# Contents

## Chapter 1. Administering  
1

- Starting and stopping servers  
1
- Sametime component URLs  
6
- Adding administrators  
9
- Changing the administrator password  
10
  - Updating your DB2 administrator password  
10
  - Updating your LDAP Bind password  
10
  - Updating your WebSphere Application Server administrator password  
11
- Managing users with policies  
12
  - Finding policies associated with a user  
13
  - Creating new user policies  
13
  - Assign users and groups to policies  
15
  - Changing a user policy’s weight  
36
  - Using nested groups in policy assignments  
37
- Administering a Sametime System Console  
39
  - Backing up the console database  
39
- Administering a Sametime Community Server  
40
  - Managing administrator access and roles  
40
  - Managing trusted IP addresses  
51
  - Managing community services  
52
  - Managing anonymous access to virtual places  
58
  - Sending a message to all users  
59
  - Managing business cards  
60
  - Changing user names  
85
  - Changing the IP address of an IBM i Sametime Community Server  
105
  - Changing the host name of an IBM i Sametime Community Server  
105
  - Monitoring the Sametime Community Server  
107
- Administering a Sametime Proxy Server  
114
  - Updating Sametime Proxy Server connection properties on the console  
114
- Administering a Sametime Media Manager  
115
  - Updating Sametime Media Manager connection properties on the console  
115
  - Managing UDP ports for voice chat and video calls  
116
  - Managing multiple audio and video streams  
117
  - Changing the SIP transport protocol in the Sametime Media Manager  
118
  - Managing media encryption and codecs  
119
  - Changing the default number of maximum users  
120
- Administering a SIP Proxy and Registrar  
121
  - Updating SIP Proxy and Registrar connection properties on the console  
122
- Monitoring bandwidth usage for individual links  
132
- Monitoring bandwidth usage for sites  
133
- Monitoring calls for selected links  
133
- Monitoring calls for selected sites  
134
- Bandwidth Manager statistics  
135
- Administering a Sametime Meeting Server  
137
  - Updating Sametime Meeting Server connection properties on the console  
137
  - Managing file sharing  
138
  - Requiring meeting passwords  
139
  - Limiting guest access to the Meeting Room Center  
140
  - Defining a Sametime Proxy server for awareness in meeting rooms  
141
  - Customizing the Sametime Meeting Server configuration  
142
  - Turning on full-text indexing in the Meeting Room Center  
143
  - Monitoring meeting room statistics  
145
  - Backing up user data for Sametime meeting rooms  
145
- Administering a Sametime Gateway Server  
146
  - Updating Sametime Gateway Server connection properties on the console  
146
  - Assigning users access to external communities  
147
  - Enabling spam filtering  
149
  - Maintaining and monitoring Sametime Gateway Reference  
150
- Administering Widgets and Live Text  
193
  - Widgets and Live Text overview  
194
  - Creating the widget catalog  
200
  - Embedded ST Only: Controlling Widgets and Live Text access using Domino policy  
204
  - Controlling Widgets and Live Text access using Eclipse preferences  
209
  - How do I create a Features and Plugins deployment widget?  
215
  - Creating a features and plugins deployment widget  
217
  - Deploying client plug-ins with widgets and the widget catalog  
217
  - Using public widget provider APIs  
230
  - Specifying Widget settings for a desktop policy  
231
  - Backing up WebSphere Application Server configurations  
236

## Chapter 2. Performance  
239

- Increasing the number of open files on a Sametime server running on Linux  
239
- Tuning a Sametime Community Server  
240
  - Tuning Sametime LDAP settings  
240
  - Advanced settings to control contact list size  
244
  - Setting a Sametime Polling “Keep Alive” interval for client requests  
245
Chapter 3. Security ................................................. 265
Working with Sametime servers that are enabled for SSL ................................................. 265
  Configuring Sametime Community Server to use SSL encryption ............................. 265
  Configuring Transport Layer security for the Sametime Media Manager .................. 296
  Configuring Transport Layer security for the Sametime Bandwidth Manager .......... 303
  Configuring Sametime Meeting Server for secure access to an LDAP repository .......... 307
  Replacing the default IBM self-signed certificate with another certificate ............... 307
  Adding a Sametime server SSL certificate to the Sametime System Console .............. 308
  Importing an SSL certificate from Sametime Unified Telephony .............................. 309
  Configuring TLS/SSL for Sametime Gateway ......................................................... 310
  Setting up compliance for FIPS 140-2 ................................................................. 332
  Installing the FIPS administration portlet ......................................................... 332
  Installing the FIPS Server ................................................................................. 333
  Setting up single sign-on (SSO) for Sametime clients ........................................... 335
  Preparing servers running on WebSphere Application Server for single sign-on ........ 335
  Configuring the Sametime Community Server for single sign-on ......................... 336
  Importing a shared LTPA key to enable SSO for a server in a different cell .............. 337
  Verifying that servers have the same single sign-on settings .................................. 338
  Configuring single sign-on with WebSphere Portal ............................................. 338
  Configuring single sign-on with Microsoft Windows Active Directory .................. 340
  Configuring security for the Sametime Community Server .................................... 341
  Authentication by token using LTPA and Sametime tokens .................................... 341
  Working with Sametime security .......................................................................... 353

Chapter 4. Troubleshooting and support ............................................................... 375
Troubleshooting Sametime clients ................................................................. 375
  Logging and tracing on Sametime Connect ....................................................... 375
  Locating the Sametime Connect workspace ...................................................... 376
  Troubleshooting audio and video in the Sametime Connect client ....................... 379
  Troubleshooting the Sametime web audio-visual plugin ...................................... 380
  Troubleshooting meeting invitations ................................................................... 384
  Troubleshooting Business Cards ........................................................................ 384
  Troubleshooting a Sametime System Console .................................................... 386
  Sametime System Console log locations ............................................................... 386
  Determining Sametime server status using the Integrated Solutions Console ..... 387
  The console.properties file ............................................................................... 387
  The productConfig.properties file for WebSphere-based servers ...................... 388
  The productConfig file for the Sametime Community server ............................... 391
  Troubleshooting clustering ................................................................................. 391
  Troubleshooting a Sametime Community Server .................................................. 392
  Troubleshooting general issues in the Sametime Community Server ..................... 393
  Troubleshooting login issues with the Sametime Community Server ..................... 397
  Troubleshooting LDAP in Sametime ................................................................. 398
  Troubleshooting network issues on the Sametime Community Server ................ 398
  Troubleshooting a Sametime Proxy Server ......................................................... 402
    Enabling logging and tracing for a Sametime Proxy Server ............................... 402
  Troubleshooting a Sametime Media Manager ...................................................... 403
    Setting a diagnostic trace on a Sametime Media Manager server ..................... 403
    Gathering Sametime Media Manager logs and traces for IBM Support .......... 404
  Troubleshooting a Sametime Media Manager using JVM logs .............................. 405
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting video quality</td>
<td>406</td>
</tr>
<tr>
<td>Troubleshooting Sametime Media Manager component clusters</td>
<td>406</td>
</tr>
<tr>
<td>Troubleshooting Sametime Bandwidth Manager</td>
<td>408</td>
</tr>
<tr>
<td>Setting a diagnostic trace on a Sametime Bandwidth Manager</td>
<td>408</td>
</tr>
<tr>
<td>Troubleshooting using JVM logs</td>
<td>409</td>
</tr>
<tr>
<td>Troubleshooting using the Bandwidth Manager Monitor and Policy Testing tools</td>
<td>410</td>
</tr>
<tr>
<td>Troubleshooting Sametime Bandwidth Manager clusters</td>
<td>410</td>
</tr>
<tr>
<td>Troubleshooting a Sametime TURN Server</td>
<td>411</td>
</tr>
<tr>
<td>Troubleshooting a Sametime Meeting Server</td>
<td>412</td>
</tr>
<tr>
<td>Setting a diagnostic trace on a Sametime Meeting Server</td>
<td>412</td>
</tr>
<tr>
<td>Gathering Sametime Meeting Server logs and traces for support</td>
<td>413</td>
</tr>
<tr>
<td>Troubleshooting a Sametime Meeting Server using JVM logs</td>
<td>414</td>
</tr>
<tr>
<td>Troubleshooting a Sametime Meeting Server cluster</td>
<td>414</td>
</tr>
<tr>
<td>Troubleshooting a Sametime Gateway Server</td>
<td>415</td>
</tr>
<tr>
<td>Setting a diagnostic trace on Sametime Gateway</td>
<td>416</td>
</tr>
<tr>
<td>Setting a diagnostic trace for specific user names and domains</td>
<td>417</td>
</tr>
<tr>
<td>Troubleshooting Sametime Gateway using</td>
<td>420</td>
</tr>
<tr>
<td>Self-Service configuration tests</td>
<td>420</td>
</tr>
<tr>
<td>Gathering logs and traces for IBM support</td>
<td>421</td>
</tr>
<tr>
<td>Gathering performance data with the PMI tool</td>
<td>423</td>
</tr>
<tr>
<td>Troubleshooting installation</td>
<td>429</td>
</tr>
<tr>
<td>Troubleshooting WebSphere Application Server</td>
<td>430</td>
</tr>
<tr>
<td>Troubleshooting the Sametime Gateway using</td>
<td>430</td>
</tr>
<tr>
<td>JVM logs</td>
<td>430</td>
</tr>
<tr>
<td>Troubleshooting a failed WebSphere Application Startup</td>
<td>431</td>
</tr>
<tr>
<td>Troubleshooting starting a cluster</td>
<td>432</td>
</tr>
<tr>
<td>Troubleshooting secondary node problems</td>
<td>432</td>
</tr>
<tr>
<td>Troubleshooting connections to external communities</td>
<td>433</td>
</tr>
<tr>
<td>Troubleshooting message handlers</td>
<td>434</td>
</tr>
<tr>
<td>Troubleshooting slow or missing awareness changes</td>
<td>435</td>
</tr>
<tr>
<td>Troubleshooting XMPP and Google community connections and awareness</td>
<td>436</td>
</tr>
<tr>
<td>Error message severity levels and situations</td>
<td>437</td>
</tr>
<tr>
<td>Log file locations</td>
<td>439</td>
</tr>
<tr>
<td>Directory conventions</td>
<td>441</td>
</tr>
<tr>
<td><strong>Notices</strong></td>
<td>445</td>
</tr>
<tr>
<td><strong>Trademarks</strong></td>
<td>447</td>
</tr>
</tbody>
</table>
Chapter 1. Administering

IBM® Sametime administrators set up and maintain users and their ability to use Sametime features. They also maintain and monitor the servers.

This section contains information about user registration and policies and the tools that you can use to administer the server.

Starting and stopping servers

You may use a command window to start and stop Sametime® components running on WebSphere® Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Sequence for starting and stopping servers

Follow the sequence below when starting or stopping servers associated with a Sametime server.

Start server sequence
1. Start the Deployment Manager.
   - If you installed a server in a cell profile, the Deployment Manager is on the same machine as the Sametime server. If you installed a server in a cluster, the Deployment Manager is probably not on the same machine unless you are running on IBM i.
2. Start the node agent.
3. Start the Sametime server.

Stop server sequence
1. Stop the Sametime server.
2. Stop the node agent.
3. Stop the Deployment Manager.
   - If you installed a server in a cell profile, the Deployment Manager is on the same machine as the Sametime server. If you installed a server in a cluster, the Deployment Manager is probably not on the same machine unless you are running on IBM i.

Note: Before uninstalling WebSphere Application Server, you must stop the application server. If the server belongs to a cluster, you will also need to stop all node agents in the cluster, and then stop the Deployment Manager. Finally, close all browsers and command windows that may have been accessing the WebSphere Application Server.

Server command directories

Run the commands from a command window on the machine where the server is installed and navigate to the appropriate bin directory shown in the following table.
Table 1. Server command directories

<table>
<thead>
<tr>
<th>Type</th>
<th>Profile /bin directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stSSC_profile_root/bin</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stM_profile_root/bin</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stP_profile_root/bin</td>
</tr>
<tr>
<td>Media Manager</td>
<td>stMS_profile_root/bin</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stgw_profile_root/bin</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>stAdv_profile_root/bin</td>
</tr>
</tbody>
</table>

AIX®, Linux, or Solaris

Note: The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

Table 2. Start server commands for AIX, Linux, or Solaris

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Sametime System Console| ./startNode.sh  
                          | ./startServer.sh STConsoleServer             |
| Meeting Server         | ./startNode.sh  
                          | ./startServer.sh STMeetingHttpProxy          |
| Proxy Server           | ./startNode.sh  
                          | ./startServer.sh STMeetingServer             |
| Media Manager          | Linux only:  
                          | ./startNode.sh                             
                          | ./startServer.sh STMediaServer              |
| Sametime Gateway       | ./startNode.sh  
                          | ./startServer.sh RTCGWServer                |
| Sametime Advanced      | ./startNode.sh  
                          | ./startServer.sh STAdvancedServer           |

Note: Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

Table 3. Stop server commands for AIX, Linux, or Solaris

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Sametime System Console| ./stopServer.sh STConsoleServer   
                          | -username username -password password     |
|                        | ./stopNode.sh -username username             
                          | -password password                      |
Table 3. Stop server commands for AIX, Linux, or Solaris (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Server</td>
<td><code>.stopServer.sh STMeetingServer -username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopServer.sh STMeetingHttpProxy -username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Proxy Server</td>
<td><code>.stopServer.sh STProxyServer -username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Media Manager</td>
<td><code>.stopServer.sh STMediaServer -username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td><code>.stopServer.sh RTCGWServer -username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td><code>.stopServer.sh STAdvancedServer -username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
</tbody>
</table>

Windows

The Start Programs menu is also a convenient way to start and stop Sametime servers running on WebSphere Application Server.

Note: The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

Table 4. Start server commands for Windows

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STMeetingHttpProxy</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STMeetingServer</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STMediaServer</td>
</tr>
</tbody>
</table>
### Table 4. Start server commands for Windows (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Gateway</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STAdvancedServer</td>
</tr>
</tbody>
</table>

**Note:** Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

### Table 5. Stop server commands for Windows

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stopServer.bat STConsoleServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stopServer.bat STMeetingServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopServer.bat STMeetingHttpProxy -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stopServer.bat STProxyServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>stopServer.bat STMediaServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stopServer.bat RTCGWServer</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>stopServer.bat STAdvancedServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
</tbody>
</table>

### IBM i

**Note:** The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.
### Table 6. Start server commands for IBM i

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer STMeetingHttpProxy</td>
</tr>
<tr>
<td></td>
<td>startServer STMeetingServer</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Not supported on IBM i</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>Not supported on IBM i</td>
</tr>
</tbody>
</table>

**Note:** Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

### Table 7. Stop server commands for IBM i

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stopServer STConsoleServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stopServer STMeetingServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopServer STMeetingHttpProxy -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stopServer STProxyServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Not supported on IBM i</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stopServer RTCGWServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>Not supported on IBM i</td>
</tr>
</tbody>
</table>
Sametime component URLs

This section lists the URLs for IBM Sametime servers and components.

The following table lists the URLs for logging in to Sametime:

Table 8. Sametime URLs

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A single Integrated Solutions Console URL is only applicable if you deploy a cluster and choose to use the Sametime System Console as the Deployment Manager for all Sametime products.

For IBM i, the port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary. To check the port, open the /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt file and use the setting specified for the "Administrative console port." For the default profile name (STSCDmgrProfile), the file is located here:

/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt
<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
</table>

The default port is 9060 for all platforms except IBM i.

For IBM i, the port number may not be 9060. To check the port, open the logs/AboutThisProfile.txt file for the Websphere Application Server profile that is running the ISC for your Gateway server and use the setting specified for the "Administrative console port."

If you have installed a single Sametime Gateway server, this will be the one Sametime Gateway profile you have. If you have a cluster setup, this profile will be the Deployment Manager profile that your Sametime Gateway server has been clustered with.
Table 8. Sametime URLs (continued)

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime web client</td>
<td><code>http://proxyserverhostname.domain:port/stwebclient/index.jsp</code></td>
<td>Log in with your user name and password.</td>
</tr>
<tr>
<td></td>
<td>To verify the port number being used by the Lotus® Sametime Proxy Server, log in the Lotus Sametime System Console. In the WebSphere Application Server administrative console, click <strong>Servers</strong> - <strong>WebSphere application servers</strong> - <strong>STProxyServer</strong> - <strong>ports</strong> - <strong>WC_defaulthost</strong> to find the port number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>For IBM i</strong>, to verify the HTTP port number being used by the Lotus Sametime Proxy Server, open the <strong>AboutThisProfile.txt</strong> file for the Sametime Proxy Application Server Profile and use the setting specified for the HTTP transport port. The default profile name is <strong>STPAppProfile</strong>. On IBM i, look for the <strong>AboutThisProfile.txt</strong> file in the following location:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs/AboutThisProfile</code></td>
<td></td>
</tr>
</tbody>
</table>
Table 8. Sametime URLs (continued)

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Room Center</td>
<td><a href="http://meetingserver">http://meetingserver</a> hostname.domain:port/stmeetings</td>
<td>Log in with your user name and password.</td>
</tr>
<tr>
<td></td>
<td>To verify the HTTP port number being used by the Lotus Sametime Meeting Server, open the AboutThisProfile.txt file for the Sametime Meeting Application Server Profile and use the setting specified for the HTTP transport port. The default profile name is STMAppProfile. For IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STMAppProfile/logs/AboutThisProfile.txt</td>
<td></td>
</tr>
<tr>
<td>Sametime Community Server Administrator Tool</td>
<td><a href="http://communityserver">http://communityserver</a> hostname.domain:port/stcenter.nsf</td>
<td>Log in with your Domino® administrator's name and password. Under Administrator Tools, click Administer the server.</td>
</tr>
<tr>
<td></td>
<td>Specify the port number if it is not the default port number 80.</td>
<td></td>
</tr>
</tbody>
</table>

Adding administrators

Add yourself or others as administrators for the WebSphere Application Server-based IBM Sametime components.

About this task

You must give yourself and users that you designate as administrators the same roles as the WebSphere administrator (the “wasadmin” account) in order to manage Sametime using the Sametime System Console. The wasadmin ID is the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.

Procedure

1. From a browser, enter the URL for the Sametime System Console.
2. Enter the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.
   The default name is wasadmin.
3. Click Applications > Application types > WebSphere enterprise applications.
4. Click Sametime System Console (deployment.ear).
5. Under Detail Properties, click Security role to user/group mapping.
6. Note the roles for wasadmin. For information on the access level of the roles see "Administrative roles" in the WebSphere Application Server information center.
   Click Cancel to return to the Integrated Solutions Console.

7. Click Users and Groups.

8. Select either Administrative user or Administrative group to assign yourself and other designated administrators to the Administrator and Admin Security Manager roles, and other roles assigned to wasadmin.

   Note: An administrator cannot map users and groups to the administrator roles without having the Admin Security Manager role.

9. Save your changes.

Changing the administrator password

The following topics explain how to change your administrator passwords.

Updating your DB2 administrator password

If you change your administrator password in IBM DB2®, you must update your password in the Sametime System Console, as well as the Meeting Server and, if applicable, Sametime Advanced. If you do not update your password, IBM Sametime stops working.

Procedure
1. Log in to the Integrated Solutions Console for the Sametime System Console.
2. Click Resources > JDBC > Data sources.
3. Click the data source in the table.
4. Under Related Items, click JAAS - J2C authentication data.
5. Click your DB2 administrator alias.
6. Under General Properties, type your new password.
7. Click Apply and then click OK.
8. Repeat this procedure for the Sametime Meeting Server and, if applicable, the Sametime Advanced server.
9. Restart the deployment manager, then restart the Sametime System Console and Meeting Server or Advanced Server.
   The changed password only takes effect after you restart the server, so be sure to restart the server.

Updating your LDAP Bind password

You can change the LDAP Bind password that you defined when you first connected the LDAP server.

About this task

Change your LDAP Bind password by running the Connect to LDAP Servers prerequisite in the Sametime System Console. Changing the password updates the Sametime Community Server database, stconfig.nsf and the WebSphere Application Server. Then send the update to any other Deployment Managers in the environment and to the Directory Assistance database on the Sametime Community Server.
Procedure
1. From the Sametime System Console, run the Connect to LDAP Servers prerequisite. Update the LDAP Bind password when you are prompted to do so and save the changes.
   The change updates the LDAP repository configured for WebSphere Application Server.
2. Wait for the next scheduled update task to run, which updates the LDAP Server document in the Sametime Community Server configuration database (stconfig.nsf) with the password change.
3. If the Sametime System Console is the Deployment Manager for all Sametime servers, proceed to the next step.
   If there are other Deployment Managers in the Sametime environment, update the Bind password on each Deployment Manager. Make the change by editing the LDAP repository as described in the WebSphere Application Server information center topic Lightweight Directory Access Protocol repository configuration settings.
   a. From the Notes® client, open the Directory Assistance database (usually named da.nsf) on the Community Server.
   b. Open the Directory Assistance document for the LDAP server.
   c. On the LDAP tab, under Connectivity Settings, update the Administrator password.
   d. Save and close the document.
5. Restart the Community Servers, Deployment Managers, and Application Servers that share the LDAP repository.

Updating your WebSphere Application Server administrator password
You can change your WebSphere Application Server administrator password.

About this task
You can change your WebSphere Application Server administrator (wasadmin) password on the following WebSphere-based Sametime servers. If you change the wasadmin password on any of these servers, then you must also update the wasadmin password for that server that is stored in the Sametime System Console.

- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Gateway Server
- SIP Proxy and Registrar
- FIPS Proxy Server
- Sametime Advanced

The complete Sametime Media Manager installations are listed under both the Media Manager and the SIP Proxy and Registrar administration listings. There is only one entity and changing the connection properties in one place is reflected in the other.
A FIPS Proxy Server uses the same credentials as the Sametime Proxy Server on which it was installed. Changing the credentials in either location affects both administrative connections. The FIPS Proxy Server list depends on a valid server connection, so if the connection information is not correct, the FIPS Proxy server is not be listed. You can correct this by editing the connection properties in the Sametime Proxy Server listing.

**Procedure**

1. Change the wasadmin password of the WebSphere-based Sametime application server.
   a. Log in to the Integrated Solutions Console on the WebSphere-based Sametime application server.
   b. Click **Users and Groups** > **Manage Users**.
   c. Under Search for Users, select **User ID** in the **Search by** field, and then enter **wasadmin** in the **Search for** field. Click **Search**.
   d. Click **wasadmin** in the results dialog.
   e. Enter a new password in the **Password** and **Confirm Password** fields.
   f. Click **Apply** and then click **OK**.

2. Update the wasadmin password that you changed in the previous step on the Sametime System Console.
   a. Log in to the Integrated Solutions Console for the Sametime System Console.
   b. Click **Sametime System Console** > **Sametime Servers**.
   c. Click the Sametime application server that has the wasadmin password that you changed in step 1.
   d. Locate the deployment name and click **Edit** under **Connection Properties**.
   e. Enter a new password.
   f. Click **Save** and then click **Done**.

**Managing users with policies**

All IBM Sametime users are automatically assigned to default policies. Sametime Instant Messaging, Meetings, and Media Services each has a default policy to be applied to users. You can create additional user policies, and assign users and groups to these policies.

**Before you begin**

If you upgraded from an earlier release, complete the steps for migrating policy assignments before setting any new ones.

**About this task**

When a user authenticates, Sametime applies a default policy if no other policy can be found for that user. You can create new policies that grant or limit access to features, and assign users to these policies. Users can be assigned to more than one policy. If a user belongs to more than one policy, then Sametime uses the policy weight to determine policy precedence. Custom policies can be designed for specific groups in the company, and the default policy can be inherited or assigned. Meetings policy changes take effect immediately, while Instant Messaging and Media Services policy changes take effect within an hour.
There is also an anonymous policy that is assigned by default to users who have not authenticated, and unauthenticated users always receive this policy.

Note: If your deployment includes the Sametime System Console, you must manage policies there because all settings made in the legacy Sametime Administration Tool (STCenter.nsf) are ignored. This includes the override all feature, as well. Moreover, there is no automatic migration of policies from the Sametime Administration Tool to the Sametime System Console. You must do this manually because Sametime Administration Tool policies do not map one-to-one to policies in the Sametime System Console.

Do not use the ampersand character (&) in the policy's name or in any one of the values of policy attributes.

Finding policies associated with a user

You can find all the policies associated with a user for all the IBM Sametime products to which the user has access.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click any user Sametime component. It does not matter which component that you select, because your search results display all the policies for all the Sametime components to which the user has access.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Click Find Active Policies.
6. Select the criterion for the user for which you want to find the associated policies in the Search by field.
   - User ID
   - Name
   - E-mail address
7. Enter the entire or partial user ID, email address, or name of the user or group in the Search for field. If you enter partial information, use an asterisk as a wild card character for missing or incomplete information. For example, type sm* for all names starting with sm.
8. Select the number of listings in the search results in the Maximum results field.
9. Click Search. The results display the users that match your search criteria.
10. Select a name in the results table, and then click Find Active Policies to show the policies for that user.
11. Click Done.

Creating new user policies

You can create user policies, and assign users and groups to these policies.
About this task

You can set policy for users to have access to specific IBM Sametime features, depending upon their level of need. For example, the maximum size for a file being transferred is set by default at 1 megabyte to help manage traffic over the server(s); however, if you have a group that routinely transfers large files for business reasons, you can create a new policy specifically for those users and set the maximum size of files that they can send to a much higher number.

Note: When you create a new policy, it uses the default policy settings as the base settings in the new policy. You can update these settings.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime product for which you want to create a policy.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Click New.
6. Enter a name to use to identify the policy in the Policy Name field.
   
   Note: Do not use the following special characters in the policy’s name or in any one of the values of policy attributes:
   - Ampersand (&)
   - Apostrophe (’)
   - Quotation mark (”)
   - Greater than character (>)
   - Less than character (<)
7. Specify the features that you want to enable or disable for the users or groups that you will assign to this policy. Some instant messaging features are flagged with IC characters after the field label. This flag indicates that a feature is only available for installed clients. The feature is not available to browser clients.
8. Click OK.

Results

Tip: You can follow these same basic steps to delete or edit a policy. Delete a policy by selecting the policy and then click the Delete button. Edit a policy by clicking the policy name. You cannot delete the anonymous or default policies, but you can edit them. If you edit a policy, you cannot change the policy ID. To do this, you must make a copy of the policy by selecting it and clicking Duplicate, then you can enter a new ID in the copy. Before you delete the original, be sure to reassign the users and groups to the copy and give it the proper policy weight.

What to do next

You can now assign users and groups to this policy.
Assign users and groups to policies

You can assign users and groups to specific user policies to grant or limit access to features in IBM Sametime.

About this task

You cannot assign users to the default or anonymous policies. Authenticated users are automatically assigned to the default policies. Unauthenticated users are assigned to anonymous policies.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime component with the policy to which you want to assign a user or a group.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Select a policy name from the list, and click Assign.
6. Click Add Users or Add Groups.
   At this point you could remove a user from a policy, by selecting the user in the list and then clicking Remove.
7. Select the criterion for searching for the user or group that you want to add to the policy in the Search by field.
   - User ID
   - Name
   - E-mail address
8. Enter user ID, email address, or name or partial name with wildcard characters (asterisks) of the user or group in the Search for field
9. Select the number of listings on each search results page in the Maximum results field.
10. Click Search. The results display the DN, display name, and e-mail address of the users that matched your search.
11. Select a user and click Assign.
12. Click Done.

Sametime Instant Messaging user policy settings

You can grant or limit access to features in IBM Sametime Instant Messaging by enabling or disabling various policies for users. Instant Messaging policy changes take effect in 60 minutes by default.

You can change the default time that Instant Messaging and Media Manager policies take effect by editing the REFRESH_RULES_INTERVAL setting in the sametime.ini file.

All unauthenticated users have the anonymous policy, Sametime Instant Messaging Anonymous Policy, applied to them. For authenticated users, the Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match, then the default policy, Sametime Instant Messaging Default Policy, is applied.
In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

**Table 9. Chat**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must set this community as the default server community</td>
<td>Determines if this community can be connected to as a secondary community or if must it be the default community for the Sametime Connect client. When this policy is selected, users must log in to this community before they can log in to other communities. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 9. Chat (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to add multiple server communities</td>
<td>If this is checked, community preferences and menus are available to users. When the Allow user to add multiple server communities policy is set to Not selected, users cannot add their own secondary communities. When the policy becomes enabled, clients cannot log in to any secondary communities that were not set by the administrator. Administrator-defined secondary communities are not impacted by the policy. The client recognizes they are defined by the administrator and allows the user to log into them. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Allow user to add external users using Sametime Gateway communities</td>
<td>Allowing users to connect to external communities such as AIM, OCS, and Google Talk. If this policy is not allowed, the check box and text for adding external users by email address is not available in clients.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow user to save chat transcripts</td>
<td>If this is enabled, users see the File-Save option in the chat window. Chat history capabilities are available. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically save chat transcripts</td>
<td>This is not valid unless <strong>Allow user to save chat transcripts</strong> is selected. If this is not selected, then users do not see preferences for chat history or the chat history viewer in their clients. This setting does not apply to browser users. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 9. Chat (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum days to save automatically saved chat transcripts</td>
<td>If <strong>Allow to automatically save chat transcripts</strong> is selected, then a value must be entered in this field. Users cannot set a larger value in their clients than the one specified here. This setting does not apply to browser users.</td>
<td>10</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>Limit contact list size</td>
<td>This limits the number of contacts that users can enter in their contact lists.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Contacts</td>
<td>If <strong>Limit contact list size</strong> is selected, then a value must be entered in this field. Specify the number of contacts that users can enter in their contact lists.</td>
<td>650</td>
<td>500</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Enable organization tree view for this user</td>
<td>For Sametime Advanced clients, this policy allows users to see the company directory in a hierarchical structure. The Organization view service must be configured on the Community Server in advance. By default, this applies to the default community. To enable the tree view for a non-default community, specify <code>com.ibm.collaboration.realtime/defaultOrgTreeHost=hostname</code> in the <code>plugin_customization.ini</code> file.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Allow users to send offline messages</td>
<td>For Sametime Advanced clients, this policy lets users send text messages that include regular text, rich text, and basic emoticons. Advanced client users can send messages to any users who are offline or who have set their status to &quot;Do not disturb.&quot; The messages are delivered when the offline users next log in or when they retrieve their messages manually. Offline messaging must be enabled on the Community Server in advance.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow all Sametime Connect features to be used with integrated clients</td>
<td>If this is not selected, some Sametime Connect features do not display when Sametime is integrated with other products. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow mobile client</td>
<td>This feature lets users deploy Sametime awareness and chat features on a mobile device.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 9. Chat (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime update site URL</td>
<td>Provides a URL where users can retrieve updates to features for the Sametime Connect client. This setting does not apply to browser users.</td>
<td>Blank</td>
<td>Blank</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Table 10. Image Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow custom emoticons</td>
<td>Allows all actions on the preferences palette: new, import, export, add picture, add palettes. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow screen capture and images</td>
<td>Allows pasting and right-click copying of image and screen captures. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Set maximum image size for custom emoticons, screen captures, and inline images</td>
<td>This setting includes images pasted inline through the palette emoticons, cut and paste, screen captures, and print screen. It does not include images sent through file transfer. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>KB</td>
<td>If set maximum image size for custom emoticons, screen captures, and inline images is selected, then a value must be entered in this field. Users sees a message if they attempt to send a file that is larger than the specified size. This setting does not apply to browser users.</td>
<td>100</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to transfer files</td>
<td>Allows user to transfer files to other users. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Maximum file transfer in Kilobytes</td>
<td>Limits the size of the file that can be transferred by the specified value. In kilobytes. This setting does not apply to browser users.</td>
<td>1000</td>
<td>1000</td>
<td>No</td>
</tr>
<tr>
<td>Allow client-to-client file transfer</td>
<td>Allows users to transfer files without passing the files through the Sametime server. These files are not logged. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Allow transferring multiple files and folders</td>
<td>For Sametime Advanced clients, this option allows the transfer of multiple files and folders during a chat session if “Allow client-to-client file transfer” is allowed. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow transferring files to participants in an n-way session</td>
<td>For Sametime Advanced clients, this setting allows a person to transfer one file to multiple participants at the same time if “Allow client-to-client file transfer” is allowed. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
<tr>
<td>Maximum number of users to receive a single file in one file transfer session</td>
<td>For Sametime Advanced clients, this setting limits how many people can receive a file in one session if “Allow transferring files to participants in an n-way session” is enabled. This setting does not apply to browser users.</td>
<td>10</td>
<td>10</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 11. File Transfer (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use exclude file types transfer list</td>
<td>Limits the types of files that users can transfer. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Types to exclude from transfer.</td>
<td>If <strong>Use exclude file types transfer list</strong> is selected, then a value must be entered in this field. Type the three-letter extension of each file type, separated by a comma or semicolon. This setting does not apply to browser users.</td>
<td>exe,com,bat,dll</td>
<td>exe,com,bat</td>
<td>No</td>
</tr>
</tbody>
</table>

### Table 12. Plugin Management

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to install plug-in</td>
<td>Allows users to install plugins and updates from the Sametime Connect Tools &gt; Plug-ins menu. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 12. Plugin Management (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime optional plug-in site URLs. Type the URLs separated by a comma or semicolon. This setting does not apply to browser users.</td>
<td>If no value is specified, then the Check for Optional Features item on the Tools &gt; Plug-ins menu not valid. This setting does not apply to browser users.</td>
<td>Blank.</td>
<td>Blank</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Meetings user policy settings

You can grant or limit access to features in meetings by enabling or disabling various policies for users. Policy changes take effect immediately.

All unauthenticated IBM Sametime users have the anonymous policy, Sametime Meetings Anonymous Policy, applied to them. For authenticated users, Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match the default policy, Sametime Meetings Default Policy is applied.

Sametime does not allow anonymous users to create meeting rooms. Therefore, any policy that is related to authenticated users or the ability to create meeting rooms, does not apply to anonymous users.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

Note: Although Sametime Classic meetings are still managed on the server itself, you can set user policy for Sametime Classic meetings on the Meetings policy tab in the Sametime Classic Meetings section.

Table 13. General Meeting Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum persistent meeting rooms this user can own</td>
<td>Users are limited to creating this number of meeting rooms per user. When this limit is reached or set to zero, users cannot create more meeting rooms.</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 13. General Meeting Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to create instant (nonpersistent) meeting rooms</td>
<td>If not selected, user does not see the capabilities for creating instant meetings. User can, still see the capabilities for using an existing room.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Automatically connect to meeting server when logging into Sametime Connect</td>
<td>If not selected the user must manually connect to each meeting room server to view the meetings there. This setting is stored with the client, so that changes in the policy do not take effect until after the next time the user logs in to the server. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow searching for meeting rooms</td>
<td>If not selected, users can attend meeting rooms only with a direct URL. The meeting room manager interface never shows. Only affects browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow searching for hidden meeting rooms</td>
<td>If selected, the interface allows the user to explicitly search for hidden meeting rooms by exact name. If not selected, the interface for searching for hidden meeting rooms does not appear, and hidden meeting rooms are never returned in search results.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Show &quot;Scheduled Meetings&quot; view</td>
<td>Determines whether to show the &quot;Scheduled Meetings&quot; view in the shelf. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
</tbody>
</table>
Table 13. General Meeting Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow meetings to be recorded</td>
<td>Allows users to record meetings for rooms they have created. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow meeting room content to be downloaded</td>
<td>Allows users to download content from the meeting library.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Meeting room group chats</td>
<td><strong>Hidden</strong> - Users cannot see or create group chats.</td>
<td>Interactive</td>
<td>Interactive</td>
</tr>
<tr>
<td></td>
<td><strong>Read-only</strong> - Users can only read what others have typed into the group chat.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Interactive</strong> - Users can type and read group chats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow meeting room polls</td>
<td>Determines whether a presenter can send a poll to meeting participants.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Allow annotations of uploaded content</td>
<td>Determines whether a presenter can use meeting room annotation tools when sharing documents from the meeting room library.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 14. Meeting Room Library

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum file upload size, in Megabytes</td>
<td>Maximum file upload size for an individual user in megabytes. Users cannot upload a larger file into the library.</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 14. Meeting Room Library (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum total size of library in Megabytes</td>
<td>Maximum total size in megabytes of files that a meeting room library can hold. When the library contains the maximum size or if the size is set to zero, users cannot upload files to the library. In addition, when the library’s maximum storage capacity has been reached, users may be unable to upload all their files even though their individual file upload size.</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

### Table 15. Screen Sharing

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow screen sharing</td>
<td><strong>No screen sharing allowed</strong> - Users cannot share screens or applications. <strong>Application only</strong> - Users can share a specific application. No other applications or their desktops are shared. <strong>Entire screen, frame, and applications</strong> - Users share their whole screen including any applications that they open on their screens.</td>
<td>Entire screen, frame, and applications</td>
<td>Entire screen, frame, and applications</td>
</tr>
<tr>
<td>Allow user to control another user’s shared screen</td>
<td>Allow others to control a user’s shared screen. Any participant can make changes to the shared information. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
</tbody>
</table>
### Table 15. Screen Sharing (continued)

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow peer-to-peer application sharing</td>
<td>Whenever this user hosts screen sharing, peer-to-peer can be used by any viewers that support it. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Enforce bandwidth limits</td>
<td>Any time the user hosts sharing, the experience is limited by the value specified in the Maximum bandwidth size</td>
<td>Not selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Maximum bandwidth size, in Kilobytes per second:</td>
<td>This is not used unless “Enforce bandwidth limitations” is selected.</td>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

### Table 16. Sametime Classic Meetings

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to create instant meetings and breakout sessions.</td>
<td>Lets users start a meeting from the contact list, from an existing chat, and from within a meeting (breakout session).</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Feature list</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Allow Sametime IP audio and video in instant meetings and breakout sessions.</td>
<td>No Does not allow use of Sametime Internet Protocol audio and video in instant meetings and breakout sessions.</td>
<td>IP audio and video</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>IP audio only</strong> Allow use of Sametime Internet Protocol audio but not video in instant meetings and breakout sessions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IP audio and video</strong> Allows use of Sametime Internet Protocol video but not audio in instant meetings and breakout sessions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow participation in meeting room chats</td>
<td>Allows participants in the meeting to use the chat window to communicate with any other participant in the meeting.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 16. Sametime Classic Meetings (continued)

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow screen sharing</td>
<td><strong>No</strong> - Users cannot share screens or applications.</td>
<td>Entire screen, frame, and applications</td>
<td>Entire screen, frame, and applications</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Application only</strong> - Users can share a specific application. No other applications or their desktops are shared.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Entire screen, frame, and applications</strong> - Users share their whole screen including any applications that they open on their screens.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow user to control another user's shared screen</td>
<td>Allow others to control a user's shared screen. Any participant can make changes to the shared information. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
</tbody>
</table>

### Media Manager user policy settings

You can grant or limit access to media features in by enabling or disabling various policies for users. Media Manager policy changes take effect in 60 minutes by default.

You can change the default time that Instant Messaging and Media Manager policies take affect by editing the `REFRESH_RULES_INTERVAL` setting in the `sametime.ini` file.

All unauthenticated users will have the anonymous policy, Media Manager Anonymous Policy, applied to them. For authenticated users, Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match for the default policy, Media Manager Default Policy is applied.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied
when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

Table 17. Voice and Video

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings</td>
<td>Allows outside vendors to provide audio and video for instant messages and instant meetings. This setting does not apply to browser meetings.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow changes to preferred numbers</td>
<td>If not selected, user cannot add telephony devices. This gives the administrator control over the devices that can make or receive calls in the system. &quot;Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings&quot; must be selected to specify this setting.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
</tbody>
</table>
| Voice and video capabilities available through the Sametime Media Server | Allows users to use computer audio and video in instant messages and instant meetings. Choices are:  
  • None  
  • Audio only  
  • Audio and video  
This setting does not apply to browser users. | Audio and video      | Audio and video     | No                                  |
Table 17. Voice and Video (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Audio/Video use in the web browser</td>
<td>Allows users to have audio-video capabilities in Sametime Meetings from a web browser.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow access to Packet Switcher for internal audio video conferences</td>
<td>Allows users to make internal audio/video calls using the Packet Switcher for better performance.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 17. Voice and Video (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video resolution</td>
<td>Video quality is affected by the available network bandwidth. The higher the video resolution, the more bandwidth is required and the better quality. The Sametime video codec automatically adapts to the available bandwidth and reduces the bit-rate to a certain threshold for each chosen video resolution. However, the quality suffers when the available bandwidth becomes too low, especially during peak utilization when the contention in the network routers causes packet loss. The video resolution is composed of the following elements: • Resolution name - The video resolution name, for example, Common Intermediate Format (CIF) • Width x Height - The dimensions of the video in pixels • Framerate - Frames per second • Bit-rate - Maximum</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CIF352x288@15fps 384kbps</td>
<td>CIF352x288@15fps 384kbps</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 18. Sametime Unified Telephony

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow changes to the permanent call routing rule</td>
<td>If this setting is not selected a lock appears next to this rule in the user’s preferences. “Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings” must be selected to specify this setting. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow use of “Offline” status in call routing rules</td>
<td>Allows users to add their own devices to make and receive calls. “Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings” must be selected to specify this setting. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
</tbody>
</table>

Changing a user policy's weight

IBM Sametime products implement user policies that have higher weights over policies with lower weights. You can change the weight of policies.

About this task

User policies in Sametime have weights. A policy’s weight determines whether or not its attributes take precedence over the attributes of other policies. For a given user or group assigned two or more policies, Sametime implements the policy with the highest weight. Anonymous policies always have the lowest weight; default
policies have the next lowest weight. For authenticated users, Sametime searches for an exact ID match, and then applies the highest weighted policy. If there is no match for the user ID in any policy, the Sametime applies the highest weighted group match. If no group matches are found, the default policy applied. You can change the weight of policies by moving them up and down the policy list of a Sametime product.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console**.
3. Click **Manage Policies**.
4. Click the Sametime component with the policy with the weight that you want to change.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Select a Policy ID from the list, and click **Move Up** or **Move Down**. Moving the policy up increases its weight; moving the policy down decreases its weight. You cannot change the weight of a default or and anonymous policy.

**Using nested groups in policy assignments**

You can configure whether or not Sametime considers nested groups when it applies policies and how many levels deep that Sametime searches for the highest weighted group.

**About this task**

For authenticated users, Sametime searches for an exact ID match, and then applies the highest weighted policy. If there is no match for the user ID in any policy, the Sametime applies the highest weighted group match to which the user belongs. By default, Sametime searches through four levels of nested groups when determining the highest weighted policy.

For example, a fourth level assigned group would mean that the group is four levels above the user. In the following example the EMEAGroup is four levels above the user: EMEAGroup (level 4) contains UKGroup (level 3), which contains LondonGroup (level 2), which contains MarketingGroup (level 1), which contains the user.

Follow these steps to change the number of levels of nested groups that Sametime searches for the highest weighted policy. If a policy is assigned to a group higher than the nesting depth, that the default policy is assigned. Entering a large number as the maximum nested group depth can have an impact on performance.

**Note:** To change the maximum nested group depth for the Sametime Instant Messaging user policy, edit DIR_SEARCH_LEVEL_LIMIT parameter of the Sametime Community Server sametime.ini file.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console**.
3. Click **Manage Policies**.
4. Click **Preferences**.
5. Enter a numerical value of -1 or greater in the **Maximum Nested Group Depth** field.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Sametime searches an infinite number of levels of nested groups.</td>
</tr>
<tr>
<td>0</td>
<td>Sametime searches for the user ID directly, and does not look in groups, nested or otherwise.</td>
</tr>
<tr>
<td>1</td>
<td>Sametime searches within groups, but not nested groups (groups within groups).</td>
</tr>
<tr>
<td>2 or greater</td>
<td>Sametime searches nested groups up to and including the level specified.</td>
</tr>
</tbody>
</table>

6. Enter a number in minutes in the **Policy Cache Timeout** field. The default value is 30 minutes. The Policy cache stores policy assignments. This cache reduces the number of database operations required to provide policy information. For example, if Sametime calculates that user1 gets policy1, that is stored in the cache. The next time that something requests user1’s policy it does not have to calculate it. The timeout is how long the information stays in the cache.

7. Enter a number in minutes in the **Group Membership Cache Timeout** field. The default value is 30 minutes. The Group Membership cache stores the group membership information. This cache alleviates potential LDAP load issues due to group membership look-ups. You might want to update this timeout to reflect your site’s LDAP administration operating procedures.

8. Click **Apply**.
9. Restart the servers.

**Example**

In following examples, use the this group structure:

1. Group1 contains user1
2. Group2 contains user2 and group1
3. Group3 contains user3 and group2
4. Group4 contains user4 and group3
5. Group5 contains user5 and group4
6. Group6 contains user6 and group5

**Example 1: Nested group matches**

Policy1 has a weight of 2 and is assigned Group6. Nesting level is the default of 4.

1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets the default policy because it is over the nesting level limit.
3. User3 gets policy1 because it is in the 4th group nesting level.
4. User4 gets policy1 because it is in the 3rd group nesting level.
5. User5 gets policy1 because it is in the 2nd group nesting level.
6. User6 gets policy1 because it is in the 1st group nesting level.
User1 and User2 get the default policy because they are not within the group search depth limit.

**Example 2: Nesting has priority over policy weight**

Policy1 has a weight of 2 and is assigned Group5. Policy2 has a weight of 3 and is assigned Group6. The nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets policy1 because it is in the 4th group nesting level from Group5.
3. User3 gets policy1 because it is in the 3rd group nesting level from Group5.
4. User4 gets policy1 because it is in the 2nd group nesting level from Group5.
5. User5 gets policy1 because it is in the 1st group nesting level from Group5.
6. User6 gets policy1 because it is in the 4th group nesting level from Group5.

Even though policy2 has a higher weight, it is not assigned to User2, User3, User4, and User5 because they have a lower level policy match.

**Example 3: Policy weight breaks ties**

Policy1 has a weight of 3 and is assigned to Group6. Policy2 has a weight of 2 and is assigned to Group6. The nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets the default policy because it is over the nesting level limit.
3. User3 gets policy1 because it is in the 4th group nesting level.
4. User4 gets policy1 because it is in the 3rd group nesting level.
5. User5 gets policy1 because it is in the 2nd group nesting level.
6. User6 gets policy1 because it is in the 1st group nesting level.

Since both Policy1 and Policy2 were at the same level, Policy1 won the tie breaker because it has a higher weight.

---

**Administering a Sametime System Console**

This section describes how to manage the IBM Sametime System Console.

**Backing up the console database**

The IBM Sametime System Console database stores information about all the Sametime servers that are connected to it.

**About this task**

Back up the database regularly to protect the server data and to minimize downtime if you need to restore lost or corrupted data. Follow the instructions in the DB2 information center:

BACKUP DATABASE command

**Starting the Sametime System Console so you can administer servers**

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.
Before you begin

Verify that the Deployment Manager is running for the cell.

Procedure

1. Open a command window (on IBM i, run QSH command).
2. Navigate to the local app_server_root/profiles/STSCAppProfile profile directory and change to the bin directory.
3. Run the following command. Note that the name of the server is case sensitive:
   - **AIX, Linux, or Solaris**
     
     ./startNode.sh
     ./startServer.sh STConsoleServer
   - **Windows**
     
     startNode.bat
     startServer.bat STConsoleServer
   - **IBM i**
     
     startNode
     startServer STConsoleServer

Administering a Sametime Community Server

This section describes how to manage an IBM Sametime Community Server

About this task

Use the instructions in this section to manage connectivity, community services, anonymous access, and business cards on the Sametime Community Server.

Managing administrator access and roles

Manage administrator access and roles using the Sametime Administration Tool.

Starting the Sametime Administration Tool

You administer Sametime through a web browser application. You must enable Java applets and JavaScript or ActiveX Controls in your browser to use the Sametime Administration Tool.

About this task

To start the Sametime Administration Tool:

Procedure

1. Enter the URL for the Sametime server:

   http://host_name/stcenter.nsf

   where hostP_name is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime server you want to administer.

   Note: For versions of Sametime that do not support web conferencing, enter the following URL in your browser: http://hostname.
Note: For Sametime Entry and other Sametime offerings that do not include web conferencing, access the server page by typing http://hostname/ into a browser URL field where hostname is the fully qualified name of your Sametime server.

2. From the Sametime server home page (Sametime Welcome page), click Administer the Server.

3. Enter the administrator name and password specified during the Sametime server installation. The Sametime Administration Tool opens in its own web browser window.

Related concepts:
User requirements for basic password authentication
When accessing the Sametime server with a Web browser, a user must enter a user name and Internet password to access any protected database on the Sametime server.

Adding a new Sametime administrator
Use the Domino Directory to give a group of administrators access to the Sametime Administration Tool.

Adding a Sametime administrator in Domino LDAP
Use the Domino Directory to give a group of administrators access to the Sametime Administration Tool.

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

This is the procedure for adding an administrator in Domino. If your Sametime server is configured for LDAP, then you must create the new administrator using your LDAP Directory tools.

Creating a Person document for the administrator:

Administrators must have a Person document in the Domino Directory.

About this task

Follow these steps to create a Person document using the Sametime Administration Tool. If the administrator whom you are adding already has a Person document that contains a last name, user name, and Internet password, skip this procedure.

Procedure
1. From the Sametime server home page, click Administer the Server.
2. From the Sametime Administration Tool, click LDAP Directory.

Note: For native Domino Directory (non-LDAP) click Domino.

3. Choose Add Person.
4. In the Person document, select the Basics tab.
5. Enter the user’s first, middle, and last name in the appropriate fields. Only the last name is required.
6. Enter a name for the user in the User Name field. An entry in this field is required for the user to authenticate with the Sametime server.
You can use any of the following characters in a user name: A - Z, 0 - 9, dash (-), period (.), underscore (_), and space. Using other characters can cause unexpected results.

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

**Password character restrictions**
In addition to non-English characters, the following characters must not be included in passwords used by Sametime:
: \ } ' " &

8. Click **Save & Close**. The Person document is added to the Directory.

**Creating an Administrators Group document:**

Create a group document to hold the names of Sametime administrators.

**About this task**

Use the Sametime Administration Tool to create an Administrators Group document.

**Procedure**

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

**Adding the Administrators Group document to Sametime database ACLs:**

Add the Administrators Group document to Sametime database Access Control Lists (ACLs) and provide the Manager access level to the group.
About this task

In addition to ACL access levels, you must also specify the ACL privileges and roles that the Administrators Group (or an individual user) has in each database. Generally, for an Administrators Group, select all ACL privileges and roles.

Note: If you are adding individual user names to Sametime database ACLs instead of a group name, database roles can be used to prevent or allow access to specific features of the Sametime Administration Tool.

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

- **Sametime Configuration (stconfig.nsf)** - Stores the configuration parameters that are set from the Sametime Administration Tool.
- **Domino Directory or Address Book (names.nsf)** - Stores Person and Group documents, ACL settings, and other configuration information for the Domino/Web Application Services.
- **Sametime Log (stlog.nsf)** - Stores logging information.
- **Domino Web Administration (webadmin.nsf)** - Contains the Domino Web Administration client, which includes monitoring features for the HTTP Services and free disk space. This is the full Domino Web Administration client that is included with Domino servers.

Procedure

1. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
2. Choose **Add Sametime Administrators** - Give the administrator group Manager access for all appropriate databases, such as stconf.nsf and stcenter.nsf (Set Access Control).
   - The Access Control options appear.
3. Click the **Files** tab and make sure that the path to the Data directory is selected in the navigation pane.
4. From the "Databases" list, select **Sametime Configuration (stconfig.nsf)**.
   - **Note**: The database filename appears below the Databases list.
5. Click the **Tools** button near the top right of the page, then expand Database and choose Manage ACL.
6. Click **Add**. Enter the Administrators Group document name in the dialog box (for example, "Administrators" or "Sametime Administrators").
   - If you are adding individual user names, enter the person’s user name in the dialog box. Enter the name as it is entered in the top entry of the "User name" field on the user's Person document.
7. Click **OK**.
8. Select the Administrators Group name (or individual person’s name) from the list in the Database Security window.
9. In the "User Type" list, select **Group** (or **Person** if you are adding an individual user's name).
10. In the "Access" list, select **Manager**.
11. Make sure that all ACL privileges, such as "Create documents" and "Delete documents," are selected.

12. Click Roles.

13. If you want the Administrators Group to have access to the full range of administrative functions, select all roles; then click OK.

   The roles determine which administration tasks the members of the group can perform. If you are adding individual user names to the ACLs, you can use the roles to control the administrative features that are available to individual administrators. For more information, see Roles in Sametime databases ACLs.

14. Click OK.

15. After adding the Administrators Group to the ACL of the Sametime Configuration database (stconfig.nsf), repeat steps 4 through 14 to add the Administrators Group to the ACL of each of the Sametime databases listed below:

   - Domino Address Book or Domino Directory (names.nsf)
   - Sametime Online Meeting Center (stconf.nsf)
   - Sametime Log (stlog.nsf)
   - Sametime Self Registration (streg.nsf)
   - Domino Web Administration (webadmin.nsf)
   - Sametime Policy (stpolicy.nsf)
   - Sametime Name Change (stnamechange.nsf)
   - Log (log.nsf)

Modifying the Server document of the Sametime server:

Add the Administrators Group document (or the name of an individual user) to two fields on the Server document.

Procedure

1. From the Sametime Administration Tool:

   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.

2. Choose "Add Sametime Administrators - Edit the Server document."

3. Click Security.

4. In the "Administrators" field of the Administrators section, type the name of the Administrators Group (or enter the name of an individual user).

   **Note:** Type a group name exactly as it appears in the Group document. If you are entering an individual user name in this field, type the user name exactly as it is entered in the topmost entry of the "User name" field on the Person document. Separate multiple entries in the "Administer the server from a browser" field with commas.

5. In the "Run unrestricted methods and operations" field of the Programmability Restrictions section, type the Administrators Group name (or an individual user's name). Separate multiple entries in this field with commas.

6. Click Save & Close.

Adding and removing names from an Administrators Group document:
Control access to the Sametime Administration Tool by editing the Group document.

**About this task**

Adding a user's name to the Administrators Group document provides the user with access to the Sametime Administration Tool. Removing a user's name from the Group document revokes the user's access to the Sametime Administration Tool.

**Procedure**

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

**Sametime database default ACL settings**

See the following tables to determine the default ACL settings for Sametime databases.

*Table 19. stconfig.nsf database default ACL settings*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>No Access</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>
### Table 20. stconf.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Author</td>
</tr>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

### Table 21. names.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Author</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

### Table 22. stpolicy.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>No Access</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

### Table 23. stlog.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Reader</td>
</tr>
</tbody>
</table>
Table 23. stlog.nsf database default ACL settings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 24. stnamechange.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Manager</td>
</tr>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Roles in Sametime database ACLs

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

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

Access Control List (ACL) roles are defined in the following Sametime databases:

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

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

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

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Command or feature</th>
<th>Role required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message From Administrator</td>
<td>Sends message to all users logged into Community Services</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Monitoring</td>
<td>All monitoring features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Logging</td>
<td>All logging features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Directory</td>
<td>Add directory features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Configuration</td>
<td>Connectivity, Community Services, Meeting Services, Audio/Video Services</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Help</td>
<td>Online help for administrators</td>
<td>No roles required</td>
</tr>
</tbody>
</table>

**Note:** The Domino server cannot resolve the user if given the internet address in the person entry that defines the internal ID of a Sametime user. The mail attribute is not supported in this field. The field may be left blank.

**Roles in the Domino Directory (names.nsf):**

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

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

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

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

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

Related reference:
Roles in Sametime database ACLs
Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

Roles in the Sametime Meeting Center (stconf.nsf):
The Sametime Meeting Center database contains only the Sametime Admin role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Admin</td>
<td>Allows an administrator to see hidden meetings displayed in the All Meetings view of the Meeting Center.</td>
</tr>
<tr>
<td></td>
<td>Allows an administrator to see the Hidden Meetings view in the Meeting Center. This view displays only hidden meetings.</td>
</tr>
<tr>
<td></td>
<td>Allows the administrator to alter the meeting details of any meeting. For example, the administrator can delete or change the end time of a meeting that the administrator did not create.</td>
</tr>
<tr>
<td></td>
<td>Allows an administrator to see and use the &quot;Delete the Recording,&quot; &quot;Export the Recording,&quot; &quot;Replace the Recording,&quot; and Import Recording options in the Meeting Center forms. These features enable the administrator to manage the recorded meeting files if the administrator makes the Record and Playback feature available on the Sametime server.</td>
</tr>
</tbody>
</table>
Note: The Domino server cannot resolve the user if given the internet address in the person entry that defines the internal ID of a Sametime user. The mail attribute is not supported in this field. The field may be left blank.

Related reference:
Roles in Sametime database ACLs
Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

Roles in the Domino Web Administration database (webadmin.nsf):

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

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

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

Domino log
To access the Domino log, choose Logging - Domino Log in the Sametime Administration Tool, and then click the link that appears on the right. The Domino log launches in a new browser window.

Managing trusted IP addresses
Whenever you install a server that communicates with a community server, you must add the new server’s IP address to the community server’s settings.

About this task
The community server accepts connections from the Sametime Media Manager, the Sametime Gateway, the Sametime Community Multiplexer, and the Sametime Proxy Server, as well as other servers that are listed in the Community Services page. To ensure that the Sametime Community Server trusts these components when they establish a connection, you must add the trusted server’s IP address to the community server.

If you are installing a cluster of media manager servers, gateway servers, or proxy servers, be sure to complete include the IP address of the primary node as well as every secondary node in the cluster (you do not need to include the deployment manager).

You do not need to add the system console's IP address because it is added automatically when you install the community server using a deployment plan or when you register the community server with the system console after installation.

This task must be completed separately for each server within a community server cluster, as well as for multiple non-clustered community servers.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
4. Click the Connectivity tab.
5. Under Trusted Servers, enter the IP address of the server that must connect to the Sametime Community Server in the New IP Address field, and click Add.

Note:
• If you have a cluster, type the IP addresses of the primary node and all secondary nodes, separating each address with a comma. Do not include the IP address of the deployment manager.
• For the media manager, enter the Conference Manager server IP address.
To delete an IP address from the list, select it and click Delete Selected.
6. Click OK.
7. Restart the community server for the change to take effect.
Managing community services

Community services settings support all online presence (or awareness), instant messaging, and chat features at a server-wide level. These settings supersede any feature settings that you set at the policy level for users or groups. Community services settings carry a greater weight.

Managing general community services

The general community services settings control the interaction of the IBM Sametime Community Server with an LDAP directory and the maximum number of users allowed on the server.

About this task

These settings must be addressed for each server within a Sametime Community Server cluster.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. Use the following table to set general server-wide settings for users of the Sametime Community Server.

Table 25. Server-wide settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of entries on each page in dialog boxes that show names in the directory</td>
<td>Controls the number of user and group names that display when a user browses the directory. When an user browses the names and groups in the directory, the directory entries (names and groups) are listed on &quot;pages&quot; in a dialog box. The default is 100 entries per page. It is best to use a setting between 100 and 200 entries. Higher settings cause more data to be transmitted on the network when a user browses the directory.</td>
</tr>
<tr>
<td>How often to poll for new names added to the Sametime community directory (minutes)</td>
<td>Controls how frequently the cache of user names is updated with new information from the directory. The Sametime Community Server maintains a cache that contains information about the users and groups in the community. This cache must be or refreshed periodically to ensure that users who have recently been added to a directory can be displayed in the presence lists of all Sametime clients. The update occurs only if changes are made to the directory during the update interval. The default setting is 60 minutes.</td>
</tr>
</tbody>
</table>
Table 25. Server-wide settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How often to poll for new servers added to the Sametime community (minutes)</strong></td>
<td>Controls the time interval in which the Sametime Community Server receives an updated list of all Sametime servers. If you have deployed more than one Sametime Community Server, the community services on each server must maintain a list of all other Sametime Community Servers in the Sametime community. Community services use this list to ensure that users who have different home servers or different home clusters can see each other in presence lists and communicate through instant messaging and chat. The default setting is 60 minutes.</td>
</tr>
<tr>
<td><strong>Maximum user and server connections to the community server</strong></td>
<td>Controls the maximum number of connections allowed to Sametime Community Server. The connections include both client connections and server-to-server connections. A client connection occurs when a user starts the Sametime client. Server-to-server connections occur when you have deployed multiple Sametime Community Servers and different home servers are specified for users. The limit is 20,000 connections.</td>
</tr>
<tr>
<td>Select the authentication type that users can use while logging into the Community server:</td>
<td>Controls the authentication type. When LTPA or Sametime Tokens option is selected, the Sametime Community Server accepts authentication tokens generated by both Single-Sign On (SSO) and the Secrets and Tokens databases on the Sametime Community Server. This option is selected by default. When LTPA only is selected, the Sametime Community Server accepts authentication tokens generated only by SSO (LTPA tokens).</td>
</tr>
</tbody>
</table>
  - LTPA or Sametime token
  - LTPA only

6. Click **OK**.
7. Restart the Sametime Community Server for settings to take effect.

**Saving transcripts of chats and meetings**

You can enable the Sametime Community Server to save transcripts from two-way and multiple-user chats and from chats in meetings. Two-way chats are managed with the server’s native Chat Logging application. Multiple-user chats and meeting chats are managed with the Places server application.

**Enabling local chat logging:**

Each text chat has a transcript, the record of the text messages exchanged between chat partners during a chat session. You can configure the IBM Sametime Community Server to automatically log all chats and announcements, making these transcripts available to users for viewing in their chat history. If chat logging is enabled, offline messages sent by the sender to an offline recipient are also logged.
Procedure

1. In a text editor, open the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: C:\Program Files\lotus\domino).

2. In the `[Config]` section, set the value for **CHAT_LOGGING_MANDATORY**.
   - **CHAT_LOGGING_MANDATORY=0** is the default behavior, which makes chat logging optional. If this line is missing, Sametime also uses the default behavior to make chat logging optional.
   - **CHAT_LOGGING_MANDATORY=1** enforces chat logging.

3. In the `[Config]` section, set the value for **REMOTE_CHAT_LOGGING** to 1.
   - **REMOTE_CHAT_LOGGING=0**, the default, does not enable remote chat logging.
   - **REMOTE_CHAT_LOGGING=1** ensures that a given server can enable remote chat logging for multiple-user chats and chats in meetings.

4. In the `[Config]` section, set the value for **CL_USE_USER_DN**. If this setting is not found, the server defaults to using the Sametime user ID as the user’s identifier for a chat log.
   - **CL_USE_USER_DN=0** uses the Sametime user ID as the user’s identifier for a chat log.
   - **CL_USE_USER_DN=1** uses the user DN and if the DN is not found, uses the Sametime user ID as the user’s identifier for a chat log. The DN may be either the Sametime user ID or another attribute. Announcement originators and recipients can only be identified by their Sametime user IDs. Banning and logging must be done with Sametime user IDs rather than DNs. Do not set the value to 1 if that behavior does not work for your environment.

5. In the `[ST_BB_NAMES]` section, set the value for **ST_CHAT_LOG**. The StChatLogFile library (or libstchatlogfile.so on AIX, Linux, and Solaris platforms) is a sample of how to implement a chat logging black box using the Sametime SDK.
   - **ST_CHAT_LOG=N/A**
     The default of *N/A* means that Sametime does not attempt to load any chat logging black box. If you do not want StChatLog.dll to be used by Sametime, leave the default of *N/A*; do not remove the line.
   - **ST_CHAT_LOG=File**
     The value *File* describes the suffix to an StChatLog base name of the chat logging black box library. For example, to load your StChatLogMyCustom.dll file, set the value to **ST_CHAT_LOG=MyCustom**.

   **Note:** The StChatLogFile sample is not supported, and is not recommended for use in deployment environments.


7. Log in to the Integrated Solutions Console.

8. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.

9. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.

10. Click the **Community Services** tab.

11. In the Server Features section, under **Enable chat logging**, select one of the following choices:
   - **Always**
With mandatory logging, the `sametime.ini` file must have this value to classify the server as a mandatory chat logging server:

```
CHAT_LOGGING_MANDATORY=1
```

- **When available**
  
  When logging is enabled when it is available, the `sametime.ini` file must have these values to allow remote chat logging:
  
  - `REMOTE_CHATLOGGING=1`
  - `CHAT_LOGGING_MANDATORY=0` (or is not provided)

- **Never**
  
  With logging set to Never, the `sametime.ini` file must have these values to allow remote chat logging for other servers:
  
  - `REMOTE_CHATLOGGING=1`
  - `CHAT_LOGGING_MANDATORY=0` (or is not provided)

12. Click **OK**.
13. Restart the Sametime Community Server for settings to take effect.

**What to do next**

To find out more IBM Sametime chat logging and how to extend its features, see this article in the Sametime wiki: New features of IBM Sametime 8.x chat logging and how to extend its SDK.

**Enabling remote chat logging for places:**

Mandatory chat logging server settings on a user’s home server determine if chat logging is mandatory for this server’s users. If a user has access to multiple-user chats or chats in meetings on servers that do not require mandatory logging, set up the server that manages a given n-way chat as a remote chat logging server to fulfill the mandatory chat logging requirement. Remote logging handles chat logs for multiple-user chats and chats in meetings if a local Chat Logging service is disabled (either Never chat logging mode is defined or a local Chat Logging service is down). The two-way chats are logged on the home server of the chat participants. If two-way chat participants have different home servers, the chat is logged on both servers. Mandatory chat logging configuration requires all servers in the distributed environment to be running Sametime 8.5.2.

**About this task**

A home server with mandatory chat logging must have the following settings to be recognized by remote logging servers:

- The server logging mode is set to **Always** in the Community Services tab in the Sametime System Console (or **STRICT** if set in `stconfig.nsf`).
- `CHAT_LOGGING_MANDATORY=1` flag is set in the `[Config]` section of the `sametime.ini` file.

All servers involved in remote logging must be configured like this:

- The server logging mode is set to **When available** or **Never** in the Community services tab in the Sametime System Console (or **OFF** or **RELAX** if set in `stconfig.nsf`).
- `REMOTE_CHATLOGGING=1` flag is set in the `[Config]` section of the `sametime.ini` file.
In most cases, the n-way chat logging is logged on users’ home servers. The one exception is if a user whose home server is set to mandatory chat logging joins a chat that is already being logged on a remote chat logging server. In that case, the n-way chat continues to be logged only on that server in Always logging mode. N-way chats are not logged on multiple servers.

Other chat logging settings are determined by the server’s chat logging black box. If chat logging fails, for example, if there is a database error, the chat log for a mandatory chat user is destroyed.

**Defining offline message settings for individual Community Servers**

Edit the `sametime.ini` file on a Sametime Community Server to change offline message settings that define the deletion task intervals, the server locale, and debugging levels.

**Procedure**

1. In a text editor, open the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`).
2. Navigate to the `[stofflinemessages]` section.
3. Edit or confirm the start time for the deletion task, which purges expired offline messages from the database. Run the deletion task during off hours if possible for best performance.
   - The `STOFFLINE_MSGS_DELETE_TASK_START_TIME` flag defines a specific start time for the deletion task, expressed in the format HH:MM:SS. Hours are defined in 24-hour format, from 00 to 23. Minutes are from 00 to 59 and seconds are 00 to 59. Without a start time set, the deletion task runs by default as soon as the StOfflineMessages application starts.
   - The start time goes into effect after the offline message service starts. A start time of `23:00:00` runs the deletion task at 11:00 PM if the service has been started before that time. As long as the service continues to run, the deletion task runs once every 24 hours.
4. Edit or confirm the value for the server locale in the `STOFFLINE_MSGS_LANGUAGE` flag. The default is `en`.
5. Edit or confirm the value for the debugging level. The value can be a number from 0 to 5. The default is 5, the highest level of debugging.
   - 0 - no debugging
   - 1 - SEVERE
   - 2 - WARNING
   - 3 - INFO
   - 4 - FINER
   - 5 - FINEST (highest level of debugging)
   - The offline messaging debugging log is stored in the Trace folder with other logs and is saved in the following format:
     `OfflineMessages_DATE_TIME_INDEX.txt`

**Allowing users to transfer files to each other**

Community Services allow users to transfer files to each other over the network while using Sametime Connect.
About this task

When you enable this feature, you should also set a file size limit and virus scanning preference.

Computer viruses can be spread through transferred files. To protect against this possibility, users should have current third-party anti-virus software installed. The Virus scan files setting should be enabled and set to scan all files.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. In the Server Features section, click Allow users to transfer files to each other.
6. To increase or decrease the size of files that users can transfer, enter a value in the Maximum file transfer size, in Kilobytes field.
7. Under Virus scan files, select one of the following choices:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>If scanning cannot be done, the file is not transferred</td>
</tr>
<tr>
<td>When available</td>
<td>The file is sent with a message that the file was not scanned, allowing the user to decide how to handle the file, or it is not sent if scanning reveals a virus</td>
</tr>
<tr>
<td>Never</td>
<td>Files are not scanned</td>
</tr>
</tbody>
</table>

8. Click OK.
9. Restart the Sametime Community Server for settings to take effect.

Allowing users to send announcements

Community Services allows users to send unencrypted announcements to others who are online in the Sametime Community.

About this task

When you enable this feature users can:

- Send unencrypted announcements to anyone who is online in Sametime Connect or in an online meeting. To receive an announcement, a user must be online, and in either active or away status. Users who are offline or have a status of “do not disturb” do not receive announcements.
- Allow the recipients of the announcement to respond to the announcement, or prevent them from responding.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.

4. Click the **Community Services** tab.

5. In the Server Features section, click **Allow users to send announcements (unencrypted one-way messages)**.

6. Click **OK**.

7. Restart the Sametime Community Server for settings to take effect.

### Managing anonymous access to virtual places

The Sametime Software Development Kit provides developers with the capability to build applications that create virtual places. Anonymous users can enter a virtual place and have awareness of other users in the same virtual place.

#### About this task

This capability to have awareness of other users in the same virtual place is sometimes called **place-based awareness**. **Place-based awareness** differs from **community-wide awareness**. With **community-wide awareness**, users can have awareness of any user in the community who is online. IBM Sametime Connect provides users with **community-wide awareness** functionality. Anonymous users are not allowed to have **community-wide awareness** in any Sametime clients.

The **Anonymous users can enter virtual places** field controls the ability of anonymous users to enter virtual places created by custom-built applications created with the Sametime Software Development Kit. For more information on virtual places, see the IMWC Directory and Database Access Toolkit documentation available from IBM developerWorks® at http://www.ibm.com/developerworks/lotus/downloads/toolkits.html.

Enter information for anonymous access to a virtual place. Each attendee who accepts the default name has a number added to the end (For example, User1, User2).

This task must be completed separately for each server within a Sametime Community Server cluster.

#### Procedure

1. Log in to the Integrated Solutions Console.

2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.

3. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.

4. Click the **Anonymous** tab.

5. Click the **Anonymous users can enter virtual places**

   **Note:** The following fields do not take effect unless the **Anonymous users can enter virtual places** field is selected.

6. If you want to let an anonymous user have a unique display name when accessing a Sametime application that includes awareness, click **Users of Sametime applications (databases such as stconf.nsf or websites) can specify a display name so that they do not appear online as "anonymous."** A display name entry dialog box appears when a user accesses the Sametime
application. This display name allows the anonymous user to be individually identified in any presence lists in the Sametime application.

Note: The ACL settings of the application must allow anonymous access, too.

7. If you want to have a domain name automatically appended to the display name entered by the user at the name entry dialog box, click Default domain for anonymous users.

8. If you want a name to appear by default in the name entry dialog box, click Default name. For instance, if the Default name field contains the entry User the first person entering a meeting sees User displayed by default in the name field of the name entry dialog box. If the person accepts the default and enters the application, the person is identified as User1 in any presence list in the application.

9. Specify the level of access that an anonymous user of an application enabled with Sametime technology has to the directory. You can limit an anonymous user's ability to view names in the directory. For example, you might prevent anonymous users from browsing all names in a directory or searching for names in the directory.
   • Users cannot browse or search the Directory
     Anonymous users cannot search or browse the directory.
   • Users can type names to add them to an awareness list
     Anonymous users can type text in an user search interface to search for person or group entries in the directory. However, users cannot view or browse a list containing all entries in the directory. Users might perform such searches to add users to a presence list.
   • Users can browse the directory (see a list of names) or type names (resolve users and groups)
     Anonymous users can type text in an user search interface and search for group or person entries in the directory. Anonymous users can also browse lists that contain all entries in the directory. When this option is selected, anonymous users can see all group and name entries in the directory, but cannot see the content of a group entry (the list of names within a group entry). Users cannot browse the LDAP directory on the LDAP server.
   • Users can browse the directory to see group content and names, or type names
     Anonymous users have all searching and browsing privileges described for the Users can browse the directory (see a list of names) or type names (resolve users and groups) setting above. In addition, users can search and browse within group entries in the directory and access the user and group names that are specified within group entries in the directory.

10. Click OK
11. Restart the Sametime Community Server for settings to take effect.

**Sending a message to all users**

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

**About this task**

Follow these steps to send a message to all users currently logged in to Community Services.
Procedure
1. Open a browser and navigate to the Sametime Community Server.
   Type the following address:
   http://host_name/servlet/auth/admin
   where host_name is the fully qualified host name of the server; for example:
   http://commsvr1.example.com/servlet/auth/admin
2. From the Sametime home page, click Administer the Server.
3. Log in as the Sametime administrator.
4. Select Message From Administrator.
5. Enter the message in the text box provided.
6. Click Send. You receive a confirmation that your message was sent.

Managing business cards
You can configure the IBM Sametime Community Server so that business card information about an individual displays when a user hovers over a name in a chat window or a contact list.

About this task
Business card can access user information from any of three types of storage repositories: the native Domino directory, the LDAP directory (including Domino LDAP), or a custom Notes application. Each repository stores user information differently, so to facilitate user searches, Sametime provides a search engine, called a black box, for each storage type.

Since there are three different storage types, Sametime provides three different black boxes to search for user information (one per storage type). These are:

- LDAP – used to search a LDAP directory
- Notes – used to search a native Domino directory
- Notes_custom_db – used to search a customized Notes application

Using information in the LDAP server or the native Domino directory, you can choose the fields that represent the information that you want to display in the business card. The available fields are:

- Photo
- Name
- Company
- E-mail address
- Telephone
- Address or location
- Title

You can set up or change the details you want to retrieve by changing the values for these fields on the main Business Card page.

Configuring business cards using an LDAP directory
Follow these steps to configure the business card using an LDAP directory. Domino LDAP is considered an LDAP directory.
Before you begin

Before you start setting up your business cards, be sure the following conditions are true for your site.

- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- All LDAP attributes needed by Business Card are accessible for query via anonymous connection or by using a specific bind account and password
- The Sametime Community Server is running

- **For Domino LDAP only:** To allow anonymous users to access required user details, you can edit the All Servers document in names.nsf. Under the LDAP tab, all LDAP attributes that you want to be retrieved by anonymous users should be added to the list of Anonymous Users Can Query.

About this task

This task must be completed separately for each server within a Sametime Community Server cluster.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.
4. Click the Business Card tab.
5. In the Business Card Contents section, select the attribute you want displayed in users' business cards, and then click Add to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click Remove.
6. Under Attribute Definition, choose Attribute Values that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose User Defined. The following table lists the default attribute value that is mapped to each attribute name.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

Table 26. Attribute names and values
Domino LDAP does not contain the **postalAddress** field. The value retrieved for this LDAP attribute is the concatenation of **City**, **State/Province**, and **Country**. Also, Domino LDAP contains a hidden field for the **ou** attribute. This field cannot be set through the Domino LDAP, and a third-party LDAP management tool can be used to add a value to it.

7. If you select **User Defined** for an **Attribute Value**, then enter an attribute to map to the **Attribute Name**.
8. Click **OK**.
9. Restart the Sametime Community Server.

**What to do next**

**Special considerations**

In a configuration where:
- Sametime is configured with LDAP
- UserInfo is configured to ignore configuration updates
- The Sametime ID is configured to an attribute different then a DN

You must add additional parameters to the `UserInfoConfig.xml` file to correctly support this type of Sametime ID.
1. Open the `UserInfoConfig.xml` file.
2. Locate the **StorageDetail** tag of the relevant LDAP and add the following flags:
   ```
   UserIdAttribute= <the chosen attribute for userid such as cn>
   PersonObjectClass= <the required object class such as OrganizationalPerson>
   ```
3. Save and close the file.
4. Restart the server.

**Configuring business card photos for Domino LDAP:**

To store photos in Domino LDAP and enable UserInfo to retrieve them, please follow the steps below. A third-party LDAP management tool is required for adding a JPEG Photo field to Domino LDAP. Most LDAP V3-compliant tools will work.

**Before you begin**

Configuring Business Card with an authenticated LDAP bind account is highly recommended. Allowing Anonymous LDAP Schema write access is a security risk and additional security changes to Domino Directory Access Control List may be required to allow anonymous write access to Domino LDAP.

**Procedure**

1. Use Domino Administrator to enable Domino LDAP write access. Within default **Configuration Setting Document LDAP**, click **Yes** next to **Allow LDAP users write access**.
2. Using the third party LDAP tool, connect to the Domino LDAP server and bind as a Domino Administrator. Once a successful connection is made, select a user and add an Attribute. The Attribute name for Domino LDAP should be specified as: `jpegphoto;binary` and the type should be selected as binary. Note the name being used for the attribute. If you use just `jpegPhoto` or `Photo` as the
name, depending on the LDAP tool, you might not be able to store images in the field. The `-;binary` is required for Domino LDAP to understand the binary data.

3. Use the third party LDAP tool to import the JPEG or GIF photo into the new field.

**Note:** The size of the image should be smaller than 64kb.

4. Use `ldapsearch` or the LDAP tool to check that the photo has uploaded successfully.

5. Log in to the Integrated Solutions Console.
   a. Click `Sametime System Console > Sametime Servers > Sametime Community Servers`.
   b. In the `Sametime Community Servers` list, click the deployment name of the server with the connectivity information that you want to change.
   c. Click the `Business Card` tab.
   d. In the Business Card Contents section, select the `Photo` attribute, and then click `Add` to include it in the business card.
   e. Under `Attribute Definition`, choose `User Defined` as the attribute value for `Photo`.
   f. In the User Defined column next to `Photo`, type `jpegphoto;binary`.
   g. Click `OK`.

   a. Expand the `Configurations > Servers`, and select the `Configurations` view.
      Open this document in `Edit` mode and click the `Basic` tab. Enable the `Use these settings as the default settings for all servers` option. The LDAP tab appears.
   b. Click the `LDAP` tab. Click `Choose Fields that Anonymous Users Can Query via LDAP`.
   c. Click `New` in the window that displays.
   d. Type `jpegphoto` in the field and click `OK` to save the value. Click `OK` again to close the window.
   e. `Save` and close the document.

7. Restart the LDAP server. From the server console, type `tell ldap quit` and then `load ldap`.


9. Browse to `UserInfoConfig.xml` file within the Domino Install folder. Under Details section, check to make sure `Photo` field is set to `jpegPhoto;binary`.
   ```xml```
   <Detail Id="Photo" FieldName="jpegPhoto;binary" Type="image/jpeg" />
   ```xml```

10. Restart the Sametime Community Server.

**Configuring business card photos for the Sametime browser client:**

Follow these steps to configure the business card photo that displays for users that chat using the IBM Sametime browser client.
Before you begin

Enable the PhotoURL attribute in your LDAP directory. Refer to the documentation for your LDAP directory.

Procedure
1. In the Sametime Community Server, find the UserInfoConfig.xml file.
2. Open the file with a text editor, and add the following tag to the Details section:
   <Detail Id="PhotoURL" FieldName="PhotoURL" Type="text/plain"/>
3. Restart the Sametime Community Server.
4. Upload user photos into a web server repository, so that users can access the photos using a URL. For example: http://iddirectory.mycompany.com/userphoto/mybuscardpic.jpg

Verifying business card configuration:

After you have configured your business card feature, you can verify the configuration.

About this task

To display user information, the business card uses an IBM Sametime Community Server application named UserInfo. UserInfo retrieves and delivers user information for each client request to view a user's business card. Follow these instructions to verify your business card configuration.

Procedure
1. Open \lotus\domino\UserInfoConfig.xml in a text editor. When you use an LDAP directory to store user information, the UserInfoConfig.xml should look like this:
   <UserInformation>
   <Resources> <Storage type="LDAP"> <CommonField CommonFieldName="MailAddress"/>
   <StorageDetails HostName="ldap.mycompany.com" Port="389" UserName="username"
Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2"
SearchFilter="(&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)
(mail=%s)))"/>
   <!-- Add another StorageDetails tag to support another ldap server. The listing order
implies the searching order -->
   <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->
   <SslProperties KeyStorePath="" KeyStorePassword=""/>
   <Details>
   <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
   <Detail Id="Name" FieldName="cn" Type="text/plain"/>
   <Detail Id="Title" FieldName="title" Type="text/plain"/>
   <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>
   <Detail Id="Company" FieldName="ou" Type="text/plain"/>
   <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
   </Details> </Storage>
   </Resources> <ParamsSets>
   <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
   <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
   </ParamsSets> <BlackBoxConfiguration>
   <BlackBox type="LDAP" name="com.ibm.sametimeuserinfo.userinfobb.UserInfoLdapBB"
MaxInstances="5"/>
   </BlackBoxConfiguration>
   </UserInformation>
2. Verify that stconfig.nsf has valid data for the LDAP document and the UserInfo document.

3. Verify that the HTTP server has been restarted after any changes have been made to the xml file.

Configuring business cards using a Domino directory
This task demonstrates how to configure the business card using the Domino directory.

Before you begin

Prerequisites:

- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Sametime authentication is configured to use a Domino directory
- The Sametime Community Server is running

About this task

Note: IBM recommends that you use a third party LDAP directory, and not Domino, because Domino does not have a standard field for photos (a jpegPhoto field). Using a third party LDAP directory avoids unnecessary replacement of the default jpegPhoto field.

Follow these steps to configure the Business Card to display data that is stored in a single data repository–a Domino directory.

Procedure

1. Open an Internet browser and enter this URL into the URL-locater field: http://example.com/stcenter.nsf, substituting the host name example.com with your server's actual host name.

2. Click Administer the server, and then log in as Administrator.

3. Click the plus sign next to Configuration to expand the contents, and then click Business Card Setup.

4. In the User Information section, select the entry you want displayed in users' business cards, and then click Add to move the entry to the right-side list box. To remove preselected entries, click the entry and click Remove. In most cases, the Attribute name and Attribute value section of the business card interface requires no modification; however, if the information you want displayed in the users' business cards is not mapped to the default fields provided by the users' person documents, then you might need to update the Attribute name and Attribute value section. The following table lists the default attribute value that is mapped to each attribute name.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
</tbody>
</table>
Table 27. Attribute names and values (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

5. Click **Update** to save the changes.

To display user information, the business card feature uses a server application called **UserInfo** which is designed to retrieve and deliver user information for each incoming request from a client to view a specific user's business card. To ensure this application is configured properly to search the proper data storage, confirm the settings as defined in **UserInfo.xml**.

6. Open the **UserInfoConfig.xml** file in a text editor. The file is located in the Domino program directory (``\lotus\domino\UserInfoConfig.xml``). Here is a section of the **UserInfoConfig** file edited for XYZ's scenario:

```
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
  <BlackBoxConfiguration>
    <BlackBox type="NOTES" name="com.ibm.sametimeuserinfo.userinfobb.UserInfoNotesBB" MaxInstances="4"/>
  </BlackBoxConfiguration>
</UserInformation>
```

**What to do next**

There might be specific configurations where the names in the Domino directory include commas (,). By default, these special characters are treated as LDAP separators. In order to treat them as regular characters, add the following flag to **UserInfoConfig.xml**:

```
<UseUnformattedNotesNames/>
```

This setting takes effect after the server is restarted.

**Photos in the Domino directory:**

The Domino directory does not have a standard field for photo, but photos can be retrieved from the Domino Name and Address Book (NAB) as follows:
1. Add a rich text field or rich-text lite field to the Person form of the Name and Address Book in Domino.
   a. Open names.nsf in Domino Designer.
   b. Open the Person form.
   c. Click the section where you want to add the field. A sub-form will open.
   d. In the sub-form, click where you want to add the field.
   e. Select Create > field from the menu, and edit the field’s properties.
   f. Add the name to the field and select Rich Text as the type.
   g. Save the form.

2. To store photo information in the newly-added rich-text field, choose either:
   - Import--click on the rich text field and choose Create > Picture. This adds the file contents to the field.
   - Attach--save the image file in the rich text field as an attachment.

3. Using the Sametime Administration tool, go to the Business Card Attribute page.

4. In the text box for the Photo attribute, type the name of the rich text field that you added to the Name and Address Book, above, matching the case, then click Update.

5. Restart the Sametime server.

Photo types used by Domino are .jpeg and .gif.

**Configuring business cards to use two repositories**

For retrieving business card information, you can set up a dual repository:

When you set up dual repositories, you set up a primary repository and a secondary repository:

**Primary repository** – The first storage repository search by the UserInfo application to retrieve user information; must always be the Sametime directory.

**Secondary repository** – The second storage repository searched by the UserInfo application to retrieve user information.

**Note:** The primary storage can never be of the same type as the second repository; for example, the primary and secondary storage cannot both be a Domino directory.

There are a variety of ways you can use dual repositories:

- The dual repository with Domino/LDAP directories
- The dual repository with LDAP/Domino directories
- The dual repository with Domino/Custom Notes databases
- The dual repository with LDAP/Custom Notes databases

**Configuring a dual repository with LDAP and a native Domino Directory:**

For retrieving business card information, you can set up a dual repository of a LDAP directory and a native Domino Directory.
Before you begin

This section describes how to configure the business card using two storage repositories: LDAP directory as the primary storage, a native (non-LDAP) Domino Directory as the secondary storage.

About this task

These directions assume the following:

- Lotus Domino & IBM Sametime Community Server have already been installed & configured to run properly
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- All LDAP attributes needed by business card accessible for query via anonymous connection or using a specific bind account/password
- The Sametime Community server is running
- Business card information can be retrieved from your Sametime directory
- A Notes database based off of the Domino directory template (pubnames.ntf) has been created and contains person documents for each corresponding user account defined in the Sametime directory. (In our example, this database is named bcardstorage.nsf; and the user accounts correspond to the accounts in the Sametime directory by users' email address.

Procedure

1. Using Lotus Notes, open your Directory Assistance database (typically da.nsf). If such a database does not exist, you must create one based upon the Directory Assistance template.

2. Click Add Directory Assistance to add an additional directory assistance document, and then specify the secondary storage. See the sample Directory Assistance document for the bcardstorage.nsf below:

Naming contexts (Rules) tab
Note: For Business Card purposes, the secondary storage does NOT have to be trusted for credentials.

Note: The directory assistance database must be listed on the Basics tab of the Sametime server document in the Directory assistance database name field. If it is not listed, fill in the field, and restart the Sametime server to effect that change.

3. Once you have completed the changes, save and close the document. The resultant Directory Assistance database may show the following:

4. Log in to the Integrated Solutions Console.
5. Click Sametime System Console > Sametime Servers > Sametime Community Servers.

6. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.

7. Click the Business Card tab.

8. In the Business Card Contents section, select the attribute you want displayed in users’ business cards, and then click Add to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click Remove.

9. Under Attribute Definition, choose Attribute Values that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose User Defined. The following table lists the default attribute value that is mapped to each attribute name.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

10. If you select User Defined for an Attribute Value, then enter an attribute to map to the Attribute Name.

11. In the Attribute Definition table, change the Attribute Value for the attributes that will be retrieved from the secondary storage to User Defined and leave the User Defined field blank. For example, if you are retrieving users’ Telephone and Title information from the Domino Directory; therefore, change the values for the Telephone & Title attributes to User Defined, and leave the User Defined field blank, and then click OK to save the changes.

   **Note:** These values are blank to ensure they are retrieved from the secondary repository (the Domino Directory) and not from the primary repository, which is the LDAP directory.

12. Modify the UserInfoConfig.xml file located in the Domino program directory (\lotus\domino\UserInfoConfig.xml) using a text editor. The UserInfo application fetches and delivers user information for each incoming client request (an user’s request to view a particular user’s business card). When you are using an LDAP directory as primary storage and a Domino Notes directory as secondary storage, make the following modifications. Add an additional Storage tag of Notes type within the Resources tag:
Note: The Details section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are retrieving Title and Telephone information from Domino.

13. To ensure Telephone and Title fields come from Domino, remove the following from the Details tag of the LDAP storage type:

```xml
<Detail Id="Title" FieldName="title" Type="text/plain"/>
<Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>
```

14. 13. Add the following to the `<BlackBoxConfiguration>` section. Make sure it is listed after the LDAP black box as the order defines the search order:

```xml
<BlackBox type="NOTES" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesBB" MaxInstances="4"></BlackBoxConfiguration>
```

Note: Since Sametime is the storage to be searched first by the UserInfo application, and the LDAP directory is the Sametime directory, the NOTES black box must be listed after the LDAP black box.

15. Once these changes are made, the UserInfoConfig.xml looks like this:

```xml
<UserInformation>
<Resources>
<Storage type="LDAP">
<StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username"
Password="password" SslEnabled="false" SslPort="636"
BaseDN="o=ibm" Scope="2"
SearchFilter="(&(objectclass=organizationalPerson)((cn=%s)(givenname=%s)
(sn=%s)(mail=%s)))"/>
<!-- Add another StorageDetails tag to support another ldap server. 
The listing order implies the searching order -->
<!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->
<SSLProperties KeyStorePath="" KeyStorePassword=""/>
<Details>
<Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
<Detail Id="Name" FieldName="cn" Type="text/plain"/>
<Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
<Detail Id="Company" FieldName="ou" Type="text/plain"/>
<Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
</Details>
</Storage>
<Storage type="NOTES">
<CommonField CommonFieldName="MailAddress"/>
<Details>
<Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
<Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
</Details>
</Storage>
</Resources>
<ParamsSets>
<Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
<Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
</ParamsSets>
<BlackBoxConfiguration>
<BlackBox type="LDAP" name="com.ibm.sametime.userinfo.userinfobb.UserInfoLdapBB" MaxInstances="5"></BlackBoxConfiguration>
```

Chapter 1. Administering
16. UserInfo must have a common field shared among the various storage repositories to retrieve data for a single user—from multiple sources. By default, the user’s email address is the common attribute, but any unique value may be used. If you prefer to use a different attribute, update the following field:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

17. Restart your Sametime Community and Domino servers to effect the changes.

Results

You have successfully configured the business card to display information for a single user from dual storage repositories: an LDAP directory and the Domino Directory.

Configuring a dual repository with LDAP and a custom application:

For retrieving business card information, you can set up a dual repository of an LDAP directory and a custom IBM Lotus Notes application.

Before you begin

This section describes how to configure the business card using two storage repositories: LDAP with a custom Lotus Notes application repository. Here, we describe how you can set up LDAP as the primary storage, and a custom Lotus Notes application as the second storage.

These directions assume the following:

- Lotus Domino & IBM Sametime Community Server have already been installed and configured to run properly
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- Business card information can be retrieved from your Sametime directory
- A custom Lotus Notes application based upon any template has been created and contains user records for each corresponding person document defined in the Sametime directory. (In our example, this custom application is named bcardstorage.nsf).
- To use a custom Lotus Notes application as a secondary repository, each user record in the custom application must have a common field whose unique value matches the value of the same field for the person in the Sametime directory. By default, the common field that is used is the internet email address).
- The view you use in this database must have at least one column sorted for every key. A sorted column must exist for the database field used as the common field.

About this task

Procedure

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console** > **Sametime Servers** > **Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the business card information that you want to add or change.

4. Click the **Business Card** tab.

5. In the Business Card Contents section, select the attribute you want displayed in users' business cards, and then click **Add** to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click **Remove**.

6. Under **Attribute Definition**, choose **Attribute Values** that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose **User Defined**. The following table lists the default attribute value that is mapped to each attribute name.

   **Table 28. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

7. If you select **User Defined** for an **Attribute Value**, then enter an attribute to map to the **Attribute Name**.

8. In the **Attribute Definition** table, change the **Attribute Value** for the attributes that will be retrieved from the secondary storage to **User Defined** and leave the **User Defined** field blank. For example, if you are retrieving users’ Telephone and Title information from the custom Lotus Notes application; therefore, change the values for the Telephone & Title attributes to **User Defined**, and leave the **User Defined** field blank, and then click **Reset** to save the changes.

   **Note:** These values are blank to ensure they are retrieved from the secondary repository (the Lotus Notes application) and not from the primary repository, which is the LDAP directory.

9. Modify the UserInfoConfig.xml file located in the Domino program directory (`\lotus\domino\UserInfoConfig.xml`) using a text editor. The UserInfo application fetches and delivers user information for each incoming client request (an user’s request to view a particular user’s business card). When you are using an LDAP directory as primary storage and a custom Notes application as secondary storage, make these modifications:

   a. Add the following **NOTES_CUSTOM_DB Storage** tag inside the Resources tag:

   ```xml
   <Storage type="NOTES_CUSTOM_DB">
   <StorageDetails DbName="bcardstorage.nsf" View="$BCardView"/>
   <Details>
   ```
Note: In the <StorageDetails> tag, the following settings are specified:

- **DbName** = database_path Filename of the custom Notes application (relative path to the domino data directory)
- **View** = view_name The name of the Notes view that displays the documents containing the user records.
- The <Details> section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are pulling the telephone attribute from the custom Notes application database.

b. The attributes Title and Telephone must come from the custom Notes application rather than from LDAP, so remove the following information from the <details> tag of the LDAP storage: 

   ```xml
<html>
   <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
</html>
```

c. Add the following information to the <BlackBoxConfiguration> section. Make sure it is listed after the LDAP blackbox as the list order defines the search order:

   ```xml
<html>
<BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametime.userInfo.userInfoBB.UserInfoNotesCustomBB" MaxInstances="4"/>
</html>
```

d. The UserInfoConfig.xml now looks like this:

```xml
<UserInformation>
<Resources>
<Storage type="LDAP">
<CommonField CommonFieldName="MailAddress"/>
<StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username" Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2" SearchFilter="(&(objectclass=organizationalPerson)|((cn=%%{givenname=%%}{sn=%%}{mail=%%})) (s=%%))">
<!-- Add another StorageDetails tag to support another ldap server.
The listing order implies the searching order -->
<!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->  
<SslProperties KeyStorePath="" KeyStorePassword=""/>
<Details>
   <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
   <Detail Id="Name" FieldName="cn" Type="text/plain"/>
   <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
   <Detail Id="Company" FieldName="ou" Type="text/plain"/>
   <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
</Details>
</Storage>
<Storage type="NOTES_CUSTOM_DB">
<StorageDetails DbName="bcardstorage.nsf" View="$BCardView"/>
<Details>
   <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
</Details>
</Storage>
</Resources>
<ParamsSets>
   <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
   <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
</ParamsSets>
<BlackBoxConfiguration>
<BlackBox type="LDAP" name="com.ibm.sametime.userInfo.userInfoBB.UserInfoLdapBB" MaxInstances="5"/>
<BlackBox type="NOTES_CUSTOM_DB"/>
</BlackBoxConfiguration>
</UserInformation>
```
UserInfo must have a common field shared among the various storage repositories to retrieve data for a single user–from multiple sources. By default, the user’s email address is the common attribute, but any unique value may be used. If you prefer to use a different attribute, update the following field:<CommonField CommonFieldName="MailAddress"/>

10. Restart the Sametime Community Server and the Lotus Domino server to effect the changes.

What to do next

You have successfully configured the business card to display information for a single user from dual storage repositories: an LDAP directory and a custom Notes application.

Configuring a dual repository with Domino Directory and LDAP:

You can configure Business Card with the use of two (dual) repositories–Domino and LDAP. The primary storage repository is the native (non-LDAP) Domino Directory, and the auxiliary storage is the LDAP directory.

Before you begin

These directions assume the following:
• IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
• Sametime authentication is configured to use an Domino directory
• The Sametime Community Server is running
• The LDAP server is running and is accessible by the Sametime Community Server
• All LDAP attributes needed by Business Card are accessible for query via anonymous connection or by using a specific bind account/password
• Business card information can be retrieved from your Sametime directory

About this task

Enter this URL in the address window of a browser: http://hostname/stcenter.nsf, using your server’s actual host name.

Procedure

1. Click **Administer the server**, and then log in as Administrator.
2. Click the plus sign next to Configuration to expand the contents, and then click **Business Card Setup**.
3. In the User Information section, select the entry you want displayed in users’ business cards, and then click **Add** to move the entry to the right-side list box.
   To remove preselected entries, click the entry and click **Remove**. The following table lists the default attribute value that is mapped to each attribute name in the **Attribute Names and Attribute Values** section.
Table 29. Attribute names and values

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

4. In the **Attribute Names and Attribute Values** section, remove the attribute values for the attributes that will be retrieved from the auxiliary storage. In the following example, the Telephone information is retrieved from the LDAP directory, so delete the value for the Telephone attribute. Removing attributes insures they are pulled from auxiliary storage, and not primary storage.

Table 30. Attribute names and values

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

5. Click **Update** to save the changes.

To display user information, the business card feature uses a server application called **UserInfo** which is designed to retrieve and deliver user information for each incoming request from a client to view a specific user’s business card. To ensure this application is configured properly to search the proper data storage, confirm the settings as defined in **UserInfo.xml**.

6. When Domino Directory is primary storage and LDAP is auxiliary storage, make the following modifications:

   a. Add the following LDAP `<storage>` tag within the `<Resources>` tag:

   ```xml
   <Storage type="LDAP">
     <StorageDetails HostName="ldap.austin.ibm.com" Port="389"
                     UserName="username" Password="password" SslEnabled="false"
                     SslPort="636" BaseDN="o=ibm" Scope="2"
                     SearchFilter="(&(objectclass=organizationalPerson)
                                  (|(cn=%s)(givenname=%s)(sn=%s)(mail=%s)))"/>
     <!-- Add another StorageDetails tag to support another ldap server. The listing order implies the searching order -->
     <Details>
       <Detail Id="Telephone" FieldName="telephonenumber" Type="text/plain"/>
     </Details>
   </Storage>
   ```

   Update the Storage details tag with the appropriate settings for your LDAP directory. The Details section defines the attributes that Sametime will
retrieve from the corresponding storage repository. In this example, we are pulling the **telephonenumber** attribute from the LDAP directory.

b. To ensure the telephone number is retrieved from LDAP, and not from Domino, remove the following from the <details> tag of the DominoNotes storage type:

```xml
<Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
```

After you have made these changes, the UserInfoConfig.xml file should look like the below:

```xml
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
        <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
      </Details>
    </Storage>
    <Storage type="LDAP">
      <StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username" Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2" SearchFilter="(&(objectclass=organizationalPerson) (|(cn=%s)(givenname=%s)(sn=%s)(mail=%s)))"/>
      <!-- Add another StorageDetails tag to support another ldap server. The listing order implies the searching order -->
      <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->  
      <SslProperties KeyStorePath="" KeyStorePassword=""/>
      <Details>
        <Detail Id="Telephone" FieldName="telephonenumber" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
</UserInformation>
```

c. So the **UserInfo** application can retrieve data for a user from multiple data sources, a common field must be shared among the storage repositories. This field must be unique for its corresponding directory. By default, users' email address are used as the common attribute. Consequently, users must be uniquely identified by their email addresses. If another attribute is preferred, the following line must be updated to reflect the field for that attribute:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

7. Restart your Sametime server and the Domino server to effect all the changes.

### Configuring a dual repository server with Domino Directory and a custom application:

---

Chapter 1. Administering 77
For retrieving Business Card information, you can set up a dual repository of a Domino Directory and a custom Lotus Notes application.

**Before you begin**

This section describes how to configure the Business Card using two storage repositories: Domino Directory with a custom Lotus Notes repository. Here, we describe how you can set up Domino Directory as the primary storage, and a custom Lotus Notes application as the secondary storage.

These directions assume the following:
- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Business card information can be retrieved from your Sametime directory
- A custom Lotus Notes application based upon any template has been created and contains user records for each corresponding person document defined in the Sametime directory. (In our example, this custom application is named bcardstorage.nsf).
- To use a custom Lotus Notes application as a auxiliary repository, each user record in the custom database must have a common field whose unique value matches the value of the same field for the person in the Sametime directory. By default, the common field that is used is the internet email address).
- The view you use in this database must have at least one column sorted for every key. A sorted column must exist for the database field used as the common field.

**Procedure**

1. Click **Administer the server**, and then log in as Administrator.
2. Click the plus sign next to Configuration to expand the contents, and then click **Business Card Setup**.
3. In the User Information section, select the entry you want displayed in users’ business cards, and then click **Add** to move the entry to the right-side list box. To remove preselected entries, click the entry and click **Remove**. The following table lists the default attribute value that is mapped to each attribute name in the **Attribute Names and Attribute Values** section.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

4. In the **Attribute Names and Attribute Values** section, if the information you want displayed in users’ business cards is not mapped to the appropriate attributes used in your company, then you may need to update it.
5. To prepare attributes for use by the auxiliary storage, in the attribute name/attribute value section, remove the values for the attributes that are to be
retrieved from the auxiliary storage. In this example, we are retrieving the Telephone information from the custom Notes application; therefore, you should delete the value for the Telephone attribute, and then click **Update** to save the changes. These values are removed to ensure the appropriate values are retrieved from the auxiliary data repository, and not the first.

**Table 32. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

6. Modify the `UserInfoConfig.xml` file located in the Domino program directory (`\lotus\domino\UserInfoConfig.xml`) using a text editor. The *UserInfo* application fetches and delivers user information for each user's request to view a particular user's business card.

   a. Add the following **NOTES_Custom_DB** Storage tag inside the Resources tag:

   ```xml
   <Storage type="NOTES_CUSTOM_DB">
   <StorageDetails DbName="bcardstorage.nsf" View="persons"/>
   <Details>
   <Detail Id="Telephone" FieldName="telephone" Type="text/plain"/>
   </Details>
   </Storage>
   ```

   **Note:** In the StorageDetails tag, the following settings are specified:

   - DbName = database_path Filename of the custom Lotus Notes application (relative path to the domino data directory)
   - View = view_name The name of the Notes view that displays the documents containing the user records
   - The Details section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are pulling the telephone attribute from the custom Lotus Notes application.

   b. Since the Telephone number must come from the custom Notes application, ensure the information is not retried from the Domino directory by removing the following information from the Details tag of the Notes storage:

   ```xml
   <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
   ```

   c. Add the following information to the BlackBox Configuration section. The Notes black box must come first since the listed order defines the search order:

   ```xml
   <BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametimeuserinfo.userinfoBlackBox">
   <UserInfoNotesCustomBB MaxInstances="4"/>
   ```

   **Note:** The Sametime directory must be configured as the primary storage so it can be searched first by the UserInfo application. In this example, the Domino directory is the Sametime directory; therefore, the NOTES_CUSTOM_DB black box is listed **AFTER** the Notes black box.
Now the UserInfoConfig.xml should look like this:

```xml
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
        <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
      </Details>
    </Storage>
    <Storage type="NOTES_CUSTOM_DB">
      <StorageDetails DbName="bcardstorage.nsf" View="persons"/>
      <Details>
        <Detail Id="Telephone" FieldName="telephone" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
  <BlackBoxConfiguration>
    <BlackBox type="NOTES" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesBB" MaxInstances="4"/>
    <BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesCustomBB" MaxInstances="4"/>
  </BlackBoxConfiguration>
</UserInformation>
```

7. So the UserInfo application can retrieve data for a single user from multiple sources, a common field must be shared among the storage repositories. By default (though any unique value may be used), the user's email address is the common attribute, so in both storage repositories, users must be uniquely identified by their email addresses. If you want to use a different attribute, you must update this line to show which attribute you plan to use:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

8. Restart the Sametime server and the Domino server to effect all the changes.

What to do next

You have successfully configured the business card to display information for a single user from dual storage repositories: the Domino directory and a custom Notes application.

Additional configurations for black boxes

Though IBM Sametime ships with two "black boxes" or special implementations already present for configuring with LDAP or IBM Domino, additional black boxes can be configured to retrieve data from more than one resource. A special configuration can be used to designate NOTES as its first box, if Sametime is configured with Domino, and with LDAP as its second black box.

For a Sametime installation that is configured to work with Domino but that can also retrieve data from Domino LDAP, Notes would be listed as the first black box, and LDAP as the second. Each of these special configurations requires manual settings in the UserInfoConfig.xml file.
This version of Sametime includes an additional black box that enables data retrieval from a separate Notes database (other than the Domino directory). This black box should be applied as a part of a special configuration designated to retrieve data from the Sametime directory and from an additional Notes database that contains users' business card details.

See the topic “Retrieving data from a customized database” for more information on how to configure data retrieval from the additional Notes database.

A newly-written black box or special implementation can be used to retrieve data from any selected data resource. The black box should be implemented and configured according to the Application Programming Interface (API) and to the instructions published with the Sametime Software Development Kit (SDK).

Starting with Sametime 8.5, the Sametime UserInfo service operates as both a server application and as a servlet. Customized black boxes can be configured differently for the servlet and for the server application.

To configure a customized black box for UserInfo servlet, follow these steps:
1. Add a black box JAR name to the LSTJava4 key value of the notes.ini file:
   
   LSTJava4=UserInfo.jar;custom_bb.jar; telephony_ext\TelephonyService.jar

   Here, custom_bb.jar is the customized black box jar name.
2. Save the notes.ini file.
3. Restart the Domino server.

To configure a customized black box for the UserInfo Sametime server application, follow these steps:
1. Add a full customized black box JAR path and name to the JVM_CLASS_PATH key under the [stuserinfo] subsection of the sametime.ini file:

   [stuserinfo]
   JVM_CLASS_PATH=C:\Program Files\IBM\Lotus\Domino\STCore.jar;C:\Program Files\IBM\Lotus\Domino\UserInfo.jar;C:\Program Files\IBM\Lotus\Domino\jvm\

   Here, custom_bb.jar is the customized black box jar name.
2. Remove the USERINFO_LOAD_SVC_IN_SERVLET=1 flag from the sametime.ini file (if it was included).
3. Save and close the sametime.ini file.
4. Restart the Community Server.

For additional help with these special configurations, please contact Support.

**Retrieving data from a customized database:**

For the user data included in the Business Card, Administrators can retrieve details about the user from separate Notes databases that are dedicated to storing user details and that function independently of the Domino directory that is used for Sametime.

**About this task**

Retrieving user data from customized Notes databases allows you to:
• Retrieve some details from the Sametime Domino directory and the rest from a customized Notes database (Domino)
• retrieve some details from the LDAP directory Sametime is configured to work with and the rest of the details from an additional Notes database.
An additional black box, which functions as a customized special implementation, is provided to enable data retrieval from the customized Notes database. This 'customized' black box should always be preceded by a call to the black box that handles the Sametime directory. A CommonField tag is used for synchronization between the black boxes. If the common field is defined as MailAddress, then the value retrieved for MailAddress from the first storage (LDAP or Domino) is used as the ID to query for in the customized database. The application first queries the database using the userID received as a parameter; if no record is found, it queries the database again, using the value retrieved for the CommonFieldName as userID. To use the customized database feature:

- Perform the following manual steps:

Procedure
1. Open UserInfoConfig.xml and update the CommonField tag in the first 'storage' section to hold the ID property of a Detail tag that represents the same detail in the different storage types. This detail tag is assigned a different field name in each storage section, but the value in each of these fields should be identical for the specific user. The default value for the Common field tag is "MailAddress." The attributes holding the email address for a user should have the same value in both storages.

2. Using the Administrator's Tool, update the Business Card attribute page with the values to be retrieved from the Sametime directory, leaving blank the field name for items required from the customized database.

3. Remove the Detail tags of the fields you left blank in the set-up page from the first 'storage' section in the UserInfoConfig.xml file.

4. Add an additional 'storage' section to the UserInfoConfig.xml as the second storage. This storage section is a new section added specifically for this feature; it differs from the standard Notes storage section through the additional parameters specified below:

   ```xml
   <Storage type="NOTES_CUSTOM_DB">
     <StorageDetails DbName="" View="$users" />
     <Details>
       <Detail Id="Location" FieldName="Location" Type="text/plain" />
       <Detail Id="Title" FieldName="JobTitle" Type="text/plain" />
       <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain" />
       <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain" />
       <Detail Id="Company" FieldName="CompanyName" Type="text/plain" />
       <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain" />
     </Details>
   </Storage>
   ```

5. In the newly-added "storage" section, delete the Detail tags of the items that you do not want to retrieve from this database, and update:
   a. The DbName property, including the full path
   b. The view name (if needed)
   c. The mapping of the 'Detail' tag so each item is mapped to the correct field name of the new database

6. Add a BlackBox tag to the BlackBoxConfiguration section in UserInfoConfig.xml as a second record:

   ```xml
   <BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametimeuserinfo.userinfobb.
   UserInfoNotesCustomBB" MaxInstances="4" />
   ```

7. Restart StConfiguration and the HTTP task.
What to do next

Note: For complete information on how to use these "black boxes" and on how to use all the storage repositories for LDAP, Sametime, and Domino, see the section in Business Card entitled "Using repositories." This section provides detailed information on how to store and retrieve user data contained in both single and dual repositories.

Mapping a detail to multiple attributes

An optional setting in UserInfoConfig.xml file lets you map a detail to more than one attribute. As a result, the returned value for a detail is composed of a list of attributes retrieved from the storage.

About this task

You can do this by mapping an item to a comma-separated list of attributes.

```
<Detail Id="Telephone" FieldName="telephoneNumber,mobile" Type="text/plain" />
```

The response can contain a list of values separated by any character chosen by the administrator. To apply the new separator, edit the UserInfoConfig.xml file.

Procedure

1. Open UserInfoConfig.xml in an editor.
2. Choose the Detail tag that you want to use to retrieve a list of attributes.
3. Complete the FieldName property with the list of attributes to retrieve, separated by commas.
4. Add an additional property: DisplaySeparator. Set its value to the required character that should appear in the response xml between any 2 retrieved attributes values. For example, `<Detail Id="Telephone" FieldName="telephoneNumber,mobile" Type="text/plain" DisplaySeparator="/"/>`
5. Log in to the Integrated Solutions Console.
   a. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
   b. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
   c. Click the Business Card tab
   d. Verify that the mapping of this detail (the Telephone detail in the example) is empty.
   e. Click OK.
6. Restart the server.

UserInfoConfig Debug tracing

If additional information is need to trace a problem, tracing information can be collected. To enable trace collection, set the USERINFO_DEBUG_LEVEL flag of the sametime.ini file.

1. Stop the IBM Sametime Community Server.
2. Set or add this flag in the debug section of sametime.ini file:

   USERINFO_DEBUG_LEVEL=5
The trace file will have a name and format like UserInfo_091021_1818.txt for the UserInfo Server Application and UserInfoHTTP_091231_2240.txt for the UserInfo servlet. You can find the file in the Trace folder.

**Linux and IBM i only:** If you are running Sametime Community Server 8.5.1 on Lotus Domino 8.5.2, then edit the domino_directory/servlets.properties file by removing UserInfoServlet from the servlets.startup= line.

3. Restart the Sametime Community Server.
4. When the server is fully started, send an http request using a web browser to activate the servlet.

**Resolving problems with business cards**

If Business Cards are not displaying user information as expected, check the server configuration, then the client, and finally, the business cards themselves.

**Checking the server configuration**

Check and validate the configuration on the storage repository you use with the Sametime Community Server. A configuration problem is the most likely cause of problems with Business Cards. For more information, see the appropriate section in Managing business cards.

**Checking the UserInfo servlet on the client**

The UserInfo servlet on the client receives and responds to client requests. The servlet must be working correctly to provide the requested details for Business Cards. Follow these steps to verify that the UserInfo servlet is responding correctly.

1. Determine the distinguished name (DN) of the user whose Business Card you want to view. Here are sample DNs of the various directory types:
   - Domino directory: cn=sametime User/O=IBM
   - Active directory: cn=Sametime User, cn=users,dc=austin,dc=ibm,dc=com
   - TDS directory: uid=Sametime user,ou=Austin,o=IBM

2. Compose a URL to simulate the HTTP request that the client makes to retrieve details for a Business Card:
   - [protocol]://[hostname]/servlet/UserInfoServlet?operation=3&setid=1&UserId=[User DN]
   - [protocol] = {http, https}
   - [hostname] = {Fully qualified hostname of the Sametime server}
   - [User DN ] = {The full distinguished name of the user for whose information you are seeking}

**Examples:**

- Domino Directory:
- Active Directory:
- TDS Directory:
  - http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=uid=Sametime user,ou=Austin,o=IBM

**Note:**
- Do not use spaces in the URL for the UserInfo servlet operation.
A space is translated into %20 in the URL, and the servlet will not produce a result; for example:

http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
User/O=IBM

is translated to:

http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=
 cn=Sametime%20User/O=IBM

. The characters "%20" are inserted before the word "User" to represent the space.

- The name "UserInfoServlet" is case sensitive.
- Do not use apostrophes or quotation marks in the URL.

3. Enter the URL you've composed into a web browser's address field, and view the result.

You should see the details you are expecting to see. If you do not, enable tracing for the UserInfo servlet as described in UserInfoConfig Debug tracing.

An UNKNOWN error for the "user id" means the user ID specified could not be located. The most common reasons for this error are:

- An incorrect user distinguished name has been specified
- The directory in which the user is located is not reachable/searchable

**Checking the client**

If the UserInfo servlet on the client is responding correctly, enable client-side tracing to determine what is happening on the client. Follow the instructions in Logging and tracing on Sametime Connect.

**Checking that Business Cards meet requirements**

Finally, verify that the business cards follow these requirements.

- Photos must be less than 45 kilobytes (recommended: 10 kb).
- Business Card photo requires .jpg or .gif.
- Using the jpegPhoto LDAP attribute to store photos requires the inetOrgPerson objectClass.

**Note:** Active Directory 2000 native/mixed mode does not provide inetOrgPerson objectClass by default.

- When you are using more than one storage type to store user information, the secondary storage repository cannot be of the same TYPE as the primary storage (the directory used by Sametime for authentication). For example, if Sametime is configured to use the Domino directory, then the secondary storage cannot also be a Domino directory.

**Changing user names**

After users have been registered in IBM Sametime, you can change their names if their user IDs must change due to a name or location change.
About this task

The name conversion tool or use the AdminP feature should be used for changing user names as needed. To eliminate the need to run name changes in the future, you can migrate older user IDs to a unique directory attribute, which requires you to run the name conversion tool only once. This can be done only for an LDAP directory and only when the names in the directory are already synchronized with Sametime.

Changing names as needed

When you change user or group names in the directory, the change is not reflected in IBM Sametime Community Server databases. In order to synchronize the directory names with the names in the Sametime Community Server databases, you must run the name conversion utility.

About this task

Running the name conversion utility updates Sametime Community Server user or group names with the latest directory changes. The name conversion utility uses a comma-separated value list that you compile to change names, delete names, or convert all names from Domino to Domino LDAP formatted names.

Users create a contact list, a privacy list, and an alert-me-when list in the IBM Sametime Connect client by selecting user names or group names from the Domino or Domino LDAP directory that is used with the IBM Sametime Community server. These contact, privacy, alert-me-when lists are stored in the user information database (vpuserinfo.nsf) on Sametime Community servers. When a user starts the Sametime Connect client, the lists are downloaded from the database to update the lists stored on the client’s local computer.

You do not need to run the name conversion utility when you add new users or groups to the Domino or LDAP directory.

Run the name conversion utility manually on a stand-alone Sametime Community server, or on a server in a cluster which will replicate the change throughout the cluster.

Note: Be sure to stop the Domino server before you run the name conversion utility.

The name conversion utility accepts the following name changes:

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Change specified first names, last names, display names, or group names.</td>
</tr>
<tr>
<td>ORGANIZATION</td>
<td>Change the organization name for all users.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Changes all contact list information from Domino directory format to LDAP format. For example, a user listed as CN=Maria Smith/OU=Sales/O=IBM changes to CN=Maria Smith,OU=Sales,O=IBM.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Remove specified individual contact names from contact lists and privacy lists.</td>
</tr>
</tbody>
</table>
Table 33. Descriptors for the name change utility (continued)

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>REPORT</td>
<td>This feature can be used to confirm a name change in the vpuserinfo.nsf database by taking snapshots before and after the change and comparing them.</td>
</tr>
</tbody>
</table>

Preparing for changing names:

Before you can run the name conversion utility, you need to perform the following tasks:

About this task

You do not need to use the name conversion utility if you add new users or groups to directory. Use the name conversion utility only if you change user names or group names that exist in the directory.

Creating a comma separated value file:

A comma-separated value (CSV) file created in a text editor provides the name conversion utility with the information it needs to make a name change to user contact, privacy, and alert-me-when lists. The CSV file includes the type of change and typically provides details such as the old name and the new name, and optionally, the display name.

Procedure

1. Use a text editor that supports UTF-8 saving format to create a comma-separated file.
2. Create a CSV for only one type of change; you cannot mix name change types in the same CSV.
   - ID
   - ORGANIZATION
   - DELETE
   - LDAP
   - REPORT
3. Name and save the file with an extension of .csv in a directory accessible by the Sametime server. The text file should be saved in UTF-8 format.

Syntax for comma-separated value file used in name change utility:

A CSV file created in a text editor provides the server with the information it needs to make a name change to user contact lists or privacy lists. The CSV file includes the type of change (or descriptor) and typically provides details such as the old name and the new name, and optionally, the display name.

You can create the CSV text file using any text editor. Some spreadsheet programs also allow you to export spreadsheet values to a CSV file. The CSV file should include only the list of comma-separated old name, new name pairs that reflect the changes you have made to the directory. Do not include any header information in your CSV file. Name the file at your discretion. After you create the CSV file, store
it in a network location that is accessible from the Sametime server. You must browse to this file to import it when you create the Name Change Task from the Administrator's tool in Sametime.

When you create a CSV file, you must format it correctly following the syntax rules below. CSV files are case-sensitive and sensitive to spaces. You can create multiple CSV files. The CSV file can include only one descriptor:

<table>
<thead>
<tr>
<th>Table 34. Descriptors for the name change utility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Descriptor</strong></td>
</tr>
<tr>
<td>ID</td>
</tr>
<tr>
<td>ORGANIZATION</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
<tr>
<td>DELETE</td>
</tr>
<tr>
<td>REPORT</td>
</tr>
</tbody>
</table>

Using the REPORT descriptor

To use the REPORT descriptor, create two CSV files in the trace folder that capture the vpuserinfo.nsf tables for user's contact list, alert me list, and privacy list. The CSV file names will be similar to:

- ConvertStorage_110308_0548.csv
  The first file contains the contact list and alert me list.
- ConvertPrivacy_110308_0548.csv
  The second file contains the privacy list.

This feature is also available for releases prior to release 8.5.2 as a hotfix. See Technote #1469735 for more information.

The second part of the CSV file includes one line for each change that includes the old name, the new name, and, optionally, the new display name. The following tables show the syntax for a variety of name changes.

Changing the user and group IDs
## CSV File Syntax Example

<table>
<thead>
<tr>
<th>ID</th>
<th>&quot;old ID&quot;, &quot;new ID&quot;[,&quot;new display name&quot;]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>

where the [] indicate that the new display name is optional but if you use it, you must precede it with a comma as in the first example (where "Maria Brown" is the new display name), and the new display name must immediately follow the comma (if you leave a blank space between the comma and the new display name, the conversion will not work).

### Sample CSV showing changes from a Domino directory:

<table>
<thead>
<tr>
<th>ID</th>
</tr>
</thead>
</table>
| "CN=Maria Smith/OU=Sales/O=IBM",
| "CN=Maria Brown/OU=Sales/O=IBM",
| "Maria Brown"
| "CN=John/OU=New York/O=IBM",
| "CN=John/OU=Texas/O=IBM"
| "52e811 85256500/Old Group",
| "52e811 85256500/New Group Name", |
| "New Group Name"|

Note that "52e811 85256500" in the example above is replica ID of Domino Directory. Be sure to change the colon in the replica ID to a space. For example: "52e811:85256500" should be "52e811 85256500".

### Sample CSV showing changes from an LDAP directory:

<table>
<thead>
<tr>
<th>ID</th>
</tr>
</thead>
</table>
| "CN=Maria Smith,OU=Sales,O=IBM",
| "CN=Maria Brown,OU=Sales,O=IBM",
| "Maria Brown"
| "CN=John,OU=New York,O=IBM",
| "CN=John,OU=Texas,O=IBM"
| "CN=Old Group,OU=groups,O=IBM",
| "CN=New Group Name,OU=groups,O=IBM",
| "New Group Name"

### Changing the organization name

<table>
<thead>
<tr>
<th>CSV File Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORGANIZATION</td>
<td>Sample CSV showing changes from a Domino or LDAP directory: ORGANIZATION &quot;lotus&quot;,&quot;ibm&quot;</td>
</tr>
</tbody>
</table>

### Changing all contact list information from Domino directory format to LDAP format (converts forward slashes in the hierarchical name to commas)

<table>
<thead>
<tr>
<th>CSV File Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Sample CSV: LDAP</td>
</tr>
<tr>
<td></td>
<td>You cannot change the format from LDAP to Domino.</td>
</tr>
</tbody>
</table>

### Deleting specified users and groups
CSV File Syntax | Example
--- | ---
DELETE uid | Sample CSV:
DELETE uid=John Deere,ou=sametime,dc=ibm,dc=com
uid=Marta Smith,ou=sametime,dc=ibm,dc=com
cn=portaladminid,o=example.com

Verifying a name change

CSV File Syntax | Example
--- | ---
REPORT | Sample CSV:
REPORT

Creating a Name Change task:

Create a name change task on the IBM Sametime Community server.

Before you begin

Before you create a name change task, create a comma-separated value (CSV) file of the name changes in the Sametime Community Server directory.

About this task

A name change task is not actually a scheduled program; its timestamp merely indicates when the task was created and not when it will be run. The list of tasks is ignored until you run the stnamechange.cmd program, which then operates on all of the tasks in the list, using the .CSV files specified in the Name Change page.

Follow the steps below to create a name change task.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server where you want to add a name change task. If you want to create a task to run on multiple servers, then click the deployment name of any of the servers on which you want to run the task.
4. Click the Name Change tab.
5. Click New.
6. Enter a name in the Name of Task field. The name is at your discretion. By default, the name is the date the task is created.
7. Optional: Enter a description for the task.
8. Browse for the CSV file you want to use, and then click OK.
9. The name change task appears in the list of scheduled tasks.
   All tasks listed here run when the stnamechange.cmd is run.

Note: If you only want to edit a task, you can click the name of the scheduled task to edit it.
Results

After you have completed these steps on one Sametime Community server, it is necessary to repeat this process on other servers in distributed environment.

When you are finished configuring the task, name changes are saved to the stnamechange.nsf file. For a clustered environment, create this task on one server per cluster. All other servers receive the changes through the cluster replication process.

Lotus Domino picks up all valid name change tasks in the stnamechange.nsf file. You choose the servers or cluster on which the name change task runs on a regular basis using general scheduling tools. The application does not run by default; you must run the task manually.

To Delete a name change task, on the Name Change page, select the task, and then click Delete. If any name changes are entered incorrectly, you can import a new CSV file.

Running the name conversion utility:

To run a name change task, start the name conversion utility. The name conversion utility uses the CSV file to update user contact and privacy lists with the latest directory changes.

Before you begin

Before you begin, create a comma-separated value file with name changes, and then create a name change task. IBM recommends running the name conversion utility at off-peak hours, and stopping the Domino server before you begin.

About this task

Starting the name conversion utility starts the name change task. You can create many tasks, but the name change conversion utility executes only one task at a time. You can have only one name change task scheduled or in progress. If a name change task is scheduled or in progress, you cannot create another name change task until the existing name change task completes.

It is not necessary to run the name change conversion utility on every IBM Sametime Community Server in a cluster. For clusters, the task should run once on one server and then replicate to other servers in the cluster.

Running the name conversion utility on Windows:

Follow these steps to run the name conversion utility on Microsoft Windows.

Procedure
1. Stop the IBM Sametime Community Server and the Lotus Domino server.
2. Type the following command:
   stnamechange.cmd
3. When the name change task completes, restart the Sametime Community Server and the Lotus Domino server. Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Running the name conversion utility on UNIX:

Follow these instructions to run the name conversion utility on a UNIX operating system.

Procedure
1. Stop the IBM Sametime Community Server and the Lotus Domino server.
2. Open a new shell and change to the domino data directory.
   `cd /domino/notesdata`
3. Type the following command:
   `./stnamechange.sh domino_bin_directory domino_data_directory`
   For example:
   `./stnamechange.sh /domino/opt/lotus/notes/80020/linux /domino/notesdata`
4. When the name change task completes, restart the Sametime Community Server and the Lotus Domino server. Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Running the name conversion utility on IBM i:

Follow these instructions to run the name conversion utility on an IBM i operating system.

Procedure
1. Stop the IBM Sametime Community Server.
2. From an IBM i command line, run the "QSH" command. This command starts the QShell interpreter, where the Name Change task is run.
3. Type the following commands:
   `cd server data directory`
   `stnamechange server_data_directory domino_bin_directory`
   where `domino_bin_directory` is an optional parameter. The default directory is `/qibm/proddata/lotus/notes`, which causes the command to use the latest version of Lotus Domino installed on the system.
If the Sametime Community server is using an earlier release of Domino, specify the appropriate Domino bin directory.

<table>
<thead>
<tr>
<th>Lotus Domino version used by Sametime Community server</th>
<th>Associated domino bin directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino 8.5.2</td>
<td>/qibm/proddata/lotus/domino852</td>
</tr>
<tr>
<td>Domino 8.5.1</td>
<td>/qibm/proddata/lotus/domino851</td>
</tr>
<tr>
<td>Domino 8.5.0</td>
<td>/qibm/proddata/lotus/domino850</td>
</tr>
<tr>
<td>Domino 8.0.2</td>
<td>/qibm/proddata/lotus/domino802</td>
</tr>
<tr>
<td>Domino 8.0.1</td>
<td>/qibm/proddata/lotus/domino801</td>
</tr>
<tr>
<td>Domino 8.0.0</td>
<td>/qibm/proddata/lotus/domino800</td>
</tr>
</tbody>
</table>

4. When the command completes, press **F3** to exit QSH. To verify whether all of the names were changed successfully, view the following files in the /trace subdirectory of the server data directory:

- namechange_YYMMDD_XXXX.txt
- name_change_summary_report_YYMMDD_XXXX.log

If you encounter problems, add `VP_NCSA_TRACE=1` to the Debug section of the sametime.ini file to collect additional debug information when you run the name change utility.

5. Restart the Sametime Community Server.

   Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

*Name Change task replication:*

When you create a name change task, the task is saved in a file called stnamechange.nsf, and this file is replicated to all home IBM Sametime Community Servers so that updates can be made to each server's vpuserinfo.nsf database. The file vpuserinfo.nsf is the Sametime user information database that contains contact lists and privacy lists.

Set up a Domino replication task to replicate stnamechange.nsf among all servers. By default, stnamechange.nsf is replicated to all servers in a cluster, but not between clusters. This step makes it unnecessary to add future tasks to each stnamechange.nsf database in the environment. When a new task is added, all servers get the new information as a result of the replication procedure.

Note that the **All servers** option on the name change page in the Sametime System Console does not work because of the procedure for replicating across all servers. If you create a name change task and select **All servers**, only the server you are logged on to contains the task—other servers do not. This is viewable in stnamechange.nsf through the Notes client. The correct procedure is to create the name change task on all the servers in the community.

If several Sametime Community Servers operate as a cluster, create a name change task on only one server in the cluster. The **vpuserinfo.nsf** database replicates in real time among the servers in the cluster. When the name change task changes the vpuserinfo.nsf database on one server, the changes are automatically replicated to the vpuserinfo.nsf databases on all other servers in the cluster. Declaring the task in one cluster can populate all the clusters because you set replica information for the stnamechange.nsf between all the clusters.
Sample deployments

The examples below illustrate how you might run name change tasks in different Sametime Community Server deployments.

Example Deployment 1

In this example, the Sametime community has the following characteristics:

Three Sametime Community Servers are deployed.

None of the servers are clustered.

With this deployment, you must create and run the name change task three times—one on each server. Though you create the task only once, you run it three times, and the run can be scheduled automatically.

Example Deployment 2

In this example, the Sametime community has the following characteristics:

Eight Sametime Community Servers are deployed.

Three Sametime Community Servers operate as Community Services cluster 1.

Three Sametime Community Servers operate as Community Services cluster 2.

Two Sametime Community Servers operate as home Sametime Community Servers but are not part of a Community Services cluster.

With this deployment, you must run the name change task four times. You can schedule the tasks to run automatically on one Sametime Community Server in Community Services cluster 1, on one Sametime Community Server on Community Services cluster 2, and on each of the two Sametime Community Servers that operate as home Sametime Community Servers but are not part of a cluster.

Example Deployment 3

In this example, the Sametime community has the following characteristics:

- Six Sametime Community Servers are deployed
- Three Sametime Community Servers operate as a Community Services cluster
- Two Sametime Community Servers operate as home Sametime Community Servers but are not part of a Community Services cluster
- One Sametime server is not used as a home Sametime server and is not part of a Community Services cluster

With this deployment, you must create the name change task three times. Create the name change task on one of the Sametime Community Servers in the Community Services cluster and on each of the two Sametime Community Servers that operate as home Sametime Community Servers but are not part of a cluster. You do not need to create the name change Task on the Sametime Community Server that is not part of a cluster.

Name Change task status:
This topic describes the status of the name change tasks, how to view tasks in progress, and how to delete a name change task.

After you create a name change task, the task defaults to the **Scheduled** status. A scheduled task begins executing on the IBM Sametime Community Server at the time specified in the server setting on the Name Change page of the Sametime System Console (**Sametime System Console > Sametime Servers > Sametime Community Servers > server_name > Name Change**). You cannot edit a name change task that has the **Scheduled** status. The only way to change a scheduled task is to delete the task and then create a new task in its place.

Once a task begins executing, its status changes from **Scheduled** to **In Progress** if any of the servers have the name change task with the status that is in progress or scheduled. You cannot delete a task that is in progress. If all the servers have tasks that are marked **Check error log** or **Disabled**, the name change task can be marked **Finished**.

**Finished** means the task has completed the name change successfully. At this status level, you can add or delete any task.

**Check error log** means there were errors incurred while the task was running. At this stage, you can add or delete a task.

**Note:** The status column provides only the status of the task running on the server being used; it does not provide a summary of the task across servers and clusters of servers.

You can have only one name change task scheduled or in progress on a IBM Sametime Community Server. If a name change task is scheduled or in progress, you cannot create another name change task on the Sametime Community Server until the existing name change task completes.

You cannot delete a task that is marked **In Progress**. You can delete a task that is marked **Scheduled**, **Finished** or **Check log status**. There is a log file on the server that collects failures in Name Conversion.

- A user name that is changed in the directory but is not yet changed in the vpuserinfo.nsf database will appear as offline in the contact list and privacy list of another user until the name change task executes on the other user's home Sametime Community Server.
- All members of a changed group appear as offline in the contact list and privacy list of a user until the name change task executes on the user's home Sametime Community Server.

You can view the status of the names being changed. The **vpuserinfo.nsf** database includes a view for name change tasks. The task you are running is not marked complete. If several Sametime Community Servers operate as a Community Services cluster, you view the status of a name change task on only one Sametime Community Server in the cluster. The database replicates in real-time among the servers in the cluster. When the name change task changes the vpuserinfo.nsf database on one server, the changes are automatically replicated to the vpuserinfo.nsf databases on all other servers in the cluster.

Below is an example of viewable statuses. In the example, Servers X, Y, and Z are not clustered, and servers A, B, and C are clustered.
<table>
<thead>
<tr>
<th>Servers</th>
<th>task is created on Server X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server X</td>
<td>task appears in Name Change page</td>
</tr>
<tr>
<td>Server Y</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server Z</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server A</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server B</td>
<td>task does NOT appear in the Name Change page, and it does NOT appear in the log file</td>
</tr>
<tr>
<td>Server C</td>
<td>task does NOT appear in the Name Change Status page, and it does NOT appear in the log file</td>
</tr>
</tbody>
</table>

**Note:** Turn on the sametime.ini flag if you are working locally:

```
NC_LOCAL_CONVERSION = 1
```

**Name Change summary report:**

After you run the name conversion utility, review the summary report to verify successful name changes and find any that were unsuccessful.

When the utility runs, it creates a log file that summarizes the errors found during the conversion. It stores the log file in the trace folder with a name that includes the time and date that the utility ran, such as `name_change_summary_report_110308_0548.log`.

The following excerpt from a log indicates that seven name changes were unsuccessful. In such a case, you would contact IBM Support for additional information.

```
processing vpuserinfo.nsf:
- user id = [3YUKI@jp.ibm.com], attribute = [XML buddylist] : failed to process attribute
- user id = [40164@pl.ibm.com], attribute = [XML buddylist] : failed to process attribute
- user id = [40337@pl.ibm.com], attribute = [XML buddylist] : failed to process attribute
- user id = [4gvn@us.ibm.com], attribute = [XML buddylist] : failed to process attribute
- user id = [60757@pl.ibm.com], attribute = [classic buddylist] : failed to read attribute
- user id = [61815894@at.ibm.com], attribute = [XML buddylist] : failed to process attribute
- user id = [61815894@at.ibm.com], attribute = [XML buddylist] : failed to process attribute

Statistics:
- number of users scanned: 388
- number of users that their document was changed: 0
- number of users that had an error during their change: 7
```

**Changing names with AdminP**

This feature allows IBM Sametime to synchronize name change updates made to the IBM Lotus Domino directory via the Domino Administration Process (AdminP) with updates to Sametime User Information database (vpuserinfo.nsf).
Prior to Sametime 8.0.1, when a Lotus Domino Administrator executed name changes through the Lotus Domino Administrator client and the AdminP process, the users' names were changed automatically in the Lotus Domino Directory but were not changed in the corresponding Sametime records. The administrator had to manually generate a CSV text file that contained the renaming information, and run the Sametime name change utility on one or more servers, depending on the configuration.

In Sametime 8.0.1, this process is enhanced, allowing Sametime to update VPUserInfo.nsf and add a new CSV text file to stnamechange.nsf whenever a change is made in the Domino Directory.

Note: It is still necessary to manually run the name conversion utility even when AdminP integration code is working. The Name Change Integration with AdminP feature creates a new Name Change task and only partially updates vpuserinfo.nsf. For example, it does not update the contact lists that include the old name. For a full update, the Name conversion utility must be executed.

In addition, the AdminP functionality is only available for Sametime servers that use Lotus Domino authentication running on Lotus Domino 8.0.2 or later. If the Sametime server is using LDAP authentication, or if you are using a version of Lotus Domino earlier than 8.0.2, you cannot use the AdminP feature to change names.

AdminP integration components

The following components contain the code for the Name change integration with AdminP feature. These components are located under the Domino program directory (by default \Lotus\Domino in Windows):

- StUpdateAdminP.dll -- the code loaded by the AdminP process. This DLL file receives notifications from Domino regarding renaming operations. We will refer to it as the AdminP add-in.
- AdminUpdate.jar -- the java code executed by the StUpdateAdminP.dll
- NameChangeUtils.jar -- a library that provides services of updating the different Sametime databases. called by AdminUpdate.jar to perform the actual change in vpuserinfo.nsf and stnamechange.nsf

Known issues with AdminP integration

Please note the following issues concerning AdminP integration with Sametime:

- This feature is supported starting in Domino 6.0, but is currently not available with Domino 8.0.1.
- In Sametime, this feature is supported starting with release 8.0.1.
- Only name updates are handled; deletions and additions are not supported by AdminP.
- To complete the name change process, you must still execute the name change application (AdminP integration simplifies the process but does not replace it)
- When Sametime databases are being updated as a result of the AdminP operation, warning messages are seen on the Domino console. These messages are not an indication of any issue with the process and should be ignored.

Enabling AdminP integration:
The name change AdminP integration will run on one Sametime server in each cluster, is part of a Sametime server installation, and is disabled by default.

**Before you begin**

The name change AdminP integration functionality is only available for Sametime 8.0.1 servers hosted on Microsoft Windows and configured to use IBM Domino Directory for authentication. If your deployment uses an LDAP directory, you must use the Name Conversion utility as in previous releases. For information on the Name Conversion utility, see the topic, "About the Name Conversion utility" in this Sametime information center.

**About this task**

Enable the AdminP integration for your Sametime environment by completing the following steps:

**Procedure**

1. Remove the comment marker from the following statement in the notes.ini file:
   
   `EXTMGR_ADDINS=StUpdateAdminP.dll`

   If there are multiple servers in one community, only perform this step on one server.

2. Using a text editor, open sametime.ini and confirm that the following flags are set as follows:

   ```
   ST_JAVA_CLASS_PATH=C:\Lotus\Domino\java;C:\Lotus\Domino\StConfig.jar;C:\Lotus\Domino\AdminpUpdate.jar
   ST_JAVA_JVM_PATH=C:\Lotus\Domino\ibm-jre\jre\bin\classic\jvm.dll
   ST_JAVA_LIB_PATH=C:\Lotus\Domino
   ```

   The paths may be different based on your deployment.

   **Note:** Ensure ST_JAVA_CLASS_PATH contains the full path of the AdminpUpdate.jar file (the default path is `C:\Lotus\Domino\AdminpUpdate.jar`).

3. If the Sametime community consists of more than one Sametime server, ensure that the following databases are replicated among all of the servers in the community: names.nsf, admin4.nsf.

   A Domino administrator can configure Connection documents to ensure these databases are replicated on a defined schedule. For more information on how to create Connection documents, see the "Scheduling server-to-server replication" topic in the Domino Administrator Help information center.

   Now the environment is setup properly for Sametime to capture name changes carried out by the AdminP.

4. Run the stnamechange.cmd as described in the topic, "Running Name Change Tasks on Sametime servers in a community" in this Sametime information center.

**Specifying an administration server for databases:**

AdminP uses administration servers to manage administrative changes that apply to IBM Domino databases. Either the administrator or the database manager can specify the administration server for a database. Perform this procedure on an as-needed basis.
Before you begin

To change the administration server for a Domino database, you must have Manager access to the database or be designated as a Full access administrator on the Security tab of the Server document.

About this task

Procedure

1. From the IBM Lotus Domino Administrator, open the domain containing the server with the database for which you are setting an administration server.
2. From the Servers pane, select the server containing the database you are setting as an administration server.
3. Click the Files tab and then select the database to which you are assigning an administration server.
4. From the "Tools" pane, click Tools > Database > Manage ACL.
5. Click Advanced.
6. Complete these fields and then click OK:

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Server</td>
<td>Choose one of these:</td>
</tr>
<tr>
<td></td>
<td>• None -- If you do not want an administration server assigned for the database.</td>
</tr>
<tr>
<td></td>
<td>• Server -- Select a server from the list.</td>
</tr>
<tr>
<td></td>
<td>Choose one of these according to whether you want modifications to the indicated fields to occur during a rename group, rename user, or rename server action; or during a delete server, delete group, or delete user action:</td>
</tr>
<tr>
<td></td>
<td>• Do not modify Names fields -- Names fields are not updated during any of the above rename and delete actions.</td>
</tr>
<tr>
<td></td>
<td>• Modify all Readers and Authors fields -- Reader and Author fields are updated during the rename and delete actions listed above.</td>
</tr>
<tr>
<td></td>
<td>• Modify all Names fields -- All names fields are updated during any of the rename or delete actions listed above.</td>
</tr>
</tbody>
</table>
7. If you will be processing administration requests across domains, complete the procedure in the topic "Creating a Cross-domain Configuration document" in the Domino Administration information center.

Sample configurations:

AdminP operates with various configurations of the IBM Sametime server and IBM Domino.
Sametime and the Domino Directory are hosted on the same machine

The Sametime and Domino directory are on the same server. When a rename is made the AdminP add-in is notified and the callback updates the relevant databases. After the Name Change Utility is run all users can see each other’s updated names.

Two or more Domino servers, each hosting Sametime and a Domino Directory

The Domino directories are replicated between all servers. Names.nsf and admin4.nsf are replicated on all servers. A name change executed on either one of these servers will trigger the AdminP process on both servers. Each AdminP process updates only the database that their administration server matches. This setting avoids replication conflicts.

Domino Directory hosted remotely from Sametime but within the same Domino domain

One or more Sametime servers and Domino directory are in the same domain. Each Sametime server accesses the Domino Directory through the directory assistance feature. Since all are in the same domain and the remote directory is accessed through da.nsf, updates are done on the remote directory and are
received on the Sametime server. The Sametime server triggers the update of the databases that set their administration server to be the local server and activate the callback in the AddIns.

**Domino Directory hosted remotely from Sametime, in a different Domino domain**

This time, the Sametime servers and the Domino directory are in different domains. For rename updates to go from the Domino directory on Domain A to the Sametime servers on Domain B, a cross domain configuration should be applied on these domains. When a name is updated on the directory in domain B, a mail message is sent to domain A (assuming cross domain configuration is applied). This mail message is treated as a request for the AdminP and is added to the admin4.nsf which logs the request for the AdminP process.

Refer to the Domino Administration guide for additional information on cross-domain configuration.
Domino Directory hosted remotely from Sametime, in a different Domino domain, and not serving as primary directory

The Sametime servers and Domino directory are in different domains, and the Domino directory is not the primary directory for the deployment.

As in the previous configuration, the Cross Domain Configuration should be applied and the da.nsf on the Sametime servers should point to the required NAB in the remote Domino server (instead of names.nsf).

Two or more Domino Directories on remote servers, replicated with one or more Sametime servers

The Sametime servers and the Domino directories are in different domains. A Cross Domain Configuration should be applied and the da.nsf on each Sametime server should point to the required NAB in the remote Domino cluster. One server in the Domino environment (domain B) should be defined as the Administration server of the Primary address book for the Domino Domain. The da.nsf of each Sametime server should point to the NAB on this server.

[Diagram showing the relationship between Domino and Sametime servers in different domains, with replication and cross domain configuration.]
Changing a person's name with AdminP:

You can use the AdminP feature to change a user's name in IBM Sametime.

About this task

To change a name in an environment with the AdminP add-in enabled:

Procedure

1. From the IBM Lotus Domino Administrator, click the People & Groups tab.
2. In the left-hand column, choose People under the selected directory.
3. Select the name that you want to change; for example, "Sara Lester".
4. On the right-hand side, select the People tab and choose Rename.
5. In the 'Rename selected HTTP, POP3, and IMAP people' dialog box, specify the time frame allowed for a user to login with both the old and the new names and click Next.
6. Now select a user name, fill in information in the appropriate fields to change the name, and click Next.

For example, to change Sara's last name from "Lester" to "Webster," type Webster in the Last Name field. Domino processes these name changes periodically (every 60 minutes by default). When the process is complete, the changes are reflected in vpuserinfo.nsf and stnamechange.nsf as follows:

- In vpuserinfo.nsf, the storageUserId of the renamed user is changed to the new name. For example, "Sara" storageUserId is changed from "CN=Sara Lester" to "CN=Sara Webster".
- In stnamechange.nsf, a new name change task is created, containing a CSV file that describes the name change.

An adminp.csv file containing your changes is then attached to the newly created task. For example, the adminp.csv file for changing Sara’s last name looks like this:

| ID | "CN=Sara Lester/O=ExampleCorp", "CN=Sara Webster/O=ExampleCorp", "Sara Webster/ExampleCorp" |

7. Run the stnamechange.cmd to complete the name change process.

For more information, refer to the topic "Running Name Change Tasks on Sametime servers in a community" in this Sametime Information Center. Additional information is available in the Tech Note "NameChange administration tasks in Sametime 8" at the following web address:

http://www.ibm.com/support/docview.wss?&uid=swg21290627

Troubleshooting AdminP integration:

If your AdminP integration does not work properly, use the information below to help resolve issues.

The AdminP feature is not working

1. Ensure the AdminP name change add-in is enabled by the following line in the notes.ini:

EXTMGR_ADDINS=StUpdateAdminP.dll

2. Turn on the trace files flags, rename in the directory, and analyze the trace files.

The trace files indicate that the JNI does not find the java class

1. Ensure the following files are located in the program directory:
• nadminp.exe
• StUpdateAdminP.dll
• AdminpUpdate.jar
• NameChangeUtils.jar
• stnamechange.jar

2. Ensure the following directory flags in sametime.ini have the correct values:
• ST_JAVA_CLASS_PATH
• ST_JAVA_JVM_PATH
• ST_JAVA_LIB_PATH

Working with trace files:

Trace files are located in the trace directory.

The Trace flags are located in the [Debug] section of sametime.ini:
VP_ADMINP_UPDATE_TRACE=1
ADMINP_ADDIN_DEBUG_LEVEL=5

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>StUpdateAdminP_080608_1046_2508_000.txt</td>
<td>C trace files</td>
</tr>
<tr>
<td>stupdateJava_080608_1122.txt.0</td>
<td>Java code trace files for the AdminP name change addin and Name Change API together</td>
</tr>
</tbody>
</table>

Validation

Do the following to validate that a name change worked:
1. Rename a user in the Domino directory.
2. On the Domino console, type: r tell adminp process all (this will process all the AdminP requests immediately).
3. Verify that a new task with the correct name change was added to stnamechange.nsf.
4. Verify that the user’s “StorageUserld” value was renamed.

Updated trace information

Verify that the StUpdateAdminP_080624_1451_3192_000.txt trace file contains a line similar to the following:
080624_145626, INF, DEBUG , JNI call completed for name = CN=Sara Lester/O=ExampleCorp

Verify that the stupdateJava_080624_1456.txt.0 trace file contains lines similar to the following:
Jun 24, 2008 2:56:23 PM
com.ibm.sametime.stupdate.StUpdateDBs updateDb
FINE: from java method old name is CN=Sara Lester/O=ExampleCorp newName = CN=Sara Webster/O=ExampleCorp

Jun 24, 2008 2:56:23 PM
com.ibm.sametime.namechangeutils.NameChangeUtils createChangeNameTask
INFO: completed.
Changing the IP address of an IBM i Sametime Community Server

Your IBM i Sametime Community Server should be set up so that it uses host names and does not refer directly to IP addresses. This allows you to change the IP address for your Sametime Community server by simply updating the host table and DNS.

About this task

To change the IP address for your Sametime Community server, follow these steps:

Procedure

1. Update your host table so that the new IP address is associated with the appropriate host name. Make sure that the fully qualified host name is listed first among the entries for your IBM i Sametime Community Server, before any short names. For more information, see “Updating the host table on IBM i.”

2. Likewise, update your DNS entries so that the new IP address is associated with the appropriate host name. Check whether your server is configured to search the Domain Name Server (DNS) before the host table. If it is, you must also make sure that the fully qualified host name of your Sametime Community Server is listed first in the DNS. To check the configured search order, see “Updating the Domain Name Server for IBM i.”

3. Stop and restart the Sametime Community Server for the changes to take effect.

Changing the host name of an IBM i Sametime Community Server

The command CHGLSTDOM simplifies the process for changing the host name setting of an IBM i Sametime Community Server.

About this task

The procedure described in this section can also be used to correct problems with the configuration of your Sametime server. For example, if your TCP/IP host table did not correctly list the fully qualified host name first at the time that you setup your Sametime Community Server, many elements of your server configuration may be incorrect. You can correct this problem by following this procedure to change the host name of your Sametime Community Server.

To change the host name, follow these steps:

Procedure

1. Update your host table so that the new host name is associated with the appropriate IP address. Make sure that the fully qualified host name is listed
first among the entries for your Sametime server, before any short names. For more information, see "Updating the host table on IBM i."

2. Likewise, update your DNS entries so that the new host name is associated with the appropriate IP address. Check whether your server is configured to search the Domain Name Server (DNS) before the host table. If it is, you must also make sure that the fully qualified host name of your Sametime Community Server is listed first in the DNS. To check the configured search order, see "Updating the Domain Name Server for IBM i."

3. End the IBM i Sametime Community Server.

4. Update the host name for the Domino server using the CHGDOMSVR command. For detailed information on changing the configuration of a Domino server, refer to "Updating the configuration of existing IBM i Domino servers."

5. On any IBM i command line, type the following and press F4:
   
   CHGLSTDOM

6. On the Change Sametime on Domino display, specify the following and then press Enter:
   - The name of the IBM i Sametime Community Server where you want to make this change (for example, stdom1).
   - The new fully qualified host name for the IBM i Sametime Community Server (for example, stdom1.acme.com).
     - Updates the Ports - Notes Network Ports - Net Address field in the Server document.
     - Adds the host name to the Internet Protocols - HTTP - Host name field in the Server document.
     - Updates Sametime files that reference the host name.

   **Note:** If your server is enabled for both IPv4 and IPv6 addressing, you must manually update the sametime.ini file so that "VPS HOST=" is set to an explicit IP address, rather than the host name, after running the CHGLSTDOM command. See Configuring the Community Services for IPv6 for detailed instructions.

7. Start the IBM i Sametime Community Server.

8. Open the Domino directory (names.nsf) on your IBM i Sametime Community Server and edit the Server document. Look at the Internet Protocols - HTTP tab in the Server document and locate the Basics - Host name(s) field.

9. The Basics - Host name(s) field may contain more than one name. If any of the names are incorrect or not needed, delete them. Make sure that the correct fully qualified host name is listed first in the field.

   **Note:** If your server is configured for both IPv4 and IPv6 addressing, there are additional considerations when updating the Host name field. See Configuring Lotus Domino for IPv6 on IBM i for detailed instructions.

10. Save and close the Server document.

11. If you are using HTTP Tunneling with multiple IP addresses, then additional configuration updates are required. See "Updating the host names when using HTTP Tunneling with multiple IP addresses" later in this section.

12. Stop and restart the IBM i Sametime Community Server for the changes to take effect.
What to do next

Updating the IBM i host names when using HTTP Tunneling with multiple IP addresses

If you are using HTTP Tunneling with multiple IP addresses, then you must update your configuration manually after using the CHGLSTDOM command to change the IBM i server host name. If you are not using HTTP Tunneling with multiple IP addresses then this step is not applicable.

The CHGLSTDOM command placed the new host name in the tunneling host name fields, but did not preserve the required prefixes, such as community-, meeting- and broadcast-, in the Sametime configuration. Use the Sametime Administration tool to update the host names in the following fields in the "Connectivity" section:

- Community Services Network settings -> Address for client connections-Host name should have prefix of community-
- Community Services Network settings -> Address for HTTP tunneled client connections-Host name should have prefix of community-

Monitoring the Sametime Community Server

The IBM Sametime monitoring charts allow you to monitor Sametime Community server statistics by providing up-to-the-second information about Community Services, web statistics, and free disk space on the server.

About this task

All monitoring charts are available from the Monitoring menu in the Sametime Administration Tool. The charts that are available from the Miscellaneous link in the Monitoring menu are part of the Domino web Administration Tool. These charts provide information on web statistics, server memory, and disk space. To view the status of the Sametime Community services since the last server restart, click the Overview link in the Sametime Administration Tool. Also note that the time of day that is listed in the monitoring charts is calculated according to the browser's time zone, not the server's time zone.

Procedure

1. Enter the URL for the Sametime Community server:
   http://host_name/servlet/auth/admin

   Where host_name is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime Community server you want to administer.

2. Enter the administrator name and password specified during the Sametime Community server installation.
3. Select Monitoring.

   Note: To view the status of the Sametime services since the last server restart, click Overview.

4. Select the appropriate chart for monitoring.

Monitoring general Sametime Community Server status

General Server Status monitoring chart allows you to see the status of the IBM Sametime Community Server at a glance.
**Total Community Logins**

The Total Community Logins chart displays current information about:

- **Total Community Logins** - The total number of logins to Community Services on the Sametime Community Server that you are monitoring. The Total Community Logins chart includes multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user.

- **Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, the Total Unique Logins chart records only one login for that user. A user logged in from multiple clients is considered a single unique login. Use this chart to determine the current number of Community Services users.

- **Total 2-way Chats** - The total number of 2-person chats taking place on the Sametime Community Server. This chart only includes chats that were started from the Sametime Community Server you are monitoring. For example, if you are monitoring server A and a user who has specified server A as her home server starts a chat with another user, that chat will be counted in the Total 2-way Chats chart. You will not see chats that were started by users who have specified a server other than server A as their home server.

- **Total n-way Chats** - The total number of multi-person chats taking place on the Sametime Community Server. This chart only includes chats that were started from the Sametime Community Server you are monitoring. For example, if you are monitoring server A and a user who has specified server A as her home server starts a chat with two other users, that chat will be counted in the Total n-way Chats chart. You will not see chats that were started by users who have specified a server other than server A as their home server.

- **Total Number of Active Places** - The Total Number of Active Places chart lists the combined number of n-way Chats and active meetings. Both n-way Chats and online meetings are counted as Active Places; 2-way Chats are not counted in this chart.

**Monitoring Sametime Community Services logins**

A user can be logged in to the IBM Sametime Community Services from more than one client.

To access the Logins chart, open the Sametime Administration Tool and select Monitoring > Logins. The Logins chart displays:

- **Community Server Total Logins** - The total number of logins to Community Services, including multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user. Internal components of the Community Services also log in to the Community Services. These are intra-server connections between Community Services components that occur as part of the normal operations of the Community Services. These logins are also counted in the total logins chart.

- **Community Server Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, this chart records only one login for that user. A user logged in from multiple clients is considered a single “unique” login. Use this chart to determine the current number of Community Services users.
The Logins chart updates at the time interval specified in the Polling Interval (seconds). Enter a new interval to change the rate at which the chart updates. To update the chart immediately, click Refresh.

**Monitoring miscellaneous Domino web Administration statistics**

The Miscellaneous charts are part of the IBM Lotus Domino Web Administration pages. The IBM Sametime Community Server uses features in the Lotus Domino server and its associated web administration pages.

You can monitor various statistics and events from the Lotus Domino Web Administration pages, including:

- Memory
- Statistics
- Disk Space

To access the Domino Web Administration pages, choose Monitoring > Miscellaneous in the Sametime Administration Tool, and then click the link that appears at the bottom: You can view the Lotus Domino web Administration pages in a new browser window.

**Monitoring the Domino log**

To access the Domino log, choose Logging - Domino Log in the Sametime Administration Tool, and then click the link that appears on the right. The Domino log launches in a new browser window.

The Domino log is only available from the Sametime Administration Tool. If you record Sametime log information in a text file, the text file does not include information about the Domino log.

A administrator can view additional information about the Sametime server in the Domino log database (log.nsf). The Domino log database records server activity information related to the Domino server and Domino databases, including databases used by the Sametime server (such as the Sametime Meeting Center). During setup, the Domino log database is automatically created and the server is assigned Manager access in the database’s Access Control List (ACL). The default access for all other users is Reader.

The Domino log database records information about all server activities, such as database size and usage, server events, calls made to and from the server, and billing for server services. Check the Domino log to monitor:

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

**Content of the Domino log**

The administrator cannot use the Sametime log settings or the Sametime Administration Tool options to determine what appears in the Domino log. The Domino log records information about the activities of the Domino server on which Sametime is installed. Generally, the default settings should provide an adequate record of server activity. However, you can record additional information
in this log file by altering settings in the notes.ini file. Recording this additional information might be necessary to troubleshoot a specific system problem.

For more information, see the Maintenance section of the Domino R5 Administration documentation.

**Views in the Domino log**

The Domino log includes many views that do not apply to Sametime. Use the table below to determine which views are relevant for Sametime.

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database-Sizes</td>
<td>Lists the size of the database, the percentage of the database’s disk space in use, and the weekly usage for all databases on the server. Use this view to check unused views, database size, and unused space in a database. <strong>Note:</strong> The stconf.nsf database grows in size depending on the number of meetings that have been created. You can archive this database frequently to prevent it from growing too large.</td>
</tr>
<tr>
<td>Database-Usage</td>
<td>Lists the date and time the database was accessed, the type of access, and the name of the user accessing the database for all databases on the server. Use this view to check unused views and unused space in a database.</td>
</tr>
<tr>
<td>Mail Routing Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Miscellaneous Events</td>
<td>Shows Sametime events and error messages not contained in other views. Messages are sorted in order of occurrence. Use this view to check for Sametime error messages, server crashes, and corrupted databases.</td>
</tr>
<tr>
<td>NNTP Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Object Store Usage</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Passthru Connections</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By Date</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By User</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Replication Events</td>
<td>Not used by the Sametime server.</td>
</tr>
</tbody>
</table>
Sample Billing Shows the same information provided in the Usage views, but the information is not categorized. The information in this view can be easily exported to a spreadsheet.

Use this view for billing purposes, such as Meeting Center usage, network usage, and database usage.

Usage-By Date Shows Sametime user transactions sorted by date. Transactions are operations such as starting meetings, attending meetings, opening documents, and updating documents. Each record lists the date and time of the transaction, the user name, the minutes of usage, the number of read operations, the number of write operations, the size of the database, and the total number of transactions.

Use this view to check database use on a specific date and users’ transactions with the server.

Usage-By User Shows Sametime user transactions by user name. Transactions are operations such as starting meetings, attending meetings, opening documents, and updating a document. Each record lists the user name, the date and time of the transaction, the minutes of usage, the number of read operations, the number of write operations, the size of the database, and the total number of transactions.

Use this view to check a particular user’s transactions on a database.

General log settings
The General log settings allow you to specify the format for the Sametime log and to control the information that the log records.

The four types of General log settings are: (Note that meeting server events do not apply to Sametime Limited Use.)

- **Database or text file settings** - Allow you to specify the format for the log and to automatically remove information from the log.

- **Sametime statistics settings** - Allow you to control whether to log statistics related to chats, meetings, and users.

- **Server community events to log settings** - Allow you to control which Community Services events are recorded in the Sametime log.

- **Meeting server events to log settings** - Allow you to control which Meeting Services events are recorded in the Sametime log.

Log output location:
To access the "Database or text file" settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

The "database or text file" settings allow you to specify the format for the log and to automatically remove old information from the log.

**Enable logging to a Domino database (STLog.nsf)**

Select this setting to record Sametime Meeting Services and Community Services data in the Sametime log database (stlog.nsf). During setup of the Sametime server, the Sametime Log database is automatically created, and the administrator specified during setup is assigned Manager access in the database Access Control List (ACL). The server is also assigned Manager access to the database so that it can write information to the log. The default access for all other users is Reader.

When this option is selected, a Sametime administrator can view all of the information in the Sametime log by opening the Sametime Administration Tool and selecting Logging. The links available from the Logging menu display different views of the Sametime log database.

When this option is selected, you can use the "Remove history after (days)" setting to prevent the Sametime log from growing too large.

If the "Enable logging to a Domino database" option is not selected, Sametime activity is not recorded in the Sametime database, and the links beneath the logging option in the Sametime Administration Tool do not appear.

If you select this option, you cannot select the "Enable logging to a text file" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

**Remove history after (days)**

Select this setting to automatically remove old information from the Sametime log database (stlog.nsf). In the field provided, specify the age (in days) of information that is automatically removed from the database. The default setting is 60 days.

This setting only applies to the Sametime log database; it does not remove Sametime log information stored in text files. You must manually delete old text files.

After selecting this option, click Update and restart the server for the setting to take effect.

**Logger output location**

Select this setting to record Sametime log information in a text file. When this option is selected, a new Sametime log text file is created every day. By default, the name of each text file contains the date on which the file was created (for example, log_23_Mar_2009.txt). After you select this option, specify a path and file name for the log file in the "Path to log text file" field; for example, in Microsoft Windows: d:\notesdata\chatlogs\txtfiles\log.txt
To view the file, open it in your preferred text editor. You cannot view the text file log from the Sametime Administration Tool.

If you log Sametime activity to a text file:
- Sametime activity is not recorded in the Sametime log database, and the links beneath the logging option in the Sametime Administration Tool do not appear. You cannot access the Domino log when you log to a text file.
- You must manually delete the text files from the server hard drive periodically to conserve hard disk space.

If you select this option, you cannot simultaneously select the “Enable logging to a Domino database” option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

**Sametime Community Server log size and content settings**

To access the log settings, choose Logging - Settings in the Sametime Administration Tool.

The IBM Sametime Community Server uses these log settings:
- General settings - Allow you to specify the format and content of the Sametime Community Server log.
- Capacity Warnings - Allow you to set server usage parameters. When these parameters are exceeded, warning messages are written to the Sametime log. These messages help you monitor server usage and determine the cause of slow server performance.

**Sametime Community Server events log settings:**

To access the IBM Sametime Community Server events log settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

The Community Server events log settings allow you to control which Community Services events are recorded in the Sametime Community Server log. After selecting any of these options, click Update for the settings to take effect.

**Note:** The settings take effect within a reasonable time period. The longest time period you will wait for these settings to take effect is the time interval specified for the “How often to poll for new servers added to the Sametime community” setting in the Configuration - Community Services settings of the Sametime Administration Tool. The default time interval for that setting is 60 minutes.

**Successful logins**

Select this setting to record information about successful Community Services logins and logouts in the Community Logins/Logouts section of the Sametime log. This option is selected by default.

**Failed logins**

Select this setting to record information about failed logins to Community Services in the Place Login Failures, Meeting Login Failures, and Community Logins/Logouts sections of the Sametime log.
Community server events and activities

Select this setting to record information about Community Services events in the Community Events section of the Sametime log. For example, you can view the name and status of each service.

Administering a Sametime Proxy Server

This section describes how to manage a IBM Sametime Proxy Server.

Updating Sametime Proxy Server connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Proxy Server.

Before you begin

If you are configuring the Sametime Proxy Server to use SSL (Secure Socket Layer), make sure the server’s certificate has been added to the Sametime System Console’s trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Proxy Server. These settings are only used by the Sametime System Console to connect to the Sametime Proxy Server.

Follow these steps to update connection setting information.

Procedure

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Proxy Server.
3. In the Sametime Proxy Servers list, click the Edit next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator’s User name and Password for connecting to the Sametime Proxy Server.
5. By default, the Sametime Proxy Server trusts other Sametime components. If you want to change this, then select Do not auto-accept SSL certificate.
6. Click Save.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.
**Related tasks:**

“Adding a Sametime server SSL certificate to the Sametime System Console” on page 308

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

---

**Administering a Sametime Media Manager**

The audio/video services are enabled by default following an IBM Sametime Media Manager installation. You can enable and disable the audio/video services from the Sametime System Console. This section describes how to manage the Sametime Media Manager.

**About this task**

The Sametime Media Manager manages Sametime meeting rooms by maintaining a dialog with each participant, and ensuring that all media flows between those participants. The Sametime Media Manager supports interactive IP audio and video capabilities and enables clients with the appropriate hardware (sound card, microphone, speakers, and camera) to transmit and receive real-time audio and video in a Sametime meeting room.

**Updating Sametime Media Manager connection properties on the console**

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Media Manager.

**Before you begin**

If you are configuring the Sametime Media Manager to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

**About this task**

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Media Manager. These settings are only used by the Sametime System Console to connect to the Sametime Media Manager.

Follow these steps to update connection setting information.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the Sametime Media Managers list, click the **Edit** next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's **User name** and **Password** for connecting to the Sametime Media Manager.
5. By default, the Sametime Media Manager trusts other Sametime components. If you want to change this setting, then select **Do not auto-accept SSL certificate**.
6. Click Save.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

Related tasks:
“Adding a Sametime server SSL certificate to the Sametime System Console” on page 308
If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

Managing UDP ports for voice chat and video calls
Change the default UDP ports for computer-to-computer voice chats and video calls in an IBM Sametime deployment.

Before you begin
When the NAT traversal feature is enabled, the Connect client no longer uses the traditional ports (20830+2); instead it uses random ports for ICE negotiation. You should still leave the original ports open so they can be used by older clients that are not supported by the NAT traversal feature.

About this task
IBM Sametime comes with voice chat. With voice chat, users can place and receive audio calls using their computer’s and their chat partners’ computer audio capabilities. Once a user has a computer-to-computer voice chat started, the user can convert it to a video call so that the user can both see and hear call participants.

Voice chat works with user datagram protocol (UDP) packets which flow through UDP ports on the firewall of every client machine to allow users to speak to other users orally over the computer. The client machines use a single port (UDP port 20830 is the default) for all audio chats, so this port must be opened for both incoming and outgoing UDP traffic.

Video calls also work with user datagram protocol (UDP) packets which flow through UDP ports on the firewall of every client machine to allow users to see video of users with whom they are chatting over the computer. The client machines use a single port (UDP port 20832 is the default) for all video calls, so this port must be opened for both incoming and outgoing UDP traffic.

Note: The client might require ports for the audio and video channels to send RTP and RTCP packets over UDP.

Follow these steps to change the UDP ports:

Procedure
1. Log in to the Integrated Solutions Console as the IBM WebSphere administrator.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
4. Click the Configuration tab.
5. The Sametime Media Manager listens for inbound audio streams from clients on a range of 100 UDP port numbers. Under Participants, enter the starting number of this range of ports in the **Starting UDP port for audio calls** field.

6. The Sametime Media Manager listens for inbound video streams from clients on a range of 100 UDP port numbers. Under Participants, enter the starting number of this range of ports in the **Starting UDP port for video calls** field.

7. Click **OK**.

8. Restart the Sametime Media Manager.

### Managing multiple audio and video streams

The IBM Sametime Media Manager manages multiple audio and video streams in a meeting.

#### About this task

The Sametime Media Manager scans the meeting participants and locates the person currently speaking (transmitting audio packets). The Sametime Media Manager performs switching operations as different people speak during a meeting. When a meeting participant speaks, the Sametime Media Manager locks onto that client's audio stream and distributes that stream to all other clients in the meeting. When a participant stops speaking, the Sametime Media Manager waits for a brief period of time, and then begins scanning for the other active audio clients.

The video follows the audio. When the Sametime Media Manager switches to a new audio source (speaking person), the Sametime Media Manager through its connections to the clients, ensures that the icon indicating the current speaker is properly updated for all clients. After this update, the Sametime Media Manager sets the video source to the person currently speaking. It is important to ensure that the video does not switch too quickly. Rapid video switching reduces usability. You can control the time interval that must pass before the video switches to the new speaking person.

**Note:** If the current speaker does not have video capabilities or has the video window paused, the Sametime Media Manager sends the next loudest speaker's video as the active speaker to all participants.

By default, the Sametime Media Manager can lock onto and broadcast a maximum of five audio streams at the same time. In a meeting, if five people speak at the same time, it is possible for all meeting participants to simultaneously hear five people speaking. The Sametime Media Manager designates the audio stream that has been transmitting the longest (generally, the person who started speaking first) as the primary audio stream. The source of the primary audio stream is also the source of the video stream. Audio and video services provided by the Sametime Media Manager have been tested and optimized for sessions with 20 participants. The actual number of participants will vary based on network and environmental conditions. The higher the number of switched audio streams, then the more bandwidth that is required.

In meetings, especially in large meetings, IBM recommends that participants, who are not talking, mute their speakers to reduce noise.

#### Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
4. Click the Configuration tab.
5. Under Presence, type a number between 2 and 16 in the Number of switched audio streams field to change the number of simultaneous audio streams.

   **Note:** The more switched audio streams, the more people are heard simultaneously in a meeting. Meetings could become quite noisy, so use caution when you increase this number.
6. Under Set the time in milliseconds before switching to the next active speaker, select a number in Video switching wait time to control the time interval that must pass before the video switches to the new speaking person.
7. Click OK.
8. Restart the Sametime Media Manager.

### Changing the SIP transport protocol in the Sametime Media Manager

You can change the transport protocol that IBM Media Manager uses for the SIP Proxy and Registrar.

**About this task**

SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for media services, and provide Sametime Media features to users. SIP also provides a registration function that allows users to send their current locations for use by proxy servers.

The transport protocol determines the network transport mechanism to use for sending SIP messages. The SIP proxy application examines all requests sent by the Sametime Media Manager to determine whether a given request is sent by an appropriate proxy application. All requests are routed according to the transport protocol defined here.

In a multiple machine deployment where Sametime Media Manager components are installed on different machines, you must update the SIP transport protocol on all components: Conference Manger, Packet Switcher, and SIP Proxy and Registrar. Moreover, if you change the SIP transport protocol from TLS to TCP, then the port changes are automatically reflected in the stavconfig.xml file on the Conference Manager. You must manually change the ports in the stavconfig.xml files of the Packet Switcher component.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
4. Click the Configuration tab.
5. Under Server Integration, select a Transport protocol of TLS or TCP. UDP is not supported.
6. Set how frequently in seconds you want SIP to check if a client is still connected. Enter a number between 30 and 300 in the Session expiration field.

7. Click OK.

8. Update SIP Registrar security role settings by following these steps.
   a. Log in to the SIP Proxy and Registrar.
   b. Click Applications > Enterprise Applications.
   c. Click IBM SIP Registrar setting.
   d. Under Detail Properties, click Security role to user/group mapping.
   e. Change security role settings from All Authenticated in Application’s Realm to Everyone if the protocol is updated to TCP. Do this by selecting the check box for the AllAuthenticatedUsers role, then select Map Special Subjects and select Everyone. Leave All Authenticated in Application’s Realm if the protocol is selected as TLS.

9. Restart the Sametime Media Manager.

What to do next

If you have deployed the Conference Manager, Packet Switcher, and SIP Proxy and Registrar on separate application servers, and you have changed the SIP transport protocol from TLS to TCP, the Conference Manager stavconfig.xml file automatically reflects this change. You must edit the stavconfig.xml files on the Packet Switcher to reflect this update by changing the secure ports to nonsecure ports. Follow the steps in “Configuring ports for Transport Layer encryption on an upgraded Sametime Media Manager” on page 297.

Managing media encryption and codecs

You can manage the type of media encryption and codecs used in meetings on the IBM Sametime Media Manager.

About this task

A codec compresses streaming data, such as audio or video, on the transmitting side and decompresses it for playback on the receiving side. Codecs reduce the amount of bandwidth required to send streaming data. Generally, higher compression conserves more bandwidth. Higher compression also results in poorer audio or video quality and requires more resources to compress and decompress the data streams.

You can change the type audio and video codecs.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
4. Click the Configuration tab.
5. Follow the procedure appropriate for your deployment:
   • Single box deployment with all components on one machine: Under Audio Video Media, keep the default encryption option as Disable or click Enable. Calls made between the Sametime Connect client and any other endpoint supporting SRTP including another Sametime Connect client or a partner
conference bridge are encrypted. Audio/video conferences with three or more participants using the Media Manager Packet Switcher or the Sametime Unified Telephony Media Server are not encrypted.

• **Non-clustered distributed and clustered deployments:**
  a. Under Audio Video Media change the encryption option to **Enable** or **Disable**. This action only automatically updates the stavconfig.xml file of the Conference Manager component.
  b. A manual update is required on Packet Switcher deployments. Update the stavconfig.xml encryption field values to **NoEncryption** if you have selected **Disable**, or to **SRTP** if **Enable** is selected, into the Deployment Manager server's scope stavconfig.xml files, and run Full-resynchronize on nodes, then restart the Packet Switcher servers.

  **Note:**

  **NoEncryption** and **SRTP** are the only string literals to update stavconfig.xml with.

The Sametime Community server default refresh interval is one hour. The Sametime Connect client gets the updated server policy attribute after one hour.

6. Prioritize the audio codecs by using the **Up** and **Down** buttons to move the audio codecs in the list.
   Sametime Media Manager supports the following audio codecs:
   - **ISAC** - Internet Speech Audio Codec (ISAC) is a wideband and adaptive bit rate codec. The bit rate ranges from 10 to 32 kbps (Kilobit per second) depending on the available network bandwidth. This is the default codec.
   - **iLBC** - Internet Low Bit-rate Codec (iLBC) is a narrowband low bit rate speech codec. It requires 15.2 kpbs bandwidth.
   - **G.722.1** - Popular wideband audio codec that operates at one of three selectable bit rates: 32000, 24000, 16000. G7221 is a licensed royalty-free standard audio codec providing high quality, moderate bit rate audio coding.
   - **G.711** - Old and widely supported narrowband codec. It requires 64 kbps bandwidth but consumes less CPU to process.

7. Prioritize the video codecs by using the **Up** and **Down** buttons to move the video codecs in the list.
   Sametime Media Manager supports two video codecs:
   - **H264** - Also known as AVC and MPEG-4 part 10. It provides high quality, block-oriented, motion-compensation-based video codec for video conferencing. It supports the Baseline Profile without Flexible Macroblock Ordering (FMO).
   - **H263** - A legacy codec and lower quality than H264.

8. Click **OK**.
9. Restart the Sametime Media Manager.

**Changing the default number of maximum users**

As demands on video conferencing change, you can update the maximum number of participants to ensure that your network can support this feature.
About this task

The default maximum number of participants in a single audio-only or video conferences is set to 20. You can adjust this number up or down to accommodate specific network consumption requirements.

Note: The maximum number of users can set independently internally (on the Sametime Packet Switcher) and externally (on the MCU that bridges video-conferencing connections).

Procedure

1. On the server hosting IBM Sametime Media Manager, open the ConferenceManager.properties file. In a multiple-machine deployment where Sametime Media Manager components are installed on different machines, go to the server hosting the Conference Manager.
   
   You can adjust the maximum participants setting for each Service Provider Implementation (each adapter); each adapter has its own ConferenceManager.properties file.
   
   websphere_install_path/AppServer/profiles/profile_name/installedApps/cell_name
   /ConferenceFocus.ear/ConferenceFocus.war/ConferenceManager.properties

2. Edit the values in the following settings:
   
   MaximumAudioConferenceUsers=20
   
   MaximumVideoConferenceUsers=20

   For example, the Radvision TCSPI Adapter ConferenceManager.properties file contains this setting by default:
   
   #
   # PerConferenceMaximum is the maximum number of users the service provider supports for each conference call.
   #
   MaximumConferenceUsers=200

   so you will probably want to lower that value to provide better performance within your network.

3. Restart the Sametime Media Manager.

Administering a SIP Proxy and Registrar

This section describes how to manage the properties of a SIP proxy and registrar.

About this task

Session Initiation Protocol (SIP) is a protocol that manages communication in IBM Sametime meeting rooms by maintaining a dialog with each participant, and ensuring that all media flows between meeting participants. SIP makes use of elements called proxy servers to help route information to the user's current location, authenticate and authorize users for meetings, and provide features to users. SIP also provides a registration function that allows users to send their current locations for use by proxy servers.

Adding a Sametime Media Manager's SSL certificate to the Sametime System Console

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.
About this task

To enable SSL, you must extract the certificate from the Sametime product server and add it to the trust store of the Sametime System Console. The Sametime product servers include:

- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Gateway Server
- SIP Proxy and Registrar

Follow these instructions. See the WebSphere Application Server information center for more information on extracting and adding certificates.

Procedure

1. Log in to the Integrated Solutions Console for the Sametime product server.
2. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
3. Select the alias named root, and click Extract.
4. Enter the name of the .cer file, and select Base64 as the type for storing the process server signer certificate.
5. Log in to the Integrated Solutions Console for the Sametime System Console.
6. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
7. Click Add.
8. Enter an alias.
9. Enter the file name where you stored the extracted process server signer certificate from the product server.
10. Click Apply.
11. Restart the Sametime System Console deployment manager.

Updating SIP Proxy and Registrar connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the SIP Proxy and Registrar.

Before you begin

If you are configuring the SIP Proxy and Registrar to use SSL (Secure Socket Layer), make sure the server’s certificate has been added to the Sametime System Console’s trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the SIP Proxy and Registrar. These settings are only used by the Sametime System Console to connect to the SIP Proxy and Registrar.
If you are configuring the SIP Proxy and Registrar to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store using the Integrated Solutions Console (Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates). See the WebSphere Application Server information center for more information on adding certificates.

Follow these steps to update connection setting information.

**Procedure**
1. Log in the Integrated Solutions Console.
2. Click **Sametime System Console** > **Sametime Servers** > **SIP Proxies and Registrars**.
3. In the SIP Proxy and Registrar list, click the Edit next to the deployment name of the SIP Proxy and Registrar with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's **User name** and **Password** for connecting to the SIP Proxy and Registrar.
5. By default, the SIP Proxy and Registrar trusts other Lotus Sametime components. If you want to change this, then select **Do not auto-accept SSL certificate**.
6. Click **Save**.
7. Click **Done** to return the SIP Proxy and Registrar list.
8. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

**Managing SIP proxy properties**

You can set properties for the SIP proxy server.

**About this task**

SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users to access media services, and provide Sametime media features to users.

**Procedure**
1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console** > **Sametime Servers** > **SIP Proxies and Registrars**.
3. Click the Deployment Name of the SIP Proxy server.
4. In **SIP Proxy and Registrar**, click **Proxy Administration**.
5. Use the following table to set basic SIP proxy properties:
Option | Description
---|---
Record route mode | When record route mode is enabled, the optional Record-Route header is inserted by the SIP proxy server that wants to remain in the signalling path for the duration of the session. The Record-Route header is used to establish a route for transactions belonging to a session. When record route mode is disabled, SIP messages flow directly through the SIP gateways once a call has been established.

Parallel search mode | When parallel search mode is enabled, a SIP proxy server sends many requests to possible user locations when it receives an incoming request. Instead of sending one request and then waiting for the final response before sending another request, a parallel search sends requests without waiting for the result of previous requests.

Add public IP to outgoing request | When this option is enabled, the SIP proxy server adds an IBM-Destination-Public-IP header field to outgoing initial requests. This header contains the public IP of the endpoint.

6. Specify Handled Domains. These are domains that are managed by the SIP Proxy and Registrar
7. Routing rules define how SIP messages are routed through the Sametime SIP proxy server. The table shows any existing rules, with the highest priority granted to the first rule in the table.
   Click a rule to open it for editing or click New to create a new routing rule.
8. Click OK.
9. Restart the SIP Proxy and Registrar.

Creating and editing routing rules for SIP-based messaging
Add or edit routing rules that define how the SIP Proxy server routes SIP-based messages.

About this task
Routing rules tell Sametime where to direct SIP-based messages under certain conditions. The rule consists of one or more conditions, and a destination (SIP endpoint) where call requests that meet the conditions will be routed.

A routing rule uses the same transport protocol as the Sametime Media Manager components. For example, if the Media Manager is configured to use TLS for the SIP signalling, you must use TLS for all routing rules. The supported transport protocols are TCP and TLS over TCP. UDP is not supported.

Procedure
Use the routing rules table in the Proxy Administration page to view, create, or edit rules.
1. On the Sametime System Console, log in to the Integrated Solutions Console as the IBM WebSphere administrator.
2. In the navigation tree, click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.

3. On the SIP page, look in the proxies table and click the Deployment Identifier of the SIP Proxy and Registrar.

4. On the SIP Proxy and Registrar page, click Proxy Administration.

5. In the routing rules table, do one of the following:
   - Click the name of a rule to edit it.
   - Click New to create a new rule.

6. Add or modify settings for the routing rule as follows:
   a. Type a name and description of the route in the Name and Description fields.
      It is helpful to indicate the route’s direction and endpoint in the name so you can easily distinguish among routes in the routing rules table later.
   b. Use the “Conditions” section to configure the routing rule by defining at least one condition:

   Table 35. Conditions fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>A predefined value indicating the type of request: INVITE, INFO, MESSAGE, or ANY. Select the appropriate value from the field’s list; if you do not select a method, then all methods are accepted by this condition.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The originating caller’s IP address, which must match the pattern specified in the regular expression that you provide. You could specify a single IP address: 9\1.3.186.215 or use an expression to specify a range of IP addresses: 9\1.3.186.215</td>
</tr>
<tr>
<td>Request URI</td>
<td>The resource, usually the origin server, on which to apply the request. The URI must match the pattern specified in the regular expression that you provide. For example: .<em>example\1.com.</em> matches both of these incoming initial requests: sip:example.com:5060;transport=tcp SIP/2.0 and sips:subdomain.example.com:5061 SIP/2.0</td>
</tr>
<tr>
<td>Contact Header</td>
<td>The SIP URI of the originating caller. The URI must match the pattern specified in the regular expression that you provide. For example, .<em>201000192\1.192\1.0\2\12:506&lt;01&gt;</em> matches incoming initial requests with either of these contact header values: <a href="">sip:201000192\1.192\1.0\2\12:5060;transport=tcp</a> or <a href="">sips:user99201000192\1.0\2.12:5061;transport=tcp</a></td>
</tr>
</tbody>
</table>
c. In the "Destination" section, select the method to use for storing the address of the destination SIP endpoint:

Table 36. Destination addressing methods and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push a Route header field</td>
<td>Insert the destination address into a Route header field of the outgoing SIP request.</td>
</tr>
<tr>
<td>Replace a Request-URI</td>
<td>Replace the original Request-URI with the destination address when creating the outgoing request.</td>
</tr>
</tbody>
</table>

d. Construct the destination address using the method you selected in substep c.

**Push a Route header field**
Supply a value in one or more of the fields described in the table.

Table 37. SIP URI addressing fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>The scheme can be either SIP or SIPS (the secure version of SIP); the default is SIP. This field is required.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or fully qualified host name of the destination server (the SIP endpoint). For incoming calls, use the fully qualified domain name of the Sametime Media Manager’s Conference Manager component. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the destination server (the SIP endpoint) is listening on for SIP-based communications. This field is optional; if you do not provide a value, the server uses the correct port. <strong>Note:</strong> Make sure you specify the correct port for the transport protocol. For unsecured TCP communications, the Conference Manager typically uses port 5063; for encrypted TLS communications, the Conference Manager typically uses port 5062.</td>
</tr>
<tr>
<td>Transport</td>
<td>The network transport protocol to use for sending SIP messages: TCP or TLS over TCP (UDP is not supported). Use the same transport protocol throughout the entire route (from the Sametime client to the SIP Proxy/Registrar to the third-party SIP endpoint). For example, if the Media Manager is configured to use TLS for SIP communications, you must use TLS for all routes. This field is optional; if you do not provide a value, the server supplies a transport protocol.</td>
</tr>
</tbody>
</table>

**Replace a Request-URI**
Construct regular expressions to define the original **Request-URI pattern** and its replacement **Output pattern**, which are explained in the table.
Table 38. URI pattern fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request-URI pattern</td>
<td>A regular expression defining the pattern of the original Request URI. Use this field to extract fields or parameters from a Request-URI of a SIP request. A variable stores the part of the Request-URI matched by the part of the regular expression inside the parentheses, indicated by a number. The variables are recalled with the dollar-sign, for example, $1, $2, and so on. These fields or parameters can be used to build the Output pattern. This field is optional.</td>
</tr>
<tr>
<td>Output pattern</td>
<td>A regular expression defining the pattern of the destination’s URI (address). This field can contain either a SIP URI or a replacement expression with variables for example, $1, $2, and so on. Variables store the portion of a parenthesized pattern captured from the Request-URI pattern field. After processing any captured variables, the resulting field value must be a valid SIP or SIPS URI. Note: If you do not provide a value in the Request-URI pattern field, this field must contain a valid SIP or SIPS URI.</td>
</tr>
</tbody>
</table>

**Remember:** Regular expressions must follow a strict notation, different from other notation forms you may use. For example, the operating system shell notation for a wildcard (series of 0 or more characters) is the asterisk character: *, The regular expression equivalent for a wildcard is different: it is a combination of a dot followed by an asterisk, as follows: .*

Before adding the regular expression to the routing rule, you should test the expressions using any of the testing engines available online. To learn more about creating regular expressions, see the Java Regular Expressions class on the Oracle web site.

e. Click OK to save the rule.
f. Repeat from step 5 until all your routing rules have been defined.

You must create at least one inbound route and one outbound route between Sametime and each third-party SIP endpoint. You can create different versions of a route using different sets of conditions (all of a route’s conditions must be satisfied for that route to be selected), and you can prioritize routing rules as explained in the next step.

7. Prioritize the routing rules by arranging them in the sequence in which you want them processed:

   It is acceptable to have inbound routes mixed with outbound routes in the sequence because if a message does not satisfy all of the routing conditions, the route will be ignored.

   a. In the routing rules table, select a route and click the **Move Up** button or the **Move Down** button until the route is positioned in the correct sequence.

   b. Repeat as needed until the rules appear in priority sequence.

8. Save the set of routing rules and priorities by clicking **Save** link in the "Messages" box at the top of the page.
9. Restart the SIP Proxy and Registrar’s server or cluster:
   - For a stand-alone Media Manager or SIP Proxy and Registrar, restart it now as follows:
     a. In the server’s Integrated Solutions Console, click **Servers > Server Types**
        > **server_type**.
     b. In the list of servers, select your server and click the **Restart** button at the top of the table.
     c. Click the **Refresh** button and verify that all components are active.
   - For a cluster of SIP Proxy/Registrars, synchronize the nodes before restarting them:
     a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Nodes**.
     b. Select all nodes in the cluster, and then click the **Full Resynchronize** button at the top of the table.
     c. Back in the navigation tree, click **System Administration > Node agents**.
     d. Select all nodes in the cluster, and then click the **Restart** button at the top of the table.

**Example**

The following examples show different combinations of values for Request-URI pattern and Output pattern that produce specific destination addresses.

- Route all incoming SIP requests to this destination:
  sip:example.com;transport=tcp
  Request-URI pattern: **empty**
  Output pattern: sip:example.com;transport=tcp
  Because the Request-URI pattern field is empty, the destination is modified on all incoming requests.

- Route incoming SIP requests to a new host, keeping the original user name
  Request-URI pattern: sip:(.+@.*
  Output pattern: sip:$1@example.com
  The expression in parentheses for Request-URI pattern captures the user name in a variable and the output pattern refers to the variable as $1.
  For example, assume an incoming initial SIP request with a Request-URI of sip:12345@company.com. The Request-URI pattern runs, resulting in the variable $1=12345. The SIP URI for the destination address maintains the same user name, but adds a new host name: sip:12345@example.com.

- Route incoming SIP requests to "host," keeping the original user name if the user-name prefix in the Request-URI is "45"
  Request-URI pattern: sip:(45.+@.*
  Output pattern: sip:$1@host

- Route incoming SIP requests to "host," omitting the prefix if the user-name prefix in the Request-URI is "45"
  Request-URI pattern: sip:45(.+@.*
  Output pattern: sip:$1@host

**Managing SIP registrar properties**

You can set registration expiration properties for the SIP registrar.
About this task

SIP provides a registrar that allows users to send their current locations for use by proxy servers. The SIP registrar accepts user requests and places the information it receives from those requests into the registration table. Registration is how media services learn the current location of a Sametime user. Upon login, and at periodic intervals, the user sends registration messages to the SIP registrar application. These messages associate the user’s SIP URI with the machine into which he is currently logged in. The registrar records this association, also called registration instance or a binding, to the registration table, where it can be used by the SIP proxy.

Follow these steps to set expiration properties for the SIP registrar.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registrar Administration.
5. In the Default Registration Expiration field, type a value in seconds to use as the registration expiration when there is no such parameter set in the user request.
6. In the Minimum Registration Expiration field, type a value in seconds for the minimum expiration interval the SIP Registrar is willing to honor. A request with an expiration interval lower than the minimum expiration will be rejected.
7. In the Maximum contacts for user field, type a value for the maximum number of contacts a user can register, for the same address-of-record.
8. In the Maximum Anonymous users field, type a value for the maximum number of anonymous users that can be registered with the IBM Lotus SIP Registrar.
9. Click OK.
10. Restart the SIP Proxy and Registrar.

Managing SIP registered bindings

Use the SIP Proxy Registration page to monitor SIP registrations.

About this task

The registration of the user occurs during client login and is extended by the client automatically if the client remains logged in. The registration table is a location service used by a SIP to obtain information about a user’s possible location. The registration table specifies the SIP addresses associated with device addresses, as well as the expiration times for currently registered users.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registered Bindings. Use this page to find, view, or delete bindings.

5. Use the following table to view binding properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP URI</td>
<td>Identifies a user in IBM Sametime. A SIP URI contains the information to initiate and maintain a communication session with another user. It can have the following formats: sip:user_identifier@host or sips:user_identifier@host.</td>
</tr>
<tr>
<td>Device Address</td>
<td>The location of the machine into which the user is currently logged. The format is sip:host:port;transport=&lt;transport-type&gt;.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>The time when the registration expires, unless it is automatically extended by the Sametime client.</td>
</tr>
</tbody>
</table>

## Managing the SIP Proxy and Registrar domains

Use the Handled Domains page to set the domains for which the SIP Proxy and Registrar are responsible.

### About this task

If you do not add any domains to the Handled Domains page, then all domains will be managed by the SIP Proxy and Registrar.

### Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Handled Domains.
5. To add a domain which will be handled by the SIP Proxy and Registrar, enter a domain in the Domain field and click Add.
6. Click OK.

## Administering a Sametime Bandwidth Manager

IBM Sametime Bandwidth Manager provides a number of monitoring and management tools. Use these tools to ensure that the bandwidth management component is configured and tuned to best serve your organization’s day-to-day needs and support the organization’s network policies.

### Monitoring the status of bandwidth manager modules

Use the Status tab to monitor the status of the IBM Sametime Bandwidth Manager modules. You can start, stop, or restart server modules as needed.

### About this task

The bandwidth manager comprises three components, which can be started and stopped independently:
• **Bandwidth Pool Manager:** Manages bandwidth allocations.
• **Media Session Controller:** Implements the business logic of the bandwidth management component (such as user lookup and application of policies).
• **SIP Frontend:** Handles incoming SIP requests and acts as SIP proxy.

To monitor bandwidth manager modules:

**Procedure**

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime Servers > Bandwidth Manager**.
3. Click the **Status** tab.
4. Examine the values in the table. Each row represents a component currently deployed in the environment.
5. Note that the table displays most of the same information as in the Configuration tab, but it adds one more column, **State**. This column indicates the current status of the component instance. It could take four values: Idle, Active, Stopping, and Down. All components go to Idle state after installation or WebSphere Application Server startup. Then all components can be activated or deactivated with "Start" or "Stop" buttons.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component type</td>
<td>The type of the component instance: Bandwidth Pool Manager, Media Session Controller, or SIP Frontend.</td>
</tr>
<tr>
<td>Server name</td>
<td>The full IBM WebSphere Application Server name of the server where this component was installed, in the following format -- &quot;CELL/NODE/SERVER&quot; (for example, Websphere302Node01Cell\Websphere302Node01\server1).</td>
</tr>
<tr>
<td>HTTP URI</td>
<td>The HTTP URL of this particular instance of the component, in the following format <a href="http://HOSTNAME:HTTPPORT/APPLICATIONPATH/">http://HOSTNAME:HTTPPORT/APPLICATIONPATH/</a> where HOSTNAME is the hostname or IP address of the WebSphere Application Server server where the component is installed. HTTPPORT is the HTTP port configured for this server.</td>
</tr>
<tr>
<td>Cluster HTTP URI</td>
<td>The common HTTP URL for all instances of the given component type on the cluster (for a single server installation use the same value as for the &quot;HTTP URI&quot; field).</td>
</tr>
<tr>
<td>SIP URI</td>
<td>The SIP Address of the bandwidth management component of this particular instance of the &quot;SIP Frontend&quot; (leave it blank for other types). It should be defined in the following format sip:HOSTNAME:SIPPORT where HOSTNAME is hostname or IP address of the WebSphere Application Server where the component is installed. SIPPORT is SIP Port configured for this server.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster SIP URI</td>
<td>The common SIP address for all instances of “SIP Frontend” on the cluster (for single server installation use the same value as for “SIP URI”).</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the current instance. This is an integer value used only for “Bandwidth Pool Manager” components to determine which instance will be acting as primary and which will be running as secondary servers. The lower number means higher priority.</td>
</tr>
</tbody>
</table>

### Monitoring bandwidth usage for individual links

Use the Links table to monitor bandwidth usage for individual links in the network managed by IBM Sametime Bandwidth Manager.

#### About this task

The monitoring interface includes tabs for links, sites, link calls, and site calls. The **Links** tab provides the following information:

- What is the source site and destination site for each link?
- What city and region are associated with the link?
- How much bandwidth is currently utilized on a link?
- How much non-utilized bandwidth remains for the link?
- What is the percentage of available bandwidth is currently being utilized?
- How many calls are utilizing the bandwidth on that link?

From the link monitoring area, administrators can drill down and see which calls are utilizing the bandwidth on that link.

To monitor links, perform the following steps:

#### Procedure

1. On the server hosting the Bandwidth Manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime Servers > Bandwidth Manager**.
3. Click the **Monitoring** tab.
4. Click the **Links** tab to see a table of links configured for this network.
5. In the **Links** table, click a link name in the **Name** column to see the site configuration page for that link.
6. In the **Links** table, click a number in the **Calls** column to see what calls are currently utilizing bandwidth in the link displayed in that table row.

### Monitoring bandwidth usage for sites

Use the Sites table to monitor bandwidth usage for each site in the network managed by IBM Sametime Bandwidth Manager.

**About this task**

The monitoring interface includes tabs for links, sites, link calls, and site calls. At the top level, the table on the **Sites** tab provides the following information:

- How much bandwidth is currently utilized on a site?
- How much non-utilized bandwidth remains for the site?
- What is the percentage of available bandwidth is currently being utilized?
- How many calls are utilizing the bandwidth on that site?

From the site monitoring area, administrators can drill down and see which calls are utilizing the bandwidth in that site.

To monitor sites, perform the following steps:

**Procedure**

1. On the server hosting the Bandwidth Manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime Servers > Bandwidth Manager**.
3. Click the **Monitoring** tab.
4. Click the **Sites** tab to see a table of sites configured for this network.
5. In the **Sites** table, click a site name in the **Name** column to see the site configuration page for that site.
6. In the **Sites** table, click a number in the **Calls** column to see what calls are currently utilizing bandwidth in the site displayed in that table row.

### Monitoring calls for selected links

Use the Link Calls table to monitor details for calls on a selected link within the network managed by IBM Sametime Bandwidth Manager.

**About this task**

The monitoring interface includes tabs for links, sites, link calls, and site calls. The **Link Calls** tab shows calls that are currently in progress. By choosing a specific
link in the **Link Calls** dropdown list, the administrator can limit the calls shown to those using the selected link. Choosing **Any** will cause all calls in progress to be displayed.

Clicking a call in the **Start Time** column opens the **Call Details** page, which provides the following information:

- Details about the caller: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Details about the callee: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Call route, including the total distance configured for the route taken by the call.
- Call rate policy, including peak utilization policy.

To monitor calls for a link or links, perform the following steps:

**Procedure**

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime Servers > Bandwidth Manager**.
3. Click the **Monitoring** tab.
4. Click the **Link Calls** tab on the monitoring page.
5. Optionally, click a specific link in the **Link Calls** dropdown list to see calls in progress for that link only. To see all calls currently in progress, choose **Any**.
6. Click the **Link Calls** tab to see a table of calls currently in progress.
7. In the **Links** table, click a link name in the **Name** column to see the site configuration page for that link.
8. In the **Links** table, click a number in the **Calls** column to see what calls are currently utilizing bandwidth in the link displayed in that table row.
9. End any call by checking the checkbox next to the start time for that call and then clicking the **End Call** button. To refresh the list of calls at any time click the **Refresh** button.

**Monitoring calls for selected sites**

Use the **Site Calls** table to monitor calls for each site in the network managed by IBM Sametime Bandwidth Manager.

**About this task**

The monitoring interface includes tabs for links, sites, link calls, and site calls. The **Site Calls** tab shows calls that are currently in progress. By choosing a specific site
in the **Site Calls** dropdown list, the administrator can limit the calls shown to those originating from or terminating at the selected site. Choosing **Any** will cause all calls in progress to be displayed.

Clicking a call in the **Start Time** column opens the **Call Details** page, which provides the following information:

- Details about the caller: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Details about the callee: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Call route, including the total distance configured for the route taken by the call.
- Call rate policy, including peak utilization policy.

### Procedure

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime Servers > Bandwidth Manager**.
3. Click the **Monitoring** tab.
4. Click the **Site Calls** tab on the monitoring page to see a table of calls currently in progress.
5. Optionally, click a specific site in the **Site Calls** dropdown list to restrict the display to calls in progress for that site only. To see all calls currently in progress, choose **Any**.
6. In the **Site Calls** table, click a call link in the **Start Time** column to see the site details for that call.
7. The administrator can end any call by checking the checkbox next to the start time for that call and then clicking the **End Call** button. To refresh the list of calls at any time click the **Refresh** button.

### Bandwidth Manager statistics

Understanding the Bandwidth Manager monitor statistics can be useful for fine-tuning site and link bandwidth allocations and peak utilization points.

### Links and sites

- **Bandwidth in Use** shows the static amount of bandwidth allocated for the call, link, or site based on applied Call Rate policies. As such, it is not a reflection of the real-time current bandwidth consumed – rather, it should be considered a maximum allowed for the call.

  The allocated bandwidth does not affect other activities that might be occurring in the monitored element – it affects only audio/video traffic. Chat, call setup,
server communication overhead are all not counted towards the bandwidth allocation. The allocated bandwidth affects only the payload and does not include any transport-related data.

- **Bandwidth Remaining**
  shows the difference between the configured maximum bandwidth for the site or link and the current Bandwidth in Use.

- **Utilization** is the percentage of the maximum bandwidth currently allocated.

- **Calls** is the current number of active calls on the link or site. For conference calls hosted on an MCU or the Sametime Packet Switcher, each individual call leg for each participant is reported as a separate call in the Bandwidth Manager Monitor.

As a general rule-of-thumb for planning purposes, you can assume the actual single-call one-way send bit rate is around 65-75% of the configured maximum call rate as defined in the policy, assuming the client utilizes a codec/resolution that matches the policy. This general rule assumes H264 video is used with ISAC audio, and takes into account transport-independence, normal call activity, and overhead, but it does not take into account other non-audio/video activity that might be taking place concurrently (although unless users are doing lots of big file downloads, this affect should be small relative to the A/V traffic). The receive bit rate will vary depending on the sender's codec/resolution, and this can also change during a conference call as the active speaker changes. For a large population of users, it should be possible to estimate with a good degree of accuracy the best maximum bandwidths and peak utilization points of any given site or link, but this exercise is beyond the scope of this documentation.

**Call details**

The call details give information about the specific call or call legs on a site or link such as time started, duration, and bandwidth sent or received. Note that the 'Callee sent' statistic makes sense only in the context of point-to-point calls since for conference calls the callee is always the MCU, and the data sent from the MCU differs depending on the other originating call leg.

**Sametime Client auto-tuning feature and its effect on allocated bandwidth**

The Sametime client has an auto-tune feature that potentially reduces either frame-rate or video resolution during a call depending on the current load of the CPU on which the client is running. Overall real bandwidth consumed for a site or link may be further reduced if there are a significant number of overtaxed machines running Sametime on those sites or links. If link and site capacity seems to be consistently insufficient, the auto-tune feature may be the reason.

**Holding calls and pausing videos and their effects on allocated bandwidth**

When the user holds a call (or pauses video), the Bandwidth Manager retains the original bandwidth allocation for the call. Retaining the original bandwidth allocation keeps the bandwidth available when the call resumes. However, this policy results in certain calls being allocated more bandwidth than they are actually using, which is a necessary trade-off for the guarantee of being able to resume calls. When resuming a call from a prior hold, the Bandwidth Manager server gets a new look at the negotiated session, which might or might not match the initial session parameters. As such, Bandwidth Manager might fine-tune the allocated bandwidth to match the new session. The Bandwidth Manager never
denies such a call, but it will never allocate more bandwidth than was previously allocated for the same call leg because initial allocations make the most conservative assumptions.

**Reflector policies and their effects on allocated bandwidth**

Reflectors in the topology also affect the amount of bandwidth allocated for each call that flows through reflectors. Defining a reflector on a site effectively doubles the bandwidth allocated for that site for each affected call to account for the extra hop that media traffic must take as it traverses the reflector site.

For example, assume you have the following route:

Caller site → Transit site → Receiver site

Without a reflector, the bandwidth used for a single call on each of the three sites is \( n \). When you add a reflector on the Transit site, the allocated bandwidth is still \( n \) on the Caller and Receiver sites, but becomes \( 2n \) on the Transit site.

---

**Administering a Sametime Meeting Server**

This section describes how to manage an IBM Sametime Meeting Server.

**About this task**

The Sametime Meeting Server supports real-time collaboration through screen sharing and a shared whiteboard. The Sametime Meeting Server also provides a variety of other types of support for the meeting activity occurring in Sametime.

**Updating Sametime Meeting Server connection properties on the console**

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Meeting Server.

**Before you begin**

If you are configuring the Sametime Meeting Server to use SSL (Secure Socket Layer), make sure the server’s certificate has been added to the Sametime System Console’s trust store.

**About this task**

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Meeting Server. These settings are only used by the Sametime System Console to connect to the Sametime Meeting Server.

Follow these steps to update connection setting information.

**Procedure**

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Server.
3. In the Sametime Meeting Servers list, click the **Edit** next to the deployment name of the server with the connection information that you want to change.

4. Under Connection Properties, enter the administrator’s **User name** and **Password** for connecting to the Sametime Meeting Server.

5. By default, the Sametime Meeting Server trusts other Sametime components. If you want to change this setting, then select **Do not auto-accept SSL certificate**.

6. Click **Save**.

7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

**Related tasks:**

“Adding a Sametime server SSL certificate to the Sametime System Console” on page 308

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

---

**Managing file sharing**

You can limit the types of files that can be shared in meeting rooms as well as edit file conversion settings for your IBM Sametime Meeting Server configuration.

**About this task**

You can edit but not delete any of the file conversion settings that come installed with IBM Sametime. You can delete any new settings that you have added.

**Procedure**

1. Log in to the Integrated Solutions Console.

2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.

3. In the **Meeting Servers** list, click a server with the configuration that you want to change.

4. Click the **Server Configuration** tab.

5. Click **Edit**.

6. Edit the appropriate configuration value. You can only edit the value; you cannot edit a configuration key name.

**Table 39. Configuration key values**

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.conversion.include</td>
<td>pdf, sam, bmp, gif, cgm, htm, html, jpg, jpeg, jpe, 123, wk3, wk4, 123, pre, prz, pic, lwp, xls, xlsx, ppt, pptx, doc, docx, sdd, sxi, sxw, sdc, sxc, pco, pcp, png, rft, rdfs, odp, odi, tiff, tif, eps, txt, bat, ini, vsd, umf, wpd, wpg, wp2, xml</td>
<td>List of file type extensions that can be converted by the Sametime Meeting Server for document sharing. Separate extensions by a comma.</td>
</tr>
</tbody>
</table>
### Table 39. Configuration key values (continued)

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.fileio.codebase</td>
<td><code>c:\temp\docshare</code></td>
<td>Location of the temporary directory for document sharing used by the Sametime Meeting Server. Examples: <code>c:\temp\docshare</code> or <code>/opt/temp</code></td>
</tr>
<tr>
<td>docshare.native.codebase</td>
<td><code>c:\Program Files\IBM\Websphere\STMeetingServer\stellent\exporter.exe</code></td>
<td>Location of the executable file for the Sametime Meeting Server document conversion. Examples: <code>c:\Program Files\IBM\Websphere\STMeetingServer\stellent\exporter.exe</code> or <code>/opt/IBM/WebSphere/STMeetingServer/stellent/exporter</code></td>
</tr>
</tbody>
</table>

7. Click **OK**.

#### Results

Configuration changes immediately take effect.

### Requiring meeting passwords

You can require that all meeting rooms in IBM Sametime have passwords.

#### About this task

Meeting rooms are not required to have passwords by default. You can change this configuration setting so that meeting rooms are required to have passwords.

#### Procedure

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.

4. Click the **Server Configuration** tab.

5. Click **Edit**.

6. Scroll down to the `meetingroomcenter.passwords` configuration key. You can only edit the value; you cannot edit a configuration key name.

7. Change the **Configuration Value** to one of the following values:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No password required. This is the default value.</td>
</tr>
<tr>
<td>1</td>
<td>Password required. The password must contain at least five characters.</td>
</tr>
<tr>
<td>2</td>
<td>Strong password required. A strong password must contain eight or more characters, mixed upper and lower case letters, at least one number, and at least one special character (for example: comma, exclamation point, or asterisk).</td>
</tr>
</tbody>
</table>

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

`: \ } ' " & < >`

8. Click **OK**.

**Results**

This configuration change immediately takes effect.

**Limiting guest access to the Meeting Room Center**

You can prevent unauthenticated users (guests) from accessing the Meeting Room Center.

**About this task**

Unauthenticated users have limited access to the Meeting Room Center. They can view information in the Meeting Room Center, but they can never create meeting rooms or edit meeting room information. You can change this default value to completely deny them access to the Meeting Room Center. This change does not prevent guest access to an actual meeting; it only prevents access to the Meeting Room Center.

**Procedure**

1. Log in to the Integrated Solutions Console.

2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.

3. In the **Meeting Servers** list, click a server with the configuration that you want to change.

4. Click the **Server Configuration** tab.

5. Click **Edit**.
6. Scroll down to the `meetingroomcenter.allowGuestAccess` configuration key. You can only edit the value; you cannot edit a configuration key name.

7. In the `Configuration Value` field, type 0 to deny unauthenticated user access to the Meeting Room Center.

   **Note:** If you change your mind, or if you ever want to grant unauthenticated user access, type 1.

8. Click OK.

**Results**

This configuration change immediately takes effect.

**Defining a Sametime Proxy server for awareness in meeting rooms**

You must define the IBM Sametime Proxy server that is used for awareness so that Sametime users can be detected when they are in Sametime meeting rooms.

**Before you begin**

You must have a Sametime Proxy server installed and configured. You must set up SSO between the Sametime Meeting Server and the Sametime Community Server.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click `Sametime System Console > Sametime Servers > Sametime Meeting Servers`.
3. In the `Meeting Servers` list, click a server with the configuration that you want to change.
4. Click the `Server Configuration` tab.
5. Click `Edit`.
6. Scroll down to the `meetingroomcenter.stProxyAddress` configuration key. You can only edit the value; you cannot edit a configuration key name.
7. Enter the URL for the Sametime Proxy Server used for awareness in the `Configuration Value` field. For example:
   ```plaintext```
   http://myhostname.mydomain.com:9080
   ```plaintext```
8. Click OK.
9. Restart the Sametime Meeting Server.
Related tasks:
Setting up SSO between the Sametime Meeting Server and the Sametime Community Server
Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

Customizing the Sametime Meeting Server configuration
You can customize your IBM Sametime Meeting Server by changing configuration keys. You can also add your own configuration keys.

About this task
The custom configuration keys that you create yourself display after the configuration keys that come pre-configured with the Sametime Meeting Server. Custom configuration keys that you create yourself can be edited and these are the only configuration keys that can be deleted. Do not delete any of the pre-configured custom configuration keys unless directed to do so by IBM.

Table 40. Pre-configured custom configuration keys

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.conversion.timeout.minutes</td>
<td>5</td>
<td>Upload duration (in minutes). Upload a file to the meeting room. If the file cannot be converted in X minutes, then the file cannot be converted any more.</td>
</tr>
<tr>
<td>docshare.jpeg.quality</td>
<td>90</td>
<td>Quality of shared document. The lower the value, the lower the quality.</td>
</tr>
<tr>
<td>meetingroomcenter.maxRoomsPerPage</td>
<td>100</td>
<td>Number of rooms listed on a page in the Meeting Room Center. The configuration key is ignored if the value is less than 100.</td>
</tr>
<tr>
<td>meetingroomcenter.openRoomInNewWindow</td>
<td></td>
<td>Determines if meetings opened from the web browser room manager open in a new window or in the current window.</td>
</tr>
<tr>
<td>meetingroomcenter.stProxySSLAddress</td>
<td>none</td>
<td>Detects which protocol (SSL or non-SSL) was used to access the meeting server and picks the correct Sametime proxy address to use.</td>
</tr>
<tr>
<td>rtc4web.ejectionTimeout</td>
<td>300</td>
<td>Length of time in seconds that users are locked out of a room when they have been ejected.</td>
</tr>
</tbody>
</table>
Table 40. Pre-configured custom configuration keys (continued)

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>meeting.managedAccess.override</td>
<td>0 (do not enforce)</td>
<td>Determines whether rooms on the Sametime Meeting Server use managed access, or whether it is optional.</td>
</tr>
<tr>
<td>meetingroom.allowGuestAccess</td>
<td>1 (allow guest access)</td>
<td>Determines whether guests can access meeting rooms.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Click the **Server Configuration** tab.
5. Click **Edit**.
6. Enter the name of your **Configuration Key**.
7. Enter the **Configuration Value**.
8. Click **OK**.

**Turning on full-text indexing in the Meeting Room Center**

By default, the Meeting Room Center searches the Meeting Room Center database for rooms without using an index. If the database becomes too big, your deployment might experience performance degradation during searches. You can enable full-text indexing on the room name and owner name fields for enhanced performance on large datasets.

**About this task**

Full-text indexing takes advantage of the IBM DB2 Text Search service to build, maintain, and search by an enhanced set of indexes on the meeting room name and owner name. This augments search performance.

Full-text indexing is only used when you explicitly search for listed meeting rooms from the meeting room search box. It is not used when you search for hidden rooms, access **My Meeting Rooms** or access a **Selected Contact's Meeting Rooms**.

Full-text indexes are created for both the room name and owner name.

Full-text indexes are updated every 12 hours. Rooms created in the past 24 hours cannot be found by their full-text index, but can be found by a limited table scan. This action avoids missing a room because the index has not been created, yet. Once a room has been live for more than 24 hours, full-text indexing is available.

Follow these steps to enable full-text indexing:

**Procedure**

1. Copy `enableFullTextIndexing.bat` (Windows) or `enableFullTextIndexing.sh` (Linux, Unix) from the root directory of the Sametime Meeting Server install image to the DB2 bin directory.
If you have an extremely large database, this script can be edited to customize the location of the index files.

2. Run the command to start the DB2 Text Search service, which sets up the full-text indexes and enables the database for full-text searches.

   - **Windows**
     
     `enableFullTextIndexing.bat STMS dbadmin password`

   - **AIX, Linux, or Solaris**
     
     `enableFullTextIndexing.sh STMS dbadmin password`

Replace **STMS** with the name of the Meeting Server database if you chose a different database name when you created it.

Replace **dbadmin** and **password** with the DB2 Application user ID and password you created when you installed DB2.

3. Follow these instructions to turn on full-text indexing for the Meeting Room Center in the Sametime System Console.
   a. Log in to the Integrated Solutions Console.
   b. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers.**
   c. In the **Meeting Servers** list, click a server with the configuration that you want to change.
   d. Select **Server Configuration.**
   e. Click **Edit.**
   f. Change the value of **meetingroomcenter.useFullTextIndexing** to **true.** This setting is a custom key. If a search has been previously performed on the server, then the key and the value display in the interface.
   g. Click **OK.** The changes take effect within one minute.

**What to do next**

If you restart the server, the service does not restart automatically.

On Windows, you can go into Services and change the **DB2TS** service to start automatically. From the Start menu, click **Run,** and type **services.msc,** and change the DB2TS services to start automatically.

On Linux, you can edit one of the startup scripts to start **db2ts** when you restart. The command to start **db2ts** is **db2ts start for text.**

For more information on DB2 maintenance, see Best Practices for DB2 maintenance in Sametime.

**Turning off full-text indexing in the Meeting Room Center**

Follow these steps to disable full-text indexing in the Meeting Room Center.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers.**
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Select **Server Configuration.**
5. Click **Edit.**
6. Change the value of `meetingroomcenter.useFullTextIndexing` to `false`.
7. Click OK. The changes take effect within one minute.

What to do next

These steps are sufficient to turn off full-text indexing; however, the full-text indexes still exist and take up disk space. If you want to permanently delete the full-text indexes, copy `dropFullTextIndexing.bat/sh` to the DB2 bin directory and run `dropFullTextIndexing.bat/sh database_name`. For example, `dropFullTextIndexing.bat STMS`. If you remove the database, the `dropFullTextIndexing` script should be run first to properly clean up the indexes.

Monitoring meeting room statistics

You can view usage statistics for IBM Sametime meeting rooms in the Meeting Room Center.

About this task

Only administrators can view statistics for meeting rooms. Other Sametime users cannot view meeting room statistics. Deleted meeting rooms are not included in these statistics.

Procedure

1. Log in to the Sametime Meeting Room Center.
   
   http://hostname/stmeetings/
2. Click Meeting Room Statistics.
3. Click one of the following views:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays the total number of rooms and active participants, and the total size of all libraries. An active participant is a participant that is currently in a room.</td>
</tr>
<tr>
<td>Active rooms</td>
<td>Lists all the rooms by meeting room name that currently have participants.</td>
</tr>
<tr>
<td>Usage by room</td>
<td>Lists all active and inactive rooms by meeting room name.</td>
</tr>
<tr>
<td>Usage by owner</td>
<td>Lists all room owners by Sametime ID. Rooms can be active or inactive.</td>
</tr>
</tbody>
</table>

You can click on a column heading in any view to sort the information.

In the Active room or Usage by room views, you can click an owner or room name to get detailed usage statistics on that particular owner or room. In the Usage by owner view, you can click an owner name to get detailed usage statistics.

Backing up user data for Sametime meeting rooms

All IBM Sametime meeting room user data is stored in an IBM DB2 database, and can be backed up using the DB2 backup commands.
About this task

The default Sametime configuration requires that DB2 be shut down for backup. This is because by default, DB2 is configured to reuse the recovery logs. If you want online backup, the database can be configured to archive the recovery logs. In that case, the database is backed up, and all archived recovery logs are backed up. The recovery logs that have been backed up must also be periodically removed. If the database runs out of space to archive the recovery logs, the database will stop accepting changes until space is available.

Database backup and recovery is fully outlined in the DB2 information center. See "Backup overview."

Example for online backup

```
db2 update database configuration for STMS using logretain on
db2stop
db2start
```

Perform an offline backup to be kept:

```
db2 backup database STMS
```

Afterwards, you can perform online backups:

```
db2 backup database STMS online include logs
```

---

Administering a Sametime Gateway Server

Set up and begin using the IBM Sametime Gateway to enable local IBM Sametime users to have real-time collaboration with users of other instant messaging systems. After installing the Sametime Gateway, you can create a local and external community, manage user access, add message handlers if necessary, and set properties such as session time outs and blacklist domains.

Updating Sametime Gateway Server connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Gateway Server.

Before you begin

If you are configuring the Sametime Gateway Server to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Gateway Server. These settings are only used by the Sametime System Console to connect to the Sametime Gateway Server.

Follow these steps to update connection setting information.

Procedure

1. Log in the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Gateway Server**.

3. In the Sametime Gateway Servers list, click the **Edit** next to the deployment name of the server with the connection information that you want to change.

4. Under Connection Properties, enter the administrator's **User name** and **Password** for connecting to the Sametime Gateway Server.

5. By default, the Sametime Gateway Server trusts other Sametime components. If you want to change this setting, then select **Do not auto-accept SSL certificate**.

6. Click **Save**.

7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

**Related tasks:**

"Adding a Sametime server SSL certificate to the Sametime System Console” on page 308

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

---

**Assigning users access to external communities**

Assign local users access to external or clearinghouse communities so that they can exchange real-time communications with users from external communities. You can assign access only for local users.

**About this task**

Before you assign users, you must first add an external community or clearinghouse and set its properties. You must also make sure that the IBM Sametime Gateway is configured for use with an LDAP directory that contains person records of users in the local Sametime community.

**Expected state:**

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.

2. Select an external community from the table.

3. Click **Assign users**.

4. Determine if you want to assign equal access to the external community or clearinghouse for everyone or set access for each user.
   - Select **Assign access to all users for this route** to give everyone the same access.
   - Select **Assign access to individual users and groups for this route** to set access for each user.

5. In the **Search by** field, select group, first name, or last name.

6. In the **Search for** field, type the name, or use an asterisk (*) as a wildcard.

7. From the **Search results**, select the users to be given access to the external community. Use the **Page** buttons to see additional names. Search results show
names from the local community only because only local users may be
assigned to an external or clearinghouse community.

8. Select users and click Add to assign the users. Note that any user assigned to
access the external community automatically receives both instant messaging
and presence capabilities. These capabilities cannot be changed.

9. Optional. To take names off the assigned users list, select the users and click
Remove Selected Names.

10. Click OK.

What to do next

No assignment of external users to the local community is necessary. External
community user access to local users is determined when a local community user
subscribes to instant messaging and presence with an external user.

Note: When the server is configured to require permission from the Sametime
user, the Sametime user sees a popup window requesting permission for the
external user to watch the Sametime user’s status. The Sametime user can approve
or decline.

Related reference:
“Assign local users and capabilities” on page 158
Assign users and groups from the local community permission to exchange
real-time messages with an external community or clearinghouse community. Use
this panel to control access to Sametime Gateway and external messaging
communities.

Finding users
Determine if a local user is assigned access to an external community. In addition,
determine the capabilities assigned to the user.

Before you begin

You must create an external community and assign users to the community first.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime
  Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Communities .
2. Select an external community from the table.
3. Click Find Users.
4. Type the user’s email address and click Search to determine if the user is
   assigned to access the external or clearinghouse community, and to see the
capabilities assigned to the user.
**Related reference:**
“Find user” on page 160
Find a user in LDAP and view the capabilities that the user has permission to use when accessing the selected instant messaging community.

**Viewing users**
Determine the users and groups that are assigned to access an external community or clearinghouse community.

**Before you begin**
You must create an external community and assign users and groups to the community first.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**
1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. Click the name of an external or clearing house community to open the details about that community.
3. Click **View Users** to view the users and groups assigned to the external community. To find an individual user, use **Find User** on the community list page.

**Related reference:**
“View users” on page 160
See who has access to exchange real-time messaging with an external community or clearinghouse.

**Enabling spam filtering**
You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

**About this task**
Adding a message handler involves first installing the application as a J2EE application through WebSphere Application Server, starting it, then using the Sametime Gateway administrative console to configure its properties. After the message handler is configured, you must enable it and then restart the application.

The message handler must be a J2EE application that implements the Sametime Gateway plug-in API. See the Sametime Gateway Integration Guide that is included in the Sametime Software Development Kit for information on how to create a message handler plug-in.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.
Procedure
1. To add a message handler to Sametime Gateway, log into the Integrated Solutions Console (http://localhost:9060/ibm/console) and click Applications > Enterprise Applications.
2. Click Install and follow the instructions for installing the application.
3. Click Start to start the application. Starting the application causes it to appear in the list of message handlers.
4. Click Sametime Gateway > Message Handlers to view the message handler list.
5. Click the newly installed message handler to edit its properties.
6. Select the type: event logger, access control list, user locator, or other.
7. Optional. Select Run the message handler regardless of whether previous handlers complete their processing of messages. If not selected, the message handler does not run if the preceding message handler failed to complete its handling of a message.
8. Click OK. You should now be back on the message handler list page.
9. Click Sametime Gateway > Message Handlers, select a message handler, and click the Move Up and Move Down buttons to change the order in which the message handler processes messages. Note that User locator message handler must be first and the Event logger message handle must be last.
10. On the Message Handler list page, select the newly installed message handler and click Enable.

Results
To remove a message handler, you must disable the message handler first, and then uninstall the plug-in through WebSphere Application Server.

Related reference:
“Troubleshooting message handlers” on page 434
This topic discusses how to troubleshoot message handlers in various stopped and started or enabled and disabled conditions.
“Message handler properties” on page 160
Use this page to configure the properties of a message handler such as the user locator, authorization controller, or event logger.
“Message handler list” on page 162
Use this page to configure message handlers that perform such tasks as finding users in the local community for whom to relay messages, checking the access control for local community members, and logging IBM Sametime Gateway events. Message handlers that are provided by Sametime Gateway, with the exception of the Event logger, do not need configuring.

Maintaining and monitoring Sametime Gateway
The IBM Sametime wiki provides recommended procedures for maintaining and monitoring Sametime Gateway.

About this task
You can find recommendations in the Sametime wiki on the following areas:
• Log files lifecycle and maintenance
• Renewing any SSL certificates
• Monitoring communities
Periodic maintenance for DB2
Recycling of Websphere processes
File system cleanup

See this article in the Sametime wiki: Sametime Gateway - Recommended production maintenance procedures.

Reference

This topic provides property reference help for the administrative user interface, scripting commands, and sample JACL scripts.

Sametime Gateway reference

These topics provide details about IBM Sametime Gateway properties and settings for communities, message handlers, and translation protocols which you can administer through the Integrated Solutions Console.

Sametime Gateway properties:

Use this page to set the maximum chat sessions. You can also specify domains from which to block messages.

Set maximum sessions

This option sets the maximum instant messaging and presence sessions. A limit of 1000 instant messaging and 1000 presence sessions is set by default. Note that maximum sessions set here override the maximum sessions that are set for a route to a community.

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>no limit</td>
</tr>
<tr>
<td>0</td>
<td>no sessions allowed</td>
</tr>
<tr>
<td>(n)</td>
<td>(n) sessions allowed, (n) is any integer between 1 and 2147483647</td>
</tr>
</tbody>
</table>

Blacklist domains

Specify the DNS blacklist sites to check when the Sametime Gateway receives a subscription request. The Sametime Gateway rejects messages when either the destination or source domains are in this list. Use Fully qualified domain names or TCP/IP addresses separated by a comma, semicolon, or space. Wild cards using an asterisk in the left-most subdomain position are allowed. For example, *.spamalot.com is allowed.

Related tasks:
“Setting a global limit on sessions” on page 252
You should set a global limit for the maximum number of sessions allowed on a server, which helps prevent out-of-memory errors. The value set here will supersede a larger value set in the “Route maximum sessions” property.

Sametime Gateway communities:

View the list of communities and use the list as the starting place to set up communities, assign local users access to external communities, and set properties on communities. The communities list shows the community name, the type of community, and the translation protocol used.
Task buttons

Use the communities list to create a new community or edit the properties of an existing community. Select a community first before using the button actions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Sets up a connection to a local, external, or clearinghouse community. You must supply domain names of the community. The type of community often determines the translation protocol used. External and clearinghouse communities usually use the SIP translation protocol, which relies on the SIP infrastructure in WebSphere Application Server to handle message routing, or the XMPP protocol. The local community is connected to the IBM Sametime Gateway by means of the VP (Virtual Places) protocol.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a community from the Sametime Gateway.</td>
</tr>
<tr>
<td>Find user</td>
<td>Determines if a local user is assigned to the community and determines the capabilities such as instant messaging and presence that are assigned to the user. Enable the Find user button by selecting an external or clearinghouse community. Search by email address only.</td>
</tr>
<tr>
<td>Assign users</td>
<td>Assigns users from the local community permission to access the selected community. You can assign users from the local community only, not from external or clearinghouse communities. Enable the Assign users button by selecting an external or clearinghouse community.</td>
</tr>
</tbody>
</table>

Select and filter buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Selects all items.</td>
</tr>
<tr>
<td></td>
<td>Deselects all items.</td>
</tr>
<tr>
<td></td>
<td>Searches the custom properties by column. To filter the table, select the column by which to filter, then enter filter criteria. You can use wildcard characters (*, ?, %) and the text is not case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>Hides the filter names from being displayed.</td>
</tr>
</tbody>
</table>

Name

The name is the name given to the community when the community is first created. Click a name to configure properties or assign users to the community.

Type

A community is generally a set of users connected by a common user directory. There are three types of communities: local, external, and clearinghouse communities. You can have an unlimited number of external communities, but you can have only one local community and one clearinghouse community. IBM recommends that you do not configure both the AOL clearinghouse and the AOL communities, as users served by the AOL clearinghouse are a superset of users served by the AOL community. If you set up AOL only, and later decide to connect
with the AOL clearinghouse community, delete the AOL community first before adding the AOL clearinghouse community to Sametime Gateway.

The local community is the local Sametime community.

An external community is a set of users in domains connected by a common directory and belonging to a remote company or organization.

A clearinghouse community is a federated group of users linked by an enterprise's message router. When a message contains destination domains not found elsewhere in a routing configuration, the message may be routed to a clearinghouse community if one exists. A route to a clearinghouse enables Sametime Gateway users to connect to a much wider community.

**Translation protocol**

A translation protocol is the communication standard used by the Sametime Gateway to code and decode messages from communities into a format understood by Sametime users. The Sametime Gateway provides the following translation protocols:

<table>
<thead>
<tr>
<th>Translation Protocol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for Sametime Gateway</td>
<td><strong>SIP for Sametime Gateway</strong> is used to exchange messages with other Sametime communities who use Sametime Gateway versions 7.5 or later.</td>
</tr>
<tr>
<td>SIP for AOL</td>
<td><strong>SIP for AOL</strong> is used to connect with AOL Instant Messaging.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td><strong>SIP for legacy Sametime Gateway</strong> is used to connect with Sametime 6.5.1 and 7.0 servers.</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td><strong>SIP for OCS</strong> is used to connect with Office Communications Server communities.</td>
</tr>
<tr>
<td>VP</td>
<td><strong>VP</strong> (Virtual Places) is the proprietary protocol used to connect the Sametime Gateway with the local community on the Sametime 7.5 or later server.</td>
</tr>
<tr>
<td>XMPP</td>
<td><strong>XMPP</strong> is the Extensible Messaging and Presence Protocol (XMPP) for connecting to Google Talk and XMPP communities.</td>
</tr>
</tbody>
</table>

**Assign users**

Click this link to assign users and groups to the route to this community. Note that you must first create the community, and then select the community in the table before you can assign users to the community.

**View users**

Click this link to view users assigned to the route for this community. Note that you must first create the community, and then select the community in the table before you can view users in the community.

**Community properties:**
Use this page to connect IBM Sametime Gateway to one internal community and multiple external communities, or to edit the connection properties of an existing community. Specify the type of community, the domains to use when accessing the community, the translation protocol that Sametime Gateway uses to communicate with the community, connection details, and any custom properties for the connection or community. After you create a community, use the Assign local users to this community link to give permission to local users to access the external or clearinghouse community.

**Name**

Type a descriptive name for the community.

**Community type**

Select the type of community:

<table>
<thead>
<tr>
<th>Community type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL clearinghouse</td>
<td>The AOL clearinghouse community acts like a message router with links to several communities.</td>
</tr>
<tr>
<td>Local</td>
<td>The local community is the internal IBM Sametime community served by the Sametime Gateway. The Sametime Gateway can connect to only one local community, but the local community can be made up of many domains within the community, as long as those domains are connected by a single user directory.</td>
</tr>
<tr>
<td>External</td>
<td>An external community is any community connected by a common directory and belonging to another company or organization outside the fire wall.</td>
</tr>
</tbody>
</table>

**Community custom properties**

Click this link to add custom properties to the community, or edit existing custom properties. Some external communities may require extending the Sametime Gateway functionality by adding a custom property in order to connect to the community.

**Domains**

Type at least one unique, Fully qualified domain name or TCP/IP address for the community. List multiple domain names separated by a comma, semicolon, or space. Domain names have two or more parts separated by dots, such as example.com. Each domain name must access the same user directory. For example: example.com, us.example.com, fr.example.com, de.example.com must access the same user directory in the community. The wildcard asterisk (*) is accepted in the first subdomain only.

<table>
<thead>
<tr>
<th>Wildcards</th>
<th>Case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct wildcard use</td>
<td>Asterisk as the first subdomain</td>
<td>*.domain.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.subdomain2.subdomain1.domain.com</td>
</tr>
</tbody>
</table>
Wildcards | Case | Examples |
--- | --- | ---
Incorrect wildcard use | Single asterisk | * |
Asterisk as the domain | * .com |
Asterisk as part of a domain or subdomain | * domain.com |
Multiple asterisks in one domain | * * . domain.com |
Asterisk is any position other than the first | subdomain * . domain.com |
Asterisk in a TCP/IP address | 9.92.128. * |
Domains that are already included when using a wildcard | * domain.com and subdomain . domain.com. Including the second domain is not needed. |

If connecting to any of the following instant messaging communities, include the community domains listed in the following table:

<table>
<thead>
<tr>
<th>Instant messaging communities</th>
<th>Available domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL Instant Messenger</td>
<td>aol.net, corp.aol.com, aol.com</td>
</tr>
<tr>
<td>Google Talk</td>
<td>gmail.com</td>
</tr>
</tbody>
</table>

**Translation protocol**

A translation protocol translates instant messages from one code standard to another to allow different instant messaging systems that rely on different protocols to talk with each other. Select a protocol that matches the protocol used by the community’s instant messaging application.

<table>
<thead>
<tr>
<th>Translation protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for AOL</td>
<td>Use <strong>SIP for AOL</strong> for all AOL Instant Messenger and AOL clearinghouse community connections.</td>
</tr>
<tr>
<td>SIP for Sametime Gateway</td>
<td>Use <strong>SIP for Sametime Gateway</strong> for connections to Sametime Gateway 7.5 or later communities.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td>Use <strong>SIP for legacy Sametime Gateway</strong> for connections to Sametime server versions 7.0 or 6.5.1 only.</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td>Use <strong>SIP for OCS</strong> for all Office Communication Server connections.</td>
</tr>
<tr>
<td>VP</td>
<td>Use <strong>VP</strong> (Virtual Places) for connecting to the local or internal Sametime community only.</td>
</tr>
<tr>
<td>XMPP</td>
<td>Use <strong>XMPP</strong> to connect with communities that use Google Talk or XMPP.</td>
</tr>
</tbody>
</table>
Translation protocol details

Click this link to view translation protocol properties and custom properties for the protocol.

Connection

Specify the connection properties that the Sametime Gateway uses to connect to the local, external, or clearinghouse community. You are prompted for connection information based on the translation protocol that you select.

<table>
<thead>
<tr>
<th>Community</th>
<th>Translation protocol</th>
<th>Default port</th>
<th>Transport Protocol</th>
<th>Connection details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>VP</td>
<td>1516</td>
<td>TCP</td>
<td>Domain: Fully qualified domain name or TCP/IP address of the Sametime server in the local community. For example: rtcgatewayserver.de.example.com The port number must match the VP port number on the Sametime server.</td>
</tr>
<tr>
<td>External</td>
<td>SIP for AOL</td>
<td>5061</td>
<td>TLS</td>
<td>Domains: aol.net, corp.aol.com, aol.com Requires hostname: sip.oscar.aol.com.</td>
</tr>
<tr>
<td>External</td>
<td>SIP for OCS</td>
<td>5061</td>
<td>TLS</td>
<td>Host name: host name or the IP address of the OCS Edge Server. Domains: domain names of the Office Communications Server community. For example: ocs.example.com</td>
</tr>
<tr>
<td>External</td>
<td>SIP for Sametime Gateway</td>
<td>5060 or 5061</td>
<td>TCP (5060) or TLS (5061)</td>
<td>Host name: domain name of the external Sametime Gateway server or Sametime Server such as ExampleServer1.com, for example. Domains: list of domains used by the external Sametime community.</td>
</tr>
<tr>
<td>External</td>
<td>XMPP (for Google Talk)</td>
<td>5269</td>
<td>TCP</td>
<td>Requires that you set up a domain service (SRV) record and publish it to DNS if connecting to Google Talk. Configure additional connection detail by using the Custom properties link.</td>
</tr>
<tr>
<td>External</td>
<td>XMPP</td>
<td>5269</td>
<td>TCP or TLS</td>
<td>Host name: domain name of the external XMPP server. Domains: list of domains used by the XMPP community.</td>
</tr>
<tr>
<td>AOL Clearinghouse</td>
<td>SIP for AOL</td>
<td>5061</td>
<td>TLS</td>
<td>Host name: sip.oscar.aol.com.</td>
</tr>
</tbody>
</table>

Route properties

You must add an internal community before you can view or edit Route properties.
Enable route for this community

Select to enable the route to this community.

Set the maximum sessions for each capability for the route

Select to set the maximum sessions for each capability on the route. Sessions should always be larger than presence. Note that global maximum allowed Sametime Gateway sessions override the maximum sessions for each capability. To increase maximum sessions for each capability, make sure you increase the maximum allowed Sametime Gateway sessions.

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>no limit</td>
</tr>
<tr>
<td>0</td>
<td>no sessions allowed</td>
</tr>
<tr>
<td>n</td>
<td>( n ) sessions allowed, where ( n ) is any integer between 1 and 35000.</td>
</tr>
</tbody>
</table>

Note that community maximum sessions override gateway maximum sessions.

Select the capabilities to assign local users for the route

Select the capabilities, instant messaging and presence, to assign to the route. Both capabilities are assigned to the route and are disabled. You must click Assign users to complete the set up of the community by assigning users to use the route.

Translation protocol list:

A translation protocol is a communication standard used by an instant messaging service to initiate interactive, real-time sessions between users. Use this page to view and edit translation protocols installed with the IBM Sametime Gateway.

Name

Click the translation protocol to view or edit properties its properties.

Translation protocols

The following protocols are included with Sametime Gateway:

<table>
<thead>
<tr>
<th>Translation protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for AOL</td>
<td>Use SIP for AOL for all AOL Instant Messenger and AOL clearinghouse community connections.</td>
</tr>
<tr>
<td>SIP for Sametime Gateway</td>
<td>Use SIP for Sametime Gateway for connections to Sametime Gateway versions 7.5 or 7.5.1 communities.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td>Use SIP for legacy Sametime Gateway for connections to Sametime server versions 7.0 or 6.5.1.</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td>Use SIP for OCS to connect to Office Communications Server communities.</td>
</tr>
</tbody>
</table>
Translation protocol properties:

Use this page to view properties for translation protocols. A translation protocol is a communication standard used by a collaborative service provider to initiate interactive, real-time sessions between users. You cannot edit the Name or Java Class.

Name

Sametime Gateway name for the translation protocol.

Java Class

Shows the Java class that implements the protocol.

Custom properties

Click the custom properties to set name and value pairs for the translation protocol, or to edit the session timeout or subscription timeout properties for SIP-based protocols. This link supports the configuration of custom properties, allowing you to capture third-party software requirements that are not covered by the configuration provided by the Sametime Gateway.

Assign local users and capabilities:

Assign users and groups from the local community permission to exchange real-time messages with an external community or clearinghouse community. Use this panel to control access to Sametime Gateway and external messaging communities.

Give users from the local community permission to use instant messaging and presence with the external community. You must map your LDAP directory to the WebSphere Application Server repository before you assign users. The LDAP directory contains members of the local community. You can assign access to internal community users only. It's up to the administrator of an external community to give their users access to the local community through the IBM Sametime Gateway.

Select capabilities

- The capabilities of instant messaging and presence are automatically assigned to the route to the community and cannot be changed.
- The "Rich text" capability allows internal and external users to exchange rich text messages, which contain a variety of fonts, colors, and text formatting. This capability is available for the SIP for Sametime Gateway translation protocol only.

Note: When federating two Sametime communities, also enable the "rich text" capability for the external Sametime Gateway.
• The "Is typing" capability shows in real time when a chat partner is typing a message. This capability is available for the SIP for Sametime Gateway and SIP for OCS translation protocols only.

Note: When federating two Sametime communities, also enable the "Is typing" capability for the external Sametime Gateway.

Assign access

Select to allow access to the external community to all users, or select to allow access to the external community to individual users and groups in the local directory. When you select the All users option, the user interface hides the Search and assign users and groups field.

Search and assign groups and users

Use the Search by field to select one of the attributes by which you want to search. The default value is Group.

Use the Search for field to type a value that you want to search for, or use the wildcard character (*). The default value is * (all). Whether the search is case-sensitive depends on the user registry that is being used. For example, you might type these values if searching by group:
• To search for all groups, type *.
• To search for groups that begin with the letters luc, type luc*.
• To search for groups that end with the letters cas, type *cas.
• To search for groups that begin with the letters lu and ending with the letter s, type lu*s.

The search field cannot be blank.

In the Maximum results field, type the maximum number of search results that you want to be displayed. Valid values are 1 to 100.

Click Search to find and display a list of one or more existing users that match your search criteria.

In the Search results table, use the Select column to select individual or multiple users or groups. Click the select all icon ( ) to select all users listed. Only those visible on the table are selected if the list of users takes more than one page. If you have more than one page, you must select users from additional pages separately. You can then clear (deselect) only those users that you do not want to select.

Click the deselect all icon ( ) to clear all check boxes on the visible page of the table only.

The Name column lists group names if groups are searched, or short names or user ID if last names or first names are searched.

The Email column lists the email address of the user. Nothing appears in this column when you are searching for groups.

In the Selected names field, after you select names, click Add to move the selected groups or names to the Selected names table. The names in the Selected names
table have access to the external community. The Selected names table may potentially be very large, so it displays names over several pages if necessary. Data are thus sorted by data subset only. To use the Remove selected name tool, select a name and click this button to remove users from accessing the external community through the Sametime Gateway.

Related tasks:
“Assigning users access to external communities” on page 147
Assign local users access to external or clearinghouse communities so that they can exchange real-time communications with users from external communities. You can assign access only for local users.

Find user:
Find a user in LDAP and view the capabilities that the user has permission to use when accessing the selected instant messaging community.

Purpose
Use this page to determine if a local user is assigned to access the external or clearinghouse community. Also, you can determine the capabilities such as instant messaging and presence that are assigned to the user.

General properties
Type the user’s email address and click Search to return a list of capabilities.

Related tasks:
“Finding users” on page 148
Determine if a local user is assigned access to an external community. In addition, determine the capabilities assigned to the user.

View users:
See who has access to exchange real-time messaging with an external community or clearinghouse.

Purpose
Use this page to view a list of users who have access to capabilities on the route between the local IBM Sametime community and an external community.

General Properties
Both instant messaging and presence cannot be edited.

Related tasks:
“Viewing users” on page 149
Determine the users and groups that are assigned to access an external community or clearinghouse community.

Message handler properties:
Use this page to configure the properties of a message handler such as the user locator, authorization controller, or event logger.

Message handlers, also known as plug-ins, process instant messages as they pass through IBM Sametime Gateway. They perform such tasks as locating users,
checking the access list to use, checking for spam instant messages, and logging events. Messages are processed by handlers in the order that the message handlers appear in the list. Message handlers that are installed and started but are not yet configured are labeled Undefined in the message handler list. The User locator message handler must always be first on the message handler list. The event log handler must run and appear last in the list.

Message handlers are WebSphere Application Server applications that you install through the Integrated Solutions Console by clicking Applications > Enterprise Applications.

You add a message handler by first installing it as a WebSphere Application Server application, configuring its properties, and then enabling the message handler.

Name

There are three message handlers that are part of Sametime Gateway and cannot be removed:

<table>
<thead>
<tr>
<th>Message handler name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>User locator</td>
<td>The User locator finds the profiles associated with the originator and the target user of the message using the user name and domain from email addresses. The User locator returns an error if an inbound request contains a blacklisted domain name. The handler adds the community identifiers of the originating and target users to the message header.</td>
</tr>
<tr>
<td>Authorization controller</td>
<td>Only messages successfully processed by the User locator are passed to the Authorization controller for further processing. The Authorization controller’s main task is to allow or disallow the initiator of the message in one community to perform the requested operation with the destination user in another community.</td>
</tr>
</tbody>
</table>
| Event logger           | The Event logger records instant messaging content and events and publishes them to the SystemOut.log file. Logged events contain the following information:  
  • Message request type – subscription or instant messaging request  
  • Message initiator’s email address and community name  
  • Message receiver’s email address and community name  
  • Event status: success or failure  
  • Reason for failure  
  • Date and time  
  • Optional message content  

You must install the Sametime Gateway samples ear file available from the Sametime Software Development Kit before you enable the Event logger.

Type

Select the type of message handler. Choices are User locator, Access control, Event log, and Other. When a message handler is first installed, the default type is undefined and its status is disabled. To enable the message handler, you must select Enable the message handler.
Run this message handler regardless of the status of previous message handlers

Select to make running the message handler mandatory. That is, run the message handler regardless of whether a previously run message handler completed its process or encountered an error. If this setting is not selected, and any preceding message handler raises an error, the message handler will not run. A message handler that is not mandatory is considered conditional.

For example, the table that follows shows that in processing a message the Custom User Locator raises an error. Consequently, the mandatory Virus Checker and System Logger handlers run (in that order), while the conditional handlers, the SPIM Filter and the Custom Logger are skipped.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Mandatory or Conditional</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default User Locator</td>
<td>Access Control List</td>
<td>Conditional</td>
<td>Run</td>
</tr>
<tr>
<td>Custom User Locator</td>
<td>Access Control List</td>
<td>Conditional</td>
<td>Error</td>
</tr>
<tr>
<td>Virus Checker</td>
<td>Virus Checker</td>
<td>Mandatory</td>
<td>Run</td>
</tr>
<tr>
<td>SPIM Filter</td>
<td>Other</td>
<td>Conditional</td>
<td>Skip</td>
</tr>
<tr>
<td>Custom Logger</td>
<td>Event Logger</td>
<td>Conditional</td>
<td>Skip</td>
</tr>
<tr>
<td>System Logger</td>
<td>Event Logger</td>
<td>Mandatory</td>
<td>Run</td>
</tr>
</tbody>
</table>

Custom properties

Click Custom properties to configure additional message handler properties such as name and value pairs.

Related tasks:

“Enabling spam filtering” on page 149

You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

Message handler list:

Use this page to configure message handlers that perform such tasks as finding users in the local community for whom to relay messages, checking the access control for local community members, and logging IBM Sametime Gateway events. Message handlers that are provided by Sametime Gateway, with the exception of the Event logger, do not need configuring.

Message handlers are WebSphere Application Server applications that you install using the Integrated Solutions Console by clicking Applications > Enterprise Applications. You can add a custom message handler to the Sametime Gateway by first installing it, configuring its properties, and then enabling the application through the Message handler list.

You can enable and disable message handlers or move message handlers up or down to change the order in which a message handler processes messages.

Note: The Default User Locator must be at the top of the list.
<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the message handler after it has been installed and configured.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables the message handler.</td>
</tr>
<tr>
<td>Move Up</td>
<td>Moves the message handler up in the list so that it will process messages before other message handlers. The Default User Locator must remain at the top of the list to function properly. For best results, keep the Event Logger in the last position.</td>
</tr>
<tr>
<td>Move Down</td>
<td>Moves the message handler down in the list so that it processes messages after other message handlers. The Default User Locator must remain at the top of the list to function properly. For best results, keep the Event Logger in the last position.</td>
</tr>
</tbody>
</table>

**Table columns**

Use the **Select** column to select individual or multiple message handlers. Click the select all icon (✓) to select all message handlers listed, if, for example, you want to enable or disable all message handlers. Only those visible on the table are selected if the list of message handlers takes more than one page. If you have more than one page, you must select handlers from additional pages separately. You can then clear (deselect) only those message handlers that you do not want to select.

Click the deselect all icon (✗) to clear all check boxes on the visible page of the table only.

The **Name** is the programmatic name of the message handler. Click the name to view or edit the message handler properties.

The **Type** is one of four types assigned to the message handler. The type provides a general description of the message handler’s purpose but has no effect on how the message handler functions.

The **Status** shows whether the message handler is enabled or not.

**Related tasks:**

“Enabling spam filtering” on page 149

You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

**Custom properties list:**

Use this page to create new properties or to edit existing custom properties for communities, message handlers, connections, or translation protocols. Custom properties provide a way for you to extend the IBM Sametime Gateway by adding, for example, an outbound port number for an additional translation protocol.

**Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates a new custom property.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected custom properties.</td>
</tr>
<tr>
<td>Button</td>
<td>Resulting action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Selects all items.</td>
</tr>
<tr>
<td></td>
<td>Deselects all items.</td>
</tr>
<tr>
<td></td>
<td>Searches the custom properties by column. To filter the table, select the column by which to filter, then enter filter criteria. You can use wildcard characters (*, ?, %) and the text is not case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>Hides the filter names from being displayed.</td>
</tr>
</tbody>
</table>

**Custom properties details:**

Use this page to edit custom properties for a community, translation protocol, or message handler. You can also specify new properties that are needed to configure third-party elements used by the IBM Sametime Gateway.

You can set arbitrary name-value pairs of data, where the name is a property key and any value that can be used to set internal system configuration properties. Defining a new property enables you to configure a setting beyond that which is available in the Integrated Solutions Console. The Sametime Gateway contains several custom properties pages that work similarly to other property pages in the Integrated Solutions Console.

You can change the value of a translation protocol custom property and add a new name-value pair to an existing translation protocol. You can add new name-value pairs when adding a third party message handler or when changing the properties of an existing message handler.

**Required**

Required properties are those custom properties that are provided by the Sametime Gateway. If you create a new custom property, it cannot be considered required. Required properties cannot be deleted or renamed, but you can edit the **Value** and **Description** fields.

**Name**

Specifies the name (or key) for the property. Each property name must be unique. If the same name is used for multiple properties, the value specified for the first property that has that name is used. Do not start your property names with \texttt{was} because this prefix is reserved for properties that are predefined in the application server. Existing custom property names must not be changed if they are required, although you can change the value.

**Value**

Specifies the value paired with the specified name.

**Description**

Provides information about the name-value pair.
### Custom properties provided by Sametime Gateway

Sametime Gateway provides the following default properties that you can change to fit your environment.

<table>
<thead>
<tr>
<th>Custom Property</th>
<th>Type</th>
<th>Name</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message handler</td>
<td>Event logger</td>
<td>enableContentLogging</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>Message handler</td>
<td>Event logger</td>
<td>enableImLogging</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>Message handler</td>
<td>Event logger</td>
<td>enablePresenceLogging</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>Translation protocol</td>
<td>SIP for Sametime</td>
<td>session_timeout</td>
<td>3600 (seconds)</td>
</tr>
<tr>
<td>Translation protocol</td>
<td>legacy Sametime</td>
<td>subscription_timeout</td>
<td>3600 (seconds)</td>
</tr>
<tr>
<td>Community</td>
<td>SIP for AOL</td>
<td>servers</td>
<td>205.188.<em>, 64.12.</em>.*</td>
</tr>
</tbody>
</table>
|                          |                       |                          | **Note:** If the host name is an IPv6–format network address, set an explicit address here; do not use an abbreviated address (no brackets, no leading zeroes). For example, all of these IPv6–format network addresses are equivalent, but only the first form is accepted:  
  • 1:2:0:0:6:7:8 [acceptable]  
  • 1:2:6:7:8 [do not use this abbreviated format]  
  • 01:2:0:0:006:0007:8 [do not use leading zeroes]  
  Wildcards (such as 205:188:*:* ) are supported, as well as a mixture of IPv4 and IPv6 network addresses. |
| Community                | XMPP (for Google Talk)| servers                  | talky.l.google.com, talkz.l.google.com |
| Community                | Local community       | Sametime community exclusion list | none (disabled) |
| Community                | Local community       | server reconnection timeout | 60000 (milliseconds or 1 minute) |
| Community                | Local community       | server reconnection attempts | -1 (no limit) |
### Custom Property Type Name Default value

| Community      | External community | im failure message | none (disabled) |

### Script commands

Sametime Gateway provides many wsadmin script commands to help you administer and maintain the Sametime Gateway.

The Sametime Gateway accepts a hash table in string format ($HashString) from the wsadmin script. A hash table, or a hash map, is a data structure that associates keys with values. The primary operation it supports efficiently is a look up. For example, when given a key such as person’s email address for example, find the corresponding value for that person’s Virtual Member Manager (VMM) ID. The hash table works by transforming the key using a hash function into a hash, a number that the hash table uses to locate the desired value. The script commands handles objects in the Sametime Gateway such as a community, translation protocol, message handler, and so on, in which each entry’s key is the name of an attribute in the object, and the entry’s value is the associated object value. If there is a nested object in the encoded object, this is represented by a nested hash table.

For example, a community has a corresponding RTCGWServer object, so in the hash table that encodes community, the Sametime Gateway server is represented by a hash entry whose key is “RTCGWServer” and whose value is a hash table. The RTCGWServer to community is one-to-one mapping. Sametime Gateway converts the incoming hash table into the objects used in the Sametime Gateway administration API and performs the requested function. After process, the Sametime Gateway converts returned objects back into hash tables and returns them as hash table objects to wsadmin.

#### Related tasks:

“Running sample Jacl scripts” on page 192
Complete these steps to run a sample Jacl script.

#### Related reference:

“Sample Jacl scripts” on page 191
Sametime Gateway includes several sample scripts written in Jacl (Java TCL) to add communities to Sametime Gateway, give users access to communities, enable logging, and set properties on message handlers.

#### Related information:

- Jacl reference
- Wsadmin tool

### Hash string format:

A hash string has the following format (white space ignored except in quotation marks):

key=value,...

Or:

{key=value,...}

Where key is:
a string
And, where value is:
a string
Or:
{key=value}
Or:
[{{key=value},...}]
String A sequence of any characters except quotation mark ("), apostrophe ('), comma (,), backslash (\), and space ( ). However, you can include the above characters by enclosing in single or double quotes. But a nested single or double quote must be escaped by preceding it with a backslash. The backslash is excluded.

A non-terminal token is an apostrophe (') or quotation mark (") or backslash (\).

Examples
The following are examples of valid hash table syntax:
name=foo,value=bar
{ name='Mike\ Community', customProperties=[{name=foo,value=bar}, {name=bar, value="foo bar"] } }
{ "some key":"some value", provider={ name='a provider' }}

General Sametime Gateway operations:
This topic describes commands that perform general Sametime Gateway operations.

getRestrictedDomains:
Returns a list of restricted or blacklisted domains.

Syntax
getRestrictedDomains

Purpose
The getRestricted Domains command returns a list of blacklisted domains only if such domains were set in the Sametime Gateway. When the Sametime Gateway receives a subscription request, the Sametime Gateway checks the DNS blacklist sites and rejects messages when either the destination or source domains are in this list.

Data type: String

Sample
This sample returns a list of blacklisted domains in the Sametime Gateway:
set ons [${AdminControl completeObjectName type=RTCAdminMbean,*}]
$AdminControl invoke $ons getRestrictedDomains
addRestrictedDomain:

Adds a restricted or blacklisted domain.

Syntax

addRestrictedDomain "domain_name"

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>A Fully qualified domain name or IP address.</td>
</tr>
</tbody>
</table>

Purpose

The addRestrictedDomain command adds a blacklisted domain to the Sametime Gateway. When the Sametime Gateway receives a subscription request, the Sametime Gateway checks the blacklist domains and rejects messages when either the destination or source domain is a member of the blacklist.

Data type: String

Sample

This sample adds a blacklisted domain to the Sametime Gateway:

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons addRestrictedDomain "spamalot.com"

deleteRestrictedDomain:

Deletes a restricted or blacklisted domain.

Syntax

deleteRestrictedDomain "domain_name"

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>A Fully qualified domain name or IP address.</td>
</tr>
</tbody>
</table>

Purpose

The deleteRestrictedDomain command deletes a blacklisted domain from the Sametime Gateway. When the Sametime Gateway receives a subscription request, the Sametime Gateway checks the blacklist domains and rejects messages when either the destination or source domain is a member of the blacklist.

Data type: String

Sample

This sample deletes a blacklisted domain to the Sametime Gateway:

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons deleteRestrictedDomain "spamalot.com"
setMaxIMSessions:

Sets the maximum instant messaging sessions.

Syntax

setMaxIMSessions session_count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_count</td>
<td>Maximum instant messaging sessions in the Sametime Gateway.</td>
</tr>
<tr>
<td></td>
<td>Set to -1 to allow unlimited sessions.</td>
</tr>
<tr>
<td></td>
<td>Set to 0 to allow no sessions.</td>
</tr>
</tbody>
</table>

Purpose

The `setMaxIMSessions` command sets the maximum instant messaging sessions for the Sametime Gateway. Note that maximum sessions set with this command override community-based settings.

Data type: Integer

Sample

This sample allows unlimited sessions in the Sametime Gateway:

```bash
set ons [{$AdminControl completeObjectName type=RTCAdminMbean,*}]
$AdminControl invoke $onssetMaxIMSessions -1
```

setMaxPresenceSessions:

Sets the maximum presence sessions.

Syntax

setMaxPresenceSessions session_count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_count</td>
<td>Maximum presence sessions in the Sametime Gateway.</td>
</tr>
<tr>
<td></td>
<td>Set to -1 to allow unlimited sessions.</td>
</tr>
<tr>
<td></td>
<td>Set to 0 to allow no sessions.</td>
</tr>
</tbody>
</table>

Purpose

The `setMaxPresenceSessions` command sets the maximum presence sessions or subscriptions for the Sametime Gateway. Note that maximum sessions set with this command override community-based settings.

Data type: Integer
Sample

This sample allows 1000 presence sessions in the Sametime Gateway:
```
set ons [\$AdminControl completeObjectName type=RTCAadminMbean,*]
\$AdminControl invoke \$ons setMaxPresenceSessions 1000
```

getMaxIMSessions:

Returns the maximum instant messaging sessions.

Syntax

getMaxIMSessions

Purpose

The `getMaxIMSessions` command returns the maximum instant messaging sessions for the Sametime Gateway.

Data type: Integer

Sample

This sample gets the maximum sessions allowed in the Sametime Gateway:
```
set ons [\$AdminControl completeObjectName type=RTCAadminMbean,*]
\$AdminControl invoke \$ons getMaxIMSessions
```

getMaxPresenceSessions:

Returns the maximum presence sessions.

Syntax

getMaxPresenceSessions

Purpose

The `getMaxPresenceSessions` command returns the maximum presence or subscriptions for the Sametime Gateway.

Data type: Integer

Sample

This sample gets the maximum presence sessions allowed in the Sametime Gateway:
```
set ons [\$AdminControl completeObjectName type=RTCAadminMbean,*]
\$AdminControl invoke \$ons getMaxPresenceSessions
```

getAuthenticationAliases:

Returns an array containing the valid authentication types for the Sametime Gateway.

Syntax
getAuthenticationAliases

**Purpose**

The `getAuthenticationAliases` command returns the valid authentication aliases used by some non-SIP translation protocols in Sametime Gateway.

**Data type:** String

**Sample**

This sample gets the authentication types in the Sametime Gateway:

```
set ons [$AdminControl completeObjectName type=RTCAadminMbean,*]
$AdminControl invoke $ons getAuthenticationAliases
```

`getUserIDBye-mailAddress`:

Returns a VMM ID based on a user's email address.

**Syntax**

```
getUserIDBye-mailAddress email address
```

**Purpose**

The `getUserIDBye-mailAddress` command returns a user's Virtual Member Manager (VMM) ID from LDAP using their email address. The command throws an exception if no matches are found.

**Data type:** String

**Sample**

This sample script gets the user id of jsmith@example.com:

```
set ons [$AdminControl completeObjectName type=RTCAadminMbean,*]
$AdminControl invoke $ons getUserIDBye-mailAddress jsmith@example.com
```

`getPersonPropertiesByVMMID`:

Returns a person's display name and email address based on their VMM ID.

**Syntax**

```
getPersonPropertiesByVMMID "vmmid"
```

**Purpose**

The `getPersonPropertiesByVMMID` command gets a person's display name and email address from LDAP using the person's VMM ID. The command returns a hash table that has VMMID as the key, a list of requested properties, and the display name and email address as key-values pairs. There is no need to actually submit the VMM ID to obtain properties. Use the `getPersonPropertiesByVMMID` command with the `getUserIDBye-mailAddress` command to get this information.

**Data type:** string
Sample

This sample program first gets the user IDs from email addresses, then uses the result to obtain properties of the users based on their VMM ID.

```java
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*] $AdminControl
set m [$AdminControl invoke $ons getUserIDByEmailAddress ahernm@us.ibm.com] $AdminControl
set p [$AdminControl invoke $ons getUserIDByEmailAddress wangpin@us.ibm.com] $AdminControl
$AdminControl invoke $ons getPersonPropertiesByVMMID "$m $p"
```

`getListGroupOfUser`:

Returns the list of groups a person is member of, including nested groups.

Syntax

`getListGroupOfUser(vmmid)`

Purpose

The `getListGroupOfUser` command returns a list of groups of which the user is a member, based on the person's VMM ID.

Data type: string

Sample

```java
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*] $AdminControl
$AdminControl invoke $ons getListGroupsOfUser(vmmid)
```

`getPersonPropertiesBySearchExp`:

Returns properties about a person or group.

Syntax

`getPersonPropertiesBySearchExp(searchProp, searchExpr, returnSize)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchProp</td>
<td>integer</td>
<td>The <code>searchProp</code> parameter controls the type of search. Type 0 for group names, 1 for last names, or 2 for first names.</td>
</tr>
<tr>
<td>searchExpr</td>
<td>string</td>
<td>The <code>searchExpr</code> parameter controls what is searched and is not case sensitive. A wildcard asterisk (*) is supported. For example if <code>searchExpr=&quot;mike&quot;</code>, find any user or group named &quot;mike&quot;. If <code>searchExpr=&quot;m*&quot;, then find any user or group beginning with the letter 'm'. If </code>searchExpr=&quot;m&quot;, find any user or group ending with the letter 'm'. Note that &quot;<em>XXX</em>&quot; is not a valid search expression.</td>
</tr>
<tr>
<td>returnSize</td>
<td>integer</td>
<td>The <code>returnSize</code> parameter is the number of search results to be returned.</td>
</tr>
</tbody>
</table>

Purpose

The `getPersonPropertiesBySearchExp` command allows you to return properties such as last name or group name using a search expression. Note that group email addresses are not supported and thus do not appear in search results.
Sample

The example that follows searches for last names beginning with "m".

```java
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getPersonPropertiesBySearchExp "2 m* 3"
```

| C2E755D660D018968525719A00642F8E |
| mail5 |
| mail5@us.ibm.com |
| 9DB3D27FF355A6568525719A00643C0C |
| mail7 |
| mail7@us.ibm.com |
| 04687B65F5492BA58525719A006448A3 |
| mail9 |
| mail9@us.ibm.com |

Message handler operations:

This topic describes wsadmin commands that perform message handler operations.

**getMessageHandlerList:**

Returns a list of message handlers in the Sametime Gateway.

**Syntax**

```java
getMessageHandlerList handlerName
```

**Purpose**

The `getMessageHandlerList` command returns a list of message handlers. If `handlerName` is the name of a handler in the system, then the array contains a single hash table populated with key-value pairs, where the key is the UID of the attribute and the value is its value.

**Data type:** string

**Sample**

```java
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getMessageHandlerList "*"
```

**setMessageHandlerProperties:**

Sets the attributes on a message handler.

**Syntax**

```java
setMessageHandlerProperties handlerName, attributes
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>handlerName</code></td>
<td>string</td>
<td>Logical name of the message handler.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Data type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| attributes | hash string | Properties of the message handler:  
  - **type**: undefined, Event logger, Authorization controller, User locator, and other  
  - **enabled**: true or false  
  - **order**: 0 being first  
  - **mandatory**: true or false |

**Purpose**

The `setMessageHandlerProperties` command sets the properties for the named message handler.

**Sample**

```java
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*]
set mhp { enabled=true, type=eventLogger, customProperties=\[
{name=A, value=B} \] }
\$AdminControl invoke \$ons setMessageHandlerProperties *evtlogger \($mhp\)*
```

**Community operations**:

This topic describes `wsadmin` commands that perform community operations.

**getLocalCommunityName**:

Returns the name of the local community.

**Syntax**

```java
getLocalCommunityName
```

**Purpose**

The `getLocalCommunityName` command returns the name of the local community as a string result.

**Sample**

```java
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [\$AdminControl invoke \$ons getLocalCommunityName]
\$AdminControl invoke \$ons getRouteByCommunities \"$local company\"
```

**getLocalCommunityUid**:

Returns the unique identifier of the local community.

**Syntax**

```java
getLocalCommunityUid
```

**Purpose**

The `getLocalCommunityUid` command returns the UID of the local community as a string result.

**getCommunityList**:
_returns a list of all local, external, and clearinghouse communities in Sametime Gateway.

**Syntax**

getCommunityList communityName

**Purpose**

The `getCommunityList` command returns an array of hash tables. If communityName is the name of a community in the system, then the array contains a single hash table populated with key-value pairs. If communityName is ", the hash table contains representations of all the communities in the system.

**Data type:** string

**Sample**

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getCommunityList "*

newCommunity:

Adds a new community to the Sametime Gateway.

**Syntax**

newCommunity hashString

**Purpose**

The `newCommunity` command adds a community based on the attributes that you specify in a hash string.

**Data type:** string

The following samples are taken from the sample Jacl scripts available in stgw_server_root/samples/scripts. Consult the actual scripts for information on properties and parameters.

**Sample: adding the local community**

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]

set c {name=InternalCommunityTestName,rTCServers=[{transport=TCP,hostname=localhost,port=1516}],
internal=true,protocolConnector={name="VP"},domains=[internal.com,internal2.com]}
puts [$AdminControl invoke $ons newCommunity "{c}"]

**Sample: adding an external community**

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]

set c {name=externalCommunityTestName,rTCServers=[{transport=TLS,hostname=localhost,port=5061}],
internal=false,protocolConnector={name="SIP for legacy Sametime Gateway"},customProperties=
[[name="session_timeout",value=3600,required=false,description="Optional session timeout for externalCommunityTestName"],
[name="subscription_timeout",value=3600,required=false,description="Optional subscription timeout for externalCommunityTestName"]},domains=
[test1.com,test2.com]}puts [$AdminControl invoke $ons newCommunity "{c}"]

setCommunityProperties:
Sets the attribute named by the key to the value in the community named by `communityName`.

**Syntax**

`setCommunityProperties (communityName, properties)`

**Purpose**

The `setCommunityProperties` command sets the attribute named by the key to the value in the `communityName`.

**Data types:** string and hash string

**Sample**

```java
set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
set c {provider = {name=GenericProvider }, customProperties=[{name=f, value="some value"}]}
AdminControl invoke $ons setCommunityProperties "aol {$c}" removeCommunity
```

**removeCommunity:**

Removes a community from the Sametime Gateway.

**Syntax**

`removeCommunity communityName`

**Data type:** string

**Sample**

```java
set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
AdminControl invoke $ons removeCommunity "Company" removeCommunity
```

**Connection operations:**

This topic describes `wsadmin` commands that perform connection operations.

**getRTCServerList:**

Returns a list of Sametime Gateway servers.

**Syntax**

`getRTCServerList (communityName, primaryProvider, serverName)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>communityName</td>
<td>String</td>
</tr>
<tr>
<td>primaryProvider</td>
<td>boolean</td>
</tr>
<tr>
<td>serverName</td>
<td>String</td>
</tr>
</tbody>
</table>

**Purpose**

The `getRTCServerList` command returns a list of server hash strings containing a server with the specified server name. If "*" is specified, a list of all servers is returned.
setPrimaryRTCServerProperties:

Sets the connection properties for a given community.

Syntax

setPrimaryRTCServerProperties communityName, attributes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Data type</td>
</tr>
<tr>
<td>communityName</td>
<td>string</td>
</tr>
<tr>
<td>attributes</td>
<td>hash string</td>
</tr>
</tbody>
</table>

Purpose

The setPrimaryRTCServerProperties command sets the connection properties for a given community.

Sample

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
set s {hostname=example.com, port=15, transport=TLS, customProperties=\{\{name=A, value=B\}\}]
$AdminControl invoke $ons setPrimaryRTCServerProperties "GE {$s}"

Route operations:

This topic describes wsadmin commands that perform general route or connector operations.

getRouteByCommunities:

Returns the attributes for the local and destination communities, including access control information.

Syntax

getRouteByCommunities sourceName, destName

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external community or clearinghouse community</td>
</tr>
</tbody>
</table>

Purpose

The getRouteByCommunities command returns the route between the local and external community as a hash string table.

Sample

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [$AdminControl invoke $ons getLocalCommunityName]
$AdminControl invoke $ons getRouteByCommunities "$local company"
setRoutePropertiesByCommunities:

Sets properties for the route between the local and external communities.

Syntax

```
setRoutePropertiesByCommunities sourceName, destName, attributes
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external community or clearinghouse community</td>
</tr>
<tr>
<td>attributes</td>
<td>hash string</td>
<td>Properties for the route.</td>
</tr>
</tbody>
</table>

Purpose

The `setRoutePropertiesByCommunities` command sets properties for the route.

User and group operations:

This topic describes wsadmin commands that perform Sametime Gateway user and group operations.

getUsers:

Returns a list of users that are granted access to the specified capabilities on this route.

Syntax

```
getUsers routeUid, capability, index, pageSize
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
</tbody>
</table>
| capability | integer   | Numerical index for capabilities. Only 2 (return all capabilities) is valid. Do not use 0 or 1.  
|            |           | • 0 returns instant messaging  
|            |           | • 1 returns presence  
|            |           | • 2 returns all capabilities                                                  |
| index      | integer   | Page at which to start returning pages specified by `pageSize`. For example, if index is 0 and pageSize is 10, the command returns pages 1 to 10. If the index is 1 and the pageSize is 18, the command returns pages 2 to 19. |
| pageSize   | integer   | Number of pages of users to return.                                         |

Purpose

The `getUsers` command returns a list of users associated with the specified capability on the named route for the named community. Capabilities are
numerically indexed but only 2 is valid. Additionally, the command returns 
\textit{pageSize} entries at a time starting at \textit{index}. User operations may only be performed 
on all capabilities.

\textbf{Sample}

\begin{verbatim}
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [\$AdminControl invoke $ons getLocalCommunityName]
\$AdminControl invoke $ons getUsers "$somerouteuid 2 0 10"
\end{verbatim}

\textit{getUsersByCommunities:}

Returns a list of users by community to which they have access.

\textbf{Syntax}

\texttt{getUsersByCommunities sourceName, destName, capabilities, index, pageSize}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
</tbody>
</table>
| capabilities | integer | Numerical index for capabilities. Only 2 (all capabilities) is supported.  
- 0 returns instant messaging  
- 1 returns presence  
- 2 returns all capabilities |
| index      | integer   | Page at which to start returning pages specified by \textit{pageSize}. For example, if index is 0 and \textit{pageSize} is 10, the command returns pages 1 to 10. If the index is 1 and the \textit{pageSize} is 18, the command returns pages 2 to 19. |
| pageSize   | integer   | Number of pages of users to return. |

\textbf{Purpose}

The \texttt{getUsersByCommunities} command returns a list of users associated with the 
specified capability on the named route for the named community. Capabilities are 
numerically indexed. Additionally, the command returns \textit{pageSize} entries at a time 
starting at \textit{index}. User operations may only be performed on all capabilities.

\textbf{Sample}

\begin{verbatim}
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [\$AdminControl invoke $ons getLocalCommunityName]
\$AdminControl invoke $ons getUsersByCommunities "$local company2 0 10"
\end{verbatim}

\textit{getGroups:}

Returns a list of groups.

\textbf{Syntax}

\texttt{getGroups routeUid, capability, index, pageSize}
Parameter | Data type | Description
--- | --- | ---
routeUid | string | UID of route between the local and external community.
capability | integer | Numerical index for capabilities. Only 2 (all capabilities) is supported.
- 0 returns instant messaging
- 1 returns presence
- 2 returns all capabilities
index | integer | Page at which to start returning pages specified by pageSize. For example, if index is 0 and pageSize is 10, the command returns pages 1 to 10. If the index is 1 and the pageSize is 18, the command returns pages 2 to 19.
pageSize | integer | Number of pages of groups to return.

Purpose

The `getGroups` command returns a list of groups associated with the specified capability on the named route for the named community. Capabilities are numerically indexed. Additionally, the command returns pageSize entries at a time starting at index. Group operations may only be performed on all capabilities.

Sample

```text
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [$AdminControl invoke $ons getLocalCommunityName]
$AdminControl invoke $ons getGroups "$somerouteuid 2 0 10"
```

`getGroupsByCommunities`:

Returns a list of groups by community.

Syntax

`getGroupsByCommunities sourceName, destName, capability, index, pageSize`

Parameter | Data type | Description
--- | --- | ---
sourceName | string | Logical name of the local community.
destName | string | Logical name of the external or clearinghouse community.
capability | integer | Numerical index for capabilities. Only 2 (all capabilities) is supported.
- 0 returns instant messaging
- 1 returns presence
- 2 returns all capabilities
index | integer | Page at which to start returning pages specified by pageSize. For example, if index is 0 and pageSize is 10, the command returns pages 1 to 10. If the index is 1 and the pageSize is 18, the command returns pages 2 to 19.
pageSize | integer | Number of pages of groups to return.
Purpose

The getGroupsByCommunities command returns a list of groups associated with the specified capability on the named route for the named community. Capabilities are numerically indexed. Additionally, the command returns pageSize entries at a time starting at index. Group operations may only be performed on all capabilities.

Sample

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [$AdminControl invoke $ons getLocalCommunityName]
$AdminControl invoke $ons getGroupsByCommunities "$local company2 0 10"

addUser:

Adds a user with capabilities to a route.

Syntax

addUser routeUid, capability, username

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Name of user.</td>
</tr>
</tbody>
</table>

Purpose

The addUser command gives a user access to an external community. User operations may only be performed on all capabilities.

Sample

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons addUser "$somerouteuid 2 jsmith"

addUserByCommunities:

Adds a user so that the user can access an external community.

Syntax

addUserByCommunities sourceName, destName, capability, username

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
</tbody>
</table>
### Purpose

The `addUserByCommunities` command adds a user with specified capabilities to access the named external community. Capabilities are numerically indexed. User operations may only be performed on all capabilities.

### Sample

```plaintext
set ons [\$AdminControl completeObjectName type=RTCAadminMbean,*]
set local [\$AdminControl invoke \$ons getLocalCommunityName]
\$AdminControl invoke \$ons addUserByCommunities "\$local aol 2 jsmith"
```

### addGroup:

Adds a group to a route.

### Syntax

```plaintext
addGroup routeUid, capability, groupname
```

#### Parameter Data type Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>groupname</td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

#### Purpose

The `addGroup` command gives a group access to an external community. Group operations may only be performed on all capabilities.

#### Sample

```plaintext
set ons [\$AdminControl completeObjectName type=RTCAadminMbean,*]
\$AdminControl invoke \$ons addGroup "$somerouteuid 2 sales"
```

### addGroupByCommunities:

Adds a group so that the group can access an external community.

### Syntax
addGroupByCommunities sourceName, destName, capability, groupName

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>groupName</td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

Purpose

The addGroupByCommunities command adds a group with specified capabilities to access the named external community. Capabilities are numerically indexed. Group operations may only be performed on all capabilities.

Sample

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [$AdminControl invoke $ons getLocalCommunityName]
$AdminControl invoke $ons addGroupByCommunities "$local aol 2 sales"

removeUser:

Removes a user with capabilities from a route.

Syntax

removeUser routeUid, capability, username

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Name of user.</td>
</tr>
</tbody>
</table>

Purpose

The removeUser command stops a user's access to an external community. User operations may only be performed on all capabilities.

Sample

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons removeUser "$somerouteuid 2 jsmith"

removeUserByCommunities:
Removes a user so that the user cannot access an external or clearinghouse community.

Syntax

removeUserByCommunities sourceName, destName, capability, username

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>User name.</td>
</tr>
</tbody>
</table>

Purpose

The removeUserByCommunities command removes a user with specified capabilities and prevents them from accessing the named external community. Capabilities are numerically indexed. User operations may only be performed on all capabilities.

Sample

set ons [${AdminControl completeObjectName type=RTCAdminMbean,*}]
set local [${AdminControl invoke $ons getLocalCommunityName}]
${AdminControl invoke $ons removeUserByCommunities "$local aol 2 jsmith"

removeGroup:

Removes a group from the specified route.

Syntax

removeGroup routeUid, capability, groupname

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>groupname</td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

Purpose

The removeGroup command removes a group's access to an external community. Group operations may only be performed on all capabilities.
**RemoveGroupByCommunities**

Removes a group so that the group can no longer access the specified external community.

**Syntax**

```plaintext
removeGroupByCommunities sourceName, destName, capability, groupName
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sourceName</code></td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td><code>destName</code></td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td><code>capability</code></td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td><code>groupName</code></td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

**Purpose**

The `removeGroupByCommunities` command removes a group with specified capabilities and prevents it from accessing the named external community. Capabilities are numerically indexed. Group operations may only be performed on all capabilities.

**Sample**

```plaintext
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons removeGroup "$somerouteuid 2 sales"
```

**getNumOfUsers**

Returns the number of users that are present on a given route and capability.

**Syntax**

```plaintext
getNumOfUsers routeUID, capability
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routeUid</code></td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td><code>capability</code></td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
</tbody>
</table>

Chapter 1. Administering
Purpose

The `getNumOfUsers` command returns the number of users present on a given route and capability.

Sample

set ons [$AdminControl completeObjectName type=RTCAadminMbean,*]
$AdminControl invoke $ons getNumOfUsers "$somerouteuid 2"

`getNumOfUsersByCommunities`:

Returns the number of users that are present on a given community and capability.

Syntax

`getNumOfUsersByCommunities sourceName, destName, capability`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sourceName</code></td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td><code>destName</code></td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td><code>capability</code></td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
</tbody>
</table>

Purpose

The `getNumOfUsersByCommunities` command returns the number of users present on a given route and capability.

Sample

set ons [$AdminControl completeObjectName type=RTCAadminMbean,*]
$AdminControl invoke $ons getNumOfUsersByCommunities "$somerouteuid 2"

`getNumOfGroups`:

Returns the number of groups that are present on a given route and capability.

Syntax

`getNumOfGroups routeUID, capability`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routeUid</code></td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td><code>capability</code></td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
</tbody>
</table>
Purpose

The `getNumOfGroups` command returns the number of users present on a given route and capability.

Sample

```
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getNumOfGroups "$somerouteuid 2"
```

getNumOfGroupsByCommunities:

Returns the number of groups that are present on a given community and capability.

Syntax

```
getNumOfGroupsByCommunities sourceName, destName, capability
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sourceName</code></td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td><code>destName</code></td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
</tbody>
</table>
| `capability` | integer | Numerical index for capabilities. Only 2 (all capabilities) is supported.  
  - 0 returns instant messaging  
  - 1 returns presence  
  - 2 returns all capabilities |

Purpose

The `getNumOfGroupsByCommunities` command returns the number of groups present on a given community and capability.

Sample

```
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getNumOfGroupsByCommunities "$somerouteuid 2"
```

Script exceptions:

A script command can return two types of exceptions: java.lang.IllegalArgumentException and java.rmi.RemoteException.

IllegalArgumentException signal that your request is invalid or incorrectly formatted. In the case of invalid requests, such as removing a community by name for which no matching name can be found or adding a user to a route by community names, the exception wraps the invalid argument data. In the case that the hash-string is incorrectly formatted or cannot be parsed into the desired object, a no-arg IllegalArgumentException will be thrown. The exception java.rmi.RemoteException is used to wrap administrative run time and database exceptions.

Object attribute reference:
This topic describes the attributes available for each object type and provides the data type and whether the attribute is read, write, or both read and write.

**Community object**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>The name of the community</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>domains</td>
<td>List of domains</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>customProperties</td>
<td>Community custom properties</td>
<td>List: custom properties</td>
<td>RW</td>
</tr>
<tr>
<td>internal</td>
<td>Indicates if the community is a local (internal=true) or external (internal=false) community</td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>clearingHouse</td>
<td>Indicates if the community is a clearing house community (true)</td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>protocolConnector</td>
<td>The translation protocol used by this community</td>
<td>ProtocolConnector</td>
<td>RW</td>
</tr>
<tr>
<td>sTGWServer</td>
<td>The connections defined for the community.</td>
<td>List: STGWServer</td>
<td>R (W only on community creation)</td>
</tr>
</tbody>
</table>

**STGWServer object**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>The name of the connection</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>transport</td>
<td>The transport type for this connection. Accepted values: TCP or TLS</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name for this connection</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>port</td>
<td>The port number for this connection</td>
<td>Integer</td>
<td>RW</td>
</tr>
</tbody>
</table>

**ProtocolConnector Object**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
</tbody>
</table>
### Attribute Description Data type  Read (R) or Write (W)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of connector</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>protocol</td>
<td>The translation protocol supported by this connector. Accepted values include SIP for Sametime, SIP for legacy Sametime servers, SIP for AOL, SIP for OCS, VP, and XMPP.</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>customProperties</td>
<td>Custom properties for the translation protocol such as subscription timeout or session timeout.</td>
<td>List: customProperties</td>
<td>RW</td>
</tr>
</tbody>
</table>

### MessageHandler Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>Name of the community.</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>customProperties</td>
<td>Custom properties for the message handler.</td>
<td>List: CustomProperties</td>
<td>RW</td>
</tr>
<tr>
<td>mandatory</td>
<td>Run the message handler regardless of whether a previously run message handler completed its process or encountered an error.</td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>order</td>
<td>Specifies the order of precedence of the message handlers.</td>
<td>Integer</td>
<td>RW</td>
</tr>
<tr>
<td>type</td>
<td>The message handler type. Accepted values are: undefined, Event logger, Authorization controller, User locator, and other</td>
<td>String</td>
<td>RW</td>
</tr>
</tbody>
</table>

### Route Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>source</td>
<td>The local community.</td>
<td>Hash table</td>
<td>R</td>
</tr>
</tbody>
</table>
### Attribute Description Data type Read (R) or Write (W)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>The destination or external community.</td>
<td>Hash table</td>
<td>R</td>
</tr>
<tr>
<td>enabled</td>
<td>Indicates if the route is enabled or disabled.</td>
<td>Boolean</td>
<td>RW</td>
</tr>
</tbody>
</table>
| capabilities | Capabilities such as instant messaging and presence for the route. Only 2 is valid.  
* 0 = instant messaging  
* 1 = presence  
* 2 = both capabilities | Integer | RW |

### Access Control List (ACL) Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>users</td>
<td>The Virtual Member Manager (VMM) IDs of the users whom are on this access control list.</td>
<td>List : String</td>
<td>RW</td>
</tr>
<tr>
<td>groups</td>
<td>The VMM IDs of the groups whom are on this access control list.</td>
<td>List : String</td>
<td>RW</td>
</tr>
</tbody>
</table>

### CustomProperty Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>Name of the community.</td>
<td>String</td>
<td>R (Write only on creation.)</td>
</tr>
<tr>
<td>value</td>
<td>Value of the property.</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>description</td>
<td>Text description of the custom property</td>
<td>String</td>
<td>RW</td>
</tr>
</tbody>
</table>
Related tasks:
“Running sample Jacl scripts” on page 192
Complete these steps to run a sample Jacl script.

Related reference:
“Sample Jacl scripts”
Sametime Gateway includes several sample scripts written in Jacl (Java TCL) to
add communities to Sametime Gateway, give users access to communities, enable
logging, and set properties on message handlers.

Related information:

- Jacl reference
- Wsadmin tool

Sample Jacl scripts
Sametime Gateway includes several sample scripts written in Jacl (Java TCL) to
add communities to Sametime Gateway, give users access to communities, enable
logging, and set properties on message handlers.

Script location
The sample Jacl scripts are located in the following directory:
\stgw_server_root\samples\scripts

Jacl scripts
Jacl scripts are a non-graphical alternative that you can use to configure and
manage the Sametime Gateway. The WebSphere administrative scripting tool,
wsadmin, is a non-graphical command interpreter environment enabling you to
run administrative operations on a server in Jacl.

The scripts perform some of the functions available using the Integrated Solutions
Console. But in some cases, the scripts offer increased flexibility. For example,
when using the graphical interface to add or update an external community that
uses a SIP-based protocol, you must use TLS (Transport Layer Security) as the
transport protocol. The updateExternalCommunity script commands allows you to
use other transport protocols such as TCP or UDP.

The sample scripts include documentation inside each script. See the script and
script command reference for command details and syntax.

<table>
<thead>
<tr>
<th>Script</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>updateExternalCommunity.jacl</td>
<td>Updates the external community by changing its properties such as hostname, domains, port number, and so on.</td>
</tr>
<tr>
<td>GiveAllAcl.jacl</td>
<td>Gives all local Sametime users access to an external community.</td>
</tr>
<tr>
<td>disableAuthz.jacl</td>
<td>Disables the authorization controller message handler. The Authorization controller's main task is to allow or disallow the initiator of the message in one community to perform the requested operation with the destination user in another community.</td>
</tr>
<tr>
<td>EnableEventlogging.jacl</td>
<td>Enables content, instant message, or presence logging in the systemOut.log file.</td>
</tr>
<tr>
<td>getMsgHandlerList.jacl</td>
<td>Gets information on message handlers, including message handler names.</td>
</tr>
</tbody>
</table>
### Script Purpose

**updateMsghandler.jacl**

Configures a message handler by setting its properties.

### Related reference:

“Script commands” on page 166

Sametime Gateway provides many wsadmin script commands to help you administer and maintain the Sametime Gateway.

“Object attribute reference” on page 187

This topic describes the attributes available for each object type and provides the data type and whether the attribute is read, write, or both read and write.

### Related information:

Jacl reference

### Running sample Jacl scripts:

Complete these steps to run a sample Jacl script.

#### Procedure

1. Log in to the Sametime Gateway server machine as a user with administrative privileges.
2. If the Sametime Gateway server is not started, open a command window. If the server is started, skip to step 5.
3. In the command window, navigate to the Sametime Gateway profile directory that contains binary files: `stgw_profile_root\bin`
4. Type the following command to start Sametime Gateway. Note that `RTCGWServer` is case-sensitive.
   - **AIX, Linux, and Solaris**
     ```bash
     ./startServer.sh RTCGWServer
     ```
   - **Windows**
     ```bash
     startServer.bat RTCGWServer
     ```
   - **IBM i**
     ```bash
     startServer RTCGWServer
     ```
5. Copy the sample scripts from:
   ```bash
   stgw_server_root/samples/scripts
   ```
   to:
   ```bash
   stgw_profile_root/bin
   ```
6. Using a text editor, open the sample script to customize it for your task. The script contains documentation to guide you while editing the script.
7. Open a command window (QSH session on IBM i) and navigate to `stgw_profile_root/bin`.
8. Run the script as follows:
   ```bash
   wsadmin -username username -password password -f script_name.jacl
   ```

   Where `username` and `password` are the credentials that you created when you enabled administrative security, and `script_name.jacl` is the name of the sample Jacl script. You must run the wsadmin tool with the `-f` option. To see your
changes in the Integrated Solutions Console, you must log out of the console, and then log back into it. Some operations may require stopping and restarting the Sametime Gateway server.

Related reference:
“Script commands” on page 166
Sametime Gateway provides many wsadmin script commands to help you administer and maintain the Sametime Gateway.
“Object attribute reference” on page 187
This topic describes the attributes available for each object type and provides the data type and whether the attribute is read, write, or both read and write.

Related information:

Wsadmin tool

Administering Widgets and Live Text

Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.

Power users can create widgets and make them available to specific users. They can also create a widgets to deploy features and plug-ins to client users.

Administrators control access to a centrally managed widget catalog and widget categories using policy settings (or preferences) and standard database ACLs, as well as levels of user access to Widgets and Live Text functionality.

Note: Certain topic titles in this documentation set have been labeled Embedded ST Only, which means that their content only applies to deployments of IBM Sametime Connect that are embedded in the Notes client and not the standalone version of Sametime Connect.
Widgets and Live Text overview

Widgets and Live Text enables users to see and act on automatically recognized Live Text in any supported content like chat windows, chat history, Notes documents, and so on, using widgets created specifically for their use. For example, a user can see a specially highlighted Live Text string (for example, a flight number) and instantly act on it (for example, look up a flight status) by opening a third-party flight status widget that is linked to that Live Text. Widgets and Live Text also enables power users and administrators to create and edit widgets, and deploy them to users to engage a Notes form, view, or document or third party services such as Web page, feed, or Google Gadget as well as deploy an existing feature or plug-in from an Eclipse or NSF-based update site.

A widget is a tool that can consist of one or more components and actions. An action can optionally contain a wired content type and recognizer to define the Live Text pattern to act on and specifically how to act on that Live Text.

A widget can also be designed to provision items to client systems. For example, a widget can be used to install and update a stand-alone or third-party feature by calling a feature update site to either initially deploy or later provision updates to a client plug-in.
For Sametime embedded in Lotus Notes only: The IBM Lotus Domino server contains desktop policy settings to control Widgets and Live Text functionality, and an application template, toolbox.ntf, to provide the basis for the widget catalog.

- The Widgets desktop settings policy tab contains settings applicable to Widgets and Live Text feature access, server and catalog access, and catalog categories.
- The catalog is based on the toolbox.ntf template Widget Catalog, which is installed with and resides on a Domino server and houses all widgets. Administrators and power users create and publish widgets to the catalog. Widgets are provisioned to users automatically based on user policy and widget category name.
- Administrator can also use the Custom Settings > Managed Settings desktop settings policy tab to push a managed setting during plug-in deployment or client install easily enter managed settings in the format of pluginID/ preferenceID=preferenceValue.

The Widgets and Live Text feature is designed for three main user types -- end user, power user and application developer, and administrator. Policy and preferences control various access levels. Roles often overlap.

**Note:** Widgets and Live Text user documentation is supplied with the Lotus Notes user help.

- **Administrators** create and manage the widget catalog and assigns Widgets and Live Text access capabilities using a combination of IBM Lotus Domino server-managed policy and Eclipse preferences. Administrators can also create and configure widgets to deploy features and plug-ins to an existing IBM Lotus Notes or IBM Lotus Expeditor client install. Widgets and the widget catalog play a central role in client management in the areas of feature and plug-in deployment and provisioning for clients in the enterprise, in conjunction with Domino policy and Eclipse preferences.
- **Power users** typically create, edit, and deploy widgets for specific end users. A wizard is available to assist power users in creating new widgets and optionally wiring content types and recognizer elements to actions within those widgets. Power user and administrator user capabilities often overlap.
  Power user tasks primarily involve creating and publishing widgets and are documented in the Notes client help.
- **End users** typically act on auto-recognized Live Text in their open Notes document, or select text to act upon, and engage widgets or widget actions that have been created for them. They may also have the ability to see and add widgets to their My Widgets sidebar panel and/or their sidebar. End users may not actually see the widgets that have been created for them yet can still engage those widgets to act on their Live Text.
  End user tasks typically involve using Widgets and Live Text and are documented in the Notes client help.
Related concepts:

“Understanding Widgets and Live Text user types”
Widgets and Live Text is designed to accommodate various user types. For example, a power user or application developer will typically create and deploy widgets to end users while end users may use widgets that have been created for them, rather than create their own.

“Default Widgets and Live Text behavior” on page 198
Users can browse the widgets catalog and obtain widgets from it, and optionally add widgets to the catalog, provided their Widgets preferences point to the catalog and the catalog ACL settings enable their access.

“Catalog options and access” on page 202
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

“Administering Widgets and Live Text” on page 193
Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.

“Using public widget provider APIs” on page 230
A set of public APIs are available that developers can use to create custom widget types for use with either supplied or custom applications.

Related tasks:

“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

Understanding Widgets and Live Text user types
Widgets and Live Text is designed to accommodate various user types. For example, a power user or application developer will typically create and deploy widgets to end users while end users may use widgets that have been created for them, rather than create their own.

The general user types are administrator, power user or application developer, and end user.

Note: Widgets and Live Text user documentation is supplied with IBM Sametime Connect user help.

• Administrator
The administrator is responsible for creating the catalog application and assigning Widgets and Live Text access. Administrators control which users are designated as power users and end users. They also perform the following tasks:
  – Create and edit the catalog on a central server.
  – Control user access to the catalog using Domino desktop policy settings and ACLs.
  – Control what Widgets and Live Text functionality is available to specific users.
- Create and manage widgets in the catalog.
- Create and designate widget categories to control which widgets are available to specific users.
- Deploy features and plug-ins to client users using specially created widgets that call an Eclipse or NSF-based update site.
- Manage clients by provisioning client plug-in and policy updates using a centrally managed widget catalog. For example, the administrator can control which plug-ins, and which plug-in versions, are deployed on any given client system at any given time.
- Enable initial display of the My Widgets sidebar panel and toolbar for specific users.

• Power user and application developer

The power user or application developer is responsible for creating and managing, such as widgets designed to act on Live Text recognizers. For example, a power user could create a widget that links a zip code with a national weather Web site. By clicking on a Live Text zip code, the end user could automatically engage that widget and discover the current weather conditions in that zip code. The power user will typically perform the following tasks:

**Note:** Power users also have all the capabilities listed for the end user and may also have some or all of the capabilities listed for the administrator.
- Use a wizard to configure new Notes-based or Web-based widgets.
- Create and manage widgets in the catalog.
- Create and designate widget categories to control which widgets are available to specific users.
- Publish widgets to the catalog to make available to other users.
- Control which users have access to specific widgets based on use of widget categories.
- Configure new and edit existing widgets components and actions, content types, and recognizers.
- Create new actions, content types, and recognizers for new or existing widgets.
- Display and act on Live Text in the active document.
- Browse the catalog to obtain new widgets, content types, or recognizers.
- Wire content types and recognizers for different types of content (for example, use a Web site to map a zip code or track an airline flight number).
- Set preferences such as catalog server and application name.
- Import and export widgets.
- E-mail a widget to another user.
- Remove a widget from the My Widgets sidebar panel.
- Create a recognizer using a Java regular expression.
- Update the My Widgets sidebar panel with widgets from the catalog.

• End user

The end user uses existing and available widgets to act on Live Text in their documents based on policy and preferences settings. The end user will typically perform the following tasks:

**Note:** End users may also have some of the capabilities described for the power user.
- Act on Live Text in the current document using widgets that have been made available to them.
- Change the display of Live Text or optionally toggle that display on and off using Live Text preferences.
- Create a dashboard if multiple actions are available for a Live Text instance.
- Add a Notes view or document or Web page, feed, or Google Gadget widget.
- Add a widget when received in an XML file attachment.
- Set Widget preferences such as catalog server and application name.

Related concepts:

"Default Widgets and Live Text behavior"
Users can browse the widgets catalog and obtain widgets from it, and optionally add widgets to the catalog, provided their Widgets preferences point to the catalog and the catalog ACL settings enable their access.

"Widgets and Live Text overview" on page 194
Widgets and Live Text enables users to see and act on automatically recognized Live Text in any supported content like chat windows, chat history, Notes documents, and so on, using widgets created specifically for their use. For example, a user can see a specially highlighted Live Text string (for example, a flight number) and instantly act on it (for example, look up a flight status) by opening a third-party flight status widget that is linked to that Live Text. Widgets and Live Text also enables power users and administrators to create and edit widgets, and deploy them to users to engage a Notes form, view, or document or third party services such as Web page, feed, or Google Gadget as well as deploy an existing feature or plug-in from an Eclipse or NSF-based update site.

"Administering Widgets and Live Text" on page 193
Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.

Related tasks:

"Deploying client plug-ins with widgets and the widget catalog" on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

**Default Widgets and Live Text behavior**
Users can browse the widgets catalog and obtain widgets from it, and optionally add widgets to the catalog, provided their Widgets preferences point to the catalog and the catalog ACL settings enable their access.

For the stand-alone version of IBM Sametime, both Widgets are Live Text are initially disabled, including the preferences panels, which are hidden. To enable them, the Sametime administrator must enable this preference using either managed preferences or the plugin_customization.ini file as follows:

```ini
com.ibm.collaboration.realtime/enableSametimeLiveText=true
```

For the version of IBM Sametime embedded in Lotus Notes, users will not see the My Widgets panel by default; however, they can display it by clicking File > Preferences > Widget and enabling the Show Widget Toolbar and the My Widgets Sidebar panel option, which is disabled by default. Enabling the Show Widget Toolbar and the My Widgets Sidebar panel option allows for full Widgets
and Live Text access. The My Widgets sidebar panel and the Widgets menus and toolbar will be visible and the user can create and publish widget components, actions, content types, and recognizers. However, the administrator can use IBM Lotus Domino policy or Eclipse preferences to control user access to various aspects of Widgets and Live Text functionality, often based on end user or power user type.

Before installing IBM Sametime, the administrator can change the default behavior specified above using Domino policy or the install kit’s plugin_customization.ini file. These settings can also be changed after install using Domino policy or the installed plugin_customization.ini (for example, install dir\framework\rcp\plugin_customization.ini).

If no Domino policy or plugin_customization.ini file Eclipse preferences are specified, all Widgets and Live Text functionality is available.

Whether the user can see the My Widgets panel and toolbar or not, she can see and act on Live Text.

**Default policy and preferences**

By default, the following conditions exist when no policy or preferences changes have been made:

- The Catalog server preference is blank.
- The Catalog name preference is toolbox.nsf.
- The Categories to install preference is blank.
- The Show Widget Toolbar and the My Widgets Sidebar panel preference is available but unchecked (Notes only).

If the option is checked, the following default settings are set and their associated behaviors are available.

- The Create and manage an action setting is enabled.
- The Create and manage recognizers and content types setting is enabled.
- The Send widgets using e-mail setting is enabled.
- The Install widgets from e-mail or other setting is enabled.
- The Publish to catalog setting is enabled.
- The Enable default recognizers (these are the supplied advanced recognizers of People (names), Address, and Organization) setting is enabled.
Related concepts:

“Widgets and Live Text overview” on page 194
Widgets and Live Text enables users to see and act on automatically recognized Live Text in any supported content like chat windows, chat history, Notes documents, and so on, using widgets created specifically for their use. For example, a user can see a specially highlighted Live Text string (for example, a flight number) and instantly act on it (for example, look up a flight status) by opening a third-party flight status widget that is linked to that Live Text. Widgets and Live Text also enables power users and administrators to create and edit widgets, and deploy them to users to engage a Notes form, view, or document or third party services such as Web page, feed, or Google Gadget as well as deploy an existing feature or plug-in from an Eclipse or NSF-based update site.

“Controlling Widgets and Live Text access using Eclipse preferences” on page 209
Access to Widgets and Live Text functionality and the widgets catalog is set using Eclipse preferences in the plugin_customization.ini file or managed preferences. This is applicable to Sametime standalone environments where Domino policy is not used.

“Administering Widgets and Live Text” on page 193
Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.

Related tasks:

“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

Creating the widget catalog

The widgets catalog centrally houses available widgets.

About this task

Administrators and power users can use the supplied catalog template to create a widgets catalog on a server.

Procedure

1. Obtain the widget catalog template (toolbox.ntf).
   The template is installed with the IBM Lotus Domino server.
2. Create the widget catalog, for example named toolbox.nsf, using the supplied toolbox.ntf template.
3. Assign ACLs to control access rights to the catalog application for administrators, power users, and end users.
   Administrators and power users need read and write access to the catalog.
   Administrators must be granted the [Admins] role in the catalog Access Control List (ACL). Administrators also need one of the following access rights to the catalog:
   • Manager
   • Designer
   • Editor
End users may not be set up to browse and access the catalog directly but rather to obtain widget actions automatically by way of their membership in specific widget categories. End users, if they are not allowed to create and configure widgets, need Reader access to the catalog; otherwise it is recommended that end users are granted Author access to the catalog.

4. Once you have created the catalog, optionally create an initial set of categories for the catalog.

There are two types of predefined categories in the catalog - administrator categories and categories. Both of these categories are defined in the Administration/Keyword view. Administrator categories are named "ADMIN-Categories", while the other categories keyword is named "Categories".

**Note:** You can assign policies or preferences to designate user access to the catalog.

5. Enable the Toolbox Sweeper agent, which is a scheduled agent set to run against new and modified documents. This agent ensures that Widget documents are properly created and populated; if a problem is found the offending document is removed from the user views, is placed in the Administration/Document Queue, and an e-mail is sent to the document author informing him of the problem. Enable the Sweeper agent by selecting **View > Agents**, highlighting the Toolbox Sweeper agent, and then clicking **Enable**. You will be prompted to choose which server to run the agent on; choose the server where you have deployed the catalog.
Related concepts:
“Widgets and Live Text overview” on page 194
Widgets and Live Text enables users to see and act on automatically recognized Live Text in any supported content like chat windows, chat history, Notes documents, and so on, using widgets created specifically for their use. For example, a user can see a specially highlighted Live Text string (for example, a flight number) and instantly act on it (for example, look up a flight status) by opening a third-party flight status widget that is linked to that Live Text. Widgets and Live Text also enables power users and administrators to create and edit widgets, and deploy them to users to engage a Notes form, view, or document or third party services such as Web page, feed, or Google Gadget as well as deploy an existing feature or plug-in from an Eclipse or NSF-based update site.

“Catalog options and access”
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

Related tasks:
“Creating a features and plugins deployment widget” on page 217
You can create a widget to assist in managing new feature deployment and update provisioning on the client based on policy or preferences.

Catalog options and access
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

Power users can configure new widgets and publish them to the catalog for user access. Users obtain the latest widgets from the catalog on a scheduled basis. Depending on how users are configured they can browse the catalog for new widgets and update the widgets in their local catalog replica on demand.

The widgets catalog does not contain Lotus-supplied components. However, it does contain some advanced recognizers, and their content types, such as the following:
- Person (name)
- Place (address)
- Organization

Note: These supplied, advanced Live Text recognizers are currently available for American English-only and some German names. You can create your own Live Text recognizers using Java™ regular expressions.
The widgets that a user would see in their sidebar, and actions that are available to users based on category provisioning from the catalog, are stored in the local replica of the central catalog application.

**Catalog documents**

Each widget is represented in the catalog as a Notes document containing the following elements.

- **Widget graphic for display in the catalog document**
  Note: You can use the default graphic or specify another for display in the catalog document. However, the graphic you specify for the catalog document has no effect on the widget thumbnail used in the My Widgets sidebar panel. The widget thumbnail is specified in the .XML file attachment using the "imageUrl" variable.

- **Title, Description, and Detail**
  Use the default widget name or specify a different catalog document title. Use the Description and Details fields to describe the widget.

- **Category**
  Control user access to the widget based on widget category grouping such as team name or job. This is the how you specify which users have access to which widgets. Users whose "category" policy or preference allows them access to widgets of a specific category name will be provisioned with those widgets automatically. Type Optionally specify the widget type(s) -- for example content type only, recognizer only, component, feature or plug-in, or any combination.

  **Note:** Content types and recognizers do not need to be bundled with a component to be added to the catalog.

- **XML extension attachment**
  This contains the widget XML itself, which informs the client what to do when the widget is provisioned to the user, for example deploy a plug-in from a named update site or install a gadget.

**Catalog views**

The catalog is supplied with the following views:

- All Widgets
- By Author
- By Category

**Catalog access rights**

The administrator can assign catalog access right based on user type, using a combination of Notes application ACLs and policy or preference settings.

- **Using catalog application ACLs**
  Users with read and write access to the catalog can create, edit, and remove components, content types, and recognizers in the catalog. They can change or add widget categories to catalog documents which, in use with policies or preference, can force deployment to specific users or groups. They can also create, edit, or remove widgets and can publish new widgets to the catalog from the My Widgets sidebar panel.

  **Note:** A user with Editor access or above to the catalog and assigned the Administrator role can create, edit, and remove widgets, content types, and
recognizers in the catalog. A user with Author or Editor access to the catalog can view and use components, content types and/or recognizers and can also create new widget documents in the catalog.

Note: If you are assigned the Administrator role in the catalog ACL and are not provided with the Administrator features in your local replica, you may need to enable "Enforce consistent access across replicas" in the ACL of your local replica.

Using policy or PLUGIN_CUSTOMIZATION.INI file preferences

The administrator can control a variety of Widgets and Live Text and catalog access setting using policy. If using Widgets and Live Text outside of a server-managed environment, there are equivalent settings in the PLUGIN_CUSTOMIZATION.INI file. For example, an administrator can control widget deployment based on categories. Categories are created in the catalog, but are administered by way of user policy or preference settings. Specific widgets can be deployed to specific users based on the category in which a given widget resides and the categories for which a given user is assigned.

Catalog action buttons

The catalog contains the following action buttons:

• Open
  This allows you to open and view the selected catalog document for the purposes of viewing and optionally adding it to the My Widgets sidebar panel. Provided you have edit rights to that document, you can also open it for edit.

• Add Widget to Catalog
  Use this to add a widget, content type, or recognizer to the catalog. This action opens a dialog in which you can attach your .XML file and add a title, category name (optional), type designation, short description, and detailed description.

  Note: To automatically create a new document in the catalog for a specific widget in the My Widgets panel, if policies or preferences allow you to do so, you can right-click the widget in the My Widgets panel and select Publish to Catalog.

Embedded ST Only: Controlling Widgets and Live Text access using Domino policy

You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.

The "Default Widgets and Live Text behavior" topic describes Widgets and Live Text behavior when no policy or preference changes have been made.

Note: If you are not using a server-managed environment, you can use the plugin_customization.ini file either before or after install to control user access to Widgets and Live Text functionality. You can also use the Widgets preferences panel to set the catalog server, catalog name, and categories to install values, as well as the Show Widgets Toolbar and the My Widgets Sidebar panel preference. Policy settings take precedence over Eclipse preferences.

Note that some policy settings contain a "How to apply this setting" column, which you can use to establish one of the following conditions for that setting.

• Don’t set value
The value set is not applied to the client's Widgets preferences panel. The user can specify a preference value and this policy setting will not overwrite that value.

- **Set initial value**
  The value is applied once to the client but the user can change the setting on the Widgets or Live Text preferences panel. If the administrator changes the policy value later, the user's setting is not overwritten.

- **Set value whenever modified**
  The value is applied to the client and is reapplied (overwriting a user-set change) whenever the policy setting is modified.

- **Set value and prevent changes**
  The value is applied to the client and the preference is then disabled on the Widgets or Live Text preferences panel, such that the user cannot change the value.

Note: For related Domino policies tips and best practices, search the Lotus Notes and Domino wiki.

The Domino policy settings available on the Widgets tab of the desktop policy settings document are as below.

- **Widget catalog server**
  Specify the catalog server from which to provision at application startup and periodically during replication from the catalog to the user's local replica (by default, replication occurs on whatever schedule is set for Normal priority applications). Use server/domain format or a fully qualified name. If you use a server/domain format, server failover is supported.
  If this policy's "How to apply this setting" column is set to "Set value and prevent changes", users will not be able to change the value on the Widgets preferences panel.
  By default, this value is not set.

- **Widget catalog application name**
  Specify the Widget catalog application name, for example toolbox.nsf, on the catalog server, from which to provision at client application startup and periodically during replication from the catalog to the user's local replica (by default, replication occurs on whatever schedule is set for Normal priority applications). Use the Widget Catalog template (toolbox.ntf) to create the catalog application.
  If this policy’s *How to apply this setting* column is set to *Set value and prevent changes*, the end user will not be able to change the value on the Widgets preferences panel.
  The default catalog name is toolbox.nsf.

- **Widget catalog categories to install**
  Specify the widget categories to install and update for this user. These categories will appear in the **Categories to install** list box on the Widgets preferences panel. Use this setting to limit user access to specific widget categories. If this field is blank, no widgets are installed in the user’s My Widgets sidebar panel. Categories typically equate to a user grouping, such as a specific project team or job type.
  The categories listed in this policy cause the equivalent category names in the Widgets preferences panel to be selected and disabled; the end user cannot deselect them.
By default, this value is not set.

- Enable Live Text
  Specify if auto-recognized Live Text appears as dash-underlined text in the user's Notes document. Live Text display can be toggled on and off when working in a session.
  If this setting is disabled, then the Live Text preference panel is hidden from the user.
  By default, this setting is enabled.

- Enable Default Recognizers
  Specify if the Lotus-supplied, advanced Live Text recognizers such as person (name), place (address), and organization are enabled.
  If this setting is disabled, then the user cannot enable it.
  By default, this setting is enabled.

- Show the My Widgets panel in the sidebar
  Specify if the My Widgets sidebar panel is visible in the Notes sidebar and if the Widgets menus and toolbar are visible.
  If this setting is enabled and its How to apply this setting column is set to Set value and prevent changes, the end user will not be able to change the 'Show Widgets Toolbar and the My Widgets Sidebar panel' value on the Widgets preferences panel.
  If this setting is disabled and its 'How to apply this setting' column is set to 'Set value and prevent changes', the Widgets preferences panel will not be visible to the end user.
  By default, this setting is disabled.

- Restrict the addition of widgets to specific types
  Restrict creation and edit of widgets to certain types (referred to as provider IDs).
  The Widgets and Live Text feature includes an extension point for widget providers. The supplied providers include Notes view, Feeds, Web page or service, and Google Gadget.
  If this setting is disabled, the user can create or edit widgets with no restriction on type.
  If this setting is enabled, the user can only create or edit widgets of a certain type. The administrator can then specify which widget types (provider IDs) are available using the setting below.
  By default, this setting is disabled.

- Enable provider IDs for widget addition
  Specify the widget types available for creation and edit. Use a comma to separate types in the list. The available widget type/Provider ID entries include the following and correlate to the available widget types.
  com.ibm.notes.toolbox.provider.NotesViewPaletteProvider
  com.ibm.notes.toolbox.provider.NotesFormPaletteProvider
  com.ibm.rcp.toolbox.web.provider.WebServicesPaletteProvider
  com.ibm.rcp.toolbox.feeds.FeedPaletteProvider
  com.ibm.rcp.toolbox.google.provider.internal.GooglePaletteProvider
  com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning
  com.ibm.rcp.toolbox.search.provider.SearchPaletteProvider
  The default is as below:
For example, if the policy setting **Restrict the addition of widgets to specific types** is set to "Enabled" and "Enable provider IDs for widget addition" is set to the value below, the user could only create Google Gadget widget types:

```
com.ibm.rcp.toolbox.google.provider.internal.GooglePalleteProvider
```

- **Restrict provider IDs for installation/execution**

Restrict installation and update of widgets to specific types (referred to as provider IDs). If enabled, the administrator can then specify which widget types (provider IDs) are available using the setting below. Note that if you restrict what widget types are available for installation, you should also restrict creation of those same widget types using the **Restrict the addition of widgets to specific types** and **Enable provider IDs for widget addition** policies.

By default, this setting is disabled.

- **Enable provider IDs for installation/execution (only applicable if field above is enabled)**

Specify the widget types available for install and update. Use a comma to separate types in the list.

The available widget type/Provider ID entries include the following and correlate to the available widget types.

```
com.ibm.notes.toolbox.provider.NotesViewPalleteProvider
com.ibm.notes.toolbox.provider.NotesFormPalleteProvider
com.ibm.rcp.toolbox.web.provider.WebServicesPalleteProvider
com.ibm.rcp.toolbox.feeds.FeedPalleteProvider
com.ibm.rcp.toolbox.google.provider.internal.GooglePalleteProvider
com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning
com.ibm.rcp.toolbox.search.provider.SearchPalleteProvider
```

The default is as below:

```
```

For example, if the policy setting "Restrict provider IDs for installation/execution" is set to "Enabled" and "Enable provider IDs for installation/execution" is set to the value below, the user could only install or provision Google Gadget widget types:

```
com.ibm.rcp.toolbox.google.provider.internal.GooglePalleteProvider
```

- **Restrict extension point IDs for installation/execution**

Restrict installation of widgets that contain certain extension points. If enabled, the administrator can then specify which extension point IDs are allowed using the setting below.

**Note:** Extension points are an Eclipse feature. They define new function points for the platform that other plug-ins can plug into. Eclipse provides many extension points with the core platform. The Widgets and Live Text feature also provides some extension points.

The Eclipse platform provides the following identifiers, and many others:

```
org.eclipse.ui.popupMenus, org.eclipse.ui.viewActions, org.eclipse.ui.views identifiers
```

Notes and Expeditor provide the following identifiers, and many others:

```
```

By default, this setting is disabled.

- **Enable extension point IDs for installation/execution (only applicable if field above is enabled)**

You can restrict this list or add to it. Use a comma to separate items in the list.

The default is as below:
For example, if the policy setting **Restrict extension point IDs for installation/execution** is enabled and **Enable extension point IDs for installation/execution** is set to "com.ibm.rcp.content.contentTypes", then widgets containing regular expression recognizers (com.ibm.rcp.annotation.regex.regexTypes) would not be allowed to be installed/provisioned.

- Create and manage an action
  Specify whether the user can create, edit, and remove actions while working in the My Widgets panel and the Widget Management view.
  By default, this option is enabled.

- Create and manage recognizers and content types
  Specify whether the user can create, edit, and remove recognizers and content types while working in the My Widgets panel. If enabled, the user can create, remove, or edit recognizers and content types and can use the **Manage Widgets, Content, and Recognizers** My Widgets option. This also enables display of the **Recognize All Content** option in the My Widgets menu and the "Display type properties" action when right-clicking on a content type in a Notes document.
  By default, this setting is enabled.

- Send widgets using e-mail
  Specify whether the user can send widgets to others as XML extension attachments using the "E-mail to" action and also whether the user can output an XML file containing selected widgets from the My Widgets panel using the **Export** option.
  By default, this setting is enabled.

- Install widgets from e-mail or other
  Specify whether a user can install widgets using an XML extension file obtained from e-mail or from the user's file system. If enabled, the user can use drag and drop to install widgets from e-mail (or any document that contains an attached extension.xml file, not including the configured catalog) or an import action from the user's file system.
  By default, this setting is enabled.

- Install widgets from catalog
  Specify whether a user can browse the configured catalog and select widgets to install to the My Widgets panel or sidebar. If enabled, the user can select a widget from the catalog and drag and drop the widget's XML extension attachment to their My Widgets sidebar panel. They can also select additional categories to be provisioned with (in addition to those listed in the **Widget catalog categories to install** policy) using their Widgets preferences panel.
  By default, this setting is enabled.

- Publish to catalog so others can browse (subject to catalog ACLs)
  Grant access to the user, typically the power user or application developer user, to publish widgets from their My Widgets panel to the catalog for use by others. Note that this option applies to widgets, content types, and recognizers.
  When you publish a widget to the catalog, you should assign widget categories to it.
  By default, this setting is enabled.
Related concepts:
“Default Widgets and Live Text behavior” on page 198
Users can browse the widgets catalog and obtain widgets from it, and optionally
add widgets to the catalog, provided their Widgets preferences point to the catalog
and the catalog ACL settings enable their access.

“Widgets and Live Text overview” on page 194
Widgets and Live Text enables users to see and act on automatically recognized
Live Text in any supported content like chat windows, chat history, Notes
documents, and so on, using widgets created specifically for their use. For
example, a user can see a specially highlighted Live Text string (for example, a
flight number) and instantly act on it (for example, look up a flight status) by
opening a third-party flight status widget that is linked to that Live Text. Widgets
and Live Text also enables power users and administrators to create and edit
widgets, and deploy them to users to engage a Notes form, view, or document or
third party services such as Web page, feed, or Google Gadget as well as deploy an
existing feature or plug-in from an Eclipse or NSF-based update site.

“Understanding Widgets and Live Text user types” on page 196
Widgets and Live Text is designed to accommodate various user types. For
example, a power user or application developer will typically create and deploy
widgets to end users while end users may use widgets that have been created for
them, rather than create their own.

“Controlling Widgets and Live Text access using Eclipse preferences”
Access to Widgets and Live Text functionality and the widgets catalog is set using
Eclipse preferences in the plugin_customization.ini file or managed preferences.
This is applicable to Sametime standalone environments where Domino policy is
not used.

“Using public widget provider APIs” on page 230
A set of public APIs are available that developers can use to create custom widget
types for use with either supplied or custom applications.

Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an
existing IBM Lotus Notes client using a combination of the widgets catalog, an
NSF-based update site in which the feature resides, an XML file attached to the
widget that calls the feature’s update site, and Domino policy or Eclipse
preferences.

Controlling Widgets and Live Text access using Eclipse preferences
Access to Widgets and Live Text functionality and the widgets catalog is set using
Eclipse preferences in the plugin_customization.ini file or managed preferences.
This is applicable to Sametime standalone environments where Domino policy is
not used.

If a setting resides in both the Domino policy (when IBM Sametime is embedded
in the Lotus Notes client ) and the plugin_customization.ini file, the Domino policy
value takes precedence. As well, if a setting is changed using the Widgets
preferences panel, that setting takes precedence for the duration of the active
session.
The following list corresponds to either a policy name from the Widgets desktop policy settings document in the Domino Administrator or a preference from the Widgets preferences panel with an equivalent Eclipse preference in the plugin_customization.ini file.

Note: The default plugin_customization.ini file is provided in the Notes install kit in the deploy subdirectory. The file path of the installed plugin_customization.ini file is `install_dir\framework\rcp\ plugin_customization.ini`.

The "Default Widgets and Live Text behavior" topic describes how Widgets and Live Text appears to the user when no policy or preference changes are made.

Note: If the following four parameters are set in the plugin_customization.ini file, the local catalog replica is created from the specified catalog shortly after client application startup.

- **Catalog server**
  This setting specifies the catalog server from which to provision at client application startup and periodically during replication from the catalog to the user's local replica (by default, replication occurs on whatever schedule is set for Normal priority applications).
  com.ibm.rcp.toolbox.admin/toolboxCatalogServer
  Example:
  com.ibm.rcp.toolbox.admin/toolboxCatalogServer=server_name.myserver.mycompany.com

  Note: Using this setting does not prevent the user from changing the catalog server name in the Widgets preferences panel. This corresponds to the **Widget catalog server** policy and the **Catalog server** preference on the Widgets preferences panel.
  The preference default is blank.

- **Catalog name** (Sametime embedded in Lotus Notes only)
  This setting specifies the catalog application name, on the catalog server, from which to provision at client application startup and periodically during replication from the catalog to the user's local replica. The catalog is created using the Domino server-supplied Widget Catalog template (toolbox.ntf).
  com.ibm.rcp.toolbox.admin/toolboxCatalogDBName=name.nsf
  Example:
  com.ibm.rcp.toolbox.admin/toolboxCatalogDBName=toolbox.nsf
  Using this setting does not prevent the user from changing the catalog name in the Widgets preferences panel. This corresponds to the **Widget catalog application name** policy and the **Catalog name** preference on the Widgets preferences panel.
  The preference default is blank.

- **Local catalog replica name** (Sametime embedded in Lotus Notes only)
  This setting specifies the local replica catalog name and enables creation of the required local catalog replica on the user's client system. The name specified should match that of the catalog application on the server, for example toolbox.ntf. The Widgets and Live Text functionality requires the local catalog replica.
  com.ibm.rcp.toolbox.admin/toolboxCatalogLocalDBName=name.nsf
  Example:
  com.ibm.rcp.toolbox.admin/toolboxCatalogLocalDBName=toolbox.nsf
Note: If you are using a catalog and are not using Domino policy, you must specify a local catalog replica name using the setting.

Note: There is no corresponding setting in the Widgets desktop policy settings document and there is no setting on the Widgets preferences panel that allows the user to control this value.

The preference default is blank.

- Widget categories to install
  This setting enables you to list the widget categories from which to provision at client application startup and periodically during replication from the catalog to the user's local replica (by default, replication occurs on whatever schedule is set for Normal priority applications).

  com.ibm.rcp.toolbox.admin/catalogCategoriesToInstall
  Example:
  com.ibm.rcp.toolbox.admin/catalogCategoriesToInstall=ABXID,Team1

Note: Using this setting does not prevent the user from adding or removing categories in the Widgets preferences panel. This corresponds to the Widget catalog categories to install policy and the Categories to install preference on the Widgets preferences panel.

The preference default is blank, meaning no categories are selected in the Widgets preferences panel.

Additional preferences can be specified using the following settings.

- Show Widget Toolbar and the My Widgets Sidebar panel (Notes only)
  This setting specifies whether the Show Widget Toolbar and the My Widgets Sidebar Panel preference is enabled by default. The preference default is false, such that the option is not checked on the Widgets preferences panel. If the user enables Show Widget Toolbar and the My Widgets Sidebar panel on the Widgets preferences panel, she can see the three Widgets toolbar buttons, the Tools - Widgets menu options, and the My Widgets sidebar panel.

  com.ibm.rcp.toolbox.admin/toolboxvisibleChild
  Options are =true and =false.
  The preference default is true, but you will see that in your installer's plugin_customization.ini file, this preference is already set as below:
  com.ibm.rcp.toolbox.admin/toolboxvisibleChild=false

- Enable the display of Live Text in supported windows like chat windows, chat history, Notes documents, and so on.
  This corresponds to the Enable Live Text policy setting.
  If this setting is disabled, then the Live Text preference panel is hidden from the user. Live Text and Widgets are disabled by default in the stand-alone version of Sametime but can be enabled using plugin_customization.ini or managed preferences using this preference com.ibm.collaboration.realtime/enableSametimeLiveText=true.

  com.ibm.rcp.toolbox.admin/toolboxenableRecognizers
  Options are =true and =false. The preference default is true.

- Enable Default Recognizers
  Specify if the Lotus-supplied, advanced Live Text recognizers such as person (name), place (address), and organization are enabled.
  If this setting is disabled, then the user cannot enable it.
  This corresponds to the Enable Default Recognizers policy setting.
Restrict widget creation and edit to specific types (provider IDs)
Restrict creation and edit of widgets to certain types (referred to as provider IDs). This corresponds to the **Restrict the addition of widgets to specific types** policy setting.
The Widgets and Live Text feature includes an extension point for widget providers. The supplied providers include Notes view, Feeds, Web page or service, and Google Gadget.
If this setting is disabled, the user can create or edit widgets with no restriction on type.
If this setting is enabled, the user can only create or edit widgets of a certain type. The administrator can then specify which widget types (provider IDs) are available using the setting below.

```
com.ibm.rcp.toolbox.admin/toolboxEnableDefaultRecognizers
Options are =true and =false. The preference default is true.
```

```
com.ibm.rcp.toolbox.admin/createTool
Options are =true and =false. The preference default is false.
```
If enabled you can then specify which widget types (provider IDs) are available for creation or edit using the setting below, which corresponds to the **Enable provider IDs for widget addition** policy setting.

```
com.ibm.rcp.toolbox.admin/createToolProviderIDs
```
Specify the widget types available for creation and edit. Use a comma to separate types in the list. The available widget type/Provider ID entries include the following and correlate to the available widget types.

```
com.ibm.notes.toolbox.provider.NotesViewPalleteProvider
com.ibm.notes.toolbox.provider.NotesFormPalleteProvider
com.ibm.rcp.toolbox.web.provider.WebServicesPalleteProvider
com.ibm.rcp.toolbox.feeds.FeedPalleteProvider
com.ibm.rcp.toolbox.google.provider.internal.GooglePalleteProvider
com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning
com.ibm.rcp.toolbox.search.provider.SearchPalleteProvider
```
The default is as below:
```
```
For example, if the setting is as below, the user could only create Google Gadget widget types:
```
com.ibm.rcp.toolbox.google.provider.internal.GooglePalleteProvider
```

Restrict the installation of widgets to specific widget types (provider IDs)
Restrict installation and update of widgets to specific types (referred to as provider IDs). This corresponds to the **Restrict provider IDs for installation/execution** policy.
Options are =true and =false. The preference default is false.
If enabled, the administrator can then specify the widget types (provider IDs) available for install and update using the setting below, which corresponds to the **Enable provider IDs for installation/execution** policy. Use a comma to separate types in the list.

```
com.ibm.rcp.toolbox.admin/toolboxinstallProviderIDs
```
The available widget type/Provider ID entries include the following and correlate to the available widget types.
```
com.ibm.notes.toolbox.provider.NotesViewPalleteProvider
com.ibm.notes.toolbox.provider.NotesFormPalleteProvider
com.ibm.rcp.toolbox.web.provider.WebServicesPalleteProvider
```
com.ibm.rcp.toolbox.feeds.FeedPaletteProvider
com.ibm.rcp.toolbox.google.provider.internal.GooglePaletteProvider
com.ibm.rcp.toolbox.pub.provider.ToolboxProvisioning
com.ibm.rcp.toolbox.search.provider.SearchPaletteProvider

The default is as below:

For example, if the setting is as below, the user could only install or provision Google Gadget widget types:
com.ibm.rcp.toolbox.google.provider.internal.GooglePaletteProvider

For example, to restrict the user such that they can only install Notes view-type widgets (from a non-catalog source), add the following entries:
com.ibm.rcp.toolbox.admin/toolboxrestrictProviderIDs
com.ibm.rcp.toolbox.admin/toolboxinstallProviderIDs
com.ibm.notes.toolbox.provider.NotesViewPaletteProvider

- Enable create, remove, and edit actions

Specify whether the user can create, edit, and remove actions while working in the My Widgets panel and the Widget Management view. This corresponds to the **Create and manage an action** policy setting. If enabled, the user can perform those tasks.
com.ibm.rcp.toolbox.admin/toolboxcreateAction
Options are =true and =false. The preference default is true.

- Enable create, remove, or edit recognizers and content types and can use the "Manage Actions, Content, and Recognizers" option

Specify whether the user can create, edit, and remove recognizers and content types while working in the My Widgets panel. If enabled, the user can create, remove, or edit recognizers and content types and can use the **Manage Widgets, Content, and Recognizers** option. This also enables display of the **Recognize All Content** option in the My Widgets menu and the "Display type properties" action when right-clicking on a content type in a document. This corresponds to the **Create and manage recognizers and content types** policy setting.
This also enables display of the "Recognize all Content" in the My Widgets options menu and the "Display type properties" action when right-clicking in a document.
com.ibm.rcp.toolbox.admin/toolboxcreateRecognizer
Options are =true and =false. The preference default is true.

- Enable the ability to send widgets using email

Specify whether the user can send widgets to others and output an XML file containing selected widgets from the My Widgets panel. This corresponds to the **Send widgets using email** policy setting.
If enabled, the user can send widgets to others as XML extension attachments using the "Email to" action and also output an XML extension containing selected widgets in the My Widgets panel using the "Export" menu option.
com.ibm.rcp.toolbox.admin/toolboxsendAsEmail
Options are =true and =false. The preference default is true.

- Enable the ability to install widgets from email or other non-catalog means

Specify whether a user can install widgets using an XML extension file obtained from email or from the user's file system. If enabled, the user can use drag and drop to install widgets from email (or any document that contains an attached
extension.xml file, not including the configured catalog) or an import action from the user's file system. This corresponds to the **Install widgets from email or other** policy setting.

If enabled, the user can drag and drop to add widgets from email (or any document that contains an attached extension.xml file, not including the catalog) or use the **Import** menu option.

**com.ibm.rcp.toolbox.admin/toolboxinstallFromOther**

Options are =true and =false. The preference default is true.

- **Enable the ability to install widgets from the catalog and to browse the catalog from the My Widgets panel**
  Specify whether a user can browse the configured catalog and select widgets to install to the My Widgets panel or sidebar. This corresponds to the **Install widgets from catalog** policy setting.

  If enabled, the user can select a widget from the catalog and drag and drop the widget's XML extension attachment to their My Widgets panel. They can also select additional categories to be provisioned with (in addition to those listed in the **Widget catalog categories to install** policy) using their Widgets preferences panel.

  **com.ibm.rcp.toolbox.admin/toolboxinstallFromCatalog**

  Options are =true and =false. The preference default is true.

- **Enable ability to publish widgets from the My Widgets panel to the catalog**
  Grant access to the user, typically the power user or application developer user, to publish widgets from their My Widgets panel to the catalog for use by others. This corresponds to the **Publish to catalog so others can browse** policy setting.

  You must have edit rights to the catalog to publish to it.

  **com.ibm.rcp.toolbox.admin/toolboxpublishToCatalog**

  Options are =true and =false. The preference default is true. Restrict installation to specific extension point types

  Restrict installation of widgets that contain certain extension points. This corresponds to the **Restrict extension point IDs for installation/execution** policy setting.

  **com.ibm.rcp.toolbox.admin/toolboxspecifyExtPtIDs**

  Options are =true and =false. The preference default is false.

**Note:** Extension points are an Eclipse feature. They define new function points for the platform that other plug-ins can plug into. Eclipse provides many extension points with the core platform. The Widgets and Live Text feature also provides some extension points. For example:

The Eclipse platform provides the following identifiers, and many others:

org.eclipse.ui.popupMenus, org.eclipse.ui.viewActions, org.eclipse.ui.views identifiers

Notes and Expeditor provide the following identifiers, and many others:


If "toolboxspecifyExtPtIDs" is set to true, the administrator can then specify which extension point IDs are allowed using an additional entry in the INI file.

**com.ibm.rcp.toolbox.admin/toolboxdynamicExtPtIDs**

This corresponds to the **Enable extension point IDs for installation/execution** policy setting.

By default, this setting is disabled.
The default is as below:

```
```

For example, the following settings specify that widgets containing regular expression recognizers cannot be installed or provisioned:

```
com.ibm.rcp.toolbox.admin/specifyExtPtIDs=com.ibm.rcp.content.contentTypes,com.ibm.rcp.annotation.regex.regexTypes
```

**Related concepts:**

- “Default Widgets and Live Text behavior” on page 198
- Users can browse the widgets catalog and obtain widgets from it, and optionally add widgets to the catalog, provided their Widgets preferences point to the catalog and the catalog ACL settings enable their access.

- “Understanding Widgets and Live Text user types” on page 196
- Widgets and Live Text is designed to accommodate various user types. For example, a power user or application developer will typically create and deploy widgets to end users while end users may use widgets that have been created for them, rather than create their own.

- “Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
- You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.

- “Using public widget provider APIs” on page 230
- A set of public APIs are available that developers can use to create custom widget types for use with either supplied or custom applications.

**Related tasks:**

- “Deploying client plug-ins with widgets and the widget catalog” on page 217
- You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature’s update site, and Domino policy or Eclipse preferences.

**How do I create a Features and Plugins deployment widget?**

You can create a widget for deploying features and plug-ins to client users.

**About this task**

This option guides you through the process of creating a feature and plug-in deployment widget for pushing new and updated features and plug-ins to client users – a process documented in the “Deploying client plug-ins with widgets and the widget catalog” section of Sametime help. The wizard guides you through the widget definition process, prompting for the update site where the target plug-in resides. After specifying the plug-in, entering the name, image url, and description for the widget, the wizard creates the widget’s install manifest content, saves the new widget, and installs the specified plug-in. You can then export or publish the widget.

For widgets samples, see the public catalog and the Lotus Notes and Domino wiki.

This procedure is designed for application developers, power users, and administrators.

**Note:** This process assumes that you already have created and signed the feature’s update site contents and that you have a properly configured site.xml file.
Note: You cannot create a provisioning widget using the Configure a widget from the current context wizard.

Note: Use of this wizard is controlled by the managed preference settings used to enable creation of all widget types – com.ibm.rcp.toolbox.admin/createTool and com.ibm.rcp.toolbox.admin/createToolProviderIDs.

**Procedure**

1. Click the Getting Started with Widgets toolbar button to start the wizard.
2. Click Features and Plugins and then click Next.
3. In the Enter the URL ... field, specify the existing update site URL, specifically the path to the site.xml file in the target update site, and click Load.

   **Note:** The URL can be of the nrpc://, http:// or https://, or file:// format as follows:
   
   - nrpc:// – Use Notes nrpc protocol to specify the path to the update site application (for example, updatesite.nsf) in which the feature's update site resides.
     
     nrpc://server_name\directory_path\updatesite.nsf
   
   - http:// or https:// – Use http or secure https protocol to specify the path to the update site in which the feature's update site resides.
     
     http://server_name/directory_path/updatesite/site.xml
     
     jar:http://server_name/directory_path/updatesite.zip/
   
   - file:// – Use a simple file path protocol if, for example, the update site is resident on disk.
     
     file:///C:\directory_path\updatesite\site.xml
     
     jar:file:///c:\directory_path\updatesite.zip/

   All the available features and plug-ins in the update site are displayed and available for selection. To simplify deployment for users, be sure that you have signed the features and plug-ins using a trusted certificate authority; this prevents users from being prompted to respond to trust screens during provisioning.

4. Select one or more features for the widget to deploy and click Next or Finish. Click Finish to complete the widget by accepting all defaults.
   
   If you select only one feature and click Next, the feature name appears in the **Widget Name** field and the feature description appears in the **Description** field. Features do not require a description, so this field may be blank.
   
   If you select more than one feature, **Provisioning Widget** appears in the **Widget name** field and **This widget will provision the following features: feature_ids** appears in the **Description** field.

5. Confirm or modify the **Widget name** field entry. This field is required.
6. Optionally specify an **Image URL** to use as the widget's thumbnail in the My Widgets panel.
7. Confirm or modify the **Description** field entry to appear in the widget's catalog document (if published) and click Next.
8. Preview and optionally edit the install manifest snippet (<installfeature> code block) and click Next.
9. Click Finish and, as prompted, be sure to test the widget before sharing it with others.
10. If you publish the widget to the catalog, open the widget document and specify its provisioning type. After creating the widget, a thumbnail is added to the My Widgets panel representing the provisioning widget you just created. The features are then installed and you are prompted to restart your client.

For details on the elements that should be configured to use a widget, widget catalog, and central update site to deploy client plug-ins to users, as well as steps for testing the new widget prior to sharing it with others, see the Sametime Administrator help topic "Deploying client plug-ins with widgets and the widget catalog".

Creating a features and plugins deployment widget

You can create a widget to assist in managing new feature deployment and update provisioning on the client based on policy or preferences.

In the client, use the Getting Started with Widgets option Features and Plugins to simplifying the process of creating a widget to deploy a client plug-in.

To display the needed user interface, click File > Preferences > Widgets and enabling the Show Widget toolbar and the My Widgets side bar panel option in the client.

For procedure details, see "Deploying client plug-ins with widgets and the widget catalog" in this product documentation and "How do I create a Features and Plugins deployment widget?" in IBM Sametime Connect help.

Related concepts:

“Administering Widgets and Live Text” on page 193
Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.

“Catalog options and access” on page 202
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

“Using public widget provider APIs” on page 230
A set of public APIs are available that developers can use to create custom widget types for use with either supplied or custom applications.

Related tasks:

“Creating the widget catalog” on page 200
The widgets catalog centrally houses available widgets.

Deploying client plug-ins with widgets and the widget catalog

You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature’s update site, and Domino policy or Eclipse preferences.
Before you begin

This process is written as an ordered procedure and assumes you have a valid Eclipse update site containing a features folder, plugins folder, and site.xml file and that all JAR files in the update site folders are properly signed. It also assumes you want to deploy this plug-in to an existing user such that it be installed, and that any updates to it be automatically provisioned, for that user.

About this task

Once you have performed these steps, users will be automatically provisioned with the feature called by the widget’s extension.xml. The feature called by the widget you are about to create will be installed when the user’s local widgets catalog is updated. As well, any updates you make to the feature will be provisioned to the user by way of the widget. The client checks the widget catalog for updates periodically and upon user request.

CAUTION:
You can use the "Features and Plugins" option on the Getting Started with Widgets wizard in Notes to simplify the process of creating a feature and plug-in deployment widget. See "How do I configure a Features and Plugins deployment widget?" for usage details. The wizard especially simplifies the process of creating the widget's attachment XML.

You will use these items to complete the process:
- Widgets catalog on named Domino server
- Correctly configured Widgets section of Domino Desktop policy settings document
- Correctly formed and signed Eclipse update site containing the feature(s) to deploy
- NSF-based update site containing your Eclipse update site
- Widget resident in the widgets catalog and of the same category as the user’s policy or preference
- Correctly formed widget XML file attachment that calls the update site

Note: Two sample extension.xml files are attached to the above-specified tech note.

Note: The Start Configuring Widgets wizard dialog (click Getting Started with Widgets in the toolbar or My Widgets sidebar panel) contains Features and Plugins option. This option launches a wizard sequence designed to simplify the process of creating a Notes client plug-in deployment widget. The wizard guides you through the widget definition and extension.xml creation process.

The main steps for deploying a new feature using a widget are as follows:
- Place the feature’s valid Eclipse update site, containing the signed features and plug-ins, in a central location
- Install or upgrade the server and client, create the widgets catalog, and set widgets policy or preferences
- Create an NSF-based update site and import the Eclipse update site
- Create the extension.xml that the widget will use to call the feature’s update site
- Display the Widgets sidebar and verify or set catalog access
• Create the widget in the widgets catalog and attach its extension.xml file to call the update site
• Test the widget by dragging it from the catalog view to your My Widgets sidebar
• Communicate to users how to obtain the widget or inform them that they will be automatically provisioned with the widget and its feature

**Note:** In addition to the topic references in the procedure steps, the following topics provide additional information.

• Catalog options and access
• Format of the Eclipse update site
• Specifying available update sites
• Controlling feature install and update with update sites
• Controlling My Widgets access with Eclipse preferences
• Updating a widget-deployed client feature or plug-in

Related information is also available in the Lotus Notes and Domino wiki.

**Procedure**

Perform the following tasks:
Related concepts:

“Understanding Widgets and Live Text user types” on page 196
Widgets and Live Text is designed to accommodate various user types. For example, a power user or application developer will typically create and deploy widgets to end users while end users may use widgets that have been created for them, rather than create their own.

“Creating a features and plugins deployment widget” on page 217
You can create a widget to assist in managing new feature deployment and update provisioning on the client based on policy or preferences.

Related tasks:

“Place the feature's updateSite folder centrally”
In this example, you’ll import the Eclipse update site into an NSF-based update site on a central Domino server in the "Create an NSF-based update site and Import the Eclipse update site."

“Embedded ST Only: Prepare the Domino server and Notes client” on page 221
Perform these steps to install or upgrade your IBM Lotus Domino server and IBM Lotus Notes client, create the widgets catalog, and specify widgets policy or preference settings for users.

“Create an NSF-based update site and import the Eclipse updateSite content” on page 222
The update site can reside on any HTTP or IBM Lotus Domino server that can be reached using HTTP or Notes NRCP protocols. Importing the update site into the NSF-based update site is the recommended method for deploying features and plug-ins using widgets.

“Embedded ST Only: Create the widget attachment file to call the feature's update site” on page 223
The widget’s extension.xml file will contain an install manifest install feature snippet with a pointer to the update site and specifications on how to install or update the feature. You can simplify the process described here by using the Features and Plugins wizard in Lotus Notes.

“Test the deployment widget” on page 227
Always test a feature deployment widget before making it available to your users.

“Communicate deployment to users” on page 228
Tell IBM Lotus Notes users how to obtain the widget or inform them they will be automatically provisioned with the widget, and the feature it is designed to deploy, upon their next catalog update.

“Updating a widget-deployed client feature or plug-in” on page 229
When you have a new version of a widget deployed client plug-in, use this procedure to update the update site and the deployment widget’s XML attachment in the widgets catalog.

“Creating the widget catalog” on page 200
The widgets catalog centrally houses available widgets.

Place the feature's updateSite folder centrally
In this example, you’ll import the Eclipse update site into an NSF-based update site on a central Domino server in the "Create an NSF-based update site and Import the Eclipse update site."

About this task

Perform these steps to place the feature's valid Eclipse updateSite folder containing the signed features and plugins, in a central location.
Procedure

Place the feature’s signed Eclipse updateSite folder, including the features and plugins subdirectories and the valid site.xml file, onto your local client system. The NSF-based update site can reside on either an HTTP server or Domino server. This process assume that you already have a valid Eclipse update site, containing the signed features and plugins. For information about signing the contents of an update site, see “Signing custom or third-party features and plug-ins for install and update.”

Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature’s update site, and Domino policy or Eclipse preferences.

Embedded ST Only: Prepare the Domino server and Notes client
Perform these steps to install or upgrade your IBM Lotus Domino server and IBM Lotus Notes client, create the widgets catalog, and specify widgets policy or preference settings for users.

About this task
Prepare a Notes client plug-in deployment environment as follows.

Procedure

1. Install or upgrade a Domino server.
   This server will house the widget catalog application and NSF-based update site, and optionally be used to configure the user's desktop policy settings with new Widgets policy settings.
   In this example, the Domino server name is WidgetCatalogServer.abx.com.
2. Install or upgrade a Notes client.
3. Create the widgets catalog on the server using the widgets catalog template as described in the “Creating the widget catalog” topic.
4. Configure Domino policy to specify the catalog server name, catalog name, and catalog categories to install using the Widgets tab on the Domino desktop policy settings document as described in the “Controlling Widgets and Live Text access with Domino policy” topic.

   Note: Alternatively, establish these settings with either the user's My Widgets preference panel or Eclipse preferences in the plugin_customization.ini file on the client.

   For this example, specify values for the first two settings for both your own policy and your users; specify the third setting for users only. Leave all other settings as is. These values are for this example only:
   Widget catalog server -- WidgetCatalogServer.abx.com
   Widget catalog application name -- toolbox.nsf
   Widget catalog categories to install -- widgetsforyou

   Note: The “widgetsforyou” category is for your target Notes users; you do not need it for your own policy setting as you create and test the widget.
5. If you have used the Enable provider IDs for widget addition or Restrict provider IDs for installation/execution settings on the Widgets tab in the
desktop policy settings document to control which widget types your users can install and use, note that a fifth type, prov.provider.ToolboxProvisioning, has been added which allows a widget to be used to deploy a client plug-in, which you should enable. An equivalent setting in the plugin_customization.ini file is also now available. For more information, see the “Controlling Widgets and Live Text access with Domino policy” topic.

Related concepts:
“Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.

“Catalog options and access” on page 202
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

“Administering Widgets and Live Text” on page 193
Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.

Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

“Creating the widget catalog” on page 200
The widgets catalog centrally houses available widgets.

Create an NSF-based update site and import the Eclipse updateSite content
The update site can reside on any HTTP or IBM Lotus Domino server that can be reached using HTTP or Notes NRCP protocols. Importing the update site into the NSF-based update site is the recommended method for deploying features and plug-ins using widgets.

About this task
The NSF-based update site provides a central location for housing features for user deployment and provisioning. In this example, the NSF-based update site will reside on WidgetCatalogServer.abx.com.

You can import an Eclipse update site into an NSF-based update site (for example updatesite.nsf) as described in the “Creating and using an NSF-based update site” topic in this guide and the general steps below.

To import an Eclipse update site into an NSF-based update site do the following:
Procedure

1. Create the NSF-based update site as below:
   a. Click File > Application > New.
   b. Click Show Advanced Templates and specify the Eclipse Update Site template (updatesite.ntf) as the template.
      The NSF-based update site template (updatesite.ntf) is installed as part of the Domino server install or upgrade.
   c. Specify a title and NSF file name (for example, updatesite.nsf) for the new application and click OK.

2. Import the Eclipse update site into the new and open NSF-based update site as below.
   a. Click Features in the left pane navigator and then click Import Local Update Site.
   b. As prompted, browse to the update site, select its site.xml file, and click OK.

Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

“Updating a widget-deployed client feature or plug-in” on page 229
When you have a new version of a widget deployed client plug-in, use this procedure to update the update site and the deployment widget's XML attachment in the widgets catalog.

Related information:

  "NSF based Update Sites" on My developerWorks Blog

Embedded ST Only: Create the widget attachment file to call the feature’s update site
The widget's extension.xml file will contain an install manifest install feature snippet with a pointer to the update site and specifications on how to install or update the feature. You can simplify the process described here by using the Features and Plugins wizard in Lotus Notes.

About this task

Perform these steps to create the widget's extension.xml attachment file that you will use to call the update site and provision the feature to users.

Note: The Start Configuring Widgets toolbar button contains a Features and Plugins option. This option launches a wizard sequence designed to simplify the process of creating a Notes client plug-in deployment widget. The wizard guides you through the widget definition and extension.xml creation process. For details, see “How do I configure a Features and Plugins deployment widget?” in Notes user help.

Procedure

Create the extension.xml file. Use the sample XML below as a guide.
Note: See the related information for details about the contents of an install manifest, available in the Provisioning manifest DTD topic in the Lotus Expeditor wiki.

Sample XML

The items in bold are the fields you need to customize for your own feature.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<webcontextConfiguration version="1.1">
    <preferences>
    </preferences>
    <data>
      <installManifest>
        <![CDATA[
          <install>
            <installfeature description="Comp XYZ Custom Plugin" id="Test_Feature_ABX" name="Test Feature ABX">  
              <requirements>
                <feature download-size="10" id="Test_Feature_ABX" match="perfect" shared="true" size="10" version="1.0"/>
              </requirements>
              </installfeature>
            </install>
          ]]>  
        </installManifest>
      </data>
    </paletteItem>
  </webcontextConfiguration>
```

Sample XML definitions:

About this task

Items in the top section of an extension.xml file are described below:

Note: This example points to the site.xml file in an NSF-based update site.

Note: By default, only public update sites that do not require authentication are available for feature deployment using widgets. However, you can use accounts to configure access to update sites that require user authentication.

Note: Provided that shared="true" is set in the install manifest of the widget's .XML, the plug-in is installed to Notes_install_dir\framework\shared\eclipse. If there is no write access to that directory, the plug-in is installed to Notes_install_dir\data\workspace\applications.

Note: You can obtain the sample extension.xml file used in this example; see the related information links.

- xml version = internal setting, use exactly as specified in the sample
- encoding = internal setting, use exactly as specified in the sample
- webcontextConfiguration version = internal setting, use exactly as specified in the sample
• palletitemid = internal ID setting, this must adhere to the namespace/ID format as specified in the sample - this value must be unique for each pallette item
• imageUrl = URL at which the widget graphic that appears in the My Widgets sidebar resides, if no value is specified a default graphic is used
• providerID = states the widget’s intent, for widgets that deploy features you must use exactly as specified in the sample
• title = widget name that appears in the My Widgets sidebar panel
• url = pointer by which the update site and site.xml are located. You can specify a URL value using NRCP protocol if the update site resides in an NSF-based update site (for example, updateSite.nsf) on a Domino server or using an HTTP protocol if the update site exists on an HTTP server.

Related concepts:
“Catalog options and access” on page 202
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

Related information:
[Provisioning manifest DTD]

How to use a Notes widget to deploy a new plug-in to an existing Notes installation

Display the My Widgets sidebar panel and set catalog access

About this task

Perform these steps to start the Notes client, display the My Widgets sidebar panel, and ensure that the catalog server and catalog name preferences are correct.

Procedure
1. Start Notes and open the Widgets preference panel by clicking File > Preferences > Widgets.
2. Enable the Show Widgets Toolbar and the My Widgets sidebar panel option (this option is typically disabled by default when not using policies).
   If you specified policy settings for the catalog earlier, they will be visible on this preference panel. In this example, those values should be as below:
   Catalog server -- WidgetCatalogServer.abx.com
   Catalog name -- toolbox.nsf
   Catalog categories to install -- (leave this setting as is for now)
3. Click OK to display the My Widgets sidebar panel and toolbar and connect to the widgets catalog.
Related concepts:

“Default Widgets and Live Text behavior” on page 198
Users can browse the widgets catalog and obtain widgets from it, and optionally add widgets to the catalog, provided their Widgets preferences point to the catalog and the catalog ACL settings enable their access.

“Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.

“Controlling Widgets and Live Text access using Eclipse preferences” on page 209
Access to Widgets and Live Text functionality and the widgets catalog is set using Eclipse preferences in the plugin_customization.ini file or managed preferences. This is applicable to Sametime standalone environments where Domino policy is not used.

“Catalog options and access” on page 202
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

Create the deployment widget
You can create the deployment widget directly in the catalog, as described here, or create the widget using a configuration wizard and then publish the widget to the catalog. You can simplify the process described here by using the Features and Plugins wizard.

About this task
Perform these steps to open the widgets catalog, create the widget, and attach the extension.xml file that you created earlier.

Note: The Start Configuring Widgets toolbar button contains a Features and Plugins option. This option launches a wizard sequence designed to simplify the process of creating a Notes client plug-in deployment widget. The wizard guides you through the widget definition and extension.xml creation process. For details, see "How do I configure a Features and Plugins deployment widget?" in Notes user help.

Procedure
1. Open the widgets catalog by clicking Browse the Widget Catalog in the My Widgets panel toolbar.
2. Create the widget.
   a. In the widget catalog, click the All Widgets view option.
   b. Click Add Widget to Catalog.
   c. Enter a widget title, for example "FeatureABX" in the Title field.
   d. Click Category and select a existing or type a new category name, for example widgetsforyou. For this example scenario, type the new catalog category "testFeatureABX" name.
   e. Optional: Click Platform and select all that apply.
   f. For view sorting purposes, click Plugin and Features.
g. In the Description field, enter a brief descriptor, such as "Provision FeatureABX to users."

h. Click Attach and select the extension.xml file that you created earlier.

i. Click Save and Close.

Related concepts:
“Administering Widgets and Live Text” on page 193
Widgets and Live Text enables end users to see and act on recognized Live Text in any supported content like chat windows, chat history, Notes documents (Sametime embedded in Lotus Notes client only), and so on, using XML extensions (widgets) created specifically for their use.
“Creating a features and plugins deployment widget” on page 217
You can create a widget to assist in managing new feature deployment and update provisioning on the client based on policy or preferences.
“Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.
“Controlling Widgets and Live Text access using Eclipse preferences” on page 209
Access to Widgets and Live Text functionality and the widgets catalog is set using Eclipse preferences in the plugin_customization.ini file or managed preferences. This is applicable to Sametime standalone environments where Domino policy is not used.

Related tasks:
“Creating the widget catalog” on page 200
The widgets catalog centrally houses available widgets.
“Updating a widget-deployed client feature or plug-in” on page 229
When you have a new version of a widget deployed client plug-in, use this procedure to update the update site and the deployment widget's XML attachment in the widgets catalog.

Test the deployment widget
Always test a feature deployment widget before making it available to your users.

About this task
You can test the widget by dragging it from the catalog view to your My Widgets sidebar

Procedure
1. Drag the new widget from the widgets catalog view to your My Widgets sidebar panel.
2. Respond to any feature install prompts that appear.
   When you install a new feature you are prompted to restart the client.
3. Upon restart, note the addition of the FeatureABX widget in the My Widgets sidebar panel.
4. Test the functionality that you expected to be installed by the widget.
5. Once you are satisfied with the widget behavior, change the widget's category name to make it available to users whose Widgets categories to install policy or preference matches the widget's category. In this example, reopen the widget in the catalog and change its widget category from "testFeatureABX" to "widgetsforyou" as used in this example as specified in their Widget catalog categories to install policy setting.
Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an
existing IBM Lotus Notes client using a combination of the widgets catalog, an
NSF-based update site in which the feature resides, an XML file attached to the
widget that calls the feature's update site, and Domino policy or Eclipse
preferences.

Communicate deployment to users
Tell IBM Lotus Notes users how to obtain the widget or inform them they will be
automatically provisioned with the widget, and the feature it is designed to deploy,
upon their next catalog update.

About this task

Procedure
1. Install the widget from the catalog.
   If using policies:
   • Click Catalog > Update Widgets from your My Widgets sidebar panel
     options menu.
   • Allow the local catalog to be updated/replicated on its regular schedule and
     be aware that the new widget will be added and the feature it is designed to
     deploy will be installed, when the local catalog is updated.
   If not using policies:
   • Click Catalog > Update Widgets from your My Widgets sidebar panel
     options menu. Click Catalog > Preferences, select the category in which the
     widget resides, and click Apply.
   • Open the catalog (click Browse the Widget Catalog in the My Widgets
     sidebar panel toolbar), highlight the widget, and drag it to your My Widgets
     sidebar panel.
2. Respond to any feature installation prompts that appear.
   Note: When you install a new feature, you are prompted to restart the client.
3. Upon restart, note the addition of the FeatureABX widget in the My Widgets
   sidebar panel and the feature called by that widget.
   The widget catalog is checked for updates based on a replication schedule.
   Adding or removing a category in the Widgets preference panel adds or
   removes widgets on the client in or from that category. Any features called by a
   widget in a category to which a user is subscribed are installed on that user's
   client system.
Related concepts:
“Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.
“Controlling Widgets and Live Text access using Eclipse preferences” on page 209
Access to Widgets and Live Text functionality and the widgets catalog is set using Eclipse preferences in the plugin_customization.ini file or managed preferences. This is applicable to Sametime standalone environments where Domino policy is not used.

Related tasks:
“Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.
“Updating a widget-deployed client feature or plug-in”
When you have a new version of a widget deployed client plug-in, use this procedure to update the update site and the deployment widget's XML attachment in the widgets catalog.

Updating a widget-deployed client feature or plug-in
When you have a new version of a widget deployed client plug-in, use this procedure to update the update site and the deployment widget's XML attachment in the widgets catalog.

About this task
Feature updates are provisioned to the user automatically provided that you have properly updated and signed the contents of your feature update site, properly updated the widget's extension.xml file by incrementing the version= setting in the requirements section of the extension.xml, and updated the version number in the feature's Eclipse update site site.xml file to match the widget's extension.xml file's feature version= setting.

The updated widget and plug-in will be provisioned when the user's local widgets catalog is updated (either manually or on their defined replication schedule).

Note: Your client plug-in update procedure depends on whether you installed the client using an add-on installer or using the widget deployment method presented here. You should not swap methods when updating from one version to another.

Note: For related information, see "Deploying client plug-ins with widgets and the widget catalog."

Procedure
1. Obtain the updated feature's Eclipse updateSite and copy it to your local computer.
2. Update your existing update site with the new feature. If using a Notes-based update site, update (reimport) the updated feature's Eclipse updateSite into your Notes-based update site (updatesite.nsf) by opening your updatesite.nsf, clicking Import Local Update Site and specifying the updated feature's Eclipse updateSite/site.xml.
3. Open the widgets catalog. For example, click the **Browse the Widget Catalog** option in the My Widgets sidebar panel toolbar to open the catalog specified in the Widgets preference panel.

4. Double-click the deployment widget name in the widgets catalog to open the widget document, and then click **Edit**.

5. In the Attachments section of the widget document, right-click the extension.xml file and save the file locally. Open the file in an XML editor.

   **Note:** Edit the extension.xml content to match the correct `version` setting in the `installfeature` section of the updated feature.

6. Save and exit the extension.xml file.

7. In the widget document, click the **Remove** button to remove the attachment. Then click the **Attach** button to attach the new file created in step 6.

8. Save and close the widget document.

**Related concepts:**
"Creating a features and plugins deployment widget” on page 217
You can create a widget to assist in managing new feature deployment and update provisioning on the client based on policy or preferences.

**Related tasks:**
"Deploying client plug-ins with widgets and the widget catalog” on page 217
You can use a widget to deploy a new feature and corresponding plug-in to an existing IBM Lotus Notes client using a combination of the widgets catalog, an NSF-based update site in which the feature resides, an XML file attached to the widget that calls the feature's update site, and Domino policy or Eclipse preferences.

"Create the deployment widget” on page 226
You can create the deployment widget directly in the catalog, as described here, or create the widget using a configuration wizard and then publish the widget to the catalog. You can simplify the process described here by using the **Features and Plugins** wizard.

**Using public widget provider APIs**
A set of public APIs are available that developers can use to create custom widget types for use with either supplied or custom applications.

After deploying the plug-in containing the new widget type, the new widget types can then be disabled or enabled for users in the same way as the supplied widget types (using either Domino policy or a plugin_customization.ini file). Power users can then create widgets of these additional widget types and deploy them to end users.

**Note:** For information about deploying a plug-in using a widget, see “Deploying client plug-ins with widgets and the widget catalog” in this product documentation.

The com.ibm.rcp.toolbox plug-in provides the set of public APIs that allow for the following:

- use of a new custom widget type
- creation of the new widget type using wizards
- a custom widget provider to manages the new widget type
- use of utilities for common widget functions
The set of public APIs are provided as part of the installed Notes client. API JavaDoc is available in the Lotus Notes and Domino Application Development wiki containing documentation about how to use the new provider APIs and samples.

The extension point names for these public APIs are:

com.ibm.rcp.toolbox.widgetWizard
com.ibm.rcp.toolbox.widgetProvider
com.ibm.rcp.toolbox.customWidgetAction

Related information about enabling widget creation by extension point/type using policy or the plugin_customization.ini file is available in product documentation as related links below and in the "Widgets: Policies and Roll Out Best Practices" article in the Lotus Notes and Domino wiki.

Related concepts:
“Catalog options and access” on page 202
The widgets catalog is a server-based application that contains all centrally managed widgets and their underlying XML extension definitions, including content types and recognizers. The catalog is based on the IBM® Lotus® Domino® server-supplied Widget Catalog template (TOOLBOX.NTF) and its access is controlled by a combination of application ACLs and Domino policies (or PLUGIN_CUSTOMIZATION.INI preferences), as well as widget categories.

“Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.

“Controlling Widgets and Live Text access using Eclipse preferences” on page 209
Access to Widgets and Live Text functionality and the widgets catalog is set using Eclipse preferences in the plugin_customization.ini file or managed preferences. This is applicable to Sametime standalone environments where Domino policy is not used.

Related tasks:
“Creating the widget catalog” on page 200
The widgets catalog centrally houses available widgets.

Specifying Widget settings for a desktop policy
Use the Widgets tab of the Desktop Settings policy to control access to Widgets and Live Text for users of the policy.

About this task
Note that some policy settings contain a "How to apply this setting" column, which you can use to establish one of the following conditions for that setting.

• Don't set value
  The value set is not applied to the client's Widgets preferences panel. The user can specify a preference value and this policy setting will not overwrite that value.

• Set initial value
  The value is applied once to the client but the user can change the setting on the Widgets or Live Text preferences panel. If the administrator changes the policy value later, the user's setting is not overwritten.

• Set value whenever modified
The value is applied to the client and is reapplied (overwriting a user-set change) whenever the policy setting is modified.

- Set value and prevent changes
  The value is applied to the client and the preference is then disabled on the Widgets or Live Text preferences panel, such that the user cannot change the value.

**Note:** If you are not using a server-managed environment, you can use the plugin_customization.ini file either before or after install to control user access to Widgets and Live Text functionality. You can also use the Widgets preferences panel to set the catalog server, catalog name, and categories to install values, as well as the *Show Widgets Toolbar and the My Widgets Sidebar panel* preference. Policy settings take precedence over Eclipse preferences.

*Default Widgets and Live Text behavior* describes Widgets and Live Text behavior when no policy or preference changes have been made.

**Procedure**

Complete the following fields on the **Widgets tab**:

*Table 41. Widgets tab fields*

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
</table>
| Widget catalog server         | Specify the catalog server from which to provision at application startup and periodically during replication from the catalog to the user’s local replica (24 hours by default). Use server/domain format or a fully qualified name. If you use a server/domain format, server failover is supported.  
  If this policy’s “How to apply this setting” column is set to “Set value and prevent changes”, users will not be able to change the value on the Widgets preferences panel.  
  By default, this value is not set.                                                                                                           |
| Widget catalog application name | Specify the Widget catalog application name, for example toolbox.nsf, on the catalog server, from which to provision at client application startup and periodically during replication from the catalog to the user’s local replica (24 hours by default). Use the Widget Catalog template (toolbox.ntf) to create the catalog application.  
  If this policy’s *How to apply this setting* column is set to *Set value and prevent changes*, the end user will not be able to change the value on the Widgets preferences panel.  
  The default catalog name is toolbox.nsf.                                                                                                  |
| Enable Live Text              | Specify if auto-recognized Live Text appears as dash-underlined text in a user’s document. Live Text display can be toggled on and off when working in a session.  
  If this setting is disabled, then the Live Text preference panel is hidden from the user.                                                                 |
  By default, this setting is enabled.                                                                                                       |
### Table 41. Widgets tab fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget catalog categories to install</td>
<td>Specify the widget categories to install and update for this user. These categories will appear in the <strong>Categories to install</strong> list box on the Widgets preferences panel. Use this setting to limit user access to specific widget categories. If this field is blank, no widgets are installed in the user’s My Widgets sidebar panel. Categories typically equate to a user grouping, such as a specific project team or job type. The categories listed in this policy cause the equivalent category names in the Widgets preferences panel to be selected and disabled; the end user cannot deselect them. By default, this value is not set.</td>
</tr>
<tr>
<td>Show the My Widgets panel in the sidebar</td>
<td>Specify if the My Widgets panel is visible in the Notes sidebar (for embedded Sametime) and if the Widgets menus and toolbar are visible. If this setting is enabled and its <strong>How to apply this setting</strong> column is set to <strong>Set value and prevent changes</strong>, the end user will not be able to change the “Show Widgets Toolbar and the My Widgets Sidebar panel” value on the Widgets preferences panel. If this setting is disabled and its ”How to apply this setting” column is set to ”Set value and prevent changes”, the Widgets preferences panel will not be visible to the end user. By default, this setting is disabled.</td>
</tr>
<tr>
<td>Restrict the addition of widgets to specific types</td>
<td>Restrict creation and edit of widgets to certain types (referred to as provider IDs). The Widgets and Live Text feature includes an extension point for widget providers. The supplied providers include Notes view, Feeds, Web page or service, and Google Gadget. If this setting is disabled, the user can create or edit widgets with no restriction on type. If this setting is enabled, the user can only create or edit widgets of a certain type. The administrator can then specify which widget types (provider IDs) are available using the setting below. By default, this setting is disabled.</td>
</tr>
<tr>
<td>Field</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Enable provider IDs for widget addition | **Note:** This field appears in the form only when *Restrict the addition of widgets to specific types* is enabled.  
com.ibm.notes.toolbox.provider.NotesViewPalletteProvider  
com.ibm.notes.toolbox.provider.NotesFormPalletteProvider  
com.ibm.rcp.toolbox.web.provider.WebServicesPalletteProvider  
com.ibm.rcp.toolbox.feeds.FeedPalletteProvider  
com.ibm.rcp.toolbox.google.provider.internal.GooglePalletteProvider  
com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning  
com.ibm.rcp.toolbox.search.provider.SearchPalletteProvider  
The default is as below:  
For example, if the policy setting "Restrict the addition of widgets to specific types" is set to "Enabled" and "Enable provider IDs for widget addition" is set to the value below, the user could only create Google Gadget widget types:  
com.ibm.rcp.toolbox.google.provider.internal.GooglePalletteProvider |
| Restrict provider IDs for installation/execution | Restrict installation and update of widgets to specific types (referred to as provider IDs). If enabled, the administrator can then specify which widget types (provider IDs) are available using the setting below. Note that if you restrict what widget types are available for installation, you should also restrict creation of those same widget types using the *Restrict the addition of widgets to specific types* and *Enable provider IDs for widget addition* policies.  
By default, this setting is disabled. |
| Enable provider IDs for installation/execution | **Note:** This field appears in the form only when *Restrict provider IDs for installation/execution* is enabled.  
Specify the widget types available for install and update. Use a comma to separate types in the list.  
The available widget type/Provider ID entries include the following and correlate to the available widget types.  
com.ibm.notes.toolbox.provider.NotesViewPalletteProvider  
com.ibm.notes.toolbox.provider.NotesFormPalletteProvider  
com.ibm.rcp.toolbox.web.provider.WebServicesPalletteProvider  
com.ibm.rcp.toolbox.feeds.FeedPalletteProvider  
com.ibm.rcp.toolbox.google.provider.internal.GooglePalletteProvider  
com.ibm.rcp.toolbox.google.provider.webbrowser.GooglePalletteProvider  
com.ibm.rcptoolbox.prov.provider.ToolboxProvisioning  
com.ibm.rcp.toolbox.search.provider.SearchPalletteProvider  
The default is as below:  
For example, if the policy setting "Restrict provider IDs for installation/execution" is set to "Enabled" and "Enable provider IDs for installation/execution" is set to the value below, the user could only install or provision Google Gadget widget types:  
com.ibm.rcp.toolbox.google.provider.internal.GooglePalletteProvider |
Table 41. Widgets tab fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
</table>
| Restrict extension point IDs for installation/execution | Restrict installation of widgets that contain certain extension points. If enabled, the administrator can then specify which extension point IDs are allowed using the setting below.  
**Note**: Extension points are an Eclipse feature. They define new function points for the platform that other plug-ins can plug into. Eclipse provides many extension points with the core platform. The Widgets and Live Text feature also provides some extension points.  
The Eclipse platform provides the following identifiers, and many others:  
org.eclipse.ui.popupMenus, org.eclipse.ui.viewActions, org.eclipse.ui.views identifiers  
Notes and Expeditor provide the following identifiers, and many others:  
By default, this setting is disabled. |
| Enable extension point IDs for installation/execution | **Note**: This field appears in the form only when **Restrict extension point IDs for installation/execution** is enabled.  
You can restrict this list or add to it. Use a comma to separate items in the list. The default is as below:  
For example, if the policy setting **Restrict extension point IDs for installation/execution** is enabled and **Enable extension point IDs for installation/execution** is set to "com.ibm.rcp.content.contentTypes", then widgets containing regular expression recognizers (com.ibm.rcp.annotation.regex.regexTypes) would not be allowed to be installed/provisioned. |
| Create and manage an action | Specify whether the user can create, edit, and remove actions while working in the My Widgets panel and the Widget Management view.  
By default, this option is enabled. |
| Create and manage recognizers and content types | Specify whether the user can create, edit, and remove recognizers and content types while working in the My Widgets panel. If enabled, the user can create, remove, or edit recognizers and content types and can use the **Manage Widgets, Content, and Recognizers** My Widgets option. This also enables display of the **Recognize All Content** option in the My Widgets menu and the "Display type properties" action when right-clicking on a content type in a Notes document.  
By default, this setting is enabled. |
| Enable default recognizers | Specify if the Lotus-supplied, advanced Live Text recognizers such as person (name), place (address), and organization are enabled.  
If this setting is disabled, then the user cannot enable it.  
By default, this setting is enabled. |
### Table 41. Widgets tab fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send widgets using e-mail</td>
<td>Specify whether the user can send widgets to others as XML extension attachments using the &quot;E-mail to&quot; action and also whether the user can output an XML file containing selected widgets from the My Widgets sidebar panel using the Export option. By default, this setting is enabled.</td>
</tr>
<tr>
<td>Install widgets from e-mail or other</td>
<td>Specify whether a user can install widgets using an XML extension file obtained from e-mail or from the user's file system. If enabled, the user can use drag and drop to install widgets from e-mail (or any Notes document that contains an attached extension.xml file, not including the configured catalog) or an import action from the user's file system. By default, this setting is enabled.</td>
</tr>
<tr>
<td>Install widgets from catalog</td>
<td>Specify whether a user can install widgets using an XML extension file obtained from e-mail or from the user's file system. If enabled, the user can use drag and drop to install widgets from e-mail (or any Notes document that contains an attached extension.xml file, not including the configured catalog) or an import action from the user's file system. By default, this setting is enabled.</td>
</tr>
<tr>
<td>Publish to catalog so others can browse (subject to catalog ACLs)</td>
<td>Grant access to the user, typically the power user or application developer user, to publish widgets from their My Widgets panel to the catalog for use by others. Note that this option applies to widgets, content types, and recognizers. When you publish a widget to the catalog, you should assign widget categories to it. By default, this setting is enabled.</td>
</tr>
</tbody>
</table>

**Related concepts:**

- “Default Widgets and Live Text behavior” on page 198
- Users can browse the widgets catalog and obtain widgets from it, and optionally add widgets to the catalog, provided their Widgets preferences point to the catalog and the catalog ACL settings enable their access.
- “Embedded ST Only: Controlling Widgets and Live Text access using Domino policy” on page 204
- You can use the IBM Lotus Domino desktop policy settings document to define Widgets and Live Text availability for specific users.

### Backing up WebSphere Application Server configurations

As part of a routine maintenance schedule or before upgrading Sametime servers that run on WebSphere Application Server, back up the WebSphere Application Server configurations.

**About this task**

Run the backupConfig command for each of the configurations that are relevant to Sametime. Note the exact name and location of the backed-up configurations so that you can find them if you need to roll back to an earlier configuration.
1. Back up the Deployment Manager configuration.
2. Back up the application server configuration.
3. Back up the federated node configurations.

For more information, see backupConfig command in the WebSphere Application Server information center.
Chapter 2. Performance

IBM Sametime administrators can make adjustments to the servers they maintain to provide optimal performance for users as they use instant messaging and web conferencing.

This section contains information about tools provided by WebSphere Application Server and Sametime that help you fine-tune server response time.

Increasing the number of open files on a Sametime server running on Linux

If your IBM Sametime server is hosted on Linux, increase the number of concurrent open files on the server to prevent performance problems.

About this task

Java opens many files and Sametime uses a lot of file descriptors. When a high number of concurrent users (for example, 1,000 or more) connect to the Sametime Community Server, the server may run out of file descriptors.

Procedure

1. Follow the procedure that matches the way you start the Sametime server, either as a system service or as a regular process.
   • If you start the server as a system service
     a. Use a text editor and open the /etc/init.d script file and add the following lines to the file:
        ulimit -Hn 65535
        ulimit -Sn 65535
        Important: Exercise caution while editing the /etc/init.d script file. If you do not do this properly, your system may fail to boot properly. Consult your system documentation for more details.
     b. If no file of this name exists on your system, create a file with that name and add the following lines to the file:
        ulimit -Hn 65535
        ulimit -Sn 65535
        eval exec "$4"
     c. Save the file.
   • If you start the server as a regular process
     a. Use a text editor and open the /etc/security/limits.conf file.
     b. Increase the upper limit on the number of file descriptors by adding the following lines to the file:
        * soft nofile 65535
        * hard nofile 65535
     c. Save the file.
2. Restart the Linux server for the operating system change to take effect for all processes.
Tuning a Sametime Community Server

Complete the following tuning procedures to enhance performance.

**About this task**

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

In addition to the topics in this section, see Optimizing Sametime’s Name Lookup solution on the Sametime wiki.

**Tuning Sametime LDAP settings**

Complete the following procedures to enhance performance

**Managing Sametime LDAP internal queues**

You can manage advanced configuration settings for the maximum and minimum (MAX/LOW) number of LDAP requests that are pending per connection in the pending queue.

The following settings can be specified in the [Directory] section of the sametime.ini file.

- **ST_DB_LDAP_PENDING_MAX**
  
  Defines the maximum number of LDAP requests that can be pending per connection in the pending queue. Each connection is for a different type of request; whether search or bind. A Pending Resolve Request is a request that has been sent to the LDAP Server. The request is considered pending until the IBM Sametime Community Server receives a response from the LDAP server for that request. The Sametime Community Server sends, at most, MAX PENDING Requests to the LDAP server. After MAX Pending Requests are sent to the LDAP server on a particular connection, the Sametime Community Server does not send any additional LDAP requests on this connection until the Pending Queue Size drops to the ST_DB_LDAP_PENDING_LOW Pending Request queue size.

  For versions prior to Sametime 8.5, the value is set to 10 by default. In Sametime 8.5 and higher, the value is set to 60 by default. Any Sametime service that connects to the LDAP server utilizes the LOW and MAX PENDING queue.

- **ST_DB_LDAP_PENDING_LOW**

  Strongly linked to the ST_DB_LDAP_PENDING_MAX setting and to the request queuing feature of Sametime. Once ST_DB_LDAP_PENDING_MAX is reached for a certain connection, new LDAP requests are not sent on this connection until the number of pending operations drops to the value set by the ST_DB_LDAP_PENDING_LOW setting.

  For versions prior to Sametime 8.5, the value is set to 5 by default. In Sametime 8.5 and higher, the value is set to 30 by default.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sametime 8.5</th>
<th>Sametime pre-8.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST_DB_LDAP_PENDING_MAX</td>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>ST_DB_LDAP_PENDING_LOW</td>
<td>60</td>
<td>5</td>
</tr>
</tbody>
</table>
Special considerations for the PENDING MAX/LOW settings

As the PENDING MAX/LOW settings (ST_DB_LDAP_PENDING_MAX and ST_DB_LDAP_PENDING_LOW) relate to each LDAP connection, Sametime Community Server might be configured to work with multiple connections per Sametime module, and one connection may stop handling requests while other connections are working well.

The MAX and LOW pending queue sizes are highly dependent upon many factors, such as the resources available to the Sametime Community Server process on the host machine, the resources available to the LDAP process on the LDAP server, the network latency between the Sametime Community Server and LDAP servers, the types of generated searches, and so on. As a result, there is no golden number to guarantee the greatest efficiency for all configurations. By default, MAX and LOW are set to 10 and 5, respectively. However, advanced guidelines for optimizing LDAP configurations generally recommend 60 and 30. IBM typically recommends a size of 120 and 100 for larger corporations with high-powered LDAP servers.

Example of a Pending Low/Max Queue in Sametime.ini:

ST_DB_LDAP_PENDING_LOW = 5
ST_DB_LDAP_PENDING_MAX = 10

As the Sametime Community Server receives LDAP queries (for example, Sametime Resolve or Authentication requests requiring LDAP look ups), Sametime tries to fulfill those queries by sending corresponding LDAP queries to the LDAP Server. These LDAP queries remain in the “Pending” queue until they are resolved or responded back from the LDAP Server or timed out.

If the PENDING MAX value is 10, the Sametime Community Server does not send more than ten requests to the LDAP Server initially until at least 5 requests are resolved by the LDAP Server so that the low end threshold value specified by PENDING_LOW is reached. Once the number of requests waiting for responses reaches the PENDING_LOW value, the Sametime Community Server once again starts sending more requests to the LDAP Server but repeats the cycle and limits the number of requests in flight to the LDAP Server.

Note: If the MAX and LOW sizes for the Pending Queue are not set appropriately, it is possible to overwhelm the LDAP server or artificially reduce the potential high throughput of LDAP requests sent by the Sametime Community Server to the LDAP server.

Tuning the Sametime LDAP bind operation

There are different types of bind operations supported by the LDAP protocol. The most common are anonymous and simple bind, also known as authenticated bind.

About this task

An anonymous bind is the easiest way to establish a connection with the LDAP server. However, the anonymous client will have limited access to the directory when compared to authenticated clients. Using a simple bind, a client can be authenticated on the LDAP server by providing its DN and password in plain text. The server verifies that such a person exists in the directory and that the supplied password is correct.

The LDAP protocol is asynchronous, so a client can send multiple requests to the LDAP server on the same connection, and does not need to wait for the response.
of one request before sending the next one. Each request is identified by a request ID, and every response is associated with the original request ID. However, some LDAP servers limit the maximum number of requests that can be pending per single connection.

The following settings are under the [Directory] section of the sametime.ini file:
- \ST_DB_LDAP_PENDING_BIND_MAX=X
- \ST_DB_LDAP_PENDING_BIND_LOW=Y

These settings only affect the bind requests allowing other requests (mainly search requests) to be sent to LDAP in different rates.

To force the IBM Sametime Server to send BIND requests synchronously use the following settings:
- \ST_DB_LDAP_PENDING_BIND_MAX=1
- \ST_DB_LDAP_PENDING_BIND_LOW=0

This settings make sure that no other requests will be sent to LDAP on the same connection before getting the response to the bind request. For more information see the TechNote Adding the ability to send bind requests to LDAP synchronously.

**Tuning multiple connections in Sametime LDAP**

You can edit advanced configuration settings to increase the number of connections per Sametime module.

**About this task**

The **ST_DB_LDAP_CONNECTIONS_NUMBER** setting increases the number of concurrent connections from the IBM Sametime Community Server to the LDAP server(s) specified in the StConfig.nsf per Sametime module. The default setting is set to one connection per module except for StAuthentication.dll, which has two connections.

Before increasing the value to greater than one consider the following points:

- Assume that **ST_DB_LDAP_CONNECTIONS_NUMBER=3**. Note that a value of 3 means that the Sametime Community Server creates $3^N$ connections to the LDAP server, where $N$ stands for the number of Sametime components that have an open connection to LDAP. In addition, meeting and Domino components are connected to LDAP so the overall number of connections is greater than $3^N$.

- This setting should only be modified if requests are taking an exceptionally long time to process due to long processing queues and there are plenty of resources available on the Sametime Community Server and the LDAP server. Increasing the value of this setting increases the number of LDAP threads available to service the request and multiplies the resource requirements for each one of the Sametime LDAP modules.

**Tuning the Sametime LDAP Keep Alive Interval setting**

You can manage advanced configuration settings to make sure that there is consistent traffic over the LDAP connection

Specify the **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting in the [Directory] section of the sametime.ini file.

The **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting defines the duration (in minutes) to wait while keeping alive messages that are sent by the IBM Sametime Community Server on idle LDAP connections. Its default value is set to 1 minute.
ST_DB_LDAP_KEEPALIVE_INTERVAL is an LDAP-based dummy search message whose purpose is to avoid the LDAP server or any network device along the way between the Sametime Community Server and the LDAP server from closing idle connections. This setting is needed in certain LDAP environments where the LDAP server abruptly closes or resets the LDAP connection between Sametime Community Server and LDAP due to no traffic activities on this connection per interval of time set by the LDAP server. To avoid this situation, make sure that there is consistent traffic over the connection by turning on the ST_DB_LDAP_KEEPALIVE_INTERVAL setting.

**Tuning the Sametime LDAP Respray Interval setting**

You can manage advanced configuration settings to set how often the connection to the LDAP server should be dropped and re-established.

The ST_DB_LDAP_RESPRAY_INTERVAL setting in the [Directory] section of the sametime.ini file defines the frequency, in minutes, that the connection to the LDAP server should be dropped and then re-established. In pre-8.5 versions of Sametime 8.5, the RESPRAY interval must be higher than the KEEPALIVE interval. By default, the ST_DB_LDAP_RESPRAY_INTERVAL setting is disabled.

**Note:** In pre-8.5 versions of Sametime, the RESPRAY interval must be higher than the KEEPALIVE interval. Bear in mind that the RESPRAY operation is an expensive resource task, and might impact performance in an environment where the RESPRAY intervals are set to low values.

**Tuning the Sametime LDAP Maximum Number of Results per Search Query setting**

You can manage advanced configuration settings to define the LDAP maximum number of results per search query.

Specify the ST_DB_LDAP_MAX_RESULTS setting in the [Directory] section of the sametime.ini file to define the maximum number of entries that can be returned in a single search when searching for people or groups. The default value is 1000.

**Tuning the Sametime LDAP Minimum Number of Characters to Match setting**

You can manage advanced configuration settings to define the minimum number of characters in the search string required to perform a search.

The ST_DB_LDAP_MIN_WILDCARD setting in the [Directory] section of the sametime.ini file defines the minimum number of characters to match when searching the LDAP user using wild card characters. When trying to resolve a user or group with a name that is too short than that defined by the ST_DB_LDAP_MIN_WILDCARD setting, the IBM Sametime Community Server does not search the LDAP server.

For more information on sametime.ini file settings related to the LDAP directory and other techniques for tweaking the Sametime server behavior, refer to these two articles on the IBM Sametime wiki:

- Optimizing Sametime's Name Lookup solution
- Best Practices for using LDAP with Sametime

These articles provide information about fine-tuning a directory to achieve optimal performance and streamlined connections for Sametime.
Advanced settings to control contact list size

You can manage advanced configuration settings for controlling contact list size.

The **MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT** setting in the **[Config]** section of the **sametime.ini** file limits the number of users that the client can subscribe to, or see awareness on. A public group is counted as one subscription. This limit is published as a server attribute, and the client is responsible for enforcing it. In order to enforce this limit on the server, set the **IGNORE_SUBSCRIBES_ABOVE_MAX** value in the **[Config]** section of the **sametime.ini** file.

The **ST_GROUPS_MAX_MEMBERS** setting in the **[Directory]** section of the **sametime.ini** file limits the maximum number of users that the IBM Sametime Community Server will allow in a public group. A public group that is too big will appear empty. Once a group is marked too big, it will remain this way until the server is restarted, even if its contents have changed in the directory to less than the maximum. Set the value to be a number from 1 - 1000. 1,000 members is the maximum recommended group size. You should not set a value of 0 (zero), which indicates the feature is off.

Policies and **MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT**

The **Limit contact list size** and **Contacts** policy settings control the size of the contact list and do not restrain subscriptions. For example, you can set this to 5 and open chat history which has 200 contacts, and the client subscribes to 205 users. If you set this to 5 and the user has 100 contacts on the list already, it does not remove anyone, but it prompts the user to do so. The **MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT** limits the client so it does not subscribe to users beyond this limit.

**Sametime.ini file**

```ini
[Config]
MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT=750
IGNORE_SUBSCRIBES_ABOVE_MAX=751

[Directory]
ST_GROUPS_MAX_MEMBERS=900
```

**Sametime Unified Telephony considerations**

For Sametime Unified Telephony environments the following settings must be applied:

*Table 43. Sametime Unified Telephony*

<table>
<thead>
<tr>
<th>Sametime server version</th>
<th><strong>IGNORE_SUBSCRIBES_ABOVE_MAX</strong> default Value</th>
<th><strong>IGNORE_SUBSCRIBES_ABOVE_MAX</strong> required settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0.x</td>
<td>-1 (disabled)</td>
<td><strong>Must be</strong> -1. The setting can be omitted from <strong>sametime.ini</strong>, or explicitly set to -1.</td>
</tr>
<tr>
<td>8.5.x</td>
<td>-1 (disabled)</td>
<td><strong>Must be</strong> -1. The setting can be omitted from <strong>sametime.ini</strong>, or explicitly set to -1.</td>
</tr>
</tbody>
</table>
Setting a Sametime Polling "Keep Alive" interval for client requests

You can have the Sametime Polling service keep a client request alive for a certain number of second in cases where a temporary connection loss prevents an immediate response. The setting applies to clients who connect through HTTP and use the Sametime Polling service.

About this task

The VP_MAX_PENDING_TIME setting in the [Polling] of the sametime.ini file defines the interval (in seconds) to keep messages pending that are sent by the client. Its default value is set to 0 seconds, which keeps a request pending indefinitely. When the VP_MAX_PENDING_TIME is set to a value larger than 0, the Sametime Polling service sends a response to the client after the specified number of seconds.

### Sametime.ini file

```
[Config]
VP_MAX_PENDING_TIME=10
```

Tuning Sametime Media Manager

Complete the following tuning procedures to enhance performance.

**Before you begin**

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

**Limiting participants in a video conference**

The default maximum number of participants in a single audio-only or video conferences is set to 20. You can adjust this number up or down to accommodate specific network consumption requirements.

About this task

Network factors affecting audio and video services include bandwidth and latency. The more bandwidth available to the server and the shorter latency will allow more participants per call. The bandwidth to the server is recommended at least 1Gbps (Gigabit per second), and latency from client to server should be less than 150ms.

Environmental conditions affecting audio and video services include server capacity, total number of simultaneous users, selected audio codec and video resolution, expected number of interactive participants, expected number of video participants, and expected number of simultaneous calls. These conditions will effect the limit of the number of participants per call.

Edit the ConferenceManager.properties for every Conference Manager and change the MaximumVideoConferenceUsers value to a number participants appropriate for your network and the environmental conditions at your site.
**Procedure**

1. On the server hosting the Sametime Media Manager Conference Manager component, navigate to the following directory:

   ```
   WAS_INSTALL_ROOT/profiles/STMSAppProfile/installedApps/cell_name/
   ConferenceFocus.ear/ConferenceFocus.war
   ```

2. Open the `ConferenceManager.properties` file for editing.

3. Locate the section shown here:

   ```
   #
   # MaximumAudioConferenceUsers is the maximum number of users the service provider supports for each audio conference call.
   #
   MaximumAudioConferenceUsers=20
   #
   # MaximumVideoConferenceUsers is the maximum number of users the service provider supports for each video conference call.
   #
   MaximumVideoConferenceUsers=20
   ```


5. Save and close the file.

6. Restart the server so the change can take effect.

7. Repeat this process on every Conference Manager component. If you have a clustered deployment, apply to every cluster member.

**Setting a retry interval for client connections**

The IBM Sametime SIP Proxy and Registrar allows clients to keep trying to connect until they are successful. The default retry interval is 120 seconds, but you can edit the default value for `ClientSIPRegisterRetryDelay` in the `stavconfig.xml` file.

**Procedure**

1. On the Deployment Manager for the Media Manager’s Conference Manager, open the `stavconfig.xml` file for editing. Use the Deployment Manager profile.

2. Set the retry interval in seconds as the value for `ClientSIPRegisterRetryDelay`. The default is 120 seconds.

   For example, to increase the retry interval to 180 seconds, add this value:

   ```xml
   <configuration lastUpdated="1226425838277" name="ClientSIPRegisterRetryDelay" value="180"/>
   ```

3. Save and close the file.

4. In a clustered environment, you must change all instances of the `stavconfig.xml` file in the Deployment manager profile. Repeat the previous steps for all other instances of the file.

5. Synchronize all nodes in the cell:
   a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Nodes**.
   b. Click **Full Resynchronize**.
Related concepts:
“Authentication by token using the Domino Single Sign-On (SSO) feature” on page 342
The Domino Single Sign-On (SSO) feature must be enabled on the Sametime server. This feature creates Lightweight Third Party Authentication (LTPA) tokens that enable web browser users to log in a single time to access multiple Sametime, Domino, or IBM WebSphere servers that are in the same DNS domain. This capability is called “single sign-on.”

Related tasks:
“Setting up single sign-on (SSO) for Sametime clients” on page 335
Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

Modifying the dynamic port range to improve Packet Switcher performance
Make sure that the port range is available for the IBM Sametime Media Manager Packet Switcher

About this task
The default range of audio and video ports on the Packet Switcher might fall in the range of dynamic port for the system. If the port is already allocated by a system process when the Packet Switcher tries to allocate it for a conference, the packet switcher marks this as a bad port and will not use this port again, until after restart. If too many ports in the range get marked as bad ports, this could lead to performance degradation. You can change the default port range by using the Sametime System Console (Sametime System Console > Sametime Servers > Sametime Media Manager > deployment_name) or in the stavconfig.xml.

Procedure
To determine UDP dynamic port range, type the following command from the command line:
Windows 2008:
netsh int ipv4 show dynamicport udp

For Windows 2003, use 1025 as your start port and use 3975 as your end port for both TCP and UDP.
Linux:
cat /proc/sys/net/ipv4/ip_local_port_range

Setting log files size and rotation for the Sametime Media Manager
You can specify the maximum size and number of log files to be stored on the IBM Sametime Media Manager.
Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the Sametime Media Manager retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file "Maximum Size" (shown in the table below) to more than 20MB.

About this task

Complete these steps using the Integrated Solutions Console on the Sametime Media Manager where the logs will be stored. If you installed Sametime Media Manager components on separate machines or as separate cell profiles, you must adjust the log file information on all Conference Manager and Packet Switcher servers.

Procedure

1. In the Integrated Solutions Console for the Sametime Media Manager component, click Servers > Server Types > WebSphere application servers > STMediaServer.
4. Under "General Properties," update the following fields both for System.out and System.err sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click OK.
6. Return to Additional Properties.
8. Click File and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click OK.
10. Click Save to save these changes to the master configuration.
11. If the Sametime Media Manager is clustered, repeat these steps for each node within the cluster.
Setting log files size and rotation for the SIP Proxy and Registrar

You can specify the maximum size and number of log files to be stored on the server.

Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the SIP Proxy and Registrar retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file "Maximum Size" (shown in the table below) to more than 20MB.

About this task

Complete these steps using the Integrated Solutions Console on the SIP Proxy and Registrar where the logs will be stored.

Procedure

1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere application servers > STMediaServer.
4. Under "General Properties," update the following fields both for System.out and System.err sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click OK.
6. Return to Additional Properties.
8. Click File and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click OK.
10. Click Save to save these changes to the master configuration.
Tuning Sametime Bandwidth Manager

Complete the following tuning procedures to enhance performance.

Tuning the SIP Session timeout on the Sametime Bandwidth Manager

You can set the amount of time the IBM Sametime Bandwidth Manager leaves inactive calls connected by setting a timeout value in the Bandwidth Manager Configuration page.

About this task

Sametime uses SIP heartbeats to detect if a user has been disconnected and these heartbeats keep a session active. Because of these SIP heartbeats, an inactive session timeout does not occur under normal circumstances on an active call even if the parties are not actively speaking for longer than the timeout interval. Nonetheless, in order to prevent stale sessions from remaining in the system in the event of heartbeat failure, set this value to a reasonably short timeframe of 1 hour (which is the default).

Procedure

1. In the Integrated Solutions Console for the Sametime Bandwidth Manager component, click Sametime Servers > Bandwidth Manager.
2. Navigate to the “Configuration” tab.
3. Change the “Inactive Session Timeout” to a specific number of minutes, such as 60. “0” means no timeout.

Setting log files size and rotation for the Sametime Bandwidth Manager

You can specify the maximum size and number of log files to be stored on the IBM Sametime Bandwidth Manager

Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the Sametime Bandwidth Manager retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file “Maximum Size” (shown in the table below) to more than 20MB.

About this task

Complete these steps using the Integrated Solutions Console on the Sametime Bandwidth Manager where the logs will be stored.

Procedure

1. In the Integrated Solutions Console for the Sametime Bandwidth Manager, click Servers > Server Types > WebSphere application servers > Bandwidth_manager_name.
4. Under "General Properties," update the following fields both for System.out and System.err sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click OK.
6. Return to Additional Properties.
8. Click File and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click OK.
10. Click Save to save these changes to the master configuration.
11. If the Sametime Bandwidth Manager is clustered, repeat these steps for each node within the cluster.

**Configuring automatic thread dumps for hung threads for the Sametime Bandwidth Manager**

To help troubleshoot hung processes and performance slowdowns, configure your IBM Sametime Bandwidth Manager to generate a thread dump automatically when the servers detect hung threads.

**About this task**

Follow these steps to create a custom property to automatically generate a thread dump when a hung thread is detected. Repeat these steps for each server. In the case of a clustered environment, repeat these steps on all Sametime Bandwidth Manager servers in the cluster.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Servers > Server Types > WebSphere application servers.
3. In the table listing the WebSphere application servers, click the link representing the server you want to modify.
5. Supply the name of the custom property:
   com.ibm.websphere.threadmonitor.dump.java
6. Set the value to true.
7. Click OK, and then click Save to save changes to the master configuration.

---

**Tuning a Sametime Gateway Server**

Complete the following tuning procedures to enhance performance. Set the thread pool and the Java virtual machine (JVM) garbage collection policy. Fine tune the SIP proxy service settings and modify the Data Replication Services on a cluster. Some procedures must be repeated on each server in a cluster.

**Before you begin**

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

**Limiting Sametime Gateway global and community-level sessions**

You can limit the number of sessions that a particular server supports, or choose to leave the sessions unrestricted.

Whenever a user subscribes to be notified of another user's status changes; a presence session object is created. Whenever two users start a new chat, an instance messaging session object is created. These session objects take up considerable space in memory. To avoid a scenario in which a very high level of user activity might cause an out-of-memory error to occur, set the maximum session property to a predefined limit that you know is supported. In the event of these limits being reached, the server will not create any new sessions, but will continue to serve existing sessions.

**IBM Sametime Gateway global limits and Community limits**

There are two configuration levels regarding the maximum sessions limit in Sametime Gateway: global limits and community limits. The global limit will be enforced on all communities in your Sametime Gateway deployment as a whole (that is, the sum of all the external communities’ sessions cannot exceed the global limit). The community limit is applied to a specific Sametime Gateway community and helps ensure that a single community doesn’t use up all of the available memory for its own sessions while blocking others from creating new sessions. If you have only one community, then there is no need to specify community limits; specifying global limits is enough.

In a cluster, the maximum number of sessions is applied to each node, so the true maximum is the number of nodes multiplied by the maximum sessions value; for example, if your cluster has two nodes and your maximum sessions is set to 5000, then your cluster actually supports a maximum of 2 * 5000 = 10,000 sessions.

**Note:** If you set a community’s session limits to a value higher than the overall global limit, the global limit will still be enforced.

**Setting a global limit on sessions**

You should set a global limit for the maximum number of sessions allowed on a server, which helps prevent out-of-memory errors. The value set here will supersede a larger value set in the “Route maximum sessions” property.
About this task

The procedure that follows sets a global limit for the maximum number of sessions allowed at one time on a particular server. The global limit that you specify here will be enforced on all communities in your IBM Sametime Gateway deployment as a whole (that is, the sum of all the external communities sessions cannot exceed the global limit).

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Gateway Properties.
2. Select Set maximum sessions.
   Deselect the box if you do not want to limit instant messaging and presence sessions.
3. Set the maximum sessions for instant messaging by typing an integer.
   Assuming max JVM heap was set to 1.5GB, the recommended value is 8,000 for a single server deployment.
4. Set the maximum sessions for presence by typing an integer.
   Assuming max JVM heap was set to 1.5GB, these are the recommended values:
   - For a single server, or a cluster instance without SIP session replication enabled, the recommended value is 100,000.
   - For a cluster instance with SIP session replication enabled, the recommended value is 100,000.
5. Click Apply.
6. Restart the Sametime Gateway server; if you have a cluster of Sametime Gateway servers, restart the cluster.

Related reference:
“Sametime Gateway properties” on page 151
Use this page to set the maximum chat sessions. You can also specify domains from which to block messages.

Setting a community-level limit on sessions in Sametime Gateway

You can limit the maximum number of sessions allowed on a server by each community in IBM Sametime Gateway, which helps prevent out-of-memory errors. The total sessions for individual communities on a particular server contribute to that server’s “global” total number of sessions.

Before you begin

If you have more than one external community, there are a number of factors to consider when deciding on community-level maximum session limits. The following table shows different strategies for choosing community limits:
### Scenario Settings Comments

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Settings</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Scenario 1 | global max=10  
community A max=5  
community B max=5 | Because G=10, there cannot be more than 10 sessions in a community.  
Pros: An overloaded community (A=5) will not interfere with community B reaching its own specified maximum (B=5).  
The server resources are not fully utilized: even if community A uses less than 5 sessions, community B cannot use more than its own limit of 5 sessions. |

| Scenario 2 | global max=10  
community A max=10  
community B max=10 | Because G=10, there cannot be more than 10 sessions in a community.  
Pros: The server resources are fully used; if community A uses less than 5 sessions then community B could use more than 5 sessions.  
Cons: Communities are not insulated and protected from each other. If community A has 8 sessions, then community B can only have 2 sessions (since G=10). |

**Attention:** In a cluster, the maximum number of sessions is applied to each node, so the true maximum is the number of nodes multiplied by the maximum sessions value; for example, if your cluster has two nodes and your maximum sessions is set to 5000, then your cluster actually supports a maximum of 2 * 5000 = 10,000 sessions.

### About this task

The procedure that follows sets community-level limits for the maximum number of sessions allowed at one time on a particular server.

**Expected state:**
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.

### Procedure

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. In the "Communities" table, select a community for which you want add or change session limits.
3. Select **Set maximum sessions for the route**.  
   Deselect this option if you do not want to limit the number of instant messaging and presence sessions.
4. Set the maximum sessions for instant messaging by typing an integer.  
The recommended value is the matching global value divided by the number of external communities, though you may choose a different limits strategy.
5. Set the maximum sessions for presence by typing an integer.  
The recommended value is the matching global value divided by the number of external communities, though you may choose a different limits strategy.
6. Click Apply.
7. Restart the Sametime Gateway server; if you have a cluster of Sametime
   Gateway servers, restart the cluster.

What to do next

Note: If you set either (or both) of the community's session limits to a value higher
than the overall global limit, the global limit will still be enforced.

Specifying connection attempts and a time out when
connecting with the local Sametime server

You can optionally set properties for when the IBM Sametime Gateway server
becomes disconnected from the local Sametime community server. You can set how
many times Sametime Gateway should try to reconnect to the local Sametime
community server. Also, you can set the time to wait between attempts to
reconnect.

About this task

When the Sametime Gateway server is disconnected from the Sametime server, by
default Sametime Gateway tries to reconnect for one minute, then stops, then tries
again to reconnect. This process goes on indefinitely unless you change these
defaults by creating two custom properties, one for reconnection attempts and the
other for the reconnection time out.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. In the table that lists communities, click the Local community.
3. On the local community panel, click Custom properties, and then click New.
4. To set the number of reconnection attempts, in the name field, type Server
   reconnection attempts.
5. In the value field, type -1 (to try infinitely), or some other number.
6. Click OK.
7. To set the reconnection time out, in the name field, type Server reconnection
time out.
8. In the value field, type a number in milliseconds. For example, type 30000 to
   set the time out to 30 seconds.
9. Click OK.
10. Restart the Sametime Gateway server, or, if you have a cluster of Sametime
    Gateway servers, restart the cluster.

Related reference:

“Custom properties details” on page 164
Use this page to edit custom properties for a community, translation protocol, or
message handler. You can also specify new properties that are needed to configure
third-party elements used by the IBM Sametime Gateway.

Setting thread pool values

Set the thread pool values for an IBM Sametime Gateway server and the SIP
container to improve performance between the SIP container and the Sametime
Gateway application server layer. By using a thread pool, server components can reuse existing threads, which helps improve performance by reducing the overhead of creating new threads at run time.

**Procedure**

1. From Integrated Solutions Console, click **Servers > Server Types > WebSphere application servers > RTCGWServer**, and then under Additional Properties, click **Thread Pools**.
2. Click **New**, and then type a name of your choice, such as **STGWPool**, in the **Name** field.
3. Type 30 in the **Minimum Size** field.
4. Type 30 in the **Maximum Size** field.
5. Keep the default value of 5000 for thread inactivity.
6. Click **OK**, and click **Save** to save changes to the master configuration.
7. Click **Servers > Server Types > WebSphere application servers > RTCGWServer**, and under Container Settings, select **SIP Container Settings > SIP Container**.
8. From the dropdown list of **Thread pool**, select the thread pool that you just created.
9. Set Maximum dispatch queue size to 5000.
10. Keep the default values of 120000 for **Maximum application sessions**, and 5000 for **Maximum messages per averaging period**.
11. Click **OK**, and click **Save** to save changes to the master configuration.
12. If Sametime Gateway is clustered, repeat the preceding steps for each node of the cluster.

**Configuring automatic thread dumps for hung processes**

To help troubleshoot hung processes and performance slowdowns, configure your IBM Sametime Gateway servers and XMPP/SIP Proxy servers to generate a thread dump automatically when the servers detect hung threads.

**About this task**

Follow these steps to create a custom property to automatically generate a thread dump when a hung thread is detected. Repeat these steps for each Sametime Gateway and XMPP/SIP Proxy servers. In the case of a clustered environment, repeat these steps on all Gateway servers and XMPP/SIP Proxy servers in the cluster.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Servers > Server Types > WebSphere application/proxy servers**.
3. In the table listing the WebSphere application and proxy servers, click the link representing the proxy server you want to modify.
4. Under **Server Infrastructure**, click **Administration > Custom Properties**. Then click **New**.
5. Supply the name of the custom property: `com.ibm.websphere.threadmonitor.dump.java`
6. Set the value to **true**.
7. Click **OK**, and then click **Save** to save changes to the master configuration.
Setting the JVM garbage collection policy

Set the following required JVM arguments and memory settings for all of your IBM Sametime Gateway server instances. The instructions in this topic are not applicable to any of the SIP Proxy instances you might have.

About this task

Attention: Do not set the following JVM garbage collection policy on SUN Solaris machines, otherwise you will not be able to start Sametime Gateway.

Procedure

1. From Integrated Solutions Console, click Servers > Application Servers > RTCGWServer.
4. In the Generic JVM arguments field, enter the following value as one continuous line. (It has been formatted with line breaks to fit into this page format.)
   -Xgcpolicy:gencon -Xgc:scvNoAdaptiveTenure,scvTenureAge=8,stdGlobalCompactToSatisfyAllocate
   -Xmn256m -Xverbosegclog:${SERVER_LOG_ROOT}/gc.log,1,14000

   The Generic JVM arguments must be entered as a single continuous line, despite the fact that it might have been broken into several lines due to documentation formatting limitations. If the user this is split into multiple lines, the server will not start up.
5. In the Initial Heap Size field, enter 1500.
6. In the Maximum Heap Size field, enter 1500.
7. Click OK, and click Save to save changes to the master configuration.
8. If IBM Sametime Gateway is clustered, repeat the preceding steps for each node of the cluster.

Setting log files size and rotation

You can specify the maximum size and number of log files to be stored on the server.

Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the IBM Sametime Gateway server retain a history at least 2 GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file "Maximum Size" (shown in the table below) to more than 20 MB.

About this task

Complete these steps using the Integrated Solutions Console on the Sametime Gateway server where the logs will be stored.

Procedure

1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere application servers > RTCGWServer.
4. Under “General Properties,” update the following fields both for System.out and System.err sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20 MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>A value of 2 is the recommended maximum.</td>
</tr>
</tbody>
</table>

5. Click OK.
6. Return to Additional Properties.
8. Click File and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20 MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>A value of 15 is the recommended maximum.</td>
</tr>
</tbody>
</table>

9. Click OK.
10. Click Save to save these changes to the master configuration.
11. If Sametime Gateway is clustered, repeat these steps for each node within the cluster.

**Related tasks:**
“Setting a diagnostic trace on Sametime Gateway” on page 416
You can specify how the server handles Sametime Gateway log records. You can select a Sametime Gateway server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

### Setting threshold warnings for monitoring server load

Set up a warning so that a message appears when the maximum number of subscriptions or instant messaging sessions is approached. This is useful for monitoring server load due to instant messaging and subscriptions.

**About this task**

Create custom properties that define two threshold values: one for instant messaging sessions, and one for subscriptions. Whenever either of these values is reached, the warning message will appear in the log.

**Expected state:**
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.
Procedure
1. In the Integrated Solutions Console, open the Custom properties page for the server.
   • On a single server: Click Servers > Server Types > WebSphere application servers > server_name > Server Infrastructure > Administration > Custom Properties.
   • On a clustered server: Click System administration > Cell > Custom Properties
2. Click New and enter the following information for the subscriptions threshold warning:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>com.ibm.sametime.gateway.max.subscriptions.warning.threshold</td>
</tr>
<tr>
<td>Value</td>
<td>A number representing the threshold value (the maximum number of subscriptions allowed before the warning message is generated in the log).</td>
</tr>
<tr>
<td>Description</td>
<td>Threshold warning message for maximum subscriptions</td>
</tr>
</tbody>
</table>

3. Click OK to save the new custom property.
4. Click New again, and enter the following information for the instant messaging threshold warning:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>com.ibm.sametime.gateway.max.im.warning.threshold</td>
</tr>
<tr>
<td>Value</td>
<td>A number representing the threshold value (the maximum number of instant messages allowed before the warning message is generated in the log).</td>
</tr>
<tr>
<td>Description</td>
<td>Threshold warning message for maximum instant messaging sessions</td>
</tr>
</tbody>
</table>

5. Click OK to save this new custom property.
6. Restart the Sametime Gateway server; if you have a cluster of Sametime Gateway servers, restart the cluster.

Tuning the WebSphere SIP proxy server for a Sametime Gateway cluster
This sections describes the steps for tuning a WebSphere SIP proxy server for a Sametime Gateway cluster.

About this task
Tune the JVM garbage collection policy for the WebSphere SIP proxy server as follows:

Procedure
1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers > SIPProxyServer.
2. Perform the following instructions for each of the sip proxies in the list:
   a. Select a proxy server by clicking it in the list.
   d. In the Initial Heap Size field, enter 600.
   e. In the Maximum Heap Size field, enter 600.
   f. In the Generic JVM arguments field, enter the following value as one continuous line:
      
      -Xmn150m -Xgcpolicy:gencon -Xgc:noAdaptiveTenure,tenureAge=8,
      stdGlobalCompactToSatisfyAllocate -Xtgc:parallel
   g. Click OK, and click Save to save changes to the master configuration.

Resolving email addresses as Sametime IDs more efficiently

You can configure a custom Java class filter to ensure the efficient resolving of email address as IBM Sametime IDs (STId).

About this task

When you process an external user request to interact with an internal user, the Sametime Gateway requests that the Sametime Community Server interpret (resolve) the internal user’s email address as the internal user’s Sametime ID (STId). The Sametime Community Server resolves the STId, by searching LDAP with the user’s email as the search filter. Multiple simultaneous queries could lead to a performance issue. Sametime Gateway is expected to report slow resolve behavior with messages like the following one:

CLFRC0268W
Performance warning: The resolve operation: Email --> STId ( {0} --> {1} )
 took {2} seconds to complete. Review your community server and/or LDAP configuration, and consult the Sametime Gateway Infocenter.
Awaiting {3} more resolve requests to complete.

Procedure

To ensure an effective LDAP search, verify that you have a configured a custom Java class that can generate an efficient email to STId LDAP search. Using the Sametime Community Server default LDAP search leads to degraded performance caused by a full scan of the LDAP tree. The example StLdapCustomized class described in Creating custom Java classes for searching the LDAP provides an efficient way to resolve email to STId. You might also consider limiting the base DN in which to search. See one of the steps in Sametime prerequisite: Connecting to an LDAP server on configuring a base DN.

What to do next

As an additional step for optimizing the LDAP searches on the Community server, you can also include or exclude certain domains from user and group directory lookups.

Tuning a WebSphere proxy server

This section contains procedures for tuning a WebSphere proxy server that is used by a cluster of IBM Sametime servers running on WebSphere Application Server.
About this task

Note that this section is not referring to the SIP Proxy, but rather to a WebSphere proxy server.

Disabling the proxy read-ahead mechanism on the WebSphere proxy server

You can disable the read-ahead mechanism on the IBM WebSphere proxy server to resolve a HIGH CPU issue that occurs when terminating connections with read-ahead enabled.

Procedure

1. Log in to the Integrated Services Console.
2. Click Servers > Server Types > WebSphere proxy servers.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
5. Click Proxy settings.
6. Under Additional Properties, click Custom properties.
7. Click New to create a custom property.
8. Specify the Name of the new property as http.connectionPoolReadAheadEnabled.
9. Set the Value of the new property to false.
10. Click New to create another custom property.
11. Specify the Name of the new property as dynacache.extension.lookup_timeout_property.
12. Set the Value of the new property to 20000.
13. Click Apply, and then click Save.

Adjusting the WebSphere proxy server thread pool settings

Increase the WebContainer thread pool settings of the IBM WebSphere proxy server to match the same settings as the IBM Sametime Meeting Server.

About this task

A thread pool lets servers reuse threads instead of creating new threads at run time.

Procedure

1. Log in to the Integrated Services Console.
2. Click Servers > Server Types > WebSphere proxy servers.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
5. Click Proxy.
6. Under General Properties, make sure the Minimum Size and Maximum Size are both set to 50 threads.
7. Click Apply, and then click Save.
**Setting JVM verbose garbage collection and heap sizes on the WebSphere proxy server**

In order to monitor IBM WebSphere Application Server JVM heap for specific applications, enable the JVM verbose garbage collection logging for the WebSphere Application Servers.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Servers > Server Types > Websphere proxy servers**.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
5. Click **Process definition**.
6. Under **Additional properties**, click **Java Virtual Machine**.
7. Under **General Properties**, make sure the **Verbose garbage collection** check box is cleared.
8. Under **General Properties**, make sure the **Initial heap size** is set to 512MB.
9. Under **General Properties**, make sure the **Maximum heap size** is set to 1024MB.
10. Click **Apply**, and then click **Save**.

**Extending the HTTP persistent timeout on the WebSphere proxy server**

You can extend the HTTP persistent timeout on the IBM WebSphere proxy server to stay connected longer.

**Before you begin**

**About this task**

The default rtc4web timeout value is 30 seconds. This is the default timeout for the WebSphere proxy server persistent timeout setting, too. This can causes a rare condition to occur where both sides of the connection can let go at the same time. In order to minimize this conflict, extend the WebSphere proxy server HTTP Persistent timeout to stay connected longer.

**Procedure**

1. Log into Integrated Solutions Console on the server where the WebSphere proxy server is configured.
2. Click **Servers > Server Types > WebSphere proxy servers**.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
4. Under **Proxy Settings**, expand the **HTTP Proxy Server Settings** tree.
5. Click **Proxy server transports**.
6. Click **HTTP_PROXY_CHAIN**. It should be associated with port 80.
7. Click **HTTP inbound channel (HTTP 3)**.
8. Under **General Properties**, set the **Persistent timeout** to 60 seconds.
9. Click **Apply**, and then click **Save**.
10. Click **Servers > Server Types > WebSphere proxy servers**.
11. Click the name of the proxy server.
12. Under Proxy Settings, expand the HTTP Proxy Server Settings tree.
13. Click Proxy server transports.
14. Click HTTPS_PROXY_CHAIN. It should be associated with port 443.
15. Click HTTP inbound channel (HTTP 4).
16. Under General Properties, set the Persistent timeout to 60 seconds.
17. Click Apply, and then click Save.
18. Repeat for every WebSphere proxy server that you configured for the cluster.
Chapter 3. Security

After setting up your initial IBM Sametime environment, you may want to make additional changes to safeguard information at your site, including limiting user access to certain features, using encryption, and modifying default security settings.

This section contains information about securing your Sametime servers running on Domino and WebSphere Application Server.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server deployments.

Working with Sametime servers that are enabled for SSL

Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

Configuring Sametime Community Server to use SSL encryption

Configure IBM Sametime Community Server to use SSL (Secure Socket Layer) for its services; and configure HTTPS when communicating with Web clients or enable LDAPS (LDAP over SSL) with LDAP server.

About this task

You can encrypt communications for Sametime Services and the communication between Sametime and web browsers. You can also encrypt communications between an LDAP server and the Sametime server with the LDAPS protocol.

You can set up either, or both, of these protocols independently. If you are upgrading from a previous release, take steps to upgrade the GSKit and iKeyMan utility as described in the related topic.

Enabling encryption for Sametime Services, and between Sametime and web browsers

Configure SSL encryption for IBM Sametime Services and enable HTTPS for Web browsers.

About this task

Enabling SSL encryption with the HTTPS (browser-based) protocol involves the following tasks:

Preparing Lotus Domino to use SSL:

Because IBM Sametime resides on an IBM Lotus Domino server, you must enable the Lotus Domino server's HTTP component to support Secure Socket Layer (SSL) before you can configure the Sametime server to encrypt communications.
About this task

Follow these steps in the Lotus Domino Administrator information center to set up a Lotus Domino server to support SSL for HTTP connections:

Setting up SSL on a Domino server

Preparing Sametime to use SSL:

Set up SSL encryption on the IBM Sametime server by importing the SSL certificate used by IBM Lotus Domino and configuring the Sametime server to use it.

About this task

Install the GSKit and use the IKeyMan program to create a keystore on the Sametime server before you import the Lotus Domino server’s SSL certificate and complete configuration changes to enable support for SSL. Complete the following tasks in the sequence shown:

Setting up a keystore for the SSL certificate used by Lotus Domino:

Install the IBM GSKit with the IBM IKeyMan utility and then create a keystore file to hold the IBM Lotus Domino server’s SSL certificate.

About this task

Sametime on IBM i already includes a keystore file called stkeys.jks, so you can skip this procedure and proceed directly to obtain and import a copy of the SSL certificate from the Lotus Domino server into the Sametime server.

On IBM AIX, Linux, Solaris, and Microsoft Windows, you must create the keystore file yourself by completing the following tasks:

Installing GSKit on the Sametime Community Server:

To configure the server for SSL, you must install the most recent release of GSKit provided with IBM Sametime. Install GSKit on the IBM Sametime Community Server.

Installing GSKit on a Sametime Community Server (AIX):

Install GSKit on a server that runs on IBM AIX.

About this task

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on AIX, follow the steps below:

Procedure

1. Log on to the server as the root user.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit directory to a temporary location on the server.
   Open this release’s Download document at the following web address:
4. Expand the GSKit package.

5. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
   a. Change to the directory into which you expanded the package.
   b. Uncompress the .tar files by using the following commands:

   ```
   zcat gsckrypt32-version_number.aix.ppc.tar.Z | tar -xf -
   zcat gsckssl32-version_number.aix.ppc.tar.Z | tar -xf -
   ```

   The string `version_number` represents the version number of GSKit being installed, such as 8.0.14.6, and can vary as new modifications of GSKit are released.
   c. Install GSKit v8 by using the following command:

   ```
   inutoc /tmp/gsk8
   installp -acgw -d /tmp/MQ/gsk8 GSKit8.gsckrypt32.ppc.rte \ 
   GSKit8.gsckssl32.ppc.rte \
   GSKit8.gsckrypt32.ppc.rte \
   GSKit8.gsckssl32.ppc.rte \
   /tmp
   ```

   `/tmp` represents the directory into which you expanded the package.

6. Set the `JAVA_HOME` environment variable to the Java VM installed under the Sametime binaries directory:

   ```
   JAVA_HOME=/opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/
   ```

---

**Installing GSKit on a Sametime Community Server (Linux):**

Install GSKit on a server that runs on Linux.

**About this task**

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on Linux, follow the steps below:

**Procedure**

1. Log on to the server as the root user.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit directory to a temporary location on the server.

   Open this release's Download document at the following web address:

   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

4. Expand the GSKit package into a temporary directory.

5. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:

   a. Change to the temporary directory where you expanded the GSKit package.
   b. Install the packages into the `usr/lib` directory by using the following command:

   ```
   rpm -Uv -ivh /usr/lib gsckrypt32-version_number.linux.arch.rpm gsckssl32-version_number.linux.arch.rpm
   ```

   The string `version_number` represents the version number of GSKit being installed, such as 8.0.14.6, and can vary as new modifications of GSKit are released.

   The string `arch` represents your system architecture, for example x86.

6. Set the `JAVA_HOME` environment variable to the Java VM installed under the Sametime binaries directory:
JAVA_HOME=/opt/ibm/lotus/notes/latest/linux/ibm-jre/jre export JAVA_HOME

Installing GSKit on a Sametime Community Server (Solaris):

Install GSKit on a server that runs on Solaris.

About this task

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on Solaris, follow the steps below:

Procedure
1. Log on to the server as the root user.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit package to a temporary location on the server.
   Open this release's Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
4. Expand the GSKit package.
5. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
   a. Change to the directory into which you expanded the package.
   b. Uncompress the .tar files by using the following commands:
      
      zcat gskcrypt32-version_number.sun.sparc.tar.Z | tar -xf 
      zcat gskssl32-version_number.sun.sparc.tar.Z | tar -xf 

      The string version_number represents the version number of GSKit being installed, such as 8.0.14.6, and can vary as new modifications of GSKit are released.
   c. Install GSKit v8 by using the following command:
      pkgadd -d. gsk8cry32 gsk8ssl32 gsk8cry64 gsk8ssl64
6. Set the JAVA_HOME environment variable to the java VM installed under the Sametime binaries directory:
   JAVA_HOME=/opt/ibm/lotus/notes/latest/sunspa/ibm-jre/export JAVA_HOME

Installing GSKit on a Sametime Community Server (Windows):

Install the GSKit on a server that runs on Windows.

About this task

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on Microsoft Windows, follow the steps below:

Procedure
1. Log on to the server as the Windows administrator.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit directory to a temporary location on the server.
   Open this release's Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
4. Extract the GSKit package to a temporary directory.
5. Open a command prompt and navigate to the path of the temporary directory.
6. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
   a. Double-click the gsk8crypt32.exe file and follow the installation prompts, and progress through the wizard following the prompts until the product is successfully installed.
   b. Repeat for the gsk8ssl32.exe file.
7. Set the JAVA_HOME environment variable to the Java VM installed under the
   Sametime binary directory:
   a. From the Windows desktop, right click on the My Computer icon and select System Properties.
   b. In the "System Properties" dialog box, select the Advanced tab.
   c. Click the Environment Variables button.
   d. In the "New System Variable" dialog box, click the New button under the "System Variables" list, and enter the following information:

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Variable value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAVA_HOME</td>
<td>Sametime_install_root\ibm-jre\jre</td>
</tr>
</tbody>
</table>
   e. Click OK to close the "New System Variable" dialog box.
   f. Click OK to close the "Environment Variables" dialog box.
   g. Click OK to close the "System Properties" dialog box.

Updating the .jar files for the iKeyMan utility:
The iKeyMan utility on the IBM Sametime Community Server requires a specific version of the Java runtime environment and updated .jar and java security files for this release.

Procedure
1. On the Sametime Community Server, download and Install Java 1.6 SR 3 from the Java web site into a java6sr3 directory.
2. Navigate to the Sametime_install_root\ibm-jre\lib\ext directory.
3. Find gskikm.jar and ibmcmprovider.jar, back them up in a different folder, but with the same names. Then remove them from the ext directory.
4. Copy gskikm.jar and ibmcmprovider.jar from java6sr3\jre\lib\ext to the Sametime_install_root\ibm-jre\jre\lib\ext directory.
5. Use a text editor to add com.ibm.security.cmskeystore.CMSPublisher to the list of providers in the java.security file as follows:
   a. Navigate to the Sametime_install_root\ibm-jre\jre\lib\security directory. For example:
      AIX
      /opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre/lib/security
      Linux
      /opt/ibm/lotus/notes/latest/linux/ibm-jre/jre/lib/security/
      Solaris
      /opt/ibm/lotus/notes/latest/sunspa/ibm-jre/jre/lib/security/
      Windows
b. Open the `java.security` file.

c. In the `java.security` file, and add the following statement to the list of security providers as shown, where `number` is the last sequence number in the list.

```java
security.provider.number=com.ibm.security.cmskeystore.CMSProvider
```

The example below illustrates this line added to the `java.security` file (notice that the preference numbers must be in sequence):

```java
## List of providers and their preference orders (see above)#
security.provider.1=com.ibm.jsse.IBMJSSEProvider
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.security.jgss.IMBJGSSProvider
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=com.ibm.security.cmskeystore.CMSProvider
#
```

d. Close and save the file.

Creating a keystore file for the Domino server’s SSL certificate:

Use the IBM IKeyMan utility to create a keystore .jks file on the IBM Sametime Community Server, which will be used for storing a copy of the IBM Lotus Domino server’s SSL certificate.

About this task

On IBM AIX, Linux, and Solaris, create a keystore file called `keys.jks`; on Microsoft Windows, call it `stkeys.jks`.

Note: On IBM i, if the keystore already exists; skip this procedure.

Follow these steps to create a keystore file on the Sametime Community Server:

Procedure

1. Open a command prompt and navigate to the `Sametime_install_root\ibm-jre\jre\bin` directory. For example:
   
   **AIX**
   
   `/opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre/bin`
   
   **Linux**
   
   `/opt/ibm/lotus/notes/latest/linux/ibm-jre/jre/bin`
   
   **Solaris**
   
   `/opt/ibm/lotus/notes/latest/sunspa/ibm-jre/jre/bin`
   
   **Windows**
   
   `C:\Program Files\Lotus\Domino\ibm-jre\jre\bin`
   
   2. Start the IKeyMan program by running the following command:

   **AIX, Linux, and Solaris**
   
   `java com.ibm.gsk.ikeyman.Ikeyman`
   
   **Windows**
   
   `ikeyman.exe`
   
   3. Click **Key Database File > New**.
   
   4. In the "New" dialog box, complete these fields and then click **OK**:
### Obtaining a copy of the SSL certificate used by Lotus Domino:

When the IBM Lotus Domino server is configured to use SSL, an SSL server certificate is received from a Certification Authority (CA) and merged into the Lotus Domino Server Certificate Admin database. When you configure SSL for IBM Sametime, you import a copy of this certificate to the Sametime server.

#### About this task

There are two versions of the SSL certificate that you can use:

- **Obtaining the SSL certificate directly from the Lotus Domino server:**

  When configuring SSL for IBM Sametime, you can import a copy of the SSL certificate directly from the IBM Lotus Domino server.

#### About this task

When the Lotus Domino server was configured to use SSL, an SSL server certificate was received from a Certification Authority (CA) and merged into the Lotus Domino Server Certificate Admin (certsrv.nsf) database. In this procedure, you export a copy of that certificate and save it as a file so that you can import it into Sametime in a later task.

#### Procedure

1. Open a browser and navigate to the Lotus Domino server where you enabled SSL.
Note: The steps below use the Microsoft Internet Explorer browser; steps for your own browser may differ.

You can locate the Lotus Domino server by navigating to the Sametime server that is hosted on the same computer, using an address similar to the following (replace Sametime.acme.com with your fully qualified Internet host name):

https://Sametime.acme.com

2. Install the SSL certificate in Microsoft Internet Explorer to ensure it is available for export:
   a. When prompted to "select the certificate to use when connecting," click OK.
   b. At the "Security Alert" dialog box, click View Certificate.
   c. At the "Certificate" dialog box, click Install Certificate.
   d. At the "Certificate Manager Import Wizard" screen, click Next.
   e. Click the **Automatically select the certificate store based on the type of certificate** option, and then click Next.
   f. Back at the "Certificate Manager Import Wizard" screen, click Finish.
   g. When the message indicating that the SSL server certificate was imported successfully appears, click OK repeatedly until you have closed all of the dialog boxes.

3. Now export the SSL certificate from Internet Explorer and save it as a file.
   a. From the browser, click **Tools > Internet Options**.
   b. Click the **Contents** tab.
   c. Click the **Certificates** button.
   d. Click the **Other People** tab.
   e. Scroll down the list of certificates and select the server certificate that you imported earlier in this procedure.
      The certificate name should provide some indication that the certificate is associated with the Domino server from which it was imported. For example, if the certificate was imported from a server named Sametime.acme.com, the certificate might be issued to "Sametime" or to "Example."
   f. Click the **Export** button.
   g. At the "Certificate Manager Export Wizard" screen, click Next.
   h. At the "Certificate Export File" screen, select **Base64 encoded X.509 (.CER)**, and then click Next.
   i. At the "Export File Name" screen, provide a name for the file, select the Sametime server's data directory as the location where you want to store the file, and then click Next.
      For example, on Windows, you might enter SSLservercertificate.cer as the file name, and select C:\Lotus\Domino\data as the location.

      **Note**: On IBM i, save the file directly to your server if you have mapped to the server drive. Otherwise, save the file on your client workstation and transfer it to your IBM i server later.

   j. When the message appears indicating the export was successful, click OK.

**Obtaining a copy of the trusted root certificate:**

If you are unable to obtain a copy of the IBM Lotus Domino server's SSL certificate, you can request a trusted root certificate from a CA or export a trusted root certificate from your web browser.
About this task

If you need to obtain a trusted root certificate, you must obtain the same trusted root certificate that is used by the Domino server to sign the Domino SSL server certificate. For example, if the VeriSign Class 4 Public Primary Certification Authority trusted root certificate is used to sign the Domino SSL server certificate, you must either export this certificate from your web browser or request a VeriSign Class 4 Public Primary Certification Authority trusted root certificate from VeriSign.

There are two ways to obtain a copy of the trusted root certificate:

Obtaining a trusted root certificate from the web browser:

When configuring SSL for the IBM Sametime server, you can import a copy of the trusted root certificate that was used for signing the IBM Lotus Domino server's own SSL certificate from a web browser, and then import it in the Sametime server's keystore.

About this task

Rather than obtaining a copy of the Lotus Domino server's own SSL certificate, you may choose to obtain a copy of the trusted root certificate that was used for signing the Lotus Domino server's certificate. The easiest way to obtain a trusted root certificate is to export one from your web browser.

Web browsers include many different SSL trusted root certificates by default. If your Web browser contains a trusted root certificate that corresponds with the Lotus Domino server's trusted root certificate that was used to sign the Lotus Domino SSL server certificate, you can export it from the browser and save it as a file.

Note: You must use the same trusted root that signed the Lotus Domino server's own SSL certificate.

The procedure below illustrates how you can export a trusted root certificate from a Microsoft Internet Explorer web browser:

Procedure

1. From the browser, click Tools > Internet Options.
2. Click the Contents tab.
3. Click the Certificates button.
4. Select the Trusted Root Certification Authorities tab.
5. Select the appropriate trusted root certificate from the list.
6. Click the Export button.
7. At the ‘Certificate Manager Export Wizard” screen, click Next.
8. At the ‘Certificate Export File” screen, select Base64 encoded X.509 (.CER), and then click Next.
9. At the “Export File Name” screen, provide a name for the file, select the Sametime server’s data directory as the location where you want to store the file, and then click Next.

For example, on Windows, you might enter SSLservercertificate.cer as the file name, and select C:\Lotus\Domino\data as the location.
Note: On IBM i, save the file directly to your server if you have mapped to the server drive. Otherwise, save the file on your client workstation and transfer it to your IBM i server later.

10. When the message appears indicating that the export was successful, click OK.

Obtaining a trusted root certificate from the Certification Authority:

When configuring SSL for the IBM Sametime server, you can obtain a copy of the trusted root certificate used for signing the IBM Lotus Domino server’s SSL certificate from the original Certificate Authority.

About this task

If you are unable to obtain a copy of the Lotus Domino server’s SSL server certificate, you can request a copy of the trusted root certificate from a CA.

Normally, you request a certificate from a CA by browsing to the CA’s website. For example, follow these steps to request a certificate from VeriSign:

Procedure

1. Open a browser and navigate to the VeriSign site:
   
   www.verisign.com

2. Follow the instructions on the website to request a certificate.
   
   Once the certificate request is approved, you will receive an email explaining how to pick up the certificate.

3. Pick up the certificate as instructed (for example, by browsing to the website and copying it from a field on the specified page).
   
   You can provide a file name for the certificate when receiving it from the CA and then store it in the Sametime server’s data directory.

Importing the Lotus Domino server’s SSL certificate into the keystore:

After you obtain a copy of either the IBM Lotus Domino server’s own SSL certificate, or the trusted root certificate that was used to sign it, import your copy into the IBM Sametime server’s keystore.

About this task

The procedure for importing the SSL certificate depends on your operating system:

Importing an SSL certificate on AIX, Linux, Solaris:

To enable SSL for IBM Sametime running on IBM AIX, Linux, or Solaris, import the IBM Lotus Domino server’s SSL certificate into the keystore.

Before you begin

Make sure you have copied one of the following certificates from the server into the Sametime server’s data directory:

- CA.txt (the trusted root certificate)
- Server.txt (the SSL server certificate)
About this task

Follow the steps below to import the SSL certificate into the keystore on the Sametime server:

Procedure

1. Verify that the `ikeyman.sh` file's SAMETIME_HOME variable specifies the correct path for your server's installation directory, modifying it as needed.
   The default installation directories for Sametime are as follows:
   - **AIX**: `/opt/ibm/lotus/notes/latest/ibmpow`
   - **Linux**: `/opt/ibm/lotus/notes/latest/linux`
   - **Solaris**: `/opt/ibm/lotus/notes/latest/sunspa`
2. Make sure the `ikeyman.sh` file has execute privileges.
3. Start the `ikeyman.sh` utility.
   The `ikeyman.sh` utility requires a graphical interface. If you run it in a text-only terminal, be sure to redirect the display to an x-windows session.
4. Click the **Add** button.
5. In the "Add CAs certificate from a File" dialog box, do the following:
   a. Verify that **Base64-encoded ASCII data** is selected as the "Data type".
   b. Set the Certificate file name to the name of the text file (for example, `CA.txt`) into which you copied the certificate.
   c. Set the **Location** to the location to which you transferred the `CA.txt` file in the previous procedure (for example, `/local/notes/data`).
   d. Click **OK**.
6. Close IKeyMan after the file is imported successfully.

**Importing an SSL certificate on IBM i**:

To enable SSL for IBM Sametime running on IBM i, import the IBM Lotus Domino server's SSL certificate into the keystore.

**Before you begin**

Make sure you have copied one of the following certificates from the server into the Sametime server's data directory:
- **CA.txt** (the trusted root certificate)
- **Server.txt** (the SSL server certificate)

**About this task**

Follow the steps below to import the SSL certificate into the keystore on the Sametime server:

**Procedure**

1. From an IBM i command line, run the following command to start qshell:
   ```
   strqsh
   ```
2. From qshell, run the following keytool command:
   ```
   keytool -import -alias certificate_name
   -file certificate_filename
   -storepass keystore_password
   -keystore keystore_path_and_filename
   ```
Where:

- `certificate_name` is `CA.txt`
- `certificate_filename` is also `CA.txt`
- `keystore_password` is "sametime."

**Note:** On IBM i versions of Sametime, `stkeys.jks` is provided by default and uses "sametime" as the default password

- `keystore_path_and_filename` is `stserver/data/stkeys.jks`

Example:
```
keytool -import -alias stserver1cert
    -file /stserver/data/CA.txt
    -storepass sametime
    -keystore /stserver/data/stkeys.jks
```

3. After you have imported the certificate, use the following command to view the list of certificates in the `stkeys.jks` file and verify that the certificate was imported successfully:
```
keytool -list -storepass keystore_password
    -keystore keystore_path_and_filename
```

Example:
```
keytool -list -storepass sametime
    -keystore /stserver/data/stkeys.jks
```

4. Press **F3** to exit qshell.

**Importing an SSL certificate on Windows:**

To enable SSL for IBM Sametime running on Microsoft Windows, import the IBM Lotus Domino server's SSL certificate into the keystore.

**Before you begin**

Make sure you have copied one of the following certificates from the server into the Sametime server's data directory:

- CA.txt (the trusted root certificate)
- Server.txt (the SSL server certificate)

**About this task**

Follow the steps below to import the SSL certificate into the keystore on the Sametime server:

**Procedure**

1. Open a command prompt and navigate to the `Sametime_install_root\ibm-jre\jre\bin` directory.
   
   The default installation path for Sametime is `C:\Lotus\Domino`.
2. Start the IKeyMan utility by running the `ikeyman.exe` program.
3. Browse to and select the `stkeys.jks` key store file.
4. Enter the password required to access this file.
5. In the "Key database content" area, select Signer certificates.
6. Click the **Add** button.
7. In the "Add CAs certificate from a File" dialog box, do the following:
   a. Verify that **Base64-encoded ASCII data** is selected as the "Data type"
b. Browse to and select the SSL certificate you want to import.
c. Click OK.

8. In the "Enter a Label" dialog box, do the following:
   a. Type a label for the certificate.
      This label identifies the certificate in the Signer Certificates list of the IBM
      IKeyMan program.
   b. Click OK.
      The new certificate's label appears in the list of Signer Certificates.

10. Close the IKeyMan utility.

*Modifying the Sametime server configuration for SSL:*

Modify the configuration of the IBM Sametime server to encrypt connections.

**About this task**

Modify the Sametime server's configuration by making changes to the
sametime.ini file. The necessary changes vary with your operating system:

*Modifying the Sametime configuration on AIX, Linux, Solaris:

Modify the IBM Sametime server's sametime.ini file on IBM AIX, Linux, or Solaris
to support Secure Socket Layer (SSL) encryption.

**About this task**

To modify the Sametime configuration, complete the following steps:

**Procedure**

1. Stop the Sametime server.
2. Use a text editor to open the sametime.ini file.
   This is located in the Sametime installation directory.
3. Locate the `ConfigurationPort=` setting. Make sure that it specifies the port on
   which the Lotus Domino HTTP server listens for SSL connections (by default,
   this is port 443), modifying the setting if necessary.
   For example:
   ```
   ConfigurationPort=443
   ```
4. If these settings are not present in the [Config] section at the bottom of the
   sametime.ini file, manually type them in:
   ```ini
   [Config]
   ConfigurationSSLEnabled=true
   javax.net.ssl.keyStore=/local/notesdata/key.jks
   javax.net.ssl.trustStore=/local/notesdata/key.jks
   javax.net.ssl.keyStorePassword=keystore_password
   javax.net.ssl.trustStorePassword=truststore_password
   ```
   **Note:** Specify the complete path name of the key.jks file for both the
   `javax.net.ssl.keyStore` and the `javax.net.ssl.trustStore` settings. Specify
   the password that you provided for key.jks when you created it for both the
   `javax.net.ssl.keyStorePassword` and `javax.net.ssl.trustStorePassword`
   settings.
5. If these two lines appear in the sametime.ini file, remove them:
javax.net.ssl.trustStoreType=JKS
javax.net.ssl.keyStoreType=JKS

6. Save and close the sametime.ini file.
7. Restart the Sametime Community Server.

Modifying the Sametime Configuration on IBM i:

Modify the IBM Sametime server's sametime.ini file on IBM i to support Secure Socket Layer (SSL) encryption.

About this task

To modify the Sametime configuration for IBM i, complete the following steps:

Procedure

1. Stop the Sametime server.
2. Use a text editor to open the sametime.ini file.
   This is located in the Sametime server's data directory.
3. Locate the ConfigurationPort= setting. Make sure that it specifies the port on which the Lotus Domino HTTP server listens for SSL connections (by default, this is port 443), modifying the setting if necessary.
   For example:
   ConfigurationPort=443
4. If these settings are not present in the [Config] section at the bottom of the sametime.ini file, manually type them in:
   [Config]
   ConfigurationSSLEnabled=true
   javax.net.ssl.keyStore=stkeys.jks
   javax.net.ssl.trustStore=stkeys.jks
   javax.net.ssl.keyStorePassword=sametime
   javax.net.ssl.trustStorePassword=sametime
   
   Note: By default, the password for the stkeys.jks file is "sametime." If you change the password for stkeys.jks, you must change the setting of both javax.net.ssl.keyStorePassword and javax.net.ssl.trustStorePassword to match the new password. The full path for the stkeys.jks file is not needed for the IBM i version of Sametime.
5. Save the sametime.ini file.
6. Restart the Sametime server.

Modifying the Sametime configuration on Windows:

Modify the IBM Sametime server's sametime.ini file on Microsoft Windows to support Secure Socket Layer (SSL) encryption.

About this task

To modify the Sametime configuration for Windows, complete the following steps:

Procedure

1. Stop the Sametime server.
2. Use a text editor to open the sametime.ini file, which is located in the Sametime server installation directory (for example: C:\Program Files\lotus\domino).
3. Verify that the "ConfigurationPort=" setting specifies the port on which the Lotus Domino HTTP server listens for SSL connections (default port is 443).
   For example:
   ConfigurationPort=443

4. Verify that the [Config] section contains the following settings (or modify as needed):
   
   [Config]
   ConfigurationSSLEnabled=true
   javax.net.ssl.keyStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
   javax.net.ssl.trustStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
   javax.net.ssl.keyStorePassword=passw0rd
   javax.net.ssl.trustStorePassword=passw0rd

   Where:
   • For the javax.net.ssl.keyStore and the javax.net.ssl.trustStore settings, you specify the complete path name for the stkeys.jks file.
   • For the javax.net.ssl.keyStorePassword and the javax.net.ssl.trustStorePassword settings, you specify the password that you provided for the stkeys.jks file when you created it.

5. Save and close the sametime.ini file.

6. Start the Sametime server.

Tunneling through the firewall when SSL is enabled:

Configure an IBM Sametime server to allow clients to tunnel through a firewall when SSL is enabled.

Before you begin

Sametime Connect clients communicate with the Sametime server by directing messages to the HTTP server, which listens on port 80. When SSL is enabled, port 443 is normally used for sending encrypted messages; however, the Lotus Domino server (which hosts Sametime) is already listening on port 443 for encrypted Web-based communications. If Sametime Connect clients also send messages to the HTTP server on port 443, a conflict arises.

You can work around this conflict by configuring clients to access the Sametime server by tunneling to its Community Services multiplexer with an HTTPS proxy. In this type of configuration, both the Sametime Community Server and the Lotus Domino server listen for connections on port 443 – but they use different addresses to avoid conflicts. You set up this type of connection by assigning an additional IP address to the Sametime server, and then configuring both the Community Services multiplexer and your clients to use that address when communicating on port 443.

The following picture shows an example of this type of connection:
Restriction: This connection is not encrypted. In addition, clients using this connection will not have access to the Meeting Server and the web server, so Meeting services, as well as audio and video services, are not supported in this configuration.

About this task

If you want to allow clients to tunnel to the Community Services multiplexer on port 443 when SSL is enabled, complete the following tasks:

*Binding the base DNS to the HTTP server:*

Before assigning an additional IP address to an IBM Sametime server, avoid potential conflicts by binding the server's base DNS to the HTTP server where it listens for communications. This ensures that the IBM Lotus Domino server hosting Sametime (and using this HTTP server) still receives all communications intended for it.

About this task

Bind the server's base DNS to the HTTP server by completing the following steps:

Procedure

1. On the Sametime server, open the Sametime Administration Tool.
2. Click Configuration > Connectivity > Networks and Ports.
3. On the "Networks and Ports" page, click Configure HTTP services on a web page in its own window.
   The "HTTP" section of the Lotus Domino Directory's Server document opens in a separate window.
4. Locate the Host name field.
5. Under the "Basics" heading, type the base DNS for the HTTP server (for example: sametime1.acme.com).
6. Still in the same field, type a comma and the following IP address: 127.0.0.1 so it looks like this: sametime1.acme.com,127.0.0.1
   This additional entry is required for enabling the Sametime Administration Tool to operate in this configuration.
7. Click the Save & Close button at the top of the Server document.
Adding a new IP address to the Sametime server:

Assign an additional IP address to an IBM Sametime server.

Before you begin

To add a new IP address to a Sametime server, you can either install an additional Network Interface Card (NIC) or assign multiple IP addresses to a single NIC. For additional information, see IBM Tech Note #1181387, "Forcing a Sametime server with multiple NICs to bind to the correct IP address," at: www.ibm.com/support/docview.wss?rs=899&uid=swg21181387

About this task

To assign multiple IP addresses to a single NIC on server running Microsoft Windows:

Procedure
1. Open the Windows Control Panel.
2. Click the Protocols tab.
3. Click TCP/IP Protocols > Properties > Specify an IP Address.
4. Click the Advanced tab.
5. Use the "Advanced IP Addressing" page to assign multiple IP addresses to a single NIC.
6. Save your changes and close all of the dialog boxes.

Mapping the IP address and DNS for Community Services:

Configure an IBM Sametime server to map an IP address to the specific DNS and port used by Sametime Community Services.

Before you begin

You must have already assigned the IP address to the Sametime server.

Procedure

Set up your DNS server to map the new IP address to a new DNS name for the Sametime server's Community Services.
To avoid confusion, it is recommended that your new DNS for the Community Services use the old DNS name plus "community-" as a prefix. For example, if your base DNS for the server is sametime1.example.com, use the following name for the new DNS:

community-sametime1.example.com

Configuring HTTPS tunneling settings for clients using port 443:

Configure the IBM Sametime Community Services to listen for client communications using the new DNS and port 443.

Before you begin

You must have already assigned an additional IP address to the Sametime server, then mapped a new DNS to it for use by the Community Services.
Procedure

1. On the Sametime server, open the Sametime Administration Tool.
2. Click Configuration > Connectivity > Networks and Ports.
3. On the "Networks and Ports" page, click Community Services Network > Address for HTTPS-tunneled client connections and fill in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>community-base_DNS</td>
</tr>
<tr>
<td></td>
<td>For example, if your base DNS for the server is sametime1.example.com, type the following name for the new DNS: community-sametime1.example.com</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
</tbody>
</table>

4. Restart the Sametime and Lotus Domino servers.
5. Close the Sametime Administration Tool.

Results

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

Connecting clients to the new Community Services DNS:

Configure an IBM Sametime Connect client to communicate with a Sametime server that is listening for HTTPS connections using the host name (DNS) and port that you specified in the HTTPS tunneling settings for the server.

About this task

Every Sametime Connect client located outside of the firewall requires this configuration to tunnel through the firewall to the Sametime Community Services.

Procedure

For each Sametime Connect client, configure the following settings in the "Sametime Connectivity" tab:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Type the new DNS that you mapped to the IP address that will be used for the Community Server. For example, if your base DNS for the server is sametime1.example.com, it was recommended that you use the following name for the new DNS: community-sametime1.example.com That is the name you should type here.</td>
</tr>
<tr>
<td>Community port</td>
<td>443</td>
</tr>
<tr>
<td>Use proxy</td>
<td>Select this setting.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use HTTPS proxy</td>
<td>Select this setting and enter the host name (community-sametime1.example.com) and port (443) on which the Sametime Connect clients connect to the HTTPS proxy.</td>
</tr>
</tbody>
</table>

**Enabling encryption between Sametime and the LDAP server**

Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

**About this task**

When you enable this protocol, you can choose whether to encrypt only the data used for authenticating users in Sametime, or to encrypt all data that is transmitted between the two servers.

*Note:* If you are using an IBM Lotus Domino Directory and it is not configured as an LDAP directory, this section does not apply to you. You can skip these procedures.

Enabling SSL encryption for an LDAP server involves the following tasks:

**Enabling SSL on the LDAP server:**

You must enable SSL on your LDAP server before you can configure the IBM Sametime server to encrypt its communications with the LDAP directory.

**About this task**

*Note:* If you are using a Domino Directory and Sametime is not configured with an LDAP directory, this section does not apply to you and you should skip these procedures.

The procedure for enabling SSL depend on the LDAP directory that you use:

*Setting up a Lotus Domino LDAP directory to use SSL:*

You must enable the IBM Lotus Domino server’s LDAP component to support SSL before you can configure the IBM Sametime server to encrypt its communications with the Lotus Domino LDAP Server.

**About this task**

Follow these steps in the Lotus Domino Administrator information center to set up a Lotus Domino server to support SSL for LDAP connections:

*Setting up SSL on a Domino server*

*Enabling IBM Tivoli Directory Servers to use SSL:*

You must enable the LDAP server to support SSL before you can configure the IBM Sametime server to encrypt communications to the LDAP directory hosted on the IBM Tivoli® Directory Server.
About this task

Refer to the documentation provided by IBM Tivoli Directory Server for instructions on enabling SSL. The server must be running GSKit 7.0.4.29 or later. If it is not, you must upgrade to a later version.

Related tasks:
“Installing a supported release of GSKit on Tivoli Directory Server” on page 287
You should install the latest version of GSKit available on the IBM Tivoli Directory Server web site. At a minimum, you must upgrade to 7.0.4.28.

Related information:

Secure Sockets Layer (Tivoli Directory Server)

Enabling third-party LDAP servers to use SSL:

You must enable the LDAP server to support SSL before you can configure the IBM Sametime server to encrypt communications to the LDAP directory hosted on that server.

About this task

Refer to the documentation provided by the LDAP directory's vendor for instructions on enabling SSL.

Using SSL to encrypt connections between the Sametime and LDAP servers:

When Sametime is configured to connect to an LDAP server, the Sametime Community Server makes five separate connections to the LDAP server.

About this task

The Sametime Community Server makes a separate connection to the LDAP server to perform each of these five tasks:

- Authenticate users
- Resolve a user name to a distinguished name as part of the login procedure
- Resolve user and group names (for example, as a response to an "Add Person or Group" request from a Sametime Connect client)
- Browse the directory
- Get the content of public groups

The Sametime Community Server and LDAP servers exchange directory information, including user names and passwords, over these connections. To ensure this information is secure, the administrator can use SSL to encrypt the data that passes over these connections. The administrator should consider the level of protection required before enabling SSL. Using SSL to encrypt these connections can slow the server performance. The administrator has the following options when using SSL to encrypt the data transmitted between the Sametime and LDAP servers:

- **Encrypt all data** - This option encrypts all directory information (both user names and passwords) that is transmitted between the Sametime Community Server and the LDAP server. If you encrypt all data, all five connections between the Sametime Community Server and LDAP server are encrypted with SSL. This option provides the most security but also has the greatest affect on server performance.
- **Encrypt only user passwords** - This option encrypts passwords but not other directory information (such as user names) passing over the connections between the Sametime Community Server and LDAP servers. If you encrypt only user passwords, only the "authenticating users" connection between the Sametime server and the LDAP server is encrypted with SSL. This option provides an intermediate level of security and has less affect on server performance than encrypting all of the data.

- **Encrypt no data** - This option allows all directory information and passwords to pass unencrypted between the Sametime and LDAP servers. This option does not affect server performance and should be used if the administrator feels there is no chance that an unauthorized user can intercept information transmitted over the connections between the Sametime and LDAP servers.

- **Using SSL to encrypt connections between the Sametime servlet and LDAP**

- **Ensuring the Sametime Community Server trusts the LDAP server certificate on Windows and AIX/Solaris/Linux servers**

**Note:** If you are encrypting connections between an AIX version of the Sametime server and an LDAP directory, xIC.aix50.rte must be 6.0.0.3 (or higher).

**Setting up a keystore for the SSL certificate used by the LDAP server:**

On IBM AIX, Linux, Microsoft Windows, and Oracle Solaris, install the GSKit program and the IBM IKeyMan utility so you can store a copy of the LDAP server's SSL certificate. On IBM i, Sametime Community Server comes with the IKeyMan utility already installed, but you must install DCM software instead; the instructions are in this section.

**About this task**

The Sametime server must store a copy of LDAP Server's SSL trusted certificate to complete the SSL handshake when making an SSL connection to that LDAP server. Before you can import the SSL certificate from the LDAP Server, you will use the GSKit program and IKeyMan utility (the DCM program on IBM i) to create a keystore file on the Sametime server for storing the certificate.

**Note:** You only need to install these programs once. If you have already installed these programs during an earlier procedure, you can skip this task.

The instructions for installing GSKit and IKeyMan, or DCM, vary according to your server's operating system. Use the instructions in the appropriate topic:

*Installing and setting up Digital Certificate Manager on IBM i:*

Install and set up the DCM (Digital Certificate Manager) program on an IBM i server hosting IBM Sametime, and ensure that Sametime trusts the LDAP server's SSL certificate.

**About this task**

Set up DCM and ensure that Sametime trusts the LDAP server by completing the following tasks:

*Installing Digital Certificate Manager:*
Install the DCM (Digital Certificate Manager) program on an IBM i server that hosts IBM Sametime.

About this task

On IBM i, SSL certificates are managed using the integrated DCM program. You must install and set up DCM before you can establish SSL encryption for communications between the IBM i server’s LDAP client and the deployment’s LDAP server. All of the following software must be installed on the IBM i server where your Sametime server is located:

- 5722-SS1 Option 34, Digital Certificate Manager
- 5722-DG1, IBM HTTP Server
- 5722-AC3, Crypto Access Provider 128-bit

If you need more detailed information about setting up and using DCM in order to complete the steps in this section, see the IBM i information center at: www.ibm.com/as400/infocenter

After selecting the appropriate IBM i release and your preferred language, select the "Digital Certificate Manager" topic in the "Security" section.

Ensuring that the LDAP client trusts the LDAP server’s certificate:

Ensure that the IBM i LDAP client trusts the SSL certificate used by the LDAP server with which it communicates.

About this task

IBM Sametime for IBM i uses the LDAP client included with the IBM Directory Server that is installed as part of the IBM i operating system. Enable the LDAP client to trust the LDAP server by importing the server’s SSL certificate into the store on the client (the IBM i server) and then adding the Certificate Authority to the trust list.

Procedure

1. Use the DCM (Digital Certificate Manager) program to determine whether the CA Certificate that signed the LDAP directory server’s certificate is already included in the DCM *SYSTEM certificate store.

   Well-known public Internet Certificate Authorities (CA) that most web browsers can recognize readily, such as VeriSign, are already included in the DCM. If the appropriate CA is included in the certificate store, you have finished this task; skip the remaining steps.

   If the CA used by your LDAP server’s certificate does not appear in the DCM *SYSTEM certificate store, import it now by completing the remaining steps in this procedure.

2. Import the LDAP directory server’s certificate into the DCM *SYSTEM certificate store.

3. Use DCM to add the CA Certificate to the trust list of the IBM Directory Server LDAP client application.

   The application ID is QIBM_GLD_DIRSRV_CLIENT.

Ensuring that Sametime has access to the *SYSTEM certificate store:

Assign IBM Sametime access to the IBM i *SYSTEM certificate store.
About this task

Sametime must be able to access certificates located in the DCM *SYSTEM certificate store when connecting to an LDAP server using SSL. The DCM *SYSTEM certificate store is located in the /qibm/userdata/icss/cert/server directory on an IBM i server.

QNOTES is an IBM i user profile created by IBM Lotus Domino and used by Sametime. By default, the QNOTES user profile does not have access to the DCM *SYSTEM certificate store or the /qibm/userdata/icss/cert/server directory, although the higher level directories usually have *PUBLIC *RX authority which allows QNOTES to access those directories.

Provide Sametime with access to the *SYSTEM certificate store by completing the following step:

Procedure

1. Run the following command from any IBM i command line to view the contents of the /qibm/userdata/icss/cert/server directory and verify the name of the certificate store:
   By default, the certificate store is named default.kdb and uses “sametime” as the password.
   WRKLNK '/QIBM/USERDATA/ICSS/CERT/Server/*'

2. Run the following commands from any IBM i command line to ensure QNOTES has the necessary authority to the DCM *SYSTEM certificate store and associated directory:
   CHGAUTH OBJ('/QIBM/USERDATA/ICSS/CERT/Server') USER(QNOTES) DTAAUT(*RX)
   CHGAUTH OBJ('/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.RDB') USER(QNOTES) DTAAUT(*RX)
   CHGAUTH OBJ('/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.KDB') USER(QNOTES) DTAAUT(*RX)
   In this example:
   • QNOTES is the user receiving access
   • default.kdb is the name of the certificate store

Setting up GSKit, IKeyMan, and the key database on AIX, Linux, Solaris, Windows:

Install the GSKit program and the IBM IKeyMan utility on IBM AIX, Linux, Microsoft Windows, or Solaris and then use IKeyMan to create a key database for storing the LDAP server’s SSL certificate.

About this task

Install the programs and create the key database by completing the following tasks:

Installing a supported release of GSKit on Tivoli Directory Server:

You should install the latest version of GSKit available on the IBM Tivoli Directory Server web site. At a minimum, you must upgrade to 7.0.4.28.

About this task

Tivoli Global Security Kit (GSKit) is an optional software package included with Tivoli Directory Server. You can enable the SSL feature by installing the IBM GSKit package. For instructions about installing GSKit 8, see the Tivoli Directory Server 6.3 information center.
Creating a keystore database for the LDAP server's SSL certificate:

The Sametime Community Server must store a copy of the IBM Lotus Domino server's SSL trusted root certificate to complete the SSL handshake when making an SSL connection to a browser-based client. Before you can import the SSL certificate from the Lotus Domino server, use the GSKit and IKeyMan utility to create a keystore file on the Sametime Community Server for storing the certificate. This procedure applies to IBM AIX, Linux, Microsoft Windows, or Oracle Solaris, but does not apply to IBM i. The keystore database is not used by Sametime on IBM i.

Before you begin

Update the iKeyMan utility and add com.ibm.security.cmskeystore.CMSProvider to the java.security file before you begin this procedure to enable the required CMS key database type used in this procedure.

About this task

Use the IBM iKeyMan utility to create a keystore database of type "cms" on the IBM Sametime Community Server. The keystore database that you create for storing the LDAP server's SSL certificate is different from the keystore file used for storing the Lotus Domino server's SSL certificate and must use a different file name. Create the keystore database by completing the following steps:

Procedure

1. Start the IBM IKeyMan utility:
   a. Open a command prompt and navigate to the Sametime_install_root/ibmjre/jre/bin directory.
      The default installation path for Sametime is as follows:
      • AIX: /local/notesdata
      • Linux: /local/notesdata
      • Solaris: /local/notesdata
      • Windows: C:\Program Files\IBM\Lotus\Domino
      • 64-bit Windows: C:\Program Files (x86)\IBM\Lotus\Domino
   b. Run the ikeyman.sh or ikeyman.exe program.
2. From the iKeyMan utility's menu, click Key Database > File > New.
3. In the "New" dialog box, fill in the following fields and click OK:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key database type</td>
<td>CMS key database file</td>
</tr>
<tr>
<td>File name</td>
<td>key.kdb</td>
</tr>
</tbody>
</table>

Note: If you enabled the HTTPS protocol, make sure that this keystore database's file name is different from that file name, to avoid conflicts.
### Option Description

<table>
<thead>
<tr>
<th>Location</th>
<th>Enter the path to the directory where the <code>sametime.ini</code> file is stored. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX:</td>
<td><code>/local/notesdata</code></td>
</tr>
<tr>
<td>Linux:</td>
<td><code>/local/notesdata</code></td>
</tr>
<tr>
<td>Solaris:</td>
<td><code>/local/notesdata</code></td>
</tr>
<tr>
<td>Windows:</td>
<td><code>C:\Program Files\IBM\Lotus\Domino</code></td>
</tr>
<tr>
<td>64-bit Windows:</td>
<td><code>C:\Program Files (x86)\IBM\Lotus\Domino</code></td>
</tr>
</tbody>
</table>

4. In the "Password" dialog box, fill in the following fields and click **OK**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password you will use for accessing this keystore database.</td>
</tr>
<tr>
<td><strong>Confirm password</strong></td>
<td>Confirm the password by typing it again.</td>
</tr>
<tr>
<td><strong>Stash the password to a file?</strong></td>
<td>You must click this option to enable it.</td>
</tr>
</tbody>
</table>

**Results**

The following key files are created in the Sametime directory: `key.kdb`, `key.sth`, and `key.rdb`.

**Importing a copy of the LDAP server's trusted root certificate:**

Import a copy of the LDAP server's trusted root SSL certificate into the keystore database on the IBM Sametime server to encrypt communications between Sametime and the LDAP server.

**Before you begin**

When the `key.kdb` database is created, it contains several trusted root (or "signer") certificates by default. If a trusted root certificate used by the LDAP server exists in the `key.kdb` database by default, then you can skip this procedure.

If the `key.kdb` database does not contain an appropriate trusted root certificate by default, you must obtain a trusted root certificate from the appropriate CA and add it to the `key.kdb` database.

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime server's data directory. The data type should be **Base64-encoded ASCII**. The file format can be `.cer`, `.p12` or `.txt`.

**About this task**

The procedure for importing the trusted root certificate depends on your operating system:

**Importing a trusted root certificate on AIX, Linux, Solaris:**

To enable SSL between IBM Sametime running on IBM AIX, Linux, or Solaris and an LDAP server, import the server's trusted root certificate into the key database.
Before you begin

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime Community Server's data directory. The data type should be **Base64-encoded ASCII**. The file format can be .CER, .p12 or .txt. You use this file in the following procedure.

About this task

Follow the steps below to import the SSL certificate into the key database on the Sametime server:

Procedure

1. Verify that the `ikeyman.sh` file's `SAMETIME_HOME` variable specifies the correct path for your server's installation directory, modifying it as needed.
   
   The default installation directories for Sametime are as follows:
   
   - **AIX**: `/local/notes/data`
   - **Linux**: `/local/notes/data`
   - **Solaris**: `/local/notes/data`

2. Make sure the `ikeyman.sh` file has execute privileges.

3. Start the `ikeyman.sh` utility.

   The `ikeyman.sh` utility requires a graphical interface. If you run it in a text-only terminal, be sure to redirect the display to an x-windows session.

4. Open the key.kdb file.

5. Click the **Add** button.

6. In the "Open" dialog box, do the following:
   
   a. Browse to and select the file into which you copied the SSL certificate in the last procedure (for example, CA.txt).
   
   b. Click **OK**.

7. In the "Enter a Label" dialog box, do the following:
   
   a. Type a label for the certificate.

   This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program.

   b. Click **OK**.

   The new certificate's label appears in the list of Signer Certificates.

8. Close the keystore file.

9. Close the IKeyMan utility.

**Importing a trusted root certificate on IBM i:**

To enable SSL between IBM Sametime running on IBM i and an LDAP server, import the server's trusted root certificate into the keystore file.

Before you begin

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime server's data directory. The data type should be **Base64-encoded ASCII**. The file format can be .CER, .p12 or .txt.
Follow the steps below to import the SSL certificate into the keystore file on the Sametime server:

Procedure
1. From an IBM i command line, run the following command to start qshell:
   `strqsh`
2. From qshell, run the following keytool command:
   ```
   keytool -import -alias certificate_name
   -file certificate_filename
   -storepass keystore_password
   -keystore keystore_path_and_filename
   ```
   Where:
   * `certificate_name` is CA.txt
   * `certificate_filename` is also CA.txt
   * `keystore_password` is "sametime."
   
   **Note:** On IBM i versions of Sametime, the keystore is called "stkeys.jks" and uses "sametime" as the default password
   * `keystore_path_and_filename` is stserver/data/stkeys.jks
   Example:
   ```
   keytool -import -alias stserver1cert
   -file /stserver/data/CA.txt
   -storepass sametime
   -keystore /stserver/data/stkeys.jks
   ```
3. After you have imported the certificate, use the following command to view the list of certificates in the stkeys.jks file and verify that the certificate was imported successfully:
   ```
   keytool -list -storepass keystore_password
   -keystore keystore_path_and_filename
   ```
   Example:
   ```
   keytool -list -storepass sametime
   -keystore /stserver/data/stkeys.jks
   ```
4. Press F3 to exit qshell.

Importing a trusted root certificate on Windows:

To enable SSL between IBM Sametime running on Microsoft Windows and an LDAP server, import the server's trusted root certificate into the key database.

Before you begin

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime Community Server's data directory. The data type should be **Base64-encoded ASCII**. The file format can be .CER, .p12 or .txt. You use this file in the following procedure.

About this task

Follow the steps below to import the SSL certificate into the key database on the Sametime server:
Procedure
1. Open a command prompt and navigate to the `Sametime_install_root\ibm-jre\jre\bin` directory.
   The default installation directories for Sametime are as follows:
   - **Windows**: `C:\Program Files\IBM\Lotus\Domino`
   - **64-bit Windows**: `C:\Program Files (x86)\IBM\Lotus\Domino`
2. Start the IKeyMan utility by running the `ikeyman.exe` program.
3. Browse to and select the `key.kdb` key database.
4. Enter the password required to access this file.
5. In the "Key database content" area, select Signer certificates.
6. Click the **Add** button.
7. In the "Open" dialog box, do the following:
   a. Browse to and select the file into which you copied the SSL certificate in the last procedure (for example, CA.txt).
   b. Click **OK**.
8. In the "Enter a Label" dialog box, do the following:
   a. Type a label for the certificate.
      This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program.
   b. Click **OK**.
      The new certificate's label appears in the list of Signer Certificates.
10. Close the IKeyMan utility.

**Configuring Directory Assistance for SSL:**

Modifying the IBM Lotus Domino Directory Assistance document is required when you use SSL to encrypt data transmitted between the IBM Sametime and the LDAP server. This procedure is needed when you are using Sametime Classic Meetings, using the Sametime Community Server.

**About this task**

In this procedure, you modify the Directory Assistance document for the LDAP server to ensure that the connection between the Sametime server and the LDAP server is encrypted using SSL.

**Procedure**
   a. Click **File > Database > Open**.
   b. For the Server, select **Local**.
   c. Select the **Directory Assistance** database (da.nsf).
   d. Click **Open**.
2. In the Directory Assistance database, double-click the Directory Assistance document for the LDAP server to open the document.
3. Click **Edit Directory Assistance**.
4. Next, click the **Basics** tab.
5. In the **Make this domain available to** field, select **Notes Clients & Internet Authentication/Authorization**.
6. Now click the **LDAP** tab.
7. Fill in the following fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel encryption</td>
<td>Select SSL.</td>
</tr>
</tbody>
</table>
| Port                                        | Specify the same port that appears in the **LDAP SSL port** field of the "LDAP Directory - Connectivity" options in the Sametime Administration Tool.  

This port is the one on which the LDAP server listens for SSL connections; the default is port 636. |
| Accept expired SSL certificates             | Select Yes (the default setting) to accept a certificate from the LDAP directory server, even if the certificate has expired.  

For tighter security, select No to require the Sametime server to check certificate expiration dates. If the certificate presented by the LDAP server has expired, the connection is terminated. |
| SSL protocol version                        | Select the version number of the SSL protocol to use. The choices are:  

  - **V2.0 only** - This setting allows only SSL 2.0 connections.  
  - **V3.0 handshake** - This setting attempts an SSL 3.0 connection. If this connection attempt fails but Sametime detects that SSL 2.0 is available on the LDAP server, Sametime attempts the connection using SSL 2.0.  
  - **V3.0 only** - This setting allows only SSL 3.0 connections.  
  - **V3.0 and V2.0 handshake** - This setting attempts an SSL 3.0 connection, but starts with an SSL 2.0 handshake that displays relevant error messages. This setting is used to receive V2.0 error messages when trying to connect to the LDAP server. These error messages might provide information about any compatibility problems found during the connection.  
  - **Negotiated** - This setting allows SSL to determine the handshake and protocol version required. |
| Verify server name with remote server's certificate | Select **Enabled** (the default setting) to verify the server name with the remote server's certificate.  

If **Enabled** is selected, the Sametime server verifies the name of the LDAP server with the remote server's certificate. If the names do not match, the connection is terminated. For more relaxed security, select **Disabled** (the server name is not verified with the certificate). |
8. Click **Save and Close** to close the Directory Assistance document.

**Connecting Sametime to the LDAP server:**

Enable SSL encryption for connections between IBM Sametime and the LDAP server.

**Before you begin**

The Sametime Community server must be running.

**Procedure**

1. Configure LDAP connectivity settings in the Sametime Administration Tool as follows:
   a. From the Sametime server’s home page, click the **Administer the Server** link to open the Sametime Administration Tool.
   b. Click **LDAP Directory > Connectivity**.
   c. In the **Host name or IP address of the LDAP server** list, select the name of the LDAP server.
   d. Click the option called **Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server**.
   e. In the **LDAP SSL port** field, specify the port on which the LDAP server is listening for SSL LDAP connections (the default is port 636).
   f. Click **Update**.
   g. Close the Sametime Administration Tool.

At this point, you have enabled SSL encryption for all data that is transmitted between the Sametime server and the LDAP server.

2. (Optional) To improve performance, you may choose to loosen security and encrypt only user credentials as follows:
   a. Open the **sametime.ini** file (located in the Sametime installation directory).
   b. Locate the **[Directory]** section within the file.
   c. Add the following setting:
      ```ini
      ST_DB_LDAP_SSL_ONLY_FOR_PASSWORDS=1
      ```
   d. Save and close the file.
3. Restart the Sametime server

**Modifying the LDAP server configuration for SSL:**

Modify the configuration of the IBM Sametime server to encrypt connections between the LDAP server and the Sametime Community Server.

**About this task**

Modify the Sametime server’s configuration by making the following changes to the **sametime.ini** file.

**Procedure**

1. Open the **sametime.ini** file in a text editor.
2. If these settings are not present in the [Config] section at the bottom of the
sametime.ini file, manually type them in. Follow the instructions for your
operating system.

**AIX, Linux, and Solaris**

```
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=/local/notesdata/key.jks
javax.net.ssl.trustStore=/local/notesdata/key.jks
javax.net.ssl.keyStorePassword=keystore_password
javax.net.ssl.trustStorePassword=truststore_password
```

**Note:** Specify the complete path name of the key.jks file for both the
javax.net.ssl.keyStore and the javax.net.ssl.trustStore settings. Specify
the password that you provided for key.jks when you created it for both the
javax.net.ssl.keyStorePassword and javax.net.ssl.trustStorePassword
settings.

**IBM i**

```
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=stkeys.jks
javax.net.ssl.trustStore=stkeys.jks
javax.net.ssl.keyStorePassword=sametime
javax.net.ssl.trustStorePassword=sametime
```

**Note:** By default, the password for the stkeys.jks file is "sametime." If you
change the password for stkeys.jks, you must change the setting of both
javax.net.ssl.keyStorePassword and javax.net.ssl.trustStorePassword to
match the new password. The full path for the stkeys.jks file is not needed for
the IBM i version of Sametime.

**Windows**

```
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
javax.net.ssl.trustStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
javax.net.ssl.keyStorePassword=passw0rd
javax.net.ssl.trustStorePassword=passw0rd
```

Where:

- For the javax.net.ssl.keyStore and the javax.net.ssl.trustStore settings,
you specify the complete path name for the stkeys.jks file.
- For the javax.net.ssl.keyStorePassword and the
  javax.net.ssl.trustStorePassword settings, you specify the password that
  you provided for the stkeys.jks file when you created it.

3. If these two lines appear in the sametime.ini file, remove them:

```
javax.net.ssl.trustStoreType=JKS
javax.net.ssl.keyStoreType=JKS
```

4. Save and close the sametime.ini file.

5. Restart the Sametime Community Server.

**Encrypting the UserInfo servlet:**

If your IBM Sametime deployment uses SSL encryption when communicating with
the LDAP server, you can additionally choose to encrypt the UserInfo servlet.
Before you begin

You must have created a keystore .jks file on the IBM Sametime Community Server, which stores a copy of the IBM Lotus Domino server's SSL certificate.

About this task

This configuration is necessary to enable the Business Card feature when you have chosen to encrypt all data transmitted between the Sametime server and the LDAP server, where the Business Card data is stored.

Procedure

1. Open a command prompt and navigate to the following directory:
   - IBM AIX, IBM i, Linux, Solaris: the Sametime server's data directory
   - Windows: the Sametime server's installation directory
2. Open the UserInfoConfig.xml file in an editor and make the following changes:
   a. Locate the <ReadStConfigUpdates> tag and set to value="true". If this statement is not in the file, you do not need to add it.
      The statement should look like this:
      <ReadStConfigUpdates value="true"/>
   b. Locate the <StorageDetails> tag and set the following values:
      SslEnabled="true"
      SslPort="636"
      Use the value of the port that your LDAP server listens on for SSL communications (the default is port 636).
   c. In the <SslProperties> tag, set the following values:
      <SslProperties KeyStorePath="D:\IBM\Lotus\Domino\jvm\bin\key.jks_OR_stkeys.jks"
      KeyStorePassword="mypwd"/>
      Where:
      • KeyStorePath indicates the path to where the keystore database is stored.
         On Windows and IBM i, the file is named stkeys.jks; on AIX, Linux, and Solaris, the file is named keys.jks.
      • KeyStorePassword indicates the password you created for accessing the keystore database.
3. Save and close the file
4. Restart the Sametime Community Server.

Related tasks:

“Creating a keystore file for the Domino server’s SSL certificate” on page 270
Use the IBM IKeyMan utility to create a keystore .jks file on the IBM Sametime Community Server, which will be used for storing a copy of the IBM Lotus Domino server's SSL certificate.

Configuring Transport Layer security for the Sametime Media Manager

Configuring the IBM Media Manager SIP Proxy and Registrar component to use SIP authentication and authorization requires some additional steps.

About this task

Follow the instructions in this section to configure Transport Layer Security (TLS) if you chose it as the encryption protocol and to set up user authentication.
Configuring ports for Transport Layer encryption on an upgraded Sametime Media Manager

After upgrading an IBM Sametime Media Manager, edit settings in the stavconfig.xml file to specify secure ports for TLS encryption. Do this only if all clients are running 8.5.1 or later; otherwise older clients cannot connect to the upgraded Media Manager.

Before you begin

Make a note of the values you need to transfer to stavconfig.xml from the SIP/Proxy Registrar, Conference Manager, and Packet Switcher servers. Open the WebSphere Application Server Integrated Solutions Console for each server and click Servers > Server Types > WebSphere Application servers > STMediaServer > Ports.

Find the values for a non-clustered or clustered environment.

Non-clustered environment

- **SIP/Proxy Registrar**
  
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE

- **Conference Manager**
  
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

- **Packet Switcher**
  
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

Clustered environment

- **SIP/Proxy Registrar**
  
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE
  
  (Clustered node) WebSphere Application Server proxy host
  
  (Clustered node) WebSphere Application Server proxy secure port

- **Conference Manager**
  
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
  
  (Clustered node) WebSphere Application Server proxy host
  
  (Clustered node) WebSphere Application Server proxy secure port

- **Packet Switcher**
  
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

About this task

The default settings in the stavconfig.xml file specify non-secure ports and must be modified for use with TLS encryption. Edit the stavconfig.xml files on the Conference Manager and Packet Switcher to reflect this update by changing the non-secure ports to secure ports. Follow these steps on both machines. This file is not used by the SIP Proxy and Registrar.

Follow these steps to update the stavconfig.xml file for every instance of the Media Manager components. When multiple profiles are installed on the same computer, each profile uses its own copy of the file and requires the updates.

Procedure

1. Log in to the Integrated Solutions Console for the machine.
2. On the server hosting the Conference Manager, Packet Switcher, or SIP Proxy and Registrar, navigate to the following directory:

   `dm_install_root/config/cells/cell_name/nodes/node_name/servers/server_name`

3. In a text editor, open the `stavconfig.xml` file.

4. Modify the following settings:
   - The `ConferenceServerPort` setting should contain the `SIP_DEFAULTHOST_SECURE` port value from the Conference Manager server.
   - The `SIPProxyServerPort` setting should contain the `SIP_ProxyRegSECURE` port value from the SIP Proxy/Registrar server.
   - The port setting in the `[packetswitches]` section should contain the `SIP_DEFAULTHOST_SECURE` port value from the Packet Switcher server.
   - **Clustered environment only:** Change the `SIPProxyServerTransportProtocol` setting value to TLS.

5. (Packet Switcher only) Add these three attributes if they are missing.

   ```xml
   <configuration lastUpdated="1226425838277" name="isEncryptedConferenceEnabled" value="false"/>
   <configuration lastUpdated="1226425838277" name="AudioRTCPEnabled" value="false"/>
   <configuration lastUpdated="1226425838277" name="VideoRTCPEnabled" value="true"/>
   ```

   **Note:** If you have Sametime 8.5.0 clients in your environment, set the third attribute for "VideoRTCPEnabled" to "false" instead.

6. **(Clustered environment only)**

   Make these additional changes in the file if you are configuring on a clustered node server.

   **Conference Manager node**
   - `SIPProxyServerHost` field
     `SIP Proxy/Registrar WAS proxy host`
   - `SIPProxyServerPort` field
     `SIP Proxy/Registrar WAS proxy secure port`

   **Packet Switcher node**
   - `SIPProxyServerHost` field
     `SIP Proxy/Registrar WebSphere Application Server proxy host`
   - `SIPProxyServerPort` field
     `SIP Proxy/Registrar WebSphere Application Server proxy secure port`
   - `ConferenceServerHost` field
     `Conference Manager WebSphere Application Server proxy host`
   - `ConferenceServerPort` field
     `Conference Manager WebSphere Application Server proxy secure port`

7. Close and save the updated file.

8. Synchronize all nodes in the Deployment Manager that manages the component.
   - In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
   - Click **Full Resynchronize**.
Results

Communications will now take place over the secure ports. If you later switch back to (nonencrypted) TCP or UDP transport protocol, you must change the port settings back to their original values. For SIP transport, you should use either TLS or TCP transport protocols.

Distributing certificates for Transport Layer encryption to all Media Manager components

If you installed Media Manager components on separate machines or as separate cell profiles, you must extract the signed security certificate from the SIP Proxy and Registrar server. Then add the certificate to all Conference Manager and Packet Switcher servers. This step does not apply if you installed all components of the media manager on the same cell profile.

Before you begin

Extract the certificate used by the SIP Proxy and Registrar and copy it to a location from which each Media Manager component can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the SIP Proxy and Registrar certificate.
2. Click Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
   - In a non-clustered environment, the certificate is on the same machine as the SIP Proxy and Registrar component.
   - In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the SIP Proxy and Registrar.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the Media Manager component can retrieve the file.

About this task

Follow these steps to add a signed certificate to each Media Manager component.

Procedure

1. Log in to the Media Manager component’s Integrated Solutions Console.
2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
   
   Note: If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.
3. Click Add.
4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.
5. In the File name field, type the path to the certificate file; for example: c:sip-pr.cer
6. Click OK.
7. Click Save.
8. Restart the server.
9. Repeat these steps for each Media Manager component.

**Distributing certificates for Transport Layer encryption to the SIP Proxy and Registrar**

If you installed the SIP Proxy and Registrar on separate machines or as a separate cell profile from the other IBM Sametime Media Manager components, you must extract the signed security certificate from the Conference Manager and Packet Switcher components and add the certificates to the SIP Proxy and Registrar. This step does not apply if you installed all components of the Sametime Media Manager and SIP Proxy and Registrar on the same cell profile.

**Before you begin**

Extract the certificate used by each Conference Manager and Packet Switcher component and copy it to a location from which the SIP Proxy and Registrar can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the Conference Manager certificate.
2. Click **Security > SSL Certificates and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates**.
   - In a non-clustered environment, the certificate is on the same machine as the Sametime Media Manager component (Conference Manager or Packet Switcher)
   - In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the Conference Manager.

   **Note:** The Packet Switcher does not run in a cluster.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click **Extract**.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the SIP Proxy and Registrar component can retrieve the file.
6. Repeat this procedure for the Packet Switcher.

**About this task**

Follow these steps to add from the Conference Manager and Packet Switcher components the signed certificates to the SIP Proxy and Registrar.

**Procedure**

1. Log in to the SIP Proxy and Registrar component's Integrated Solutions Console.
2. Click **Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates**.

   **Note:** If **CellDefaultTrustStore** is not in the table then choose **NodeDefaultTrustStore**.
3. Click **Add**.
4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.
5. In the File name field, type the path to the certificate file; for example:
c:\cm-pr.cer or c:\ps-pr.cer
6. Click OK.
7. Click Save.
8. Restart the server.
9. Repeat these steps for each Media Manager component.

**Exchanging certificates between the Packet Switcher and the Conference Manager**

The Packet Switcher component of the IBM Sametime Media Manager opens a TLS connection to the Conference Manager, so you need to exchange certificates between the Packet Switcher and the Conference Manager. You must extract the certificate used by the Conference Manager and then add this certificate to the Packet Switcher.

**Before you begin**

Extract the certificate used by the Conference Manager component and copy it to a location from which the Packet Switcher component can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the Conference Focus certificate.
2. Click Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
   - In a non-clustered environment, the certificate is on the same machine as the Conference Manager component.
   - In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the Conference Manager.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the Packet Switcher component can retrieve the file.

**About this task**

Follow these steps to add a signed certificate to the Packet Switcher.

**Procedure**

1. Log in to the Packet Switcher component's Integrated Solutions Console.
2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.

   **Note:** If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.
3. Click Add.
4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.
5. In the File name field, type the path to the certificate file; for example:
   c:\conf-focus.cer
6. Click OK.
7. Click Save.
Adding trusted IP addresses to the Media Manager SIP Proxy and Registrar

The Sametime SIP Proxy and Registrar accepts connections from the Sametime Media Manager components – Conference Manager and Packet Switcher. To ensure that the SIP Proxy and Registrar trusts these components when they establish a connection, you must add a custom SIP container property that uses the IP address or fully qualified domain name for these trusted components as its value.

About this task

Complete these steps for each server in a Sametime SIP Proxy and Registrar cluster or for every SIP Proxy/Registrar in a multiple-server deployment.

Procedure

1. Log in to the Sametime Media Manager’s Integrated Solutions Console.
   
   If you installed the SIP Proxy/Registrar component on a separate server, log in to the SIP Proxy and Registrar’s Integrated Solutions Console.

2. Click Servers > Server Types > WebSphere Application Servers.

3. Click the name of the Media Manager server.
   
   In a clustered environment, click the name of a cluster member.

4. Under Container settings, click SIP Container Settings > SIP container.

5. Click Custom Properties.

6. Add this new property if it does not exist:

   com.ibm.ws.sip.security.trusted.iplist

7. Add the Conference Manager and Packet Switcher as trusted IP addresses.
   Use commas to separate multiple values if you are using multiple servers.

   In a non-clustered environment, use the servers’ IP addresses or fully qualified domain names.

   Note: If the Conference Manager operates in a cluster, use the IP address or fully qualified domain name for the WebSphere Application Server proxy used by the Conference Manager cluster instead.

8. Click OK.

9. Click Save.

10. Restart the SIP Proxy and Registrar server.

Configuring secure access to an LDAP repository

Configure secure access to a Lightweight Directory Access Protocol (LDAP) repository used by the IBM Sametime SIP Proxy and Registrar server.

Before you begin

Ensure that the enterprise LDAP server is running.

About this task

If the LDAP server is using a public certificate, then you need to obtain the public root CA and import it. If your LDAP server is using a self-signed certificate, then you simply import the self-signed certificate.
Procedure
1. Import the certificate:
   a. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
   b. Select Security > SSL Certificate and key management > Key stores and
certificates > CellDefaultTrustStore > Signer certificates.
   c. Click Add.
   d. In the Alias field, type a description for the certificate, whether it's
self-signed or a public CA.
   e. In the File name field, type the path to the certificate file. For example,
c:\ldap.cer.
   f. Click Apply and then Save.
   g. Restart all WebSphere Application Server processes for the change to take
effect.
2. Enable SSL between the SIP Proxy and Registrar server and the LDAP
repository.
   a. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
   b. Select Security > Global security.
   c. Click Configure.
   d. In Repositories in the realm table select the LDAP server identifier.
   e. In the Port field type 636. For some LDAP servers, you can specify a
different port for a SSL connection.
   f. Click Require SSL communications.
   g. Click Apply and then Save.
   h. Restart the SIP Proxy and Registrar server for the change to take effect.

Configuring Transport Layer security for the Sametime
Bandwidth Manager
If the IBM Sametime Media Manager is configured to use Transport Layer Security
(TLS), you must also configure TLS on the server hosting IBM Sametime
Bandwidth Manager.

Configuring the stand-alone Bandwidth Manager to use TLS
encryption
If the IBM Sametime Media Manager is configured to use Transport Layer Security
(TLS), you must also configure TLS on the server hosting IBM Sametime
Bandwidth Manager.

About this task
Sametime Bandwidth Manager can use TLS (Transport Layer Security) encryption
for security. In IBM WebSphere Application Server, the TLS functionality requires a
certificate. This certificate can be a self-signed for testing or demonstration
environment purposes, but IBM recommends using a certificate issued by a valid
Certificate Authority (CA) for any production environment.

Because the Bandwidth Manager exchanges information with the Sametime Media
Manager, you must import a copy of the certificate to the Media Manager cell’s cell
default trust store to ensure it will accept communications from the Bandwidth
Manager.
Procedure

1. Import the Bandwidth Manager security certificate into the Media Manager’s SIP Proxy and Registrar:
   a. On the server hosting the Media Manager’s SIP Proxy and Registrar component (if that component is clustered, use the server hosting its deployment manager), open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
   b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.
   c. Click CellDefaultTrustStore.
   d. Click Signer certificates.
   e. Click Retrieve from port and enter the Bandwidth Manager’s host name and TLS port.
   f. Save the retrieved signer certificate.

2. Import the Media Manager’s SIP Proxy and Registrar security certificate into the Bandwidth Manager:
   a. On the server hosting the Bandwidth Manager, open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
   b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.
   c. Select the correct trust store:
      For a stand-alone Bandwidth Manager server, click NodeDefaultTrustStore.
      For a clustered Bandwidth Manager server, click CellDefaultTrustStore.
   d. Click Signer certificates.
   e. Click Retrieve from port and enter the SIP Proxy and Registrar’s host name and TLS port.
   f. Save the retrieved signer certificate.

3. Locate the secure port value:
   a. From the Bandwidth Manager’s WebSphere Integrated Solutions Console, return to the navigation tree and click Servers > Server types > WebSphere application servers.
   b. On the Application servers page, navigate to the servers table and click the name of your Bandwidth Manager server.
   c. On the Configuration page, navigate to the Container Settings section and click SIP Container Settings > SIP container transport chains.
   d. In the Transport Chains table, locate the Port value in the SIPCInboundDefaultSecure row.
      This is the secure port value, which you will need in the next step.

4. Configure the Bandwidth Manager to use the secure port:
   a. Back on the navigation tree, click Sametime Servers > Bandwidth Manager.
   b. On the Status page, click the Configuration tab.
   c. On the Configuration page, click the SipFrontend component listed in the table at the bottom of the page.
   d. On the General Properties page for the SipFrontend component, edit the SIP URI field, typing the value of the secure port that you obtained earlier from the value of SIPCInboundDefaultSecure in the Transport Chains table.
   e. Cluster only: If you are setting up a cluster, also change the Cluster SIP URI field to use that same secure port.
f. Click Apply and then click the Save link in the “Messages” box at the top of the page.

5. Restart the server or cluster:
   • For a stand-alone server, restart it now as follows:
     a. On the server’s Configuration page, click the Status tab.
     b. On the Status page, click the Start/Restart button at the top of the table.
     c. Click the Refresh button and verify that all components are active.
   • For a clustered server, synchronize nodes and restart the cluster as follows:
     a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
     b. Select all nodes in the cluster
     c. Click Full Resynchronize.
     d. Back in the navigator, click System Administration > Node agents.
     e. Click a node agent, and then click Restart; repeat for each node agent.

Configuring the Bandwidth Manager node to use TLS encryption
If the IBM Sametime Media Manager is configured to use Transport Layer Security (TLS), you must also configure TLS on the server hosting IBM Sametime Bandwidth Manager.

About this task
Sametime Bandwidth Manager can use TLS (Transport Layer Security) encryption for security. In IBM WebSphere Application Server, the TLS functionality requires a certificate. This certificate can be a self-signed for testing or demonstration environment purposes, but IBM recommends using a certificate issued by a valid Certificate Authority (CA) for any production environment.

Because the Bandwidth Manager exchanges information with the Sametime Media Manager, you must import a copy of the certificate to the Media Manager cell’s cell default trust store to ensure it will accept communications from the Bandwidth Manager.

Procedure
1. Import the Bandwidth Manager security certificate into the Media Manager’s SIP Proxy and Registrar:
   a. On the server hosting the Media Manager’s SIP Proxy and Registrar component (if that component is clustered, use the server hosting its deployment manager), open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
   b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.
   c. Click CellDefaultTrustStore.
   d. Click Signer certificates.
   e. Click Retrieve from port and enter the Bandwidth Manager’s host name and TLS port.
   f. Save the retrieved signer certificate.
2. Import the Media Manager’s SIP Proxy and Registrar security certificate into the Bandwidth Manager:
   a. On the server hosting the Bandwidth Manager, open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
b. On the navigation tree, click **Security > SSL certificate and key management > Key stores and certificates.**

c. Select the correct trust store:
   - For a stand-alone Bandwidth Manager server, click **NodeDefaultTrustStore.**
   - For a clustered Bandwidth Manager server, click **CellDefaultTrustStore.**

d. Click **Signer certificates.**

e. Click **Retrieve from port** and enter the SIP Proxy and Registrar's host name and TLS port.

   f. Save the retrieved signer certificate.

3. Locate the secure port value:
   a. From the Bandwidth Manager's WebSphere Integrated Solutions Console, return to the navigation tree and click **Servers > Server types > WebSphere application servers.**

   b. On the Application servers page, navigate to the servers table and click the name of your Bandwidth Manager server.

   c. On the Configuration page, navigate to the Container Settings section and click **SIP Container Settings > SIP container transport chains.**

   d. In the Transport Chains table, locate the **Port** value in the **SIPCInboundDefaultSecure** row.

      This is the secure port value, which you will need in the next step.

4. Configure the Bandwidth Manager to use the secure port:
   a. Back on the navigation tree, click **Sametime Servers > Bandwidth Manager.**

   b. On the Status page, click the Configuration tab.

   c. On the Configuration page, click the **SipFrontend** component listed in the table at the bottom of the page.

   d. On the General Properties page for the SipFrontend component, edit the **SIP URI** field, typing the value of the secure port that you obtained earlier from the value of **SIPCInboundDefaultSecure** in the Transport Chains table.

   e. Cluster only: If you are setting up a cluster, also change the **Cluster SIP URI** field to use that same secure port.

   f. Click **Apply** and then click the **Save** link in the "Messages" box at the top of the page.

5. Restart the server or cluster:
   - For a stand-alone server, restart it now as follows:
      a. On the server’s Configuration page, click the **Status** tab.

      b. On the Status page, click the **Start/Restart** button at the top of the table.

      c. Click the **Refresh** button and verify that all components are active.

   - For a clustered server, synchronize nodes and restart the cluster as follows:
      a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes.**

      b. Select all nodes in the cluster.

      c. Click **Full Resynchronize.**

      d. Back in the navigator, click **System Administration > Node agents.**

      e. Click a node agent, and then click **Restart;** repeat for each node agent.
Configuring Sametime Meeting Server for secure access to an LDAP repository

Configure secure access to a Lightweight Directory Access Protocol (LDAP) repository used by the IBM Sametime Meeting Server.

Before you begin

Ensure that the enterprise LDAP server is running.

About this task

If the LDAP server is using a public certificate, then you need to obtain the public root CA and import it. If your LDAP server is using a self-signed certificate, then you simply import the self-signed certificate.

Procedure

1. Import the certificate:
   a. Log in to the Integrated Solutions Console for the Sametime Meeting Server.
   b. Select Security > SSL Certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
   c. Click Add.
   d. In the Alias field, type a description for the certificate, whether it's self-signed or a public CA.
   e. In the File name field, type the path to the certificate file. For example, c:\ldap.cer.
   f. Click Apply and then Save.
   g. Restart all WebSphere Application Server processes for the change to take effect.

2. Enable SSL between the Sametime Meeting Server and the LDAP repository.
   a. Log in to the Integrated Solutions Console for the Sametime Meeting Server.
   b. Select Security > Global security.
   c. Click Configure.
   d. In Repositories in the realm table select the LDAP server identifier.
   e. In the Port field type 636. For some LDAP servers, you can specify a different port for a SSL connection.
   f. Click Require SSL communications.
   g. Click Apply and then Save.
   h. Restart the Sametime Meeting Server for the change to take effect.

Replacing the default IBM self-signed certificate with another certificate

The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, using a self-signed certificate from IBM. If you want to use a different certificate, you can import it into the keystore yourself.

About this task

The following Sametime servers install with SSL already enabled, using a self-signed certificate provided by IBM:

- Sametime Proxy Server
Adding a Sametime server SSL certificate to the Sametime System Console

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

About this task

To enable SSL, you must extract the certificate from the Sametime product server and add it to the trust store of the Sametime System Console. The Sametime product servers include:

- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Gateway Server
- SIP Proxy and Registrar

Follow these instructions. See the WebSphere Application Server information center for more information on extracting and adding certificates.

Procedure

1. Log in to the Integrated Solutions Console for the Sametime product server.
2. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
3. Select the alias named root, and click Extract.
4. Enter the name of the .cer file, and select Base64 as the type for storing the process server sign certificate.
5. Log in to the Integrated Solutions Console for the Sametime System Console.
6. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
7. Click Add.
8. Enter an alias.
9. Enter the file name where you stored the extracted process server signer certificate from the product server.
10. Click Apply.
11. Restart the Sametime System Console deployment manager.

Related tasks:
“Updating Sametime Proxy Server connection properties on the console” on page 114
You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Proxy Server.
“Updating Sametime Media Manager connection properties on the console” on page 115
You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Media Manager.
“Updating Sametime Meeting Server connection properties on the console” on page 137
You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Meeting Server.
“Updating Sametime Gateway Server connection properties on the console” on page 146
You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Gateway Server.

Importing an SSL certificate from Sametime Unified Telephony

If you plan to configure telephony services in your deployment using IBM Sametime Unified Telephony, import the Telephony Application Server's SSL certificate into the Sametime Proxy Server's truststore.

Before you begin

Secure Socket Layer (SSL) encryption is required for telephony services. You must import the telephony server's SSL certificate into the Sametime Proxy Server's truststore before you enable SSL between Sametime Proxy Server and Sametime Unified Telephony.

Procedure

1. Copy the SSL certificate from Sametime Unified Telephony:
   a. On the Telephony Application Server, log in to the IBM WebSphere Application Server Integrated Solutions Console as the WebSphere administrator.
   b. Click Security > SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates.
   c. Select the Alias default_signer or the appropriate one, if you customized, and click Extract.
   d. Type a file name for storing the signer certificate. The Telephony Application Server WebSphere Application Server console displays the location of the extracted certificate. For example:

```
/opt/IBM/WebSphere/AppServer/profiles/<AppSrvxx>/etc/<file>
```

   Note this location because you need to copy the file to the live names proxy server in the following step.

2. Move the file from the previous step to the etc/ directory under the Deployment Manager for the Live Names Proxy cell. For example:

```
/opt/IBM/WebSphere/AppServer/profiles/<xxxSTPDMProfile>/etc/<file>
```

3. Now import the SSL certificate into the Sametime Proxy Server's truststore:
a. On the Sametime Proxy Server, log in to the WebSphere Application Server Integrated Solutions Console as the WebSphere administrator.
b. Click Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
c. Click Add.
d. Type an alias for the certificate; for example, "SUT".
e. Type the name of the file where you stored the SSL certificate.
f. Click Apply.
g. Save the imported certificate by clicking Save in the "Messages" box at the top of the page.
h. Restart the Sametime Proxy Server.

Configuring TLS/SSL for Sametime Gateway

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) provide encrypted SIP communications between Sametime Gateway and the external instant messaging communities such as AOL, Office Communications Server, and Sametime communities, but only if the other Sametime community requires SSL. TLS/SSL also provides encrypted XMPP communications for XMPP communities. The TLS/SSL protocols allow Sametime messages to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. Use these steps to set up SSL with a certificate signed by a Certificate Authority and exchange trusted certificates with external communities.

About this task

Messages that flow between Sametime Gateway and AOL and Office Communications Server always require a TLS/SSL connection. Sametime and XMPP communities may or may not require a TLS/SSL connection, depending whether the external community requires a CA-signed certificate. Google Talk does not work over TLS/SSL.

This section provides steps for a single Sametime Gateway server or cluster of Sametime Gateway servers. In addition, this section provides steps needed to set up SSL on a Sametime 6.5.1 or later server in an external community. You can provide these steps as a courtesy to an external community or refer them to the Sametime documentation.

SSL can encrypt sensitive information for SIP and XMPP communications, and provides authenticity and data signing to ensure a secure connection between the local Sametime Gateway community and an external instant messaging community. The foundation technology for SSL is public key cryptography, which guarantees that when an entity encrypts data using its private key, only entities with the corresponding public key can decrypt that data.

SSL is required for connections to the following communities:
- External community using AOL Instant Messenger
- External community using Office Communications Server
- AOL clearinghouse community

SSL is not required but it is recommended for connections to XMPP or Sametime communities.

You cannot use SSL between Sametime Gateway and Google Talk communities.
SSL is not needed between Sametime Gateway and the local Sametime community because the connection uses the Virtual Places (VP) protocol over TCP and includes built-in encryption.

**Setting up SSL on a single server**
These procedures describe how to set up Secure Sockets Layer (SSL) on a single Sametime Gateway server for both SIP and XMPP communications.

**Before you begin**
Before you begin, make sure the Sametime Gateway server is running.

**About this task**
To have a secure network connection, you will create a key for secure network communications and receive a certificate from a certificate authority (CA) that is designated as a trusted CA on your server.

WebSphere Application Server uses the certificates that reside in keystores to establish trust for a SSL connection. WebSphere Application Server creates the key.p12 default keystore file and the trust.p12 default truststore file during profile creation.

A default, self-signed certificate is also created in the key.p12 file at this time. Do not use this self-signed or other self-signed certificate to connect to external communities.

**Note:** Ensure that the SSL certificate contains the Basic Constraints extension. Do not use a non-SSLv3-compliant self-signed CA. WebSphere Application Server 6.1 uses the IBM JDK 1.5.0 JSSE2 which checks for the presence of the Basic Constraints extension. If the extension is not set, WebSphere Application Server assumes that the CA is not a valid CA but a user certificate, which in returns doesn’t allow to validate a server certificate as valid, because the issuing CA is not found.

Trial certificates are not publicly trusted and so cannot be used to test against public instant messaging providers such as AOL Instant Messenger.

The following procedures describe how to:
1. Import the certificate authorities’ public certificate used by each of the public or private external communities your Sametime Gateway server will be communicating with.
2. Request a CA-signed certificate, and then import the signed certificate that the CA provided in response. Before performing this step you might have to import intermediary certificates.
3. Configure the WebSphere environment to make use of the imported keys.

A complete technical reference of how to setup up SSL on the WebSphere Application Server can be found in the WebSphere Application Server information center.

**Adding trust for certificate authorities used by external communities:**
External communities certificates are signed by a specific certificate authority - probably a different authority from the CA used to sign your Sametime Gateway
certificate. In order for the Sametime Gateway to trust a certificate presented by an external community, the CA that issued this certificate would have to be configured to be trusted in advance.

About this task

This topic explains what CA certificate needs to be downloaded and imported into the WebSphere Application Server trust store.

• Steps 1-4 explain how to obtain the required CA certificate.
• Steps 5-7 explain how to import the obtained CA certificates into the WebSphere Application Server.

Procedure

1. To connect to AOL, download the following CA certificate. Navigate to http://www.geotrust.com/resources/root_certificates/index.asp and download the Equifax Secure Certificate Authority:
   Download - Equifax Secure Certificate Authority (Base-64 encoded X.509)
2. To connect to AOL, you are also required to download the following additional certificates:
   a. Navigate to https://pki-info.aol.com/AOL/ and download both certificates titled: "America Online Root CA 1 certificate" and the "America Online Root CA 2 certificate."
   b. Navigate to https://pki-info.aol.com/AOLMSPKI/index.html and download the certificate titled: "AOL Member CA certificate
3. To connect to an external Sametime-based IM community over SSL you will need to obtain the CA certificate used by external community
   a. Check with the external community administrator to determine which trusted certificate authority they are using.
   b. Obtain the CA certificate.
4. To connect to an external XMPP-based IM community over SSL. Note that the Google talk public community does not use SSL you need to obtain the CA certificate used by external community.
   a. Check with the external community administrator to determine which trusted certificate authority they are using.
   b. Obtain the CA certificate.
5. In case the received certificate is stored in any type of a certificate file database (a file with a suffix of .db or .p12, for example), you have to extract the certificate to an independent file, before you can import it to WebSphere Application Server.
6. Complete the following tasks in the Integrated Solutions Console: Click Security > SSL Certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer Certificate.
7. Click Add.
   a. Type an alias to identify the Certificate Authority in the Alias field. This is a freeform value used to identify the certificate inside WebSphere, a good idea would be to set the alias to the certificate's CN (common name) field value.
   b. Type in the full path to the file name containing the Certificate Authority's public key. For example: c:\certificates\acme_external_community.arm.
   c. Select the data type.

Note: Attention: For IBM i, you must select binary as the data type.
d. Click OK.

**Note:** For IBM i only, Certificates are automatically downloaded with the .CER file extension, so you must manually rename them to the .DER file extension.

**Requesting a certificate signed by a Certificate Authority:**

To ensure Secure Sockets Layer (SSL) communication, servers require a personal certificate that is signed by a certificate authority (CA). You must first create a personal certificate request to obtain a certificate that is signed by a CA.

**Before you begin**

The keystore that contains a personal certificate request must already exist. In WebSphere Application Server, the keystore file key.p12 exists.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Security > SSL certificate and key management > Related items > Key stores and certificates > NodeDefaultKeyStore.**
3. Under "Additional Properties," click **Personal certificate requests.**
4. Click **New.**
5. In the **File for certificate request** field, type the full path where the certificate request is to be stored, plus a file name. For example: c:\servercertreq.arm (for a Windows machine).
6. Type an alias name in the **Key label** field. The alias is the name you use to identify the certificate request in the keystore. For example: stgwcertificate
7. Type a common name (CN) value. The CN must be your external visible DNS address to which the external community (AOL for example) would be opening a TCP connection to. The CN value **does not** have to be identical to any of the email domains associated with your community. You should decide on the CN value in advance primarily by consulting your network administrator.
8. Type an organization name in the **Organization** field. This value is the "organization" value in the certificate's distinguished name.
9. In the **Organization unit** field, type the "organization unit" portion of the distinguished name.
10. In the **Locality** field, type the "locality" portion of the distinguished name.
11. In the **State or Province** field, type the "state" portion of the distinguished name.
12. In the **Zip Code** field, type the "zip code" portion of the distinguished name.
13. In the **Country or region** drop down list, select the two-letter "country code" portion of the distinguished name.
14. Click **Apply and Save.** The certificate request is created in the specified file location in the keystore. The request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore.
Note: Key store tools (such as iKeyman and keyTool) cannot receive signed certificates that are generated by certificate requests from WebSphere Application Server. Similarly, WebSphere Application Server cannot accept certificates that are generated by certificate requests from other keystore utilities.

15. Send the certification request arm file to a Certificate Authority for signing. For more information, see List of supported Certificate Authorities.

16. Stop the Sametime Gateway server.

17. Make a backup copy of your keystore file. Make this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is WebAS. The Integrated Solutions Console has the path information for the keystore’s location.

   The path to the NodeDefaultKeyStore is listed in the Integrated Solutions Console as:
   stgw_profile_root\config\cells\cell_name\nodes\node_name\key.p12

18. Start the Sametime Gateway server.

Importing any intermediate CA certificates into the keystore:

If your server certificate is issued by an intermediary CA, then complete the steps that follow.

Before you begin

You have received the signed certificate from the certificate authority, but before importing the signed certificate into the keystore, you have to determine if the received certificate had been signed by a root Certificate Authority (CA), or by an intermediary Certificate Authority. If the certificate was signed by a root CA you could skip this topic completely and continue straight to "Importing a signed certificate into the keystore". If the certificate was signed by an intermediary CA you will need to import the intermediary signer certificates as described in this topic.

About this task

IBM WebSphere Application Server creates a certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Therefore, it is important to import all intermediate certificates as signer certificates into the keystore before receiving the Certificate Authority-signed certificate. When you purchase a server certificate for Sametime Gateway, the certificate is issued by a Certificate Authority (CA). The CA can either be a root CA or an intermediary CA.

Procedure

1. The following steps describe how to tell if your certificate was signed by a root CA or an intermediary CA (example given is on the Windows operating system)
   a. Save the signed certificate to a text file with a .cer extension. For example: signed-certificate.cer. Include the Begin Certificate and End Certificate lines when you save the file. For example:

      -----BEGIN CERTIFICATE-----
      ZZZZ3zCCAk1gAwI8AgIDB5iRMA6GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
      MRAwDgZZZ3KExwRc45MS0wKwYDVQQLEyRFcXVpZmF4MSIwEAYDVQQKDAQz
      314
      IBM Sametime: Administration Guide

      -----END CERTIFICATE-----
b. Double-click the new file that you created and a Certificate dialog box opens.

c. Click the **Certification Path** tab.

d. Look at the tree-like structure representing the full certificate chain. The top of the chain is referred to as the root Certificate Authority (CA). The bottom of the chain represents your server’s certificate. If your server is not listed one-level below the root CA, then your certificate was issued by an intermediary CA. However, if your server is listed one-level below the root CA, then the certificate was issued by the root CA. For example, the following screen capture shows a certificate chain where an intermediary CA, VeriSign Class 3 Secure Server CA, issued a certificate for
If the server certificate is not issued by an intermediary CA, stop here and click **Next topic** at the bottom of this topic.

2. One you determine that the certificate is an intermediate certificate, you must export the certificate from the chain into its own certificate file:
   a. Double-click the server's certificate (i.e. server.cer) file and a Certificate dialog box opens.
   b. Click **Certification Path** tab.
   c. Highlight an entry of the certificate chain.
   d. Click **View Certificate**.
   e. In the **Certificate** dialog window, click the **Details** tab.
   f. Click **Copy to File...**.
   g. In the **Certificate Export Wizard** that appears, click **Next**.
   h. Select **Base-64 encoded X.509 (.CER)**, and click **Next**.
   i. Type in a unique name for the certificate you are exporting and click **Next**. For example, "VS-intermediary-CA" for VeriSign's intermediary certificate authority.
   j. Click **Finish**.
   k. Click **OK** in the dialog box that displays the following message: **The export was successful.**
1. Repeat the preceding sub steps for each intermediate certificate in the chain. Note that there is no need to repeat these steps for the bottom entry of the chain because the server’s certificate already exists. When you are done, you will have a certificate file (.cer) for each entry of the chain. In our example, there are three certificate files:

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Name</th>
<th>Certificate file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>VeriSign Class 3 Public Primary CA</td>
<td>VS-root-CA.cer</td>
</tr>
<tr>
<td>Intermediary</td>
<td>VeriSign Class 3 Secure Server CA</td>
<td>VS-intermediary-CA.cer</td>
</tr>
<tr>
<td>Server</td>
<td>stgw.lotus.com</td>
<td>stgw.cer</td>
</tr>
</tbody>
</table>

3. Finally, import the intermediary CA certificate into the keystore by completing the following steps:
   a. Using the Integrated Solutions Console, click Security > SSL Certificate and key management.
   b. Click Key stores and certificates.
   c. Click NodeDefaultKeyStore.
   d. Click Signer certificates.
   e. Click Add.
   f. In the Alias field, type a short descriptive name for the certificate. For example, “Verisign Intermediary CA.”
   g. In the File name field, type the path to the certificate file of the intermediary CA. For example, C:\certs\VS-intermediary-CA.cer.
   h. Accept the default file data type.
   i. Click Apply and Save.
   j. Repeat the preceding steps for each intermediary CA that is part of the certificate chain. In most cases, only one intermediary CA exists.

**Importing a signed certificate issued into the keystore:**

A Certificate Authority (CA) creates a certificate from a certificate request. WebSphere Application Server keystore receives the certificate from the CA and generates a CA-signed personal certificate that your Sametime Gateway can use for Secure Sockets Layer (SSL) security.

**Before you begin**

You have received the signed certificate from the certificate authority. You have determined whether the certificate is signed by a root CA or an intermediate CA, if the certificate was signed by an intermediate CA, then you have imported into the keystore all intermediate CA certificates. Now you are ready to import the signed certificate itself into the keystore.

**About this task**

WebSphere Application Server can receive only those certificates that are generated by a WebSphere Application Server certificate request. It cannot receive certificates that are created with certificate requests from other keystore tools, such as iKeyman and keyTool. The keystore must contain the certificate request that was created and sent to the CA. This means that you cannot import a certificate to the keystore if the keystore does not contain the original certificate request.
Make sure the certificate file you have received does not contain any text lines before the " -----BEGIN CERTIFICATE-----" line appears on top. These lines can cause the certificate import process to fail, and therefore you must delete these lines if they are present in the certificate file.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Related items > Key stores and certificates > NodeDefaultKeyStore.
4. Click Receive a certificate from a certificate authority.
5. Type the full path and name of the certificate file. For example on windows: 
   c:\mycertificate.cer
6. Do not change the default data type on the list (Base64-encoded ASCII Data).
7. Click Apply and Save.

Setting up Sametime Gateway to use a new certificate:

Set up IBM Sametime Gateway server to use the new certificates.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Configuration settings > Manage endpoint security configurations.
3. Expand the Inbound node, and then expand all levels below Nodes.
4. In the tree view, click the Sametime Gateway server.
5. On the configuration panel, under Specific SSL configuration for this endpoint, select Override inherited values if this option is available.
6. Select NodeDefaultSSLSettings in the SSL configuration drop down.
7. Click Update certificate alias list.
8. Select the certificate alias from the Certificate alias in key store drop down that you specified when you received the certificates from the CA.
9. Click Apply and then Save.
10. Important: Repeat the preceding steps on the Outbound node of the local topology tree.
11. Restart the Sametime Gateway server.
   For a standalone: the single Java process.
   For a cluster configuration: restart the DMGR, STGW servers, XMPP proxies, SIP Proxies.
   You do not need to restart the node agents.

Replacing and renewing a certificate for a single Gateway server:

Replacing or renewing a certificate is similar to importing it for the first time, but you also replace the old certificate with the new one.

Before you begin

You have received the signed certificate from the certificate authority. You have determined whether the certificate is signed by a root CA or an intermediate CA. If the certificate was signed by an intermediate CA, then you have imported into the
keystore all intermediate CA certificates. Now you are ready to import the signed certificate itself into the keystore.

About this task

WebSphere Application Server can receive only those certificates that are generated by a WebSphere Application Server certificate request. It cannot receive certificates that are created with certificate requests from other keystore tools, such as iKeyman and keyTool. The keystore must contain the certificate request that was created and sent to the CA. This means that you cannot import a certificate to the keystore if the keystore does not contain the original certificate request.

Make sure the certificate file you have received does not contain any text lines before the " -----BEGIN CERTIFICATE-----" line appears on top. These lines can cause the certificate import process to fail, and therefore you must delete these lines if they are present in the certificate file.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Related items > Key stores and certificates > NodeDefaultKeyStore.
4. Click Receive a certificate from a certificate authority.
5. Type the full path and name of the certificate file. For example on windows: c:\mycertificate.cer
6. Do not change the default data type on the list (Base64-encoded ASCII Data).
7. Click Apply and Save.
8. From the Integrated Solutions Console, click Security > SSL certificate and key management > Key stores and certificates.
9. Select the keystore that contains the new and old certificates.
10. Select the old certificate and click Replace.
11. Verify that the old certificate is listed in the "Old certificate" field.
12. Select the new certificate from the "Replace with" list.
13. Click OK and Save.
   
   For a standalone: the single Java process.
   
   For a cluster configuration: restart the DMGR, STGW servers, XMPP proxies, SIP Proxies.
   
   You do not need to restart the node agents.

Setting up SSL on a cluster

These procedures describe how to set up Secure Sockets Layer (SSL) on a cluster of Sametime Gateway servers.

Before you begin

You must first install Sametime Gateway on each node, including a Deployment Manager node, create the cluster, and create a SIP proxy server for the cluster.
About this task

To have a secure network connection, create a key for secure network communications and receive a certificate from a certificate authority (CA) that is designated as a trusted CA on your server.

WebSphere Application Server uses the certificates that reside in keystores to establish trust for a SSL connection. WebSphere Application Server creates the key.p12 default keystore file and the trust.p12 default truststore file during profile creation. A default, self-signed certificate is also created in the key.p12 file at this time.

Note: If you use a certificate other than the default self-signed certificate provided, ensure that the SSL certificate contains the **Basic Constraints** extension. Do not use a non-SSLv3-compliant self-signed CA. WebSphere Application Server 6.1 uses the IBM JDK 1.5.0 JSSE2 which checks for the presence of the **Basic Constraints** extension. If the extension is not set, WebSphere Application Server assumes that the CA is not a valid CA but a user certificate, which in returns doesn't allow to validate a server certificate as valid, because the issuing CA is not found.

Trial certificates are not publicly trusted and so cannot be used to test against public instant messaging providers such as AOL Instant Messenger.

The following procedure describes how to request a Certificate Authority-signed certificate, receive the request, then extract the certificate to the keystore.

For complete details for setting up SSL in WebSphere Application Server, see the WebSphere Application Server information center.

**Purchasing a certificate from a Certificate Authority:**

Purchase a Certificate Authority-signed certificate for secure connections between Sametime Gateway and other instant messaging providers.

About this task

The CA certificate installed on Sametime Gateway must conform to RFC 3280 certificate standards. The CA certificate can be a root certificate or an intermediary certificate. When requesting a certificate, check with the vendor to make sure that the certificate supports both TLS Web Server Authentication and TLS Web Client Authentication. Some certificate authorities provide certificates that support server authentication only or client authentication only. Certificates must include both server and client authentication EKU flags. Thawte certificates meet these standards. It is your responsibility to make sure that the certificate supports both.

**Procedure**

1. Review the list of Certificate Authorities recognized by AOL and XMPP.
   For more information, see List of supported Certificate Authorities.
2. Purchase a certificate that supports both client and server authentication.

**Creating a new keystore:**

The keystore file is a key database file that contains both public keys and private keys. Public keys are stored as signer certificates while private keys are stored in the personal certificates. A Secure Sockets Layer (SSL) configuration references
keystore configurations during WebSphere Application Server runtime. Whether a keystore file was created by another keystore tool or saved from a previous configuration, the file must be part of a keystore configuration object. You can create a keystore configuration for the existing keystore object.

Before you begin

Expected state: the Deployment Manager, node agents, and servers are started.

Procedure
1. Stop all Sametime Gateway servers, but leave the Deployment Manager and node agents running.
2. Using the Integrated Solutions Console, click Security > SSL certificate and key management > Key stores and certificates.
3. Click New.
4. Type a name in the Name field that specifies the unique name to identify the keystore; for example: STGWKS.
5. In the Path field, specify this location for the keystore file:
   $\{CONFIG_ROOT\}/STGWKS.p12.
6. Type a password in the Password field. The password is used to protect the keystore.
7. Type the keystore password again in the Confirm Password field to confirm the password.
8. Select PKCS12 from the list. The type that you select is for the keystore file that you specified in the Path field.
9. Click Apply and Save.
10. Ensure that all of the nodes in the cluster are started.
    a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Node agents.
    b. Start any node agent that is not running.
11. Synchronize all the nodes.
    a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
    b. Select all available nodes and click Full Resynchronize.

Creating a certificate request:

To ensure Secure Sockets Layer (SSL) communication, servers require a personal certificate that is signed by a certificate authority (CA). You must first create a personal certificate request to obtain a certificate that is signed by a CA.

Before you begin

The keystore that contains a personal certificate request must already exist. In WebSphere Application Server, the keystore file p12 exists.

About this task

Complete the following tasks in the WebSphere Integrated Solutions Console.

Expected state: the Deployment Manager and node agents are started. The servers are stopped.
Procedure

1. Click Security > SSL certificate and key management > Key stores and certificates.
2. Click the keystore that you created in the previous step.
3. Click Personal certificate requests, then click New.
4. In the File for certificate request field, specify the fully qualified file name from which the certificate request is exported. This portion of the certificate request can be given to the certificate authority to generate the real certificate. For example: c:\servercertreq.arm (for a Windows machine).
5. Type an alias name in the Key label field. The alias is the name you give to identify the certificate request in the keystore.
6. Type a common name (CN) value in the Common Name field. The common name must be the Fully qualified domain host name of your proxy server node machine. The CN of the certificate must match the domain name of your community. For example, if your Sametime community is us.acme.com, then the CN of the SSL certificate that you create for your community must be us.acme.com.
7. Type an organization name in the Organization field. This value is the organization value in the certificate distinguished name.
8. In the Organization unit field, type the organization unit portion of the distinguished name.
9. In the Locality field, type the locality portion of the distinguished name.
10. In the State or Province field, type the state portion of the distinguished name.
11. In the Zip Code field, type the zip code portion of the distinguished name.
12. In the Country or region drop down list, select the two-letter country code portion of the distinguished name.
13. Click Apply and Save. The certificate request is created in the specified file location in the keystore. The request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore. **Note:** Key store tools (such as iKeyman and keyTool) cannot receive signed certificates that are generated by certificate requests from WebSphere Application Server. Similarly, WebSphere Application Server cannot accept certificates that are generated by certificate requests from other keystore utilities.
14. Synchronize your changes to all nodes in the cluster. Click System Administration > Nodes.
15. Select all nodes in the cluster, then click Full Resynchronize.
16. Stop the Sametime Gateway server.
17. Make a backup copy of your keystore file. Make this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is WebAS. The Integrated Solutions Console has the path information for the keystore’s location. The path to the CellDefaultKeyStore is listed in the Integrated Solutions Console as:

\stgw_profile_root\config\cells\cell_name\key.p12

18. Now start the Sametime Gateway server.

What to do next

After you receive the certificate back from the Certificate authority, you are ready to proceed to the next step.
Importing intermediate CA certificates into the keystore:

IBM WebSphere Application Server creates a certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Therefore, it is important to import all intermediate certificates as signer certificates into the keystore before receiving the Certificate Authority-signed certificate. When you purchase a server certificate for Sametime Gateway, the certificate is issued by a Certificate Authority (CA). The CA can either be a root CA or an intermediary CA.

About this task

If your server certificate is issued by an intermediary CA, then complete the steps that follow, otherwise skip these steps and click Next topic at the bottom of this topic.

Procedure

1. Before you import an intermediate CA, first determine if your server’s certificate was issued by an intermediary CA:
   a. Save the signed certificate to a text file with a .cer extension. For example: signed-certificate.cer. Include the Begin Certificate and End Certificate lines when you save the file. For example:

```
-----BEGIN CERTIFICATE-----
ZZZZ3zCCkIgAwIBAgIDB5iMRMGAOGBSogX8QIBAgYEMjF6ME4xCzAJBgNV
BAYTAlVTMRMGAOGBSogX8QIBAgYEMjF6ME4xCzAJBgNVBAYTAlVT
MRAwDgZZZQEKwEfcXCvZmF4S50bKwYDQQLyRfcXvZmF4S50bKwYD
awZpYZFOZ5c8dXRRZPPPdXkWhlhcMNdCwNjEMTkwNDI3hXcMNdCwNjEMT
 awZpYZFOZ5c8dXRRZPPPdXkWhlhcMNdCwNjEMTkwNDI3hXcMNdCwNjEMT
 kJbQyMQswQYDVQQExJUZGV2XzAAMDAFMB8GA1UdIwQYMBaAIG7yZ
 bJEMMAoGAIUEChMDSUINMMRQoYMDQQLdvdzdXpb3QMRoGAYDVQDEExYd
 YRILmzxdHVzLmNvbTCBmzANBZZZgZGWo8AQEEFAAOBJQAQwYKcEA1b7f
 obgdUzU0OFujRwZqZIvBseKFMSQoQwQ4Tw0aPy3xZ7ddFHSHwoFVOl
 OPiRCY8oYiI5R7BqfIlt5MFUTJhYm7k6z9j5fIufzai2Bn3eYj7m7i
 Gm3ajjYQwjc3BfOh7PY9FII3dNWSZ9ZwCwEAaABoBrjCBoAO8gYHQ
 BACMBPAmQYDVQDUBBYEFMFFt2o6Gbc6H7591nRZZZz9n+N5MDoAA10dW
 L6AToCuUKWh0HA6fL9jcmwzZEVdihOlJ13QuYtzzgYjZunMDnEuwYj
 MBBGAG10dWQxMBaAFEjmaPkr8K70Y1AATxY3k/j/ZZZ5AI1dJQQVMBG
 AQQFbMWBgggBGFB0cDAdjANBZZZgZG9wOBAUFAAO8gQBQg8lU1VJ/DO
 IG1rr10t8VoNZ7ZZZI+geQL0mmZtJlDrkbaeH04N3x3q5QVZS/h4JZ
 FeRHFFyfGZZZ4hXHwZQZf/PjWjhpPKEwsiKFaAGJS5VzP3bMG8tGan0z
 wPZZZpMmvPI3U12W+76byvVVe==
-----END CERTIFICATE-----
```

b. Double-click on the new file that you created and a Certificate dialog box opens.

c. Click on the Certification Path tab.

d. Look at the tree-like structure representing the full certificate chain. The top of the chain is referred to as the root Certificate Authority (CA). The bottom of the chain represents your server’s certificate. If your server is not listed one-level below the root CA, then your certificate was issued by an intermediary CA. However, if your server is listed one-level below the root CA, then the certificate was issued by the root CA. For example, the following screen capture shows a certificate chain where an intermediary CA, VeriSign Class 3 Secure Server CA, issued a certificate for stgw.lotus.com.
2. If the server certificate is not issued by an intermediary CA, stop here and click Next topic at the bottom of this topic.

2. One you determine that the certificate is an intermediate certificate, you must export the certificate from the chain into its own certificate file:

a. Double-click the server’s certificate (i.e. server.cer) file and a Certificate dialog box opens.

b. Click Certification Path tab.

c. Highlight an entry of the certificate chain.

d. Click View Certificate.

e. In the Certificate dialog window, click the Details tab.

f. Click Copy to File...

g. In the Certificate Export Wizard that appears, click Next.

h. Select Base-64 encoded X.509 (.CER), and click Next.

i. Type in a unique name for the certificate you are exporting and click Next. For example, "VS-intermediary-CA" for VeriSign’s intermediary certificate authority.

j. Click Finish.

k. Click OK in the dialog box that displays the following message: The export was successful.

l. Repeat the preceding sub steps for each intermediate certificate in the chain. Note that there is no need to repeat these steps for the bottom entry of the chain because the server’s certificate already exists. When you are done, you will have a certificate file (.cer) for each entry of the chain. In our example, there are three certificate files:
<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Name</th>
<th>Certificate file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>VeriSign Class 3 Public Primary CA</td>
<td>VS-root-CA.cer</td>
</tr>
<tr>
<td>Intermediary</td>
<td>VeriSign Class 3 Secure Server CA</td>
<td>VS-intermediary-CA.cer</td>
</tr>
<tr>
<td>Server</td>
<td>stgw.lotus.com</td>
<td>stgw.cer</td>
</tr>
</tbody>
</table>

3. Finally, import the intermediary CA certificate into the keystore by completing the following steps:
   a. Using the Integrated Solutions Console, click **Security > SSL Certificate and key management**.
   b. Click **Key stores and certificates**.
   c. Click **CellDefaultKeyStore**.
   d. Click **Signer certificates**.
   e. Click **Add**.
   f. In the **Alias** field, type a short descriptive name for the certificate. For example, "Verisign Intermediary CA."
   g. In the **File name** field, type the path to the certificate file of the intermediary CA. For example, C:\certs\VS-intermediary-CA.cer.
   h. Accept the default file data type.
   i. Click **Apply** and **Save**.
   j. Repeat the preceding steps for each intermediary CA that is part of the certificate chain. In most cases, only one intermediary CA exists.

**Receiving a signed certificate:**

A Certificate Authority (CA) creates a certificate from a certificate request. WebSphere Application Server keystore receives the certificate from the CA and generates a CA-signed personal certificate that your Sametime Gateway cluster can use for Secure Sockets Layer (SSL) security.

**Before you begin**

The keystore must contain the certificate request that was created and sent to the Certificate Authority. Also, the keystore must be able to access the certificate that is returned by the Certificate Authority.

Expected state: the Deployment Manager and the node agents are started. The servers are stopped.

**Note:** WebSphere Application Server creates the certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Be sure to import all intermediate certificates as signer certificates into the keystore before receiving the CA-signed certificate.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Security > SSL certificate and key management > Key stores and certificates**.
3. Click the **keystore** that you created previously.
4. Click Personal certificates.
5. Click Receive a certificate from a certificate authority.
6. Type the full path and name of the certificate file generated by the CA.
7. Select the appropriate data from the list.
8. Click Apply and Save.

What to do next

Now you are ready to define a new SSL configuration.

Defining the SSL configuration for a cluster:

Complete these steps to create a new SSL configuration for a cluster of Sametime Gateway servers.

About this task

Secure Sockets Layer (SSL) configurations contain the attributes that you need to control the behavior of client and server SSL endpoints. You create a single SSL configuration to be used on the inbound and outbound trees in the configuration topology.

Expected state: the Deployment Manager and node agents are started. The servers are stopped.

Procedure

1. Using the Integrated Solutions Console, click Security > SSL certificate and key management > SSL Configurations.
2. Click New to display the SSL configuration panel.
3. Type name in the Name field for your SSL configuration.
4. In the Trust store name drop-down list, replace the default CellDefaultKeyStore value with CellDefaultTrustStore. The truststore name refers to a specific truststore that holds signer certificates that validate the trust of certificates sent by remote connections during an SSL handshake.
5. Select the keystore that you created from the Keystore name drop-down list. A keystore contains the personal certificates that represent a signer identity and the private key that WebSphere Application Server uses to encrypt and sign data.
6. Click Get certificate aliases.
7. Select your certificate alias as the default server certificate alias.
8. Select your certificate alias as the default client certificate alias.
9. Click Apply, and then Save.
10. Synchronize your changes to all nodes in the cluster. Click System Administration > Nodes.
11. Select all nodes in the cluster, then click Full Resynchronize.

Obtaining the root certificate:

Download a certificate authority’s (CA) root certificate. After you download the certificate, you must add it to the WebSphere Application Server truststore. For connections to AOL, download the Equifax Secure CA because this certificate is used by both communities. For connections to XMPP communities, you must
determine what root certificate, if any, is being used, and then check to see if WebSphere Application Server already recognizes the certificate, and, if necessary, download and add the certificate to your truststore.

**About this task**

XMPP communities are free to use either a TLS/SSL or TCP connection, so a certificate may not be needed. If the XMPP community is using TLS/SSL, the root certificate CA may already be in the WebSphere Application Server truststore. If not, you must obtain it.

**Procedure**

1. To obtain the same certificate used by AOL:
   b. In the list of certificates, navigate to the following:
      All other SSL certificates except for Quick SSL: Equifax Secure Certificate Authority
   c. Select the following download:
      Download - Equifax Secure Certificate Authority (Base-64 encoded X.509)
   d. Add this root CA to your WebSphere Application Server truststore (see next step in setting up SSL).

2. AOL users require additional certificates:
   a. Navigate to [https://pki-info.aol.com/AOL/](https://pki-info.aol.com/AOL/) and download both the "America Online Root CA 1" certificate and the "America Online Root CA 2" certificate.
   b. Navigate to [https://pki-info.aol.com/AOLMSPKI/index.html](https://pki-info.aol.com/AOLMSPKI/index.html) and download the "AOL Member CA" certificate.

3. To obtain a root certificate used by a XMPP community:
   a. Check with the XMPP community to determine which trusted certificate authority they are using.
   b. Determine if WebSphere Application Server supports the certificate.
   c. If the certificate is recognized, there's nothing more to do on this step.
   d. If the certificate is not recognized, obtain the certificate from the CA and add it to your truststore (see next step in setting up SSL).

**What to do next**

If for any reason the root certificate authority for an instant messaging community changes or you add an additional instant messaging community to your Sametime Gateway, you must explicitly add the new root CA to your WebSphere Application Server truststore.

**Adding a trusted CA certificate to the keystore:**

Add your new Certificate Authority certificate to the keystore to establish the trust relationship in SSL communication.

**Before you begin**

The keystore that you want to add the CA certificate to must already exist.
Expected state: the Deployment Manager and node agents are started. The servers are stopped.

Procedure
1. In the Integrated Solutions Console, click **Security > SSL certificates and key management**.
2. Click **Key stores and certificates > CellDefaultTrustStore > Signer certificates**.
3. Click **Add**.
4. Type a certificate alias in the **Alias** field. The alias is how the certificate is referenced in the keystore.
5. In the **File name** field, type the file name and path to where the certificate is located.
6. Select the appropriate file data type.
7. Click **Apply** and then **Save**.
8. Synchronize your changes to all nodes in the cluster. Click **System Administration > Nodes**.
9. Select all nodes in the cluster, then click **Full Resynchronize**.
10. Open a command window.
11. In the command window, stop the Deployment Manager and wait for the command to finish, and then restart the Deployment Manager. Use the user name and password that you provided when you enabled administrative security to stop the Deployment Manager. Open a command window and navigate to the `stgw_profile_root\bin` directory and use the following commands:
   
   **AIX, Linux, and Solaris**
   
   ```
   ./stopManager.sh -username username -password password
   ./startManager.sh
   ```

   **Windows**
   
   ```
   stopManager.bat -username username -password password
   startManager.bat
   ```

   **IBM i**
   
   ```
   stopManager -username username -password password
   startManager
   ```

12. Restart the node agents.
   b. Click **System Administration > Node agents**.
   c. Select all node agents, and then click **Restart**.
13. Choose **Servers > Clusters**.
14. Select the Sametime Gateway cluster and click **Start**.
15. Click **Servers > Proxy servers**. Note that if you are not connecting to any instant messaging service over SIP, it’s not necessary to start the SIP proxy server.
16. Select the SIP proxy server or servers and click **Start**.
17. Choose **Server > Application servers**.
18. Select the XMPP proxy server and click **Start**. Note that if you are not connecting to any instant messaging service over XMPP, it’s not necessary to start the XMPP proxy server.
Configuring the SIP proxy server to use SSL:

Apply the new SSL definition to the SIP proxy server.

Before you begin

Expected state: the Deployment Manager, node agents, and all servers in the cluster are started.

Procedure

1. In the Integrated Solutions Console, click Security > SSL certificate and key management > Manage endpoint security configurations.
2. Expand the Inbound node on the local topology tree.
   a. Expand cell with sip proxy.
   b. Expand nodes.
   c. Expand node with sip proxy.
   d. Expand servers.
3. Select sip proxy server from the tree.
4. On the configuration panel, select Override inherited values.
5. Select the SSL configuration that you defined from the SSL configuration list.
6. Click Update certificate alias list.
7. Select your certificate alias from the Certificate alias in key store list.
8. Click Apply.
9. Repeat the preceding steps on the Outbound node of the local topology tree.
10. Change the SSL configuration on the SIP proxy server:
    a. Click Servers > Proxy Servers > name of your SIP proxy server > SIP Proxy Server Settings > SIP proxy server transports > SIPS PROXY CHAIN > SSL inbound channel (SSL_4).
    b. Under SSL Configuration, select Centrally Managed.
    c. Click OK, and then Save.
11. Synchronize your changes to all nodes in the cluster. Click System Administration > Nodes.
12. Select all nodes in the cluster, then click Full Resynchronize.
13. Open a command window.
14. In the command window, stop the Deployment Manager and wait for the command to finish, and then restart the Deployment Manager. Use the user name and password that you provided when you enabled administrative security to stop the Deployment Manager. Open a command window and navigate to the stgw_profile_root\bin directory and use the following commands:
    AIX, Linux, and Solaris
    ./stopManager.sh -username username -password password
    ./startManager.sh
    Windows
    stopManager.bat -username username -password password
    startManager.bat
    IBM i
    stopManager -username username -password password
    startManager
15. Restart the node agents.

b. Click System Administration > Node agents.

c. Select all node agents, and then click Restart.

16. Click Servers > Clusters.
17. Select the Sametime Gateway cluster, and click Stop, and wait for the cluster to stop.
18. Click Servers > Clusters.
19. Select the Sametime Gateway cluster, and click Start.
20. Click Servers > Proxy servers.
21. Select the SIP proxy server and click Start.

What to do next

Now you can exchange signer certificates with other server communities.

Configuring the XMPP proxy server to use SSL:

Apply the new SSL definition to the XMPP proxy server.

Before you begin

Expected state: the Deployment Manager, node agents, and all servers in the cluster are started.

Procedure

1. In the Integrated Solutions Console, click Security > SSL certificate and key management > Manage endpoint security configurations.
2. Expand the Inbound node on the local topology tree.
   a. Expand cell with XMPP proxy.
   b. Expand nodes.
   c. Select the node with the XMPP proxy.
3. On the configuration panel, select Override inherited values.
4. Make sure NodeDefaultSSLSettings is selected in the SSL configuration drop-down list.
5. Click Update certificate alias list.
6. Select your certificate alias from the Certificate alias in key store drop-down list.
7. Click Apply.
8. Repeat the preceding steps on the Outbound node of the local topology tree.
9. Click OK and Save.

What to do next

Now you can exchange signer certificates with other server communities.

Replacing and renewing a certificate in a Gateway cluster:

Replacing or renewing a certificate for an IBM Sametime Gateway cluster is similar to importing it for the first time, but you also replace the old certificate with the new one.
Before you begin

The keystore must contain the certificate request that was created and sent to the Certificate Authority. Also, the keystore must be able to access the certificate that is returned by the Certificate Authority.

Expected state: the Deployment Manager and the node agents are started. The servers are stopped.

Note: WebSphere Application Server creates the certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Be sure to import all intermediate certificates as signer certificates into the keystore before receiving the CA-signed certificate.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Key stores and certificates.
3. Click the keystore that you created previously.
4. Click Personal certificates.
5. Click Receive a certificate from a certificate authority.
6. Type the full path and name of the certificate file generated by the CA.
7. Select the appropriate data from the list.
8. Click Apply and Save.
9. From the Integrated Solutions Console, click Security > SSL certificate and key management > Key stores and certificates.
10. Select the keystore that contains the new and old certificates.
11. Select the old certificate and click Replace.
12. Verify that the old certificate is listed in the "Old certificate" field.
13. Select the new certificate from the "Replace with" list.
14. Click OK and Save.
15. Restart the Sametime Gateway server.
   For a standalone: the single Java process.
   For a cluster configuration: restart the DMGR, STGW servers, XMPP proxies, SIP Proxies.
   You do not need to restart the node agents.

List of supported Certificate Authorities
Certificate authorities (CAs) can issue public key certificates which state that the CA attests that the public key contained in the certificate belongs to you. You then use your CA-signed certificate to exchange certificates with AOL and XMPP to provide for the secure exchange of instant messages.

Certificate vendors sometimes change the product names of their offerings without changing the underlying CA certificate. AOL and XMPP cannot keep track of all the product-naming conventions of each certificate vendor.
Attention: Server certificate installed on Sametime Gateway must conform to RFC 3280 certificate standards. When requesting a certificate, make sure the certificate supports both server and client authentication. Some certificate authorities provide certificates that support server authentication only or client authentication only. Certificates must include both server and client authentication EKU flags. Thawte certificates in the following list meet these standards. It is your responsibility to make sure that the certificate supports both.

As part of a public key infrastructure (PKI), a CA checks with a registration authority to verify information provided by your digital certificate. If the registration authority verifies your information, the CA can then issue a certificate to you.

For the current list of Certificate Authorities and accepted by Sametime Gateway and AOL and XMPP, see the IBM FAQ Tech Note #1372445, “List of Certificate Authorities (CAs) accepted by Sametime Gateway” at: www.ibm.com/support/docview.wss?uid=swg21372445

Setting up email notifications for certificate expiration

This optional procedure allows the Sametime Gateway administrator to receive email notifications about SSL certificates that are about to expire soon.

About this task

Follow these steps to create a list of people who need to be notified of SSL certificate expirations.

Procedure

1. On the Sametime Gateway, log in to the Integrated Solutions Console.
2. Click Security > SSL Certificate and key management > Manage certificate expiration.
3. Click NotificationsMessageLog.
4. Select Email sent to notification list.
5. In the Email address to add field, add the administrator's email address.
6. In the Outgoing mail (SMTP) server, provide your organization's outgoing SMTP server host name.
7. Click to add the email address to the list of email addresses.
8. Repeat Steps 4 - 6 for additional email addresses you want to add.
9. Click OK.
10. Click Save.

Setting up compliance for FIPS 140-2

IBM Sametime supports the U.S. government-defined security requirements for cryptographic modules known as FIPS 140-2 (Federal Information Processing Standard 140-2). If your Sametime deployment must maintain FIPS 140-compliance for all data exchanged between clients and Sametime Community Servers, you must install the FIPS Server on the Sametime Proxy Server to accept data on behalf of Sametime Community Servers.

Installing the FIPS administration portlet

To administer the FIPS Server from the Sametime System Console, you must install the FIPS administration portlet before you install the FIPS Server.
Procedure

Install the FIPS administration portlet into the Sametime System Console of the Integrated Solutions Console. Go to WebSphere\STSCServerCell\optionalConsoleApps\fips.proxyadmin and install the portlet using the instructions in the readme.txt.

Results

Note: After you install the FIPS server on the Sametime Proxy server, you can make configuration changes. Always restart the Sametime Proxy Server if you make any configuration changes using the administration portlet. Currently, you cannot administer the per-node configuration or vertical clustering of FIPS on the Sametime System Console. The administrative portlet only administers and therefore shows registered cell deployments or horizontal cluster deployments. It will not show individual primary or secondary nodes of the cluster.

Installing the FIPS Server

IBM Sametime supports the U.S. government-defined security requirements for cryptographic modules known as FIPS 140-2 (Federal Information Processing Standard 140-2). Installing the FIPS Server is only necessary if your Sametime deployment must be FIPS-compliant; otherwise, it is optional.

Before you begin

You should have already installed the IBM Sametime System Console and the Sametime Proxy Server. If you want to administer the FIPS Server from the Sametime System Console, you should have already installed the FIPS administration portlet.

If you did not install the FIPS administration portlet, you can manage the FIPS Server using information in FIPS Support for IBM Sametime 8.

About this task

The FIPS administration portlet can connect to the FIPS Server only if the server is installed on the Sametime Proxy Server. You cannot have multiple FIPS Servers running on the same machine.

Note: Currently, you cannot administer the per-node configuration or vertical clustering of FIPS on the Sametime System Console. The administrative portlet only administers and therefore shows registered cell deployments or horizontal cluster deployments. It will not show individual primary or secondary nodes of the cluster.

Procedure

1. On the server where you will install the FIPS server, enable FIPS on the WebSphere Application Server by following the procedure in Configuring Federal Information Processing Standard Java Secure Socket Extension files.
2. Copy sametimefipsproxy.war from setup\STIPLaunchpad\disk1\FIPSProxy on the image disk to your local drive.
3. Log in to the Integrated Solutions Console on the machine where you are installing the FIPS Server.
4. Click Applications > Application Types > WebSphere Enterprise Applications.

5. On the Enterprise Applications page, click Install.

6. Under Path to the new application, browse to the sametimefipsproxy.war file. Keep the default settings to install the server, and then click Next.

7. Enter the context root that you want for the FIPS Server, for example, /fipsProxy.

8. Click Finish and save the configuration.

9. Restart the Sametime Proxy Server to automatically start the FIPS Server.

10. Log in to the Integrated Solutions Console.

11. Click Sametime System Console > Sametime Servers > FIPS Proxy Servers.
You can only edit data for FIPS if the FIPS war is running on the installed server. Make sure that your FIPS Server is running in order to administer it.

12. Click the FIPS Server that you installed.

13. Enter a fully qualified inbound host name and port and an outbound host name and port to which FIPS connects.

If you are using the FIPS administration portlet, also replace the serverAddress entries with entries for the Sametime Community server that is connected to the Sametime Proxy Server. Click OK.

14. Restart the Sametime Proxy Server again to automatically start the FIPS Server.

15. In a text editor, open the sametimeProxy.xml file. This file defines the port routing so the TLS connections can use the proxy to access the Sametime server.

The file is located in the \WebSphere\AppServer\profiles\profile_name\installedApps\cell_name\sametimefipsproxy_war.ear\sametimefipsproxy.war directory.

16. If you are using the FIPS administration portlet, skip to the next step.

If you are not using the FIPS administration portlet, edit the SametimeProxyChannel properties in the sametimeProxy.xml file. Replace the serverAddress entries with entries for the Sametime Community server that is connected to the Sametime Proxy Server.

In the following entries, replace "temp.sametimeserver.com" with your Sametime server name, for example, "yourserver.yourdomain.com".

```
<channel name="SametimeProxyChannel" factory="com.ibm.sametime.proxy.channel.impl.SametimeProxyChannelFactory" sequence="2" weight="1">
...
<property name="serverAddress1" value="temp.sametimeserver.com:8081" />
<property name="clientAddress2" value="*:1533" />
<property name="serverAddress2" value="temp.sametimeserver.com:1533" />
<property name="clientAddress3" value="*:554" />
<property name="serverAddress3" value="temp.sametimeserver.com:554" />
...
</channel>
```

17. Edit the TLSInboundChannel properties in the sametimeProxy.xml file:

- For the com.ibm.ssl.keyStore property, replace the wccmDefault value of DummyServerKeyFile.jks with the actual keyFileName and location for the keystore on this WebSphere Application Server. Replace the file://c: designation with the operating system’s absolute path to the file.

- For the com.ibm.ssl.trustStore property, replace the wccmDefault value of DummyServerTrustFile.jks with the actual trustFileName and location for the keystore on this WebSphere Application Server. Replace the file://c: designation with the operating system’s absolute path to the file.
<channel name="TLSInboundChannel" factory="com.ibm.ws.ssl.channel.impl.SSLChannelFactory" sequence="2" weight="1">

For the com.ibm.ssl.protocol property, replace the SSLv3 value with TLSv1.

18. Close and save the file.

19. Restart the Sametime Proxy Server again to put the configuration changes into effect.

Results

Sametime Connect clients use the "Direct connection using TLS" Connection option when setting up the server community connected to the FIPS-enabled server.

Setting up single sign-on (SSO) for Sametime clients

Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

Preparing servers running on WebSphere Application Server for single sign-on

Prepare for single sign-on (SSO) by exporting a LTPA key from the servers running on WebSphere Application Server. This step applies to the Sametime Media Manager SIP Proxy and Registrar server, the Sametime Meeting server, and Sametime Advanced. If you plan to enable the Click to Call feature, it also applies to the Sametime Unified Telephony Application Server. The Sametime Proxy Server does not need to be set up for single sign-on.

Before you begin

Servers using SSO must use the same LDAP directory that the Sametime Community Server uses.

About this task

The Sametime Community Server installation creates a Domino SSO key. You must replace the Domino SSO key with a WebSphere LTPA key to allow the Sametime Community server running on Domino and the other servers running on WebSphere Application Server to have an identical key for token validation and generation. If Sametime servers running on WebSphere Application Server are managed by different Sametime System Console, you must export the LTPA key from one of the servers (the Media Manager SIP Proxy and Registrar, Meeting Server, or Advanced server).

Procedure

1. Log in to the Integrated Solutions Console for the Sametime server.
3. Make sure that the Domain name matches the Sametime Server domain.

   **Note:** Verify that **Interoperability Mode** is selected.

4. Click **OK** and save the master configuration.

5. Click **Security > Global Security**.

6. Under Authentication, click **LTPA**.

7. In the LTPA timeout section, set the timeout value to a value larger than the default to minimize the potential for an LTPA token to expire during an active meeting. A value that covers a period somewhat longer than a typical work day, such as 600 minutes, is recommended.

8. Under Cross Cell single sign-on, enter a Password, confirm the password, and specify a file name to store the key. Click **Export keys**. Make a note of the location of the file created. You need to know its location when you import the file to the Sametime Community Server.

9. Navigate to the directory where you exported the LTPA key.

10. Copy the LTPA key to a location where you can access the file from the Sametime Community Server.

**Configuring the Sametime Community Server for single sign-on**

After creating LTPA keys for Sametime servers, configure the Sametime Community Server for single sign-on.

**Before you begin**

Make sure all servers use the same LDAP directory.

**About this task**

By default the Sametime installation creates a Domino SSO key. This key should be replaced by the WebSphere LTPA key you exported in the previous section, preparing servers running WebSphere Application Server for single sign-on. Follow these steps to import the LTPA key from WebSphere to Domino.

**Procedure**

1. Import the LTPA keys used by Sametime servers in the same DNS domain.
   b. Click **Configuration > Web Web Configurations** view.
   c. Open the **Web SSO Configuration for LtpaToken** document.
   d. Click **Edit SSO Configuration**.
   e. Click **Keys > Import WebSphere LTPA keys**.
   f. Type in the exact file location of the key file you created on the Sametime SIP Proxy and Registrar server.
   g. Enter the password you created on the server when you enabled single sign-on.
   h. Click **OK**.
      The message “Successfully imported WebSphere LTPA keys” appears after the key has been imported.

2. **For Domino 8.0 and higher:**
Note: Sametime 8.5 requires Lotus Domino 8.0 and higher; if you are maintaining an older Sametime server it may be running a version of Lotus Domino prior to R8.

In the Token Format field of the WebSphere Information section, select the LTPA token formats to be supported by Domino.

- LtpaToken - LTPAv1 only
- LtpaToken2 - LTPAv2 only
- LtpaToken and LtpaToken2 - both LTPAv1 and LTPAv2 formats are supported

With this last option selected, both tokens are created, but the token returned to the client is determined by the TOKEN_TYPE_TO_RETURN flag under the AuthToken section of sametime.ini. The default value is LTPA, which returns the LTPAv1 token. Changing the value to LTPA2 results in the LTPAv2 token being returned instead.

3. Click Save and Close.

4. Configure the Sametime Community Server so that LtpaToken gets set by the Sametime Proxy web client instead of the Sametime token:
   a. Log in to the Sametime System Console as the Sametime administrator.
   b. Click Sametime Servers > Sametime Community Servers.
   c. In the list of Community Servers, click the name of a Sametime Community Server to open its Configuration page.
   d. Click the Community Services tab.
   e. Under the "General" section, select the authentication type that users can use while logging into the community server: LTPA only.

5. Restart the Lotus Domino server to put your changes into effect.

Importing a shared LTPA key to enable SSO for a server in a different cell

If you set up SSO between IBM Sametime servers running on WebSphere Application Server that are in different cells, import the shared LTPA key you exported as described in “Preparing servers running on WebSphere Application Server for single sign-on” into each Media Manager SIP Proxy and Registrar server, Sametime Meeting Server, and Advanced server that is part of the same SSO environment. If the servers are managed by one Sametime System Console, you do not need to perform this step because they already share the same LTPA key.

Procedure

1. From the Integrated Solutions Console of the Sametime server, click Global security > LTPA.
2. Scroll down to "Cross-cell single sign-on."
3. In the Password and Confirm password fields, enter the password that is used to decrypt the LTPA keys. This password must match the password that was used in the cell from which you are importing the keys.
4. Enter the fully qualified key file name, and click Import.
5. Click Apply and then Save.
6. Restart the Sametime server to put your changes into effect.
7. Repeat these steps for every Sametime server that belongs to a different cell.
What to do next

From the Deployment Manager's Integrated Solutions Console, select all nodes in the environment and select Full Resynchronize. Then start or restart all node agents.

Verifying that servers have the same single sign-on settings

Confirm that the IBM Sametime Meeting Server and the Media Manager SIP Proxy and Registrar server use the same SSO settings.

About this task

Check the settings first on the Meeting Server, then on the Media Manager SIP Proxy and Registrar server and verify that they are the same.

Procedure

1. Log in to the server's Integrated Solutions Console.
3. Make a note of the domain name and Interoperability mode.

Results

Both servers must have the same settings for single sign-on to work.

Configuring single sign-on with WebSphere Portal

If you will use IBM Sametime with IBM WebSphere Portal, you can enable single sign-on by importing the WebSphere Portal LTPA token into the IBM Domino server used by Sametime, and then configuring WebSphere-based servers from both deployments to use the same realm.

Procedure

1. Retrieve the realm name used in WebSphere Portal:
   a. On the server hosting WebSphere Portal, log into the Integrated Solutions Console as the WebSphere administrator.
   b. In the navigator, click Security > Global Security.
   c. Under "User account repository", select the federated repository and then click the Configure button.
   d. Write down the name shown in the Realm name field; you will need the name in step 4 of this task.
   e. Click Cancel to ensure you do not make any accidental changes.
   f. Leave the Integrated Solutions Console open for the next step.
2. Export the LTPA used by WebSphere Portal:
   a. In the Integrated Solutions Console navigator, click Security > Global Security.
   b. Under "Authentication", click Authentication mechanisms > LTPA.
   c. Look under "Additional properties" and click Single signon (SSO).
   d. Make sure Web inbound security attribute propagation is not selected (if you must make a change to it now, click Apply to save it).
   e. Click the LTPA link to return to the Configuration page.
   f. Type a password in the Password field and note it down for use in step 3.
g. Type a name, path, and file name in the **Key File Name** field.

h. Click the **Export Keys** button

i. If you changed any settings (for example, in substep 2e), save the changes to the master configuration by clicking the **Save** link in the "Messages" box at the top of the page.

j. Log out of the Integrated Solutions Console.

k. Copy the exported file to a place that is accessible by the Domino servers hosting the Sametime Community Servers.

3. Import the LTPA token into Domino on every Sametime Community Server:


   b. Click **Configuration > Web > Web Configurations**.

   c. Open the **Web SSO Configuration for LtpaToken** document.

   d. Click **Edit SSO Configuration**.

   e. Click **Keys > Import WebSphere LTPA keys**.

   f. Type the exact path and file name of the key file you exported from WebSphere Portal in step 2.

   g. Type the password you created with the key file when you exported it from WebSphere Portal in step 2.

   h. Click **OK** to import the LTPA token from the key file into Domino.

      The message **Successfully imported WebSphere LTPA keys** appears after the key has been imported.

   i. **Important**: Make sure the realm name matches the realm used by WebSphere Portal.

      A Portal realm often uses the value `ldaphost:389` as display, which must be modified to `ldaphost:/389` in Domino before saving the SSO configuration.

   j. Click **Save** to update the SSO configuration for this Domino server.

   k. Repeat this process on every Sametime Community Server.

4. Configure all WebSphere-based Sametime servers to use the same LTPA realm as WebSphere Portal.

   a. On the Sametime server cell’s (or cluster’s) deployment manager, log into the WebSphere Application Server’s Integrated Solutions Console as the WebSphere administrator.

      In Sametime, the System Console typically serves as the deployment manager for cells and clusters.

   b. In the navigator, click **Security > Global Security**.

   c. Under "User account repository", select the federated repository and then click the **Configure** button.

   d. In the **Realm name** field, delete the existing name and type the realm name used in WebSphere Portal, making sure to match it exactly (including spelling and capitalization).

      This is the realm name that you wrote down in step 1.

   e. Click **OK**.

   f. Save the changes to the master configuration by clicking the **Save** link in the "Messages" box at the top of the page.

   g. In the navigator, click **Users and Groups > Administrative user roles**.

   h. Select all administrators (click the check box in front of each user name), and reassign all roles to those users.
Important: After you change the realm definition, you must map the \texttt{wsadmin} account to the required security and administrative roles for use within the new realm.

i. Save the changes to the master configuration by clicking the \texttt{Save} link in the "Messages" box at the top of the page.

j. Restart the deployment manager.

k. If you deployed multiple cells or clusters, repeat this process on every deployment manager.

For example, you must update the deployment manager associated with each type of Sametime server, whether it is deployed as a single-server cell or as a cluster.

5. After all of the Sametime cells and clusters have been updated to use the WebSphere Portal realm, manually synchronize the nodes within each cell or cluster:

   a. On a node, stop the nodeagent and all application servers.
   
   b. Open a command prompt and navigate to the following directory: \texttt{websphere/apps\server/profiles/Profile\_Name/bin}.

   c. Run the following command:

      \texttt{IBM AIX, Linux, Solaris}
      
      \texttt{syncNode.sh dMgr\_Host\_Name.comSOAP\_port}

      \texttt{Microsoft Windows}
      
      \texttt{syncNode.bat dMgr\_Host\_Name.comSOAP\_port}

   where:

   \begin{itemize}
   \item \texttt{dMgr\_Host\_Name.com} is the fully qualified host name of the cell or cluster’s deployment manager.
   \item \texttt{SOAP\_port} is the deployment manager’s SOAP port; typically 8703.
   \end{itemize}

   d. Restart the nodeagent and application servers.

   e. Repeat for every node within the current cell or cluster; then proceed to the next cell or cluster and repeat the manual synchronization process.

6. Monitor each cell or cluster’s startserver and systemout logs for any errors related to security, as this may indicate that the new realm information is not entirely in sync and you may need repeat the synchronization process in step 5.

### Configuring single sign-on with Microsoft Windows Active Directory

The Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) replaces Microsoft Windows Single Sign-On, which is no longer supported by Sametime. If the Sametime Community Server uses a Microsoft Windows Active Directory, you must integrate all server components to allow Sametime users to log in and authenticate only once at their desktop and thereafter automatically authenticate with the Sametime server.

**About this task**

This white paper on the developerWorks site explains the procedure:

Integrating SPNEGO with IBM Sametime components using IBM WebSphere Application Server 7.0
Configuring security for the Sametime Community Server

The IBM Sametime server uses the Internet and intranet security features of the Domino server on which it is installed to authenticate web browser users who access Domino databases on the server.

About this task

Follow the instructions in this section to set up SSL, HTTP tunneling, and user authentication.

Authentication by token using LTPA and Sametime tokens

Sametime uses authentication by token to authenticate connections that occur after a user has authenticated to Domino once using password authentication.

Authentication by token prevents a user from having to re-enter authentication credentials when accessing different servers or using Sametime web clients or Domino applications that connect to a Sametime server.

The Sametime server includes two separate security features capable of generating the authentication token used by Sametime:

• Domino Single Sign-On (SSO) authentication feature - The Domino SSO feature must be enabled on a Sametime server.

  If the Domino SSO feature is not enabled on the Domino server when you install Sametime, the Sametime installation automatically enables and configures the Domino SSO feature. In some environments, you might need to alter the default SSO configuration provided by the Sametime installation. For more information, see Altering the Domino Web SSO configuration following the Sametime server installation.

  The user must enter the fully qualified domain name of the Sametime server (for example, sametimeserver.meetings.example.com) in the web browser URL locator when accessing the Sametime server to authenticate successfully using SSO.

  If your Sametime environment includes only Sametime 3.0 (or higher) servers, and you do not use Sametime TeamRoom or Discussion databases that were available with earlier Sametime server releases, only the Domino SSO feature is required to support authentication by token.

  If your Sametime environment includes Sametime 3.0 (or higher) servers that interoperate with Sametime servers from releases earlier than Sametime 3.0, both the Domino SSO feature and the Secrets and Tokens databases must be supported on the Sametime server to enforce authentication by token.

  Sametime includes a custom logon form for the SSO feature. This custom logon form can be used in place of the default SSO logon form. The custom logon form is presented to the user the first time the user accesses a database on the server that requires basic password authentication.

Note: If the Sametime Server is configured to use Internet Sites, the Notes client integration with Sametime (and therefore SSO with Sametime) has been supported only since Sametime 8.5.1 and Notes client 8.5. When configuring the Sametime Server to use Internet Sites the following settings must be configured under the [AuthToken] section of the sametime.ini file:

• ST_TOKEN_TYPE must contain the name of the Web SSO document used by the Sametime Community server. The default value is LtpaToken.
• **ST_ORG_NAME** must contain the organization name that is set in the Web SSO document used by Sametime Community server. The default value is an empty organization name.

For additional information about the Domino Internet Sites configuration see Domino documentation.

• Secrets and Tokens authentication databases - Sametime server releases earlier than Sametime 3.0 used only the Secrets and Tokens authentication databases to create authentication tokens. When Sametime 8.x operates in environments that include servers from Sametime releases earlier than Sametime 3.0, the Sametime 8.x server supports both the Domino SSO feature and the Secrets and Tokens authentication databases.

A Sametime 8.x server supports Secrets and Tokens authentication by default. The following are required to support Secrets and Tokens authentication:

  - The Secrets and Tokens databases must be present on the server following a Sametime server installation.
  
  - The "Allow users to authenticate using either LTPA token or Sametime Token (stauths.nsf and stautht.nsf)" option must be selected in the Configuration-Community Services-General settings of the Sametime Administration Tool.

Both conditions above exist on a Sametime server following the server installation, so no additional procedures are required to support Secrets and Tokens authentication following the installation. However, if you have enhanced security by enabling the SametimeSecretsGenerator agent in one Secrets database on one Sametime server in your community, you must ensure that this Secrets database is replicated to all Sametime servers in the community. For more information, see Replicating the Secrets database (optional).

**Authentication by token using the Domino Single Sign-On (SSO) feature**

The Domino Single Sign-On (SSO) feature must be enabled on the Sametime server. This feature creates Lightweight Third Party Authentication (LTPA) tokens that enable web browser users to log in a single time to access multiple Sametime, Domino, or IBM WebSphere servers that are in the same DNS domain. This capability is called "single sign-on."

Sametime also uses LTPA tokens to authenticate connections from Sametime clients to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services on the Sametime server. These clients are Java applets and include the Meeting Room client, and Recorded Meeting client.

Sametime supports two versions of LTPA tokens: LTPAv1 and LTPAv2. Sametime allows authenticating by a single LTPA token or by a list of LTPA tokens. For example, a client can send an LTPAv1 token and LTPAv2 token in the same authentication request to authenticate a user. The Domino configuration determines which token is validated.

The LTPA token types supported by Domino are configured in the Web SSO document in names.nsf. When using a Domino SSO key, only LTPAv1 tokens are supported. When importing a WebSphere LTPA key, both LTPAv1 and LTPAv2 tokens are supported by Domino. The supported formats are defined in the Token Format field under the WebSphere Information section of the Web SSO document.
Sametime can generate a single LTPA token or a list of LTPA tokens depending on the SSO key that is configured in Domino and the Token Format field in the case of WebSphere LTPA keys.

**Note:** Sametime also requires users to present an authentication token when attending an instant meeting. Client applications generate this token from the user’s home Sametime server. Users with Sametime 2.5 (or earlier) home Sametime servers will present Sametime tokens (generated from the Secrets and Tokens databases) when connecting to instant meetings started on a Sametime 8.x server. For this reason, Sametime 8.x servers operating in Sametime environments that include Sametime servers from previous releases must also support the Secrets and Tokens databases for authentication by token.

Authentication by LTPA token occurs after a user has already authenticated once using password authentication. For example, authentication by token on a Sametime server might occur as follows:

1. A user accesses a Sametime Meeting Center database that requires authentication or clicks the “Log onto Sametime” link in the Sametime Meeting Center.
   
   **Note** To successfully authenticate, the user must enter the fully qualified domain name of the Sametime server (for example, sametimeserver.meeting.acme.com) in the web browser URL locator when accessing the Sametime server.

2. An SSO logon form appears, and the user enters a valid user name and password from the Domino Directory (or LDAP directory) to authenticate.
   
   **Note** Sametime provides a custom Sametime SSO logon form that can be enabled by the administrator. If the custom logon form is not enabled, the standard Domino SSO logon form displays to the user.

3. After a successful authentication, the Domino Single Sign-On (SSO) feature generates an LTPA token containing the user’s authentication information and passes the token to the user’s web browser in a cookie.
   
   The user’s web browser must have cookies enabled to accept the LTPA token.

4. The user attends a meeting, and the Meeting Room client loads in the user’s web browser.

5. The Meeting Room client connects to the Meeting Services and Community Services and passes the LTPA token to Sametime. The Meeting Services and Community Services connections are authenticated using the LTPA token. The user is not required to re-enter authentication credentials to authenticate these connections.

The same LTPA token described above can be used to authenticate the user when the user accesses other Sametime, Domino, or WebSphere servers in the same DNS domain during a single web browser session. The other Sametime, Domino, or WebSphere servers must also support the SSO feature (that is, the servers must accept LTPA tokens).

If the Domino SSO feature is not enabled when you install Sametime, the Sametime installation automatically enables and configures the Domino SSO feature. In some environments, it may be necessary to alter the SSO configuration following the Sametime server installation. For more information, see Altering the Domino Web SSO configuration following the Sametime server installation.
Related concepts:
Authentication by token using Secrets and Tokens databases
To authenticate by token, the Sametime server can accept an authentication token created by the Secrets and Tokens authentication databases, the Domino Single Sign-On (SSO) feature, or both. The Sametime server can also generate tokens using the Secrets and Tokens authentication databases or the Domino SSO feature.

Altering the Domino Web SSO configuration following the Sametime server installation:

The IBM Sametime installation automatically enables and configures the Domino SSO feature on the Domino server. In some cases, it may be necessary to alter the default configuration of the Domino SSO feature following the Sametime server installation.

This topic discusses the following issues pertaining to the Sametime installation and the Domino SSO feature:

- **SSO configurations performed by the Sametime installation** - This section explains how the Sametime installation configures the Domino Web SSO feature. You can use this information to determine if it is necessary to alter the default SSO configuration following a Sametime server installation.

- **Altering the SSO configuration** - This section explains the most common reasons for altering the SSO configuration following the Sametime server installation. In multiple Sametime server environments, it is frequently necessary to add the Domino server names of Sametime servers to the Domino Web SSO Configuration document.

- **Viewing and editing the Domino Web SSO configuration document** - This section explains how to edit the Domino Web SSO configuration document in the Domino Directory. This document contains the parameters for the Web SSO configuration that you may need to change.

- Sametime includes a custom SSO logon form. See Using the Sametime custom logon form for SSO for information about enabling this form following the Sametime server installation.

Note: If for some reason it is necessary to manually enable the Domino SSO feature, you can use the procedures described in Manually enabling the Domino SSO feature. You can also review these procedures to understand all configurations that are required to support SSO for the Sametime server.

**SSO configurations performed by the Sametime installation**

The Sametime installation enables the Domino SSO feature and performs the SSO configurations described below. The Sametime installation:

- Creates a Web SSO Configuration document named LtpaToken. This document contains the SSO configuration needed for generation and validation of LTPA tokens. The following fields are populated into this document:
  - DNS Domain - To populate the DNS Domain field, the installation determines the fully-qualified domain name of the Sametime server machine and then subtracts the hostname value from the fully-qualified domain name.

For example, if the installation determines the fully qualified name of the Sametime server is "Sametimeserver.east.acme.com," the installation writes ".east.acme.com" in the DNS Domain field.

The LTPA token is then valid for the servers that belong to the DNS domain specified in the DNS Domain field.
Expiration (minutes) - This field specifies the length of time for which the LTPA token is valid. This value is 30 minutes by default. You may want to provide a longer value for the token expiration. Lotus software recommends a setting of 120 minutes.

Domino Server Names: Each Domino/Sametime server that can accept the SSO token must be listed in the Domino Server Names field. By default, the installation writes only the name of the Domino server on which Sametime is installed in this field. It may be necessary to add the names of all other Domino/Sametime servers in the community to this field. For more information, see Altering the SSO configuration.

- Alters the Sametime/Domino server Server document. The installation changes the Internet Protocols-Domino Web Engine-Session authentication field in the Server document to the value "Multiple servers (SSO)." The Server authentication field must have the "Multiple servers (SSO)" value even if your Sametime community uses only one Sametime server. If the "Multiple server (SSO)" value is not selected, the SSO feature will not function properly for Sametime.
- Automatically configures the Sametime server to use the Sametime custom logon form for SSO. To enable the custom logon form, the Sametime installation:
  - Creates a Domino Configuration database named domcfg.nsf in the root data directory of the Domino server.
    Note: If a domcfg.nsf database already exists on the Domino server when Sametime is installed, the Sametime installation overwrites the existing domcfg.nsf database.
  - Creates a "Mapping a Login Form" document in the domcfg.nsf database.
  - Populates the following fields in the Mapping a Login Form document:
    - Target database filename - This field is set to the value "stcenter.nsf."
    - Target form name - This field is set to STLogonForm.nsf.

The configurations described above ensure that the custom logon form named "STLogonForm.nsf" displays to users when users authenticate with the server.

Altering the SSO configuration

The default configuration outlined above meets the basic requirements necessary for a Sametime server to support SSO. In some cases, it may be necessary for the administrator to alter the "DNS Domain" field or the "Domino Server Names" field of the Domino Web SSO Configuration document following the Sametime server installation.

- **Altering the DNS Domain field** - The Sametime installation may not always accurately detect the fully-qualified domain name of the Sametime server machine. If this problem occurs, the DNS Domain field may not specify the appropriate DNS domain. The administrator might need to manually edit the Domino web SSO Configuration document to add the appropriate entry in the DNS Domain field of the Domino web SSO Configuration document. Follow the instructions in "Viewing and editing the Domino Web SSO Configuration document" below to manually edit the document.

- **Altering the Domino Server Names field** - If the Sametime community consists of multiple Sametime/Domino servers, the Domino server names of all of the Sametime/Domino servers in the Sametime community must exist in the "Domino Server Names" field of the Domino Web SSO Configuration document. By default, the installation writes only the name of the Domino server on which Sametime is installed to this field. If you have multiple Sametime servers, it may
be necessary to manually open the Domino Web SSO configuration document and enter the names of the Domino/Sametime servers in the "Domino Server Names" field.

For example, if you have Sametimeserver1/East/Example and Sametimeserver2/East/Example in your Sametime community, and you install Sametimeserver3/East/Example, only Sametimeserver3/East/Example is written to the Domino Server Names field during the Sametime installation. The administrator may need to open the Domino Web SSO Configuration document and manually enter the names Sametimeserver1/East/Example and Sametimeserver2/East/Example in the "Domino Server Names" field on the Domino Web SSO Configuration document on Sametimeserver3/East/Example to ensure that all servers in the community are entered in this field. To manually open the Domino Web SSO Configuration document, see "Viewing and editing the Domino Web SSO Configuration document" below.

Note that in multiple server environments, the Domino Directory may already be replicated to the Domino server at the time the Sametime server is installed. If the Domino Directory already exists on the server and contains a Domino Web SSO configuration document, the Sametime installation will not attempt to alter the existing configuration in any way. In this case, the existing Domino Web SSO configuration document may already contain the names of the existing servers in the community and it may be necessary to add the name of the newly installed Sametime server to the Domino Web SSO configuration document.

For example, the names Sametimeserver1/East/Example and Sametimeserver2/East/Example may already exist in the Domino Web SSO configuration document in the Domino Directory on the server reserved for the Sametimeserver3/East/Example installation. Since the Sametimeserver3/East/Example installation does not alter an existing SSO configuration, that server name will not appear in the Domino Web SSO Configuration document following the Sametime server installation. In this scenario, it is necessary to open the Domino Web SSO configuration document in the Domino Directory on Sametimeserver3/East/Example and manually enter "Sametimeserver3/East/Example" in the "Domino Server Names" field. All other parameters in the existing Web SSO Configuration document should be valid for the newly-added server.

Altering the SSO key

By default the Sametime installation creates a Domino SSO key. If WebSphere is participating in SSO, this key should be replaced by the WebSphere LTPA key to allow both Domino and WebSphere to have an identical key for token validation and generation. Do this by importing the LTPA key from WebSphere to Domino. For more information, see Setting up single sign-on for Sametime browser clients.

Viewing and editing the Domino Web SSO Configuration document

To view or edit the Web SSO configuration document that is created by the Sametime installation, do the following:

1. From a Lotus Notes client, open the Domino Directory on the Sametime server.
2. Choose the Configuration > Web > Web Configurations view.
3. In the right-hand pane, select the twistie to display the document under "Web SSO Configurations."
5. Click Edit to put the document in edit mode.
6. Edit the appropriate field (for example, the DNS Domain or Domino Server Names field).

7. Click **Save and Close** after editing the document.

In some cases the name of the Web SSO configuration document can be different than *LtpaToken*, and the **Organization** field in the document might not be empty. This is mainly relevant for Internet Sites configuration. In this case the following settings must be set under the [AuthToken] section of the `sametime.ini` file:
- **ST_TOKEN_TYPE** must contain the name of the Web SSO document used by the Sametime Community server. The default value is *LtpaToken*.
- **ST_ORG_NAME** must contain the organization name that is set in the Web SSO document used by Sametime Community server. The default value is an empty organization name.

**Manually enabling the Domino SSO feature**

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**About this task**

This procedure is identical to the procedure used to enable the SSO feature on a Domino server. After manually enabling the feature, you can configure the server to use the Sametime custom SSO logon form.

Generally, the Domino SSO feature will be enabled by default during the Sametime installation and it is not necessary to manually enable the feature. For more information, see Altering the Domino Web SSO feature following the Sametime server installation.

To enable the Domino SSO feature on the Sametime server:

**What to do next**

After enabling the Domino SSO feature, follow the procedure described in Using the custom Sametime SSO logon page to use the custom Sametime SSO logon form.

Create the Web SSO Configuration document in the Domino Directory:

Create a Web SSO document that specifies the servers participating in the shared authentication, the time-out value for the cookie containing the LTPA access token, and the encrypted secret used to create the cookie.

**Procedure**

2. Select **Configuration > Servers > All Server Documents**.
3. Select the **Web** button on the taskbar.
4. Select **Create Web SSO Configuration**.
5. In the document, select the Keys pull-down menu button.
6. The default value for the **Configuration Name** field is *LtpaToken*. This is the preferred value and usually it should not be changed. In case another value is
configured as the Web SSO document name, the ST_TOKEN_TYPE setting under the [AuthToken] section of the sameTime.ini file must contain the same value.

7. Select **Create Domino SSO Key**.
   
   **Note** The Import WebSphere LTPA Keys option is usually used to enable a WebSphere server to communicate with a Domino server. To enable a WebSphere server to communicate with a Domino server, you must export the LTPA keys from the WebSphere server and import the LTPA keys to the Domino server. See the WebSphere Information Center documentation for details.

8. Configure the Token Expiration field. Note that a token does not expire based on inactivity; it is valid only for the number of minutes specified from the time of issue. The token is also valid only for a single browser session.

   **Note** Set the expiration value to a value somewhat longer than a typical work day, such as 600 minutes, to minimize the potential for an LTPA token to expire during an active meeting. Setting a higher value may create a security risk. If the LTPA token is intercepted by an attacker, the attacker may use the token to illegally gain access to the Sametime server until the token expires. Setting up the Domino server to support SSL for web browser connections provides the highest level of security against attempts to intercept LTPA tokens.

9. In the DNS Domain field, enter the DNS domain (for example, .lotus.com or .meetings.acme.com) for which the tokens will be generated. The servers enabled for SSO must all belong to the same DNS domain. This field is required and the DNS domain must start with a period.

   When users access the Sametime server, they must enter the fully qualified domain name of the Sametime server for authentication to be successful (for example, sametimeserver/meetings/acme.com).

10. In the Server Names field, enter the servers that will be participating in SSO. Generally, this field should contain the Domino hierarchical names of all Sametime servers in your environment. You can browse and select the server names from the Domino Directory.

   **Note** Groups and wildcards are not allowed in the field.

11. The Organization field should usually stay empty. In case it has a value, which is mandatory only for Internet Sites configuration, the ST_ORG_NAME field setting under the [AuthToken] section of the sameTime.ini file must contain a similar value. For additional information about Internet Sites see the Domino documentation.

12. Select **Save & Close** to save the Web SSO Configuration document. The document will appear in the Web Configurations view. This document will be encrypted for the creator of the document, the members of the Owners and Administrators fields, and the servers specified in the Server Names field.

**Related tasks:**

Manually enabling the Domino SSO feature

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**Enable SSO and "Name & Password" authentication in the Server document:**

Use this procedure to enable SSO and "Name & Password" authentication in the Server document of the Sametime server for which you are enabling the Domino SSO feature.
About this task

This procedure is the second of three required to manually enable the Domino SSO authentication feature on a Sametime server.

Procedure

1. In the Configuration - Servers - All Server Documents view of the Domino Directory, double-click the name of the Sametime server to open the Server document.
2. Select **Edit Server** to put the Server document in edit mode.
3. Select the Ports tab.
4. Select the Internet Ports tab.
5. Select the Web tab (if it is not displayed by default).
6. For the HTTP TCP/IP port Authentication Options, select Yes in the "Name & Password" field.
7. Select the Internet Protocols tab.
8. Select the Domino Web Engine tab.
9. In the "HTTP Sessions" section, select "Multiple server (SSO)" in the "Session authentication" field.
   
   **Note** You must select the "Multiple server (SSO)" value even if your environment includes only a single Sametime server.
10. Click **Save and Close** to save the Server document.

What to do next

Start (or restart) the HTTP task on the SSO-enabled server

Related tasks:
Manually enabling the Domino SSO feature
If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

Start (or restart) the HTTP task on the SSO-enabled server:

Use the Domino console to start or stop the HTTP server.

About this task

This procedure is required to manually enable the Domino SSO authentication feature on a Sametime server.

To start the HTTP task on the SSO-enabled server:

Procedure

1. Open the Domino console.
2. Start the HTTP server, or stop and restart the HTTP server if it is already running.
   - Use the Tell HTTP Quit command to stop the HTTP server.
   - Use the Load HTTP command to start the HTTP server.
3. On the Domino console, the following message should appear:
HTTP: Successfully loaded Web SSO Configuration

4. If a server enabled for SSO cannot find a Web SSO Configuration document or is not included in the Server Names field (and thus cannot decrypt the document), then the following message should appear on your server's console.
HTTP: Error Loading Web SSO configuration. Reverting to single server session authentication.

What to do next

Lotus software recommends using the custom Sametime SSO logon form. If you do not use this logon form, users will see the default Domino SSO logon form the first time they access a database on the server that requires authentication.

Note: Authentication by token does not occur if you allow anonymous access to the Sametime server and all its databases.

To configure the Sametime server to use the custom Sametime SSO logon form, see Using the Sametime custom logon form for SSO.

Using the Sametime custom logon form for SSO

The IBM Sametime installation automatically configures the Sametime server to use the Sametime custom logon form for SSO.

The Sametime installation performs the following configurations to enable the custom logon form:

1. Creates a Domino Configuration database named domcfg.nsf in the root data directory of the Domino server on which Sametime is installed. This database is created from the domcfg5.ntf template available with the Domino server.
3. Populates the following fields in the Mapping a Login Form document:
   - Target database filename - This field is set to the value "stcenter.nsf."
   - Target form name - This field is set to STLogonForm.nsf.

The configurations described above ensure that the custom logon form named "STLogonForm.nsf" displays to users when users authenticate with the server.

If a database named domcfg.nsf exists on the Sametime server when Sametime is installed, the administrator must manually enable the custom logon form. This procedure is described below.

Manually enabling the custom logon form

Follow the procedure below to manually enable the Sametime custom logon form for SSO. The custom logon form displays when the user accesses the first database on the server that requires authentication or selects the "Log on to Sametime" link in the Sametime Meeting Center.

Note: The custom logon form exists in the Sametime server home page database (stcenter.nsf). If you want to require users to authenticate when accessing the server, you should allow anonymous access to the Sametime server home page (stcenter.nsf) and require authentication to the Sametime Meeting Center database (stconf.nsf). With this arrangement, users access the server home page anonymously and are presented with the SSO logon form when attempting to create or attend a meeting.
To use the Sametime custom logon form for SSO, you must configure settings in the Domino Configuration database (domcfg.nsf) provided with the Domino server on which Sametime is installed.

To use the Sametime custom logon form for SSO:

1. Verify that the Sametime server has a Domino Configuration database named domcfg.nsf.
   
   **Note** If your server includes an existing domcfg.nsf database, but you do not want to use that database you can delete the existing domcfg.nsf database and create a new one. To create a new domcfg.nsf database, use the Domino Configuration (R5) template (domcfg5.ntf) available with a Domino server. When creating the new database, you must select the “Show advanced templates” option to access the domcfg5.ntf template.

2. If necessary, copy the domcfg.nsf Domino Configuration database to the root data directory of the Domino server on which Sametime is installed (for example C:\Lotus\Domino\Data directory).

3. From a Lotus Notes client, open the Domino Configuration database.

4. Choose **Add Mapping**.

5. Under Site Information, accept the default of All Websites/Entire Server.

6. In the "Target database filename" field, enter stcenter.nsf.

7. In the "Target form name" field, enter STLogonForm.

**Required ACL settings for the Sametime Center database (stcenter.nsf)**

The Sametime Center database (stcenter.nsf) must meet the following ACL requirements for the custom logon form to operate properly.

- In the Advanced options of the stcenter.nsf ACL settings, the "Maximum Internet name & password" field must allow at least Reader access. If either Depositor or No Access are selected, the logon form will not appear.
- In the Basics options of the stcenter.nsf ACL settings, anonymous users must have an access level of Reader or higher. If the access level provided for anonymous users is less than Reader, the logon form will not appear. The "Write public documents" and "Read public documents" options should also be selected.

**Related tasks:**  
Manually enabling the Domino SSO feature

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**Authentication by token using Secrets and Tokens databases**

To authenticate by token, the Sametime server can accept an authentication token created by the Secrets and Tokens authentication databases, the Domino Single Sign-On (SSO) feature, or both. The Sametime server can also generate tokens using the Secrets and Tokens authentication databases or the Domino SSO feature.

If the Sametime server is operating in an environment that includes Sametime servers from releases earlier than Sametime 3.0, or if Domino databases enabled with Sametime technology (such as the Sametime Discussion and TeamRoom databases that were available with earlier releases) are used in your environment, the Sametime server must support both the Secrets and Tokens authentication databases and the Domino SSO authentication feature.
The Sametime server is set up to support Secrets and Tokens authentication by default. The basic requirements for this authentication system are:

- The Secrets (stauths.nsf) and Tokens (stautht.nsf) databases must exist on the Sametime server. These databases are created during the Sametime server installation.
- The "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" option must be selected in the Sametime Administration Tool. (This option is selected by default.)

Note that previous releases of Sametime allowed an administrator to enhance the level of security provided by the Secrets and Tokens databases by enabling the SametimeSecretsGenerator agent in one Sametime Secrets database (stauths.nsf) on one Sametime server in the Sametime community. If you enable the SametimeSecretsGenerator agent on one Secrets database on one Sametime server, that Secrets database must be replicated to all Sametime servers in the community. If your environment includes Sametime servers from previous releases and you are currently replicating a Secrets database to all of the servers in your environment, you must also replicate that Secrets database to the Sametime servers.

There are two procedures associated with ensuring the Secrets and Tokens authentication databases on the Sametime server are functioning properly:

1. If necessary, select the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" option in the Sametime Administration Tool. (This option is selected by default.)

2. Replicating the Secrets and Tokens databases (optional) - This step is necessary only if you have deployed Domino databases enabled with Sametime technology (such as Sametime TeamRoom and Discussion databases) or if you have enhanced security by enabling the SametimeSecretsGenerator agent in the Secrets database.

Selecting the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" option:

The "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" setting must be enabled in the Sametime Administration Tool to enable the Sametime server to accept both the LTPA and Sametime Tokens. This setting must be set consistently on all Sametime 8.x, 7.x, 6.5.1, 3.x servers in your environment.

About this task

Note: This procedure might not be necessary as the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" setting is enabled by default following the server installation.

If you enable this setting on one Sametime server, you must enable it on all Sametime servers in your environment. If you disable it on one Sametime server, you must disable it on all Sametime servers in the environment.

To enable this setting:

Procedure

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

2. Choose Configuration.
3. Choose **Community Services**.
4. Select the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stauht.nsf)" option.
5. Click **Update**.
6. Restart the server for the setting to take effect.

**Results**

You have the option of replicating the Secrets database to enhance security.

**Related tasks:**
Manually enabling the Domino SSO feature
If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**Replicating the Secrets and Tokens databases (optional):**

If you have installed multiple Sametime servers, you can enable the SametimeSecretsGenerator agent in the Secrets database. Enabling the SametimeSecretsGenerator agent is an optional procedure that increases security against outside attacks.

**About this task**

This topic discusses the second of two procedures associated with setting up the Secrets and Tokens authentication system on a Sametime server.

The Secrets and Tokens databases exist on every Sametime server.

If you enable the SametimeSecretsGenerator agent, only one Secrets database should be used for all Sametime servers in the environment. You should replicate the Sametime Secrets database in which you have enabled the SametimeSecretsGenerator agent to all Sametime servers in the environment. Create a replication schedule for the Secrets database in which you have enabled the SametimeSecretsGenerator agent to ensure it replicates at regular intervals. Delete all other copies of the Secrets database from all Sametime servers in the environment. For more information, see Integrating a Sametime server into an existing Sametime community.

Do not replicate the Tokens database to the other Sametime servers. The replicated Secrets database can work with the Tokens database that exists on each Sametime server by default following the server installation.

If you do not enable the SametimeSecretsGenerator agent in any Secrets database on any Sametime server, it is not necessary to replicate the Secrets database. If you do not enable the SametimeSecretsGenerator agent, administration is simpler because no replications or replication schedules are required, but the security level is not as high.

**Working with Sametime security**

The IBM Sametime server uses the Internet and intranet security features of the Domino server on which it is installed to authenticate web browser users who access Domino databases on the server. These databases include the Sametime...
Center database (stcenter.nsf), which contains the Sametime server home page, and the Sametime Meeting Center database (stconf.nsf).

Sametime also uses authentication-by-token features to authenticate connections from Sametime clients to the Sametime server. The authentication-by-token features include the Secrets and Tokens databases supported by all previous Sametime releases and the Domino Single Sign-On (SSO) authentication feature that is supported by Sametime 3.0 and higher-version servers.

Sametime also provides security features that enable users to encrypt meetings and specify meeting-specific passwords. The Security section includes the following topics:

**Getting started with Sametime security**

This section includes basic security information to help you get started with IBM Sametime security.

**The required fully-qualified server name:**

The user must enter the fully qualified DNS name of the IBM Sametime server (for example, sametimeserver.meetings.acme.com) in the web browser URL locator when accessing the Sametime server to authenticate with a Sametime server.

The Domino Single Sign-On (SSO) feature must be enabled on the Sametime server. The Domino SSO feature requires the user to enter the fully qualified DNS name of the server for a successful authentication. For more information, see Authentication by token using LTPA and Sametime tokens.

**Basic password authentication and authentication by token:**

IBM Sametime uses two types of authentication: Basic password authentication and authentication by token.

**Basic password authentication**

Sametime uses basic password authentication to authenticate web browser connections and Sametime Connect client connections. Sametime uses the same Internet and intranet security features as a Domino server to authenticate the web browser connections. These features include Domino database Access Control Lists (ACLs) and security settings in the Server document of the Domino server on which Sametime is installed.

The Domino security features also allow you to configure databases for anonymous access. When a database is configured for anonymous access, the user is not authenticated when accessing the database.

The following topics in this section discuss basic password authentication:

- User requirements for basic password authentication
- Using database ACLs for identification and authentication
- Basic password authentication and database ACLs
- Setting up basic password authentication in a database Access Control List (ACL)
Authentication by token

After a web browser user authenticates using basic password authentication, Sametime Java applet clients (such as the Meeting Room client, Recorded Meeting client, and Sametime Connect for browsers client) load in a user’s web browser. These Sametime clients make connections to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services when a user attends a meeting. Sametime uses "authentication by token" to authenticate the connections from these Sametime clients to the Sametime services.

Note: Connections from the Sametime clients to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services are authenticated only if the Sametime Meeting Center database (stconf.nsf) requires basic password authentication. If the Sametime Meeting Center allows anonymous access, these connections are not authenticated.

When the Sametime Meeting Center requires basic password authentication, authentication by token is supported on the Sametime server using the Domino Single Sign-On (SSO) authentication feature.

If your environment includes only Sametime 3.0 (or higher) servers, it is only necessary to enable the Domino SSO feature on the Sametime servers.

Note: Sametime TeamRoom and Discussion databases were available with previous Sametime releases but are no longer included in the Sametime product.

The Sametime server must support both the Domino SSO feature and the Secrets and Tokens database authentication system if your environment includes Sametime 3.0 (or higher) servers that interoperate with Sametime servers from releases earlier than Sametime 3.0.

The following topics discuss authentication by token:

• Authentication by token
• Authentication by token using the Domino Single Sign-On (SSO) feature
• Authentication by token using Secrets and Tokens databases

User requirements for basic password authentication:

When accessing the Sametime server with a Web browser, a user must enter a user name and Internet password to access any protected database on the Sametime server.

A protected database is a database that has its Access Control List (ACL) set to require basic password authentication. If the ACL settings of a database allow anonymous access, the user is not authenticated (promoted for a user name and Internet password) when accessing the database.

Note: It is important for a user to enter a name when accessing a Sametime database so that the user's name can be displayed in any presence list within the database. If the ACL settings of a database allow anonymous access, a user is not prompted for a name unless the "Users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting is selected in the Configuration-Community Services-Anonymous Access settings of the Sametime Administration Tool. When this option is selected, it forces a name entry prompt to appear when an anonymous user attends a scheduled meeting.
this name entry prompt, the user can enter a name for display purposes in a presence list. The server accepts any name entered by the user at the name entry prompt; the user is not authenticated.

A Sametime Connect user must also be authenticated each time the user starts the Sametime Connect client and connects to the Community Services on the Sametime server. Sametime Connect users must enter the user name and Internet password from the Person document in the Domino Directory when logging on to Sametime Connect.

**Note:** If you have configured Sametime to operate with an LDAP directory, Sametime authenticates users based on the user names and passwords stored in the person entries of the LDAP directory.

**Person document, User names, and Internet passwords in the Domino Directory**

This section discusses the requirements for basic password authentication when Sametime is installed to operate with a Domino Directory. You must choose either the Domino Directory or an LDAP directory during the Sametime installation.

Each member of the Sametime community must have a Person document in the Domino Directory to authenticate with the Sametime server. The names and password that a user can enter when accessing a Sametime server are maintained in the Basics tab of a Person document in the Domino Directory.

To access a Person document, open the Sametime Administration Tool and select **Domino Directory > Domino > Manage People.** Double-click a person’s name to open that user’s Person document.

The table below shows a sample entry in the Basics section of a user’s Person document. The text that follows the table explains how these entries are used in the web browser and Sametime Connect client password authentication processes.

**Sample settings in the Basics section of a Person document**

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>Gary</td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Middle initial</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Last name</td>
<td>Ollerman</td>
<td>This field is required.</td>
</tr>
<tr>
<td>User name</td>
<td>Gary Ollerman/Community GOllerman</td>
<td>This field is required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The Community (or domain) name is appended to the first entry in the user name field by default.</td>
</tr>
<tr>
<td>Alternate name</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Short name/UserID</td>
<td></td>
<td>This field is optional.</td>
</tr>
</tbody>
</table>
The following fields on the Person document are used by the authentication process:

- **First name** - This field is optional.
  - **Web browser** - If an entry exists in the "First name" field in the Basics tab of the Person document, the user can enter just this name at the User Name prompt that appears when accessing a protected database on the Sametime server with a web browser. The user must also enter the Internet password to access the database. (A protected database is a database that has its ACL set to require basic password authentication.)
  - **Sametime Connect** - The first name is not a valid entry at the User Name prompt that appears when logging on to the Sametime Connect client.

- **Last name** - This field is required. An entry must exist in the "Last name" field of the Basics tab of a Person document.
  The last name can be entered in the User Name prompt that appears when accessing a protected database on the Sametime server with a Web browser. The last name can also be used when logging on from the Sametime Connect client. A user must also enter the Internet password to complete the authentication process.

**Note:** If both the "First name" and "Last name" fields contain entries, the user can enter the first and last names at the User Name prompt that appears when accessing the Sametime server.

- **User name** - This field is required. An entry must exist in the "User name" field in the Basics tab of a Person document.
  Generally, it is good practice to use a user's first and last name in the "User name" field. The "User name" field can contain multiple entries. In our example, the User name field contains both Gary Ollerman/Community and G0llerman. (Each entry must be separated by a semicolon or a carriage return in the "User name" field of the Person document.)
  A user can enter any name that appears in the "User name" field of the Person document when logging on to the Sametime server from the Sametime Connect client or a web browser. For example, the user could enter Gary Ollerman/Community or G0llerman at a Sametime Connect or web browser User Name prompt. The name entered by the user is resolved to the topmost name (Gary Ollerman/Community in the example) in the "User name" field. The topmost name in the "User name" field is the name that is displayed in the presence lists of all Sametime clients.

**Note:** If you want a user's email address to display in presence lists, enter the user's email address as the topmost name in the "User name" field of the Person document. If the email address is included in the User name field, the user can also enter the email address at the "User name" prompt when logging in from a Sametime Connect client or web browser.

Sametime uses the topmost name in the "User name" field to validate a user in a database ACL. If you require basic password authentication for a database and you enter the names of individual users in the ACL of a database, enter the

### Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generational qualifier</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Internet password</td>
<td>(FCF5F3960B0A289D3)</td>
<td>This field is required.</td>
</tr>
</tbody>
</table>

Chapter 3. Security 357
topmost name that appears in the “User name” field of the Person document in the database ACL. Although the user can enter “G0llerman” when logging on, Sametime uses “Gary Ollerman/Community” to validate the user in the database ACL. Therefore, “Gary Ollerman/Community” must be the name that appears for this user in database ACLs.

- **Internet password** - This field is required. Users must enter the Internet password to authenticate with the Sametime server using a Web browser or the Sametime Connect client. In the example, the Internet password is “sametime.” The password displays as a series of random characters because Internet passwords are encrypted on the Person document.

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

`: \ } ' * &

**Self-registration**

If you are using the self-registration feature of the Sametime server, a Person document containing a last name, user name, and Internet password is automatically created for a user in the Domino Directory on the Sametime server at the time the user self-registers. Agents in the Self-Registration database (streg.nsf) access the Domino Directory to create these Person documents. The signers of these agents must have the proper access levels and permissions in the Domino Directory for self-registration to work properly. If you allow self registration, you might need to add these signers to the Domino Directory ACL.

The Sametime self-registration feature cannot be used if you have configured the Sametime server to operate with an LDAP directory on a third-party server (such as a Microsoft Exchange or Netscape Directory Server).

**LDAP**

If you have configured the Sametime server to operate with an LDAP directory on a third-party server, the authentication process uses the user names and passwords stored in the LDAP directory. It is not necessary to create Person documents containing separate user names and passwords in the Domino Directory on the Sametime server.

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

`: \ } ' * &
Related concepts:
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Related tasks:
Changing a user's password
When accessing the IBM Sametime server from any Sametime client, the user might be prompted for a user name and password. The password is specified in the Internet password field on the user's Person document in the Domino Directory on the Sametime server.

Setting up basic password authentication in a database Access Control List (ACL)
You can require users to specify a valid name and password when accessing a database on the Sametime server.

Changing a user's password:

When accessing the IBM Sametime server from any Sametime client, the user might be prompted for a user name and password. The password is specified in the Internet password field on the user's Person document in the Domino Directory on the Sametime server.

About this task

To change a user's password, open the user's Person document and enter a new password in the "Internet password" field.

Note: If you have configured the Sametime server to operate with an LDAP directory on an LDAP server, the authentication process uses the passwords specified in the LDAP directory. Use the administrative tools provided with the third-party LDAP server to access the LDAP directory and make password changes for individual users. You cannot change passwords stored in an LDAP directory from the Sametime Administration Tool.

To change a user's Internet password in the Domino Directory on the Sametime server:

Procedure
1. From the Sametime server home page, open the Sametime Administration Tool.
2. Select Domino Directory.
3. Select Domino.
4. Select Manage People.
5. Double-click the name of the user whose password you want to change.
6. Click Edit Person.
7. Enter the new password in the "Internet password" field of the Person document. You might want to write the new password down before closing and saving the Person document. After you close and save the Person document, the Internet password is encrypted and you cannot view it.

Password character restrictions
In addition to non-English characters, the following characters must not be included in passwords used by Sametime:
8. Select **Save and Close**.

### Ensuring Sametime servlet access when Domino requires SSL for all connections:

An IBM Sametime server installs on a Domino server and relies on the Domino HTTP server to handle all HTTP traffic to the Sametime server. To encrypt web browser access to the Sametime Meeting Center with SSL, the administrator must configure the Domino HTTP server to support SSL.

**About this task**

When setting up a Domino HTTP server to support SSL, the administrator can force all connections to the Domino server to use SSL. The administrator forces all HTTP connections to use SSL by performing either of the following configurations in the Ports-Internet Ports-Web section of the Domino Server document during the Domino HTTP server SSL set up procedure:

- Setting the Web HTTP "TCP IP port status" setting to "Disabled" and setting the Web HTTP "SSL port status" to "Enabled."
- Setting the Web HTTP "TCP IP port status" to "Redirect to SSL."

If you force all HTTP connections to use SSL, you must also configure the Sametime server to support SSL for HTTP connections to its servlets. If you do not configure the Sametime server to support SSL for connections to its servlets, users will be unable to access the Sametime server.

To ensure access to the Sametime servlets when Domino requires SSL for all connections, complete the following steps:

**Procedure**

1. Set up the Domino server to support SSL
2. Import the SSL trusted room or SSL server certificate into the key store database on the Sametime server
3. Modify the Sametime configuration for SSL

**Results**

You can use these procedures regardless of whether your Sametime server operates on the Windows, AIX, Solaris, Linux or IBM i operating system.

**Note:** It is possible to configure a Domino server to allow unencrypted HTTP connections on port 80 and simultaneously allow SSL-encrypted HTTP (or HTTPS) connections on port 443. This configuration enables you to encrypt connections to databases containing sensitive data while allowing unencrypted connections to databases that do not contain sensitive data. Since the Domino server on which Sametime is installed is dedicated to supporting only Sametime, it is unlikely that such a configuration would be implemented on a Domino/Sametime server.

### Domino security and the web browser connection

To attend a meeting on the Sametime server, a user first connects to the Sametime HTTP server with a web browser. By default, the user is not authenticated when accessing the Sametime server over this port and is able to access the Sametime server home page database (stcenter.nsf) without entering a user name and password.
By using the Access Control List (ACL) settings of individual databases, the Sametime administrator can force users to authenticate using basic password authentication when they attempt to access the databases on the server.

Generally, the first database that a user accesses when connecting to the Sametime server is the Domino database that contains the Sametime server home page (stcenter.nsf). By default, the ACL settings of the stcenter.nsf database allow anonymous access so users can access the Sametime server home page without being authenticated (entering a user name and password that is verified against entries in a directory).

After accessing the home page, a user selects links to access other databases on the Sametime server. Most users will access the Sametime Meeting Center (stconf.nsf). The Sametime Administrator can alter the ACLs of these databases to force users to authenticate at the time they select the link that accesses the database.

The databases on the Sametime server that are accessible from the Sametime server home page include:

- **Self-Registration (streg.nsf)** - An administrator controls whether self-registration is available on the server. The administrator controls self-registration by selecting or clearing the "Allow people to register themselves in the Directory" check box available from the Domino Directory - Domino option in the Sametime Administration Tool. The self-registration database (streg.nsf) should always allow anonymous access to enable anonymous users to self register when the administrator allows self-registration.

- **Server Administration** - You must add users to the ACLs of several Sametime databases when allowing other users to have administrative privileges on the Sametime server. For more information about controlling access to the Sametime Administration Tool, see Adding a new Sametime administrator.

**Note:** By default, the connection from a web browser to the Sametime server is neither authenticated nor encrypted. The authentication occurs at the time a user accesses an individual database on the Sametime server. You can configure Sametime so that all HTTP traffic (including passwords and authentication tokens) that passes over the connection between the web browser and the HTTP server is encrypted using the Secure Sockets Layer (SSL).

**Note:** References to the Sametime Meeting Center and to the web browser connection do not apply to Sametime Entry servers.
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

Anonymous access and database ACLs
You can set a database ACL to allow anonymous access.

Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Related tasks:
- Setting up anonymous access in a database Access Control List (ACL)
- Setting up basic password authentication in a database Access Control List (ACL)

Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

For each database on the server, you can set the ACL to allow:
- Anonymous access
- Basic password authentication

The settings in the database ACLs work together with the "Maximum Internet name & password" setting for each database to control the level of access that web browser users have to a database on the Sametime server.

Using database ACLs
The database ACL defines user access to the content of the database. Before you set up basic password authentication or anonymous access to a database, you should be familiar with how to add users to a database ACL and the available settings within the ACL. For more information, see:
- Adding a name to a database ACL
- Database ACL settings

Maximum Internet name & password setting
The "Maximum Internet name & password" setting on the Advanced panel of each database ACL specifies the maximum level of access to the database that is allowed for web browser clients. This setting overrides individual levels set in the ACL.

Generally, administrators should not need to change the "Maximum Internet name & password" settings for databases on the Sametime server. The default settings should function adequately in most cases.

Adding a name to a database Access Control List (ACL):
Use the Sametime Administration Tool to add a name to a database Access Control List.

**Procedure**

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

2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select **LDAP Directory**.

3. Select **Access Control**.

4. Select a database from the list.

5. Click **Access**. The database ACL displays.

6. Click **Add**.

7. In the dialog box, type the exact user name from a Person document or the group name from a Group document. Click **OK**.

   When entering a user name for a user with a Person document in the Domino Directory on the Sametime server, type the name exactly as it appears in the topmost entry of the "User name" field in the user's Person document.

   When entering the names of users or groups registered in an LDAP directory in a Sametime database ACL, use the fully qualified Distinguished Name, but use forward slashes (/) as delimiters instead of commas. For example, if the Distinguished Name for the user in the LDAP directory is:

   - uid = Joe Waters, ou=West, o=Example

   enter the name in the Sametime database ACL as follows:

   - uid = Joe Waters/ou=West/o=Example

   You can also use asterisks for wildcards when entering names from an LDAP directory or a Domino Directory in an ACL. For example, entering *

   */ou=West/o=Example is equivalent to entering all users in the ou=West/o=Example branch of the directory to the ACL.

   **Note** It is possible to enter entities other than user and group names in an ACL. For more information about the types of entries that can exist in an ACL, see User type - ACL settings.

8. Click the name entered in the previous step so that the name is selected (highlighted).

9. In the User Type box, select the type of user (Unspecified, Person, Server, Person Group, Server Group, or Mixed Group). For more information, see User type - ACL settings.

10. In the Access Box, assign an access level for the user (Manager, Designer, Editor, Author, Reader, Depositor, or No Access). For more information, see Access level - ACL settings.

11. Edit the privileges if necessary. For more information, see Privileges - ACL settings.

12. Click **Submit**.
Related concepts:
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Database ACL settings:
A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database.

For each user in the database ACL, you can specify the following ACL settings:

User type - ACL settings:
When you add a user or group to an ACL, you specify a user type for the entry in the ACL. A user type identifies whether a name in the ACL is for a person, server, group, or other entity. You assign a user type to a name to specify the type of ID required for accessing the database with that name.

You can designate an entry in the ACL as any of the following user types:

Unspecified
Select the Unspecified user type if you want to enable the name you are entering to access the database with any type of ID (Person, Server, or Group). The Default entry in an ACL is always assigned the Unspecified user type. IDs used to sign agents, such as Sametime Development/Lotus Notes Companion Products, are also assigned the Unspecified user type when entered in a database ACL.

Person
Select the Person user type if the name you are entering belongs to a user who has a Person document containing a user name and Internet password in the Directory on the Sametime server or if the user has a Person entry in an LDAP directory on a third-party server.

Server
Select the Server user type if the name you are entering belongs to another server in the Domino domain. When multiple servers are installed in a Domino environment, it might be necessary for a server to access data within the database or to replicate a database. Server names are frequently added to the pre-existing LocalDomainServers and OtherDomainServers server groups. The Server user type is generally used only if you have
installed Sametime in a Domino environment. This user type performs the same function as it does on a Domino server.

**Mixed Group**

Select the Mixed Group user type if the name you are entering belongs to a group that consists of both Server and Person names.

**Person Group**

Select the Person Group user type if you are entering the name of a group that contains only people. You can enter a group from the Directory on the Sametime server, or you can enter a group stored in an LDAP directory on a third-party server in the ACL of a database.

**Server Group**

Select the Server Group user type if the name you are entering belongs to a group that consists of only servers.

---

**Access level - ACL settings:**

Access levels are the database ACL settings that control the type of actions a user can perform on the contents of a database and on the database itself.

Access levels range from No Access, which prevents a user from opening a database, to Manager, which lets a user read, create, and edit the ACL and all documents in the database.

Users that are listed both individually and in one or more groups in the ACL might be assigned different levels of access. The access level granted in an individual entry takes precedence over the access level granted through a group entry. If a user is in multiple groups, the user is granted the access level of the group with the highest level of access.

If a user or group has one level of access in the ACL and another level of access in a database component (such as a Read or View access list), the database component access level takes precedence over the user or group access level.

The following access levels are listed from lowest to highest. A higher access level has all the privileges granted to lower access levels. For example, Authors can perform all of the functions of a Depositor and a Reader.

**No Access**

No Access prevents a user from accessing the database. For example, if you assign No Access as the Default access for a database, only a user who has a Person document in the Address Book and is listed in the ACL can access the database.

**Depositor**

Depositor access allows a user to create documents but not view any documents in the database, including the documents created by the user. This access level is not generally used for Sametime databases. This ACL type is most frequently used for automatic agents to write documents into a database for Domino workflow applications.

**Reader**

Reader access allows a user to read documents in a database, but not create or edit documents. For example, you can assign Reader access in the Meeting Center (stconf.nsf) ACL to users who are allowed to attend but not start meetings.
Note: If you assign a user the Reader access level in the Meeting Center (stconf.nsf), the user can attend listed meetings but cannot attend unlisted meetings in the Meeting Center. To enable a user with Reader access to also attend unlisted meetings, you must select the "Write public documents" check box for that user in the ACL.

Author
Author access allows a user to create and edit documents. Users with Author access can edit documents they have created themselves, but they cannot edit documents created by other users.

Assign Author access in the Meeting Center ACL to allow users to create meetings in the Sametime Meeting Center. Meeting Center users with Author access can modify the meetings they create, but they cannot modify meetings created by other users. To create a meeting, the user must have Author access and the Write Public Documents privilege selected.

Editor
Editor access allows users to read, create, and edit all documents in the database, including those created by other users.

Assign Editor access in the Meeting Center ACL to users who are allowed to modify meetings they create and meetings that are created by other users. Editors can also start meetings in the Meeting Center. To create meetings, the user must also have the Write Public Documents privilege selected.

Designer
Designer access allows a user to create full-text indexes, modify all database design elements, and read, create, and edit all documents in the database. This access level is primarily for programmers and database developers.

Manager
Manager access allows a user to read, create, and edit the ACL and all documents in a database, modify ACL settings, and delete the database. Modifying the ACL and deleting databases are tasks permitted by no other access level. This access level is usually assigned to Sametime administrators and is not recommended for general users.

Each database must have at least one Manager. Generally, the Manager access level is provided in each database to the person specified as the administrator during the Sametime installation and setup procedure. You should assign Manager access to two people in case one manager is unavailable. For information about granting other users administrative privileges, see Allowing others to use the Sametime Administration Tool.

Privileges - ACL settings:
The database Access Control List (ACL) defines privileges for users.

Depending on the access level assigned to a user, some ACL permissions are granted, denied, or optional. Privileges listed in the ACL are:

Create documents
This privilege allows users to create documents in a database. This privilege is:

- Permanently granted to Managers, Designers, Editors, and Depositors
- Permanently denied to Readers
- Optionally granted to Authors
Delete documents
This privilege allows users to delete documents from a database. This privilege is:
• Permanently denied to Readers and Depositors
• Optionally granted to Managers, Designers, Editors, and Authors

Create personal agents
This privilege allows an Lotus Notes developer or user to create agents that perform automated procedures in a database. This privilege is:
• Permanently granted to Managers and Designers
• Optionally granted to Editors, Authors, and Readers
Clear this option on server databases to prevent certain users from creating personal agents that take up server disk space and processing time. Use the Agent Restrictions settings in the Security tab of the Server document in the Directory to prevent users from running personal agents on a server, even if the “Create personal agents” permission in a server database ACL is selected.

Create personal folders/views
This privilege is:
• Permanently granted to Managers and Designers
• Permanently denied to Depositors
• Optionally granted to Editors, Authors, and Readers
Personal folders and views created on a server are more secure and are available on multiple servers. Also, administrative agents can operate only on folders and views stored on a server. If this permission is not selected, users can still create personal folders and views that are stored on their local workstations. Clear this option to save disk space on a server.

Create shared folders/views
This privilege is:
• Permanently granted to Managers and Designers
• Permanently denied to Authors, Readers, and Depositors
• Optionally granted to Editors
Deny this privilege to Editors to save disk space on a server and maintain tighter control over database design.

Create LotusScript®
This privilege is:
• Permanently granted to Managers
• Permanently denied to Depositors
• Optionally granted to Designers, Editors, Authors, and Readers
Clear this option on server databases to prevent certain users from running restricted and unrestricted LotusScript agents that take up server disk space and processing time. Use the Agent Restrictions settings in the Security tab of the Server document in the Directory to prevent users from running restricted and unrestricted LotusScript agents on a server, even if the “Create personal agents” permission in a server database ACL is selected.

Read Public Documents
This privilege is:
- Permanently granted to Managers, Designers, Editors, Authors, and Readers
- Optionally granted to Depositors

Write Public Documents

This privilege is:
- Permanently granted to Managers, Designers, and Editors
- Optionally granted to Authors, Readers, and Depositors

Public documents, such as the meeting details document in the Sametime Meeting Center, are designed to be accessed by a wide audience. Users with the Write Public Documents permission can read, create, edit, and delete public documents from a database. To create a meeting in the Sametime Meeting Center, a user must have the Author access level with the Write Public Documents privilege selected.

A user must also have the Write Public Documents privilege selected to attend unlisted meetings on the Sametime server.

Users without the Write Public Documents privilege are prompted for a password when accessing a database with public documents. After entering the user name and Internet password, the user is given the Default access level to the database.

Roles - ACL settings:

Database Access Control List (ACL) roles grant access to individual database components, such as forms or views.

You can use ACL roles to delegate authority for managing specific documents in a database. You can create up to 75 roles in a database. For example, you can assign the roles of UserCreator and UserModifier in the Directory (Address Book) ACL to the administrator who has the responsibility for creating and maintaining Person documents.

ACL roles are optional in most databases. You can choose to rely on a broader access level and not use roles.

For more information on roles available in important Sametime databases, see Roles in Sametime databases ACLs.

Anonymous access and database ACLs:

You can set a database ACL to allow anonymous access.

Anonymous access has the following characteristics:
- Users are not identified or authenticated when they access databases and applications on the server.
- Data sent between the user and the Sametime server is not encrypted.
- Anonymous users are not identified in the maintenance log files. All anonymous user activity is recorded under the name "Anonymous."

The anonymous access level requires the least maintenance from the administrator, but it is the least secure. You should only allow anonymous access when you do not need to know the identity of users accessing your server. For example, use
anonymous access if the Sametime server is behind your firewall and you plan to allow only trusted intranet users to access it.

Setting up anonymous access in a database Access Control List (ACL):

To allow anonymous access to a database, you can add the Anonymous entry to the ACL and assign an access level to the Anonymous entry.

About this task

Note: Alternatively, you can remove the Anonymous entry from the ACL and assign an access level to the Default entry in the ACL. When the Anonymous entry is removed from the ACL, anonymous users receive the access level and privileges assigned to the Default entry in the database ACL.

Use the following procedure to allow anonymous users to access a database:

Procedure
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select LDAP Directory.
4. Select a database from the list.
5. Click the Advanced button.
6. Set the "Maximum Internet name & password" access to Manager, which is the maximum access level.
   Note The "Maximum Internet name & password" setting on the advanced panel of each database Access Control List (ACL) specifies the maximum database access level granted to web browser clients. This setting overrides higher individual access levels set in the ACL. For example, if you set the "Maximum Internet name & password" to Author, and assign Editor access to the Anonymous entry in the database ACL, anonymous users will only have Author access to the database. Alternatively, if you set the "Maximum Internet name & password" to Manager, and assign Reader access to the Anonymous entry in the database ACL, anonymous users will only have Reader access to the database.
7. Click the Access button.
   If the Anonymous entry exists in the ACL, select the Anonymous entry and assign an access level (for example, Author). Edit the default privileges if necessary.
   If the Anonymous entry does not exist in the ACL, users who access the database anonymously receive the access level and privileges assigned to the Default entry in the ACL.
   Note If the Anonymous entry does not exist in the ACL, the administrator also has the option to create an Anonymous entry and assign an access level and privileges. In this case, users receive the access level associated with the Anonymous entry instead of the Default entry.
8. Click Submit.
What to do next

If you set the ACL of the Sametime Meeting Center database to allow anonymous access, you should ensure that users are required to enter a display name when accessing the database. To ensure that users will be required to enter a display name to appear in the Participant List of the Sametime Meeting Room during a scheduled meeting, make sure that the "Users of Sametime or Sametime applications can specify a display name so that they do not appear online as 'anonymous'" setting is selected in the Sametime Servers > Sametime Community Servers > deployment_name > Anonymous setting of the Sametime System Console.

Basic password authentication and database ACLs:

You can set a database ACL to require basic password authentication.

Basic password authentication has the following characteristics:
- Users are identified or authenticated when they access databases and applications on the server.
- A web browser user must have a user name and an Internet password stored in the user's Person document to access databases. Only users with these credentials can access a database that requires basic password authentication.
- Data transmitted between the user and the Sametime server (including the name and password) is not encrypted.
- Users are identified in the maintenance log files.

Basic password authentication identifies users, but it does not prevent unauthorized users from listening to network transmissions or gaining server access by guessing passwords. For information on using Secure Sockets Layer (SSL) to encrypt the data that passes over the web browser connection to the IBM Sametime server, see Configuring Sametime to use SSL encryption.

Using the Default entry or individual names in database ACLs

When basic password authentication is enabled for a database, browser clients are authenticated when they attempt to open a database. For example, a web browser user might be authenticated when selecting the "Attend a Meeting" link from the Sametime server home page to access the Sametime Meeting Center database (stconf.nsf).

The Sametime server challenges the user to supply a valid name and password and then verifies that the user's response matches the information stored in the user's Person document in the Domino Directory (or LDAP directory if you have configured Sametime to operate with an LDAP directory). Authentication succeeds if the user name and password provided by the user matches the user name and password in the directory and:
- The user is listed individually or as a member of a group in the database ACL.
  or
- The Anonymous entry is set to No Access while an access level is specified for the Default entry in the ACL. Using this method allows you to require users to authenticate but prevents you from having to add individual entries for every user and group in the ACL.
When the Anonymous entry in the database ACL is set to No Access, users are presented with a logon prompt when they attempt to access the database.

Users must enter the user name and Internet password at the logon prompt. Users that are successfully authenticated are then provided with the access level that is specified for the Default entry in the database ACL.

If both the Anonymous entry and the Default entry in the database ACL are set to No Access, a user must be listed in the ACL individually or as part of a group to access the database. Setting the Anonymous and Default entries to No Access provides the strictest control over access to the database because only users and groups that are listed in the ACL are allowed to access the database.

An individual name receives precedence over the Default entry. If a user's name is entered in a database ACL and provided with an access level, the user receives the access level assigned to the user name entry in the database. Only users who are not listed individually in the database ACL receive the Default access level.

**Note:** If the Anonymous entry does not exist in the database ACL, the Default entry in the ACL must be set to "No access" to require basic password authentication to the database. When the Anonymous entry does not exist in the database ACL, anonymous users can access the database and receive the access level assigned to the Default entry in the database. If the Anonymous entry exists in the ACL and is assigned the "No access" access level, users are authenticated when accessing the database and receive the access level specified for the Default entry in the ACL.

**Related concepts:**
Database ACL settings
A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database.

**Related tasks:**
Setting up basic password authentication in a database Access Control List (ACL)
You can require users to specify a valid name and password when accessing a database on the Sametime server.

*Setting up basic password authentication in a database Access Control List (ACL):*

You can require users to specify a valid name and password when accessing a database on the Sametime server.

**About this task**

Follow these steps to set up basic password authentication for a database.

**Procedure**

1. From the Sametime server home page, click **Administer the Server** to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select **Domino Directory > Domino**. If you are using an LDAP directory with the Sametime server, select **LDAP Directory**.
3. Select **Access Control**.
4. Select a database from the list.
5. Click **Advanced**.
6. Set the "Maximum Internet name & password" access to Manager, which is the maximum access level.

   **Note** The "Maximum Internet name & password" setting on the advanced panel of each database Access Control List (ACL) specifies the maximum database access level granted to web browser clients. This setting overrides higher individual access levels set in the ACL. For example, if you set the "Maximum Internet name & password" to Author and assign Manager access to the Anonymous entry in the database ACL, anonymous users will only have Author access to the database. Alternatively, if you set the "Maximum Internet name & password" to Manager and assign Reader access to the Anonymous entry in the database ACL, anonymous users will only have Reader access to the database.

7. Click **Access**.

8. Select the Anonymous entry, and then select No Access in the Access box.

   If the Anonymous entry does not exist, you must create it. Use the following procedure to create an Anonymous entry and assign the No Access level to the entry:
   
   • Click Add.
   • Type Anonymous in the dialog box and click **OK**.
   • Select the Anonymous entry, and then select **No Access** in the Access box.

9. Select the Default entry. You can either set an access level for the Default entry, or set the Default entry to No Access.

   • If you specify an access level for the Default entry other than No Access, all users are required to authenticate when accessing the database. Each authenticated user receives the access level you have specified for the Default entry. It is not necessary to enter individual names or groups in the ACL. After selecting an access level for the Default entry, click **Submit**. You have finished the procedure required to set up basic password authentication in a database ACL. Skip the remaining steps.

   • If you select No Access for the Default entry, you must enter individual user names or group names in the ACL. Only the names and groups you enter can access the database. Complete steps 10 and 11 to add users to the ACL.

10. Click **Add** to add user names or group names to the ACL. Click **OK** after adding each name.

11. Click **Submit**.

**Related concepts:**

   Using database ACLs for identification and authentication
   Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

   Basic password authentication and database ACLs
   You can set a database ACL to require basic password authentication.

   Database ACL settings
   A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database.

**Setting up single sign on authentication**

IBM Sametime single sign-on (SSO) authentication allows web users to log in once to a Domino or WebSphere server, and then access any other Domino or WebSphere server in the same DNS domain that is enabled for single sign-on (SSO) without having to log in again. In a multiple server environment, it is possible that
one or more servers in your Domino domain are already configured for Domino SSO, and the Domino Directory already contains a Domino Web SSO configuration document. When you install Sametime, it creates a Web SSO configuration document called LtpaToken unless one already exists in the Domino Directory. If an LtpaToken configuration document already exists, Sametime does not attempt to alter it.

**About this task**

In some cases, it may be necessary to alter the default configuration of the Domino SSO feature following the Sametime server installation. For instructions, see “Altering the Domino Web SSO configuration following the Sametime server installation” on page 344.

**Configuring the Domino Server for Web SSO**

Complete the steps in this section if your Domino server is not configured for Web SSO, and you want to use the Web SSO document that Sametime creates to configure it.

**Procedure**

1. From the Domino Administrator or a Lotus Notes client, click **File > Database > Open**. Browse to the Domino server and type names.nsf in the Filename field. Click **Open**.

   **Note:** If you attempt to open this document from Domino Administrator Configurations tab, Web - web Configurations view, the Web SSO Configuration document will not display.

2. Expand the list of Web SSO Configurations.

3. Double click the "Web SSO Configuration for LtpaToken" document to open it in edit mode.

4. Update these fields as necessary:
   - Configuration name -- Enter LtpaToken.
   - DNS Domain -- make sure this is the fully qualified domain suffix of the Sametime server. For example, if the server’s fully qualified name is server.domain.com, the .domain.com should be entered in this field. Ensure that the leading period (.) is present in front of the domain suffix.
   - Organization -- Leave this field blank.
   - Participating servers -- Add the Sametime server and other servers that belong to the SSO realm to the list.

5. After entering the information, select **Keys** and do one of the following:
   - Create a Domino SSO Key
   - If WebSphere is participating in SSO, the Domino SSO key created by the install program should be replaced by the WebSphere LTPA key to allow both Domino and WebSphere to have an identical key for token validation and generation. Do this by importing the LTPA key from WebSphere to Domino. For more information, see Setting up single sign-on for Sametime browser clients.

   **Note:** When adding servers to the Participating servers field, click the arrow and choose the name from an Address Book when possible. If this is not possible, make sure that you use the full hierarchical name when you add a server (for example, Server1/Example where CN=Server/O=Org).
Chapter 4. Troubleshooting and support

When users or servers are having problems with IBM Sametime, administrators take steps to find and solve problems as quickly as possible.

This section contains information about troubleshooting and logging tools that can help you debug and fix problems affecting servers or users.

Other sources of information

Use the following links to find other hints and tips when troubleshooting Sametime servers:

- Sametime wiki:
  www.lotus.com/ldd/stwiki.nsf/
- Support Portal for Sametime:
  http://www.ibm.com/software/lotus/support/sametime/support.html
- Tech Notes for Sametime Gateway:
  Search results for Sametime Gateway Tech Notes

Troubleshooting Sametime clients

Use the following information to troubleshoot problems with IBM Sametime Connect and browser-based clients.

Logging and tracing on Sametime Connect

IBM Sametime Connect users can enable tracing on their clients.

1. On the machine where you use the Sametime Connect client, open the .config/rcpinstall.properties file in a text editor.
   To locate your Sametime workspace, see the topic Locating the Sametime Connect workspace.
2. Add the following lines to the end of the file, depending on what kind of issue you're diagnosing.

   General client issues:
   com.ibm.collaboration.realtime.level=FINE

   Telephony and audio/video issues, including Sametime Unified Telephony and Meetings:
   General issues:
   com.ibm.collaboration.realtime.internal.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.tcspi.level=FINEST
   com.ibm.collaboration.realtime.multimedia.level=FINE
   Audio/video quality issues:
   com.ibm.collaboration.realtime.internal.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.softphone.level=FINER
   com.ibm.collaboration.realtime.multimedia.level=FINER

   Note: In Sametime 8.5.1, the last line above will generate a substantial number of large audio/video trace files in your Sametime logs directory. During audio/video or Sametime Unified Telephony softphone calls, you might get 10
MB of tracing or more for each minute of the call. Do not use that level unless you have been instructed to do so and have ample free space on your hard drive.

**Instant messaging issues:**
com.lotus.sametime.community.kernel.level=FINER
com.lotus.sametime.im.level=FINEST
com.lotus.sametime.places.level=FINEST
com.ibm.collaboration.realtime.rtcadapter.level=FINEST
com.ibm.collaboration.realtime.people.internal.level=FINE
com.ibm.collaboration.realtime.internal.sametime.level=FINER
com.ibm.collaboration.realtime.login.level=FINEST
com.ibm.collaboration.realtime.community.internal.level=FINEST

**Login issues:**
General login failures:
com.ibm.collaboration.realtime.community.internal.level=FINEST
com.ibm.collaboration.realtime.im.community.level=FINEST
org.apache.commons.httpclient.level=FINE
com.ibm.rcp.internal.security.auth.module.level=FINEST
com.ibm.collaboration.realtime.login.level=FINEST
com.lotus.sametime.community.level=FINEST

SSO failures:
com.ibm.collaboration.realtime.community.internal.level=FINEST
com.ibm.collaboration.realtime.im.community.level=FINEST
org.apache.commons.httpclient.level=FINE
com.ibm.rcp.internal.security.auth.module.level=FINEST
com.ibm.collaboration.realtime.login.level=FINEST
com.lotus.sametime.community.level=FINEST
com.ibm.rcp.internal.security.level=FINEST
com.ibm.rcp.security.level=FINEST

**Managed settings:**
com.ibm.collaboration.realtime.policy.sametime.managedsettings.level=FINEST

**Meetings:**
General issues:
com.ibm.rtc.meetings.level=FINER
com.ibm.rtc.spaces.level=FINE
com.ibm.collaboration.realtime.appshare.level=FINER
com.ibm.rtccore.level=FINE
com.ibm.sharedmaps.level=FINER
com.ibm.rcp.level=FINER

Calendar integration issues:
com.ibm.rtc.meetings.servers.level=FINEST
com.ibm.rtc.meetings.shelf.level=FINEST
com.ibm.rtc.meetings.shelf.ui.level=FINEST
com.ibm.rtc.level=FINEST
com.ibm.collaboration.realtime.calendar.level=FINEST
com.ibm.collaboration.realtime.calendar.notes.level=FINEST

Connectivity issues:
com.ibm.rtccore.level=FINE
com.ibm.rtc.spaces.level=FINER

Screen sharing issues:
com.ibm.rtc.meetings.appshare.level=FINER
com.ibm.collaboration.realtime.appshare.level=FINE

Document sharing/conversion issues:
com.ibm.rtc.meetings.documents.level=FINE
com.ibm.rtc.meetings.appkit.image.level=FINE
com.ibm.workplace.converter.level=FINE

3. Save and close the file.
4. Restart your Sametime Connect client.
5. View the error log and trace files in Sametime Connect, by clicking Help > Support > View Log and View Trace.
   In most cases, View Trace provides the most useful information.

6. (Optional) If you need to provide logs to someone else for diagnostics, you can use IBM Support Assistant to collect logs and other data.
   For the Sametime 8.5.2 Connect standalone client and Lotus Notes 8.5.2:
   a. Click Help > Support > Collect Support Data.
      After a few moments, the Collect Support Data dialog opens.
   b. Click Next to start the collection. When the collection completes, a link to the collection zip file appears in the Collect Support Data dialog.
   c. Send the zip file to the person diagnosing the problem.
   For Lotus Notes 8.5.x:
   a. Click Help > Support > IBM Support Assistant.
   b. Select the Collect Data tab.
   c. Under Lotus Notes 8.5.x, select Notes General Problem Data Collection and click Add.
   d. Click Collect All to start the collection.
   e. When you are prompted for a reason, enter a descriptive response, and click OK.
   f. When you are prompted about collecting the .metadata directory, click OK.
   g. When the collection completes, a link to the collection zip file appears in the Collect Support Data dialog.
   h. Send the zip file to the person diagnosing the problem.

Alternate logging and tracing (standalone client only)

If you are using the standalone IBM Sametime Connect client for Release 8.5.1 or later, you can use IBM Support Assistant to enable or disable logging for certain client components. You can also do this with the Sametime Connect 8.5 Connect client, but the procedure is different. This procedure gives you the opportunity to reproduce the issue during the collection process, optionally restarting the client if that's required to reproduce the problem. Although this procedure method doesn't provide as much control over logging as the procedure above, it does not require restarting your client in order to enable/disable logging. The Lotus Notes embedded client does not provide the ability to enable or disable logging for individual Sametime components.

1. Click Help > Support > Collect Support Data. After a few moments, the Collect Support Data dialog opens.
2. Click the Customize link. The Collect Data - Sametime dialog displays.
3. Expand the Sametime Connect node in Collector Selection and select Sametime Connect Custom Tracing, then click Add to add custom tracing to the Collector Queue.
4. Click Collect All. After a few moments, the User Input dialog opens.
5. Select up to three components to collect tracing data.
6. Click OK and follow the instructions on the screen to complete the data collection.
7. When the collection completes, a link to the collection zip file appears on the dialog. You might have to scroll down in the dialog to see the link.
Locating the Sametime Connect workspace

Both IBM Sametime Connect and IBM Lotus Notes store user-specific data, including configuration data, preferences, and trace logs, in a workspace folder on your local hard drive or a network drive. In order to diagnose Sametime Connect issues, you might be asked to update or collect files in your workspace.

About this task

The workspace location varies depending on whether you are using the standalone Sametime Connect client or Lotus Notes, the operating system, and the product release. This topic helps you locate your workspace.

Sametime Connect standalone client

This release of Sametime Connect uses the following default workspace locations:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 and Vista</td>
<td>C:\Users\user_name\AppData\Roaming\Lotus\Sametime</td>
</tr>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\user_name\Application Data\Lotus\Sametime</td>
</tr>
<tr>
<td>Linux</td>
<td>~/lotus/Sametime</td>
</tr>
<tr>
<td>Linux (upgrade older client)</td>
<td>~/Lotus/Sametime</td>
</tr>
<tr>
<td>Mac OS</td>
<td>~/Library/Application Support/Lotus Sametime Data</td>
</tr>
<tr>
<td>Mac OS (upgrade older client)</td>
<td>~/Lotus/Sametime</td>
</tr>
</tbody>
</table>

**Note:** If you upgrade an older Sametime Connect 8.x client to this release, the existing workspace location is used, rather than the default workspace location.

Lotus Notes

Lotus Notes stores the workspace in the Notes data directory. For Notes 8.5.1 and later releases, the default workspace locations are:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows (single-user client)</td>
<td>C:\Program Files\IBM\Lotus\Notes\Data\workspace</td>
</tr>
<tr>
<td>Linux</td>
<td>~/lotus/notes/data/workspace</td>
</tr>
<tr>
<td>Mac OS</td>
<td>~/Library/Application Support/Lotus Notes Data/Expeditor/Applications</td>
</tr>
</tbody>
</table>

For Microsoft Windows, the location of the Notes data directory varies depending on whether the client is single user or multi user, whether you’re upgrading an existing client or installing a new one, and which version of Windows you’re using. For more information, see Notes installation directories for Windows in the Lotus Notes information center.
Troubleshooting audio and video in the Sametime Connect client

Enable diagnostics for audio and video in the IBM Sametime Connect client to assist with troubleshooting issues.

About this task

The following properties can be appended to the rcpinstall.properties file to enable audio and video diagnostic information. Find the file in the following location:

Microsoft Windows

In Microsoft Windows, this file is stored in the following directory: C:\Documents and Settings\user\Application Data\Lotus\Sametime\config\rcpinstall.properties.

Linux

home_dir/Lotus/Sametime/.config/rcpinstall.properties

Mac OS X

$HOME/Library/Application Support/Lotus Sametime Data/.config/rcpinstall.properties

The properties are listed by priority; they should not all be enabled at the same time.

# use for basic audio/video session troubleshooting
com.ibm.collaboration.realtime.multimedia.phonegrid.internal.client.level=FINE
# only use for ICE troubleshooting
com.ibm.ice.level=FINE
# only use for SIP troubleshooting
com.ibm.collaboration.realtime.telephony.softphone.level=FINE

The following notes about audio and video in the IBM Sametime Connect client can help you with issues raised by users.

Audio-video calls require 8.5 or later

Sametime 8.5 and later releases require the Sametime Media Manager for computer audio and video calls. In order to participate in audio or video calls, all parties must be using Sametime 8.5 or later clients, and must be logged in to a Sametime 8.5 or later server configured with the Sametime Media Manager.

Audio-video connectivity with a Sametime 8.5.1 embedded client for Lotus Notes

When attempting to connect a Sametime 8.5.1 embedded client for Lotus Notes to a newly installed Sametime 8.5.2 Media Server in a clustered configuration, the client cannot achieve audio video (AV) capability. A certificate error will be printed to the logs, indicating that the server certificate was not trusted. To resolve this issue, use the instructions in this technote:

Sametime 8.5.1.x Embedded client is unable to connect with audio video capability to a Sametime 8.5.2 Media Server
Troubleshooting the Sametime web audio-visual plugin

Consider these guidelines to help users troubleshoot the IBM Sametime web audio-visual plugin.

Enabling diagnostics for audio and video in the Sametime web audio-visual plugin

Enable diagnostics for audio and video for the IBM Sametime web audio-visual plugin to assist with troubleshooting.

About this task

The following logs help you and IBM Support troubleshoot and debug issues with the Sametime Web audio-visual plugin:

- UI traces
- Client logs
- Server logs

UI traces

To enable the UI traces for JavaScript processing, append the following parameters to the meeting or meeting room URL in the browser’s address bar:

?stmeetingsDebugLevel=debug&stmeetingsDebugScope=all

Client logs

Logs for the Sametime web audio-visual plugin are stored in the following locations:

- Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\n- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\n- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

The logging level is set with the LogFileLevel parameter in the WebPlayer.ini file. Logging level options are:

- 0 (default - no log information)
- 2 (errors only)
- 8 (errors and traces)
- 16 (maximum level of errors, traces, and notifications)

Find the WebPlayer.ini file in the following location:

- Microsoft Windows XP: %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\n- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\n- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

ICE diagnostics

Enable diagnostics on the use of ICE with the log_level setting in the ice.properties file. The trace level fine is sufficient. Trace options are:

- fine
- finer
Find the ice.properties file in the following location:

- Microsoft Windows XP: %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\ 
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\ 
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

GIPS Debug Trace

Set the GIPSDebugTraceEnable variable to true in the preferences.ini file.

Find the preferences.ini file in the following location:

- Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\Plugins\stwebsoftphone 
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\Plugins\stwebsoftphone 
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/Plugins/stwebsoftphone

Additional troubleshooting tools

Macintosh client running Firefox

Install XCode on the client machine, then install gdb, the GNU Project Debugger.
1. In a command window, type gdb and press Enter.
2. Type attach Firefox and press Enter.
3. Type c to continue.
4. When the browser crashes, type bt or backtrace and press Enter.
5. Copy all the traces into a file and include it in a Support request.
6. Type detach and q to exit.

Windows client

For Windows clients, running Internet Explorer 6 or 7, first try installing and using WinDBG, the Windows debugging tool available from Microsoft.
1. Start Internet Explorer.
2. Start WinDBG and use the File - Attach to a Process menu command to attach to the Internet Explorer process.
3. When a crash occurs, use View - Stack Trace to see the stack trace. Save the file as a .dmp file and include it in a Support request.

If WinDBG is changing the timing and not reproducing the crash, install and run the usercoredump.exe instead. Instructions are in this Microsoft Support article: How to use the Userdump.exe tool to create a dump file.

Install the program as described here: http://www.microsoft.com/downloads/details.aspx?FamilyID=E089CA41-6A87-40C8-BF69-28AC08570B7E&displaylang=en

Unless you have a specific need, disable the "dump on process termination" feature when you run the Setup.exe program.
Capture debugging information with one of these two methods:

- Set up user dump rules in advance.
  1. Go to the Control Panel and double-click **Process Dump**.
  2. Click **New**.
  3. Add Firefox.exe.
  4. Select Firefox and click **Rules**.
  5. Add a custom rule with the following selections:
     - Select c:\crashdump as the Dump file folder.
     - Leave the default Exception Codes and select **Ignore exceptions that occur inside Kernel32.dll**.
     - Set the MinDump Type as **Complete** and Save Mode as **Overwrite**.
     - Do not select anything else.
  6. Repeat the previous steps to add a custom rule for Iexplorer.exe.

- Capture process information after a crash.
  - When the program stops responding, move to the version of Userdump.exe for your processor at the command prompt, and then type the following command:
    
    userdump **PID**
    
    where **PID** is the process ID (PID) of the program that has stopped responding.
    
    To obtain the PID of the program, open Task Manager, and then click the **Process** tab.

The user dump file is generated in the c:\crashdump folder and can be included in a Support request.

**Related concepts:**
- “Log file locations” on page 439
  Use this reference to locate log files for IBM Sametime components.

**Related tasks:**
- “Enabling logging and tracing for a Sametime Proxy Server” on page 402
  The IBM Sametime Proxy Server utilizes the JSR-47 logging to record various events for troubleshooting. Using the IBM Websphere Integrated Solutions Console, you can fine tune the amount of captured trace content.
- “Setting a diagnostic trace on a Sametime Media Manager server” on page 403
  You can specify how the server handles IBM Sametime Media Manager log records. You can select a Sametime Media Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Troubleshooting issues with the Sametime web audio-visual plugin**

Consider these guidelines to help users troubleshoot the IBM Sametime web audio-visual plugin.

**Installing the plugin**

- The plugin works only with Internet browser (32-bit) on supported 32-bit or 64-bit operating systems (32-bit certifications only).
- The plugin can be installed on the client by any user. If the plugin is installed under the Administrator account, verify that the plugin installed into %WINDIR%\Downloaded Program Files folder, then uninstall the plugin and install the plugin again without using the administrator account.
• If a new profile is created for Firefox on a Mac client at a non-default location, the plugin installation will not succeed. Modify the path to an absolute path for newly created profiles in the Firefox profiles.ini file.

Issues with using the plugin

The meeting moderator sees the “Waiting for moderator” message in the Conferencing Panel upon entering his or her own meeting room. Clear the browser’s cache, restart the browser, and then join the meeting again.

The message “Video Starting” appears, but the call does not start. Take the following steps to ensure the connection can be completed:

1. Make sure that only one browser instance (tab or window) is opened for the Sametime Meeting Room client (a Sametime client cannot attend multiple meetings at the same time).
2. Exit the client.
3. On the client workstation, check the sip.log file to determine whether the client was able to register with the SIP Proxy and Registrar.
   
   Find the log in the Logs directory:
   
   Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\Logs
   Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\Logs
   Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/Logs
   
   a. Look for a “200 OK” message from the SIP Proxy and Registrar.
   b. Search for “Message In -> SIP/2.0 200 OK” and “CSeq: 1 REGISTER”:
      
      If the “200 OK” message was received from the SIP Proxy and Registrar, then check the Sametime Proxy Server log for an indication of why the client registration failed.
      
      If there was no “200 OK” message received from the SIP Proxy and Registrar, then verify that the client can telnet to the server as described in the next step.
4. Test the telnet connection to the SIP Proxy and Registrar server by opening a command prompt on the client workstation and running the following command:

   telnet SIP_hostname_or_IPaddress port
   
   for example:
   
   telnet 10.10.10.10 5080
   
   If the client can telnet to the server, check whether the SIP Proxy server received the REGISTER request (using a network sniffer or WebSphere traces).
   
   If the client cannot telnet to the server, check your network connections.

The user's status disappears in the meeting room.

Refresh the page or exit and then re-enter the meeting.

If remote video is not rendering and a user pauses the video, “Hide My Video” does not hide the local video.

Refresh the page or exit and then re-enter the meeting.
The audio-video plugin may experience problems if Gmail, Skype, or NetMeeting applications are running.

For best results, exit those applications before entering the Sametime meeting room.

IE6 and IE7 performance deteriorates if a user leaves and rejoins an audio-visual call multiple times in multiple-window mode.

Run the meeting room client in single-window mode.

If a user attempts to join the same meeting from two types of clients, the attempt from the second client will be unsuccessful.

Leave the Meeting room from one client before joining the other.

Audio and video are not working as expected.

Make sure that the appropriate latest sound and video device drivers are installed on the client machine.

The user sees a Conferencing Panel disabled in an A/V-enabled Meeting room or does not see live names.

Refresh the browser page. If that does not correct the problem, contact the administrator to make sure all Sametime servers are running and configured properly.

Troubleshooting meeting invitations

If users at your site are having difficulty inviting other users to meetings, verify the host name for the meeting room in their client preferences.

About this task

If a user enters a value for a server preference that is not a fully qualified host name, then the users that he or she invites into meetings might not be able to attend.

Procedure

1. In the IBM Lotus Sametime Connect client, click File > Preferences...
2. In Preferences, click Server Communities.
3. Click the host name for the server community that hosts the meeting room.
4. Click the Server tab.
5. Verify that the host name is fully qualified.
   For example, it should be messaging.yourcompany.com and not messaging.
6. If it is not a fully qualified host name, click Server Communities and remove the server community and re-add with the correct host name.
7. Click OK.

Troubleshooting Business Cards

If Business Cards are not displaying user information as expected, check the server configuration, then the client, and finally, the business cards themselves.

Checking the server configuration

Check and validate the configuration on the storage repository you use with the Sametime Community Server. A configuration problem is the most likely cause of problems with Business Cards. For more information, see the appropriate section in Managing business cards.
Checking the UserInfo servlet on the client

The UserInfo servlet on the client receives and responds to client requests. The servlet must be working correctly to provide the requested details for Business Cards. Follow these steps to verify that the UserInfo servlet is responding correctly.

1. Determine the distinguished name (DN) of the user whose Business Card you want to view. Here are sample DNs of the various directory types:
   - Domino directory: cn=sametime User/O=IBM
   - Active directory: cn=Sametime User, cn=users,dc=austin,dc=ibm,dc=com
   - TDS directory: uid=Sametime user,ou=Austin,o=IBM

2. Compose a URL to simulate the HTTP request that the client makes to retrieve details for a Business Card:
   - [protocol]://[hostname]/servlet/UserInfoServlet?operation=3&setid=1&UserId=[User DN]
   - [protocol] = {http, https}
   - [hostname] = {Fully qualified hostname of the Sametime server}
   - [User DN] = {The full distinguished name of the user for whose information you are seeking}

   Examples:
   - Domino Directory:
     http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User/O=IBM
   - Active Directory:
     http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User,cn=users,dc=austin,dc=ibm,dc=com
   - TDS Directory:
     http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=uid=Sametime user,ou=Austin,o=IBM

   Note:
   - Do not use spaces in the URL for the UserInfo servlet operation. A space is translated into %20 in the URL, and the servlet will not produce a result; for example:
     http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User/O=IBM
     is translated to:
     http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime%20User/O=IBM
     . The characters "%20" are inserted before the word "User" to represent the space.
   - The name “UserInfoServlet” is case sensitive.
   - Do not use apostrophes or quotation marks in the URL.

3. Enter the URL you’ve composed into a web browser's address field, and view the result.

   You should see the details you are expecting to see. If you do not, enable tracing for the UserInfo servlet as described in UserInfoConfig Debug tracing.
An UNKNOWN error for the "user id" means the user ID specified could not be located. The most common reasons for this error are:

- An incorrect user distinguished name has been specified
- The directory in which the user is located is not reachable/searchable

**Checking the client**

If the UserInfo servlet on the client is responding correctly, enable client-side tracing to determine what is happening on the client. Follow the instructions in Logging and tracing on Sametime Connect.

**Checking that Business Cards meet requirements**

Finally, verify that the business cards follow these requirements.

- Photos must be less than 45 kilobytes (recommended: 10 kb).
- Business Card photo requires .jpg or .gif.
- Using the jpegPhoto LDAP attribute to store photos requires the inetOrgPerson objectClass.

**Note:** Active Directory 2000 native/mixed mode does not provide inetOrgPerson objectClass by default.
- When you are using more than one storage type to store user information, the secondary storage repository cannot be of the same TYPE as the primary storage (the directory used by Sametime for authentication). For example, if Sametime is configured to use the Domino directory, then the secondary storage cannot also be a Domino directory.

**Troubleshooting a Sametime System Console**

Use the following topics to troubleshoot problems in an IBM Sametime System Console.

**Sametime System Console log locations**

The following table shows you where to find IBM Sametime System Console logs.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Solutions Console administration logs</td>
<td>was_install_root\profiles\STSCDMgrProfile\logs</td>
</tr>
</tbody>
</table>
| Find WebSphere Application Server-specific logs. The majority of messages that administrators are interested in are here. | was_install_root\profiles\STSCAppProfile\logs  
| Sametime System Console server logs | system_console_install_location\console\logs  
| Find logs for the application server of the cell profile of the console. | For example: c:\WebSphere\STServerCell\Console\logs  
| Sametime System Console client registration utility | temp\SSClogs  
| Find logs for the product server registration into the console. This post-registration utility refers to product servers as being clients of the console. |
Determining Sametime server status using the Integrated Solutions Console

You can use the Integrated Solutions Console to determine if an IBM Sametime Meeting Server, Proxy Server, or Media Manager is running.

About this task

You should verify the node agent, the server, and installed applications are running.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click System Administration > Node agents.
3. Locate the node for your server and verify that the Started indicator is displaying in the Status column.
4. Click Servers > Server Types > WebSphere application servers.
5. Locate your server and verify that the Started indicator is displaying in the Status column.
6. Click Applications > Application Types > WebSphere enterprise applications.
7. Locate your resource and verify that the Started indicator is displaying in the Application Status column.

What to do next

To start a server or node, see Starting and stopping servers from the Sametime System Console.

The console.properties file

The console.properties file contains settings used to register an IBM Sametime server with the Sametime System Console. This file is used with both IBM WebSphere-based servers and IBM Lotus Domino-based servers.

Sample settings for registering a Sametime server with the Sametime System Console:

#Specify the fully qualified host name for Sametime System Console
SSCHostName=ssc.in.ibm.com

#SSC WAS credentials
SSCUserName=wsadmin
SSCPASSWORD=password

#Specify true if you want to connect to Sametime System Console server using Secure Connection, else false.
SSCSSLEnabled=true

#Specify the HTTP port to Connect, can be found in <WAS_installRoot>/profiles/<profileName>/logs AboutThisProfile.txt.SSCHTTPPort=9080

#Specify the Secure Https port to Connect, can be found in <WAS_installRoot>/profiles/<profileName>/logs AboutThisProfile.txt.
SSCHTTPSPort=9446

#The log level for the Sametime System Console Client logs
The productConfig.properties file for WebSphere-based servers

The productConfig.properties file contains settings used to register an IBM Sametime server running on IBM WebSphere with the Sametime System Console.

Sample settings for registering a WebSphere-based Sametime server with the Sametime System Console; settings will vary depending on the server and your own environment.

#ProductType - It specifies the type of product installed
ProductType=com.ibm.lotus.sametime.meetingserver

#OfferingVersion - Version of the installed server
OfferingVersion=8.5.0.0

#InstallType - Installation Type - PN, SN, DM or Cell (WAS based product) . For Domino Based STNODE.
InstallType=Cell

#DepName - Specify a unique Deployment Name with which you want to register the server.
DepName=Meeting Server 85

#NodeIP - The IP of the machine on which the product server is installed
NodeIP=9.126.186.45

#NodeHostName - The fully qualified Hostname of the machine on which the product is installed
NodeHostName=myserver.abc.com

#WAS#
# Was Credentials - User Name and Password of Product Was server
WASUserID=wsadmin
WASPassword=wsadmin

#WASInstall - The root location where WAS is installed.
WASInstall=C:/ibm/WebSphere/AppServer

#WASSoapPort - The Soap Connector address for product WAS
WASSoapPort=8503

#WASHost - The hostname of the machine on which WAS is installed.
WASHost=myserver.abc.com

#WasCell - The Cell name of the Was Default profile
WASCell=myServerCell

#WASDMNode - The Node name of the Deployment Manager profile
WASDMNode=myServerDMNode

#WASNode - The Node name of the Secondary Node profile
WASNode=myServerNode

#WASAppProfile - The Appserver Profile name (Primary Node/Secondary profile)
WASAppProfile=STMApProfile

#WASAppServerName - The servername for the AppServer profile.
WASAppServerName=STMeetingServer

#WASDMProfile - The Dmgr Profile name (DM profile)
WASDMProfile=STMDMgrProfile

#WASDMServerName - The servername for the DM profile
WASDMServerName=dmgr

#WASSNProfile - The SN profile name
WASSNProfile=STMSNProfile

#WASDMSoapPort - The Soap Connector address for DM Profile
WASDMSoapPort=8503

# WASDMHost - The Deployment Manger host name
WASDMHost=hare.abc.com

#############################
#PreRequisite Database Details
#DBHost - The hostname of the DB used by product.
DBHost=9.122.64.26

#DBPort - The port on which the database server listens
DBPort=50000

#DBAppID - The application username for Database server
DBAppID=db2inst1

#DBAppPassword - The application password for Database server
DBAppPassword=passw0rd

#DBName - The database Name used by the product
DBName=testDB

#############################
#PreRequisite Ldap Details
#LDAPHost - The hostname of ldap registered with the product.
LDAPHost=bluepages.ibm.com

#LDAPPort - The port of ldap registered with the product.
LDAPPort=389

#LDAPBindAnonymous - Is anonymous access allowed for ldap registered with the product.
LDAPBindAnonymous=true

#LDAPBindDN - The Bind Distinguished name for ldap registered with the product.
LDAPBindDN=cn=root

#LDAPBindPwd - The Bind password for ldap registered with the product.
LDAPBindPwd=password

#LDAPType - The Type of ldap registered with the product.
LDAPType=IDS6

#LDAPLoginField - The LoginField of ldap registered with the product.
LDAPLoginField=mail;cn;uid

#LDAPBaseDN - The search base of ldap registered with the product.
LDAPBaseDN=o=abc.com

#LDAPDisplayName - The display name of ldap registered with the product.
LDAPDisplayName=cn

#LDAPPersonObjectClass - The object class of ldap registered with the product.
LDAPPersonObjectClass=Person

#LDAPSSLEnabled - Specifies if configured LDAP is SSL enabled.
LDAPSSLEnabled=false

#PreRequisite Community Server Details
#STCommunityServerHost - The hostname of the community server registered with the product.
STCommunityServerHost=xyz.abc.com

#STCommunityServerPort - The Community server port which registered with the product.
STCommunityServerPort=1516

#ConferenceFocusHost - The Confernce Focus server hostname used by media server
ConferenceFocusHost=stdev3.abc.com

#ConferenceFocusPort - The WAS SIP port for Conference Focus
ConferenceFocusPort=5063

#AVPacketSwitcherHost - The Packet Switcher server hostname used by media server
AVPacketSwitcherHost=stdev3.abc.com

#AVPacketSwitcherPort - The port for Packet Switcher.
AVPacketSwitcherPort=5063

#ProxyRegistrarHost - The Proxy Registrar server hostname used by media server
ProxyRegistrarHost=stdev3.abc.com

#ProxyRegistrarPort - The port for Proxy registrar
ProxyRegistrarPort=5080

#ComponentName - The component installed on the Media Server
ComponentName=Complete

#AVPacketSwitcherServerName - The WAS server name for media server.
AVPacketSwitcherServerName=STMediaServer

#AVPacketSwitcherSwitchId - Its a combination of "AVPacketSwitch" + NodeName.
AVPacketSwitcherSwitchId=PacketSwitchamalvadkMediaNode

#STReflectorHost - The Sametime reflector host
STReflectorHost=

#STReflectorPort - The Sametime reflector port
STReflectorPort=
The productConfig file for the Sametime Community server

The productConfig.properties file contains settings used to register an IBM Sametime Community Server with the Sametime System Console. This file is used only with the Sametime Community Server; a different copy of the file is used for IBM WebSphere-based servers.

### Purpose

Example settings for registering a Sametime Community server with the Sametime System Console:

```
#ProductType - It specifies the type of product Installed
#Community Server - com.ibm.lotus.sametime.communityserver
#Proxy Server - com.ibm.lotus.sametime.proxyserver
#Media Server - com.ibm.lotus.sametime.mediaserver
#Gateway Server - com.ibm.lotus.sametime.gatewayserver
#Meeting Server - com.ibm.lotus.sametime.meetingserver
ProductType=com.ibm.lotus.sametime.communityserver

# OfferingVersion = Version of the Installed Server
OfferingVersion=8.5.0.0

#InstallType-Installation Type -PN,SN,DM or Cell (WAS based Product). For Domino Based STNODE.
InstallType=STNODE

#DepName = Specify a unique Deployment Name with which you want to register the server.
DepName=Comm Server

#NodeHostName- The fully qualified Hostname of the machine on which the product is installed
NodeHostName=myserver.abc.com
```

### Troubleshooting clustering

This section describes how to troubleshoot problems with clustering servers in IBM Sametime.
Each of the WebSphere-based Sametime products is installed with an SSCConnecter servlet, which starts an mbean that allows the Sametime System Console to initiate a limited number of remote configuration commands before the Sametime product is federated into the WebSphere cell of the Sametime System Console. During the clustering process, this mbean is contacted, and the application initiates the addNode command, which starts the federation process. During this process, the Primary Node’s server where the mbean is running stops. This is required in order to federate properly. As a result, the Sametime System Console actually has no communication with the Primary Node during the federation process.

The Sametime System Console tests as many factors as possible to ensure that the federation succeeds prior to actually running the addNode command, and gives the user a warning if one of these conditions is found. Once the addNode command is initiated, the Sametime System Console begins polling the Deployment Manager configuration at intervals until it detects that the Primary Node’s configuration has been added successfully. Once it determines it has been successfully added, it alerts the administrator that the federation was successful. If after 5 minutes it does not detect the node in the Deployment Manager’s configuration, it gives an error stating that federation did not succeed.

Occasionally, federation actually takes longer than 5 minutes. In this case, simply waiting a few minutes and clicking Federate Node again results in a success message. Other times, the Deployment Manager has to be restarted, and then clicking Federate Node results in a success message. Very rarely, there is another condition that cannot be anticipated by the Sametime System Console that leads to the failure. In these cases, the administrator needs to look at the Primary Node’s AddNode.log for additional information to help resolve the issue, and if necessary, contact IBM Support for assistance.

In other extremely rare cases, running the federation from the Sametime System Console results in an error in the AddNode.log, but running the addNode command directly successfully federates the node into the Deployment Manager. This is an acceptable workaround if the administrator cannot figure out why the clustering guided activity is failing. Run one of the following commands to federate the node:

```
addNode.bat dmgrhost dmgrsoapport -username username -password password -includeapps -includebuses

./addNode.sh dmgrhost dmgrsoapport -username username -password password -includeapps -includebuses
```

After manually running addNode, the administrator can use the clustering guided activity for the remainder of the clustering process without any issues. The application recognizes the federated status of the node and proceeds accordingly.

After running the clustering guided activity, the administrator should make sure that all nodes are synchronized before restarting any node agents. In the Integrated System Console, click System Administration > Nodes, and select the nodes you want to synchronize, and then click the Synchronize.

### Troubleshooting a Sametime Community Server

Use the following information to troubleshoot problems with an IBM Sametime Community server.
Troubleshooting general issues in the Sametime Community Server

The topics in this section describe how to debug general issues with the IBM Sametime Community server that can be easily reproduced.

Gathering Sametime Community Server general diagnostic data

Collect information for IBM Support to investigate Sametime awareness problems and related issues.

About this task

The recommended trace level for gathering general diagnostic information, VP_TRACE_ALL=1, is very verbose, and therefore should only be used in on servers which have available disk space and CPU utilization to spare. If you are enabling trace on a production server which is running near capacity, please contact IBM Support to get more specific diagnostic settings which do not have as high of an impact on system resource.

Follow these instructions to set the trace level, and then reproduce the problem to gather information.

Procedure

1. Stop the Lotus Domino and Sametime Community Server.
2. Remove old log files from the Sametime trace directory.
3. Use a text editor to edit the sametime.ini file, which is located in the Sametime Community Server installation directory (for example: C:\Program Files\lotus\domino). Add the following line to the Debug section to set the trace level:
   
   VP_TRACE_ALL=1
   UCM_SNFF=0
   VP_SNFF=0
   UCM_DELAY_SNFF=0
   VP_DELAY_SNFF=0

4. Restart the Lotus Domino and Sametime Community Server.
5. Reproduce the problem that you want to troubleshoot, so you can collect diagnostic information.
6. Collect diagnostic information:
   a. Run the following collector utility: stdiagzip.bat located in the Sametime binary folder. For Windows, this is C:\Lotus\Domino by default. The output file is in the following format:
      \Trace\stdiags_hostname_MM_DD@hh_mm.zip
   b. Collect the following data:
      • The sametime.log file - Preserve as much history as possible. Do not remove data from this log.
      • The sametime.ini file
      • The communityConfig.txt file
      • The Stlog.nsf file - Keep this file small, not more then 1M.
      • STConfig.nsf
      • Details of user IDs that were used to reproduce the problem.
      • The exact time and date of the reproduced failure.
      • Client Application type and version that was used to reproduce the problem.
If you are troubleshooting a server crash, send all the core dump files which were created at the time of the crash.

Any additional details about the deployment, configuration, abnormal behavior, or any other general details that might help IBM Support with the problem investigation.

What to do next

After collecting the diagnostic information, any trace which was enabled on the Sametime Community Server should be disabled or reverted back to the default level. Use the STRuntimeDebug tool to enable and disable traces without having to restart the server.

Controlling the size and content of diagnostic data

You can set the maximum size file of each trace file and the maximum number of trace files used until the files are recycled. The setting is applicable to the IBM Sametime C++ -based Community Service Application.

Procedure

1. Use a text editor to edit the sametime.ini file, which is located in the Sametime Community Server installation directory (for example: C:\Program Files\lotus\domino).

2. Add the following lines to the Debug section:
   - ST_TRACEFILE_SIZE=file_size - Sets the maximum file size of each trace file.
   - ST_TRACEFILE_CNT = number_of_files - Set the number of trace files generated per Sametime service application. 
   
   ST_TRACEFILE_SIZE multiplied by ST_TRACEFILE_CNT equals the maximum size of the trace files on the Operating System hard disk per Sametime Community Service Application.

3. And finally, this.

Example

If the sametme.ini contains the following settings:

ST_TRACEFILE_SIZE=10
ST_TRACEFILE_CNT=25

Then 10 X 25 equals 250, so 250 MB is the maximum disk space each Sametime Service application consumes for the trace files.

Sametime Community Server log and trace file formats

The IBM Sametime Community Server log and trace files follow a specific naming format.

Log files

For Sametime 8.5 and later, log files are named Sametime_YYYYMMDD.log, where YYYYMMDD is the date. The log files are located in the ../Domino/Trace folder.

Note: For older versions of Sametime, the log file is named samtime.log and is located in the main application directory (data directory on Unix).

When the Sametime Community Server starts, a script runs that purges old logs. The script purges sametime_YYYYMMDD.log files that were created X number (X
is 30 by default) of days ago or more. You can change the number of days by editing the `T_PURGE_LOGS_OLDER_THAN` setting in the `sametime.ini` file.

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`).

2. Add or edit the following line in the `Control` section:
   
   ```
   T_PURGE_LOGS_OLDER_THAN=number_of_days
   ```

### Sametime.err file

The Sametime.err file includes detailed information about errors that occur when users attempt to log in to the Sametime Community Server. The name of the process always displays in the log file. Other information relevant to the login is also included, such as `UserID`, `UserName`, and `UserCluster`. Most errors are configuration-related problems that you can fix.

### Trace files

Trace files are logged in the `.../Domino/Trace` folder. Once a process starts, most of the components in the name of the trace file remain unchanged until the process is restarted. Only the counter part changes. The pattern for generating file names follows this format. The name of the process always displays in the log file. The other components of the format are optional:

```
<The name of the process>_<date of process startup>_<time of process startup>_<the process id number in the OS>_<trace file counter>
```

For example, if the trace file is named `StResolve_090720_1922_5544_088.txt`, then the name has the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Always displays/Optionally displays</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the process</td>
<td>Always</td>
<td>StResolve</td>
</tr>
<tr>
<td>Date of process startup</td>
<td>Optional</td>
<td>090720</td>
</tr>
<tr>
<td>Time of process startup</td>
<td>Optional</td>
<td>1922</td>
</tr>
<tr>
<td>Process id number in the OS</td>
<td>Optional</td>
<td>5544</td>
</tr>
<tr>
<td>Trace file counter</td>
<td>Optional</td>
<td>088</td>
</tr>
</tbody>
</table>

### Related reference:

“Troubleshooting login issues with the Sametime Community Server” on page 397

The Sametime.err file includes detailed information about errors that occur when users attempt to log in to the Sametime Community Server. The messages that follow are some typical issues related to user logins.

### Sametime Community Server trace files location

The Sametime Community Server has a series of configuration and log files for problem determination. You can run a script that automatically collects these logs.

- **Windows**
  
  From the Domino program directory, run the `stdiagzip.bat` file.
  
  For example:
  
  ```
  C:\Program Files\ibm\Lotus\Domino\stdiagzip.bat
  ```

- **AIX/Linux/Solaris**
  
  ```
  /local/notesdata> sh stdiagzip.sh
  ```
A zip file generated by the stdiagzip script is created in the data_dir/Trace directory

**IBM i**

```bash
  call QSAMETIME/STDIAZGZIP servername
```

A zip file generated by the stdiagzip program is created in the data_dir_TRACE directory.

### Gathering Sametime Community Server name change utility diagnostic data

Collect information for IBM Support to investigate the IBM Sametime name change utility.

### About this task

Since the trace files require large amounts of disk space, you should leave these settings turned off by default, and only enable them when you need to run the name change utility for special overall organization migrations.

Before you start the name change utility task, follow these instructions to set the trace level for gathering diagnostic information.

### Procedure

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory. For example:
   ```bash
   C:\Program Files\lotus\domino.
   ```
2. Add the following line to the Debug section to set the trace level:
   ```bash
   VP_NCSA_TRACE=1
   VP_LDAP_TRACE=1
   ```
3. Restart the Sametime Community Server.
4. After the name change task finishes, you can collect the diagnostic information:
   - A `namechange_*.txt` debug log file
   - If you ran a name change task in RESOLVE mode, then a `StResolve_*.txt` is produced, too.
5. Disable the `sametime.ini` file settings after the utility successfully finishes by setting the values to 0.

### NSD Log and core dump file location

When an IBM Sametime Community Services process crashes, an NSD log or core dump file is created with the relevant information about the crash.

The NSD log contains information about the tasks that were running when the process crashed, as well as general system information that may help determine the cause of the crash. The log is stored in the server's .\data\trace directory. On Windows, the log is stored in the server's .\trace directory. Part of the Sametime Community Components, using Notes API libraries, creates an NSD log in an alternate directory:.\data\IBM_TECHNICAL_SUPPORT.

**Important:** The date in the NSD log file's name is not its creation date, but rather the date when the crashing process was first executed. To find the date when the NSD log was produced, look inside the log or use the file creation date based on the operating system information.
Troubleshooting login issues with the Sametime Community Server

The Sametime.err file includes detailed information about errors that occur when users attempt to log in to the Sametime Community Server. The messages that follow are some typical issues related to user logins.

**Cannot redirect user to home cluster: Unknown cluster name UserClusterUserID, UserName**

Check the home cluster value of the user in the directory. It is possible that the home cluster of the user is correctly defined in the directory, but cannot be reached from the current server. Review communityConfig.txt to see which clusters are defined to verify the full mesh concept. For more information about clustering requirements, see the related tech note on the IBM Support site:


**Empty password is defined in person document for UserID**

Verify that the password in the Person document is defined correctly in the directory.

**Error: corrupted user storage attribute Attr for User ID UserID**

**Error: invalid type for storage attribute Attr for User ID UserID**

**Error: unable to read storage attribute Attr for User ID UserID**

**Error: storage attribute Attr type is different from opaque for User ID UserID**

Errors like these usually mean that the stored content for a specific user in the vpuserInfo.nsf database includes wrong data. Re-create the stored user document to correct the problem.

**Authentication failed: Empty user name is used with secrets token**

**Authentication failed for UserID: method is LTPA_TOKEN_ONLY. It does not allow to authenticate by secrets token**

**Verify secrets token failed for UserID. Reason: ReasonCode**

Failed generate token: Failed to get remote ldap directory user id for UserID

Failed generate LTPA token: empty token array is to be returned

Failed generate LTPA token: SECTokenListGenerate failed with error ReasonCode

Errors like these usually point to a problem with the single sign-on configuration. For more information, see the Sametime wiki article.
Related tasks:
“Setting up single sign-on (SSO) for Sametime clients” on page 335
Configure servers for single sign-on (SSO) as a convenience to users running the
Sametime browser client. With SSO configured, users who log in once to any
server in the DNS domain do not have to log in again when they access any other
server running on Domino or WebSphere Application Server. Enabling SSO
between the servers also helps the Connect Client as well. If the community server
is in the single sign-on domain, the component services can re-use the token from
the Connect client to login to other services.

Troubleshooting LDAP in Sametime

See the following article to troubleshoot LDAP problems in IBM Sametime.

About this task

The ”Best Practices for using LDAP with Sametime” article in the Sametime wiki
contains a table with common problems and resolutions:

Troubleshooting network issues on the Sametime Community
Server

The topics in this section describe how to diagnose networking problems that
affect performance with the IBM Sametime Community server.

About this task

Some environments are sensitive to network behavior, or use a configuration that
is insufficient for the expected Sametime capacity, which may result in the
following symptoms:
  • Delayed messages are caused by slow network performance. The messages may
    be one-to-one chats, group chats, and status updates of users.
  • Lost messages can occur when network slowdowns delay the delivery of
    messages and they are sent after the intended recipient logs out.
  • Failure to start a chat can occur when the request to start a chat times out on the
    recipient's end. The timeout is typically set to 30 seconds.

Best practices for performance of the Sametime Community
Server

Delays can be caused by insufficient throughput of server-to-server connections.
Follow these best practices to improve the throughput between servers.

About this task

Occasional delays, especially when data centers from different continents or remote
geographies are online and active together, can be caused by large individual
messages. If a large message is sent out and the throughput is insufficient, the
message can take an unusually long time to be transferred. While one message is
being transferred, no other message can be transferred on the same server-to-server
connection.

Frequent or sustained delays indicate that the throughput is not high enough
between two servers or given servers on remote geographies. In this situation, the
delays get progressively longer, until it appears that no messages are being
transferred.
Although network bandwidth can be a factor in low throughput, in most production environments, bandwidth is more than sufficient for Sametime. However, high network latency combined with a small TCP send buffer can often result in network delays. In particular, sites with servers in remote geographies may encounter this problem.

Use these best practices to improve throughput.

- All Sametime Community servers and multiplexers (if used) should be located in the same data center. Maintaining a short distance between servers is much more important than the distance between servers and clients.
- If the policy is to deploy servers on remote sites for site redundancy, try to set up sites with very low latency between them. High latency (for example, 250 ms) lowers throughput significantly. Low throughput causes congestion, which in turn causes long delays of 30 seconds or more.
- Here is a simple formula for calculating the throughput of a server-to-server connection:
  \[ \text{throughput} = \frac{\text{buffersize}}{\text{roundtrip\_latency}} \]
  - Buffer size is 8 KB by default on Windows. Sametime. Server-to-server connections default to 64 KB, which is the largest useful size on standard TCP.
  - Estimate the round trip latency by using the `ping` command.

**Improving throughput on Sametime 8.5 servers**

Sametime 8.5 Community Server, as well as hotfixes on top of earlier select releases, allows you to change the default server-to-server buffer size to improve performance. In the `sametime.ini` file, use the following buffer size settings, which match the default settings of Sametime 8.5.1 and later servers.

```ini
[Connectivity]
VPS_SERVER_SOCK_SO_SNDBUF=65536
VPS_SERVER_SOCK_SO_RCVBUF=65536
```

For older servers, contact IBM support to see if a fix is available for SPR #ICA27QLJJP for your release and operating system that supports the changes.

**Collecting data about network congestion problems that affect the Sametime Community server**

To diagnose network problems that affect performance and stability of the IBM Sametime Community Server, add specific flags related to network traffic to the `sametime.ini` file. Running the server with these flags allows you to collect data that you can then send to IBM Support for evaluation.

**About this task**

Follow these steps to add specific data collection flags to the `sametime.ini` file.

**Procedure**

1. Open a text editor on the Sametime Community Server.
2. Open the `sametime.ini` file located in the Sametime Community Server installation directory. For example, the default directory in Windows is `C:\program files\lotus\domino`.
3. Navigate to the Sametime Community Server's config section. The name is specific to the operating system you're running on.

**Windows**

[Debug-STCommunity]

**AIX, Linux, and Solaris**

[Debug-stserver]

**Note:** If you are troubleshooting a Sametime server running a release earlier than Sametime 8.5, contact IBM Support for the "per-component debug" feature, which is based on SPR#ICA3E7QLJJP. This feature provides the Debug-STCommunity or Debug-stserver sections described above.

4. Add one or more of the following flags.

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCM_TRANSFER_RATE_SAMPLE</td>
<td>The interval, in seconds, of sampling transfer rates of all Sametime TCP connections. A value of 0 indicates no sampling.</td>
<td>Recommended value for investigating delays and slow traffic: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCM_TRANSFER_RATE_TRACE</td>
<td>Indicates whether all transfer rate samples should be printed to debug trace files. A value of 1 indicates samples should be printed.</td>
<td>Recommended value for investigating delays and slow traffic: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPS_SERVER_TRANSFER_RATE</td>
<td>Setting this flag to a number greater than 0 sends reports of the transfer rates of server-to-server TCP connections to the sametime.log file. The flag is not useful for investigating delays or slow traffic, but rather to get an idea of the transfer rates. A value of 0 indicates no reports. Any other number represents how many times a day you want to generate reports.</td>
<td>In order to get a report once every 3 hours (8 times a day), set it to 8.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCM_DELAY_THRESHOLD</td>
<td>The threshold, in seconds, above which data queued for sending and not yet sent is reported as &quot;delayed&quot; in the socket layer. A value of 0 indicates no delay detection in the socket layer.</td>
<td>Recommended value for investigating delays: 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCM_DELAY_SNIFF</td>
<td>When set to 1, this flag dumps buffer contents to the debug trace files when a delay is detected by UCM_DELAY_THRESHOLD.</td>
<td>This flag is only useful in a few special cases. Recommended value: 0</td>
</tr>
</tbody>
</table>
Table 45. Sametime.ini flags related to network diagnostics (continued)

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VP_DELAY_THRESHOLD</td>
<td>The threshold, in seconds, above which encrypted data queued for sending and not yet sent would be reported as “delayed” in the encryption layer. A value of 0 indicates no delay detection in the encryption layer.</td>
<td>Recommended value for investigating delays: 10</td>
</tr>
<tr>
<td>VP_DELAY_SNIFF</td>
<td>When set to 1, this flag dumps buffer contents to the debug trace files when a delay is detected by VP_DELAY_THRESHOLD.</td>
<td>This flag is only useful in a few special cases. Recommended value: 0</td>
</tr>
</tbody>
</table>

5. Save the sametime.ini file.
6. Restart the Sametime Community Server.

**What to do next**

When you no longer need to collect the data, set the flags back to 0 and restart the server.

**Troubleshooting network problems on Domino**

Learn about the tools and utilities that you can use when troubleshooting problems on a Sametime Community Server.

**Basic networking knowledge and skills**

Sametime relies on networking to "work" as does Domino.

Use Ping, Telnet, Netstat and IPCconfig to verify that tunneling is set up correctly on the network and in DNS.

Use Ipconfig (at the DOS or command prompt) to:
- gather pertinent information for troubleshooting general TCP/IP network problems
- troubleshoot IP issues on DHCP clients.

Use Netstat to determine:
- if an application other than a Domino server task is bound to a specific port
- if there is a network connectivity problem at the network interface or with the physical media of the network
- if the local network segment might be overloaded.

Use Traceroute to determine the physical layout of a network or internetwork.

Use the Ping utility to:
- test connectivity to a host
- gather information for troubleshooting connectivity problems.

Use the Telnet utility to connect to a Domino server and check the status of an application on a well-known port.
Use the NotesConnect utility to determine:
- services running on a machine
- network configuration problems
- if the target host name can be resolved to its IP address

The link below is provided as a reference:

Networking Basics - Key Concepts in Computer Networking

**Troubleshooting a Sametime Proxy Server**

Use the following topics to troubleshoot problems in an IBM Sametime Proxy Server.

**Enabling logging and tracing for a Sametime Proxy Server**

The IBM Sametime Proxy Server utilizes the JSR-47 logging to record various events for troubleshooting. Using the IBM Websphere Integrated Solutions Console, you can fine tune the amount of captured trace content.

**Before you begin**

Ensure that the Sametime Proxy Server is running.

**About this task**

Follow these steps to enable tracing on the Sametime Proxy Server.

**Procedure**

1. Login to the WebSphere Integrated Solutions Console with administrator privileges on port 8601.
   
   For example: https://yourserver.com:8601/ibm/console
2. Select **Troubleshooting > Logs and Trace**.
3. Select **STProxyServer**.
4. Select **Diagnostic Trace**.
5. Select the **Runtime** tab.
6. Select **Change log level details**.
7. Type in the desired log setting, or select the components and levels by expanding the *[All Components] twistie.
8. Enable the **Save runtime changes to configuration as well** checkbox.
   
   Trace.log will be created in \profiles\STAppProfile\logs\STProxyServer for Windows or /opt/IBM/WebSphere/AppServer/profiles/xxxxSTPPNProfile logs/STProxyServer for Linux.

**Log Levels by Component**

<table>
<thead>
<tr>
<th>Log levels</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>*=info</td>
<td>Enabled by default. All SEVERE, WARNING, and INFO messages will be logged to Systemout.log and Systemerr.log.</td>
</tr>
<tr>
<td><em>=info: com.ibm.rtc.stproxy.</em>=all;com.ibm.collaboration.realtime.*=all</td>
<td>Enables Sametime Proxy related logging to the FINEST level.</td>
</tr>
</tbody>
</table>
### Troubleshooting a Sametime Media Manager

Use the following topics to troubleshoot problems in an IBM Sametime Media Manager.

**Setting a diagnostic trace on a Sametime Media Manager server**

You can specify how the server handles IBM Sametime Media Manager log records. You can select a Sametime Media Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Procedure**

1. In the Integrated Solutions Console, click **Troubleshooting --> Logs and Trace**.
2. Click the **STMediaServer** of if components are stored on different servers, the server component you want to change.
3. Under General Properties, click **Change Log Detail Levels**.
4. In the text box, append the following settings.
   - For a single server:
     ```
     :com.lotus.sametime.telephony.=*all:
     com.ibm.mediaserver.=*all:
     com.ibm.telephony.conferencing.spi.=*all:
     com.ibm.ws.sip.=*all:
     com.lotus.sametime.telephony.sipfocus.=*all:
     com.ibm.sip.=*all:
     com.ibm.sametime.packetswitch.=*all:
     com.ibm.sametime.telephonymanager.=all
     com.ibm.ice.=*all
     ```
   - For the conference manager only:
     ```
     :com.lotus.sametime.telephony.=*all:
     com.ibm.mediaserver.=*all:
     com.ibm.telephony.conferencing.spi.=*all:
     com.ibm.ws.sip.=*all:
     com.lotus.sametime.telephony.sipfocus.=*all:
     com.ibm.sip.=*all:
     com.ibm.sametime.telephonymanager.=all
     ```
   - For the packet switcher only:
     ```
     :com.ibm.ws.sip.=*all:
     com.ibm.sip.=*all:
     com.ibm.sametime.packetswitch.=*all:
     com.ibm.ice.=*all
     ```
   - For the SIP Proxy and Registrar only:
5. Check the box to reflect the log settings in the Configuration tab as well.

6. Click **OK**, and then **Save**.

7. Restart the Sametime Media Manager.

8. Monitor the log files in the following locations.
   - Windows: `WAS_Install_Root\WebSphere\AppServer\profiles\HostName_Media_deploymentType_Profile_Number\logs`
   - Linux: `/opt/IBM/WebSphere/AppServer/profiles/HostName_Media_deploymentType_Profile_Number/logs`

Logging and tracing on Sametime Media Manager

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.

2. If you cannot solve the problems using these files, try using a trace.

3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at [http://www-01.ibm.com/software/webservers/appserv/was/library/](http://www-01.ibm.com/software/webservers/appserv/was/library/).

Gathering Sametime Media Manager logs and traces for IBM Support

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

About this task

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem.

Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite.

Procedure

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
For more information, see the following topic in the WebSphere Application Server information center:
Gathering information with the collector tool (deprecated).

2. Run the collector on the IBM Sametime Media Manager server.
   • Run collector on the WebSphere Application Server profiles.
     The profiles are stored in the \profiles directory; for example on Microsoft Windows:
     C:\Program Files\ibm\WebSphere\AppServer\profiles

     The profile name follows this format:
     HostName_Media_deploymentType_Profile_Number
   • The collector resides in the \bin directory below the profile; for example:
     C:\Program Files\ibm\WebSphere\AppServer\profiles\wp1ccdlvm053MediaPNProfile1\bin\collector.bat

     The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:
     HostName_Media_deploymentType_Profile_Number-WASenv.jar

     Note: The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

3. To help with troubleshooting, IBM Support also needs a copy of the SIP Proxy and Registrar proxy.xml file from the Sametime System Console.
   The proxy.xml file is found in the following location on the Sametime System Console: \IBM\WebSphere\STSC\AppServer\profiles\STSCDMgrProfile\config\cells\cell_name\nodes\node_name\servers\STMediaServer

4. Submit the collector-generated log files and the proxy.xml file to IBM Support.

Troubleshooting a Sametime Media Manager using JVM logs
To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

About this task
An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.
   • SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it's better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
   • SystemErr.log contains exception stack trace information that is useful when performing problem analysis.
The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure
1. In the Integrated Solutions Console, click Troubleshooting > Logs and Trace.
2. Click STMediaServer.

   Note: Any configuration changes to the JVM logs that are made to a running IBM Sametime Media Manager do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting video quality
To ensure good quality video in your video-enabled IBM Sametime meeting rooms and Sametime Connect video calls, check your video driver.

Sametime Connect video calls and video-enabled Sametime meeting rooms take advantage of the hardware acceleration available in modern video cards and their associated drivers. If you are experiencing difficulty in establishing video call connections, or experience poor video quality in video in meeting rooms, ensure that you are using a video driver that takes full advantage of your video card's acceleration hardware.

Refer to the A/V Client Support & Requirements section in the system requirements:
http://www.ibm.com/support/docview.wss?rs=477&uid=swg27016451

Troubleshooting Sametime Media Manager component clusters
This section explains how to troubleshoot clusters of IBM Sametime Media Manager components.

Enabling logging and tracing for a Conference Manager cluster
Enable traces and logs for the members in a Conference Manager cluster.

Procedure
1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   :com.lotus.sametime.telephony.*=all:
   com.ibm.mediaserver.*=all:
   com.ibm.telephony.conferencing.spi.*=all:
   com.ibm.ws.sip.*=all:
Enabling logging and tracing for a SIP Proxy and Registrar cluster

Enable traces and logs for the members in a SIP Proxy and Registrar cluster.

**Procedure**

1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Troubleshooting > Logs and trace**.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click **Diagnostic Trace**.
5. Under "Additional Properties" click **Change Log Detail Levels**.
6. In the text box, append the following settings:
   ```
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all
   com.lotus.sametime.telephonymanager.*=all
   ```
7. Click **Apply**.
8. Save your changes by clicking the **Save** link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

Configuring a Sametime Community Server to allow connections from Conference Manager nodes

Add Conference Manager nodes to the list of Trusted IPs for an IBM Sametime Community Server.

**About this task**

This task is only necessary if you see the `ST_CONNECT_HOST_UNREACHABLE` error in the Conference Manager logs, which means that the Community Server is not allowing connections from the Conference Manager nodes. Enable the connection by adding each Conference Manager node's IP address to the list of Trusted IPs for the Sametime Community Server.

**Procedure**

1. Log into the Sametime System Console's Integrated Solutions Console as the WebSphere administrator.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the "Sametime Community Servers" table, click the name of a Community Server.
4. Click the **Connectivity** tab.
5. Add the Conference Manager nodes to the list of trusted servers:
   a. Under "Trusted Servers" enter the IP address (or host name) of the server where a Conferencing Manager node is hosted.
b. Click Add.
c. Repeat for each node in the Conference Manager cluster.
d. Click OK.

6. Restart the Sametime Community Server.

**Enabling traces and logs for the WebSphere proxy server used by a Media Manager cluster**

Enable traces and logs for an IBM WebSphere proxy server that is used with an IBM Sametime Media Manager cluster.

**About this task**

Both Conference Manager clusters and SIP Proxy and Registrar clusters can use a WebSphere proxy server; this task applies to both clusters.

**Procedure**

1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a WebSphere proxy server to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   :com.ibm.ws.sip.*=all
   :com.ibm.ws.proxy.*=all
7. Click Apply and then save the changes by clicking the Save link in the "Messages" box at the top of the page.

---

**Troubleshooting Sametime Bandwidth Manager**

Use the following topics to troubleshoot problems in an IBM Sametime Bandwidth Manager.

**Setting a diagnostic trace on a Sametime Bandwidth Manager**

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log. You can specify how the server handles IBM Sametime Bandwidth Manager log records. You can select a Bandwidth Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Procedure**

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the server name of the Bandwidth Manager.
3. Under General Properties, click Change Log Detail Levels.
4. In the text box, append the following settings.
   For a single server:
   :com.avistar.*=all
   If you suspect a problem with the SIP messaging, append:
If you suspect a problem with federated repository or LDAP access, append:

com.ibm.ws.sip.*=all:
com.ibm.sip.*=all:

If you suspect a problem with federated repository or LDAP access, append:

5. Click **Apply**, and then **Save**.
6. Restart the Sametime Bandwidth Manager.
7. Monitor the log files in the following locations.
   - Windows:
     
     WAS_Install_Root\WebSphere\AppServer\profiles\Bandwidth_Manager_profile\logs\Bandwidth_Manager_server_name
   - Linux:
     
     /opt/IBM/WebSphere/AppServer/profiles/Bandwidth_Manager_profile/logs/Bandwidth_Manager_server_name

### Troubleshooting a Sametime Bandwidth Manager using JVM logs

To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

### About this task

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it is better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

### Procedure

1. In the Integrated Solutions Console, click **Troubleshooting > Logs and Trace**.
2. Click the server name of the Bandwidth Manager.
3. Under General Properties, click **JVM Logs**.

   **Note:** Any configuration changes to the JVM logs that are made to a running IBM Sametime Bandwidth Manager do not take effect until you restart the server.

4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the **Runtime** tab, then click **View**.
Troubleshooting using the Bandwidth Manager Monitor and Policy Testing tools

IBM Sametime Bandwidth Manager provides tools in the administrative interface that can help troubleshoot problems in network topology setup.

About this task

The administrative tools you can use to troubleshoot problems are the Monitor and the route, call policy, and bandwidth test pages.

- **Monitor**
  The Monitor is accessed from the “Monitoring” tab in the user interface. It provides views into the currently active calls in the system. This activity can be organized in views by the Links and Sites that are configured, and also by individual calls. The Bandwidth Manager statistics topic explains the different statistics you can view.

- **Testing Routes, Call Rate Policies, Reflector Policies, and Bandwidth**
  The administrative interface allows you to test out call rate policies, routes, and bandwidth allocation before actually deploying them. There are buttons to access the Test Bandwidth Manager Policies page from the Call Rate Policies tab, the Monitoring tab, the Sites tab, and the Reflector Policies tab. The test page allows you to enter the caller and callee endpoint addresses, site names or groups, and user and group names to see which sites are used, which routes are used, how much bandwidth is allocated, and which reflector policies (if any) are used.

Related reference:
“Bandwidth Manager statistics” on page 135
Understanding the Bandwidth Manager monitor statistics can be useful for fine-tuning site and link bandwidth allocations and peak utilization points.

Troubleshooting Sametime Bandwidth Manager clusters

This section explains how to troubleshoot clusters of IBM Sametime Bandwidth Manager servers.

**Enabling logging and tracing for a Bandwidth Manager cluster**

Enable traces and logs for the members of an IBM Sametime Bandwidth Manager cluster.

**Procedure**

1. Log into the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings.
   For a single server:
   
   ```
   :com.avistar.*=all
   ```
   If you suspect a problem with the SIP messaging, append:
   
   ```
   com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all:
   ```
   If you suspect a problem with federated repository or LDAP access, append:
7. Click **Apply**.
8. Save your changes by clicking the **Save** link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

---

### Troubleshooting a Sametime TURN Server

If your IBM Sametime deployment experiences problems with NAT traversal, begin by troubleshooting the Sametime TURN Server.

**About this task**

**Attention:** Diagnostics should only be enabled under the advice of IBM Technical Support. IBM Technical Support will be able to determine whether extended diagnostics are required.

**Procedure**

1. On the TURN Server, navigate to the directory where the TURN Server files were installed (for example, `C:\TURN`).
2. Open the `logging.properties` file for editing.
3. Change the following settings as shown:
   ```
   java.util.logging.FileHandler.level=ALL
   java.util.logging.ConsoleHandler.level=ALL
   com.ibm.turn.server.level=FINER
   com.ibm.turn.server.level=FINEST
   com.ibm.network.agent.level=FINER
   ```

   Trace levels are:
   - **FINE:** Information logs as well as severe messages
   - **FINER:** Information logs and all messages
   - **FINEST:** ALL logs
4. Save and close the file.
5. Stop the TURN Server by pressing **Ctrl + C**.
6. Restart the TURN Server by running the batch file again.

**What to do next**

If you cannot isolate a problem on the TURN Server, you may need to troubleshoot other Sametime components that are involved in NAT traversal:
- Sametime Connect client
- Sametime web audio-visual plugin
- Sametime Proxy Server
- Sametime Media Manager - SIP Proxy and Registrar
Troubleshooting a Sametime Meeting Server

Use the following topics to troubleshoot problems in an IBM Sametime Meeting Server.

Setting a diagnostic trace on a Sametime Meeting Server

You can specify how the server handles IBM Sametime Meeting Server log records. You can select a Sametime Meeting Server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Procedure
1. In the Integrated Solutions Console, click Troubleshooting --> Logs and trace.
2. Click the Sametime Meeting Server that you want to trace.
3. Under General Properties click Diagnostic Trace
4. Under Additional Properties, click Change Log Detail Levels.
5. In the text box, append the following settings:

   To get even more detailed traces, use this setting instead:
   *=info: com.ibm.rtc.*=all

6. Click Apply, and then Save.
7. Monitor the log file in IBM\WebSphere\AppServer\profiles\HostName_Meeting_deploymentType_Profile_Number\logs
8. When you have identified and fixed the problem, free up system resources by reverting the trace level back to its default:
   *=info

Logging and tracing on Sametime Meeting Server

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log
files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.
2. If you cannot solve the problems using these files, try using a trace.
3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

Gathering Sametime Meeting Server logs and traces for support

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

About this task

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite.

Procedure

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
   For more information, see the following topic in the WebSphere Application Server information center:
   Gathering information with the collector tool (deprecated)
2. Run the collector on the IBM Sametime Meeting Server.
   • Run collector on the WebSphere Application Server profiles.
     The profiles are stored in the \profiles directory; for example on Microsoft Windows:
     C:\Program Files\ibm\WebSphere\AppServer\profiles
   • The collector resides in the \bin directory below the profile; for example:
     C:\Program Files\ibm\WebSphere\AppServer\profiles\HostName_Meeting_deploymentType_Profile_Number\bin\collector.bat

   The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:
   HostName_Meeting_deploymentType_Profile_Number-WASenv.jar

   Note: The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.
3. Submit the collector generated log files to IBM support.
Troubleshooting a Sametime Meeting Server using JVM logs

To start troubleshooting a problem on an IBM Sametime meeting server, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

About this task

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it's better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the IBM Sametime Meeting Server.

   Note: Any configuration changes to the JVM logs that are made to a running Sametime Meeting Server do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting a Sametime Meeting Server cluster

Use the following topics to troubleshoot problems in an IBM Sametime Meeting Server cluster.

Troubleshooting WebSphere proxy issues with the Sametime Meeting Server cluster

You can troubleshoot issues with the IBM WebSphere proxy server used with the IBM Sametime Meeting Server cluster by setting traces and logs.

Procedure

1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a WebSphere proxy server to open its "Logging and Tracing" page.
4. Under "General Properties" click **Diagnostic Trace**.
5. Under "Additional Properties" click **Change Log Detail Levels**.
6. In the text box, append the following settings:
   
   ```
   com.ibm.rtc.proxy.filter.*=all
   ```
   
   Based on this output, IBM might recommend other settings.
7. Click **Apply** and then save the changes by clicking the Save link the "Messages" box at the top of the page.
8. Repeat for every WebSphere proxy server used by the cluster.

### Improving performance when tracing is enabled on the WebSphere proxy server

If you enable tracing on an IBM WebSphere proxy server, improve performance by disabling attempts to resolve the client’s IP addresses to host names before writing to the log.

### About this task

Follow these steps to create a custom property called "disableTraceHostNameLookup."

### Procedure

1. Log in to the Deployment Manager's Integrated Solutions Console as the WebSphere administrator.
2. Click **Servers > Server Types > WebSphere proxy servers**.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
   
   This displays the Configuration tab for the selected proxy server.
4. Click **SIP Proxy Server Settings > SIP proxy settings**.
5. Under "Additional Properties," click **Custom Properties**.
6. In the table listing the custom properties, click **New**.
7. Create a new entry named `disableTraceHostNameLookup` with the value `true`.
8. Click **OK** to save the new custom property.
9. Click **Save**.
10. Repeat this process for every WebSphere proxy server that is operating with the cluster.
11. Synchronize the nodes and restart the cluster of Sametime servers:
   
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
   
   b. Select all nodes in the cluster.
   
   c. Back in the navigator, click **System Administration > Node agents**.
   
   d. Click a node agent, and then click **Restart**; repeat for each node agent.

---

**Troubleshooting a Sametime Gateway Server**

Use the following topics to troubleshoot problems in an IBM Sametime Gateway Server.

**Other sources of information**

Use the following links to find other hints and tips when troubleshooting Sametime Gateway:
Setting a diagnostic trace on Sametime Gateway

You can specify how the server handles Sametime Gateway log records. You can select a Sametime Gateway server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the RTCGWServer that you want to trace.
3. Under General Properties, click Change Log Detail Levels.
4. Select the Runtime tab.
5. Under com.ibm.rtc.*, click com.ibm.rtc.gateway.*.
6. From the context menu, select All Messages and Traces. You should now see the following text in the log detail level field: **info:
com.ibm.rtc.gateway.**=all
7. If SIP traces are required, add the following string to the detail level field, using a colon (:) as a delimiter.
com.ibm.ws.sip.stack.transaction.transport.TransportCommLayerMgr=all
The result looks like this:
8. Select Save runtime changes to configuration as well.
9. Click OK, and then Save. Restarting server1 is not necessary.
10. Monitor the log file in stgw_profile_root\logs\server_name\trace.log
11. If Sametime Gateway is clustered, repeat Steps 1 through 9 for each node in the cluster.

What to do next

Set a diagnostic trace on the SIP Proxy server, as described in Tracing a Session Initiation Protocol proxy server in the WebSphere Application Server information center.

Related tasks:
“Setting log files size and rotation” on page 257
You can specify the maximum size and number of log files to be stored on the server.

Setting a diagnostic trace for specific components

The IBM Sametime Trace Flags Composer tool allows you to generate flags that limit the diagnostic trace logging to specific Sametime Gateway components. Setting up diagnostic trace logging in this way gives you accurate results and minimizes the time that you and IBM Support spend troubleshooting a problem.
About this task

Follow these steps to set up a diagnostic trace for specific components.

Procedure
1. In the Integrated Solutions Console, expand the Sametime Gateway group.
2. Click Trace Flags Composer.
3. Select the components that you need to collect traces for.
4. Copy the result of the trace flags from the orange rectangle at the bottom of the page.
5. Return to the Integrated Solutions Console and click Troubleshooting > Logs and Trace.
6. Click the RTCGWServer that you want to trace – typically, all of the servers in the cluster.
7. Under General Properties, click Change Log Detail Levels.
8. The screen initially shows the Configuration tab. If the server is not running, the Configuration tab is the only tab on screen. If the server is running, an additional Runtime tab is available. If it is available, switch to the Runtime tab, and also select Save runtime changes to configuration as well.
9. Click OK and Save.

Logging and tracing

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.
2. If you cannot solve the problems using these files, try using a trace.
3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

Setting a diagnostic trace for specific user names and domains

In IBM Sametime Gateway, you have the option to turn on diagnostics traces only for those transactions that are in the context of specific user names and domains. This feature is also known as selective tracing.
About this task

If Sametime Gateway is a production system at your site that handles a high number of transactions per second, you might not be able to safely turn on server-wide diagnostic without exhausting the system's CPU resources. Another factor to consider when using server-wide diagnostic traces is that the volume of the produced traces can get quite large. To avoid these unwanted effects, you have the option to turn on diagnostics traces only for those transactions that are in the context of specific user names and domains. For example, you might want to trace only those transactions that are executed in context of the user joe@example.com, or for all of the users of the domain im.com, or even both. The user names and domains specific diagnostic is designed to work in parallel with the normal WebSphere server-wide diagnostic trace. One method does not contradict the other. The user names and domains pattern by which the diagnostic trace is produced is given as a regular expression. You have the option to engage this selective tracing without having to restart your Sametime Gateway servers.

Follow these steps to set the user names and domains specific diagnostic trace:

Procedure

1. Turn on WebSphere Application Server tracing.
   a. In the Integrated Solutions Console, click Troubleshooting > Logs and Trace.
   b. Click the RTCGWServer that you want to trace – typically, all of the servers in the cluster.
   c. Under General Properties, click Change Log Detail Levels.
   d. The screen initially shows the Configuration tab. If the server is not running, the Configuration tab is the only tab on screen. If the server is running, an additional Runtime tab is available. If it is available, switch to the Runtime tab, and also select Save runtime changes to configuration as well.
   e. In the text area you should see the following text:
      *=info:
      Replace it with:
      *=info: com.ibm.rtc.gateway.tracing.StgwLogger=all:
   f. Click OK, and then click Save.

2. Define a trace pattern as a custom property
   Create a custom property that defines the user names and domains pattern to trace by. Whenever a transaction is executing in the a user name and domain context that matches the pattern, the transaction produces the required diagnostic traces. If the transaction's context does not match the set pattern, no diagnostic trace is produced.

   How to compose a pattern
   Suppose we want to trace all of those transactions which involve:
   user1@domain10.com, or user2@domain2.com, or user20@domain2.com, or user212@domain2.com
   We could use the following pattern:
   (OE )?user1@domain10.com|(OE )?user2.*@domain2.com

   Regular expression breakdown
   • (OE )? - a required prefix that should always appear before the user name.
   • user1@domain10.com - the user's email address.
- the pipe character denotes an OR logical condition.
- user2.*@domain2.com - matches any user name that begins with user2, then contain any number of characters, and ends with @domain2.com.

IBM recommends that you test your regex pattern, before applying it. You can find an online web tester by entering java online regular expression testing in a search engine. For additional help on regular expressions, see the Java Regular Expression tutorial: http://java.sun.com/docs/books/tutorial/essential/regex/index.html

**Expected state**
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.

a. In the Integrated Solutions Console, open the Custom properties page for the server.
   - On a single server, click Servers > Server Types > WebSphere application servers > server_name > Server Infrastructure > Administration > Custom Properties.
   - On a clustered server, click System administration > Cell > Custom Properties.

b. Click New and enter the following information for trace pattern filter custom property:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>tracing.filter.pattern</td>
</tr>
<tr>
<td>Value</td>
<td>Regular expression</td>
</tr>
<tr>
<td>Description</td>
<td>A regular expression to serve as a user names and domains pattern For example: (?)?<a href="mailto:user1@domain10.com">user1@domain10.com</a></td>
</tr>
</tbody>
</table>

c. Click OK to save the new custom property.

d. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster. Traces are printed to the log file: stgw_profile_root/logs/trace.log. See the following additional procedure if you do not wish to restart the environment for these settings to take effect.

**3. Optional: Additional steps to apply the pattern in runtime without restarting the server.**

If you are not able to restart your Sametime Gateway environment, then the following procedure can be used to apply the new pattern during runtime without a server restart. You are still required to enter the described custom property in order to persist the trace across server restarts. If in a cluster, the following steps need to be executed once on the Sametime Gateway deployment manager only (there’s no need to execute on each cluster member directly), or on the standalone server (if not in a cluster):

a. Copy the following script from stgw_server_root/config/adminscripts/setTracePattern.py to the Deployment Manager node: app_server_root/bin.

b. Open a command window and navigate to app_server_root/bin

c. Run the following command:
   
   wsadmin -lang jython -username username -password password -f setTracePattern.py "pattern"
Where *username* is the administrative user ID that you use to log in to the Integrated Solutions Console. You created this user ID when you installed Sametime Gateway. Where *pattern* is a regular expression, surrounded by quotation marks, by which to trace individual users or domains. For example:

```
wsadmin -lang jython -username wasadmin -password gateway4u -f setTracePattern.py "(@E\s{1})?user1@domain10.com|(@E\s{1})?user2.*@domain2.com"
```

Note that when you enter the pattern using the shell command line, due to character escaping requirements, use `\s{1}` instead of the space character. Other than this difference, the custom property pattern and the command line pattern should be identical. In order to stop tracing and remove the pattern use "remove" as the pattern. For example:

```
wsadmin -username wasadmin -password gateway4u -f setTracePattern.py "remove"
```

**Note:** Any pattern will be lower case, because the tracing filter is not case sensitive.

d. Make sure that the last line that the script prints is the following message:

   OK: successfully set pattern on all servers.

e. Make sure have performed the previous steps of starting WebSphere traces and creating the required custom property, in order to preserve the trace settings for server restarts.

4. Optional: Set runtime Diagnostic Trace from the WebSphere Application Server administrative console to apply selective trace during runtime.

   When the server is restarted, these settings are recycled. Follow these steps to set up the runtime diagnostic trace.

   a. In the Integrated Solutions Console, expand the Sametime Gateway group and click **Selective Trace**.

   b. Type the pattern in the User name pattern field and click **Add**. The added pattern appears in the table.

   c. Repeat step 2 for all the patterns you want to trace.

   d. Click **Apply**.

   The selective trace runs and produces traces for the patterns you selected. You do not need to restart the Gateway server or clustered servers.

### Troubleshooting Sametime Gateway using Self-Service configuration tests

The IBM Sametime Gateway Self Service tool allows you to check configuration and connectivity health for a group of Sametime Gateway servers.

**About this task**

Follow these steps to run configuration tests on each Sametime Gateway server and see the cumulative results.

**Procedure**

1. In the Integrated Solutions console, expand the Sametime Gateway group.
2. Click **Self Service Tests**.
3. Select one of the following tests and click **Run Selected**. Or click **Run All** to run all the tests.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Status Log</td>
<td>Test result shows all the changes in communities’ status since the last restart of Gateway.</td>
</tr>
<tr>
<td>Community Active Sessions</td>
<td>Test result shows the active sessions for all the communities. The sessions are for instant messaging, inbound and outbound awareness</td>
</tr>
</tbody>
</table>
| Connectivity to internal community         | 1. Tests connectivity to the internal community “main” access point.  
2. Retrieves the Community Server deployment configuration from the “main” access point.  
3. Verifies connectivity to every Community server from this list. |
| Connectivity to external community (SIP and OCS) | Connects to the defined external community host and port and verifies basic connectivity.                                                  |
| Connectivity to external community (AOL)   | Verifies basic connectivity to the predefined AOL server (sip.oscar.aol.com) over port 5061.                                                   |
| Connectivity to external community (XMPP)  | • Verifies the XMPP DNS SRV record for every internal domain (_xmpp-server._tcp.domain).  
• Verifies the XMPP DNS SRV record for every external domain (_xmpp-server._tcp.domain).  
• Verifies the connection to every external host (defined in the DNS record) over port 5269. |
| WebSphere required fix level verification  | Verifies that all the required WebSphere Application Server fixes are installed on the machine. The list of the fixes is embedded in the Gateway package with every Gateway release. |
| XMPP Proxy configuration                   | This test is available only when the Gateway deployment is clustered. Tests the definition of several required Custom Properties. Also tests the definition of a required Port on the XMPP Proxy server. |

4. The test execution results appear when the tests are complete. Click any test name to see more details about the test.

**Gathering logs and traces for IBM support**

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting your problem.

**About this task**

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files,
operating system and Java data, and the presence and level of each software prerequisite. Be sure you set the log file size and rotation before you collect the information. The default log file rotation leaves the user only one file, which fills up and gets overwritten rather quickly.

**Procedure**

1. Follow these steps to configure the log file size and rotation settings.
   a. Log in to the Integrated Solutions Console.
   b. Click **Servers > Server Types > WebSphere Application Server**.
   c. In the Application Servers list, click the server name.
   d. Under Troubleshooting, click **Diagnostic trace service**.
   e. Under General Properties, update the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

   f. Click **OK**, and then click **Save**.

2. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.

   For information on using the Websphere Collector tool, see the WebSphere information center at the following web address:

   Gathering information with the collector tool (deprecated)

3. Run the collector on each of the computers in the Sametime Gateway deployment.

**Notes**

- On each machine, run collector once for each of the WebSphere Application Server profiles.
  
  The profiles are stored in the `\profiles` directory; for example on Microsoft Windows:

  C:\Program Files\ibm\WebSphere\AppServer\profiles

  - The collector resides in the `\bin` directory below the profile; for example:

    C:\Program Files\ibm\WebSphere\AppServer\profiles\RTCGW_Profile\bin\collector.bat

  The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:

  `myHostName-MyCellName-MyNodeName-RTCGW_Profile-WASenv.jar`

  **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

4. Submit the collector generated log files to IBM support.
Gathering performance data with the PMI tool

Starting with version 8.5.2, IBM Sametime Gateway exposes new application metrics through the standard IBM WebSphere PMI (Performance Monitoring Infrastructure). The metrics provided by the PMI tool replace the four metrics provided by Sametime Gateway versions 8.0.x - 8.5.1.x.

About this task

The WebSphere PMI tool provides performance metrics on WebSphere Application Servers and the applications they host. Tivoli-based monitoring solutions can sample these application PMI metrics. All of the metrics are measured for each application server instance. If you have a cluster of servers, you might want to perform custom offline aggregation processes in order to view cluster scope metrics.

The PMI provides three levels of metrics collection:

1. Server Health
   This lightweight metrics set is guaranteed not to cause any server performance degradation. When you enable metrics collection, this level is used by default.

2. Problem Determination
   This extended set of application metrics can be enabled to assist in a problem determination scenario. This level should only be turned on if instructed by IBM Support. All metrics that are part of the Server Health set are also included of the Problem Determination set.

3. Off

For Sametime Gateway, the PMI tracks information including the number of subscriptions and instant messaging requests, requests for each community, and the response time of subscriptions. You can view these statistics to help tune or troubleshoot Sametime Gateway problems.

Note: The PMI metrics are available for the Sametime Gateway application servers only, and are not available for the SIP proxy server or the XMPP proxy server used with Sametime Gateway.

Enabling metrics collection for Sametime Gateway

Enable the IBM WebSphere PMI (Performance Monitoring Infrastructure) tool and begin collecting performance metrics on WebSphere Application Server.

Before you begin

Before enabling metrics collection, make sure that the Sametime Gateway server is running. In a cluster, the Deployment Manager must be running; also, the node agent and the Sametime Gateway application must be running on at least one node.

About this task

The PMI tool collects and displays general WebSphere Application Server performance metrics on servers hosting Sametime Gateway. You can enable metrics collection for Sametime Gateway by creating a custom property that specifies the level of metrics that you want to collect. If you do not specify a custom level, the ServerHealth level is used by default. There are three levels of metrics collection:

- Server Health
This lightweight metrics set is guaranteed not to cause any server performance degradation. When you enable metrics collection, this level is used by default.

- Problem Determination

This extended set of application metrics can be enabled to assist in a problem determination scenario. This level should only be turned on if instructed by IBM Support. All metrics that are part of the Server Health set are also included of the Problem Determination set.

- Off

Metrics collection is disabled.

Procedure
1. Log in to the Integrated Solutions Console as the WebSphere administrator.
2. Open the Custom properties page:
   a. On a single server, click Servers > Server Types > WebSphere application servers > Gateway_server_name > Server Infrastructure > Administration > Custom Properties.
   b. On a clustered server, click System administration > Cell > Custom Properties.
3. In the custom properties table, click New.
4. In the Name field, type com.ibm.rtc.gateway.pmi.mode as the property’s name.
5. In the Value field, type the value representing the level of metrics collection that you want to enable: ServerHealth, ProblemDetermination, or Off.
6. Click OK to save the new custom property.
7. Save the change to the master configuration by clicking the Save link in the "Messages" box at the top of the page.
8. Restart the Sametime Gateway server. In a cluster, synchronize the nodes and restart the cluster as follows:
   a. In the navigation tree, click System Administration > Nodes.
   b. Select all nodes in the cluster, and then click the Full Resynchronize button at the top of the table.
   c. Back in the navigation tree, click System Administration > Node Agents.
   d. Select all nodes in the cluster, and then click the Restart button at the top of the table.

Results

Metrics collection is automatically enabled (or disabled) and set to the specified level after the server or cluster has started.

Modifying the PMI metrics collection for Sametime Gateway

When metrics collection is enabled for Sametime Gateway, you can optionally enable or disable counters through the PMI tool.

About this task

When you enable or disable counters, the setting remains only for the current session; when you restart the server the change is lost.

Procedure
1. In the Integrated Solutions Console, click Monitoring and Tuning > Performance Monitoring Infrastructure (PMI)
2. Click RTCGWServer.
3. On the Runtime tab, select Custom.
4. Click Apply and Save.
5. Click RTCGWServer.
6. On the Runtime tab, click (not select) Custom.
7. Select the STGWStats_Group.
   The panel on the right shows the counters that belong to Sametime Gateway. If you can't find the STGWStats Group in the tree view, the object is not being called or initialized, possibly because there are no successful subscribes between communities.
8. Select STGWCounters and click Enable.
9. In a cluster, repeat this process for every server in the cluster.

**Viewing PMI performance metrics**

There are a variety of tools you can use to view performance metrics collected by the IBM WebSphere PMI tool.

**About this task**

There are several ways to view performance data; including:
- Using the IBM Tivoli Performance Viewer that is incorporated into the Integrated Solutions Console, as explained below.
- Manually sampling the server's PMI metrics by installing the WebSphere PerfServlet on your server.
  After installing PerfServlet, you can view the metrics in an XML document by browsing to the following address: http://Gateway_host:9080/wasPerfTool/servlet/perfservlet?module=STGWStats_Group
- Querying the server's PerfMBean object using the wsadmin console.
- Creating your own periodic sampler utility, using the following utility as a reference: stgw_server_root/config/adminscripts/gw_perfservlet_retrieve.bash
- Using a third-party tool performance management tool, such as Tivoli Monitoring for Web Infrastructure, to review your performance metrics.
  For example, the Tivoli tool lets you collect, analyze, alert, and present the Sametime Gateway performance metrics.

**Procedure**

To view the PMI metrics through the Performance Viewer:
1. In the Integrated Solutions Console, click Monitoring and Tuning > Performance Viewer > Current activity.
2. Click RTCGWServer.
3. Expand Performance Modules.
4. Select either, or both, of the following options:
   - STGWStats_Group to see only group-level data
   - STGWStats_Group > Communities to see community-level data
5. Click View Module.
Example

In the image below, STGWStats_Group is selected to show community averages, plus community Southeast and community Northwest are also selected to show performance data for the individual communities.

List of PMI metrics for Sametime Gateway servers:

In addition to the general metrics collected for IBM WebSphere Application Server, the PMI tool collects the following metrics for IBM Sametime Gateway application servers.

Each metric (in the Metric Name column) can have multiple instances, with each instance measuring a different community or time resolution, described in the columns that follow.

Note: You must have metrics collection enabled (to either "Server Health" or "Problem Determination" level) for Sametime Gateway before you can view these statistics.

When reviewing the table, use the following column descriptions to help you understand the value of each metric:

By Community slicing

    Specifies how many different instances of this metric per community we will have:
    1. Global scope: the metric is gathered across all communities.
2. Sliced by source community: that there would be multiple metric instances.

Each instance measuring events generated by a specific source community. For a subscription event, the source community is the subscriber's community. For a chat invitation event, the source community is the chat initiator community. The total number of by community metric instances will be multiplied by the number of time-resolution metric instances (see next row).

**By Time-resolution slicing**

Specifies how many different instances of this metric we will have. For example: Since startup AND for the last 60 seconds means that there will be two metric instances, one counting since measurements were started (server started, or PMI enabled), and another that keeps measurement for the last full 60-second cycle.

**Statistic types**

Statistic types are taken from the PMI Data statistic types table.

**Set types**

Denotes whether this metric is included in the Server Health set or only in the Problem Determination set.

**Table 48. List of metrics collected by each Sametime Gateway server instance**

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Description</th>
<th>Community Slicing</th>
<th>Time-resolution Slicing</th>
<th>Statistic type</th>
<th>Set type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeriodCount</td>
<td>Time period counter, increases by 1 when a time period ends</td>
<td>Global scope</td>
<td>Current state</td>
<td>CountStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>IsCommunityConnected</td>
<td>Community connectivity state, value is 1 if the specific community is connected; 0 otherwise</td>
<td>By each community</td>
<td>Current state</td>
<td>CountStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>PresenceSessions</td>
<td>Current number of active presence sessions</td>
<td>Global scope</td>
<td>All time peak and current value</td>
<td>RangeStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>MaxAllowedSessions</td>
<td>Maximum number of allowed presence sessions</td>
<td>Global scope</td>
<td>Constant</td>
<td>Constant</td>
<td>Server Health</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Description</td>
<td>Community Slicing</td>
<td>Time-resolution Slicing</td>
<td>Statistic type</td>
<td>Set type</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>IMSessionsCount</td>
<td>The current number of active IM sessions</td>
<td>Global scope AND Sliced by target community</td>
<td>All time peak and current value</td>
<td>RangeStatistic: peak and current value</td>
<td>Server Health</td>
</tr>
<tr>
<td>MaxAllowedImSessions</td>
<td>The maximum number of allowed IM chat sessions</td>
<td>Global scope AND Sliced by community (a limit on the number of sessions involving this community)</td>
<td>Constant</td>
<td>Constant</td>
<td>Server Health</td>
</tr>
<tr>
<td>TranxTotalByStartup</td>
<td>The total number of processed transactions</td>
<td>Global scope AND Sliced by source community</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>CountStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>TranxTotalByPeriodCount</td>
<td>The total number of processed transactions for the last period of 60 seconds</td>
<td>Global scope AND Sliced by source community</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>CountStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>TranxFailedByStartup</td>
<td>The number of transactions that have failed (exceptions)</td>
<td>Global scope AND Sliced by source community</td>
<td>Since startup AND For the last period of 60 seconds (configurable)</td>
<td>CountStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>TranxFailedByPeriodCount</td>
<td>The number of transactions that have failed (exceptions) for the last period of 60 seconds</td>
<td>Global scope AND Sliced by source community</td>
<td>Since startup AND For the last period of 60 seconds (configurable)</td>
<td>CountStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>ExtCommByStartupResponseTime</td>
<td>Response time (in milliseconds) for receiving a response to requests sent to external communities</td>
<td>Global scope AND Sliced by external community</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>AverageStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>ExtCommByPeriodResponseTime</td>
<td>Response time (in milliseconds) for a transaction to complete processing by all Gateway plugins</td>
<td>Global scope AND Sliced by source community</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>AverageStatistic</td>
<td>Server Health</td>
</tr>
<tr>
<td>SipSendQueueSize</td>
<td>Current size of the SIP throttling queue size</td>
<td>N/A</td>
<td>Current state</td>
<td>CountStatistic</td>
<td>Problem Determination</td>
</tr>
<tr>
<td>PluginsByStartupResponseTime</td>
<td>Response time (in milliseconds) for a transaction to complete processing by all Gateway plugins</td>
<td>Global scope AND Sliced by source community</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>AverageStatistic</td>
<td>Problem Determination</td>
</tr>
<tr>
<td>ResolverCallsByStartup</td>
<td>The number of resolve requests sent to the Community Servers</td>
<td>Global scope</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>CountStatistic</td>
<td>Problem Determination</td>
</tr>
<tr>
<td>ResolverCallsByPeriod</td>
<td>The number of resolve requests sent to the Community Servers for the last period of 60 seconds</td>
<td>Global scope</td>
<td>Since startup AND For the last period of 60 seconds</td>
<td>CountStatistic</td>
<td>Problem Determination</td>
</tr>
</tbody>
</table>
Table 48. List of metrics collected by each Sametime Gateway server instance (continued)

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Description</th>
<th>Community Slicing</th>
<th>Time-resolution Slicing</th>
<th>Statistic type</th>
<th>Set type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResolverByStartup</td>
<td>Response time (in milliseconds) for resolve requests sent to Community Servers</td>
<td>Global scope Since startup</td>
<td>AverageStatisticProblem Determination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ResolverByPeriod</td>
<td></td>
<td>AND For the last period of 60 seconds</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Troubleshooting installation

These steps help you troubleshoot installation problems by describing how you can use a different tablespace name for the database and how you can clean your system of previous installations.

About this task

Many installation problems are caused when the installer cannot locate the database or when installing a new instance of Sametime Gateway and a previous installation has not been completely removed from the system. The following steps describe how to use a different tablespace in the database or clean your system of previous installations.

Procedure

1. Open the installation log file at `stgw_server_root\logs\installlog.txt`
2. If log reports an error in finding the DB2 database, check to make sure you are using the tablespace name `USERSPACE1`. Sametime Gateway expects `USERSPACE1` by default. To install using a different tablespace name, use the following command when you run the installer:
   ```
   install.bat -VTableSpaceName="tableSpaceName"
   ```
   Where `tableSpaceName` is the name of the tablespace that you want the installer to use.
3. To clean your system of previous installations, use the log to find the location of the Install Shield Multiplatform (ISMP) database called the Vital Product Database (VPD). For example, examine this log entry from Windows (formatted to fit on the page):
   ```
   (Nov 24, 2007 2:22:22 PM), stGwInstall,
   com.ibm.rtc.gateway.install.CheckVPDRegistry, msg1,
   using VPD registry at C:\Program Files\Common Files\InstallShield\Universal\common\Gen2\vpddb\vpd
   ```
   The location of this registry varies from system to system. On windows, VPD is usually found in the `\Program Files\Common Files\InstallShield\Universal\common\Gen2` folder. If a Sametime Gateway server is uninstalled, but an error occurs and the product is not unregistered, the VPD shows that Sametime Gateway is installed on the system. When a new installation is initiated, and a previously installed Sametime Gateway server is detected, the installer prompts you to upgrade or install a new version, or the installer forces you to install a
Deployment Manager server or a Primary Server on the same system. None of these scenarios are desired because there are no Sametime Gateway servers installed on the system.

4. Back up the Gen2 folder. Note that the VPD registry may be used by other programs that are installed with InstallShield, so removing this registry may interfere with other programs. It's recommended that you do not remove the Gen2 folder unless absolutely necessary.

5. Remove the original Gen2 folder.

6. If installing on Windows, delete the following left over files:
   - C:\Windows\nifregistry
   - C:\Windows\vpd.properties

7. Start the installation again.

**Troubleshooting WebSphere Application Server**

Transaction files may become locked and WebSphere Application Server may be in a state where nodes need to manually synchronized. If WebSphere Application Server is not responding in a logical manner, try carrying out these steps.

**Procedure**

1. Backup all configuration files on each node by running the backupConfig command.
2. Stop the node agents on each node.
3. Stop all servers.
4. Stop the Deployment Manager.
5. Manually synchronize the configurations, even if it says the nodes are fully synchronized, by copying the file system stgw_profile_root/config directory from the Deployment Manager to the config directory on each cluster member, including the proxy server node.
6. Delete all tranlog lock files from the file system. On each node, delete the contents of stgw_profile_root/tranlog.
7. Delete files in the temp and wstemp directories. On each node, delete the contents of:
   - stgw_profile_root/temp
   - stgw_profile_root/wstemp
   - stgw_profile_root/config/temp
8. Reboot each node.
9. Start the cluster.

**Related information:**

- WebSphere Application Server backupConfig command
- wsadmin backup command reference

**Troubleshooting the Sametime Gateway using JVM logs**

To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

**About this task**

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of
a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it’s better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the RTCGWServer.

   Note: Any configuration changes to the JVM logs that are made to a running RTCGWServer do not take effect until you restart the server.

4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting a failed WebSphere Application Startup

In the event that a change is made to a WebSphere Application Server component of Sametime Gateway, WebSphere Application Server could fail to start.

Procedure

1. Use a text editor to open the WebSphere Application Server file here:
   
   `<stgw_profile_root>\config\cells\<CellName>\nodes\<NodeName>\servers\RTCGWServer\server.xml`

2. In the server.xml file, search for `jvmEntries`. For example:

   ```xml
   <jvmEntries xmi:id="JavaVirtualMachine_1190064977109" verboseModeClass="false" verboseModeGarbageCollection="false" verboseModeJNI="false" initialHeapSize="1024" maximumHeapSize="1280" runHProf="false" debugMode="false" debugArgs="-Djava.compiler=NONE -Xdebug -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777" genericJvmArguments="-Xgcpolicy:gencon -Xgc:scvNoAdaptiveTenure,scvTenureAge=8,scvGlobalCompactToSatisfyAllocate -Xm256m" disableJIT="false"/>
   ```

   If the JVM arguments are incorrect, you must modify the `genericJvmArguments` attribute of the `jvmEntries` element of server.xml. You could leave it blank, to eliminate all errors, or try modifying the value of the attribute until it is correct. Two value here are the heap sizes. These values are set when you set the JVM garbage collection policy. But you can set them set them in the server.xml as well. These values are the `initialHeapSize` with a recommended value of 1024, and `maximumHeapSize`, set to a recommended value of 1280.

3. Save the file and restart the server.
Troubleshooting starting a cluster

Complete these steps to troubleshoot starting a cluster of Sametime Gateway servers.

Procedure

1. View the log file `stgw_profile_root\logs\SystemOut.log` for errors such as these:
   
   [CommonEventInfrastructure_Bus:STGW_Cluster.000-CommonEventInfrastructure_Bus]
   CWSIS1538I: The messaging engine, ME_UUID=35D47B7F8071E6CC, INC_UUID=7F6C7F6C371ED5F7, is attempting to obtain an exclusive lock on the data store.
   [CommonEventInfrastructure_Bus:STGW_Cluster.000-CommonEventInfrastructure_Bus]
   CWSIS1545I: A single previous owner was found in the messaging engine's data store, ME_UUID=D0E28FE74BF48C2E, INC_UUID=622662687271260A2
   [CommonEventInfrastructure_Bus:STGW_Cluster.000-CommonEventInfrastructure_Bus]
   CWSIS1535E: The messaging engine's unique id does not match that found in the data store. ME_UUID=35D47B7F8071E6CC, ME_UUID(DB)=D0E28FE74BF48C2E
   [CommonEventInfrastructure_Bus:STGW_Cluster.000-CommonEventInfrastructure_Bus]
   CWSIS1546I: The messaging engine, ME_UUID=35D47B7F8071E6CC, INC_UUID=7F6C7F6C371ED5F7, has lost an existing lock or failed to gain an initial lock on the data store.
   [8/22/06 14:22:50:421 EDT] 0000003d ConnectionEve A J2CA0056I: The Connection Manager received a fatal connection error from the Resource Adapter for resource jdbc/com.ibm.ws.sib/STGW_Cluster-CommonEventInfrastructure_Bus. The exception which was received is (none)

2. Use the Integrated Solutions Console to stop the Sametime Gateway servers, but do not stop the node agents.

3. Open a command window and navigate to: `stgw_profile_root/translog`

4. Delete all the files in this directory.

5. Start the DB2 Control Center.

6. Click All Systems > `<nodename>` > Instances > DB2 > Databases > STGW > Tables.

7. Find the table named IBMWSSIB.SIBOWNER.

8. Select all rows that appear in this table and click Delete.

9. Click Commit and then close the DB2 Control Center.

10. Click Servers > Clusters.

11. Select the Sametime Gateway servers and click Start to start the cluster.

12. To ensure that the CommonEventInfrastructure_Bus has started properly, click Service Integration > Buses.

13. Click CommonEventInfrastructure_Bus.

14. Click Messaging engines.

15. Look for a status green arrow next to the `@ClusterName@.000-CommonEventInfrastructure_Bus` which indicates that the bus started correctly. If it is not started, check the SystemOut.log for details.

Troubleshooting secondary node problems

In a cluster configuration, when a primary node is stopped, and awareness or instant messaging is not working when relying on a secondary node, check to make sure there are virtual host definitions created for each cluster member for the configured ports.
About this task

View the log file stgw_profile_root\logs\SystemOut.log for this error:

If you find this error, the virtual hosts definitions must be updated to have host
aliases defined for the SIP ports configured on each cluster member.

Procedure
1. In the Integrated Solutions Console, gather the port configurations for each
defined cluster member by selecting Servers > Application Servers.
2. Select a cluster member.
4. Record both the SIP_DEFAULTHOST and SIP_DEFAULTHOST_SECURE port
   numbers.
5. Repeat the preceding steps for each cluster member.
7. Select default_host
8. Under Additional Properties, click Host Aliases.
9. For each of the defined cluster members, ensure the ports that you recorded
   are present in the definitions.
   For example, if the secondary node is defined on server1.example.com at ports
   5062 and 5063, ensure the host aliases are defined as *:5062 and *:5063.
10. To create a new virtual host definition:
   a. Click New.
   b. Type the Fully qualified domain name of the host.
   c. Type the port number.
   d. Click OK and Save.
   e. Repeat for each port that requires a virtual host.

Troubleshooting connections to external communities
Consult the SIP return codes when you are troubleshooting a failed connection to
an external community.

About this task
While attempting to connect to external communities, various undocumented
return codes are received in the event of error or configuration mismatches.
Specifically, if a user has an issue while connecting to the SIP proxy, return codes
408 and 503 are returned. Use these return codes to determine what the Sametime
Gateway error messages mean.

<table>
<thead>
<tr>
<th>SIP Return Code Range</th>
<th>Link to Table</th>
</tr>
</thead>
</table>
Troubleshooting message handlers

This topic discusses how to troubleshoot message handlers in various stopped and started or enabled and disabled conditions.

Log messages

If you see "Not all the message handlers are up" in the SystemOut.log:

- Use the Integrated Solutions Console to check if all default message handler plugins are up and running. Click Applications > Enterprise Applications to view the state of the message handler applications.
- Also check if any message handler is disabled. Click Sametime Gateway > Message Handlers to view the message handler list.

If an application is enabled and you stop an application without first disabling it, the plugin manager considers this as a fatal condition and starts failing the requests. To disable a plugin, disable the application from the message handler page first, then stop the application from Integrated Solutions Console. This will alert the core plugin manager to omit the message handler from the execution sequence without failing the requests.

Message handler is disabled first and then stopped

Always disable the message handler first, and then stop it before removing the message handler. If you are debugging the core functionality, and wishes to disable the plugin, this is the sequence to follow. When a message handler plugin stops after being disabled, the configuration service removes the message handler object from the database. The configuration service alerts the core plugin manager of the change, and the core plugin manager subsequently omits this message handler from the execution sequence without adversely affecting the requests. You do not need to restart the server in order to disable or delete the message handler.

Message handler is stopped without being disabled first

Stopping the message handler before disabling it creates an error condition. The core plugin manager fails all the requests until the message handler plugin is disabled.

Message handler is disabled while it is running

The core plugin manager takes the message handler plugin out of the execution sequence. Requests continue to be processed and the plugin application is not invoked. If the message handler plugin is enabled, the core plugin manager puts the plugin back in the execution sequence, and starts forwarding requests to the newly enabled plugin.

Message handler is stopped, and then uninstalled without being disabled first

Stopping the message handler before disabling it creates an error condition. Disabling the message handler does not remove the message handler from the configuration. The disabled message handler remains in the configuration until the next time Sametime Gateway starts.
You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

**Troubleshooting slow or missing awareness changes**

The IBM Sametime Gateway server uses the Sametime community server resolve mechanism for resolving emails of internal community users to Sametime Ids - the unique representation of a Sametime user - and resolving Sametime Ids to user details - email and home cluster.

**About this task**

For each resolve request, the Sametime community server consults the directory server. Receiving the response from the Sametime community server is time consuming. To provide a warning on unreasonable response times, the Sametime Gateway collects resolve statistics. By default, the Sametime Gateway provides a warning only if the response time of the resolve request is greater then 25 seconds. The warning time is configurable, and it is possible to change it by adding a custom property to the local community.

Custom property name: **resolver.stat**

Valid values:

- **All** - prints the response time of all resolve requests.
- **Number of seconds** - Prints the response time of the resolve requests which are greater then the defined value.

To avoid a heavy load of messages on the Sametime Gateway server, for each 1000 identical messages only the first 5 are printed to the *SystemOut.log* file. If there are more than 5 identical messages, the first five are printed individually, followed by a summary of the rest of the identical messages.

```
[6/9/09 15:39:58:948 IDT] 00000021 ResolverStat W com.ibm.rtc.gateway.vp.util.resolve. ResolverStat printToTrace The previous log message printed by this thread has been printed 5 times. The next 999 messages of this message code would not be printed to the log.
```
Troubleshooting XMPP and Google community connections and awareness

This section describes how to troubleshoot XMPP/Google community connection and awareness problems. You can find missing SRV records, and fix firewall wrong settings and "Google Apps" registration.

About this task

Follow these steps for troubleshooting XMPP/Google community connections and awareness

Procedure

1. If the XMPP/Google community cannot connect, check the following areas:
   - The firewall is open for all possible incoming and outgoing connections from the other domain. For Google, see the following topic. Google sometimes changes their IPs, so the firewall should be updated: Opening ports in the firewalls
   - SRV records are well defined for ALL domains defined in the internal domains community page. Use the following command:
     ```
     nslookup -type=SRV -class=all _xmpp-server._tcp.DOMAIN_NAME.com
     ```
     Where `DOMAIN_NAME` is your domain name.
     For example:
     ```
     C:\>nslookup -type=SRV -class=all _xmpp-server._tcp.gvarim.com
     unknown query class: all
     Server: dhcpsrv3.haifa.ibm.com
     Address: 9.148.45.11
     
     _xmpp-server._tcp.gvarim.com    SRV service location:
     priority = 5
     weight = 0
     port = 5269
     svr hostname = vmgwteam1.haifa.ibm.com
     gvarim.com    nameserver = dhcpsrv3.haifa.ibm.com
     vmgwteam1.haifa.ibm.com internet address = 9.148.45.161
     dhcpsrv3.haifa.ibm.com internet address = 9.148.45.11
     ```
   - Your SRV record can be resolved by a public DNS. You can use the `nslookup` command from a computer outside the organization or by using public DNS resolution websites. You can use SRV verification instructions from this document: http://www-01.ibm.com/support/docview.wss?rs=899 &uid=swg21316296
   - Your partner domain SRV record can be resolved by your DNS, Can be checked by this command:
     ```
     nslookup -type=SRV -class=all _xmpp-server._tcp.DOMAIN_NAME.com
     ```
     Where `DOMAIN_NAME` is your partner domain name.
     For example:
     ```
     C:\>nslookup -type=SRV -class=all _xmpp-server._tcp.google.com
     unknown query class: all
     Server: dhcpsrv3.haifa.ibm.com
     Address: 9.148.45.11
     
     _xmpp-server._tcp.google.com    SRV service location:
     priority = 20
     weight = 0
     ```
port = 5269
svr hostname = xmpp-server1.l.google.com
_xmpp-server._tcp.google.com SRV service location:
priority = 20
weight = 0
port = 5269
svr hostname = xmpp-server2.l.google.com

- For Google, make sure there is no domain from your defined internal domains, which is registered with “Google Apps.” See this Technote: http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21295505

2. If an XMPP proxy is installed, check the following:
   - Your proxy should listen to the correct port and not conflict with another port definition on this machine. See the following topic: Configuring the XMPP proxy server.
   - Custom properties well defined with the correct cluster node and proxy name. See the following topic: Configuring the XMPP proxy server.

3. If there is no awareness after the community is already connected:
   - For Google, make sure there is no domain from your defined internal domains, which is registered with “Google Apps.” See this technote: http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21295505
   - For the Assign Users definitions, see the following topic: Assigning users access to external communities
   - For presence and chat limitations, see the following topic: Limiting Sametime Gateway global and community-level sessions.

4. If there are still connection and awareness issues, see the following Technote on collecting data: http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21316296

**Error message severity levels and situations**

This topic describes error message severity levels and the situations in which you are likely to encounter them.

In addition to the following information, see "Monitoring Sametime Gateway system events by tailing the SystemOut.log file" in the IBM Sametime wiki.

There are three message severity levels:
- Informational: the event only contains general information and is not reporting an error.
- Warning: a harmless error event that won't interfere with normal operation or a significant event that might require an action on the administrator's part.
- Error: Minor, Critical, and Fatal events.

The following situations will prompt log messages:
- Any message written to the server console.
- Any operation or action that affects the operation of the system such as starting and stopping a server or reconfiguration.
- Any changes to connected systems or environment (network connectivity, database availability) that can affect the components' continued operation.
- Failures or errors of any related component and any recovery or restart operations performed.
• Any response to operator commands for statistics, status, or other information that might need to be correlated to other events or information.

The following types of messages might be issued:

**Start messages**
- indicate when a component begins the startup process, finishes the startup process, or aborts the startup process. Start messages could include words like: *starting, started, initializing, and initialized.*

**Stop messages**
- indicate when a component begins to stop, has stopped, or has failed to stop. Stop messages could include words like: *stop, stopping, stopped, completed, and exiting.*

**Feature messages**
- announce when a component feature is ready (or not ready) for service requests. Messages could include words like: *now available, currently available, and transport is listening on port 123.*

**Dependency messages**
- Are produced by a component that cannot find another component or feature that it needs, such as messages about not finding the expected version of the component or that say a resource was not found, or that an application or subsystem that was unavailable. Dependency messages could include words like: *could not find, and no such component.*

**Request messages**
- Identify the completion status of a request. Typically these requests are complex management tasks or transactions that a component undertakes on behalf of a requester and not the mainline simple requests or transactions. Request messages could include words like: *configuration synchronization started, and backup procedure completed.*

**Configure messages**
- Identify any changes that a component makes to its configuration or messages that describe current configuration state. Configure messages could include words like: *port number is, address is, and process id.*

**Connect messages**
- Identify aspects about a connection to another component, for example, that say a connection failed, was created, or has ended. Connect messages could include words like: *connection reset, connection failed, and failed to get a connection.*

**Create messages**
- Register when a component creates an entity, for example, indicating that a document or file was created or that an EJB was created. Create messages could include words like: *was created, about to create, and now exists.*

**Report messages**
- Collect heartbeat or performance data reported from a component, such as current CPU utilization or current memory heap size. Report messages could include words like: *utilization value is, buffer size is, and number of threads is.*

**Availability messages**
- Report data about a component’s operational state and availability. This situation provides a context for operations that can be performed on the component by distinguishing whether a product is installed, operational and ready to process functional requests, or operational but ready or not
ready to process management requests. This type of message is different from Dependency messages, which pertain to services. Availability messages could include words like: now ready to take requests, online, and offline.

Log file locations

Use this reference to locate log files for IBM Sametime components.

Collecting the proper files and information helps to expedite problem determination and resolution for IBM Sametime when you are working with IBM Support. Provide the following information:

- A precise description of the issue, error message, and steps to reproduce
- Applicable screen shots of the problem or error message
- Log files pertaining to your problem

**collectLogs utility**

You can use the collectLogs utility to gather logs. collectLogs is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var/ibm/InstallationManager/logs

**SSC connection log:**

/tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Windows 2003**

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

**SSC connection log:**

Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**Installation Files**

Installation log files can be found in the following locations:

- **Windows**
  
  C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs**Windows 2008**
  
  C:\ProgramData\IBM\Installation Manager\logs

- **AIX/Linux/Solaris**

  /var/ibm/InstallationManager/logs

- **Websphere-based application log files** are created on the server's file system for each server's instance.
Sametime System Console

Sametime System Console log files can be found in the following locations:

- **Windows**
  - C:\Program Files\ibm\WebSphere\AppServer\profiles\STSCDMgrProfile\logs
  - C:\Program Files\ibm\WebSphere\AppServer\profiles\STSCAppProfile\logs

- **AIX/Linux/Solaris**
  - /opt/IBM/WebSphere/AppServer/profiles/STSCDMgrProfile/logs
  - /opt/IBM/WebSphere/AppServer/profiles/STSCAppProfile/logs

- **IBM i**
  - /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STSCDMgrProfile/logs
  - /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs

Sametime Proxy Server

Sametime Proxy Server log files can be found in the following locations:

- **Windows**
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STPAppProfile\logs
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STPDMgrProfile\logs

- **AIX/Linux/Solaris**
  - /opt/IBM/WebSphere/AppServer/profiles/STPDMgrProfile/logs
  - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile/logs

- **IBM i**
  - /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STPDMgrProfile/logs
  - /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs

Sametime Meeting Server

Sametime Meeting Server log files can be found in the following locations:

- **Windows**
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STMDMgrProfile\logs
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STMAppProfile\logs

- **AIX/Linux/Solaris**
  - /opt/IBM/WebSphere/AppServer/profiles/STMDMgrProfile/logs
  - /opt/IBM/WebSphere/AppServer/profiles/STMAppProfile/logs

- **IBM i**
  - /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STMDMgrProfile/logs
  - /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STMAppProfile/logs
**Sametime Media Manager**

Sametime Media Manager log files can be found in the following locations:

- **Windows**
  
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSdmgrProfile\logs
  
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSAppProfile\logs

- **Linux**
  
  /opt/IBM/WebSphere/AppServer/profiles/STMSdmgrProfile/logs
  
  /opt/IBM/WebSphere/AppServer/profiles/STMSAppProfile/logs

**Sametime Community Server**

The Sametime Community Server has a series of configuration and log files for problem determination. You can run a script that automatically collects these logs.

- **Windows**
  
  From the Domino program directory, run the stdiagzip.bat file.
  
  For example:
  
  C:\Program Files\ibm\Lotus\Domino\stdiagzip.bat

- **AIX/Linux/Solaris**
  
  /local/notesdata> sh stdiagzip.sh
  
  A zip file generated by the stdiagzip script is created in the data_dir/Trace directory

- **IBM i**
  
  call QSAMETIME/STDIAGZIP servername
  
  A zip file generated by the stdiagzip program is created in the data_dir/trace directory

**Sametime clients**

The Sametime Connect log files are in the logs directory, which is located under the client workspace directory described in “Locating the Sametime Connect workspace” on page 378.

**Related concepts:**

  “Logging and tracing on Sametime Connect” on page 375

  IBM Sametime Connect users can enable tracing on their clients.

**Directory conventions**

Directory variables are abbreviations for the default installation paths for IBM AIX, Linux, Solaris, IBM i, and Microsoft Windows. This topic defines the directory variable and its matching default installation directory for each supported operating system.
<table>
<thead>
<tr>
<th>Directory variable</th>
<th>Operating system</th>
<th>Default installation root</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AIX</td>
<td>/usr/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td>/QIBM/ProdData/WebSphere/AppServer/V7/ND</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>[drive]:\Program Files\IBM\WebSphere\AppServer</td>
</tr>
<tr>
<td></td>
<td>AIX</td>
<td>/usr/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td>/QIBM/UserData/WebSphere/AppServer/V7/ND</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>[drive]:\Program Files\IBM\WebSphere\AppServer</td>
</tr>
<tr>
<td></td>
<td>All platforms</td>
<td>Primary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STSCAppProfile</td>
</tr>
<tr>
<td></td>
<td>All platforms</td>
<td>Primary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STMAppProfile</td>
</tr>
<tr>
<td></td>
<td>All platforms</td>
<td>Secondary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STMSNAppProfile</td>
</tr>
<tr>
<td></td>
<td>All platforms</td>
<td>Primary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STPAppProfile</td>
</tr>
<tr>
<td></td>
<td>All platforms</td>
<td>Secondary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STPSNAppProfile</td>
</tr>
</tbody>
</table>

WebSphere Application Server installation directory.

For Sametime Gateway upgrade:
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:
AIX: /usr/IBM/WebSphere/AppServer7
Linux and Solaris: /opt/IBM/WebSphere/AppServer7
IBM i: /QIBM/ProdData/WebSphere/AppServer/V7/ND
Windows: [drive]:\Program Files\IBM\WebSphere\AppServer7

Root directory for the creation of WebSphere Application Server profile directories.

For Sametime Gateway upgrade:
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:
AIX: /usr/IBM/WebSphere/AppServer7
Linux and Solaris: /opt/IBM/WebSphere/AppServer7
IBM i: /QIBM/ProdData/WebSphere/AppServer/V7/ND
Windows: [drive]:\Program Files\IBM\WebSphere\AppServer7

Primary node: app_server_root/profiles/STSCAppProfile
Secondary node: app_server_root/profiles/STMAppProfile
STMSNAppProfile
STPAppProfile
STPSNAppProfile
<table>
<thead>
<tr>
<th>Directory variable</th>
<th>Operating system</th>
<th>Default installation root</th>
</tr>
</thead>
</table>
| stMS_profile_root         | All platforms      | Primary node
  app_server_root/profiles/STMSAppProfile
  Secondary node
  app_server_root/profiles/STMSSNAppProfile |
|                           |                    | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | /opt/IBM/WebSphere/AppServer/profiles/RTC GW_Profile[1,2,...]    | IBM i
  /QIBM/UserData/WebSphere/AppServer/V7/ND/RTC GW_profile |
|                           | AIX                | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | /opt/IBM/WebSphere/AppServer/profiles/RTC GW_Profile[1,2,...]    | Windows
  [drive]:\Program Files\IBM\WebSphere\AppServer\profiles\RTC GW_Profile[1,2,...] |
|                           | Linux and Solaris  | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | /opt/IBM/WebSphere/AppServer/7/profiles/RTC GW_Profile[1,2,...] |
|                           | IBM i              | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | /QIBM/UserData/WebSphere/AppServer/7/profiles/RTC GW_Profile[1,2,...] |
|                           | [drive]:\Program Files\IBM\WebSphere\AppServer\profiles\RTC GW_Profile[1,2,...] |
| stgw_profile_root         | AIX                | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | /opt/IBM/WebSphere/AppServer/profiles/RTC GW_Profile[1,2,...]    | stADV_profile_root
  The Sametime Advanced Server profile directory
|                           | IBM i              | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | /QIBM/UserData/StGateway/[profile name]                        |
|                           | Windows            | For SameTime Gateway upgrade:                                  |
|                           |                    | If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: |
|                           |                    | [drive]\Program Files\IBM\WebSphere\StGateway                |
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
5 Technology Park Drive
Westford Technology Park
Westford, MA 01886
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,
modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

These terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
AIX
DB2
DB2 Universal Database Domino
Domino
Domino Designer
Domino Directory
i5/OS
Lotus
Lotus Notes
Notes
OS/400
Sametime
WebSphere

AOL is a registered trademark of AOL LLC in the United States, other countries, or both.

AOL Instant Messenger is a trademark of AOL LLC in the United States, other countries, or both.

Google Talk is a trademark of Google, Inc, in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.