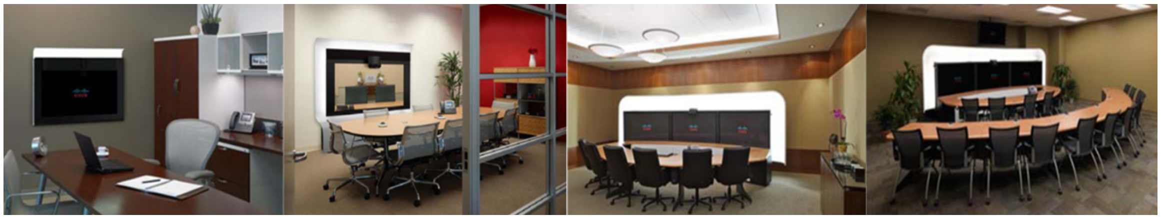


CHAPTER 12

Troubleshooting Cisco TelePresence System Passwords

Revised: March, 2011, OL-21351-01

Contents

This chapter contains information about troubleshooting the Cisco TelePresence System (CTS) and includes the following sections:

Troubleshooting CTS Passwords

This section contains the following information about managing and troubleshooting password issues with the Cisco TelePresence System (CTS):

- Resetting Your CTS Codec Password, page 12-1
- Restoring Connectivity to the Codec, page 12-3

Resetting Your CTS Codec Password

Note You must be in the Cisco TelePresence room to read the newly requested passcode that shows on the main display.

At each point where the pwrecovery account requires input, the program will wait up to 60 seconds. If nothing is entered, the system will inform you that the entry took too long and will exit.

If you encounter any difficulty, open a case with Technical Assistance Center (TAC) via the Internet at http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered about the problem.

Before You Begin

Make sure that the CTS is not in a call, and that there is only one instance of someone trying to reset the password, otherwise the session will abort.

Procedure

To reset your CTS codec password, follow these steps:

Step 1 SSH into the codec from your laptop.

Step 2 Login with the following:

- Username: **pwrecovery**
- Password: **pwreset**

The following message appears in the SSH client window:

Example 12-1 Welcome to Password Reset

```
dhcp-249:~ $ ssh pwrecovery@10.00.00.100
pwrecovery@10.00.00.100's password:

***********************************************
***********************************************
**                                           **
**     Welcome to password reset              **
**                                           **
***********************************************
***********************************************

Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:
```

Step 3 The system will ask whether you want to continue. Type **Y** then **return** to continue

Note If desired, type any other key then **return** to exit.

This system will now prepare for password reset and prompt you for a passcode. The new passcode is displayed on the CTS main display, as shown in the following example:

Password reset is now being run

Passcode: 919175

Note The passcode is a randomly generated number and will be different for each login attempt. If you enter the wrong passcode, the system will inform you that the passcode was incorrect and will exit, as shown in the following example. If this happens, repeat Step 1 and Step 2.

Example 12-2 Invalid Password Reset Request

```
Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:12345
Sorry that was an invalid passcode...
Logging off
Connection to 10.00.00.100 closed.
dhcp-249:~ $
```

When you enter the correct passcode, the CTS will then reset the administration account name and password to the system defaults. The following example shows successful password reset information:

Example 12-3 Successful Password Reset Request

```
Please enter the passcode:507530
resetting admin name and password
stopping any existing admin session
admin account and password reset to default
success in applying security rules
Logging off
Connection to 10.00.00.100 closed.
dhcp-249:~ $
```

Note If you are using the CTS with a Cisco Unified Communications Manager, the next time you perform a “Refresh” or “Reset” from the Cisco Unified CM, the administration account name and password will be reconfigured to the values specified in the Cisco Unified CM device page.

Restoring Connectivity to the Codec

If you lose connectivity to the codec, refer to the Cisco TelePresence System Assembly, Use & Care, and Field-Replaceable Unit Guide for your system on Cisco.com:

Support > **Products** > **TelePresence** > **Cisco TelePresence System**

Troubleshooting Cisco Unified CM Passwords

This section contains the following information about managing and troubleshooting password issues with Cisco Unified Communications Manager:

- Password Aging, page 12-4
- Password Notices, page 12-4
- Resetting Administrator and Security Passwords, page 12-6

Password Aging

To ensure that your system is protected when using Cisco TelePresence Command Line Interface (CLI), you must periodically update your password. The system alerts you to the number of days remaining on your current password in the login banner when you log onto the system. The system issues a warning when 14 days remain on your current password, and so on until the password expires. You may get a message similar to the following at login:

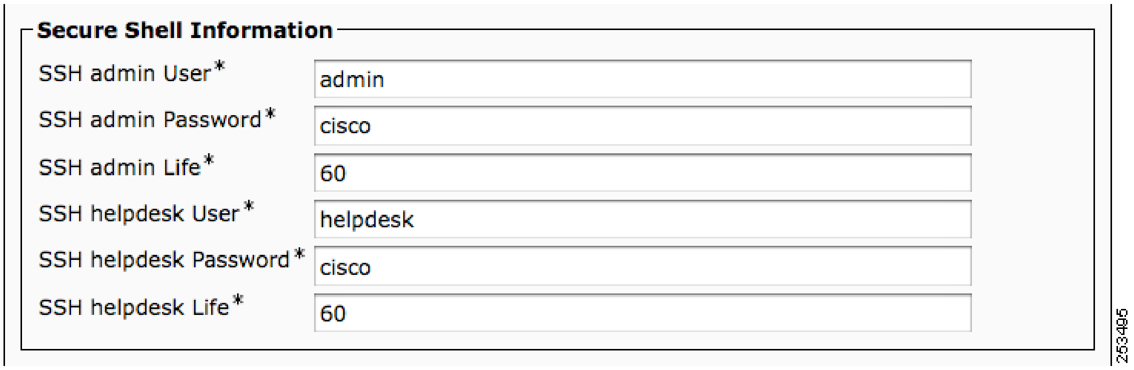
“Password change required in 10 days”

The password life (the maximum age, in days) can be configured using new fields on the Cisco Unified Communications Manager (Cisco Unified CM) **Device** > **Phone** > **Product Specific Configuration Layout** > **Secure Shell Information** page:

- SSH Admin Life
- SSH Helpdesk User
- SSH Helpdesk Password
- SSH Helpdesk Life

Figure 12-1 shows the Secure Shell (SSH) Information window.

Figure 12-1 SSH Information Window



Secure Shell Information

SSH admin User*	admin
SSH admin Password*	cisco
SSH admin Life*	60
SSH helpdesk User*	helpdesk
SSH helpdesk Password*	cisco
SSH helpdesk Life*	60

The password expiration can be set to have a value between 0 and 365. A setting of 0 disables password aging, and the default is 60 days. Unless the configured life has been disabled (by being set to 0), password age is set to have 2 days remaining in the following situations:

- New installations and factory resets.
- Software upgrades (if the password age is less than the configured age).
- Password recovery (using the **pwrecovery** command).

Password Notices

When the password age has expired, a warning message is shown briefly on-screen before logging out. Notice information is printed at login when there are 14 days or less remaining on the current password.

When you log in, you will receive one of three banners:

Example 12-4 7 to 14-Day Warning

If your password is about to expire within 7 to 14 days, you will see a message similar to the following:

```
customer@mypc #1000:ssh admin@108.100.000.25
admin@108.100.000.25's password:
Command Line Interface is starting up, please wait ...

Welcome to the TelePresence Command Line Interface (version 1.1)

Last login: Wed Dec 9 22:22:58 PST 2009 from philly.cisco.com
Password change required in 10 days

admin:
```

Example 12-5 0 to 7-Day Warning

If your password is about to expire within 0 to 7 days, you will see a message similar to the following:

```
customer@mypc #1000:ssh admin@108.100.000.25
admin@108.100.000.25's password:
Command Line Interface is starting up, please wait ...

****** Warning ******
You must change your admin password in the next 2 days
****** Warning ******

Welcome to the TelePresence Command Line Interface (version 1.1)
Last login: Fri Nov 13 13:12:42 PST 2009 from mypc.cisco.com
Password change required in 2 days

admin:
```

Example 12-6 0 Days Remaining

If your password is expiring with 0 days remaining on the current password, the following banner is shown. The session waits for 10 seconds then disconnects.

```
customer@mypc #1000:ssh admin@108.100.000.25
admin@108.100.000.25's password:
Command Line Interface is starting up, please wait ...

****** Warning ******

You have not changed your admin password in more than 60 days
The admin account login has been disabled

*******************************************************
* *
* Please go to the CUCM and change the password *
* *
*******************************************************

****** Warning ******

Connection to 108.100.000.25 closed.
```

For more information see the *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System.* See also the *Cisco TelePresence System Command-Line Interface Reference Guide*.

Resetting Administrator and Security Passwords

If you lose the administrator password or security password, use the following procedure to reset these passwords in Cisco Unified CM.

To perform the password reset process, you must be connected to the system through the system console, that is, you must have a keyboard and monitor connected to the server. You cannot reset a password when connected to the system through a secure shell session.

Caution The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Caution You must reset each server in a cluster after you change its security password. Failure to reboot the servers (nodes) causes system service problems and problems with the Cisco Unified Communications Manager Administration windows on the subscriber servers.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: **pwrecovery**
- Password: **pwreset**

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

Note For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.

Troubleshooting CTS-Manager Passwords

This section contains the following information about managing and troubleshooting password issues with CTS-Manager:

- Resetting Your CTS-Manager Password, page 12-7

Resetting Your CTS-Manager Password

Use the information in this section to change the password for Cisco TelePresence Manager.

Before You Begin

Follow these guidelines to reset your CTS-Manager password:

- You must know the current password to access CTS-Manager and use the password fields.
- Use only English; International words or characters are not supported in this release.
- The password cannot be changed until at least 24 hours after it was created, unless you reinstall CTS-Manager.

Procedure

Step 1 Log in to CTS-Manager.

Step 2 Choose **Configure** > **System Settings** > **Password**.

Step 3 Click the **Password** tab to display the password fields.

Step 4 Enter your current password.

Step 5 Go to the **New Password** field and enter your new password, using only English characters.

Note The password should contain both upper and lower-case alphabetic and non-alphabetic characters. It should not be similar to the current password or be based on common words found in the dictionary.

Step 6 Re-enter your new password in the **New Password (verify)** field to verify it.

Step 7 To register the new password, click **Apply**.

Step 8 To restore the original password, click **Reset**.

Troubleshooting CTMS Passwords

This section contains the following information about managing and troubleshooting password issues with the Cisco TelePresence MultiPoint Switch:

- Managing CTMS Passwords, page 12-8

Managing CTMS Passwords

CTMS administration access management software recognizes three administrative roles:

- Administrator—Administrators have the authority to perform all tasks associated with CTMS, including configuring settings; managing multipoint meetings; and maintaining, monitoring, and troubleshooting CTMS.
- Meeting Scheduler—Meeting Schedulers have the authority to perform multipoint meeting management tasks, such as defining meeting templates and setting up (and breaking down, as necessary) ad hoc, static, and scheduled meetings.
- Diagnostic Technician—Diagnostic Technicians have the authority to perform CTMS monitoring and troubleshooting tasks.

Access to certain tasks and information is dependent the administrative role.

To configure or edit Access Management settings:

Step 1 Log in to the CTMS using your current access information.

Step 2 In the left navigation area, choose **Configure** > **Access Management**. The Access Management page appears displaying a table providing information about previously defined users.

Step 3 Choose one of the following actions to manage current settings:

- To delete a user, click the radio button to the left of the entry. Then click **Delete**.
- To edit a user, click the radio button to the left of the entry. Then click **Edit**.
- To define a new user, click **New**,

Step 4 When you click **New** from the Access Management page, the Access Management dialog box to create a new user appears.

Step 5 Enter settings as described in Table 12-1.

Table 12-1 New User Settings

Field or Button	Setting
User Name	Username of the new user. **Note** Usernames must be at least 5 characters, but not more than 64 characters in length, and can contain upper- and lowercase alphanumeric characters. The username must contain letters and numbers, but it cannot contain special characters except for the underscore character. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.
Password	Password for the username indicated in the Username field. **Note** Passwords must be at least 5 characters, but no more than 64 characters. Passwords must contain numbers and uppercase and lowercase letters. They can also contain special characters, such as the asterisk (*) or the hyphen (-). **Note** When you change the Administrator role password for the first time after software installation, the new password cannot be similar to password that was configured during installation.
Verify Password	Re-enter the password defined for this user.
Role	Defines a specific user role. There are three possible roles, each with specific levels of administrative access: • Administrator: Administrators have access to all pages and configuration tasks. • Conference Scheduler (Meeting Scheduler): Conference schedulers have access only to the Manage pages and associated configuration tasks. • Diagnostic Technician: Diagnostic technicians have access only to Troubleshoot pages and one task (system restart). **Note** A single user can have more than one role. Click the appropriate checkboxes to select.

Step 6 To register new or modified settings, click **Apply**.

Step 7 To edit an existing user profile, click the radio button to the left of the table entry to select the user, and then click **Edit**. CTMS Administration software takes you to the Edit User Settings table.

Step 8 Enter settings (as needed) as described in Table 12-2.

Table 12-2 Edit User Settings

Field or Button	Setting
Username	View only. Username of the CTMS user.
Current password	Current password for the CTMS user.

Table 12-2 Edit User Settings

Field or Button	Setting
New Password	New password for the CTMS user. **Note** Passwords must be at least 5 characters, but no more than 64 characters. Passwords must contain numbers and uppercase and lowercase letters. They can also contain special characters, such as the asterisk (*) or the hyphen (-). **Note** When you change the Administrator role password for the first time after software installation, the new password cannot be similar to password that was configured during installation.
Verify New Password	Re-enter the password defined for this user.

Step 9 To register new settings, click **Save**.

Additional Password Management Information

Use the information in this section to manage associated system passwords:

- Resetting Your MXE Root Password, page 12-10

Resetting Your MXE Root Password

Use the information in this section to change your MXE root password.

Before You Begin

You must have physical and console access to the MXE system.

Procedure

To change your MXE root password, follow these steps:

Step 1 Power cycle the MXE system.

Step 2 Press any key to stop at the Calistoga=> prompt before Linux boots.

Step 3 Boot Linux in single user mode. For example:

```
Calistoga=>set env othbootargs ‘init=/bin/bash’ boot
```

Step 4 Wait for the # prompt and enter the **psswd** command to set the new password. For example:

```
rm -rf /PSS/*
```

Step 5 Power cycle the system again to start from setup.

For more information about the MXE, see the Cisco MXE 5000 Series (Media Experience Engines) home page on Cisco.com.

Related Information

For more information about setting up, testing, and troubleshooting the CTS, see the following documentation on Cisco.com:

- *Cisco TelePresence System Administration Guide*
- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.
- *Cisco TelePresence System Command-Line Interface Reference Guide*.
- Cisco TelePresence Administration Software Error and System Messages