Main page: Cisco Unified MeetingPlace, Release 7.1

Navigation: Integration > Integrating with IBM Lotus Notes

Contents

- 1 Enabling Automatic Authentication for IBM Lotus Notes Users
  - 1.1 Preparing the System for Lotus Domino Authentication
  - 1.2 Importing the User IDs
  - 1.3 Verifying the Import
  - 1.4 Setting the Authentication Method
- 2 Copying IBM Lotus Notes Templates and Files to the Lotus Domino Server
- 3 Setting Up Database and Mail Templates for IBM Lotus Notes
  - 3.1 Granting Permission to Run Restricted and Unrestricted Agents on the Lotus Domino Server
  - 3.2 Signing the MeetingPlace Server Agent Template
  - 3.3 Signing the Cisco Unified MeetingPlace Mail Template
- 4 Expanding the Document Capacity of the Lotus Notes Account
- 5 Configuring SSL Support for IBM Lotus Notes
  - 5.1 Installing the Sun SDK File
  - 5.2 Adding Certificates to the Lotus Domino Keystore
  - 5.3 Editing the java.policy File
- 6 About Load Balancing for IBM Lotus Notes with Cisco Unified MeetingPlace Release 7.1

Enabling Automatic Authentication for IBM Lotus Notes Users

You can improve the speed of the meeting scheduling process by configuring your Lotus Domino Server to automatically authenticate users to Cisco Unified MeetingPlace. With automatic authentication, the Lotus Domino Server can pass user IDs to Cisco Unified MeetingPlace for verification whenever a user schedules a meeting. If the user IDs on both systems match, the system automatically signs users in to Cisco Unified MeetingPlace.

Without automatic authentication, users must enter their Cisco Unified MeetingPlace user IDs and passwords in the Calendar Entry form when they schedule a Cisco Unified MeetingPlace meeting.

Preparing the System for Lotus Domino Authentication

Before You Begin

You must have a user ID with administrator privileges to log in to the Cisco Unified MeetingPlace Web Server.

Procedure

1. Log in to the Cisco Unified MeetingPlace Web Server as an administrator.
2. Select **Start > Control Panel > Administrative Tools > Component Services**.
3. Select **console root > Component Services > Computers > My Computer > DCOM Config > LNNotify** from the left pane.
4. Right click **LNNotify**.
5. Click **Properties**.
6. Click the Security tab.
7. Select **Customize** from Launch and Activation Permissions.
8. Click **Edit**.
9. Highlight the user ID called Local Service.
10. Grant the Local Service user ID Local Launch and Local Activation permissions.

Importing the User IDs

Restriction

You must configure Cisco Unified MeetingPlace to use only Cisco Unified MeetingPlace authentication before you can enable Lotus Domino authentication because IBM Lotus Notes does not support other authentication methods, such as Windows Integrated Authentication (WIA). For information on authentication, see the *Configuration Guide for Cisco Unified MeetingPlace Release 7.1* or the online help in the administrator interface.

Before You Begin

You must have a user ID with administrator privileges to log in to the Lotus Domino Server.

Procedure

1. Log in to the Lotus Domino Server as an administrator.
2. Use one of the following methods to enter Cisco Unified MeetingPlace user IDs:
   - Import the Cisco Unified MeetingPlace user IDs.
   - Import the Lotus Domino address book ShortName field into the Cisco Unified MeetingPlace profile of each user as their user ID.
     Note: Although any Lotus Domino address book field can contain a Cisco Unified MeetingPlace user ID, we recommend using the ShortName field because it contains unique values, and has configurable security settings. If you decide to use another field that contains multiple values, make sure that the Cisco Unified MeetingPlace user ID is listed first. By default, Cisco Unified MeetingPlace uses the first value in the field for authentication.
3. Set the security option in the ShortName field to **Must Have at Least Editor Access to Use**. This prevents users from changing their user IDs and signing in to Cisco Unified MeetingPlace as someone else.

Related Topics

For information about how to import Cisco Unified MeetingPlace user IDs, see the "Raw Data Export and Import Specifications" topic in the *Configuration Guide for Cisco Unified MeetingPlace Release 7.1* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html.

Verifying the Import

Before You Begin

You must have a user ID with administrator privileges to log in to the Cisco Unified MeetingPlace Web Server.

Procedure

1. Log in to the Cisco Unified MeetingPlace Web Server.
2. Open the Gateways Configuration utility.
3. Click the **Notes Gateway** tab.
4. Verify that the authentication field contains the Cisco Unified MeetingPlace user IDs.
5. Close the Gateway Configuration utility.

Setting the Authentication Method

Before You Begin

You must have user IDs with administrator privileges to log in to the Lotus Domino Server, IBM Lotus Notes server, and Cisco Unified MeetingPlace Administration Center.

Procedure

1. Log in to the Lotus Domino Server as an administrator.
2. Open the MeetingPlace Server Agent Database.
3. Click **Use Domino Authentication**.
4. Click **Save**.
5. Click **Close**.
6. Open a web browser.
7. Connect to the Cisco Unified MeetingPlace Web Server by entering **http://*<hostname>***, where *<hostname>* is the hostname of the internal Web Server.
8. Click **Sign In**.
9. Enter an administrator username and password.
10. Click **Admin**.
11. Click **Web Server**.
12. From the Web Server Administration page, click the name of your server on the bottom half of the page. Server information populates the top half of the page.
13. Choose **Yes** in **Set Trust Web Server Authentication**.
14. Click **Web Server Name** in the View area.
15. Scroll to the Web Authentication area.

16. Choose **Web Page Form** in Step 2: Login Method.
17. Click **Submit**.
18. Exit Cisco Unified MeetingPlace.

Tip: After you synchronize the user IDs on Cisco Unified MeetingPlace and Lotus Domino, you can develop a process to ensure that all new users have a Cisco Unified MeetingPlace profile. By developing scripts and using the Cisco Unified MeetingPlace import capabilities, you can automate this process so that Lotus Domino and Cisco Unified MeetingPlace are synchronized. For information about how you can use scripts to update the Cisco Unified MeetingPlace database, contact Cisco Technical Support.

Copying IBM Lotus Notes Templates and Files to the Lotus Domino Server

The template and Java files are in *drive*:\Program Files\Cisco Systems\Cisco MeetingPlace for Notes\Files. You must copy these templates and files to the Lotus Domino Server data directory.

File	Description
MPSA.ntf	The MeetingPlace Server Agent Database. Use this file if you do *not* want to set up SSL support.
MPSA_SSL.ntf	The MeetingPlace Server Agent Database. Use this file if you *do* want to set up SSL support.
mail*xx*_*xx*MP.ntf	The Cisco Unified MeetingPlace mail template for the version of IBM Lotus Notes that you are using. For example, mail70_1MP.ntf corresponds to the 7.0.1 mail template.
jcert.jar jnet.jar jsse.jar	Additions to the Java setup for Lotus Domino. These files allow you to support SSL.

Before You Begin

- Log in to the Cisco Unified MeetingPlace Application Server as an administrator.
- Use ftp to connect to the Lotus Domino Server.
- Log in to the Lotus Domino Server with a user ID that has rwx privileges in the Lotus\Domino\Data directory.

Procedure

1. Copy the following files to your Lotus Domino Server:
   - If you do *not* want to set up SSL support, copy the MPSA.ntf and mail*xx_xx*MP.ntf files to the Lotus\Domino\Data directory on your Lotus Domino Server.
   - If you *do* want to set up SSL support, copy the MPSA_SSL.ntf and mail*xx_xx*MP.ntf files to the Lotus\Domino\Data directory on your Lotus Domino Server. Copy the three Java extension files (jcert.jar, jnet.jar, jsse.jar) to the Lotus\Domino\jvm\lib\ext directory on your Lotus Domino Server.
     Note: If any of the template files already reside on the Lotus Domino Server and you overwrite these files with new ones, exit and restart the Lotus Domino Server after copying the new template files. This prevents the Lotus Domino Server from mistakenly signing templates stored in its cache.
2. Enter **Exit** at the console command prompt.
3. Choose **Start > Programs > Lotus Applications > Domino Server** to restart the Lotus Domino Server.

Setting Up Database and Mail Templates for IBM Lotus Notes

- Granting Permission to Run Restricted and Unrestricted Agents on the Lotus Domino Server
- Signing the MeetingPlace Server Agent Template
- Signing the Cisco Unified MeetingPlace Mail Template

Granting Permission to Run Restricted and Unrestricted Agents on the Lotus Domino Server

Before You Begin

- Log in to the Lotus Domino Server as an administrator.
- Open Domino Administrator.
- Click your Domain tab (for example, CISCO_Domain).

Procedure

1. Click **Configuration**.
2. Expand the **Server** view.
3. Click **Current Server Document**.
4. Click **Security** in the right pane.
5. Double-click the page to bring it in to edit mode.
6. Scroll to the right until you see the Programmability Restrictions area.
7. In the Who Can column next to the following restrictions, add MeetingPlace to give yourself these permissions:
   - Run unrestricted methods and operations

- ♦ Run restricted LotusScript/Java agents

8. Click **Save & Close**.

Signing the MeetingPlace Server Agent Template

You must sign the MeetingPlace Server Agent template to verify that it is has permissions to run agents on the Lotus Domino Server.

Before You Begin

- Copy the MeetingPlace Server Agent template to the Lotus Domino Server. See Copying IBM Lotus Notes Templates and Files to the Lotus Domino Server.
- Log in to the Lotus Domino Server as an administrator.
- Open Domino Administrator.
- Click your Domain tab (for example, CISCO_Domain).

Procedure

1. Click **Files**.
2. Choose **Templates Only**.
3. Right-click the file name of the MeetingPlace Server Agent template (either MPSA.ntf or MPSA_SSL.ntf).
4. Choose **Sign**.
5. Click **All Design Documents**.
6. Click **OK**.

Signing the Cisco Unified MeetingPlace Mail Template

Before You Begin

- Copy the mail template to the Lotus Domino Server. See Copying IBM Lotus Notes Templates and Files to the Lotus Domino Server.
- Log in to the Lotus Domino Server as an administrator.
- Open Domino Administrator.
- Click your Domain tab (for example, CISCO_Domain).

Procedure

1. Click **Files**.
2. Choose **Templates Only**.
3. Right-click the file name of the Cisco Unified MeetingPlace mail template (such as mail65_5MP.ntf or mail70_2MP.ntf).
4. Choose **Sign**.
5. Click **OK**.

Note: To access the Cisco Unified MeetingPlace mail template from other Lotus Domino Servers, replicate the template file to those servers. See the Lotus Domino documentation for information about replicating files.

Expanding the Document Capacity of the Lotus Notes Account

Back-end notifications begin to fail if the Lotus Notes account for Cisco Unified MeetingPlace exceeds 5000 documents. This is caused by a default limitation on the Lotus Domino Server where it is unable to handle index files larger than 5000 documents.

Complete the following procedure to increase the capacity of the Lotus Domino Server to handle more than 5000 documents.

Procedure

1. Navigate to the Lotus Domino Server installation folder.
2. Open the file called **notes.ini**.
3. At the end of the file, add these two lines:
   - Temp_Index_Max_Doc=10000
   - FT_Max_Search_Results=10000
4. Restart the Lotus Domino Server.

Note: The values you choose to set for the Temp_Index_Max_Doc and FT_Max_Search_Results parameters (e.g., 10000) are based on your specific system requirements. These are not Cisco Unified MeetingPlace-specific parameters so there is no recommended value. For a complete explanation of the usage of these parameters, see http://www.ibm.com/developerworks/lotus/documentation/notes-ini/index.html.

Configuring SSL Support for IBM Lotus Notes

Secure Socket Layer (SSL) increases the security of your transmissions by enabling HTTPS encryption. For HTTPS encryption to function properly, you must configure both Lotus Domino and Cisco Unified MeetingPlace for SSL authentication. If you have a Lotus Domino cluster with multiple servers, repeat the

procedures in this section for each of the Lotus Domino servers in the cluster containing an MPSA database. See the *Configuration Guide for Cisco Unified MeetingPlace Release 7.1* or the online help in the administrator interface for information on configuring SSL support for Cisco Unified MeetingPlace.

- Installing the Sun SDK File
- Adding Certificates to the Lotus Domino Keystore
- Editing the java.policy File

Installing the Sun SDK File

The Sun SDK provides the keytool.exe tool which is used for importing certificates.

Before You Begin

- Log in to the Lotus Domino Server as an administrator.
- Copy the three .jar files onto your Lotus Domino Server. See Copying IBM Lotus Notes Templates and Files to the Lotus Domino Server.

Procedure

1. Open a web browser.
2. Navigate to http://java.sun.com/j2se/1.4.2/download.html.
3. Click **Download J2SE SDK**.
4. Select a platform.
5. Check **I agree to the Java 2 Software Development Kit (J2SDK) Standard Edition 1.4.2 License Agreement**.
6. Click **Continue**.
7. Choose a download file from the Windows Platform area.
8. Follow the prompts until the file is completely downloaded.

Adding Certificates to the Lotus Domino Keystore

After you obtain your certificates, use keytool.exe to add the certificates to the list of trusted certificates (your keystore) on your Lotus Domino Server. Your keystore is the cacerts file in the Lotus\Domino\jvm\lib\security directory of your Lotus Domino Server.

For more information about obtaining certificates, see the *Configuration Guide for Cisco Unified MeetingPlace Release 7.1* or the online help in the administrator interface.

Before You Begin

Log in to the Cisco Unified MeetingPlace Web Server as an administrator.

Procedure

1. Use FTP or a similar program to copy your **HOMEPAGE** certificate file from the Cisco Unified MeetingPlace Web Server to the Lotus Domino Server.
2. Log in to the Lotus Domino Server as an administrator.
3. Choose **Start > Run**.
4. Enter **cmd**.
5. Click **OK**.
6. Enter the following command, replacing values as indicated below:

   <*path*> \jre\bin\keytool -import -alias [*anyalias*] -file [*yourcertificate.cer*] -keystore [*cacerts*]

Replace	With
path	The path to your Java SDK files (for example, c:\j2sdk1.4.2_03)
anyalias	The alias that you are applying to the certificate (for example, WebHomePageCertificate). This is how your certificate will be listed in the keystore.
yourcertificate.cer	The path to your .cer file for the Home Page hostname (for example, c:\temp\webhomepage.cer)
cacerts	The path to the cacerts file on your Lotus Domino server (for example, c:\Lotus\Domino\jvm\lib\ security\cacerts). cacerts is the name of your keystore.

For example:

```
c:\j2sdk1.4.2_03\jre\bin\keytool -import -alias Ciscocertificate -file

c:\temp\newcertificate.cer -keystore
c:\Lotus\Domino\jvm\lib\security\cacerts
```

Note: Enter the default password, **changeit**, if your Lotus Domino cacerts file requires a password.

7. Enter **yes** at the IBM Lotus Notes client prompt.

8. Close the command-line interface.

Editing the java.policy File

The java.policy file contains permission to set the system properties.

Before You Begin

Log in to the Lotus Domino Server as an administrator.

Procedure

1. Navigate to *drive*:\Lotus\Domino\jvm\lib\security.
2. Double-click java.policy to open it in Notepad.
3. Add the following line to the end of the grant{} section just before the closing brace (};)
   permission java.util.PropertyPermission "java.protocol.handler.pkgs", "write";
4. Save and close the file.

About Load Balancing for IBM Lotus Notes with Cisco Unified MeetingPlace Release 7.1

There are no special considerations for load balancing when using IBM Lotus Notes with Cisco Unified MeetingPlace Release 7.1. For load balancing information, see About Load Balancing Options for the Web Server.