



# Copyrights

## 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, IBM DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SAME. 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 IBM (OR ITS 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, except in the manner described in the documentation or the applicable licensing agreement governing the use of the software.

©Copyright IBM Corporation 1998, 2004

All rights reserved.

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

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

## List of Trademarks

1-2-3, Ami Pro, Domino, Freelance Graphics, Lotus, LotusScript, Notes, Notes Mail, Sametime, TeamRoom, and Word Pro are trademarks or registered trademarks of Lotus Development Corporation and/or IBM Corporation, in the United States, other countries, or both. UltraPort, iSeries, pSeries, and zSeries are trademarks and IBM, SecureWay, Thinkpad, and WebSphere are registered trademarks of International Business Machines Corporation. AOL Instant Messenger is a service mark and America Online and AOL are registered service marks of America Online, Inc. Intel, MMX, and Pentium are trademarks or registered trademarks of Intel Corporation or

its subsidiaries in the United States and other countries. Latitude Communications and MeetingPlace are trademarks of Latitude Communications, Inc. ActiveX, Microsoft, MSN, NetMeeting, Outlook, PowerPoint, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Java and JavaScript are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Other company, product, and service names may be trademarks or service marks of others.

All other trademarks are the property of their respective owners.



# Table of Contents

<b>SYSTEM REQUIREMENTS</b> .....	<b>3</b>
EMS SYSTEM REQUIREMENTS.....	3
IBM LOTUS INSTANT MESSAGING AND WEB CONFERENCING (SAMETIME) SERVER SYSTEM REQUIREMENTS .....	4
<b>UPGRADING FROM EMS 1.0 TO EMS 3.0 IF1</b> .....	<b>5</b>
REPLACING THE SAMETIME 3.X SERVERS WITH SAMETIME 6.5.1 SERVERS .....	5
Removing the Sametime servers from the EMS.....	5
Uninstall the Sametime 3.x servers .....	6
Install the Sametime 6.5.1 servers .....	6
Install the “IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade” on the Sametime 6.5.1 servers.....	7
BACK UP AND UNINSTALL THE EMS 1.0 APPLICATION.....	8
Backing up the EMS 1.0 application .....	8
Uninstalling the EMS 1.0 application.....	9
INSTALL THE WEBSHERE APPLICATION SERVER 4.0 FIXPAK 7 ON THE WEBSHERE SERVER .....	9
INSTALL THE WEBSHERE MQ FIX PACK 7 ON THE WEBSHERE MQ SERVER.....	11
MIGRATE THE DB2 SERVER AND EMS DB2 DATABASES .....	11
INSTALL THE EMS 3.0 IF1 FILES ON THE WEBSHERE 4.0.7 COMPUTER .....	12
CREATE THE WEBSHERE MQ QUEUES .....	13
CREATE THE JMS MESSAGING QUEUES .....	15
Editing the setenv.cmd file .....	15
Editing the JMSAdmin.config file.....	16
Editing the jms.ems.scf file.....	17
Setting up the Java environment and create the JMS queues .....	18
CREATE TWO NEW JMS DESTINATIONS FROM THE WEBSHERE ADMINISTRATOR’S CONSOLE.....	19
DEPLOYING THE EMS 3.0 IF1 APPLICATION ON THE WEBSHERE 4.0.7 SERVER.....	20
Deploy the Sametime Enterprise Archive (EAR) file.....	20
Start the Default Server and stadmin application servers .....	22
ADD THE SAMETIME SERVERS TO THE EMS 3.0 IF1 APPLICATION.....	22
Synchronizing Single Sign-On (SSO) support for the EMS and Sametime servers.....	23
Editing the Sametime.ini file on the Sametime servers .....	25
Editing the MeetingServices document in the Configuration database on the Sametime server.....	26
Add the Sametime server using the Sametime EMS Administration Tool.....	27
Specifying Usage Limits and Denied Entry settings for the Sametime servers.....	28
SECURING END USER ACCESS TO THE EMS.....	29
<b>PERFORMANCE ENHANCEMENT TIPS</b> .....	<b>30</b>
Altering maxSearchResults and allowEmptySearchStrings .....	30
Altering Sametime Directory Assistance.....	30
Altering minimum and maximum thread sizes.....	30
<b>KNOWN ISSUES</b> .....	<b>32</b>
INSTALLATION ISSUES .....	32
Do not create the virtual organization when setting up the EMS .....	32
Compiling JSPs after EMS installation optimizes page loading performance.....	32
Unable to install the EMS files from a network drive .....	33
Domino and Sametime processes hang after installing additional Sametime server.....	33
LDAP DIRECTORY ISSUES .....	33
Cannot browse the LDAP directory .....	33
“Update Security Configuration Failed” message when enabling LDAP Directory Access for WebSphere .....	34

ADMINISTRATION ISSUES .....	35
User with a person entry in the Domino Directory cannot authenticate .....	35
The stadmin application server must be started before a Sametime server is started .....	35
Not always necessary to restart a Sametime server after changing administration settings .....	35
Some of the Usage Limits and Denied Entry settings are not hard limits .....	36
MEETING CENTER AND MEETING ISSUES .....	38
Recorded meetings are not sorted by status.....	38
Reattaching edited whiteboard files to a meeting .....	38
INTERNATIONAL ISSUES .....	38
Installing the JMS Providers with the Simplified Chinese, Traditional Chinese, or Korean language operating system.....	38
Double-Byte Character Set (DBCS) names for whiteboard files do not display correctly .....	39
Problem installing the JMS providers when deploying EMS on a Spanish language version of WebSphere .....	39
User names with accented characters may cause a WebSphere login failure.....	40
Anonymous meeting moderator cannot edit a meeting, change meeting duration, or delete a meeting	40
A user that is a member of a group that has a name that uses DBCS characters cannot log in to the Sametime EMS Meeting Center .....	41
Name display problems caused by directory entries that use mixed code pages.....	41
<b>DOCUMENTATION CORRECTIONS.....</b>	<b>42</b>
Incorrect version of WebSphere MQ documented in administrator's guide .....	42

## System Requirements

This section discusses the system requirements of the IBM Lotus Enterprise Meeting Server (EMS) 3.0 IF 1 computer and the system requirements of the IBM Lotus Instant Messaging and Web Conferencing (Sametime®) servers that must inter-operate with the EMS.

**Note:** The Enterprise Meeting Server (EMS) application interoperates with Sametime servers to provide fail over and load balancing for a group of Sametime servers. The EMS provides no functionality by itself. You must install a group of Sametime servers, install the EMS, and then add the Sametime servers to the EMS to use the functionality provided by the EMS.

### EMS system requirements

The EMS 3.0 IF 1 is a Java 2 Enterprise Edition (J2EE) compliant application that must be installed into a J2EE environment consisting of the following:

- An IBM DB2 Universal Database V8.1.4.428 Enterprise Edition
- An IBM WebSphere MQ V5.3.0.7 (WebSphere MQ V5.3 with fix pack 7 and MQSeries 5.3 Publish/Subscribe SupportPac ma0c installed)
- A WebSphere Application Server V4.0.7 server (WebSphere Application Server V4.0 with Fixpack 7 installed)
- IBM HTTP server 1.3.19

**Note:** The software release levels listed above reflect the release levels with which the EMS 3.0 IF 1 was tested. You can install the latest fix pack available for any of the software listed above. The EMS 3.0 IF 1 should function properly when the latest fix packs are installed.

For detailed information about setting up the J2EE environment required by the EMS, see "Chapter 19 - Setting up the Enterprise Meeting Server and a Meeting Services cluster" in the *IBM Lotus Instant Messaging and Web Conferencing 6.5.1 and Enterprise Meeting Server 3.0 IF1 Administrator's Guide* (sthelapd.pdf) provided with the EMS.

The EMS application installs on the same machine as a WebSphere Application Server V4.0.7. The system requirements of this machine are noted below:

- **CPU** - Pentium® 4 1.8GHz or higher recommended
- **Operating system** - Windows NT Server with Service Pack 6a or Windows 2000 Server or Advanced Server with Service Pack 1
- **Memory:**
  - Windows NT - 1GB RAM recommended; 512MB minimum
  - Windows 2000 - 1GB RAM recommended; 512MB minimum
- **Disk space** - 500MB of free disk space. 1GB + is recommended

## IBM Lotus Instant Messaging and Web Conferencing (Sametime) server system requirements

The system requirements of the Sametime 6.5.1 servers are listed below. All of the Sametime servers used with the EMS 3.0 IF 1 must be Sametime 6.5.1 servers with the IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade installed (this server upgrade is provided with the EMS software).

A Sametime 6.5.1 server machine must meet these system requirements.

- **CPU** - Pentium® II 400MHz or higher recommended
- **Operating system** - Windows® 2000 with Service Pack 2 or Windows 2003
- **Memory:** - 1GB RAM recommended; 512MB minimum  
Disk space - 500MB of free disk space. 1GB + is recommended  
Disk swap space - 64MB
- **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.
- **Domino Server requirements** - The Sametime server can be installed on a Domino server version 6.03, 6.5, or 6.5.1.

The Sametime server computers should also:

- Be registered in the same DNS domain as the EMS/J2EE machine.
- Have TCP/IP connectivity with the EMS/J2EE machine on the following ports:  
Port 80 for HTTP connections.  
Port 900 for Java Naming and Directory Interface (JNDI) connections.  
Port 1414 for WebSphere MQ connections

## Upgrading from EMS 1.0 to EMS 3.0 IF1

This section explains how to upgrade the previous EMS release (EMS 1.0) to EMS 3.0 IF1.

The twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1 are discussed below.

1. Replace the Sametime 3.x servers with Sametime 6.5.1 servers
2. Backup and uninstall the EMS 1.0 application
3. Install the WebSphere Application Server 4.0 Fixpak 7 on the WebSphere server
4. Install the WebSphere MQ Fixpak 7 on the WebSphere MQ server
5. Migrate the DB2 server and EMS DB2 databases to DB2 V8.1
6. Install the EMS 3.0 IF1 files on the WebSphere 4.0.7 server
7. Create the WebSphere MQ queues
8. Create the JMS messaging queues
9. Create two new JMS Destinations from the WebSphere Administrator's Console
10. Deploying the EMS 3.0 IF1 application on the WebSphere 4.0.7 server
11. Add the Sametime servers to the EMS 3.0 IF1 application
12. Secure end user access to the EMS

### Replacing the Sametime 3.x servers with Sametime 6.5.1 servers

Replacing the Sametime 3.x servers with Sametime 6.5.1 servers is the first of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

This task is described in four steps:

1. Remove the Sametime servers from the EMS.
2. Uninstall the Sametime 3.x servers.
3. Install the Sametime 6.5.1 servers in place of the Sametime 3.x servers.
4. Install the IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade on the Sametime 6.5.1 servers.

### Removing the Sametime servers from the EMS

Removing all of the Sametime 3.x servers from the EMS is the first of four steps required to upgrade the Sametime servers to operate with the EMS 3.0 IF1.

To remove a Sametime 3.x server from the EMS:

1. Enter the following URL in a Web browser to browse to the Sametime EMS Administration Tool on the EMS 1.0 machine:  
`http://<ems server host name>/sametime-admin`
2. Enter an administrator name and password to access the Sametime EMS Administration Tool.

3. Select **Configuration > Meeting Cluster**.
4. Select the **Edit/Remove a Meeting Server** tab.
5. In the “Meeting servers in this cluster” list box, select a Sametime 3.x server and click **Remove**.
6. Repeat step 6 until you have removed all of the Sametime 3.x servers from the EMS 1.0.

### **Uninstall the Sametime 3.x servers**

Uninstalling the Sametime 3.x servers is the second of four steps required to replace the Sametime 3.x servers with Sametime 6.5.1 servers.

After removing the Sametime 3.x servers from the EMS, uninstall Sametime 3.x from the Sametime server computers.

To uninstall a Sametime server:

1. Stop the Sametime server.
2. From the Windows Start menu, select **Settings > Control Panel > Add/Remove Programs**.
3. Select the Sametime server from the list and click **Add/Remove**. Click **Yes** when prompted to remove the Sametime server.
4. When the Windows uninstall program completes, click **OK** to exit the uninstall program.

### **Install the Sametime 6.5.1 servers**

Installing the Sametime 6.5.1 servers is the third of four steps required to replace the Sametime 3.x servers with Sametime 6.5.1 servers.

In this step, you install the Sametime 6.5.1 servers on the machines previously used to host the Sametime 3.x servers.

Note the following when installing the Sametime 6.5.1 servers to operate with the EMS:

- Completely uninstall the Sametime 3.1 servers and then install the Sametime 6.5.1 servers as new servers. Do not upgrade the Sametime 3.x servers to Sametime 6.5.1.
- All Sametime 6.5.1 servers must operate as part of the same Domino domain to operate with the EMS. To be part of the same Domino domain, the Sametime servers must be registered in the same Domino Directory. The Domino Directory must replicate between the servers.

**Note:** The Domino Directory must replicate between the Sametime/Domino servers even though you are maintaining the user community in an LDAP directory on a separate server that is not part of the Community Services cluster. Replication of the Domino Directory is required for proper functioning of the Domino servers on which Sametime is installed.

- Each Sametime 6.5.1 server must be installed in the same DNS domain as the machine reserved for the EMS and J2EE installations. (This recommendation ensures that the Single Sign-On functionality works properly.)

- Each Sametime 6.5.1 server that you install must have TCP/IP connectivity with the EMS/J2EE machine on the following ports:

**Port 80** - The EMS and Sametime servers communicate using HTTP on port 80 to perform meeting scheduling and materials management activity.

**Port 900** – The EMS and Sametime servers use this port for Java Naming Directory Interface (JNDI) communications.

**Port 1414** – The EMS and Sametime servers use this port for Java Messaging Service (JMS) communications (via WebSphere MQ message queuing functionality). This communication supports the load balancing, meeting booking, and fail over functionality provided by the EMS.

- Each Sametime 6.5.1 server must be configured to connect to the same LDAP directory as the EMS. For information about connecting a Sametime server to an LDAP directory, see the *IBM Lotus Instant Messaging and Web Conferencing 6.5.1 and Enterprise Meeting Server 3.0 IF1 Administrator's Guide* (sthelapad.pdf) provided with the EMS software.

For the step-by-step instructions for installing a Sametime 6.5.1 server, see the *IBM Lotus Instant Messaging and Web Conferencing (Sametime) 6.5.1 Installation Guide*.

### **Install the “IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade” on the Sametime 6.5.1 servers**

Installing the “IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade” on the Sametime 6.5.1 servers is the last of four steps required to replace the Sametime 3.x servers with Sametime 6.5.1 servers.

After you have replaced your Sametime 3.1 servers with Sametime 6.5.1 servers, you must install the “IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade” on each of the Sametime 6.5.1 servers. The IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade enables the Sametime 6.5.1 servers to operate with the EMS 3.0 IF1.

**Note:** After you install the IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade on each of the Sametime 6.5.1 servers, the Sametime servers must be used with the EMS 3.0 IF1. A Sametime 6.5.1 server that includes this upgrade functions properly only when it is attached to the EMS 3.0 IF1.

To install the IBM Lotus Web Conferencing EMS Room Server 6.5.1 upgrade on a Sametime 6.5.1 server:

1. Stop the Sametime 6.5.1 server. If you cannot stop the Sametime 6.5.1 services, reboot the server.
2. Insert the EMS 3.0 IF1 CD into the CD-ROM drive of the server. You can begin the upgrade installation by clicking on the setup.exe file located in the <root>\RoomServer\Server directory of the CD.
3. Read, follow directions, and click **Next** through the following screens:
  - IBM Software License Agreement
  - Welcome
4. The following dialog box displays: "An existing version of Sametime is found at C:\Sametime. Would you like to upgrade? If yes, make sure you stop the Sametime server." Click **Yes**.

5. When the files have completed copying, the server reboots and the set up program launches.
6. The "Upgrade the Sametime Server" dialog box displays. Type the filename of the Sametime server ID or browse to and select the Sametime server ID file.  
**Note:** The Sametime server ID is the one you created when you registered the server or the one that was created by a previous Sametime 6.5.1 installation.
7. The "Sametime Server Connectivity" dialog box displays.  
Disable the checkbox. Usually, it is not necessary to support HTTP tunneling on port 80 for a Sametime server that operates with the EMS as part of a Meeting Services cluster.
8. Click **Next**. The Sametime Server Setup Progress bar displays; when done the "Setup Finished" dialog box displays.

## Back up and uninstall the EMS 1.0 application

Backing up and uninstalling the EMS 1.0 application is the second of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

In this task, you first back up and then uninstall the EMS 1.0 application. Instructions are provided below.

### Backing up the EMS 1.0 application

Follow the instructions below to back up the EMS 1.0 application. Perform these steps on the WebSphere server on which the EMS 1.0 application is installed.

1. Stop the WebSphere server.
2. Make a back up copy of all files in the C:\WebSphere\AppServer\bin\Sametime directory.  
Copy all files in this directory to a floppy disk or a secure network location. You will need these back up files if you need to restore the EMS 1.0 application on the WebSphere computer.
3. Use the WebSphere Administrator's Console to export (backup) the Sametime.EAR file.
  - a Start the WebSphere Administrator's Console on the WebSphere computer on which the EMS 1.0 is installed.
  - b Click **Applications > Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
  - c Place a checkmark in the check box beside the EMS application name and click **Export**.  
**Note:** You created the EMS application name when you deployed the Sametime.EAR file during the EMS 1.0 installation. The specific name provided for the EMS application was at your discretion.
  - d On the Export Application EAR Files page, click on the link to download the exported Sametime.EAR file.
  - e Use the browser dialogue to specify a location at which to save the exported EAR file and click **OK**.

**Note:** The file containing binding information is exported to the specified node and directory, and has the name `enterprise_application_name.ear`.

## Uninstalling the EMS 1.0 application

After you have backed up the EMS 1.0 application, follow the procedure below to uninstall the EMS 1.0 application from the WebSphere server.

From the WebSphere Administrator's Console:

1. Click **Applications > Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
2. Stop the EMS application. Place a checkmark in the check box beside the EMS application name and click **Stop**.
3. With a checkmark in the check box beside the EMS application name, click **Uninstall**.
4. Confirm the uninstallation operation.
5. Click **Save** on the console taskbar to save changes made to the administrative configuration.

## Install the WebSphere Application Server 4.0 Fixpak 7 on the WebSphere server

Installing the WebSphere Application Server 4.0 Fixpak 7 on the WebSphere server is the third of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

The EMS 1.0 release operated on a WebSphere 4.0.3 server. In this task, you upgrade the WebSphere server to version 4.0.7 by installing the WebSphere Application Server 4.0 Fixpak 7 on the WebSphere 4.0.3 server.

**Note:** For detailed information about the WebSphere Application Server 4.0, Advanced Edition Fixpak 7, see the "was40\_ptf\_7.Readme" text file that is available with the Fixpak.

To perform this procedure, you must know the directories in which the IBM HTTP server and the WebSphere Application Server are installed. The installation instructions provided below assume that install directories for these servers are `C:\IBM HTTP Server` and `C:\WebSphere\AppServer`.

To install WAS Fixpak 7 on the EMS machine:

1. Ensure the following Windows services are stopped:
  - IBM HTTP Administration
  - IBM HTTP Server
  - IBM WS AdminServer
2. You must download the zipped WebSphere Application Server 4.0 Fixpak 7 file from an IBM Web site. On the machine reserved for EMS deployment, create a working directory (for example, `c:\WAS FP7`) to which you can download the zipped file.

3. Download the WebSphere Application Server 4.0, Advanced Edition Fixpak 7 file from the following location:  
[http://www.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q1=fixpak+7&q2=Fix+Pack+7&uid=swg24005733&loc=en\\_US&cs=utf-8&lang=en](http://www.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q1=fixpak+7&q2=Fix+Pack+7&uid=swg24005733&loc=en_US&cs=utf-8&lang=en)
4. Unzip the was40\_ae\_ptf\_7.zip file and run the "install.bat" file to begin the installation.
5. Review the information concerning the "FixPak License." You must type "Accept" in the command window and press the Enter key to accept the terms of the FixPak License.
6. When prompted with a message indicating you must shut down the Application Server, AAT, and any Web Servers, press any key to continue.  
**Note:** If you stopped the services described in step 1 above, all of these services should be stopped.
7. When prompted with "Update the Application Server (yes/no)?," type "yes" and press Enter.
8. When prompted with "Enter the Application Server Home...," type c: <WebSphere Application Server install directory> and press Enter. If you are using the default installation directories, the appropriate entry is:  
C:\WebSphere\AppServer (and press Enter)
9. When prompted with "Use the Application Server JDK (yes/no)?," type "yes" and press Enter.
10. When prompted with "Perform update of the JDK (yes/no)?," type "yes" and press Enter.
11. When prompted with "Update Sun ONE Web Server (iPlanet) configuration support by WebSphere (yes/no)?," type "no" and press Enter.
12. When prompted with "Perform update of the IBM HTTP server (yes/no)?," type "yes" and press Enter.
13. When prompted with "Enter the IBM HTTP Server home:," type c:\<IBM HTTP Server installation directory> and press Enter. If you are using the default installation directories, the appropriate entry is:  
C:\IBM HTTP Server (and press Enter)
14. When prompted with "Perform update of the Apache web server (yes/no)?," type "no" and press Enter.
15. When prompted with "Install/Update Connector Architecture for WebSphere (J2C) (yes/no)?," type "yes" and press Enter.
16. When prompted with "Use the Application Server Logs directory (yes/no)?," type "yes" and press Enter.
17. When prompted with "Place backups under the WebSphere Application Server Home (yes/no)?," type "yes" and press Enter.
18. When prompted with "About to perform selected updates," press any key to continue.

The file runs for several minutes as the updates are performed. As each update is performed, a success message appears on the screen to indicate the update is successful.

When the file completes successfully, the command line returns.

**Note:** After installing Fixpak 7 on the IBM WebSphere Application Server V4.0.3, the server version number changes to IBM WebSphere Application Server V4.0.7.

## Install the WebSphere MQ Fix Pack 7 on the WebSphere MQ server

Installing the WebSphere MQ Fix Pack 7 on the WebSphere MQ server is the fourth of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF 1.

You must install the WebSphere MQ Fix Pack 7 (CSD07) on the WebSphere MQ server to enable the WebSphere MQ server to function with the EMS 3.0 IF 1.

You can obtain the WebSphere MQ Fix Pack 7 (CSD07) from the following web site:

[http://www.ibm.com/support/docview.wss?rs=0&q1=WebSphere+MQ&uid=swg24007281&loc=en\\_US&cs=utf-8&cc=us&lang=en](http://www.ibm.com/support/docview.wss?rs=0&q1=WebSphere+MQ&uid=swg24007281&loc=en_US&cs=utf-8&cc=us&lang=en)

The installation instructions for WebSphere MQ Fix Pack 7 are also provided at the web site above.

**Note:** The *IBM Lotus Instant Messaging and Web Conferencing (Sametime) 6.5.1 Administrator's Guide* states that you must use the IBM WebSphere MQ V5.3.1 server with the EMS 3.0 IF 1. This requirement is incorrect. You must use the IBM WebSphere MQ V5.3.0.7 server (a WebSphere MQ 5.3 server with WebSphere MQ Fix Pack 7 installed) with the EMS 3.0 IF 1.

## Migrate the DB2 server and EMS DB2 databases

Migrating the DB2 server and the EMS DB2 databases is the fifth of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

In this procedure, you must migrate the DB2 server from the DB2 V7.2 version used with the EMS 1.0 to the DB2 V8.1 version required by the EMS 3.0 IF 1.

The detailed instructions for migrating a DB2 server from the V7 to V8 level are provided in an IBM publication titled *Quick Beginnings for DB2 Servers* available from the DB2 Version 8 Support Web site on [www.ibm.com](http://www.ibm.com). A direct link to this publication is

<ftp://ftp.software.ibm.com/ps/products/db2/info/vr8/pdf/letter/db2ise80.pdf>.

The steps required to perform the DB2 migration are summarized below. (Detailed information on each of these steps is available in "Part 2. Migrating your DB2 Server" in the *Quick Beginnings for DB2 Servers* publication.)

1. Record configuration settings before the DB2 migration.
2. Change the diagnostic error level.
3. Take the DB2 server offline for DB2 migration.
4. Back up your databases.

5. Install your DB2 V8.1 server.
6. Migrate databases.

Note that in steps 4 and 6, the databases you must back up and migrate are the database used by the WebSphere server and the database used by the EMS application. In previous publications, these databases were named the "WAS 40" database and the "Sametime" database, respectively.

## Install the EMS 3.0 IF1 files on the WebSphere 4.0.7 computer

Installing the EMS 3.0 IF 1 files on the WebSphere 4.0.7 computer is the sixth of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

This task installs all files required to deploy the EMS 3.0 IF1 application on the WebSphere server.

**Note:** This Sametime Administrator Information screen of this installation prompts you for a user name and password. This user name and password is used to authenticate connections from the EMS to configuration servlets on the Sametime server. IBM Lotus software recommends that you create a unique person entry in the LDAP directory containing the user name and password used strictly for the purpose of authenticating these connections.

To install the EMS 3.0 IF1 files:

1. Insert the EMS CD in the WebSphere 4.0.7 computer and select **Install the Enterprise Meeting Server**.
2. Choose the Setup language and click **OK**.
3. Read, follow directions, and click Accept or Next through the following screens:
  - Software License Agreement
  - Welcome
4. In the Sametime Prerequisites window, verify you have installed all required applications and then click **Next**.
5. In the Verify Location of WebSphere Application Server window, verify that the WebSphere location is correct. In our example, the correct location is c:\WebSphere\AppServer. If the location is incorrect, browse to the correct location. Click **Next**.
6. In the Sametime Enterprise Meeting Server Cluster Name dialog box, enter a name for your Meeting Services cluster (for example, SametimeMeetingServicesCluster). The cluster name is at your discretion. Click **Next**.
7. In the Sametime Administrator Information screen, enter the name and password of the LDAP directory account that is used to protect the configuration servlets on the Sametime servers in the Meeting Services cluster.

The EMS must access the configuration servlet on each Sametime server. This name and password is used to authenticate the EMS when accessing the configuration servlet on each Sametime server.

To enter an administrator name for access to the configuration servlets on the Sametime servers, complete the following fields:

- Name
- Password
- Verify (In the Verify field, re-enter the administrator password.)

Click **Next**.

8. The Connection Information screen specifies the connectivity parameters for the "stadmin" WebSphere application server that supports the Sametime EMS Administration Tool.

The EMS application resides on the "Default Server" application server and must connect to the "stadmin" application server. The EMS application uses the connection information on this screen to establish this connection.

**Note:** In this example, the stadmin application server resides on the same machine as the EMS application and uses the DNS name and port of the WebSphere server.

- **Network Address** - Enter the IP address or the fully-qualified DNS name of the WebSphere server containing the stadmin application server. (In this example, this is the same WebSphere server that contains the EMS application.)
- **Port Number** - Enter the port number on which the IBM HTTP server listens for HTTP or HTTPS connections. Generally, this setting will specify either port 80 for HTTP connections or port 443 for HTTPS connections.
- **Enable SSL** - Select this setting if you want to enhance security by encrypting connections between the EMS and Sametime servers with SSL. If you select this setting, you must perform some additional configurations to encrypt the connections. For more information, see "Encrypting HTTP traffic between the EMS and Sametime servers with SSL" in Chapter 21 of the *IBM Lotus Instant Messaging and Web Conferencing 6.5.1 and Enterprise Meeting Server 3.0 IF1 Administrator's Guide* (sthelpad.pdf) provided with the EMS software.

Click **Next**.

9. At the Start Copying Files dialog box, review your settings and click **Next**.
10. At the Setup Complete dialog box, click **Finish**.

## Create the WebSphere MQ queues

Creating the WebSphere MQ queues is the seventh of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

To create the new WebSphere MQ queues required by the EMS 3.0 IF1, you must run the mq.qdef.pcf script file. The mq.qdef.pcf file is installed with the EMS 3.0 IF1 files and is located in the <root>:\WebSphere\AppServer\bin\sametime directory by default following the installation of the EMS files. You must run this file from the WebSphere MQ server installation directory.

Follow the instructions below to run the mq.qdef.pcf file from the command prompt of the WebSphere MQ computer:

1. By default, the mq.qdef.pcf file is a read-only file. Use Windows Explorer to remove the Read-only attribute from this file. For example:

- Open Windows Explorer.
- Open the c:\WebSphere\AppServer\bin\sametime directory
- Right click on the mq.qdef.pcf file and select **Properties**.
- Clear the check mark from the Read-only attribute.

2. Start the Command Prompt on the WebSphere MQ computer.

**Note:** This procedure requires you to run a command from the computer on which the WebSphere MQ server is installed. This example assumes the WebSphere server and the WebSphere MQ server are installed on the same computer. If you have installed WebSphere MQ on a separate computer from WebSphere, you must copy the mq.qdef.pcf file from the WebSphere server to the WebSphere MQ server as noted below.

3. In the Command Prompt window, change to the <WebSphere MQ installation>\bin directory. For example, enter:

```
cd mqseries\bin
```

4. From the Command Prompt, run the following command:

```
runmqsc < mq.qdef.pcf
```

Remember that the mq.qdef.pcf file is located in the c:\WebSphere\AppServer\bin\sametime directory. For example, if WebSphere MQ and the EMS 3.0 IF1 files are installed on the same computer, your command string might look like this:

```
c:\mqseries\bin> runmqsc <  
c:\WebSphere\AppServer\bin\sametime\mq.qdef.pcf
```

Alternately, you can copy the mq.qdef.pcf file to the <WebSphere MQ installation>\bin directory and enter the following command:

```
c:\mqseries\bin> runmqsc < mq.qdef.pcf
```

**Note:** If you have installed WebSphere MQ on a different computer than WebSphere (and the EMS 3.0 IF1 files), you must copy the mq.qdef.pcf file from the WebSphere computer to the WebSphere MQ computer and run the file from the WebSphere MQ computer.

5. When the "All valid MQSC commands were processed" message appears, the file has finished running. To ensure that the file completed successfully, verify that there are no error messages displayed on the screen above the "All valid MQSC commands were processed" message. A list of queues that were created also appears in the command prompt window above the "All valid MQCS commands were processed" message.

## Create the JMS messaging queues

Creating the JMS messaging queues is the eighth of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

To complete this task, you must edit three files required to create the JMS messaging queues and then run the command to create the JMS messaging queues. This task includes these four steps:

1. Edit the setenv.cmd file.
2. Edit the JMSAdmin.config file.
3. Edit the jms.ems.scp file.
4. Set up the Java environment and create the JMS queues.

### Editing the setenv.cmd file

Editing the setenv.cmd file is the first of four steps required to create the JMS messaging queues.

You might need to edit the setenv.cmd file so that the top two lines of the file specify the WebSphere Application Server installation directory and the java subdirectory of the WebSphere MQ server installation directory.

**Note:** If you have installed the WebSphere Application Server to the "C:\WebSphere\AppServer" directory and the WebSphere MQ software to the "C:\MQSeries" directory, you do not need to edit the setenv.cmd file. Skip this procedure and continue with the next procedure titled "Editing the JMSAdmin.config file."

If you installed either the WebSphere Application Server or the WebSphere MQ server to a directory that is different than noted above, you must edit the setenv.cmd file.

Follow these instructions to edit the setenv.cmd file:

1. Use a text editor to open the setenv.cmd file located in the C:\WebSphere\AppServer\bin\sametime directory on the EMS computer.
2. Ensure that the top two lines in the setenv.cmd file specify the WebSphere Application Server installation directory and the java subdirectory of the WebSphere MQ installation directory. If these lines do not specify the appropriate directories, edit them to specify the directories used in your environment.

By default, the top two lines in the setenv.cmd file specify the values below:

```
Set WAS_HOME=c:\WebSphere\AppServer
Set MQ_JAVA_INSTALL_PATH=c:\mqseries\java
```

If you have specified a different installation directory for either the WebSphere Application Server or the WebSphere MQ server, you must edit the lines appropriately. For example, if you specified the c:\was\appserver directory as the WebSphere installation directory and the c:\webspheremq directory as the WebSphere MQ installation directory, the correct format for the lines is:

```
Set WAS_HOME=c:\was\appserver
```

```
Set MQ_JAVA_INSTALL_PATH=c:\webspheremq\java
```

3. After editing the top two lines to match your environment, save the file.

### Editing the JMSAdmin.config file

Editing the JMSAdmin.config file is the second of four steps required to create the JMS messaging queues.

The JMSAdmin.config file is located in the <WebSphere MQ install>\java\bin directory (for example, c:\mqseries\java\bin).

In this file you must comment out two lines and comment in two lines. You must also add the text string ":900" to the last line that you comment in to the file. Follow the instructions below.

**Note:** An example at the bottom of this topic shows how the file should appear after you have edited it.

1. Use a text editor to open the c:\mqseries\java\bin\JMSAdmin.config file.
2. Locate the following line:

```
INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
```

Type the pound sign (#) character in front of this line to comment the line out of the file and prevent it from running. For example:

```
#INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
```

3. Locate the following line:

```
#INITIAL_CONTEXT_FACTORY=com.ibm.websphere.naming.WsnInitialContextFactory
```

Delete the pound sign (#) character in front of this line to comment the line in and enable it to run. For example:

```
INITIAL_CONTEXT_FACTORY=com.ibm.websphere.naming.WsnInitialContextFactory
```

4. Locate the following line:

```
PROVIDER_URL=ldap://polaris/o=ibm,c=us
```

Type the pound sign (#) character in front of this line to comment the line out of the file and prevent it from running. For example:

```
#PROVIDER_URL=ldap://polaris/o=ibm,c=us
```

5. Locate the following line:

```
#PROVIDER_URL=iiop://localhost/
```

Delete the pound sign (#) character in front of this line to comment the line in and enable it to run. For example:

```
PROVIDER_URL=iiop://localhost/
```

6. In the PROVIDER\_URL=iiop://localhost/ line you have just commented in, add the text string ":900" after the word "localhost" but before the forward slash (/) character. After the line is edited, it should look like this:

```
PROVIDER_URL=iiop://localhost:900/
```

7. Save the JMSAdmin.config file.

When you have finished editing the JMSAdmin.config file, the portion of the file you have edited should look like this:

```
#INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.RefFSContextFactory
#INITIAL_CONTEXT_FACTORY=com.ibm.ejs.ns.jndi.CNInitialContextFactory
INITIAL_CONTEXT_FACTORY=com.ibm.websphere.naming.WsnInitialContextFactory
#
# The following line specifies the URL of the service provider's initial
# context. It currently refers to an LDAP root context. Examples of a
# file system URL and WebSphere's JNDI namespace are also shown, commented
# out
#
#PROVIDER_URL=ldap://polaris/o=ibm,c=us
#PROVIDER_URL=file:/C:/JNDI-Directory
PROVIDER_URL=iiop://localhost:900/
```

## Editing the jms.ems.scp file

Editing the jms.ems.scp file is the third of four steps required to create the JMS messaging queues.

You must edit the jms.ems.scp batch file to include the host name of the WebSphere MQ computer.

1. Using a text editor, open the jms.ems.scp batch file located in the c:\WebSphere\AppServer\bin\sametime directory on the EMS computer.
2. In the jms.ems.scp file, locate the following two lines near the middle of the file:

```
def qcf(SametimeQueueConnectionFactory) TRAN(CLIENT)
HOST(MUST_PUT_MQSERIES_HOSTNAME)

def tcf(SametimeTopicConnectionFactory) TRAN(CLIENT)
HOST(MUST_PUT_MQSERIES_HOSTNAME)
```

3. In the two lines above, the HOST () parameter must specify the fully-qualified DNS name of the computer on which the WebSphere MQ software is installed. In each line, delete the text MUST\_PUT\_MQSERIES\_HOSTNAME and type the fully-qualified DNS name of the server on which WebSphere MQ is installed in its place.

For example, if WebSphere MQ is installed on a computer with a fully-qualified DNS name of sametime.ems.ibm.com, the lines must be edited as follows:

```
def qcf(SametimeQueueConnectionFactory) TRAN(CLIENT)
HOST(sametime.ems.ibm.com)

def tcf(SametimeTopicConnectionFactory) TRAN(CLIENT)
HOST(sametime.ems.ibm.com)
```

4. Save the jms.ems.scp batch file and close the text editor.

## Setting up the Java environment and create the JMS queues

Setting up the Java environment and creating the JMS queues is the last of four steps required to create the JMS messaging queues.

To create the JMS messaging queues, you must first run the "setenv" command to set up the Java environment and then run the "jms.ems.scp" command to create the JMS messaging queues. You must run both of these commands from within the same Command Prompt window.

Follow the instructions below to set up the Java environment and create the JMS messaging queues:

1. If necessary, start the Command Prompt on the EMS/WebSphere MQ computer.
2. Change to the c:\WebSphere\AppServer\bin\sametime directory (or other directory in which you have saved the setenv.cmd file). For example, enter the following command:

```
cd c:\WebSphere\AppServer\bin\sametime
```

3. Run the setenv file by typing the setenv command at the prompt and pressing Enter. For example:

```
c:\WebSphere\AppServer\bin\sametime>setenv (and press Enter)
```

**Note:** The setenv.cmd file sets the java class path and environment variables for the command prompt window. Do not close the command prompt window after running the setenv command. The jms.ems.scp file must be run from within the same command prompt window as the setenv command. If you close the command prompt window and open a new command prompt window, you must rerun the setenv.cmd file and then run the jms.ems.scp file as described below from within the same command prompt window.

4. From the Command Prompt, change to the c:\<websphere mq install>\java\bin directory. The next command must be run from the java\bin subdirectory of the WebSphere MQ installation directory.

For example, enter the following command:

```
cd c:\mqseries\java\bin
```

5. From the command prompt, run the following command:

```
jmsadmin < jms.ems.scp
```

Remember that the jms.ems.scp file is located in the <root>:\WebSphere\AppServer\bin\sametime directory. For example, if your WebSphere MQ server and the EMS files are installed on the same computer, your command string might look like this:

```
c:\mqseries\java\bin> jmsadmin <  
c:\WebSphere\AppServer\bin\sametime\jms.ems.scp
```

Alternately, you can copy the "jms.ems.scp" file to the WebSphere MQ installation\java\bin directory and enter the following command:

```
c:\mqseries\java\bin> jmsadmin < jms.ems.scp
```

**Note:** The WebSphere MQ software can be installed on a different computer than the EMS. If you have installed WebSphere MQ on a different computer than the EMS, copy both the setenv.cmd file and the jms.ems.scp batch file from the WebSphere computer to the <MQ install>\java\bin subdirectory on the WebSphere MQ computer. Then run the following two commands to set the Java environment and execute the jms.ems.scp file on the WebSphere MQ computer:

```
c:\mqseries\java\bin>setenv (and press Enter)  
c:\mqseries\java\bin> jmsadmin < jms.ems.scp (and press Enter)
```

6. When the "Stopping MQSeries classes for Java Messaging Service Administration" message appears, the file has run successfully.

**Note:** Running the jms.ems.scp creates the following two new JMS queues that are required by the EMS 3.0 IF1:

SametimePostProcessingQueue

SametimeProvisioningEventQueue

## Create two new JMS Destinations from the WebSphere Administrator's Console

Creating two new JMS Destinations from the WebSphere Administrator's Console is the ninth of twelve tasks required to upgrade the WebSphere server to support the EMS 3.0 IF1.

In this task, you use the WebSphere Administrator's Console to create two new JMS Destinations. These JMS Destinations support the new SametimePostProcessingQueue and SametimeProvisioningEventQueue used by the EMS 3.0 IF1.

To create the new JMS Destinations:

1. Start the WebSphere Administrator's Console on the EMS machine. Choose **Start > Programs > WebSphere > Application Server V4.0 > Administrator's Console** from the Windows desktop.
2. Expand **Resources > JMS Providers > IBM MQSeries**.
3. Right-click on **JMS Destinations** and select **New**.

4. In the JMS Destinations dialog box, make the entries below in the Name and External JNDI Path fields:
  - **Name** – SametimePostProcessingQueue
  - **External JNDI Path** – jms\SametimePostProcessingQueue
5. Click **OK**.
6. Right-click on **JMS Destinations** and select **New**.
7. In the JMS Destinations dialog box, make the entries below in the Name and External JNDI Path fields:
  - **Name** – SametimeProvisioningEventQueue
  - **External JNDI Path** – jms\SametimeProvisioningEventQueue
8. Click **OK**.

## Deploying the EMS 3.0 IF1 application on the WebSphere 4.0.7 server

Deploying the EMS 3.0 IF1 application on the WebSphere 4.0.7 server is the tenth of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

This task is described in these two steps:

1. Deploy the EMS 3.0 IF1 application on the WebSphere server.
2. Restart the Default Server and stadmin application servers.

### Deploy the Sametime Enterprise Archive (EAR) file

Deploying the Sametime Enterprise Archive (EAR) file on the WebSphere 4.0.7 server is the first of two steps required to install the EMS 3.0 IF1 application on the WebSphere server.

**Note:** The Sametime EAR file was placed in the c:\WebSphere\AppServer\InstallableApps directory when you installed the EMS 3.0 IF1 files on the WebSphere server.

This procedure assumes you have created an stadmins group in the LDAP directory to support access to the Sametime EMS Administration Tool.

To deploy the Sametime EAR file:

1. If necessary, start the WebSphere Administrator's Console.
2. Expand **WebSphere Administrative Domain**.
3. Right-click on **Enterprise Applications** and select **Install Enterprise Applications**. The Install Enterprise Application Wizard starts.
4. Verify that the "Browse for file on node" setting specifies the machine name of the server on which WebSphere is installed.
5. At the "Install Applications (\*.ear)-Path" field, browse to the Sametime EAR file.

**Note:** The Sametime EAR file is located in the c:\WebSphere\AppServer\InstallableApps directory.

6. Select the Sametime EAR file and click **Open**.

7. In the "Application name:" field, enter a name for your application. The name is at your discretion. For example, enter "Sametime Enterprise Meeting Server." Click **Next**.
8. In the "Mapping Users to Roles" dialog box, ensure the "stadmin" and "stservices" roles are mapped to the "stadmins" group under the Users/Groups column. Click **Next**.

**Note:** If the Users/Groups column has a blank entry associated with the "stadmin" and "stservices" roles, the "stadmins" group does not exist in the LDAP directory. Create the "stadmins" group in the LDAP directory and restart this procedure or assign an individual user name or group name to the "stadmin" and "stservices" roles. To assign an individual user name to the "stadmin" and "stservices" roles:

From the "Mapping Users to Roles" dialog box:

- Select the **stadmin** role.
  - Click **Select**.
  - Choose **Select users groups**.
  - Select an individual user from the Available Users/Groups column.
  - Click **Add** to move the user to the Selected User/Groups column.
  - Click **OK**.
  - Repeat this process for the "stservices" role. Assign the "stservices" role to the same user to whom you assigned the "stadmin" role.
9. Click **Next** in each of the following dialog boxes:
    - Mapping EJB RunAs Roles to Users (This dialog box should contain no entries. Click **Next**.)
    - Binding Enterprise Beans to JNDI Names (This dialog box should contain no entries. Click **Next**.)
    - Mapping EJB References to Enterprise Beans (This dialog box should contain no entries. Click **Next**.)
    - Mapping Resources References to Resources (This dialog box should contain several entries. Click **Next**.)

**Note:** If you have not followed the suggested default settings provided in the previous steps, or if you have incorrectly typed required case-sensitive names or file paths, you cannot proceed past the "Mapping Resources References to Resources" dialog box. You might want to review your entries in the previous procedures if you are unable to proceed past this point.

10. Click **Next** in the following dialog boxes:
  - Specifying Default Datasource for EJB Modules (This dialog box should contain no entries. Click **Next**.)
  - Specifying Data Sources for individual CMP Beans (This dialog box should contain no entries. Click **Next**.)

11. In the "Selecting Virtual Host for Web Modules" dialog box, ensure that "Sametime," "stadmin," and "stserver," are listed in the Web Modules and that the Virtual Host value is correct. Click **Next**.  
**Note:** In this example, the correct Virtual Host value is "default\_host." If you have an existing environment in which multiple virtual hosts are defined, you can use a different virtual host value.
12. In the "Selecting Application Servers" dialog box, you must assign each EMS module to the appropriate WebSphere Application Server. The "Sametime" and "Stserver" modules are associated with the Default Server. The "stadmin" module is associated with the Stadmin server. Follow the instructions below:
  - Select the **Sametime** module.
  - Click **Select Server....**
  - Select **DefaultServer[MACHINE NAME]**, where MACHINE NAME is the server name of the WebSphere/EMS server.
  - Click **OK**.
  - Select the **stadmin** module.
  - Click **Select Server....**
  - Select **Stadmin[MACHINE NAME]**.
  - Click **OK**.
  - Select the **stserver** module.
  - Click **Select Server....**
  - Select **DefaultServer[MACHINE NAME]**.
  - Click **OK**.
13. Click **Next**.
14. Click **Finish**. When the installation completes, a message appears indicating the installation completed successfully. Click **OK**.

### **Start the Default Server and stadmin application servers**

After you have deployed the Sametime EAR file, use the WebSphere Administrator's Console to start both the Default Server and stadmin application servers.

### **Add the Sametime servers to the EMS 3.0 IF1 application**

Adding the upgraded Sametime 6.5.1 servers to the EMS 3.0 IF1 application is the eleventh of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

At this point you have deployed the EMS on the WebSphere server. To complete the upgrade process, you must add the upgraded Sametime 6.5.1 servers to the EMS to create the Meeting Services cluster.

This task is described in five steps:

1. Synchronize Single Sign-On (SSO) support for the EMS and Sametime servers.
2. Edit the Sametime.ini file on the Sametime servers.

3. Edit the MeetingServices document in the Configuration database on the Sametime server.
4. Add the Sametime server using the Sametime EMS Administration Tool.
5. Specifying Usage Limits and Denied Entry settings for the Sametime server.

### **Synchronizing Single Sign-On (SSO) support for the EMS and Sametime servers**

Synchronizing the Single Sign-On (SSO) support for the EMS and Sametime servers is the first of five steps required to add a Sametime server to the EMS 3.0 IF1.

This step ensures that the same LTPA keys are used to authenticate both client access to the EMS on the WebSphere server and client access to the Sametime servers.

**Note:** This step is required even if you allow all users to access the EMS anonymously.

To synchronize the SSO support you must export the LTPA Key file from the WebSphere server and import it to the Sametime server that is being added to the Meeting Services cluster. Both of these procedures are described below.

#### **Exporting the LTPA Key file from the WebSphere server**

To export the LTPA Key file from the WebSphere server:

1. Start the WebSphere Administrator's Console.  
From the Windows desktop, choose **Start > Programs > IBM WebSphere Application Server V4.0 AE > Administrator's Console**.
2. Select **Console > Security Center** from the WebSphere Administrative Console menu bar.
3. Select the **Authentication** tab.
4. In the LTPA Settings box, select the **Export key...** button.

**Note:** In the LTPA Settings box, note the values specified in the Token Expiration field (default 120 minutes) and the Domain field. You must specify the same token expiration period and domain name when importing these keys to the Sametime server.

5. In the Export to a file dialog box, specify a file name and location. This file will contain the LTPA keys. You can use any file name and extension (for example, EMS.keys).

You will need to import this file to the Sametime server that is being added to the Meeting Services cluster. You should export the file to a diskette or a network drive and directory that is accessible from the Sametime server.

6. Click **Save** to save the file.
7. Click **Cancel** to close the "Export to a file" dialog box.

#### **Importing the LTPA Key file to the Sametime server**

The Sametime server installation creates a Domino LTPA key by default. Note that this Domino LTPA key is reset when you import the WebSphere LTPA Key file to the Sametime server. It is not necessary to delete the existing Domino LTPA key before importing the WebSphere LTPA Key file.

## Importing the WebSphere LTPA Key file

To import the WebSphere LTPA Key file, you must create a new Domino Web SSO Configuration document in the Domino Directory on the Sametime server. This new document includes the following fields, which must contain values that are identical to the values that were specified when the WebSphere LTPA keys were created:

- **Token Domain** - The Token Domain field specifies the DNS domain name in which the EMS server and Sametime servers operate. The token domain does not include a specific host name. An example entry is `ibm.com`.

Make sure that the entry in the Token Domain field of the Web SSO document is the same as the entry you specified in the Domain field of the Authentication tab in the WebSphere Security Center component of the WebSphere Administrator's Console.

- **Expiration** - The Expiration field specifies the length of time for which an SSO token is valid.

This Expiration value must also match the expiration value you specified in the Token Expiration field on the Authentication tab in the WebSphere Security Center.

**Note:** The instructions provided in "Exporting the LTPA Key file from the WebSphere server" above explain how to determine the Token Domain and Expiration values that were specified for the WebSphere LTPA keys.

After you have created the new Domino Web SSO Configuration document with the appropriate Token Domain and Expiration values, you can import the WebSphere LTPA keys by entering the LTPA password that you specified when creating the WebSphere LTPA keys. This password was specified when you enabled WebSphere security and LDAP directory access during the WebSphere server installation.

To create the Domino Web SSO Configuration document and import the WebSphere LTPA keys:

1. In the Domino Directory, select **Server > Servers** to open the Servers view.
2. From the Servers view, select the **Web...** pull-down menu button.
3. Select **Create Web SSO Configuration**.
4. Complete the following fields in the Web SSO Configuration document. The values entered in these fields must be identical to the values that were entered when you created the WebSphere LTPA keys following the WebSphere installation.
  - **Token Domain** - The domain entered in this field must be identical to the domain specified for the WebSphere LTPA keys, as noted above.
  - **Expiration** - The value entered in this field must be identical to the value specified for the WebSphere SSO token. The suggested value is 120 minutes.
  - **Domino Server Names** - This field should contain the names of all Sametime servers that are part of the Sametime community in which the Meeting Services cluster operates. The server names must be entered in the Domino server name format (for example, `Sametimeserver1/East/Acme`). You can browse the Domino Directory to add the server names to this field.
5. Select the **Keys > Import WebSphere LTPA Keys** menu option.

6. In the Enter Import File Name dialog box, type the directory path to the WebSphere LTPA key file you exported from the WebSphere server. This directory path should specify a network location or the floppy disk to which you copied the WebSphere LTPA file.
7. In the Enter Import File Password dialog box, enter the password associated with the WebSphere LTPA import file.
8. A "Successfully imported WebSphere LTPA keys" message appears on the screen. Click **OK**.
9. After the WebSphere LTPA keys have been imported, a WebSphere Information section appears in the Domino Web SSO Configuration document. You must alter the entry that appears in the LDAP Realm field of the WebSphere Information section.

In the LDAP Realm field, the LDAP server name will appear in one of the following formats (assuming the LDAP server name is ldap1.acme.com):

- ldap1.acme.com
- ldap1.acme.com:389

**Important:** If the LDAP server name has the port number appended (for example, ldap1.acme.com:389), you must alter the LDAP Realm entry so that a back-slash character ( \ ) appears after the LDAP server name but in front of the colon. For example, if your LDAP server name is ldap1.acme.com, the correct entry in the LDAP Realm field is "ldap1.acme.com\ :389".

If the LDAP server name does not have the port number appended (for example, ldap1.acme.com), do not alter the entry in the LDAP Realm field. Leave the entry as "ldap1.acme.com" in the LDAP Realm field.

10. Click **Save and Close** to save the Web SSO Configuration document.

**Note:** Each Sametime server that you will add to the EMS must have a copy of the Web SSO Configuration document and the LTPA keys. Ensure that the Domino Directory to which you have imported the LTPA keys replicates to each Sametime server that you will add to the EMS.

### **Editing the Sametime.ini file on the Sametime servers**

Editing the Sametime.ini file on the Sametime servers is the second of five steps required to add a Sametime server to the EMS 3.0 IF1.

Each Sametime server that is added to the EMS contains processes that must access a configuration servlet on the EMS machine. The Sametime servers must authenticate when accessing the configuration servlet. To ensure that each Sametime server can authenticate, you must enter a user name and password in the Sametime.ini file on the Sametime server.

The user name and password you enter in the Sametime.ini file on each Sametime server should be the same user name and password that was entered in the "Sametime Administrator Information" screen when you installed the Enterprise Meeting Server 3.0 IF1 files.

To add the user name and password to the Sametime.ini file on each Sametime server:

1. Use a text editor to open the Sametime.ini file located in the C:\Lotus\Domino directory.
2. At the bottom of the [Config] section of the Sametime.ini file, manually type the following entries into the file:
  - SametimeAdminUsername=
  - SametimeAdminPassword=

Populate the entries with the same user name and password that you entered in the "Sametime Administrator Information" screen when you installed the EMS files. For example, if you created a special directory account for Sametime configuration servlet access named "Sametime Servlet Access" with a password of "sametime," populate the entries as follows:

- SametimeAdminUsername=Sametime Servlet Access
  - SametimeAdminPassword=sametime
3. Save the Sametime.ini file.
  4. Repeat this procedure on every Sametime server that you want to add to the EMS.

**Note:** In a subsequent procedure, you will reboot the Sametime server. After you reboot the server, the SametimeAdminUsername and SametimeAdminPassword entries are encrypted and the user name and password will not be visible in the Sametime.ini file.

### **Editing the MeetingServices document in the Configuration database on the Sametime server**

Editing the MeetingServices document in the Configuration database on the Sametime server is the third of five steps required to add a Sametime server to the EMS 3.0 IF1.

Editing the MeetingServices document involves adding a user name and password to four different sections of the MeetingServices document. Adding the user name and password to the MeetingServices document ensures that processes on the EMS can authenticate when accessing the Meeting Management API (MMAPI) on the Sametime server.

The user name and password you enter in the MeetingServices document should be the user name and password of an LDAP directory account that is used strictly for the purpose of authenticating EMS processes that access the MMAPI on the Sametime server. The example below assumes you have created an LDAP directory account with a user name of "Meeting Management Access" and a password of "sametime" for this purpose.

**Note:** For more information about the LDAP directory accounts required by the EMS, see the topic "Create or identify the required LDAP directory accounts" in "Chapter 19 – Setting up the Enterprise Meeting Server and a Meeting Services cluster" in the *IBM Lotus Instant Messaging and Web Conferencing 6.5.1 and Enterprise Meeting Server 3.0 IF1 Administrator's Guide* (sthelapad.pdf) provided with the EMS software.

To edit the MeetingServices document:

1. Add the LDAP directory account user name (for example "Meeting Management Access") to the ACL of the Configuration database (stconfig.nsf) on the Sametime server. Provide this user name with the Manager access level. Also, assign all available Roles in the stconfig.nsf database ACL to the user name.

**Note:** The LDAP directory account used in step 1 should exist solely for the purpose of authenticating access to the MMAPi, as noted earlier in this topic.

2. Use a Lotus Notes client to open the Configuration database (stconfig.nsf) on the Sametime server.
3. In the Configuration database, open the MeetingServices document (by double-clicking on the date associated with the document).
4. Scroll to the "Remote Service Access" section at the bottom of the MeetingServices document.
5. Populate the eight fields in the "Remote Service Access" section with the user name and password you created for this purpose. For example:

Meeting Management Username Meeting Management Access  
Meeting Management Password sametime

Recorded Meeting Management Username Meeting Management Access  
Recorded Meeting Management Password sametime

Materials Refresh Username Meeting Management Access  
Materials Refresh Password sametime

Materials Control Username Meeting Management Access  
Materials Control Password sametime

6. Save the Meetingservices document and close the Configuration database.

**Note:** In the next procedure, you will reboot the Sametime server. The Sametime server must be rebooted before the user name and password can be used to authenticate access to the MMAPi.

## **Add the Sametime server using the Sametime EMS Administration Tool**

Adding a Sametime server using the Sametime EMS Administration Tool is the fourth of five steps required to add a Sametime server to the EMS 3.0 IF1.

To add a Sametime server to the EMS:

1. Verify that both the EMS application server and the Sametime EMS Administration Tool application server are running on the EMS machine. In this example, the EMS runs on the WebSphere application server named "Default Server" and the Sametime EMS Administration Tool runs on the WebSphere application server named "stadmin." If either of these application servers are stopped when the Sametime server is added to the EMS, the Sametime server will not function.

To verify that both the "Default Server" and "stadmin" application servers are running, do the following:

- Open the WebSphere Administrator's Console on the EMS machine.
  - Expand the node on which the EMS is installed.
  - Right-click on the **Default Server** application server.
  - If the "Start" menu item is grayed out, the Default Server is running. If the "Start" menu item is not grayed out, click on it to start the Default Server.
2. Enter the following URL in a Web browser to browse to the Sametime EMS Administration Tool:  
  
http://<Fully-qualified DNS name of the EMS machine>/iwc-admin (for example, enter http://sametime.ems.ibm.com/iwc-admin)
  3. Enter an administrator user name and password to access the Sametime EMS Administration Tool.  
  
**Note:** To access the Sametime EMS Administration Tool, the user must be a member of the "stadmins" group in the LDAP directory used in your Sametime environment.
  4. Select **Configuration > Meeting Cluster**. (This tab may be displayed by default when you open the Sametime EMS Administration Tool.)
  5. In the "Host name, IP address, or full URL of the additional server" field, enter the Host name, IP address, or full URL of the Sametime server that is to be added to the EMS and click **Add**.
  6. When you see the message indicating the Sametime server is successfully added to the Meeting Services cluster, reboot the Sametime server you have just added to the Meeting Services cluster.
  7. Repeat this procedure for each Sametime server you want to add to the EMS.

## **Specifying Usage Limits and Denied Entry settings for the Sametime servers**

Specifying Usage Limits and Denied Entry settings for the Sametime servers is the last of five steps required to add a Sametime server to the EMS 3.0 IF1.

The Usage Limits and Denied Entry settings for the Sametime servers are set from the Configuration > Meeting Cluster > Edit/Remove a Meeting Cluster tab of the Sametime EMS Administration Tool.

After you have added an upgraded Sametime server to the EMS, you can accept the default Usage Limits and Denied Entry settings and continue to the next task, or you can adjust the Usage Limits and Denied Entry settings as needed for your environment.

For detailed information about changing the Usage Limits and Denied Entry settings, see the topic "Specifying Usage Limits and Denied Entry settings for the Sametime server" in "Chapter 19 – Setting up the Enterprise Meeting Server and a Meeting Services cluster" in the *IBM Lotus Instant Messaging and Web Conferencing 6.5.1 and Enterprise Meeting Server 3.0 IF1 Administrator's Guide* (sthelapad.pdf) provided with the EMS software.

## **Securing end user access to the EMS**

Securing end user access to the EMS is the last of twelve tasks required to upgrade the EMS 1.0 to EMS 3.0 IF1.

The default security settings of the EMS 3.0 IF1 enable any anonymous user to access the EMS application. If you want users to authenticate to access the EMS, or authenticate to perform specific tasks on the EMS, you must secure end user access to the EMS.

To secure end user access to the EMS, see the topic "Securing user access to the Enterprise Meeting Server" in "Chapter 21 – Setting up security for the Enterprise Meeting Server" of the *IBM Lotus Instant Messaging and Web Conferencing 6.5.1 and Enterprise Meeting Server 3.0 IF1 Administrator's Guide* (sthelpad.pdf) provided with the EMS software.

## Performance enhancement tips

In EMS 3.0 IF1 testing, the following configuration adjustments have improved EMS performance. Note that these configuration adjustments are only suggestions for improving performance and may not improve performance in all environments.

### Altering maxSearchResults and allowEmptySearchStrings

LDAP performance may improve if you alter the maxSearchResults and allowEmptySearchStrings settings in the directory.config file on the WebSphere server.

In the directory.config file, you should set the maxSearchResults to a value less than 100 and set allowEmptySearchStrings to 0 (zero). Some experimentation with the maxSearchResults setting may be required to find the value appropriate for your environment.

The directory.config file is located in the following directory on the WebSphere server:

C:\WEBSHERE INSTALL PATH\InstalledApps\<<EAR-FILE>\<WAR-FILE>\WEB-INF\classes\config\

For example, to alter the maxSearchResults and allowEmptySearchStrings settings:

1. Use a text editor to open the directory.config file in the C:\WebSphere\AppServer\installedApps\Sametime.ear\stadmin.war\WEB-INF\classes\config\ directory.
2. In the directory.config file set:
  - maxSearchResults=80
  - allowEmptySearchStrings=0
3. Save and close the directory.config file.

### Altering Sametime Directory Assistance

LDAP performance may also improve if you alter the "Deference alias on search" setting in the Directory Assistance database (da.nsf) on a Sametime server that has been added to the EMS.

To alter this setting:

1. Use a Lotus Notes client to open the Directory Assistance database on a Sametime server that has been added to the EMS.
2. Click on the LDAP tab.
3. Change the "Deference alias on search" setting to "never."
4. Save the change and restart the Domino/Sametime server.

### Altering minimum and maximum thread sizes

EMS performance may improve if you alter the minimum and maximum thread sizes from the WebSphere Administration Tool.

To alter the minimum and maximum thread sizes:

1. Open the WebSphere Administrator's Console on the WebSphere/EMS computer.
2. Right click on the Default Server application server that contains the EMS (or other application server you want to modify).
3. Select Properties.
4. Select the Services tab.
5. Choose Web Container Service.
6. Click the Edit properties button.
7. Modify the minimum and maximum thread sizes to values that are appropriate for your system.

## Known Issues

The known issues are categorized as follows:

- Installation issues
- LDAP Directory issues
- Meeting Center and Meeting issues
- Administration issues
- International issues

## Installation issues

### Do not create the virtual organization when setting up the EMS

The *Instant Messaging and Web Conferencing (Sametime) 6.5.1 and Enterprise Meeting Server 3.0 IF 1 Administrator's Guide* includes instructions that explain how to set up the Enterprise Meeting Server 3.0 IF1 and a Meeting Services cluster.

The final task in these instructions is titled "Creating the Virtual Organization." This task is not needed to set up the EMS. Do not attempt to create the virtual organization when installing and setting up the EMS.

Note that omitting this task from the EMS setup affects the URL that users enter in a Web browser to access the EMS Welcome page after the EMS set up is complete. When the EMS setup is complete, users must enter the following URL in the Web browser to access the EMS Welcome page:

[http://<ems\\_server\\_name>/iwc/center](http://<ems_server_name>/iwc/center)

**Note:** Do not use the URL documented in the *Instant Messaging and Web Conferencing (Sametime) 6.5.1 and Enterprise Meeting Server 3.0 IF 1 Administrator's Guide* when attempting to access the EMS Welcome page.

### Compiling JSPs after EMS installation optimizes 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  
SPR #MJON5E3M53
```

## 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.

SPR #STER5FE9TK

## Domino and Sametime processes hang after installing additional Sametime server

A problem may occur when installing an additional Sametime server where the Domino and Sametime processes hang after an additional Domino/Sametime server is installed.

The example below illustrates this problem.

1. Install Domino as an additional server.
2. Replicate the Domino Directory from an existing Sametime/Domino server during the server installation.
3. Install Sametime on the additional Domino server.
4. Some Domino and Sametime services will not start properly and Sametime does not work.

To prevent this problem you must make sure that the server.id of the additional Domino server is not password protected. To disable password protection of the server.id file on the additional Domino server, open a Notes client on the Domino server and select File – Tools – User ID – Clear Password.

SPR #NKUO5FFG2K

## LDAP Directory issues

### 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.

SPR #TCAL5FKLHR

### **“Update Security Configuration Failed” message when enabling LDAP Directory Access for WebSphere**

*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 “kmliller.”
- 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 “kmliller,” 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 3.0 and Enterprise Meeting Server 1.0 Administrators Guide (sthelapad.pdf or sthelapad.nsf) available with the EMS.  
SPR #DHOD5FPSGZ

## **Administration issues**

### **User with a person entry in the 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.

SPR #JDUM5G2HYM

### **The stadmin application server must be started before a Sametime server is started**

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.

SPR #STER5DA3L4

### **Not always necessary to restart a Sametime server after changing administration 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.

SPR #CPRE5EYKQD

### **Some of the Usage Limits and Denied Entry settings are not hard limits**

The Sametime EMS Administration Tool contains Usage Limits and Denied Entry settings. The primary purpose of these settings is to enable the administrator to impose maximum limits on specific server activities. Limiting server usage in this way can prevent a high demand for these activities from overwhelming the system or network resources.

**Note:** The Usage Limits and Denied Entry settings are available from the Configuration – Meeting Cluster – Edit/Remove a Meeting Server tab of the Sametime EMS Administration Tool.

Some of the Usage Limits and Denied Entry settings impose hard limits on server activity and other settings impose soft limits. A hard limit is a limit that will prevent a specific activity from occurring once the administrator-specified threshold is reached. A soft limit is a limit that is used by other software components of the EMS (such as the Booking Agent) with the intent of preserving system resources. Soft limits can be exceeded. In some cases, warning messages may appear to the user or be written in Sametime logs when a soft limit is exceeded.

The lists below show which of the Usage Limits and Denied Entry settings impose soft limits and hard limits on Sametime server activities.

The soft limits include:

- Set a maximum number of scheduled meetings allowed on the server
- Set a maximum number of participants in any one meeting
- Set a maximum number of participants on the server

The soft limits above are used by the components of the EMS (such as the Booking Agent) when scheduling and starting meetings on Sametime servers in the server cluster. These limits are implemented as soft limits because some flexibility is needed to accommodate brief periods of over capacity.

The following example illustrates why soft limits are imposed for these settings. Assume Meeting A is scheduled to end at 10:30 AM but runs longer than expected. Meeting B is scheduled to start at 10:30 AM but when Meeting B starts exceeds the soft limits imposed by the administrator (because Meeting A did not end as scheduled). In this scenario, Meeting B is allowed to start even though the limits are exceeded. Imposing a hard limit in such a scenario introduces too much unpredictability for scheduled meetings and server failover situations. For these and similar reasons, soft limits are used for the Usage Limits and Denied Entry settings listed above.

The hard limits include:

- Set a maximum number of instant meetings allowed on the server
- Set a maximum number of interactive audio connections for all instant meetings on the server
- Set a maximum number of interactive video connections for all instant meetings on the server
- Set a maximum number of interactive audio connections for all scheduled meetings on the server
- Set a maximum number of interactive video connections for all scheduled meetings on the server
- Set a maximum number unicast audio streams for all broadcast meetings
- Set a maximum number unicast video streams for all broadcast meetings

Hard limits are imposed for these settings for the reasons noted below.

The spontaneous and unpredictable nature of instant meetings makes it impossible to manage over-capacity scenarios. When the maximum number of instant meetings across all servers in the cluster has been reached, instant meetings are no longer allowed on the server.

Hard limits are imposed on the audio/video activities to enable the administrator to manage the network bandwidth consumption of these activities. Generally, the audio/video streams rely on the User Datagram Protocol (UDP). UDP packets are generally considered low priority by network components and are the first to be discarded on a congested network. Soft limits are not appropriate for the settings that control the level of audio/video activity. (If the soft limits were exceeded, the network congestion increases and audio/video UDP packets are more likely to be discarded due to network congestion. In this scenario, users may be unable to receive the audio/video streams if you allow the limits to be exceeded).

Providing hard limits for the settings that control number of audio/video connections and broadcast streams enables the administrator to control the network bandwidth consumed by these streams. The administrator should consider the bandwidth-handling capabilities of the network when setting limits on audio/video connections and broadcast meeting streams.

Note that when the maximum number of audio/video connection limits are reached, users may be able to attend meetings and receive meeting data (such as screen sharing and question and answer data), but will be unable to receive the audio/video data.

SPR #RMAN5G8RHY

## Meeting Center and Meeting issues

### 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.

SPR #GECI5FCCDT

### Reattaching edited whiteboard files to a meeting

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.

If you want to edit an attached whiteboard file, you should rename the file, edit the file, and then attach the renamed and edited file to the meeting.

SPR #BCOL5FT24B

## International issues

### Installing the JMS Providers with the Simplified Chinese, Traditional Chinese, or Korean language operating system

*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 3.0 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**.

SPR #GECI5FG6N5

### **Double-Byte Character Set (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.

### **Problem installing the JMS providers when deploying EMS on a Spanish language version of 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 "Instaler 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.

SPR #ODAY5EKEBT

## **User names with accented characters may cause a WebSphere login failure**

If a WebSphere server uses the Greek, Eastern European, Russian, or Turkish 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. This same problem also occurs for user names with DBCS characters.

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 publication date for these release notes. It is uncertain whether this problem will be resolved in the released product.

SPR #SSCN5DMHUB

## **Anonymous meeting moderator cannot edit a meeting, change meeting duration, or delete a meeting**

This release note pertains to the following language versions of the EMS:

- Brazilian Portuguese
- French
- Italian
- Spanish
- Danish
- Dutch
- Norwegian
- Finnish
- Japanese (and other languages that use DBCS)

If an anonymous (unauthenticated) user accesses the Meeting Center on the EMS and creates a meeting that specifies an "Anonymous" moderator, the user will be unable to edit the meeting details for the meeting, change the meeting duration, or delete the meeting. The example below illustrates this problem.

1. An anonymous user accesses the EMS Meeting Center and creates a meeting with a moderator setting of "Anonymous."
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.

SPR #NKUO5G3CWS, GECI5FW7T3

### **A user that is a member of a group that has a name that uses DBCS characters cannot log in to the Sametime EMS Meeting Center**

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.

SPR #STTE5DXE4R

### **Name display problems caused by directory entries that use mixed code pages**

If the LDAP directory accessed by the EMS contains user names that use different character sets (for example Greek and Czech), EMS users will experience name display problems when viewing these names from EMS user interfaces (such as the "Add to Invitation List" dialog in the Meeting Center). For example, users may see names interspersed with garbage characters.

**Note:** EMS users may view names in the directory when inviting specific users to a meeting.

In cases where a directory contains user names that use different character sets, the characters that display correctly depend on the locale settings of the operating system on the client machine. For example, if the directory includes names that use Greek and Czech character sets, the Greek names will display correctly for users that have Greek specified as the locale for the operating system. The Czech names will not display correctly for for users that have Greek specified as the locale for the operating system. There is no workaround for this problem.

SPR #DSCY5DHKEG

## Documentation Corrections

All documentation corrections pertaining to the EMS 3.0 IF 1 are listed below.

### **Incorrect version of WebSphere MQ documented in administrator's guide**

The *IBM Lotus Instant Messaging and Web Conferencing (Sametime) 6.5.1 Administrator's Guide* states that you must use the IBM WebSphere MQ V5.3.1 server with the EMS 3.0 IF 1. This requirement is incorrect. You must use the IBM WebSphere MQ V5.3.0.7 server (WebSphere MQ 5.3 with WebSphere MQ Fix Pack 7 installed) with the EMS 3.0 IF 1.

You can obtain the WebSphere MQ Fix Pack 7 (CSD07) from the following web site:

[http://www.ibm.com/support/docview.wss?rs=0&q1=WebSphere+MQ&uid=swg24007281&loc=en\\_US&cs=utf-8&cc=us&lang=en](http://www.ibm.com/support/docview.wss?rs=0&q1=WebSphere+MQ&uid=swg24007281&loc=en_US&cs=utf-8&cc=us&lang=en)

The installation instructions for WebSphere MQ Fix Pack 7 are also provided at this web site.