh file to start IKeyMan, you may need to edit the file to ensure that the SAMETIME_HOME variable specifies the server installation directory.

By default, the SAMETIME_HOME variable in the ikeyman.sh file specifies these installation directories:
- **AIX** - /opt/ibm/lotus/notes/latest/ibmpow
- **Solaris** - /opt/ibm/lotus/notes/latest/sunspa

If you have installed the Sametime server to a different directory, use a text editor to open the ikeyman.sh file and change the SAMETIME_HOME variable so that it specifies the installation directory appropriate for your server. The ikeyman.sh file is located in the server installation directory.

Creating the key file: In this step you start IKeyMan and use it to create the key file.
1. From the command line, change your directory to the server’s binary directory. The binary directories are shown below:
   - **AIX** - /opt/ibm/lotus/notes/latest/ibmpow
   - **Solaris** - /opt/ibm/lotus/notes/latest/sunspa
2. Run the ikeyman.sh file.
   **Note** The ikeyman.sh file must have execute privileges.
3. When IKeyMan starts, choose Key Database File - New.
4. In the New window, complete these fields:
   - **Key database type:** - Accept the default of "JKS."
   - **File name:** - Enter the name "key.jks" as the file name.
   - **Location:** - Enter the server’s data directory. For example, enter /local/notes/data
5. Click OK after completing the fields in the New window.
6. In the Password prompt window, do the following:
   - Type and confirm the password that will be used to access the keys.jks key database. This documentation assumes you enter a password of “sametime.” The actual password is at your discretion.
   - Check "Set expiration time?” And specify the number of days for which the password will be valid before it must be changed. If no expiration date is required, you can leave the “Set expiration time?” Field blank.
7. Import the Certificate Authority certificate text file (ca.txt) into the key file.
   a. Click on the Add button.
   b. In the dialog box that appears, make sure that the "Data Type" field is set to "Base64-encoded ASCII data."
   c. Set the “Certificate file name” to the name of the text file (CA.txt) into which you copied the certificate.
   d. Set the “Location” to the location to which you transferred the CA.txt file to via FTP in the previous procedure (for example, /local/notes/data).
   e. Click OK.
8. Close IKeyMan after the file imports successfully.

Next step:

Modify the Sametime.ini file (Solaris/AIX)
Modify the Sametime.ini file (Solaris/AIX)

Modifying the Sametime.ini file is the last of six procedures required to use SSL to encrypt Web browser connections to a Sametime server that runs on the Solaris or AIX operating system.

In this procedure, you use a text editor to edit the Sametime.ini file so that it includes the parameters needed to support SSL connections. You must stop the Sametime server before modifying the Sametime.ini file and then start the server after you are finished modifying the file.

1. Stop the Sametime server.
2. Open a text editor on the Sametime server.
3. Open the Sametime.ini file located in the server’s data directory. Add these settings to the Sametime.ini file. (If these settings are already in the file, change the value as indicated below.)
   
   ConfigurationPort=443
   ConfigurationSSLEnabled=true
   javax.net.ssl.keyStore=/local/notesdata/key.jks
   javax.net.ssl.trustStore=/local/notesdata/key.jks
   javax.net.ssl.keyStorePassword=sametime
   javax.net.ssl.trustStorePassword=sametime

   **Note:** For javax.net.ssl.keyStorePassword and javax.net.ssl.trustStorePassword, enter the password you specified when creating the keys.jks file. Also, if these two lines appear in the Sametime.ini file, remove them:
   
   javax.net.ssl.trustStoreType=JKS
   javax.net.ssl.keyStoreType=JKS

4. Save and close the Sametime.ini file.
5. Start the Sametime server.

---

**Ensuring Sametime servlet access when Domino requires SSL for all connections**

A Sametime server installs on a Domino server and relies on the Domino HTTP server to handle all HTTP traffic to the Sametime server. To encrypt Web browser access to the Sametime Meeting Center with SSL, the administrator must configure the Domino HTTP server to support SSL.

**Note:** For information about how to configure a Domino HTTP server to support SSL, see [Using SSL with Sametime](#).

When setting up a Domino HTTP server to support SSL, the administrator can force all connections to the Domino server to use SSL. The administrator forces all HTTP connections to use SSL by performing either of the following configurations in the Ports-Internet Ports-Web section of the Domino server Server document during the Domino HTTP server SSL set up procedure:

- Setting the Web HTTP "TCP IP port status" setting to "Disabled" and setting the Web HTTP "SSL port status" to "Enabled."
- Setting the Web HTTP "TCP IP port status" to "Redirect to SSL."

If the administrator forces all HTTP connections to use SSL, the administrator must also configure the Sametime server to support SSL for HTTP connections to its
obtaining certificate

Obtaining Certificate received When Domino

To ensure access to the Sametime servlets when Domino requires SSL for all connections, the administrator must perform the procedures below. You can use these procedures regardless of whether your Sametime server operates on the Windows, AIX, Solaris, or IBM i5/OS operating system.

To ensure access to the Sametime servlets when Domino requires SSL for all connections:

1. Obtain the appropriate SSL trusted root or SSL server certificate
2. Import the SSL certificate into the STKeys.jks database.
3. Configure the Sametime.ini file on the Sametime server

Each of these procedures is described in detail in a subsequent topic.

Note: It is possible to configure a Domino server to allow unencrypted HTTP connections on port 80 and simultaneously allow SSL-encrypted HTTP (or HTTPS) connections on port 443. This configuration enables you to encrypt connections to databases containing sensitive data while allowing unencrypted connections to databases that do not contain sensitive data. Since the Domino server on which Sametime is installed is dedicated to supporting only Sametime, it is unlikely that such a configuration would be implemented on a Domino/Sametime server.

Obtaining the appropriate SSL trusted root or SSL server certificate

Obtaining the appropriate SSL trusted root or SSL server certificate is the first of three procedures needed to ensure Sametime servlets can be accessed using SSL when the Domino HTTP server is configured to require SSL for all connections.

If the Domino HTTP server is configured to require SSL for all connections, the Domino Server Certificate Admin database on the Domino/Sametime server will already contain two certificates that are required to support SSL connections:

- An SSL trusted root certificate signed by a specific Certificate Authority (CA), such as VeriSign.
- An SSL server certificate signed by the same CA as the trusted root certificate.

You must obtain a copy of one of these certificates. Later in this process, you must import one of the certificates described above into a key database on the Sametime server. To clarify, you must obtain either the same SSL trusted root certificate that the Domino server uses to sign its SSL server certificate or a copy of the SSL server certificate used by the Domino server. You must have a copy of one of these certificates, but you do not need a copy of both of them.

Below are some examples of how you can obtain either the SSL server certificate used by the Domino server or an SSL trusted root certificate.

Obtaining a copy of the SSL server certificate used by the Domino server

When the Domino server is configured to use SSL, an SSL server certificate is received from a Certification Authority (CA) and merged into the Domino Server Certificate Admin (certsrv.nsf) database.
If you saved a copy of this certificate, make sure a copy of the certificate is available on the Sametime server hard drive or an accessible network location and continue to the next procedure. The certificate must be available so that you can import it into a key database in a subsequent procedure.

If you did not save a copy of the Domino server SSL server certificate, you can attempt to import one into your Web browser and then export the server certificate from the Web browser to your local file system. For example:

1. From the Internet Explorer Web browser, browse to the Domino/Sametime server that requires SSL for all connections. (For example, enter the URL https://Sametime.acme.com to browse to the server).
2. When prompted to "select the certificate to use when connecting," click OK.
3. At the Security Alert dialog box, select View Certificate.
4. At the Certificate dialog box, click Install Certificate.
5. At the Certificate Manager Import Wizard, click Next.
6. Select the "Automatically select the certificate store based on the type of certificate" option. Click Next.
7. At the Certificate Manager Import Wizard screen, click Finish. You should see a message indicating that the SSL server certificate was imported successfully. Click OK and then close the Certificate and Security Alert dialog boxes.
8. From the Web browser, choose Tools - Internet Options.
9. Select the Contents tab.
10. Select the Certificates button.
12. Scroll down the list of certificates and select the server certificate that you imported earlier in this procedure. The certificate name should provide some indication that the certificate is associated with the Domino server from which it was imported. For example, if the certificate was imported from a server named Sametime.acme.com, the certificate might be issued to "Sametime" or "Acme."
13. Click the Export button.
14. At the Certificate Manager Export Wizard screen, click Next.
15. At the Certificate Export File screen, select "Base64 encoded X.509 (.CER)." Click Next.
16. At the Export File Name screen, provide a name for the file and browse to a location on the local file system in which you want to store the SSL server certificate file.
   For example, on the Windows platform you might enter C:\My Documents\SSLservercertificate.cer to store the file in the C:\My Documents directory.
   **Note** For the i5/OS operating system, save the file directly to your server if you have mapped to the server drive. Otherwise, save the file on your client workstation. Later, you can use ftp or any other convenient method to copy it to your i5/OS server.
   Click Next.
17. When the message appears indicating the export was successful, click OK.

**Obtaining a trusted root certificate from a Certification Authority**

If you are unable to obtain a copy of the Domino server SSL server certificate, you can request a trusted root certificate from a CA or export a trusted root certificate from your Web browser.
If you need to obtain a trusted root certificate, you must obtain the same trusted root certificate that is used by the Domino server to sign the Domino SSL server certificate. For example, if the VeriSign Class 4 Public Primary Certification Authority trusted root certificate is used to sign the Domino SSL server certificate, you must either export this certificate from your Web browser or request a VeriSign Class 4 Public Primary Certification Authority trusted root certificate from VeriSign.

The easiest way to obtain a trusted root certificate is to export one from your Web browser. Web browsers include many different SSL trusted root certificates by default. If your Web browser contains a trusted root certificate that corresponds with the Domino server trusted root certificate used to sign the Domino SSL server certificate, you can export the trusted root certificate from the Web browser.

The procedure below illustrates how you can export a trusted root certificate from an Internet Explorer Web browser:

1. From the Internet Explorer Web browser, choose Tools - Internet Options.
2. Select the Contents tab.
3. Select the Certificates button.
4. Select the Trusted Root Certification Authorities tab.
5. Select the appropriate trusted root certificate from the list.
6. Click the Export button.
7. At the Certificate Manager Export Wizard screen, click Next.
8. At the Certificate Export File screen, select "Base64 encoded X.509 (.CER)." Click Next.
9. At the Export File Name screen, provide a name for the file and browse to a location on the local file system in which you want to store the SSL server certificate file.

   For example, on the Windows platform you might enter C:\My Documents\SSLservercerfile.cer to store the file in the C:\My Documents directory.

   Note For the i5/OS operating system, save the file directly to your server if you have mapped to the server drive. Otherwise, save the file on your client workstation. Later, you can use ftp or any other convenient method to copy it to your i5/OS server.
10. When the message appears indicating that the export was successful, click OK.

Another way to obtain a trusted root certificate is to request the certificate directly from a CA. Normally, you request a certificate from a CA by browsing to the CA’s web site.

For example, to request a certificate from VeriSign, begin by browsing to the www.verisign.com Web site. Follow the instructions on the Web site to request a certificate. Once the certificate request is approved, you will receive an e-mail explaining how to pick up the certificate. (Normally, you pick up the certificate by browsing to the Web site and copying it from a field on a Web page.) You can provide a file name for the certificate when receiving it from the CA and store the trusted root certificate on a local directory or network directory accessible from the Sametime server.

Next step

[Import the SSL certificate into the STKeys.jks key database]
Import the SSL certificate into the STKeys.jks key database

Importing the SSL trusted root or SSL server certificate into the STKeys.jks database is the second of three procedures needed to ensure access to Sametime servlets when the Domino HTTP server is configured to require SSL for all connections.

In this procedure, you import an SSL certificate into the STKeys.jks key database. (The STKeys.jks key database is provided by default with all Sametime servers on all platforms.)

For Windows, AIX and Solaris servers, you use the iKeyman program to import the certificate. For i5/OS servers, you can use iKeyman if you already have it installed and normally use it for managing certificates. Otherwise, you use a qshell command called keytool.

You must import either the SSL trusted root certificate or the SSL server certificate used by the Domino server for SSL connections into the STKeys.jks file. You obtained this certificate in an earlier procedure titled Obtaining the appropriate SSL trusted root or SSL server certificate.

Two procedures for importing the SSL certificate into the key database are provided below: one procedure applies to a Sametime server that runs on the Windows, AIX, or Solaris operating system and the other procedure applies to a Sametime server that runs on the IBM i5/OS operating system. Follow the procedure appropriate for your environment.

Note: Each of these procedures assumes you have exported the required SSL certificate to a file on the local operating system and that you will import this file from a local directory. The IBM IKeyMan program offers several other options for importing SSL certificates, including importing a certificate that has been copied to the Windows clipboard or importing a certificate from a remote network location. For more information about the other options for importing SSL certificates, see the IKeyMan documentation. This documentation is available by selecting Start - Programs - IBM IKeyMan - Documentation from the Windows desktop.

Importing the SSL certificate to the key database on a Windows, AIX, or Solaris version of the Sametime server

If your Sametime server runs on the Windows, AIX, or Solaris operating system, use this procedure to import the SSL certificate into the STKeys.jks key database:

1. Start the IKeyMan program from the command prompt of the Sametime server:
   - For AIX/Solaris servers, enter this command:
     `/Lotus/Domino/WAS51Client/java/jre/bin/java.com.ibm.gsk.ikeyman.IKeyman`
   - For Windows servers, enter this command:
     `C:\Lotus\Domino\WAS51Client\java\jre\bin\IKeyMan.exe`

2. Choose Key Database File - Open.

3. Browse to and select the "STkeys.jks" key database (located in the Sametime server data directory).

4. Enter the password required to access the STKeys.jks file. The default password for the STKeys.jks file is "Sametime."

5. In the Key database content area, select "Signer certificates." (Signer certificates may be selected by default.)

6. Click the "Add" button.
7. In the "Add Cas certificate from a File" dialog box:
   • Verify that "Base64-encoded ASCII data" is selected as the Data type.
   • Browse to and select the SSL certificate you want to import.
   • Click Open and then click OK.
8. In the "Enter a Label" dialog box, provide a label for the certificate. This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program. Click OK.
   If the certificate is imported successfully, the certificate label displays in the Signer Certificates list.

**Importing the SSL certificate to an IBM i5/OS version of the Sametime server**

If you already have iKeyman installed and normally use it for managing certificates, you can use it as described in the previous section. Otherwise, you can use a qshell command called keytool that is provided with the i5/OS operating system to import the certificate.

1. If you saved the SSL trusted root or SSL server certificate to your client workstation in the previous step, use ftp or another convenient method to copy it to your i5/OS server. The example in a later step assumes that you have copied it to the Sametime server data directory but this is not required.
2. From any i5/OS command line, run the following command to start qshell:
   ```
   strqsh
   ```
3. From qshell, run the following keytool command:
   ```
   keytool -import -alias <certificate_name> -file
   <file_containing_certificate> -storepass <keystore_password>
   -keystore <keystore_name>
   ```
   You must specify the full pathname to the file containing the certificate and the server keystore. The keytool command example below assumes the following:
   • The certificate file name is stserver1cert.
   • The server keystore file name is stkeys.jks.
   • The password for the stkeys.jks keystore is sametime. (Be sure you are in a secure environment when issuing this command because the command includes the keystore password.)
   • Both the certificate file and the stkeys.jks database are stored in the Sametime server data directory:
   ```
   keytool -import -alias stserver1cert -file
   /lotus/domino/data/stserver1cert -storepass sametime
   -keystore /lotus/domino/data/stkeys.jks
   ```
4. After you have imported the certificate, you can use this command to view the list of certificates in the stkeys.jks file to verify that the certificate was imported successfully.
   ```
   keytool -list -storepass sametime
   -keystore /lotus/domino/data/stkeys.jks
   ```
5. Press F3 to exit qshell.

**Next step**

Configure the Sametime.ini file on the Sametime server
Configure the Sametime.ini file on the Sametime server

Configuring the Sametime.ini file on the Sametime server is the last of three procedures needed to ensure Sametime servlets can be accessed using SSL when the Domino HTTP server is configured to require SSL for all connections.

The Sametime.ini file is located in the Sametime installation directory (default C:\Lotus\Domino on Windows or <root>/Lotus/Domino on IBM i5/OS). The Sametime.ini file on the Sametime server contains parameters that must be configured appropriately to ensure HTTP connections to the Sametime servlets can be encrypted with SSL.

To configure the Sametime.ini file on the Sametime server:

1. Use a text editor to open the Sametime.ini file in the Sametime server install directory on Windows or the Sametime server data directory on i5/OS.
2. In the [Config] section of the Sametime.ini file, alter the following settings (the default values for some of these settings may already be set to the appropriate value):
   - **ConfigurationPort** - This Sametime.ini setting must specify the same SSL port specified in the Ports-Internet Ports-Web section of the Domino server Server document. An example value for this setting for a Sametime server on either the Windows or IBM i5/OS platform is:
     ConfigurationPort=443
   - **ConfigurationSSLEnabled** - This setting must be set to true for Sametime servers on both the Windows and IBM i5/OS platforms, as shown in the example below:
     ConfigurationSSLEnabled=true
   - **Javax.net.ssl.keyStore** -This setting must specify the complete file path to the STKeys.jks file for Windows, AIX and Solaris servers. For i5/OS servers, specify the path relative to the server data directory. Examples are provided below:
     For 'windows:
     Javax.net.ssl.keyStore=c:\lotus\domino\stkeys.jks
     For AIX/Solaris:
     Javax.net.ssl.keyStore=/lotus/domino/stkeys.jks
     For i5/OS:
     Javax.net.ssl.keyStore=stkeys.jks
   - **Javax.net.ssl.trustStore** - This setting must also specify the complete file path to the STKeys.jks file for Windows, AIX and Solaris servers. For i5/OS servers, specify the path relative to the server data directory. Examples are provided below:
     For 'windows:
     Javax.net.ssl.keyStore=c:\lotus\domino\stkeys.jks
     For AIX/Solaris:
     Javax.net.ssl.keyStore=/lotus/domino/stkeys.jks
     For i5/OS:
     Javax.net.ssl.keyStore=stkeys.jks
   - **Javax.net.ssl.keyStorePassword** - This setting must specify the password required to access the STKeys.jks file. The default password for the STKeys.jks file on all platforms is "sametime," as shown in the example below:
Javax.net.ssl.keyStorePassword=sametime

- **javax.net.ssl.trustStorePassword** - This setting must also specify the password required to access the STKeys.jks file. The default password for the STKeys.jks file on all platforms is "sametime," as shown in the example below:
  
  javax.net.ssl.trustStorePassword=sametime

3. Save and close the Sametime.ini file and restart the Sametime server.

This concludes the procedures required to ensure Sametime servlets can be accessed using SSL when the Domino HTTP server is configured to require SSL for all HTTP connections.
Chapter 14. Deploying Multiple Lotus Sametime Servers

A Sametime community can include more than one IBM Lotus Sametime server. If you have a large number of Sametime users, you can install multiple Sametime servers for load balancing and to reduce network usage. This chapter includes:

- Information about installing multiple Sametime servers and synchronizing multiple Sametime servers to operate as a single community.
- An explanation of how to use a multiple server deployment to enable users on your corporate intranet and users from the Internet to attend the same Sametime meetings.
- A brief discussion of techniques that can be used to extend a single Sametime community across multiple Domino domains.

**Note:** This chapter discusses how you can deploy multiple Sametime servers without creating Sametime server clusters. If you are interested in clustering Sametime servers, see the chapter titled “Introduction to Sametime server clusters and the IBM Lotus Enterprise Meeting Server.”

About Sametime server clusters

Sametime includes the concept of Sametime server clustering. You can create Sametime Community Services server clusters to support server failover and load balancing for large populations of Community Services users and Sametime Meeting Services clusters to support server failover and load balancing for large populations of Meeting Services users. Creating a Meeting Services cluster requires you to deploy an application called the IBM Lotus Enterprise Meeting Server.

This chapter discusses how to deploy multiple Sametime servers without creating Sametime server clusters. If you are interested in creating a multiple server environment in which the Sametime servers are clustered, see Introduction to Sametime Server Clusters and the Enterprise Meeting Server.

Advantages of using multiple Sametime servers

You can install multiple Sametime servers to:

- Spread the load of a large user population among multiple servers.
- Reduce network usage and improve server performance when you have significant user populations in remote or distributed locations.
- Securely extend meetings conducted on a Sametime server inside your network firewall to a Sametime server deployed outside the firewall in your network DMZ. This arrangement allows Internet users to participate in meetings with users on your corporate intranet without compromising network security.

When multiple Sametime servers are installed, you can synchronize the Sametime servers to operate as a single Sametime community. Two key advantages of server synchronization are:

- You can specify different home Sametime servers for members of the Sametime community.
- Individual meetings can be simultaneously active on multiple Sametime servers.
Advantages of multiple home Sametime servers

If you install multiple Sametime servers, you can assign different home Sametime servers for users in the community. Specifying different home Sametime servers for Sametime community members allows you to spread the load of a large number of users among the Community Services of multiple Sametime servers.

The home Sametime server is the server to which each user connects for the online presence (or awareness) and chat functionality supported by the Community Services. After installing a new Sametime server, you can assign specific users to the new server by entering the name of the new Sametime server in the “Sametime server” field in each user’s Person document.

All users in the community will have presence and chat capabilities with all other users, but users connect to different Sametime servers to get this functionality. Server-to-server connections among the Community Services of the multiple Sametime servers ensure that all users in the community have presence and chat capabilities with all other users.

For more information on the purpose of the home Sametime server, see Connecting to the home Sametime server.

Note: Sametime also provides a Community Services clustering solution to support large populations of Community Services users. For more information, see Overview of Community Services clustering.

Advantages of a single meeting on multiple servers

A multiple Sametime server deployment includes the concept of "invited servers." When one Sametime server "invites" another server to a meeting, a meeting started on the inviting server becomes simultaneously active on the invited server. To enable one Sametime server to invite another to a meeting, the administrator creates a Connection Document in the Domino Directory that connects the Sametime server to another Sametime server. These Connection Documents are of the connection type "Sametime."

When a Connection Document of the type Sametime exists between two Sametime servers, one Sametime server can invite the other server to a Sametime meeting. For example, if the administrator creates a Connection Document that connects Sametime server A to Sametime server B, a meeting started on Sametime server A can also appear in the list of active meetings in the Sametime Meeting Center on Sametime server B. When the meeting starts on Sametime server A, Sametime server A "invites" Sametime server B to the meeting, and the meeting becomes simultaneously active on both servers. Users can access either Sametime server A or Sametime server B to attend the same meeting.

Advantages of a single meeting being simultaneously active on multiple Sametime servers are:

- **Better server performance** - Large numbers of users in a single location can access different servers to attend the same meeting. The burden of the meeting is spread among the system resources of multiple servers, which results in better server performance. In addition, using multiple servers in a single location helps prevent network bottlenecks that can occur if a large number of users simultaneously attempt to access a single server.

- **Reduced network bandwidth usage** - Users in remote locations can access a local Sametime server to attend the meeting, which reduces network bandwidth
usage and improves meeting performance. For example, if you have a WAN environment serving Boston and Dublin, you can install a Sametime server in each location. When a meeting starts, the meeting becomes simultaneously active on the Boston and Dublin servers. Users in Dublin attend the meeting on the Dublin server, and users in Boston attend the meeting on the Boston server. Network bandwidth usage is reduced because individual clients do not use the WAN connection to attend the meeting. Boston users connect on the Boston LAN, while Dublin users connect on the Dublin LAN. The meeting data passes on a single WAN connection between the two servers.

- **Secure meeting access for Internet users** - A meeting on a Sametime server inside the firewall can be simultaneously active on a Sametime server outside the firewall (in the network DMZ). This capability enables meetings conducted on Sametime servers inside your firewall to be securely extended to Internet clients.

  For example, if you have Sametime server A operating on your corporate intranet inside your firewall, you can install Sametime server B on a server machine located in the network DMZ (outside of the firewall that protects the corporate intranet). You can connect the two Sametime servers so that a meeting started on Sametime server A on the corporate intranet can become simultaneously active on Sametime server B in the network DMZ. Internet clients can access Sametime server B in the network DMZ to participate in a meeting started on Sametime server A. This arrangement enables Internet clients to participate in a meeting started on a server inside the firewall without making connections through your firewall. By connecting two Sametime servers on opposite sides of a firewall, the administrator can extend Sametime meetings and services to Internet users so that users on the corporate intranet and Internet users can attend the same Sametime meetings without compromising network security.

  For information on the firewall configurations required to support this scenario, see [Extending Sametime to Internet users](#).

*Note:* For information on how "invited servers" are presented to end users in the Sametime user interface, see [Configure the Network Connectivity settings for the Sametime server](#).

---

**Integrating a Sametime server into an existing Sametime community**

The basic processes and issues involved with integrating a new Sametime server into an existing Sametime community include:

- **Installing a Sametime server into an existing Sametime community**
  - Managing administration settings for multiple Sametime servers
- **Configuring ports for server-to-server connections**
- **Synchronizing the Sametime server with other Sametime servers**
  - Directory management for multiple Sametime servers
  - Assigning users to the new Sametime server (setting the home Sametime server)
  - Creating Connection Documents to connect multiple Sametime servers
  - Configuring the "Servers in this Community" settings for the Sametime server
Installing a Sametime server into an existing Sametime community

Installing the Sametime server is the first procedure you must perform when integrating a new Sametime server into an existing Sametime community.

Before you install the new Sametime server, decide whether you want the server to be accessed by Internet and intranet clients or intranet clients only. If you want the server to be accessed by both Internet and intranet clients, you should install the Sametime server on a server that is located in the network DMZ (outside the firewall that protects the corporate intranet). For more information, see Extending Sametime to Internet users.

Managing administration settings for multiple Sametime servers

When you have a multiple Sametime server environment, there are specific administration settings that must be kept consistent across all Sametime servers in the Sametime community. The administrator can use the Sametime Administration Tool on each Sametime server to manually configure the settings on each Sametime server so that the settings specify the same values on all servers in the community.

Note: You should not replicate the entire Configuration database (stconfig.nsf) among the Sametime servers. Some documents in the Configuration database contain the IP address or host name of a Sametime server. Replication of these parameters to a different Sametime server will prevent that server from functioning properly.

The administration settings that must have the same values on all Sametime servers in the community are listed below. It is mandatory that some of these settings are consistent on all Sametime servers in the community. For other settings, it is recommended that you keep consistent settings across all Sametime servers in the community, but it is not mandatory.

Administration settings that must be consistent on all Sametime servers in a community: It is mandatory that the administration settings below have the same values on all Sametime servers in a community. If these settings are not consistent across all servers, the servers may not function properly or end users may experience unexpected behavior when attending meetings on invited servers.

Community Services settings: In the Configuration-Community Services tab of the Sametime Administration Tool, the following settings must specify the same values on all Sametime servers in the community:

- Number of entries on each page in dialog boxes that show names in the directory
- How often to poll for new names added to the directory
- How often to poll for new servers added to the community

For more information on the settings above, see Community Services configuration settings

In the Configuration-Community Services-Anonymous Access tab of the Sametime Administration Tool, the following settings must specify the same values on all Sametime servers in the community:

- Anonymous users can participate in meetings or enter virtual places
- Users of Sametime applications (databases such as stconf.nsf or Web sites) can specify a display name so that they do not appear online as “anonymous”
– Default domain name for anonymous users
– Default name

- Users cannot browse or search the Directory
- Users can type names (resolve users and groups) to add them to an awareness list
- Users can browse the directory (see a list of names) or type names (resolve users and groups)
- Users can browse the directory to see group content and names, or type names (resolve users and groups)

For more information on the settings above, see Anonymous Access Settings for Community Services

LDAP Directory settings: If your community of users is defined in an LDAP directory (or directories), all LDAP Directory configuration settings must be consistent on all Sametime servers in the community. The Sametime LDAP Directory settings are divided into five categories in the Sametime Administration Tool:

- LDAP Directory - Connectivity settings
- LDAP Directory - Basics settings
- LDAP Directory - Authentication settings
- LDAP Directory - Searching settings
- LDAP Directory - Group Content settings

For more information on these settings, see LDAP directory settings

Meeting Services settings: In the Configuration-Meeting Services-General settings, the following settings must have the same values on all Sametime servers in the community:

- Automatically extend meetings beyond scheduled end time when there are still people in the meeting
- Allow people to choose the screen-sharing tool in meetings
  – Participants can share their screen, view a shared screen, or control a shared screen if the moderator permits
  – Participants can share their screen if the moderator permits or view a shared screen.
- Allow people to choose the whiteboard tool in meetings
  – Allow people to save the whiteboard annotations as attachments to the meeting
- Allow people to enable the Send Web Page tool in meetings
- Allow people to choose the Polling tool in meetings
- Allow people to record meetings for later playback (scheduled meetings only)
- Allow people to schedule broadcast meetings

Some of the settings above control the collaborative tools that are available to end users for a Sametime meeting that is started on a Sametime server. In a multiple Sametime server environment, a single meeting can be simultaneously active on multiple Sametime servers. If these settings are not consistent across servers, some servers might not allow access to collaborative tools that are needed in a meeting.
The following example scenario illustrates the problems that can occur if the "Allow people to choose the whiteboard tool in meetings" is selected on Sametime server A and C, but not selected on Sametime server B.

1. Gina creates a meeting on Sametime server A (located in the home office in Atlanta) to make a whiteboard presentation for a human resources employee benefits program.

2. This presentation is also relevant to employees at the branch offices in Boston (the location of Sametime server B) and Chicago (the location of Sametime server C). When creating the meeting, Gina selects the option in the end-user interface that enables the meeting to become active on all Sametime servers in the organization.

3. When the meeting becomes active, users who connect to Sametime server B in Boston to attend the meeting will not have access to the whiteboard tool, and will not be able to view the presentation. (The administrator of Sametime server B has disabled the "Allow people to choose the whiteboard tool in meetings" setting on that server.) Because Gina is not exposed to the administration settings of the Sametime server, she might not be aware that the whiteboard tool is not available on the Boston server.

For more information on the Meeting Services - General settings, see [General Settings for Meeting Services](#).

**Administration settings that should be consistent on all Sametime servers in a community:** If the settings below are not consistent on all Sametime servers in the community, the servers will continue to function. However, it is recommended that you keep these settings consistent on all Sametime servers in a community to ensure consistency of end user functionality and logging functions across all servers in your community.

**Community Services settings:** In the Configuration-Community Services tab of the Sametime Administration Tool, the following settings should be consistent on all Sametime servers in the community:

- Allow Connect users to save their user name, password, and proxy information (automatic login)
- Display the "Launch Sametime Connect for browsers" link on the Sametime home page
- Display the "Launch Sametime Connect for the desktop" link on the Sametime home page
- Allow authenticated users to transfer files to each other
- Allow users to send announcements

For more information on the settings above, see [Community Services configuration settings](#).

**Logging settings:** In the Logging-Settings-General tab of the Sametime Administration Tool, the following settings should be consistent on all Sametime servers in the community:

- Community Server events to log
  - Successful logins
  - Failed logins
- Community Server events and activities
- Meeting Server events to log
  - Failed meeting authentications
– Client connections
– Connection to other meeting servers in this community
– Meeting events
– Meeting server events and activities

For more information on the settings above, see [General log settings](#).

In the Logging-Settings-Capacity Warnings tab of the Sametime Administration Tool, the following settings should be consistent on all Sametime servers in the community:

- Capacity Warnings - Sharing in Instant Meetings
  – Number of active screen sharing/whiteboard meetings exceeds
  – Number of people in all screen sharing/whiteboard meetings exceeds
  – Number of people in one active screen sharing/whiteboard meetings exceeds
- Capacity Warnings - Sharing in Scheduled Meetings
  – Number of active screen sharing/whiteboard meetings exceeds
  – Number of people in all screen sharing/whiteboard meetings exceeds
  – Number of people in one active screen sharing/whiteboard meetings exceeds

For more information on the settings above, see [Capacity Warnings log settings](#).

**Next step:** After you ensure that the administrative settings are consistent for the new Sametime server, verify that the appropriate ports are open for communication between the two servers. See [Configuring ports for server-to-server connections](#).

### Configuring ports for server-to-server connections

When multiple Sametime servers are installed in a Domino environment, the Sametime servers must be able to communicate on specific ports.

**Note:** If you are deploying a Sametime server in the network DMZ for access by Internet users, see [Extending Sametime to Internet users](#) for more information about the firewall configurations required to support communications between the two servers.

### Ports required for communication between Sametime servers

The table below lists the ports on which Sametime servers communicate with each other. When these ports are open, Community Services, Meeting Services, and Broadcast Services data can pass between the two servers, and one Sametime server can invite the other to a meeting.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 1503</td>
<td>Port 1503 is the default “Meeting Server port for server connections.” This port is configurable from the Configuration - Connectivity - Network and Port Settings - Meeting Services Network options in the Sametime Administration Tool. The “Meeting Server port for server connections” setting must be set to the same port number for the Sametime servers. The servers must communicate on TCP/IP port 1503 to exchange Meeting Services data.</td>
</tr>
</tbody>
</table>
### About invited servers, audio/video, and client connectivity

When one Sametime server invites another Sametime server to a meeting that includes interactive audio/video, the audio/video data is not transmitted between the two Sametime servers. A user must always connect to the Sametime server on which a meeting was started to receive the audio/video streams. For example, assume a meeting that includes chat, screen sharing, and audio/video is started on Sametime server A and Sametime server A invites Sametime server B to the meeting. A user can attend the meeting on Sametime server B (the invited server) and receive the chat and screen sharing data from Sametime server B. However, the user is redirected to Sametime server A for the audio/video data.

The issue above pertains only to interactive audio/video meetings. For broadcast audio/video meetings, all meeting data, including audio/video, passes between the servers on port 1503 (the default "Meeting server port for server connections"). If a broadcast audio/video meeting is started on Sametime server A and becomes simultaneously active on Sametime server B, the Sametime Broadcast client can connect directly to Sametime server B and receive all broadcast meeting streams from Sametime server B, including the audio/video stream. The client is not redirected to Sametime Server A to receive the audio/video broadcast streams.

For more information on client connectivity issues, see "About Sametime Connectivity" and "Extending a Sametime server to the Internet".

### Next step

Next, perform the procedures described in "Synchronize the Sametime server with other Sametime servers" deployed in the environment.

### Synchronizing the Sametime server with other Sametime servers

When multiple Sametime servers are installed, you must synchronize the Sametime servers to operate as a single community. Synchronizing multiple Sametime servers to operate as a single community involves the following:

- Directory management for multiple Sametime servers
- Assigning users to the new Sametime server (setting the home Sametime server)
- Creating Connection Documents to connect Sametime servers
- Configuring the Servers in this Community settings for the Sametime server
**Directory management for multiple Sametime servers**

After you have installed a new Sametime server, the administrator should determine how to manage the Directory for the Sametime community.

Use these recommendations to manage Domino Directories in multiple Sametime server environments:

- If the Sametime server is installed into a Domino environment that uses only a single Domino Directory, the Directory in which all Sametime servers are registered must be replicated to each Sametime server.
- If the Sametime server is installed into a Domino environment that uses multiple Domino Directories, the primary Domino Directory (the Directory in which the Sametime server is registered) should be replicated to the Sametime server.

Directory Assistance should be set up on the Sametime server to access the other Domino Directories of interest in the environment. The Sametime server can use Domino Directory Assistance to obtain all needed Directory information from the other Directories used in the environment. Ideally, the Directory Assistance database should point to a Directory server that is dedicated to providing Directory services. However, it is not a requirement that Directory servers be used in a Sametime community that includes multiple Sametime servers.

For information on setting up Directory Assistance on the Sametime server, see your Domino server Administration documentation. Use the same procedures to set up Directory Assistance on a Sametime server that you use to set up Directory Assistance on a Domino server. The Domino Administration documentation is available from the Documentation Library at the following Internet location: http://www.lotus.com/ldd/doc (and also in the Help subdirectory of the Domino server on which Sametime is installed).

- Optionally, in a Domino environment that uses multiple Domino Directories, an Extended Server Directory Catalog can be set up on the Sametime server to enable the server to access Directory information from all directories of interest in the environment. For more information on setting up an Extended Server Directory Catalog for use with Sametime, see [Alternate ways to share Directory information across domains](#).

For more information about the Directory issues relevant to extending a single Sametime community across multiple Domino domains, see [Extending a single Sametime community across multiple Domino domains](#).

**Next step:** After determining your directory management strategy, assign users to the new Sametime server.

**Assign users to the new Sametime server (setting the home Sametime server)**

To assign a user to the new Sametime server, enter the Sametime server name in the "Sametime server" field in the Real-Time Collaboration section of a user’s Person document in the Domino Directory. This field identifies the “home” Sametime server of each user.

**Note:** Only a portion of the users in your environment should be assigned to the new Sametime server. For load balancing purposes, you should assign an equal number of users to each Sametime server in your environment. The network proximity of the user to the server is also a consideration when assigning users to a home Sametime server. Generally, you should assign the user to the closest Sametime server on the network. For more information on the home Sametime server, see [Connecting to the Home Sametime server](#).
To specify a home Sametime server, open the Domino Directory (Address Book), go to the Real-Time Collaboration section of each user’s Person document, and enter the name of a Sametime server in the “Sametime server” field. If necessary, you can create a simple agent to automate the process of populating the Sametime server field in each user’s Person document with the name of a Sametime server.

When entering the name of the Sametime server in the “Sametime server” field on the Person document, you can enter the name of the Sametime server in the Domino hierarchical name format (for example sametime.acme.com/west/acme). The “Sametime server” field automatically converts the name to the full canonical name format. For example, if you enter sametime.acme.com/west/acme in the “Sametime server” field, the server name is stored as cn=sametime.acme.com/ou=west/o=acme. You can also enter the server name in the “Sametime server” field using the full canonical name format.

Community services reads the server name from the Servers view ($Servers) of the Domino Directory. The name entered in the “Sametime server” field on the Person document must match the name of the Sametime server as it appears in the Servers view of the Domino Directory. If you are using an agent to populate the home “Sametime server” field, ensure that the agent specifies the full canonical name of the Sametime server.

Note also that a user’s Sametime Connect client Sametime Connectivity settings should specify the same Sametime server as the “Sametime server” field on the user’s Person document. In the Sametime Connect client Sametime Connectivity settings, the server name must be specified using the DNS name or IP address of the Sametime server (for example, sametime.acme.com or 111.111.111.111).

**Next step:** After assigning users to the server, the next step is **Creating Connection Records to connect Sametime servers**

**Creating Connection Records to connect Sametime servers**

Use the Configuration - Connectivity - Servers in this Community settings of the Sametime Administration Tool to create Connection Records that enable a meeting started on one Sametime server to be simultaneously active on another Sametime server. (You must create a Connection Record to enable one Sametime server to "invite" another Sametime server to a meeting.) Note the following when creating Connection Records:

- Connection Records enable the Meeting Services of one Sametime server to connect to the Meeting Services of another Sametime server. This connection occurs on the port specified as the "Meeting server port for server connections" (TCP/IP port 1503 by default) in the Configuration - Connectivity settings of the Sametime Administration Tool.

- A single Connection Record establishes a one-way connection between the Meeting Services of two Sametime servers. For example, if you create a Connection Record that specifies Sametime Server A as the “Source” Sametime server and Sametime Server B as the "Destination" Sametime server, a meeting started on Sametime server A can be simultaneously active on Sametime server B. (Sametime server A can "invite" Sametime server B to the meeting.) However, a meeting started on Sametime server B cannot be simultaneously active on Sametime server A until you create a separate Connection Record that specifies Sametime server B as the "Source" Sametime server and Sametime server A as the "Destination" Sametime server.

To create a Connection Record that specifies Sametime server A as the "Source" Sametime server, you must use the Sametime Administration Tool on Sametime
server A. To create a Connection Record that specifies Sametime server B as the "Source" Sametime server, you must use the Sametime Administration Tool on Sametime server B.

- Any Sametime server can be connected to multiple Sametime servers. For example, if you have Sametime servers A, B, C, and D, Sametime server A can be connected to Sametime servers B, C, and D, Sametime server B can be connected to Sametime servers A, C, and D, and so on. A separate Connection Record must exist for each server connection, as noted above.

- After creating and adding the Connection Record, the server specified as the "Destination" server appears in the "Meeting Servers That Are Connected" list available from the Configuration - Connectivity - Servers in this Community settings of the Sametime Administration Tool. For each server in the "Meeting Servers That Are Connected" list, you should select the "People Can Attend from Inside the Organization" or the "People Can Attend from the Internet" option. For more information, see Configuring the "Meeting Servers That Are Connected" options.

- You can use either the Sametime Administration Tool or a Lotus Notes client to create the Connection Records that enable one Sametime server to invite another Sametime server to a meeting. The instructions below explain how to create Connection Records using the Sametime Administration Tool. For information on using a Lotus Notes client to create these Connection Records, see Using a Lotus Notes client to create Connection Records for invited servers.

To create a Connection Record to connect the Meeting Services of two Sametime servers:

1. Open the Sametime Administration Tool on the server that will be the "Source" Sametime server for this connection. (The "Source" Sametime is the server from which the meeting originates. The Source server invites the "Destination" server to the meeting.)

   To open the Sametime Administration Tool, click the "Administer the Server" link on the Sametime server home page.

2. Choose Configuration.

3. Choose Connectivity.

4. Choose the Servers in this Community tab.

5. Complete the following fields to create the Connection Record.

   **Source server** - This is a read-only field that contains the name of the Source server in the Domino hierarchical server name format that includes the domain or community name (for example, sametimeA.acme.com/ACME, where ACME is the domain name). The Source server is the server on which the Meeting is created and started.

   **Destination server** - Enter the name of the Destination server in the Domino hierarchical server name format that includes the domain or community name (for example, sametimeB.acme.com/ACME). The Destination server is the remote server on which the meeting will become active (or the server that is "invited" to the meeting by the Source server).

   Make sure the server name you enter is an exact case-sensitive match with the server name that appears in the destination Sametime server's Server Document in the Domino Directory. Also, ensure that the domain or community name (/ACME in the example) is included in the server name.

   **Destination server IP address** - You must enter the fully qualified DNS name or IP address of the destination server in this field. If this field is left blank, meetings started on the source server will not become active on the destination server.
6. Click the Add button.

After clicking the Add button, the server specified as the "Destination" server in the Connection Record appears in the "Meeting Servers That Are Connected" list in the Configuration - Connectivity - Servers in this Community settings of the Sametime Administration Tool. In the "Meeting Servers That Are Connected" list, you should specify the settings you want in the "People Can Attend from Inside the Organization" and "People Can Attend from the Internet" columns. To make the appropriate selections, see Configuring the "Meeting Servers That Are Connected" options.

Using a Lotus Notes client to create Connection Records for invited servers: A Lotus Notes client can also be used to create the Connection Records described above. To use a Lotus Notes client:

1. Open the Directory on the Sametime server.
2. Select the Configuration - Servers - Connections view.
3. Click Add Connection.
4. Click the Replication/Routing tab.
5. In the "Replication task" field, select Disabled.

Note The purpose of the Connection document is to enable one Sametime server to invite the other server to a meeting. This step ensures that the Connection document does not cause unexpected replication to occur.

6. Click the Basics tab.
7. In the Connection Type field, select "Sametime."
8. Enter the name of the Destination server (described above).
9. Select either the "within my organization" or "from the Internet" option on the Connection Document. These settings correspond to similar settings in the Sametime Administration Tool that are described in Configuring the "Meeting Servers That Are Connected" options below.
10. In the Optional Network Address field, enter the fully qualified DNS name or IP address of the destination server. This field is mandatory for a Sametime Connection document.
11. Save and close the Connection document.

Configuring the "Meeting Servers That Are Connected" options

The administrator can use the Sametime Administration Tool to configure the "Meeting Servers That Are Connected" settings for connections between Sametime servers. (The "Meeting Servers That Are Connected" settings are accessible from the Configuration - Connectivity - Servers in the Community settings of the Sametime Administration Tool.)

The "Meeting Servers That Are Connected" settings list all servers that are specified as "Destination servers" in the Connection Records that connect a Sametime server with other Sametime servers in the community. A meeting started on a Sametime server can be simultaneously active on any Sametime server that appears in the "Meeting Servers That Are Connected" list. (The Sametime server can "invite" any Sametime server in the "Meeting Servers That Are Connected" list to a meeting.)

When creating a meeting on a Sametime server, the end user controls whether the Destination servers are invited to the meeting by selecting options in the Locations tab of the New Meeting form. The options available to the end users are "People are attending from Internal Sametime servers" and "People are attending from the Internet (outside the organization)."

460 Sametime Administrator’s Guide
The administrator uses the check boxes available in the "Meeting Servers That Are Connected" list to determine which options appear to the end user on the Locations tab of the New Meeting creation form. The check boxes in the "Meeting Servers That Are Connected" list also control which Destination servers are invited to a meeting when the end user selects one of the options in the Locations tab of the New Meeting form. The check boxes the administrator uses to control this behavior include:

- People Can Attend from Inside the Organization
- People Can Attend from the Internet

The functioning of these check boxes is described below.

**People Can Attend from Inside the Organization:** This option should be selected for a Sametime server in the "Meeting Servers That Are Connected" list if both of the following are true:

- The Sametime server is deployed inside the firewall (on the corporate intranet and available to internal users).
- You want meetings that are started on this Sametime server to be active on the destination Sametime server in the "Meeting Servers That Are Connected" list. (This Sametime server can invite the Sametime server in the "Meeting Servers That Are Connected" list to the meeting.) This capability is controlled by the end user in the manner described below.

If the "People Can Attend from Inside the Organization" option is selected for a Sametime server, the following occurs:

- A "People are attending from internal Sametime servers" option appears in the Locations tab of the New Meeting form in the Sametime Meeting Center on the Sametime server.

If the end user selects the "People are attending from internal Sametime servers" option in the Locations tab when creating a meeting, the meeting becomes simultaneously active on every Sametime server that has the "People Can Attend from Inside the Organization" option selected in the "Meeting Servers That Are Connected" list of the Sametime Administration Tool.

If the "People Can Attend from Inside the Organization" setting is not selected for a Sametime server in the Sametime Administration Tool, the meeting does not become active on that Sametime server even if the end user selects the "People are attending from internal Sametime servers" option in the Locations tab when creating the meeting.

To illustrate, consider the following example scenario:

1. An organization has five Sametime servers (servers A, B, C, D, and E).
2. The administrator creates Connection documents to enable every Sametime server to connect to every other Sametime server. Every Sametime server can "invite" every other Sametime server to a meeting.
3. The administrator opens the Sametime Administration Tool on Sametime server A and selects the "People Can Attend from Inside the Organization" for Sametime servers B and C, but not D and E.
4. An end user accesses the Sametime Meeting Center on Sametime server A and schedules a meeting. When scheduling the meeting, the end user selects the "People are attending from internal Sametime servers" option on the Locations tab of the New Meeting form.
5. When the meeting starts, the meeting becomes simultaneously active on Sametime server A, B, and C, but not D or E. Users can attend the meeting by accessing either Sametime server A, B, or C.

**People Can Attend from the Internet:** Similar to the "People Can Attend from Inside the Organization" setting, the "People Can Attend from the Internet" setting also affects the options that are available to the end user and determines whether a meeting started on a Source Sametime server can be simultaneously active on a Destination Sametime server in the "Meeting Servers That Are Connected" list. This option should be selected for a Sametime server if both of the following are true:

- The Sametime server is deployed outside the firewall (in the network DMZ and accessible to Internet clients). For more information, see Extending Sametime to Internet users.
- You want meetings that are started on other Sametime servers to be simultaneously active on this Sametime server. This capability is controlled by the end user in the manner described below.

If the "People Can Attend from the Internet" option is selected for a Sametime server, the following occurs:

- A "People are attending from the Internet (outside the organization)" option appears in the Locations tab of the New Meeting form in the Sametime Meeting Center when creating a new meeting.
- If the end user selects the "People are attending from the Internet (outside the organization)" option in the Locations tab when creating a meeting, the meeting becomes simultaneously active on every Sametime server that has the "People Can Attend from the Internet" setting selected in the "Meeting Servers That Are Connected" list in the Sametime Administration Tool.
- If the "People Can Attend from the Internet" setting is not selected for a Sametime server, meetings started on other Sametime servers cannot become active on the Sametime server deployed in the network DMZ.

To illustrate, consider the following example scenario:

1. An organization has five Sametime servers (servers A, B, C, D, and E).
2. The administrator creates Connection Documents to enable every Sametime server to connect to every other Sametime server. Every Sametime server can "invite" every other Sametime server to a meeting.
3. The administrator opens the Sametime Administration Tool on Sametime server A, and selects the "People Can Attend from the Internet" for Sametime servers D and E, but not B and C.
4. An end user accesses the Sametime Meeting Center on Sametime server A and schedules a meeting. When scheduling the meeting, the end user selects the "People are attending from the Internet (outside the organization)" option on the Locations tab of the New Meeting form.
5. When the meeting starts, the meeting becomes simultaneously active on Sametime server A, D, and E, but not B or C. Users can attend the meeting by accessing either Sametime server A, D, or E.

The meeting becomes active on Sametime servers D and E because the administrator has created Connection Records that connect Sametime server A to Sametime servers D and E and the administrator has also selected the "People Can Attend from the Internet" option for servers D and E in the "Meeting Servers That Are Connected" list in the Sametime Administration Tool.
Configuring the Meeting Servers That Are Connected settings: To configure the Meeting Servers That Are Connected settings:

1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Connectivity.
4. Choose the Servers in this Community tab.
5. Perform the remaining steps using the "Meeting Servers That Are Connected" settings at the bottom of the Servers in this Community tab.
6. In the Optional Network Address field, verify that the IP address of the Sametime server is correct.

   The IP address of each Sametime server must be available to all Sametime servers to ensure that the servers can communicate and "invite" each other to meetings. You can modify or add an IP address in the "Optional Network Address" column if necessary.

7. If you have installed the Sametime server on a server machine that is physically located inside the internal firewall (or in the corporate intranet), and you want to allow meetings started on other internal Sametime servers to be simultaneously active on this Sametime server, select Yes in the "People Can Attend from Inside the Organization" column.

   If you do not want meetings started on other Sametime servers to be simultaneously active on this Sametime server, do not select Yes in the "People Can Attend from Inside the Organization" column.

8. If you have installed the Sametime server on a server machine that is physically located outside the firewall (in the network DMZ and accessible to Internet clients), and you want to allow meetings started on other Sametime servers to be simultaneously active on this Sametime server, select Yes in the "People Can Attend from the Internet" column for this Sametime server.

   If you do not want meetings started on other Sametime servers to be simultaneously active on this Sametime server, do not select Yes in the "People Can Attend from the Internet" column for this Sametime server.

9. Click the Update button and restart the Sametime server for the changes to take effect.

Next step: At this point, the newly installed Sametime server is fully integrated into the existing Sametime community.

If the newly installed Sametime server is located in the network DMZ and accessible by Internet clients, you might want to review Extending Sametime to Internet users later in this chapter to ensure the firewalls are configured appropriately to allow the necessary client and server connections.

Extending Sametime to Internet users

In some situations, you may want Internet users to attend the same Sametime meetings as users on your corporate intranet. Generally, firewall restrictions make it impossible for users from the Internet to directly access a Sametime server on your corporate intranet.

The recommended solution for extending Sametime meetings to Internet users involves a multiple Sametime server deployment in which a server inside your corporate firewall invites a server outside the firewall (in the network DMZ) to a meeting. This solution requires you to install a Sametime server on the corporate
intranet and a Sametime server in the network DMZ, synchronize the two Sametime servers, and configure the firewalls to enable the servers and clients to establish the appropriate connections with the servers.

The remaining topics in this section describe the recommended solution for extending Sametime meetings to Internet users and provide information on the firewall configurations required:

- Positioning a Sametime server in the network DMZ
- Opening ports on the internal firewall
- Opening ports on the external firewall

**Positioning a Sametime server in the network DMZ**

Allowing users on a corporate intranet and users from the Internet to attend the same Sametime meetings requires a multiple server deployment. Generally, one Sametime server is installed on the corporate intranet and another Sametime server is installed in the network DMZ as shown in the illustration below.

![Diagram](image_url)

**Note:** DMZ is a networking term that comes from the military term "demilitarized zone." DMZ refers to an area of a network, usually between two firewalls, where users from the Internet are permitted limited access over a defined set of network ports and to predefined servers or hosts. A DMZ is used as a boundary between the Internet and a company’s internal network. The network DMZ is the only place on a corporate network where Internet users and internal users are allowed at the same time.

The two servers are installed and synchronized according to the procedures and recommendations described in "Advantages of using multiple Sametime servers" and "Synchronizing the Sametime server with other Sametime servers" earlier in this chapter. Following these procedures enables one Sametime server to "invite" another Sametime server to a meeting. Internal users on the Acme corporate network can attend a Sametime meeting by connecting to the internal Sametime server while Internet users can attend the same meeting by connecting to the Sametime server in the network DMZ.

After you have installed and synchronized the two Sametime servers, you must make firewall configurations to both the internal firewall that protects the
corporate intranet and the external firewall that separates the network DMZ from the Internet to ensure that the servers and users can communicate through the firewalls. See the following topics for information on the firewall configurations required:

- Opening ports on the internal firewall
- Opening ports on the external firewall

Opening ports on the internal firewall

After you have deployed a Sametime server on the corporate intranet and a Sametime server in the network DMZ, you must configure the internal firewall to enable the Sametime servers to communicate with each other and for users to communicate with the servers.

The illustration below shows an internal firewall machine that separates the internal Acme corporate network from the Acme network DMZ. The firewall machine contains two Network Interface Cards (NICs). One NIC is connected to the internal network and the other NIC is connected to the network DMZ.

The table below provides port configurations for the internal firewall that will enable the clients and Sametime server inside the firewall to communicate with the Sametime server in the network DMZ.

<table>
<thead>
<tr>
<th>Port</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Open TCP port 80 on the internal firewall for outbound connections from the Acme corporate network to the Acme network DMZ. Opening port 80 enables internal users to access the Meeting Center on the Sametime server in the network DMZ with a Web browser to schedule meetings on that server when necessary. A Sametime administrator can also access the Web-based Sametime Administration Tool on the Sametime server in the network DMZ using a Web browser.</td>
</tr>
<tr>
<td>1516</td>
<td>Open TCP port 1516 on the internal firewall for outbound/inbound connections between the Acme corporate network and the Acme network DMZ. Opening port 1516 enables the Community Services of the two Sametime servers to exchange presence and chat data and to perform directory updates.</td>
</tr>
<tr>
<td>Port</td>
<td>Explanation</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Port 1503 | Open TCP port 1503 on the internal firewall for outbound/inbound connections between the Acme corporate network and the network DMZ.  
All Meeting Services and T.120 protocol data passes between the two Sametime servers on port 1503.  
**Note:** If you open port 1503 for outbound/inbound connections, the internal Sametime server can invite the DMZ Sametime server to a meeting and the DMZ Sametime server can invite the internal Sametime server to a meeting. If you do not want Internet users to invite the internal Sametime server to meetings, you can open port 1503 for outbound connections only from the Acme corporate network to the Acme network DMZ. Note also that a Connection document must exist between two servers to enable one server to invite another server to a meeting. If you do not create a Connection document that connects the DMZ Sametime server to the internal Sametime server, the DMZ server cannot invite the internal Sametime server to a meeting. For more information, see [Creating Connection Records to connect Sametime servers](#). |
<table>
<thead>
<tr>
<th>Port</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Port 8084 or UDP ports | To allow internal users to participate in interactive audio/video meetings with users from the Internet, you must either open TCP port 8084 (the default TCP Tunneling port for the Audio/Video Services) or a range of UDP ports through the internal firewall.  
Open TCP port 8084 if the security policies of your organization do not allow UDP traffic through the internal firewall. Opening port 8084 enables users on the Acme corporate network to receive audio/video streams through TCP tunneling from the Sametime server in the network DMZ. It is only necessary to open an outbound connection from the Acme corporate intranet to the Acme network DMZ. Internal users make the outbound connection to the DMZ server using TCP and receive the audio/video streams from the DMZ Sametime server through TCP/ACK packets. For more information on audio/video connectivity, see [Interactive Audio/Video Network Settings](#).  
Alternately, you can open a range of UDP ports through the internal firewall to enable internal users to receive audio/video streams from the DMZ Sametime server. If you choose to open UDP ports through the internal firewall, you can define the range of UDP ports that must be open from the Configuration - Connectivity - Networks and Ports - Interactive Audio/Video Network - Multimedia Processor (MMP) start at/end at settings of the Sametime Administration Tool on the DMZ Sametime server. (The default port range is UDP ports 49152 - 65535.)  
If you want users on the Acme corporate network to participate in audio/video meetings with Internet users, the audio/video meetings should be started on the Sametime server in the network DMZ.  
If a meeting is started on the DMZ Sametime server and the internal Sametime server is invited by the DMZ Sametime server, internal users can attend the meeting on the internal Sametime server. The internal users receive the Community and Meeting Services data from connections to the internal Sametime server, but must receive the audio/video streams from the DMZ Sametime server through TCP tunneled connections or UDP. (In an audio/video meeting that includes invited servers, a user can connect to an invited server for Community Services and Meeting Services functionality, but must always connect to the Sametime server on which the meeting was started to receive the audio/video streams.) Internet users connect to the DMZ Sametime server and receive all meeting data, including audio/video streams, from the DMZ Sametime server.  
If an audio/video meeting is started on the internal Sametime server, and the internal Sametime server invites the DMZ Sametime server to the meeting, Internet users will be unable to receive audio/video streams from the internal server until you open inbound connections through the firewall on port 8084 or a range of UDP ports. Opening these ports for inbound access may violate the security policies of your organization. For this reason, you may want to stipulate that all audio/video meetings that include both intranet and Internet users must be started on the Sametime server in the network DMZ. |
<table>
<thead>
<tr>
<th>Port</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Port 554 | Open TCP port 554 on the internal firewall if you want internal users and Internet users to participate in the Broadcast meetings, and you are not allowing the DMZ Sametime server to invite the internal Sametime server to meetings.  
In a broadcast meeting where one Sametime server invites another Sametime server to a meeting, all broadcast meeting data (including whiteboard, screen sharing, chat, and audio/video) passes between the servers using port 1503.  
If the internal Sametime server can invite the DMZ Sametime server to meetings, and the DMZ Sametime server can invite the internal Sametime server to meetings, it is not necessary to open port 554 on the internal firewall.  
If port 1503 is open, the internal users can attend a broadcast meeting on the internal Sametime server and the external users can attend a broadcast meeting on the DMZ Sametime server.  
However, if you do not allow the DMZ Sametime server to invite the internal Sametime server to meetings, it will be impossible for an Internet user to start a broadcast meeting on the DMZ Sametime server that can also be attended by users on the internal network unless you open port 554 for outbound connections from the Acme internal network to the Acme network DMZ.  
Opening port 554 enables the internal broadcast clients to connect to the DMZ Sametime server to attend broadcast meetings started on the DMZ Sametime server. If the broadcast meeting also includes audio/video, the audio/video streams can be tunneled to the client using TCP on port 554 as described in [Broadcast Services Network settings](#).  
You also have the option of opening a range of UDP ports through the internal firewall to enable internal broadcast clients to receive audio/video streams associated with a broadcast meeting started on the DMZ Sametime server. The issues associated with opening UDP ports on the internal firewall to support audio/video streams are discussed in the “Port 8084 or UDP ports” section above. |
| Port 1352 | If you have integrated the Sametime server in the network DMZ into the same community as the internal Sametime server, you must open TCP port 1352 for outbound/inbound access through the internal firewall. Port 1352 supports Notes Remote Procedure Calls (RPCs). Opening port 1352 enables the two Sametime servers to replicate Notes databases and also allows an administrator on the internal network to access the DMZ Sametime server with a Notes client, if necessary. |

**Opening ports on the external firewall**

The illustration below shows an external firewall machine containing two Network Interface Cards (NICs). One NIC is connected to the network DMZ; the other NIC connects to the Internet. You must configure the external firewall that protects the network DMZ to enable Internet clients to make the appropriate connections to the external Sametime server deployed in the network DMZ.
The table below provides information on port configurations for the external firewall that will enable the Internet clients to make the appropriate connections with the Sametime server in the Acme network DMZ.

<table>
<thead>
<tr>
<th>Port</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 80</td>
<td>Open TCP port 80 on the external firewall for inbound TCP connections from the Internet to the DMZ Sametime server. The firewall must allow TCP/ACK packets to pass from the DMZ Sametime server to the Internet users. Opening port 80 enables a Sametime Internet user to authenticate with the Sametime HTTP server. Internet users can also access the Sametime Meeting Center database (stconf.nsf) and download Sametime clients from the Sametime server. Access to the Sametime Meeting Center database can be restricted through the ACL settings of the database. For more information, see <a href="#">Using database ACLs for identification and authentication</a>. The DMZ Sametime server can also be configured so that connections to the Meeting Services, Community Services, and Broadcast Services also occur over port 80. With this configuration, it may not be necessary to open ports 1533, 8082, or 8081 as described below. For more information, see <a href="#">HTTP Tunneling on port 80</a>.</td>
</tr>
<tr>
<td>Port</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port 1533 or Port 8082</td>
<td>Open either TCP port 1533 or 8082 to enable the Internet users to access the Community Services on the DMZ Sametime server. Port 1533 is the recommended port for Community Services client connections. Opening port 1533 enables Sametime clients from the Internet to access the Sametime server using a direct TCP/IP connection, a direct HTTP connection, or through an HTTP proxy server. <strong>Note:</strong> The Sametime Connect client includes a Preferences-Sametime Connectivity-Community Port setting that specifies the port on which the Sametime Connect client attempts connections to the Community Services. The default Community Port setting is port 1533. The Community Port setting on the Sametime Connect client must specify the port that is open through the firewall to enable a Sametime Connect client from the Internet to connect to the Sametime server in the network DMZ. For more information on Community Services connectivity, see <a href="#">Community Services Network settings</a>. Some Internet clients may operate behind restrictive firewalls that block outbound connections to the Internet on port 1533 or 8082. The recommended method for enabling these clients to establish connections with the DMZ Sametime server is to enable HTTP tunneling on port 80. For more information, see <a href="#">HTTP Tunneling on port 80</a>.</td>
</tr>
<tr>
<td>Port 8081</td>
<td>Open port 8081 to enable the Internet users to access the Meeting Services on the DMZ Sametime server. Opening port 8081 enables Internet users to participate in Sametime meetings using the Sametime Meeting Room client. The whiteboard, and screen sharing components of the Sametime Meeting Room client connect to the Sametime server on this port. The Meeting Room client can establish direct TCP/IP connections with the Sametime server, or connect to the Sametime server through a SOCKS or HTTP proxy server. For more information, see <a href="#">Meeting Services Network settings</a>. <strong>Note:</strong> Some Internet clients may operate behind restrictive firewalls that block outbound connections to the Internet on port 8081. The recommended method for enabling these clients to establish connections with the DMZ Sametime server is to enable HTTP tunneling on port 80. For more information, see <a href="#">HTTP Tunneling on port 80</a>.</td>
</tr>
</tbody>
</table>
### Port 8084

<table>
<thead>
<tr>
<th>Port 8084 or UDP ports</th>
</tr>
</thead>
</table>
| To allow Internet users to participate in interactive audio/video meetings on the DMZ Sametime server, you can either open TCP port 8084 or a range of UDP ports through the external firewall. Open TCP port 8084 if the security policies of your organization do not allow UDP traffic through the external firewall. Opening port 8084 enables users on the Internet to receive audio/video streams through TCP tunneling from the Sametime server in the network DMZ. The Internet users make a TCP connection to the Audio/Video Services on port 8084 and receive the audio/video streams from the server through TCP/ACK packets. Alternately, you can open a range of UDP ports through the external firewall to enable Internet users to receive the audio/video streams. If you open UDP ports through the external firewall, you can control the range of UDP ports that are used to transmit audio/video data from the Configuration-Connectivity-Networks and Ports-Interactive Audio/Video Network-Multimedia Processor (MMP) start at/end settings of the Sametime Administration Tool on the DMZ Sametime server. (The default port range is UDP ports 49152 - 65535.) The range of ports that you specify in this administration setting is the range of UDP ports that must be open through the external firewall. **Note:** If the client also operates behind a firewall, the client-side firewall must also allow communications on either port 8084 or the range of UDP ports to receive the audio/video streams. Unlike the Community Services, Meeting Services, and Broadcast Services data, the Audio/Video Services data cannot be tunneled over port 80 using HTTP. For more information about audio/video connectivity, see [Interactive Audio/Video Network settings](#).

### Port 554

<table>
<thead>
<tr>
<th>Port 554</th>
</tr>
</thead>
</table>
| Open TCP port 554 on the external firewall to allow Internet users to participate in Broadcast meetings on the DMZ Sametime server. Once you have opened port 554, the Internet Broadcast clients can receive all broadcast meeting data, including any audio/video streams associated with the meeting. The Broadcast client can establish a direct TCP/IP connection with the DMZ Sametime server, or connect to the server through a SOCKS or HTTP proxy server and the meeting streams are tunneled to the client on port 554 as described in [Broadcast Services Network settings](#). Broadcast meeting performance is more efficient if you open UDP ports through the external firewall. The UDP transport operates more efficiently than TCP tunneling of broadcast streams. If you open UDP ports on the external firewall, the range of ports that you open must correspond to the range of ports specified in the Configuration-Connectivity-Network and Ports-Interactive Audio/Video Network-Multimedia Processor (MMP) start at/end settings of the Sametime Administration Tool on the DMZ Sametime server. **Note:** If the broadcast client also operates behind a firewall, the client-side firewall must also allow communications on either port 554 or UDP ports to receive the audio/video streams. The recommended method for enabling these clients to establish connections with the DMZ Sametime server is to enable HTTP tunneling on port 80. For more information, see [Tunneling on port 80](#).

### Screen-sharing security and Internet users

The Sametime Administration Tool includes a "Participants can view the shared screen only" option that is provided for screen-sharing security when Internet users and intranet users attend the same Sametime meetings. This setting is located in
the Configuration-Meeting Services-General-When people start an instant meeting or schedule a meeting settings of the Sametime Administration Tool.

If an organization frequently conducts screen-sharing meetings where the Sametime server in the network DMZ is invited to meetings by the internal Sametime server, the administrator may want to enable the "Participants can view the shared screen only" option. Enabling this option allows an Internet user to view screen sharing activity in a meeting but prevents the user from controlling a shared screen on an intranet computer.

**Note:** The "Participants can view the shared screen only" option prevents any user connected to a server from sharing a screen. This option is intended for invited server scenarios only. The setting enables users attending a screen-sharing meeting on an invited server to view screen-sharing activity, but only users attending the meeting on the "source" Sametime server have the ability to share screens. (The "source" Sametime server is the server from which the meeting originates. The source Sametime server invites the destination Sametime server to the meeting.)

Preventing Internet users from controlling a shared screen provides security against an Internet user inadvertently gaining access to computers, network drives, and directories on the corporate intranet. For example, if a user on your corporate intranet is sharing a screen on an intranet computer, and the intranet user leaves the screen-sharing computer unattended, an Internet user can use the screen sharing features to gain access to applications and network drives that are available from the intranet computer. If the Sametime server in the network DMZ (the invited server) has the "Participants can view the shared screen only" setting enabled, an Internet user cannot use the screen-sharing features and cannot gain access to the intranet computer.

To enable the "Participants can view the shared screen only" option:
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. Choose Configuration.
3. Choose Meeting Services.
5. Select the "Participants can view the shared screen only" option. (This option is located beneath the "Allow people to choose the screen-sharing tool in meetings" setting.)
6. Click Update and restart the server for the change to take effect.

---

**Extending a single Sametime community across multiple Domino domains**

This section provides instructions and suggestions on how to link different Domino domains into a single Sametime community. Read this section if your organization includes multiple Domino domains and you want users in the multiple Domino domains to belong to the same Sametime community. When separate Domino domains are linked into a single Sametime community, users in each domain can share presence and chat capabilities and participate in Sametime meetings with users in the other domain. This section includes the following topics:

- Example of extending a single Sametime community across two Domino domains
Example of extending a single Sametime community across two Domino domains

The procedure below provides an example of how one Sametime server in a Domino domain can be linked with a different Sametime server operating in a different Domino domain. Linking the two Sametime servers extends a single Sametime community to both Domino domains.

When a single Sametime community is extended to both Domino domains:

- Users in one Domino domain can add users from the other Domino domain to presence lists in Sametime clients and engage in Sametime communications with users in the other domain.
- Users in the Sametime community can authenticate on either of the domains to participate in Sametime meetings and communications.
- The Sametime server in one Domino domain can invite the Sametime server in the other Domino domain to a meeting so that a single Sametime meeting can be attended by users in both Domino domains.

Follow the procedures below to link two Sametime servers that operate in different Domino domains:

1. **Set up the environment**
2. **Connect the communities (share Directory information)**
3. **Share meetings between the communities**

Setting up the environment

This is the first of three procedures that illustrate how you can extend a single Sametime community across multiple Domino domains.

To set up the environment, you must ensure that the two Sametime servers are cross-certified.

In this example, the two Sametime servers are Sametimeserver1/East and Sametimeserver2/West. To cross-certify these servers, the West organization certifier (/West) must obtain a cross-certificate for the East organization certifier (/East). Conversely, the East organization certifier must obtain a cross-certificate for the West organization certifier. These cross-certificates are stored in the Domino Directories on the respective Sametime servers.

The example below describes the simplest way to cross-certify the two Sametime servers.

1. On Sametimeserver1/East, open the Notes client. From the Windows desktop choose Start - Run and browse to C:\Sametime\nnotes.exe. Click OK.
2. Select File - Database - Open and specify the Sametimeserver2/West server.
3. When prompted for a cross-certificate, select OK.
4. Repeat this procedure, except this time use the Notes client on Sametimeserver2/West to access Sametimeserver1/East, and accept the cross-certificate from the Sametimeserver2/West server.

**Note:** For more information about cross-certification, see the Domino Administration Help database available in the Help directory of a Domino server. Domino administration documentation is also available from the documentation library at www.lotus.com/ldd/doc.
Next step: After performing this procedure for both Sametime servers, the servers should be cross-certified and contain the appropriate certificates in their Domino Directories. Next, you must connect the communities.

Connecting the communities
This is the second of three procedures that illustrate how you can extend a single Sametime community across two Domino domains.

In this procedure, the administrator connects the Sametime communities by ensuring that Directory information is shared between the two Domino domains. This procedure includes the following steps:

1. **Replicating the Directories**
2. **Setting up Directory Assistance**

In this example, the two Sametime servers that operate in different domains are Sametimeserver1/East and Sametimeserver2/West.

Note: This example describes replicating the entire Directories of both domains. There are more efficient ways to share Directory information between two Domino domains when connecting the communities. For more information on alternate methods for sharing the Directory information, see [Alternate ways to share Directory information across domains](#).

Step 1 - Replicating the Directories: This procedure provides an example of replicating Directories between two Sametime servers (Sametimeserver1/East and Sametimeserver2/West) operating in different Domino domains.

1. Using the Lotus Notes client on Sametimeserver1/East, open the Directory (names.nsf) on Sametime server2/West.
3. Specify "Local" for the Server and change the filename (names.nsf) to something different, such as sametimeserver2west.nsf.
4. Select Create: "Immediately" to ensure that the database is created immediately. Click "OK."
5. Repeat this procedure, except this time create a replica of the Directory existing on Sametimeserver1/East on the Sametimeserver2/West server.

After you have created replicas of the Directories on each Sametime server, you must create Connection Documents to ensure the Directories replicate at regular intervals. When creating the Connection Documents:

- For Connection Type, select Local Area Network.
- Complete the Destination Server, Source Domain, Destination Domain, and Optional Network Address fields.
- For Replication Type, select Pull Push.
- In the "Files/Directories to Replicate" field, enter names.nsf.
- In the Schedule field, select Enabled.

Note: Be sure to create a Connection Document on each server. One Connection Document should enable the names.nsf file on Sametimeserver1/East to replicate to the Sametimeserver1east.nsf file on the Sametimeserver2/West server. The other Connection Document should enable the names.nsf file on Sametimeserver2/West to replicate to the sametimeserver2west.nsf file on the Sametimeserver1/East server.
After creating the Connection Documents, set up Directory Assistance on each of the Sametime servers to ensure that each Sametime server can locate the Directories you have just replicated.

**Step 2 - Setting up Directory Assistance:** The procedures required for setting up Directory Assistance on each of the Sametime servers are summarized below. For more information on Directory Assistance, see the Domino server Administration Help available at www.lotus.com/ldd/doc of the Help directory on the Domino server.

To set up Directory Assistance you must:
- Ensure that a Directory Assistance database is available on the Sametime server.
- Identify the Directory Assistance database on the Sametime server.
- Create a Directory Assistance Document within the Directory Assistance database that points to the appropriate Directory.

Follow the procedures below to set up Directory Assistance:

**Ensure that a Directory Assistance database is available on each Sametime server:** To ensure that a Directory Assistance database is available on each Sametime server, you can either replicate an existing Directory Assistance database to the Sametime server or create a new Directory Assistance database on the Sametime server.

If a Directory Assistance database is already in use on Domino servers in the domain, you can replicate the existing Directory Assistance database to the Sametime server. To replicate an existing Directory Assistance database, follow the normal Domino procedure for replicating a database. First create a new replica of the Directory Assistance database on the Sametime server and then create a Connection Document to schedule replication of the database. See the Domino server Administration Help for more information on these procedures.

To create a new Directory Assistance database on each Sametime server:
2. Choose File - Database - New.
3. Create the Directory Assistance database as you would any other Domino database.
   - Create the database on the Sametimeserver1/East server
   - Provide a database name and filename for the Directory Assistance database
   - Use the Directory Assistance template (da50.ntf) when creating the database
4. Repeat this procedure to create a Directory Assistance database on the Sametime server in the other domain (Sametimeserver2/West in this example).
5. Perform the procedure below to identify the Directory Assistance database on each Sametime server.

**Identify the Directory Assistance database on each Sametime server:** After replicating or creating the Directory Assistance databases on the Sametime servers, you must identify the Directory Assistance databases on each server.

To identify a Directory Assistance database on each Sametime server:
2. Select Configuration - Server - All Server Documents.
3. Double-click the name of the Sametime server (Sametimeserver1/East) to open the Server document.
4. If necessary, select the Basics tab of the Server document.
5. Click Edit Server.
6. In the "Directory Assistance database name" field, enter the filename (for example, da.nsf) of the Directory Assistance database.
7. Click "Save and Close."
8. Repeat this procedure to identify the Directory Assistance database on the Sametime server in the other domain (Sametimeserver2/West in this example).
9. Perform the procedure below to create a Directory Assistance Document in each Directory Assistance database.

Create a Directory Assistance Document in each Directory Assistance database:
You must create a Directory Assistance Document in each Directory Assistance database on each Sametime server so that each Sametime server can access the new Directory information that has been replicated to it.

To create a Directory Assistance document in the Directory Assistance database on each Sametime server:
1. From the Notes client:
   - Choose File - Database - Open.
   - Select the Sametimeserver1/East server.
   - Select the Directory Assistance database (default name is da.nsf).
   - Click Open.
2. Click "Add Directory Assistance."
   In the Basics tab, enter these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type</td>
<td>Choose Notes.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Enter the name of the Domino domain associated with the secondary Directory (or Directory that was replicated from the other domain to this Sametime server). The domain name must be different from the primary Notes domain and from all other domain names configured in Directory Assistance.</td>
</tr>
<tr>
<td>Company name</td>
<td>Enter the name of your company.</td>
</tr>
<tr>
<td>Search order</td>
<td>A number representing the order in which this directory is searched, relative to other directories in the Directory Assistance database.</td>
</tr>
<tr>
<td>Group expansion</td>
<td>The suggested setting is Yes. This setting enables Directory Assistance to examine the contents of groups in the LDAP directory. This capability is necessary if you enter the name of a group defined in the LDAP directory in the ACL of a database on the Sametime server.</td>
</tr>
<tr>
<td>Nested group expansion</td>
<td>The suggested setting is Yes. This setting enables Directory Assistance to examine the content of an LDAP directory group that is a member of another LDAP directory group. This capability is also used when an LDAP directory group name is entered in the ACL of a database on the Sametime server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Set to Yes to enable Directory Assistance for the LDAP Directory.</td>
</tr>
</tbody>
</table>
3. Select the Rules tab and enter these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule #</td>
<td>One or more rules that describe the names in the directory. By default, the first rule contains all asterisks, indicating all names in the Directory.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Choose one: • No to disable a specific rule. • Yes to enable a specific rule. By default, the first rule is enabled.</td>
</tr>
<tr>
<td>Trusted for Credentials</td>
<td>Choose Yes to allow Domino to use this Directory to authenticate Web clients.</td>
</tr>
</tbody>
</table>

4. Select the Replicas tab and do the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Links</td>
<td>Open the replica of the secondary directory, and then choose Edit - Copy As Link - Database Link. Select the &quot;Database links&quot; field, and then choose Edit - Paste. For example, assume you are creating the Directory Assistance document in the Directory Assistance database on the Sametime server1/East server and you have replicated the directory file named sametimeserver2west.nsf to the Sametime server1/East server. In this example, you must open the sametimeserver2west.nsf file and copy the file as a Database Link. Paste this Database Link into the &quot;Database links&quot; field in the Directory Assistance Document you are creating in the Directory Assistance database on the Sametime server1/East server. Conversely, when creating a Directory Assistance Document on the Sametime server2/West server, you would open the directory file sametimeserver1east.nsf, copy the file as a Database Link, and paste the link into the &quot;Database links&quot; field.</td>
</tr>
</tbody>
</table>

5. You must repeat this procedure to create a Directory Assistance document in the Directory Assistance database on the Sametime server in the other domain (Sametime server2/West in this example).

**Next step:** After replicating the Directories and setting up Directory Assistance to connect the communities, you can create Connection Records that enable a Sametime meeting started on the Sametime server in one domain to be simultaneously active on the Sametime server in the other domain. For more information, see [Sharing meetings between communities](#).

**Sharing meetings between communities**
This is the last of three procedures that illustrate how you can extend a single Sametime community across two Domino domains.

In this procedure, you create Connection Records to connect the Sametime servers that operate in different Domino domains. Creating these Connection Records
enables a meeting started on one Sametime server to be simultaneously active on the other Sametime server. This capability is sometimes referred to as “invited servers.”

If a single meeting is simultaneously active on both Sametime servers, users in the different Domino domains can participate in the same Sametime meeting by accessing the Sametime server installed in the local domain. For example, a user can start a meeting on Sametimeserver1/East and the meeting can be simultaneously active on the Sametimeserver2/West server. Users in the /East domain access Sametimeserver1/East to attend the meeting while users in the /West domain access Sametimeserver2/West to attend the meeting. Note that for this capability to function, the Sametime servers must be able to communicate with each other on the TCP/IP ports described in "Configuring ports for server-to-server connections" earlier in this chapter.

To enable the invited servers functionality, follow the procedure below to create Connection Records that enable each Sametime server to invite the other to a meeting. You must create a Connection Record on each Sametime server to enable both servers to invite each other to meetings.

Note: The procedure below explains how to use the Sametime Administration Tool to create Connection Records. You can also use a Lotus Notes client to create these Connection Records. For more information, see [Using a Lotus Notes client to create Connection Records for invited servers](#).

1. On Sametimeserver1/East, open the Sametime Administration Tool. (Select the "Administer the server" link on the Sametime server home page.)
2. Choose Configuration.
3. Choose Connectivity.
4. Choose the Servers in this Community tab.
5. Complete the fields to create the Connection Record.

**Destination server** - Enter the name of the Destination server in the Domino hierarchical server name format that includes the domain or community name. The Destination server is the remote server on which the meeting will become active (or the server that is "invited" to the meeting by the Source server).

For example, when creating the Connection Record on the Sametimeserver1/East server, you specify the Sametimeserver2/West server as the Destination server.

Make sure the server name you enter in the “Destination server” field is an exact case-sensitive match with the server name that appears in the destination Sametime server’s Server Document in the Domino Directory. Also, ensure that the domain or community name (/West in the example) is included in the server name.

**Destination server IP address** - You must enter the fully qualified DNS name or IP address of the destination server in this field. If this field is left blank, meetings started on the source server will not become active on the destination server.

6. Click the Add button.
7. In the "Meeting Servers That Are Connected" settings specify either "People Can Attend from Inside the Organization" or "People Can Attend from the Internet" for the server that you entered in the "Destination server" field when creating the Connection document. It is probable that you will need to select the “People Can Attend from Inside the Organization” setting for the
Note: For more information on these settings, see the "Meeting Servers That Are Connected" options.

8. Repeat this procedure to connect the server in the other domain to the server in this domain. For example, repeat this procedure by using the Sametime Administration Tool on Sametimeserver2/West to create a Connection Record that specifies Sametimeserver1/East as the Destination server. Creating this Connection Record enables Sametimeserver2/West to invite Sametimeserver1/East to the meeting.

This concludes the example of how a single Sametime community can be extended across two Domino domains. These same procedures can be used to extend a Sametime community across more than two Domino domains.

**Alternate ways to share Directory information across domains**

The example procedure for extending a single Sametime community across two Domino domains earlier in this section explains how you can share Directory information to connect two Sametime communities. This topic discusses the Directory information that is shared and describes some alternate, more efficient ways to share Directory information when connecting Sametime communities.

When extending a single Sametime community across multiple Domino domains, each Sametime server that is part of the community must have access to the following Directory information for the other domain(s):

- Person documents
- Group documents
- Server documents - The following fields in the Server document are needed for each Sametime server to support online presence (or awareness) between servers:
  - **Server name** - This field in the Basics tab of the Server document must contain the name of the Sametime server.
  - **Is this a Sametime server?** - This field in the Basics tab of the Server document must be set to "Yes" to indicate that the Server document describes a Sametime server.
  - **Port** - This field in the Ports-Notes Network Ports tab of the Server document must be set to TCP/IP.
  - **Net Address** - This field in the Ports-Notes Network Ports tab must contain the TCP/IP address (for example, sametime.acme.com) of the Sametime server.

**Note:** For more detailed information about the Directory information required by Sametime, see the "Directory views used according to Sametime feature".

To share this Directory information, each domain must replicate the information to the other domains that comprise the Sametime community. In the example scenario described in "Example of extending a single Sametime community across two Domino domains," the entire Directories of two separate Domino domains are replicated between the two Sametime servers. The Domino components of Sametime provide features that you can use to replicate the Directory information in a more efficient manner. You can use either of the following alternate techniques to share Directory information across Domino domains:

- Selective replication of Directory information across domains
- Set up Extended Directory Catalogs to share Directory information across domains

Each technique is discussed briefly below.
Selective replication of Directory information across domains: Instead of replicating the entire Domino Directory between domains, you can use selective replication to replicate only the Person, Group, and Server documents. For example, you can open the Directory database to be replicated to the other domain and use the Replication Settings to replicate a subset of the documents contained in the database. Use a selection formula, such as (Type="Person") | (Type="Group") | (Type="Server" and Sametime="1") to ensure that only the Person, Group, and Server documents (for which the "Is this a Sametime server?" field is set to Yes) are replicated.

For more information on selective replication, see the Domino Administration documentation available from the Documentation Library at the Web site www.lotus.com/ldd.)

Using Extended Directory Catalogs to share Directory information across domains: An Extended Directory Catalog is another Domino feature that can be used to share Directory information when a Sametime community is extended across multiple Domino domains. The Extended Directory Catalog feature allows you to aggregate directory information from several different Domino directories, including directories for different Domino domains, into a single directory catalog. The servers are then configured to access the Extended Server Directory catalog to access directory information.

Before using this feature, the administrator should read the documentation in Domino Administration Help that explains the function and set up of Extended Server Directory Catalogs. This documentation is available from the documentation library on the www.lotus.com/ldd site.

You can follow the procedures in the Domino administration documentation to set up an Extended Server Directory Catalog on the Sametime server. When setting up the Extended Server Directory Catalog to be used by Sametime, note the following when creating the Configuration document for the Extended Server Directory Catalog.

- The Configuration document includes an "Additional fields to include" list in the Basics tab. The following field name entries must exist in the "Additional fields to include" list to ensure that all information needed by Sametime is available in the Extended Server Directory Catalog:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerName</td>
<td>Server name field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>ServerTitle</td>
<td>Server title field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain name field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>ServerBuildNumber</td>
<td>Server build number field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Administrator field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>ServerPlatformDisplay</td>
<td>Operating system field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Sametime</td>
<td>Is this a Sametime server? field in the Basics section of the Server document.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port_0 - Port_7</td>
<td>Ports fields in the Ports - Notes Network Ports section of the Server document. The Port_0 field is required. For completeness it is recommended that you list seven port fields (for example Port_0, Port_1, Port_2, Port_3, Port_4, Port_5, Port_6, and Port_7).</td>
</tr>
<tr>
<td>Protocol_0 - Protocol_7</td>
<td>Protocol fields in the Ports - Notes Network Ports section of the Server document. For completeness, it is recommended that you list seven protocol fields (for example, Protocol_0, Protocol_1, Protocol_2 and so on).</td>
</tr>
<tr>
<td>NetName_0 - NetName_7</td>
<td>Notes Network fields in the Ports - Notes Network Ports section of the Server document. For completeness, it is recommended that you list seven Notes Network fields (for example, NetName_0, NetName_1, NetName_2, and so on.</td>
</tr>
<tr>
<td>NetAddr_0 - NetAddr_7</td>
<td>Net Address fields in the Ports - Notes Network Ports section of the Server document. The NetAddr_0 field is required. For completeness, it is recommended that you list seven Net Address fields.</td>
</tr>
<tr>
<td>Enabled_0 - Enabled_7</td>
<td>Enabled fields in the Ports - Notes Network Ports section of the Server document. The Enabled_0 field is required. For completeness, it is recommended that you list seven Enabled fields.</td>
</tr>
<tr>
<td>SametimeServer</td>
<td>Sametime server field in the Administration section of the Person document.</td>
</tr>
</tbody>
</table>

- The "Advanced" tab of the Configuration document provides a "Selection formula (do not include form)" setting that enables you to specify a selection formula that ensures only the Directory documents required by Sametime are used when the DirCat task creates the Directory Catalog. The selection formula for selecting only the documents required by Sametime is (Type = "Person") | (Type = "Group") | (Type = "Server" and Sametime = "1").
Chapter 15. Introduction to server clusters and the Enterprise Meeting Server

IBM Lotus Sametime server clusters and the IBM Lotus Enterprise Meeting Server (EMS) are Sametime features designed to improve the scalability and reliability of Sametime.

Note: The Lotus Enterprise Meeting Server (EMS) is an optional add-on product for a Sametime deployment that supports a Meeting Services cluster. The EMS is a separate application from the Sametime server and must be purchased separately from IBM. The EMS is not included as part of the Sametime release.

This is the first chapter in a series of chapters that discuss issues and procedures associated with Sametime server clusters and the EMS. You should read the information in this chapter before performing the procedures described in the other chapters about Sametime server clustering. This chapter discusses the following topics:

- Introduction to Sametime server clusters
- Overview of Community Services clustering
- Overview of the Enterprise Meeting Server and Meeting Services clustering

The other chapters that discuss Sametime server clusters and the Lotus Enterprise Meeting Server (EMS) are:

- Chapter 16 - Setting Up a Community Services Cluster Without Clustering the Meeting Services
- Chapter 17 - Setting Up the Enterprise Meeting Server and a Meeting Services Cluster
- Chapter 18 - Clustering the Community Services with the EMS
- Chapter 19 - Setting Up Security for the Enterprise Meeting Server
- Chapter 20 - Administering Server Clusters from the EMS Administration Tool

Creating Sametime server clusters

Creating a Sametime server cluster involves the deployment of multiple Sametime servers for the purpose of:

- Enhancing server scalability and reliability to enable Sametime to meet the demands of large user populations.
- Providing load balancing and failover capabilities for Sametime Community Services and Meeting Services to ensure efficiency of performance and continuity of service in the event of a server failure.

Clustering Community Services and Meeting Services

A single Sametime server includes both Community Services and Meeting Services. These services support the following functionality for Sametime end users:

- **Community Services** - Provide instant messaging and presence capabilities. The Community Services support one-to-one instant messaging sessions and "n-way" chat conferences. (An "n-way" chat conference is an instant messaging session
involving three or more users.) The Community Services also support all presence capabilities of a Sametime server.

- **Meeting Services** - Provide online meeting capabilities including the screen-sharing, whiteboard, interactive audio/video, send Web page, and polling meeting activities. The Sametime Broadcast meeting functionality is also considered a meeting service.

**Note:** For more detailed descriptions of the functionality provided by the Community Services and Meeting Services, see [About the Community Services](#) and [About the Meeting Services](#).

Sametime server clustering enables you to cluster the Community Services separately from the Meeting Services. The ability to cluster the services separately provides the flexibility to manage the services according to the needs of your community. There are three possible clustering options that you can employ to manage the Sametime services. You can:

- Cluster the Community Services without clustering the Meeting Services
- Cluster the Meeting Services without clustering the Community Services
- Cluster both the Community Services and the Meeting Services

Each of these options is discussed below.

**Clustering the Community Services without clustering the Meeting Services**

Organizations that only want to deploy the chat and presence functionality provided by the Community Services might want to cluster the Community Services without clustering the Meeting Services. Such a community would enable users to use the online awareness and instant messaging functionality available with the Sametime Connect client but would not support any meeting functionality, such as the Sametime whiteboard or screen sharing activity.

If you create a Community Services cluster without clustering the Meeting Services, it is not necessary to deploy the Lotus Enterprise Meeting Server (EMS) application. The EMS is required only by the Meeting Services cluster.

Other options are also possible. For example, if Community Services activity in your community is high and Meeting Services activity is low, you might deploy a Community Services cluster to support Community Services activity and a separate single Sametime server to support Meeting Services activity. In this scenario, load balancing and failover is available for the Community Services, but not the Meeting Services.

**Clustering the Meeting Services without clustering the Community Services**

Some organizations may want to cluster the Meeting Services without clustering the Community Services.

To create a Meeting Services cluster, you must deploy the EMS application. After you deploy the EMS, you add Sametime servers to the EMS to create the Meeting Services cluster.

There are two basic scenarios in which the Meeting Services can be clustered without clustering the Community Services:
• You can create a Meeting Services cluster without clustering the Community Services of the Sametime servers. In this scenario, the Sametime servers are added to the EMS to form a Meeting Services cluster. Users can log into the Community Services on the Sametime servers to use the chat and presence functionality, but the Community Services of the Sametime servers do not function as a Community Services cluster.

This configuration provides failover and load balancing for the Meeting Services but not the Community Services. Each user logs into the server specified as the home Sametime server to receive the Community Services functionality. Users access the EMS to schedule and attend meetings in the Meeting Services cluster.

• You can create a Meeting Services cluster while preventing users from accessing the Community Services. In this scenario, only Meeting Services functionality is available to the end users in the community. The Community Services are active on the Sametime servers, but users do not use the instant messaging and presence functionality supported by the Community Services.

In this configuration, you must prevent users from logging into the Community Services on the clustered Sametime servers. To prevent users from logging in, ensure that none of the clustered Sametime servers is specified as a home Sametime server in the LDAP directory person entries of your users. This configuration supports a “meeting-only” deployment of Sametime.

**Note:** In this type of deployment, the Participant List and chat features of the Sametime Meeting Room client will not be available in online meetings.

### Clustering both the Community Services and the Meeting Services

To provide a complete load balancing and failover solution for your Sametime community, you can cluster both the Community Services and Meeting Services of your Sametime servers. If your organization has heavy usage of both the Meeting Services and Community Services functionality, clustering both the Community Services and the Meeting Services of a group of Sametime servers may provide the best solution for enhancing Sametime performance and reliability.

If you use this solution, you must follow this order when creating the server clusters and deploying the EMS:

1. Install the Sametime servers.
2. Deploy the EMS on a separate server.
3. Create the Meeting Services cluster.
4. Create the Community Services cluster.

When you cluster both the Community Services and the Meeting Services of a group of Sametime servers, all of the following are true:

• Administration of all of the Sametime servers in both clusters occurs through an administration tool on the EMS computer called the “EMS Administration Tool.”

• The EMS supports load balancing and failover activity for the Meeting Services cluster only. The EMS does not support the load balancing and failover for the Community Services functionality.

• The Community Services cluster operates independently to support load balancing and failover for the Community Services functionality. However, the servers in the Community Services cluster are “managed” from the EMS application. Essentially, this means that you can administer the servers in the Community Services cluster from the EMS Administration Tool on the EMS.
server, but the EMS does not provide the failover and load balancing functionality for the servers in the Community Services cluster.

Clustering each of the services separately also enables you to dedicate servers to the support of one service or the other. For example, assume you have six Sametime servers (Sametime servers A, B, C, D, E, and F). You can create a Community Services cluster consisting of Sametime servers A and B, and a Meeting Services cluster consisting of Sametime servers C, D, E, and F.

After you have created the clusters, you can configure the Community Services cluster so that only Community Services activity (chat and presence) occurs on Sametime servers A and B. To ensure that only Community Services activity occurs on these servers, you use settings in the EMS Administration Tool to prevent Meeting Services activity from occurring on Sametime servers A and B.

Similarly, you can perform configurations that ensure only Meeting Services activity occurs on Sametime servers C, D, E, and F in the Meeting Services cluster. To ensure that only Meeting Services activity occurs on these servers, you prevent users from logging into the Community Services on Sametime servers C, D, E, and F. You prevent users from logging into the Community Services on Sametime servers C, D, E, and F by performing configurations in the directory that direct all Community Services user logins to the Community Services cluster consisting of Sametime servers A and B.

Segregating Community Services activity to one set of servers and Meeting Services activity to a different set of servers makes it easier to ensure that you have deployed the correct number of servers to support the Community Services and Meeting Services loads of your community.

In addition, the administrator can use the EMS Administration Tool to impose limitations on the amount of Meeting Services activity that occurs on a Sametime server in the Meeting Services cluster. These limitations ensure that each server in the Meeting Services cluster does not incur a larger Meeting Services load than its processing capabilities can handle. If all servers in the Meeting Services cluster are operating near the limits imposed by the administrator, the administrator can add a new server to the Meeting Services cluster to ensure that the appropriate resources are available to support the increased Meeting Services load of the community.

Together, these clustering features increase the reliability of your Sametime community and enable you to scale the Sametime capabilities appropriately as Sametime usage in the community increases.

**About clustering both the Meeting Services and the Community Services**

There are two separate procedures for clustering the Community Services:

- If you want to cluster the Community Services Sametime servers without clustering the Meeting Services, you must perform the procedures discussed in the [Setting up a Community Services cluster without clustering the Meeting Services](#) chapter of this documentation.

- If you want to cluster the Community Services of Sametime servers that have been added to the EMS to function as a Meeting Services cluster, you must perform the procedures discussed in the [Creating a Community Services cluster with the EMS](#) chapter of this documentation.
Overview of Community Services clustering

A Community Services cluster consists of multiple Sametime servers configured to operate together, providing failover and load balancing for the Sametime instant messaging and presence functionality.

Failover ensures that a large community of Sametime users has continuous access to the Community Services. If a server fails, the users in the community can reconnect to a different Sametime server in the Community Services cluster to receive the Community Services functionality.

Load balancing ensures that the Community Services client connections are distributed equally among the Sametime servers in the Community Services cluster.

Because a Community Services cluster operates independently from a Meeting Services cluster, it is possible to cluster the Community Services of Sametime servers without clustering the Meeting Services.

This section provides an overview of Sametime Community Services clustering. This section discusses the following topics:

- **Differences between Community Services clustering and the single server approach** - Creating a Community Services cluster overcomes the limitations imposed by the single-server approach to Community Services used in previous Sametime releases.
- **Load balancing and failover in Community Services clusters** - Discusses how load balancing and failover occurs for the Community Services.

Note that separate procedures are required for each of the following Community Services clustering scenarios:

- **Creating a Community Services cluster without clustering the Meeting Services** - For a step-by-step example of how to create a Community Services cluster without also creating a Meeting Services cluster, see [Setting up a Community Services cluster without clustering the Meeting Services](#).
- **Clustering both the Community Services and the Meeting Services with the EMS** - For a step-by-step example of creating a Community Services cluster that operates with a Meeting Services cluster, see [Creating a Community Services cluster with the Enterprise Meeting Server](#). The procedures in that section explain how to create a Community Services cluster that is managed by the EMS. Note that before you can create a Community Services cluster that is managed by the EMS, you must first deploy the EMS and create the Meeting Services cluster. For information about creating a Meeting Services cluster, see [Setting up the Enterprise Meeting Server and a Meeting Services cluster](#).

### Differences between the clustering and single-server approaches

The Community Services single-server approach requires a user to receive all Community Services functionality from a single Sametime server (or "home" Sametime server).

The Community Services clustering approach enables a user to receive the Community Services functionality from any server within a group (or cluster) of Sametime servers. This capability ensures that users have continuous access to
Community Services functionality if a Sametime server fails. The differences between the Community Services single-server and clustering approaches are discussed below.

**Community Services single-server approach**

In contrast to the Community Services clusters, you can employ a single-server approach to provide Community Services functionality to a community of users. The single-server approach provides Community Services functionality to the community but has no failover capabilities if a server goes down. In the single-server approach:

- Each user receives Community Services functionality from a single Sametime server, which is referred to as a user’s “home” Sametime server.
- To assign a user to a specific home Sametime server, the administrator enters the name of the home Sametime server in the "Sametime server" field of a user’s Person document in the Domino Directory.

**Note:** If the Sametime server is configured to connect to an LDAP directory, the administrator must manually add a field to the LDAP directory to contain the name of each user’s home Sametime server, or use an existing field in the LDAP directory to hold the name of each user’s home Sametime server. For more information, see [Setting the Home Sametime Server](#)

- If the Sametime community includes multiple Sametime servers, the user can make a Community Services connection to any Sametime server in the community, but the user is always redirected to the home Sametime server to receive Community Services functionality. The user receives all Community Services functionality from a single server.

**Note:** Although the user can connect to any Sametime server, the user is always logged in to the Community Services on the user’s home Sametime server. If the user connects to a Sametime server that is not the user’s home Sametime server, the Community Services determine the user’s home Sametime server by examining the user’s directory information and then direct the user login to the home server. Server-to-server communications between the Community Services on different Sametime servers enable the user to be directed to the appropriate server.

The single-server approach provides a form of static load balancing. For example, if a community includes 12,000 users and two Sametime servers, the administrator can assign 6,000 users to home Sametime server 1 and 6,000 users to home Sametime server 2. With this form of load balancing, there is no attempt to distribute the load dynamically. For example, all 6000 users might be logged into Sametime server 1, while only 1,000 users are logged into Sametime server 2. Sametime makes no attempt to divide the load evenly between the two servers.

The single-server approach provides no server failover. In the example above, if Sametime server 1 fails, 6,000 users lose the Community Services functionality. Sametime server 2 could support these 6,000 users; however, the users cannot log in to Sametime server 2 because each user must receive the Community Services functionality from a single “home” Sametime server. The users assigned to home Sametime server 1 must wait until the server is functional again to use any Community Services features.

**Note:** For more information about using multiple Sametime servers without server clustering, see [Deploying multiple Sametime servers](#)
Community Services clustering approach

The Community Services clustering approach enables the administrator to cluster the Community Services of multiple Sametime servers. In the example above, the administrator can cluster the Community Services of Sametime servers 1 and 2 so that they operate as a single logical server. When the Community Services of these servers are clustered, and one server fails, the Sametime Connect client can reconnect and receive the Community Services functionality from another Sametime server in the Community Services cluster. The user is not dependent on a single home server for Community Services functionality.

In the Community Services clustering approach:

- The administrator creates a Domino server cluster. The Domino servers on which the Sametime servers are installed must be clustered to support the Community Services cluster. The administrator also sets up real-time replication of the Sametime databases required to support the Community Services cluster.

- The administrator deploys a rotating DNS system or IBM WebSphere Edge Server (Network Dispatcher) that directs client connections to the Community Services multiplexers on the Sametime servers. This configuration ensures that user connections are distributed equally to the clustered servers. The rotating DNS system or WebSphere Edge Server accomplishes load balancing between the clustered servers.

- (Optional) The administrator can install Community Services multiplexers on separate computers in front of the cluster to remove the connection-handling load from the clustered servers. If the administrator installs Community Services multiplexers on separate computers, the rotating DNS system or WebSphere Edge Server is set up to load balance connections to the Community Services multiplexer machines instead of the Sametime server machines.

- To create a Community Services cluster without also clustering the Meeting Services, the administrator defines a Community Services cluster by creating a document in the Configuration database (stconfig.nsf) on a Sametime server. This document contains a name for the cluster, the DNS name of the rotating DNS system or WebSphere Edge Server that performs load balancing operations, and the list of Sametime servers in the cluster. A user can receive Community Services functionality from any server in the cluster.

To create a Community Services cluster that operates with a Meeting Services cluster and is managed by the EMS, you define the Community Services cluster by altering parameters in the DB2 database used by the EMS. These parameters specify the cluster name, the DNS name of the rotating DNS system or WebSphere Edge Server that performs load balancing operations, and the list of Sametime servers in the cluster.

- Sametime Connect clients that connect to the Community Services cluster must specify the DNS name of the rotating DNS system or WebSphere Edge Server in the "Host" field of the Sametime Connect client Sametime Connectivity settings to connect to the Community Services cluster.

- The administrator assigns each user to a home Sametime cluster (instead of a home Sametime server as required with the single-server approach). The administrator enters the name of the Sametime cluster in the "Sametime server" field of a user’s Person document in the Domino Directory. This Community Services cluster includes multiple Sametime servers and the user can receive Community Services functionality from any Sametime server in the cluster.

If the Sametime server is configured to connect to an LDAP directory, the administrator manually adds a field to the LDAP directory to contain the name of each user’s home Sametime cluster. This is essentially the same requirement as with the single-server approach. The difference is that the field added to the
LDAP directory must contain the name of the Community Services cluster instead of a single home Sametime server.

Note: If you are creating a Community Services cluster that operates with a Meeting Services cluster and is controlled by the EMS, an LDAP directory is mandatory.

Subsequent chapters of this administrator’s guide provide step-by-step examples of how to create the following clusters:

- A Community Services cluster without clustering the Meeting Services
- A Meeting Services cluster without clustering the Community Services
- Both a Meeting Services cluster and a Community Services cluster that is managed by the EMS

Load balancing and failover in Community Services clusters

Load balancing and failover in a Community Services cluster is accomplished primarily through the rotating DNS system or WebSphere Edge Server (Network Dispatcher). Community Services load balancing and failover are discussed briefly below.

Load balancing

When creating a Community Services cluster, you must deploy a rotating DNS system or IBM WebSphere Edge Server in front of the clustered servers. As each client connects, the rotating DNS system or IBM Edge Server distributes the client connections evenly to the servers in the Community Services cluster.

Server failover

If a server in a Community Services cluster fails, the Sametime Connect client attempts a reconnection. The rotating DNS system or WebSphere Edge Server ensures that the client connects to a different server on subsequent connection attempts.

After you have clustered the Community Services, a user is not dependent on a single Sametime server for the Community Services functionality. A successful reconnection to a different server in the cluster enables the Sametime Connect client to continue receiving the Community Services functionality.

For a step-by-step example of how to create a Community Services cluster, see Setting up a Community Services cluster.

Overview of the Enterprise Meeting Server and Meeting Services clustering

A Meeting Services cluster consists of multiple Sametime servers that are controlled by a Sametime application called the Lotus Enterprise Meeting Server (EMS). The EMS and multiple Sametime servers operate together to provide failover and load balancing for Sametime online meetings, including screen-sharing/whiteboard meetings, interactive audio/video meetings, and broadcast meetings.

Failover ensures that a large community of Sametime users has continuous access to the Meeting Services. If a server fails in the middle of a meeting, the active meetings on that server are restarted on a different server in the cluster.
Load balancing ensures that the scheduled and instant meeting load is spread equally among the clustered Sametime servers.

To create a Meeting Services cluster, you must install the Sametime 7.0 servers that will comprise the Meeting Services cluster, deploy the EMS, and then use the EMS Administration Tool to add Sametime servers to the Meeting Services cluster.

The EMS provides the end user and administrator interface to all Sametime servers in the Meeting Services cluster. The EMS also includes the components that accomplish meeting scheduling, meeting booking, load balancing, and meeting file management for meetings occurring on the clustered Sametime servers.

This section provides an overview of Sametime Meeting Services clustering. This section includes the following topics:

- What is the Enterprise Meeting Server?
- Scheduling and load balancing in a Meeting Services cluster
- Booking meetings in the Meeting Services cluster
- Monitoring the health of servers in the cluster
- Managing meeting materials with the EMS
- User interaction with the Enterprise Meeting Center
- Client connectivity in a Meeting Services cluster
- Enterprise Meeting Server security
- LDAP directory access and the Enterprise Meeting Server

### What is the Enterprise Meeting Server?

The Lotus Enterprise Meeting Server (EMS) is the central component of a Sametime Meeting Services cluster. The EMS provides the end user interface, administration tool, and meeting management functionality for all Sametime servers in the Meeting Services cluster.

**Note:** The EMS is a separate product from the Sametime server. The EMS does not ship with the Sametime server and must be purchased from IBM as a separate add-on product.

The EMS is built using Java 2 Platform, Enterprise Edition (J2EE) technologies. These technologies include Java servlets, JavaServer Pages (JSPs), Java applications, and a relational database. The J2EE infrastructure must be in place before you can deploy the EMS. Specifically, this release of the EMS requires the following J2EE infrastructure:

- IBM Universal Database V8.2
- IBM WebSphere MQ 5.3.0.8
- IBM WebSphere Application Server V5.1.1.2

The EMS:

- Installs on a dedicated computer and provides the user interface for all of the Sametime servers in the Meeting Services cluster. Users schedule and attend meetings by accessing the EMS computer. If a user tries to access an individual Sametime server that is part of a Meeting Services cluster, the user is redirected to the EMS. The Sametime Meeting Center interface on a Sametime server is not used after a Sametime server is added to the Meeting Services cluster.
- Provides the central point of administration for the Sametime servers in the Meeting Services cluster. To make administration settings, the administrator
browses to the EMS Administration Tool on the EMS machine. This administration tool provides the administrator interface to all of the Sametime servers in the cluster and allows the administrator to add Sametime servers to the Meeting Services cluster.

- Includes several components that communicate with the clustered Sametime servers to manage the meetings occurring on the servers. These components perform scheduling and load balancing operations that distribute the meeting load equally across the Sametime servers in the Meeting Services cluster. The EMS performs meeting booking operations to ensure that appropriate server resources are available for meetings scheduled in the future and to ensure server performance does not degrade because of high demand.
- Ensures failover occurs if a Sametime server in the Meeting Services cluster becomes unavailable for any reason. The EMS ensures that the meeting load on a failed Sametime server is transferred to the other functioning Sametime servers in the Meeting Services cluster.
- Manages meeting attachments (such as whiteboard files) to ensure these meeting materials are converted to the appropriate formats and stored in a DB2 database so that they are available to end users during Sametime meetings.
- Communicates with the Sametime servers in the cluster using HTTP to perform meeting scheduling and meeting materials management activity. Generally, this communication occurs on HTTP port 80. The HTTP communication between the EMS and the Sametime servers can be encrypted with SSL for tighter security.
- Communicates with the Sametime servers using the Java Message Service (JMS). This JMS communication is implemented using IBM WebSphere MQ message queuing functionality. This JMS communication supports the load balancing, meeting booking, and failover functionality that enables the EMS to provide central meeting management for all of the clustered Sametime servers. The EMS communicates with the Sametime servers using HTTP over port 80. The Sametime servers communicate with the EMS using HTTP over port 80 and TCP/IP port 1414 (WebSphere MQ port).
- Receives and logs information from the Sametime servers. This logging information is available to the administrators through the logging features of the EMS Administration Tool.
- Uses a single LDAP directory that is available on a separate server. You specify the LDAP server to be used by the EMS during the installation and set up of the IBM WebSphere Application Server.

**Note:** The Sametime servers in the cluster must also be configured to connect to this LDAP server. The Sametime servers should be configured to connect to the LDAP server when you install the Sametime servers.

- Does not host meetings. All meetings occur on the clustered Sametime servers. To receive meeting data, the Sametime clients (such as the Meeting Room or Broadcast client) connect directly to the Sametime server in the cluster that hosts the meeting.

**Note:** Users connect to the EMS with a Web browser to attend or schedule meetings. When a user attends the meeting, the Sametime client loads to the user from the Sametime server, not the EMS. The Sametime client then connects to the Sametime server to receive the meeting data (such as screen sharing, whiteboard, or audio/video data).

The diagram below illustrates the interaction between Sametime users and the EMS, the EMS and the Sametime servers, and the Sametime servers and the Sametime clients (end users).
Important: The EMS is not fully functional until at least one Sametime server is added to the EMS. For example, if you have not added a Sametime server to the EMS, some parts of the EMS user interface may function, but you cannot schedule and attend meetings from the EMS until you have added a Sametime server. Multiple Sametime servers must be added to the EMS to support the load balancing and failover functionality.

Scheduling and load balancing in the Meeting Services cluster

The Enterprise Meeting Server (EMS) contains a Scheduler component and a Load Balancer component. These components work together to ensure that a meeting is started on the Sametime server in the Meeting Services cluster that is best able to bear the load of the meeting.

Load balancing of meetings across the Sametime servers in the Meeting Services cluster is accomplished as follows:

1. When an end user schedules a Sametime meeting, all information associated with that meeting, including the meeting start time, is stored in a DB2 database.

   **Note:** The DB2 server is installed as part of the Java 2 Platform, Enterprise Edition (J2EE) infrastructure required to support the EMS application.

2. The Scheduler component runs on the EMS and queries the DB2 database to locate meetings that must be started.

3. The Load Balancer component runs on the EMS and monitors the load on each Sametime server. To monitor the load, the load balancer receives JMS messages from each Sametime server in the cluster. (The JMS messages are transmitted...
on WebSphere MQ messaging queues.) The JMS messages provide information such as the number of meetings active on each Sametime server and the number of users in each meeting.

4. When the Scheduler locates a meeting to be started, it consults the Load Balancer to determine which Sametime server in the cluster should host the meeting.

   The Load Balancer considers several factors to determine the Sametime server that should host a meeting. These factors include the past reliability of the server, the current load of the server, and the usage limits (or booking limits) imposed on the server by the system administrator.

5. After consulting the Load Balancer, the Scheduler starts the meeting on the Sametime server selected by the Load Balancer.

**Booking meetings in the Meeting Services cluster**

The Enterprise Meeting Server (EMS) contains a Booking Agent component that enables an administrator to reserve the resources of Sametime servers that are part of the Meeting Services cluster. The Booking Agent:

- Ensures that server resources are available for meetings scheduled in the future.
- Enhances the reliability of servers in the cluster. The booking capability can prevent a Sametime server from failing or performing poorly because of a sudden, unexpected surge in meeting activity.
- Provides a way to limit Meeting Services usage on each server in the cluster to administrator-specified limits
- Prevents meetings from being scheduled at times when the anticipated load on the Meeting Services cluster is already high.
- Enables the administrator to "turn off" all Meeting Services functionality on a Sametime server. This capability can be used to ensure that a server managed by the EMS is dedicated to supporting only Community Services functionality.

The booking functionality is summarized below:

1. Immediately after adding a Sametime server to the Meeting Services cluster, the administrator uses the EMS Administration Tool to set Meeting Services usage limits for the server.

   The administrator can set several different parameters to limit the meeting activity, including:
   - Maximum number of meetings on the server
   - Maximum number of instant meetings on the server
   - Maximum number of participants in any one meeting

2. These server limits provide the EMS Booking Agent with a way to determine the aggregate demand that can be supported by the entire Meeting Services cluster.

   For example, if you have two Sametime servers in the Meeting Services cluster, and you set the maximum number of meetings on each server to 100 meetings, the Booking Agent assumes the two servers in the Meeting Services cluster can support an aggregate demand of 200 meetings at any given time.

3. When an end user schedules a meeting, the Booking Agent determines if the meeting exceeds the aggregate limits for the Meeting Services cluster (as specified by the administrator).
For example, if the aggregate limit of meetings in a cluster is 200, and an end user schedules a meeting to start on April 5 at 2:00 PM when there are already 200 meetings scheduled to be active, the end user is prompted to reschedule the meeting.

The administrator can also use the server limits settings to "turn off" or prevent Meeting Services activity from occurring on the Sametime server. For example, if the administrator sets the "Maximum number of meetings on the server" to 0 (zero) and the "Maximum number of instant meetings" to 0, no meeting activity can occur on the server. Turning off the Meeting Services functionality enables the administrator to dedicate that server to the Community Services functionality.

The administrator can use the logging and monitoring features of the EMS Administration Tool to determine the load that each server in the cluster is handling. If the servers in the cluster are consistently operating near the limits specified by the administrator, the administrator can add new Sametime servers to the cluster to spread the meeting load among a greater number of servers.

For more information about adding Sametime servers to a Meeting Services cluster and setting the parameters that limit server capacity, see the following topics in the Setting up the Enterprise Meeting Server and a Meeting Services cluster section of this documentation:

- Adding Sametime servers to the Meeting Services cluster
- Specifying capacity limits for the Sametime servers

Monitoring the health of servers in the cluster

The Enterprise Meeting Server (EMS) listens for health messages from the Sametime servers in the Meeting Services cluster. These health messages provide the EMS with information indicating that a Sametime server has failed, or has problems that may cause a server failure.

Health monitoring component of each Sametime server

Each Sametime server contains a health monitoring component that is responsible for periodically sending a positive health message to the EMS. This health message is transmitted using the Java Messaging Service (JMS) on a WebSphere MQ messaging queue. The health monitor can also send a negative message if it determines that one or more of the critical Sametime server components is unavailable.

Note: The health monitor component on the Sametime server uses a server event system to communicate with other internal components of the Sametime server. The health monitor sends health requests to these internal components of the Sametime server. If a server component fails to respond to one of these requests, the health monitor assumes an error has occurred and that the server is unable to function. The health monitor then sends a negative health message to the EMS on the JMS queue.

Health monitoring components of the EMS

The DB2 database used by the EMS maintains a list of Sametime servers that are available for scheduled meetings. When the EMS receives a negative health message from one of the Sametime servers, the health monitoring components on the EMS remove the Sametime server from the list of servers available for scheduled meetings.
The EMS Scheduler application is also alerted to the unhealthy state of the server. The EMS Scheduler and the Load Balancer work together to move the currently active meetings on the unhealthy server to other servers in the Meeting Services cluster. The server is taken off line and its meeting load fails over to the functioning (or "healthy") servers in the Meeting Services cluster.

**Note:** All communication between the EMS health monitoring components and the Sametime servers occurs using JMS over WebSphere MQ messaging queues.

**Managing meeting materials with the EMS**

The Enterprise Meeting Server (EMS) contains a materials management system that handles meeting materials posted to the EMS for use during Sametime meetings.

**Note:** With standard Sametime deployments, the term "meeting materials" is synonymous with files posted to the EMS for display in the whiteboard tool of the Sametime Meeting Room client. Developers can use the IBM Software Development Kits to create applications that allow users to present other types of meeting materials during Sametime meetings. Software developers can also extend the materials management system to store and retrieve these meeting materials.

The basic operation of the EMS materials management system is described below.

1. An end user accesses the EMS to schedule a whiteboard meeting.
2. When creating the meeting, the user selects the Files tab on the New Meeting page of the EMS and attaches a file (for example, a word processor file) to be presented on the whiteboard during a meeting.
3. The user saves the meeting.
4. When the user saves the meeting with the attached file, a "user servlet" on the EMS stores the attached file in the DB2 database used by the EMS.
5. When the meeting starts, a "materials system servlet" on the Sametime server connects to the EMS to retrieve the file (or meeting material) associated with the meeting.
6. A "server servlet" on the EMS responds to the request from the "materials system servlet" on the Sametime server. The EMS "server servlet" locates the file in the DB2 database and returns it to the materials system on the Sametime server.
7. The Sametime server converts the file to the format required by the Meeting Room client whiteboard tool and loads the file into the whiteboard for presentation during the meeting.
8. In addition to loading the converted file to the whiteboard, the Sametime server materials system returns the converted files to the "server servlet" on the EMS.
9. The server servlet on the EMS saves the converted file to the DB2 database. Storing the converted files in the DB2 database ensures that the files are:
   - Available if a server crashes while a meeting is in progress. When a server crashes, the failover process ensures the meeting is restarted on a different server in the Meeting Services cluster. Storing converted files in DB2 ensures the whiteboard files can be retrieved for the restarted meetings.
   - Converted only once for repeated meetings. The server in the cluster that hosts a particular meeting is determined at meeting start time. When a user schedules a meeting to repeat as a series, each meeting in the series might be started on a different server in the cluster. Storing the files in DB2 ensures
that the files are converted only once for the series of repeated meetings and can be easily retrieved if the next meeting in the series starts on a different server than the previous meeting.

**Setting up security for the EMS materials management system**
The materials management system described above uses HTTP to transmit meeting materials between the EMS machine and the clustered Sametime servers. The transmission of meeting materials between these machines creates a security risk. Unauthorized users may attempt to gain access to the meeting materials handled by the servlets on the Sametime server and the EMS. The administrator can use SSL to encrypt the HTTP traffic between the EMS and Sametime servers to protect these materials. For more information, see [Encrypting HTTP traffic between the EMS and Sametime servers with SSL](#).

**User interaction with the Enterprise Meeting Server**
Once the Enterprise Meeting Server (EMS) is deployed, and Sametime servers are added to the EMS to create the Meeting Services cluster, the EMS becomes the user interface for all of the Sametime servers in the cluster.

Any user attempting to directly access a Sametime server in the Meeting Services cluster with a Web browser is redirected to the EMS. Although the meetings actually occur on different servers in the cluster (as determined by the Scheduler and Load Balancer components), the end user always accesses the EMS machine to schedule and attend meetings. The end user is not aware these meetings occur on different servers.

The end-user interface for the EMS includes some features that are not available in the end-user interface of a non-clustered Sametime server. For example, end users can use an EMS search feature to search for meetings in the EMS. Users can also use a calendar to view scheduled meetings, or search for meetings by day, week, or month. For more information about the EMS end-user features, see the end user help available from the user interface of the EMS.

**Note:** The administrator can use the Unlisted view in the EMS end-user interface to view unlisted meetings. The Unlisted view is not available to end users. However, an end user can search for an unlisted meeting or view his or her own unlisted meetings.

**Meeting Services failover and reattending meetings**
Meeting Services failover occurs in any of the following situations:

- A Sametime server crashes
- Connectivity is lost between the EMS and a server in the Meeting Services cluster
- The health monitoring components of the EMS detect a problem with a Sametime server

When failover occurs, all active meetings on the server are restarted on a different server in the cluster. The meetings are restarted based on interactions between the EMS Scheduler and Load Balancer.

When a server fails and a meeting is active, users attending the meeting receive a message indicating a problem has occurred. The meeting is restarted on a different server in the Meeting Services cluster. In most cases, the end user can reattend the
meeting simply by refreshing the browser window. The user can also reattend the meeting by browsing back to the EMS machine and selecting the meeting name from the list of available meetings.

**Client connectivity in a Meeting Services cluster**

End users schedule and attend meetings in a Meeting Services cluster by making Web browser (HTTP) connections to the EMS.

When a meeting starts, end users receive the Sametime Meeting Room client or Sametime Broadcast client directly from the Sametime servers. The meeting data also passes directly from the Sametime servers to the Meeting Room and Broadcast clients. Client connectivity to servers in a Meeting Services cluster is summarized briefly below.

**Meeting Room and Broadcast client connections**

The EMS operates as the meeting scheduling and attending interface for the end users, but the users do not receive clients or any interactive or broadcast meeting data from the EMS.

When a user attends a meeting, Meeting Room client and Broadcast client connectivity works as follows:

1. The user accesses the EMS using a Web browser and selects a link to attend a meeting.
2. The EMS retrieves the following information from the DB2 database:
   - The server in the Meeting Services cluster that the EMS has selected to host the meeting.
   - The client connectivity parameters, such as TCP/IP ports and HTTP tunneling settings, for the selected server.
   The EMS uses HTTP to pass this information to the connecting Web browser.
3. The Web browser uses the information received from the EMS to make an HTTP connection to the Sametime server hosting the meeting.
4. At this point, Sametime client connectivity to the Meeting Services, Audio/Video Services, and Broadcast Services on a clustered Sametime server functions exactly like Sametime client connectivity to a server that is not clustered.

The Meeting Room client or Broadcast client required to attend the meeting is loaded to the user’s Web browser from the Sametime server in the Meeting Services cluster that is hosting the meeting.

The meeting data also passes between the Sametime servers and the user’s Meeting Room or Broadcast client. The Sametime clients connect to the Sametime server in the cluster that is hosting the meeting to receive the meeting data. A user does not receive the Sametime clients or the meeting data from the EMS.

For more information about how Sametime clients connect to Sametime servers, see [Sametime Connect client connection processes](#) and [Meeting Room and Broadcast client connection processes](#).

**Sametime Connect client connections**

The connection process of Sametime Connect clients depends on whether the Community Services of the Sametime servers are clustered or not clustered:

- If the Community Services are clustered, a Sametime Connect client connects to a rotating DNS system or WebSphere Edge Server (Network Dispatcher). For a description of this process, see Configuring client connectivity for the
Enterprise Note: Encrypting names of users EMS Server
To Encrypting for Use of Authentication specified in the following sections
The role of users can be assigned to the roles or connections in the directory or community Services. In this case, you can use the WebSphere Community Access plug-in or Java Plug-in connectivity settings.

Note: In either case above, Sametime Connect clients do not access the EMS. Note that it is also possible for Sametime Connect clients to connect to other Sametime servers in the community that are not part of either a Community Services cluster or a Meeting Services cluster (but are members of the same community in the sense that they share the directory accessed by the EMS and its clustered servers).

Enterprise Meeting Server security
The Enterprise Meeting Server security involves the following:
- Authentication and user access control
- Encrypting Web browser connections to the EMS with SSL
- Encrypting connections between the EMS and Sametime servers with SSL

Each of these security topics are discussed briefly below.

Authentication and user access control
The EMS uses security roles to determine whether users are authenticated and to specify the level of access an individual user or group has to the EMS. Authentication and access control are discussed below.

- **Authentication** - The administrator can configure the EMS security roles to require authentication or allow anonymous access to the EMS. If the security roles are configured to require authentication, the users are authenticated against an LDAP directory.

- **Access control** - If authentication is required, the security roles also determine the level of access a particular user (or group) has to the EMS. For example, you can assign a security role to one group of users to enable users in that group to attend but not create meetings in the EMS. You can assign a different security role to another group of users to enable those users to both create and attend meetings in the EMS.

Use the WebSphere Advanced Administration Console to configure security roles for authentication and access control. For more information about configuring the EMS security roles, see **Securing user access to the Enterprise Meeting Server**

Encrypting Web browser connections to the EMS with SSL
To access the EMS, an end user makes an HTTP connection to the IBM HTTP Server on the EMS machine. The IBM HTTP Server passes HTTP requests to the EMS on the WebSphere server. The HTTP traffic passing between the Web browser and the EMS might contain sensitive meeting information such as user names and passwords. To protect this information, the administrator can encrypt connections to the IBM HTTP Server with SSL. For more information, see **Encrypting Web browser connections to the EMS with SSL**
Securing connections between the EMS and the Sametime servers
Servlets on the EMS and Sametime servers communicate to start meetings, manage meetings, and transmit meeting materials, such as whiteboard files, between the servers. To protect this information, the administrator must configure the servers to authenticate when making these server-to-server connections. Connections to Sametime server and EMS servlets can also be encrypted with SSL to prevent unauthorized users from gaining access to the data or meeting materials transmitted over these connections. For more information, see Encrypting HTTP traffic between the EMS and Sametime servers with SSL.

LDAP directory access and the Enterprise Meeting Server
Enterprise Meeting Services (EMS) users are maintained in a single LDAP directory on a dedicated LDAP directory server. This topic briefly discusses the following issues pertaining to LDAP directory access in an EMS environment:
• Purposes for LDAP directory access
• Synchronizing LDAP directory access for Sametime and WebSphere/EMS servers

Purposes for LDAP directory access
In an EMS environment, the WebSphere server on which the EMS is installed and the Sametime servers that comprise the Meeting Services cluster require access to the same LDAP directory. The Sametime server and the WebSphere server access the LDAP directory for different reasons. These reasons are discussed below.

WebSphere server LDAP directory access
Web browser users access the EMS to schedule meetings, attend meetings, download clients, or administer the server. The WebSphere server must access the LDAP directory to perform the following operations for these Web browser users:
• Authenticate the users against the LDAP directory. Users are authenticated (or not authenticated) based on the configuration of EMS security roles. If the EMS security roles are configured to require authentication, the Security Server component of the WebSphere administrative server authenticates the Web browser users against the entries in the LDAP directory.
• Enable Web browser users to search person and group entries in the LDAP directory. Web browser users must search these LDAP directory entries when adding people and groups to the Restrict To list when restricting meeting attendance from the New Meeting form in the EMS.

Sametime server LDAP directory access
The Sametime servers in the Meeting Services cluster authenticate Sametime Connect users and must enable the users to search the LDAP directory. The Sametime server must access the LDAP directory to perform the following operations for these Sametime Connect users:
• Authenticate Community Services clients such as Sametime Connect. Sametime Connect clients connect to the Community Services on the Sametime servers, not the EMS. Sametime Connect clients do not connect to the EMS and cannot be authenticated by WebSphere.
• Enable Sametime Connect users to search the LDAP directory when adding people and groups to the Sametime Connect contact list or privacy list.
Synchronizing LDAP directory access for Sametime and WebSphere servers

Because the WebSphere server and the Sametime servers must access the LDAP Directory, there are two separate LDAP configurations that occur during an EMS deployment: a Sametime server LDAP configuration and a WebSphere server LDAP configuration.

When the Sametime server is installed, it is configured to connect to the LDAP server. During the Sametime server installation, the administrator selects an option that enables the Sametime server to access an LDAP directory. After the Sametime installation completes, the administrator uses the Sametime Administration Tool on the Sametime server to configure the LDAP Directory settings that enable the Sametime server to access a specific LDAP directory type. Common LDAP directory types used with Sametime include:

- Netscape Directory
- Microsoft Exchange Directory
- Microsoft Active Directory
- IBM SecureWay Directory
- Domino Directory

For more information on configuring a Sametime server to access an LDAP directory, see Setting up an LDAP connection.

In a separate procedure, the WebSphere server is configured to access the LDAP server following the WebSphere installation. The administrator uses the WebSphere Administrative Console to configure the LDAP Directory settings that enable the WebSphere/EMS server to access a specific LDAP directory type.

Both the Sametime server LDAP configuration and WebSphere server LDAP configuration require the administrator to have knowledge of LDAP search filters and LDAP directory schemas. Generally, the specific schema used by an LDAP directory depends on the LDAP directory type used in the EMS environment.

Because both the Sametime servers and the EMS/WebSphere server will access the same LDAP directory, the same LDAP search filters and directory entry attributes that are specified during the Sametime server LDAP configuration can be specified during the WebSphere server LDAP configuration. For more information on the WebSphere LDAP configuration, see Configuring WebSphere server security and LDAP directory access in the “Setting Up the Enterprise Meeting Server and a Meeting Services Cluster” chapter of this documentation.
Chapter 16. Setting up a Community Services cluster without clustering the Meeting Services

Community Services clusters provide Community Services load balancing and failover functionality for large communities. This chapter provides an example of how to cluster the Community Services of a group of IBM Lotus Sametime servers without also clustering the Meeting Services of the Sametime servers. The example in this chapter explains how to cluster the Community Services of two Sametime servers. Once you understand how to cluster the Community Services of two Sametime servers, you can easily add the Community Services of other Sametime servers to the cluster.

Important: If you also want to cluster the Meeting Services of the Sametime servers, or if you want to administer the servers in the Community Services cluster from the Lotus Enterprise Meeting Server (EMS), do not use the procedures in this chapter to create a Community Services cluster. In those scenarios, you must use the procedures discussed in "Chapter 20 - Creating a Community Services cluster with the EMS" to create the Community Services cluster.

This chapter includes the following topics pertaining to creating a Community Services cluster without creating a Meeting Services cluster:

- Community Services cluster setup procedures (without the EMS)
- Adding another server to a Community Services cluster
- Creating multiple Community Services clusters in a single Sametime community
- Rotating DNS Limitations with cached DNS resolve requests

Note: For more information about the purpose of a Community Services cluster, see "Overview of Community Services clustering."

You can find additional information about the EMS and Sametime server clusters in the following chapters:

- Chapter 15 - Introduction to Sametime Server Clusters and the Enterprise meeting Server
- Chapter 17 - Setting up a Web Conference Management Server and a Meeting Services cluster
- Chapter 18 - Creating a Community Services cluster with the EMS
- Chapter 19 - Setting up security for the Enterprise meeting Server
- Chapter 20 - Administering server clusters from the EMS Administration Tool

Community Services cluster setup procedures

The procedures required to set up a Community Services cluster without clustering the Meeting Services are listed below. Use the information in these procedures in conjunction with your existing knowledge of your Sametime environment when clustering the Community Services of your Sametime servers. Your unique Sametime environment might require some variation from these procedures.
These procedures provide an example of how to cluster the Community Services of two Sametime servers. Once you understand how to cluster the Community Services of two servers, you can easily add the Community Services of other Sametime servers to the cluster.

The process of setting up a Community Services cluster without clustering the Meeting Services is described in ten steps:

1. Community Services clustering preparations
2. Deploying an LDAP Directory server
3. Installing the Sametime servers
4. Creating a Domino server cluster
5. Setting up replication of Sametime databases
6. (Optional) Deploying separate Community Services multiplexers
7. Setting up the load balancing mechanism (rotating DNS or Network Dispatcher)
8. Creating a cluster document in the Configuration database (stconfig.nsf)
9. Creating a cluster document on other Sametime servers in the community
10. Configuring client connectivity

Note: The process of setting up a Community Services cluster requires you to create a Domino server cluster (as described in step 4). A maximum of six Domino servers can operate as part of a Domino server cluster. Because of this limitation, the maximum number of Sametime servers that can operate as part of a Community Services cluster is six. Generally, the largest communities can be supported with less than six Sametime servers operating in a cluster.

Community Services clustering preparations

Ensuring you have the hardware necessary to complete this example is the first of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services.

This example of a Community Services cluster requires the test computers listed below.

- Two computers are required for Sametime server installations.
- (Optional) One computer to serve as an LDAP Directory server. You can maintain your Sametime community in either an LDAP or a Domino Directory.
- (Optional) Two computers are required if you want to install Community Services multiplexers on separate machines.

This example also requires you to set up a rotating DNS system or IBM WebSphere Edge Server (Network Dispatcher) to accomplish load balancing for the Community Services cluster. The rotating DNS system is configured on a DNS server. If you decide to use a WebSphere Edge Server for load balancing instead of rotating DNS, an additional machine is also required for the IBM WebSphere Edge Server installation.

Next step:

Next, review the information provided for deploying an LDAP Directory server.
Deploying an LDAP directory server

Deploying an LDAP Directory server is the second of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services.

Using an LDAP directory is optional. You can use the Domino Directory that is on the Sametime servers that operate as part of the Community Services cluster as the directory that defines your community of users. The Domino Directory can be maintained in its native format; it is not mandatory to enable the LDAP task on the Domino servers on which Sametime is installed. If you do not want to use an LDAP directory, skip the procedure "Using a Domino server as an LDAP server," described below, and continue to the next procedure, "Installing the Sametime servers."

In this example, the community of users is defined in an LDAP directory that is maintained on a separate server; the server containing the LDAP directory is not part of the Community Services cluster.

If you want to use an LDAP directory with your Community Services cluster, continue with the procedures below. Note the following advantages and issues pertaining to deploying an LDAP directory on a separate server:

• Using an LDAP directory on a separate server can conserve system resources for the real-time interactive services of Sametime by removing directory management tasks from the Sametime servers.

• You can set up the LDAP directory server to failover to another LDAP directory server. Providing failover for the directory server improves the reliability of the Community Services cluster.

• After you install the Sametime servers that will be part of the Community Services cluster, you must configure the Sametime servers to connect to the LDAP server. This process is described in "Installing the Sametime servers."

Using a Domino server as an LDAP server

In this example, you maintain the LDAP directory on a separate Domino server. This Domino server is not part of the Community Services cluster. The Domino server has the LDAP task enabled so that the Domino Directory on the server can function as an LDAP directory.

Note: If you choose to use an LDAP directory with your Community Services cluster, you are not limited to using a Domino directory with the LDAP task enabled. You can also use other LDAP directories, such as Microsoft Exchange 5.5, Microsoft Active Directory, Netscape LDAP directory, or IBM SecureWay directory as the directory that defines your Sametime community.

The information below summarizes how you can use a Domino server as an LDAP server. For more detailed information on this topic, see the Lotus Domino Administrator 7 Help available from the documentation library at www.lotus.com/ldd.

To use a Domino server as the LDAP directory server:

1. Install the Domino server and either replicate an existing Domino Directory to the server or populate the Domino Directory by registering users.

   Note: Sametime requires each user to have an Internet password on their Person document in the Domino Directory.

2. Create a full-text index for the Domino Directory on the Domino server.
3. Start the Domino server.
4. Start the LDAP task. To start the LDAP task, enter "load LDAP" at the Domino server console.

**Next step:**
Next, review the information provided for **installing the Sametime servers**

**Installing the Sametime servers for the Community Services cluster**

Installing the Sametime servers is the third of ten tasks associated with [setting up a Community Services cluster without clustering the Meeting Services](stinstall.nsf or stinstall.pdf). Note the following about the Sametime server installations.

- You must install two Domino 7.0 servers and install the Sametime 7.0 servers on top of the Domino servers, as described in the *Lotus Sametime Installation Guide*.
- The Sametime servers must operate as part of the same Domino domain. To be part of the same Domino domain, the Sametime servers must be registered in the same Domino Directory. The Domino Directory must replicate between the servers.

**Note:** The Domino Directory must replicate between the Sametime/Domino servers even if you are maintaining the user community in an LDAP directory on a separate server that is not part of the Community Services cluster. Replication of the Domino Directory is required for administrative purposes. The LDAP directory serves as the user repository for the members of the Sametime community; the Domino Directory is required for the proper functioning of the Sametime servers on which Sametime is installed.

- The Sametime servers must have TCP/IP connectivity on the following ports:
  - **Port 1516** - The default port for Sametime server-to-server Community Services connections and for extending meeting invitations to other Sametime servers in a community to support Sametime "invited server" functionality.
  - **Port 1503** - The default port for Sametime server-to-server Meeting Services connections.
  - **Port 1352** - The default port for server-to-server connections between the Domino servers on which the Sametime servers are installed.
- If you have deployed an LDAP directory on a separate server, each of the Sametime servers must be configured to connect to the LDAP directory server you set up in the previous procedure ("Deploying an LDAP directory server"). The Sametime servers must have TCP/IP connectivity to the LDAP server on port 389 (the default LDAP port for Sametime).

**Setting up a connection to a Domino LDAP server**

If you are maintaining your Sametime community in a Domino LDAP-enabled directory, you can use the information below to enable the Sametime servers to connect to the LDAP directory.

If you are maintaining your Sametime community in a Domino directory in its native format (the directory is not LDAP-enabled), skip this procedure and continue to the procedure titled [create a Domino server cluster](create).**Note:** The values used below are suggested values for a Domino Directory enabled for LDAP access and do not apply to other LDAP directories. For more
information about setting up the LDAP connection and the configuration settings described below, or to configure Sametime to access an LDAP directory on a different LDAP server (such as a Microsoft, Netscape, or IBM LDAP server), see [Using LDAP with the Sametime server](#) and [Setting up an LDAP connection](#).

To set up a connection to a Domino LDAP server:

1. Install a Domino server and then install a Sametime server on top of the Domino server as described in the *Lotus Sametime Installation Guide* (stinstall.nsf or stinstall.pdf).
2. During the Sametime server installation, choose “LDAP directory” when prompted for the directory type.
3. After the installation completes, open the Sametime Administration Tool on the Sametime server.
5. In the LDAP Directory-Connectivity settings of the Sametime Administration Tool, enter the following settings:
   - **Host name or IP address of the LDAP server** - Must specify the address of the LDAP server.
   - **Position of this server in the search order** - Suggested value is ”1.”
   - **Use authenticated binding to the LDAP server (optional)** - For a test deployment, clear the check mark from this setting to enable the Sametime server to bind to the LDAP server as an anonymous user.
   - **Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server** - For a test deployment, clear the check mark from this setting to prevent passwords and other directory information that is passing between the Sametime server and the LDAP server from being encrypted with SSL.
6. Click the Update button at the bottom of the Connectivity tab.
8. In the LDAP Directory-Basics settings of the Sametime Administration Tool, enter the following settings:
   - **Where to start searching for people** - Suggested value is o=servername (where servername is the name of the LDAP server).
   - **Scope for searching for a person** - Suggested value is ”recursive.”
   - **The attribute of the person entry that defines the person’s name** - Suggested value is ”cn.”
   - **Attribute used to distinguish between two similar person names** - Suggested value is ”mail.”
   - **The object class used to determine if an entry is a person** - Suggested value is ”organizationalPerson.”
   - **Where to start searching for groups** - Leave this setting blank.
   - **Scope for searching for groups** - Suggested value is ”recursive.”
   - **Attribute used to distinguish between two similar group names** - Suggested value is ”description.”
   - **The group object class used to determine if an entry is a group** - Suggested value is ”groupOfNames.”
9. Click the Update button.
11. In the LDAP Directory-Authentication settings of the Sametime Administration Tool, make the following settings:
   • **Search filter to use when resolving a user name to a distinguished name** - Suggested value is:
     \( (&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s*))) \)
   • **Name of the Home Server attribute** - Suggested value is the attribute in the LDAP directory that holds the home Sametime server name. In a Domino Directory, this is the "Sametime Server" field of the Person document.

12. Click the Update button.
14. In the LDAP Directory-Searching settings of the Sametime Administration Tool, make the following settings:
   • **Search filter for resolving person names** - Suggested value is:
     \( (&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s*))) \)
   • **Search filter for resolving group names** - Suggested value is:
     \( (&(objectclass=groupOfNames)(cn=%s*)) \)

15. Click the Update button.
17. In the LDAP Directory-Group Contents settings of the Sametime Administration Tool, make the following setting:
   • **Attribute in the group object class that has the names of the group members** - Suggested value is "member."

18. Click the Update button and restart the server for the changes to take effect.

**Next step:**

Next, create a Domino server cluster

### Creating a Domino server cluster

Creating a Domino server cluster is the fourth of ten tasks required to set up a Community Services cluster without clustering the Meeting Services.

**Note:** This topic provides basic information on creating a Domino server cluster. If you are unfamiliar with the functioning of Domino clusters, see the *Lotus Domino Administrator 7 Help*, which is available from the Documentation Library at www.lotus.com/ldd, before creating the Domino server cluster.

To create a cluster, you must have at least Author access and Delete Documents rights in the Domino Directory, and at least Author access in the Administration Requests database.

To create a Domino server cluster:

1. On one of the Sametime servers, start the Domino administrator client. (To start this client on a Windows machine, choose Start - Run and type nlnotes.exe adminonly.)
   **Note** When the administrator client starts, make sure the Sametime server is the current server.

2. Click the Configuration tab.

3. In the Tasks pane, expand Server and click All Server Documents.

4. In the Results pane, select the servers you want to add to the cluster. (Select both Sametime servers that you installed in the previous step)

5. Click "Add to Cluster."
6. In the Cluster Name dialog box, choose Create New Cluster, and then click OK.
7. Type the name of the new cluster and then click OK.
8. Choose Yes to add the servers to the cluster immediately. The cluster information is immediately added to the Domino Directory of the server you used to create the cluster.
9. If the server you used to create the Domino cluster is part of the cluster, the server immediately starts the cluster processes and replicates its Domino Directory with another server in the cluster. This process informs other servers in the cluster that they are a part of the cluster. If you did not use a cluster member to create the cluster, this process starts when the Domino Directory of the server you used to create the cluster replicates with the Domino Directory of a server in the cluster.

**Note:** The Domino Administration Process can also be used to create a Domino server cluster. For more information about Domino server clusters, see the *Lotus Domino Administrator 7 Help*, which is available from the Documentation Library at www.lotus.com/ldd.

### Verifying a cluster was created properly

You can do the following to verify the cluster was created correctly.

<table>
<thead>
<tr>
<th>Action</th>
<th>What you should see</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Domino Administrator, expand Clusters in the Server pane.</td>
<td>The name of the cluster followed by the names of the cluster servers.</td>
</tr>
<tr>
<td>From the Domino Administrator, click a cluster server in the Server pane, and then click the Server - Status tab.</td>
<td>CLDBDIR (the Cluster Database Directory Manager) and CLREPL (the Cluster Replicator) in the Task list.</td>
</tr>
<tr>
<td>From the Domino Administrator, click a cluster server in the Server pane, and then click the Files tab.</td>
<td>The title “Cluster Directory (R4)” and the file name “clddb.rsn” to show that Domino created the Cluster Database Directory.</td>
</tr>
<tr>
<td>Compare the replica IDs of the Cluster Database Directories on each cluster server.</td>
<td>The same replica ID on each server.</td>
</tr>
</tbody>
</table>

### Next step:

Next, set up replication of the Sametime databases required to support the Community Services cluster.

### Setting up replication of Sametime databases

Setting up replication of Sametime databases is the fifth of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services.

To set up real-time replication between the clustered Domino servers, you must create a new replica of each of the databases listed below on the clustered Domino servers. For example, on Sametime server 1, use a Notes client to open vpuserinfo.nsf, choose File-Replication-New Replica, and create a new replica of vpuserinfo.nsf on Sametime server 2.

Creating the new replica is the only procedure required to set up real-time replication of the databases in the Domino server cluster. Whenever a change occurs to one of the databases, the change is automatically pushed to the replicas on the other servers in the Domino cluster.
Note: By default, a Domino server does not allow you to create new replicas on a server. To ensure you can create new replicas on the Sametime server, you must do the following:

1. Use a Notes client to open the Server document of the Domino server on which Sametime is installed.
2. Click on the Security tab.
3. In the Server Access - Create replica databases: field, enter the appropriate user or group name to enable those users to create new replicas on the Domino server.

To support a Community Services cluster, the following databases must replicate in real-time between the clustered Domino servers. You must create replicas of the following databases on each of the clustered Domino servers that will be part of the Community Services cluster:

- **The Privacy database (vpuserinfo.nsf)** - Stores privacy information and contact lists for Sametime Connect users.
- **The Domino Directory database (names.nsf)** - Contains Domino and Sametime server configuration data. This database must be replicated to all Sametime servers in the Community Services cluster.

Note: Real-time replication functionality is available only in a Domino server cluster. If you are unfamiliar with the functioning of Domino clusters, you should review the information in *Lotus Domino Administrator 7 Help*, which is available from the Documentation Library at www-10.lotus.com/ldd, before creating the Domino server cluster.

**Ensuring database synchronization and prompt replication**

The administrator should be aware of these issues regarding replication of the Sametime databases:

- To ensure that these databases remain synchronized, you should also set up a scheduled replication of the databases using Domino Connect documents. You might want to schedule these replications to occur during times of low server usage to minimize their impact on server performance for the users.
- The vpuserinfo.nsf database must replicate quickly. If a user makes changes to the privacy settings in the Sametime Connect client, these changes should be reflected on all servers in the Community Services cluster in the shortest time possible. If real-time replication is taking too long for these changes to be reflected on all servers in the cluster, modify the server parameter VP_OD_CACHE_AGE in the [Config] section of the Sametime.ini file on the server. Set the value of VP_OD_CACHE_AGE to the maximum interval in minutes between replication operations. The value specifies the maximum amount of time it should take for a change to the vpuserinfo.nsf database on one server to replicate to another server.

The diagram below shows the server cluster at this point:
Next step: Next, **deploy separate Community Services multiplexers** on separate machines.

**Deploying separate Community Services multiplexers (optional)**

Deploying separate Community Services multiplexers is the sixth of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services. Deploying separate multiplexers in front of a Community Services cluster is an **optional** configuration that increases the Community Services load-handling capabilities.

Each Sametime server contains a Community Services multiplexer (or MUX) component that maintains connections from Sametime clients to the Community Services on the Sametime server.

During a normal Sametime server installation, the Community Services multiplexer is installed with all other Sametime components on the Sametime server computer. The Sametime server CD provides an option to install only the Community Services multiplexer component. This option enables the administrator to install the Community Services multiplexer on a different machine than the Sametime server.

When the Sametime Community Services multiplexer is installed on a different computer than the Sametime server:

- The Sametime Connect clients connect to the Community Services multiplexer computer, not the Sametime server. This configuration frees the Sametime server from the burden of managing the live client connections; the multiplexer machine is dedicated to this task.

- The Community Services multiplexer maintains a single IP connection to each Sametime server in the cluster. The data for all Community Services clients is transmitted over this single IP connection to the Community Services on the Sametime server.
Installing a Community Services multiplexer on a separate computer to remove the connection-handling load from the Sametime server computer enables the Sametime server to handle a larger number of users and improves the stability of the Sametime server.

For more information about deploying separate Community Services multiplexers, see:

- Deploying separate multiplexers in front of Sametime servers in a Community Services cluster
- Installing and configuring a Community Services multiplexer

If you do not want to deploy separate Community Services multiplexers, continue to the procedure Set up the load balancing mechanism (rotating DNS or Network Dispatcher).

Deploying separate multiplexers in front of a Community Services cluster

The illustration below shows separate Community Services multiplexers deployed in front of clustered Sametime servers to reduce the client connection load on the clustered servers.

In the illustration, note the following:

- The Community Services multiplexers are installed on separate computers and handle the connections from the Community Services clients.

Note: In a subsequent step, you can set up a rotating DNS mechanism or WebSphere Edge Server (Network Dispatcher) to distribute the client connections to the Community Services multiplexer machines.

- Each Community Services multiplexer maintains a single IP connection to Sametime server 1, and a single IP connection to Sametime server 2. The Community Services data is passed from the multiplexer computers to the Sametime servers over these IP connections. Each Sametime server maintains only two IP connections to handle all Community Services data.
- The scenario shown above can significantly increase the Community Services load-handling capabilities of the Sametime servers. The table below illustrates the advantages of deploying separate multiplexers.
<table>
<thead>
<tr>
<th>Multiplexer deployment</th>
<th>Number of Community Services connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Sametime servers with the multiplexer installed on the same machines as the servers</td>
<td>Each Sametime server can handle approximately 10,000 Community Services connections, for a total of 20,000 connections.</td>
</tr>
</tbody>
</table>
| Two Sametime servers with the multiplexers installed on different machines (as seen in the illustration above) | • Each Sametime server can service approximately 100,000 active Community Services connections.  
  **Note:** This estimate of 100,000 connections assumes that the Meeting Services and Broadcast Services are not in use. When the Sametime server is simultaneously supporting interactive and broadcast meetings, it will support fewer Community Services users.  
  • Each Community Services multiplexer machine can handle as many as 20,000 to 30,000 live IP port connections, for a possible total of 60,000 connections.  
  • The machines in the illustration above might be able to handle 160,000 active connections. You can increase the load handling capability further by adding additional Community Services multiplexers in front of the two Sametime servers. For example, adding two more Community Services multiplexers to the cluster shown above might accommodate as many as 120,000 active connections (4 x 30,000 connections per Community Services multiplexer). |

**Note:** The server capacity numbers used above are approximations meant to provide a rough estimate of the possible load-handling improvement if you deploy Community Services multiplexers on separate machines. The actual server capacity is affected by variables such as:

- The average number of users in the contact lists of all Sametime clients
- The number of HTTP-tunneled connections
- The number of instant messages that users send

**Installing and configuring a Community Services multiplexer**

Use the instructions below to install and configure a Community Services multiplexer on a separate machine.

**Preinstallation considerations:** Consider the following before installing a Community Services multiplexer on a separate machine:

- The minimum system requirements for the Community Services multiplexer machine are the same as the system requirements for the core Sametime server. For more information, see the *Lotus Sametime Installation Guide* (stinstall.nsf or stinstall.pdf).

A machine that meets the minimum system requirements should be able to handle approximately 20,000 simultaneous client connections.
Testing indicates that machines with dual 1133 MHz CPUs and 2 GB of RAM can handle approximately 30,000 simultaneous client connections.

- TCP/IP connectivity must be available between the Community Services multiplexer machine and the Sametime servers in the cluster. Port 1516 is the default port for the connection from the Community Services multiplexer machine to the Sametime servers.

**Installing the Community Services multiplexer:** To install the Community Services multiplexer:

1. Insert the Sametime CD into the Community Services multiplexer computer and choose the option to install the Community Services multiplexer (or MUX).
2. Follow the instructions on the installation screens. Ensure that you enter the DNS name or IP address of one of the Sametime servers in the Community Services cluster. The DNS name or IP address of the Sametime server is the only significant parameter you must enter during the Community Services multiplexer installation.
3. Configure the settings in the Configuration database (stconfig.nsf) on the Sametime server machine and the Sametime.ini file on the Community Services multiplexer machine as described below.

**Configuring security settings in the Configuration database (stconfig.nsf) on the Sametime server:** After you have installed the Community Services multiplexers on separate machines, you must configure the Sametime servers in the Community Services cluster to accept connections from the Community Services multiplexers.

A Sametime server only accepts connections from Community Services multiplexers that are listed in the stconfig.nsf database on the Sametime server. Specifically, the Community Services multiplexer machines must be listed in the "CommunityTrustedIps" field of a "CommunityConnectivity" document in the stconfig.nsf database. This security setting prevents Community Services multiplexers on unauthorized machines from connecting to the Sametime server.

To enable the Sametime servers in the Community Services cluster to accept connections from the Community Services multiplexers:

1. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on one Sametime server in the server cluster.
2. Open the CommunityConnectivity document in the stconfig.nsf database by double-clicking on the date associated with the document. If the CommunityConnectivity document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnectivity document, choose Create-CommunityConnectivity from the menu bar in the stconfig.nsf database.
3. In the "CommunityTrustedIps" field, enter the IP addresses of the Community Services multiplexer machines. **Note** The IP addresses of SIP Connector machines associated with a Sametime community are also entered in this field.
4. Save and close the CommunityConnectivity document.
5. Repeat this procedure on the other Sametime server in the Community Services server cluster. All servers in the Community Services cluster must contain the IP addresses of the Community Services multiplexer machines in a CommunityConnectivity document. This CommunityConnectivity document must be available in each Configuration database on each Sametime server in the cluster.
Note: You can either create the CommunityConnectivity document manually as described above or copy the CommunityConnectivity document from the Configuration database on one Sametime server and paste it into the Configuration database on the other Sametime server. Do not replicate the Configuration database between the Sametime servers in the Community Services cluster.

Configuration settings available in the Sametime.ini file on the multiplexer machine: The Sametime.ini file on the Community Services multiplexer machine contains all configuration parameters for the Community Services multiplexer, including:

- The host name of the Sametime server to which the Community Services multiplexer connects (specified during the Community Services multiplexer installation and in the stconfig.nsf database as discussed above).
- The port the Community Services multiplexer uses to establish the connection with the Sametime server (default port 1516).
- The maximum number of simultaneous connections allowed for the multiplexer. To specify a maximum number of simultaneous connections, use the VPMX_CAPACITY= parameter of the Sametime.ini file. The default value is 20,000 connections (for example, VPMX_CAPACITY=20000).

Note: Multiplexer machines that meet the minimum system requirements can successfully handle 20,000 connections. This value may vary depending on the processing capabilities of the multiplexer machine. Machines with dual 1133 MHz CPUs and 2GB of RAM can successfully handle as many as 30000 connections.

If it is necessary to modify the settings above, open the Sametime.ini file on the Community Services multiplexer machine with a text editor, alter the setting, and save the Sametime.ini file.

Next step: Set up the load balancing mechanism (rotating DNS or Network Dispatcher)

Set up the load-balancing mechanism (rotating DNS or Network Dispatcher)

Setting up the load-balancing mechanism is the seventh of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services.

The way in which you set up the load-balancing mechanism varies slightly depending on whether you have deployed Community Services multiplexers on separate machines.

Without separate Community Services multiplexers

If you have not deployed Community Services multiplexers on separate machines, do one of the following to set up the load balancing mechanism:

- Set up a rotating DNS system to accomplish load balancing. Use rotating DNS to associate the IP addresses of the Sametime server machines to a single DNS name.

  For example, associate the IP address of Sametime server 1 (11.22.33.66) and Sametime server 2 (11.22.33.77) to the DNS name cscluster.sametime.com.

- Set up an IBM WebSphere Edge Server (Network Dispatcher) in front of the Sametime servers that you intend to cluster. Use the WebSphere Edge Server
Network Dispatcher to distribute connections to the Sametime server machines. See the WebSphere Edge Server documentation for more information. This documentation is available at the Web site www.redbooks.ibm.com and also provided with the WebSphere Edge Server.

The diagram below shows the Sametime servers with the rotating DNS system in place. Note that the WebSphere Edge Server can be used in place of the rotating DNS system.

### With separate Community Services multiplexers

If you have deployed Community Services multiplexers on separate machines, do one of the following to set up the load balancing mechanism:

- Set up a rotating DNS system to accomplish load balancing. Use rotating DNS to associate the IP addresses of the Community Services multiplexer machines to a single DNS name.

  For example, associate the IP address of Community Services multiplexer machine 1 (11.22.33.44) and Community Services multiplexer machine 2 (11.22.33.55) to the DNS name cscluster.sametime.com.

- Set up a WebSphere Edge Server (Network Dispatcher) in front of the Sametime servers that you intend to cluster. Use the WebSphere Edge Server Network Dispatcher to distribute connections to the Community Services multiplexer machines. See the WebSphere Edge Server documentation for more information. Documentation for the WebSphere Edge Server is available at the Web site www.redbooks.ibm.com.

  The diagram below shows the Community Services multiplexers with the rotating DNS system in place. Note that the WebSphere Edge Server can be used in place of the rotating DNS system.
Next step:
Next, create a cluster document in the Configuration database (stconfig.nsf) to define the Community Services cluster.

Creating a cluster document in the Configuration database (stconfig.nsf)

Creating a cluster document in the Sametime Configuration database (stconfig.nsf) is the eighth of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services.

The Sametime administrator must manually create a cluster document in the Sametime Configuration database (stconfig.nsf) on a Sametime server in the Community Services cluster. The cluster document defines the Community Services cluster.

The cluster document stores the following information:
- The Community Services cluster name.
- The DNS name assigned to the rotating DNS system or IBM WebSphere Edge Server that performs the load-balancing operations.
- A list of all servers in the Community Services cluster.

To create the cluster document in the Sametime Configuration database:
1. Using a Notes client, open the Sametime Configuration database (stconfig.nsf) that replicates between the Sametime servers in the cluster.
2. Choose Create-Cluster Information.
3. In the Cluster Name field, enter the cluster name.
   The cluster name is at your discretion. You can name the cluster after one of the servers in the cluster, but it is not mandatory. If you name the cluster after one of the servers in the cluster:
• You might save time when you add the cluster name to the "Sametime server" field of each user’s Person document to configure client connectivity; some users will already have that server name listed in their Person documents (or LDAP directory person entries).

• Use the full canonical name of the server when entering the name in the Cluster Name field (for example, cn=servername/ou=organizational unit/o=organization).

4. In the "DNS Name" field, enter the fully-qualified DNS name for the cluster. This name must be the DNS name of the rotating DNS system or the WebSphere Edge Server Network Dispatcher that performs the load balancing operations for the clustered Community Services.

5. In the "List of Servers in Cluster" field, enter the names of all the servers that are part of the cluster. The names must be entered in the Domino full canonical name format. Do not use the fully-qualified DNS names in the "List of Servers in Cluster" field. You must separate the server names with a semicolon and a space as shown in the example below.

   Example: cn=sametimeserver1/ou=west/o=acme;
   cn=sametimeserver2/ou=west/o=acme

6. Save and close the cluster document.

   Leave the Configuration database open. In the next procedure, you must copy the Cluster Information document you just created to all other Sametime servers in the Sametime community.

   **Next step:**

   Next, create a cluster document on all other Sametime servers in the community.

**Creating a cluster document on other Sametime servers in the community**

Creating a cluster document on other Sametime servers in the community is the ninth of ten tasks associated with clustering the Meeting Services.

You must copy the Cluster Information document to all Sametime servers that are part of the community; this includes all Sametime servers that are part of the Community Services cluster and all Sametime servers that are part of the community, but not part of the Community Services cluster.

**Note:** Every server in the Sametime Community must contain the Cluster Information document in its Configuration database. This document enables the servers in the cluster to operate as part of the cluster and enables servers outside of the cluster to interoperate with the cluster. This procedure enables users who have a home Sametime server that is not part of the Community Services cluster to share presence and instant messaging capabilities with users who are assigned to the Community Services cluster (have the cluster name listed as the home cluster in the user’s Domino or LDAP directory entry). Do not replicate the Configuration database. The Configuration database contains some fields that cannot be replicated to all Sametime servers in a community.

To copy the Cluster Information document to all other Sametime servers in the community:

1. If necessary, open the Sametime Configuration database (stconfig.nsf) in which you created the Cluster Information document that defines the cluster. (The
database should still be open if you created the Cluster Information document in the as discussed in the previous topic.)

2. Copy the Cluster Information document. To copy this document:
   a. Locate Cluster Information in the Form Name column of the Configuration database.
   b. In the Cluster Information - Last Modified Date column, right-click on the date that represents the Cluster Information document.
   c. Select Copy.
   d. From the menu bar, select File-Close to close the Configuration database.

3. Paste the Cluster Information document into the Configuration database on each Sametime server in the community. To paste this document in the Configuration databases on other Sametime servers:
   a. From the Lotus Notes client, choose File-Database-Open.
   b. In the Server field, enter the name of another Sametime server in the community.
   c. Click Open.
   d. In the Database list, select the Configuration database (stconfig.nsf).
   e. Click Open.
   f. Select the Edit-Paste menu option to paste the Cluster Information document into the Configuration database on this Sametime server. The document name and date will appear in the Form Name - Last Modified Date column of the Configuration database.
   g. Save and close the Configuration database.
   h. Repeat step 3 for every Sametime server in the Sametime community. Perform this procedure on both the clustered Sametime servers and the non-clustered Sametime servers.

Next step:
Next, ensure that clients can access the Community Services cluster by Configuring client connectivity for the Community Services cluster.

Configuring client connectivity for the Community Services cluster

Configuring client connectivity for the Community Services cluster is the last of ten tasks associated with setting up a Community Services cluster without clustering the Meeting Services.

After you have created and named the cluster, you must make the configuration changes required to ensure that the Community Services clients can connect to the Community Services cluster. The configuration fields that affect client connectivity are:

- The "Sametime server" field of the user’s Person document in the Domino Directory, or a Sametime cluster field you have added to an LDAP directory.

Note: Sametime uses this field to ensure that a user connects to one of the Sametime servers in the Community Services cluster. This field serves the same purpose as the "home Sametime server" field in the single-server approach to Community Services deployment that was used in previous Sametime releases. For more information, see Community Services connectivity and the home Sametime server and Differences between the clustering and single server approaches.
• The "Host" field in the Sametime Connect client.

**Adding the cluster name to a field in each user's Person entry in the LDAP directory**

When the Sametime servers are configured to connect to an LDAP directory on an LDAP server (as in this example), the administrator can do one of the following:

• Manually add a field to the LDAP directory to contain the name of the Community Services cluster. The added field must exist in the Person record of every Sametime user in the LDAP directory. For more information, see Setting the Home Sametime Server setting for LDAP.

• Use an existing field in the LDAP directory to hold the name of the Community Services cluster. This field must exist in the Person record of every Sametime user in the LDAP directory. In this case, you must specify the cluster name in this field in the LDAP directory.

**Note:** This example uses the "Sametime server" field of each user's Person document in the Domino Directory as the field that holds the Sametime cluster name. The field you select to hold the name of the Community Services cluster must be specified in the LDAP Directory-Authentication-Name of the Home Server attribute setting in the Sametime Administration Tool. In this example, the "Sametime server" field was specified when you configured the connection to the LDAP server when installing the Sametime servers.

To complete the example, you can enter the cluster name in the "Sametime server" field of each user's Person document in the Domino Directory on the Domino LDAP server. Note that you defined the cluster name when creating a cluster document in the Configuration database.

If you used a server name as the cluster name, you can enter the server name in the Domino hierarchical name format (sametimeserver1/west/acme) when entering the name in the Sametime server field of the Person document.

**Configuring the "Host" field for Sametime Connect clients**

The Sametime Connect client attempts to connect to the network address specified in the Options-PREFERENCES-Sametime Connectivity-Host field of the Sametime Connect client. The users in the Sametime community must enter the DNS name or IP address of the load-balancing mechanism for the Community Services cluster in the "Host" field of their Sametime Connect clients:

• If you have set up a rotating DNS system for load balancing, users must specify the DNS name (for example, sametime.cscluster.com) of the rotating DNS system in this field.

• If you have set up a WebSphere Edge Server to perform load balancing, users must enter the IP address or DNS name of the WebSphere Edge Server machine in this field.

**Running the client packager application**

You can run the Sametime client packager application on a Sametime server to ensure that each Sametime Connect client downloaded from a Sametime server is pre-configured with the appropriate connectivity settings for your environment, including the Host name setting required to connect to the rotating DNS system or WebSphere Edge Server. For more information, see the Lotus Sametime Installation Guide (stinstall.nsf or stinstall.pdf).

**Connectivity issues associated with a rotating DNS setup**

If DNS resolve requests are cached, users might experience some problems when reconnecting following a server failure. For more information on connectivity
issues associated with using a rotating DNS setup to accomplish load balancing, see: Rotating DNS Limitations with cached DNS resolve requests

Next step:
At this point, your Community Services cluster is complete.

Adding another server to the Community Services cluster

Once you have created a Community Services cluster, you can easily add another Sametime server to a Community Services cluster that is not controlled by the EMS.

To add a Sametime server to an existing Community Services cluster:
1. Add the Sametime server to the Domino server cluster following the guidelines described in Creating a Domino server cluster
2. Replicate the Sametime databases to the newly-added Sametime server following the guidelines described in Setting up replication of Sametime databases
3. Update the Cluster Information document and copy the updated document to all Sametime servers in the community. To update and copy the Cluster Information document:
   a. Add the name of the new Sametime server to the "List of Servers in Cluster" field in the Cluster Information document in the Configuration database (stconfig.nsf) on one Sametime server.
      Enter the server name in the Domino full canonical name format (for example, cn=servername/ou=organizational unit/o=organization). Do not use the fully-qualified DNS names in this field. Separate the server names with a semicolon and a space as shown in the example below:
      cn=Sametimeserver1/ou=West/o=acme;
      cn=Sametimeserver2/ou=West/o=acme
      After adding the new Sametime server name to the "List of Servers in Cluster" field of the Cluster Information document, the "List of Servers in the Cluster" field should contain the names of every Sametime server in the Community Services cluster.
   b. Copy the updated Cluster Information document and paste it into the Configuration databases on all Sametime servers in the community. Make sure you add the Cluster Information document to the Configuration databases on both clustered and non-clustered Sametime servers.
      Note: After pasting the new Cluster Information document in the Configuration database, you can delete the previous version of the Cluster Information document.
4. (Optional) You can deploy an additional Community Services multiplexer as described in Deploying separate Community Services multiplexers to ensure the connection load for your Community Services cluster is handled efficiently. However, if you do not deploy another Community Services multiplexer, the existing Community Services multiplexers can still make connections to the newly-added Sametime server.
   If you deploy an additional Community Services multiplexer, make sure to update the CommunityConnectivity configuration document on each Sametime server in the cluster to include the IP address of the new Community Services multiplexer.
Creating multiple Community Services clusters in a single Sametime community

If you have a large Sametime community consisting of many Sametime servers, it is possible to create multiple Community Services clusters within this single Sametime community.

You might want to create multiple Community Services clusters if you have users who are in the same community, but work in remote locations. For example, you might want to create a Community Services cluster for workers in your Dublin office and a separate Community Services cluster for workers in your Paris office. Creating two separate clusters enables the clusters to function more efficiently. If the servers in Dublin and the servers in Paris were part of the same Community Services cluster, it would be necessary to replicate databases in real-time across a WAN connection, which might result in inefficient performance.

Creating multiple Community Services clusters
To create multiple Community Services clusters in a single community:
1. Create each Community Services cluster using the procedures described earlier in this chapter.
2. Copy the Cluster Information documents to all servers in the Sametime community.

Each of these steps is described in more detail below.

Create the Community Services clusters
When creating multiple Community Services clusters in the same Sametime community, you can create each cluster using the procedures described in Setting up a Community Services cluster without clustering the Meeting Services.

Copy the Cluster Information documents to all servers in the community
When you create a Community Services cluster, you create a Cluster Information document in the Configuration database (stconfig.nsf) on one Sametime server in the cluster and copy this Cluster Information document to the Configuration databases of every Sametime server in the community.

When you create multiple Sametime server clusters in a single community, the Configuration database of every Sametime server in the community must include a Cluster Information document for every cluster in the Sametime community. In such an environment, the Configuration database on each Sametime server in the community will contain multiple Cluster Information documents.

For example, if you have three Community Services clusters in your community (Cluster 1, Cluster 2, and Cluster 3), the configuration database of every Sametime server in the community must include three cluster documents (one for each cluster).

Note that the rule above applies to all servers in the community, even if the servers do not operate as a member of a cluster. For example, each server in the three clusters must have three cluster documents in the Configuration database. A server that is in the community but not a member of any cluster must also have the three Cluster Information documents in its Configuration database.
Rotating DNS Limitations with cached DNS resolve requests

This section describes some of the limitations related to setting up a rotating DNS system to load balance connections to the Community Services cluster.

Ideally, as users connect to the rotating DNS system, consecutive attempts to resolve a cluster name will result in an even distribution of connections to the servers in the cluster. In practice, the DNS caching mechanism can cause Sametime Connect to repeatedly attempt connections to the same server in the cluster. If a server fails, and the DNS resolve requests are cached, Sametime Connect might attempt to reconnect to the server that is down instead of failing over to a different server.

The Sametime Connect client Sametime Connectivity settings control whether the client attempts to connect to the Sametime server through a proxy server or attempts a direct connection to the Sametime server. These connectivity settings affect the failover behavior when DNS resolve requests are cached. This behavior varies for the "Sametime Connect for the desktop" client and the "Sametime Connect for browsers" client.

The failover behavior of the Sametime Connect clients when DNS resolve requests are cached is discussed below.

Sametime Connect for the desktop

When the DNS resolve requests are cached and a server fails, "Sametime Connect for the desktop" automatically attempts reconnection to another server in the cluster. When any of the following settings are selected on the Sametime Connectivity tab, successful reconnection to the cluster depends on the client machine and its settings:

- Direct connection using standard Sametime protocol
- Use SOCKS4 proxy with "Resolve server name locally" checked
- Use SOCKS5 proxy with "Resolve server name locally" checked
- Direct connection using HTTP protocol

If Sametime Connect cannot reconnect to the cluster when these settings are selected, the user can try any of the following options:

- On Windows NT and Windows 98 machines, restart the Sametime Connect client or restart the Web browser.
- On Windows 2000 machines, change the registry key that controls the cache time for DNS requests so the DNS requests are cached for only one second:
  1. Start the registry editor and open
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
  2. Change the value of the registry key "MaxCacheEntryTtlLimit" to "1"
- In the Sametime Connect client Sametime Connectivity settings, change the name in the Host setting from the cluster name to a specific server in the cluster.

When any of the following settings are selected in the Sametime Connectivity tab, a proxy server resolves the cluster name. Resolving the cluster name depends on
the settings of the proxy server. The proxy server might return a valid server name in the cluster, or it might return the address of the server that is already down.

- Use HTTP proxy
- Use HTTPS proxy
- Use SOCKS4 proxy with "Resolve server name locally" unchecked
- Use SOCKS5 proxy with "Resolve server name locally" unchecked

If Sametime Connect cannot reconnect to the cluster when these settings are selected, check the settings on the proxy server to verify the proxy is attempting to connect to the servers in the cluster in rotating order.

When the "Use my Microsoft Internet Explorer browser settings" option is selected in the Sametime Connectivity tab, the behavior of the client depends on the proxy connectivity settings of the Internet Explorer Web browser.

- If the browser settings do not specify a proxy server, the client attempts a "Direct connection using HTTP protocol." If the client is unable to reconnect following a server failure, the user can try any of the options listed for "Direct connection using HTTP protocol" above.
- If the browser settings specify an HTTP proxy server, the HTTP proxy server resolves the cluster name. If the client cannot reconnect, check the settings on the proxy server to verify the proxy is attempting to connect to the servers in the cluster.

**Sametime Connect for browsers**

With "Sametime Connect for browsers," the client resolves the cluster name when any of the following options are selected:

- Direct connection using standard Sametime protocol
- Direct connection using HTTP protocol
- Use SOCKS4 proxy with "Resolve server name locally" checked
- Use SOCKS5 proxy with "Resolve server name locally" checked

If Sametime Connect for browsers cannot reconnect to the cluster when these settings are selected, the user should:

- On Windows NT and Windows 98 machines, restart the Sametime Connect client or restart the Web browser.
- On Windows 2000 machines, change the registry key that controls the cache time for DNS requests so the DNS requests are cached for only one second:
  1. Start the registry editor and open
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
  2. Change the value of the registry key "MaxCacheEntryTtlLimit " to "1"
- In the Sametime Connect client Sametime Connectivity settings, change the name in the Host field from the cluster name to a specific server in the cluster.

When any of the following settings are selected in the "Sametime Connect for browsers" Sametime Connectivity tab, a proxy server resolves the cluster name. Resolving the cluster name depends on the settings of the proxy server. The proxy server might return a valid server name in the cluster, or it might return the address of the server that is already down.

- Use SOCKS4 proxy with "Resolve server name locally" unchecked
- Use SOCKS5 proxy with "Resolve server name locally" unchecked
- Use HTTP proxy
• Use HTTPS proxy

If Sametime Connect cannot reconnect to the cluster when these settings are selected, check the proxy settings to verify the proxy is attempting to connect to the servers in the cluster in rotating order.

When the "Use my browser settings" option is selected in the Sametime Connectivity tab, the behavior of the client depends on the proxy connectivity settings of the Web browser.

• If the browser settings do not specify a proxy server, the client attempts a "Direct connection using standard Sametime protocol" or a "Direct connection using HTTP protocol." If the client is unable to reconnect following a server failure, the user can try any of the options listed for "Direct connection using standard Sametime protocol" and "Direct connection using HTTP protocol" above.

• If the browser settings specify a SOCKS proxy server, and the client is unable to reconnect following a server failure, the user can try any of the options listed for the Use SOCKS4 and Use SOCKS5 proxy settings above.

• If the browser settings specify an HTTP or HTTPS proxy server, the proxy server resolves the cluster name. If the client cannot reconnect, check the settings on the proxy server to verify the proxy is attempting to connect to the servers in the cluster.
Chapter 17. Setting Up the Enterprise Meeting Server and a Meeting Services Cluster

This chapter explains how to deploy the IBM Lotus Enterprise Meeting Server (EMS) and set up a Meeting Services cluster in a test environment. A Meeting Services cluster consists of the EMS working with a group of IBM Lotus Sametime servers to provide failover and load balancing functionality for online meetings.

Note: The Lotus Enterprise Meeting Server (EMS) is a separate product from the Lotus Sametime server. The EMS does not ship with the Sametime server and must be purchased separately.

You must deploy the EMS before you can create a Meeting Services cluster. The EMS controls the servers in the Meeting Services cluster and supports the failover and load balancing functionality of a Meeting Services cluster.

This chapter includes a step-by-step example for the EMS deployment and creating a Meeting Services cluster. You can use the instructions in this chapter to cluster the Meeting Services of Sametime servers without clustering the Community Services of those Sametime servers.

If you also want to cluster the Community Services of Sametime servers that operate as part of a Meeting Services cluster, you must perform the clustering procedures in the following order:

1. Deploy an LDAP directory (mandatory).
2. Install the Sametime 7.0 servers. To create server clusters with the EMS 7.0, all Sametime servers must be Sametime 7.0 servers. You cannot use earlier versions of the Sametime server with the EMS 7.0.
3. Deploy the EMS.
4. Create the Meeting Services cluster.
5. Create the Community Services cluster.

Note: In this scenario, you must create the Community Services cluster after you create the Meeting Services cluster, and you must use the procedures described in Chapter 20 "Creating a Community Services cluster with the Enterprise Meeting Server" to create the Community Services cluster.

To begin the EMS deployment and Meeting Services cluster set up procedures, see "EMS deployment and Meeting Services cluster setup procedures" later in this chapter.

You can find additional information about the EMS and Sametime server clusters in the following chapters:

- Chapter 15 - Introduction to Sametime Server clusters and the Enterprise Meeting Server
- Chapter 16 - Setting up a Community Services cluster without clustering the Meeting Services
- Chapter 18 - Creating a Community Services cluster with the Enterprise Meeting Server
- Chapter 19 - Setting up security for the Enterprise Meeting Server
EMS deployment and Meeting Services cluster setup procedures

Meeting Services clusters are controlled by the EMS. The EMS installs and runs on an IBM WebSphere V5.1.2 Application Server in a Java 2 Platform Enterprise Edition (J2EE) environment. Installing this J2EE environment is one of several procedures associated with deploying the EMS and setting up a Meeting Services cluster.

When clustering the Meeting Services of your Sametime servers, use the procedures in this chapter in conjunction with existing knowledge of your Sametime and IBM WebSphere environments. Your unique environment might require some variation from these procedures.

Deploying the EMS and creating a Meeting Services cluster involves the five tasks listed below. Each of the five tasks includes several sets of procedures. Detailed instructions for all of these tasks are provided in this chapter.

1. **EMS pre-deployment requirements and considerations** - The procedures associated with this task are listed below.
   a. Ensure the hardware required for a EMS deployment is available.
   b. Deploy an LDAP directory server for the Meeting Services cluster.
   c. Create or identify the required LDAP directory accounts.
   d. Install the Sametime servers.
   e. Ensure the software required for a EMS deployment is available.

2. **Install the J2EE infrastructure on the EMS computer** - The procedures associated with this task are listed below.
   a. Setting up the required Windows system administrator account.
   b. Installing the DB2 server.
   c. Installing WebSphere MQ V5.3.0.2.
   d. Installing WebSphere MQ V5.3 CSD08 (Fix Pack 8).
   e. Installing the WebSphere Application Server V5.1.
   f. Installing WebSphere Application Server V5.1 Fix Pack 1.
   g. Installing WebSphere Application Server V5.1.1 Cumulative Fix 2.
   h. Setting up the JMS system queues.
   i. Ensuring WebSphere MQ supports the Double-Byte Character Set (DBCS).

   **Note:** In the EMS deployment example described in this section, DB2, WebSphere MQ, the WebSphere server, and the EMS are installed on a single Windows server. You can install these components on a single server for testing purposes. In a production environment, it is mandatory to install these components on separate computers.

3. **Configuring WebSphere server security and LDAP directory access** - This task includes the procedures required to secure access to the WebSphere Administrative Console, set up basic WebSphere security, and enable the WebSphere server to access the LDAP directory.

4. **Deploying the Enterprise Meeting Server** - This task involves all procedures required to deploy the EMS on a WebSphere server. The procedures associated with this task are listed below.
   a. Creating three additional WebSphere Application Servers.
   b. Installing the Enterprise Meeting Server files.

---

528  Sametime Administrator’s Guide
c. Creating the DB2 database

d. Creating the WebSphere MQ queues

e. Defining the WebSphere Variables

f. Defining the JAAS Alias

g. Setting up the JDBC Provider Resource and creating the Data Source

h. Creating the JMS Connection Factory

i. Creating the JMS Destinations

j. Ensuring UTF-8 Unicode character support for the EMS

k. Deploying the STAdmin, STCenter, and STServer Enterprise Archive (EAR) files

l. Regenerating the WebServer plugin and starting the Enterprise Meeting Server Enterprise Applications

5. **Adding Sametime servers to the EMS** - This task involves all procedures required to add a Sametime server to the EMS. The procedures associated with this task are listed below:

a. **Synchronize Single Sign-On (SSO) support for the EMS and Sametime servers**

b. **Edit the Sametime.ini file on the Sametime servers**

c. **Edit the MeetingServices document in the Configuration database on the Sametime server**

d. **Provide the WebSphere and EMS administrator account with Manager access to the stconfig.nsf database**

e. **Enable the Sametime servers to store recorded meeting files on a remote computer**

f. **Start the EMS Administration Tool for the first time**

g. **Add the Sametime server using the EMS Administration Tool**

h. **Specifying Usage Limits and Denied Entry settings for the Sametime server**

---

**EMS pre-deployment requirements and considerations**

Ensuring that you have met the EMS pre-deployment requirements and considerations is the first of five tasks associated with setting up the EMS and a Meeting Services cluster.

Use the requirements and procedures discussed in this section as a check list to ensure that you have created an environment into which you can deploy the EMS. The EMS pre-deployment requirements and considerations include:

1. **Ensuring the hardware required for an EMS deployment is available** - You must ensure that you have the minimum number of computers available for the EMS deployment.

2. **Deploy an LDAP directory server for the Meeting Services cluster** - This task ensures that you have an LDAP directory available for the Meeting Services cluster. The EMS and Meeting Services cluster deployment requires a single LDAP directory.

3. **Create or identify the required LDAP directory accounts** - This task ensures that your LDAP directory contains the user accounts required by the EMS deployment procedures.

4. **Install the Sametime servers** - This task involves installing the Sametime servers that will form the Meeting Services cluster. You must configure these servers to connect to your LDAP directory.
5. **Ensuring the software required for EMS deployment is available**

You must have the IBM DB2, WebSphere MQ, and WebSphere V5.1 Application Server software required by the EMS available before you can deploy the EMS.

### Ensuring the hardware required for an EMS deployment is available

Ensuring that the hardware required for an EMS deployment is available is the first of five [EMS pre-deployment requirements and considerations](#).

The number of computers required by an EMS environment varies depending on the size of the Sametime server cluster that you want to create. This documentation describes an EMS test deployment that includes a Meeting Services cluster consisting of two Sametime servers and a Community Services cluster consisting of two Sametime servers. To deploy the EMS and support clusters of this size in a test environment, six computers are required as noted below.

**Note:** Creating a Community Services cluster is optional. If you want to create an EMS environment consisting of only a Meeting Services cluster, you can set up an EMS test deployment with as few as four computers.

### Computers required to complete the test EMS deployment

The computers required to complete the test EMS deployment described in this documentation are listed below:

- One computer is required to host an LDAP directory. An EMS deployment requires a single LDAP directory to be installed on a dedicated directory server. For information on the system requirements of the LDAP directory server, refer to the documentation that came with the LDAP directory.

- The example provided in this documentation uses four computers for Sametime server installations. Two computers will be used to create the Meeting Services cluster and two computers will be used to create a Community Services cluster. If you do not want to create a Community Services cluster that is controlled by the EMS, only two Sametime servers are needed to create the smallest possible Meeting Services cluster. (You can create a larger Meeting Services cluster if you want. The number of Sametime servers you want to include in your Meeting Services cluster is at your discretion.)

  For more information on the system requirements of the Sametime servers, see [Sametime server system requirements](#) below.

- One computer is required to host the EMS application and the J2EE infrastructure required by the EMS. For information on the system requirements of this computer, see [Enterprise Meeting Server and J2EE computer requirements](#) below.

**Note:** In a test environment, the J2EE infrastructure and EMS application can reside on a single computer. In a production environment, it is recommended that three computers be used to host the EMS and its J2EE environment. One computer hosts the IBM DB2 software, a second computer hosts the WebSphere MQ server, and a third computer hosts the WebSphere 5.1.2 Application Server and the EMS.

Note also that in a production environment, you should designate an additional system as a storage system for recorded meeting files. Later in this procedure, you can use Windows Explorer to map to the network drive of this remote system for the purpose of storing recorded meeting files on it. Recorded meeting files can be very large and may affect the performance of the EMS if they are stored on the same computer as the EMS.
Enterprise Meeting Server and J2EE computer requirements
The system requirements of the EMS computer and its J2EE infrastructure are shown below. This system should be dedicated to running only the EMS and J2EE components. Do not install a Sametime server or any other Sametime components on this computer.

- **CPU** - Pentium® 4 1.8GHz or higher recommended
- **Operating system** - Windows 2000 Server or Advanced Server with Service Pack 4; Windows 2003
- **Memory:**
  - Windows 2000 - 1GB RAM recommended; 512MB minimum
  - Windows 2003 - 1GB RAM recommended, 512MB minimum
- **Disk space** - 500MB of free disk space. 1GB + is recommended
- **Communication Adapter Support**

The EMS computer should also:
- Be registered in the same DNS domain as the Sametime servers.
- Have TCP/IP connectivity with the Sametime server computers on port 80 for HTTP connections.

**Note:** HTTP connections between the EMS and Sametime servers can be encrypted with SSL. For more information, see Encrypting HTTP traffic between the EMS and Sametime servers with SSL.

Before you can deploy the EMS on this computer, you must install the J2EE infrastructure required by the EMS. These procedures are described in Installing the J2EE infrastructure on the EMS machine.

Sametime server system requirements
Your server cluster must consist of all Sametime 7.0 servers. Only Sametime servers that operate on the Windows platform can be attached to the EMS. For Sametime server system requirements, see the Lotus Sametime 7.0 Release Notes.

The Sametime server computers should also:
- Be registered in the same DNS domain as the EMS/J2EE computer.
- Have TCP/IP connectivity with the EMS/J2EE computer on the following ports:
  - Port 80 for HTTP connections.
  - Port 1414 for WebSphere MQ connections

Next:
Deploying an LDAP directory

**Deploying an LDAP directory**

Deploying an LDAP directory is the second of five EMS pre-deployment requirements and considerations.

The community of users that access the EMS and the Meeting Services cluster must be defined in a single LDAP directory. Before you begin the EMS deployment and Meeting Services clustering procedures, you must either install a single LDAP directory on a separate server and populate the directory with the community of users or have access to an existing LDAP directory that is already populated.
You should be aware of the following issues pertaining to the LDAP directory. At this point it is not necessary to address these issues, but it will be necessary to address them in the course of the EMS deployment and Meeting Services clustering process.

- Only one LDAP directory can be used with a Meeting Services cluster. The Sametime servers that will be members of the Meeting Services cluster must be configured to access this single LDAP directory. Usually, a Sametime server is configured to access the LDAP directory at the time the Sametime server is installed.
- The IBM WebSphere server on which the EMS will be installed must also be configured to access this single LDAP directory. Enabling WebSphere to access the LDAP directory is one of the procedures that you must perform when setting up the EMS. This configuration is performed when you complete the procedure titled "Configuring WebSphere server security and LDAP directory access" later in this chapter.
- The EMS computer and Sametime servers must have TCP/IP connectivity with the LDAP directory server. Port 389 is the default port for this connection. If necessary, you can alter this port during the Sametime server and WebSphere LDAP configurations.
- The most common LDAP directories used with WebSphere and the EMS include: Netscape, Domino, Microsoft Active Directory, or IBM Secureway LDAP directories. Other LDAP directories may be used but these directories may require more customization of LDAP directory access settings than the directories listed above.
- You must create or identify specific accounts in your LDAP directory that will be required during the EMS deployment procedures. For more information on these accounts, see the next procedure "Create or identify the required LDAP directory accounts".

Next:
Next, create or identify the required LDAP directory accounts

Create or identify the required LDAP directory accounts

Creating or identifying the required LDAP directory accounts is the third of five EMS pre-deployment requirements and considerations.

The EMS deployment and Meeting Services cluster setup procedures require the existence of four separate LDAP directory accounts. These LDAP directory accounts include:

- An account (or person entry) for a WebSphere and EMS server administrator. A single account can be used for both administrators.
- An account for EMS access to the Sametime configuration servlets on the Sametime servers in the Meeting Services cluster.
- An account for EMS access to the Sametime Meeting Management API (MMAPI) on the Sametime servers in the Meeting Services cluster.

These required LDAP directory accounts are discussed in more detail below.

WebSphere and EMS system administration accounts

During the setup procedures, you must specify one person in the LDAP directory as the WebSphere server and EMS administrator. When the EMS setup procedures are complete, this user will have access to both the WebSphere Administrative Console used to administer the WebSphere server and the EMS Administration Tool used to administer the clustered Sametime servers.
This documentation assumes you have created the following LDAP directory person entry for this purpose:

cn=emsadmin, ou=people, o=ems

In this documentation, the password associated with this directory entry is "sametime."

**Configuration servlet access account**
The EMS on the WebSphere server contains processes that must access configuration servlets on the clustered Sametime servers. These EMS processes must authenticate when accessing the Sametime server configuration servlets.

Similarly, the clustered Sametime servers contain processes that access servlets on the EMS. These Sametime processes must also authenticate when accessing the servlet on the EMS.

You must create a directory entry in the LDAP directory that can be used to authenticate access to the configuration servlets on the EMS and Sametime servers.

IBM Lotus software recommends that you create a unique LDAP directory entry specifically for authenticating access to the configuration servlets. For example, you might create the following LDAP directory entry for this purpose:

cn=configservlet, ou=people, o=ems

You must also provide a password for this LDAP directory person entry.

You must enter this user name and password when you install the EMS files later in this process.

*Important:* Each Sametime server contains a configuration servlet that must be accessed by the EMS application. This configuration servlet is not secure following a Sametime server installation. The administrator must perform a set of procedures to ensure this configuration servlet is secure following a Sametime server installation. These procedures are performed on the Sametime server. The administrator should perform these procedures on each Sametime server that will be added to the Meeting Services cluster.

The procedures required to secure the configuration servlet on the Sametime server are described in the Sametime 7.0 Release Notes. To review these procedures, see the topic titled "Configuration servlet is not secure following installation" in the "Things You Need to Know" section of the Sametime 7.0 Release Notes.

The Sametime 7.0 Release Notes PDF file (strn70.pdf) containing the procedure for securing the configuration servlet is available from the Documentation Library at the Lotus Developer’s Domain web site (http://www.lotus.com/ldd).

**Sametime Meeting Management API (MMAPI) access account**
The EMS on the WebSphere server contains processes that must access the Meeting Management API (MMAPI) on the clustered Sametime servers. These EMS processes must authenticate when accessing the MMAPI. You must create a directory entry in the LDAP directory that the EMS processes can use to authenticate when accessing the MMAPI on the Sametime servers in the Meeting Services cluster.
IBM Lotus software recommends that you create a unique LDAP directory entry specifically for authenticating access to the MMAPI on the Sametime servers. For example, you might create the following LDAP directory person entry for this purpose:

cn=mmapi, ou=people, o=ems

You must also provide a password for this LDAP directory person entry.

You must enter this user name and password when you install the EMS files later in this process.

**Next:**
Next, *Install the Sametime servers*

### Installing the Sametime servers

Installing the Sametime servers is the fourth of five **EMS pre-deployment requirements and considerations**

Note the following concerning the installation of the Sametime servers:

- To complete the example EMS deployment described in this documentation, you must install two Domino 7.0 servers and install the Sametime 7.0 servers on top of the Domino servers, as described in the *Sametime Installation Guide* (stinstall.nsf or stinstall.pdf).

  In a production environment, the size of the Meeting Services cluster is at your discretion. You can install as many Sametime servers as needed to support the Meeting Services demands of your community.

  You can use only Sametime 7.0 servers as cluster members. You cannot use earlier versions of the Sametime servers with the EMS 7.0.

**Note:** For testing purposes, you can install a single Sametime server to operate with the EMS. If you install only one Sametime server, you cannot test the failover and load balancing capabilities of the EMS.

- The Sametime server installation provides an option to enable HTTP tunneling on port 80 for Sametime clients. Do not select this option during the Sametime server installation. A Sametime server attached to the EMS should not be configured to support HTTP tunneling on port 80.

- Optionally, you can install two additional Domino/Sametime 7.0 servers to operate as a Community Services cluster that is under the control of the EMS. As with the Meeting Services cluster, the size of the Community Services cluster is at your discretion. As many as six Sametime servers can operate as part of a Community Services cluster.

  The example provided in this documentation assumes you install four Sametime servers: two servers will form a Meeting Services cluster and two servers will form a Community Services cluster. All four servers will be controlled by the EMS.

- All Sametime servers that will be controlled by the EMS must operate as part of the same Domino domain. To be part of the same Domino domain, the Sametime servers must be registered in the same Domino Directory. The Domino Directory must replicate between the servers.

**Note:** The Domino Directory must replicate between the Sametime/Domino servers even though you are maintaining the user community in an LDAP directory on a separate server that is not part of the Community Services
cluster. Replication of the Domino Directory is required for Domino administrative purposes. The LDAP directory serves as the user repository for the members of the Sametime community; the Domino Directory is required for the proper functioning of the Domino servers on which Sametime is installed.

- Each Sametime server must be installed in the same DNS domain as the computer reserved for the EMS and J2EE installations. (This recommendation ensures that the Single Sign-On functionality works properly.)
- Each Sametime server that you install must have TCP/IP connectivity with the EMS/J2EE computer on the following ports:
  - **Port 80** - The EMS and Sametime servers communicate using HTTP on port 80 to perform meeting scheduling and materials management activity. You also have the option of encrypting the HTTP traffic between the EMS and Sametime servers with SSL. If you encrypt this traffic with SSL, port 443 is usually used for this communication. For more information, see [Encrypting HTTP traffic between the EMS and Sametime servers with SSL](#).
  - **Port 1414** - This port is used to support Java Messaging Service (JMS) communications using WebSphere MQ message queuing functionality. This communication supports the load balancing, meeting booking, and failover functionality provided by the EMS.
- Each Sametime server must be configured to access the LDAP directory. This process is summarized below.

**Note:** After you have configured the Sametime server to connect to the LDAP server, you should remove all person entries (documents) from the Domino Directory on the Sametime server. The LDAP directory serves as the user repository in an EMS environment. If a user has a person entry in both the Domino Directory of a Sametime server and the LDAP Directory accessed by the EMS and Sametime servers, that user may be unable to authenticate when accessing the EMS.

### Setting up a connection between a Sametime server and an LDAP server

In an EMS environment, the Sametime servers must be configured to connect to the LDAP directory. You configure a Sametime server to connect to an LDAP server at the time the Sametime server is installed. The procedure required to configure a Sametime server to connect to an LDAP server is summarized below. For detailed information on using LDAP directories with a Sametime server, see the chapter titled [Using LDAP with the Sametime server](#).

To configure a Sametime server to connect to an LDAP server, you must perform these basic procedures:

1. Install a Domino server and then install a Sametime 7.0 server on top of the Domino server as described in the *Sametime Installation Guide* (install.nsf or stinstall.pdf).
2. During the Sametime server installation:
   - Select “LDAP directory” when prompted for the directory type.
   - Select the check box that indicates the Sametime server will be managed by the EMS.
3. After the installation completes, use a Lotus Notes client to open the Directory Assistance database (da.nsf) on the Sametime server and alter the “Base DN for
search” setting in the da.nsf database. This setting must reflect the Base DN from which searches are conducted when searching for user and group entries in the LDAP directory.

4. Open the Sametime Administration Tool on the Sametime server. Configure the following settings using the Sametime Administration Tool on the Sametime server:

- LDAP Directory-Connectivity - For information on each of these settings, see Configuring LDAP Connectivity settings
- LDAP Directory-Basics - For information on each of these settings, see Configuring the LDAP Basics settings
- LDAP Directory-Authentication - For information on each of these settings, see Configuring LDAP Authentication settings
- LDAP Directory-Searching - For information on each of these settings, see Configuring the LDAP Searching setting
- LDAP Directory-Group Contents - For information on each of these settings, see Configuring the LDAP Group Contents setting

5. Remove any existing Person documents from the Domino Directory on the Sametime server.

Next:
Ensuring the software required for EMS deployment is available

Ensuring the software required for EMS deployment is available

Ensuring the software required for EMS deployment is available is the last of five EMS pre-deployment requirements and considerations.

Before you continue with the EMS deployment, ensure that you have all of the required software available. The list of required software is provided below:

- **IBM DB2 Universal Database V8.2 Enterprise Edition** - This software is available on CD with the IBM Lotus EMS Media Pack.
- **IBM WebSphere MQ V5.3.0.2 (formerly called MQSeries)** - This software is available on CD with the IBM Lotus EMS Media Pack. The WebSphere MQ V5.3.0.2 server is a WebSphere MQ V5.3 server that is extended to automatically include WebSphere MQ CSD01 (Fix Pack 1) as part of the installation. Optionally, you can install a WebSphere MQ 5.3 server and then manually install WebSphere MQ CSD01 (Fix Pack 1) on the WebSphere MQ 5.3 server to upgrade the service level to WebSphere MQ 5.3.0.2. This example assumes that the WebSphere MQ CSD01 is automatically installed with the WebSphere MQ 5.3 server.
- **WebSphere MQ V5.3 CSD08** (Fix Pack 8) - This fix pack includes the MA0C publish/subscribe add-on required by the EMS. You can download WebSphere MQ fix packs from this location:
  Installing this fix pack upgrades the service level to WebSphere MQ 5.3.0.8.
- **IBM WebSphere Application Server V5.1** - This software is available on CD with the IBM Lotus EMS Media Pack.
- **IBM WebSphere Application Server V5.1 Fix Pack 1** - This fix pack upgrades the WebSphere Application Server version to 5.1.1. You can download WebSphere Application Server fix packs from this location:
http://www-1.ibm.com/support/docview.wss?rs=180&tc=SSEQTP&uid=swg24007195

- **IBM WebSphere Application Server V5.1 Cumulative Fix 2** - This fix pack updates the WebSphere Application Server V5.1.1 to 5.1.1.2. You can download WebSphere Application Server V5.1 Cumulative Fix 2 from this location: http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&dc=D420&q1=5.1.1.2&uid=swg24007195

- **IBM Lotus EMS installation files** - This software is available on CD with the IBM Lotus EMS Media Pack. You deploy the EMS files on the IBM WebSphere Application Server V5.1.1.2.

**Next:**

This procedure completes the first task required to set up the EMS and a Meeting Services cluster. Next, begin the second task, *Installing the J2EE infrastructure on the EMS computer*.

### Installing the J2EE infrastructure on the EMS computer

Installing the Java 2 Platform Enterprise Edition (J2EE) infrastructure on the computer reserved for the Enterprise Meeting Server (EMS) application is the second of five tasks associated with setting up the EMS and a Meeting Services cluster.

The EMS is dependent on a J2EE infrastructure consisting of the following:

- IBM Universal Database V8.2 Enterprise Edition server
- IBM WebSphere MQ 5.3.0.8 middleware for asynchronous messaging (an IBM WebSphere MQ 5.3 server with IBM WebSphere MQ 5.3 CSD08 (Fix Pack 8) installed).
- IBM WebSphere Application Server V5.1.1.2 (an IBM WebSphere Application Server V5.1 with both the IBM WebSphere Application Server V5.1 Fix Pack 1 and the IBM WebSphere Application Server V5.1.1 Cumulative Fix 2 installed).

You must install the J2EE infrastructure on the computer reserved for the EMS deployment before you deploy the EMS. In this example, the DB2, WebSphere MQ, and WebSphere Application Server software are all installed on the same computer. In a production environment, DB2, WebSphere MQ, and the WebSphere Application Server should be installed on separate computers.

**Note:** The procedures in this section assume you do not have an existing WebSphere (J2EE) environment. If you have an existing J2EE environment, use these procedures in combination with other product installation guides and your knowledge of your WebSphere environment to determine whether your existing environment is appropriate for the EMS. Some modifications to your existing environment might be needed to support the EMS.

The task of installing the J2EE infrastructure on the EMS computer is described in nine steps. You must perform these steps in the order shown below.

1. **Setting up the required Windows system administrator account**
2. **Installing the DB2 server**
3. **Installing WebSphere MQ V5.3.0.2**
4. **Installing WebSphere MQ V5.3 CSD08 (Fix Pack 8)**
5. **Installing the WebSphere Application Server V5.1**
6. **Installing WebSphere Application Server V5.1 Fix Pack 1**
7. **Installing WebSphere Application Server V5.1.1 Cumulative Fix 2**
8. **Setting up the JMS system queues**
9. **Ensuring WebSphere MQ supports the Double-Byte Character Set (DBCS)**

**Note:** If you install DB2 successfully, but encounter a problem with the WebSphere MQ installation, it is not necessary to start over from the beginning and reinstall DB2. You can uninstall just WebSphere MQ and reinstall only the WebSphere MQ software. Similarly, if you successfully install DB2 and WebSphere MQ, but encounter a problem when installing the WebSphere 5.1 Application Server, it is only necessary to uninstall and reinstall the WebSphere 5.1 Application Server. It is not necessary to start over and reinstall the DB2 or WebSphere MQ software.

### Setting up the required Windows administrator account

Ensuring that you have the appropriate Windows administrator account is first of nine steps required to **install the J2EE infrastructure** on the computer reserved for the Enterprise Meeting Server (EMS).

Installing the J2EE infrastructure involves the installation of IBM DB2, IBM WebSphere MQ, and the IBM WebSphere Application Server software packages on the Windows server that will host the EMS.

To successfully install these software packages, you must define a Windows administrator account with specific user rights on the Windows operating system of the computer reserved for EMS deployment. You must log into the Windows operating system using this account when installing the software packages that comprise the J2EE infrastructure.

The Windows system administrator account required to install the J2EE infrastructure must meet these requirements:

- Belong to the local "Administrators" group that exists by default in the Windows operating system user groups (required by the DB2, WebSphere MQ, and WebSphere V5.1 server installations).
- Have the following advanced users rights (you can assign an individual user or a group, such as the "Administrators" group, to these rights):
  - **Create token object** (required by the DB2 installation)
  - **Increase quotas** (required by the DB2 installation)
  - **Replace a process level token** (required by the DB2 installation)
  - **Act as part of the operating system** (required by the DB2 and WebSphere installations)
  - **Log on as a service** (required by the WebSphere installation)
  - **Log on locally** (required by the WebSphere installation)
- Not exceed twelve characters. For example, you can not use "Administrator" as the name for this Windows administrator account because the name exceeds twelve characters. Some of the required software will not install under an administrator name consisting of more than twelve characters.

Procedures to provide advanced user rights on both the Windows NT and Windows 2000 operating systems are provided below. Once you have defined a Windows system user account that meets the requirements above, use this account when logging into Windows to install the IBM DB2, IBM WebSphere MQ, and IBM WebSphere Application Server software required by the EMS.
How to grant advanced user rights on Windows 2000

To grant user rights on Windows 2000:
2. In the left window pane, expand the Local Policies object.
3. In the left window pane, select User Rights Assignment.
4. In the right window pane, select the user right that you want to assign.
   (The required user rights are Create token object, Increase quotas, Replace a process level token, Act as part of the operating system, and Log on as a service.)
5. From the menu, select Action-Security.
6. Click Add, then select the appropriate user or group and click Add.
7. Click OK.

Next:

Next, installing the DB2 server

Installing the DB2 server

Installing the DB2 server is the second of nine steps required to install the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS).

This procedure describes the simplest way to install the DB2 V8.2 server to support a test deployment of the EMS. You can vary from these instructions as you deem appropriate for your environment.

To install the DB2 V8.2 Server:
1. Log in to the Windows operating system using a Windows system user ID that has the rights necessary to install the DB2 server. For more information about this user ID, see Setting up the required Windows administrator account.
2. Insert the IBM DB2 Universal Database V8.2 Enterprise Edition for Windows CD.
3. If the installation program does not start automatically, double-click Setup.exe in the root directory of the CD.
4. At the Setup window, click "Install Products."
5. At the Select the product you would like to install prompt, make sure that the "DB2 UDB Enterprise Edition" check box is selected and then click Next.
6. At the Welcome to the DB2 Setup wizard screen, click Next.
7. At the License Agreement screen, accept the terms of the License Agreement and click Next to continue.
8. At the Select the installation type window, select the Typical button and then click Next.
9. At the Select the installation action window, select the "Install DB2 Enterprise Edition on this computer" option and click Next.
10. At the Select installation folder screen, you can select the default installation directory of C:\Program Files\IBM\SQLLIB\ and click Next.
11. At the Set user information for the DB2 Administration Server window, enter the following:
   • Domain- <your Windows domain>
   • Username - db2admin
   • Password - <your password>
• **Confirm password** - <your_password>

After entering the information above, select the "Use the same values for the remaining DB2 services" check box and then click Next.

**Note** By default, the setup program creates a Windows user account using the "db2admin" user name and the password you specify. You can accept the default user account, create your own user account by modifying the default user name, or specify an existing user account. The instructions in this documentation assume that you accept the default user account of "db2admin." For more information about these accounts, refer to the DB2 Information Center installed with your DB2 software.

12. At the Setup the administration contact list window, select "Local - Create a contact list on this system" and click Next.

13. At the Warning message indicating an SMTP server has not been specified, click OK.

14. At the Configure DB2 instances window, ensure that DB2 is highlighted in the DB2 Instances area and click Next. (You do not need to alter any default settings at this window.)

15. At the Prepare the DB2 tools catalog window, select "Do not prepare the DB2 tools catalog on this computer" and click Next.

16. At the Specify a contact for health monitor notification window, either specify a new contact or defer this task until the installation is complete. Click Next.

17. When the Start copying files window appears, click Install.

18. At the DB2 Setup Wizard completed screen, click Finish.

19. A "First Steps" DB2 tutorial program starts automatically. Click Exit if you wish to review the tutorial at a later time.

20. The IBM Product Registration screen appears. Complete the product registration and click Next, or click Exit to complete the Product Registration at a later time.

**Note:** In this example, the DB2 server, WebSphere MQ server, and WebSphere Application Server all reside on a single computer. If you install the DB2 server on a separate computer from the computer that hosts the WebSphere Application Server, you must install a DB2 client on the WebSphere Application Server and use this DB2 client to catalogue and connect to DB2 databases maintained on the DB2 server. For information about installing the DB2 client, see the DB2 Information Center provided with the DB2 software.

**Next step:**

install WebSphere MQ V5.3.0.2

**Installing WebSphere MQ V5.3.0.2**

Installing WebSphere MQ V5.3.0.2 is the third of nine steps required to install the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS).

The EMS communicates with the clustered Sametime servers using the Java Messaging Services (JMS). This JMS communication is implemented using IBM WebSphere MQ for Java. The JMS messaging queues are used to transmit data required by the scheduling, load balancing, health monitoring, and failover functionality supported by the EMS. To facilitate this communication, install WebSphere MQ V5.3.0.2 on the server computer reserved for the EMS.
**Note:** The WebSphere MQ V5.3.0.2 server is a WebSphere MQ V5.3 server that has been updated to automatically include WebSphere MQ CSD01 (Fix Pack 1) as part of the installation. Optionally, you can install a WebSphere MQ 5.3 server and then manually install WebSphere MQ CSD01 (Fix Pack 1) on the WebSphere MQ 5.3 server to upgrade the server to the WebSphere MQ 5.3.0.2.

The installation procedure documented in this section is for the Windows 2000 platform. The concepts can be applied to a remote WebSphere MQ server and installations on other operating system platforms.

For more information about WebSphere MQ, see the web site: http://www.ibm.com/software/integration/wmq/

**Note:** WebSphere MQ was formerly called "MQSeries." The MQSeries name continues to appear in some files and interfaces used in the EMS setup procedures. If you see the MQSeries name in a file or interface during these procedures, note that the name is synonymous with WebSphere MQ.

**WebSphere MQ pre-installation considerations**
A local "mqm" group is created automatically on the Windows server when WebSphere MQ for Windows is installed.

WebSphere MQ for Windows works with the Security accounts database. It is important that you give the appropriate definitions in the accounts to the user IDs that are going to use WebSphere MQ for Windows.

Your user ID must belong to the local "mqm" or Windows "Administrators" group in order to administer any queue manager on the system, or to run any of the WebSphere MQ for Windows control commands.

The user ID can belong to this group either directly or indirectly (by the inclusion of global groups in the local "mqm" group).

**WebSphere MQ installation**
To install WebSphere MQ V5.3.0.2 on a Windows NT or Windows 2000 server:

1. Ensure that you are logged in to the Windows operating system using a Windows system user ID that has the rights necessary to install the WebSphere MQ server. For more information about this user ID, see Setting up the required Windows administrator account.

2. Insert the WebSphere MQ V5.3.0.2 Server CD.

3. Select the Software Prerequisites option. Verify that all prerequisite software is installed on the computer. If all required software is not installed, follow the instructions on the screen to install it.

4. Select the Network Prerequisites option.

   If both of the following conditions exist, you must set up a special account for WebSphere MQ administration:
   • Any Windows domain controller on which users are defined is running a Windows 2000 server.
   • Local user accounts are not authorized to query the group membership of the Windows 2000 domain users accounts.

   Instructions for creating this account are available from a link on the Network Prerequisites installation screen.

5. Select the "WebSphere MQ Installation" option.
6. Select the "Launch WebSphere MQ Installer" option to begin the WebSphere MQ V5.3.0.2 installation. (The Launch WebSphere MQ Installer option is located at the bottom of the WebSphere MQ Launchpad screen.)

7. Read, follow directions, and click Next through the following screens:
   - Welcome
   - License Agreement

8. At the Setup Type screen, choose the Custom installation option and click Next.

9. At the Destination Folder screen, change the default directory. You must supply a subdirectory name. A short directory path is recommended. For example: c:\MQSeries. Remember the WebSphere MQ installation directory name; it is referenced throughout these procedures.
   - After changing the directory name, click OK and then click Next.
   - Note: Do not install WebSphere MQ into a directory name that contains a space.

10. At the "Program files folder" destination screen, click Next to install into the directory path chosen in step 9.

11. At the "Data-files folder" destination screen, click Next to install into the directory path chosen in step 9.

12. At the "Log files folder" destination screen, click Next to install into the directory path chosen in step 9.

13. At the Features window, ensure that "Java Messaging" is selected and click Next.

14. At the "Ready to Install WebSphere MQ" window, review your selections and click Install.
   - Note: At this window, you can use the Back button to change any of your selections. To continue with the installation, select the Next button or press Enter. The status bar displays the progress of the installation.

15. At the "Have you purchase sufficient license units to install IBM WebSphere MQ on this computer" prompt, verify that you have purchased the license units and click "Yes."

16. At the Installation complete screen, select Finish.

**Running the Prepare WebSphere MQ Wizard**

Run the Prepare WebSphere MQ Wizard to complete the WebSphere MQ installation. This procedure creates the default queue manager that manages the messaging queues used by the EMS.

**Note:** The steps below describe an example WebSphere MQ configuration that accepts all default values. If WebSphere MQ is already in use in your environment, you can vary from these procedures. In an existing WebSphere MQ environment, you must use your knowledge of the existing environment to determine the appropriate configuration.

1. When the installation completes, the Prepare WebSphere MQ Wizard Welcome screen appears. Click Next.

2. When prompted with "Are any of the domain controllers in your network running Windows 2000 servers?" provide the answer appropriate for your network environment.
   - If you are unsure of the answer, click the More Information button to access the WebSphere MQ Information Center or consult your network administrator.
3. Follow the instructions on the screens. The screens that appear are dependent on the answer you gave for step 2. Some assistance from your network administrator may be required to complete these screens.

4. When prompted, select "Setup the Default Configuration."

5. At the Default Configuration Wizard Welcome screen, click Next.

6. At the Set up Default Configuration screen, click Next.

7. At the Select Options screen, accept the default settings and click Next.
   
   Note A default queue manager is created with the name of QM_[MACHINENAME], where [MACHINENAME] is the name of the computer on which WebSphere MQ is installed. This queue manager will manage the JMS messaging queues that are created later in this process.

   Note also that both the "Allow remote administration of the queue manager" and the "Join the queue manager to the default cluster" options can be selected.

8. When prompted with "Is this the first computer in the default cluster," select "Yes, make it the repository for the cluster," and click Next.

9. At the Repository Location screen, click Next.

10. At the Default Configuration Summary screen, review your selections and click Finish. A progress bar appears while the default configuration is set up.

11. At the WebSphere MQ Default Configuration screen, wait for the "Default configuration is complete" message to appear in the status window at the bottom of the screen. When the message appears, click Close.

12. At the Prepare WebSphere MQ screen, click Next.

13. At the "Completing the Prepare WebSphere MQ" screen, choose the desired options, or clear all check marks from the options and click Finish to complete the WebSphere MQ server installation.

Next step:

Installing WebSphere MQ 5.3 CSD08 (Fix Pack 8)

Installing WebSphere MQ 5.3 CSD08 (Fix Pack 8) is the fourth of nine steps required to install the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS).

The WebSphere MQ 5.3 CSD08 (Fix Pack 8) includes the WebSphere MQ V5.3 Publish/Subscribe mac0 SupportPac. This SupportPac provides the publish/subscribe broker that assists the WebSphere MQ software with the distribution of messages. You can download WebSphere MQ Fix Packs from this location:


After you have downloaded WebSphere MQ 5.3 CSD08 (u200215a.exe), follow the instructions below to install the fix pack on the WebSphere MQ V5.3.0.2 server:

To install WebSphere MQ 5.3 CSD08:

1. Run the u200215a.exe file.
2. At the Location to Save Files screen, accept the default location and click Next.
3. When prompted to "Click Install to begin installation of CSD08," click Install.
4. Click Finish to complete the installation.
Next step: Install the WebSphere Application Server V5.1

Installing the WebSphere Application Server V5.1, Advanced Edition

Installing the WebSphere Application Server (WAS) V5.1 is the fifth of nine steps required to install the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS). When you install the WebSphere server, perform a custom installation and do not install the Embedded Messaging feature.

To install the WebSphere Application Server V5.1, Advanced Edition on the EMS computer:

1. Ensure that you have logged in to the Windows operating system using a Windows system user ID that has the rights necessary to install the DB2 server. For more information on this user ID, see Setting up the required Windows administrator account.

2. Insert the WebSphere Application Server V5.1, Advanced Edition CD.

3. Start the WebSphere Application Server V5.1, Advanced Edition CD by double-clicking Install.exe from the root of the CD.

   Note If you have downloaded the WebSphere Application Server V5.1 image from a network location, and are executing the install.exe file from a command prompt, make sure that no spaces exist in the path to the install.exe file. The install will not function correctly if spaces exist in the path to the install.exe file.

4. At the Welcome screen, review the warning and click Next.

5. At the Software License Agreement screen, accept the terms of the license agreement and click Next.

6. When prompted to "Choose the setup type that best suits your needs," select "Custom" and click Next.

7. When prompted to "Select the features for "IBM WebSphere Application Server, Version 5 you would like to install;," clear the check mark from the "Embedded Messaging" option so that "Embedded Messaging" is not selected. Accept all of the other default selections, and click Next.

8. When prompted with the default locations for the WAS and HTTP server files, change the defaults to the following and click Next:
   - C:\WebSphere\AppServer
   - C:\IBMHttpServer

9. When prompted to "Enter a Node name and hostname for this installation" review the instructions on the screen and enter the Node name and Host name for the EMS server. Click Next.

10. When prompted with "You can use Windows Services to run the following WebSphere Services," select these two options:
    - Run WebSphere Application Server as a service.
    - Run IBM HTTP Server as a service
    Enter the password associated with the user ID under which you are running the installation and click Next.

11. When prompted with "The following features have been selected for install;" review the list of features and click Next to continue with the installation. A progress bar displays as the installation completes.
12. When prompted to register the product, click Next to register the product or clear the check box and click Next to register the product at a later time.
13. Verify the success of the installer program by examining the Exit summary panel for installation success.
14. Click Finish to exit the installation wizard.
15. Restart the computer.

Next step:
Install the WebSphere Application Server V5.1 Fix Pack 1

Installing the WebSphere Application Server V5.1 Fix Pack 1

Installing the WebSphere Application Server V5.1 Fix Pack 1 is the sixth of nine steps required to install the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS).

The WebSphere Application Server 5.1, Advanced Edition Fix Pack 1 is required by the EMS. For more detailed information about the WebSphere Application Server 5.1, Advanced Edition Fix Pack 1, see the "readme_was51_fp1.html" file that is available with the Fix Pack.

Note: This procedure requires you to know the directories in which the IBM HTTP server and the WebSphere Application Server were installed in the previous procedure. The default directories for the HTTP Server and the Application server are C:\IBMHttpServer and C:\WebSphere\AppServer, respectively.

To install the WebSphere Application Server V5.1 Fix Pack 1 on the EMS computer:

1. Create a working directory on the computer reserved for the EMS installation. This example assumes the working directory is named C:\Update.
2. Download the WebSphere Application Server V5.1 Fix Pack 1 (was51_fp1_win.zip) to the C:\Update directory. You can download the fix pack from this location.  
   http://www-1.ibm.com/support/docview.wss?rs=180&tc=SSEQTP&uid=swg24007195
3. Unzip the contents of was51_fp1_win.zip to the C:\Update directory.
4. Use the Windows Control Panel to stop the following services:
   - IBM HTTP Server 1.3.28
   - IBM HTTP Administration 1.3.28
   - IBM WebSphere Application Server V5 - server 1
   Note: Also stop any of the following services if they are used in your environment: the nodeagent process, the deployment manager process, and all server processes, such as the jms server process, that belong to serviceable features. Also, stop any process_spawner.exe processes.
5. Open a command prompt window on the server.
6. In the command prompt window, change to the <WebSphere install path>\bin directory. For example, enter this command:
   cd WebSphere\AppServer\bin
7. Enter the SetupCmdLine.bat command to set up the Java environment. For example:
   c:\WebSphere\AppServer\bin\setupCmdLine.bat
8. In the command prompt window, change to the Update directory. For example, enter this command:
9. Enter the command updateWizard.bat to begin the installation. For example:
c:\Update\updateWizard.bat
10. At the language selection window, select the appropriate language. Click OK.
11. At the Welcome screen, click Next.
12. At the "The following WebSphere products were found on your computer..." screen, make sure that "IBM WebSphere Application Server v5.1.0" is highlighted and click Next.
13. At the "You can install or uninstall fix packs for this product" screen, select "Install fix packs" and click Next.
14. At the "Enter the directory where fix packs are located" screen, select the "fixpacks" subdirectory in the directory to which you downloaded the fix pack (for example, C:\Update\fixpacks). Click Next.
15. At the "Carefully review and select a fix pack to install for your product" screen, make sure that "was51_fp1_win" is selected and click Next.
16. At the "Specify the file path for the following features if the Update installation wizard cannot locate the features..." screen, do the following:
   • Make sure that "IBM HTTP server" is selected and the correct installation directory for the IBM HTTP server is specified.
   • Make sure that "Embedded Messaging" is not selected.
   • Click Next.
17. Verify that the was51_fp1_win installation details are correct and click Next.
18. When the message appears indicating the fix pack was successfully installed, click Finish.

Next step:
Installing the WebSphere V5.1.1 Cumulative Fix 2

Installing the WebSphere V5.1.1 Cumulative Fix 2 is the seventh of nine steps required to install the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS).

To install the WebSphere V5.1.1 Cumulative Fix 2 on the EMS computer:
1. Create a working directory on the computer reserved for the EMS installation. This example assumes the working directory is named C:\CF2.
2. Download the WebSphere V5.1.1 Cumulative Fix 2 from the following location to the C:\CF2 directory:
   http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&dc=D420&q1=5.1.1.2&uid=swg240
3. If necessary, use the Windows Control Panel to stop the following services (You were also instructed to stop these services in the previous procedure):
   • IBM HTTP Server 1.3.28
   • IBM HTTP Administration 1.3.28
   • IBM WebSphere Application Server V5 - server 1
   Note Also stop any of the following services if they are used in your environment: the nodeagent process, the deployment manager process, and all server processes, such as the jmsserver process, that belong to serviceable features. Also, stop any process_spawner.exe processes.
4. Open a command prompt window on the server.
5. In the command prompt window, change to the `<WebSphere install path>\bin` directory. For example, enter this command:
   ```
   cd WebSphere\AppServer\bin
   ```
6. Enter the SetupCmdLine.bat command to set up the Java environment. For example:
   ```
   c:\WebSphere\AppServer\bin\setupCmdLine.bat
   ```
7. In the command prompt window, change to the CF2 directory. For example, enter this command:
   ```
   cd CF2
   ```
8. Enter the command updateWizard.bat to begin the installation. For example, your complete command string will look like this:
   ```
   c:\CF2>updateWizard.bat
   ```
   **Note** Wait a few seconds for a language selection window to appear. If the language selection window does not appear, you may need to set the Java environment (JAVA_HOME) for the command prompt window. If it is necessary to set the Java environment, instructions for how to do this will appear in the command prompt window (and are also available in the readme file provided with the fix pack). After you set the Java environment, leave the command window open and run the updateWizard.bat command again.
9. At the language selection window, select the appropriate language. Click OK.
10. At the Welcome screen, click Next.
11. At the "The following WebSphere products were found on your computer..." screen, make sure that "IBM WebSphere Application Server v5.1.1" is highlighted and click Next.
12. At the "You can install or uninstall fix packs for this product" screen, select "Install fix packs" and click Next.
13. At the "Enter the directory where fix packs are located" screen, select the "fixpacks" subdirectory in the directory to which you downloaded the fix pack (for example, C:\CF2\fixpacks). Click Next.
14. At the "Carefully review and select a fix pack to install for your product" screen, make sure that "was511_cf2_win" is selected and click Next.
15. Verify that the was511_cf2_win installation details are correct and click Next.
16. When the message appears indicating the fix pack was successfully installed, click Finish.
17. Restart the server computer.

**Next step:**

Setting up the JMS system queues

**Setting up the JMS system queues** is the eighth of nine steps required to **install the J2EE infrastructure** on the computer reserved for the Enterprise Meeting Server (EMS).

The EMS is an MQSeries publish/subscribe application. To ensure a publish/subscribe application runs correctly, you must:
- Ensure the publish/subscribe broker is running.
- Create several JMS publish/subscribe system queues.

Both of these procedures are described below.
Ensuring the publish/subscribe broker is running
To ensure the publish/subscribe broker is running:

1. From the Windows desktop, choose Start -> Programs -> IBM WebSphere MQ -> WebSphere MQ Services to open the MQServices console.
2. Stop the WebSphere MQ Queue Manager:
   a. In the panel on the left side of the WebSphere MQServices console, expand the "WebSphere MQ Services (Local)" icon.
   b. Click once on the QM_<computername> icon so that it is highlighted.
   c. In the MQServices console taskbar, click the black square icon.
   d. In the End Queue Manager window, select Controlled and click OK.
   e. Wait until each of the components displays the "Stopped" status in the right-hand panel of the MQServices console.
3. Right-click the Custom Services folder located underneath the Queue Manager icon and select New -> Custom Service.
4. Complete the following fields in the Create Custom Service window:
   - **Service Name** - run Broker
   - **Start Command** - stmqbrk
   - **End Command** - endmqbrk
   - **Execution** - Process
   - **Startup** - After
5. Click Apply, then click OK.
6. Start the WebSphere MQ Queue Manager:
   a. In the panel on the right side of the WebSphere MQServices console, click "Queue Manager" once so that it is highlighted.
   b. In the MQServices console task bar, click the black triangle icon.
   c. Wait until each of the components displays the "Running" status in the right-hand panel of the MQServices console.

Note that In the MQServices console, the run mqbrk services always displays a status of "stopped" even when the service is running. To verify that the run Broker service is running, or to start the service, follow these steps:

1. Open a command prompt.
2. Change to the <MQ server install path>\java\bin\ directory. For example:
   cd mqseries\java\bin
3. Enter the command strmqbrk. For example:
   C:\mqseries\java\bin>strmqbrk
4. If the service is currently running, a message appears indicating the service is running. If the service was not running, the strmqbrk command starts the service.

Creating the JMS system queues
To create these system queues, run the MQSC script file named "MQJMS_PSQ.mqsc." This file is provided with the WebSphere MQ 5.3 installation.

The MQJMS_PSQ.mqsc script file is located in the "java\bin" subdirectory of the directory in which MQ Series is installed (or C:\<WebSphere MQ install directory>\java\bin). In this example, the MQJMS_PSQ.mqsc file is located in the c:\MQseries\java\bin directory.
1. If necessary, start the Command Prompt on the computer on which WebSphere MQ is installed.
   
   Note In this example, DB2, WebSphere MQ, and WebSphere are all installed on the computer reserved for the EMS deployment.

2. In the Command Prompt window, change to the directory: c:\<WebSphere MQ install directory>\java\bin.
   
   For example, enter:
   
   cd mqseries\java\bin

3. From the command prompt, run the following command:
   
   runmqsc < MQJMS_PSQ.mqsc
   
   For example, the complete command string required to run the MQJMS_PSQ.mqsc file might look like this:
   
   c:\mqseries\java\bin> runmqsc < MQJMS_PSQ.mqsc

4. When the "All valid MQSC commands were processed” message appears, the file has finished running. To ensure that the file completed successfully, verify that there are no error messages displayed on the screen above the "All valid MQSC commands were processed” message.

   Note: The MQJMS_PSQ.mqsc script file creates the following queues:
   
   • SYSTEM.JMS.ADMIN.QUEUE - the JMS publish/subscribe administration queue.
   • SYSTEM.JMS.PS.STATUS.QUEUE - the JMS publish/subscribe subscriber status queue.
   • SYSTEM.JMS.REPORT.QUEUE - the JMS publish/subscribe report queue.
   • SYSTEM.JMS.MODEL.QUEUE - the JMS publish/subscribe subscribers model queue. (This model queue is used by subscribers to create a permanent queue for subscriptions.)
   • SYSTEM.JMS.ND.SUBSCRIBER.QUEUE - the JMS publish/subscribe default non-durable shared queue. (The default shared queue used by non-durable subscribers.)
   • SYSTEM.JMS.ND.CC.SUBSCRIBER.QUEUE - the JMS publish/subscribe default non-durable shared queue for connectionconsumer functionality.
   • SYSTEM.JMS.D.SUBSCRIBER.QUEUE - the JMS publish/subscribe default durable shared queue. (The default shared queue used by durable subscribers.)
   • SYSTEM.JMS.D.CC.SUBSCRIBER.QUEUE - the JMS publish/subscribe default durable shared queue for connectionconsumer functionality.

   Next step:

   Ensuring WebSphere MQ supports the Double-Byte Character Set (DBCS)

   Ensuring WebSphere MQ supports DBCS is the last of nine steps associated with installing the J2EE infrastructure on the computer reserved for the Enterprise Meeting Server (EMS).

   This step is required when you install WebSphere MQ on a Windows server that uses an Asian language that require DBCS support (for example, Chinese, Korean, Japanese, or Taiwanese). This step ensures that conversion between code page 819 and DBCS is supported. This step is not required if WebSphere MQ is installed on an English language server.
To ensure that WebSphere MQ supports DBCS:
1. Start the Command Prompt on the Windows server.
2. In the Command Prompt window, change to the directory: \<WebSphere MQ install directory>\bin.
   For example, enter:
   `cd mqseries\bin`
3. From the command prompt window, run the `runmqsc` command. For example:
   `C:\mqseries\bin\runmqsc` (and press Enter)
4. After you run the `runmqsc` command, the cursor will flash in the command prompt window. Type the following command:
   `Dis qmgr all` (and press Enter)
   The Queue Manager details will display in the command prompt window.
5. After the Queue Manager details display, the cursor will flash in the command prompt window. Type the following command:
   `alter qmgr ccsid(819)` (and press Enter)
   A message will appear indicating the Queue Manager is changed.
6. After the message appears indicating the Queue Manager is changed, the cursor will flash in the command prompt window. Type the end command to complete the session, as shown below:
   `end` (and press Enter)
7. Close the command prompt window.

**Next step:**
This procedure completes the second task required to set up the EMS and a Meeting Services cluster. Next, begin the third task, configuration of the WebSphere server security and LDAP directory access.

### Configuring WebSphere server security and LDAP directory access

Configuring WebSphere server security and LDAP directory access is the third of five tasks associated with setting up the EMS and a Meeting Services cluster.

Before you can deploy the EMS on the WebSphere server, you must configure the WebSphere server security settings. When you configure WebSphere server security, you perform all of the following actions:
- Provide a user in the LDAP directory with the ability to access the WebSphere Administrative Console. (This user is specified in the Server User ID field of the LDAP User Registry page, as noted below.)
- Enable WebSphere security and Single Sign-On (SSO) functionality
- Enable the WebSphere server to access the LDAP directory

To configure the WebSphere security settings and LDAP directory access:
1. Use the Windows Control Panel to verify the following services are started. If the services are not started, start them: now
   - IBM HTTP Server 1.3.28
   - IBM WebSphere Application Server V5 - server 1
2. Start the WebSphere Administrative Console. When prompted for a user ID, click OK.

   Note To start the WebSphere Administrative Console from the Windows desktop, choose Start -> Programs -> IBM WebSphere -> Application Server v5.1 -> Administrative Console.

3. In the left-hand panel of the Administrative Console, select Security -> User Registries -> LDAP.

   In the LDAP User Registry page, make sure that these options are specified:
   - **Server User ID** - Enter the User ID under which the server will run. This User ID must be a valid entry in the LDAP directory beneath the Base Distinguished Name. After specifying this User ID, you must use this User ID to access the WebSphere Administrative Console.
   - **Server User Password** - Enter the password associated with the Server User ID entry in the LDAP directory. After specifying this password, you must use this password to access the WebSphere Administrative Console.
   - **Type** - Specify the LDAP directory type that is appropriate for the LDAP directory that serves as your user repository.
   - **Host** - Enter the DNS name of the LDAP server (for example, ldap.ibm.com).
   - **Port** - Enter the Port on which the LDAP server listens for connections. The default is Port 389.
   - **Base Distinguished Name** - Enter the branch of the LDAP directory tree from which LDAP directory searches must be conducted (for example, o=ibm, c=us).
   - **Ignore Case** - Select this option to ensure that authorization checks are case-insensitive.
   - **Bind Distinguished Name** and **Bind Password** - If the LDAP directory requires authentication, enter the name and password required to authenticate with the LDAP server in these fields.

   Note: These settings are needed when setting up the EMS in a test environment to ensure that the EMS functions correctly. Further configuration of the LDAP directory access is at your discretion.

4. Click the Apply button.

5. In the left-hand panel of the Administrative Console, select Security -> Authentication Mechanisms -> LTPA.

   In the LTPA page, specify these options:
   - **Password** - Enter the password used to encrypt and decrypt the LTPA keys.
   - **Confirm Password** - Retype the password entered above.
   - **Timeout** - Enter 120. This setting specifies the number of minutes after which an LTPA token will expire.

   Note: Later in this process, you will export these LTPA keys to the Sametime servers. Remember the password and Timeout values you have specified for the LTPA keys.

6. In the Additional Properties box at the bottom of the LTPA page, select “Single Sign-On (SSO).”

   In the LTPA -> Single Signon (SSO) page, specify these options:
   - **Enabled** - Select this check box to enable SSO.
   - **Domain name** - Enter the domain name (for example, ibm.com) that is used by all hosts to which the SSO functionality applies.

   Click Apply.

8. In the Global Security page of the Administrative Console, make sure these options are specified:
   - Enabled - Select this check box to enable security for the WebSphere domain.
   - Enforce Java 2 Security - Select this check box to enable Java 2 security.
   - Active Authentication Mechanism - Select "LTPA (Lightweight Third Party Authentication)."
   - Active User Registry - Select "LDAP."

   Note: You can accept all other default settings on the Global Security page.

9. Click the "Save" option in the WebSphere Administrative Console task bar to save the security settings.

10. On the Save to Master Configuration page, click "Save" to write changes to the master repository.

11. Log out of the WebSphere Administrative Console and close the Web browser.

12. Open the Web browser and log back into the WebSphere Administrative Console.

13. Open a command prompt on the server and restart server1 from a command line so that the new security settings take effect. The command to stop a WebSphere application server has this format:

   ```
c:\WebSphere\install_path\bin\stopserver.bat <servername> -username <username> -password <password>
   ```

   In this command <servername> is the name of the WebSphere application server you want to stop. The <username> and <password> values are the name and password of the user to whom you have granted access to the WebSphere Administrative Console. For more information on this user name and password, see [WebSphere and EMS system administration accounts](#).

   For example, to stop server1, open a command prompt on the server and enter this command at the command line:

   ```
c:\WebSphere\AppServer\bin\stopserver.bat server1 -username cn=emsadmin, ou=people, o=ems -password
   ```

   To start server1, enter this command on the command line:

   ```
c:\WebSphere\AppServer\bin\StartServer server1
   ```

14. Verify that the settings on the Global Security page of the WebSphere Administrative Console are still in effect.

   In the left-hand panel of the Administrative Console, select Security -> Global Security.

   In the Global Security page of the Administrative Console, make sure these options are specified:
   - Enabled - Verify this option is selected. If this option in not selected, select it.
   - Enforce Java 2 Security - Verify this option is selected. If this option in not selected, select it.
   - Active Authentication Mechanism - Verify that the "LTPA (Lightweight Third Party Authentication)" option is selected. If this option is not selected, select it.
   - Active User Registry - Verify that the "LDAP" option is selected. If this option is not selected, select it.

   Click OK.
Next step:
This procedure completes the third task required to set up the EMS and a Meeting Services cluster. Next, begin the fourth task, Deploying the Enterprise Meeting Server.

Deploying the Enterprise Meeting Server

Deploying the Web Conference Management Server (EMS) is the fourth of five tasks associated with setting up the EMS and a Meeting Services cluster.

Deploying the Enterprise Meeting Server is described in thirteen steps:

1. Creating three additional WebSphere Application Servers
2. Installing the Enterprise Meeting Server files
3. Creating the DB2 database
4. Creating the WebSphere MQ queues
5. Defining the WebSphere Variables
6. Defining the JAAS Alias
7. Setting up the JDBC Provider Resource and creating the Data Source
8. Creating the JMS Connection Factory
9. Creating the JMS Destinations
10. Ensuring UTF-8 Unicode character support for the EMS
11. Deploying the STAdmin, STCenter, and STServer Enterprise Archive (EAR) files
12. Regenerating the WebServer plugin and starting the Enterprise Meeting Server Enterprise Applications

Creating and configuring three additional WebSphere Application Servers

Creating and configuring three additional WebSphere Application Servers to support EMS application components is the first of twelve steps required to deploy the EMS application.

The IBM Lotus Enterprise Meeting Server (EMS) requires four WebSphere Application Servers. One application server (named "server1") is created by default during the WebSphere server installation. Do not delete server1 from the WebSphere server.

In this procedure you create and configure these three additional WebSphere application servers to support components of the EMS:

- **STAdmin** - Supports the EMS Administration Tool
- **STCenter** - Supports the EMS Meeting Center
- **STServer** - Supports all other EMS server components, such as the Health Monitor and Load Balancer.

Follow the steps below to create and configure the STAdmin, STCenter, and STServer application servers. Configuring the servers involves adding the appropriate Listener Ports to each of the application servers.

**Note:** All entries in the dialog boxes used in this procedure are case-sensitive. Type the entries exactly as shown in the steps below.
To create and configure the STAdmin, STCenter, and STServer application servers:

1. Start the WebSphere Administrative Console.
   From the Windows desktop, choose Start -> Programs -> IBM WebSphere -> Application Server v5.1 -> Administrative Console.
   To log in to the WebSphere Administrative Console, you must enter the WebSphere Administrator name and password you specified when you configured WebSphere server security and LDAP directory access.
2. In the left-hand panel of the Administrative Console, select Servers -> Application Servers.
3. Click the New button.
4. In the Server name field, enter "STAdmin".
5. Click the Next button and then click the Finish button.
6. Click the New button.
7. In the Server name field, enter "STCenter".
8. Click the Next button and then the Finish button.
9. Click the New button.
10. In the Server name field, enter "STServer".
11. Click the Next button and then the Finish button.
12. Click Save.
13. In the left-hand panel of the Administrative Console, select Servers -> Application Servers, and then click on "STAdmin."
14. In the Additional Properties box at the bottom of the STAdmin page, select "Message Listener Service."
15. In the Additional Properties box at the bottom of the "Message Listener Service" page, select "Listener Ports."
16. Click the New button.
17. Select the Configuration tab (if necessary) and complete the following fields for the STAdmin server Listener Ports:
   - **Name** - ConfigurationChangeMDBPort
   - **Connection factory JNDI name** - jms/SametimeTopicConnectionFactory
   - **Destination JNDI name** - jms/SametimeConfigurationTopic
   - **Maximum retries** - 2147483647
   
   **Note** You can accept the default settings for all other fields on the Listener Ports page.
18. Click OK.
19. In the left-hand panel of the Administrative Console, select Servers -> Application Servers, and then click on "STCenter."
20. In the Additional Properties box at the bottom of the STCenter page, select "Message Listener Service."
21. In the Additional Properties box at the bottom of the "Message Listener Service" page, select "Listener Ports."
22. Select the Configuration tab (if necessary) and complete the following fields for the STCenter server Listener Ports:
   - **Name** - ConfigurationChangeMDBPort
   - **Connection factory JNDI name** - jms/SametimeTopicConnectionFactory
   - **Destination JNDI name** - jms/SametimeConfigurationTopic
   - **Maximum retries** - 2147483647
23. Click OK.
24. In the left-hand panel of the Administrative Console, select Servers -> Application Servers, and then click on “STServer.”
25. In the Additional Properties box at the bottom of the STServer page, select "Message Listener Service.”
26. In the Additional Properties box at the bottom of the "Message Listener Service” page, select "Listener Ports.”
27. Select the Configuration tab (if necessary) and complete the following fields for the STServer server Listener Ports:
   - **Name** - ConfigurationChangeMDBPort
   - **Connection factory JNDI name** - jms/SametimeTopicConnectionFactory
   - **Destination JNDI name** - jms/SametimeConfigurationTopic
   - **Maximum retries** - 2147483647
28. Click OK.
29. Click Save.
30. Click New and repeat the previous procedure to add the following six listener ports to the STServer application server:
   - **Name** - HealthMonitorMDBPort
   - **Connection factory JNDI name** - jms/SametimeQueueConnectionFactory
   - **Destination JNDI name** - jms/SametimeHealthQueue
   - **Maximum retries** - 2147483647
   - **Name** - LoadMonitorMDBPort
   - **Connection factory JNDI name** - jms/SametimeQueueConnectionFactory
   - **Destination JNDI name** - jms/SametimeStatisticsQueue
   - **Maximum retries** - 2147483647
   - **Name** - LogServiceMDBPort
   - **Connection factory JNDI name** - jms/SametimeQueueConnectionFactory
   - **Destination JNDI name** - jms/SametimeLogQueue
   - **Maximum retries** - 2147483647
   - **Name** - PostProcessorMDBPort
   - **Connection factory JNDI name** - jms/SametimeQueueConnectionFactory
   - **Destination JNDI name** - jms/SametimePostProcessingQueue
   - **Maximum retries** - 2147483647
   - **Name** - SchedulerMDB1Port
   - **Connection factory JNDI name** - jms/SametimeQueueConnectionFactory
   - **Destination JNDI name** - jms/SametimeMeetingStateQueue
   - **Maximum retries** - 2147483647
   - **Name** - SchedulerMDB2Port
   - **Connection factory JNDI name** - jms/SametimeQueueConnectionFactory
   - **Destination JNDI name** - jms/SametimeMeetingCommandQueue
   - **Maximum retries** - 2147483647
31. After the last Listener Port is created, click OK and then click Save in the Administrative Console task bar.
32. Open a command prompt on the server and restart server1 from a command line so that the new settings take effect. The command to stop a WebSphere application server has this format:
   
   ```
   c:\<WebSphere install path>\bin\stopserver.bat <servername> -username <username> -password <password> -stop
   ```
In this command <servername> is the name of the WebSphere application server you want to stop. The <username> and <password> values are the name and password of the user to whom you have granted access to the WebSphere Administrative Console. For more information on this user name and password, see WebSphere and EMS system administration accounts.

For example, to stop server1, open a command prompt on the server and enter this command at the command line:

c:\WebSphere\AppServer\bin\stopserver.bat server1 -username cn=emsadmin, ou=people, o=ems -password

To start server1, enter this command on the command line:

c:\WebSphere\AppServer\bin\StartServer server1

Next step:
Installing the Enterprise Meeting Server files

Installing the Enterprise Meeting Server files is the second of twelve steps required to deploy the EMS application.

Install the EMS files on the computer on which you have installed the WebSphere V5.1.1.2 server. This step installs the files required to deploy the EMS on the WebSphere server.

To install the EMS files:
1. Insert the EMS CD in the computer reserved for the EMS installation and select Install the Enterprise Meeting Server.
2. Choose the Setup language and click OK.
3. Read, follow directions, and click Accept or Next through the following screens:
   - Welcome
   - Software License Agreement
   - Information
4. In the "Verify Location of WebSphere Application Server" window, verify that the WebSphere location is correct. In our example, the correct location is C:\WebSphere\AppServer. If the location is incorrect, browse to the correct location. Click Next.
5. In the "Verify Location to Install Files" window, specify the directory where the files will be installed. This example assumes that you install the files to the C:\WebConferencing directory.
6. In the "Summary Information" screen, review the information and click Next.
7. At the "Setup Complete" screen, click Finish.

Next step:
Create the DB2 database

Creating the DB2 database used by the Enterprise Meeting Server (EMS) is the third of twelve steps required to deploy the EMS.

To create the DB2 database, you must run the castddb2.db2 file that was installed into the C:\WebConferencing directory with all other EMS files in the previous step.
Note: This example assumes that the DB2 and WebSphere software are installed on the same computer. In a production environment, you may choose to install DB2 on a separate, dedicated computer. In this case, you must copy the createstdb2.db2 file to the DB2 computer and create the DB2 database on that computer. After you create the DB2 database on the DB2 server, you must install a DB2 client on the WebSphere Application Server and use this DB2 client to catalogue and connect to the Sametime DB2 database created with the createstdb2.db2 file on the DB2 server. For information about installing and using the DB2 client, see the DB2 Information Center provided with the DB2 software.

To create the DB2 database:
1. In the server Command Prompt window on the EMS computer, change to the directory in which you have installed the EMS files (for example, C:\WebConferencing).
2. From the command prompt, run the following command:
   createstdb.bat db2admin (where db2admin is the user name of the DB2 server administrator)
   For example, the complete command string required to run the createstdb command might look like this:
   C:\WebConferencing>createstdb db2admin
3. When prompted, enter the password for the DB2 server administrator. Press Enter.
   After a brief delay, a succession of "SQL command completed successfully" messages appears on the screen. When a message indicating "the SQL DISCONNECT command completed successfully" appears, the EMS DB2 database creation is complete.

Next step: Create the WebSphere MQ queues

Creating the WebSphere MQ queues
Creating the WebSphere MQ queues for the Enterprise Meeting Server (EMS) is the fourth of twelve steps required to deploy the EMS.

To create the WebSphere MQ queues required by the EMS, you must run the "mq.qdef.pcf" script file from the WebSphere MQ installation directory. The "mq.qdef.pcf" file is located in the directory to which you have installed the EMS files (for example, C:\WebConferencing).

To run the "mq.qdef.pcf" file from the Command Prompt:
1. By default, the mq.qdef.pcf file is a read-only file. Use Windows Explorer to remove the Read-only attribute from this file. For example:
   a. Open Windows Explorer.
   b. Open the C:\WebConferencing directory.
   c. Right click on the mq.qdef.pcf file and select Properties.
   d. Clear the check mark from the Read-only attribute.
2. If necessary, start the Command Prompt on the EMS computer.
   Note: This procedure requires you to run a command from the computer on which WebSphere MQ is installed. In this example, DB2, WebSphere, and WebSphere MQ are all installed on the same computer so you can run this command from the EMS computer. If you have installed WebSphere MQ on a separate computer from WebSphere, you must open the Command Prompt on
the computer on which WebSphere MQ is installed and run the runmqsc command from that computer, as noted below.

3. In the Command Prompt window, change to the `<WebSphere MQ installation>`\bin directory. For example, enter:

cdmqseries\bin

4. From the command prompt, run the following command:

runmqsc < mq.qdef.pcf

Remember that the "mq.qdef.pcf" file is located in the C:\WebConferencing directory. For example, if WebSphere MQ and the EMS files are installed on the same computer, your command string might look like this:
c:\mqseries\bin>runmqsc < c:\WebConferencing\mq.qdef.pcf

Alternatively, you can copy the "mq.qdef.pcf" file to the `<WebSphere MQ installation>`\bin directory and enter the following command:
c:\mqseries\bin>runmqsc < mq.qdef.pcf

**Note** If you have installed WebSphere MQ on a different computer than WebSphere (and the EMS files), you must copy the mq.qdef.pcf file from the WebSphere computer to the WebSphere MQ computer and run the file from WebSphere MQ computer.

5. When the "All valid MQSC commands were processed" message appears, the file has finished running. To ensure that the file completed successfully, verify that there are no error messages displayed on the screen above the "All valid MQSC commands were processed" message. A list of queues that were created also appears in the command prompt window above the "All valid MQSC commands were processed" message.

**Next step:**
Define the WebSphere variables

**Defining the WebSphere Variables**

Defining the WebSphere variables is the fifth of twelve steps required to deploy the EMS.

In this procedure, you define the WebSphere variables that specify the path to the DB2 JDBC Driver and the path to the WebSphere MQ Server installation directory.

To define the WebSphere variables:

1. Start the WebSphere Administrator’s Console, if necessary.

   From the Windows desktop, choose Start -> Programs -> IBM WebSphere -> Application Server v5.1 -> Administrative Console.

   To log in to the WebSphere Administrator’s Console, you must enter the WebSphere Administrator name and password you specified when you configured WebSphere server security and LDAP directory access.

2. In the left-hand panel of the Administrative Console, select Environment -> Manage WebSphere Variables.

3. In the list of variables, click on DB2_JDBC_DRIVER_PATH.

4. In the Value field, enter the path to the DB2 JDBC Driver. The driver resides in the java subdirectory of the DB2 server installation directory. In this example, the path to the DB2 JDBC Driver is:

   C:\Program Files\SQLLIB\java

5. Click OK.

6. In the list of variables, click on MQ_INSTALL_ROOT.
7. In the Value field, enter the MQ Server installation directory. In this example, the MQ Server is installed in the C:\MQSeries directory.

8. Click OK.

9. Click Save in the Administrative Console task bar.

**Next step:**
Define the JAAS Alias

### Defining the JAAS Alias
Defining the JAAS alias is the sixth of twelve steps required to **deploy the EMS**

In this procedure, you provide the Java Authentication and Authorization Service (JAAS) with the administrator user name password needed to authenticate when connecting to the DB2 server. You specified this user name and password when installing the DB2 server.

To define the JAAS Alias:
1. Start the WebSphere Administrative Console, if necessary.
2. In the left-hand panel of the Administrative Console, select Security -> JAAS Configuration -> J2C Authentication Data.
3. Click New.
4. Complete the following fields on the New J2C Authentication Data page:
   - **Alias** - db2admin
   - **User ID** - db2admin
   - **Password** - <db2admin password>
   *Note* The user ID and password you enter at this screen must correspond to the user ID and password you specified for the DB2 administrator when you installed the DB2 server.
5. Click OK.
6. Click Save in the Administrative Console task bar.

**Next step:**
Setting up the JDBC Provider Resource and creating the Data Source

### Setting up the JDBC Provider Resource and creating the Data Source
Setting up the JDBC Provider Resource and creating the Data Source from the WebSphere Administrator Console is the seventh of twelve steps required to **deploy the EMS**

All entries in the dialog boxes used in this procedure are case sensitive. Type the entries exactly as shown in the steps below.

To set up the JDBC Provider Resource and create the Data Sources from the WebSphere Administrative Console:
1. Start the WebSphere Administrative Console, if necessary.
2. In the left-hand panel of the Administrative Console, select Resources -> JDBC Provider.
3. Click New.
4. In the drop-down list, select "DB2 Legacy CLI-based Type 2 JDBC Driver (XA)".
5. Click Apply.
6. In the Additional Properties box at the bottom of the DB2 Legacy CLI-based Type 2 JDBC Driver (XA) configuration page, select "Data Sources."
7. Click New.
8. In the New Data Sources page, complete these fields:
   - Name - SametimeDataSource
   - JNDI name - jdbc/SametimeDataSource
   - Component Managed Authentication Alias - Select "db2admin" from the drop-down list.
   - Container Managed Authentication Alias - Select "db2admin" from the drop-down list.
9. Click Apply.
10. In the Additional Properties box at the bottom of the SametimeDataSource configuration page, select "Connection Pool."
11. In the "Max Connections" field, change the value to "100".
12. Click OK.
13. In the Additional Properties box at the bottom of the SametimeDataSource configuration page, select "Custom Properties."
14. Click on the "databaseName" setting and change its value to "Sametime."
15. Click OK.
16. Click Save in the Administrative Console task bar.

At this point, you should test the connection to the DB2 database. To test this connection, do the following:

1. From the WebSphere Administrative Console, select Resources ->JDBC Providers-> DB2 Legacy CLI-based Type 2 JDBC Driver(XA) -> Data Sources.
2. Select the check box next to SametimeDataSource.
3. Click the "Test Connection" button.
4. A message at the top of the window indicates whether the database connection was successful.

**Next step:**
Create the JMS Connection Factory

**Creating the JMS Connection Factory**

Creating the JMS Connection Factory from the WebSphere Administrator Console is the eighth of twelve steps required to deploy the EMS.

All entries in the dialog boxes used in this procedure are case-sensitive. Type the entries exactly as shown in the steps below.

To install the JMS Connection Factory from the WebSphere Administrative Console:

1. Start the WebSphere Administrative Console, if necessary.
2. In the left-hand panel of the Administrative Console, select Resources -> WebSphere MQ JMS Provider.
3. In the Additional Properties box at the bottom of the WebSphere MQ JMS Provider configuration page, select "WebSphere MQ Queue Connection Factories."
4. Click New.
5. In the New WebSphere MQ Queue Connection Factories page, complete these fields:
   - **Name** - SametimeQueueConnectionFactory
   - **JNDI Name** - jms/SametimeQueueConnectionFactory
   - **Host** - <fully qualified DNS name of the server hosting the MQ queue manager>
   - **Port** - 1414
   - **Transport Type** - Client

6. Click OK.

7. In the left-hand panel of the Administrative Console, select Resources -> WebSphere MQ JMS Provider.

8. In the Additional Properties box at the bottom of the WebSphere MQ JMS Provider configuration page, select "WebSphere MQ Topic Connection Factories."

9. Click New.

10. In the New WebSphere MQ Queue Topic Connection Factories page, complete these fields:
    - **Name** - SametimeTopicConnectionFactory
    - **JNDI Name** - jms/SametimeTopicConnectionFactory
    - **Host** - <fully qualified server name of the server that hosts the WebSphere MQ queue manager>
    - **Port** - 1414
    - **Transport Type** - Client
    - **Broker Version** - Basic

11. Click OK.

12. Click Save in the Administrative Console task bar.

**Next step:**

Create the JMS Destinations

Creating the JMS Destinations

Creating the JMS Destinations from the WebSphere Administrative Console is the ninth of twelve steps required to deploy the EMS.

All entries in the dialog boxes used in this procedure are case sensitive. Type the entries exactly as shown in the steps below.

To create the JMS Destinations from the WebSphere Administrative Console:
1. Start the WebSphere Administrator’s Console, if necessary.
2. In the left-hand panel of the Administrative Console, select Resources -> WebSphere MQ JMS Provider.
3. In the Additional Properties box at the bottom of the WebSphere MQ JMS Provider configuration page, select "WebSphere MQ Topic Destinations."
4. Click New.
5. In the New WebSphere MQ Topic Destinations page, complete these fields:
   - **Name** - SametimeConfigurationTopic
   - **JNDI Name** - jms/SametimeConfigurationTopic
   - **Base Topic Name** - SametimeConfigurationTopic

**Note** You can accept all other default settings on the page.
6. Click OK.
7. In the left-hand panel of the Administrative Console, select Resources -> WebSphere MQ JMS Provider.
8. In the Additional Properties box at the bottom of the WebSphere MQ JMS Provider configuration page, select "WebSphere MQ Queue Destinations."
9. Click New.
10. In the New WebSphere MQ Queue Destinations page, complete these fields:
   - Name - SametimeLogQueue
   - JNDI Name - jms/SametimeLogQueue
   Note: You can accept all other default settings on the page.
11. Click OK.
12. Click New and repeat the previous procedure to add the following seven Queue Destinations:
   - Name - SametimeStatisticsQueue
   - JNDI Name - jms/SametimeStatisticsQueue
   - Name - SametimeHealthQueue
   - JNDI Name - jms/SametimeHealthQueue
   - Name - SametimeMeetingStateQueue
   - JNDI Name - jms/SametimeMeetingStateQueue
   - Name - SametimeMeetingCommandQueue
   - JNDI Name - jms/SametimeMeetingCommandQueue
   - Name - SametimePostProcessingQueue
   - JNDI Name - jms/SametimePostProcessingQueue
   - Name - SametimeProvisioningEventQueue
   - JNDI Name - jms/SametimeProvisioningEventQueue
13. After the last Queue Destination is created, click OK and then click Save in the Administrative Console task bar.

**Next step:**

**Ensuring UTF-8 Unicode character support for the EMS**

Ensuring Unicode character support for the EMS is the tenth of twelve steps required to deploy the EMS.

This procedure ensures that the STAdmin, STCenter, and STServer WebSphere application servers can support the Double-Byte Character Set (DBCS) and extended ASCII characters for text handling and display purposes. This procedure enables UTF-8 encoding of the Unicode character set.

To ensure UTF-8 Unicode character support for the STAdmin, STCenter, and STServer application servers, use the WebSphere Administrative Console to perform the following steps:
1. Start the WebSphere Administrative Console, if necessary.
2. In the left-hand panel of the Administrative Console, select Servers -> Application Servers.
3. In the Application Servers list, click on "STAdmin."
4. In the Additional Properties box at the bottom of the STAdmin configuration page, click "Process Definition."
5. In the Additional Properties box at the bottom of the Process Definition configuration page, click "Java Virtual Machine."
6. In the Java Virtual Machine configuration page, type the following string in the "Generic JVM Arguments" field exactly as shown below:
   -Dclient.encoding.override=UTF-8
7. Click OK.
8. In the Administrative Console, return to Servers -> Application Servers and repeat steps 4 through 7 for both the STCenter and STServer application servers.
9. Click Save in the Administrative Console task bar.

**Next step:**

Deploying the STAdmin, STCenter, and STServer Enterprise Archive (EAR) files

Deploying the STAdmin, STCenter, and STServer Enterprise Archive (EAR) files is the eleventh of twelve steps required to deploy the EMS.

When you install the EMS files, the STAdmin, STCenter, and STServer EAR files are placed in the C:\WebSphere\AppServer\InstallableApps directory.

You use the same procedure to deploy all three of the EAR files. Follow the procedure below to deploy the STAdmin EAR file. After you deploy the STAdmin.ear file, follow this same procedure to deploy the STCenter.EAR and the STServer.EAR files.

To deploy the EAR files:
1. Start the WebSphere Administrative Console, if necessary.
2. In the left-hand panel of the Administrative Console, select Applications -> Install New Applications.
3. On the "Preparing for the application installation" page, select "Local path," then browse to the C:\WebSphere\AppServer\installableApps directory and select the STAdmin.ear file.
4. Click Next.
5. In the "Preparing for the application installation" page, select all of the following options:
   - Generate Default Bindings
   - Override existing bindings
   - Default virtual host name for web modules (This option is selected by default. Also verify that the text box below this option contains the value "default_host".)
6. Click Next.
7. At the "Application Security Warnings" page, click Continue.
8. At the "Step 1: Provide options to perform the installation" page, select "Deploy EJBs."
   **Note** You can accept the other default selections on the "Step 1: Provide options to perform the installation page."
9. Click Next.
10. Click Next at each of the following configuration pages. You do not need to change or enter any settings on these configuration pages.
• Step 2: Provide options to perform the EJB deploy
• Step 3: Provide L1Listener Ports for Messaging Beans
• Step 4: Provide JNDI Names for Beans
• Step 5: Map EJB References to Beans
• Step 6: Map resource references to resources
• Step 7: Map virtual hosts for web modules

11. In the "Step 8: Map modules to application servers" configuration page, do the following:
   a. In the "Clusters and Servers" window, select the server that corresponds to the EAR file that you are deploying. For example, if you are deploying the STAdmin.ear file, you would select an entry similar to this from the Clusters and Servers window:
      WebSphere:cell=ACME,node=ACME,server=STAdmin
   b. In the Module column, select the check boxes available for the EJB and WAR modules that correspond to the EAR file that you are deploying. For example, if you are deploying the STAdmin.ear file, select the check boxes next to these two modules:
      STAdmin EJB
      STAdmin WAR
   c. Click Apply.
   d. Click Next.

12. In the "Step 9: Map security roles to users/groups" configuration page, do the following to provide EMS administrator privileges to the user specified as the WebSphere\EMS administrator.
    Note You specified the WebSphere\EMS administrator in the procedure titled "Configuring WebSphere security and LDAP directory access. This user is also discussed in the Create or identify the required LDAP directory accounts topic earlier in this chapter.
    a. Select these three roles from the list of roles:
       stadmin
       stmanager
       stservices
    b. Select Lookup users.
    c. In the "Search String" field, type the name of the user in the LDAP directory you have chosen as the WebSphere\EMS administrator.
    d. In the "Available" column, select the WebSphere administrator name and click the >> button to move the administrator into the "Selected" column.
    e. Click OK (and you are returned to the "Step 9: Map security roles to users/groups" configuration page).

13. Perform this step only when deploying the STCenter.EAR file. The security roles you assign in this step are not applicable to the STAdmin.EAR or STServer.EAR files.
    In the "Step 9: Map security roles to users/groups" configuration page, do the following to require all users to authenticate when accessing the EMS. This configuration enables any authenticated user to have access to all end user features of the EMS.
    a. Select these roles from the list of roles:
       stcreate
       stattend
For each of the roles above, select the "Everyone?" value.

c. Select the "stauthenticateduser" role from the list of roles.

d. For the "stauthenticateduser" role, select the "All Authenticated?" value.

e. Click Next.

Note After you complete these installation procedures, you can refine the access levels you provide for end users. See Securing user access to the Enterprise Meeting Server for more information.

14. At the "Step 10: Ensure all unprotected 2.0 methods have the correct level of protection" configuration page, accept the default settings and click Next. This step is required only when deploying the STServer.ear file.

15. At the "Step 11: Summary" page, click Finish. When the installation completes, a message appears indicating the application installed successfully.

16. Click the "Save to Master Configuration" link.

17. At the "Save to Master Configuration" page, click Save to conclude the deployment of the EAR file.

18. Open a command prompt on the server, and start the newly deployed server application from a command line. To start a WebSphere application server enter the command in this format:

c:\<WebSphere install path>\bin\StartServer <servername>

For example, to start the STAdmin server, enter this command:

c:\WebSphere\AppServer\bin\StartServer STAdmin

19. Repeat this procedure to install STCenter.ear file and the STServer.ear file (select the appropriate file in step 3 and start the appropriate server in step 18 when repeating this procedure).

Next step: Regenerate the WebServer plugin and start the Enterprise Meeting Server Enterprise Applications

Regenerating the WebServer plugin and starting the Enterprise Meeting Server Enterprise Applications is the last of twelve steps required to deploy the EMS.

To regenerate the WebServer plugin and start the Enterprise Meeting Server Enterprise Applications:

1. Start the WebSphere Administrative Console, if necessary.

2. In the left-hand panel of the Administrative Console, select Environment -> Update Web Server Plugin.

3. At the "Update web server plugin configuration" screen, click OK.

4. Restart the IBM HTTP server. From the Windows desktop:
   a. Select Programs - IBM HTTP Server - Stop HTTP Server.
   b. Select Programs - IBM HTTP Server - Start HTTP Server.
Next step:
This procedure completes the fourth task required to set up the EMS and a Meeting Services cluster. Next, begin the last task, **Adding Sametime servers to the EMS**.

---

**Adding Sametime servers to the EMS**

Adding Sametime servers to the Meeting Services cluster is the last of five tasks associated with **setting up the EMS and a Meeting Services cluster**.

At this point, you have installed the Sametime servers and deployed the EMS. Next, you must add the Sametime servers to the EMS. After the Sametime servers are added to the EMS, the EMS:

- Provides the central end user and administrative interface to the Sametime servers.
- Performs all Meeting Services cluster management functions discussed in the **Overview of the Enterprise Meeting Server and Meeting Services clustering** section of this documentation.

When you add Sametime servers to the EMS, you use the “Usage Limits and Denied Entry” settings in the EMS Administration Tool to determine whether Meeting Services activity can or cannot occur on the Sametime server.

Lotus IBM software recommends that you use the “Usage Limits and Denied Entry” settings of the EMS Administration Tool to prevent Meeting Services activity from occurring on the Sametime servers that will comprise a Community Services cluster. For example, if you have added Sametime servers A, B, C, and D to the EMS, and you want Sametime servers A and B to operate as a Community Services cluster, use the “Usage Limits and Denied Entry” settings to prevent Meeting Services activity from occurring on Sametime servers A and B.

In the scenario discussed above, you must also perform the procedures discussed in [Creating a Community Services cluster with the EMS](#) to enable Sametime servers A and B to operate as a Community Services cluster. Sametime servers C and D will operate as a Meeting Services cluster after you complete the eight steps below. The eight steps below are the only procedures required to enable Sametime servers C and D to operate as part of a Meeting Services cluster.

To add a Sametime server to the EMS:

1. **Synchronize Single Sign-On (SSO) support for the EMS and Sametime servers**
2. **Edit the Sametime.ini file on the Sametime servers**
3. **Edit the MeetingServices document in the Configuration database on the Sametime server**
4. **Provide the WebSphere and EMS administrator account with Manager access to the sconfig.nsf database**
5. **Enable the Sametime servers to store recorded meeting files on a remote computer**
6. **Start the EMS Administration Tool for the first time**
7. **Add the Sametime server using the EMS Administration Tool**
8. **Specifying Usage Limits and Denied Entry settings for the Sametime server**
Synchronizing the Single Sign-On (SSO) support for the EMS and Sametime servers

Synchronizing the Single Sign-On (SSO) support for the EMS and Sametime servers is the first of eight steps required to **add a Sametime server to the EMS**.

This step ensures that the same LTPA keys that authenticate users when they access the EMS on the WebSphere server can be used to authenticate Sametime client connections to the Sametime servers in the cluster. The users are authenticated against the LDAP directory.

**Note:** This step is required even if you allow all users to access the EMS anonymously. You determine whether users must authenticate when accessing the EMS or are allowed to access the EMS anonymously when you secure user access to the Enterprise Meeting Server as described in the “Setting up security for the Enterprise Meeting Server” chapter of this documentation.

To synchronize the SSO support you must export the LTPA Key file from the WebSphere server and import it to the Sametime server that is being added to the Meeting Services cluster. Both of these procedures are described below.

**Exporting the LTPA Key file from the WebSphere server**

To export the LTPA Key file from the WebSphere server:

1. Start the WebSphere Administrator’s Console.
   
   From the Windows desktop, choose Start-Programs-IBM WebSphere-Application Server V5.1-Administrative Console.
   
2. Select Security -> Authentication Mechanisms -> LTPA.
   
3. Scroll to the bottom of the LTPA screen and enter a name in the Key File Name field. For example, enter "WASKeys."
   
4. Click Export Keys.
   
   **Note** In the LTPA Settings box, note the values specified in the Timeout field (default 120 minutes). You must specify the same token timeout period when importing these keys to the Sametime server.
   
5. The WASKeys LTPA key file is exported to the WebSphere installation directory (for example, C:\WebSphere\AppServer). Copy the WASKeys file from the WebSphere installation directory to a network location that is accessible from the Sametime servers, or copy the WASKeys file directly to a Sametime server.

**Import the LTPA Key file to the Sametime server**

The Sametime server installation creates a Domino LTPA key by default. Note that this Domino LTPA key is reset when you import the WebSphere LTPA Key file to the Sametime server. It is not necessary to delete the existing Domino LTPA key before importing the WebSphere LTPA Key file.

**Importing the WebSphere LTPA Key file**

To import the WebSphere LTPA Key file, you must create a new Domino Web SSO Configuration document in the Domino Directory on the Sametime server. This new document includes the following fields, which must contain values that are identical to the values that were specified when the WebSphere LTPA keys were created:

- **Token Domain** - The Token Domain field specifies the DNS domain name in which the EMS server and Sametime servers operate. The token domain does not include a specific host name. An example entry is .ibm.com.
Make sure that the entry in the Token Domain field of the Web SSO document is the same as the entry you specified in the Domain Name field located in the Security - Authentication Mechanisms - LTPA - Additional Properties - Single Sign-On (SSO) page of the WebSphere Administrative Console. You specified that domain setting in the Configuring WebSphere server security and LDAP directory access procedure earlier in this documentation.

- **Expiration** - The Expiration field specifies the length of time for which an SSO token is valid.
  
  This Expiration value must be the same as the value you specified in the Timeout field of the Security - Authentication Mechanisms - LTPA page of the WebSphere Administrative Console.

After you have create the new Domino Web SSO Configuration document with the appropriate Token Domain and Expiration values, you can import the WebSphere LTPA keys by entering the LTPA password that you specified when creating the WebSphere LTPA keys. This password was specified during the Configuring WebSphere server security and LDAP directory access task following the WebSphere installation.

To create the Domino Web SSO Configuration document and import the WebSphere LTPA keys:

1. In the Domino Directory, select Server-Servers to open the Servers view.
2. From the Servers view, select the “Web...” pull-down menu button.
3. Select Create Web SSO Configuration.
4. Complete the following fields in the Web SSO Configuration document. The values entered in these fields must be identical to the values that were entered when you created the WebSphere LTPA keys following the WebSphere installation.
   
   - **Token Domain** - The domain entered in this field must be identical to the domain specified for the WebSphere LTPA keys, as noted above.
   
   - **Expiration** - The value entered in this field must be identical to the Timeout value specified for the WebSphere SSO token, as noted above. The suggested value is 120 minutes.
   
   - **Domino Server Names** - This field should contain the names of all Sametime servers that are part of the Sametime community in which the Meeting Services cluster operates. The server names must be entered in the Domino server name format (for example, Sametimeserver1/East/Acme). You can browse the Domino Directory to add the server names to this field.
5. Select the Keys-Import WebSphere LTPA Keys menu option.
6. In the Enter Import File Name dialog box, type the directory path to the WASKeys LTPA key file. (In the previous procedure, you were instructed to copy the WASKeys file from the WebSphere server to a network location accessible to the Sametime server or to the Sametime server itself.)
7. In the Enter Import File Password dialog box, enter the password associated with the WebSphere LTPA import file.
8. A "Successfully imported WebSphere LTPA keys" message appears on the screen. Click OK.
9. After the WebSphere LTPA keys have been imported, a WebSphere Information section appears in the Domino Web SSO Configuration document. You must alter the entry that appears in the LDAP Realm field of the WebSphere Information section.
In the LDAP Realm field, the LDAP server name will appear in one of the following formats (assuming the LDAP server name is ldap1.acme.com):

- ldap1.acme.com
- ldap1.acme.com:389

**Important:** If the LDAP server name has the port number appended (for example, ldap1.acme.com:389), you must alter the LDAP Realm entry so that a back-slash character (\) appears after the LDAP server name but in front of the colon. For example, if your LDAP server name is ldap1.acme.com, the correct entry in the LDAP Realm field is "ldap1.acme.com:389".

If the LDAP server name does not have the port number appended (for example, ldap1.acme.com), do not alter the entry in the LDAP Realm field. Leave the entry as "ldap1.acme.com" in the LDAP Realm field.

10. Click "Save and Close" to save the Web SSO Configuration document.

11. The Domino Directory to which you have imported the WebSphere LTPA keys must replicate to the other Sametime servers that you plan to add to the EMS to complete the SSO synchronization. Either manually replicate the Domino Directory, or wait for the scheduled replication to occur before proceeding to the next step.

If you manually replicate the Domino Directory, you can restart the HTTP server to ensure that the new SSO configuration is immediately in effect on the server. If you do not restart the Domino HTTP server, the new SSO configuration may not take effect immediately.

**Next step:**

**Edit the Sametime.ini file on the Sametime servers**

Editing the Sametime.ini file on the Sametime servers is the second of eight steps required to **add a Sametime server to the EMS**.

Each Sametime server that is added to the EMS contains processes that must access a configuration servlet on the EMS computer. The Sametime servers must authenticate when accessing the configuration servlet. To ensure that each Sametime server can authenticate, you must enter a user name and password in the Sametime.ini file on the Sametime server.

The user name and password you enter in the Sametime.ini file on each Sametime server should be the user name and password associated with the Configuration servlet access account you created earlier in this process. For more information, see **Configuration servlet access account in the EMS pre-deployment requirements and considerations** section of this documentation.

To add the user name and password to the Sametime.ini file on each Sametime server:

1. Use a text editor to open the Sametime.ini file located in the C:\Lotus\Domino directory.

2. At the bottom of the [Config] section of the Sametime.ini file, manually type the following entries into the file:

   - SametimeAdminUsername=
   - SametimeAdminPassword=

   Populate the entries with the same user name and password associated with the Configuration servlet access account. For example, if you created a special
directory account for Sametime configuration servlet access named "Configuration Servlet Access" with a password of "sametime," populate the entries as follows:

- SametimeAdminUsername=Configuration Servlet Access
- SametimeAdminPassword=sametime


4. Repeat this procedure on every Sametime server that you want to add to the EMS.

**Note:** In subsequent procedure, you will reboot the Sametime server. After you reboot the server, the SametimeAdminUsername and SametimeAdminPassword entries are encrypted and the user name and password will not be visible in the Sametime.ini file.

**Next step:**

**Edit the Meeting Services document in the Configuration database on the Sametime server**

Editing the MeetingServices document in the Configuration database on the Sametime server is the third of eight steps required to add a Sametime server to the EMS.

The EMS contains processes that must access the Meeting Management API (MMAPI) on the Sametime server. To ensure the EMS processes can be authenticated when accessing the MMAPI, you must do the following:

- Provide the MMAPI access account user name with the Manager access level in the Sametime Configuration database. For more information about this user account, see Sametime Meeting Management API (MMAPI) access account topic in the EMS pre-deployment requirements and considerations section of this documentation.
- Enter the MMAPI access account user name and password in four different sections of the MeetingServices document in the Configuration database.

To add the MMAPI account to the Configuration database ACL and edit the MeetingServices document:

1. Use a Lotus Notes client to open the stconfig.nsf database on the Sametime server.
2. Select File - Database - Access Control.
3. Click the Add button.
4. Enter the MMAPI access account name in the Add User dialog box.
5. Click OK.
6. Select the MMAPI access account name from the list in the Database Security window.
7. In the User Type drop-down list, select Person.
8. In the Access drop-down list, select Manager.
9. Make sure that all ACL privileges, such as “Create documents” and “Delete documents” are selected.
10. Click the Roles button.
11. Select the DatabaseAdmin, SametimeAdmin, and SametimeMonitor roles. Click OK.

12. In the Configuration database, select the "All - By Form and Date" view and then open the MeetingServices document (by double-clicking on the date associated with the document).

13. Scroll to the "Remote Service Access" section at the bottom of the MeetingServices document.

14. Populate the eight fields in the "Remote Service Access" section with the user name and password you created for this purpose. For example:


15. Save the Meetingservices document and close the Configuration database.

**Note:** In the next procedure, you will reboot the Sametime server. The Sametime server must be rebooted before the user name and password can be used to authenticate access to the MMAPI.

**Next step:**

Provide the WebSphere and EMS administrator account with Manager access to the stconfig.nsf database

**Provide the WebSphere and EMS administrator account with Manager access to the stconfig.nsf database**

Providing the WebSphere and EMS administrator account with Manager access to the stconfig.nsf database is the fourth of eight steps required to add a Sametime server to the EMS.

The WebSphere and EMS administrator account must have Manager access to the Sametime Configuration (stconfig.nsf) database on each Sametime server that you plan to add to the EMS. The WebSphere and EMS administrator account must also have all roles (DatabaseAdmin, SametimeAdmin, and SametimeMonitor) selected in the stconfig.nsf database.

**Note:** The WebSphere and EMS administrator account is discussed in [WebSphere and EMS system administration accounts](#). Note that the user name that you add to the ACL of the stconfig.nsf database in this step must be the same user name that you provided with the stadmin, stmanager, and stservices roles when you deployed the STAdmin, STCenter, and STServer Enterprise Archive (EAR) files earlier in this process.

To provide the WebSphere and EMS administrator account with Manager access to the stconfig.nsf database:

1. Use a Lotus Notes client to open the stconfig.nsf database on the Sametime server.
2. Select File - Database - Access Control.
3. Click the Add button.
4. Enter the WebSphere and EMS administrator account name in the Add User dialog box.
5. Click OK.
6. Select the WebSphere and EMS account name from the list in the Database Security window.
7. In the User Type drop-down list, select Person.
8. In the Access drop-down list, select Manager.
9. Make sure that all ACL privileges, such as “Create documents” and “Delete documents” are selected.
10. Click the Roles button.
11. Select the DatabaseAdmin, SametimeAdmin, and SametimeMonitor roles. Click OK.
12. Repeat this procedure on each Sametime server that you will add to the EMS.

**Next step:**
Enable the Sametime servers to store recorded meeting files on a remote server

**Enable the Sametime servers to store recorded meeting files on a remote server**

Enabling Sametime servers to store recorded meeting files on a remote computer is the fifth of eight steps required to:

Recorded meeting files can consume significant disk space and should be stored on a separate server from the EMS computer. In this procedure, you set up a specific directory structure on the remote server and then configure each Sametime server to store the recorded meeting files within the directory structure on the remote server.

To enable the Sametime servers to store recorded meeting files on a remote server:

1. On the remote server, create a directory to store the recorded meeting files. This example assumes that you create a directory named C:\RecordedMeetings on the remote server.
2. Make the C:\RecordedMeeting directory on the remote server available for sharing and provide Everyone with Full Control to the shared directory. For example:
   a. In Windows Explorer, right-click on the C:\RecordedMeetings directory and select “Sharing...”
   b. In the Sharing tab, select “Share this folder.”
   c. Click the Security tab.
   d. Select the Everyone entry so that it is highlighted (if necessary). In the Permissions box, make sure that the “Allow” option is selected for each of the Permissions listed in the Permissions box. The Everyone entry should be provided with all Permissions to the shared folder.
3. In the C:\RecordedMeetings directory, create a subdirectory for each of the Sametime servers that will operate as part of the Meeting Services cluster controlled by the EMS. For example, if your Meeting Services cluster consists of two Sametime servers, you might create an STServer_1 and STServer_2 subdirectory on the remote server, as shown below:
   • C:\RecordedMeetings\STServer_1
   • C:\RecordedMeetings\STServer_2
4. On each of the Sametime servers, use Windows Explorer to map to the directory created in step 4 that is associated with the Sametime server. For example, on Sametime server 1 create a mapping to the T:\RecordedMeetings\STServer_1 directory on the remote server. When you
repeat these procedures for Sameitme server 2, create a mapping from
Sametime server 2 to the T:\RecordedMeetings\STServer_2 directory.
It is mandatory that you associate the same drive letter with the mapping on
each of the Sametime servers. In the example above, the T drive letter is used
for the mappings from both servers. If, instead, you map
R:\RecordedMeetings\STServer_1 from Sametime server 1, you must also map
to R:\RecordedMeetings\STServer_2 from Sametime server 2.

5. For each Sametime server, do the following:
   a. Use a Lotus Notes client to open the Sametime Configuration database
      (stconfig.nsf) on the Sametime server.
   b. Open the MeetingServices document (by double-clicking on the date
      associated with the document).
   c. Scroll down to the "Record Meeting Settings" section.
   d. For the Recorded Meeting Settings -> Directory Path value, enter the
directory path for the mapping you created from that server.
      For example, on STServer_1 enter "T:\RecordedMeetings\STServer_1\"
      and on STServer_2 enter "T:\RecordedMeetings\STServer_2\".
      It is mandatory to include the trailing backslash when entering the the
      mapped directory path into the Recorded Meeting Settings - > Directory
      Path value.

6. On each of the Sametime servers, do the following:
   a. In the Windows Control Panel, navigate to the "Sametime Meeting Server”
      service.
   b. Right-click on the Sametime Meeting Server service and select Properties.
   c. Click the Log On tab.
   d. Select the "This account” option to enable the service to log on as a user
      account instead of a local system account. In the fields provided, you can
      enter the user name and password of any user that has access to the
      network share.

Next step:
Start the EMS Administration Tool for the first time

Start the EMS Administration Tool for the first time

Starting the EMS Administration Tool for the first time is the sixth of eight steps
required to add a Sametime server to the EMS

The first time you start the EMS Administration Tool, you are prompted to enter
the host name of the IBM HTTP server and the WebSphere and EMS administrator
account user name and password.

Note: The WebSphere and EMS administrator account is discussed in WebSphere
and EMS system administration accounts. Note that you provided this
account with administrator access to the EMS when you deployed the
STAdmin, STCenter, and STServer Enterprise Archive (EAR) files

You must also stop and restart the STAdmin application server from the
WebSphere Administrative Console after you start the EMS Administration Tool for
the first time.

To start the EMS Administration Tool for the first time:
1. Open the WebSphere Administrative Console on the EMS computer and verify that the STAdmin application server is started. If the STAdmin application server is not started, start it now.

2. Use a Web browser to browse to the URL for the EMS Administration Tool, as shown below:
   http://<HTTP Server fully-qualified DNS name>/iwc-admin/client

3. In the Web Conferencing Manager Cluster Name screen, enter the following:
   - **Host name of the EMS cluster** - Enter the fully-qualified DNS name of the IBM HTTP server.
   - **Name** - Enter the user name associated with the WebSphere and EMS administrator account in the LDAP directory.
   - **Password** - Enter the password associated with the WebSphere and EMS administrator account.

   Click Add.

4. Close the EMS Administration Tool.

5. From the WebSphere Administrative Console on the EMS computer, stop and restart the STAdmin application server.

**Next step:**

Adding a Sametime server using the Sametime EMS Administration Tool

Adding a Sametime server using the EMS Administration Tool is the seventh of eight steps required to add a Sametime server to the EMS.

For information on what happens when you perform this procedure, see What happens when you add a Sametime server using the Sametime EMS Administration Tool.

To add a Sametime server to the EMS:

1. Use the WebSphere Administrative Console on the EMS computer to verify that the server1, STAdmin, STCenter, and STServer application servers are started. If these application servers are not started, start them now.

2. Start the Sametime server that you want to add to the EMS. Start the Sametime server from the Sametime server desktop. Select Start -> Programs -> Lotus Applications and then select Lotus Domino Server.

3. Enter the following URL in a Web browser to browse to the EMS Administration Tool:
   http://<HTTP Server fully-qualified DNS name>/iwc-admin/client

4. Enter the administrator user name and password to access the EMS Administration Tool.

5. Select Configuration -> Meeting Cluster. (This tab may be displayed by default when you open the EMS Administration Tool.)

6. In the "Host name, IP address, or full URL of the additional server" field, enter the Host name, IP address, or full URL of the Sametime server that is to be added to the EMS and click Add.

7. When you see the message indicating the Sametime server is successfully added to the Meeting Services cluster, reboot the Sametime server you have just added to the Meeting Services cluster.

8. Repeat this procedure for each Sametime server you want to add to the EMS.
What happens when you add a Sametime server using the EMS Administration Tool

When you add a Sametime server to a Meeting Services cluster from the EMS Administration Tool:

- A check is performed to determine if more than one LDAP directory is used in the community. The Sametime servers that operate in a Meeting Services cluster cannot access multiple LDAP directories.
- All configuration data that is stored in the stconfig.nsf database on the Sametime server is written into the DB2 database available to the EMS. Once this configuration data is written to the DB2 database, you must use the Sametime Administration Tool available from the EMS to administer the Sametime server. The EMS Administration Tool writes configuration parameters to the DB2 database. The Sametime servers that operate as part of the Meeting Services cluster must store and retrieve their configuration parameters in the DB2 database.

The standard Sametime Administration Tool available from the Sametime Meeting Center on the Sametime server can no longer be used to administer the Sametime servers. The standard Sametime Administration Tool writes configuration parameters to the stconfig.nsf database on the Sametime server. Sametime servers that have been added to the EMS must store and retrieve their configuration parameters from the DB2 database.
- A URL redirection document is set up for the Sametime server. The URL redirection document prevents end users and administrators from accessing the Sametime server with a Web browser. Any user attempting to access the following URLs on the Sametime server is redirected to the Enterprise Meeting Server:
  - The Sametime server home page (<servername>/stcenter.nsf)
  - The Sametime Meeting Center (<servername>/stconf.nsf)
  - The Sametime Administration client (<servername>/servlet/auth/admin)
- The following values are written to the Sametime.ini file on the Sametime server:
  - ConfigurationHost and ConfigurationPort values - These values ensure that all configuration calls go through the EMS DB2 database.
  - A Java Naming and Directory Interface (JNDI) URL and context factory classname for JNDI lookups - These values ensure that JMS communications can occur between the EMS and the Sametime servers.
  - The EMS cluster name - Each Sametime server in the cluster must be aware of the name of the Meeting Services cluster to which it belongs.
- Any existing Domino Connection documents of the connection type "Sametime" that specify this Sametime server as a source server or destination server are invalidated. These Connection documents exist to support the "invited server" functionality discussed in Deploying multiple Sametime servers. The "invited server" is not used (or needed) with Sametime servers that are controlled by the EMS.

Next step:
Specify the usage limits and denied entry settings for the Sametime server

Specifying Usage Limits and Denied Entry settings for the Sametime server

Specifying Usage Limits and Denied Entry settings for the Sametime server is the last of eight steps associated with adding a Sametime server to the EMS.
You use the EMS Administration Tool to specify the Usage Limits and Denied Entry settings for the Sametime servers that have been added to the EMS. Specifying the Usage Limits and Denied Entry settings is an important step that can serve two separate purposes. These two purposes include:

- **Preventing Meeting Services activity from occurring on a Sametime server that has been added to the EMS** - You can use the Usage Limits and Denied Entry settings to prevent Meeting Services activity from occurring on Sametime servers that will operate as part of a Community Services cluster. For more information about using the Usage Limits and Denied Entry settings for this purpose, see [Preventing Meeting Services activity from occurring on a Sametime server](#).

- **Enabling a Sametime server to operate as part of a Meeting Services cluster** - You can use the Usage Limits and Denied Entry settings to enable a Sametime server to operate as part of a Meeting Services cluster. To enable a Sametime server to operate as part of a Meeting Services cluster, you must specify the amount of Meeting Services activity that can occur on each Sametime server in the cluster. For more information about using the Usage Limits and Denied Entry settings for this purpose, see [Enabling a Sametime server to operate as part of a Meeting Services cluster](#).

### Preventing Meeting Services activity from occurring on a Sametime server

You can use the Usage Limits and Denied Entry settings of the EMS Administration Tool to ensure that no Meeting Services activity occurs on an individual Sametime server that has been added to the EMS. Generally, you only prevent Meeting Services activity from occurring on a Sametime server if you want the Sametime server to operate as part of a Community Services cluster.

For example, if you add Sametime servers A, B, C, and D to the EMS, and you want Sametime servers A and B to operate as part of a Community Services cluster, you can use the Usage Limits and Denied Entry settings of the EMS Administration Tool to prevent Meeting Services activity from occurring on Sametime servers A and B.

You prevent Meeting Services activity from occurring on Sametime servers A and B to ensure that Sametime servers A and B are dedicated to supporting only Community Services activity. Dedicating Sametime servers to the support of Community Services activity makes it easier to ensure that you have the appropriate number of Sametime servers in place to support the anticipated Community Services load of the entire community.

**Note:** The Community Services load-bearing capabilities of the Sametime servers are briefly discussed in the topics [Deploying separate multiplexers in front of a Community Services cluster](#) and [Setting up a Community Services cluster without clustering the Meeting Services](#) earlier in this documentation.

### Important notes about preventing Meeting Services activity from occurring on a Sametime server

- Preventing Meeting Services activity from occurring on a Sametime server is not the only procedure required to enable a Sametime server that has been added to the EMS to operate as part of a Community Services cluster. After preventing Meeting Services activity from occurring on a Sametime server, you must perform the procedures described in [Creating a Community Services cluster](#).
with the EMS to enable Sametime servers that are controlled by the EMS to operate as a Community Services cluster.

- It is not mandatory to prevent Meeting Services activity from occurring on a Sametime server that will operate as part of a Community Services cluster. A Sametime server that has been added to the EMS can operate both as part of a Meeting Services cluster and a Community Services cluster. This configuration is possible but not recommended because it is more difficult to predict the amount of Meeting Services and Community Services activity that may occur on the Sametime server at any given time. A sudden surge in Meeting Services or Community Services activity on the server may hinder the performance of one or both of these services. Although it is not recommended, you can enable a Sametime server controlled by the EMS to operate both as part of a Community Services cluster and a Meeting Services cluster. To do this, perform the procedures discussed in the topic "Enabling a Sametime server to operate as part of a Meeting Services cluster" and then perform the procedures discussed in the chapter "Creating a Community Services cluster with the EMS".

**Note:** Do not perform the procedure below if you want Sametime servers controlled by the EMS to operate both as part of a Meeting Services cluster and a Community Services cluster.

**Procedure for preventing Meeting Services activity from occurring on a Sametime server:** To prevent Meeting Services activity from occurring on a Sametime server, you must enter a 0 (zero) in all fields in the "Edit/Remove a Server" tab of the EMS Administration Tool that control the amount of Meeting Services activity that can occur on a Sametime server. Follow the steps below:

1. Enter the following URL in a Web browser to browse to the EMS Administration Tool:
   
   http://<HTTP Server fully-qualified DNS name>/iwc-admin/client

   **Note** If the EMS Administration Tool is already open, skip to step 4.

2. Enter an administrator user name and password to access the EMS Administration Tool.


4. Select the "Edit/Remove a Meeting Server" tab.

5. In the "Meeting Servers in this cluster" drop-down box, select the name of the Sametime server for which you want to set usage limits.

6. Enter a 0 (zero) in all of the following fields pertaining to Meeting Services activity:
   - Set a maximum number of instant meetings allowed on the server
   - Set a maximum number of interactive audio connections for all instant meetings on the server
   - Set a maximum number of interactive video connections for all instant meetings on the server
   - Set a maximum number of scheduled meetings allowed on the server
   - Set a maximum number of participants in any one meeting
   - Set a maximum number of participants on the server
   - Set a maximum number of interactive audio connections for all scheduled meetings on the server
   - Set a maximum number of interactive video connections for all scheduled meetings on the server
   - Set a maximum number of unicast audio streams for all broadcast meetings
• Set a maximum number of unicast video streams for all broadcast meetings
• Set a maximum number of unicast data streams for all broadcast meetings

7. Click Update for the changes to take effect.
8. Repeat steps 5 through 7 for every server that you have added to the EMS that you want to operate as part of a Community Services cluster.

Next step:

After you have prevented Meeting Services activity from occurring on all Sametime servers that you want to operate as part of a Community Services cluster, you must complete the set up of the Community Services cluster by performing the procedures discussed in Creating a Community Services cluster with the EMS.

To ensure that the remaining servers that you have added to the EMS can operate as part of a Meeting Services cluster, see the procedure Enabling a Sametime server to operate as part of a Meeting Services cluster.

Enabling a Sametime server to operate as part of a Meeting Services cluster

Once a Sametime server is added to the EMS, the Sametime server will operate as part of a Meeting Services cluster by default.

Note: The administrator can prevent a Sametime server from operating as part of a Meeting Services cluster by performing the procedure discussed in the topic Preventing Meeting Services activity from occurring on a Sametime server.

For example, if an administrator adds Sametime servers A, B, C, and D to the EMS, and the administrator prevents Meeting Services activity from occurring on Sametime servers A and B, but not Sametime servers C and D, Sametime servers C and D will operate as a Meeting Services cluster.

The administrator uses the Usage Limits and Denied Entry settings of the EMS Administration Tool to control the amount of Meeting Services activity that can occur in the entire Meeting Services cluster. The administrator controls the amount of Meeting Services activity that can occur in the entire cluster by specifying Usage Limits and Denied Entry settings for each Sametime server in the cluster. For example, the administrator sets the Usage Limits and Denied Entry settings on Sametime server C and then sets the Usage Limits and Denied Entry settings on Sametime server D. The aggregate amount of Meeting Services activity the administrator allows on both Sametime servers comprises the amount of Meeting Services activity that can occur in the entire cluster.

The administrator should set the usage limits for an individual server immediately after adding the server to the Meeting Services cluster from the EMS Administration Tool.

Examples of usage limit settings include:
• Maximum number of meetings on the server
• Maximum number of instant meetings on the server
• Maximum number of participants in any one meeting

These usage limits are used by the Booking Agent on the EMS. These limits provide the Booking Agent with the values it requires to determine the aggregate
meeting demand that can be supported by all Sametime servers in the Meeting Services cluster. For example, if you have two servers in a Meeting Services cluster, and you set the maximum number of scheduled meetings allowed to 100 on each of these servers, the Booking Agent is aware that the Meeting Services cluster can support 200 scheduled meetings at one time. If a user attempts to schedule a meeting for a time at which 200 other meetings are also scheduled, the user is prompted to reschedule the meeting for a different time.

**Note:** For more information about the Booking Agent, see [Booking meetings in the Meeting Services cluster](#).

The load balancer component on the EMS also uses the usage limits. At meeting start time, the load balancer determines which server in the Meeting Services cluster is the best server to host the meeting. The load balancer considers the usage limits when determining which server in the cluster is best able to support the load of the meeting.

The usage limits also prevent server failures or poor performance caused by a meeting overload on the servers within the cluster. These settings enable the administrator to ensure that the meeting load specified for an individual server matches the processing capabilities of the server. Generally, the administrator can accept the default values for the usage limits settings if the Sametime server meets the basic system requirements as shown in the [Ensuring the hardware required for an EMS deployment is available](#) topic earlier in this documentation.

If the processing capabilities of the Sametime server exceed the basic system requirements, the administrator can increase the usage limits to accommodate the enhanced processing capabilities of the server. Some experimentation with these settings might be necessary to determine the proper load for an individual server.

**Specifying Usage Limits and Denied Entry settings for Sametime servers in a Meeting Services cluster:** Use the procedures below to specify the usage limits and denied entry settings for Sametime servers in a Meeting Services cluster. Use the EMS Administration Tool to configure these settings. The EMS Administration Tool allows you to configure one set of limits for instant meetings and a separate set of limits for scheduled and broadcast meetings.

To specify the usage limits and denied entry settings for instant meetings.

1. Enter the following URL in a Web browser to browse to the EMS Administration Tool:
   
   http://<HTTP Server fully-qualified DNS name>/iwc-admin/client
   
   **Note** If the EMS Administration Tool is already open, skip to step 4.

2. Enter an administrator user name and password to access the EMS Administration Tool.


4. Select the "Edit/Remove a Meeting Server" tab.

5. In the "Meeting Servers in this cluster" drop-down box, select the name of the Sametime server for which you want to set usage limits.

6. In the "Set a maximum number of instant meetings allowed on the server" field, enter the maximum number for instant meetings. This setting defaults to 100 at the time the server is added to the cluster.

   Note that you can use this setting to segregate instant meetings and scheduled meetings to separate Sametime servers within a Meeting Services cluster. For example, if you have Sametime servers C and D, you can set the maximum
number of instant meetings allowed on Sametime server C to 200 and the maximum number of instant meetings that occur on Sametime server D to 0. Similarly, you can set the maximum number of scheduled meetings allowed on Sametime server D to 200 and the maximum number of scheduled meetings allowed on Sametime server C to 0. Segregating instant meetings and scheduled meeting activity to separate servers within a Meeting Services cluster can provide more predictable control over server performance for instant and scheduled meetings.

7. The "Set a maximum number of interactive audio connections for all instant meetings on this server" defaults to the value that is specified on the Sametime server at the time the server is added to the cluster. For more information on this setting, see Setting a maximum number of interactive audio connections for all instant meetings.

8. The "Set a maximum number of interactive video connections for all instant meetings on this server" setting defaults to the value that is specified on the Sametime server at the time the server is added to the cluster. For more information about this setting, see Setting a maximum number of interactive video connections for all instant meetings.

Use the procedure below to specify the usage limits and denied entry settings for scheduled and broadcast meetings on a Sametime server.

From the EMS Administration Tool:

1. In the "Set a maximum number of scheduled meetings allowed on the server" field, enter the maximum number for scheduled meetings. This setting is only available on a Sametime server that is part of a Meeting Services cluster. This setting defaults to 100 at the time the server is added to the cluster.

   If you set this value to zero, no scheduled meetings are allowed on the server.

2. In the "Set a maximum number of participants in any one meeting" field, enter the maximum number of users allowed in a meeting. If you have two Sametime servers in your Meeting Services cluster, and you set this value to 100 on Sametime server C and 200 on Sametime server D, the following rules apply:
   - Any meeting scheduled with more than 100 participants will start on Sametime server D.
   - Any meeting scheduled with 100 participants or less can start on Sametime server C or Sametime server D.
   - If a user attempts to schedule a meeting that includes more than 200 participants, the user receives an error message and must reschedule the meeting to include less than 200 participants.

3. In the "Set a maximum number of participants on the server" field, enter the maximum number of participants allowed in all meetings occurring on the server at any given time. The default value for this setting is 1000.

4. The "Set a maximum number of interactive audio connections for all scheduled meetings on the server" setting defaults to the value that is specified on the Sametime server at the time the server is added to the cluster. For more information about this setting, see Setting a maximum number of interactive audio connections for all scheduled meetings.

5. The "Set a maximum number of interactive video connections for all scheduled meetings on the server" setting defaults to the value that is specified on the Sametime server at the time the server is added to the cluster. For more information about this setting, see Setting a maximum number of interactive video connections for all scheduled meetings.
6. The "Set a maximum number of unicast audio streams for all broadcast meetings" setting defaults to the value specified for the "Maximum number of audio connections for all broadcast meetings" setting on the Sametime server at the time the server is added to the cluster. (This setting is labeled differently in the EMS Administration Tool than in the standard Sametime Administration Tool available from the Sametime server.) For more information about this setting, see Setting a maximum number of audio connections for all broadcast meetings.

7. The "Set a maximum number of unicast video streams for all broadcast meetings" defaults to the value specified for the "Maximum number of video connections for all broadcast meetings" setting on the Sametime server at the time the server is added to the cluster. (This setting is labeled differently in the EMS Administration Tool than in the standard Sametime Administration Tool available from the Sametime server.) For more information about this setting, see Setting a maximum number of video connections for all broadcast meetings.

8. The "Set a maximum number of unicast data streams for all broadcast meetings" setting defaults to the value specified for the "Maximum number of data connections for all broadcast meetings" setting on the Sametime server at the time the server is added to the cluster. For more information about this setting, see Setting a maximum number of data connections for all broadcast meetings.

9. Click Update for the changes to take effect.

At this point you can access the end user interface of the EMS. For information, see Accessing the EMS user interface later in this chapter.

Next step: Next you must set up security for the EMS.

Use the EMS Administration Tool to monitor and make configuration changes to all Sametime servers that are part of a Meeting Services cluster. For more information about administering Sametime servers in the Meeting Services cluster, see Using the EMS Administration Tool to administer a cluster.

If you have used the Usage Limits and Denied Entry settings to prevent Meeting Services activity from occurring on Sametime servers, you must perform the procedures discussed in Creating a Community Services cluster with the EMS to enable those servers to operate as a Community Services cluster.

---

**Accessing the EMS user interface**

After you have added Sametime servers to the EMS, you can browse to the EMS application from a Web browser by entering the following URL in the Web browser: http://<EMS server fully-qualified domain name>/iwc/center. For example, enter http://sametime.EMS.ibm.com/iwc/center in the Web browser to view the EMS user interface.
Chapter 18. Creating a Community Services cluster with the Enterprise Meeting Server

Community Services clusters provide Community Services load balancing and failure functionality for large communities. This chapter provides an example of how to cluster the Community Services of a group of IBMLotus Sametime servers after the servers have been added to the IBM Lotus Enterprise Meeting Server (EMS).

If you want to cluster the Community Services of Sametime servers that have been added to the EMS, you must use the procedures described in the "Community Services cluster setup procedures (with the EMS)" topic of this chapter.

If you want to cluster the Community Services of Sametime servers that have not been added to the EMS, use the procedures described in the "Community Services cluster setup procedures" topic in the "Setting up a Community Services cluster without clustering the Meeting Services" chapter earlier in this documentation. Note that you should perform the procedures in that chapter only if you do not intend to deploy the EMS.

You can find additional information about the EMS and Sametime server clusters in the following chapters:
- Chapter 15 - Introduction to Sametime server clusters and the Enterprise Meeting Server
- Chapter 16 - Setting up a Community Services cluster without clustering the Meeting Services
- Chapter 17 - Setting up the Enterprise Meeting Server and a Meeting Services cluster
- Chapter 19 - Setting up security for the Enterprise Meeting Server
- Chapter 20 - Administering server clusters from the EMS Administration Tool

Community Services cluster setup procedures (with the EMS)

This section discusses the procedures required to cluster the Community Services of Sametime servers that have been added to the EMS.

Before you can perform the procedures described in this chapter, you must have deployed the EMS and created a Meeting Services cluster as described in Setting up the Enterprise Meeting Server and a Meeting Services cluster earlier in this documentation.

The procedures required to set up a Community Services cluster after you have added Sametime servers to the EMS are very similar to the procedures required to set up a Community Services cluster without clustering the Meeting Services.

The primary difference between these two set up processes involves the configuration of parameters that enable the Sametime servers to function as a Community Services cluster. When you create a Community Services cluster without clustering the Meeting Services, you configure these parameters by using a Lotus Notes client to alter settings in the Configuration databases (stconfig.nsf) on the Sametime servers.
When you add a Sametime server to the EMS, all configuration data that is stored in the stconfig.nsf database on the Sametime server is written to the DB2 database used by the EMS. After a Sametime server is added to the EMS, the Sametime server relies on this DB2 database for its configuration data. The Sametime server does not get configuration information from the stconfig.nsf database on the Sametime server.

Because of this difference, you must directly alter parameters in this DB2 database to configure a Sametime server to operate as part of a Community Services cluster if that Sametime server has already been added to the EMS.

The procedures required to set up a Community Services cluster using Sametime servers that have been added to the EMS are listed below. For detailed information on some of these procedures, you must refer to procedures described in Setting up a Community Services cluster without clustering the Meeting Services chapter earlier in this documentation.

To set up a Community Services cluster after the Meeting Services of the Sametime servers have been added to the EMS to function as a Meeting Services cluster, perform these procedures:

1. **Create a Domino server cluster**
2. **Set up real-time replication of Sametime databases**
3. **(Optional) Deploy separate Community Services multiplexers**
4. **Set up a load balancing mechanism**
5. **Configure the Community Services clustering parameters in the DB2 database**
6. **Configure client connectivity**

### Create a Domino server cluster

Creating a Domino server cluster is the first of six procedures associated with setting up a Community Services cluster using Sametime servers that have been added to the EMS.

To operate as a Community Services cluster, the Domino servers on which Sametime is installed must first be configured to operate as a Domino server cluster.

The procedure used to create the Domino server cluster is identical to the procedure that is described in the Creating a Domino server cluster topic of the Setting up a Community Services Cluster without clustering the Meeting Services chapter earlier in this documentation. Use the instructions in that topic to create the Domino server cluster.

Note that you should only cluster the Domino servers of the Sametime servers that will operate as part of the Community Services cluster. Do not cluster the Domino servers of the other Sametime servers that are controlled by the EMS.

For example, if Sametime servers A, B, C, and D are added to the EMS, and you want to create a Community Services cluster consisting of Sametime servers A and B, you must create a Domino server cluster consisting of servers A and B. Do not include Sametime servers C and D in the Domino server cluster.

**Next step:**

Set up real-time replication of Sametime databases
Set up real-time replication of Sametime databases

Setting up real-time replication of Sametime databases is the second of six procedures associated with setting up a Community Services cluster using Sametime servers that have been added to the EMS.

After creating the Domino Server cluster, you must set up real-time replication of the Privacy database (vpuserinfo.nsf), the Domino Directory (names.nsf), and in some cases, the Secrets database (stauths.nsf). These databases must replicate in real-time between the Sametime servers that will operate as a Community Services cluster.

The procedure required to set up replication of these databases is identical to the procedure that is described in the "Setting up replication of Sametime databases" topic of the “Setting up a Community Services Cluster without clustering the Meeting Services” chapter earlier in this documentation. Use the instructions in that topic to set up real-time replication of the Sametime databases.

Next step:
(Optional) Deploy separate Community Services multiplexers

(Optional) Deploying separate Community Services multiplexers

Deploying separate Community Services multiplexers is the third of six procedures associated with setting up a Community Services cluster using Sametime servers that have been added to the EMS.

Deploying separate multiplexers in front of a Community Services cluster is an optional configuration that increases the Community Services load-handling capabilities. If you do not want to deploy separate multiplexers for your Community Services cluster, continue to the Set up a load balancing mechanism procedure.

If you intend to deploy separate Community Services multiplexers, be sure to review the topic Deploying separate Community Services multiplexers (optional) in the “Setting up a Community Services cluster without clustering the Meeting Services” chapter before deploying the multiplexers.

Note that the procedures required to deploy separate Community Services multiplexers in front of a Community Services cluster consisting of Sametime servers controlled by the EMS is identical to the procedure used to deploy separate Community Services multiplexers in front of a Community Services cluster consisting of Sametime servers not controlled by the EMS with one exception, as discussed below.

When creating a Community Services cluster consisting of Sametime servers not controlled by the EMS, you are instructed to enter the IP address of the Community Services multiplexer machine in the “CommunityTrustedIPs” field of the CommunityConnector document in the Configuration database on the Sametime server. This configuration ensures that the Sametime server trusts the Community Services multiplexer when the Community Services multiplexer establishes a connection to the Sametime server.

A Sametime server that is added to the EMS gets its configuration parameters from the DB2 database used by the EMS, not the Configuration database on the Sametime server. Instead of adding the IP address or DNS name of the Community

---

Chapter 18. Creating a Community Services cluster with the Enterprise Meeting Server 585
Services multiplexer machine in the “CommunityTrustedIPs” field of the CommunityConnector document in the Configuration database, you must insert the DNS name of the Community Services multiplexer machine into the stconfig.communitymux table in the DB2 database.

To deploy separate Community Services multiplexers in front of a Community Services cluster consisting of Sametime servers controlled by the EMS, do the following:

1. Perform all procedures discussed in the topic Deploying separate Community Services multiplexers (optional) in the “Setting up a Community Services cluster without clustering the Meeting Services” chapter, with the exception discussed in steps 2 through 5 below.

2. Instead of adding the IP address of the Community Services multiplexer machine in a document in the Configuration database, follow the instructions below to insert the DNS name of the Community Services multiplexer machine into the stconfig.communitymux table in the DB2 database:

3. Start the DB2 Command Line Processor. To start the DB2 Command Line Processor from the Windows desktop, choose Start - IBM DB2 - Command Line Processor.

4. At the db2=> command prompt, type the command required to connect to the DB2 database used by the EMS. Use the following format when typing this command.

   connect to <EMS DB2 database name> user <db2 administrator name> using <db2 administrator name password>

   In this example, the EMS db2 database name is "Sametime," the db2 administrator name is "db2admin," and the db2 administrator name password is "sametime." An example of the complete command string is:

   db2 => connect to sametime user db2admin using sametime

   A message indicating the "The SQL command completed successfully" appears when the command completes.

5. At the db2=> command prompt, type the following command to insert the DNS name into the DB2 database table:

   insert into stconfig.communitymux (servername) values ('<Community Services multiplexer DNS name>')

   In this example, the EMS cluster name is "SametimeMeetingServicesCluster" and the Community Services multiplexer DNS name is "csmux.sametime.com." An example of the complete command string is:

   insert into stconfig.communitymux (servername) values ('csmux.sametime.com')

   A message indicating the "The SQL command completed successfully" appears when the command completes.

   Note In the command example above, note that values you enter for clustername (SametimeMeetingServicesCluster) and servername (csmux.sametime.com) are case sensitive. If you are unsure of the exact case-sensitive strings for these values, you can use the following command to retrieve the strings from the stconfig.roomserver table in the DB2 database:

   Select servername from stconfig.roomserver

   You can use the strings returned from this command when inserting the clustername and servername into the stconfig.communitymux table in the DB2 database.

6. At the db2=> command prompt, type the following command to terminate the connection to the DB2 database:

   Connection reset

7. Close the DB2 command prompt window.
**Next step:**
Set up a load balancing mechanism

**Set up a load balancing mechanism**

Setting up a load balancing mechanism is the fourth of six procedures associated with setting up a Community Services cluster using Sametime servers that have been added to the EMS.

The procedure required to set up a load balancing mechanism is identical to the procedure that is described in the "Set up the load-balancing mechanism (rotating DNS or Network Dispatcher)" topic in the "Setting up a Community Services Cluster without clustering the Meeting Services" chapter earlier in this documentation. Use the instructions in that topic to set up the load balancing mechanism.

**Next step:**
Configure the Community Services clustering parameters in the DB2 database

**Configure the Community Services clustering parameters in the DB2 database**

Configuring the Community Services clustering parameters in the DB2 database is the fifth of six procedures associated with setting up a Community Services cluster using Sametime servers that have been added to the EMS.

In this procedure, you insert values into tables in the DB2 database used by the EMS. These values must exist in the DB2 database to enable a Sametime server that is controlled by the EMS to operate as part of a Community Services cluster.

This procedure requires you to enter the following information in DB2 command strings. You must know this information to complete the procedure below.

- **Community Services cluster name** - This name is at your discretion. In this example, we use the name "SametimeCommunityServicesCluster" as the Community Services cluster name in the DB2 command strings.
- **Community Cluster DNS name** - This name is the DNS name associated with the rotating DNS system or the IBM Network Dispatcher that load balances connections to the Community Services cluster. This example assumes the Community Cluster DNS name is "Sametime.cscluster.com."
- **Canonical names of the Sametime servers** - You must enter the Domino names of the Sametime servers that are part of the Community Services cluster in the canonical format in a DB2 command string. An example of the canonical server name format is CN=SametimeserverA/O=IBM.

**Note:** The commands below require you to enter value for the servername column in a table within the DB2 database. Note that the servername values you use in these commands must be case-sensitive. If you are unsure of the exact case-sensitive strings for these values, you can use the following command to retrieve the strings from the stconfig.roomserver table in the DB2 database:

```
Select servername from stconfig.roomserver
```

You can use the strings returned from this command when inserting the servername values into the commands discussed below.

To configure the Community Services cluster parameters in the DB2 database:
1. Start the DB2 Command Line Processor on the machine on which DB2 is installed. To start the DB2 Command Line Processor from the Windows desktop, choose Start - IBM DB2 - Command Line Processor.

2. At the db2=> command prompt, type the command required to connect to the DB2 database used by the EMS. Use the following format when typing this command.

   connect to <EMS DB2 database name> user <db2 administrator name>
   using <db2 administrator name password>

   In this example, the <EMS db2 database name> is "Sametime," the <db2 administrator name> is "db2admin," and the <db2 administrator name password> is "sametime." An example of the complete command string is:
   db2 => connect to sametime user db2admin using sametime

   A message indicating the "The SQL command completed successfully" appears when the command completes.

3. At the db2=> command prompt, type the command required to create a name for the Community Services cluster and specify the DNS name of the Community Services load balancing mechanism. Use the following format when typing this command.

   insert into stconfig.communitygroup (groupName, servername) values ('<Community Services Cluster name>',
   '<Community Cluster DNS name>')

   In this example, the <Community Services Cluster Name> is "SametimeCommunityServicesCluster," and the <Community Cluster DNS name> is "Sametime.cscluster.com." An example of the complete command string is:
   insert into stconfig.communitygroup (groupName, servername) values('SametimeCommunityServicesCluster',
   'Sametime.cscluster.com')

   A message indicating the "The SQL command completed successfully" appears when the command completes.

   **Note** In the example above, the Community Services cluster name (or groupname entry) is at your discretion. It is not mandatory to use SametimeCommunityServicesCluster as the Community Services cluster name. Remember this name. You must know this name when configuring client connectivity in the next procedure. Note also that the servername ("CN=SametimeserverA/O=IBM") value is case-sensitive.

4. At the db2=> command prompt, type the command required to add a Sametime server to the Community Services cluster.

   Use the following format when entering this command:
   insert into stconfig.communitygroupmember (groupName, servername) values ('<Community Services cluster name>',
   '<Canonical name of a Sametime server>')

   In this example, the <Community Services cluster name> is "SametimeCommunityServicesCluster," and the <Canonical name of the Sametime server> is CN=SametimeserverA/O=IBM. An example of the complete command string is:
   insert into stconfig.communitygroupmember (groupName, servername) values('SametimeCommunityServicesCluster',
   'CN=SametimeserverA/O=IBM')

   A message indicating the "The SQL command completed successfully" appears when the command completes.
Note In the command above, note that the groupname ("SametimeCommunityServicesCluster"), and servername ("CN=SametimeserverA/O=IBM") values are case-sensitive.

5. You must repeat the command in step 4 for each Sametime server that you want to operate as part of the Community Services cluster. The command to add another server to the Community Services cluster is identical to the command shown in step 4 with the exception of the "Canonical name of the Sametime server" value. The canonical name must reflect the name of the server you are adding. For example, if you want to add Sametime server B to the Community Services cluster, the command string might look like this:

```
insert into stconfig.communitygroupmember (groupname, servername)
values('SametimeCommunityServicesCluster',
  'CN=SametimeserverB/O=IBM')
```

6. At the db2=> command prompt, type the following command to terminate the connection to the DB2 database:

```
Connection reset
```

7. Close the DB2 command prompt window.

8. After you have added all of the Sametime servers to the Community Services cluster, you must restart the STAdmin, STServer, and STCenter enterprise applications from the WebSphere Administrative Console on the EMS machine.

- From the Windows desktop of the EMS machine:
  a. Start the WebSphere Administrative Console.
  b. In the left-hand panel of the Administrative Console, select Applications -> Enterprise Applications.
  c. Select the check boxes next to the STAdmin, STCenter, and STServer Enterprise Applications.
  d. Click the Stop button.
  e. Click the Start button.
  f. Messages appear indicating the applications have started successfully.

9. Restart the Sametime servers that have been added to the Community Services cluster.

- From the Windows Services dialog box on the Sametime server:
  a. Open the Windows Services dialog box on the Sametime server.
  b. In the Services dialog box, select Services (Local).
  c. Right-click "Sametime server" and select stop. Wait for the Sametime services to stop.
  d. Right-click "Sametime server" and select start.

**Next step:**

Configure client connectivity

**Configure client connectivity**

Configuring client connectivity is the last of six procedures associated with setting up a Community Services cluster using Sametime servers that have been added to the EMS.

The procedure required to configure client connectivity is identical to the procedure that is described in the **Configuring client connectivity for the Community Services cluster** topic in the "Setting up a Community Services Cluster without clustering the Meeting Services" chapter earlier in this documentation. Use the instructions in that topic to configure client connectivity to the Community Services cluster.
Note the following important issues regarding configuring client connectivity to a Community Services cluster that is controlled by the EMS:

- When you add the Community Services cluster name to the home Sametime cluster field in the LDAP directory person entry for each of your users, you must add the Community Services cluster name that was defined when you Configure the Community Services clustering parameters in the DB2 database.

- It is recommended that you configure Community Services client connectivity in such a way as to segregate the Community Services activity to the servers in the Community Services cluster and the Meeting Services activity to the servers in the Meeting Services cluster. This issue is discussed below.

**Segregating Community Services and Meeting Services activity on the clustered Sametime servers**

When you have clustered both the Meeting Services and the Community Services of Sametime servers that have been added to the EMS, it is recommended that the servers in the Community Services cluster be dedicated to supporting only Community Services activity and the servers in the Meeting Services cluster be dedicated to supporting only Meeting Services activity.

For example, assume you have added Sametime servers A, B, C, and D to the EMS, and you have created a Community Services cluster consisting of Sametime servers A and B. You can configure the clusters so that all Community Services activity for the community is handled by Sametime servers A and B, and all Meeting Services activity is handled by Sametime servers C and D.

To ensure that all Community Services activity is handled by the Community Services cluster consisting of Sametime servers A and B:

- Ensure that the cluster name associated with the Community Services cluster consisting of Sametime servers A and B is entered in the "home Sametime server" (or "home Sametime cluster") field for all users in the LDAP directory that defines the Sametime community. For more information on the "home Sametime server" field, see Configuring client connectivity for the Community Services cluster.

- Verify that no users have Sametime server C or D specified as the home Sametime server in the home Sametime server" (or "home Sametime cluster") field of the LDAP directory person entries.

This configuration ensures that all users must log into a server in the Community Services cluster to receive the Community Services functionality. Since none of the users have Sametime server C or D specified as the home Sametime server, users cannot log in to the Community Services on those servers and no Community Services user activity will occur on them. Essentially, this configuration restricts all Community Services user activity to the Community Services cluster (Sametime servers A and B).

To ensure that all Meeting Services activity is handled by Sametime servers C and D:

- Use the EMS Administration Tool to prevent Meeting Services activity from occurring on Sametime Servers A and B. This procedure is discussed in the topic Preventing Meeting Services activity from occurring on a Sametime server earlier in this documentation. This configuration in combination with the home Sametime server configurations discussed above ensures that only Community Services activity occurs on Sametime servers A and B.
• Use the EMS Administration Tool to set specific limits on the amount of Meeting Services activity that can occur on Sametime servers C and D. This procedure is discussed in Enabling a Sametime server to operate as part of a Meeting Services cluster earlier in this documentation.

If you want to increase the size (and meeting handling capabilities) of your Meeting Services cluster, install another Sametime server and add it to the Meeting Services cluster using the procedures described in Adding Sametime servers to the Meeting Services cluster.

The configurations described above ensure that Sametime servers C and D are dedicated to supporting Meeting Services functionality, while Sametime servers A and B are dedicated to supporting the Community Services functionality.

This concludes the procedures required to set up a Community Services cluster after the Meeting Services of the Sametime servers have been added to the EMS to function as a Meeting Services cluster.

This chapter discusses IBM Lotus Enterprise Meeting Server (EMS) security. This discussion of EMS security explains how to use security roles to control user access to the EMS and how to encrypt EMS HTTP traffic with the Secure Sockets Layer (SSL) protocol.

This chapter includes the following topics:
• Securing user access to the Enterprise Meeting Server
• Encrypting EMS HTTP traffic with SSL
  – Setting up SSL for Web browser connections to the Enterprise Meeting Server
  – Setting up SSL to encrypt HTTP traffic between the EMS and IBM Lotus Sametime servers

Securing user access to the Enterprise Meeting Server

Use the WebSphere Advanced Administration Console to assign security roles to the users in the LDAP directory that defines your Sametime community. These security roles determine the access levels and privileges that individual users and groups have when accessing the Enterprise Meeting Server (EMS).

The default security role settings for end users were specified when you deployed the STCenter.ear file, as discussed in the Deploying the STAdmin, STCenter, and STServer Enterprise Archive (EAR) files topic earlier in this documentation. If you followed the instructions in that topic, the current security role settings allow any anonymous (or unauthenticated) user to access all features of the EMS except the EMS Administration Tool. By default, an anonymous user can create and attend meetings and modify or delete meetings.

If you do not want to allow anonymous access to the Meeting Center (STCenter application server), you can use the security roles associated with the STCenter application server to restrict access. When you restrict access, you can require users to authenticate when:
• Accessing the EMS
• Creating a meeting in the EMS
• Attending a meeting in the EMS

You can restrict access for all users, groups of users, or individual users in the LDAP directory.

To understand the EMS security roles and how to use them, see:
• Understanding the Enterprise Meeting Server Security roles
• Sample security configurations
• Assigning security roles to users in the LDAP directory

Understanding the Enterprise Meeting Server security roles

The available security roles for the EMS are listed below. Use the Security Console of the WebSphere Advanced Administration Console to bind these roles to users.
In the Security Console, you can bind these roles to everyone (no authentication), all authenticated users, and individual users or groups of users.

**Note:** For suggested EMS security role configurations, see [Sample security configurations](#).

**Stadmin**

Users with this role can access the EMS Administration Tool to administer the Community Services, Meeting Services, Broadcast Services, and Audio/Video Services of the clustered Sametime servers.

You bound this role to the user specified as the WebSphere\EMS administrator at the time you deployed EAR files that comprise the EMS.

**Stservices**

A user must have this role to perform administrative procedures from the EMS Sametime Administration Tool.

You bound this role to the user specified as the WebSphere\EMS administrator at the time you deployed EAR files that comprise the EMS.

**Stmanager**

Users with this role can create meetings and edit or delete meetings (including meetings created by other users). Users that have this role can also view the Meeting Details documents of password-protected meetings without entering the meeting passwords. However, a user with this role cannot join a password-protected meeting without entering the meeting password.

Stmanager is the highest access level available to EMS users. You bound this role to the user specified as the WebSphere\EMS administrator at the time you deployed EAR files that comprise the EMS.

**Note:** Unlike the other roles, the Stmanager role is associated with a user and not a particular page or resource of the EMS. You can assign individual users or groups to this role. A user must authenticate before the user can be granted the access levels provided by this role. If no individual users or groups are assigned to this role, this role is not in use. If the Stmanager user role is bound to everyone (no authentication), anonymous users do not have the access levels associated with this role.

**Stuser**

The EMS Welcome page (welcome.jsp) is the home page of the EMS. A user normally accesses the Welcome page before performing any procedure in the EMS, including creating or attending meetings. You can use the Stuser role to allow users to access the EMS Welcome page (welcome.jsp) anonymously or to require users to authenticate when accessing the EMS Welcome page.

- **Allowing users to access the EMS Welcome page anonymously** - You were instructed to bind this role to everyone (no authentication) when you deployed the EAR files that comprise the EMS. When you bind the Stuser role to everyone (no authentication), all users can access the Welcome page anonymously (without authenticating).

  When a user accesses the Welcome page anonymously, the user has access to the links on the Welcome page that enable the user to create or attend meetings in the EMS. The settings that you specify for the Stcreate and Stlist roles then determine whether a user must authenticate when creating or attending meetings.
Note: A user with the Stuser role can also access the "Launch Sametime Connect for browsers" and the Download pages anonymously from the links on the EMS Welcome page. Both of these pages are accessed from links available from the EMS Welcome page.

- **Requiring users to authenticate when accessing the EMS Welcome page** - If you bind the Stuser role to all authenticated users or specific users and groups, users must authenticate when accessing the EMS Welcome page. This configuration ensures that all EMS users are authenticated. Requiring users to authenticate when accessing the EMS Welcome page is the simplest way to secure the EMS.

  If users must authenticate to access the EMS Welcome page, you should also ensure that the Stcreate, Stlist, Stattend, Stmanager, and Steditor roles also require users to authenticate.

**Stcreate**

The Stcreate role enables the administrator to control whether the ability to create meetings on the EMS is or is not protected by authentication. This role determines whether users must authenticate when accessing the New Meeting (or meeting creation) page in the EMS.

- You were instructed to bind this role to everyone (no authentication) when you deployed the EAR files that comprise the EMS. When the Stcreate role is bound to everyone (no authentication), anonymous users can create meetings in the EMS.

- If the Stcreate role is bound to all authenticated users or individual users and groups, a user must authenticate to create a meeting. If you allow anonymous access to the EMS Welcome page (via the Stuser role), but require the user to authenticate when creating a meeting, the user is authenticated when clicking the "Schedule a Meeting" link in the EMS (to access the New Meeting page).

If you require users to authenticate when accessing the EMS Welcome page, you should also require users to authenticate when creating a meeting. If you require authentication to the Welcome page, but leave the Stcreate role bound to everyone (no authentication), a user can enter the URL of the EMS meeting creation page in a Web browser and browse directly to the meeting creation page to create a meeting. In this scenario, the user bypasses the Welcome page and accesses the meeting creation page directly. If the Stcreate role does not require authentication the user can access the meeting creation page and create a meeting without authenticating (even though you have required authentication to access the EMS Welcome page).

**Stlist**

The Stlist role enables the administrator to protect the meeting list on the EMS.

Users who are assigned the Stlist role can view the list of meetings on the EMS. The administrator can provide specific authenticated users with the ability to view the meeting list or allow all anonymous users to have this privilege.

- You were instructed to bind this role to everyone (no authentication) when you deployed the EAR files that comprise the EMS. When the Stlist role is bound to everyone (no authentication), anonymous (or unauthenticated) users can view the meeting list in the EMS.

- If the Stlist role is bound to all authenticated users or individual users and groups, a user must be authenticated to view the meeting list. If you allow anonymous access to the EMS Welcome page (via the Stuser role), but require the user to authenticate when viewing the meeting list, the user is authenticated when clicking the "Attend a Meeting" link in the EMS.
If you require users to authenticate when accessing the EMS Welcome page, you should also require users to authenticate when viewing the meeting list. If you require authentication to the Welcome page, but leave the Stlist role bound to everyone (no authentication), a user can enter the URL of the EMS meeting list page in a Web browser and browse directly to the meeting list page. In this scenario, the user bypasses the Welcome page and accesses the meeting list page directly. If the Stlist role does not require authentication the user can view the meeting list without authenticating (even though you have required authentication to access the EMS Welcome page).

**Stattend**
The Stattend role enables the administrator to provide users with the ability to attend a meeting by selecting a meeting name from the list of meetings in the EMS or to attend a meeting by clicking on a URL that points directly to a specific meeting on the EMS.

**Note:** One user may invite another user to a meeting by sending the user an email or instant message containing a URL that points directly to a specific meeting on the EMS. In this scenario, a user must have the privileges associated with the Stattend role to attend the meeting by clicking on the URL for the meeting.

- You were instructed to bind this role to everyone (no authentication) when you deployed the EAR files that comprise the EMS. When the Stattend role is bound to everyone (no authentication) in the WebSphere Security Console, any anonymous (or unauthenticated) user can attend a meeting by selecting a meeting name from the list of meetings in the EMS or by clicking on a URL that points directly to a specific meeting on the EMS.
- If the Stattend role is bound to all authenticated users or individual users and groups, a user must authenticate when attending a meeting by selecting a meeting name from the meeting list in the EMS or clicking on a URL that points directly to a specific meeting.

If you have required authentication for the Stuser and Stlist roles (or just the Stlist role), you should also require authentication for the Stattend role. Requiring authentication for the Stattend role prevents anonymous users from attending a meeting by using a URL that points directly to a specific meeting on the EMS.

**Stbrowse**
The Stbrowse role enables the administrator to control whether the ability to browse the LDAP directory when creating meetings is or is not protected by authentication. Users can browse the directory to add people or groups to the Restrict To list when restricting meeting attendance from the New Meeting page in the EMS.

- You were instructed to bind this role to everyone (no authentication) when you deployed the EAR files that comprise the EMS. When the Stbrowse role is bound to everyone (no authentication), any anonymous (or unauthenticated) user can browse the directory from the EMS.
- If the Stbrowse role is bound to all authenticated users or individual users and groups in the Security Console, a user must be authenticated to browse the directory from the EMS.

**Stauthenticateduser**
This role is used only by a security servlet and must be bound to all authenticated users. Do not change the bindings for this role.
**Everybody**
This role must be bound to Everyone (no authentication). Do not change the binding for this role. This role ensures that all users can access the login page and error pages anonymously.

If a user cannot access the login page anonymously, the user is required to enter security credentials to access the login page. Because the user must enter the security credentials on the login page, but the user cannot access the login page without entering security credentials, the user enters a loop state and is unable to authenticate if this role is not bound to Everyone (no authentication).

For more information on binding these roles to users, see Sample security configurations and Assigning security roles to users in the LDAP directory.

**Sample security configurations**
Some sample security configurations are provided below to illustrate how to use the EMS security roles.

**Sample security configuration 1**
This configuration requires all users to authenticate and allows every authenticated user to perform any procedure in the EMS.
- Stuser bound to everyone (No authentication)
- Stcreate bound to all authenticated users
- Stlist bound to all authenticated users
- Stattend bound to all authenticated users
- Stbrowse bound to all authenticated users
- Stmanager bound to specific users or groups
- Stadmin, Stservices, and Stmanager bound to the EMS\EMS administrator.

This configuration allows any user to access the EMS Welcome page anonymously. All users in the LDAP directory must authenticate to create a meeting, view the meeting list, attend meetings from the meeting list (or from a meeting link), and browse the directory. Only specific users or groups in the directory have the privileges associated with the Stmanager role.

You can slightly alter this configuration and set the Stuser role to "All authenticated users." In this scenario, users authenticate when accessing the EMS Welcome page instead of authenticating at the time they select the "Attend a meeting" or "Schedule a meeting" links in the EMS.

**Note:** Users with the Stuser role can also access the "Launch Sametime Connect for browsers" page and the Download page. Providing anonymous users with the Stuser role enables the anonymous users to access the Sametime Connect clients. However, an anonymous user cannot login to a Sametime Connect client.

Only a single user (the EMS\EMS administrator) can access the EMS Administration Tool to administer the server cluster.

**Sample security configuration 2**
This configuration illustrates how you can use directory groups to control access to the EMS. This configuration enables you to limit specific tasks to particular users.
- Stuser bound to everyone (No authentication)
• Stcreate bound to the directory group "Meeting Creators"
• Stlist bound to the directory group "Meeting Attendees"
• Stattend bound to the directory group "Special Invitees"
• Stbrowse bound to the directory group "Meeting Creators"
• Stmanager bound to the directory group "Meeting Managers"
• Astadmin, Stservices, and Stmanager bound to the directory group "EMS Administrators"

This configuration allows any user to access the EMS Welcome page anonymously. Users are required to authenticate when creating or attending a meeting in the EMS.

In this configuration, a user must be a member of a specific group to perform a specific task. The "Meeting Attendees" group might consist of a large group of users that can only attend meetings. The "Meeting Creators" group might consist of a smaller subset of users from the Meeting Attendees group. (These users can both create and attend meetings and browse the directory when creating meetings).

The "Special Invitees" group might consist of users who do not work for your company but occasionally need to attend meetings. These users must be provided with a meeting link to attend a meeting; they cannot view the meeting list on the EMS to attend meetings. Note that these users must also have entries in the LDAP directory.

The "Meeting Managers" group would be a smaller group of users (most likely administrators, managers, or executives) that have the most privileges in the EMS.

Any user in the "EMS Administrators" group can access the EMS Administration Tool to administer the server cluster.

Sample security configuration 3
This configuration allows anonymous users to create and attend meetings but restricts the Stmanager and administrative privileges to a specific group of users.
• Stuser bound to everyone (No authentication)
• Stcreate bound to everyone (No authentication)
• Stlist bound to everyone (No authentication)
• Stattend bound to everyone (No authentication)
• Stbrowse bound to everyone (No authentication)
• Stmanager bound to the directory group "Meeting Managers" or specific users
• Astadmin, Stservices, and Stmanager bound to the directory group "EMS Administrators" (only users in the "EMS Administrators" group can access the EMS Administration Tool to administer the server).

When you allow anonymous users to attend meetings from the EMS, use the Configuration-Community Services-Anonymous Access settings in the EMS Administration Tool to ensure users can enter a display name when attending meetings. For more information, see Anonymous Access Settings for Community Services

Assigning security roles to users in the LDAP directory
Use the WebSphere Advanced Administration Console to adjust the security role settings for end user access to the EMS Meeting Center.
To adjust security roles for end users in the LDAP directory:

1. Start the WebSphere Administrative Console.
2. Select Applications -> Enterprise Applications -> STCenter.
3. In the Additional Properties list at the bottom of the STCenter page, select "Map Security Roles to Users/Groups."
4. In the Mapping Users to Roles page, you can assign a role to Everyone, All Authenticated Users, or Specific Users and Groups. Each of these options is discussed below:

   **Everyone** - When you assign a role to Everyone, any user can access the resources associated with the role without authenticating. Essentially, you are allowing anonymous access to the resources associated with that role.

   To assign a role to Everyone, just place a check in the check box that is underneath the Everyone column for that role.

   **All authenticated users** - When you assign a role to All authenticated users, any user that can successfully authenticate can access the resources protected by the security role. To successfully authenticate, a user requires a person entry in the LDAP directory that includes a password.

   To assign a role to All authenticated users, just place a check in the check box that is underneath the All authenticated users column for that role.

   **Specific Users and Groups** - If you assign a role to specific users or groups, the users and group members must authenticate to access the resources protected by the security role. To assign a role to specific users and groups:

   a. In the Role column, place a check in the check box that is next to the role. (This check box is to the left of the Role name.)
   
   b. Click either the Lookup Users or Lookup Groups button.
   
   c. Enter a text string in the "Search String" field to search for a specific user name or group name. You can enter an asterisk (*) in the Search String field to display all user name or group entries in the LDAP directory. Click the Search button.
   
   d. To assign a user or group to the role, select the user or group name in the "Available" list and click the >> button to move the user or group into the "Selected" column. Click OK.

5. Restart the STCenter application server for the change to take effect.

   When the STCenter application server is restarted, the individual user or group you selected has the privileges associated with the security role you selected.

For more information on security roles associated with the EMS, see [Understanding the Enterprise Meeting Server security roles and Sample security configurations](#).

For more information about administering the Sametime servers in the Meeting Services cluster, see [Using the EMS Administration Tool to administer a cluster](#).

---

## Encrypting EMS HTTP traffic with SSL

In a EMS deployment, HTTP traffic is transmitted between these entities:

- Web browsers and the IBM HTTP Server
- The IBM HTTP Server and the WebSphere server Web Container
- The EMS application and the Sametime servers
Meeting passwords, meeting materials (such as whiteboard files), and other sensitive meeting data are transmitted over these HTTP connections. To ensure the security of this data, the administrator can encrypt the EMS HTTP traffic with SSL.

The administrator has the option of encrypting only Web browser traffic to the EMS, or encrypting both the Web browser traffic to the EMS and the HTTP traffic between the EMS application and the Sametime servers. Each of these options is discussed below:

- **Encrypting Web browser traffic to the EMS** - The Web browser establishes an HTTP connection to the IBM HTTP server and the IBM HTTP server, in turn, establishes a separate HTTP connection to the WebSphere server Web Container. To ensure the security of data transmitted between the EMS and Web browsers, the administrator can encrypt these connections with SSL. For detailed instructions, see [Encrypting Web browser connections to the EMS with SSL](#).

- **Encrypting HTTP traffic between the EMS and Sametime servers** - The EMS and Sametime servers communicate using HTTP to start meetings, manage meetings, and transmit meeting materials. For complete end-to-end security, the administrator has the option to also encrypt the connections between the EMS and Sametime servers with SSL. For detailed instructions, see [Encrypting HTTP traffic between the EMS and Sametime servers with SSL](#).

### Encrypting Web browser connections to the EMS with SSL

You can use Secure Sockets Layer (SSL) to encrypt connections from Web browsers to the Enterprise Meeting Server (EMS).

To access the EMS user interface, a Web browser makes an HTTP connection to the IBM HTTP server on the EMS computer. The IBM HTTP server, in turn, makes an HTTP connection to the Web Container on the WebSphere server. The Web Container routes the data received over these connections to the components of the EMS application. To encrypt Web browser connections to the EMS with SSL, you must perform three separate tasks. These tasks include:

1. **Configure SSL between the Web browser and the IBM HTTP server**
2. **Configure SSL between the IBM HTTP server plug-in and the WebSphere server Web Container**
3. **Modify the DB2 database**

Step-by-step instructions for each of these tasks are included in this section.

### Configuring SSL between the Web browser and IBM HTTP server

Configuring SSL between the Web browser and the IBM HTTP server is the first of three tasks required to encrypt connections from Web browsers to the Enterprise Meeting Server (EMS) with SSL.

To configure SSL between the Web browser and the IBM HTTP server, perform these two procedures:

1. **Manage the SSL certificates for the IBM HTTP server**
2. **Configure the IBM HTTP server to support SSL**

### Managing the SSL certificates for the IBM HTTP server

Managing the SSL certificates is the first of two procedures required to configure SSL between the Web browser and the IBM HTTP server.
In this procedure, you use the IBM IKeyMan key management program provided with the IBM HTTP server to create the SSL key database. After creating this database, you must ensure that the database contains the following two SSL certificates:

- The signer (or "trusted root") certificate of a Certification Authority (CA).
- A server certificate signed by the trusted CA.

The procedures associated with managing SSL certificates are listed below.

1. **Create a key database for the IBM HTTP Server**
2. **Managing trusted CA signer certificates for the IBM HTTP server**
3. **Obtaining and adding an SSL server certificate for the IBM HTTP server**

**Creating a key database for the IBM HTTP Server:** Creating a key database for the IBM HTTP Server is the first of three procedures associated with managing the SSL certificates that support Web browser SSL connections to the IBM HTTP server (and EMS).

Use the IBM IKeyMan key management application provided with the IBM HTTP server to create the key database. This key database will hold the SSL certificates required to support SSL connections.

**Note:** The IBM IKeyMan application provided with the IBM HTTP server is a different application than the IBM IKeyMan application provided with the WebSphere Application Server. The IBM HTTP Server IKeyMan application supports the CMS key database format while the WebSphere Application Server IKeyMan application supports the JKS key database format. Make sure to use the appropriate IKeyMan program when creating key databases on the IBM HTTP Server and WebSphere Application Server.

To create the key database:

1. From the Windows desktop of the EMS server machine, start the HTTP Server IBM Key Management Utility. Select Start - Programs - IBM HTTP Server - Start Key Management Utility.
2. From the menu bar, select Key Database File - New....
3. In the New window, complete these fields:
   - **Key database type:** - Accept the default of "CMS key database file."
   - **File name:** - Enter the file name for the key database. The file name is at your discretion. This example assumes that you name the key database "HttpServerkey.kdb."
   - **Location:** - Enter the directory in which the "HttpServerkey.kdb" key database will be stored. The Location is at your discretion. This example assumes the key database is stored in the C:\Program Files\WebSphere\AppServer\etc directory.
   - Click OK after completing the fields in the New window.
4. In the Password prompt window, do the following:
   a. Type and confirm the password that will be used to access the HttpServerkey.kdb key database. The password is at your discretion.
   b. Select the "Stash the password to a file?" Check box.
   c. Click OK.

An information window appears indicating the password is encrypted and saved in the location C:\Program Files\WebSphere\AppServer\etc\key.sth.
Next step: Manage the trusted CA signer certificates for the IBM HTTP server.

Managing trusted Certificate Authority (CA) signer certificates for the IBM HTTP server: Managing the trusted CA signer (or "trusted root") certificates is the second of three procedures associated with managing the SSL certificates required to support Web browser SSL connections to the IBM HTTP server (and EMS).

To manage the trusted CA signer certificates, you must decide to do one of the following:

- Use one of the default signer certificates provided with the key database (Httpserverkey.kdb in this example) as your trusted CA signer certificate.
- Request a signer certificate from a CA. If you request a signer certificate from a CA, you must add this signer certificate to your key database.

Each of these possibilities is discussed below.

Using a default signer certificate provided with the key database: When you create a key database using the IBM IKeyMan key management utility, the database automatically includes signer certificates from well-known CAs.

To use one of the default signer certificates as the trusted root certificate, simply view the available certificates and decide which one you want to use. After you have decided which CA certificate you will use as the CA signer certificate, continue to the next procedure, Obtaining and adding an SSL server certificate.

To view the available signer certificates that are provided by default in a key database that is created from the IBM IKeyMan program, follow the procedure below:

1. If necessary, start the IBM IKeyMan program and open the key database.
   a. From the Windows desktop, select Start - Programs - IBM HTTP Server - Start Key Management Utility.
   b. Select Key Database File - Open to open the "Httpserverkey.kdb" database in the C:\Program Files\WebSphere\AppServer\etc directory. You are prompted for the database user name and password when opening the database.
2. In the "Key database content" drop-down list, select "Signer Certificates" to display the list of CA trusted root certificates provided by default.
3. If you choose to use one of the Signer Certificates displays in step 2 as the SSL signer (or "trusted root") certificate, you can continue with the Obtaining and adding an SSL server certificate procedure.

Requesting a signer (or trusted root) certificate from a CA: If you do not want to use one of the default signer (or trusted root) certificates in the key database, you can request a signer certificate from another CA. After you receive the trusted root certificate from the CA, you must add the certificate to the key database.

To request a signer (or trusted root) certificate from a CA, browse to the CA’s web site and follow the instructions provided by the CA to request the certificate. After requesting the signer certificate, the CA will notify you when the certificate is available and explain how to pick up the certificate. Usually, a trusted root certificate is sent on a diskette by registered mail or must be picked up in person.
The procedure below explains how to add a trusted root certificate to the key database. This procedure assumes that the name of the signer certificate you have received from the CA is "Casignercert.cer" and the database to which this file is added is named "Httpserverkey.kdb."

**Note:** The procedure below can also be used to add a self-signed certificate to the key database for testing purposes.

Follow the instructions below to add a signer (or trusted root) certificate to the Httpserverkey.kdb database:

1. If necessary, start the IBM IKeyMan program and open the key database.
   a. From the Windows desktop, select Start - Programs - IBM HTTP Server - Start Key Management Utility.
   b. Select Key Database File - Open and open the "Httpserverkey.kdb" database in the C:\Program Files\WebSphere\AppServer\etc directory.

2. In the "Key database content" drop-down list, select "Signer Certificates."

3. On the right-hand side of the "Key database content" box, click the "Add..." button.

4. In the "Add CA's Certificate from a file" window, complete the following fields:
   - **Data type:** Accept the default of "Base64-encoded ASCII data."
   - **Certificate file name:** Browse to and select the "Casignercert.cer" file (or other signer certificate file obtained from the CA). Note that at this point you must have already saved the certificate file to the local hard drive or a network hard drive accessible from the EMS machine.
   - **Location:** Ensure the location field specifies the directory path to the "Casignercert.cer" file (for example C:\Program Files\WebSphere\AppServer\etc or other local or network directory).

   Click OK.

5. In the "Enter a label" window, type the name to be used to identify the certificate in IKeyMan. (IKeyMan will display this name for the certificate in the Key database content box.) This name is at your discretion but should provide a distinctive label for the certificate, such as "ACME CA Signer Certificate." Click OK.

6. A "The requested action has successfully completed!" message appears at the bottom of IKeyMan and the name entered in step 5 above appears in the Key database content list to indicate this procedure has completed successfully.

**Next step:** Obtaining and adding an SSL server certificate for the IBM HTTP server

Obtaining and adding an SSL server certificate for the IBM HTTP server: Obtaining and adding an SSL server certificate is the last of three procedures associated with managing the SSL certificates required to support Web browser SSL connections to the IBM HTTP server with SSL.

To complete this procedure you must perform the following steps:

1. Create a server certificate request
2. Submit a server certificate request to a CA
3. Add the server certificate to the key database

Each of these steps is described below.
Creating a server certificate request: After you have chosen the CA that will provide the signer (or trusted root) certificate, you must request an SSL server certificate from that CA. For example, if you elect to use the "VeriSign Class 1 Public Primary Certification Authority" certificate as the signer certificate, you must request a separate SSL server certificate from VeriSign.

Use the IKeyMan key management program to create an SSL server certificate request. Follow the procedure below.

1. If necessary, start the IBM IKeyMan program and open the key database.
   a. From the Windows desktop, select Start - Programs - IBM HTTP Server - Start Key Management Utility.
   b. Select Key Database File - Open and open the "Httpserverkey.kdb" database in the C:\Program Files\WebSphere\AppServer\etc directory.
2. In the "Key database content" drop-down list, select "Personal Certificate Requests."
3. On the right-hand side of the "Key database content" box, click the "New..." button.
4. In the "Create New Key and Certificate Request" window, complete the following fields and click OK:
   • **Key Label:** The Key Label is at your discretion. The Key Label identifies the server certificate in IKeyMan lists. You should provide a Key Label that indicates the certificate is a server certificate (for example, "VeriSignServerCert.")
   • **Key Size:** Select "1024."
   • **Common name:** Enter the fully-qualified DNS name of the EMS Server machine that contains the IBM HTTP server (for example, sametime.EMS.ibm.com).
   • **Organization:** Enter the organization with which the server is associated. For example, "IBM."
   • **Country:** Select the country in which your server is located.
   • **Enter the name of a file in which to store the certificate request:** Specify a directory path and file name in which to store the certificate request. In this example, the certificate request will be stored in the file "HTTPcertreq.arm" in the location C:\Program Files\WebSphere\AppServer\etc\HTTPcertreq.arm.

A certificate request is a text file (HTTPcertreq.arm). You submit this file to the CA in the next procedure.

Submitting a server certificate request to a CA: The steps below provide a general summary of the process required to submit a client certificate request to a CA. The procedure to submit a server certificate request to a CA can vary for each CA.

1. To submit a server certificate request, browse to the CA’s web site and follow the instructions provided by the CA to submit the request.
2. Usually, you submit the request by providing the CA with the certificate request file (HTTPcertreq.arm in this example) or by copying the contents of the certificate request file to your Windows clipboard and pasting these contents into a field on the CA’s web site.
3. After you request the server certificate, the CA will notify you when the signed certificate is available and explain how to pick up the certificate. Usually, you pick up a signed CA server certificate by browsing to the CA’s web site and either downloading the certificate as a file or copying the certificate to the Windows clipboard.
4. After you have picked up the certificate from the CA, use the procedure described below to add the server certificate to the key database. This procedure requires that the SSL server certificate exist as a file. If you picked up the server certificate from the CA by copying the certificate to the Windows clipboard, paste the certificate into a text file and save the text file on the local file system.

The procedure below assumes that the name of the server certificate file is "HTTPServerCert.cer" and the database to which this file will be added is named "Httpserverkey.kdb."

**Adding the server certificate to the key database:** After receiving the server certificate from the CA, you must add this certificate to the key database (Httpserverkey.kdb in this example). Follow the instructions below to add the server certificate to the key database:

1. If necessary, start the IBM IKeyMan program and open the key database.
   a. From the Windows desktop, select Start - Programs - IBM HTTP Server -
   Start Key Management Utility.
   b. Select Key Database File - Open and open the "Httpserverkey.kdb" database in the C:\Program Files\WebSphere\AppServer\etc directory.
2. In the "Key database content" drop-down list, select "Personal Certificates."
3. On the right-hand side of the "Key database content” box, click the "Receive..." button.
4. In the "Receive Certificate from a file” window, complete the following fields:
   • **Data type:** Accept the default of "Base64-encoded ASCII data."
   • **Certificate file name:** Browse to and select the "HTTPServerCert.cer" file (or other server certificate file that you have obtained from the CA).
   • **Location:** Ensure the location field specifies the directory path to which the "HTTPServerCert.cer" file was saved after you received the file from the CA (for example C:\Program Files\WebSphere\AppServer\etc).
5. Click OK.

You should now see the server certificate name displayed in the Personal Certificates list in IKeyMan.

**Note:** You specified the server certificate name when creating the server certificate request.

**Next step:** Configure the IBM HTTP server to support SSL

**Configuring the IBM HTTP server to support SSL connections:** Configuring the IBM HTTP server to support SSL is the last of two procedures required to configure SSL between the Web browser and the IBM HTTP server.

Follow these steps to configure the IBM HTTP server to support SSL:

1. **Accessing the IBM HTTP Administration Server**
2. **Set up the security module**
3. **Set up the secure IP host and the additional port for the secure server**
4. **Set up the virtual host structure for the secure server**
5. **Set up the virtual host document root for the secure server**
6. **Set the keyfile and SSL timeout values for the secure server**
7. **Enable SSL and select the mode of client authorization**
**Accessing the IBM HTTP Administration Server:** Accessing the IBM HTTP Administration Server is the first of seven steps required to set up the IBM HTTP server to support SSL connections.

You use the IBM HTTP Administration Server to set up the IBM HTTP server to support SSL connections. Before beginning the set up procedures, ensure that you can access the user interface for the IBM HTTP Administration Server. Follow the steps below:

1. Make sure the IBM HTTP Server and the IBM HTTP Administration Server are running.
   a. Open the Services window in the Windows Control Panel.
   b. Verify that the “IBM HTTP Server” and the “IBM HTTP Administration Server” are started. If these services are not started, start them.

2. Set a user name and password for the IBM HTTP Administration Server. (Skip this step if you have already set a user name and password.)
   a. Open the command prompt on the Windows server that contains the IBM HTTP server.
   b. Change to the root directory of the IBM HTTP Administration Server. For example, enter the following command to change to the default installation directory for the IBM HTTP Administration server: `cd c:\Program Files\IBM HTTP Server`
   c. Use the following command to specify the user name to enter when accessing the IBM HTTP Administration Server: `htpasswd conf\admin.passwd [login name]` For example, to specify a login name of “Sametime Administrator,” the entire command string is: `c:\Program Files\IBM HTTP Server>htpasswd conf\admin.passwd Sametime Administrator (and press Enter)`
   d. When prompted, enter the password to use when accessing the IBM HTTP Administration Server and press Enter.
   e. Re-enter the password and press Enter.

3. Open a Web browser and browse to the IBM HTTP Server Welcome page. To browse to the IBM HTTP Server Welcome page, browse to the fully-qualified DNS name of the server on which you installed WebSphere and the IBM HTTP server.

   Following earlier examples in this documentation, you would enter `sametime.EMS.ibm.com` in the Web browser URL locator to access the IBM HTTP Server Welcome page.

4. At the "Welcome to the IBM HTTP Server" page, select "Configure server" to access the IBM HTTP Administration Server interface.

   You use the IBM HTTP Administration Server interface to perform all subsequent steps required to set up the IBM HTTP server for SSL.

**Next step:** Set up the Security module

**Setting up the Security Module:** Setting up the Security Module is the second of seven steps required to set up the IBM HTTP server for SSL to encrypt Web browser connections. Follow the steps below.

From the IBM HTTP Administration Server interface:

1. In the "IBM Administration Server" navigation frame at the left of the screen, expand Basic Settings - Module Sequence.
2. In the "Module Sequence" navigation frame at the right of the screen, verify that the Scope is <GLOBAL>. If the value to the right of the Scope: button is not <GLOBAL>, click the Scope: button and select <GLOBAL>.

3. In the "Module Sequence" frame below the list of active server modules, select the "Add" button.

4. Select the "Select a module to add:" button.

5. Go to the bottom of the list and click ibm_ssl from the list. The module dynamic link library (DLL) appears to the right.

6. Click the "Apply" button.

7. Click the "Close" button.

8. Click the "Submit" button.

**Note:** Do not close the IBM HTTP Administration Server interface.

**Next step:** Set up the secure IP host and the additional port for the secure server

*Setting up the secure IP host and the additional port for the secure server:* Setting up the secure IP host and the additional port for the secure server is the third of seven steps required to set up the IBM HTTP server for SSL to encrypt Web browser connections. Follow the steps below.

From the IBM HTTP Administration Server interface:

1. In the "IBM Administration Server" navigation frame at the left of the screen, expand Basic Settings - Advanced Properties.

2. In the "Advanced Properties" navigation frame at the right of the screen, verify that the Scope is <GLOBAL>. If the value to the right of the Scope: button is not <GLOBAL>, click the Scope: button and select <GLOBAL>.

3. Click the "Add" button located underneath the "Specify additional ports and IP addresses" window.

4. A small box appears containing these two settings:
   - **IP address (optional):** - Leave this setting blank. If you leave this setting blank, the IBM HTTP server listens for HTTPS connections on all IP addresses assigned to the IBM HTTP server machine.
   - **port:** - Type 443 in the port field. The IBM HTTP server listens for SSL (or HTTPS) connections on this port number. Port 443 is the standard port for SSL connections.

5. Click the Apply button.

6. Click the Close button.

7. Click the Submit button (at the bottom of the "Advanced Properties" navigation frame).

**Note:** Do not close the IBM HTTP Administration Server interface.

**Next step:** Set up the virtual host structure for the secure server

*Setting up the virtual host structure for the secure server:* Setting up the virtual host structure for the secure server is the fourth of seven steps required to set up the IBM HTTP server for SSL to encrypt Web browser connections.

**Note:** A "virtual host" is a WebSphere filtering mechanism that ensures connections to a specific host name and port can be processed by the WebSphere HTTP server plug-in. The virtual host does not represent a physical machine.
To set up the virtual host structure for the secure server, follow the steps below.

From the IBM HTTP Administration Server interface:
1. In "IBM Administration Server" navigation frame at the left of the screen, expand Configuration Structure - Create Scope.
2. Verify the scope is <GLOBAL>. The scope is global if <GLOBAL> is highlighted in the tree structure in the right panel. If the scope is not global, select the <GLOBAL> option so that it is highlighted.
3. In the "Select a valid scope to insert within the scope selected" drop-down list, select "VirtualHost."
4. In the "Virtual host IP address or fully-qualified domain name:" field, type the virtual host IP address or fully qualified domain name. Use the domain name of the machine on which the IBM HTTP server is installed. Following our earlier examples, you would enter "sametime.EMS.ibm.com."
5. In the "Virtual host port (optional)" field, type "443." (Port 443 is the standard SSL port and the port specified for secure connections in the previous procedure.)
6. In the “Server name:" field, re-enter the fully qualified server name. For example, "sametime.EMS.ibm.com."
7. You can leave the "Alternate name(s) for host:,” "Server path:,” and "Maximum size of the HTTP request" fields blank.
8. Click the Submit button.

   **Note:** The newly-added virtual host appears in the right-hand panel after you click the Submit button. Do not close the IBM HTTP Administration Server interface.

**Next step:** Set up the virtual host document root for the secure server.

*Setting up the virtual host document root for the secure server:* Setting up the virtual host document root for the secure server is the fifth of seven steps required to set up the IBM HTTP server for SSL to encrypt Web browser connections. Follow the steps below.

From the IBM HTTP Administration Server interface:
1. In "IBM Administration Server" navigation frame at the left of the screen, expand Basic Settings - Core Settings.
2. Set the scope to the virtual host you specified in the previous procedure. For example:
   a. In the "Core Settings" pane, select the Scope: button.
   b. Select "<VirtualHost sametime.EMS.ibm.com:443>".
3. In the "Server name:" field, type the fully-qualified name DNS name of the server. In this example, the name is sametime.EMS.ibm.com.
4. In the "Document root directory name:" field, type the document root directory name. The entry is <IBM HTTP Server installation directory>\htdocs. In this example, the correct entry is c:\Program Files\IBM HTTP Server\htdocs.
5. You can leave the remaining fields in the "Core Settings" pane blank.
6. Click the Submit button.

   **Note:** Do not close the IBM HTTP Administration Server interface.

**Next step:** Set the keyfile and SSL timeout values for the secure server.
Setting the keyfile and SSL timeout values for the secure server: Setting up the keyfile and SSL timeout values for the secure server is the sixth of seven steps required to set up the IBM HTTP server for SSL to encrypt Web browser connections. Follow the steps below.

From the IBM HTTP Administration Server interface:
1. In navigation frame at the left of the screen, expand Security - Server Security.
2. Set the scope to <GLOBAL>. Select the Scope button and select Global.
3. In the "Enable SSL" option, select "No."
   Note Selecting this option disables SSL globally, but you will soon enable SSL for the virtual host created in an earlier procedure.
4. In the "Keyfile filename:" field, type the path and filename to the keyfile database that contains the SSL certificates you obtained earlier. For example:
   Note This example assumes you will select "None" as the mode of client authentication. The IBM HTTP server and EMS can be configured to support client certificate authentication but this configuration is not discussed in this documentation. For information about setting up client certificate authentication for Web browser connections to an IBM HTTP server, see the redbook titled IBM WebSphere V5.0 Security WebSphere Handbook Series available at www.redbooks.ibm.com.
   • None - If you select "None," the server does not request an SSL certificate from a client. Select this option if you do not want to support SSL client certificates in your EMS environment. When you select "None," web browser connections are encrypted using SSL but the individual clients are not authenticated using SSL certificates. Individual clients accessing the EMS will
be authenticated according to the security roles discussed in Understanding the Enterprise Meeting Server security roles.

- **Optional** - If you select ”Optional,” the server requests an SSL certificate from the client. If the client does not provide a certificate, an SSL connection is still established.

If a client provides an SSL certificate, but the certificate is expired, or the certificate is signed by a certificate authority (CA) that is not designated as a trusted CA on the server, the server denies the connection.

Note that SSL client authentication increases network traffic.

- **Required** - If you select ”Required,” the server requests a client certificate from all clients making an HTTPS request. The server validates client certificates by checking for a trusted root CA certificate in the local key database that is signed by the same CA as the client certificate. A trusted CA root certificate is a certificate signed by a certificate authority who is designated as a trusted CA on your server.

The server establishes a secure connection if the client has a valid SSL client certificate. The server denies the request if the client has an expired certificate, or if the certificate is signed by a certificate authority (CA) that is not designated as a trusted CA on the server.

Note that SSL client authentication increases network traffic.

5. In the ”Server certificate to use for this virtual host” field, you must enter the name of the SSL server certificate that you added to the key database used by the IBM HTTP server.

When entering this certificate name, enter the name that you specified as the "Key Label" when you created the server certificate request for the IBM HTTP server SSL server certificate. In this example, a Key Label of "VeriSignServerCert" was used.

For more information, review the topic Obtaining and adding an SSL server certificate discussed in the ”Managing the SSL certificates” procedures earlier in this chapter.

6. You can leave the remaining fields on the ”Host Authorization” panel blank.

7. Click the Submit button.

At this point the IBM HTTP Server is configured to support SSL.

8. Restart the IBM HTTP Server for the changes to take effect.

**Note:** On Windows 2000 servers, you may see the following message after restarting the server: ”Could not start the IBM HTTP service on \... Error 1067. The process terminated unexpectedly. To prevent this problem, open the "IHS httpd.conf" file and comment out this line:

```
ClearModuleList
```

**Next step:** Configuring SSL between the IBM HTTP server plug-in and the WebSphere server Web Container.

**Configuring SSL between the IBM HTTP server plug-in and the WebSphere server Web Container:** Configuring SSL between the IBM HTTP server plug-in and the WebSphere server Web Container is the second of three tasks required to encrypt connections from Web browsers to the Enterprise Meeting Server (EMS).

To configure SSL between the IBM HTTP server plug-in and the WebSphere Web container, perform these procedures:

1. Manage the SSL certificates for the IBM HTTP server plug-in
2. Manage the SSL certificates for the WebSphere server Web container
3. Exchange certificates between the IBM HTTP server plug-in and the WebSphere server Web container
4. Modify the WebSphere server Web Container to support SSL/HTTPS
5. Modify the IBM HTTP server plugin-cfg.xml file to support SSL/HTTPS

Manage the SSL certificates for the IBM HTTP server plug-in: Managing the SSL certificates for the WebSphere server Web Container is the first of five procedures required to configure SSL between the IBM HTTP server plug-in and the WebSphere server Web Container.

In this procedure, you use the IBM IKeyMan key management program provided with the IBM HTTP Server to create a key database. After creating this database, you must ensure that the database contains the following two SSL certificates:
- The signer (or "trusted root") certificate of a Certification Authority (CA).
- A server certificate signed by the trusted CA.

The procedures for managing the SSL certificates for the IBM HTTP server plug-in are very similar to the procedures for managing SSL certificates for the IBM HTTP server described earlier in this chapter.

To manage the SSL certificates for the IBM HTTP server plug-in, you repeat the same procedure that you completed when you managed the SSL certificates for the IBM HTTP server, with the exceptions noted below. You must also perform the additional step of storing the IBM HTTP server plug-in server certificate in an accessible location, as discussed below.

Follow these steps to manage the SSL certificates for the HTTP server plug-in:

1. **Create a key database for the IBM HTTP server plug-in.**
   You must create a new CMS key database specifically for the HTTP server plug-in. When creating the database, name the database "HTTPplugin.kdb."
   To create this key database for the IBM HTTP server plug-in, follow the procedure described in Creating a key database for the IBM HTTP Server.
   When creating the database, be sure to name the database "HTTPplugin.kdb" instead of "HTTPServerkey.kdb."
   This example assumes that you store the HTTPplugin.kdb database at C:\Program Files\WebSphere\AppServer\etc\HTTPplugin.kdb

2. **Manage the trusted CA signer certificates for the IBM HTTP server plug-in.**
   To manage the trusted CA signer certificates for the IBM HTTP server plug-in, follow the procedure described in Managing trusted Certificate Authority (CA) signer certificates for the IBM HTTP server earlier in this chapter.
   When performing this procedure, make sure that you are managing the trusted CA certificates for the "HTTPplugin.kdb" database (instead of the "HTTPServerkey.kdb" that is mentioned in the original procedure.)

3. **Obtain and add an SSL server certificate for the IBM HTTP server plug-in.**
   To obtain and add an SSL server certificate for the IBM HTTP server plug-in, follow the procedure described in Obtaining and adding an SSL server certificate for the IBM HTTP server earlier in this chapter.
   When performing this procedure, name the server certificate "HTTPpluginServerCert.cer" and store this server certificate in the
HTTPplugin.kdb key database. (In the original procedure, you named the server certificate HTTPServerCert.cer and stored it in the HTTPServerkey.kdb database.)

4. **Store the HTTP server plug-in server certificate in an accessible location.**

In a subsequent procedure, you must import the IBM HTTP server plug-in server certificate into a key database that is used by the WebSphere server Web Container.

Create a directory on the EMS computer and store the IBM HTTP plug-in server certificate file (HTTPpluginServerCert.cer) in this directory.

This example assumes that you store the HTTPServerCert.cer file in a directory named C:\SSL_Certificates in the original WebSphere/EMS server.

Next step: Manage the SSL certificates for the WebSphere server Web Container.

**Manage the SSL certificates for the WebSphere server Web Container:** Managing the SSL certificates for the WebSphere server Web Container is the second of five procedures required to configure SSL between the IBM HTTP server plug-in and the WebSphere server Web Container.

In this procedure, you use the IBM IKeyMan key management program provided with the WebSphere Application Server to create a key database in the JKS (Java Key Store) file format. After creating this database, you must ensure that the database contains the following two SSL certificates:

- The signer (or “trusted root”) certificate of a Certification Authority (CA).
- A server certificate signed by the trusted CA.

The procedures associated with managing SSL certificates for the WebSphere server Web Container are listed below.

1. **Create a key database for the WebSphere server Web Container**

2. **Managing the trusted CA signer certificates for the WebSphere server Web Container**

3. **Obtaining and adding an SSL server certificate for the WebSphere server Web Container**

**Create a key database for the WebSphere server Web Container:** Creating a key database for the WebSphere server Web Container is the first of three procedures associated with managing the SSL certificates for the WebSphere server Web Container.

Use the IBM IKeyMan key management program provided with the WebSphere Application Server to create a key database in the JKS file format. This key database will hold the SSL certificates required to support SSL connections from the IBM HTTP server plug-in to the WebSphere server Web Container.

To create the key database:

1. Open a command prompt on the WebSphere/EMS server.
2. Use the ikeyman.exe command to start the IKeyMan utility provided for the WebSphere Application Server, as shown below:
   ```
c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe
   ```
3. From the menu bar, select Key Database File - New.
4. In the New window, specify these values:
   - **Key database type:** - Accept the default of "JKS."
• **File name:** - Enter the file name for the key database. The file name is at your discretion. This example assumes that you name the key database "WASWebContainer.jks."

• **Location:** - Enter the directory in which the "WASWebContainer.jks" key database will be stored. The Location is at your discretion. This example assumes the key database is stored in the C:\Program Files\WebSphere\AppServer\etc directory.

5. In the Password prompt window, type and confirm the password that will be used to access the WASWebContainer.jks key database. The password is at your discretion. Click OK.

The key database appears and a message at the bottom of the window indicates the database was created successfully.

**Next step:** Managing the trusted CA signers certificates for the WebSphere server Web Container

*Managing the trusted CA signers certificates for the WebSphere server Web Container:* Managing the trusted CA signer (or "trusted root") certificates is the second of three procedures required to configure SSL between the IBM HTTP server and the WebSphere server Web Container.

To manage the trusted CA signer certificates, you must decide to do one of the following:

• Use one of the default signer certificates provided with the key database (WASWebContainer.jks in this example) as your trusted CA signer certificate.

• Request a signer certificate from a CA. If you request a signer certificate from a CA, you must add this signer certificate to your key database.

Each of these possibilities is discussed below.

*Using a default signer certificate provided with the key database:* When you create a key database using the IBM IKeyMan key management utility, the database automatically includes signer certificates from well-known CAs.

To use one of the default signer certificates as the trusted root certificate, simply view the available certificates and decide which one you want to use. After you have decided which CA certificate you will use as the CA signer certificate, continue to the next procedure, Obtaining and adding an SSL server certificate for the WebSphere server Web Container.

To view the available signer certificates that are provided by default in a key database that is created from the IBM IKeyMan program, follow the procedure below:

1. If necessary, enter the following command from a command prompt on the WebSphere/EMS server to start the IKeyMan utility provided with the WebSphere server: c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe

2. From the menu bar, select Key Database File - Open to open the WASWebContainer.jks file in the C:\Program Files\WebSphere\AppServer\etc directory.

3. In the "Key database content" drop-down list, select "Signer Certificates" to display the list of CA trusted root certificates provided by default.
4. If you choose to use one of the Signer Certificates that displays in step 3 as the SSL signer (or "trusted root") certificate, you can continue with the Obtaining and adding an SSL server certificate procedure.

Requesting a signer (or trusted root) certificate from a CA: If you do not want to use one of the default signer (or trusted root) certificates in the key database, you can request a signer certificate from another CA. After you receive the trusted root certificate from the CA, you must add the certificate to the key database.

To request a signer (or trusted root) certificate from a CA, browse to the CA’s web site and follow the instructions provided by the CA to request the certificate. After requesting the signer certificate, the CA will notify you when the certificate is available and explain how to pick up the certificate. Usually, a trusted root certificate is sent on a diskette by registered mail or must be picked up in person.

The procedure below explains how to add a trusted root certificate to the key database. This procedure assumes that the name of the signer certificate you have received from the CA is "WASWCsignercert.cer" and the database to which this file is added is named "WASWebContainer.jks."

Note: The procedure below can also be used to add a self-signed certificate to the key database for testing purposes.

Follow the instructions below to add a signer (or trusted root) certificate to the WASWebContainer.jks database:

1. Enter the following command from a command prompt on the WebSphere/EMS server to start the IKeyMan utility provided with the WebSphere server: c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe
2. From the menu bar, select Key Database File - Open to open the WASWebContainer.jks file in the C:\Program Files\WebSphere\AppServer\etc directory.
3. In the "Key database content” drop-down list, select "Signer Certificates.”
4. On the right-hand side of the "Key database content” box, click the "Add..." button.
5. In the "Add CA’s Certificate from a file” window, complete the following fields:
   - **Data type**: Accept the default of "Base64-encoded ASCII data."
   - **Certificate file name**: Browse to and select the "WASWCsignercert.cer" file (or other signer certificate file obtained from the CA). Note that at this point you must have already saved the certificate file to the local hard drive or a network hard drive accessible from the EMS machine.
   - **Location**: Ensure the location field specifies the directory path to the "WASWCsignercert.cer" file (for example C:\Program Files\WebSphere\AppServer\etc or other local or network directory).
   Click OK.
6. In the "Enter a label” window, type the name to be used to identify the certificate in IKeyMan. (IKeyMan will display this name for the certificate in the Key database content box.) This name is at your discretion but should provide a distinctive label for the certificate, such as "ACME CA Signer Certificate.” Click OK.
7. A "The requested action has successfully completed!” message appears at the bottom of IKeyMan and the name entered in step 5 above appears in the Key database content list to indicate this procedure has completed successfully.
Next step: Obtaining and adding an SSL server certificate for the WebSphere server Web Container.

Obtaining and adding an SSL server certificate for the WebSphere server Web Container:
Obtaining and adding an SSL server certificate is the last of three procedures associated with managing the SSL certificates required to support Web browser SSL connections to the IBM HTTP server (and EMS).

To complete this procedure you must perform the following steps:
1. Create a server certificate request
2. Submit a server certificate request to a CA
3. Add the server certificate request to the key database
4. Store the WebSphere server Web Container server certificate in an accessible location

Each of these steps is described below.

Creating a server certificate request: After you have chosen the CA that will provide the signer (or trusted root) certificate, you must request an SSL server certificate from that CA. For example, if you elect to use the "VeriSign Class 1 Public Primary Certification Authority" certificate as the signer certificate, you must request a separate SSL server certificate from VeriSign.

Use the IKeyMan key management program to create an SSL server certificate request. Follow the procedure below:
1. Enter the following command from a command prompt on the WebSphere/EMS server to start the IKeyMan utility provided with the WebSphere server: c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe
2. From the menu bar, select Key Database File - Open to open the WASWebContainer.jks file in the C:\Program Files\WebSphere\AppServer\etc directory.
3. In the "Key database content" drop-down list, select "Personal Certificate Requests."
4. On the right-hand side of the "Key database content" box, click the "New..." button.
5. In the "Create New Key and Certificate Request" window, complete the following fields and click OK:
   • Key Label: The Key Label is at your discretion. The Key Label identifies the server certificate in IKeyMan lists. You should provide a Key Label that indicates the certificate is a server certificate (for example, "VeriSignServerCert.").
   • Key Size: Select "1024."
   • Common name: Enter the fully-qualified DNS name of the EMS Server machine that contains the IBM HTTP server (for example, sametime.EMS.ibm.com).
   • Organization: Enter the organization with which the server is associated. For example, "IBM."
   • Country: Select the country in which your server is located.
   • Enter the name of a file in which to store the certificate request: Specify a directory path and file name in which to store the certificate request. In this
example, the certificate request will be stored in the file "WWCcertreq.arm" in the location C:\WebSphere\AppServer\etc\certreq.arm.

A certificate request is a text file (WWCcertreq.arm). You submit this file to the CA in the next procedure.

**Submitting a server certificate request to a CA:** The steps below provide a general summary of the process required to submit a client certificate request to a CA. The procedure to submit a server certificate request to a CA can vary for each CA.

1. To submit a server certificate request, browse to the CA’s web site and follow the instructions provided by the CA to submit the request.
2. Usually, you submit the request by providing the CA with the certificate request file (WWCcertreq.arm in this example) or by copying the contents of the certificate request file to your Windows clipboard and pasting these contents into a field on the CA’s web site.
3. After you request the server certificate, the CA will notify you when the signed certificate is available and explain how to pick up the certificate. Usually, you pick up a signed CA server certificate by browsing to the CA’s web site and either downloading the certificate as a file or copying the certificate to the Windows clipboard.
4. After you have picked up the certificate from the CA, use the procedure described below to add the server certificate to the key database. This procedure requires that the SSL server certificate exist as a file. If you picked up the server certificate from the CA by copying the certificate to the Windows clipboard, paste the certificate into a text file and save the text file on the local file system.

The procedure below assumes that the name of the server certificate file is "WWCServerCert.cer" and the database to which this file will be added is named "WASWebContainer.jks."

**Adding the server certificate to the key database:** After receiving the server certificate from the CA, you must add this certificate to the key database (WASWebContainer.jks in this example). Follow the instructions below to add the server certificate to the key database:

1. Enter the following command from a command prompt on the WebSphere/EMS server to start the IKeyMan utility provided with the WebSphere server: c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe
2. From the menu bar, select Key Database File - Open to open the WASWebContainer.jks file in the C:\Program Files\WebSphere\AppServer\etc directory.
3. In the "Key database content" drop-down list, select "Personal Certificates."
4. On the right-hand side of the "Key database content" box, click the "Receive..." button.
5. In the "Receive Certificate from a file" window, complete the following fields:
   - **Data type:** Accept the default of "Base64-encoded ASCII data."
   - **Certificate file name:** Browse to and select the "WWCServerCert.cer" file (or other server certificate file that you have obtained from the CA).
   - **Location:** Ensure the location field specifies the directory path to which the "WWCServerCert.cer" file was saved after you received the file from the CA (for example C:\Program Files\WebSphere\AppServer\etc).
6. Click OK.
You should now see the server certificate name displayed in the Personal Certificates list in IKeyMan.

**Note:** You specified the server certificate name when creating the server certificate request.

*Store the WebSphere server Web Container server certificate in an accessible location:* In a subsequent procedure, you must import the server certificate of the WebSphere server Web Container into the key database that is used by the IBM HTTP server plug-in. Store the WebSphere Server Web Container certificate file ("WWCServerCert.cer" in this example) in a directory that is accessible from the IBM HTTP server. You will need to browse to and select the certificate later in this process.

In this example, the IBM HTTP Server and the WebSphere Application Server reside on the same computer. This example assumes that you store the WWCServerCert.cer file in a directory named C:\SSL_Certificates on the EMS computer.

**Next step:** Exchange server certificates between the IBM HTTP server plug-in and the WebSphere server Web Container.

*Exchange server certificates between the IBM HTTP server plug-in and the WebSphere server Web Container:* Exchanging server certificates between the IBM HTTP server plug-in and the WebSphere server Web Container is the third of five procedures required to configure SSL between the IBM HTTP server plug-in and the WebSphere server Web Container.

In this procedure, do the following:

- Import the WebSphere Web Container server certificate into the IBM HTTP server plug-in key database as a Signer certificate.
  
  Following the earlier examples, you would import the "WWCServerCert.cer" certificate into the HTTPplugin.kdb database as a Signer certificate.

- Import the IBM HTTP server plug-in server certificate into the WebSphere Web Container key database as a Signer certificate.
  
  Following the earlier examples, you would import the "HTTPpluginServerCert.cer" into the WASWebContainer.jks database as a Signer certificate.

These procedures ensure that each server trusts the server certificate of the other server during an SSL handshake. Follow the instructions below.

*Importing the Web Container certificate into the IBM HTTP server plug-in key database:* The instructions below assume the IBM HTTP server plug-in key database is named HTTPplugin.kdb and the WebSphere server Web Container certificate is named WWCServerCert.cer file.

1. Start the IBM IKeyMan application provided with the IBM HTTP server and open the key database.
   a. From the Windows desktop, select Start - Programs - IBM HTTP Server - Start Key Management Utility.
   b. Select Key Database File - Open and open the "HTTPplugin.kdb” database.
2. From the Key database content drop-down list, select "Signer Certificates."
3. Click the Add button.
4. In the Add CA’s certificate from a file window, specify the following:
• **Data type:** Base64-encoded ASCII data
• **Certificate file name:** WWCServerCert.cer
• **Location:** C:\SSL_Certificates

Click OK.

5. When prompted for a label name by which the signer certificate will be known, enter "WASWebContainer."

6. Close the key database and quit IKeyMan.

**Importing the HTTP server plug-in certificate into the WebSphere server Web Container key database:** The instructions below assume the WebSphere Web Container key database is named WASWebContainer.jks and the IBM HTTP server plug-in server certificate is named HTTPpluginServerCert.cer.

1. Enter the following command from a command prompt on the WebSphere/EMS server to start the IKeyMan utility provided with the WebSphere server:
c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe

2. From the menu bar, select Key Database File - Open to open the WASWebContainer.jks file in the C:\Program Files\WebSphere\AppServer\etc directory.

3. From the Key database content drop-down list, select "Signer Certificates."

4. Click the Add button.

5. In the Add CA’s certificate from a file window, specify the following:
   • **Data type:** Base64-encoded ASCII data
   • **Certificate file name:** HTTPpluginServerCert.cer
   • **Location:** C:\SSL_Certificates

Click OK.

6. When prompted for a label name by which the signer certificate will be known, enter "HTTPPlugin."

7. Close the key database and quit IKeyMan.

**Next step:** Modify the WebSphere server Web Container to support SSL/HTTPS

**Modify the WebSphere server default SSL repertoire to use the WASWebContainer.jks database:** Modifying the WebSphere server default SSL repertoire to use the WASWebContainer.jks database is the fourth of five procedures required to configure SSL between the IBM HTTP server plug-in and the WebSphere server Web Container.

To modify the default SSL repertoire to use the WASWebContainer.jks database:

1. Start the WebSphere Administrative Console on the EMS computer.

2. Click Security -> SSL.

3. Click the <Servername>DefaultSSLSettings entry to display the settings for the default SSL repertoire.

4. Change the following fields so that they specify the location and password of the WASWebContainer.jks database (instead of the DummyServerKeyFile.jks and DummyServerTrustFile.jks):
   • **Key File Name** - ${USER_INSTALL_ROOT}\etc\WASWebContainer.jks
   • **Key File Password** - Enter the password you specified when creating the database.
   • **Trust File Name** - ${USER_INSTALL_ROOT}\etc\WASWebContainer.jks
• **Trust File Password** - Enter the password you specified when creating the database.

5. Click OK and then click Save in the WebSphere Administrative Console task bar.

**Note on using a new SSL repertoire instead of the default SSL repertoire:** By default, the server1, STAdmin, STCenter, and STServer application servers are configured to use the default SSL repertoire that you have just modified. If you do not want to use the default SSL repertoire, you can create a new SSL repertoire, and specify the WASWebContainer.jks file as the key file and trust file used by the new SSL repertoire. If you create a new SSL repertoire, use the procedure below to assign the new SSL repertoire to the application servers. Note that you must repeat this procedure four times; once each for the server1, STAdmin, STCenter, and STServer application servers.

1. Open the WebSphere Administrative Console.
2. Select Servers -> Application Servers.
3. Click the application server name (either server1, STAdmin, STCenter, or STServer).
4. In the Additional Properties box at the bottom of the application server page, select Web Container.
5. In the Additional Properties box at the bottom of the Web Container page, select HTTP transports.
6. In the Host column, click the asterisk (*) associated with the HTTP transport port that you want to secure. You must make a different selection here for each of the four application servers:
   • For STAdmin, click the asterisk associated with port 9081.
   • For STCenter, click the asterisk associated with port 9083.
   • For STServer, click the asterisk associated with port 9082.
   • For server1, click the asterisk associated with port 9080.
7. In the port page, make the following settings:
   • **SSL Enabled** - Select this check box.
   • **SSL** - From the drop-down list, select the Alias for the new SSL repertoire you have just created (select "Web Container SSL" in this example).
8. From the panel on the left side of the WebSphere Administrative Console, select Environment -> Update Web Server Plugin.
9. Click OK and then click Save in the WebSphere Administrative Console task bar.

**Next step:** Modify the IBM HTTP server plugin-cfg.xml file to support SSL/HTTPS:

Modifying the IBM HTTP server plugin-cfg.xml file to support SSL/HTTPS is the last of five procedures required to configure SSL between the IBM HTTP server plug-in and the WebSphere server Web Container.

In this procedure, you modify the plugin-cfg.xml file by editing the Transport tag entry for port 9080. The Transport entry for port 9080 must specify the following:

• The HTTPS protocol
• The location of the IBM HTTP server plug-in key database
• The location of the password stash file for the HTTP server plug-in key database
To modify the IBM HTTP server plugin-cfg.xml file to support SSL/HTTPS:

1. Use a text editor to open the plugin-cfg.xml file on the EMS computer.
2. Locate the Transport entry in the plugin-cfg.xml file shown below:
   
   ```xml
   <Transport Hostname="sametime.EMS.ibm.com" Port="9080" Protocol="http" />
   ```

3. Change the Transport line in the plugin-cfg.xml file so that it specifies the "https" protocol and the locations of the IBM HTTP server plug-in key database (or keyring) and password stash file. The additions to the code are shown in bold below.

   ```xml
   <Transport Hostname="sametime.EMS.ibm.com" Port="9080" Protocol="https" />
   <Property name="keyring" value="C:\Program Files\HTTPServer\conf\keys\HTTPplugin.kdb" />
   <Property name="stashfile" value="C:\Program Files\HTTPServer\conf\keys\HTTPplugin.sth" />
   ```

4. Save and close the plugin-cfg.xml file.

**Next step:** Modify the DB2 database

**Modifying the DB2 database**

Modifying the DB2 database is the last of three procedures required to encrypt connections from Web browsers to the Enterprise Meeting Server (EMS). This procedure ensures that all URLs for EMS resources begin with the string "HTTPS" instead of "HTTP."

To modify the DB2 database used by the EMS:

1. Start the DB2 Command Line Processor on the EMS machine. To start the DB2 Command Line Processor from the Windows desktop, choose Start - IBM DB2 - Command Line Processor.

2. At the \( db2=\) command prompt, type the command required to connect to the DB2 database used by the EMS. Use the following format when typing this command.

   ```sql
   connect to <EMS DB2 database name> user <db2 administrator name> using <db2 administrator name password>
   ```

   In this example, the EMS db2 database name is "Sametime," the db2 administrator name is "db2admin," and the db2 administrator name password is "sametime." An example of the complete command string is:

   ```sql
   db2 => connect to sametime user db2admin using sametime
   ```

   A message indicating the "The SQL command completed successfully" appears when the command completes.

3. At the \( db2=\) command prompt, type the following command to ensure that EMS URLs begin with HTTPS:

   ```sql
   update stconfig.organization set mtgcntrconnectionurl='https://sametime.EMS.ibm.com/sametime'
   ```

4. At the \( db2=\) command prompt, type the following command to terminate the connection to the DB2 database:

   ```sql
   connection reset
   ```

5. Close the DB2 command prompt window.

This concludes the procedure required to encrypt connections from Web browsers to the EMS.

For the highest level of security, you can also encrypt the data that is transmitted between the EMS and Sametime servers. For more information, see Encrypting HTTP traffic between the EMS and Sametime servers with SSL.
Encrypting HTTP traffic between the EMS and Sametime servers with SSL

The EMS and Sametime servers communicate using HTTP to start meetings, manage meetings, and transmit meeting materials (such as whiteboard files) between the EMS and Sametime servers. The administrator can encrypt the HTTP communication between the EMS and Sametime servers with SSL to ensure that attackers cannot gain access to meeting materials, passwords, or other sensitive data transmitted between the EMS and Sametime servers.

Note: Using SSL to encrypt HTTP traffic between the EMS and Sametime servers requires a different set of procedures than setting up SSL for Web browser access to the EMS. To encrypt Web browser traffic to the EMS, see Encrypting Web browser connections to the EMS with SSL earlier in this chapter.

In a Meeting Services cluster, the EMS can operate as both a client and server in an SSL handshake. A Sametime server in the Meeting Services cluster can also operate as both a client and server in an SSL handshake. For example:

- The EMS can initiate an HTTP (or HTTPS) connection to a Sametime server in the cluster. In this scenario, processes on the EMS call servlets on the Sametime servers. The EMS processes operate as the client to the Sametime server in an SSL handshake. (Specifically, the EMS processes operate as the client to the Domino HTTP server residing on the Domino/Sametime server.)
- The Sametime server can initiate an HTTP (or HTTPS) connection to the EMS. In this scenario, the processes on the Sametime server call servlets on the EMS. This scenario requires the Sametime processes to operate as a client to the IBM HTTP server. The IBM HTTP server connects to the EMS on behalf of the Sametime servers.

Because the EMS can be either the client or server in an SSL handshake, and a clustered Sametime server can also either be the client or server in an SSL handshake, you must perform the configurations that enable the EMS and Sametime servers to operate as both a client and server for SSL connections.

To encrypt all HTTP traffic between the EMS and Sametime servers with SSL, you must perform all five of the following procedures. Detailed instructions for each of these procedures are provided in the following sections.

1. Configure the EMS to operate as the server for an SSL connection
2. Configure the Sametime servers to operate as clients for an SSL connection
3. Configure the Sametime servers to operate as the servers for an SSL connection
4. Configure the EMS to operate as the client for an SSL connection
5. Restart the servers

Configuring the EMS to operate as the server for an SSL connection

Configuring the EMS to operate as the server in an SSL handshake with a clustered Sametime server is the first of five procedures required to use SSL to encrypt HTTP traffic between the EMS and the clustered Sametime servers.

To communicate with the EMS using HTTP, the Sametime servers connect to the IBM HTTP server that is installed on the WebSphere/EMS machine. The IBM HTTP server communicates with the EMS. To ensure that communications from
the Sametime server to the EMS are encrypted with SSL, you must configure the IBM HTTP server to support SSL connections.

These procedures are identical to the procedures required to encrypt Web browser connections to the IBM HTTP server. To configure the EMS to operate as the server for an SSL connection, perform all procedures discussed in the section earlier in this chapter.

If you have already performed these procedures, you can continue with the next step.

Next step: Configuring the Sametime servers to operate as clients for an SSL connection

Configuring the Sametime servers to operate as clients for an SSL connection

Configuring the Sametime servers to operate as clients in an SSL handshake with the IBM HTTP Server is the second of five procedures required to encrypt HTTP traffic between the EMS and the clustered Sametime servers.

To communicate with the EMS, the Sametime server processes must connect to the IBM HTTP server.

To configure the Sametime servers to operate as the client in an SSL handshake with the IBM HTTP server, perform the steps listed below:

1. Ensure the SSL trusted root or SSL server certificate used by the IBM HTTP server is available
2. Use the IBM IKeyMan program to create a key store file on the Sametime server
3. Import the SSL trusted root or SSL server certificates into the key store file on the Sametime server
4. Edit the Sametime.ini file on the Sametime server

Note: You must repeat the four steps above on every Sametime server that is a member of the Meeting Services cluster controlled by the EMS. To achieve a completely secure environment, all Sametime servers in a Meeting Services cluster must be configured to communicate with the EMS using SSL.

Ensuring the SSL trusted root or SSL server certificates used by the IBM HTTP server is available: Ensuring that the appropriate SSL trusted root or SSL server certificate is available is the first of four procedures required to configure a Sametime server to operate as a client in an SSL handshake with the IBM HTTP server.

To enable a Sametime server to operate as a client in an SSL handshake with the IBM HTTP server, you will need a copy of one of the following certificates:

• The trusted root certificate used by the IBM HTTP server to sign its SSL server certificate.
• A copy of the SSL server certificate used by the IBM HTTP server.

Note: You only need a copy of one of the certificates listed above. Either one of these certificates can be used to enable the Sametime server to establish trust with IBM HTTP server during an SSL handshake.
A subsequent procedure requires you to import one of these certificates into a key store file on the Sametime server. If necessary, you can use the IKeyMan program available with the IBM HTTP Server to export either of these certificates to a file.

The procedure below provides an example of how to use the IKeyMan program available with the IBM HTTP Server to export a trusted root (or "signer") certificate from the IKeyMan database on the IBM HTTP Server. This procedure assumes that you need to export the "VeriSign Class 1 Public Primary Certification Authority" from the IKeyMan database used by the IBM HTTP Server.

From the Windows desktop of the IBM HTTP Server:
1. Select Start-Programs-IBM HTTP Server-Start Key Management Utility.
2. Choose Key Database File - Open.
3. Browse to the key database file that holds the certificates used by the IBM HTTP server. (In an earlier example, this database was named "Htppserverkey.kdb.")
4. In the Key database content window, select "Signer Certificates."
5. Select the "Verisign Class 1 Public Primary Certification Authority" certificate (or other signer certificate used as the trusted root certificate).
6. Click the "Extract" button.
7. In the "Extract Certificate to a File" dialog box, complete the following fields:
   - Data type - Select "Base 64-encoded ASCII data."
   - Certificate file names - Accept the default of "cert.arm."
   - Location - Browse to a local or network directory, but preferably a network directory that is accessible from the Sametime server machine.
8. Click OK. The certificate file is exported to the location above.

Once you have obtained a copy of the appropriate trusted root certificate, or server certificate, you can continue with the next step.

Next step: Use the IBM IKeyMan program to create a key store file on the Sametime server.

Using the IBM IKeyMan program to create a key store file on the Sametime server: Creating the IBM IKeyMan key store file is the second of four procedures required to configure a Sametime server to operate as a client in an SSL handshake with the IBM HTTP server.

In this procedure, you use the IKeyMan program provided on the Sametime 7.0 server to create a key store file named "stkeys.jks and store this file in the Sametime installation directory. In this example, the Sametime installation directory is the default installation directory of C:\Program Files\Lotus\Domino.

To create a key database on the Sametime server:
1. Start the IKeyMan program from a command prompt on the Sametime server. The IKeyMan program resides in the "jvm" sub-directory of the Sametime server installation directory (default C:\Program Files\Lotus\Domino). Use the command "java com.ibm.gsk.ikeyman.Ikeyman" to start the IKeyMan program. For example, the command string to start IkeyMan might look like this: C:\Program Files\Lotus\Domino\jvm\java.com.ibm.gsk.ikeyman.Ikeyman
2. From the menu bar, select Key Database File - New....
3. In the New window, complete these fields:
**Key database type:** - Accept the default of "JKS."

**File name:** - Enter the file name for the key database. The file name is at your discretion. This example assumes that you name the key database "stkeys.jks."

**Location:** - Enter the directory in which the "stkeys.jks" key database will be stored. The Location is at your discretion. This example assumes the key database is stored in the C:\Program Files\Lotus\Domino\jvm directory.

Click OK after completing the fields in the New window.

4. In the Password prompt window, do the following:
   a. Type and confirm the password that will be used to access the stkeys.jks key database. The password is at your discretion.
   b. Check "Set expiration time?" And specify the number of days for which the password will be valid before it must be changed. If no expiration date is required, you can leave the "Set expiration time?" Field blank.

   In a production environment, it is recommended that you set an expiration date for the password for the highest level of security.
   c. Click OK.

5. Close the stkeys.jks key database file.

**Next step:** Import the SSL trusted root certificate or SSL server certificates into the key store file on the Sametime server

**Importing the SSL trusted root certificate or SSL server certificates into the key store file on the Sametime server:** Importing the SSL trusted root certificate or SSL server certificates used by the IBM HTTP server is the third of four procedures required to configure a Sametime server to operate as a client in an SSL handshake with the IBM HTTP server.

In this procedure, you must do one of the following:

- Import the SSL trusted root certificate used by the IBM HTTP Server to sign its SSL server certificate.
- Import a copy of the SSL server certificate used by the IBM HTTP Server.

**Note:** You were instructed to export one of these certificates to a file in the procedure titled Ensure the SSL trusted root or SSL server certificates used by the IBM HTTP server is available earlier in this process. This procedure assumes you have exported the SSL trusted root or SSL server certificate to a file as discussed in that procedure.

To import an SSL certificate to the IBM IKeyMan key store file (stkeys.jks):

1. Start the IKeyMan program from a command prompt on the Sametime server. The IKeyMan program resides in the "jvm" sub-directory of the Sametime server installation directory (default C:\Program Files\Lotus\Domino). Use the command "java com.ibm.gsk.ikeyman.Ikeyman" to start the IKeyMan program. For example, the command string to start IkeyMan might look like this: C:\Program Files\Lotus\Domino\jvm>java.com.ibm.gsk.ikeyman.Ikeyman

2. Choose Key Database File - Open.

   Browse to and select the "stkeys.jks" key database (or other database you have created to manage the SSL certificates on the WebSphere server).

3. Enter the password required to access the Stkeys.jks file.

4. In the Key database content area, select "Signer certificates."

5. Click the "Add" button.
6. In the "Add Cas certificate from a File" dialog box:
   • Verify that "Base64-encoded ASCII data" is selected as the Data type.
   • Browse to and select the SSL certificate you want to import.
   
   Click OK.

7. In the "Enter a Label" dialog box, provide a label for the certificate. This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program. Click OK.

   The certificate label will display in the Signer Certificates list.
   After you have imported the trusted root certificate, or individual server certificates for all Sametime servers in the Meeting Services cluster, import the certificate to encrypt HTTP communication between the EMS and EMS Administration Tool application as discussed below.

Next step: Edit the Sametime.ini files on the Sametime servers

Editing the Sametime.ini files on the Sametime servers: Editing the Sametime.ini files on the Sametime servers is the last of four procedures required to configure a Sametime server to operate as a client in an SSL handshake with the IBM HTTP server.

The Sametime.ini file on the Sametime server must contain the parameters that enable the Sametime servers to connect to the EMS machine using SSL. You must use a text editor to edit the Sametime.ini file.

Follow these instructions to edit the Sametime.ini file in the Sametime installation directory on the Sametime/Domino server.

1. Open a text editor on the Sametime server.

2. Open the Sametime.ini file located in the Sametime server installation directory (the default directory is C:\program files\lotus\domino).

3. Locate the "ConfigurationPort=" setting. Make sure that the "ConfigurationPort=" setting, specifies the port on which the IBM HTTP server listens for SSL connections (default port 443). You may need to alter the ConfigurationPort setting to specify the IBM HTTP server SSL port. For example:

   ConfigurationPort=443

4. The following settings must exist in the Sametime.ini file. If necessary, manually add the following settings to the [Config] section of the Sametime.ini file. (At the bottom of the Config section, manually type these settings into the file):

   [Config] ConfigurationSSLEnabled= javax.net.ssl.keyStore=
   javax.net.ssl.trustStore= javax.net.ssl.keyStorePassword=
   javax.net.ssl.trustStorePassword=

   Use the instructions below to populate each of the fields in the Sametime.ini file on the EMS machine:

   • ConfigurationSSLEnabled - This setting should be set to true. An example value is:

     ConfigurationSSLEnabled=true.

   • javax.net.ssl.keyStore - This setting must specify the complete file path, including the filename, of the IKeyMan database you have created on the Sametime server. For example:

     javax.net.ssl.keyStore=C:\program files\lotus\domino\stkeys.jks
5. Save the Sametime.ini file.

**Next step:** Configuring the Sametime server to operate as a server for an SSL connection

**Configuring the Sametime server to operate as a server for an SSL connection**

Configuring the Sametime servers to operate as a server in an SSL handshake with the EMS on the WebSphere Application Server is the third of five procedures required to encrypt HTTP traffic between the EMS and the clustered Sametime servers.

To communicate with the Sametime server, the EMS processes initiate connections to the Domino HTTP server residing on the Sametime server machine.

To configure the Sametime server to operate as a server for an SSL handshake with the EMS processes, you must set up the Domino HTTP server on which Sametime is installed to support SSL. Setting up the Domino HTTP server to support SSL is the only procedure required to configure a Sametime server to operate as a server in an SSL handshake with the EMS processes on the WebSphere Application Server.

The procedure for setting up a Domino HTTP server to support SSL is described in the Domino server administration documentation available from the documentation library at www-10.lotus.com/ldd. This documentation is also provided in the C:\program files\lotus\domino\Data\Help directory on the Sametime/Domino server.

A summary of the procedure required to configure a Domino HTTP server to support SSL is provided below.

**IMPORTANT:** Before performing these procedures on each Sametime/Domino server, review the topic titled **important tips about certificate management** below.

1. Create a Server Certificate Administration database using the csrv50.ntf template.
2. Create a key ring in the Certificate Administration database.
3. Ensure that a trusted root certificate is available in the key ring file.
4. Create a server certificate request.
5. Merge the signed server certificate into the server key ring file.
6. Configure the Server document to enable SSL for the Domino HTTP server.
7. Repeat this procedure on every Sametime/Domino server that is part of the Meeting Services cluster.

**Next step:** After you have configured each Sametime/Domino server in the Meeting Services cluster to support SSL, configure the EMS to operate as the client for an SSL connection.

**Important tips about certificate management:** When you complete the procedure above to set up SSL on the Sametime/Domino servers in the Meeting Services cluster, each Sametime/Domino server will store two certificates required to support SSL connections. These certificates include:
- An SSL trusted root certificate signed by a specific Certificate Authority (CA), such as VeriSign or the Domino Certificate Authority.
- An SSL server certificate signed by the same CA as the trusted root certificate.

In the next procedure ("Configuring the EMS to operate as the client for an SSL connection"), you must perform one of the following two tasks:
- Import the SSL trusted root certificate used to sign the SSL server certificates for each Sametime/Domino server into a key database on the EMS machine.
- Import the SSL server certificates used by each Sametime/Domino server into a key database on the EMS machine.

**Note:** The EMS must have access to one of these certificates to establish trust with the Sametime/Domino server during the SSL handshake.

To accomplish this task, you must have either a copy of the trusted root certificate used to sign each Domino server SSL server certificate or a copy of each Domino SSL server certificate (If you have four Sametime/Domino servers in your cluster, you must have four SSL server certificates - one for each server).

IBM Lotus software recommends that you do one of the following regarding SSL certificate management:
- Make sure that the same trusted root certificate (or signer certificate) is used on each Domino/Sametime server in the cluster. For example, if you have clustered four Domino/Sametime servers (Sametime servers 1, 2, 3, and 4), and the "VeriSign Class 1 Public Primary Certification Authority" certificate is used as the signer certificate on Sametime server 1, you should also use the "VeriSign Class 1 Public Primary Certification Authority" certificate as the trusted root certificate on Sametime servers 2, 3, and 4.

When choosing the trusted root (or "signer") certificate, make sure that it is a trusted root certificate that can be exported from a Web browser. For example, the "VeriSign Class 1 Public Primary Certification Authority" certificate can be used as the trusted root certificate because it is available in both the Server Certificate Administration database on the Sametime/Domino server and in an Internet Explorer Web browser. When it becomes necessary to import the trusted root certificate into the key database in the next procedure, you can export that trusted root certificate from the web browser and import it into the key database.

Using a single trusted root certificate for all Sametime/Domino servers is most efficient because it will be necessary to import only one trusted root certificate into the key database in the next procedure. If the same trusted root certificate is
used to sign the Domino SSL server certificates of Domino/Sametime servers 1, 2, 3, and 4, only that single trusted root certificate must be imported to the key store token in the next procedure.

• If for some reason you cannot export a single trusted root certificate from a Web browser and import it to your key database as described above, you have the option of importing the individual SSL server certificates of each Sametime/Domino server in the Meeting Services cluster into the key database in the next procedure. If you handle certificates in this way, you must save a copy of the SSL server certificate used on each Sametime/Domino server. Save each copy to a floppy disk or network drive that is accessible from the EMS machine before importing the file into the Domino Server Certificate database when you are configuring the Domino HTTP server to support HTTPS.

You will need to browse to these certificates to import them into the key database in the next procedure. Note that it will be necessary to import multiple server certificates (one for each Sametime server in the Meeting Services cluster) into the key database in the following procedure.

**Configuring the EMS to operate as the client for an SSL connection**

Configuring the EMS to operate as a client in an SSL handshake with the clustered Sametime servers is the fourth of five procedures required to encrypt HTTP traffic between the EMS and the clustered Sametime servers.

To configure the EMS to operate as a client in an SSL handshake with the clustered Sametime servers, follow the steps below:

1. **Ensure the SSL trusted root or SSL server certificates used by the Sametime/Domino servers are available.**
2. **Ensure the SSL trusted root certificate used by the IBM HTTP server is available.**
3. **Import the required certificates into the key database.**
4. **Create the JVM Custom Properties for the three application servers.**
5. **Edit the DB2 database.**

**Ensuring the SSL trusted root certificate or SSL server certificates used by the Domino/Sametime servers are available:** Ensuring that the appropriate SSL trusted root or SSL server certificates used by the Sametime/Domino servers are available is the first of five procedures required to configure the EMS to operate as a client in an SSL handshake with a Sametime server.

This procedure simply ensures that you have the appropriate SSL certificate or certificates available. These certificates are required to complete subsequent procedures. To ensure you have the appropriate SSL certificates available, do the following:

1. Review the topic titled **Important tips about certificate management** earlier in this chapter.
2. Decide which of the following ways you will use to manage the SSL certificates that will be required to enable the EMS to operate as client when making an SSL connection to the Sametime servers:

   • You will use a single trusted root certificate as the signer certificate for all SSL server certificates on all Sametime/Domino servers in the Meeting Services cluster. In this case, you must have a copy of this trusted root certificate. You can export a trusted root certificate from a Web browser if necessary. An example of how to export a trusted root certificate from a Web browser is provided below.
• You will use the individual SSL server certificates that were imported into the Server Certificate Administration databases on each of the Sametime/Domino servers in the Meeting Services cluster. In this case, you must have a copy of each of the SSL server certificates used on each Sametime/Domino server. For example, if you have four Sametime/Domino servers in your cluster, you must have four separate server certificate copies available (one from each server). Verify that you have these server certificates available.

Next step: Once you have verified that you have the appropriate trusted root certificate, or appropriate server certificate copies, used by the Sametime/Domino servers, ensure the trusted root CA certificate used by the IBM HTTP server is available.

Example of exporting a trusted root certificate from a Web browser: The instructions below provide an example of how you can export a trusted root certificate from an Internet Explorer web browser:

1. From the Internet Explorer Web browser, choose Tools - Internet Options.
2. Select the Content tab.
3. Select the Certificates button.
4. Select the Trusted Root Certification Authorities tab.
5. Select the appropriate trusted root certificate from the list.
6. Click the Export button.
7. At the Certificate Manager Export Wizard screen, click Next.
8. At the Certificate Export File screen, select "Base64 encoded X.509 (.CER)." Click Next.
9. At the Export File Name screen, provide a name for the file and browse to a location on the local file system in which you want to store the SSL server certificate file. For example, you might enter C:\My Documents\SSLtrustedrootcertificate.cer to store the file in the C:\My Documents directory. Click Next.
10. When the message appears indicating that the export was successful, click OK.

Another way to obtain a trusted root certificate is to request the certificate directly from a CA. The most common way to request a certificate from a CA is by browsing to the CA’s web site. For example, to request a certificate from VeriSign, begin by browsing to the www.verisign.com Web site. Follow the instructions on the Web site to request and receive trusted root certificates.

Ensuring the SSL trusted root certificate used by the IBM HTTP server is available: Ensuring that the SSL trusted root certificate used by the IBM HTTP server is available is the second of five procedures required to configure the EMS to operate as a client in an SSL handshake with a Sametime server.

When you encrypt connections between the EMS and the Sametime servers with SSL, you must also ensure that the STCenter, STAdmin, and STServer application servers can communicate using SSL. These three application servers reside on the EMS computer and communicate with each other using HTTP via the IBM HTTP server. For example, to communicate with the STAdmin application server, the STServer application server connects to the IBM HTTP server.

To enable these three application servers to communicate using SSL, you must ensure that the trusted root CA certificate used to sign the SSL server certificate of
the IBM HTTP server is available on the EMS computer. Later in this process, you will import this certificate into a key database on the EMS computer.

To ensure that the CA trusted root certificate used to sign the SSL server certificate of the IBM HTTP server is available, you must export this certificate from the IKeyMan key database on the IBM HTTP server.

**Note:** For more information about this IKeyMan database and identifying a trusted root CA certificate, see [Managing the SSL certificates](#) earlier in this documentation.

Use the procedure below to export an SSL trusted root (or "Signer") certificate from the IKeyMan database on the IBM HTTP server. This procedure assumes the IKeyMan database name is "Httpserverkey.kdb" and the trusted root certificate used to sign the IBM HTTP Server SSL server certificate is "VeriSign Class 1 Public Primary Certification Authority."

To export a trusted root (or "Signer") certificate from the IKeyMan database on the IBM HTTP server:

1. From the Windows desktop of the IBM HTTP server machine, select Start - Programs - IBM HTTP Server - Start Key Management Utility.
2. Select Key Database File - Open.
   
   Browse to and select the Httpserverkey.kdb database file (or other key database file that you have created to store certificates for the IBM HTTP server).
3. Enter the password required to access the Httpserverkey.kdb database. Click OK.
4. In the "Key database content" window, select "Signer Certificates."
5. Select the trusted root certificate used to sign the IBM HTTP server SSL server certificate. (In an earlier example, the "VeriSign Class 1 Public Primary Certification Authority" was used for this purpose.)
6. Select "Extract...."
7. In the "Extract Certificate to a File" dialog box, make the following settings:
   - **Data type:** - Select "Base64-encoded ASCII data."
   - **Certificate file name:** - Accept the default of "cert.arm" or specify a different name.
   - **Location:** - Type the drive and directory where you want to store the file or use the "Browse..." button to browse to a drive and directory.
   
   Click OK to export the trusted root CA certificate to the file name and directory specified above.

    **Next step:** Import the required certificates into the key database on the WebSphere server.

**Importing certificates to encrypt HTTP communications between the EMS and Sametime servers:** Importing certificates to encrypt HTTP communications between the EMS and Sametime servers is the third of five procedures required to configure the EMS to operate as a client in an SSL handshake with a Sametime server.

To import the certificates required to encrypt HTTP communications between the EMS and Sametime servers, you must do one of the following:
• Import the single SSL trusted root certificate used to sign the SSL server certificates of all Sametime/Domino servers in the Meeting Services cluster into the WASWebContainer.jks database on the WebSphere server.

If you elect to handle certificates in this way, you must import only one trusted root certificate into the WASWebContainer.jks database.

• Import the individual SSL server certificates of each Sametime/Domino server in the Meeting Services cluster into the WASWebContainer.jks database.

If you elect to handle certificates in this way, you must import multiple SSL server certificates into the database. You must import one SSL server certificate from each Sametime/Domino server in the Meeting Services cluster into the WASWebContainer.jks database.

For more information about these certificates, see the topics Important tips about certificate management and Ensuring the SSL trusted root certificate or SSL server certificates used by the Domino/Sametime servers are available earlier in this section.

To import the trusted root or server certificates into the key database on the WebSphere server:

1. Use the ikeyman.exe command to start the IKeyMan utility provided for the WebSphere Application Server, as shown below:
   c:\Program Files\WebSphere\AppServer\java\jre\bin\ikeyman.exe

2. Choose Key Database File - Open.

   Browse to and select the WASWebContainer.jks file. (For example, browse to C:\Program Files\WebSphere\AppServer\etc\WASWebContainer.jks).

3. Enter the password required to access the WASWebContainer.jks file.

4. In the Key database content area, select “Signer certificates.”

5. Click the "Add" button.

6. In the “Add Cas certificate from a File” dialog box:
   • Verify that "Base64-encoded ASCII data" is selected as the Data type.
   • Browse to and select the SSL certificate you want to import.
   Click OK.

7. In the "Enter a Label" dialog box, provide a label for the certificate. This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program. Click OK.

   The certificate label will display in the Signer Certificates list.

   After you have imported the trusted root certificate, or individual server certificates for all Sametime servers in the Meeting Services cluster, import the certificate to encrypt HTTP communication between the EMS and EMS Administration Tool application as discussed below.

Note: In this example, the default SSL repertoire on the WebSphere server specifies the WASWebContainer.jks file as both the key store file and the trust store file so it is only necessary to import the certificates into this single key store database. If the default SSL repertoire specifies one database as the key file and a different database as the trust file, you must import the certificates into both of those databases.

Next step: Create the JVM Custom Properties for the three application servers
Create the JVM Custom Properties for the three application servers: Creating the JVM Custom Properties for the three application servers is the fourth of five procedures required to configure the EMS to operate as a client in an SSL handshake with a Sametime server.

In the procedure, you use the WebSphere Administrative Console to create the JVM Custom Properties for the STAdmin, STCenter, and STServer application servers. You use the JAM Custom Properties to specify the path and password to the database specified as the key file and trust file used by the default SSL repertoire on the WebSphere server. You create new JVM Custom Properties for each of the three application servers.

Note: This example assumes the WASWebContainer.jks file is specified as the key file and the trust file in the default SSL repertoire on the WebSphere server.

To set the JVM Custom Properties for the three application servers, follow the steps below:

1. Start the WebSphere Administrative Console.
2. Select Servers -> Application Servers.
3. Click the STAdmin application server.
4. In the Additional Properties box at the bottom of the STAdmin page, select "Process Definition."
5. In the Additional Properties box at the bottom of the Process Definition page, select "Java Virtual Machine."
6. In the Additional Properties box at the bottom of the Java Virtual Machine page, select "Custom Properties."
7. Click the New button.
8. On the New page, complete these fields:
   - Name - javax.net.ssl.keyStore
   - Value - ${USER_INSTALL_ROOT}/etc/WASWebContainer.jks
9. Click OK.
10. Click the New button.
11. On the New page, complete these fields:
    - Name - javax.net.ssl.keyStorePassword
    - Value - Enter the password for the WASWebContainer.jks database.
12. Click OK.
13. Click the New button.
14. On the New page, complete these fields:
    - Name - javax.net.ssl.trustStore
    - Value - ${USER_INSTALL_ROOT}/etc/WASWebContainer.jks
15. Click OK.
16. On the New page, complete these fields:
    - Name - javax.net.ssl.trustStorePassword
    - Value - Enter the password for the WASWebContainer.jks database.
17. Click OK.
18. Click Save in the Administrative Console task bar.
19. Repeat this procedure for both the STCenter and STServer application servers. (Select the appropriate application server in step 3.)
Next step: Edit the DB2 database

**Editing the DB2 database:** Editing the DB2 database is the last of five procedures required to configure the EMS to operate as a client in an SSL handshake with a Sametime server.

In this procedure, you must edit parameters in two DB2 database tables. These edits are required for each Sametime server to operate correctly in an SSL environment. The two DB2 database tables that you edit are stconfig.roomserver and stconfig.meetingcluster.

**Important:** If the Sametime servers were configured to support SSL before you added them to the EMS, you can skip this procedure and continue with **Restart the servers**. Perform this procedure only if you configured the Sametime server to support SSL after you added the server to the EMS. Note that a Sametime server is configured to support SSL if you have performed the procedures discussed in Configuring the Sametime servers to operate as clients for an SSL connection and the procedures discussed in Configuring the Sametime server to operate as a server for an SSL connection earlier in this documentation.

To edit the parameters in the stconfig.roomserver and stconfig.meetingcluster tables in the DB2 database:

1. Start the DB2 Command Line Processor. To start the DB2 Command Line Processor from the Windows desktop, choose Start - IBM DB2 - Command Line Processor.

2. At the `db2=` > command prompt, type the command required to connect to the DB2 database used by the EMS. Use the following format when typing this command.

   ```sql
   connect to <EMS DB2 database name> user <db2 administrator name> using <db2 administrator name>
   ```

   In this example, the EMS db2 database name is "Sametime," the db2 administrator name is "db2admin," and the db2 administrator name password is "sametime." An example of the complete command string is:

   ```sql
   db2 => connect to sametime user db2admin using sametime
   ```

   A message indicating the “The SQL command completed successfully” appears when the command completes.

3. At the `db2=>` command prompt, type the following command to insert the the required parameters into the stconfig.roomserver table in the DB2 database.

   **Note** Use the command below to insert the required parameters for one Sametime server that has been added to the EMS and configured to support SSL into the DB2 database table. Note that you must repeat this command for each Sametime server. If you have added four Sametime servers to the EMS and configured the four servers to support SSL, you must run this command four times.

   To successfully run this command, you must know the fully qualified DNS name of each Sametime server and the Domino canonical name of each server. In this example, the DNS name is "sametime1.ibm.com" and the Domino canonical name is "CN=Sametime1, OU=East, O=IBM").

   ```sql
   update stconfig.roomserver
   set httpbaseurl='https://sametime1.ibm.com',
   httpssl_en='1',
   httpclear_en='0',
   httpsport='443',
   recmtgmgmtcontrolurl='https://sametime1.ibm.com/servlet/auth/rapfile',
   ```
mtgmgntcontrolurl='https://sametime1.ibm.com/servlet/auth/mmapi' ,
materialsrefreshurl='https://sametime1.ibm.com/servlet/refresh' ,
materialscontrolurl='https://sametime1.ibm.com/servlet/auth/fileupload' ,
commsvcadmincgiurl='https://sametime1.ibm.com/cgi-bin/STAdminAct.exe'
where servername='CN=Sametime1,OU=East,O=IBM'

A message indicating the "The SQL command completed successfully" appears
when the command completes.

4. Repeat the command above to add the required parameters to the DB2
database for each Sametime server that is added to the EMS and configured
to support SSL. For example, to add the required parameters to the DB2 database
for a Sametime server with a DNS name of "sametime2.ibm.com" and a
Domino canonical server name of "CN=Sametime2,OU=West,O=IBM," use this
command:
update stconfig.roomserver
sethttpbaseurl='https://sametime2.ibm.com',
https1_en='1',
httpclear_en='0',
recmmtgmgntcontrolurl='https://sametime2.ibm.com/servlet/auth/rapfile',
mtgmgntcontrolurl='https://sametime2.ibm.com/servlet/auth/mmapi',
materialsrefreshurl='https://sametime2.ibm.com/servlet/refresh',
materialscontrolurl='https://sametime2.ibm.com/servlet/auth/fileupload',
commsvcadmincgiurl='https://sametime2.ibm.com/cgi-bin/STAdminAct.exe'
where servername='CN=Sametime2,OU=West,O=IBM'

5. Repeat the command until the stconfig.roomserver table is updated
appropriately for all of the Sametime servers that have been added to the EMS.
For example, if you have added four Sametime servers, you must repeat the
command four times.

6. At the db2=> command prompt, type the following command to insert the the
required parameters into the stconfig.meetingcluster table in the DB2 database.
update stconfig.meetingcluster

mtgmgntcontrolurl='https://sametime1.ibm.com/servlet/auth/mmapi',
materialsrefreshurl='https://sametime1.ibm.com/servlet/refresh',
materialscontrolurl='https://sametime1.ibm.com/servlet/auth/fileupload'

7. As with the updates to the stconfig.roomserver table above, you must repeat
the command in step 6 one time for each Sametime server that you have added
to the EMS. Be sure to change the server name appropriately with each
repetition of the command.

8. After you have added the parameters for all Sametime servers to the DB2
database, type the following command to terminate the connection to the DB2
database:
Connection reset

9. Close the DB2 command prompt window.

Next step: Restart the servers

Restarting the servers

Restarting the servers is the last of five procedures required to encrypt HTTP
traffic between the EMS and the clustered Sametime servers.
After performing all configurations required to encrypt HTTP traffic between the EMS and clustered Sametime servers, you must restart the application servers that support the EMS. You must also restart each of the Sametime servers. Use the instructions below.

**Restarting the WebSphere enterprise applications:** Restart the STAdmin, STCenter, STServer, and adminconsole enterprise applications.

1. Start the WebSphere Administrative Console.
2. Click Applications -> Enterprise Applications.
3. Select the check boxes to the left of each of these Enterprise Applications.
   - Stamen
   - STCenter
   - STServer
   - adminconsole
4. Select the Stop button.
5. Select the Start button.
6. Close the WebSphere Administrator’s Console.

**Restarting the Sametime servers:** You must restart each of the Sametime/Domino servers that you have configured to support SSL. Because you have performed configurations to both the Domino components and Sametime components of the Sametime servers, you should reboot each Sametime machine and restart Domino on each machine to ensure all changes go into effect.

After rebooting all of the Sametime servers, you have concluded the procedures required to encrypt HTTP traffic between the EMS and the clustered Sametime servers.
Chapter 20. Administering Sametime servers from the Enterprise Meeting Server

If you cluster the Meeting Services, you must install the IBM Lotus Enterprise Meeting Server (EMS) and use the administration tool available from the EMS to administer the clustered servers. To reach this EMS administration tool, enter the following URL in your browser: http://<HTTP Server fully-qualified DNS name>/iwc-admin/client (for example, enter sametime.EMS.ibm.com/iwc-admin/client).

Note: You can use the administration tool available from the EMS to administer any Lotus Sametime server that has been added to the EMS using the procedures discussed in Adding Sametime servers to the EMS. If you have created a Community Services cluster without clustering the Meeting Services, you cannot administer Sametime servers from the EMS. In that scenario, you must use the Sametime Administration Tools available on the individual Sametime servers in the Community Services cluster to administer the servers.

The earlier chapters of this documentation discuss procedures and administration settings associated with administering a Sametime server in a normal Sametime deployment (that is, a deployment that does not include the EMS).

This chapter discusses the differences between using the EMS Administration Tool to administer a Sametime server that is added to the EMS and using the Sametime Administration Tool to administer a Sametime server in a normal Sametime deployment.

• Using the EMS Administration Tool to administer a cluster
• Sending a message from the administrator
• Monitoring Sametime servers added to the EMS
• Using the EMS Administration Tool logging features
• Managing the Community Statistics and Meeting Statistics logging views
• Configuring LDAP directory settings from the Sametime EMS Administration Tool
• Configuring connectivity for Sametime servers added to the EMS
• Configuring the Community Services of Sametime servers added to the EMS
• Configuring the Meeting Services of Sametime servers added to the EMS
• Configuring the Audio/Video Services of Sametime servers added to the EMS
• Working with the Broadcast Services of Sametime servers added to the EMS

Using the EMS Administration Tool to administer Sametime servers

When you deploy the EMS and add Sametime servers to the EMS, you must use the Sametime Administration Tool available from the EMS to administer the Sametime servers you have added to the EMS. To access the EMS Administration Tool, enter the following URL in your browser: http://<HTTP Server fully-qualified DNS name>/iwc-admin/client (for example, enter sametime.EMS.ibm.com/iwc-admin/client).
The **Sametime EMS** Administration tool is similar to the **standard Sametime Administration Tool** that is available from the "Welcome to Sametime" page in a typical Sametime server deployment (that is, a deployment that does not include the EMS). However, some of the links that are available in the standard Sametime Administration Tool are not available in the EMS Administration Tool.

Note the following about the EMS Administration Tool:

- To allow a user to access the EMS Administration Tool, you must use the WebSphere Administrative Console to provide the user with the stadmin, stmanager, and stservices security roles for the STAdmin, STCenter, and STServer enterprise applications.
- The simplest way to provide access to the EMS Administration Tool for more than one user is to create a group named "stadmins" and provide the stadmins group with the stadmin, stmanager, and stservices security roles for the STAdmin, STCenter, and STServer enterprise applications. You can then grant and revoke access to the EMS Administration Tool by adding or removing users from the stadmins group.

For example, to provide the stadmins group with access to the EMS Administration Tool:

1. Start the WebSphere Administrative Console.
2. Select Applications -> Enterprise Applications -> STAdmin.
3. In the Additional Properties list at the bottom of the STCenter page, select "Map Security Roles to Users/Groups."
4. Select the stadmin, stmanager, and stservices roles.
5. Click Lookup groups.
6. In the Search String field, enter stadmins and click Search.
7. Select the stadmins group in the Available column and click the >> button to move the group to the Selected column.
8. Click OK and then click OK again.
9. Repeat steps b through h for both the STServer and STCenter Enterprise Applications.
10. Restart the STAdmin, STServer, and STCenter Enterprise Applications.

- The following features are not available from the EMS Administration Tool:
  - The Miscellaneous monitoring features
    
    **Note:** In the administrator interface on a Sametime server, the "Monitoring - Miscellaneous" page provides a link that launches the Domino Web Administration Tool provided with the Domino server on which the Sametime server is installed. The Domino Web Administration Tool enables an administrator to view memory and disk space statistics for the Sametime server and also provides access to a variety of other administrative features for the Domino server that hosts Sametime. You cannot access the Domino Web Administration Tool of a Sametime server that has been added to the EMS from the EMS Administration Tool.
  - The Domino log features

- The only directory that is available from the EMS Administration Tool is an LDAP directory. A Domino Directory can be used as an LDAP directory if the LDAP task is enabled on the Domino server. For more information, see [Deploying an LDAP directory](#).
- When using the EMS, it is important to note that security is based on WebSphere settings rather than Domino settings. None of the Domino information in the "Working with Sametime security" chapter of this documentation applies to the
EMS environment. For more information about EMS and WebSphere security, see Setting up security for the Enterprise Meeting Server.

Sending a message from the administrator

Use the EMS Administration Tool to simultaneously send a single message to all users logged in to a Sametime community.

The message can be received by all users in the LDAP directory that are currently logged into the Community Services on a Sametime server configured to access that LDAP directory.

To send a message to all users in the Sametime community:
1. To open the EMS Administration Tool, enter the following URL in your browser:
   http://<EMS fully-qualified DNS name>/iwc-admin/client (for example, enter sametime.EMS.ibm.com/iwc-admin/client).
2. Select Message From Administrator.
3. Enter the message in the text box provided.
4. Click Send. You will receive a confirmation that your message was sent.

Monitoring Sametime servers added to the EMS

Monitoring Sametime servers from the EMS Administration Tool is similar to monitoring a Sametime server from the standard Sametime Administration Tool. To access the monitoring charts for the EMS, open the EMS Administration Tool and choose Monitoring. Each monitoring chart displays aggregate statistics for all the servers added to the EMS or individual statistics for each server that is added to the EMS.

The following charts are available:
• General Server Status
• Total Logins
• Meetings and Participants
• Tools in Meetings

Note: The Miscellaneous monitoring charts that are available from the standard Sametime Administration Tool are not available from the EMS Administration Tool. The Miscellaneous monitoring charts are part of the web administrator interface of a Domino server on which a Sametime server is installed. Since the EMS installs and operates on a WebSphere server, these charts are not available from the EMS Administration Tool.

General Server Status

The tables in the General Server Status monitoring chart allow you to see the status of the Sametime servers at a glance. You can see the status of all servers added to the EMS or the individual status of each server.

Use this chart to keep track of the types of meetings occurring on servers controlled by the EMS, the types of connections to servers controlled by the EMS, and the Community Services activity occurring on servers controlled by the EMS.

Be aware of the following information when monitoring the status of a cluster:
• The General Server Status chart displays current information about all servers added to the EMS or about an individual server added to the EMS.

• The data in the Total Community Logins section of the General Server Status chart displays the aggregate Community Services logins for all servers added to the EMS. You cannot see the Total Community Services logins statistics for an individual server that was added to the EMS.

• The following information applies to the Total n-way Chats and Total 2-way Chats charts in the Total Community Logins section of the General Server Status chart:
  – If you have clustered the Community Services, the user does not log into a home Sametime server. The user can login to any server in the Community Services cluster. User logins are distributed equally to the Sametime servers in the Community Services cluster by a rotating DNS or Network Dispatcher load balancing mechanism. In this scenario, the number of n-way chats or 2-way chats started on each server in the Community Services cluster should be relatively equal.

  The Total n-way Chats and Total 2-way Chats charts in the Total Community Logins section of the Genera Server Status Chart do not display statistics for individual servers in the Community Services cluster. These charts display aggregate totals for all servers in the Community Services cluster. To determine the number of chats occurring on an individual server in the Community Services cluster, you must divide the number of chats by the number of servers in the cluster.

  For example, if you have two servers in your Community Services cluster and the Total n-way Chats chart indicates there are 1000 n-way Chats, you can assume that the number of n-way chats supported by each server in the cluster is approximately 500 (1000 chats divided by 2 servers = 500 chats per server).

  If the number of chats is consistently high, you might need to add another Sametime server to the Community Services cluster.

• If you notice any of the following conditions on servers added to the EMS, you might want to adjust the usage limits and denied entries settings for the servers or add another server to the cluster. These conditions are a concern only if you notice them on a regular basis:
  – A high number of meetings on one server
  – A high number of people attending instant meetings or scheduled meetings. You can set separate limits for instant and scheduled meetings.
  – A high number of broadcast unicast connections to the server

  Note: Use the "Edit/Remove a Meeting Server” tab to adjust the usage limits and denied entries settings. To access the “Edit/Remove a Meeting Server” tab, choose Configuration - Meeting Cluster in the EMS Administration Tool. For more information about these settings, see Specifying Usage Limits and Denied Entry settings for the Sametime server.

Logins

Be aware of the following information when monitoring the logins for a cluster:

• The Logins chart displays current information about Community Services logins for all servers added to the EMS or for an individual server added to the EMS.
• You can only view the aggregate Community Services login statistics for all Sametime servers controlled by the EMS. You cannot view the Community Services login statistics for individual Sametime servers in the Community Services cluster.

• The Logins chart includes logins from multiple Community Services clients, including Sametime Connect and the Participant List of the Meeting Room.

Meetings and Participants
The Meetings and Participants chart displays current information about meetings and participants for all servers controlled by the EMS or for an individual server controlled by the EMS.

If you notice a consistently high number of meetings or participants on the servers in the cluster:
• Adjust the Usage Limits and Denied Entries settings for the individual servers in the Meeting Services cluster by using the "Edit/Remove a Meeting Server" tab. To access this tab, choose Configuration - Meeting Cluster in the EMS Administration Tool.
• Add Sametime servers to the Meeting Services cluster

Tools in Meetings
The Tools in Meetings chart in the EMS Administration Tool displays the tools that are available in meetings on all servers controlled by the EMS or on an individual server controlled by the EMS.

If you notice a consistently high number of audio/video meetings, you might want to:
• Adjust the usage limits and denied entries settings for the individual servers in the Meeting Services cluster by using the "Edit/Remove a Meeting Server" tab. To access this tab, choose Configuration - Meeting Cluster in the EMS Administration Tool.
• Add Sametime servers to the Meeting Services cluster

Using the EMS Administration Tool logging features
Viewing the Sametime log from the EMS Administration Tool is similar to viewing the log from the standard Sametime Administration Tool. To access the Sametime log from the EMS, open the EMS Administration Tool and click Logging, and then select a choice in the logging menu. The following options are available from the Logging menu of the EMS Administration Tool:

• Community Logins/Logouts - Login and logout information for each user who logged in to Community Services. Also includes information about failed login attempts.

• Community Statistics - The total and peak number of users, logins, chats, and places in the Community Services. The number of users differs from the number of logins if some users are logged in to Community Services from more than one client (for example, a single user may be logged into the Community Services from Sametime Connect and from the Sametime Meeting Room client).

Important: By default, the Community Statistics are calculated and cached on a daily basis. As EMS usage increases, calculating and caching the Community Statistics can become a time consuming process that may require a significant amount of CPU usage. To ensure that the calculation and caching of these statistics does not affect server performance, you may want to adjust the
scheduling of the Community Statistics caching process. For more information, see Managing the Community Statistics and Meeting Statistics logging views.

- **Community Events** - Information about the status of Community Services applications.
- **Place Login Failures** - Includes failed user attempts to authenticate when entering an online place or meeting and failed user attempts to enter a password-protected place or meeting.
- **Meeting Login Failures** - Includes failed user attempts to authenticate when entering a Sametime meeting and failed user attempts to enter a password-protected meeting.
- **Meeting Connections** - Sametime server connections to clients, such as the Sametime Meeting Room client and the Broadcast client.
- **Server Connections** - Connections and disconnections between Sametime servers.
- **Meeting Statistics** - Information about the total and peak number, duration, and average number of participants in meetings occurring on the Sametime server or throughout the cluster.

**Important:** By default, the Meeting Statistics are calculated and cached on a daily basis. As EMS usage increases, calculating and caching the Meeting Statistics can become a time consuming process that may require a significant amount of CPU usage. To ensure that the calculation and caching of these statistics does not affect server performance, you may want to adjust the scheduling of the Meeting Statistics caching process. For more information, see Managing the Community Statistics and Meeting Statistics logging views.

- **Meeting Events** - Information about the status of Meeting Services applications in instant and scheduled meetings.
- **Capacity Warnings** - The capacity warnings that occur when Meeting Services usage exceeds parameters specified by the administrator in the log settings.
- **Usage Limits** - Information about the usage limits that the administrator defines on the “Edit/Remove a Meeting Server” tab of the EMS Administration Tool. Users are denied entry to meetings when a usage limit is reached.
- **Settings** - Options to determine the content of the Sametime log. You cannot use the settings to determine the format of the log for the EMS Administration Tool; the log is always a database.

**Note:** The **Domino Log** option that is available from the Sametime Administration Tool on a Sametime server is not available in the EMS Administration Tool.

When viewing the log, be aware of the following information:

- Use the drop-down box at the top of the Sametime log to view data for all servers added to the EMS or for a single server added to the EMS. Use the View drop-down box to select a way to view the information in the log.
- Community Services data (such as logins) is the aggregate data for all Sametime servers controlled by the EMS. Community Services data is not available for individual servers that are controlled by the EMS.
- The User ID that is listed in some views of the log is the end user’s LDAP user name.
- The following information applies to the Community Statistics and Meeting Statistics sections of the log:
– The Community Statistics and Meeting Statistics statistics data is maintained in a cache. When you view the Community Statistics and Meeting Statistics logging pages, you are viewing cached information, which will not include the latest statistics.

To view the most up-to-date statistics, you must click the Refresh button. When you click the Refresh button, the statistics are recalculated and the cache repopulated. Note that if the EMS has been in service for an extended period of time (approximately a year), clicking the Refresh button may put an additional strain on the CPU for several minutes and affect the performance of the server. For more information about this issue, see Managing the Community Statistics and Meeting Statistics logging views.

– There is no date field below the View drop-down box.

– There is no selected date range for the following options in the Community Statistics section of the log: Total Users, Total Logins, Peak 2-Way Chats, Total 2-Way Chats, Total n-Way Chats, Peak Places, and Total Places.

– There is no selected date range for the following options in the Meeting Statistics section of the log: Total Meetings, Average Participants/Meeting, Average Meeting Duration, and Total Meeting Hours.

– When you click Refresh, the data in these sections of the log might take a few minutes to refresh. Also, if the EMS has been active for

• In the logging Settings:
  – You cannot choose the format (database or text file) for the log. When you are administering the log settings from the EMS Administration Tool, the Sametime log is always maintained as a database; you cannot choose the text file format for the Sametime log.
  – The General settings apply to all servers controlled by the EMS.
  – You can set Capacity Warnings for each server controlled by the EMS. Choose the name of the server from the drop-down box at the top of the Capacity Warnings page.

Managing the Community Statistics and Meeting Statistics logging views

This section discusses server performance and caching issues related to the Community Statistics and Meeting Statistics logging views of the EMS Administration Tool.

The EMS Administration Tool contains two logging views that display cumulative statistics that reflect the total usage of the EMS. The two logging views are Community Statistics and Meeting Statistics. These logging views, and the statistics they display, are listed below:

Logging - Community Statistics
• Users and Logins by Day
• Users and Logins by Week
• Users and Logins by Month
• Users and Logins by Year
• Chats and Places by Day
• Chats and Places by Week
• Chats and Places by Month
• Chats and Places by Year
Logging - Meeting Statistics

- Statistics by Day
- Statistics by Week
- Statistics by Month
- Statistics by Year

The Community Statistics and Meeting Statistics listed above are maintained in a cache. When viewing these statistics from the Community Statistics and Meeting Statistics logging views in the EMS Administration Tool, the administrator has two options:

- The administrator can click the Refresh button on the Community Statistics or Meeting Statistics page in the EMS Administration Tool. Clicking the Refresh button purges the currently cached statistics, recalculates the statistics, and repopulates the cache with the current statistics.
- The administrator can view the statistics stored in the cache. If the administrator does not click the Refresh button on the Community Statistics or Meeting Statistics page in the EMS Administration Tool, the Community Statistics or Meeting Statistics page displays data that was current at the time the last statistics cache update occurred.

The volume of the Community and Meeting Statistics increases the longer the EMS is in service. As the volume of these statistics increases, the amount of time and CPU usage required to process and cache these statistics also increases. Eventually, the volume of these statistics may become large enough that the processing effort required to calculate and cache them can affect server performance.

Note: Generally, the calculation and caching of the Community and Meeting statistics may begin to significantly affect the CPU after the EMS has been in service for one year. This time interval will vary depending on the amount of Community Services and Meeting Services activity that occurs in your EMS environment and the process capabilities of the CPU.

If the EMS has been in service for an extended period of time, you should refrain from clicking the Refresh button when EMS usage is high. Clicking the Refresh button may put an additional strain on the CPU and adversely affect the meeting scheduling, load balancing, and failover performance of the EMS for several minutes.

If you do not click the Refresh button, the Community Statistics and Meeting Statistics pages display the data that was current when the last cache update occurred. By default, the statistics listed above are automatically calculated and cached every day at 2:00 AM. To further reduce the system resource usage required to calculate the Community and Meeting Statistics, the administrator has the following options for altering the caching behavior. The administrator can:

- Adjust the caching schedule
- Disable the caching feature

Each of these options is discussed below.

Adjusting the Community and Meeting statistics caching schedule

By default, the EMS admin web application is configured to automatically calculate and cache Community Services and Meeting Services statistics on a daily basis at 2:00 AM.
To prevent the automatic calculation and caching of these statistics from consuming too much time or CPU usage, the administrator can adjust the schedule by which the statistics are calculated and cached. The administrator adjusts this schedule by altering parameters in the “StatCacheSchedule.xml” file that is installed with the EMS administration web application.

When adjusting the caching schedule, note that both the Community Statistics and Meeting Statistics are calculated by day, by week, by month, and by year. If you want to ease the statistics processing burden on the CPU of the EMS computer, you can reschedule the statistics processing so that the daily statistics are processed (calculated and cached) once a day, the weekly statistics are processed once a week, the monthly statistics are processed once a month, and the yearly statistics are processed once a year.

If you configure the statistics in this way, the daily statistics are automatically updated and cached on a daily basis. However, the weekly statistics are only updated and cached once each week so the cached data will not reflect the statistics for the current week. The monthly statistics are updated and cached once a month and the yearly statistics once a year.

In this configuration, the administrator will not always see the latest statistics when viewing the cached data displayed on the Logging - Community Services and Logging - Meeting Services pages in the EMS Administration Tool. However, such a configuration can considerably lessen the time and CPU usage required to process the statistics and still provide the administrator with reasonably up-to-date information for each statistical area.

The following example illustrates how you can adjust the caching schedule in the manner discussed above:

1. Use a text editor to open the StatCacheSchedule.xml file on the EMS machine. The default location of the StatCacheSchedule.xml file is:
   C:\Program FilesWebSphere\AppServer\installedApps\<servername>\STAdmin.ear\stadmin.war\WEB-INF\classes\config\StatCacheSchedule.xml

2. The example below shows the default settings for the first four lines of the StatCacheSchedule.xml file.
   
   <taskset>
   <task name="UsersAndLoginsByDay" type="daily" hour="2" minute="0"/>
   <task name="UsersAndLoginsByWeek" type="daily" hour="2" minute="0"/>
   <task name="UsersAndLoginsByMonth" type="daily" hour="2" minute="0"/>
   <task name="UsersAndLoginsByYear" type="daily" hour="2" minute="0"/>

   In these lines, the attributes that determine the schedule at which the statistics are calculated include:
   • Type - Possible values are onetime, hourly, daily, weekly, monthly, or yearly
   • Hour - Possible values are 1 through 24
   • Minute - Possible values are 0 through 60.

   The four lines above illustrate the default configuration. In this configuration note that the Users and Logins statistics are calculated and cached every day at 2:00 AM.

3. The example below shows an alternate configuration in which the daily statistics are processed once a day, the weekly statistics processed once a week, the monthly statistics once a month, and the yearly statistics once a year.

Chapter 20. Administering Sametime servers from the Enterprise Meeting Server 645
<taskset>
  <task name="UsersAndLoginsByDay" type="daily" hour="2" minute="0"/>
  <task name="UsersAndLoginsByWeek" type="weekly" day="Sunday" hour="2"
        minute="0"/>
  <task name="UsersAndLoginsByMonth" type="monthly" date="1" hour="2"
        minute="0"/>
  <task name="UsersAndLoginsByYear" type="yearly" month="1" date="1"
        hour="2" minute="0"/>

Note: The StatCacheSchedule.xml file also contains lines that control the
statistics processing schedule for Chats and Places and Meetings. The
parameters for these statistics are configured in exactly the same way as the
Users and Logins parameters shown above.

4. After you have altered the StatCacheSchedule.xml file, use the WebSphere
Administrator’s Console to restart the STAdmin enterprise application.
   a. Open the WebSphere Administrator’s Console.
   b. Select Applications - Enterprise Applications.
   c. Select the check box next to STAdmin.
   d. Click the Stop button.
   e. Click the Start button.

Disabling the automatic caching feature
The EMS administration web application contains a caching servlet
(StatisticsCachingServlet) that loads the StatCacheSchedule.xml file. The
StatCacheSchedule.xml file contains the scheduling information that enables the
Community Services and Meeting Services activity to be automatically calculated
and cached at scheduled intervals.

You can disable the StatisticsCachingServlet to prevent the automatic calculation
and caching of the Community Statistics and Meeting Statistics. Preventing the
automatic calculation and caching of the Community Statistics and Meeting
Statistics conserves CPU usage for other EMS processing tasks.

Note: If you disable the automatic caching feature, you must click the Refresh
button on the Community Statistics or Meeting Statistics logging page of the
EMS Administration Tool to view the latest statistics. If the EMS has been in
service for an extended period of time, you should click the Refresh button
only during a period of low EMS usage. For more information, see
"Managing the Community Statistics and Meeting Statistics logging views."

To disable the automatic caching feature:
1. Use a text editor to open the Web.xml file on the EMS machine. The default
location of the Web.xml file is:
   C:\Program
   Files\WebSphere\AppServer\installedApps\<servername>\STAdmin.ear
   \admin.war\WEB-INF\web.xml
2. In the Web.xml file, locate the CacheSchedulingEnabled parameter: <init-param
   id="InitParam_1091653873114"> <param-name>CacheSchedulingEnabled</param-name>
   <param-value>true</param-value> </init-param>
3. In the parameter above, change the <param-value>true</param-value>
   attribute to <param-value>false</param-value>. Changing the value to "false"
disables the automatic caching feature.
4. After you have altered the StatCacheSchedule.xml file, use the WebSphere Administrator’s Console to restart the STAdmin enterprise application.
   a. Open the WebSphere Administrator’s Console.
   b. Select Applications - Enterprise Applications.
   c. Select the check box next to STAdmin.
   d. Click the Stop button.
   e. Click the Start button.

Configuring LDAP directory settings from the EMS Administration Tool

You can use the EMS Administration Tool to configure the settings that enable a Sametime server to connect to and access entries in an LDAP Directory. To reach the Directory settings, open the EMS Administration Tool and click LDAP Directory.

Note: The LDAP directory settings available from the EMS Administration Tool apply only to Sametime server access to the LDAP directory. These settings do not affect the way in which the WebSphere server accesses the LDAP directory.

For more information about LDAP directory access in the EMS environment, see:

- [LDAP directory access](#) and the Web Conference Management Server in the "Introduction to Sametime servers and the Enterprise Meeting Server" chapter.
- [Configuring WebSphere server security and LDAP directory access](#) in the "Setting up the Enterprise Meeting Server and a Meeting Services cluster" chapter.

Only a single LDAP directory can be used in an EMS environment. When configuring the LDAP settings from the EMS Administration Tool note the following:

- The LDAP settings available from the EMS Administration Tool are the same LDAP settings available from the standard Sametime Administration Tool. The chapter titled "[Using LDAP with the Sametime server](#)" discusses all available LDAP settings.
- Since all of the Sametime servers controlled by the EMS must access the same LDAP directory, the LDAP settings for each Sametime server controlled by the EMS should be identical.

Configuring connectivity for Sametime servers added to the EMS

Configuring connectivity for Sametime servers added to the EMS is very similar to configuring connectivity for Sametime servers in a standard deployment (that does not include the EMS).

Configuring connectivity for Meeting Services, Broadcast Services, and Community Services in an EMS environment is discussed below.

Meeting Room and Broadcast client connections (Meeting Services and Broadcast Services)

The EMS operates as the meeting scheduling and attending interface for the end users, but the users do not receive clients or any interactive or broadcast meeting data from the EMS.
When a user attends a meeting, Meeting Room client and Broadcast client
connectivity works as follows:

1. The user accesses the EMS using a Web browser and selects a link to attend a
meeting.
2. The EMS retrieves the following information from the DB2 database:
   • The server in the Meeting Services cluster that the EMS has selected to host
     the meeting.
   • The client connectivity parameters, such as TCP/IP ports and HTTP
     tunneling settings, for the selected server.
   The EMS uses HTTP to pass this information to the connecting Web browser.
3. The Web browser uses the information received from the EMS to make an
   HTTP connection to the Sametime server hosting the meeting.
4. At this point, Sametime client connectivity to the Meeting Services,
   Audio/Video Services, and Broadcast Services on a clustered Sametime server
   functions exactly like Sametime client connectivity to a server that is not
   clustered.
   The Meeting Room client or Broadcast client required to attend the meeting is
   loaded to the user’s Web browser from the Sametime server in the Meeting
   Services cluster that is hosting the meeting.
   The meeting data also passes between the Sametime servers and the user’s
   Meeting Room or Broadcast client. The Sametime clients connect to the
   Sametime server in the cluster that is hosting the meeting to receive the
   meeting data. A user does not receive the Sametime clients or the meeting data
   from the EMS.

For more information about how Sametime clients connect to Sametime servers,
see [Sametime Connect client connection processes](#) and [Meeting Room and
Broadcast client connection processes](#).

### Configuring connectivity for Meeting Services and Broadcast Services connections

To access the Meeting Services and Broadcast Services connectivity settings for
Sametime servers that have been added to the EMS, open the EMS Administration
Tool and click Configuration - Connectivity. The “Networks and Ports” tab appears.
You can configure networks and ports for each individual server controlled by the
EMS; you cannot make global networks and ports settings that apply to all servers
controlled by the EMS.

The Networks and Ports settings that control connectivity for the Meeting Room
client and Broadcast client are discussed in the following topics in the “Configuring
Sametime Connectivity” chapter of this documentation.

**Note:** Since the Meeting Room client and Broadcast client connect to a Sametime
server to receive the meeting data (and not the EMS), the Networks and
Ports settings operate the same in an EMS environment as a standard
Sametime deployment that does not include the EMS.

- **Meeting Services Network settings**
  - Meeting Room client connection process using JVM 1.4.2 (Community
    Services and Meeting Services)
  - Meeting Room client connection process using JVM 1.4.2 (Audio/Video
    Services)
- **Broadcast Services Network settings**
Sametime Connect client connections (Community Services)

The connection process of the Sametime Connect clients depends on whether the Community Services of the Sametime servers are clustered or not clustered:

- If the Community Services are clustered, a Sametime Connect client connects to a rotating DNS system or WebSphere Edge Server (Network Dispatcher). For a description of this process, see Configuring client connectivity for the Community Services cluster in the Setting up a Community Services cluster without clustering the Meeting Services chapter of this documentation.

- If the Community Services are not clustered, the Sametime Connect client can connect to the Community Services of any Sametime server in the Meeting Services cluster. In this scenario, the Sametime Connect client follows its normal connection process as described in the Basic Sametime Connect client connection process or Sametime Connect client connection processes using the Web browser or Java Plug-in connectivity settings.

Note: In either case above, Sametime Connect clients do not access the EMS. Note that it is also possible for Sametime Connect clients to connect to other Sametime servers in the community that are not part of either a Community Services cluster or a Meeting Services cluster.

Configuring connectivity for the Community Services

If a Sametime server has been added to the EMS, you can also set the Community Services Network settings from the EMS Administration Tool. To access the Community Services connectivity settings for Sametime servers that have been added to the EMS, open the EMS Administration Tool and click Configuration - Connectivity. The "Networks and Ports" tab appears. You can configure Community Services networks and ports settings for each individual server controlled by the EMS; you cannot make global networks and ports settings that apply to all servers controlled by the EMS.

Configuring the Community Services of Sametime servers added to the EMS

To configure the Community Services of Sametime servers controlled by the EMS, open the EMS Administration Tool and choose Configuration - Community Services. When configuring Community Services of Sametime servers controlled by the EMS, note the following:

- The Community Services settings apply to every server controlled by the EMS. When you specify a setting from the Configuration - Community Services settings of the EMS Administration Tool, the setting goes into effect for every Sametime server controlled by the EMS. You cannot make Community Services configuration settings for an individual server controlled by the EMS.

Note: To cluster the Community Services of a group of Sametime servers controlled by the EMS, see Creating a Community Services cluster with the EMS. The Community Services settings apply to all Sametime servers controlled by the EMS regardless of whether the Community Services of those Sametime servers have been clustered.

- If you want anonymous (unauthenticated) users to access the EMS, you must configure the security role settings in the WebSphere security console to allow
anonymous users to create and attend meetings. For more information about WebSphere security, see [Setting up security for the Enterprise Meeting Server](#).

If you configure the security role settings in the WebSphere security console to allow anonymous access, you should use the settings on the Anonymous Access tab of the EMS Administration Tool to ensure that users can enter a display name when attending meetings from the EMS.

Note the following about settings on the Anonymous Access settings on the Community Services tab of the EMS Administration Tool:

- The **Users of Sametime applications** can specify a display name so that they do not appear online as anonymous. This setting is still a valid setting in the EMS Administration Tool. This setting takes effect if you have configured the security role settings in the WebSphere security console to allow anonymous users to attend meetings. This setting enables an anonymous user to enter a display name when attending a meeting so that each anonymous user can be individually identified in the Meeting Room client Participant List. If you do not select this setting, each user name displays as "anonymous" in the Participant List and you cannot distinguish one anonymous user from another.

- The **Number of entries on each page in dialog boxes that show names in the directory setting** functions the same in an EMS environment as in a standard Sametime deployment. In the EMS environment, all user names are stored in a single LDAP directory accessed by the EMS.

- The **How often to poll for new names... setting** functions the same in an EMS environment as in a standard Sametime deployment. In the EMS environment, the LDAP directory is polled at the intervals specified for this setting.

- Ensure that the **Allow users to authenticate using either LTPA or Sametime Tokens... setting** is selected for all Sametime servers in the cluster.

- If you select the **Allow users to send announcements** option, users will be able to send announcements to anyone in the Sametime community. The Sametime community consists of all users in the LDAP directory, the EMS, and all Sametime servers that have access to the LDAP directory.

- If you select the options to display the links for **Sametime Connect for the desktop** or **Sametime Connect for browsers**, Sametime Connect will be available to end users from the EMS. Users will not be able to access Sametime Connect from the Welcome page of the individual Sametime servers that are controlled by the EMS.

- If you select the **Allow users to save their user name, password, and proxy information (automatic login)** option, user information will be saved in the vpuserinfo.nsf database on a user’s home Sametime server. If the Community Services of some of the servers that are controlled by the EMS have been clustered, this information is stored in the vpuserinfo.nsf database that replicates in real-time between the servers in the Community Services cluster.

### Configuring the Meeting Services of Sametime servers added to the EMS

To configure the Meeting Services of Sametime servers that have been added to the EMS, open the EMS Administration Tool and click Configuration - Meeting Services. When configuring Meeting Services of Sametime servers that have been added to the EMS, note the following:

- The Configuration - Meeting Services settings in the EMS Administration Tool apply to every server controlled by the EMS. When you specify a setting from
the Configuration - Meeting Services settings of the EMS Administration Tool, the setting goes into effect for every Sametime server controlled by the EMS. You cannot make Meeting Services configuration settings for an individual server controlled by the EMS.

- When you make changes to the Meeting Services settings, your changes do not affect meetings that are in progress. Only future meetings are affected.

Note: There is one exception to the rule above. If the administrator changes the "Automatically extending meetings beyond the scheduled end time" setting, that setting goes into effect for meetings that are currently active. Any active meetings will be extended for the length of time the administrator specifies as long as meeting participants are still attending the meeting. It is not necessary to restart the server for this change to take effect.

- To set broadcast connection speeds for meetings with audio/video, click the "audio/video configuration page" link. These settings are on the Connection Speed Settings tab in the Audio/Video settings of the EMS Administration Tool.

- The following information applies to recorded meetings in a Meeting Services cluster:
  - You cannot export, import, or replace recorded meetings in a cluster. You can still delete recorded meetings.
  - Click the "Recorded meeting settings" link on the General tab of the Meeting Services settings to determine the location and the available disk space for recorded meetings on a specific server in the cluster. The recorded meeting settings are on the "Edit/Remove a Meeting Server" tab in the EMS Administration Tool. To access the "Edit/Remove a Meeting Server" tab, choose Configuration - Meeting Cluster in the EMS Administration Tool.
  - To locate a recorded meeting in the Enterprise Meeting Server, an end user can search for the meeting or use the Recorded link to view all recorded meetings. All recorded meetings for all servers in the cluster can be attended from the Enterprise Meeting Server user interface.

---

**Configuring the Audio/Video Services of Sametime servers added to the EMS**

To configure the Audio/Video Services within a cluster, open the EMS Administration Tool and click Configuration - Audio/Video Services.

When configuring Audio/Video Services in a cluster, note that:

- The settings apply to all servers controlled by the EMS. You cannot specify Audio/Video Services settings for individual Sametime servers that are controlled by the EMS.

- The Usage Limits and Denied Entries settings are available on the "Edit/Remove a Meeting Server" tab in the EMS Administration Tool. To access the "Edit/Remove a Meeting Server" tab, choose Configuration - Meeting Cluster in the EMS Administration Tool. You can set Usage Limits and Denied Entries for each server controlled by the EMS. You can use these settings to prevent Meeting Services activity (including audio/video activity) from occurring on a Sametime server. For more information, see Specifying Usage Limits and Denied Entry settings for the Sametime server.
Working with the Broadcast Services of Sametime servers added to the EMS

Configuring the Broadcast Services for Sametime servers that are controlled by the EMS is similar to configuring the Broadcast Services for Sametime servers in a standard Sametime deployment. See [Working with the Broadcast Services](#) for more information.
Chapter 21. Using the StdebugTool.exe utility

You can use the StdebugTool.exe utility to produce trace files and create new trace file sets for troubleshooting purposes. These trace files contain debug messages that aid IBM Technical Support in troubleshooting IBM Lotus Sametime problems. If you have never worked with Sametime trace files before, you should use the StdebugTool.exe utility only under the guidance of IBM Technical Support.

Note: The StdebugTool.exe utility is available only for Sametime servers that run on the Windows operating system.

Trace file reporting on a Sametime server is controlled through settings in the Sametime.ini file. You use the StdebugTool.exe utility to change settings in the Sametime.ini file to produce specific trace files. If you use this utility to change the Sametime.ini file settings, you do not need to restart the Sametime server to begin producing the trace files. The server will begin creating these files immediately after you run the tool.

You can use the StdebugTool.exe utility to change trace file settings on either a local or remote Sametime server.

An administrator can also produce trace files by using a text editor to manually edit the trace file settings in the Sametime.ini file. However, if you manually edit the Sametime.ini file settings, you must restart the Sametime server before it will begin producing the trace files.

For more information on using this utility, see "Running the StdebugTool.exe utility."

Running the StdebugTool.exe utility

To start the StdebugTool.exe utility, you enter the StdebugTool.exe command from the server command prompt.

Note: If you intend to alter settings in a Sametime.ini file on a remote computer, you must append the IP address of the remote computer to the StdebugTool.exe command when starting the utility. If you want to alter settings in a Sametime.ini file on the local computer, it is not necessary to append the IP address of the local computer to the StdebugTool.exe command. A step-by-step example of running the StdebugTool.exe utility is provided below.

When the utility starts, you are presented with a second command prompt. At this second command prompt, you enter a command option to direct the StdebugTool.exe utility to perform a specific action.

The possible command options are described below. These options include: ?, s, I, f, p, r, q:

- ? - Prints a help message
- S <FLAG_NAME> <value> - Sets a value to enable or disable a trace file flag that already exists in the Sametime.ini file. The <FLAG_NAME> string is a
variable representing a specific trace flag. The <value> parameter is usually either "1" to enable the flag or "0" to disable it.

For example, the VP_DB_TRACE flag in the Sametime.ini file is used to enable or disable all trace file reporting capabilities. The following s command option will enable the trace file reporting capabilities if the VP_DB_TRACE=0 setting already exists in the Sametime.ini file:

```
  s VP_DB_TRACE 1
```

- **i <FLAG_NAME> <value>** - Adds a specific flag to the Sametime.ini file and sets a value to enable or disable the trace file flag. Use this option if the flag you want to use does not currently exist in the Sametime.ini file. For example, the VP_LDAP_TRACE flag controls trace file reporting for LDAP directory access operations. The following I command option will add the VP_LDAP_TRACE flag to the Sametime.ini file and enable the LDAP access trace file reporting:

```
  I VP_LDAP_TRACE 1
```

- **f** - Prints a list of debug flags
- **p** - Prints a list of services
- **r** - Replaces existing trace files with new ones. Use this option to delete existing trace files, or copy over existing trace files with new ones.
- **q** - Stops (quits) the StdebugTool.exe utility.

**Trace file location**

If you use the StdebugTool.exe file to produce trace files, the trace files are output to the <Sametime server installation>\Trace directory (for example, C:\Lotus\Domino\Trace).

**Step-by-step example of running the StdebugTool.exe utility**

A step-by-step example of running the StdebugTool.exe utility is provided below. Note that StdebugTool.exe utility resides in the Sametime server installation directory (default C:\Lotus\Domino\Sametime) following a Sametime server installation. You must run the StdebugTool.exe utility from the Sametime server installation directory.

To run the StdebugTool.exe utility:

1. Start the server command prompt.
2. Change to the Sametime server installation directory. For example, enter the following command at the server command prompt:

```
  Cd Lotus\Domino\Sametime
```
3. Enter StdebugTool.exe to start the StdebugTool.exe utility. For example, you can enter the following command to start the utility if you want to alter settings in the Sametime.ini file on the local computer:

```
  C:\Lotus\Domino\Sametime\StdebugTool.exe
```

Or, you can enter the following command if you want to alter settings in the Sametime.ini file on a remote computer that has the IP address 1.2.3.5

```
  C:\Lotus\Domino\Sametime\StdebugTool.exe 1.2.3.5
```

4. The StdebugTool command prompt displays. At this command prompt, enter the command option that you want to run. For example, if you want to display a list of all debug flags, type:

```
  F   (and press Enter)
```
5. After the first command completes, you can run additional commands from the StdebugTool command prompt.
   
   For example, you could enter the following command to produce a trace file with debug messages pertaining to LDAP directory access operations:
   
   `I VP_LDAP_TRACE 1`  (and press Enter)
   
   When the command above completes, you can enter another command if necessary. For example, you could enter the following command to disable general trace file reporting. This example assumes the VP_DB_TRACE=1 setting currently exists in the Sametime.ini file.
   
   `s VP_DB_TRACE 0`  (and press Enter)
   
6. When you are finished running commands, type the letter q at the StdebugTool command prompt to quit the utility.
Chapter 22. Using the Name Conversion Utility

You use the IBM Lotus Sametime Name Conversion Utility to ensure that name updates you make in a Domino or LDAP directory are also made in Sametime Connect client buddy lists and privacy lists.

This section discusses the following topics concerning the Name Conversion Utility:

- When to run the Name Conversion Utility
- Preparing to run the Name Conversion Utility
- Running the Name Conversion Utility
- Debug and trace file information
- Known issues and limitations

Using the Name Conversion Utility

You use the IBM Lotus Sametime Name Conversion Utility to ensure that name updates you make in a Domino or LDAP directory are also made in Sametime Connect client buddy lists and privacy lists.

This section discusses the following topics concerning the Name Conversion Utility:

- **When to run the Name Conversion Utility**
- Preparing to run the Name Conversion Utility
- Running the Name Conversion Utility
- Debug and trace file information
- Known issues and limitations

When to run the Name Conversion Utility

Run the Sametime Name Conversion Utility after you make updates to user and group name data in a Sametime server Domino or LDAP directory. This utility ensures that the name updates you make in the directory are also made in Sametime Connect client buddy lists and privacy lists.

Users create buddy lists and privacy lists from the Sametime Connect client by selecting user names and group names from the directory that is used with the Sametime server. These buddy lists and privacy lists are stored on the Sametime server in the vpuserinfo.nsf database. When a user starts the Sametime Connect client, the lists are downloaded from the vpuserinfo.nsf database on the Sametime server to the client on the user’s local computer.

If you change user or group name data in the Sametime server directory, you must run the Name Conversion Utility to ensure that those same name change updates are made in the buddy lists and privacy lists that are stored in the vpuserinfo.nsf database on the Sametime server.

**Note:** Since the Name Conversion utility makes changes to the vpuserinfo.nsf database that is located on the server and shared by all users who connect
to the server, you must schedule running the utility at a time when it is convenient to stop all Sametime server activity.

You can use this utility to make the following changes to the buddy list and privacy list names that are stored in the vpuserinfo.nsf database:

- If you convert the Sametime server directory from the native Domino format to the Domino LDAP format, you must run this utility to ensure the names in the buddy lists and privacy lists are also converted to the Domino LDAP format.
- You can make changes to individual user names and group names that exist in the lists stored in the vpuserinfo.nsf database.

Specifically, you can use this utility to:

- Change the first or last names of individual users. For example, you can change the user name “Yafit Telyas” to “Yafit Sami” in all lists stored in the vpuserinfo.nsf database.
- Change the names of groups. For example, you can change the group name “Haifa Development Team” to “Westford Development Team” in all lists stored in the vpuserinfo.nsf database.

If you change the first or last name of a user in the user’s Person document in the Sametime server directory, or if you change the name of a Group in a Group document in the Sametime server directory, you must run this utility to ensure these same updates are made in the buddy lists and privacy lists.

- You can make changes to organizational unit names in the lists stored in the vpuserinfo.nsf database. For example, you can use this utility to change the organizational unit name attribute ”/team/com” to ”/branch/team/org” in all buddy lists and privacy lists.

If you make organizational unit name changes in the Sametime server directory, you must run this utility to ensure these same updates are reflected in the buddy lists and privacy lists.

Preparing to run the Name Conversion Utility

Review this information before running the utility. This section provides basic information about managing the vpuserinfo.nsf database and working with the text files that control the operation of the Name Conversion Utility.

Managing the vpuserinfo.nsf database

The Name Change Utility alters names that are stored in the vpuserinfo.nsf database. Before you run the utility:

- Make a backup copy of the vpuserinfo.nsf database. The vpuserinfo.nsf database is located in the Sametime server Data directory. (On Windows, the default directory is C:\Lotus\Domino\Data).

After you make a backup copy of the vpuserinfo.nsf database, you can run the utility on the copy of the vpuserinfo.nsf database in the Sametime server Data directory.

Alternately, you can copy the vpuserinfo.nsf database from the Data directory of an active Sametime server to a working directory and run the utility on the vpuserinfo.nsf database in the working directory. When the conversion is complete, you can stop the Sametime server and then copy the converted vpuserinfo.nsf from the working directory over the unconverted vpuserinfo.nsf database in the Sametime server Data directory.

Note that if you use this method to convert the vpuserinfo.nsf database, users may make changes to the buddy lists and privacy lists in the vpuserinfo.nsf
database that is active on the Sametime server while you are performing the conversion on the vpuserinfo.nsf that you copied to the the working directory. Any buddy list or privacy list changes that users make during this time period will be lost when you replace the unconverted vpuserinfo.nsf database with the converted database from the working directory.

- If you have clustered the Community Services on the Sametime servers in your environment, be sure that you stop all Sametime servers in the cluster before running the utility to convert names in the vpuserinfo.nsf database. After you have converted the database, make sure to replicate the converted vpuserinfo.nsf database to all servers in the cluster.

**Editing the text files that control the operation of the utility**

The two text files that control the operation of the Name Conversion Utility are located in the Sametime server Data directory and are named:

- NameConvUtil.ini
- NameConvUtil.txt

The step-by-step procedures for running the utility that appear later in this Appendix require you to edit these text files. Note the following when editing the NameConvUtil.txt file and the NameConvUtil.ini files:

- The NameConvUtil.txt file must always begin with lines shown below. Never remove these lines from the file:
  ```
  #don't delete/change/move this first section
  #save the file in UTF-8 format only
  [Encoding]
  UTF_8=1
  ```

- To comment a line out of either of the text files, enter the # character at the beginning of the line.

- The edited NameConvUtil.txt and NameConvUtil.ini file must reside in the Data directory of the Sametime server on which you run the Name Conversion Utility.

- On the IBM i5/OS platform, the owner of the NameConvUtil.txt and NameConvUtil.ini file must be QNOTES.

- Always save the NameConvUtil.txt file in the UTF-8 format. This format is mandatory when running the Name Conversion Utility on AIX/Solaris versions of Sametime and recommended when running the utility on either the i5/OS or Windows version of Sametime.

**Note:** If either the NameConvUtil.txt or NameConvUtil.ini file contains any special characters (DBCS, accented characters, or any other extending ASCII characters), then the Name Conversion Utility requires that these files be saved in UTF-8 format. The NameConvUtil.txt file is most likely to contain special characters.

Follow the instructions below to save a file in the UTF-8 format:

**For Windows servers:** Use the File-Save As menu option in your text editor to save the file in the UTF-8 format.

**For AIX/Solaris servers:** You can use any Unix UTF-8 text editor on an AIX or Solaris computer to edit and save a file in the UTF-8 format.

You can also use a UTF-8 text editor on a Windows computer to edit a file and then FTP the edited file to the AIX or Solaris system using BINARY FTP. You **cannot** FTP the edited file to an AIX or Solaris system using ASCII FTP.

**For IBM i5/OS servers:**
- From your client workstation, you can map a network drive to make the
  Sametime server Data directory accessible from your work station. Then you
  can run a text editor such as Notepad from your workstation and update the
  file directly on your IBM i5/OS server. Be sure to select File-Save As...and
  specify UTF-8 as the Encoding option, then save the file.

  Alternately, you can copy the files to your workstation using any other
  convenient method (for example, dragging and dropping with IBM i5/OS
  Navigator or FTP). Edit the files on your workstation, save them in UTF-8
  format, and then transfer them back to the Sametime server Data directory.

  **Note:** Some file transfer methods may not preserve the file owner when you
  replace the file.

- To verify that QNOTES is the owner of each file, run the following OS/400
  commands:
  
  ```
  WRKAUT OBJ('server_data_directory/NameConvUtil.ini')
  WRKAUT OBJ('server_data_directory/NameConvUtil.txt')
  ```

  If necessary, run these commands to change the owner for each file to
  QNOTES: CHGOWN OBJ('server_data_directory/NameConvUtil.ini')

  NEWOWN(QNOTES) CHGOWN
  OBJ('server_data_directory/NameConvUtil.txt')

  NEWOWN(QNOTES)

---

**Running the Name Conversion Utility**

You can run the Name Conversion Utility to make three basic types of name
changes in the vpuserinfo.nsf database. You can run this utility to change:

- Buddy lists and privacy lists from the native Domino directory format to the
  Domino LDAP directory format.
- Individual user names and group names that exist within the buddy lists and
  privacy lists.
- Organizational unit names that exist within the buddy lists and privacy lists.

You must run the utility separately to make each type of change. For example, if
you want to change individual user names and group names and also change
organizational unit names, you must run the utility twice: run the utility once to
make the individual user and group name changes and then run the utility a
separate time to make the organizational unit name changes.

See the appropriate topic below for step-by-step instructions for making each type
of name change:

- **Converting buddy lists and privacy lists from the Domino directory format to
  the LDAP directory format**
- **Changing user names and group names**
- **Changing organizational unit names**

**Converting buddy lists and privacy lists from the Domino directory format to the LDAP directory format**

Use these steps to convert the names in buddy lists and privacy lists in the
vpuserinfo.nsf database from the native Domino directory format to the Domino
LDAP directory format.

**Note:** You can use this utility only to convert the names from the native Domino
directory format to the Domino LDAP directory format. You cannot convert
the names from the native Domino directory format to other LDAP directory
formats, such as a Netscape or Microsoft LDAP directory format.
1. Review the information in [Preparing to run the Name Conversion Utility] before you run the utility.

2. Stop all Sametime activity on the server where you plan to run the Name Conversion Utility.
   • For Windows: Stop the Sametime server from the Windows Control Panel.
   • For AIX/Solaris: Enter “quit” on the Domino Console to stop Domino and Sametime.
   • For IBM i5/OS: End the Sametime components on the server where you plan to run the name conversion utility but allow the server to remain active by running the following command from the Domino server console:
     \$ tell staddin2 quit

3. Open the NameConvUtil.ini file that is located in the Sametime server Data directory and make the following changes in the [CONFIG] section:

   [CONFIG]
   CONV_INPUT_FILE_NAME=NameConvUtil.txt
   DOMINO_TO_LDAP=1
   ORGANIZATION_NAME=0

   This configuration specifies that the NameConvUtil.txt file as the file that contains the name change rules, enables the Domino to LDAP name conversion, and disables the organizational unit name changing functionality.

4. Save and close the NameConvUtil.ini file.

5. Run the Name conversion utility to convert the names in the buddy lists from the native Domino format to the Domino LDAP format.

   For Windows:
   Open a server command prompt and run the NameConvUtil.exe file that is located in the Sametime server Data directory.
   By default, the vpuserinfo.nsf database also resides in the Sametime server Data directory. In this case, you do not need to specify an additional parameter. If you are using the default for the Sametime server Data directory, use this command at the server command prompt to run the utility:
   \$ C:\Lotus\Domino\Data>NameConvUtil.exe
   
   If you have moved the vpuserinfo.nsf database to a different directory, add the directory path to the vpuserinfo.nsf database as a parameter to the command. For example:
   \$ C:\Lotus\Domino\Data>NameConvUtil.exe C:\Work\vpuserinfo.nsf
   
   Also note that if the Domino server was installed as a partitioned server, the Data directory for the Domino server will reside on a different logical drive than the other Domino server files. In this case, you must include the full drive and directory path to the vpuserinfo.nsf database in the command. For example, if the Data directory resides on the D: drive, use a command such as this to run the utility from the server command prompt:
   \$ C:\Lotus\Domino\Data>NameConvUtil.exe D:\Lotus\Domino\Data\vpuserinfo.nsf

   For AIX/Solaris:
   Use a text editor to open the stname.sh file in the Domino server Data directory.
   You must edit two parameters in the stname.sh file. The BINDIR parameter must specify the path to the Bin subdirectory of the Domino server (this is a different location for AIX and Solaris). The LOTUSDIR parameter must specify the path to the Domino server Data directory. Examples of the edited parameters are provided below.
Save and close the stname.sh file.

To start the utility, use the command line to run the following command from the Domino server Data directory:

```
./stname.sh
```

**For IBM i5/OS:**

By default, the vpuserinfo.nsf database resides in the Sametime server Data directory. If you have not moved the database to a different location, run the name conversion utility by issuing the following command from the Domino server console:

```
LOAD STNameConv
```

If vpuserinfo.nsf is not located in the server Data directory, then you must specify the full path name for the database as a parameter on the command. For example,

```
LOAD STNameConv /Work/vpuserinfo.nsf
```

When the name conversions are complete, restart the Sametime components by running the following command from the Domino server console:

```
Load STAADDIN2
```

6. If you have clustered the Community Services on the Sametime servers in your environment, ensure the converted vpuserinfo.nsf database is replicated to all Sametime servers in the cluster.

### Changing user names and group names

You can change individual user names (first and last names) and group names in the buddy lists and privacy lists that are stored in the vpuserinfo.nsf database.

You can do all of the following when using this utility to make user name and group name changes:

- You can change both user names and group names during a single execution of the utility. It IS NOT necessary to run the utility one time to make user name changes and then a second time to make the group name changes.
- You can change multiple user names and group names during a single execution of the utility. For example, you can perform six user name changes and three group name changes at the same time.
- You can change the user and group names regardless of whether the names are stored in the buddy lists and privacy lists in the native Domino format or an LDAP format. However, different name change rules are used for each of these formats.
- You can make user and group name changes when the user and group names are stored in any LDAP format supported by the Sametime server. For example, if the Sametime server is configured to use an IBM or Netscape® LDAP directory, you could use this utility to change names that are stored in either of those formats.

Follow the steps below to make individual user or group name changes:

1. Review the information in "Preparing to run the Name Conversion Utility" before you run the utility.
2. Stop all Sametime activity on the server where you plan to run the Name Conversion Utility.
   - **For Windows:** Stop the Sametime server from the Windows Control Panel.

BINDIR=/opt/lotus/notes/latest/ibmpow
LOTUSDIR=/local/notesdata

662 Sametime Administrator's Guide
• **For AIX/Solaris**: Enter "quit" on the Domino Console to stop Domino and Sametime.

• **For IBM i5/OS**: End the Sametime components on the server where you plan to run the name conversion utility but allow the server to remain active by running the following command from the Domino server console:
  ```
tell staddin2 quit
```

3. Open the NameConvUtil.ini file that is located in the Sametime server Data directory and make the following changes in the [CONFIG] section:

   ```
[CONFIG]
CONV_INPUT_FILE_NAME=NameConvUtil.txt
DOMINO_TO_LDAP=0
ORGANIZATION_NAME=0
```

This configuration specifies that the NameConvUtil.txt file as the file that contains the name change rules, and disables both the Domino to LDAP name conversion and the organizational unit name changing functionality.

4. Save and close the NameConvUtil.ini file.

5. Open the NameConvUtil.txt file that is located in the Sametime server Data directory and make the changes described in the next steps.

6. Complete this step if you want to change group names in the vpuuserinfo.nsf database.

   Under the [GROUPS] heading in the NameConvUtil.txt file, enter the rule that governs the group name change. Use this syntax for entering the group name change rule:

   ```
OLDGROUPID-->NEWGROUPID
```

   To illustrate the name change syntax, assume that you want to change the group named "Marketing" to "Sales." The specific syntax you use depends on whether group names are stored in Domino LDAP format, or stored in native Domino directory format, as noted below:

   • **Group names stored in Domino LDAP format** - If the group names are stored in the Domino LDAP directory format, use the DN of the group name for each GROUPID, as shown here:

     ```
[GROUP]
CN=Marketing,OU=East,O=Acme-->CN=Sales,OU=East,O=Acme
```

   • **Group names stored in native Domino directory format** - If the group names are stored in the vpuuserinfo.nsf database in the native Domino directory format, enter the GROUPID for each group in this format:

     Domino directory replica ID/Group name

     It is important that you specify the Domino directory replica ID in the format that Sametime uses, rather than the format used by Domino. When including the Domino directory replica ID in the name change rule syntax, you must replace the colon character (:) of the replica ID with a space, reverse the order of the two numeric sequences that comprise the replica ID, and then remove the leading zeros.

     For example, assume you have changed the group named "Marketing/East/Acme" to "Sales/East/Acme" by editing the Group document for this group in the Domino directory, which shows the following replica ID on the "i" tab of the database properties:

     85256500:0052e811

     For this example, the Domino directory replica ID must be specified as follows:
To make this group name change in the buddy lists stored in the vpuserinfo.nsf database, you must use this syntax in the group name change rule:

[GROUPS]
52e811 85256500/Marketing/East/Acme-->52e811
85256500/Sales/East/Acme

You can enter more than one group name change rule under the [GROUP] heading in the NameConvUtil.txt file if you want to change multiple group names when you run the Sametime Name Conversion Utility.

Note: There is an alternative way to retrieve the group ID that you must enter in the group name change rule. Perform the following procedure:

a. Open a Sametime Connect client.

b. Add a group to your buddy list from the same directory where you have changed the group name, or plan to change the group name.

c. Save your buddy list to a file, using the People - Save List... menu option

d. Use a text editor such as Notepad to open the saved buddy list (.dat) file.

e. Find the entry for the group you added to the list. The first column of the entry contains a G and the next item in the entry is the replica ID in this format:

52e811;85256500

f. Replace the semi-colon (;) with a blank space when specifying this replica ID in the NameConvUtil.txt file.

7. Complete this step if you want to change the first or last names of individual users in buddy lists and privacy lists of the vpuserinfo.nsf database.

Under the [USERS] heading in the NameConvUtil.txt file, enter the rule that governs the user name change. Use this format for entering this rule:

OLDUSERID-->NEWUSERID

• **User names stored in Domino LDAP format** - If the user names are stored in the Domino LDAP directory format, your name change rules should use commas as separators instead of the forward slashes, as shown in these examples:

[USERS]
CN=Lisa Marth,OU=Haifa,O=IBM-->CN=Lisa Smith,OU=Haifa,O=IBM
CN=Avi Bino,OU=Haifa,O=IBM-->CN=Avner Bino,OU=Haifa,O=IBM

• **User names stored in native Domino directory format** - If the user names are stored in the vpuserinfo.nsf database in the native Domino directory format, you can use rules such as these to change the first and last names of users:

[USERS]
CN=Lisa Marth/OU=Haifa/O=IBM-->CN=Lisa Smith/OU=Haifa/O=IBM
CN=Avi Bino/OU=Haifa/O=IBM-->CN=Avner Bino/OU=Haifa/O=IBM

Note: When composing the name change rules, be sure to use the full name formats for the user names, as shown in these examples. Do not use shortened versions of the user names, or user display names, in the name change rules. For example, you should never compose a name change rule such as this:

CN=Lisa Marth-->CN=Lisa Smith
8. Before saving and closing the NameConvUtil.txt file, make sure to delete or comment out any unwanted name change rules that appear under the [GROUPS] or [USERS] headings in the NameConvUtil.txt file. Make sure that the name change rules underneath the [GROUPS] or [USERS] headings specify only the name changes that you want to occur during this running of the utility.

9. Save and close the NameConvUtil.txt file. (Save the file in UTF-8 format if necessary.)

10. Follow the instructions below to run the Name conversion utility to make the name changes that you have configured in the NameConvUtil.txt file.

   **For Windows:**
   Open a server command prompt and run the NameConvUtil.exe file that is located in the Sametime server Data directory.
   By default, the vpuserinfo.nsf database also resides in the Sametime server Data directory. In this case, you do not need to specify an additional parameter. If you are using the default for the Sametime server Data directory, use this command at the server command prompt to run the utility:
   
   ```
   C:\Lotus\Domino\Data>NameConvUtil.exe
   ```
   If you have moved the vpuserinfo.nsf database to a different directory, add the directory path to the vpuserinfo.nsf database as a parameter to the command. For example:
   ```
   C:\Lotus\Domino\Data>NameConvUtil.exe C:\Work\vpuserinfo.nsf
   ```
   Also note that if the Domino server was installed as a partitioned server, the Data directory for the Domino server will reside on a different logical drive than the other Domino server files. In this case, you must include the full drive and directory path to the vpuserinfo.nsf database in the command. For example, if the Data directory resides on the D: drive, use a command such as this to run the utility from the server command prompt:
   ```
   C:\Lotus\Domino\Data>NameConvUtil.exe D:\Lotus\Domino\Data\vpuserinfo.nsf
   ```

   **For AIX/Solaris:**
   
   Use a text editor to open the stname.sh file in the Domino server Data directory.
   
   Edit the following parameter in the stname.sh file so that it specifies the path to the Bin subdirectory of the Domino server (this is a different location for AIX and Solaris):
   
   ```
   BINDIR=/opt/lotus/notes/latest/ibmpow
   LOTUSDIR=/local/notesdata
   ```
   
   Save and close the stname.sh file.
   
   To start the utility, use the command line to run the following command from the Domino server Data directory:
   ```
   ./stname.sh
   ```

   **For IBM i5/OS:**
   
   By default, the vpuserinfo.nsf database resides in the Sametime server Data directory. If you have not moved the database to a different location, run the name conversion utility by issuing the following command from the Domino server console:
   ```
   LOAD STNameConv
   ```
   
   If vpuserinfo.nsf is not located in the server Data directory, then you must specify the full path name for the database as a parameter on the command. For example,
   ```
   LOAD STNameConv /Work/vpuserinfo.nsf
   ```
When the name conversions are complete, restart the Sametime components by running the following command from the Domino server console:

```
Load STADDIN2
```

11. If you have clustered the Community Services on the Sametime servers in your environment, replicate the converted vpuserinfo.nsf database is replicated to all Sametime servers in the cluster.

**Changing organizational unit names**

You can change organizational unit names in the buddy lists and privacy lists that are stored in the vpuserinfo.nsf database.

Use the steps below to change organizational unit names in the buddy lists and privacy lists that are stored in the vpuserinfo.nsf database.

1. Review the information in "Preparing to run the Name Conversion Utility" before you run the utility.

2. Stop all Sametime activity on the server where you plan to run the Name Conversion Utility.
   - **For Windows:** Stop the Sametime server from the Windows Control Panel.
   - **For AIX/Solaris:** Enter "quit" on the Domino Console to stop Domino and Sametime.
   - **For IBM i5/OS:** End the Sametime components on the server where you plan to run the name conversion utility but allow the server to remain active by running the following command from the Domino server console:
     
     ```
tell staddin2 quit
```

3. Open the NameConvUtil.ini file that is located in the Sametime server Data directory and make the following changes in the [CONFIG] section:

   ```
   [CONFIG]
   CONV_INPUT_FILE_NAME=NameConvUtil.txt
   DOMINO_TO_LDAP=0
   ORGANIZATION_NAME=1
   ```

   This configuration specifies the NameConvUtil.txt file as the file that contains the name change rules, disables the Domino to LDAP name conversion, and enables the organizational unit name changing functionality.

4. Save and close the NameConvUtil.ini file.

5. Open the NameConvUtil.txt file that is located in the Sametime server Data directory.

6. Enter the organizational unit name change rules under both the [GROUPS] and [USERS] headings in the NameConvUtil.txt file, as discussed below.

   Use this format when entering the organizational unit name change rules under the [GROUPS] and [USERS] headings:

```
OLDDOMAINSUFFIX-->NEWDOMAINSUFFIX
```

To illustrate the organizational unit name change rule syntax, assume that you want to make these two organizational unit name changes in the buddy lists and privacy lists stored in the vpuserinfo.nsf database. You want to change:

- `/team/com` to `/branch/team/org`
- `/teamspace to /team space`

The specific syntax you use depends on whether names are stored in the native Domino directory format or the Domino LDAP format:
• **Names stored in native Domino directory format** - For group names stored in the vpuserinfo.nsf database in the native Domino directory format, enter the domain suffix changes in the Domino hierarchical format, as shown below:

  [GROUPS]
  /team/com-->/branch/team/org
  /teamspace-->/team space

  For user names stored in the native Domino directory format, you must enter two organizational name change rules for each organizational unit name change that you want to make. One rule must specify the organizational unit in the canonical format and the other must specify the organizational unit in the hierarchical format, as shown below:

  [USERS]
  /ou=team/O=com-->/ou=branch/ou=team,o=Acme /team/com-->/branch/team/org
  /o=teamspace-->/o=team space /teamspace-->/team space

  **Note:** Two rules are required for each organizational unit user name change because the userID and the user display name parameters are stored in a native Domino directory in different formats. A separate rule is required for each of these parameters.

• **Names stored in Domino LDAP format** - If the group and user names are stored in the Domino LDAP directory format, use commas as the separators in the organizational unit name change rules instead of the forward slashes, as shown in the examples below:

  [GROUPS]
  ,ou=team,o=com-->,ou=branch,ou=team,o=org
  ,dc=teamspace-->,dc=team space

  [USERS]
  ,ou=team,o=com-->ou=branch,ou=team,o=org
  ,dc=teamspace-->,dc=team space

  **Note:** Only one rule is required for each organizational unit user name change when names are stored in the LDAP directory format.

7. Before saving and closing the NameConvUtil.txt file, make sure to delete or comment out any unwanted name change rules that appear under the [GROUPS] or [USERS] headings in the NameConvUtil.txt file. Make sure that the name change rules underneath the [GROUPS] or [USERS] headings specify only the name changes that you want to occur during this running of the utility.

8. Save and close the NameConvUtil.txt file. (Save the file in UTF-8 format if necessary.)

9. Run the Name conversion utility to make the name changes that you have configured in the NameConvUtil.txt file.

  **For Windows:**

  Open a server command prompt and run the NameConvUtil.exe file that is located in the Sametime server Data directory.

  By default, the vpuserinfo.nsf database also resides in the Sametime server data directory. In this case, you do not need to specify an additional parameter. If you are using the default for the Sametime server Data directory, use this command at the server command prompt to run the utility:

  C:\Lotus\Domino\Data> NameConvUtil.exe
If you have moved the vpuserinfo.nsf database to a different directory, add the directory path to the vpuserinfo.nsf database as a parameter to the command. For example:

C:\Lotus\Domino\Data>NameConvUtil.exe C:\Work\vpuserinfo.nsf

Also note that if the Domino server was installed as a partitioned server, the Data directory for the Domino server will reside on a different logical drive than the other Domino server files. In this case, you must include the full drive and directory path to the vpuserinfo.nsf database in the command. For example, if the Data directory resides on the D: drive, use a command such as this to run the utility from the server command prompt:

C:\Lotus\Domino\Data>NameConvUtil.exe D:\Lotus\Domino\Data\vpuserinfo.nsf

**For AIX/Solaris:**

Use a text editor to open the stname.sh file in the Domino server Data directory.

Edit the following parameter in the stname.sh file so that it specifies the path to the Bin subdirectory of the Domino server (this is a different location for AIX and Solaris):

BINDIR=/opt/lotus/notes/latest/ibmpow
LOTUSDIR=/local/notesdata

Save and close the stname.sh file.

To start the utility, use the command line to run the following command from the Domino server Data directory:

./stname.sh

**For IBM i5/OS:**

By default, the vpuserinfo.nsf database resides in the Sametime server Data directory. If you have not moved the database to a different location, run the name conversion utility by issuing the following command from the Domino server console:

LOAD STNameConv

If vpuserinfo.nsf is not located in the server Data directory, then you must specify the full path name for the database as a parameter on the command. For example,

LOAD STNameConv /Work/vpuserinfo.nsf

When the name conversions are complete, restart the Sametime components by running the following command from the Domino server console:

Load STADDIN2

10. If you have clustered the Community Services on the Sametime servers in your environment, replicate the converted vpuserinfo.nsf database is replicated to all Sametime servers in the cluster.

---

**Debug and trace file information**

You can enable the Sametime Name Conversion Utility to produce trace messages for debugging purposes. These trace messages can be output to a file or to the monitor.

To output trace messages, follow these instructions:

1. Use a text editor to open the Sametime.ini file located in the Sametime server installation directory.

2. In the Sametime.ini file, enable trace reporting by setting the following parameter as shown: NAME_CONV_TRACE_DEBUG=1
3. Save and close the Sametime.ini file.
4. Open the NameConvUtil.ini file in the Sametime server Data directory.
5. Use the VP_USERS_TRACE_STDOUT parameter to determine the output location for the trace messages as shown below:
   • Set VP_USERS_TRACE_STDOUT=0 to output trace messages to a file in the
     <Sametime server installation>\Trace directory.
   • Set VP_USERS_TRACE_STDOUT=1 to output trace messages to the monitor.
6. Save and close the NameConvUtil.ini file.

To disable the trace message reporting, set the NAME_CONV_TRACE_DEBUG= parameter to 0 (zero) in the Sametime.ini file. No other procedures are required to disable the message reporting.

**Known issues and limitations**

This topic lists the known issues and limitations of the Name Conversion Utility:

• You can use this utility to convert all names in the buddy lists and privacy lists from the native Domino directory format to the Domino LDAP directory format but you cannot use this utility to convert names to other LDAP directory formats. For example, you cannot use this utility to convert names from the native Domino directory format to a Netscape LDAP directory or Microsoft LDAP directory format.

• You can use this utility to make changes to individual user and group names, or make organizational unit name changes to names that are currently stored in buddy lists and privacy lists in any directory format supported by the Sametime server. For example, you can make these types of name changes to user or group names that are stored in the native Domino directory server or any LDAP directory format that is supported by Sametime (such as IBM, Netscape, or Microsoft LDAP directory formats).

• When you change a user’s name in the directory, be sure to run this utility to also change the name in the vpuserinfo.nsf database BEFORE the user logs into the Community Service using the new name.

   If the user logs in with the new name, and then you later run this utility to convert the user’s name in the vpuserinfo.nsf database, the vpuserinfo.nsf database will contain two separate records with the same userID. In this situation, the administrator must manually delete one of duplicate records from the vpuserinfo.nsf database.

• If a Sametime server accesses two (or more) Domino directories, and these directories are converted from the native Domino directory format to the Domino LDAP directory format, the administrator should be aware of the following issue concerning groups that have the same name in both directories. When you run the conversion utility to convert the names in the vpuserinfo.nsf database from the native Domino format to the Domino LDAP format, only the group from one Domino LDAP directory will exist in the lists in the vpuserinfo.nsf database after the conversion completes.

   This problem occurs because groups with the same names in multiple LDAP directories have the same GroupID.

• The following issue applies if users authenticate to a Domino 6.0.2 LDAP directory when logging into the Community Services.

   If you use this utility to change a user’s name, and the changed user name includes any of these special characters (",","="","+","<","="","#",""), the changed
user’s buddy lists and privacy lists will be lost after the name conversion. The user must recreate the buddy lists after the name conversion.

This problem occurs because of the way that the special characters are handled by the Domino authentication process. This problem is not seen with Domino 5 LDAP directories.

- When creating a name change rule in the NameConvUtil.txt file to change a user name, be sure that the name change rule uses the full version of the user’s name as it exists in the vpuserinfo.nsf database. Do not use a shortened version of the user’s name (such as the user’s display name) when creating a name change rule.

For example, to change the user name Lisa Mane to Lisa Smith, use the full hierarchical name format in the name change rule, as shown below:

CN=Lisa Mane/OU=Haifa/O=IBM--->CN=Lisa Smith/OU=Haifa/O=IBM

Using shortened versions of the user name in a name change rule may result in unwanted user name changes due to character matching issues. For example, consider this example below of an incorrect name change rule that uses shortened forms of the user names:

Lisa Mane--->Lisa Smith

This name change rule will change the user’s display name from Lisa Mane to Lisa Smith. However, this rule will also change any other longer user names that begin with the same set of characters. For example, this name change rule would also make the following name changes:

- Lisa Manet to Lisa Smithth
- Lisa Manelli to Lisa Smithlli

To avoid these character matching issues, use the full name of the user in the name change rules.

- Be sure to stop the Sametime server before running this utility.

Alternately, you can copy the vpuserinfo.nsf database from the Data directory of an active Sametime server to a working directory and run the utility on the vpuserinfo.nsf database in the working directory. When the conversion is complete, you can stop the Sametime server and then copy the converted vpuserinfo.nsf from the working directory over the unconverted vpuserinfo.nsf database in the Sametime server Data directory.

Note that if you use this method to convert the vpuserinfo.nsf database, users may make changes to the buddy lists and privacy lists in the vpuserinfo.nsf database that is active on the Sametime server while you are performing the conversion on the vpuserinfo.nsf that you copied to the the working directory. Any buddy list or privacy list changes that users make during this time period will be lost when you replace the unconverted vpuserinfo.nsf database with the converted database from the working directory.

- Running this utility to change user names or group names in the group lists and privacy lists in the vpuserinfo.nsf database will not change the display name for a user in the Sametime Connect client. When the Sametime server is configured to access a native Domino directory, the Sametime Connect client uses the topmost entry in the "User name" field of the user’s Domino directory Person document as the display name. When the Sametime server is configured to access a Domino LDAP directory, the display name is determined by the "Attribute of a person entry that defines the person’s name" setting in the LDAP directory -Basics settings of the Sametime Administration Tool.
Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Office 4360
One Rogers Street
Cambridge, MA 02142
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

**Trademarks**

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
the IBM logo
1-2-3
AIX
AS/400
DB2
Domino
Domino Designer
iNotes
i5/OS
Lotus
Lotus Notes
MQSeries
Netfinity
Notes
QuickPlace
Sametime
SmartSuite
S/390
Tivoli
WebSphere
Word Pro
Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

**Third Party Notices**

The Apache Software License, Version 1.1

Copyright (c) 1999-2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Xerces" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache," nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software
For DSIG base64

COPYRIGHT 1995 BY: MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT), INRIA

This W3C software is being provided by the copyright holders under the following license. By obtaining, using and/or copying this software, you agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee or royalty is hereby granted, provided that the full text of this NOTICE appears on ALL copies of the software and documentation or portions thereof, including modifications, that you make.

THIS SOFTWARE IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. COPYRIGHT HOLDERS WILL BEAR NO LIABILITY FOR ANY USE OF THIS SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

For STLport

License Agreement

Boris Fomitchev grants Licensee a non-exclusive, non-transferable, royalty-free license to use STLport and its documentation without fee.

By downloading, using, or copying STLport or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of the United States of America, and to all of the terms and conditions of this Agreement.

Licensee shall maintain the following copyright and permission notices on STLport sources and its documentation unchanged:

Copyright 1999,2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the
code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The Licensee may distribute binaries compiled with STLport (whether original or modified) without any royalties or restrictions.

The Licensee may distribute original or modified STLport sources, provided that:

The conditions indicated in the above permission notice are met; The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met:

Copyright 1994 Hewlett-Packard Company


Copyright 1997 Moscow Center for SPARC Technology.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 2001 by STLport

For MD5 hash

Copyright (C) 1990, RSA Data Security, Inc. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.
RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

For Log4J Logging


The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."
   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.
Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.
Index

**Numerics**

360 degree video camera  373

A

Access control  client version and  248
EMS  593
Access Control  EMS  499
Access Control Lists
Access Level  411
adding a name  410
anonymous access  415, 416
basic password authentication  417, 418
identification and authentication  103, 409
Privileges  411, 413
Roles 45, 411
setting for administrator access  41
settings  411, 412, 413, 415
User Type  411
using  409, 410
Access Level
ACL  411, 412
Active meetings
monitoring  378
Active places
number on server, monitoring  375
Adding a new administrator 40, 41, 43, 60, 103
database roles  45
Adding a new Sametime server  449, 451, 452, 455, 456, 457, 460
Adding an administrator  39, 44
Adding an LDAP server  77
Adding the names of participants to the meeting document  308
Adding users from the Sametime Administration Tool  56
Adding users in the Domino environment  53
Additional Sametime servers  449, 451, 452, 455, 456, 457, 460
Addresses
collision of  151
Administrative tasks  30, 31, 32, 33, 34, 35, 36
Administrator
adding  40, 60
setting database roles for  45
Administrator distinguished name  75
Agent access to the Domino Directory  52
Agents
Same time signer and directory access  52, 55
Allow Connect users to save their user name, password, and proxy information (automatic login)  240
Allow people to choose the Polling tool in meetings  313
Allow people to enable the Send Web Page tool in meetings  312
Allow people to record meetings for later playback  314
Allowing or preventing broadcast meetings  314
Allowing people to choose Same time IP audio in meetings  352
Allowing people to choose the screen sharing tool in meetings  309
Allowing people to choose the whiteboard tool in meetings  311
Announcements
disabling  239
enabling or disabling in the EMS  649
unencrypted  239
Anonymous access  406, 415
ACLs  415, 416
allowed by default in EMS  593
Community Services  242, 243, 406
Same time databases  406
security roles in the EMS  593
setting up in a database ACL  416
to LDAP directory  75
turning off  407
Attribute  81, 82, 83, 86, 91
Audio  10
bit rate  358
cutting out  324, 349, 361, 362
delay  349
frames per packet  349, 362
Audio/Video  24, 341, 346, 347, 351
client requirements  342
clients  346
configuration  34, 350, 351, 355, 358, 365, 651
connection speed settings  360
connection speed settings in the EMS  650
disabling 351, 352, 353
EMS  651
jitter buffer  349, 361
Network and Port settings  153, 154
ports  123, 154, 455
prioritizing data  372
server components  346, 347
switching  353, 354, 355
TCP tunneling  208
tips for using  143, 339, 374
with SIP  301
Authentication  72, 87, 88, 95, 105
by token  419, 420, 428
client certificates with the SIP Gateway  298
Domino SSO, setting up  424
EMS  499, 593
Authentication (continued)
LDAP settings  75
Name and Password  424, 425
setting up a database ACL  417
tokens  237
with Sametime server  93, 401
Automatic login  240
disabling for Sametime Connect  240
Automatic microphone mode  347
Automatically extending meetings beyond the scheduled end time  308
B

Bandwidth  344, 349, 350, 364, 366, 367, 368, 369, 370, 371, 449
Basic password authentication  417, 418
setting up a database ACL  417, 418
Basics settings for LDAP  72, 78, 79, 80, 81, 82, 84, 85, 86
Bit rates
for audio and video streaming  360
Booking Agent  494, 575
Breakout sessions  5
Broadcast  15
Broadcast client  332
360-degree video streams and  373
connectivity  137, 148, 176, 188, 332
EMS  498
logging  389
Broadcast client connection process using Sun Microsystems JVM  176, 177, 188
Broadcast Gateway  147, 148, 331
connections to on server  375
control port  146
port  146
Broadcast Services  15, 23, 328, 335
Broadcast client  331, 332
client connection settings  146, 148
configuration  35, 335
EMS  498, 652
jitter buffer  351, 355
multicast and  151
network and ports settings  129, 137, 146, 147
network bandwidth usage  375
ports  123
server components  331
Small Group Multicast and  148
Browsers  19, 600
Buffering
Audio/Video streams  349
broadcast streams  332
C

Camera  342
connecting for video streaming  373

© Copyright IBM Corp. 2005

679
Capacity warnings
logging 393, 399
viewing in Meeting Services
clusters 641
Cascaded directories 457
Certificates 600
Changing a user’s password 57, 405
Chat 4
- capturing conversations 252
- logging 252
- Meeting Room client 4
- pop-up chat window placement 246
Chat window
screen placement and size 246
Client certificate authentication
for the SIP Gateway 298
client version level
and server access 248
clients
security level and 248
Clients 19, 342
Broadcast services 146
Community Services 133
EMS connectivity configuration 647
Meeting Services 142, 153
Cluster document
Community Services 517
Clustering
Community Services overview 487
Meeting Services 509
types of Sametime server
clusters 483
Codec 344, 347, 355, 358, 359
Collaborative activities 3
chat 4
hand raise 8
IP audio 10
IP video 10
meetings 4
polling tool 8
presence 4
screen sharing 6
Send Web Pages Tool 7
transferring files 9
whiteboard 6
Community 13
extending across multiple Domino
domains 472, 473, 474, 477
Community logins/logouts
logging 383
Community Services
Anonymous Access Settings 242
custom connection settings 133
configuration 33, 232, 234, 235, 236
connecting to 155, 179
file transfer feature 238
logging 398
logging server events 385
monitoring 378
multiplexer 131, 132, 135, 253, 511, 512, 513
Network and Ports settings 129, 132, 137
overview 231
ports 123
server connection settings 132
single-server vs. clustering 487
Community Services (continued)
users 375, 384
Community Services clustering 487
adding a server 506, 521
compared to single-server
approach 487
configuring from the EMS
Administration Tool 649
creating 504, 505, 506, 508, 509, 511,
515, 517, 519
failover 490
load balancing 490
Community statistics
logging 384
Compatibility
with previous releases 137
Configuration
Audio/Video Services 34
Broadcast Services 35
Community Services 33
Connectivity 129
Meeting Services 34, 306
Network and Ports settings 129
Ports and Network 32
Configuration database 109
Connecting 214, 215, 390, 452
Connection Documents
creating 474
Connection processes
Sametime clients 158, 165, 176
Connection Records
creating 458, 460, 477
Connection Speed Settings 324, 326, 328,
347, 350, 355, 356, 357, 358, 359, 361,
362, 364
Broadcast Services 324, 335
default settings for meetings 326, 357
LAN/WAN 355, 356
modem 355, 356
Connectivity 15, 32, 153, 465, 468
EMS 498, 647
from the Internet 463, 464, 465, 468
Sametime clients 129, 133, 159, 464,
465, 468
Sametime Connect for browsers 171
with a Community Services
cluster 519
Connectivity settings for LDAP 72, 74,
75, 77, 92
Cross-certification
Sametime servers and 473
Custom Logon form
for SSO 427
D
Data source, creating for EMS 559
Database size
logging 394
DB2 491, 496, 539, 556
Default domain for anonymous
users 244
Default name 244
Delay
audio 344, 349, 361, 362
Denied entries
logging 394
Denied entries (continued)
setting for a Meeting Services
cluster 651
Directory
Domino 14
LDAP 14
LDAP, with the EMS 500
managing for multiple servers 50,
457
replicating to different domains 474
Directory Assistance 50, 67, 68, 96, 105,
106, 457
setuping 474
Directory entry
group or person 82, 86
Directory Searching and Browsing
(Anonymous Access Settings) 245
Discussion databases
unavailable with EMS 637
Disk space
logging 394
monitoring 380
Display name 242, 244
in EMS environments 649
DNS base name
bound to HTTP server 201
Domino Directory 14
adding a group 57
deleting a group 58
deleting users 57
managing in the Domino
evironment 49
multiple directory environments 50
roles 46
security considerations 52
sharing Directory information across
domains 479
single directory environments 49
user management 31, 61
Domino domains 472, 473
Sametime and multiple domain
environments 472, 473, 474
Domino log 394
unavailable in EMS 637
Domino Services 21
Domino Web Administration database
roles 47
Domino Web Administration pages
monitoring 380
Duplex 344

E
EAR file, deploying for the EMS 563
Editing a group 59
EMS
adding servers to the Meeting Services
cluster 566
administering 637
administering Broadcast Services 652
administering LDAP with the
Sametime Administration Tool 647
Booking Agent 494
client connectivity 498
configuring Audio/Video
Services 651
configuring connectivity 647
configuring Meeting Services 650
creating a WebSphere server for the
EMS administration tool 553
creating JMS system queues 547
creating MQSeries queues 557
creating the data source 559
creating the DB2 database 556
creating the JMS Destinations 561
defined 491
deploying the SameTime.ear file 563
deployment procedures 553
decrypting HTTP traffic between the
EMS and the SameTime servers with SSL 621
decrypting Web browser connections
with SSL 600
decrypting user experience 497
health monitoring 495
installing DB2 539
installing files for 556
installing J2EE infrastructure 537
installing MQSeries 540
installing MQSeries SupportPac
matc 543
installing the JMS Connection
Factory 560
installing WAS 4.0 544
installing WAS 4.0 FixPack 3 545
load balancing for meetings 493
logging 641
meeting materials 496
message from the administrator 639
monitoring 639
overview of the LDAP directory
access 500
overview of security issues 499
regenerating the WebServer
plugin 565
securing user access 593
security roles 593
setup procedures 528
synchronizing SSO support for the
c cluster 567
usage limits for Meeting Services
clusters 575
Enable a H.323 gatekeeper 153
Enable H.323 server communication 153
Enable HTTP tunneling
Broadcast Services 146
Enable Reverse Proxy Discovery on the
client 226
Encryption 314, 431, 621
crypting Web browser connections
to the EMS with SSL 600
for SIP Gateway 286
SSL and LDAP servers 92, 93, 95, 96,
97, 432
End user features of Sametime 3
error message reporting 653
Event server port
described 145
Exporting recorded meetings 321
Extended Server Directory Catalog 50
Extending meetings 308

Failed meeting logins
logging 399
Failover
d end user experience with the
EMS 497
in Community Services clusters 490
meeting materials with the EMS 496
File transfer feature 9
enabling 238
Firewalls 15, 455
connection with HTTP protocols 159
HTTPS connections and 135
restrictive 201
Format
SameTime log 397

General configuration settings
Meeting Services 307
Group 57, 58, 59
Group Content settings for LDAP 91
group document 60
creating 57
ing 59
for administrators 41, 60
Group object class
attributes 86

H.263 344
H.323 341, 344, 349
360-degree camera and 373
client connectivity 153
gatekeeper 153
logging client connections 389
H.323 server communication port 153
Half duplex 344
Health monitor (EMS-only) 495
Home page
SameTime server 2, 11
Home SameTime server 59, 69, 155, 457
LDAP 88
Host name or IP address of Community
Services 132
Host name or IP address of the LDAP
server 74
HTTP port 123
HTTP server
bound to base DNS name 201
configuring the IBM HTTP server to
support SSL with the EMS 605
HTTP Services
Network and Ports settings 129, 131
HTTP task
SSO-enabled server and 426
HTTP tunneling 193
Community Services client
connections 137
enabling and disabling 132, 201
Meeting Services client
connections 143
HTTP tunneling (continued)
multiple IP addresses 200, 201, 202,
203
ports 131, 137, 146, 194, 201, 202, 203
settings, explained 195
single IP address 195
HTTPS tunneling
Community Services client
connections 135
IKeyMan
using to manage SSL certificates with
the EMS 600
Instant meetings
home server and 155
Instant messaging
SIP-enabled communities and 17
Internet
access to internal servers 215, 449,
455
extending Sametime 463
passwords 59, 405
Invited servers 452, 460
IP addresses
assigning for multiple servers 214
assigning multiple for HTTP
tunneling 200, 201, 203
Community Services 132
for Small Group Multicast (SGM)
router 146
H.323 gatekeeper 153
mapping to DNS names 202
multicast 151
J2EE
and the Sametime EMS 491
installing infrastructure for EMS 537
Java Plug-in Control Panel 177
JDBC
creating data source for EMS 559
Jitter buffer 349, 361
broadcast 332, 351, 355
management 344
JMS
and health monitor 495
and the Sametime EMS 491
creating JMS Destinations for the
EMS 561
creating system queues for EMS 547
installing the Connection Factory 560
JNDI
and the Sametime EMS 491
Keys
synchronizing SSO support for
Meeting Services clusters 567
kiosk mode 259
LAN/WAN connections 355
Latency 344, 349, 361, 362
LDAP 505
  adding and removing servers 77
  administering from EMS Administration Tool 647
  administration 65
  authentication 65, 75
  connectivity 65, 74
  Home Sametime server 88
  overview of directory access with the EMS 500
  reference material 73
  searches 65, 112, 116
  using SSL 77, 96
  using with Sametime 63, 65
  using with server clusters 505
LDAP Authentication settings 65, 72, 87, 88
LDAP Basics settings 65, 72, 78, 79, 80, 81, 82, 84, 85, 86, 116
LDAP Connectivity settings 65, 67, 68, 72, 74, 75, 77, 95, 104
LDAP Directory 14, 31, 52, 103
LDAP directory search behavior
  controlling with Java classes 112, 116
LDAP Directory Settings 69, 72
LDAP document
  creating 109
  LDAP Group Content settings 65, 72, 91
  LDAP ports 123
  LDAP Searching settings 65, 72, 89, 90
  LDAP server
  connecting to 67, 92, 104, 109
  LDAP server transmissions encryption 95, 97
LDAP settings
  accessing 74, 78
  LDAP, setting up (Domino environment) 67, 69, 104, 105, 106
  Lightweight Third Party Authentication (LTPA) tokens 420
Limiting server access 236, 350, 364, 365, 366, 367, 368, 369, 370, 371
Limits
  logging usage limits 394
  log balancing 449, 515, 523
  in Community Services clusters 490
  scheduling meetings on the Sametime EMS 493
Logging 16, 31
  Broadcast client connections 389
  capacity warnings 393, 399
  chat conversations 252
  Community logins/logouts 383
  Community server events 385
  Community Services 398
  Community statistics 384
  database size 394
denied entries 394
disk space 394
Domino log 394
general settings 396
H.323 client connections 389
invited servers 390
message events 391
Logging (continued)
  meeting login failures 388
  Meeting Room client connections 389
  Meeting Services 399
  meeting statistics 390
  place login failures 386
  Sametime activity 383
  Sametime statistics 398
  server memory 394
  server performance 394
  server to server connections 390
  settings 396, 397, 399
  settings for Community Services 398
  settings for Meeting Services 399
  T.120 client connections 389
  usage limits 394
Logins
  to Community Services 378, 383, 384, 398
  Logon form
    custom, for SSO 427
Logouts
  from Community Services 383, 398
  Lotus Notes 19
  LTPA
    synchronizing SSO support for
      Meeting Services clusters 567
  LTPA tokens 420, 429
Meeting Services 23
  accessing configuration settings 306
  client connection settings 142, 143, 153
  clustering and the Sametime EMS 490
  configuration 34, 306
  configuring for Meeting Services clusters 650
  connecting to 179
  Connection Speed Settings 326
  General configuration settings 307
  logging meeting events 391
  logging meeting statistics 390
  meeting login failures 388
  overview 305
  ports 123
  server connections 141, 215
  usage limits and the EMS booking agent 494
Meeting Services cluster deployment procedures 553
Meeting Services clustering
  adding servers to the cluster 566
  administering LDAP from the Sametime Administration Tool 647
  booking agent for meetings 494
  client connectivity 498
  configuring Community Services within a Meeting Services cluster 649
  configuring Meeting Services in a cluster 650
  creating 506
  health monitor 495
  installing J2EE infrastructure 537
  introduction 490
  load balancing 493
  logging 641
  monitoring 639
  scheduling meetings 493
  setup procedures 528
  synchronizing SSO support 567
  usage limits for servers in the cluster 575
Meeting Services events
  logging 391, 399
Meeting Services network
  Network and Ports settings 129, 140, 143
MeetingPlace server
  features not available with the EMS 637
Meetings
  booking with the Sametime EMS 494
  broadcast 15
  extending to Internet users 215
  instant and scheduled 4
  load balancing with the Sametime EMS 493
  locating in Meeting Center 37
  logging meeting events 391
  logging meeting statistics 390
  on server, monitoring 375
  online 4
  recorded 315
Message From Administrator 30
Network and Ports settings (continued) 129
Interactive Audio/Video 129, 153, 350, 351
Meeting Services network 129
Network Dispatcher
in Community Services clusters 490
NIC cards
adding 201
assigning IP addresses to 201
Notes 19
Number of entries on each page in dialog boxes that show names in the directory 234
Number of participants
monitoring 378

O
Object class
person 82
Overview of the SameTime Administration Tool features 28

P
Password 59
changing 57, 405
encrypting with SSL 93
for user authentication 402, 419
logging meeting password failures 388
meeting 315, 431
requiring for all scheduled meetings 315
requiring for database access 417, 418
People can attend from inside the organization 460
People can attend from the Internet 460
Performance optimization 37, 151, 201, 324, 339, 449
Person document 59, 402
editing 57
Places
logging 386
Plugin
regenerating the WebServer plugin 565
Polling
availability in meetings 313
Polling tool 8
Port 80 tunneling 129, 194, 201, 205
Ports 123
Audio/Video Services 123, 455
Broadcast Services 123
Community Services 123
event server 145
for LDAP connections 75
HTTP 123
LDAP 123
Meeting Services 123
Multimedia Services 455
numbers 123
server to server connections 455
SSL 123
token server 145
Ports (continued)
UDP 123
Position of this server in the search order 74
Presence 4, 232
Presence lists 4
Prioritizing Audio/Video data 372
Privileges
ACL 411, 413
Proxy servers 15, 146
Proxy support 15, 128, 146
Public group
adding or removing users 59
creating 57
deleting 58
Purge Meetings agent 37

Q
Queues
creating JMS Destinations 561
creating JMS system queues for the EMS 547
creating MQSeries queues for the EMS 557
installing MQSeries 540
installing the MQSeries Connection Factory 560

R
Real-Time Control Protocol (RTCP) 344
audio and video streams and 153, 360
Real-Time Streaming Protocol (RTSP) 344
Broadcast Services and 146, 148
Real-Time Transport Protocol (RTP) 344
Meeting Services and 153
Record and Playback
availability in meetings 314
Recorded meetings
availability on the server 317
deleting 319, 320
exporting 319, 321
importing 319, 322
invited servers 319
managing 315, 319
managing in an EMS environment 650
replacing 319, 322
Recording meetings 314
Request microphone mode 347
Require all scheduled meetings to have a password 431
Requiring all scheduled meetings to have a password 315
Restarting the SameTime server 25
Restarting the server 25
Reverse proxy support 216
affinity id (server alias) 221
configuring reverse proxy mapping rules 221, 222
enabling on a SameTime server 226
requirements and limitations 217
SameTime client connectivity 227
Sametime log (continued)
capacity warnings 393
Community logins/logouts 383
Community server events 385
Community statistics 384
database size 394
disk space 394
Domino log 394
EMS 641
format 396, 397
general settings 396
meeting events 391
meeting login failures 388
meeting room client connections 389
meeting statistics 390
place login failures 386
server memory 394
server performance 394
server to server connections 390
settings 396, 397
usage limits 394
Sametime Meeting Center 11
password authentication 237
restricting access for meeting managers and attendees 60
turning off anonymous access 407
Sametime Meeting Room client 20, 349
connectivity 153
Sametime Multimedia Multipoint Control Unit prefix 153
Sametime server
activity logging 383
authenticating with 401
checking status of 375
cross-certifying 473
defined 12
installing 2, 67
starting and stopping 25
using LDAP with 63, 97
Sametime servers
deploying multiple servers 36, 235
Sametime services 21
Sametime terms and features 12
Sametime tokens 429
Saving the whiteboard 6
Scope for searching for a person 80
Scope for searching for groups 85
Screen sharing 6
security 471
Screen sharing and whiteboard bit rate for broadcast meetings 328
Screen sharing tool 6
availability in meetings 309, 324
Search filter for resolving group names 90, 112
Search filter for resolving person names 89, 112
Search filter to use when resolving a user name to a distinguished name 87
Search result
group or person 82, 86, 116
Searching settings for LDAP 72, 89, 90, 112
Secrets and Tokens authentication database 419, 428, 429
Security 17, 401
anonymous access 416
Security (continued)
Domino Directory security considerations 49, 52
encrypting HTTP traffic between the EMS and the Sametime servers 621
encrypting meetings 314
encrypting Web browser connections to the EMS with SSL 600
cryptography 93, 431
for client connections 248, 401
for Web browser connections 408
Internet access 449
Internet password 402
managing 36
managing SSL certificates with the EMS 600
meeting materials with the EMS 496
meeting passwords 431
Person document 402
requiring a password for all scheduled meetings 315
restricting access for meeting managers and attendees 60
roles in the EMS 593
Self Registration 55, 430
synchronizing SSO support for Meeting Services clusters 567
user access to the EMS 593
Security filtering
client version level and 249
Security level
client logins and 250
effect on incoming server connections 249
setting 249
Self Registration 14, 155, 430
enabling 54
security considerations 55, 402, 430
using in the Domino environment 54, 55
Send Web Page
availability in meetings 312
Send Web Pages tool 7
Server Alias 226
Server document
modifying for administrator access 43
required fields 61
Server memory
logging 394
monitoring 380
Server Overview feature 30
Server performance
logging 394
Server to server connections 131
Broadcast Services 147
Community Services 132
logging 390
Servers
adding to a Meeting Services cluster 566
connecting Meeting 215
connections to, monitoring 375
stopping and starting 25
Servers in this Community 460
Servers, multiple 2
connecting services 214

Sametime Administration Tool 12
adding a new administrator 39
Broadcast Services in an EMS environment 652
configuration settings, storing 61
configuring Audio/Video Services in an EMS environment 651
configuring Community Services for Meeting Services clusters 649
configuring connectivity for Meeting Services clusters 647
configuring Meeting Services in an EMS environment 650
creating a WebSphere server for (EMS only) 553
for the EMS 637
logging in Meeting Services clusters 641
managing users 55
starting 27
user name and password requirements 27
using in an LDAP environment 65, 103
Sametime basics 3
Sametime Broadcast client 21
Sametime Community 13
Sametime Connect client 19, 237, 241
availability 237, 241
connection to server 158, 159, 165
cost with the EMS 498
disabling announcements 239
home server and 155
SOCKS, HTTP or HTTPS proxy connectivity 159
Sametime Connect for browsers client changing default connectivity settings 171
kiosk mode 259
Sametime Links
announcements and 239
file transfer and 9
Sametime log
as database or text file 397

S
Sametime Administration Tool 12
adding a new administrator 39
Broadcast Services in an EMS environment 652
configuration settings, storing 61
configuring Audio/Video Services in an EMS environment 651
configuring Community Services for Meeting Services clusters 649
configuring connectivity for Meeting Services clusters 647
configuring Meeting Services in an EMS environment 650
creating a WebSphere server for (EMS only) 553
for the EMS 637
logging in Meeting Services clusters 641
managing users 55
starting 27
user name and password requirements 27
using in an LDAP environment 65, 103
Sametime basics 3
Sametime Broadcast client 21
Sametime Community 13
Sametime Connect client 19, 237, 241
availability 237, 241
connection to server 158, 159, 165
cost with the EMS 498
disabling announcements 239
home server and 155
SOCKS, HTTP or HTTPS proxy connectivity 159
Sametime Connect for browsers client changing default connectivity settings 171
kiosk mode 259
Sametime Links
announcements and 239
file transfer and 9
Sametime log
as database or text file 397
Servers, multiple (continued)
example configuration 214
  integrating new server 215
  on single machine 141, 145, 214
Services
  Sametime 21
Session Initiation Protocol (SIP) 265, 267, 254
Set a maximum number of audio connections for all broadcast meetings 370
Set a maximum number of data connections for all broadcast meetings 369
Set a maximum number of interactive audio connections for all instant meetings 366
Set a maximum number of interactive video connections for all instant meetings 366
Set a maximum number of video connections for all broadcast meetings 371
Set dialog as default 246
Settings
  Sametime log 396
SGM router
  IP address 148
Shared whiteboard 6
SIP 265, 344
SIP Connector 17, 267, 272, 275
SIP Gateway 17, 267, 272
  client certificate authentication 298
  disabling 286
  enabling 270, 272, 274, 275, 276
  TLS encryption 286
SIP/SIMPLE protocol 17, 267
Small Group Multicast (SGM) router
  IP address 148
Sound card 342
SSL 440, 600, 605, 621, 626, 628
  EMS 600, 605, 621, 626, 628
  for servlet access 440
  ports 123
  using with LDAP 77, 92, 93, 96, 97
SSO authentication 419, 428
  custom logon form for 427
  setting up on Sametime server 424, 425, 426
  synchronizing for Meeting Services clusters 567
Starting the Sametime Administration Tool 27
Starting the Sametime server 25
Statistics
  Community Services 384, 398
  logging chat, meeting, and user 398
  logging meeting statistics 390
  monitoring 380
StddebugTool 653
Stopping the Sametime server 25
Switching
  audio 362
  video 347
Synchronizing multiple Sametime servers 456, 457, 460
System requirements
  J2EE infrastructure for the Sametime EMS 491
T
  T.120 client connections
    logging 389
  T.120-compliant clients
    Meeting Services and 141
    TCP Tunneling 153, 208
    described 153
    TCP Tunneling port 153
    TCP/IP connection
      client to server 133
      Sametime Connect client 159
    TeamRoom databases
      unavailable with EMS 637
    Templates
      included in Sametime 2
    Three hundred and sixty-degree video camera
      using with Sametime 373
    Time to buffer broadcast data, audio, and video 351, 355
    Time to live 146
    Time To Live (TTL) 333
    Time to live (TTL) setting
      multicast 151
    Time to wait before switching video 347, 351, 354
    Time to wait for silence before switching to next speaker 347, 351, 353
    TLS 286
    Token server port
      described 145
    Tokens
      LTTP or Sametime 237
    Toolkit
      logging for Toolkit places 386
    Tools in meetings
      monitoring 379
      trace file 653
    Transport Layer Security 286
    troubleshooting 653
    TTL 333
    TTL setting
      multicast 151
    Tunneling on port 80 129, 201, 205
      configuring 201, 205
    Type of Connection Speed Setting to use for the default 357
Usage limits
  and the EMS booking agent 494
  for Meeting Services clusters 575
  logging 394
  setting for Meeting Services clusters 651
Usage Limits and Denied Entry 350, 364, 365
  broadcast meetings 365, 369, 370, 371
  instant meetings 365, 366
  scheduled meetings 365, 367, 368
Use multicast 146
Use my Internet Explorer browser settings 165
Use my Internet Explorer HTTP settings 165
Use my Java Plug-in settings 165
User Datagram Protocol (UDP) 344
User management 31, 52, 56, 57, 59
  assigning users to a new Sametime server 457
  Domainino environment 49, 55
User Type
  ACLs 411
Users
  access to Sametime home page 2
  Community Services 384, 398
  Users can browse the directory 245
  Users can get group content 245
  Users can participate in meetings or enter virtual places 243
  Users can type names to resolve them 245
  Users have no access to the directory 245
  Users of Sametime applications can specify a display name 244
  Using the servers in this community settings 215
V
Video 10
  disabling 351
  pause in 324
  switching 354
Video bit rate 359
Video streaming
  with 360-degree camera 373
Video window
  docking or floating 373
Views
  required for online presence 61
Virtual places
  logging 386
W
Warnings
  log settings 399
  logging capacity warnings 393
Web Application Services 21
Web browser 19
  security 105, 408, 420, 432
Web SSO document
  creating 424
Web statistics
  monitoring  380
WebServer plugin, regenerating  565
WebSphere
  creating a server for the EMS
    administration tool  553
  creating data source  559
  creating the DB2 database for the
    EMS  556
  deploying the Sametime.ear file  563
  installing the JMS Connection
    Factory  560
  installing WAS 4.0 Fixpak 3 for the
    EMS  545
  installing WAS 4.0 for the EMS  544
  regenerating the WebServer
    plugin  565
  securing user access to the EMS
    security roles  593
  synchronizing SSO support for
    Meeting Services clusters  567
WebSphere Edge Server
  in Community Services clusters  490
Welcome to Sametime page  11
What is Sametime  1
Where to start searching for groups  84
Where to start searching for people  79
Whiteboard  6
  availability in meetings  311, 324, 339
  saving  6