



Troubleshooting Access Issues for the Cisco Unified MeetingPlace Express System

This chapter contains the following topics:

- [Recovering the Password for the root User Account, page 1-1](#)
- [Recovering the Password for the mpadmin Account, page 1-2](#)
- [Recovering the System Administrator Password Used in the End-User Interface and the Administration Console, page 1-3](#)
- [Accessing the System after Uploading the Wrong SSL Certificate or Key, page 1-4](#)
- [Troubleshooting a Failed LDAP Log On Attempt, page 1-5](#)

After reviewing this chapter, if you still have problems with Cisco Unified MeetingPlace Express, contact Cisco TAC. See the *“Obtaining Technical Assistance”* [section on page vi](#) for information on contacting Cisco TAC.

Recovering the Password for the root User Account

If you forget the password that you created for the root user account while installing the Cisco Unified MeetingPlace Express system, follow these steps to reset it:

Procedure

- Step 1** Reboot your server.
- Step 2** During the reboot, there is a period when you have only three seconds to choose to update the server configuration so that you can reset the root password. When you see a screen with the word GRUB at the top and a text box with Cisco Unified Communications in it, quickly press the spacebar.



Caution You only have three seconds to press the spacebar once the system displays this screen.



Note Nowhere on this screen does it say anything about pressing the spacebar to reset the root password.

- Step 3** The system displays three options. Use the up and down arrow keys to highlight the third entry. It starts with “kernel.”
- Step 4** Press **e** to edit the entry.
- Step 5** At the end of the entry, enter a space and then **single**.



Note You must type a space before you type **single**.

- Step 6** Press **Enter** to return the previous screen. The third entry should have the word single at the end.
- Step 7** Press **b** to continue rebooting the server.
- Step 8** At the prompt, enter **/root/.security/unimmunize.sh**.
- Step 9** At the prompt, enter **passwd root**. This tells the server to set a new password for the user called root.
- Step 10** At the New password: prompt, enter a new password. For security purposes, the password is displayed as a series of asterisks.



Note You may see a message that the password you entered is bad. Ignore this message.

- Step 11** At the Retype new password: prompt, re-enter the same password again.
- Step 12** At the prompt, enter **/root/.security/immunize.sh**.
- Step 13** At the prompt, enter **reboot**. This reboots the server.
The Cisco Unified MeetingPlace Express operating system login page is displayed.
- Step 14** At the username prompt, enter **root**.
- Step 15** At the password prompt, enter the new password that you created in [Step 9](#).
The system should display the Cisco Unified MeetingPlace Express operating system desktop.
-

Recovering the Password for the mpxadmin Account



Note Follow this same procedure to *change* the mpxadmin account password, too.

If you forget the password that you created for the mpxadmin account while installing the Cisco Unified MeetingPlace Express system, follow these steps to reset it:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the **root** user.
- Step 2** At the password prompt, enter the root password. (If you have forgotten the root password, first follow the steps in the [“Recovering the Password for the root User Account”](#) section on page 1-1.)
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.

- Step 5** At the prompt, enter **/root/.security/unimmunize.sh**.
- Step 6** At the prompt, enter **passwd mpxadmin**. This tells the server to set a new password for the user called mpxadmin.
- Step 7** At the New password prompt, enter a new password. For security purposes, the password is displayed as a series of asterisks.



Note You may see a message that the password you entered is bad. Ignore this message.

- Step 8** At the Retype new password prompt, re-enter the same password again.
- Step 9** At the prompt, enter **/root/.security/immunize.sh**.
- Step 10** On the desktop, click **RedHat > Network Services**.
- Step 11** Click **Log out**.

Recovering the System Administrator Password Used in the End-User Interface and the Administration Console

If you forget the password that you created for the system administrator account, which is used in the End-User Interface and Administration Center, follow these steps to reset it:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
- Step 2** At the password prompt, enter the mpxadmin password. (If you have forgotten the mpxadmin password, first follow the steps in the [“Recovering the Password for the mpxadmin Account”](#) section on page 1-2.)
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
- Step 5** At the prompt, enter **userutil -p admin <newpassword>**, where **newpassword** is the new password. This tells the server to set a new password for the End-User Interface and Administration Center user called admin.
- Step 6** On the desktop, click **RedHat > Network Services**.
- Step 7** Click **Log out**.

Accessing the System after Uploading the Wrong SSL Certificate or Key

To have Secure Socket Layer (SSL) work with the Cisco Unified MeetingPlace Express application, you must upload SSL certificates and enable SSL. See the *Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2* for information about doing this.



Note

The SSL certificate that you upload must be in the PEM format. If your SSL certificate is in the DER format, convert it to the PEM format and upload it again. Use this CLI command to convert a certificate from DER to PEM:

```
openssl -in <file1.crt> -inform DER -out <file2.crt>
```

where *file1.crt* is the name of the DER file and *file2.crt* is the name of the PEM file.

However, if you enter the wrong certificate or private key name and enable SSL, you cannot access the Cisco Unified MeetingPlace Express application and you are locked out.

Follow these steps to access the application:

Procedure

- Step 1** Open a web browser and navigate to <http://<localhostname>:8080>, where **localhostname** is your local hostname.
The Cisco Unified MeetingPlace Express application opens.
- Step 2** Log in to Cisco Unified MeetingPlace Express.
- Step 3** At the top of the page, click **Administration**.
- Step 4** On the left side of the page:
 - a. Click **Certificate Management**.
 - b. Click **Disable SSL**.
- Step 5** Disable SSL by clicking **Disable SSL**.
- Step 6** Restart the Cisco Unified MeetingPlace Express system by clicking **Restart Now**.
This updates the web conferencing configuration files and after the system restarts you should be able to correctly access the Cisco Unified MeetingPlace Express application.
Open a web browser and navigate to <http://<localhostname>>, where **localhostname** is your local hostname.
- Step 7** Log in to Cisco Unified MeetingPlace Express.
- Step 8** At the top of the page, click **Administration**.
- Step 9** On the left side of the page:
 - a. Click **Certificate Management**.
 - b. Click **Enable SSL**.
- Step 10** Enter the correct certificate or private key names.
- Step 11** Click **Upload Certificates**.

- Step 12** The system displays a dialog box stating that this will restart the server and to only proceed if you are sure. Click **OK** to upload the certificates, update the configuration, and restart the server.
-

If your system still does not enable SSL, the system may have overwritten the private keys that were created on the system during the initial Certificate Signing Request (CSR) generation. (This can happen if you generated new CSRs.) In this situation, the recovery steps are as follows:

Procedure

- Step 1** Log in to Cisco Unified MeetingPlace Express.

- Step 2** At the top of the page, click **Administration**.

- Step 3** On the left side of the page:

- a. Click **Certificate Management**.
- b. Click **Generate CSRs**.

- Step 4** Enter information in the fields.

- Step 5** Click **Generate CSRs**.

The system generates new private keys and stores them in the /usr/local/enrollment directory.

- Step 6** Send the new CSRs to the CA so that they can reissue the SSL certificates.

- Step 7** After you receive the SSL certificates from the CA, go to the Enable SSL page and upload them.
-

Troubleshooting a Failed LDAP Log On Attempt

There are certain conditions in which users may have trouble logging in to Cisco Unified MeetingPlace Express:

- If a single user is having an issue and if that user is using Cisco Unified CallManager LDAP integration and if the user cannot log in to the Cisco Unified CallManager user page, reset the password for that user in Cisco Unified CallManager. If the user still cannot log in, follow the steps in the procedure below.
- If a single user is having an issue and is using a third-party LDAP integration (such as Active Directory) and if the user cannot log in to the LDAP domain, reset the password for that user in the third-party LDAP integration. If the user still cannot log in, follow the steps in the procedure below.
- If all users are affected, check the LDAP configuration settings on the Cisco Unified MeetingPlace Express Usage Configuration page (**Administration > System Configuration > Usage Configuration**). Ensure the following:
 - The value in the LDAP URL field is correct and contains no empty spaces.



Tip

To ensure that there are no empty spaces, delete the current entry and enter the LDAP value again.

- The entries for the Directory username and Password fields are correct. See the *Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2* for information about allowable values for each field.

Restart the Cisco Unified MeetingPlace Express server if you made any changes. If this does not correct the problem, follow the steps in the procedure below.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express as the user called admin.



Note For information on logging in to Cisco Unified MeetingPlace Express, see the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2*.

Step 2 Capture the system information by following these steps:

- In Cisco Unified MeetingPlace Express click **Administration** in the top menu bar.
- On the left, click **Services**, then **Logs**, then **View System Information Capture**.
- Enter the information into the form. In the Approximate event time field, enter a time that is about the time when you tried to log in using the LDAP mechanism.
- Enter 10 in the Log capture window field.
- Click **View Logs**.
- At the pop-up message, click **OK**.
- Save the file created by clicking **Export to File**.

Step 3 Forward the saved file to Cisco TAC.

If you are using Cisco Unified CallManager, remember the following:

- Ensure that you can log in to the Cisco Unified CallManager Data Connection Directory.

For example, in Cisco Unified CallManager go to **Programs > DC Directory Administration**. Log in as the Directory Manager with the password that you specified in the Password field on the Cisco Unified MeetingPlace Express Usage Configuration page (**Administration > System Configuration > Usage Configuration**).

- Ensure that the first time a user logs in to Cisco Unified MeetingPlace Express, he uses the End-User Interface.



Note When a user logs in for the first time, Cisco Unified MeetingPlace Express creates a profile for that user “on the fly.” A successful login (and the message *Welcome “User”*) means that the user’s profile was successfully created. If the user attempts to log in for the first time using the Telephone User Interface (TUI), the system will not create a profile.

- Ensure that the user profile is not locked in Cisco Unified CallManager. (User profiles become locked after too many failed attempts to log in.)
- Check the Cisco Unified MeetingPlace Express log in the following location:
/opt/cisco/meetingplace_express/tomcat/current/logs/bounty.out