

Lotus. software



Lotus Sametime 3.1 and Enterprise Meeting Services 1.0



Release Notes

Disclaimer

THIS DOCUMENTATION IS PROVIDED FOR REFERENCE PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS DOCUMENTATION, THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER AND TO THE MAXIMUM EXTENT PERMITTED, LOTUS AND IBM DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SAME. LOTUS AND IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, DIRECT, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS DOCUMENTATION OR ANY OTHER DOCUMENTATION. NOTWITHSTANDING ANYTHING TO THE CONTRARY, NOTHING CONTAINED IN THIS DOCUMENTATION OR ANY OTHER DOCUMENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM LOTUS AND IBM (OR THEIR SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENT GOVERNING THE USE OF THIS SOFTWARE.

Copyright

Under the copyright laws, neither the documentation nor the software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, without the prior written consent of IBM Corporation, except in the manner described in the documentation or the applicable licensing agreement governing the use of the software.

Licensed Materials - Property of IBM

© Copyright IBM Corporation 1985, 2003

Lotus Software
IBM Software Group
One Rogers Street
Cambridge, MA 02142

All rights reserved. Printed in the United States.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GS ADP Schedule Contract with IBM Corp.

Revision History:
Original material produced for IBM Lotus Sametime Release 3.0.

List of Trademarks

IBM, the IBM logo, AIX, AS/400, iSeries, OS/2, OS/2 Warp, S/390, Tivoli, WebSphere, z/OS, and zSeries, Lotus, cc:Mail, Domino, Freelance, Freelance Graphics, Lotus Notes, LotusScript, Notes, 1-2-3, Organizer, Quickplace, Sametime, SmartIcons and SmartSuite are trademarks or registered trademarks of IBM 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.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

MMX and Pentium are trademarks of Intel Corporation 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 and service names may be trademarks or service marks of others.

Chapter 1 - What's new?	1
Welcome	1
Welcome to Lotus Sametime.....	1
Release Notes - availability and formats	1
Lotus/IBM Web sites containing Sametime documentation	1
New Features.....	2
Chapter 2 - Things you need to know	5
Configuration servlet is not secure following installation.....	5
System requirements	7
Server administration	9
Do not use Sametime settings in the Server document	9
Changing server administration parameters.....	9
Do not replicate the Configuration (stconfig.nsf) database.....	9
Signing Sametime databases	12
Server display color setting must be higher than 256 colors	12
Domino HTTP server must use the fully-qualified host name	13
Controlling the bandwidth usage of the Sametime server	13
Joining meetings with NetMeeting	15
Chat logging on the Sametime server.....	17
Domino server installation procedures.....	17
Setting up an LDAP connection to an ActiveDirectory server	19
Supported sound cards and cameras	20
Sound cards	20
Cameras.....	20
Enabling QuickPlace or Virtual Classroom to access Sametime servlets	20
Encrypting QuickPlace or Virtual Classroom connection to Sametime with SSL	23
Sametime and QuickPlace cannot be installed on the same machine	29
Community Services administration changes can occur without server restart.....	30
Accessibility/Section 508 issues	30
Can't tab between admin client and Domino Directory access	30
Can't tab between text and Meeting Room in Meeting Tester.....	30
Cannot sort by raised hands without using mouse.....	31
Keyboard shortcut for new line on Unix clients.....	31
Missing hotkeys in Sametime Connect for the desktop client	31
Missing mnemonic in A/V Preferences dialog box	31
Mnemonics disappear during an online meeting	31
SHIFT+TAB won't move focus backward through column headers	31
Tabbing problem in Add to Privacy List dialog box.....	31
Unable to tab between admin tool and admin Help.....	32
Sametime Connection documents are case-sensitive	32
Sametime Connect and HTTPS connections on port 443 or 563	33
Enhance security by disabling RAPFileServlet	36
Sametime is not supported on IBM zSeries servers	37
Attach a meeting material immediately after installing or restarting the EMS	37
Sametime 3.1 cannot operate with Netegrity Siteminder.....	38
Notes 6 client required to use Calendaring and Scheduling with Sametime	38
No audio/video support for Sametime Meeting Room on Unix clients	38
Print Capture not available on Unix clients	38
Granting permissions using Netscape and Unix client.....	39

Required library for application sharing on Linux and Solaris systems	39
Using page up/page down keys to present whiteboard files	39
Sametime Installation Guide NSF file has updated information.....	39
Upgrading a Sametime 3.0 server connected to the EMS to Sametime 3.1	40
Chapter 3 - Troubleshooting	41
Installation Issues	41
After Sametime uninstall, reboot before reinstalling Sametime	41
Clicking Cancel while installation is copying files	41
Deleting directories following an installation failure	41
Directory has "Enforce consistent ACLs" option selected	41
Do not install Sametime multiplexer on a Sametime server	42
Installing Sametime without a fully qualified domain name	42
Ping the Sametime server before installation (verify DNS setup).....	43
Reinstalling Sametime 3.1 over an existing 3.1 installation.....	43
Replicate the Secrets database in multiple server environments.....	44
Sametime installation fails on partitioned Domino server	44
Sametime installation locates nonexistent Netscape browsers	44
Sametime server language does not match Domino server error	45
Server name cannot include invalid XML characters	45
servlets.properties file renamed during Sametime installation	45
Set the server home page following installation or upgrade	46
Sametime Connect client issues	46
Cannot add meeting participant to Sametime Connect List	46
Cannot start instant meeting if user name contains double quotes	46
Changing Sametime Connect for browsers server connectivity	46
Disable Connect auto login with multiple user Notes client	47
Do not run both versions of Sametime Connect on the same machine	48
Do not use "Short name" to log into Sametime Connect	48
Invitation indicates no available tools if Connect is closed	48
Locked DLLs require machine reboot to complete Connect install	48
Logging into STEP changes privacy settings	49
Meeting cannot be started due to error 0x8000024.....	49
No error for empty proxy fields in Sametime Connect for browsers	49
Sametime Connect display problems at 256 colors	49
Sametime Connect startup screen is upside down	49
SHIFT+ENTER not starting new line in chat message	50
User with long name is unable to log in to Sametime Connect	50
Meeting Room client issues	50
Black boxes appear when sharing some dialog boxes.....	50
Computer entering standby mode drops audio	50
Databeam Farsite files should not be attached to a meeting	51
Empty browser frame or browser crash during client install	51
Files with embedded objects distort in the whiteboard	51
Gray whiteboard, screen sharing buttons disabled, no A/V.....	52
HTML files do not display correctly in the whiteboard	52
Initial chat transcripts do not appear in instant meetings.....	52
Meeting Room client hangs when loading whiteboard/other applet	52
Menus do not pop up when accessed via mnemonics	53
Only one spreadsheet in a file converts to whiteboard format.....	53

Participant List problems with Netscape browsers	53
Repeated saves when converting multiple spreadsheet Excel file	53
Tools still available in active meetings.....	54
Whiteboard attachments and invited servers	54
Web browser issues.....	54
Admin pages do not display in Sametime Administration Tool.....	54
Available Tools do not appear with Netscape/Win 98	54
Cannot attend meetings using Netscape.....	55
Default browser information.....	55
Meeting names with quotations display incorrectly	55
Netscape does not authenticate using international characters	56
Netscape HPUX and Sun Solaris Web browsers not supported	56
Netscape locks up when resizing Administration window	56
Netscape opens empty and Notepad opens with .tmp file displayed	56
Problem with "Administer the Server" link	56
Proxy tunneling does not work with IE.....	56
Repeated prompts for Microsoft IE VM install	57
Sametime issues using Discussion database with Internet Explorer	57
SOCKS proxy limitations with the Sun JVM 1.4.1 Plug-in	58
Sun Java plug-in does not pick up SOCKS proxy from PAC file	58
Turkish locale settings not supported for EMS	59
Wrong MeetingPlace information when scheduling conference call	59
Sametime server issues.....	59
A member of a group cannot authenticate when attending a meeting	59
Access Control Lists are unavailable to the administrator	59
Accessing Print Capture help on Windows 2000 systems	60
Administration tool unavailable after restarting STPlaces	61
Broadcast connections monitoring does not show multicast users	61
Broadcast monitoring counts TCP-tunneled streams as Unicast	61
Cannot delete or edit a meeting with a telephone conference call	61
Cannot import recorded meeting	62
Cannot search by first and last names	62
Changing HTTP port of the Sametime server	63
Changing the Broadcast gateway control port.....	63
DiagnosticsFileOutput.txt file using too much disk space.....	64
Disconnections from Community Services with NAT	64
Discussion or TeamRoom database inoperable.....	65
Discussion/TeamRoom databases and Notes Clients	66
Do not use a directory name when creating a Discussion db.....	66
Do not use invalid XML characters in Sametime server names	66
Domino Capacity Monitor fails to start.....	66
Error scheduling meeting that includes telephone conference call	66
HTTPS in URL listed in the meeting details document is incorrect	67
Instant meeting fails if .tmp file type associated with Notepad	67
Invited servers require same HTTP port number for meeting links	67
Latitude MeetingPlace server does not call user back	67
Listed user name appears not active in the public group	68
Maximum online meeting password length	68
Maximum user and server connections limit off by one.....	68

Meeting name does not appear on connected (or "invited") server	68
Meetings are not recorded as expected	69
Meetings do not become active on connected ("invited") server	69
Monitoring tab info incorrect for broadcast multicast streams	69
Multicast address ranges for Broadcast Services not working	69
Must enter full server name to log on to Sametime	70
NetMeeting meetings do not extend past scheduled end time	70
New Meeting page does not display "Telephone conference call"	70
No meetings in the "Today's Meetings" view of the Meeting Center	70
Password protected ID not supported for additional server	71
Presence lists are grayed out in Discussion database	71
Renaming the stcenter.nsf database	71
Restart the server when changing logging options	71
Scheduling a telephone conference call crashes Sametime nHTTP	71
Self registered user cannot change password	71
Self registration does not work	72
STLog.nsf on invited server does not record names	72
Subscript out of range 47 error when creating repeating meetings	72
Telephone conference calls and "invited" Sametime servers	73
Turkish regional settings on Windows require VM upgrade	73
Unable to attach large whiteboard files to Sametime meetings	73
Unable to restart Sametime after Sametime Links is installed	74
Usage Limits and Denied Entry for Broadcast Meetings	74
User cannot save the whiteboard	74
User ID displays as numbers/characters in Administration Tool	75
Users only logged into a database cannot be invited to a meeting	75
Using Lotus Notes client stops Domino processes on Sametime	75
Using self-registration with multiple Sametime servers	75
Using "Alt+159" accented characters with user registration	75
Verifying the version number of a Sametime server	76
Wrong meeting start time displays when importing a meeting	76
"Connection Broken" message for Java Sametime Connect logouts	76
"Message received when inviting others to a meeting"	77
"Sametime server (no node name config)" in NetMeeting or ST Log	77
Audio/Video services issues	77
Echo cancellation in multiple a/v meetings	77
NetMeeting video window freezes	77
Poor audio quality with G.711 audio codec and TCP Tunneling	78
Unable to join audio/video meeting with NetMeeting	79
LDAP issues	79
Administrator cannot attend meetings or use Sametime databases	79
Can't add groups from Domino LDAP directory to presence lists	79
Configuring LDAP directory settings after installation	80
Group members in Exchange server LDAP directory not online	80
Sametime Connect 2.0 or higher required in LDAP environments	80
Security issues	80
Tokens are not deleted from Sametime tokens database	80
Web browser authentication with cascaded address books	81
Software Development Kit issues	81

Location of Software Development Kit release notes	81
Problem using "Extended Live Names" Sametime C++ Toolkit sample	81
Problem with Links Toolkit "Place-based Awareness" sample	82
Problems running Sametime Java Toolkit samples	82
Outlook issues	82
Changing password in Outlook	82
Enterprise Meeting Server issues	82
Anonymous moderator unable to edit meeting (Japan EMS)	82
Any user can replay a password-protected recorded meeting	82
Cannot reattach an edited whiteboard file	83
Cannot search for meetings with DBCS file names with NS 4.51	83
DBCS names for whiteboard files do not display correctly	83
Eastern Europe accented characters cause WebSphere login failure	83
EMS users cannot browse the LDAP directory	83
Group names cannot contain DBCS characters (for EMS)	84
Installing JMS providers for EMS on Spanish WebSphere	84
Installing JMS Providers with Asian language servers	84
Meeting materials are not deleted from EMS DB2 database	85
Meeting materials are not deleted	85
Name with DBCS characters cannot log into the Meeting Center	85
Optimizing EMS page loading performance	85
Recorded meetings are not sorted by status	85
Restarting Sametime server after changing admin settings	86
Sametime/Domino HTTP port is set to Redirect to SSL	86
Start the stadmin application server before Sametime server	87
Unable to install the EMS files from a network drive	87
Update security configuration failed message for LDAP	87
User with a person entry in Domino Directory cannot authenticate	88
UNIX client issues	89
Anonymous meeting attendees cannot login and reattend a meeting	89
Application sharing on Unix systems - known issues	89
Changing a user's online status on Linux and Solaris systems	89
DBCS limitations/known issues with Sametime Unix/Linux clients	89
Limitations/known problems with AIX clients	89
Limitations/known problems with Solaris clients	90
Limitations/known problems with Linux clients	91
Dialogs do not always stay on top in the window stacking order	92
Font properties file needed for some languages	92
Frame-sharing limits on Unix systems	93
Limited resources can cause the browser to terminate	93
Log on to Sametime dialog problem with Sametime Connect on Linux	93
Menu items with checkboxes on Linux and Solaris systems	93
Problem selecting menu items on Linux client with Netscape	93
Using the Undo Full Screen button with Linux Meeting Room client	93
Chapter 4 - Documentation updates	95
Help	95
Online and print documentation	95
A broadcast meeting that uses NetMeeting as a tool	96
Audio and video not included in every meeting by default	96

Default file locations not listed for all operating systems	96
Do not use "Print to file" with Sametime Print Capture	97
External users not accessible via Sametime 3.0	98
Incorrect mnemonics listed for the Tools menu	98
Incorrect statement about private Discussion documents	98
Meeting time during a broadcast meeting	98
Mnemonics not listed for private chats in the Meeting Room	98
Plug-in for NetMeeting Meetings using Netscape is not available.....	99
Sametime 3.0 User's Guide index entry should be Sametime 3.1	99
The Help of My Meetings' description should be modified	100
Tools still available in active meetings.....	100
Use Ctrl + Enter keys to begin a new line in a chat message	100
User cannot see list of sent Web pages	100
Warning message does not mention Lotus	100
Administrator's Guide.....	101
Cannot attend audio/video meeting if video limit is reached	101
Discard the ReleaseNotes.txt file	101
Enabling self registration correction	101
LDAP setup does not overwrite an existing da.nsf database	101
Meeting passwords required for stmanager and stattend roles.....	102
Network card requirements for Community Server connections	102
No lower limit for Community server connections	102
Replace the add_meeting_cluster.xml file when updating the EMS.....	103
Users of Sametime Links can respond to announcements	103
Installation Guide	103
Administrator name/password not specified during installation	103
Check for nserver to see if Domino is running.....	103
Community Services Multiplexer invalid	104
Disable Domino DNA when upgrading from 2.5 to 3.1	104
System requirements corrections	104
v2.6 reference must be changed to 3.1 in install guide	104
Provide feedback for Sametime documentation	105
Chapter 5 - Interoperability	107
Sametime 2.5 - Sametime 3.0 compatibility	107
Accessing help in a mixed environment	107
Sametime Connect 2.5 and 3.0 compatibility issues	107
Sametime Connect for browsers interoperability	107
Chapter 6 - History of changes.....	109
Product change reporting.....	109

About Release Notes

June 2003

The Release Notes contain information about IBM® Lotus® Sametime® 3.1. Release Notes documentation contains the following chapters:

What's new? introduces you to Sametime, tells you about the new features and enhancements in this release, and points you to further information.

Things you need to know describes supported platforms and environments, and other information that you need to know before installing this release.

Troubleshooting describes known limitations and issues associated with this release of Sametime.

Documentation updates describes errata and updates to the Sametime documentation.

Interoperability describes known restrictions or potential incompatibilities between different versions of Sametime.

History of changes contains information about fixes and enhancements made in past releases of Sametime.

You can edit the documents in the online version of the Release Notes database to suit the particular needs of your site. However, if you do edit the contents of the database, it must be strictly for the sole use of users within your organization. You cannot resell or otherwise distribute this documentation, modified or unmodified, to anyone outside your organization. Lotus® and IBM® assume no responsibility for the technical accuracy of any modifications made to this documentation.

Chapter 1 - What's new?

The *What's new* chapter introduces you to Sametime, tells you about the new features and enhancements in this release, and points you to further information.

Welcome

Sametime server

Welcome to Lotus Sametime

These Release Notes for IBM® Lotus® Sametime® contain the latest information available for Sametime release 3.1. The Release Notes include topics about known issues, system requirements, documentation updates, and information not available in other Sametime documentation. Be sure to read the topics in the *Things You Need to Know* section and the list of known issues in the *Troubleshooting* section before installing the Sametime software.

Updated versions of the Sametime 3.1 Release Notes are available in the documentation library at the Web site <http://www-10.lotus.com/ldd> (formerly, <http://www.notes.net>). The Release Notes available from this Web site contain the most recent information about Sametime 3.1.

Sametime Software Development Kit release notes are provided with each kit. After installation, you can view them on your Sametime server. Visit <http://<sametime server name>/sametime/toolkits>, click the link for any kit to reach its welcome page, and then click Release Notes.

Sametime server

Release Notes - availability and formats

The Release Notes are available both in online format and as a printable PDF file.

The PDF version (STRN31.PDF) is included on the Sametime CD; it can be viewed and printed using Adobe Acrobat Reader software (version 3.0 or higher). Visit the Adobe site at <http://www.adobe.com> to download the latest version of the Adobe Acrobat Reader.

The online IBM Lotus Notes® database version (STRN31.NSF) is installed as part of the Sametime server in the Sametime data directory. It can be directly viewed and searched using a Lotus Notes client.

You can also view the most current version of the Release Notes at the Lotus Developer Domain Web site: <http://www-10.lotus.com/ldd>.

Sametime Software Development Kit release notes are provided with each kit. After installation, you can view them on your Sametime server. Visit <http://<sametime server name>/sametime/toolkits>, click the link for any kit to reach its welcome page, and then click Release Notes.

Sametime server

Lotus/IBM Web sites containing Sametime documentation

The following Web sites are designed to help you locate the latest information on Sametime 3.1:

- <http://www.lotus.com> is the Lotus Development Corporation home page, which contains general information on all Lotus products and services, including press releases, downloadable software, support, and purchasing information. You can use this Web site to access the following Web pages. You can also access these pages directly using the specific URL.
- <http://www.redbooks.ibm.com> contains links to IBM Redbooks that include in-depth information on deploying Sametime in your environment and using the Sametime Software Development Kit. After accessing this web site, search on "Sametime." The two currently available IBM Redbooks for Sametime are *Lotus Sametime Deployment Guide*, and *Lotus Sametime Application Development Guide*.
- <http://www.lotus.com/sametime> contains Sametime product and developer information, including the latest information on Sametime developer's tools and the protocols that make online awareness and real-time collaboration possible in Sametime. This Web site includes white papers, reviewer's guides, common questions and solutions, and newsletters relating to Sametime's features and benefits.

- <http://www.lotus.com/sametimedevolvers> contains the latest tools and information for enabling applications and web sites with Sametime technology. Use this web site to download the latest version of the Sametime Software Development Kit, work with sample applications, participate in discussions using Sametime technology, learn the latest tips and tricks, and review whitepapers and Redbook information.
- <http://www.lotus.com/partners> contains Lotus Notes application development and Business Partner information, including development tips and techniques, innovative applications, developer discussions, and updates on the latest product releases. You can also use this Web site to find out information and request an application for the Lotus Business Partner program.
- <http://www.lotus.com/education> contains Lotus Education information on all Lotus products, including course descriptions, schedules, Lotus Authorized Education Center locations, and Lotus certification information.
- <http://www.ibm.com/software/lotus/support> contains support information on all Lotus products, including common questions and solutions, user discussions, downloadable files, and Lotus support phone numbers. You can also use this Web site to search the KnowledgeBase for technical information on Lotus products.
- <http://www.ibm.com/lotus/idd> contains a technical webzine with articles for end-users, application developers and systems administrators, and an active discussion cafe with several discussion forums for exchanging ideas about IBM Lotus Domino™, Lotus Notes, and Sametime. Also contains Lotus product documentation in various formats for downloading. Information about ordering additional documentation, product tips, and documentation feedback forms is also available.

To access information on the Web, you must use a Web browser, such as Web Navigator, Netscape Navigator, or Microsoft® Internet Explorer. If you need information on connecting your Lotus Notes workstation to the Web, contact your Lotus Notes server administrator.

New Features

Audio/Video services, Sametime Administration Tool, Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client, Sametime server, Web browsers

New Features for Sametime 3.1

The tables below summarize the most important new features and enhancements available in Sametime 3.1. End user and administrator features are listed in separate tables.

New End User Features

Feature or Enhancement	Description
Unix 3.1 clients	<p>Sametime clients that run on the following Unix operating systems ship with Sametime 3.1:</p> <ul style="list-style-type: none"> ● Solaris 8 ● AIX 5.1 ● Redhat 7.2 (Linux) <p>The supported browser versions for these clients are:</p> <ul style="list-style-type: none"> ● Netscape 7 with Sun JVM 1.4.1 on Solaris and Redhat ● Netscape 7 with Sun JVM 1.4 on AIX
Do not disturb feature available from the Meeting Room client	Meeting Room client users can set their online status to do not disturb. This capability was available only in the Sametime Connect client in previous Sametime releases.

Feature or Enhancement	Description
Notes calendaring and scheduling enhancements	<p>If a Sametime server is integrated with the Lotus Domino calendaring and scheduling capabilities, new features are provided to enhance the end user experience. When scheduling a Sametime meeting through the calendaring and scheduling features of a Lotus Notes client, users can:</p> <ul style="list-style-type: none"> ● Create Sametime meeting attendee lists and add and remove names from this list. ● Users can check an "Only the invitees can attend" option when creating a meeting invitation list and specify a meeting password. Only the users in the meeting attendee can use this password to attend the meeting.
Selecting the default login status for Sametime Connect	<p>End users can select a default log-in status (such as "I am active" or "I am away") for their Sametime Connect clients. This log-in status to other online members of the Sametime community at the time the user starts the Sametime Connect client.</p> <p>This feature must be implemented with the Sametime toolkit.</p>
Setting the default location of chat windows	<p>End users can control the default location on a screen in which a chat windows pop up when the user participates in a chat session. End users can also control the size the chat window will have when it pops up on the screen.</p> <p>The administrator must enable this feature before it is available for end users.</p>

New Administrator Features

Feature or Enhancement	Description
Sun JDK 1.4.1 support	<p>Sametime Java applet clients can now run in a Microsoft Internet Explorer 6 or Netscape 7 web browser that operates with the Sun Microsystems JDK 1.4.1.</p>
Reverse proxy support	<p>A Sametime 3.1 server can be deployed behind a reverse proxy server. End users can connect to the Sametime server through the reverse proxy server to participate in any type of Sametime meeting activity with the exception of interactive audio/video.</p>
Audio/video tunneling on port 80	<p>A Sametime 3.1 server can be configured to support the tunneling of UDP audio and video streams over a TCP connection on port 80. TCP tunneling of audio/video streams was supported in previous releases but these streams could not be tunneled over port 80.</p> <p>An additional Network Interface Card (NIC) must be installed on the Sametime server to support this capability.</p>
Sametime Connect for browsers kiosk mode	<p>Sametime Connect for browsers can be configured to operate in a kiosk mode in which user preference settings are stored in memory and valid only for the duration of a single instant messaging session. This capability is useful in environments in which different people use the Sametime Connect for browsers client from a single client machine.</p>
Default connectivity settings for the Sametime Connect for browsers client	<p>An administrator can configure the default connectivity settings for the Sametime Connect for browsers client. This capability ensures that Sametime Connect for browsers loads to a user's web browser with the configuration settings that are appropriate for the network environment. End users are not required to manually configure these settings.</p>

Feature or Enhancement	Description
Enable users to set the default size and location of chat windows	The administrator can enable a Sametime server feature that allows end users to specify the default size and location of the chat windows that pop up on the users' screens.
New GSKit version	Sametime 3.1 requires a new GSKit (IKeyMan) program to create certificate stores when managing SSL connections to LDAP servers or setting up SSL for connections to SIP Connectors. The new GSKit version is available on Sametime server CD 2.
EMS compatibility/patches	Sametime 3.1 servers can be added to the Sametime Enterprise Meeting Server 1.0 to create a meeting services cluster. Before you add a Sametime 3.1 server to the EMS, you must replace existing files on the EMS with updated files that are available on a Sametime server CD to ensure the Sametime 3.1 servers can operate with the EMS. Instructions for updating these files are available in the <i>Sametime 3.1 and Enterprise Meeting Server 1.0 Administrator's Guide</i> provided with the Sametime 3.1 server.
Session Initiation Protocol (SIP) support	The Sametime 3.1 server ships with the capability to support SIP for instant messaging and audio/video sessions between Sametime communities. This capability was previously available only in Sametime fix packs.
Polish and Russian languages available	Unlike previous Sametime releases, Sametime 3.1 is available in the Polish and Russian languages.

Chapter 2 - Things you need to know

The *Things you need to know* chapter describes supported platforms and environments and other information that you need to know before installing this release.

Configuration servlet is not secure following installation

Sametime server

Configuration servlet is not secure following installation

The Sametime server contains a configuration servlet that is accessed by several Sametime server processes. This configuration servlet can access server configuration information and is not protected with any security mechanism following a Sametime server installation. You should protect this servlet by configuring Sametime to require authentication for access to the configuration servlet. If you do not require authentication for access to the configuration servlet, an attacker might be able to access this servlet to alter or retrieve server configuration information.

The administrator must perform the following steps to require authentication for access to the configuration servlet:

1. Create or identify a special directory account to use for authentication when accessing the configuration servlet.
2. Edit the Sametime.ini file on the Sametime server.
3. Edit the servlets.properties file in the <Sametime installation>\Data directory on the Sametime server.
4. Add the user name required for authentication to the Access Control List (ACL) of the Configuration database (stconfig.nsf).

Each of these steps is described in detail below.

Step 1 - Create or identify a special directory account to use for authentication when accessing the configuration servlet

Creating or identifying a directory account is the first of four procedures you must perform to require authentication for access to the configuration servlet.

To authenticate, the Sametime processes must present a user name and password when accessing the configuration servlet. This user name and password must exist in either the person entry of an LDAP directory or the Person document of a Domino Directory (depending on whether your Sametime community uses an LDAP or Domino Directory).

IBM Lotus software recommends that you create a special account in the directory strictly for the purpose of authenticating access to the configuration servlet. This directory account should be used for no other purpose. For example, you might want to create an account with the user name of "SametimeServletAccess" and specify a password for the account. Creating a special account for this purpose ensures that the account is not tied to a particular user or process and will not be changed inadvertently.

If you prefer, you can use an existing directory account (user name and password) for this purpose.

Step 2 - Edit the Sametime.ini file on the Sametime server

Editing the Sametime.ini file is the second of four procedures you must perform to require authentication for access to the configuration servlet.

After you have created a special directory account (or identified an existing directory account) to use for authentication, you must specify the user name and password associated with this directory account in the Sametime.ini file on the Sametime server. Follow the instructions below:

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 The default Sametime installation directory is C:\Lotus\Domino. Sametime installs into the same directory as the Domino server.

2. The Sametime.ini file contains a [Config] section. At the bottom of the [Config] section, manually add the following two Sametime.ini file settings by typing them in the Sametime.ini file with the text editor:

```
SametimeAdminUsername=  
SametimeAdminPassword=
```

The two fields above must specify the user name and password you intend to use for authenticating access to the configuration servlet. Type the appropriate user name and password as the values for these fields. For example, if you created a directory entry for the user name "SametimeServletAccess" with a password of "Sametime," the correct entries in the Sametime.ini file [Config] section would look like this:

```
SametimeAdminUsername=SametimeServletAccess  
SametimeAdminPassword=Sametime
```

3. Save and close the Sametime.ini file.

Step 3 - Edit the servlets.properties file in the <Sametime installation>\Data directory on the Sametime server

Editing the servlets.properties file is the third of four procedures you must perform to require authentication for access to the configuration servlet.

1. Use a text editor to open the servlets.properties file on the Sametime server. The servlets.properties file is located in the <Sametime installation>\Data directory. (The default is C:\Lotus\Domino\Data.)
2. In the servlets.properties file, locate the line that begins with "servlet.scs.initArgs=". An example of this line is provided below.

```
servlet.scs.initArgs=ServletURL=scs,UnchainedAccessEnabled=true
```

3. Add the following text to the end of the line identified above:

```
,AccessControl.Roles=[SametimeAdmin].
```

After you have added the text, the line should appear as follows:

```
servlet.scs.initArgs=ServletURL=scs,UnchainedAccessEnabled=true,AccessControl.Roles=[SametimeAdmin]
```

4. Save and close the servlets.properties file.

Step 4 - Add the user name required for authentication to the Access Control List (ACL) of the Configuration database on the Sametime server

Adding the user name required for authentication to the ACL of the Configuration database is the last of four procedures you must perform to require authentication for access to the configuration servlet.

In this procedure, you add the user name associated with the directory entry discussed above to the ACL of the Configuration database (stconfig.nsf) and provide the user name with the "SametimeAdmin" role in the ACL. An example of this procedure is provided below:

1. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
2. Choose File-Database-Access Control.
3. Add the user name associated with the directory entry discussed above ("SametimeServletAccess" in this example) to the stconfig.nsf ACL. Provide this user name with the "SametimeAdmin" role in the ACL.

Note The "SametimeAdmin" role is the only credential in the ACL that must be assigned to the user name specified for configuration servlet authentication. It is not necessary to assign a specific access level (such as Manager or Author) to this user name.

4. Click OK to exit the ACL.

System requirements

Audio/Video services, Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client, Sametime server

System requirements for Sametime 3.1

Sametime 3.1 server

Operating systems	Windows® 2000 Server (Service Pack 3 installed)
Processors	Pentium® II 400MHz minimum
RAM	1 GB (recommended) 500 MB (minimum)
Disk space	500 MB free disk space minimum 1 GB is recommended to allow space for meeting, meeting attachments, and recorded meetings
Disk swap space	64 MB
Network software	TCP/IP network software installed
Web browsers supported	Microsoft Internet Explorer 6 with the native Microsoft Java VM or Sun Microsystems Java VM 1.4.1. Netscape 7 with the Sun Microsystems Java VM 1.4.1
Video requirements	The server machine must have a video card installed. The video display color setting must be higher than 256 colors. A 16-bit color setting is recommended.
Lotus Domino server requirements	Installs on Domino server release 6.0.2

Sametime 3.1 client system requirements (Windows clients)

Certified operating system versions	Windows 2000 Professional (Service Pack 3 installed) Windows XP
Processors supported	Pentium II 266 MHz or higher
RAM	128 MB or higher
Web browsers supported	Microsoft Internet Explorer 6 with the native Microsoft Java VM or Sun Microsystems Java VM 1.4.1. Netscape 7 with the Sun Microsystems Java VM 1.4.1.
Additional requirements for Audio/Video	<p>Sound card: Full-duplex required for interactive meetings; half-duplex required for attending broadcast meetings as an audience member or replaying recorded meetings</p> <p>Microphone and speakers: A headset that includes a boom microphone performs best. If a desktop microphone is used, a unidirectional dynamic microphone that uses batteries is preferred. (Avoid microphones with on/off switches unless the microphones are well-made.)</p> <p>Video capturing software: Video for Windows</p> <p>Camera: A high-quality USB camera that is compatible with Video for Windows and Windows sound cards is recommended.</p> <p>A camera is optional. Users who do not have a camera can participate in audio/video meetings. When a user without a camera speaks, no video is displayed to other users in the meeting.</p>

Sametime 3.1 client system requirements (Unix/Linux clients)

Certified operating system versions	AIX 5.1 with latest updates, CDE Desktop Solaris 8 with latest updates (including patches 108434-03,108435-03), CDE Desktop Linux Red Hat 7.2 with latest updates, Gnome Desktop
Processors supported	Pentium II 266 MHz or higher
RAM	128 MB or higher
Web browsers supported	AIX: Netscape 7 with Java Plugin 1.4.0 Solaris 8: Netscape 7 with Java Plugin 1.4.1 Linux Red Hat 7.02: Netscape 7.02 with Java Plugin 1.4.1

Note: All operating systems require a minimum supported display resolution of 1024x768 and the following XWindows Extensions: XTEST, SHAPE, GLX.

Server administration

Sametime Administration Tool, Sametime server

Do not use Sametime settings in the Server document

The Sametime server Server document in the Domino Directory contains a Sametime tab. The settings available in the Sametime tab of the Server document have no affect on Sametime operations and should not be used.

Administrators should use the Sametime Administration Tool to change Sametime server administration settings. The Sametime Administration Tool accesses the Configuration database (STCONFIG.NSF) and the Sametime.ini file, which store the Sametime administration settings.

Sametime Administration Tool

Changing server administration parameters

With Sametime 3.1, the server administration parameters accessed by the XML-based Sametime Administration Tool are stored in the Configuration database (STCONFIG.NSF) on the Sametime server and in the Sametime.ini file. It is recommended that you use the Sametime Administration Tool to change server administration parameters.

If you directly access the STCONFIG.NSF database or the Sametime.ini file to change a server administration parameter, you must restart the Sametime server before the change will take affect. Generally, you should not change administration settings by accessing the STCONFIG.NSF database with a Lotus Notes client. Use the Sametime Administration Tool to change administration settings.

Sametime server

Do not replicate the Configuration (stconfig.nsf) database

If you have multiple Sametime 3.1 servers in your Sametime community, you should not replicate the entire Configuration database (stconfig.nsf) among the Sametime 3.1 servers. Some documents in the Configuration database contain the IP address or host name of a Sametime server and replication of these documents to a different Sametime 3.1 server will prevent that server from functioning properly.

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. Configuring these settings on each server ensures that the settings that must be consistent across servers are consistent.

Note A Tech Note is being created that explains how to set up a selective replication of the Configuration database. A selective replication enables you to keep some administration settings consistent across all Sametime servers while not replicating documents in the Configuration database that may cause problems on a different server. Using selective replication prevents the administrator from having to manually configure each Sametime server to ensure all administration settings that must be consistent across servers are consistent. Tech Notes can be viewed at <http://www-3.ibm.com/software/lotus/support/sametime/support.html>.

The settings that should be consistent on each Sametime server in a community are listed below. It is mandatory that some of these settings are consistent across all Sametime servers in a community. For other settings, it is recommended that you maintain 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 see unexpected behavior when attending meetings on invited servers.

In the Configuration-Community Services tab of the Sametime Administration Tool, the following settings must be consistent 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"

In the Configuration-Community Services tab of the Sametime Administration Tool, the following settings must be consistent 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)"

In the LDAP Directory settings of the Sametime Administration Tool, all LDAP settings must be consistent on all Sametime servers in the same community. These settings are used only if your community of users is defined in an LDAP directory instead of a Domino directory. These settings are listed below.

In the Sametime Administration Tool LDAP Directory settings, all of the following must have the same values across Sametime servers:

- LDAP Directory - Connectivity settings
- LDAP Directory - Basics settings
- LDAP Directory - Authentication settings
- LDAP Directory - Searching settings
- LDAP Directory - Group Content settings

Community Services server clusters and consistent administration settings

If you create a Community Services server cluster as described in the *Sametime 3.0 Administrator's Guide*, all of the settings described above should be consistent across all Sametime servers in the cluster. Note also that the Configuration database of every Sametime server in the community should contain the "Cluster Information" document that defines the cluster. You can use a Lotus Notes client to create the Cluster Information document in the Configuration database on one Sametime server in the community server cluster and then copy and paste the Cluster Information document into the Configuration databases on all of the other Sametime servers in the community (including both Sametime servers that operate as part of the cluster and Sametime servers that are not part of the cluster). For more information, see the "Creating Community Services server clusters" chapter of the *Sametime 3.0 Administrator's Guide*.

The Community Connectivity document in the Configuration databases of the Sametime servers contains a "CommunityTrustedIPs" field. This field holds the IP addresses of Community Services multiplexers that are installed on separate machines. The "CommunityTrustedIPs" field is a security setting that ensures that only Community Services multiplexers that are specified by the administrator (in the "CommunityTrustedIPs" field) can connect to the Sametime server. If you have deployed Community Services multiplexers on separate machines in front of a Community Services cluster, the Community Connectivity document must exist on every Sametime server in the Community Services cluster. For more information, see the "Creating Community Services server clusters" chapter of the *Sametime 3.0 Administrator's Guide*.

There is an exception regarding the Community Connectivity document. If a Sametime server is assigned multiple IP addresses to support HTTP tunneling functionality, the Community Connectivity document must be different on every Sametime server that uses multiple IP addresses. For more information about this scenario, see "Configuring HTTP tunneling on a machine that uses multiple IP addresses" in the "Configuring Sametime Connectivity" chapter of the *Sametime 3.0 Administrator's Guide*.

When a Sametime server is configured to use multiple IP addresses, the Community Connectivity document contains a Host Name setting that is specific to an individual server. If you copy this Community Connectivity document to another server, the document will specify the wrong Host Name and will cause connectivity problems. In this scenario, the "CommunityTrustedIPs" fields of the Community Connectivity documents must contain consistent settings on every server in the cluster, but you cannot copy and paste the document. You must use a Lotus Notes client to manually open the Configuration databases on every Sametime server in the Community Services cluster, open the Community Connectivity documents, and enter the IP addresses of the Community Services multiplexers in the "CommunityTrustedIPs" fields.

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.

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"

In the Configuration-Community Services-Server Features settings of the Sametime Administration Tool, the following settings should be consistent on all Sametime servers in the community:

- "Allow authenticated users to transfer files to each other"
- "Allow users to send announcements"

In the Configuration-Meeting Services-General settings, the following settings should be consistent across 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 choose NetMeeting (or other T.120-compatible client) for screen sharing and whiteboard instead of Sametime Web-based meeting tools."
- "Allow people to schedule Broadcast meetings"

In the Logging-Settings 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"
- "Total number of people logged in and total number of unique names logged in"
- "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"

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 meeting 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 meeting exceeds"

Signing Sametime databases

Sametime server

Signing Sametime databases

Some Sametime databases contain agents that access the Directory and provide authentication support for Sametime. Agents within these databases are signed by the "Sametime Development/Lotus Notes Companion Products" ID.

If the security policies of your organization require you to re-sign databases with a different ID, you must re-sign the following Sametime database and templates:

STCONF.NTF
STDISC50.NTF
STTEAM50.NTF
STSRC.NSF

After re-signing these files, ensure that the signer you have used is listed in the Directory ACL and in the "Run unrestricted agents" field of the Sametime server Server document.

The minimal Directory ACL requirements for the signer ID are:

Access: Reader

Roles: [Group Creator], [Group Modifier], [UserCreator], [UserModifier]

Server display color setting must be higher than 256 colors

Sametime server

Server display color setting must be higher than 256 colors

The server machine on which Sametime is installed must have a video card installed and a display color setting higher than 256 colors. A 16-bit color setting is recommended.

The following problems can occur if the server machine has a display color setting of 256 colors or less:

- The images in whiteboard attachments do not display correctly on the whiteboard.
- Users cannot save the whiteboard.
- The Meeting Room client opens with a gray whiteboard.
- Screen-sharing buttons are disabled in the Meeting Room client.
- Audio/Video features do not work.
- When a user attends a meeting, an additional Meeting Room client opens in a different window and flashes periodically.
- The license utility fails to run.

Shortly after these problems appear, meetings on the Sametime server may fail to become active.

Domino HTTP server must use the fully-qualified host name

Sametime server

Domino HTTP server must use the fully-qualified host name

Sametime 3.1 must be installed on a Domino 6.02 server. You must install the Domino server first and then install Sametime on top of the Domino server.

The HTTP server of the Domino 6.02 server on which Sametime is installed must be accessed using the fully-qualified host name. To ensure the Domino HTTP server can be accessed using the fully-qualified host name:

1. Use a Lotus Notes client to open the Domino Directory on the Domino server on which Sametime is installed.
2. Select the Server-Servers view.
3. In the right-hand pane of the Server-Servers view, double-click on the Domino server name to open the Server document for the Domino server.
4. Select the Ports-Notes Network Ports tab.
5. The Notes Network Ports tab contains an entry for the the "TCP/IP" port. The Net Address column for the "TCP/IP" port entry must contain the fully-qualified DNS host name (for example, sametime.east.acme.com) of the Domino server on which Sametime is installed.

If the Net Address column does not contain the fully-qualified DNS name of the server, select Edit Server and manually enter the fully-qualified name in the Net Address column. Save and close the Server document.

6. Restart the Domino server.

If you plan to allow self-registration for Sametime 3.1, you must make the following ACL changes in the Domino Directory on which Sametime is installed:

- Add the entry Sametime Development/Lotus Notes Companion Products to the ACL.
- Provide the Sametime Development/Lotus Notes Companion Products entry with a User type of "Person" and the Access level of "Editor."
- Provide the Sametime Development/Lotus Notes Companion Products with these four Roles in the ACL: GroupCreator, GroupModifier, UserCreator, UserModifier.

Controlling the bandwidth usage of the Sametime server

Sametime server

Controlling the bandwidth usage of the Sametime server

Sametime 3.1 contains a new feature that enables you to control the network bandwidth used by the Sametime server. 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 routers is discarding packets, you can enable the Sametime server Bandwidth Control feature. This feature allows you 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 Sametime server will send a maximum of 1000K of data on the network.

Before enabling this feature, consider the following:

- There are several highly-dynamic variables involved in determining the appropriate Bandwidth Control feature. 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 the Community 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\HTTPServer]
"MaxBandwidthAvailable"="0"
"BandwidthUpdateInterval"="10"
"BandwidthReportInterval"="300"
```

MaxBandwidthAvailable

When MaxBandwidthAvailable is set to 0, the feature is turned off.

When 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 1000 kbps, 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 diagnostic 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 stdiagviewer window, under the MEDIA T120 MCSNC module.

Joining meetings with NetMeeting

Audio/Video services, Sametime server

Joining meetings with NetMeeting

This topic discusses procedures and issues with using NetMeeting to attend meetings on a Sametime server. This discussion assumes that the administrator has enabled the following two settings in the Sametime Administration Tool:

- "Allow people to choose NetMeeting (or other T.120 compatible client) for screen sharing and whiteboard instead of Sametime Web-based meeting tools" in the Configuration - Meeting Services - General Settings of the Sametime Administration Tool.

If this option is not enabled, users can attend meetings with NetMeeting, but cannot use the screen sharing or whiteboard components of NetMeeting during the meeting.

- "Allow H.323 clients (such as Microsoft NetMeeting) to join a Sametime meeting" in the Configuration - Connectivity - Interactive Audio/Video Network settings of the Sametime Administration Tool.

If this option is not enabled, users can attend meetings with NetMeeting, but cannot use the audio/video components of NetMeeting during the meeting.

If the two administrative options above are enabled, the Sametime server is configured to allow users to attend meetings on the server with the Microsoft NetMeeting client and use the screen-sharing, whiteboard, audio, and video features of NetMeeting.

Note: For additional information about NetMeeting and Sametime, see any of the following topics in the Sametime 3.0 Administrator's Guide: "General settings for Meeting Services" in the "Configuring the Meeting Services" chapter,

- "Allowing or preventing the use of NetMeeting for screen sharing and whiteboard" in the "Configuring the Meeting Services" chapter
- "H.323-compliant clients (NetMeeting)" in the "Configuring the Audio/Video Services" chapter
- "Interactive Audio/Video network settings" in the "Configuring Sametime Connectivity" chapter
- "Allow H.323 clients (such as NetMeeting) to join a Sametime meeting" in the "Configuring Sametime Connectivity" chapter

Starting NetMeeting from a Web link (recommended use of NetMeeting with Sametime)

When using NetMeeting with the Sametime server, users must launch NetMeeting from a Web link in the Sametime Meeting Center. To ensure that NetMeeting can be launched from the Web link, the end user should select the "Use NetMeeting" option on the Tools tab of the New Meeting page on the Sametime server when creating the meeting. When the "Use NetMeeting" option is selected, the collaborative activities (screen sharing, whiteboard, audio, and video) that are available to NetMeeting users are determined by the two administrative settings described above.

To attend the meeting, the user clicks a meeting name in the Sametime Meeting Center. The Meeting Details document, which contains a link to launch NetMeeting, appears. The user selects this link to launch NetMeeting on the user's local machine and connect to the meeting. NetMeeting must already be installed on the user's machine.

Note: Netscape users may have to download and install a plug-in to launch Microsoft NetMeeting from a Netscape browser. See the *Sametime 3.0 User's Guide* (available from the Documentation link of the Sametime server home page) for more information.

Creating and attending NetMeeting meetings in this way ensures that all collaborative activities allowed by the administrator are available to the NetMeeting clients in the meeting.

Attending meetings directly from NetMeeting

If the "Use NetMeeting" option on the Tools tab of the New Meeting page is selected, it is also possible for NetMeeting users to attend the meeting by starting NetMeeting on their Windows desktops and attending the meeting by entering the Sametime server name in the NetMeeting user interface.

Attending meetings with NetMeeting in this way is not recommended and is possible only if the administrator disables the "Allow H.323 clients (such as Microsoft NetMeeting) to join a Sametime meeting" in the Configuration - Connectivity - Interactive Audio/Video Network settings of the Sametime Administration Tool.

If the user starts NetMeeting from the Windows desktop instead of launching it from the Web link as described above, the screen-sharing and whiteboard features can be used in the meeting, but audio and video features cannot.

Attending Sametime Meeting Room client meetings with NetMeeting

If the user selects the "Use the Sametime Meeting Room" option in the Tools tab of the user interface when creating the meeting (instead of selecting the "Use NetMeeting" option), the user expects other users to attend the meeting using the Sametime Meeting Room client.

However, it is possible for NetMeeting users to participate in the audio/video part of a meeting for which the "Use the Sametime Meeting Room" option was selected during Meeting creation. Note that NetMeeting users cannot participate in any screen-sharing or whiteboard activity in this meeting.

Note: The "Allow H.323 clients (such as Microsoft NetMeeting) to join a Sametime meeting" setting in the Configuration - Connectivity - Interactive Audio/Video Network settings of the Sametime Administration Tool must be enabled for NetMeeting clients to participate in a meeting in this way.

NetMeeting users can use the following procedure to attend the audio/video part of a meeting that was created as a meeting for Sametime Meeting Room clients:

1. Before the meeting begins, view the meeting details and write down the audio conference ID number. To view the details, click the meeting name in the Sametime Meeting Center.
2. Start Microsoft NetMeeting from the Windows desktop. (Microsoft NetMeeting 3.01 is required.)
3. Choose Tools - Options, and click the Advanced Calling button.
4. Select the "Use a gateway to call telephones and video conferencing systems" check box.
5. Enter the DNS name or IP address of the Sametime server in the Gateway field. (For example, www.sametimeserver.com.)
6. Click OK in the Advanced Calling Options dialog box, and then click OK in the Options dialog box.
7. Click the Call button.
8. Enter the audio conference ID from step 1 in the To field.
9. Select "Phone number" in the Using drop-down box.
10. Click Call to join the meeting.

Note: Under no circumstances can Sametime Meeting Room client users and Microsoft NetMeeting users participate in screen-sharing and whiteboard activities in the same meeting. The screen-sharing/whiteboard capabilities of the Sametime Meeting Room client and the NetMeeting client are not compatible. If the "Use NetMeeting" option is selected in the Tools tab of the user interface during meeting creation, users must attend the meeting with the NetMeeting client to use screen-sharing and the whiteboard. If the "Use the Sametime Meeting Room" option is selected in the Tools tab, users must attend the meeting with the Sametime Meeting Room client to use screen-sharing and the whiteboard.

NetMeeting users cannot attend password protected or encrypted Sametime meetings

Administrators should be aware of the distinction between a "Sametime" meeting and a "NetMeeting" meeting. A "Sametime" meeting is a meeting for which the end user has selected the "Use the Sametime Meeting Room" option when creating the meeting. A "NetMeeting" meeting is a meeting for which the end user has selected the "Use NetMeeting" option when creating the meeting.

Note the following concerning Sametime meetings and NetMeeting meetings:

- NetMeeting users cannot attend any Sametime meeting or NetMeeting meeting that is password protected. When the administrator enables the "Allow H.323 clients (such as NetMeeting) to join a Sametime meeting" option, the administrator should disable the "Require all scheduled meetings to have a password" option in the Configuration-Meeting Services-General settings of the Sametime Administration Tool.
- NetMeeting users cannot attend any Sametime meeting that is encrypted. If the administrator enables the "Allow H.323 (such as NetMeeting) to join a Sametime meeting" option, the administrator should still enable the "Encrypt all Sametime meetings" setting in the Sametime Administration Tool.

If the "Encrypt all Sametime meetings" setting is enabled in the Sametime Administration Tool, and the end user selects the "Use NetMeeting" option when creating the meeting, the meeting will not be encrypted. (The meeting is not encrypted because it is a "NetMeeting" meeting instead of a "Sametime" meeting.)

Enabling the "Encrypt all Sametime meetings" option also provides additional security when the administrator allows H.323 clients to join meetings. It is impossible for a NetMeeting client to receive H.323 data from an encrypted Sametime meeting. Encrypting all meetings ensures that NetMeeting cannot be used to gain illegal access to the audio/video portions of a Sametime meeting.

Note: When the administrator enables the "Allow H.323 clients (such as NetMeeting) to join a Sametime meeting" option, a unique H.323 meeting identifier is created and recorded on the Meeting Details document associated with each meeting in the Sametime Meeting Center. H.323 clients cannot join a meeting that does not include an H.323 meeting identifier. These unique identifiers are not created for meetings that are password-protected or encrypted. Even though the meeting identifier is not present, an attacker may still be able to use NetMeeting to gain illegal access to the H.323 portions of the Sametime meeting if the meeting is not encrypted.

Chat logging on the Sametime server

Sametime Connect client, Sametime Meeting Room client, Sametime server

Chat logging on the Sametime server

An API is 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 applications developed with the chat logging API.

To access the documentation for the chat logging API, click the Software Development Kit link at the bottom of the Sametime server home page.

Domino server installation procedures

Sametime server

Domino server installation instructions Installation Procedures

Before you can install the first Sametime server in your environment, you must install a Domino 6.0.2 server. After you have installed the Domino 6.0.2 server, you can install Sametime on top of the Domino server.

To support the **first** Sametime server installed into your environment, the Domino 6.0.2 server must be installed as a first server in a Domino domain.

Step-by-step instructions for installing the Domino 6.0.2 server in this way are provided below. These steps describe a basic Domino server installation that can support Sametime. If you need more detailed information about Domino server installations and Domino environments, see the Domino Installation Guide available from the documentation library of the Lotus Developer's Domain web site at <http://www-10.lotus.com/ldd/doc>.

Note: If you are installing more than one Sametime server, review the issues and procedures that are discussed in the "Deploying multiple Sametime servers" chapter of the Sametime Administrator's Guide before installing the additional Sametime/Domino servers. Also, during the Sametime server installation, ensure that you specify the fully-qualified DNS name of the server on which you are installing Domino.

Before you install the Domino server program files on a Windows system, do the following:

- Make sure that the required hardware and software components are in place and working.
- Temporarily disable any screen saver and turn off any virus-detection software.
- Make sure that all other applications are closed. Otherwise, you may corrupt any shared files, and the Install program may not run properly.
- If you are upgrading to Domino from a previous release, see the book "Upgrade Guide".

To install the Domino server:

1. Run the install program (SETUP.EXE), which is on the Domino server installation CD.
2. Read the Welcome screen, and click Next. Then read the License Agreement and click Yes.
3. Enter the administrator's name and the company name.
4. Do not elect to install Domino on partitioned servers.
5. Choose the program and data directory in which to copy the software, and then click Next.
6. Select "Domino Enterprise Server" as the server type.
7. Click Next to accept all components.
8. Specify the program folder or accept Lotus Applications as the program folder that will contain the software.
9. Click Finish to complete the install program.
10. Choose Start · Programs · Lotus Applications · Lotus Domino Server to start the Server Setup program.

Using the Domino Server Setup program locally

After installing the Domino server program files on a server, you can run the Domino Server Setup program locally by starting the server. The Server Setup program asks a series of questions and guides you through the setup process. Online Help is available during the process.

Starting and shutting down the Domino server

Start the Domino server so users can access shared databases and obtain other server services. Do not enter keystrokes or click the mouse while the Domino server is starting or shutting down.

Note If the server program is running, do not use CTRL+S to stop scrolling the console, because no server services take place until you press a key to continue.

Starting the Domino server

To start the Domino server from Windows NT/Windows 2000, choose Start · Programs · Lotus Applications · Lotus Domino Server.

Shutting down the Domino server

To shut down the Domino server, enter either exit or quit at the console. It may take ten seconds or more for the server to shut down.

Setting up an LDAP connection to an ActiveDirectory server

Sametime server

Setting up an LDAP connection to an ActiveDirectory server

You can set up an LDAP connection to an ActiveDirectory server; however, certain modifications to ActiveDirectory are required. Follow these procedures to use ActiveDirectory with Sametime.

Planning

1. Choose whether to allow anonymous read access to your ActiveDirectory Users.
2. If you do not allow anonymous read access to your ActiveDirectory, assign read privileges to a newly-created or existing ActiveDirectory username.

ActiveDirectory Procedures

1. Note the Base DN for the ActiveDirectory Users tree (for example, CN=Users,dc=ad,dc=mycompany,dc=com).
2. Using the ActiveDirectory Users and Computers tool, navigate to the Users container.
3. Open the Properties dialog of the Users container and select the Security tab.
4. Choose Add to add a new security privilege to this container.
5. A Choose Users dialog box appears.
 - If you allow anonymous access to your ActiveDirectory, select "Everyone." Click Add and OK.
 - If you restrict read access to an ActiveDirectory username, select that username. Click Add and OK.
6. The top-level Security dialog box appears. Select the appropriate username.
 - If you allow anonymous access to your ActiveDirectory, select "Everyone."
 - If you restrict read access to an ActiveDirectory username, select that username.
 - For either username, ensure that only Read permissions are checked.
7. Click Advanced.
8. The Access Control Settings dialog box appears. Select the appropriate username and click View/Edit.
9. The Permission Entry for Users dialog box appears. Select the "Apply onto" pull-down menu. Change "This object only" to "This object and all child objects." Click OK.
10. Complete all remaining dialog boxes by clicking OK.

Sametime installation/configuration procedures

After you have performed the ActiveDirectory procedures described above, you must configure the Sametime server to access the directory on the ActiveDirectory server. Follow the procedures described in the "Using LDAP with the Sametime server" chapter of the *Sametime 3.0 Administrator's Guide* to enable Sametime to connect to the ActiveDirectory server.

Note: You must be knowledgeable about the ActiveDirectory directory schema to configure Sametime to access the ActiveDirectory server.

Supported sound cards and cameras

Audio/Video services

Supported sound cards and cameras

The Sametime Multimedia Services provide IP audio/video capabilities to Sametime. Sound cards and cameras that work with the Multimedia Services are listed below.

Sound cards

Any correctly installed full-duplex sound card should work with Sametime. The sound cards listed below 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.

Enabling QuickPlace or Virtual Classroom to access Sametime servlets

Sametime server

Enabling QuickPlace or Virtual Classroom to access Sametime

Sametime servers can be deployed in an environment that includes IBM Lotus QuickPlace Servers or the IBM Lotus Virtual Classroom. In these environments, QuickPlace or the Virtual Classroom will require remote access to servlets on the Sametime server.

To execute a servlet on the Sametime server, a remote user (such as QuickPlace or Virtual Classroom) must be able to authenticate when accessing the servlets. The administrator must manually configure the Sametime and QuickPlace or Virtual Classroom servers to ensure that this authentication can occur.

Note A remote user must authenticate to execute the servlets because the Sametime servlets handle sensitive data, including Sametime configuration settings, API calls that can modify or delete meetings, and meeting materials such as whiteboard files. If no authentication is required, unauthorized users can access the servlets to retrieve or manipulate the data handled by these servlets.

To enable QuickPlace or the VirtualClassroom to execute servlets on the Sametime server:

1. Create or identify a special directory account for authentication when accessing the Sametime servlets.
2. Add an entry to the Configuration database Access Control List (ACL) on the Sametime/Domino server.
3. Populate the appropriate fields in the MeetingServices document in the Sametime server Configuration database (stconfig.nsf).
4. Create a Sametime.ini file on the QuickPlace or VirtualClassroom server.

Step 1 - Create or identify a special directory account for authentication when accessing the Sametime servlets

Creating or identifying a directory account is the first of four procedures you must perform to enable a QuickPlace or Virtual Classroom application to authenticate when accessing servlets on the Sametime server.

To authenticate, QuickPlace or the Virtual Classroom must present a user name and password when accessing the Sametime servlets. This user name and password must exist in either the person entry of an LDAP directory or the Person document of a Domino directory (depending on whether your Sametime community uses an LDAP or Domino Directory).

IBM Lotus software recommends that you create a special account (person entry in an LDAP directory or person document in a Domino Directory) strictly for the purpose of authenticating access to the Sametime servlets. This directory account should be used for no other purpose. For example, you might want to create an account with the user name of "SametimeServletAccess" and specify a password for the account. Creating a special account for this purpose ensures that the account is not tied to a particular user or process and will not be changed inadvertently.

If you prefer, you can use an existing directory account (person entry or document containing a user name and password) for this purpose.

Step 2 - Add the user name required for authentication to the ACL of the Configuration database on the Sametime server

Adding the user name required for authentication to the ACL of the Configuration database is the second of four procedures you must perform to enable a QuickPlace or Virtual Classroom application to authenticate when accessing servlets on the Sametime server.

In this procedure, you add the user name associated with the directory entry to the ACL of the Configuration database (stconfig.nsf) and provide the user name with the "SametimeAdmin" role in the ACL. An example of this procedure is provided below:

1. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
2. Choose File-Database-Access Control.
3. Add the user name associated with the directory entry discussed in the procedure above ("SametimeServletAccess" in this example) to the stconfig.nsf ACL. Provide this user name with the "SametimeAdmin" role in the ACL.

Note The "SametimeAdmin" role is the only credential in the ACL that must be assigned to the user name. It is not necessary to assign a specific access level (such as Manager or Author) to this user name.

4. Click OK to exit the ACL.

Note Keep the Configuration database open. You must alter a document in the Configuration database in the next procedure.

Step 3 - Populate the appropriate fields in the MeetingServices document in the Sametime server Configuration database (stconfig.nsf)

Populating the appropriate fields in the MeetingServices document in the Sametime server Configuration database is the third of four procedures you must perform to enable a QuickPlace or Virtual Classroom application to authenticate when accessing servlets on the Sametime server.

In this procedure, you add the user name and password associated with the directory entry (discussed in "Step 1 - Create or identify a special directory account for authentication when accessing the Sametime servlets" above) to fields in the MeetingServices document in the Configuration database. Follow the procedure below:

1. If necessary, use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
2. In the right-hand pane, open the MeetingServices document by double-clicking on the date associated with the document.
3. Scroll to the bottom of the MeetingServices document until you see the Remote Services Access heading.
4. Under the Remote Services Access heading, populate the eight fields with the user name and password associated with the directory entry discussed in "Step 1 - Create or identify a special directory account for authentication when accessing the Sametime servlets" above.

For example, if you created a directory entry with a user name of SametimeServletAccess and a password of Sametime, populate the eight fields under the Remote Services Access heading as shown below:

Meeting Management Username: SametimeServletAccess
Meeting Management Password: Sametime

Recorded Meeting Management Username: SametimeServletAccess
Recorded Meeting Management Password: Sametime

Materials Refresh Username: SametimeServletAccess
Materials Refresh Password: Sametime

Materials Control Username: SametimeServletAccess
Materials Control Password: Sametime

5. Save and close the MeetingServices document, then close the Configuration database.

Step 4 - Create a Sametime.ini file on the QuickPlace or Virtual Classroom server

Creating a Sametime.ini file on the QuickPlace or Virtual Classroom server is the last of four procedures you must perform to enable a QuickPlace or Virtual Classroom application to authenticate when accessing servlets on the Sametime server.

The Sametime.ini file on the QuickPlace or Virtual Classroom server must contain the parameters that enable QuickPlace or Virtual Classroom to access the Sametime server. You must create the Sametime.ini file in the QuickPlace or Virtual Classroom installation directory on the QuickPlace or Virtual Classroom server.

Follow these instructions to manually create a Sametime.ini file in the QuickPlace or Virtual Classroom installation directory.

1. Open a text editor on the QuickPlace or Virtual Classroom server.
2. Use the text editor to create a text file consisting of a [Config] section and the settings listed below (you must manually type all of this information in the file):

[Config]

VPS_Name= (This setting should specify the canonical name of the Domino/Sametime server to which QuickPlace or Virtual Classroom will connect. An example value is VPS_NAME=CN=Sametimeserver/OU=East/O=Acme.)

SametimeCluster= (This setting should also specify the canonical name of the Domino/Sametime server, e.g.: SametimeCluster=CN=Sametimeserver/OU=East/O=Acme.)

ConfigurationHost= (This setting should specify the fully-qualified DNS name of the Sametime server, e.g.: ConfigurationHost=Sametimeserver.east.acme.com.)

ConfigurationPort=80 (This setting should specify port 80.)

SametimeAdminUsername= (This setting should specify the name of the user account that was added to the ACL of the Configuration database on the Sametime server in "Step 1 - Add an entry to the Configuration database ACL on the Sametime/Domino server" above.)

SametimeAdminPassword= (This setting should specify the password associated with the administrator account above.)

About encrypting connections to the Sametime server with SSL

The configurations described above ensure that a QuickPlace or Virtual Classroom server on a remote machine can authenticate when accessing the servlets on a Sametime server. Note that the QuickPlace or Virtual Classroom server will transmit the user name and password used for this servlet access in the clear when connecting to the Sametime server. If needed, this connection between the QuickPlace or Virtual Classroom server to the Sametime server can be encrypted with SSL to prevent the user name and password from being passed in the clear. For more information, see "Encrypting QuickPlace or Virtual Classroom connection with SSL" in the Things You Need to Know section of these release notes.

Encrypting QuickPlace or Virtual Classroom connection to Sametime with SSL

Sametime server

Encrypting QuickPlace or Virtual Classroom connection with SSL

Sametime servers can be deployed in an environment that includes IBM Lotus QuickPlace servers or the IBM Lotus Virtual Classroom. In these environments, QuickPlace or the Virtual Classroom might require remote access to the Sametime server. This remote access requires QuickPlace or the Virtual Classroom to transmit a user name and password to the Sametime server. This user name and password enables the QuickPlace or Virtual Classroom server to execute servlets on the Sametime server. To prevent unauthorized users from gaining access to this user name and password, you might want to encrypt the connections from the QuickPlace or Virtual Classroom server to the Sametime server with SSL.

Note This release note describes the procedures you must perform to encrypt QuickPlace or Virtual Classroom connections to a Sametime server with SSL while allowing Web browser users to access the Sametime server with unencrypted HTTP. If QuickPlace or the Virtual Classroom server must connect to a Sametime/Domino server that requires SSL for all connections (including connections from Web browsers), you must perform the procedures described in the release note entitled "Ensuring Sametime servlet access when Domino HTTP requires SSL" in the Things You Need to Know section of these release notes.

To encrypt connections from a QuickPlace or Virtual Classroom server to a Domino/Sametime server with SSL (while allowing Web browser users to access the Domino/Sametime server with unencrypted HTTP), perform the procedures below:

1. Ensure the Domino server is enabled for SSL.
2. Obtain the SSL trusted root or SSL server certificate.
3. Install the IBM KeyMan program on the Sametime server.
4. Use the IBM KeyMan program to create a key store token on the Sametime server.
5. Import the SSL trusted root or SSL server certificate to the key store token.
6. Copy the key store token containing the SSL certificate from the Sametime server to the QuickPlace or Virtual Classroom server.
7. Add an entry to the Configuration database Access Control List (ACL) on the Sametime/Domino server.
8. Populate the appropriate fields in the MeetingServices document in the Sametime server Configuration database (stconfig.nsf)
9. Create a Sametime.ini file on the QuickPlace or Virtual Classroom server.

Each of these procedures is described in detail below.

Step 1 - Ensure the Domino server is enabled for SSL

Ensuring the Domino server is enabled for SSL is the first of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server.

The Domino server on which Sametime is installed must be set up to use SSL. To configure a Domino server for SSL, the administrator sets up the Domino Server Certificate Admin application and ensures that an SSL trusted root certificate and SSL server certificate are available to the Domino server. These procedures are described in *Administering the Domino System, Volume 2*.

Note When setting up the Domino/Sametime server to use SSL, the administrator should configure the Internet ports on the Domino/Sametime server to ensure that Web browser users can access the Domino/Sametime server using unencrypted HTTP. For example:

1. Open the Domino/Sametime server Server document.
2. Select Ports-Internet Ports.
3. For "TCP/IP port status," select Enabled. (By default, this setting enables HTTP access over port 80.)
4. For "SSL port status," select Enabled. (By default, this setting enables HTTPS access over port 443.)
5. Save and close the Server document.

Step 2 - Obtaining the SSL trusted root or SSL server certificate

Obtaining the appropriate SSL trusted root or SSL server certificate is the second of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server.

If the Domino HTTP server is set up to encrypt HTTP connections with SSL, the Domino Server Certificate Admin database on the Domino/Sametime server will already contain two certificates 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, it is necessary to import one of the certificates described above into a key store token 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.

Note The Domino Server Certificate Admin database must exist on the Domino server if the Domino server is set up for SSL. This database is created from the Server Certificate Admin template (csrv50.ntf). See the Domino server administration documentation for more information about this database.

For specific examples of how to obtain the appropriate SSL trusted root or SSL server certificate, see "Step 1 - Obtaining the appropriate SSL trusted root or SSL server certificate" in the "Ensuring Sametime servlet access when Domino HTTP requires SSL" topic in the Things You Need to Know section of these release notes.

Step 3 - Installing the IBM KeyMan program on the Sametime server

Installing the IBM KeyMan program on the Sametime server is the third of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server. The KeyMan program is used to create a key store token to manage SSL certificates for the SSL connection from QuickPlace or Virtual Classroom to the Sametime server.

To install the IBM KeyMan program:

1. Double-click on the keyman-1_43.exe file located in the C:\Lotus\Domino directory (or other Sametime server installation directory).

Note The keyman-1_43.exe file is located in the Sametime installation directory. Sametime installs into the directory in which Domino is installed. The default Domino installation directory is C:\Lotus\Domino.

2. When the KeyMan installation program window opens, click Continue.
3. Read, follow directions, and respond appropriately at the following screens:

- Welcome
- License Agreement
- User Information

4. At the Select Components (Java VM) screen, choose the Java VM to run IBM KeyMan. Your options are:
 - java (Sun JavaVM)
 - jview (Microsoft JavaVM)

Because you are installing KeyMan on a Windows server, you should select "jview (Microsoft JavaVM)" unless you have manually installed the Sun Java VM on the Windows machine.
5. At the Select Components (Web browser) screen, choose either Netscape or Internet Explorer as the browser in which KeyMan will run. Click Next.
6. At the Choose Destination Location screen, you can accept the default installation directory or browse and select a different installation directory. Click Next.
7. At the Select Program Folder screen, accept the default folder name or select a different folder. Click Next.
8. At the Setup Complete screen, click Finish.

Step 4 - Using the IBM KeyMan program to create a key store token on the Sametime server

Creating the IBM KeyMan key store token is the fourth of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server.

In this procedure, you create a KeyMan key store token named "stkeys.pfx" and store this token in the Sametime installation directory. In this example, the Sametime installation directory is the default installation directory of C:\Lotus\Domino.

To use the IBM KeyMan program to create a key store database on the Sametime server:

1. Start the IBM KeyMan program on the Windows server on which Sametime is installed. (From the Windows desktop, choose Start · Programs · IBM KeyMan · KeyMan.)
2. At the KeyMan: New/Open window, click the "Create new..." icon (located on the left side of the window).
3. At the KM: New window, select the "PKCS#12 Token (password protected)" option. Click the green check mark to continue.
4. A newly-created token appears. Choose File · Save to save the token.
5. At the "KM: Save token..." window, enter and then re-enter the passphrase that you will use to protect this key store token. You will be required to enter this password any time you open this token to manage SSL certificates. Click the blue arrow to continue.
6. At the "KM Save token...Save PKCS#12 Token" window, complete the "Save to file" and "File format" fields as described below:

Save to file: Enter the directory path and file name for the key store token in the "Save to file" field. It is recommended that you save the key store token in the Sametime installation directory and provide it with the filename of "stkeys.pfx."

For example, in the "Save to file" field, you can specify the following directory path: C:\Lotus\Domino\stkeys.pfx.

File format: Accept the default value of PKCS#12 / PFX.

Click the green check mark to continue.

Note You can leave the "Wrap key ring into a Java class" option unselected.

Step 5 - Import the SSL trusted root or SSL server certificate to the key store token

Importing the SSL trusted root or SSL server certificate used by the Domino server is the fifth of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server.

In this procedure, you import the SSL certificate into the key store token you have just created. You must import either the SSL trusted root certificate or the SSL server certificate used by the Domino server for SSL connections. This certificate is the certificate you were instructed to obtain in "Step 2 - Obtaining the SSL trusted root or SSL server certificate" above.

Note This procedure assumes you have exported the required SSL certificate to a file on the local operating system and explains how to import this file to the IBM KeyMan keystore database. The IBM KeyMan 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 location. For more information about these options for importing SSL certificates, see the KeyMan documentation. To access this documentation, select Start - Programs - IBM KeyMan - Documentation from the Windows desktop.

To import the SSL certificate to the IBM KeyMan key store token:

1. If the key store token (stkeys.pfx) you just created is already open, skip to step 2. If the key store token is closed, use the following procedure to open it:
 - a. From the Sametime server Windows desktop, choose Start - Programs - IBM KeyMan - KeyMan.
 - b. At the KeyMan: New/Open window, click the "Open existing..." icon (located on the right side of the window).
 - c. At the "KeyMan: Open... Open" window, select Local Resource. Click the blue arrow to continue.
 - d. At the next "KeyMan: Open... Open" window, select "Open a file." Click the blue arrow to continue.
 - e. Browse to and select the C:\Lotus\Domino\stkeys.pfx token (or <Sametime install directory>\stkeys.pfx token). Click the blue arrow to continue.
 - f. Enter the passphrase you specified for the stkeys.pfx token when you created the token. Click the green check mark to continue.
2. When the stkeys.pfx IBM KeyMan token opens, select File - Import.
3. At the "KM: Import..." window, select "Local resource." Click the blue arrow to continue.
4. At the next "KM: Import..." window, select "Open a file." Click the blue arrow to continue.
5. At the next "KM: Import..." window, browse to and select the SSL certificate that you obtained in "Step 2 - Obtaining the appropriate trusted root or SSL server certificate." Click the blue arrow to continue.
6. At this point, the SSL certificate is imported into the KeyMan key store token. To verify the certificate was imported successfully, select Trusted CA Certificates from the drop-down list in the KeyMan key store token. If the SSL certificate name appears in the Trusted CA Certificates list, the certificate was imported successfully.

Note Regardless of whether you import an SSL trusted root certificate or the SSL server certificate of the Domino server, the name of the server certificate should appear in the Trusted CA Certificates list of the key store token.

Step 6 - Copy the key store token containing the SSL certificate from the Sametime server to the QuickPlace or VirtualClassroom server

Copying the stkeys.pfx file from the Sametime server to the QuickPlace or VirtualClassroom server is the sixth of eight procedures required to use SSL to encrypt connections from a QuickPlace or VirtualClassroom server to a Sametime/Domino server.

Copy the stkeys.pfx file you just created on the Sametime server to the QuickPlace or Virtual Classroom server that will access the Sametime server. You can copy the stkeys.pfx file to any directory on the QuickPlace or Virtual Classroom server. Later in this process, you will specify the location of this stkeys.pfx file in the Sametime.ini file on the QuickPlace or Virtual Classroom server.

The recommended directory for the stkeys.pfx file is the QuickPlace or Virtual Classroom installation directory.

Note The stkeys.pfx file is **not** used on the Sametime server; however, it is not necessary to delete the file from the Sametime server. You might want to keep a copy of this file on the Sametime server. If you add another QuickPlace or Virtual Classroom server to your environment, and you want to encrypt connections from that server with SSL, you can skip steps 2 through 6 of this procedure and just copy the existing stkeys.pfx token to the newly-installed QuickPlace or Virtual Classroom server.

Step 7 - Add an entry to the Configuration database Access Control List (ACL) on the Sametime/Domino server

Adding an entry to the Configuration database ACL on the Sametime/Domino server is the seventh of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server.

Note This procedure is required to enable QuickPlace or the Virtual Classroom to authenticate when accessing servlets on the Sametime server, regardless of whether you are encrypting connections with SSL. This procedure is also described in the release note entitled "Enabling QuickPlace or Virtual Classroom to access Sametime" in the Things You Need to Know section of these release notes. If you have already performed this configuration, skip to step 9 below and ensure that the Sametime.ini file on the QuickPlace or Virtual Classroom server contains the parameters needed to support SSL connections to the Sametime server.

The QuickPlace or Virtual Classroom server must authenticate to execute servlets on the Sametime server. To allow the QuickPlace or Virtual Classroom server to authenticate, you must enter a user name in the ACL of the Configuration database (stconfig.nsf) on the Sametime server.

When adding this user name to the ACL of the stconfig.nsf database on the Sametime server, ensure that the user name is provided with the:

- SametimeAdmin role (mandatory)
- Manager access level (recommended)

The name you enter in the ACL of the Configuration database must exist in the Domino Directory or LDAP directory that defines the Sametime community and must have a defined password. See the recommendation below before entering a name in the ACL of the Configuration database.

In a subsequent step, you will enter this user name and password in a Sametime.ini file on the QuickPlace or Virtual Classroom server.

Recommendation: IBM Lotus software recommends that you create a special account in the directory for remote access to the Sametime servlets. This entry should be used only for the purpose described above. For example, you might create a Person document in a Domino Directory for the user name "SametimeServletAccess" and specify an Internet password for this user name. You can enter this user name and password in the Sametime.ini file and the ACL of stconfig.nsf, but this directory entry should not be used for any other purpose.

Step 8 - Populate the appropriate fields in the MeetingServices document in the Sametime server Configuration database (stconfig.nsf)

Populating the appropriate fields in the MeetingServices document in the Sametime server Configuration database is the eighth of nine procedures you must perform to enable a QuickPlace or Virtual Classroom application to authenticate when accessing servlets on the Sametime server.

Note This procedure is required to enable QuickPlace or the Virtual Classroom to authenticate when accessing servlets on the Sametime server, regardless of whether you are encrypting connections with SSL. This procedure is also described in the release note entitled "Enabling QuickPlace or Virtual Classroom to access Sametime" in the Things You Need to Know section of these release notes. If you have already performed this configuration, skip to step 9 below and ensure that the Sametime.ini file on the QuickPlace or Virtual Classroom server contains the parameters needed to support SSL connections to the Sametime server.

In this procedure, you add the user name and password associated with the directory entry discussed above to fields in the MeetingServices document in the Configuration database:

1. If necessary, use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
2. In the right-hand pane, open the MeetingServices document by double-clicking on the date associated with the document.
3. Scroll to the bottom of the MeetingServices document until you see the Remote Services Access heading.

- Under the Remote Services Access heading, populate the eight fields with the user name and password associated with the directory entry discussed in "Step 7 - Add an entry to the Configuration database Access Control List (ACL) on the Sametime/Domino server" above.

For example, if you created a directory entry with a user name of "SametimeServletAccess" and a password of Sametime, populate the eight fields under the Remote Services Access heading as shown below:

Meeting Management Username: SametimeServletAccess
Meeting Management Password: Sametime

Recorded Meeting Management Username: SametimeServletAccess
Recorded Meeting Management Password: Sametime

Materials Refresh Username: SametimeServletAccess
Materials Refresh Password: Sametime

Materials Control Username: SametimeServletAccess
Materials Control Password: Sametime

- Save and close the MeetingServices document. Also, close the Configuration database.

Step 9 - Create a Sametime.ini file on the QuickPlace or Virtual Classroom server

Creating a Sametime.ini file on the QuickPlace or Virtual Classroom server is the last of eight procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime/Domino server.

Note This procedure is also required to enable QuickPlace or Virtual Classroom to authenticate when accessing servlets on the Sametime server. If you have already performed the procedure described in the release note entitled "Enabling QuickPlace or Virtual Classroom to access Sametime" in the Things You Need to Know section of these release notes, the Sametime.ini file will already exist on the QuickPlace or Virtual Classroom server and it will not be necessary to create it as described below. However, it will be necessary to add the settings to the Sametime.ini file required to support SSL. The additional settings required to support SSL are listed below.

The Sametime.ini file on the QuickPlace or Virtual Classroom server must contain the parameters that enable the Sametime server to be accessed using SSL. You must create the Sametime.ini file in the QuickPlace or Virtual Classroom installation directory on the QuickPlace or Virtual Classroom server.

Follow these instructions to manually create a Sametime.ini file in the QuickPlace or Virtual Classroom installation directory.

- Open a text editor on the QuickPlace or Virtual Classroom server.
- Create a text file consisting of a [Config] section and the settings listed below:

[Config]

VPS_Name= (This setting should specify the canonical name of the Domino server to which QuickPlace or Virtual Classroom will connect. An example value is VPS_Name=CN=Sametimeserver/OU=East/O=Acme.)

SametimeCluster= (This setting should also specify the canonical name of the Domino server, e.g.: SametimeCluster=CN=Sametimeserver/OU=East/O=Acme.)

ConfigurationHost= (This Sametime.ini setting should specify the fully-qualified DNS name of the Sametime server, e.g.: ConfigurationHost=Sametimeserver.east.acme.com.)

ConfigurationPort=443 (This setting should specify port 443.)

ConfigurationSSLEnabled=true

SSLManagerClassName=com.lotus.sametime.configuration.IBMJSSE118Manager (This Sametime.ini parameter must specify the IBMJSSE118Manager class exactly as shown.)

javax.net.ssl.keyStore=c:/lotus/domino/stkeys.pfx (This setting must specify the complete file path, including the filename, of the KeyMan key store token created in "Step 4 - Using the IBM KeyMan program to create a key store token on the Sametime server.")

Note that it is not a requirement to name the key store token "stkeys.pfx." The name of the token is at your discretion. The only requirement is that the complete file path of the token is specified in the Sametime.ini file settings.

javax.net.ssl.trustStore=c:/lotus/domino/stkeys.pfx (This Sametime.ini file setting must also specify the complete file path of the KeyMan key store token created in "Step 3 - Using the IBM KeyMan program to create a key store token on the Sametime server.")

javax.net.ssl.keyStorePassword=sametime (This Sametime.ini file setting must specify the passphrase you provided for the KeyMan key store token when you created the token. This passphrase was specified in "Step 4 - Using the IBM KeyMan program to create a key store token on the Sametime server." The example shown here assumes the passphrase is "sametime." Alter the setting to reflect your passphrase.)

javax.net.ssl.keyStorePassword=sametime (This Sametime.ini file setting must also specify the passphrase you provided for the KeyMan key store token when you created the token. The example shown here also assumes the passphrase is "sametime." Alter the setting to reflect your passphrase.)

SametimeAdminUsername= (This Sametime.ini setting should specify the name of the user account that was added to the ACL of the Configuration database on the Sametime server in "Step 7 - Add an entry to the Configuration database ACL on the Sametime/Domino server.")

SametimeAdminPassword= (This Sametime.ini setting should specify the password associated with the administrator account above.)

3. After creating the text file containing the parameters described above, save the file to the QuickPlace or Virtual Classroom installation directory under the name "Sametime.ini."

This concludes the procedures required to use SSL to encrypt connections from a QuickPlace or Virtual Classroom server to a Sametime server (while allowing Web browsers to access the server via unencrypted HTTP).

Tip If you add another QuickPlace or Virtual Classroom server to your environment, you can copy the stkeys.pfx file and the Sametime.ini file that you created in this procedure to the newly-added server. Using the existing files prevents you from having to perform all eight steps above each time you add a new QuickPlace or Virtual Classroom server to your environment.

Sametime and QuickPlace cannot be installed on the same machine

Sametime server

Sametime and QuickPlace cannot be installed on the same machine

A Sametime server and a QuickPlace server cannot be installed on the same machine. A Domino server limitation prevents all Java class files required by both of these servers from loading when both Sametime and QuickPlace are installed on the same machine.

A Sametime server and the IBM Lotus Virtual Classroom also should not be installed on the same machine for this reason.

Community Services administration changes can occur without server restart

Sametime Administration Tool

Connectivity and log changes occur without server restart

You should not change the Community Services Network host name or port number settings on the Configuration-Connectivity-Networks and Ports tab in the Sametime Administration Tool unless you want the changes to take effect. The "Networks and Ports" configuration tab contains text that indicates it is necessary to restart the Sametime server for changes on the tab to take effect. However, changes on this tab can take effect without a server restart.

Consider the following scenario:

1. An administrator opens the Configuration-Connectivity-Networks and Ports tab in the Sametime Administration Tool and changes the Community Services Network-Address for HTTP-tunneled connections-Port number setting from 8082 to 80.
2. The administrator clicks the Update button on the Networks and Ports tab.
3. The administrator then decides that the port number change should not be implemented immediately and decides to wait to restart the server to finish implementing the port number configuration change.

Note that any change to the Community Services Network connectivity settings on the "Networks and Ports" tab will take effect without a server restart. The update will occur according to the time interval specified in the "How often to poll for new servers added to the Sametime Community (minutes)" setting located on the Configuration-Community Services tab of the Sametime Administration Tool.

Changing the Community Services Network connectivity settings on the "Networks and Ports" tab of the Sametime Administration Tool changes the data that is sent to the Community Services multiplexer and might cause connectivity problems or affect server performance. If you change Community Services Network connectivity settings, you should restart the server immediately.

The following Community Services and logging configuration settings will also be updated according to the time interval specified in the "How often to poll for new servers added to the Sametime Community" setting. You should not alter these configuration settings in the Sametime Administration Tool unless you want the changes to go into effect.

All settings on the following tabs of the Sametime Administration Tool will be updated without a server restart:

- The Configuration-Community Services tab
- The Configuration-Community Services-Anonymous Access tab
- The Logging Settings-General tab
- The Logging Settings-Capacity Warnings tab

Accessibility/Section 508 issues

Sametime Administration Tool

Can't tab between admin client and Domino Directory access

Once users access the Domino Directory - Access control from the Sametime administration client, they cannot use the keyboard to move focus back to the administration client. Users must close the browser window, then restart the browser and log on to the administration client again.

Web browsers

Can't tab between text and Meeting Room in Meeting Tester

When testing a meeting, an end user cannot tab between the Meeting Room and the help text in the browser window.

Sametime Meeting Room client

Cannot sort by raised hands without using mouse

Users might be unable to use the keyboard to sort the Participant List according to raised hands. Users can still sort by raised hands by clicking the hand icon column header in the Participant List.

UNIX clients

Keyboard shortcut for new line on Unix clients

For Unix clients, use Ctrl+Enter to enter a new line. On Windows systems, the new line shortcut is SHIFT+Enter.

Sametime Connect client

Missing hotkeys in Sametime Connect for the desktop client

In Sametime Connect for the desktop, the following hotkeys, or mnemonics, are missing. Users can still tab to each of these controls.

- The Alert Me When button in the Specific Alerts section of the Alerts tab. Users access the Alerts tab by choosing Options - Preferences.
- The OK and/or Cancel buttons in the following situations:
 - The My Available Tools dialog box that appears after users log on to Sametime Connect for the desktop.
 - The Edit Nickname dialog box.
 - The Rename Personal Group dialog box.
 - The Add to/Replace List dialog box.
 - The Send Announcement dialog box.

Sametime Meeting Room client

Missing mnemonic in A/V Preferences dialog box

The Help button in the A/V Preferences dialog box does not have a mnemonic. Users can still activate the button by tabbing to it and pressing ENTER.

Sametime Meeting Room client

Mnemonics disappear during an online meeting

During an online meeting, you can press the Alt+w and Alt+s keys to switch between the whiteboard and screen sharing tools. Note that if you use these keys to make more than four total switches during a meeting, the mnemonics may disappear from the Meeting Room client and all keyboard shortcuts may become inoperable in the Meeting Room client.

Sametime Meeting Room client

SHIFT+TAB won't move focus backward through column headers

Pressing SHIFT+TAB does not move the focus backward through the column headers in the Participant List or the Participant List details.

Sametime Connect client

Tabbing problem in Add to Privacy List dialog box

In Sametime Connect for the desktop, if a user enters a name with multiple matches in the Directory while adding a name to the Who Can See If I Am Online List, a list of these matches appears in the Add to Privacy List dialog box. When users tab to this list, there is no visible indication that the list has focus. Even though the focus is not visible at first, users can use the arrow keys to move through the names in the list once the list has focus. Once users use the arrow keys to move through the names, the focus will become visible.

Sametime Administration Tool

Unable to tab between admin tool and admin Help

Once users opens the administrator's Help from the Sametime administration tool, they are unable to use the keyboard to move the focus back to the administration tool. Users can press ALT+F4 to close the browser window, then restart the browser and log on to the administration client again. Users can also download the PDF version of the administrator's guide from the Lotus Developer Domain Web site at <http://www.ibm.com/lotus/ldd>.

Sametime Connection documents are case-sensitive

Sametime server

Sametime Connection documents are case-sensitive

A Sametime Administrator can create a Connection document of the Connection Type "Sametime" to enable a meeting started on one Sametime server to be simultaneously active on another Sametime server. This functionality is frequently called "invited servers." In this scenario, a meeting is started on one Sametime server and that Sametime server "invites" another Sametime server to the meeting. The server on which the meeting is started is the "source" server and the server that is invited to the meeting is the "destination" server.

The procedure for creating these Connection documents is described in the topic "Creating Connection Records to connect Sametime servers" in the Deploying Multiple Sametime Servers chapter of the *Sametime 3.0 Administrator's Guide*.

When creating the Connection document, you must enter the invited server's name in the "Destination server" field of the Connection document. The server name entered in the "Destination server" field must be an exact case-sensitive match with the server name as it appears in the Server document in the Domino directory. If the server name in the Destination server field is not an exact case-sensitive match with the server name on the Server document, the meeting will not be available on the invited (or destination) server.

For example, when creating a Connection Document to connect two Sametime servers, the administrator must perform the following procedure:

1. Open the Sametime Administration Tool.
2. Choose Configuration-Connectivity-"Servers in this Community."
3. Complete the following fields to create the Connection document:

Destination server - Enter the name of the Destination server in the Domino hierarchical server name format that includes the domain name of the server. For example, "sametimeB.acme.com/ACME."

Destination server IP address - Enter the fully-qualified DNS name or IP address of the destination server. If this field is left blank, meetings started on the source server will not become active on the destination server.

In the example above, the name of the server in the "Destination server" field must be an exact case-sensitive match to the server name on the Server document. If "sametimeB.acme.com/ACME" is entered in the Destination server field of the Connection document, the server name must appear exactly this way in the Server document in the Domino directory. If the Server document lists the name as "SametimeB.acme.com/ACME" or "sametimeB.acme.com/Acme" the destination server cannot be invited to the meeting because the server name is not a case-sensitive match.

Sametime Connect and HTTPS connections on port 443 or 563

Sametime Connect client

Sametime Connect and HTTPS connections on port 443 or 563

This release note discusses issues pertaining to Sametime Connect client connectivity on port 443. These issues include:

- Connecting to the Community Services on port 443 when the Domino HTTP server is configured to listen for SSL connections on port 443
- Sametime 2.5 Connect client compatibility issue when connecting to a Sametime 3.0 server on port 443 or 563
- Sametime 3.0 Connect client compatibility issue when connecting to a Sametime 2.5 server on port 443 or 563
- Community Services multiplexer on Sametime 3.0 server does not forward HTTPS connections on port 443 to the Domino HTTP server

Connecting to the Community Services on port 443 when the Domino HTTP server is configured to listen for SSL connections on port 443

Sametime installs on a Domino server. Web browser users connect to the Domino HTTP server when accessing the Sametime server. If the Domino HTTP server is configured to support SSL for Web browser connections, the Domino HTTP server is usually configured to listen for these HTTPS connections on port 443 or port 563.

Some Sametime Connect clients may operate in networks that require the clients to connect to the Internet or intranet through an HTTPS proxy. Many network environments that require users to connect through an HTTPS proxy only allow outbound connections to occur on port 443. If a Sametime Connect client operates in such an environment, the following configurations must exist on the Sametime Connect client and the Sametime server for the connection to be successful:

In the Sametime Connect client Sametime Connectivity tab:

- The "Community port" setting must specify port 443.
- The "Use proxy" and "Use HTTPS proxy" settings must be selected. The IP address or DNS name of the HTTPS proxy server and port number used to connect to the HTTPS proxy server are also specified.
- In the Sametime Administration Tool on the Sametime server, the Community Services Network - Address for HTTPS-tunneled client connections - Port number setting must specify port 443.

With these configurations, the Sametime Connect client connects to the HTTPS proxy, and the proxy connects to the Sametime server on behalf of the Sametime Connect client. The connection from the proxy server to the Sametime server Community Services occurs on port 443. The Community Services on the Sametime server must be configured to listen for the HTTPS connections on port 443 to ensure the connection can succeed.

Note The configurations above enable Sametime Connect to establish an HTTP connection to a Sametime server through an HTTPS proxy server. This connection is not encrypted with SSL.

If the Domino HTTP server is also configured to listen for HTTPS connections on port 443, a conflict occurs because the Sametime Community Services are also configured to listen for HTTPS connections on the same port number.

In this scenario, you must assign an additional IP address to the Sametime server to ensure that both Web browser users and Sametime Connect client users can connect to the Sametime server on port 443. This configuration requires the following steps:

- Bind the DNS name for the Sametime server to the Sametime HTTP server.
- Add a new IP address to the Sametime server machine.
- Map the new IP address to a new DNS name for the Sametime Community Services. This configuration is performed on the DNS server.
- Use the Sametime Administration Tool to add the new DNS name to the Community Services connectivity settings on the Sametime server. This configuration enables the Community Services to listen for HTTPS connections on the new DNS name.
- Configure the Sametime Connect clients to connect to the new Community Services DNS name.

Note The configuration described below can enable either a Sametime 2.5 Connect client or a Sametime 3.0 Connect client to connect to a Sametime 3.0 server on port 443 or 563.

Step-by-step instructions for these configurations are provided below.

Step 1 - Bind the base DNS name for the Sametime server to the Sametime HTTP server.

1. Open the Sametime Administration Tool and select Configuration-Connectivity-Networks and Ports-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.
2. Under the Basics heading in the "Host name" field, enter the base DNS name for the Sametime HTTP server (for example, www.sametime1.com).

Under the Basics heading 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 (e.g. www.sametime1.acme, 127.0.0.1)

3. Click "Save & Close" at the top of the Server document. After the document closes, close the Server-Servers view of the Domino Directory.

Step 2 - Add a new IP address to the Sametime server machine.

To add a new IP address to the Sametime server, you can either install an additional Network Interface Card (NIC) in the Sametime server machine or assign multiple IP addresses to a single NIC.

To assign multiple IP addresses to a single NIC on a Windows machine:

1. Open the Windows Control Panel.
2. Click the Protocols tab.
3. Select TCP/IP Protocols-Properties-Specify an IP Address.
4. Click the Advanced tab.
5. Use the Advanced IP Addressing screen to assign multiple IP addresses to a single NIC.

Step 3 - Set up your DNS server to map the IP address to a DNS name for Sametime Community Services.

After you have added a new IP address to the Sametime server, set up your DNS server to map the new IP address to a DNS name for the Sametime server Community Services.

For the Community Services, map the IP address to the DNS name "community-xxx.xxx.xxx" (where xxx.xxx.xxx is the DNS name that was bound to the Sametime HTTP server in step 1 above).

For example, you would map the new IP address to the DNS name "community-www.sametime1.com."

Step 4 - Configure the HTTPS-tunneling settings in the Sametime Administration Tool

You must specify the new DNS name and port number for Community Services HTTPS connections in the Sametime Administration Tool.

1. Open the Sametime Administration Tool and select Configuration-Connectivity-Networks and Ports.
2. In the Community Services Network-Address for HTTPS-tunneled connections settings, specify the following:

Host name: community-xxx.xxx.xxx (Where xxx.xxx.xxx is the DNS name that was bound to the Sametime HTTP server. For example, community-www.sametime1.com.)

Port number: 443

With this configuration, the Sametime Community Services multiplexer will listen for HTTPS-tunneled connections on host name community-www.sametime1.com on port 443.

Step 5 - Configure the Sametime Connect clients to connect to the new DNS name of the Community Services

To connect to a Sametime server configured to listen for HTTPS connections on the host name and port specified above, the Sametime Connect client must have the following settings in the Sametime Connectivity tab:

- The "Host" setting must specify community-www.sametime1.com.
Note If a Sametime 2.5 Connect client connects to a Sametime 3.0 server using HTTPS on port 443 or 563, it is only necessary to enter the server name (www.sametime1.com) in the "Host" setting of the Sametime 2.5 Connect client. For example, enter "www.sametime1.com" instead of "community-www.sametime1.com" in the "Host" field. For more information, see "Sametime 2.5 Connect client compatibility issue when connecting to a Sametime 3.0 server on port 443 or 563" below.
- The "Community port" setting must specify 443.
- "Use proxy" and "Use HTTPS proxy" must be selected. Enter the host name and port on which the Sametime Connect client connects to the HTTPS proxy.

Sametime 2.5 Connect client compatibility issue when connecting to a Sametime 3.0 server on port 443 or 563

The Sametime 2.5 Connect client is designed to use HTTPS tunneling on ports 443 or 563 to connect to a server that uses multiple IP addresses.

When a Sametime 2.5 server is configured to listen for HTTPS-tunneled client connections on port 443 or 563, the server listens for Community Services connections on the server name "Community-servername." For example, if your Sametime 2.5 server is named sametimeserver.acme.com, the server listens for HTTPS-tunneled Community Services connections on ports 443 or 563 on the server name "Community-sametimeserver.acme.com." The Sametime 2.5 server is hard-coded to prepend the string "Community-" to its server name when listening for Community Services connections on ports 443 or 563. This design in the Sametime 2.5 server accommodates the multiple IP address issues discussed in "Connecting to the Community Services on port 443 when the Domino HTTP server is configured to listen for SSL connections on port 443" above.

The Sametime 2.5 Connect client is also hard-coded to prepend the string "Community-" to its Host setting when its "Community port" setting specifies port 443 or 563. For example, assume the following settings exist in the Sametime Connectivity tab of a Sametime 2.5 Connect client:

- Host - "sametimeserver1.acme.com"
- Community port - Either port 443 or port 563 is specified.

With this configuration, the Sametime 2.5 Connect client attempts the connection to the server name "Community-sametimeserver1.acme.com" even though the string "sametimeserver1.acme.com" is entered in its Host setting.

Because the Sametime 2.5 Connect client automatically prepends the string "Community-" to its host name, it is not necessary to enter the string "Community-servername" in the Sametime 2.5 Connect client when this client connects to a Sametime 3.0 server that is configured to listen for HTTPS connections on multiple IP addresses.

Note also that when a Sametime 3.0 server listens for HTTPS-tunneled connections from Sametime 2.5 Connect clients, the additional DNS name assigned to the Community Services on the Sametime 3.0 server must begin with the "Community-" string, as described in "Connecting to the Community Services on port 443 when the Domino HTTP server is configured to listen for SSL connections on port 443" above. If the Sametime 3.0 Community Services DNS name does not begin with the "Community-" string, the Sametime 2.5 Connect client cannot connect to the Sametime 3.0 server.

Sametime 3.0 Connect client compatibility issue when connecting to a Sametime 2.5 server on port 443 or 563

If a Sametime 3.0 Connect client connects via HTTPS-tunneling to a Sametime 2.5 server on port 443 or 563, the Sametime 3.0 Connect client does not prepend the "Community-" string to its host name when making the connection to the Sametime 2.5 server.

The Sametime 2.5 server is hard-coded to prepend the string "Community-" to its server name when listening for HTTPS connections on port 443 or 563. To ensure the Sametime 3.0 Connect client can connect to the Sametime 2.5 Community Services on port 443 or 563, the string "Community-" must be manually added to the Host name in the Sametime Connectivity tab in the Sametime 3.0 Connect client.

Manually adding the "Community-" string to the Host name in the Sametime 3.0 Connect client ensures that the client attempts the connections on the name on which the Sametime 2.5 server listens for the connections.

For example, to ensure a Sametime 3.0 Connect client can connect on port 443 or 563 to the Sametime 2.5 server named "sametimeserver1.acme.com," the following settings must exist in the Sametime Connectivity tab of the Sametime 3.0 Connect client:

- Host - "Community-sametimeserver1.acme.com."
- Community port - Either port 443 or port 563 is specified. (Specify the port on which the Sametime 2.5 server listens for HTTPS-tunneled connections.)

Community Services multiplexer on Sametime 3.0 server does not forward HTTPS connections on port 443 to the Domino HTTP server

A Sametime 3.0 server can simultaneously listen for HTTP connections to multiple services on port 80 when the Sametime server machine includes a single IP address. For example:

- A Web browser can connect to the Domino HTTP server on a Sametime server on port 80.
- A Sametime Connect client can make an HTTP-tunneled connection to the Sametime Community Services on port 80.
- A Sametime Meeting Room client can make HTTP-tunneled connections to both the Sametime Community Services and Meeting Services on port 80.

All of these connections can occur to the same DNS name using port 80. On a Sametime 3.0 server, it is not necessary to assign separate IP addresses to the HTTP Services, Community Services, and Meeting Services to enable connections to all services to occur using a single DNS name on port 80. The design of the Community Services multiplexer on a Sametime 3.0 server makes this capability possible. The Community Services multiplexer can listen for HTTP connections from Web browsers, Sametime Connect clients, and Sametime Meeting Room clients on port 80. The Community Services multiplexer examines these connections and then forwards the connections to the appropriate service. For example, the Community Services multiplexer forwards the Web browser connections to the Domino HTTP Server, the Community Services connections to the Community Services, and the Meeting Services connections to the Meeting Services.

Note that the Community Services multiplexer on a Sametime 3.0 server cannot listen for connections on port 443 or 563 and then forward these connections to the Domino HTTP server. The Community Services multiplexer can forward HTTP connections on port 80 to the Domino HTTP server, but not connections on port 443 or 563. For this reason, a Sametime 3.0 server must be assigned multiple IP addresses when both the Domino HTTP server and the Sametime Community Services on the Sametime server must listen for connections on port 443 or 563.

Note The Community Services multiplexer on a Sametime 3.0 server also cannot listen for HTTPS connections to the Sametime Meeting Services or Community Services on ports 443 or 563 and forward these connections to the Community Services and Meeting Services. HTTPS-tunneling to the Sametime Meeting Services is not supported. Sametime Meeting Room clients cannot connect to the Sametime Meeting Services through an HTTPS proxy server.

Enhance security by disabling RAPFileServlet

Sametime server

Enhance security by disabling RAPFileServlet

IBM Lotus software recommends that you enhance the security of the Sametime 3.0 server by disabling the RAPFileServlet following the Sametime 3.0 installation.

To disable the RAPFileServlet, you must remove an entry from the the servlet.properties file in the Data subdirectory of the Sametime installation directory. (The default location of the servlet.properties file is C:\Lotus\Domino\Data.)

To disable the RAPFileServlet:

1. Open a text editor on the Sametime server machine.
2. Use the text editor to open the servlet.properties file in the C:\Lotus\Domino\Data directory (or <Sametime install directory>\Data).
3. Locate the following servlets.startup line at the bottom of the servlet.properties file.

```
servlets.startup=bootstrap scs auth admin mmapi stcal fileupload rapfile
```
4. In the line above, delete the "rapfile" text string. The correctly edited line will appear as follows:

```
servlets.startup=bootstrap scs auth admin mmapi stcal fileupload
```
5. Save and close the servlets.properties file.
6. Restart the Sametime server for the change to take effect.

Sametime is not supported on IBM zSeries servers

Sametime server

Sametime is not supported on IBM zSeries servers

Any references in any Sametime documentation that indicate Sametime can be installed on an IBM zSeries server are not correct. Sametime cannot be installed on or interoperate with IBM zSeries servers.

Attach a meeting material immediately after installing or restarting the EMS

Enterprise Meeting Server and server clusters

Attach a meeting material immediately after starting the EMS

Immediately after installing or restarting the Enterprise Meeting Server (EMS), the administrator should create a meeting in the EMS and attach a meeting material to the meeting. This meeting can be a temporary meeting created strictly for the purpose of attaching a meeting material.

If you fail to attach a meeting material to a meeting in the EMS immediately after installing or restarting the EMS, the following problems may occur:

- If a meeting that contains a meeting material attachment is deleted, the meeting material associated with that meeting will not be deleted.
- If the user begins the process of creating a meeting, attaches a meeting material, and then closes the browser before saving the meeting, the attached meeting material will not be deleted.

Because these problems may cause unnecessary increases in the size of the DB2 database used by the EMS, it is recommended that you attach a meeting material to a temporary meeting immediately after installing or restarting the EMS.

Note that failure to attach a meeting material immediately after installing or restarting the EMS will also cause the exception below to appear in the EMS log files:

```
javax.naming.NamingException. Root exception is java.lang.NullPointerException
```

Explanation

The EMS contains a meeting materials servlet that is responsible for deleting meeting materials from the DB2 database that are not associated with any meeting. This servlet runs every half hour. There is a problem in the timer that controls the execution of the meeting materials servlet that may cause this servlet to use uninitialized code to connect to the DB2 database. This problem will not occur if you create a temporary meeting and attach a meeting material to the EMS immediately after the EMS is started.

Sametime 3.1 cannot operate with Netegrity Siteminder

Sametime server

Sametime 3.1 cannot operate with Netegrity SiteMinder

Netegrity SiteMinder does not support Domino R6. Because Sametime 3.1 must be installed on a Domino 6.02 server, Sametime 3.1 will not operate with Netegrity SiteMinder.

Notes 6 client required to use Calendaring and Scheduling with Sametime

Sametime server

Notes 6 needed to use calendaring and scheduling with Sametime

Lotus Notes/Domino calendaring and scheduling capabilities can be integrated with a Sametime server to enable users to use the Notes calendaring and scheduling features to schedule meetings on a Sametime server.

These capabilities are limited to Lotus Notes R6.x clients only. Lotus Notes R5.x clients cannot use the Notes calendaring and scheduling features to interoperate with a Sametime server.

No audio/video support for Sametime Meeting Room on Unix clients

UNIX clients

No audio/video support for Sametime Meeting Room on Unix Clients

The Sametime Meeting Room for Unix does not provide audio/video support. The menu items related to audio/video have been disabled.

Print Capture not available on Unix clients

UNIX clients

Print Capture not available on Unix clients

The Print Capture feature is not available with the Unix clients. Refer to the *Sametime User's Guide* for a list of supported file types for display.

Granting permissions using Netscape and Unix client

UNIX clients

Granting permissions using Netscape and Unix client

When using the Netscape browser, the user grants permissions by clicking on "remember this decision". The permissions need to be granted only once. This is a Netscape design feature.

Required library for application sharing on Linux and Solaris systems

UNIX clients

Library for application sharing on Linux and Solaris systems

In order to load Application Sharing native code on Linux and Solaris platforms, the following library is required on the client machine: `libz.so.1` which resides in `/usr/lib`

Using page up/page down keys to present whiteboard files

Sametime Meeting Room client

Use page up/page down keys when presenting whiteboard files

When presenting a whiteboard file during an online meeting, you can use the PageUp and PageDown keys on the computer keyboard to page through the presentation. This capability was unavailable in previous Sametime releases.

Sametime Installation Guide NSF file has updated information

Sametime server

Sametime Installation Guide NSF file has updated information

The Sametime 3.1 server includes a PDF version and an NSF version of the *Sametime Installation Guide* (`stinstall.nsf` and `stinstall.pdf`).

The `stinstall.nsf` version of the *Sametime Installation Guide* contains system requirements updates that are not included in the `stinstall.pdf` version. The `stinstall.nsf` version also includes updates to the "Installing other Sametime 3.1 features" chapter that are not included in the `stinstall.pdf` version.

Consult the `stinstall.nsf` version of the *Sametime Installation Guide* for the updated installation documentation.

Upgrading a Sametime 3.0 server connected to the EMS to Sametime 3.1

Sametime server

Upgrading a Sametime 3.0 server connected to the EMS to 3.1

This release note explains how to upgrade a Sametime 3.0 server that has been added to the Sametime Enterprise Meeting Server (EMS) to Sametime 3.1.

Upgrading a Sametime 3.0 server added to the EMS to Sametime 3.1 is described in three steps:

1. Remove the Sametime 3.0 server from the EMS.
2. Upgrade the Sametime 3.0 server to Sametime 3.1.
3. Add the upgraded Sametime 3.1 server to the EMS.

Each of these steps is described in greater detail below.

Remove the Sametime 3.0 server from the EMS

Removing the Sametime 3.0 server from the EMS is the first of three procedures required to upgrade a Sametime 3.0 server that has been added to the EMS to Sametime 3.1. Use the Sametime EMS Administration Tool to remove a Sametime 3.0 server from the EMS.

To remove the Sametime 3.0 server from the EMS:

1. Browse to and access the Sametime EMS Administration Tool on the EMS machine.
2. In the Sametime EMS Administration Tool, select Configuration -> Meeting Cluster -> Edit/Remove a Meeting Server.
3. Select the Sametime server that you want to remove from the drop down menu.
4. Click the Remove button and click OK when prompted for confirmation about removing the server.

Upgrade the Sametime 3.0 server to Sametime 3.1

Upgrading the Sametime 3.0 server to Sametime 3.1 is the second of three procedures required to upgrade a Sametime 3.0 server that has been added to the EMS to Sametime 3.1.

In this procedure you upgrade the Sametime 3.0 server you removed from the EMS to Sametime 3.1.

To upgrade from Sametime 3.0 to Sametime 3.1:

1. Install Domino 6.0.2 on top of the existing Domino R5 server that supported the Sametime 3.0 server. It is not necessary to uninstall either Domino R5 or Sametime 3.0 before installing Domino 6.0.2. Install Domino 6.0.2 into the same directory in which the Domino R5 server is installed.
2. Install the Sametime 3.1 server on top of the Domino R6 server. (It is not necessary to uninstall Sametime 3.0 before performing this step.)

For more detailed instructions on upgrading from Sametime 3.0 to Sametime 3.1, or installing the Sametime 3.1 server, see the Sametime 3.1 Installation Guide (stinstall.nsf) that is provided with your Sametime server.

Add the Sametime 3.1 server to the EMS

Adding the Sametime 3.1 server to the EMS is the last of three procedures required to upgrade a Sametime 3.0 server to a Sametime 3.1 server.

For detailed instructions on adding a Sametime 3.1 server to the EMS, refer to the following section of the *Sametime 3.1 Administrator's Guide* (sthelppad.nsf or sthelppad.pdf) provided with your Sametime 3.1 server: Setting up the Enterprise Meeting Server and a Meeting Services cluster - EMS Deployment and Meeting Services cluster setup procedures - Adding Sametime servers to the EMS.

The steps required to add a Sametime server to the EMS are listed below. However, for detailed instructions, you must refer to the "Adding Sametime servers to the EMS" section of the Administrator's Guide.

1. Upgrade the EMS to support Sametime 3.1 servers.
2. Synchronize Single Sign-On (SSO) support for the EMS and Sametime servers.
3. Edit the Sametime.ini file on the Sametime servers.
4. Edit the MeetingServices document in the Configuration database on the Sametime server.
5. Add the Sametime server using the EMS Administration Tool.
6. Specify Usage Limits and Denied Entry settings for the Sametime server.

Chapter 3 - Troubleshooting

The *Troubleshooting* chapter describes known limitations and issues associated with this release of Sametime.

Installation Issues

Sametime server

After Sametime uninstall, reboot before reinstalling Sametime

If you uninstall a Sametime server, reboot the server machine completely before attempting to reinstall the Sametime server.

If you do not reboot the server machine before attempting to reinstall Sametime, the installation may return an error indicating that a service is marked for deletion and this service will not be added by the installation.

Note: You should reboot the server machine even if all Sametime services were stopped when you uninstalled the Sametime server.

Sametime server

Clicking Cancel while installation is copying files

If you click the Cancel button while the Sametime server is copying Community Services or Meeting Services files during the Sametime server installation, you might see a dialog box with the following message: "Setup has detected that unInstallShield is in use. Please close UnInstallShield and restart Setup." If you see this dialog box, click the OK button. The uninstallation will uninstall the files that were copied to the server by the installation program before you elected to cancel the installation.

If you click the Cancel button while the installation program is copying other files, the installation may exit without displaying any dialog box. In this case, the uninstallation should also uninstall any files that had been copied. You may want to check the Windows Add/Remove Programs feature to verify that the Sametime server is not listed as an installed program. If the Sametime server is listed as installed, use the Windows Add/Remove Programs feature to uninstall the server.

Sametime server

Deleting directories following an installation failure

If the installation fails, delete the Sametime directory from your hard drive. If the Sametime directory is not present, InstallShield has already deleted it. Run the uninstallation program to ensure all Sametime components are deleted from the Sametime server machine and install Sametime again.

Sametime server

Directory has "Enforce consistent ACLs" option selected

The administrator must add the signer "Sametime Development/Lotus Notes Companion Products" to the ACL of the Directory on the Sametime server. This signer is required so that Sametime agents in Sametime databases can interact with the Directory as needed.

If a Directory is replicated to a Sametime server from another Domino server, and the Directory has the "Enforce a consistent ACL across all replicas of this database" option selected, replication between a Domino server and a Sametime server will be broken. The replication is broken because the Directory ACL on the Sametime server has different ACL settings than the Directory on the Domino server.

If your Domino environment requires you to use the "Enforce a consistent ACL across all replicas of this database" option, you must manually modify the ACLs of the Directories in the domain to ensure that Directory replication can occur from the Domino server(s) to the Sametime server. Specifically, you may need to manually add the "Sametime Development/Lotus Notes Companion Products" signer to all Directories involved in the replication scheme in your environment. The signer must have the same access level and permissions in the Directories on the Domino servers as it has on the Sametime server.

Note: The Sametime server 3.1 uses the same Domino Directory as Domino server release 6.02. Do not replicate earlier versions of the Domino Directory to the Sametime server.

Sametime server

Do not install Sametime multiplexer on a Sametime server

Sametime 3.1 provides an installation option that allows you to install a Sametime Community Services multiplexer without installing a Sametime server or any other Sametime components.

This installation option enables you to install the Community Services multiplexer on a separate machine from the Sametime server. When the multiplexer operates on a separate machine from the Sametime server, the multiplexer machine is dedicated to maintaining the Sametime Community Services client connections while the Community Services on the Sametime server perform all other Community Services processing functions. This configuration distributes the workload required to support the Community Services among multiple servers and enables a Sametime server to support a larger number of Community Services users.

Do not install a Sametime Community Services multiplexer on the same machine as a Sametime server. When you install a Sametime server, a Community Services multiplexer is also installed with the Sametime server. If you perform a separate installation of a Community Services multiplexer on a Sametime server, the Sametime server will contain two multiplexers and will not function correctly. No error message is displayed if you attempt to install a Community Services multiplexer on a Sametime server.

The separate Community Services multiplexer installation should be performed only on a machine that does not already include Sametime.

Sametime server

Installing Sametime without a fully qualified domain name

The *Sametime Installation Guide* (stinstall.nsf or stinstall.pdf) recommends using a fully qualified domain name for your Sametime server name (for example, server1.acme.com). The following issue applies only if the Sametime server was not installed using a fully qualified DNS name. Users outside of the Sametime DNS domain must enter the fully qualified DNS name of the Sametime server in the DNS suffix search order of the user's TCP/IP network settings.

To access these settings on a user's computer:

1. From the Windows desktop, select Start - Control Panel - Network.
2. Click the Configuration tab and double-click TCP/IP.
3. Click the DNS Configuration tab to access the Domain Suffix Search Order setting.

Note: The Net Address setting on the Sametime server Server document should also specify the fully-qualified DNS name of the Sametime server. The clients must be able to resolve the name entered in the Net Address setting based on the DNS set up. To access the Net Address setting on the Server document for the Sametime server:

1. Open the Server document for the Sametime server.
2. Select the Ports tab.
3. Select the Notes Network Ports tab.
4. Verify the Net Address setting for the TCP/IP port includes the fully-qualified DNS name of the Sametime server.

Sametime server

Ping the Sametime server before installation (verify DNS setup)

Before installing the Sametime server, you must ensure the Sametime server is appropriately registered in DNS. From a client machine, ping the Sametime server using both the short host name and the fully-qualified DNS name. You must get a response from the Sametime server machine using either the hostname or the fully-qualified DNS name. For example, if the hostname is "burrito" and the full DNS name is "burrito.databeam.com," typing the following commands should get the same results:

```
ping burrito
ping burrito.databeam.com
```

Pinging burrito.databeam.com [8.88.888.88] with 32 bytes of data:

```
Reply from 8.88.888.88: bytes=32 time=30ms TTL=122
Reply from 8.88.888.88: bytes=32 time=20ms TTL=122
Reply from 8.88.888.88: bytes=32 time=30ms TTL=122
Reply from 8.88.888.88: bytes=32 time=30ms TTL=122
```

Sametime server

Reinstalling Sametime 3.1 over an existing 3.1 installation

You can reinstall Sametime 3.1 over an existing Sametime 3.1 server without uninstalling the existing Sametime 3.1 server. You might want to reinstall Sametime 3.1 over an existing Sametime 3.1 server to correct the following problems:

- Restore Sametime files that have been mistakenly moved or deleted.
- Reset all Sametime configuration settings to their default values if the server has been configured incorrectly.

If you are reinstalling Sametime 3.1 over an existing Sametime 3.1 server, and you must specify an LDAP directory as the directory type used for the Sametime server, you should delete the LDAP configuration changes that were implemented by the original installation before beginning the reinstallation.

The procedures you perform to delete the LDAP configuration changes depend on whether the Domino server was or was not configured for LDAP access at the time the original Sametime installation occurred.

LDAP configuraton changes performed by the Sametime installation

If you select the LDAP directory type during a Sametime installation, the Sametime installation automatically configures the Domino server to access the LDAP directory you specify during the installation. The LDAP configurations performed by the Sametime server installation depend on whether the Domino server on which Sametime is installed is or is not configured to support LDAP access.

If the Domino server on which you are installing Sametime is **not** configured to support LDAP access, and you select the LDAP directory type, the Sametime installation automatically performs the following configurations:

- 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 on the LDAP server specified during the Sametime installation.
- 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.

If the Domino server on which you are installing Sametime is configured to support LDAP access, and you select the LDAP directory type, the Sametime installation automatically creates a document in the existing Directory Assistance database that points to the LDAP directory on the LDAP server specified during the Sametime installation.

Deleting the LDAP configuration changes before reinstalling Sametime

If you are reinstalling Sametime 3.1 over an existing Sametime 3.1 installation, and you are required to select the LDAP directory during the reinstallation, you must delete the LDAP configuration changes performed by the original Sametime installation before beginning the reinstallation. The deletions required depend on whether the Domino server on which Sametime was installed was or was not configured for LDAP access at the time Sametime was installed. To delete the LDAP configuration changes, do the following:

If the Domino server was **not** configured for LDAP access when the original Sametime installation occurred:

- Delete the da.nsf database created by the Sametime installation.
- Delete the "da.nsf" entry created by the Sametime installation in the "Directory Assistance database name" field of the Server document.

If the Domino server was configured for LDAP access when Sametime was installed:

- Delete the Directory Assistance document in the Directory Assistance database on the Domino server. This Directory Assistance document, which was created by the Sametime installation, points to the LDAP server you specified during the Sametime installation.

Sametime server

Replicate the Secrets database in multiple server environments

If you have installed multiple Sametime servers, you have the option of activating the SametimeSecretsGenerator agent in the Secrets database (STAuthS.nsf) on one of the Sametime servers. Activating this agent enhances security for client connections to the server.

If you activate this agent, the Secrets database that contains the active agent must be replicated to every other Sametime server in a multiple Sametime server environment. If all Sametime servers do not contain a replica of the Secrets database, connectivity problems will occur.

For more information, see the topic "Enhancing Security for multiple Sametime servers" in the "Deploying Multiple Sametime Servers" chapter of the *Sametime 3.1 Administrator's Guide* (sthelapad.nsf or sthelapad.pdf). The .nsf version of the *Sametime 3.1 Administrator's Guide* is available from the "Help Topics" link in the Sametime Administration Tool.

Sametime server

Sametime installation fails on partitioned Domino server

If the user selects the multiple partition option during the Domino server installation, the Sametime installation will fail when you attempt to install Sametime on that Domino server. The Sametime server setup program will return a language error and an error stating the server name cannot be found.

Sametime server, Web browsers

Sametime installation locates nonexistent Netscape browsers

If a user has uninstalled Netscape Navigator, the Netscape uninstallation does not remove the Windows registry settings for the Netscape browser. Because the registry settings are still on the computer, the Sametime Client Packager installation might detect versions of Netscape that are not installed on the user's computer.

The Sametime Client Packager installation attempts to determine what version of Netscape is installed on a user's computer. If the Sametime Client Packager installation detects registry entries for nonexistent (uninstalled) versions of Netscape Navigator, the installation may not function properly. As a result, the user may not be able to start instant meetings from the Netscape Navigator browser.

To solve this problem, delete registry entries for nonexistent versions of Netscape Navigator from HKEY_LOCAL_MACHINE:SOFTWARE:Netscape:Netscape Navigator and then reinstall the Sametime Client Packager.

Sametime server

Sametime server language does not match Domino server error

Sametime 3.1 requires the Domino Directory design available with the Domino 6.02 server release. If you are upgrading from a previous Sametime release to Sametime 3.1, make sure that the Domino server on which you are installing Sametime 3.1 is upgraded to Domino version 6.02.

When you upgrade the Domino server version to 6.02, you must also be sure to upgrade the design of the Domino Directory to version 6.02. It may be necessary to manually upgrade the directory design to 6.02. Note that if you customized the previous version of the Domino directory, all customizations are lost when you replace the directory design.

If you install Sametime on a Domino server that uses a directory version earlier than 6.02, you may see an error during the installation indicating that "the language of the Sametime server does not match the language of the Domino server."

Sametime server

Server name cannot include invalid XML characters

Sametime must be installed on a Domino server. When installing the Domino server that will host the Sametime server, you must provide a hierarchical name for the Domino server. The Domino server name cannot include any of the following characters in either the server name component or the organization component:

```
>  
<  
&  
'  
"  
;
```

Examples of invalid server names are included below:

```
SametimeServer/B&O  
SametimeServer/WorldO'Fun  
Sametime>Server/Acme  
Sametime;Server1/Acme
```

These naming restrictions exist because of limitations associated with XML processing and escaped characters. The characters listed above should not be present in the name of any Domino/Sametime server.

If a Sametime server name includes one of the characters above, the server will not function correctly.

Sametime server

servlets.properties file renamed during Sametime installation

Sametime includes a version of the servlets.properties file used by the Domino servlets engine.

If you install Sametime on the same machine as another Lotus product that includes the Domino servlets engine (such as the Lotus Discovery Server), the Sametime installation will install its own servlets.properties file and change the name of any existing servlets.properties file to servlets.properties.old.

If you modified the original servlets.properties file (now named servlets.properties.old), you must make those same modifications in the new servlets.properties file added by the Sametime installation.

Sametime server

Set the server home page following installation or upgrade

After installing the Sametime server, you should set the Sametime server home page (STCENTER.NSF) as the home page of the Domino server on which Sametime is installed.

Note Setting the Sametime server home page as the home page of the Domino server enables a user to enter the DNS name (http://servername) of the server in the Web browser URL locator to access the Sametime features. If you do not perform this procedure, users must enter http://servername/STCenter.nsf in the Web browser URL locator to access the Sametime server home page.

To set the server home page, open the Server document for the Domino server on which Sametime is installed. In the Server document, select the Internet Protocols - HTTP tab. Enter STCENTER.NSF in the "Home URL" field of the "Mapping" section of the Server document. Save the Server document and restart the Domino server for the change to take effect.

Sametime Connect client issues

Sametime Connect client

Cannot add meeting participant to Sametime Connect List

Users may be unable to add a user who appears in the Participant List of the Sametime Meeting Room client to the Connect List of the Sametime Connect for browsers client.

Users add a meeting participant to the Connect List of the Sametime Connect client by selecting the Meeting - People - Add to Connect List menu item in the Sametime Meeting Room. This menu option may not function properly in the Sametime Connect for browsers client and users may be unable to add meeting participants to the Connect List using this feature.

Users can be added to the Connect List of the Sametime Connect for browsers client using the Add button or the People - Add menu item of the client.

Sametime Connect client, Sametime Meeting Room client

Cannot start instant meeting if user name contains double quotes

If a user logs into a Sametime Connect client with a user name that contains double quotes (for example, "Heidi Sonnheim"), the user cannot start an instant meeting.

Sametime Connect client

Changing Sametime Connect for browsers server connectivity

By default, when a user launches the "Sametime Connect for browsers" client, the client connects to the Sametime server from which it was launched.

The user can configure the "Sametime Connect for browsers" client to connect to a different server than the server from which it was launched. To do this, the user selects the Connectivity option when logging on to the client and specifies a different Sametime server name in the Sametime Connectivity tab. To consistently connect to a different Sametime server, the user must manually specify this different server each time the user logs on to the client.

"Sametime Connect for browsers" is a Java applet that is designed to log on to the server from which it is launched. This behavior is standard for Java applets and applies whether the client is connecting to a Sametime 2.0, Sametime 2.5, Sametime 3.0, or Sametime 3.1 server.

Sametime Connect client

Disable Connect auto login with multiple user Notes client

A problem can occur if the automatic login feature of Sametime Connect is enabled and a Lotus Notes client is installed in a "Multiple User" configuration. With this configuration, it is possible for one user to click on a Sametime Connect bookmark icon in the Lotus Notes client and log in to Sametime Connect as a different user.

If Lotus Notes can be installed in a Multiple User configuration, the automatic login feature of Sametime Connect should be disabled by the administrator to prevent this problem from occurring.

The steps below illustrate a scenario in which a user can be logged on to Sametime Connect as another user.

1. A user logs into the Windows operating system as User 1.
2. User 1 installs the Sametime Connect client. During this installation, the user specifies the Sametime server to which the Sametime Connect client will connect (for example, sametimeserver1.acme.com).
3. User 1 logs into Sametime Connect using the User Name and Internet password specified for the user in the Domino Directory on the Sametime server.
4. User 1 installs the Lotus Notes client using the Notes "Multiple User" option.
5. User 1 starts Lotus Notes for the first time and runs the Notes setup program.
Note A Sametime Connect icon appears in the Bookmark list of Lotus Notes.
6. User 1 clicks on the Sametime Connect icon in the Bookmark list, enters the User Name and Internet password from the Person document, and logs on to the Sametime Connect client.
7. In the Sametime Connect client Options-Logon Information menu item, User 1 selects "Log on automatically" to enable the automatic log on features of Sametime Connect.
8. A different user logs into the Windows operating system as User 2.
9. User 2 installs the Lotus Notes client using the Notes "Multiple User" option. Following the installation, User 2 runs the Lotus Notes setup program.
10. The Sametime Connect icon appears in the Bookmark list of the Lotus Notes client launched by User 2. The Bookmark may appear even though User 2 has not installed Sametime Connect.
11. When User 2 clicks on the Sametime Connect icon in the Bookmark list in Lotus Notes, User 2 is automatically logged into Sametime Connect as User 1.

To prevent this problem, the administrator must disable the automatic log on feature on the Sametime server to which the Sametime Connect clients connect. The administrator must disable the automatic log on feature for both "Sametime Connect for browsers" and "Sametime Connect for the desktop."

To disable the automatic logon feature for "Sametime Connect for browsers:"

1. Open the Sametime Administration Tool.
2. Choose Configuration-Community Services.
3. Clear the check mark from the "Allow Connect users to save their user name, password, and proxy information" setting.

To disable the automatic logon feature for "Sametime Connect for the desktop:"

To disable the automatic logon feature for "Sametime Connect for the desktop," you must run the Sametime Client Packager application on the Sametime server. The Sametime Client Packager application includes an option that enables you to disable the automatic logon feature for all "Sametime Connect for the desktop" clients that are downloaded from the Sametime server.

Sametime Connect client

Do not run both versions of Sametime Connect on the same machine

Sametime 3.1 includes two versions of the Sametime Connect client. These versions are "Sametime Connect for the desktop" and "Sametime Connect for browsers." ("Sametime Connect for the desktop" is written in the C++ language and "Sametime Connect for browsers" is written in the Java language.)

It is best if users do not have both of these clients open simultaneously on the same machine. If both of these clients are open on the same machine, users may experience problems when adding names or groups to the contact list in Sametime Connect for browsers.

Sametime Connect client

Do not use "Short name" to log into Sametime Connect

IBM Lotus software recommends that users log into Sametime Connect using an entry in the "User name" field of a user's Person document.

Users should not log in to Sametime Connect using an entry in the "Short name/User ID" field of the user's Person document. Users attempting to log in using an entry in the "Short name/User ID" field might see an "Unable to access Sametime due to incorrect logon" error. This error appears consistently for short names that are three characters or less.

Sametime Connect client

Invitation indicates no available tools if Connect is closed

When you invite a user to an instant meeting, the invitation dialog box displays the available tools (microphone, speaker, camera) that the invited user has installed on his or her computer. A check mark beneath a tool indicates the tool is available on the user's machine and an X indicates the tool is unavailable on the user's machine.

If you invite a user to an instant meeting, and the invited user is not currently running the Sametime Connect client, question marks appear for all of the available tools. These question marks might appear even when the user's machine has the tools installed. The invited user can still use the tools in the instant meeting even though the question marks in the invitation dialog indicate that the tools are not available.

Question marks can also indicate that the user has not entered information about the audio/video tools or that the user is using a version of Sametime Connect that does not support audio and video. A user without audio and video tools can still participate in a Sametime meeting.

Sametime Connect client

Locked DLLs require machine reboot to complete Connect install

The Sametime Connect client installation replaces some operating system DLL files and then registers Sametime OCX files. The Sametime OCX files can only be registered successfully if the DLL files are replaced by the Sametime Connect client installation. If the DLL files are locked by the operating system, you must reboot the system before the Sametime OCX files can be registered and the installation can complete.

The end result of this problem is that the user may need to install Sametime Connect twice to successfully install the Sametime Connect client.

If this problem occurs, the error message "Installation has not completed due to locked system DLLs - Please reboot and install again" displays during the first installation attempt. The user can install the Sametime Connect client again and the installation should conclude successfully after the second installation.

Explanation

When the DLL files are locked by the operating system, the system must be rebooted so that the DLLs can be replaced by the installation. The Sametime OCX files cannot be registered until the DLLs are replaced. After the DLLs are replaced, and the system rebooted, you can rerun the installation. Rerunning the installation enables the Sametime OCX files to be registered because the new DLLs are now present on the system.

Sametime Connect client

Logging into STEP changes privacy settings

The Sametime Connect client includes privacy settings that enable a Sametime Connect user to conceal the user's online status from other members of the community. The privacy settings enable the user to specify which other members of the community can detect when the user is online. These settings are located in the Options-Who Can See If I Am Online settings in the Sametime Connect client.

If a user establishes privacy settings from Sametime Connect, and later logs into Sametime from a Sametime Everyplace (STEP) client, the user's privacy settings are lost. The user must re-establish the privacy settings the next time the user logs into Sametime from Sametime Connect. The steps below illustrate this problem.

1. A Sametime Connect user adds specific users to the "Who can see if I am online" list (using either the "ONLY list below" or "Everybody EXCEPT list below" option).
2. The user logs off of Sametime Connect and then logs into Sametime from a STEP client.
3. The privacy settings the user set from Sametime Connect are no longer valid. The privacy settings operate in the "Everybody can see if I am online" mode and all users in the community can detect the user's online status.

When the user logs back into Sametime from Sametime Connect, the privacy settings remain in the "Everybody can see if I am online" mode. The user must reset the privacy settings by adding specific users to the "Who can see if I am online" list (as described in step 1).

Sametime Connect client

Meeting cannot be started due to error 0x8000024

When starting an instant meeting from Sametime Connect or responding to an invitation to attend an instant meeting, a user may see the error message "The meeting cannot be started due to the following error 0x8000024. Please contact your system administrator."

Either the user starting the meeting or the user attending the meeting is disconnected from the Sametime server. To fix the problem, the disconnected user should restart the Sametime Connect client.

Sametime Connect client

No error for empty proxy fields in Sametime Connect for browsers

If a user does not correctly configure the proxy settings in the Sametime Connect for browsers Sametime Connectivity settings, the user receives no notification that a problem exists.

Specifically, when a user selects the "Use proxy" option for the "Connection type" in the Sametime Connect client Options - Preferences - Sametime Connectivity tab, and leaves the the Proxy server "Host" and "Port" fields empty, no error message appears upon closing the dialog box. The Sametime Connect client attempts a direct connection (Sametime protocol over TCP/IP) to the Sametime server. If the direct connection is successful, the user receives no notification that the connection did not occur through a proxy server.

Sametime Connect client

Sametime Connect display problems at 256 colors

If the display settings on a user's machine are set to 256 colors, some elements of the Sametime Connect user interface may not display properly. For example, Group names in the Connect buddy list may be obscured by black highlighting and difficult to read. 16-bit color settings are recommended.

Sametime Connect client

Sametime Connect startup screen is upside down

When a user starts the Sametime Connect client, the startup bitmap image may appear upside down for users that have certain video cards. This is a rare problem limited to a few video cards.

Users can prevent this problem by adjusting the Video (or Display) settings available in the Windows Control Panel. In the Display settings, the users should set the "Hardware Acceleration" setting to none.

Sametime Connect client, Sametime Meeting Room client

SHIFT+ENTER not starting new line in chat message

Pressing SHIFT+ENTER does not create a new line in a chat message. This problem occurs in Sametime Connect for the desktop, Sametime Connect for browsers, and Meeting Room chat.

In Sametime Connect for the desktop, pressing CTRL+ENTER creates a new line.

Sametime Connect client

User with long name is unable to log in to Sametime Connect

Users with extremely long names in the "User Name" field of the Person document may not be able to log into Sametime Connect for the desktop. If a user's log in name is too long, the following error message displays: "Unable to access Sametime due to incorrect login. Please try again or contact your system administrator."

To work around this issue, you can enter a shortened version of the user's name in either the "User Name" field or the "Short name/UserID" field of the user's Person document. The user can enter this shortened name when logging into Sametime Connect.

Meeting Room client issues

Sametime Meeting Room client

Black boxes appear when sharing some dialog boxes

Avoid sharing applications within an application. In some applications, users can select a menu item that launches a separate application. Here are two common examples of opening a separate application from within Microsoft Word:

- A user selects File-Page Setup to launch the Page Setup application.
- A user selects Insert-Picture-Clip Art to launch the Clip Art application.

In each of these cases, the end user may think of Page Setup and Clip Art as dialog boxes within Microsoft Word, but they are actually separate applications. If the user opens the Page Setup or Clip Art application, these applications will appear as black boxes to other meeting attendees.

This problem occurs because the screen sharing tool hides the windows of other applications when the Share a Program option is used to share one specific application.

The workaround for this issue is to use the "Share My Entire Screen" or "Share Part of My Screen with a Frame" option instead of the "Share a Program" option when sharing applications.

Sametime Meeting Room client, Sametime server

Computer entering standby mode drops audio

If a user is presenting during a Sametime meeting, and that user's computer enters the standby mode during the presentation, the audio may no longer function.

If a presenter is only transmitting audio and video, or sharing a screen or whiteboard presentation with no keyboard or mouse activity, the presenter's computer may enter standby mode. When a computer enters standby mode, network activity stops and the presenter is disconnected from the meeting.

Similarly, if there is no keyboard or mouse activity, and the presenter is sharing the screen, the screen saver may activate on the presenter's computer. Other participants in the meeting will see the presenter's screen saver.

Users may want to disable the power saver and screen saver features if their meeting presentations will require little mouse or keyboard activity.

Sametime Meeting Room client

Databeam Farsite files should not be attached to a meeting

Files created from the Databeam Farsite application will not convert for display in the Meeting Room client whiteboard when attached to a meeting. These files have the same file extension (.FST) as files created from the Sametime print capture utility or files that were attached to a meeting during the meeting creation process.

If a user attaches an FST file to a meeting that was created from the Farsite application, and attempts to access this file from the drop-down list in the Sametime Meeting Room client, the user will be unable to access other valid files that have been attached to the meeting for display in the whiteboard.

Sametime Meeting Room client

Empty browser frame or browser crash during client install

Some problems may occur when installing the Sametime Meeting Room client if the user is running Norton AntiVirus 2000 and is using the Auto Protect feature or the Live Update feature of Norton AntiVirus 2000. These problems only occur when a user is running both the Internet Explorer browser and the Norton AntiVirus program.

Note: These problems do not occur with Norton AntiVirus 2001.

If a user has the Auto Protect feature of Norton AntiVirus 2000 enabled, Internet Explorer may crash (in naveng32.dll) when the user attends a meeting and agrees to install the Sametime Meeting Room client. This problem occurs with versions of Windows that are earlier than Win2000 Professional. The user can disable the Auto Protect feature before agreeing to install the Sametime Meeting Room client.

The following problems can occur when the user allows the Live Update feature to update Norton AntiVirus 2000. (The user can prevent these problems by disabling the Live Update feature of Norton AntiVirus 2000.) These problems manifest themselves differently depending on whether the user is running the Windows 2000 Professional or Windows 98SE operating system.

Windows 2000 Professional

After joining a meeting the user receives two dialogs where the user agrees to download the Sametime Meeting Room client and responds to a security warning. After responding to these dialogs, an empty browser frame may remain displayed on the screen and the CPU reports 0% usage. The machine remains in this state indefinitely.

If this occurs, the user should close both browser windows, restart the browser, and join the meeting again. The user will receive the client download and security warning dialogs again. After responding "yes" at the security warning dialog, the user will join the meeting successfully.

Windows 98SE

After joining a meeting and responding to the client download and security warnings dialogs, the browser will crash (in naveng32.dll). If this occurs, the user should close both browser windows, restart the browser, and join the meeting again. The user will receive the client download and security warning dialogs again. After responding "yes" at the security warning dialog, the user will join the meeting successfully.

Sametime server

Files with embedded objects distort in the whiteboard

Microsoft Word and Lotus Word Pro files that contain embedded objects may not display correctly after being converted to Whiteboard files. Generally, this behavior occurs when there are no printer drivers installed on the Sametime server. To prevent this problem, install a printer driver on the Sametime server. (Any printer driver can be installed; it is not necessary to connect the server machine to an actual printer).

Some of the problems that may occur if there is no printer driver installed include:

- Embedded images (such as GIF files) may not display or display as gray boxes
- Pages appear compressed or are scaled incorrectly
- Pages containing embedded objects do not display
- Images and headings are displaced on the pages

Sametime Meeting Room client

Gray whiteboard, screen sharing buttons disabled, no A/V

The server machine on which Sametime is installed must have a color setting higher than 256 colors. A 16-bit color setting is recommended.

The following problems can occur if the server machine has a display color setting of 256 colors or less:

- The images in whiteboard attachments do not display correctly on the whiteboard.
- The Meeting Room client opens with a gray whiteboard.
- Screen-sharing buttons are disabled in the Meeting Room client.
- Audio/Video features do not work.
- A new Meeting Room client opens in a different window and flashes periodically.

Shortly after these problems appear, meetings on the Sametime server may fail to become active.

Sametime Meeting Room client

HTML files do not display correctly in the whiteboard

The whiteboard will display an html file as a text file if the <HTML> tag is removed from the beginning of the HTML file before the file is attached to a meeting for conversion to the .FST file format supported by the whiteboard. If the <HTML> tag is not removed, the whiteboard attempts to display the html file as a Web browser would. Complex html pages containing multiple frames and images may not display correctly in the whiteboard when the <HTML> tag is left in the file.

If the <HTML> tag is removed from the beginning of the file, the html file displays the text-based source code of the html file in the whiteboard. In some cases, the first page of the html file will display as the last page when the file is converted into a whiteboard presentation.

Sametime Connect client, Sametime Meeting Room client

Initial chat transcripts do not appear in instant meetings

Users can begin a chat session and then start an instant meeting from the chat session by adding a collaborative activity (such as screen sharing, the whiteboard, or audio/video) to the chat. Adding a collaborative activity to a chat session launches the Sametime Meeting Room client on each user's computer and starts the instant meeting.

If two (or more) users begin a chat session and then start an instant meeting from the chat, a chat transcript of the chat activity that preceded the meeting does not appear in the chat area of the Sametime Meeting Room client.

Sametime Meeting Room client, Sametime server

Meeting Room client hangs when loading whiteboard/other applet

If a user attempts to attend a meeting, and the Sametime Meeting Room client hangs while loading the whiteboard or other Java component, the client may be unable to resolve the server name because of a problem in the Server document for the Sametime server. Specifically, the short name of the server may be listed in the Ports section of the Server document instead of the fully-qualified DNS name.

To verify that the fully-qualified DNS name is listed in the "Ports" section of the Server document, follow the instructions below:

1. Use a Lotus Notes client or Domino Administrator client to open the Domino Directory (names.nsf) that contains the Server document for the Sametime server.
2. Open the Server document for the Sametime server.
3. Select the "Ports" tab.
4. Select the "Notes Network Ports" tab.
5. Check the "Net Address" for the TCP/IP port. The "Net Address" column must specify the fully-qualified name of the Sametime server (e.g., sametimeserver.acme.com).
6. If the short name of the server (e.g. sametimeserver) is listed in the "Net Address" column, replace it with the fully-qualified DNS name of the server.

Sametime Meeting Room client

Menus do not pop up when accessed via mnemonics

When users press mnemonic keys (shortcut keys) to activate menu options in the Sametime Meeting Room, the menus do not pop up. The menus are activated, but the activation is not visible to users. For example, if a user presses t, then u, then p to activate the Tools - Audio - Increase Speaker Volume menu option, the Tools menu and the Audio pull-right menu do not appear on the screen.

Mnemonic keys do work correctly, even though the menu activation is not visible.

Sametime server

Only one spreadsheet in a file converts to whiteboard format

If you convert a Microsoft Excel or Lotus 123 file for display on the whiteboard by attaching it to the meeting during the meeting creation process, and the Excel or 123 file contains multiple spreadsheets, only the first spreadsheet of the Excel or 123 file will display in the whiteboard. The remaining spreadsheets in the file will not convert to the whiteboard format.

If you want to convert a Microsoft Excel or Lotus 123 file that includes multiple spreadsheets so that all of the spreadsheets in the file can be displayed in the whiteboard, use the Sametime Print Capture utility to convert the file to the format required by the whiteboard.

Note: When using the Sametime Print Capture utility to convert a Microsoft Excel file containing multiple spreadsheets to the file to the format required by the whiteboard, the user is prompted to enter a file name for the file in a File/Save dialog box. After naming the file, the user will see repeated prompts to save the file (as each spreadsheet is being converted). At these repeated prompts the user has the option to either "replace" the file or "append" to the file. The user should choose the "append" option at these prompts. Choosing the append option when prompted for repeated saves ensures that the multiple Excel spreadsheets can be displayed from a single whiteboard file.

Sametime Meeting Room client, Web browsers, Sametime server

Participant List problems with Netscape browsers

In the Sametime Meeting Room client, a Participant List displays the names of all online users. The names of the online users display in green text with a green box beside each user's name.

When attending a meeting with a Netscape browser, a user may see a green box in the Participant List that has no name beside it. The user can refresh the browser to make the name of the online user appear. In other cases, the name may appear, but the name has no green box associated with it. This is an intermittent problem that occurs only when the Meeting Room client is running in a Netscape browser.

Sametime Meeting Room client, Sametime server

Repeated saves when converting multiple spreadsheet Excel file

The following problem has been seen when using versions of Microsoft Excel that are earlier than the Microsoft Office2000 version.

When using the Sametime Print Capture utility to convert a Microsoft Excel file that includes multiple spreadsheets to the file format required by the whiteboard, the user is prompted to enter a file name for the file in a File/Save dialog box.

After naming the file, the user will see repeated prompts to save the file (as each spreadsheet is being converted). At these repeated prompts the user has the option to either "replace" the saved file or "append" to the saved file. The user should choose the "append" option at these prompts. Choosing the append option when prompted for repeated saves ensures that the multiple Excel spreadsheets can be saved to and displayed from a single whiteboard file.

Sametime Administration Tool, Sametime Meeting Room client

Tools still available in active meetings

The following options in the Configuration - Meeting Services settings of the Sametime Administration tool determine which tools are available to end users:

- "Allow people to choose the whiteboard tool in meetings"
- "Allow people to choose the screen sharing tool in meetings"
- "Allow people to choose the 'Send Web Page' tool in meetings"
- "Allow people to choose the Polling tool in meetings"

If the administrator removes the check mark from any of the options listed above, the associated tool will not be available in Sametime meetings. However, any meetings that already included the tool when the administrator removed the checkmark will continue to use the tool. For example, if an end user is attending a meeting that includes the whiteboard, and the administrator removes the check mark from the "Allow people to choose the whiteboard tool in meetings" option, the end user will be able to continue using the whiteboard for the duration of the active meeting. No new meetings will be able to include the whiteboard.

Sametime Meeting Room client

Whiteboard attachments and invited servers

The following information applies to whiteboard attachments on invited servers:

- Users who are attending a meeting on an invited server cannot attach files to the whiteboard during the meeting. To attach a whiteboard file, the Moderator must be attending the meeting on the server on which the meeting was created.
- Users who are attending a meeting on an invited server cannot see saved whiteboard files on the Meeting Details document. All whiteboard attachments are saved on the server on which the meeting was created. Although a user who is attending the meeting from an invited server can save a whiteboard file, he or she will not see the file on the Meeting Details document of that server. The user must go to the Meeting Details document on the server on which the meeting was created to see the file.

Note The server on which the meeting was created is listed in the Locations field of the Meeting Details document on each server that is in the meeting.

Web browser issues

Sametime Administration Tool, Web browsers

Admin pages do not display in Sametime Administration Tool

If you open the Sametime Administration Tool with a Web browser that puts an ampersand (&) in the User-Agent HTTP header, the administration pages do not display in the Web browser.

Use one of the following supported Web browsers to open the Sametime Administration Tool:

- Microsoft Internet Explorer 6 (with the native Microsoft VM 1.1 or Sun Microsystems JVM 1.4 or 1.4.1)
- Netscape 7 (with the Sun Microsystems JVM 1.4.1)

Note When using the Sametime Administration Tool with Microsoft Internet Explorer, make sure to disable the "Use HTTP 1.1" setting in the advanced settings of the web browser. To reach the advanced settings, choose Tools - Internet Options - Advanced settings.

Sametime Connect client

Available Tools do not appear with Netscape/Win 98

The following problem occurs for users who run the Java version of Sametime Connect (Sametime Connect for browsers) in a Netscape Web browser on the Windows 98 operating system.

When a Sametime Connect for browsers user right-clicks the name of another user in the Sametime Connect presence list and selects the Available Tools option, the Available Tools of the other user do not display.

Web browsers

Cannot attend meetings using Netscape

The Sametime Meeting Room client is automatically installed on a user's machine the first time a user attends a Sametime meeting or runs the Test Audio/Video application.

Netscape browser users should make sure that the Sametime Connect client is closed the first time they do either of the following:

- Attend a Sametime meeting
- Run the Test Audio/Video program

Performing either of the actions above installs the Meeting Room client on the user's machine. If the Sametime Connect client is open on a Netscape browser user's computer during the Meeting Room client installation, the Meeting Room client does not install completely. The user will be unable to attend a meeting or test the audio/video using the Netscape browser.

If this partial Meeting Room client installation occurs, the user should close all Netscape browser windows and Sametime Connect windows and restart Netscape. After restarting Netscape, the installation completes and the user can attend meetings and test audio/video using the Netscape browser.

Note: The Test Audio/Video program can be run from within Sametime Connect. If a Netscape browser user has not yet attended a Sametime meeting, or run the Test Audio/Video program from the Sametime Meeting Center, the user should not run the Test Audio/Video program from within Sametime Connect.

Web browsers

Default browser information

When a user attempts to start or attend an instant meeting, the browser specified as the Windows default browser is launched on the user's local computer. You should be aware of the following information about the default browser:

- If no browser is set as the default in Windows, users cannot start an instant meeting from Sametime Connect or attend an instant meeting by responding to an invitation.
- If Netscape Navigator is set as the Windows default browser when a user installs Sametime Connect, and the user later uninstalls Netscape, the user will be unable to start or attend instant meetings.
- When a user installs Netscape Navigator, Netscape automatically becomes the Windows default browser.
- If Microsoft Internet Explorer is set as the Windows default browser when a user installs Sametime Connect, and the user later uninstalls Microsoft Internet Explorer, the user will be unable to start or attend instant meetings.
- Microsoft Internet Explorer checks to see if it is the default browser each time that it is started. A dialog box that allows the user to select Microsoft Internet Explorer as the default browser appears each time Microsoft Internet Explorer launches. If the user has disabled this dialog box, do the following to make the dialog box display when the browser launches:
 1. From Microsoft Internet Explorer 6, choose Tools · Internet Options.
 2. Click the Programs tab.
 3. Enable the "Internet Explorer should check to see whether it is the default browser" check box.
 4. Restart Microsoft Internet Explorer.

Web browsers

Meeting names with quotations display incorrectly

If a meeting name includes double quotations (") or accent marks, the meeting name may not display correctly in the Monitoring features of the Sametime Administration Tool.

Microsoft Internet Explorer users must change the default font of the Web browser to enable meeting names with accented characters to display correctly. Suggested default font settings to resolve this problem include MS Gothic or MS Mincho.

Web browsers

Netscape does not authenticate using international characters

A Netscape browser user may not be able to authenticate with the Sametime server if the person's user name includes international characters, such as:

À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à

This issue occurs because the Netscape browser does not fully adhere to the ISO-8859-1 standard when handling user name and password credentials. This is a problem that Netscape plans to fix with browser version 6.0.

Microsoft Internet Explorer users will not see this problem.

For more information, contact Netscape and refer to Netscape Defect ID # 93760, or Netscape Call ID # 72074.

Sametime Broadcast client, Sametime Meeting Room client, Web browsers

Netscape HP/UX and Sun Solaris Web browsers not supported

Users might be unable to access the Sametime server when using Netscape Web browsers that operate on HP/UX or Sun Solaris client machines. When installed on the Windows operating system, the following browsers can be used to access Sametime:

-
- Microsoft Internet Explorer 6 that use the native Microsoft VM 1.1 or the Sun Microsystems JVM 1.4 or 1.4.1.
- Netscape 7 browsers that use the Sun Microsystems JVM 1.4.1

Note that users cannot access the Sametime Administration Tool with Netscape browsers.

Sametime Administration Tool

Netscape locks up when resizing Administration window

If you open the Sametime Administration Tool using a Netscape browser, the browser window may not repaint correctly when it is resized. Netscape may also lock up. If you are running the Sametime Administration Tool in a Netscape browser and you see this problem, you should resize the browser window only in small increments.

If Netscape locks up or will not repaint the window correctly, you may need to reboot your computer and then access the Sametime Administration Tool from Netscape.

Sametime Connect client, Web browsers

Netscape opens empty and Notepad opens with .tmp file displayed

If a user who has selected Netscape as the default browser and associated .TMP files with the Notepad program attempts to start an instant meeting or selects a menu item in Sametime Connect, an empty Netscape browser window opens and then Notepad opens and displays a .TMP file. To avoid this problem, users who have set Netscape as the default Windows browser should not associate .TMP files with Notepad.

Sametime Administration Tool

Problem with "Administer the Server" link

When using Netscape or Microsoft Internet Explorer, the "Administer the server" link might not take users directly to the Sametime Administration Tool. Instead, the link might return users to the Sametime Welcome page. If this happens, click "Administer the server" again.

Web browsers

Proxy tunneling does not work with IE

When a participant attends a meeting using Microsoft Internet Explorer (IE), the Java components of the Sametime Meeting Room and Broadcast clients may use the proxy settings of the browser to connect to the Sametime server.

Participants that use Active Desktop on Windows 95, 98, NT WorkStation, 2000 Professional, or ME machines might need to reboot their machines after changing Internet Explorer's proxy settings. The Microsoft Java Virtual Machine will not pick up the new settings until the computer is restarted.

If the user changes the Internet Explorer proxy settings without restarting Internet Explorer, the user may not be able to attend an online meeting.

Web browsers

Repeated prompts for Microsoft IE VM install

When a user attends a meeting with Microsoft Internet Explorer, the user may receive a prompt indicating that the Microsoft Virtual Machine (VM) installation is needed. After the VM installation completes, the user should restart Internet Explorer and attend the meeting again. If the prompt indicating the Microsoft VM must be installed appears again, the user should follow the procedure below to ensure the latest Microsoft VM is correctly installed on the user's machine.

Note The user must have any necessary permissions to install applications on the computer to perform the VM upgrade or installation. The instructions below explain how to get the latest version of the Microsoft VM.

1. Go to the Web site <http://windowsupdate.microsoft.com>
2. Click the Product Updates link. If a Security Warning dialog box appears asking if you want to install and run "Microsft Active Setup," click Yes. The Microsoft Active Setup applet examines your system and displays a list of all possible updates for Microsoft products that may apply to your system.
3. Select the update titled Microsoft Virtual Machine. This update contains the latest VM.

If you do not see an update titled Microsoft Virtual Machine, read the descriptions of all the updates in the update list and select the update that contains the latest version of the Microsoft VM. (For example, some users may see an update titled "Security Update, March 7, 2000" that contains the latest Microsoft VM.)

4. Deselect all other updates in the updates list. Only the Microsoft VM (selected in step 3 above) should be updated during this process.
5. Click the Download button at the top of the updates page.
6. Follow the instructions on the screen to download and install the Microsoft VM.

Web browsers

Sametime issues using Discussion database with Internet Explorer

A Discussion database enabled with Sametime technology includes a presence list from which the user can initiate Sametime communications.

To run the Java Community Services components in Microsoft Internet Explorer (IE) 6, use the latest Microsoft Java Virtual Machine (VM).

To get the latest version of the Microsoft Virtual Machine:

1. Go to the Web site <http://windowsupdate.microsoft.com>
2. Click the Product Updates link. If a Security Warning dialog box appears asking if you want to install and run "Microsft Active Setup," click Yes. The Microsoft Active Setup applet examines your system and displays a list of all possible updates for Microsoft products that may apply to your system.
3. Select the update titled Microsoft Virtual Machine. This update contains the latest VM.

If you do not see an update titled Microsoft Virtual Machine, read the descriptions of all the updates in the update list and select the update that contains the latest version of the Microsoft VM. (For example, some users may see an update titled "Security Update, March 7, 2000" that contains the latest Microsoft VM.)

4. Deselect all other updates in the updates list. Only the Microsoft VM (selected in step 3 above) should be updated during this process.
5. Click the Download button at the top of the updates page.

6. Follow the instructions on the screen to download and install the Microsoft VM.

Using other versions of the Internet Explorer Java VM may cause Internet Explorer to hang when using the Community Services components of a database enabled with Sametime.

Sametime Broadcast client, Sametime Meeting Room client, Web browsers

SOCKS proxy limitations with the Sun JVM 1.4.1 Plug-in

If a Sametime Meeting Room or Broadcast client runs in a Web browser that operates with the Sun JVM 1.4.1 Plug-in, users may experience some connectivity problems when attempting to connect to a Sametime server through a SOCKS proxy server.

These problems can occur if the Sun JVM 1.4.1 Plug-in is configured in either of the following ways:

- The "Use browser settings" option is selected in the Sun JVM Plug-in Proxies tab and the Web browser proxy settings specify a SOCKS proxy server.
- The "Use browser settings" option is disabled in the Sun JVM Plug-in Proxies tab and connectivity settings (host and port) on the Sun JVM Proxies tab specify a SOCKS proxy server.

Connectivity issue #1

The following issue applies to a scenario in which the Sametime clients and Sametime server operate on the same local network and the clients are configured to establish connections through a SOCKS proxy server.

If the specified SOCKS proxy server is configured to handle connections to external networks and cannot route connections from machines on its local network to other machines on the same local network, all of the following will be true:

- The Sametime client will not attempt a direct TCP/IP connection to the Sametime server. This connection attempt is not possible due to limitations of the Sun Java Plug-in.
- The connection attempt from the Sametime client to the Sametime server through the SOCKS proxy will fail.
- If an HTTP proxy server is also configured in the web browser proxy settings or the Sun JVM Plug-in Proxies tab, the Sametime client will not be able to connect to the Sametime server through the HTTP proxy.

In this scenario, only a direct HTTP-tunneled connection between the Sametime client and the Sametime server can succeed.

If the Sametime server is located in a different external network, the Sametime client operating behind the SOCKS proxy can establish connections with the external Sametime server through the SOCKS proxy server.

If you remove the SOCKS proxy settings (from the Web browser proxy settings or the Sun JVM Plug-in Proxies tab), the Sametime clients can bypass the proxy and establish a direct TCP/IP connection with the Sametime server.

Connectivity issue #2

No matter what SOCKS proxy port number is specified in the Web browser proxy settings or the Sun JVM Plug-in Proxies tab, the Java Plug-in always attempts connections to the SOCKS proxy server using port 1080. The SOCKS proxy server must be configured to listen for these connections on port 1080 or the connections will fail.

Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client

Sun Java plug-in does not pick up SOCKS proxy from PAC file

If an Internet Explorer Web browser runs with the Sun JVM 1.4.1 Java Plug-in, do not use a Proxy Auto-Configuration file to enable IE to connect to servers through the SOCKS proxy server.

The Sun Java Plug-in cannot use PAC file settings to establish connections through a SOCKS proxy server. Any Sametime Java applet client running under this configuration will also be unable to connect to a Sametime server through the SOCKS proxy server.

Enterprise Meeting Server and server clusters

Turkish locale settings not supported for EMS

You cannot access the EMS application with a web browser that specifies Turkish as its language setting.

Sametime server, Web browsers

Wrong MeetingPlace information when scheduling conference call

When a user accesses the Sametime Meeting Center and schedules a telephone conference call on a Latitude MeetingPlace server, users may experience a problem with Netscape browsers if they enter incorrect information that is needed by the MeetingPlace server.

If the Netscape user schedules a meeting that includes a telephone conference call and enters an incorrect user ID or password for the Latitude MeetingPlace server, the MeetingPlace server returns an error page. If the user then clicks the browser back button to correct the incorrect entry, the user must also click on the Options button for the telephone conference call and re-enter all of the options for the telephone conference call.

The options are not retained when the MeetingPlace server returns an error. This problem is not apparent to the end user unless the end user clicks the Options button to verify the telephone conference call options have been retained.

Sametime server issues

Sametime server

A member of a group cannot authenticate when attending a meeting

The Sametime end user interfaces provide applets that enable a user to browse Directories and enter individual or group names in a Restrictions list to restrict attendance to a meeting. Users can also browse the Directory and add individual or group names to a Presenters list when setting up a Broadcast meeting.

If a user adds a group to the Restrictions or Presenters list, the group must exist in the primary Directory (the Directory in which the Sametime server is registered) on the Sametime server that is being accessed.

If a user is a member of a group, and the group is defined only in a secondary Directory that is pointed to from Directory Assistance, members of that group cannot authenticate when accessing the Sametime server. (In this situation, the primary Directory exists on the Sametime server and the Sametime server contains a Directory Assistance database that points to the secondary directories. If the group is defined only in the secondary directories, members of that group cannot authenticate.) This problem occurs because of a known Domino problem regarding authentication of group members in secondary directories that should be resolved in future releases.

Sametime Administration Tool

Access Control Lists are unavailable to the administrator

Sametime administrators can use the Sametime Administration Tool to access the Access Control Lists (ACLs) for databases on the Sametime server. To access the ACLs, the administrator chooses Domino Directory - Access Control (or LDAP Directory - Access Control) from the Sametime Administration Tool.

If the ACLs are unavailable to an administrator, it may be necessary to add the administrator's name (or administrator's group) to a "File Protection Document" in the Domino Directory.

CGI scripts for the Sametime Administration Tool ACL applet are stored in the "adm-bin" directory on the Sametime server. The adm-bin directory is protected by a "File Protection Document" that is stored in the Domino Directory. This File Protection Document controls who can read, write, or execute programs that are stored in the adm-bin directory. To enable a Sametime administrator to use the ACL applet in the Sametime Administration Tool, you must ensure that the administrator's name (or administrator's group) appears in this File Protection Document.

Note: If you are running the Sametime Administration Tool in an Internet Explorer Web browser, see the note at the bottom of this topic before performing this procedure.

To add an administrator's name (or administrator's group) to the File Protection Document:

1. Use a Lotus Notes client to open the Directory on the Sametime server.
2. Select Server - Web Configurations.
3. Click the twistie to the left of the Sametime server name.
4. Click the twistie to the left of "Domino Server."
5. Double-click on the document named "Access to C:\Lotus\Domino\Data\domino\adm-bin" to open the File Protection Document.
6. Click "Edit File Protection."
7. Click the Access Control tab.
8. Click the "Set/Modify Access Control List" button. The Access Control List dialog appears.
9. Select the arrow to the right of the "Name" box to browse the list of names and groups in the Directory. The Names box appears.
10. Select the Directory for the Sametime server.
11. Select the administrator's name (or administrator's group) from the list of Directory entries and click OK.
12. From the Access: radio buttons, select the "Write/Read/Execute access (POST and GET method)" option.
13. Click Next.
14. Click OK.
15. Save and Close the File Protection Document.

You must restart the server for this change to take effect.

Note: If you are using Internet Explorer, and the names of databases do not appear in the ACL list in the Sametime Administration Tool, you may need to type a valid filename in the Filename box of the Access Control List, and click the Access button to make the entire list of databases appear. The list of databases may not appear in the Access Control List until you have manually typed in a valid filename.

1. Start Internet Explorer and open the Sametime Administration Tool on the Sametime server.
2. Select Domino Directory (or LDAP Directory) - Access Control.
3. Enter a valid Sametime filename in the "Filename:" box of the Access Control List. (For example, type STCONF.NSF in the "Filename:" box.)
4. Click the Access button.

If the list of databases still does not appear, restart Internet Explorer, access the Sametime Administration Tool, and select the Domino Directory - Access Control link. The filenames should appear in the Access Control list.

Sametime server

Accessing Print Capture help on Windows 2000 systems

On a Windows 2000 system, the Sametime Print Capture help is difficult to access.

If you are using the Sametime Print Capture application to create files for display on the whiteboard, you can access the Print Capture help system in the following way:

1. Open the Windows program and the document you want to display on the whiteboard.
2. Choose File · Print (or equivalent command).
3. In the Print dialog box, select Sametime Print Capture as the printer.
4. Select the pages you want to print, and then click OK or Print.
5. When the Sametime Print Capture dialog box appears, click the help button.

The "Windows Help" window appears. Click the "Contents" or "Index" button from that window to access the Print Capture help topics.

Sametime Administration Tool

Administration tool unavailable after restarting STPlaces

If the ST Places Windows service stops, you will be unable to access the Sametime Administration Tool. The Sametime Administration Tool remains inaccessible even if you restart the ST Places service.

If the STPlaces services stops, you must restart the Sametime server to regain access to the Sametime Administration Tool.

Sametime Administration Tool, Sametime server, Web browsers

Broadcast connections monitoring does not show multicast users

The Sametime Administration Tool includes a Monitoring - Broadcast Connections - Connected Broadcast Users graph. This graph should display the number of users connected to the Sametime server with a Sametime Broadcast client.

If a user is attending a broadcast meeting, and receives broadcast meeting streams through unicast UDP or through TCP tunneling, the user is counted in the Connected Broadcast Users graph.

If a user is attending a broadcast meeting, and receiving the broadcast meeting streams through multicast UDP, the user does not appear in the Connected Broadcast Users graph.

The Connected Broadcast Users graph counts the number of Broadcast call control connections. When a user receives broadcast meeting streams through multicast, the user initially establishes a Broadcast call control connection but this control connection is severed when the user begins receiving the streams through multicast. When a user receives streams via multicast, the user may be counted briefly in the Connected Broadcast Users graph but will not appear in the graph once the control connection is severed.

For more information on the Broadcast client connection process, see the topic "Broadcast client connection process" in the "Configuring Sametime Connectivity" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime Administration Tool, Sametime server

Broadcast monitoring counts TCP-tunneled streams as Unicast

The Sametime Administration Tool includes a Monitoring -General Server Status-Total Broadcast Streams chart.

Sametime can transmit broadcast streams in three ways:

- Unicast UDP
- TCP Tunneling
- HTTP tunneling

The Total Broadcast Streams monitoring chart contains a "Unicast streams" section that reports the number of unicast broadcast streams that are sourced from the Broadcast Services of the Sametime server. Note that the "Unicast streams" section also counts any streams that are transmitted using TCP-tunneling.

When viewing the "Unicast streams" section of the Total Broadcast Streams monitoring chart, the administrator should be aware that the Unicast streams section reports both the number of broadcast streams that are transmitted using Unicast UDP and the number of streams transmitted using TCP-tunneling. In a network in which UDP is not available, and all broadcast streams must be transmitted using TCP-tunneling, all broadcast streams are counted as "Unicast streams."

For more information about how Sametime uses TCP and UDP in Broadcast meetings, see the topic "Broadcast client connection process" in the "Configuring Ports and Network Connectivity" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime server

Cannot delete or edit a meeting with a telephone conference call

If a user schedules a meeting that also includes a telephone conference call on a Latitude server, and the user uses either the Latitude Meeting Place User ID and password specified for authenticated or anonymous users in the Sametime Administration Tool when creating this conference call, only the user specified as the Meeting Moderator can reschedule the conference call.

If an administrator attempts to edit a meeting that has a conference call associated with it, the administrator will receive a "Name field is required for the request" error.

If a personal profile (individual User ID and password) is used to create the meeting, the administrator can edit the meeting provided that the administrator uses the same individual User ID and password that was used to create the meeting when editing the meeting.

Similarly, if an anonymous Sametime user schedules a meeting on the Sametime server, and the anonymous user authenticates with the Latitude MeetingPlace server using the user ID and password specified for anonymous users in the Sametime Administration Tool, the administrator will be unable to delete this meeting. Also, neither an anonymous user or the the Sametime administrator can edit the Meeting Details page to delete the telephone conference call from the meeting.

Attempting to delete the telephone conference call from the meeting may result in a Sametime WebQuerySave error or a WebCheckProgramSupport page error, and the conference call remains scheduled on the Latitude MeetingPlace Server.

Sametime server

Cannot import recorded meeting

If you have never recorded a meeting on a Sametime server, you may not be able to import a recorded meeting to that server.

For example, assume you have two Sametime servers (Sametime server 1 and Sametime server 2). You have recorded meetings on Sametime server 1 but have never recorded a meeting on Sametime server 2. You can use the "export a recorded meeting" feature to export a meeting from Sametime server 1 to a network drive. If you use the import feature on Sametime server 2 to import the meeting, you may receive an error when attempting to save the meeting on Sametime server 2.

This problem occurs because the C:\Sametime\MeetingArchive directory in which the Sametime server stores recorded meeting files (or .RAP files) is not created until the user records a meeting.

To prevent this problem, perform either of the following procedures on the Sametime server on which meetings have not been recorded:

- Record a test meeting for the purpose of creating the C:\Sametime\MeetingArchive directory.
- Use Windows Explorer to manually create the C:\Sametime\MeetingArchive directory.

Once the C:\Sametime\MeetingArchive directory exists on the Sametime server, you can import meetings to that directory. For related information, see "Changing the directory for Record and Playback (.RAP) files" in the "Things you need to know" section of the *Sametime 3.0 Release Notes*.

For more information about managing recorded meeting files, see "Managing recorded meetings (Record and Playback)" in the "Configuring the Meeting Services" chapter of the *Sametime 3.1 Administrator's Guide* (sthelapd.nsf or sthelapd.pdf).

Sametime server

Cannot search by first and last names

Sametime users can search the Directory on the Sametime server to add users to the presence list in Sametime Connect, to add users to the Who can see me list in Sametime Connect, or to restrict attendance to a meeting in the Sametime Meeting Center.

When searching for users in the Directory, users should search by last name only, not first name and last name. For example, to locate John Smith in the Directory, users must search on the name Smith, not John Smith. Searches by first name and last name are not supported in Sametime 3.1.

Sametime server

Changing HTTP port of the Sametime server

If you change the port number of the Sametime HTTP server to a port other than port 80, note the following:

- Users connected to the Sametime server cannot start instant meetings from the Participant List of the Sametime Meeting Center. If a user is attending a meeting, the user cannot start an instant meeting (or "nested meeting") with another user who is attending a meeting.
- If SSL is also enabled, and an administrator logs into the Sametime Meeting Center with a user name and password that does not belong to an administrator, the administrator cannot also access the Sametime Administration Tool using the administrator name and password without first closing the browser. For example, an administrator cannot log in to the Sametime Meeting Center as user John Smith and then attempt to open the Sametime Administration Tool using a different name and password that provides the administrator with access to the Sametime Administration Tool. If the administrator is logged into the Sametime Meeting Center as user John Smith, the administrator must start a new instance of the Web browser to log into the Sametime Administration Tool using the administrator's user name and password.

To change the HTTP port number in the Sametime Administration Tool:

1. Choose Configuration - Connectivity.
2. Select "Configure HTTP Services on a Web page in its own window."
3. Select "Ports"
4. Select "Internet Ports." The TCP/IP port number for the HTTP server is located under the "Web (HTTP/HTTPS)" column of settings.
5. Change the port number under the "Web (HTTP/HTTPS)" column to the new port number.
6. Select "Internet Protocols."
7. Select "Domino Web Engine."
8. Under the "Generating References to this server" section, change the Port number setting to the new port number.
9. Click "Save and Close" to save the Server document.
10. Restart the server for the change to take effect.

After changing the HTTP port number in the Sametime Administration Tool, you must also change the HTTP port number specified in the Tokens database on the Sametime server. To change the HTTP port number in the Tokens database:

1. Open STAuthT.nsf in the Sametime/Data directory.
2. Under the User Name column, open the SAMETIMESERVERHTTPPORT entry.
3. Enter the new value for the HTTP port in the Token field.
4. Save your changes.

Sametime Administration Tool

Changing the Broadcast gateway control port

The Broadcast gateway control port setting in the Sametime Administration Tool controls the port on which the Sametime Broadcast Gateway Controller connects to the Broadcast Gateway. The default setting for this TCP port is 8083.

If you change the Broadcast gateway control port setting in the Sametime Administration Tool, you must also change the port setting in the Windows Registry. If you do not also change the port setting in the Windows Registry, all Broadcast clients will be immediately disconnected from the server.

To change the port setting in the Windows Registry:

1. Run Regedit on the Sametime server.
2. Change the [HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Sametime\Broadcast Gateway] "ControlPort" = setting to match the port number that is specified in the "Broadcast gateway control port" setting of the Sametime Administration Tool.
3. Restart the Sametime server.

Sametime server

DiagnosticsFileOutput.txt file using too much disk space

Sametime is configured to generate diagnostics information by default. This diagnostic information is recorded in the DiagnosticsFileOutput.txt file on the Sametime server. If you find that the DiagnosticsFileOutput.txt file is using too much disk space on the Sametime server, you can disable the creation of this file. To disable the DiagnosticsFileOutput.txt file, use the instructions below.

1. Open Windows Explorer on the server machine.
2. Open the C:\Sametime\Data directory.
3. Open the servlet.properties file. (This is a text file that can be opened with any text editor.)
4. Remove the following text from each servlet entry: `Enable.Diagnostics.Notify=true`

Note: Before making the changes above you may want to save a backup copy of the servlet.properties file and store it in a different directory. You can use this backup copy to locate all appearances of the `Enable.Diagnostics.Notify=true` text if you want to enable the creation of the DiagnosticsFileOutput.txt file at a later date.

Sametime Connect client, Sametime server

Disconnections from Community Services with NAT

To accommodate environments that include a Virtual Private Network (VPN) set up to use Network Address Translation (NAT), changes have been made to the Sametime Java toolkit and a configuration flag (`VPS_IGNORE_UNKNOWN_CLIENT_IP`) has been added to the Sametime.ini file on the Sametime server.

In previous releases of Sametime, a user attempting to log in to Community Services from two different machines was disconnected at both machines. For example, a user could not log in to Community Services from a Sametime Connect client installed on client machine A and then open a Web browser on client machine B and connect to Community Services through Sametime features in a Sametime-enabled Discussion database.

This characteristic of the Community Services resulted in the following problem, which involves a user accessing an enterprise network through a VPN using NAT:

1. A user could be logged into the Sametime Community Services from the Sametime Connect client (a C++ application), or the Sametime Meeting Room client (a signed Java applet).
2. If a user also logged into Community Services from any application developed with the Sametime Toolkit (including Sametime presence lists in Discussion or TeamRoom databases), all of the user's connections to Community Services could be disconnected (even if all of the connections originated from the same machine).

Note: Sametime applications developed with the Sametime Toolkit are unsigned Java applets.

Explanation

The problem described above can occur when a user is accessing an unsigned Java applet and connecting to the Community Services through a proxy server. This situation can cause the Community Services to read two IP addresses for one client.

The Community Services can determine a client's IP address in two ways:

1. The Community Services can receive the IP address from the client. For example, a C++ application (Sametime Connect) and a signed Java applet (the Sametime Meeting Room) both calculate their own IP addresses and send them to the Community Services. If a client specifies its own IP address, the Community Services use this address to identify the client.
2. If a client does not specify its IP address, the Community Services can use the client's socket to calculate the IP address.

An unsigned Java applet (an application developed with the Sametime Toolkit) may not specify its IP address when connecting to the Community Services. If the unsigned Java applet connected through a proxy server, the IP address on the socket may be the IP address of the proxy server and not the IP address of the unsigned Java applet's host machine. As a result, it appears as though the same user has connected to the Community Services from two different IP addresses (the IP address of the Sametime Connect host machine and the IP address of the proxy server). The Community Services therefore sever all of the user's connections.

To solve the problem described above, the following changes have been made for Sametime 2.5 regarding Community Services connectivity:

- TheJava toolkit has been changed so that an application created with the toolkit (an unsigned Java applet) will never report an IP address.
- The configuration flag `VPS_IGNORE_UNKNOWN_CLIENT_IP` has been added to the `Sametime.ini` file on the Sametime server. This configuration flag is enabled by default.
- **When the `VPS_IGNORE_UNKNOWN_CLIENT_IP` flag in the `Sametime.ini` file is enabled (default setting),** and a Sametime client does not report an IP address, the Community Services allow the client to connect. The Community Services do not determine if the user is logged in from another machine. This configuration prevents the Community Services from disconnecting a user because the proxy server's IP address is different from the IP address that the Sametime Connect client reports.

The configuration described above allows a user to log into Community Services from two different machines, if one of the logins originates from an unsigned Java applet. This procedure is not recommended and can be very confusing for the end user.

Note: When the `VPS_IGNORE_UNKNOWN_CLIENT_IP` flag is enabled, it is still not possible for a user to log into Community Services from two Sametime Connect clients (or two Meeting Room clients) on two different machines. For example, a user cannot start a Sametime Connect client on client machine A, and then attend a meeting using a Meeting Room client on client machine B. Both the Sametime Connect client and the Sametime Meeting Room client report their IP addresses to the Community Services. If the IP addresses are reported, the Community Services ensure that the same user is not logged in from two different locations. The Community Services forego this check when the IP address is not reported, as is the case with unsigned Java applets created from the Sametime toolkit.

- **When the `VPS_IGNORE_UNKNOWN_CLIENT_IP` flag is not enabled,** and a Sametime client does not report an IP address, the Community Services use the client's socket to get the IP address. The Community Services also determine if the same user is logged in from a different IP address. If the user is logged in from two different IP addresses, the new log in disconnects the existing log in.

As a result, when the `VPS_IGNORE_UNKNOWN_CLIENT_IP` flag is not enabled, a user may be disconnected from Community Services even though all Community Services connections originate from the same machine. This disconnection occurs if the unsigned Java applet connects to the Community Services through a proxy server while the user is connected to Community Services from either the Sametime Connect client or the Sametime Meeting Room client.

When the `VPS_IGNORE_UNKNOWN_CLIENT_IP` flag is not enabled, a user is also disconnected when attempting to log into Community Services from two Sametime clients that report IP addresses to the Sametime server, if the two clients are on different machines. (Both the Sametime Connect client and the Sametime Meeting Room client report IP addresses to the Sametime server.) This is the same scenario described in the note above.

Sametime server

Discussion or TeamRoom database inoperable

The Secrets database (STAuthS.nsf) on a Sametime server plays an important role in authenticating connections to Sametime Discussion and TeamRoom databases (or other databases enabled with Sametime technology). You can enhance security for a Sametime server by turning on the `SametimeSecretGenerator` agent in the Secrets database on a Sametime server.

If you have installed multiple Sametime servers, and you enable the `SametimeSecretGenerator` agent, you should also do the following:

- Ensure that only one `SametimeSecretGenerator` agent is enabled in one Sametime Secrets database on one Sametime server.
- Delete existing Secrets databases on the other Sametime servers.
- Set up a replication schedule to replicate the Secrets database that is generating Secrets to all other Sametime servers.

If you have more than one Secrets database generating secrets, or if you have not deleted the Secrets database from other Sametime servers before replicating, the Secrets databases may include more than three secrets. If a Secrets database contains more than three secrets, Discussion databases and other Sametime-enabled databases will not function properly.

For more information, see "Using Sametime Discussion and TeamRoom databases" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime server

Discussion/TeamRoom databases and Notes Clients

No error message is displayed in the Notes client when a user is accessing a Discussion or TeamRoom database (or other database enabled with Sametime technology) and the Community Services components are shut down. The client reconnects automatically if the server comes up within 10 minutes. A "Lost connection to Sametime - OX 223, Please try again later" error message is displayed only if the client fails to reconnect after 10 minutes.

Sametime server

Do not use a directory name when creating a Discussion db

Users can create a Discussion database (db) from a Web browser by selecting the Discussions link from the Welcome to Sametime page.

When creating a Discussion database from a Web browser, users should not include a directory name in the File name field of the Create a Sametime Discussion page. Enter the database filename only; do not specify a path that includes a directory name.

If a directory name is included, a link to the discussion database appears on the Welcome to Sametime Discussions page, but users cannot use the link to access the database.

Sametime server

Do not use invalid XML characters in Sametime server names

Sametime 3.0 will not work if any server in a community includes invalid XML characters in the server name. Do not use the following characters in any Sametime server name: > < & ' " ;

Sametime server

Domino Capacity Monitor fails to start

If the Domino HTTP server is configured so that anonymous access is not allowed, the Domino Capacity Monitor will not start. You must allow anonymous access to the Domino HTTP server to enable the Domino Capacity Monitor to start.

Sametime server

Error scheduling meeting that includes telephone conference call

If a user schedules a meeting that includes a telephone conference call, and the conference call is assigned a conference call ID of less than four characters, the user receives the following error message when saving the meeting:

Error [5199] Specified meeting ID length less than minimum allowed length, which is configured in scheduling parameters

To avoid this problem, assign a conference call ID that is at least four characters long when scheduling a meeting.

Sametime server

HTTPS in URL listed in the meeting details document is incorrect

If you have set up one Sametime server to encrypt Web browser connections with SSL, and you have created a Connection document of the Connection type "Sametime" to connect this SSL-enabled Sametime server to a Sametime server that is not encrypting Web browser connections with SSL, the following problem may occur:

When the SSL-enabled Sametime server invites the other (non SSL-enabled) Sametime server to a meeting, the meeting details document in the Sametime Meeting Center will indicate that the URL of the non-SSL Sametime server begins with Https: when the URL actually begins with Http:. Users attempting to attend the meeting on the non SSL-enabled Sametime server using the URL that begins with Https: will not be able to connect to the server.

Users can still access the non-SSL Sametime server using the correct URL that begins with Http: and attend the meeting. However, this URL will not be listed on the meeting details page. Only the incorrect URL beginning with Https: is listed on the meeting details page.

To avoid this problem, it is recommended that you maintain a consistent environment for SSL. If you have enabled one Sametime server to encrypt Web browser connections using SSL, you should also enable your other Sametime servers to use SSL.

Note: An administrator can create a Connection document of the Connection type "Sametime" to enable a meeting started on one Sametime server to become simultaneously active on another Sametime server. This functionality is frequently referred to as "invited servers" and is described in the "Deploying Multiple Sametime Servers" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime Connect client, Sametime server, Web browsers

Instant meeting fails if .tmp file type associated with Notepad

If the .TMP file type is associated with Notepad in Windows, an instant meeting may fail after a user responds to an instant meeting invitation. This problem occurs only if the user has a Netscape Web browser set as the default browser in Windows. When the user responds to the instant meeting invitation, Netscape launches and opens Notepad to display an HTML file.

Netscape users should not have the .TMP file type associated with Notepad in Windows.

Sametime server

Invited servers require same HTTP port number for meeting links

When one server invites another server to a meeting, both servers should use the same HTTP port number. If the servers use different HTTP ports, the links to the invited server will be incorrect in the Meeting Details document.

For example, assume that Sametime server A uses HTTP port number 8088 and Sametime server B uses HTTP port number 80. A meeting is created on Sametime server A. Sametime server A invites Sametime server B to the meeting. The Meeting Details document for the meeting on Sametime server A contains a link to the meeting on Sametime server B. Sametime server A appends the HTTP port number that it uses (port number 8088) to this link instead of the port number that Sametime server B uses (port 80), and the link does not function correctly.

Sametime Meeting Room client, Sametime server

Latitude MeetingPlace server does not call user back

When a user attends a Sametime meeting that also includes a scheduled conference call on a Latitude MeetingPlace server, the user may see a dialog box that prompts the user to enter the user's own telephone number. The dialog box indicates that the MeetingPlace server will call the user back at the telephone number that is entered in the dialog box.

In some situations, the Latitude MeetingPlace server will not call the user back, even though the dialog box informs the user to expect a call. If the Latitude MeetingPlace server does not call a user back as expected, the user must make a telephone call to the Latitude server. The call-in information required to join the conference call should be available at any of the following places:

- The Meeting Details document for the meeting in the Sametime Meeting Center
- Directly beneath the Join Now button below the Participant List in the Sametime Meeting Room
- In the dialog box that indicates the Latitude MeetingPlace server will call the user

Sametime server

Listed user name appears not active in the public group

If a user is listed in a Group document, the name in the Group document must be the first name that appears in the User name field of the Person document. If the first name in the User name field is not used in Group documents, the user will always appear to be offline when the group is opened in a Sametime presence list.

For example, assume a user's name is listed in the User name field of the Person document as:

Tom Smith/West/Acme
Tom Smith

When including the user in a Group document, you should enter the name in the Group document as Tom Smith/West/Acme (the first name that appears in the User name field).

Generally, self registered users will always have the shortened version of the name (Tom Smith) listed first in the User name field of the Person document.

If the shortened form of the name appears first in the User name field, then the shortened form of the name should also be used when adding the user to a Group document.

Sametime server

Maximum online meeting password length

When creating a password for an online meeting in the Meeting Center, the maximum password length is 80 characters.

Sametime Connect client, Sametime Meeting Room client

Maximum user and server connections limit off by one

If you have set a limit in the "Maximum user and server connections to the Community server" option in the Configuration - Community Services settings of the Sametime Administration Tool, users might be unable to connect when they reach the number specified as the limit (rather than the number one above the limit). For example, if the administrator has set the limit to 50, the 50th user might not be able to connect.

Sametime server

Meeting name does not appear on connected (or "invited") server

A Sametime Administrator can create a Connection document of the Connection Type "Sametime" to enable a meeting started on one Sametime server to be simultaneously active on another Sametime server. This functionality is frequently called "invited servers" as one server "invites" another server to the meeting.

The procedure for creating these Connection documents is described in the topic "Creating Connection Records to connect Sametime servers" in the "Deploying Multiple Sametime Servers" chapter of the *Sametime 3.1 Administrator's Guide*.

When creating a Connection Document to connect two Sametime servers, it is important that the Domino domain name is used along with the server name in the Source server and Destination server fields of the Connection document. For example, if the name of the source Sametime server (the server on which the meeting is started) is SametimeA.acme.com, and the domain name is ACME, the server should be specified as SametimeA.acme.com/ACME in the Source server field of the Connection document. Similarly, if the name of the destination server (the server being invited to the meeting) is SametimeB.acme.com and its domain is ACME, the server should be specified as SametimeB.acme.com/ACME in the Destination server field.

If the domain name is not included in the Source and Destination fields of the Connection document, the meeting name will not appear on the invited server.

Note: You should also disable the replication features in the Connection document when creating a Connection document of the Connection Type "Sametime." For more information, see the topic "Disable replication for 'invited servers' Connection documents" in the Troubleshooting - Sametime server issues section of these release notes.

Sametime server

Meetings are not recorded as expected

The Sametime server includes a record and playback feature that allows the Sametime server to record a meeting and store the recorded meeting in a Sametime Record and Playback (.RAP) file on the Sametime server. The administrator enables the record and playback feature by selecting the "Allow people to record meetings for later playback" setting in the Configuration - Meeting Services - General settings of the Sametime Administration Tool.

After selecting the "Allow people to record meetings for later playback" setting, the administrator can either accept the default settings or change the settings for the following two recorded meeting options.

- **Save recorded meetings in the following location** - This field specifies the default directory in which Sametime .RAP files are stored. The default setting is C:\Sametime\MeetingArchive\.

If you change the default directory to a different directory, you will not receive notification if the new directory does not exist or cannot be created. If the directory you specify does not exist or cannot be created, meetings will not be recorded.

If you change the directory setting in the "Save recorded meetings in the following location" field, use Windows Explorer to verify that the directory specified in the field exists on the Sametime server, or to create the directory if necessary.

- **Stop recording when this much disk space is left (Mbytes)** - This setting specifies the amount of free disk space (in Megabytes) that must exist on the Sametime server for the recording of meetings to continue. If meetings are not being recorded, verify that there is enough free disk space on the server.

For more information about the record and playback feature, see "Managing recorded meetings (Record and Playback)" in the "Configuring the Meeting Services" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime server

Meetings do not become active on connected ("invited") server

If you have created a Connection document to connect Sametime server A to Sametime server B, and a meeting started on Sametime server A does not become simultaneously active on Sametime server B as expected, verify that you have entered the DNS host name or IP address of the destination Sametime server (Sametime server B) in the "Optional network address" field of the Sametime Connection document that connects these two Sametime servers.

The "Optional network address" field is not an optional field. This field is required when creating a Connection document (of the Connection Type "Sametime") that connect two Sametime servers.

Note: A Connection document of the Connection Type "Sametime" enables a meeting started on one Sametime server to be simultaneously active on another Sametime server. This functionality is frequently called "invited servers" as one Sametime server "invites" another Sametime server to a meeting. These Connection documents can be created from a Lotus Notes client or the Connectivity - Servers in this Community settings of the Sametime Administration Tool.

If this field is left blank, the server also will not appear as available in the Locations tab of the New Meeting page in the Sametime Meeting Center.

Sametime Administration Tool, Sametime Broadcast client

Monitoring tab info incorrect for broadcast multicast streams

The Monitoring tab of the Sametime Administration Tool might display incorrect statistics for the number of multicast and unicast streams in broadcast meetings. Multicast streams might be incorrectly counted as unicast streams.

Sametime Administration Tool, Sametime server

Multicast address ranges for Broadcast Services not working

If you have a multicast-enabled network, the Sametime Broadcast Services can use multicast to transmit broadcast meeting streams on the network. A Sametime administrator can use the Sametime Administration Tool to enable the multicast functionality and enter a range of Class D multicast IP addresses to be used by the Broadcast Services.

The Broadcast Services randomly select an IP address from the range of IP addresses specified by the Sametime administrator in the Sametime Administration Tool. The Broadcast Services then begin transmitting data to the selected multicast address at a multicast-enabled router. The Sametime Broadcast clients "join" the multicast address to receive the broadcast meeting streams.

When specifying the range of available multicast addresses in the Sametime Administration Tool, the administrator must ensure that the IP addresses specified for multicast use do not contain a low octet with a value of zero.

To view the multicast address range settings, open the Sametime Administration Tool and select Configuration - Connectivity - Networks and Ports and scroll to the "Broadcast Services Network" settings. The "Multicast addresses start at IP address" and the "Multicast addresses end at IP address" fields allow you to define the range of available multicast IP addresses.

In both the "Multicast addresses start at IP address" and the "Multicast addresses end at IP address" fields, you enter an IP address that contains four octets (for example, www.xxx.yyy.zzz). If the lowest octet (zzz in the example) is zero in either the "Multicast addresses start at IP address" or the "Multicast addresses end at IP address" field, the multicast address range settings do not work. Verify that the lowest IP octet in both of the multicast address range fields has a value between 1 and 255, but not 0.

Sametime server

Must enter full server name to log on to Sametime

If an end user is able to access the Sametime Welcome page but is having trouble logging on to Sametime, he or she should enter the full DNS name of the Sametime server in the browser. For example, enter www.sametime.east.com.

Sametime Administration Tool, Sametime server

NetMeeting meetings do not extend past scheduled end time

The Sametime Administration Tool includes a "Configuration - Meeting Services - Automatically extend meetings beyond scheduled end time when there are still people in the meeting" setting that allows a meeting to extend past its scheduled end time if users are still in attendance when the scheduled end time arrives.

If the meeting includes NetMeeting clients (the user selected the "Use NetMeeting" option when creating the meeting), the meeting will end at the scheduled end time regardless of whether the "Automatically extend meetings beyond scheduled end time when there are still people in the meeting" is selected in the Sametime Administration Tool. NetMeeting meetings cannot be automatically extended.

Note: A meeting can include NetMeeting clients if a user selects the "Use NetMeeting" option in the Tools tab of the New Meeting form when creating the meeting.

Sametime server

New Meeting page does not display "Telephone conference call"

The Sametime administrator enables the Sametime server to operate with a Latitude MeetingPlace server by configuring the appropriate options in the Configuration - Meeting Services - Telephone Options of the Sametime Administration Tool.

When Sametime is configured to operate with a Latitude server, a "Telephone conference call" option appears at the bottom of the Tools tab on the New Meeting page in the Sametime Meeting Center. If the browser font size is too small, the "Telephone conference call" option is only partially visible to the user.

To fix this problem, the user should increase the font size of the browser. In Internet Explorer, use the View - Text Size menu option to increase the font size. In Netscape, use the View - Increase Font menu to increase the font size.

Sametime server

No meetings in the "Today's Meetings" view of the Meeting Center

If no meetings appear in the "Today's Meetings" view of the Sametime Meeting Center, see the release note titled "Subscript out of range 47 error when creating repeating meetings" in the Troubleshooting - Sametime server issues section of the Sametime 3.0 Release Notes.

Sametime server

Password protected ID not supported for additional server

After installing the first Domino/Sametime server, do not enable password protection for the server.id of any additional Domino server that you install (for the purpose of supporting a Sametime server).

If password protection is enabled on the server.id of the additional Domino/Sametime server, Domino, Sametime, and TCPIP will consistently hang on that server.

To disable password protection on the server.id, open a Notes client on the additional server and select Files-Tool-User ID-Disable password.

Sametime server

Presence lists are grayed out in Discussion database

If presence lists are unavailable (appear as grayed out boxes) in a Discussion or TeamRoom database, see the topic "Domino server name must include the IP host name" in the Troubleshooting - Installation Issues section of these Release Notes.

Sametime server

Renaming the stcenter.nsf database

The stcenter.nsf database contains the Sametime server home page (or the Sametime Welcome page). If you rename the stcenter.nsf database, or replace it with a different home page, you must ensure that the links in Sametime databases such as stconf.nsf (the Sametime Meeting Center) and streg.nsf (the self-registration database) are also altered to point to the new home page.

If you rename the stcenter.nsf database or use a new Lotus Notes database as the home page, you must also change the "Home URL" setting in the Internet Protocols - HTTP - Mapping section of the Sametime Server document to point to the renamed or new database.

If you use an HTML file instead of a Lotus Notes database as a home page, leave the "Home URL" setting on the Server document blank. Enter the name of the HTML page in the "Default home page" setting in the Internet Protocols - HTTP - Basics settings of the Server document. All links in other Sametime databases must also be altered to point to the HTML page.

Sametime Administration Tool

Restart the server when changing logging options

The Sametime Administration Tool contains settings that enable the administrator to log Sametime information to either a database or a text file. These settings include the "Enable logging to a Domino database" check box or the "Enable logging to a text file" check box located in the Logging - Settings menu of the Sametime Administration Tool.

If the administrator changes the logging settings (switches from a database to a text file, or from a text file to a database), the administrator must restart the Sametime server for the change to take effect.

Sametime server

Scheduling a telephone conference call crashes Sametime nHTTP

When Sametime is configured to work with a Latitude MeetingPlace/WebPublisher server, a Sametime user can access the Sametime server and use Sametime interfaces to schedule a telephone conference call on the Latitude server. The WebPublisher server associated with the Latitude server must be running when the user attempts to schedule the telephone conference call. If the Latitude WebPublisher server is not running, the Sametime HTTP server will not allow a meeting to be scheduled with the telephone conference call.

Sametime server

Self registered user cannot change password

Domino includes an Update to More Secure Internet Password... option that allows an administrator to upgrade a user's Internet password to a more secure password format. (The administrator selects this option by opening a user's Person document with a Lotus Notes client and selecting Actions - Upgrade to More Secure Internet Password Format.)

If the administrator selects this option for a self-registered Sametime user, the user cannot change their Internet Password from the Self Registration feature on the Sametime server. The administrator should not use the Update to More Secure Internet Password... feature to upgrade a user's Internet password to a more secure password format.

Sametime server

Self registration does not work

If you have followed the instructions in the *Sametime Administrator's Guide* to enable self registration, note that the administrator's guide does not state that the "Create Documents" privilege must be selected in the Domino Directory ACL to enable self registration.

To enable self registration, verify that all of the following conditions exist:

- The signer "Sametime Development/Lotus Notes Companion Products" is added to the ACL of the Domino Directory on the Domino 6.0.2 server.
- The "Sametime Development/Lotus Notes Companion Products" signer is assigned the "Author" access level in the Domino Directory ACL.
- The "Sametime Development/Lotus Notes Companion Products" signer has the following Roles assigned in the Domino Directory ACL: Group Creator, Group Modifier, User Creator, User Modifier.
- The "Create Documents" privilege is selected in the Domino Directory ACL.

Sametime server

STLog.nsf on invited server does not record names

If one Sametime server invites another Sametime server to a meeting, the invited server does not record the names of meeting participants in its Sametime log database (STLog.nsf).

You must create a Connection document of the Connection type "Sametime" to enable one Sametime server to invite another Sametime server to a meeting. You can also use the Configuration - Connectivity - Servers in this Community settings of the Sametime Administration Tool to create these Connection documents. For more information, see the "Deploying Multiple Sametime Servers" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime server

Subscript out of range 47 error when creating repeating meetings

If a user creates a repeating meeting that includes an invalid day for the specified date range, the user sees a "Subscript out of range 47(ListSort)" error. For example, assume a user schedules a meeting to repeat every Monday and then selects a date range that runs from 08/28/2001 to 09/02/2001 (or Tuesday through Sunday). Since there is no Monday in the specified range of 8/28/2001 to 9/2/2001, the user sees the error "Subscript out of range 47(ListSort)" error after clicking the OK button to save the meeting.

The meeting appears in the Scheduled and All Meetings views of the Sametime Meeting Center and cannot be deleted from the Meeting Details document for the meeting. You must use a Lotus Notes client to delete the Meeting Document for this meeting.

If a repeating meeting is scheduled with an invalid day for the specified date range, the meeting may also corrupt the "Today's Meetings" view of the Sametime Meeting Center so that no meetings appear in that view. Meetings scheduled with an invalid day in the date range will usually list the year as "-2" when displaying the scheduled date of the meeting in the Sametime Meeting Center. For example, if you see a meeting in the Sametime Meeting Center that is scheduled to start on 10/30/-2, it is likely that this meeting was scheduled in the manner described above.

The "Today's Meeting" view of the Sametime Meeting Center will function properly if you use a Lotus Notes client to delete the Meeting Details document for the meeting. To use the Lotus Notes client to delete the Meeting Details document:

1. From the Start menu of the Sametime server, open the Lotus Notes client. (Choose Start - Run, browse to C:\Lotus\Domino\lnotes.exe, and click OK.)
2. Choose File - Database - Open.

3. Select "Local" in the Server drop-down box.
4. Select the Sametime 3.0 Online Meeting Center database (stconf.nsf) and click Open.
5. From the View menu, select "Go To."
6. Select the "All Meetings" view.
7. In the right-hand pane, right-click on the Meeting document for the meeting and select "Clear."
8. Select the "View - Refresh" menu item and select "Yes" to delete the Meeting document.
9. Close the Lotus Notes client.

Sametime server

Telephone conference calls and "invited" Sametime servers

If you configure Sametime server A to operate with a Latitude Web Publisher/MeetingPlace server, and then create a Connection document (of the Connection type "Sametime") to connect Sametime server A to Sametime server B, Sametime server B should also be configured to operate with the Latitude Web Publisher/MeetingPlace server.

Note: When two Sametime servers are connected by a Connection document of the Connection type "Sametime," a meeting started on one Sametime server can become simultaneously active on another Sametime server. This capability is frequently referred to as "invited" servers, and is discussed in the "Deploying Multiple Sametime Servers" chapter of the *Sametime 3.1 Administrator's Guide*.

If two Sametime servers are connected, and Sametime server A is configured to operate with the Latitude server while Sametime server B is not, the following scenario can occur:

1. A user schedules a meeting that includes a telephone conference call on Sametime server A.
2. Sametime B, which is not configured to operate with the Latitude server, is invited to the meeting by Sametime server A.
3. A user attends the meeting on Sametime server B.
4. The user connected to Sametime server B hits the Join call button. The user will see a window that contains only an OK button but contains no calling details. The user will not have the information necessary to dial in to the telephone conference call.

The user can receive the proper information after hitting the Join call button only if Sametime server B (the invited server) is also set up to use a Latitude WebPublisher server and can connect to the Latitude MeetingPlace server on which the telephone portion of the meeting is scheduled.

Sametime server

Turkish regional settings on Windows require VM upgrade

If the Windows regional settings are set to Turkish on the server on which Sametime is installed, Sametime might not function properly. This problem pertains to the version of the Microsoft Java Virtual Machine (VM) used on the server.

If this problem occurs, you can fix it by upgrading the Microsoft VM on the Sametime server machine to the latest build. This Microsoft VM build is available at http://www.microsoft.com/java/vm/dl_vm40.htm.

Sametime server

Unable to attach large whiteboard files to Sametime meetings

When a user attempts to attach a large whiteboard file to a meeting, the user's Web browser may return an error indicating the action is not possible or that the file is too large.

The Domino server configuration limits the size of these files to 10000 Kilobytes by default. To prevent this problem, you must adjust the Domino configuration settings to allow larger files to be posted. To adjust the appropriate Domino server configuration settings:

1. In the Domino directory on the Domino/Sametime server, open the Server document for the Domino/Sametime server.
2. Select the "Internet Protocols" tab.

3. Under the HTTP tab, change the HTTP Protocol Limits -> Maximum size of request content setting from 10000K to an appropriate (higher) value. This setting should specify the size in kilobytes of the largest whiteboard file that you want to allow users to attach to a Sametime meeting.
4. Select the Internet Protocol -> Domino Web Engine tab.
5. In the POST Data -> Maximum POST Data field, enter the same value that you specified in step 3 above. This setting should also specify the size in kilobytes of the largest whiteboard file that you want to allow users to attach to a Sametime meeting.
6. Save and close the server document and restart the Domino/Sametime server.

Sametime server

Unable to restart Sametime after Sametime Links is installed

The following problem might occur after you have installed Sametime Links on a Sametime server.

You can stop the Sametime server from the Services dialog in the Windows Control Panel by selecting the "Sametime Server" service and clicking the Stop button. After stopping the Sametime server, you cannot start the Sametime server again by selecting the "Sametime Server" service in the Windows Control Panel Services dialog and clicking the "Start" button.

If the Sametime server cannot be started from the Control Panel Services dialog, restart the machine on which Sametime is installed. The Sametime services will all be started automatically when the Windows server restarts.

Sametime server

Usage Limits and Denied Entry for Broadcast Meetings

The Sametime Administration Tool contains "Usage Limits and Denied Entry for Broadcast Meetings" settings. These settings are accessible from the Configuration - Audio/Video - Usage Limits and Denied Entry options of the Sametime Administration Tool and are designed to limit the number of users of the Sametime Broadcast Services. Administrators should limit the number of users to prevent a large number of users from taxing the server CPU or bandwidth capabilities of the network to the point where meeting performance degrades.

The Usage Limits and Denied Entry for Broadcast Meetings settings allow you to limit the number of:

- Audio connections
- Video connections
- Data connections (screen share and whiteboard)

If a meeting includes multiple activities, users will be rejected once the lowest limit that is specified for any of the activities included in the meeting is reached.

For example, assume a broadcast meeting includes audio, video, and data (screen sharing/whiteboard) and the Usage Limits and Denied Entry for Broadcast Meetings settings limit the audio connections to 30 users, video connections to 30 users, and data connections to 40 users. When the 31st user attempts to join the Broadcast meeting, the user will be rejected. The user cannot receive the data (screen sharing/whiteboard) portion of the meeting even though that limit is set to 40.

If the Broadcast meeting included only data activities, 40 users would be allowed to join the meeting and the 41st user attempting to join the Broadcast meeting would be rejected.

Sametime Meeting Room client, Sametime server

User cannot save the whiteboard

If a user cannot save the whiteboard, verify that the following two options are selected in the Sametime Administration Tool Configuration - Meeting Services - General settings:

- Allow people to choose the whiteboard in meetings
- Allow people to save whiteboard annotations as attachments to the meeting

If both of these settings are selected, and the user still cannot save the whiteboard, see the release note titled "Server display setting must be higher than 256 colors" in the "Things you need to know" section of the *Sametime 3.1 Release Notes*.

Sametime Administration Tool

User ID displays as numbers/characters in Administration Tool

The Sametime Administration Tool contains several logging pages that contain a User ID column. If a user authenticates when accessing the Sametime server, the User ID column displays one of the following:

- A Lotus Notes User ID in canonical format
- A User Name from a Person document in a Domino directory
- A distinguished name from an LDAP directory

If a user does not authenticate and accesses Sametime as an anonymous user, the User ID column displays a series of numbers and characters to represent the anonymous user. For example, an anonymous user may be represented by a series of numbers and characters such as 3810 0c065e13c in the User ID column.

Sametime server

Users only logged into a database cannot be invited to a meeting

If a user is logged into Community Services from a Sametime Discussion or TeamRoom database, but the user is not logged in from Sametime Connect or the Sametime Meeting Room client, the user cannot be invited to attend a meeting with other online users. If another user invites the database-only user to a meeting, the inviting user will see a "Cannot create chat" error message.

If the user is logged into Community Services from Sametime Connect or the Sametime Meeting Room client, the user can be invited to a meeting. The user can also be invited to a meeting if the user is logged into Community Services from a Sametime database while simultaneously being logged into Community Services from either the Sametime Connect client or the Sametime Meeting Room client.

Sametime server

Using Lotus Notes client stops Domino processes on Sametime

A Lotus Notes setup client is automatically installed on the Sametime server during the Sametime server installation. An administrator can start this Notes client on the Sametime server from the Windows desktop by choosing Start - Run and browsing to the C:\Lotus\Domino\lnotes.exe file. Administrators can use this Lotus Notes setup client to change administration settings in the Domino Directory on the Sametime server and access other Domino databases on the Sametime server.

Occasionally, launching this Lotus Notes client on the Sametime server may kill the Domino processes running on the Sametime server. You should not launch this Lotus Notes client during times of heavy server usage. If the Domino process are killed, you must restart the server.

Sametime server

Using self-registration with multiple Sametime servers

You can install multiple Sametime servers in a Domino environment and synchronize the multiple servers to function as a single community. Part of this procedure involves enabling the Directory to replicate between the Sametime servers.

Note: For more information on synchronizing multiple Sametime servers to function as a single community, see the "Deploying Multiple Sametime Servers" chapter of the *Sametime 3.1 Administrator's Guide*.

If you have enabled the Directory to replicate between multiple Sametime servers, and you are also using the self-registration feature, you should enable the self-registration feature on only one of the Sametime servers. (Allowing users to self register from different Sametime servers in a multiple server environment creates duplicate groups in the Directory. For example, you might see two groups named Sametime Web Users.)

Sametime server

Using "Alt+159" accented characters with user registration

Sametime includes a self-registration feature that enables anonymous users to create Person documents in the Domino directory on the Sametime server. The self registration feature allows users to enter a User name (first, middle, and last) and Internet password.

Avoid using the "Alt+159" DOS character code in the self-registration interface. Using the "Alt+159" DOS character code in the "Last name" or "Password" fields of the self registration interface on the Sametime server causes the following problems:

- Users will receive a "User not authenticated" error when attempting to use the password containing the "Alt+159" character to authenticate with the Sametime Meeting Center.
- Users will receive an error message if they try to enter a name containing the "Alt+159" character in the "Last name" field of the self-registration interface.

Users should also avoid using the "Alt+159" character when creating new TeamRoom or Discussion databases on the Sametime server. If the "Alt+159" character is used in the database name when creating a new database, the user receives a message indicating that the name of the database already exists (even though the user is in the process of creating it). After the user receives this message, the database is created on the server.

Note: Generally, DOS character codes should not be used with Sametime. Lotus recommends using Windows code page 1252 with Sametime. With Windows code page 1252, the keyboard combination "Alt+0131" generates the same character as the "Alt+159" DOS character code. Note that using the Windows code page will not prevent the problems described above. The "Alt+0131" and "Alt+0159" Windows code page character may also produce these problems.

Sametime server

Verifying the version number of a Sametime server

If you do not know which version of Sametime is installed, you can use the following URLs to display the Sametime server version numbers:

- For Sametime 1.0 and 1.5 servers, the server version number can be accessed through the URL <http://servername/buildinfo.txt>
- For Sametime 2.0, 2.5, 3.0 servers, and 3.1 servers, the server version number can be accessed through the URL <http://servername/sametime/buildinfo.txt>

Note: servername is the name of the Sametime server.

Sametime server

Wrong meeting start time displays when importing a meeting

The Sametime server enables a user to record a Sametime meeting and then export the recorded meeting file (exporting the file involves saving and renaming the file to a local drive or network drive). The user can then import this recorded meeting file to different Sametime servers to make the recorded meeting available from these servers.

When the user imports the meeting, the meeting start time will display in a read-only field in a meeting creation screen. Note that the meeting start time may be incorrect and will not reflect the start time of the original meeting. There is no workaround for this problem.

Sametime Administration Tool

"Connection Broken" message for Java Sametime Connect logouts

The Sametime Administration Tool includes a Logging-Community Logins/Logouts view that describes the reasons for logins or logouts to the Community Services. The Community Logins/Logouts view might erroneously report a logout reason of "Connection Broken" when users logout of the Java version of Sametime Connect ("Sametime Connect for browsers").

If a user running Sametime Connect for browsers performs any of the following actions, the Community Logins/Logouts view might indicate "Connection Broken" as the reason for the logout:

- The user logs off "Sametime Connect for browsers."
- The user exits "Sametime Connect for browsers."
- The user closes the Web browser window in which "Sametime Connect for browsers" is running.

The Community Logins/Logouts view should indicate the reason for these type of logouts is "Normal exit" instead of "Connection Broken." The administrator can ignore the "Connection Broken" message for these logouts.

Sametime Connect client, Sametime server

"Message received when inviting others to a meeting

The message "You are not allowed to browse the directory because you are not a registered user" may appear when an anonymous user attending a meeting attempts to invite another user to the meeting using the "Meeting - Invite others" option in the menu bar of the Sametime Meeting Room client.

This error message appears when the Configuration - Community Services - Anonymous Access settings in the Sametime Administration Tool are set to prevent anonymous users from browsing the Directory. (The Meeting - Invite others option contains Directory browsing features.)

To prevent this error message from occurring you must configure the Anonymous Access settings in the Sametime Administration Tool to enable anonymous users to browse the Directory. To do this, make sure that the "Users cannot browse the Directory" check box in the Configuration - Community Services - Anonymous Access settings of the Sametime Administration Tool is not selected.

Sametime server

"Sametime server (no node name config)" in NetMeeting or ST Log

When a NetMeeting user attends a Sametime meeting, the T.120 connection (which supports screen sharing and whiteboard) from Sametime to NetMeeting may appear in the NetMeeting participant list as "Sametime server (No node name configured)."

The Sametime server name may also display as "Sametime server (No node name configured)" in the Logging - Meeting Connections view of the Sametime Administration Tool.

You can control how the Sametime server name appears in the NetMeeting participant list and the Sametime Log by altering the registry settings on the Sametime server. To alter the registry settings for this purpose:

1. Run Regedit.
2. Under HKEY_LOCAL_MACHINE ->SOFTWARE -> Lotus->Sametime ->Meeting server ->NC, double-click on the Node name and change the setting to the name you want to appear for the Sametime server (for example "Acme Sametime server").

After you make this change, the name you entered in the Registry will appear for the Sametime server in the NetMeeting participant list and Sametime Logging options available from the Sametime Administration Tool.

Audio/Video services issues

Audio/Video services

Echo cancellation in multiple a/v meetings

If two users are participating in more than one audio/video meeting at once, echo cancellation might not work between the two users. For example, if User 1 and User 2 are both attending a scheduled audio/video meeting, and User 1 begins an instant audio/video meeting with User 2, echo cancellation might not work for either user.

Audio/Video services

NetMeeting video window freezes

If users are attending an audio/video meeting with both Sametime Meeting Room clients and Microsoft NetMeeting clients, the video window might freeze and stop switching to display the person currently speaking in the meeting. This problem occurs for NetMeeting users only. The problem usually occurs when there is a brief period of inactivity (no one is speaking for 3 to 5 minutes) in the meeting.

The immediate workaround for this problem is to have the NetMeeting user exit and rejoin the meeting.

This problem pertains to the size of the packets that are sent on the network during an audio/video meeting. Larger packets are sent on the network when a meeting is using the Connection Speed settings that are specified for the "Meetings with LAN/WAN users" option in the Configuration - Audio/Video - Connection Speed Settings of the Sametime Administration Tool.

The default "Video bit rate" setting of 64Kbps may contribute to the video window freeze problem seen with NetMeeting clients. If your environment is such that users with Sametime Meeting Room clients and NetMeeting clients will frequently attend the same meetings, the administrator may want to experiment with lower "Video bit rate" settings for the "Meeting with LAN/WAN users" connection profile.

The steps below describe how to lower the "Video bit rate" setting for the "Meetings with LAN/WAN users" connection profile.

1. Open the Sametime Administration Tool on the Sametime server.
2. Select Configuration - Audio/Video - Connection Speed Settings.
3. Beneath the "Audio/Video and Broadcast Connection Speeds" heading, select "Meetings with LAN/WAN users" from the drop-down list.
4. For the "Video bit rate" setting, select either the 16Kbps or 32Kbps setting. (Lower settings will reduce the quality of video images in the meeting but prevent the problem described in this release note.)
5. Click the Update button and restart the Sametime server for the change to take effect.

For more information about working with audio/video Connection Speed Settings, see the "Connection Speed Settings for Audio/Video Services" section of the Configuring Audio/Video Services chapter of the *Sametime 3.1 Administrator's Guide*.

Audio/Video services, Sametime server

Poor audio quality with G.711 audio codec and TCP Tunneling

The Sametime Multimedia Services transmit audio streams using the UDP transport. If UDP is unavailable on a network (either disabled at the routers or firewall), the Multimedia Services tunnel the UDP audio streams through the TCP transport.

If a client receives the audio stream through a TCP tunneled connection with the Sametime server, and the G.711 audio codec is also being used in the meeting, the client may experience poor audio performance. The G.723 audio codec should be used whenever you expect users to attend an audio meeting through TCP tunneled connections.

Note: The G.711 audio codec is specified in the Configuration - Audio/Video Services - Connection Speed Settings of the Sametime Administration Tool. Generally, the administrator selects the "Meetings with LAN/WAN users" connection profile and selects the 64Kbps "Audio bit rate" setting to select the G.711 audio codec. The G.711 codec is then used in the meeting if an end user de-selects the "People are attending this meeting using a modem" option in the Locations tab of the New Meeting page. (De-selecting this setting invokes the "Meetings with LAN/WAN users" connection profile.)

If your network environment requires that users receive the audio streams via TCP tunneled connections, you must configure the settings in the Sametime Administration Tool so that the G.723 codec is always used in audio/video meetings.

To configure the Audio/Video Services Connection Speed Settings so that the G.723 codec is always used in a meeting, you can do the following:

- In the Configuration - Audio/Video - Connection Speed Settings of the Sametime Administration Tool, ensure that the "Type of connection speed settings to use for the default in scheduled and instant meetings" is set to "Meetings with modem users." ("Meetings with modem users" is the default setting.) This step ensures that the G.723 audio codec is used by default in all instant audio meetings.
- In the Configuration - Audio/Video - Connection Speed Settings of the Sametime Administration Tool, ensure that the "Meetings with modem users" option located beneath the "Audio/Video and Broadcast Connection Speeds" heading has an "Audio bit rate" setting of 6.3Kbps. (6.3Kbps is the default setting.)
- (Optional) In the Configuration - Audio/Video - Connection Speed Settings of the Sametime Administration Tool, the administrator can set the "Meetings with LAN/WAN users" option located beneath the "Audio/Video and Broadcast Connection Speeds" heading to use an "Audio bit rate" setting of 6.3Kbps. (64Kbps is the default setting.) In addition, set the "Video bit rate" to 16Kbps and the "Screen sharing and whiteboard bit rate for broadcast meeting only" to 16Kbps.

Performing this optional step ensures that the G.723 audio codec is used in a meeting regardless of whether the end user selects the "People are attending using a modem" option when setting up a meeting in the Sametime Meeting Center. If you do not perform this optional step, users who deselect the "People are attending using a modem" option when setting up a meeting will invoke the "Meetings with LAN/WAN users" connection speed settings, which use the G.711 codec by default.

Audio/Video services, Sametime server

Unable to join audio/video meeting with NetMeeting

If a user attempts to join a meeting on the Sametime server by starting NetMeeting on the Windows desktop and entering the Sametime server name in the NetMeeting user interface, the user may not be able to participate in the audio/video part of the meeting.

When attending meetings with NetMeeting, it is best for the user to launch the NetMeeting client from the link on the Meeting Details page available from the Sametime Meeting Center on the Sametime server.

For more information, see the the topic "Joining meetings with NetMeeting" in the "Things you need to know" section of the *Sametime 3.1 Release Notes*.

LDAP issues

Sametime server

Administrator cannot attend meetings or use Sametime databases

If you have set up Sametime to connect to an LDAP directory, you must manually add the Sametime administrator to the LDAP directory to enable the administrator to:

- Start or attend meetings on the Sametime server.
- Use Sametime Discussion or TeamRoom databases on the Sametime server.

The Sametime administrator is specified during the Sametime server installation. The installation creates a Person document for the administrator in the Domino directory on the Sametime server. The administrator is authenticated against the Domino directory when accessing the Sametime Administration Tool.

When Sametime is configured to connect to an LDAP server, all users of the Meeting Services and Community Services are authenticated against entries in the LDAP directory. The Sametime administrator is not added to the LDAP directory by the Sametime installation. As a result, by default, the Sametime administrator can access the Sametime Administration Tool but cannot start or attend meetings on the Sametime server or use Discussion or TeamRoom databases.

To enable the administrator to create and attend meetings on the Sametime server or use Sametime TeamRoom/Discussion databases, you must manually create an entry for the administrator in the LDAP directory to which Sametime connects. For more information about Sametime and LDAP, see the "Using LDAP with the Sametime server" section of the *Sametime 3.1 Administrator's Guide*.

Note: To add a new administrator when Sametime is configured to connect to an LDAP server, you must add the administrator to the Domino directory and provide the administrator with the appropriate ACL settings in the Sametime databases. For more information, see "Adding a new Sametime administrator" in the "Using the Sametime Administration Tool" chapter of the *Sametime 3.1 Administrator's Guide*.

Sametime server

Can't add groups from Domino LDAP directory to presence lists

If you have configured Sametime to connect to an LDAP directory on a Domino server, and you are unable to add public groups to presence lists in Sametime Connect or other applications, you may need to remove entries from some of the LDAP settings in the Sametime Administration Tool.

If users cannot add groups from a Domino LDAP directory, verify that the following settings have no entry in the Sametime Administration Tool. If an entry exists, remove it so that the value for the setting is blank.

- Where to start searching for people (Located in the LDAP Directory - Basics settings of the Administration Tool)
- Where to start searching for groups (Located in the LDAP Directory - Basics settings of the Administration Tool)

You will need to restart the Sametime server after removing the entries from these settings.

Sametime server

Configuring LDAP directory settings after installation

The LDAP search and authentication functionality may not work by default after you install the Sametime server. You must modify the LDAP Directory settings in the Sametime Administration Tool so that these settings are appropriate for the schema of the LDAP Directory Sametime is accessing.

For more information about configuring the LDAP Directory settings, see the "Using LDAP with the Sametime server" section of the *Sametime 3.1 Administrator's Guide* (sthelapad.nsf or sthhelpad.pdf). You can access the .nsf version of the Administrator's Guide from the "Help" link of the Sametime Administration Tool.

Sametime server

Group members in Exchange server LDAP directory not online

If you set up Sametime to connect to an LDAP server, and you specify a Microsoft Exchange server as the server containing the LDAP directory to be used by the Sametime community, a problem may occur that prevents members of a group in the LDAP directory from appearing online in Sametime client presence lists.

For example, a Sametime Connect user may add a group defined in the LDAP directory on the Exchange server to the presence list in Sametime Connect. The group name in the presence may always indicate "No online people" even though some members of the group are actually online.

This problem occurs because the Exchange server is not publishing the group content attribute of the LDAP directory. (Exchange servers do not publish the group content attribute by default.)

To solve this problem, the administrator should use the Microsoft Exchange Administration Tool to configure the Exchange server to publish the group content attribute.

1. From the Microsoft Exchange Administration Tool select "Configuration."
2. Double-click "DS Site Configuration."
3. Click the "Attributes" tab.
4. In the Attributes list, check the "Members" attribute and click "OK" for the change to take effect.

Sametime Connect client

Sametime Connect 2.0 or higher required in LDAP environments

If you have configured the Sametime server to connect to an LDAP server for client search and authentication purposes, all users in the Sametime Community must upgrade to the Sametime 2.0 or higher Sametime Connect client.

If a Sametime 1.5 Connect client connects to a Sametime 2.0, 2.5, or 3.0 server that is configured to access an LDAP server:

- The Sametime 1.5 Connect client indicates that users are offline when they are actually online.
- Sametime 1.5 Connect client users cannot start chats or instant meetings with people who are connected to the same server, but using a higher version of Connect.

Security issues

Sametime server

Tokens are not deleted from Sametime tokens database

You can deploy a Sametime TeamRoom or Discussion database on a Domino server (that does not include a Sametime server). Users can access these Sametime TeamRoom or Discussion databases on Domino servers using Lotus Notes clients and use the Sametime instant messaging and presence features built into these databases.

When you deploy a Sametime TeamRoom or Discussion database to a Domino server, it is also necessary to create a replica of the Sametime Secrets (stauths.nsf) and Sametime Tokens (stautht.nsf) databases on the Domino server. These databases produce a security token that is used to authenticate connections from a Sametime TeamRoom or Discussion database to the Sametime server. During the token creation process, a Sametime token is created in and deleted from the Sametime Tokens databases. In some cases, a Token may not be deleted from the Tokens database. These tokens must be deleted; they can be used to gain illegal entry to the Sametime server. Note that this problem occurs in the Tokens database only when a database enabled with Sametime technology (such as TeamRoom and Discussion databases) is deployed on a Domino server.

To ensure that all tokens are deleted from the Tokens database, you should enable the "Cleanup Agent" in the Tokens database after you replicate the Tokens database to the Domino server. When the Cleanup Agent is enabled in the Tokens database, the agent runs every 10 minutes and deletes any tokens that have not been deleted by the normal Token deletion process.

To enable the Cleanup Agent in the Tokens database:

1. From a Lotus Notes R5 client connected to the Domino server, choose File-Database-Open.
 - In the Server drop-down list, select the Domino server.
 - In the "Filename text" box, type stautht.nsf.
 - Click Open.
2. From the Tokens database, select the View - Agents menu option.
3. Check the box to the left of the Cleanup Agent to enable the agent.
4. Enter the name of the server the agent will run on (the name of the server containing the Tokens database).
5. Close the Tokens database.

Sametime server

Web browser authentication with cascaded address books

This release note applies for Sametime servers set up to operate in a cascaded Directory environment. For Web browser users to be properly authenticated by the server, the following entry must exist in the server's notes.ini file:

```
NoMABForWebNames=1
```

Note It is best to set up Directory Assistance on the Sametime server when Sametime is operating in a Domino domain that includes multiple Directories. Generally, you should not use cascaded Directories on a Sametime server.

Software Development Kit issues

Sametime server

Location of Software Development Kit release notes

Sametime Software Development (SDK) release notes are provided with each kit. After installation, you can view them on your Sametime server. Visit <http://<sametime server name>/sametime/toolkits>, click the link for any kit to reach its welcome page, and then click Release Notes.

Sametime server

Problem using "Extended Live Names" Sametime C++ Toolkit sample

When a user logs in with the "Extended Live Names" sample program in the Sametime C++ toolkit, you cannot invite the user to join a chat from a Sametime meeting room.

Sametime server

Problem with Links Toolkit "Place-based Awareness" sample

If you use Netscape 7 with a Java 1.4.1 plugin on a Unix platform to run the Sametime Links Toolkit Place-based Awareness sample, the console is blocked when you log in.

Sametime server

Problems running Sametime Java Toolkit samples

Developers might experience problems running the Sametime Java Toolkit samples that use the Meeting Services API, such as: Meeting Applet - Chat and Audio; Meeting Applet - Chat, Audio, and Video; Broadcast; and Meeting Room.

Outlook issues

Sametime server, Web browsers

Changing password in Outlook

Users who are using a version of Sametime that is integrated with Microsoft Outlook should be aware of the following issue:

If a user changes a meeting password in Outlook after the meeting is active, the password change will not take effect.

Enterprise Meeting Server issues

Enterprise Meeting Server and server clusters

Anonymous moderator unable to edit meeting (Japan EMS)

If an anonymous (unauthenticated) user accesses the Meeting Center on the Japanese version of the EMS and creates a meeting that specifies an "Anonymous" moderator, the user will be unable to edit the meeting details. The example below illustrates this problem.

1. An anonymous user accesses the EMS Meeting Center and creates a meeting with an Anonymous moderator.
2. The user saves the meeting.
3. Later, the anonymous user accesses the Meeting Details page for the meeting and attempts to edit the meeting details.
4. When the user attempts to save the edited meeting, an error message appears indicating the operation is not allowed because of an invalid username or password.

Enterprise Meeting Server and server clusters

Any user can replay a password-protected recorded meeting

You can create a meeting that requires a password and elect to record the meeting. Users are required to enter a password when attending the live version of the meeting. The live version of the meeting is recorded and saved on the server. Users can then view the recorded version of the meeting by selecting the meeting from the "Recorded" view of the EMS Meeting Center.

Note that EMS users are not required to enter a password to view a recorded meeting even if the original live version of the meeting was password-protected. You cannot password protect a recorded meeting. If a meeting includes sensitive information, you should not record the meeting. There is no workaround for this problem.

Enterprise Meeting Server and server clusters

Cannot reattach an edited whiteboard file

A Meeting Moderator can attach a whiteboard file to a meeting for presentation on the whiteboard while the meeting is in session. If the Meeting Moderator attaches a whiteboard file to an active meeting, the Meeting Moderator cannot edit the file and then reattach the edited version. If the Meeting Moderator edits the file and reattaches it to the meeting, the original file (not the edited one) remains displayed on the whiteboard and attached to the Meeting Details page. The edited file is not available even though the administrator attached it after attaching the original file.

Enterprise Meeting Server and server clusters

Cannot search for meetings with DBCS file names with NS 4.51

Problem A meeting is created that has a meeting name that includes DBCS characters. Later, you access the EMS user interface using a Netscape 4.51 web browser, select the "Attend a Meeting" link, select the "In progress" link, and enter the DBCS meeting name in the "Search for Meeting" option. The search returns a list of all meetings in progress, not the individual meeting you specified.

This problem occurs when searching for meetings with DBCS characters in the meeting name using a Netscape 4.51 browser. There is no workaround for this problem.

Enterprise Meeting Server and server clusters

DBCS names for whiteboard files do not display correctly

Problem: You create a meeting and add a whiteboard file that has a DBCS file name to the meeting. After the meeting is created, you attempt to download the whiteboard file from the Meeting Details page of the end user interface. When downloading the file, the File Download dialog box displays a "You are downloading the file <filename>" message but the <file name> displayed in the dialog is not correct.

Solution: If you want the file name to display correctly when downloading the file, the file name must use the US ASCII character format. The file name will not display correctly if it has a DBCS file name.

Enterprise Meeting Server and server clusters

Eastern Europe accented characters cause WebSphere login failure

If a WebSphere server uses the Greek or Eastern European locale setting, users with accented characters in their names (for example Çedilla) may be unable to authenticate with WebSphere when attempting to access the EMS using a Web browser. The WebSphere console will display the message "Authentication failed for username" in the administrator's console. This problem occurs even when WebSphere is correctly configured to support UTF-8 encoding of the Unicode character set.

Note: Investigation of this problem is ongoing at the time these release notes are being published. It is uncertain whether this problem will be resolved in the released product.

Enterprise Meeting Server and server clusters

EMS users cannot browse the LDAP directory

Users cannot browse the LDAP directory from the EMS user interface to search for user or group names in an LDAP directory.

Note: The term "browse the LDAP directory" refers to the user's ability to launch a dialog box that displays a list of names in the directory and select a name from this list.

While users cannot browse the list of names in the directory, users can still search for individual names in the directory. Users can search for individual names in an LDAP directory by typing a user's name in a search field. If the search is successful, only the individual user name is returned.

Enterprise Meeting Server and server clusters

Group names cannot contain DBCS characters (for EMS)

If the LDAP directory accessed by the EMS contains a group name that uses DBCS characters, users who are members of that group will be unable to log in to the Sametime EMS Meeting Center. This problem occurs even if the group member's user name does not contain DBCS characters.

If you remove the group member's name from the DBCS group, the user can log in to the EMS Meeting Center successfully.

Enterprise Meeting Server and server clusters

Installing JMS providers for EMS on Spanish WebSphere

If you deploy the EMS on a Spanish language version of a WebSphere server, a problem occurs when you install the JMS providers on the WebSphere server.

In the "Install Drivers" (or Instalador controlador) window, the OK (or Aceptar) button does not function and you cannot proceed with the installation.

In order to proceed with the installation, you must change the regional settings of the WebSphere server to use a different language.

Enterprise Meeting Server and server clusters

Installing JMS Providers with Asian language servers

This problem applies to installing the JMS Providers with the Simplified Chinese, Traditional Chinese, or Korean language operating systems.

Problem: Deploying the EMS application requires you to perform a procedure in which you install Java Message Service (JMS) Providers to be used by the EMS. The instructions for installing the JMS Providers available in the Sametime 3.1 and Enterprise Meeting Server 1.0 Administrator's Guide are not correct when you install the JMS Providers on a Simplified Chinese, Traditional Chinese, or Korean language version of the Windows operating system.

Solution: If you are installing the JMS Providers a Simplified Chinese, Traditional Chinese, or Korean language version of the Windows operating system, use the instructions below to install the JMS Providers.

1. Start the WebSphere Administrator's Console.

To start the WebSphere Administrator's Console from a Windows machine, choose Start-Programs-WebSphere-Application Server V4.0-Administrator's Console.

2. Expand WebSphere Administrative Domain.
3. Expand Source-JMS provider.
4. Click the JMS Provider name that represents the machine on which you have installed the EMS files. The JMS Provider name must be highlighted.

Note In the example provided in the Sametime 3.0 and Enterprise Meeting Server 1.0 Administrator's Guide, the JMS Provider name is "IBM MQSeries."

5. Select the node tab.
6. Click Install New.
7. In the Install Driver window, select IBM MQSeries. Click Specify Driver.
8. In the "Specify the Driver Files" window, click Add Driver.
9. Browse to the <WebSphere MQ install>\java\lib directory.

Note In the example provided in the Sametime 3.0 and Enterprise Meeting Server 1.0 Administrator's Guide, the directory name is c:\mqseries\java\lib.

10. Select "com.ibm.mq.jar." Click Open. The <WebSphere MQ install>\java\lib\com.ibm.mq.jar file appears in the "Specify the Driver Files" window.

11. Click Add Driver.
12. Browse to the <WebSphere MQ install>\java\lib directory again.
13. Select "com.ibm.mqjms.jar." Click Open.

The c:\mqseries\java\lib\com.ibm.mqjms.jar file appears in the "Specify the Driver Files" window.

14. In the "Specify the Driver Files" window, click Set.
15. In the Install Driver window, click OK.
16. In the node tab, click Apply.

Enterprise Meeting Server and server clusters

Meeting materials are not deleted from EMS DB2 database

The following problem may occur when a user attaches meeting materials to the EMS.

1. A user begins the process of creating a meeting.
2. The user attaches some meeting materials (such as whiteboard files) to the meeting.
3. The meeting materials upload successfully to the EMS.
4. The user closes the browser or cancels the creation of the meeting before saving the meeting.

In this scenario, the meeting materials will not be deleted from the DB2 database used by the EMS.

Enterprise Meeting Server and server clusters

Meeting materials are not deleted

If you delete meetings from the EMS, but the meeting materials for the meetings are not deleted from the DB2 database, refer to the topic titled "Attaching a meeting material immediately after installing or restarting the EMS" in the Things you need to know" section of these release notes.

Enterprise Meeting Server and server clusters

Name with DBCS characters cannot log into the Meeting Center

If the person entry for a user in the LDAP directory contains a Common Name (CN) attribute that includes DBCS characters, that user might not be able to log into the Meeting Center on the EMS.

Enterprise Meeting Server and server clusters

Optimizing EMS page loading performance

After you deploy the Sametime Enterprise Meeting Server application on the WebSphere server, you can use the jspbatchcompiler program to compile the Java Server Pages (JSPs) used by the Meeting Center on the EMS.

Running the jspbatchcompiler program can optimize performance by greatly enhancing the speed with which the JSPs are loaded.

To use the jspbatchcompiler program to optimize the JSP loading performance, run the following command from the Command Prompt of the Windows server on which the EMS is deployed:

```
jspbatchcompiler -enterpriseApp SametimeEAR -webModule Sametime
```

Enterprise Meeting Server and server clusters

Recorded meetings are not sorted by status

If an end user clicks the Status column in the EMS Meeting Center, recorded meetings are not sorted by status. Other meetings (such as in progress meetings or unlisted meetings) are sorted by status.

Enterprise Meeting Server and server clusters

Restarting Sametime server after changing admin settings

Many pages of the EMS Sametime Administration Tool contain a line of text at the bottom of the page that says "You must restart the server for the settings to take effect" that indicates you must restart the Sametime server (or servers) if you change an administration setting on the page.

This information is not always correct. In some cases, it is not necessary to restart the Sametime server after changing administration settings even though the instructions at the bottom of the administration page indicates that you must restart the server.

It is only necessary to restart the Sametime server if you make changes for the Sametime server from the following pages of the EMS Sametime Administration Tool:

- LDAP Directory - Connectivity
- LDAP Directory - Basics
- LDAP Directory - Authentication
- LDAP Directory - Searching
- LDAP Directory - Group Contents
- Configuration - Connectivity - Networks and Ports

If you change any other settings in the EMS Sametime Administration Tool, it is not necessary to start the Sametime servers for the changes to take effect. The changes will take effect immediately with the exception noted below.

Note: If you change administration settings on the Configuration-Community Services page, the changes may take up to 60 minutes to take effect. All other changes should take effect immediately without a server restart.

Enterprise Meeting Server and server clusters

Sametime/Domino HTTP port is set to Redirect to SSL

If a Sametime/Domino server is added to the EMS, and the Sametime/Domino server has a TCP/IP port status setting of "Redirect to SSL" in the Ports tab of the Domino server Server document, meetings will not go active on this Sametime/Domino server.

This problem occurs because the DB2 database used by the EMS contains an stconfig.roomserver table which uses "HTTP" as a URL parameter instead of "HTTPS."

To work around this problem, you can use the following instructions to alter the values in the stconfig.roomserver table to ensure that HTTPS is used in the URLs.

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 db=> 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.

- At db=> command prompt, enter the following SQL commands to update the stconfig.roomserver table

```
update stconfig.roomserver
  set httpbaseurl='https://ibm.acme.com',
  https_en='1',
  httpclear_en='0',
  recmtgmtcontrolurl='https://ibm.acme.com/servlet/auth/rapfile',
  mtgmtcontrolurl='https://ibm.acme.com/servlet/auth/mmapi',
  materialsrefreshurl='https://ibm.acme.com/servlet/refresh',
  materialscontrolurl='https://ibm.acme.com/servlet/auth/fileupload',
  commsvcsadmincgiurl='https://ibm.acme.com/cgi-bin/STAdminAct.exe'
where servername='CN=Servername/O=ibm'

update stconfig.organization
set mtgcntrconnectionurl='https://ibm.acme.com/sametime' where organizationname=""
```

Note: In this example, you must replace the hostname (ibm.acme.com) and the server name (CN=Servername/O=IBM) with the hostname and server name of your server.

- At db=> command prompt, type the following command to terminate the connection to the DB2 database:

```
Connection reset
```

- Close the DB2 command prompt window.
- Restart the "stadmin" server from the WebSphere Console on the EMS machine.

Enterprise Meeting Server and server clusters

Start the stadmin application server before Sametime server

The stadmin application server on the WebSphere machine must be started before a Sametime server can be added to the EMS.

Also, if you stop a Sametime server that is added to the EMS, the stadmin application server must also be started before the Sametime server can be restarted.

The Sametime server will not start successfully unless the stadmin application server is started first.

Enterprise Meeting Server and server clusters

Unable to install the EMS files from a network drive

When deploying the EMS on a WebSphere server, you must install the EMS files onto the WebSphere machine and perform several other procedures before you can deploy the Sametime EAR file on WebSphere.

You cannot install the EMS files on the WebSphere machine from a network drive unless you map the installation directory to the network drive. If you do not map the installation directory to a network drive, the installation will fail when you click OK to select the installation language.

For example, the command Start-Run <machine-name>\sametime\ems\setup.exe will cause the installation to fail.

To successfully install from a network location, map the install directory to a network drive and use the command Start-Run <network drive>:\sametime\ems\setup.exe

Note: The actual path to the setup.exe file for the EMS installation may vary from the example above.

Enterprise Meeting Server and server clusters

Update security configuration failed message for LDAP

Problem The administrator receives an "Update Security Configuration Failed" message when enabling LDAP Directory Access for WebSphere during the EMS setup procedures.

This error can occur if there is a mismatch between the name entered for the WebSphere administrator and the "User ID Map" setting in the WebSphere Security Console.

When you specify a WebSphere administrator, you must enter the administrator name in the "Security Server ID" field on the Authentication tab of the WebSphere Security Console.

The administrator name that you enter in the Security Server ID field must be a user that has a person entry in the LDAP directory.

The name entered in the "Security Server ID" field will be authenticated using LDAP directory schema settings in the "User ID Map" setting of the WebSphere Security Console Advanced LDAP properties settings.

For example, assume all of the following are true:

- You enter the name "Kathy Miller" in the "Security Server ID" field of the WebSphere Security Center Authentication tab.
- Kathy Miller has an entry in the LDAP directory that includes a common name (cn) attribute of "Kathy Miller" and a shortname attribute of "kmiller."
- The "User ID Map" setting in the WebSphere Security Console Advanced LDAP Properties settings is configured with the following value: "dominoPerson:shortname."

With this combination of settings, WebSphere will not be able to authenticate the name "Kathy Miller" because the User ID Map setting specifies that the "shortname" attribute of the directory entry be used to access user names in the directory.

If you change the name entered in the Security Server ID field of the WebSphere Security Center Authentication tab to "kmiller," the authentication should succeed. Similarly, you could leave the name Kathy Miller entered in the "Security Server ID" field and change the "User ID Map" setting to use the common name (or cn) of directory entries when authenticating a user name. Either of these changes should enable WebSphere to successfully authenticate the user name.

Note: The "Update Security Configuration Failed" message may also appear if other settings in the WebSphere Security Console Advanced LDAP Properties settings are not appropriate for the schema of the LDAP directory accessed by WebSphere.

For more information, see "Configuring WebSphere server security and LDAP directory access" in the "Setting up the Enterprise Meeting Server and a Meeting Services Cluster" chapter of the Sametime 3.1 and Enterprise Meeting Server 1.0 Administrators Guide (sthelapd.pdf or sthelapd.nsf) available with the Sametime 3.1 server.

Enterprise Meeting Server and server clusters

User with a person entry in Domino Directory cannot authenticate

An EMS environment requires users to be defined in a single LDAP directory. The WebSphere server on which the EMS is installed accesses this LDAP directory to authenticate the EMS users.

A user who has a person entry in the LDAP directory accessed by the WebSphere/EMS machine cannot also have a person entry in the Domino Directory of a Sametime server that has been added to the EMS. If a user that accesses the EMS has a person entry in both the LDAP directory used by WebSphere and the Domino Directory on a Sametime server, the authentication for this user will fail.

To prevent this problem, you must ensure that the Domino Directory of a Sametime server that has been added to the EMS does not contain any person entries for users who will access the EMS. If necessary, manually remove the names of EMS users from the Domino Directory of Sametime servers that are added to the EMS. You should also ensure that replication of the Domino Directory does not cause the removed names to reappear in the directory.

UNIX client issues

UNIX clients

Anonymous meeting attendees cannot login and reattend a meeting

The following issue applies to the AIX version of the Sametime Meeting Room client.

1. A user attends a meeting as an anonymous user (the user does not log in or authenticate with the Sametime server before attending the meeting).
2. The user's name displays as "Anonymous" in the Contact List of the Meeting Room client.
3. While the meeting is in session, the user returns to the browser window containing the Sametime Meeting Details page and logs into Sametime.
4. The user then returns to the browser window in which the Sametime Meeting Room client is running and refreshes the browser window.
5. The user's name continues to display as "Anonymous" in the Contact List of the Meeting Room client. The user's log in name will not appear in the Contact List.

In this scenario, the Windows version of the Meeting Room client will restart automatically and the user's log in name will display in the Contact List. However, the AIX version of the Meeting Room client does not restart after automatically after the user logs in.

UNIX clients

Application sharing on Unix systems - known issues

This list describes known issues with application sharing on Unix systems.

1. In order to load Application Sharing native code on Linux and Solaris platforms, the following library is required on the client machine: libz.so.1 which resides in /usr/lib
2. On Unix systems, minimized applications do not appear in the list of shared applications. This is an X Windows limitation.
3. When you are using application sharing on Unix systems, some system tasks may appear in the list of shared applications that are not user applications but XWindows references to system processes.
4. The performance of sharing an application from the Unix versions of the MRC is slower than the Windows version of the MRC. This is due to the XServer overhead.
5. When sharing an application on Linux, for example a text editor, selecting Caps Lock from the Linux system causes the input from all systems to be capitalized. This behavior is the result of the Linux implementation of the XWindows server.
6. Sharing of 3D Graphics windows is only supported if the 3D application is using GLX to display the 3D image.

UNIX clients

Changing a user's online status on Linux and Solaris systems

On Linux systems, there is no way to change a user's online status.

On Solaris systems, you must use the menu option Tools->Status Message to change a user's online status. The Status message button does not work under Solaris. This is a known Java problem.

On Linux systems, this problem can be fixed by using the version of the 1.4 Java plugin supplied by IBM on our Web site.

UNIX clients

DBCS limitations/known issues with Sametime Unix/Linux clients Limitations/known problems with AIX clients

This section lists the limitations and known problems with AIX clients.

Java Toolkit

The search button is not enabled when you type DBCS characters in Java Toolkits.

DBCS users login issue

The DBCS users cannot log in to the Sametime Meeting Center.

Blank chat messages in Java Connect

On the chat window, the vertical scroll bar may disappear after sending a message containing multiple lines. The message also displays in black in the transcript area after it is sent. This problem occurs because of a bug in the implementation of ScrollPane in the IBM 1.4.0 JVM.

The workaround for this problem is to download the new version of the IBM JVM when it is available.

Weak support of the JVMs of UNIX in AWT components (JDK1.1)

Due to poor third party support related to AWT with DBCS text. Some data entry problems exist with AIX.

<Korean only>

1. The Korean characters display blank in the transcript area of Java Connect.

This problem occurs because converted text cannot be committed into the Java text field. The text cannot be committed because the character

to end (commit) the IME session is captured by the Java app. The root cause of this problem is a faulty implementation of key event handling by the IME and/or host system. The key event should be captured first by the IME and not by the Java app.

2. You cannot type Korean characters in the login window of Java Connect.

<Traditional Chinese and Simplified Chinese only>

1. The cursor always remains at the beginning of chat window of Java Connect.

The typed string "ABC" will display as "CBA" in the transcript area after the chat is sent. This problem is related to the display problem when entering text into the IME session.

2. You can type only one DBCS character in the whiteboard tool of the Meeting Room client.

This problem occurs because the focus is shifted away from the whiteboard to another dialog box and does not return after the first character is typed. The workaround for this problem is to drag the cursor off the whiteboard and then drag the cursor back on the whiteboard (using the mouse). After you have dragged the cursor off and back on to the whiteboard one time, you can type additional characters on the whiteboard.

DBCS display as garbage under AIX EUC locale

<Japanese only>

If the user's AIX locale is EUC, DBCS characters will not display correctly in a text file (.txt) attached to the Meeting Room client.

Limitations/known problems with Solaris clients

This section lists the limitations and known problems with Solaris clients.

Issues related to SUN JVM

There is a fundamental problem in the Sun Java 1.4 VM (See bug report 4814163 at Sun) where menu items do not work. Due to this issue, the following problems occur in Sametime clients.

1. In the Meeting Room client, participants cannot raise hand by selecting menu items.
2. In the Meeting Room client, participants cannot view the remaining meeting time by selecting items.
3. In the Meeting Room client, participants cannot change the status by selecting the menu items.
4. In the Meeting Room client, users right-clicking in a contact list does not work.
5. When playing back a recorded meeting, you cannot pause or stop the meeting by clicking the tools item.

The Screen sharing tool cannot display application titles containing DBCS characters. This is caused by a problem where strings passed to the JVM cannot be displayed properly.

Meeting Room client window refresh issue

When you open the Meeting Room client, you may only see the Screen sharing/Whiteboard panel. Resize the Meeting Room client window or click the maximum button in the Meeting Room client window to display the entire Meeting Room client.

The titles of Windows display with incorrect characters

The DBCS title of the Sharing with Frame window displays with incorrect characters (such as all question marks or unreadable characters).

Directory Applet issues

Some strings in the Directory applet display with incorrect characters (such as all question marks or unreadable characters). This problem occurs because the directory applet opens with an incorrect size. There are problems with resizing the Directory applet window.

Input in the "Alert me..." field

<Japanese only>

The DBCS characters entered in the "Alert me..." field are displayed in black in the "Alert me..." field. Since the background of the field is also black, you cannot recognize the DBCS words. You must change the video display color depth setting from 8+24 to 24 bit TrueColor visual to fix this problem.

IME issues

<Korean only>

You cannot use the "Alt" key to switch to Korean input mode, so you cannot type Korean characters in Java Connect, Meeting Center, Meeting room client and so on. This is a problem with Korean IME in Sun Solaris.

Limitations/known problems with Linux clients

This section lists the limitations and known problems with Linux clients.

Netscape crashes with Sun JRE 1.4.1 plugin

A Netscape 7.02 browser that operates with the Sun JRE 1.4.1 Plug-in may crash when you click menu items in the Meeting Room client or Java Sametime Connect. The workaround for this problem is to use the Sun JRE 1.4.0_03 Plug-in with the Netscape 7.02 browser.

MRC window refresh issue

When you open the Meeting Room client, you may only see the Screen sharing/Whiteboard panel. Resize the Meeting Room client window or click the maximum button in the Meeting Room client window to display the entire Meeting Room client.

Problems related to Sun JRE

There is a problem in the Sun JVM 1.4.0_03 with converting Unicode to DBCS native code for display in the window titles. This problem causes the DBCS meeting name to display incorrect characters (such as all question marks or unreadable characters) in the Window titles. The Sun JRE 1.4.1 Plug-in does not have this issue.

Some DBCS characters in the invitation dialog sent from the Meeting Room client display as incorrect characters (such as all question marks or unreadable characters) in a Netscape browser that operates with the Sun JRE 1.4.0 plugin. The Sun JRE 1.4.1 plugin does not have this issue.

The Screen sharing tool cannot display application titles that contain DBCS characters well in the Netscape browser with the Sun JRE 1.4.0 Plug-in. The Sun JRE 1.4.1 Plug-in does not have this issue.

The search function in the Directory applets does not work due to issues with the Sun JRE.

Users that log in to the Sametime Meeting Center using DBCS characters cannot launch the Meeting Room client from a Web browser that uses the Sun JRE 1.4.0 Plug-in. The Sun JRE 1.4.1 Plug-in does not have this issue.

The DBCS users cannot start a test meeting from Java Sametime Connect or the Sametime Meeting Center from a web browser that uses the Sun JRE 1.4.0 Plug-in. The Sun JRE 1.4.1 Plug-in does not have this issue.

<Japanese only>

You cannot enter a Japanese message with FEP on chat/instant-meeting client on the Linux OS. When sending a chat message to a user who is away, incorrect characters (such as all question marks or unreadable characters) will display in the away message window.

<Korean only>

You cannot type Korean characters in the fields below.

- The search field of Directory applets
- The login field of Java Sametime Connect and the Sametime Meeting Center
- Chat panel in Java Sametime Connect and the Meeting Room Client
- The reminding message field of "Alert me..." function in Java Sametime Connect

This problem occurs because the AWT component is not well defined in the Korean font.property file

The Korean characters in the data entry fields of Java Sametime Connect display incorrectly (for example, the characters display as all question marks or unreadable characters). This problem occurs because of insufficient definition in the font.property file.

The Korean characters in the chat text field and attachment list fields display incorrectly. This problem occurs because of insufficient definition in the font.property file.

The Korean strings display incorrectly in the polling tab of the Broadcast client.

<Simplified Chinese only>

Some DBCS strings in the menu items of Java Connect or the Meeting Room client are truncated resulting in truncated words within the menus.

The Korean index in help is not working

<Korean only>

Clicking the Korean character in the index of End User Help will not jump you to the appropriate location in the index.

UNIX clients

Dialogs do not always stay on top in the window stacking order

Some dialogs do not stay on top of the window stacking order, when the browser window is selected after the dialog is displayed. The dialogs are still up, but they are hidden behind the browser window. This is an X Windows limitation.

UNIX clients

Font properties file needed for some languages

If you are having problems with the display of characters in a specific language, please contact technical support for an updated font.properties files for that language.

On the Linux platform, this problem is fixed if you use the version of the 1.4 Java plugin supplied by IBM on our Web site.

UNIX clients

Frame-sharing limits on Unix systems

This note describes issues with the frame-sharing feature on Unix systems:

1. The "Share a frame" feature may not work correctly on Unix systems where the Xserver is using an 8bit PseudoColor visual. This occurs because the color table fills up.
2. The "Share a Frame" feature works differently on the Linux platform than it does on the Windows and other Unix platforms. On Linux systems, you have to go to the Share a Frame window title bar and select the Frame type to be normal. The default Frame type for that window is Title-only. This option will work ONLY with the Gnome window manager.

UNIX clients

Limited resources can cause the browser to terminate

On Unix systems with limited resources (for example, insufficient swap space), the browser may unexpectedly terminate.

UNIX clients

Log on to Sametime dialog problem with Sametime Connect on Linux

When Sametime Connect for browsers runs on the Linux operating system, the "Log on to Sametime" dialog box (and other dialog boxes in the Sametime Connect client) may contain incorrect or unreadable characters. This problem has been seen in the Russian and Polish language versions of Sametime Connect for browsers on Linux and appears to be a font handling problem in the Linux operating system.

UNIX clients

Menu items with checkboxes on Linux and Solaris systems

Menu items that have a corresponding checkbox associated with them do not work under Linux and Solaris. This is a known Java problem dealing with pop up menus.

On Linux systems, this problem can be fixed by using the version of the 1.4 Java plugin supplied by IBM on our Web site.

UNIX clients

Problem selecting menu items on Linux client with Netscape

On Linux systems, selecting an item from a menu may crash Netscape. This is a known Java problem.

This problem can be fixed by using the version of the 1.4 Java plugin supplied by IBM on our Web site.

UNIX clients

Using the Undo Full Screen button with Linux Meeting Room client

When a user is attending an online meeting with the Linux Meeting Room client, the user can select a View-Make Shared Area Full Screen option to expand the Meeting Room client browser window to the full screen mode.

After expanding the Meeting Room client browser window, the "Undo Full Screen" button does not appear in the expanded window and may give the user the impression that it is impossible to return the window to its previous, smaller state.

Note that the "Undo Full Screen" button is available from a browser window that appears behind the expanded, full-screen version of the Meeting Room client window. The user can return the browser window to its previous state, but must navigate to the window that is behind the expanded Meeting Room client window to do so.

Chapter 4 - Documentation updates

The *Documentation updates* chapter describes errata and updates to the Sametime documentation.

Help

Sametime Administration Tool, Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client, Sametime server

Online and print documentation Sametime Documentation

Sametime includes help systems for end users and administrators.

Help for end users

From the Sametime Welcome page, click Quick Start Guide to access information that will help end users get started with the Sametime Connect client and the Sametime Meeting Center.

From the Sametime Welcome page, click Documentation to access the *Sametime User's Guide*. This help system provides comprehensive help for the end user features of Sametime. This help system is also accessible from the Help menus of the Sametime Connect client and the Sametime Meeting Room client.

If you download the Sametime Print Capture utility, you can access help for Print Capture from the Print dialog box of the program you are using. See the topic "Converting Files with Sametime Print Capture" in the *Sametime User's Guide* for more information.

The end user help systems are also available on the Sametime CD as PDF files (as listed below).

Help for administrators

Help for system administrators includes the *Sametime 3.1 Installation Guide* and the *Sametime 3.1 Administrator's Guide*. These help systems are available on the Sametime CD as Lotus Notes databases and PDF files. You can access the *Sametime 3.1 Administrator's Guide* online from the Help link in the Sametime Administration Tool.

The filenames of the Sametime 3.1 help systems are listed below.

Title	Database file name	Description
Sametime User's Guide	SametimeUsersGuide.pdf	End User's Guide in PDF format
Sametime Quick Start Guide	QuickStartGuide.pdf	Quick Start Guide in PDF format
Sametime Print Capture Help	PrintCaptureHelp.pdf	Whiteboard Print Capture help in PDF format.
Sametime 3.0 Installation Guide	Stinstall.nsf	Installation Guide in Notes database format
	Stinstall.pdf	Installation Guide in PDF format
Sametime 3.0 Administrator's Guide	Sthelpad.nsf	Administrator's Guide in Notes database format
	Sthelpad.pdf	Administrator's Guide in PDF format

You can also visit the Lotus Developer Domain Web site at <http://www.ibm.com/lotus/ldd> to download this documentation.

Domino Documentation

Sametime uses a Domino infrastructure based on the Domino 6.02 server release. Administrators interested in more information about the functioning of the Domino infrastructure can access online versions of Domino documentation at the Lotus Developer Domain Web site: <http://www.ibm.com/lotus/ldd>.

Sametime Broadcast client

A broadcast meeting that uses NetMeeting as a tool

When an end user schedules a Broadcast meeting and selects NetMeeting on the Tools tab of the New Meeting page:

- The presenters for the meeting use NetMeeting for the online portion of the meeting, including screen sharing and the whiteboard.
- The rest of the meeting participants receive the Sametime Broadcast client for the meeting.

Note The *Sametime User's Guide* (available from the "Documentation" link on the Sametime server home page) does not include documentation about broadcast meetings that include NetMeeting.

Audio/Video services

Audio and video not included in every meeting by default

The topic "Tools: How to Get Your Work Done" in the *Sametime 3.0 User's Guide* includes the following statement:

By default, every scheduled meeting includes the whiteboard, screen sharing, Meeting Room chat, polling, send Web pages, and computer audio and video.

This statement is incorrect; audio and video are not included in every meeting by default. To include audio and video in a meeting, an end user must select the radio buttons for audio and video on the Tools tab.

Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client

Default file locations not listed for all operating systems

The *Lotus Sametime User's Guide* and *Lotus Sametime Quick Start Guide* specify default locations for files such as saved chat transcripts. These default locations are correct for Windows 98, but the default locations might be different for other operating systems. The tables below list the correct default file locations for each operating system.

Note: Sametime Connect for browsers cannot save instant chat meeting transcripts.

Note: When Sametime Connect for browsers users choose People - Add to/Replace List, the Open dialog box displays the contents of the C:\WINDOWS\JAVA directory. However, the default directory for saving a contact list is C:\. Users must browse up to the C:\ directory to locate the file for a saved contact list.

Windows 95 OSR2

File	Default Location
Meeting Room Chat transcripts	C:\Windows\Java\Sametime
Instant chat meeting transcripts (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client\Chat Transcripts
Instant chat meeting transcripts (Sametime Connect for browsers)	n/a
Contact list (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client
Contact list (Sametime Connect for browsers)	C:\
Status details (same as Meeting Room Chat directory)	C:\Windows\Java\Sametime
Accepted file transfers	C:\Program Files\Lotus\Sametime Client\Transferred Files

Windows 98/98 SE

File	Default Location
Meeting Room Chat transcripts	C:\WINDOWS\JAVA\Sametime
Instant chat meeting transcripts (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client\Chat Transcripts
Instant chat meeting transcripts (Sametime Connect for browsers)	n/a
Contact list (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client
Contact list (Sametime Connect for browsers)	C:\
Status details (same as Meeting Room Chat directory)	C:\WINDOWS\JAVA\Sametime
Accepted file transfers	C:\Program Files\Lotus\Sametime Client\Transferred Files

Windows NT WorkStation 4 SP 6a

File	Default Location
Meeting Room Chat transcripts	C:\WINNT\Java\Sametime
Instant chat meeting transcripts (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client\Chat Transcripts
Instant chat meeting transcripts (Sametime Connect for browsers)	n/a
Contact list (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client
Contact list (Sametime Connect for browsers)	C:\
Status details (same as Meeting Room Chat directory)	C:\WINNT\Java\Sametime
Accepted file transfers	C:\Program Files\Lotus\Sametime Client\Transferred Files

Windows 2000 Professional SP2

File	Default Location
Meeting Room Chat transcripts	C:\WINNT\java\Sametime
Instant chat meeting transcripts (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client\Chat Transcripts
Instant chat meeting transcripts (Sametime Connect for browsers)	n/a
Contact list (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client
Contact list (Sametime Connect for browsers)	C:\
Status details (same as Meeting Room Chat directory)	C:\WINNT\java\Sametime
Accepted file transfers	C:\Program Files\Lotus\Sametime Client\Transferred Files

Windows XP

File	Default Location
Meeting Room Chat transcripts	C:\WINDOWS\java\Sametime
Instant chat meeting transcripts (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client\Chat Transcripts
Instant chat meeting transcripts (Sametime Connect for browsers)	n/a
Contact list (Sametime Connect for the desktop)	C:\Program Files\Lotus\Sametime Client
Contact list (Sametime Connect for browsers)	C:\
Status details (same as Meeting Room Chat directory)	C:\WINDOWS\java\Sametime
Accepted file transfers	C:\Program Files\Lotus\Sametime Client\Transferred Files

Sametime Meeting Room client

Do not use "Print to file" with Sametime Print Capture

The following topics mention the "Print to File" option when using Sametime Print Capture on Windows XP:

- "Changing the Sametime Print Capture Settings" in the Sametime Print Capture Help.
- "Converting Files with Sametime Print Capture" in the Sametime 3.0 User's Guide.

The information in both of these topics is incorrect; you should not use the "Print to file" option when saving a file with Sametime Print Capture on Windows XP. If you use the "Print to file" option, your file will not display correctly on the whiteboard. When saving a file with Sametime Print Capture, ensure that the "Print to file" option is NOT selected.

Sametime Connect client

External users not accessible via Sametime 3.0

Sametime 3.0 users cannot use Sametime to communicate with External users (people connected to their companies' extranets). The *Sametime User's Guide* mentions External users in the following topics:

- What's New in Sametime 3.0?
- Adding an Individual Name to the Contact List
- Chatting with People

For more information, see "SIP Gateway functionality available at a future date" in the "Things You Need to Know" section of these Release Notes.

Sametime Meeting Room client

Incorrect mnemonics listed for the Tools menu

The *Lotus Sametime User's Guide* topic "Mnemonics in the Sametime Meeting Room" specifies incorrect mnemonics (shortcut keys) for two options in the Tools menu. The correct mnemonics are listed in the table below.

Menu Option	Mnemonic
Tools - Show Responses to Everyone	r
Tools - View Individual Responses	i

Web browsers

Incorrect statement about private Discussion documents

The topic "Using a Discussion" in the *Sametime User's Guide* includes the following statement:

Other users can see the subject line, but they cannot view the document.

This statement is incorrect. When a document in a Discussion database is marked private, the subject line and the content are unavailable to everyone except the creator of the document.

Sametime Broadcast client

Meeting time during a broadcast meeting

In the *Sametime User's Guide*, the topic "Participating in a Broadcast Meeting" includes the following sentences:

You can determine whether the status bar displays the elapsed meeting time or the remaining meeting time. Choose View - Elapsed Meeting Time or View - Remaining Meeting Time.

This information is incorrect. The Elapsed Meeting Time and Remaining Meeting Time menu items are not available for an audience member in a broadcast meeting.

Sametime Meeting Room client

Mnemonics not listed for private chats in the Meeting Room

Mnemonics for chats started from the Participant List of a Sametime Meeting are not listed in the documentation. Mnemonics for chats started from the Participant List are different than the mnemonics for chats started from the contact list in Sametime Connect for the desktop. As with other mnemonics in the Meeting Room, mnemonics are not underlined. In chats started from the Participant List, the first letter of the menu option is the mnemonic.

When multiple menu options or buttons begin with the same letter, keep pressing the mnemonic or shortcut combination until you reach the desired option and then press ENTER.

The mnemonics and keyboard shortcuts for the affected menus, dialog boxes, and buttons are listed below. Mnemonics are underlined.

Chats

Main Menu Option or Button	Pull-Right Menu Options
Meeting ALT+M	<ul style="list-style-type: none"> ● Add Tools ● Invite Others ALT+I ● Close
Edit ALT+E	<ul style="list-style-type: none"> ● Cut CTRL+X ● Copy CTRL+C ● Paste CTRL+V ● Clear All DELETE
Send ENTER or ALT+S	
Invite Others ALT+I	
Close ESC or ALT+C	

Invite others to a meeting dialog box

Add Invitees ALT+A
 Cancel ESCAPE or ALT+C

Add to Invitation List dialog box

Directory ALT+D
 Close ESCAPE or ALT+C

Add to Invitation List dialog

Search ALT+S
 Add Contents ALT+A
 Contents ALT+C
 Close ESCAPE or ALT+C

Add Tools to a Meeting dialog

Send ALT+S
 Close ESCAPE or ALT+C

Available Tools dialog

Close ESCAPE or ALT+C

Sametime Meeting Room client

Plug-in for NetMeeting Meetings using Netscape is not available

The content of the "Using Netscape Communicator to Attend" help topic is invalid because the "Sametime Plug-in for NetMeeting Meetings Using a Netscape Browser" is not available in Sametime 3.1.

Sametime server

Sametime 3.0 User's Guide index entry should be Sametime 3.1

When you open the Sametime homepage and click "Document" link then select the "Index" button, the title shows Sametime 3.0 User's Guide and it should be Sametime 3.1 User's Guide.

Sametime Meeting Room client

The Help of My Meetings' description should be modified

The description of "My Meetings" is incorrect in the Meeting Center online help.

1. Launch Sametime center (stcenter.nsf) and click "Attend a Meeting " link to go to Online Meeting Center.
2. Click "Help" link and help page "View and Attending a Scheduled Meeting (without Search)" is displayed.
3. Find the description about "My Meetings".

The description says "meetings that you created" and it should say "meetings that you have created and meetings created by other people that you are invited to, you were made the moderator, or you were added as a presenter."

Sametime Meeting Room client

Tools still available in active meetings

The topic "Customization by the Administrator" in the *Sametime 3.0 User's Guide* includes the following note:

Note Tools can be removed after a meeting that uses the tools is scheduled. For example, you might select screen sharing when you create a meeting. If your administrator disables screen sharing before the meeting starts, screen sharing is unavailable during the meeting.

This note is incorrect; if the administrator disables a tool after a meeting has been scheduled, that tool will still be available for the meeting. However, no new meetings can be scheduled using the tool

Sametime Connect client, Sametime Meeting Room client

Use Ctrl + Enter keys to begin a new line in a chat message

The online help for the Sametime Connect client, and the *Sametime User's Guide*, state that you can start a new line in a chat message by pressing the Shift + Enter keys.

This information is not correct. To start a new line in a chat message, press the Ctrl + Enter keys.

Sametime Broadcast client, Sametime Meeting Room client

User cannot see list of sent Web pages

The following tip is in the topic Viewing Web Pages in the *Sametime 3.0 User's Guide*:

Tip To view the most recently sent Web page, click the Web Pages tab and click Go. (If the Web Pages tab is not visible, choose View - Interaction Tabs - Web Page Tab.) The Web page appears in a browser window on your screen. No one else can see this window.

The following sentence should be added to this tip:

You can only view the most recently sent Web page. If the Moderator has sent more than one Web page, you will not be able to view the list of Web pages in the "Web page" drop-down box.

Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client

Warning message does not mention Lotus

The *Sametime User's Guide* and the *Sametime Quick Start Guide* mention a Security warning message that states:

"Always trust content from Lotus Development Corporation."

This warning message does not mention Lotus Development Corporation. However, the documentation is correct in stating that a user must accept the warning.

Administrator's Guide

Audio/Video services

Cannot attend audio/video meeting if video limit is reached

Several topics in the "Configuring the Audio/Video Services" section of the *Sametime 3.0 Administrator's Guide* include the following statement:

You can set a maximum number of video connections that is smaller than the maximum number of audio connections. When the video limit is reached, users can communicate with audio, but video is unavailable.

This statement needs to be clarified as follows:

If a user attempts to enter an instant meeting that includes audio and video, and either the audio or video limit is reached, the user will not be able to use either audio or video. However, if the administrator has set the video limit to be higher than the audio limit, the user can attempt to attend the meeting using audio only (without video), and the call will succeed.

This statement is included in the following topics:

- "Setting a maximum number of interactive audio connections for all instant meetings"
- "Setting a maximum number of interactive video connections for all instant meetings"
- "Setting a maximum number of interactive audio connections for all scheduled meetings"
- "Setting a maximum number of interactive video connections for all scheduled meetings"

Sametime server

Discard the ReleaseNotes.txt file

The Sametime 3.0 server contains a file named ReleaseNotes.txt in a ReleaseNotes subdirectory that describes several problems with the Sametime server. The problems described in the ReleaseNotes.txt file are not valid for the Sametime 3.0 server. This readme was issued with an earlier beta release of Sametime, but was inadvertently included in the final build of the product. You can discard the ReleaseNotes.txt file and ignore the issues it describes.

Sametime server

Enabling self registration correction

If you have followed the instructions in the *Sametime Administrator's Guide* to enable self registration, but self registration is not working, verify that all of the following conditions exist:

- The signer "Sametime Development/Lotus Notes Companion Products" is added to the ACL of the Domino Directory on the Domino 6.0.2 server.
- The "Sametime Development/Lotus Notes Companion Products" signer is assigned the "Author" access level in the Domino Directory ACL.
- The "Sametime Development/Lotus Notes Companion Products" signer has the following Roles assigned in the Domino Directory ACL: Group Creator, Group Modifier, User Creator, User Modifier.
- The "Create Documents" privilege is selected in the Domino Directory ACL.

The *Sametime Administrator's Guide* does not state that the "Create Documents" privilege must be selected in the Domino Directory ACL to enable self registration.

Sametime server

LDAP setup does not overwrite an existing da.nsf database

If a user selects the LDAP directory type during a Sametime installation, and directory assistance is already configured on the Domino server on which Sametime is installed, the Sametime installation will add a Directory Assistance document to the existing directory assistance database on the Domino server. This Directory Assistance document enables the Sametime server to connect to the LDAP directory server specified during the Sametime installation.

The *Sametime 3.1 Administrator's Guide* contains a topic entitled "Selecting the appropriate LDAP options during the server installation" in the chapter "Using LDAP with the Sametime server." This topic contains text that indicates the following:

"If a Directory Assistance database named da.nsf exists on the Domino server at the time the Sametime server is installed, the existing da.nsf database is overwritten with a da.nsf database created by the Sametime installation. Also, if there is an existing entry in the "Directory Assistance database name" field in the Server document, it is overwritten with 'da.nsf.'"

Note that the text above is **not** correct. If an entry exists in the "Directory Assistance database name" field in the Server document, 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.

Enterprise Meeting Server and server clusters

Meeting passwords required for stmanager and stattend roles

During the process of securing user access to the Enterprise Meeting Server, the administrator can assign users to the "stmanager" role using the User Role Mappings feature of the WebSphere Administrator's Console.

The *Sametime 3.1 and Enterprise Meeting Server 1.0 Administrator's Guide* states that users or groups that have been assigned the stmanager role can enter password-protected meetings without entering a meeting password.

This information is incorrect. Users or groups that are assigned the stmanager role can access the Meeting Details page for a meeting without entering a meeting password. However, if the meeting is password-protected, users with the stmanager role must enter the meeting password to attend the meeting.

Sametime server

Network card requirements for Community Server connections

The *Sametime 3.1 Administrator's Guide* includes a topic titled "Maximum user and server connections to the Community server." This topic discusses the administration setting that specifies the maximum number of connections that are allowed to the Sametime Community server. This topic states the following:

"The lower limit is 50 connections and the upper limit is 20,000. Use the upper limit only for servers with high-level processing capabilities of at least 512 MB of RAM, a 1 MB network card, and dual processors."

Note that the 1 MB network card requirement may not be sufficient to support the upper limit (approximately 20,000) of connections to the Community Server. A 10 MB or 100 MB network card is recommended.

Sametime Connect client, Sametime Meeting Room client

No lower limit for Community server connections

The topic "Maximum user and server connections to the Community server" in the *Sametime 3.1 Administrator's Guide* states that the "Maximum user and server connections to the Community server" field has a lower limit of 50. This information is incorrect; there is no lower limit on this field.

Enterprise Meeting Server and server clusters

Replace the add_meeting_cluster.xml file when updating the EMS

Before you can add a Sametime 3.1 server to the Sametime Enterprise Meeting Server, you must replace some existing files on the EMS machine with some updated files that are provided in the "EMS-Patches" directory on Sametime 3.1 server CD 2.

The Sametime 3.1 Administrator's Guide indicates that you must replace the file on the EMS machine named add_meeting_cluster.xml with a file of the same name that is provided in the EMS-Patches directory of the Sametime 3.1 server CD 2.

The name of this file is not correct in the administrator's guide. The correct name of the file that must be replaced is add_meeting_cluster.xml.

Sametime server

Users of Sametime Links can respond to announcements

The *Sametime 3.1 Administrator's Guide* contains a topic in the "Configuring the Community Services" chapter entitled "Allow users to send announcements."

The "Allow users to send announcements" topic contains a statement that indicates users of Sametime Links applications can receive announcements, but cannot respond to announcements. This statement is incorrect. Users of Sametime Links can both receive and respond to announcements.

Installation Guide

Sametime server

Administrator name/password not specified during installation

You must enter an administrator name and password to access the Sametime Administration Tool from the Sametime server home page.

The Sametime 3.1 Installation Guide (stinstall.nsf) indicates that the user name and password required to access the Sametime Administration Tool are specified during a Sametime server installation. This is not correct.

Sametime installs on top of a Domino server. By default, the user name and password required to access the Sametime Administration Tool is the Domino administrator name and password that were specified during the Domino server installation. You cannot specify an administrator name and password during the Sametime server installation.

To access the Sametime Administration Tool following the Sametime server installation, use the administrator name that is listed first in the "Administrators" field of the Domino server Server document. For more information about enabling users to access the Sametime Administration Tool, see the topic "Adding a new Sametime administrator" in the "Using the Sametime Administration Tool" chapter of the *Sametime 3.1 Administrator's Guide*.

Note: The Sametime installation programmatically adds the first name listed in the "Administrators" field of the Domino server Server document to the ACL of the Configuration database (stconfig.nsf) and provides this name with Manager access to the stconfig.nsf database. This configuration enables the first user in the Administrators field of the Domino server Server document to access the Sametime Administration Tool and change Sametime configurations following a Sametime server installation.

Sametime server

Check for nserver to see if Domino is running

Look for the process name nserver to determine if Domino is running. To check if Domino is running, go to the Task Manager and select the Processes tab and then look for nserver. If nserver is found, Domino is currently running. You may want to do this when the dialog box pops up warning the user to ensure that Domino has been stopped before installing Sametime.

Sametime server

Community Services Multiplexer invalid

The topic "Installing Community Services Multiplexer (MUX)" topic is invalid for the translated versions of the Installation Guide. This topic is deleted in the English version but still appears in the translated versions.

Sametime server

Disable Domino DNA when upgrading from 2.5 to 3.1

When upgrading from a Sametime 2.5 standalone server to Sametime 3.1, you should shut down all Domino services prior to starting Sametime 3.1. If Domino DNA process is set to manual you will receive the following error:

Server is already running (in another process)" error when upgrade a 2.5 standalone server to 3.1

To avoid this error, disable Domino DNA in the service panel.

Sametime Broadcast client, Sametime Connect client, Sametime Meeting Room client, Sametime server

System requirements corrections

The *Sametime 3.1 Installation Guide* states that the Windows operating system requirement for the Sametime 3.1 server is Windows 2000 Server with Service Pack 2 installed.

This requirement is not correct. The Windows operating system requirement for the Sametime 3.1 server is the Windows 2000 Server with Service Pack 3 installed.

The *Sametime 3.1 Installation Guide* states that the Windows operating system requirement for the Sametime 3.1 clients is Windows 2000 Professional with Service Pack 2 installed.

This requirement is not correct. The Windows operating system requirement for the Sametime 3.1 clients is Windows 2000 Professional with Service Pack 3 installed.

The *Sametime 3.1 Installation Guide* pdf file (stinstall.pdf) states that the Sametime 3.1 server can be installed on a Domino 6.0.2 server or a Domino 5.0.13 server.

This requirement is not correct. Sametime 3.1 can only be installed on a Domino 6.0.2 server.

The NSF version of the Sametime Installation Guide (stinstall.nsf) contains corrections that do not exist in the PDF version of the Sametime Installation Guide (stinstall.pdf). The NSF version is more up-to-date than the PDF version.

Sametime server

v2.6 reference must be changed to 3.1 in install guide

In the *Sametime 3.1 Installation Guide* under the heading "About deinstalling and reinstalling the Sametime server" it reads as follows:

To reinstall the Sametime server, it is better to deinstall the Sametime server first. You might want to back up any important files before you reinstall the server. To deinstall the Sametime server:

1. Stop the Sametime server before deinstalling it. For instructions, see Starting and Stopping the Sametime server later in this chapter.
2. From the Windows Start menu, select Settings - Control Panel - Add/Remove Programs.
3. Select Sametime Server v2.6 from the list and click Add/Remove. Click Yes when prompted to remove the Sametime server.
4. When the Windows deinstall program completes, click OK to exit the deinstall program.
5. From Windows Explorer, delete the C:\Sametime directory. This step is not required if Sametime was deinstalled from a machine that also included a Domino server.

To reinstall the Sametime server:

Follow the procedures listed in this guide for the instructions necessary to install the Sametime 3.1 server.

The v2.6 that appears in step 3 above should be v3.1

Provide feedback for Sametime documentation

Sametime server

Provide feedback for Sametime Release Notes

Please send us your comments and suggestions about the Sametime Release Notes.

The Sametime documentation team reads this feedback and uses your comments to improve the documentation for future release.

Chapter 5 - Interoperability

The *Interoperability* chapter describes known restrictions or potential incompatibilities between the released versions of Sametime. This chapter also describes known interoperability issues among various operating system platforms and the Sametime server.

Sametime 2.5 - Sametime 3.0 compatibility

Sametime Connect client

Accessing help in a mixed environment

The help that is available from Sametime Connect corresponds to the Sametime server that the user is accessing rather than the version of Sametime Connect that the user is using. For example, if a user accesses the help from a 3.0 version of Sametime Connect, and his or her Connectivity settings specify a Sametime 2.5 server, the user receives Sametime 2.5 help (including topics that describe the 2.5 version of Sametime Connect) after choosing Help - Help Topics in Sametime Connect.

Sametime Connect client

Sametime Connect 2.5 and 3.0 compatibility issues

The following topics discuss compatibility issues for a Sametime 2.5 Connect client connecting to a Sametime 3.0 server or a Sametime 3.0 Connect client connecting to a Sametime 2.5 server:

- The "Sametime Connect client 2.5 and 3.0 compatibility issues with HTTP tunneling on port 80" topic in the "Configuring Sametime Connectivity" chapter of the *Sametime 3.0 Administrator's Guide*.
- The "Sametime Connect and HTTPS connections on port 443 or 563" topic in the "Things you need to know" section of these Release Notes.

Sametime Connect for browsers interoperability

Sametime Connect client

Sametime Connect for browsers interoperability

A Java version of the Sametime Connect client called "Sametime Connect for browsers" became available with Sametime 2.5. The interoperability issues for "Sametime Connect for browsers" are listed below.

- "Sametime Connect for browsers" must be used with 2.0, 2.5, or 3.0 Sametime servers.
- A user of "Sametime Connect for browsers" must have a 2.0, 2.5, or 3.0 Sametime server specified as the home server in the Sametime server field of the user's Person document.
- The 2.5 and 3.0 releases of the "Sametime Connect for browsers" client are supported on Windows machines only.

Chapter 6 - History of changes

Product change reporting

Sametime server

Overview of product change reporting

The Release Notes *History of changes* chapter is used by IBM Lotus Sametime to summarize enhancements made to software products in point releases and maintenance releases. For a summary of the new features that have been added for Sametime 3.0, see New Features in the *What's New* section of these Release Notes.

