Troubleshooting Security Configuration on the Cisco TelePresence System

Revised: November 2014, OL-18391-01

Contents

This chapter describes how to troubleshoot security configuration on the Cisco TelePresence System and includes the following sections:

Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch

The Cisco TelePresence Multipoint Switch (CTMS) generates log messages when it detects any of the following security configuration problems:

- Security negotiation between Cisco TelePresence elements could not be established or completed.
- Some elements of Cisco TelePresence are secure, while others are non-secure (this condition is known as a *security mismatch*).

To view the CTMS logs for security configuration, log in to the CTMS administration interface, choose **Troubleshooting > Log Files**, and view files with the file type of .properties.

Table 6-1 contains system messages that you might encounter after setting up Cisco TelePresence security.

Table 6-1 Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch

Message Type	Possible Cause	Solution
Log Message `Call in state=Connected, call id=x, conference id = xxxxxxxxxx received error from Confmgr with error='security mismatch' during verification of security policy. Num=xxxxx`	A non-secure Cisco TelePresence endpoint attempted to join a secure meeting.	Make sure that all Cisco TelePresence endpoints are secure before they join a secure meeting.
Log Message `The security property of conference xxxxxxxxxx does not allow endpoint xxxxx to join`	One of the Cisco TelePresence endpoints is not running a Cisco TelePresence System software that is release 1.5 or higher. Cisco TelePresence treats the endpoint as a non-secure, even if this endpoint is configured as secure.	Make sure that all endpoints are running Cisco TelePresence System software with a minimum version of 1.5.
Log Message `Conference Manager Conf Id xxxxxxxxxx: will downgrade security from secure to non-secure. All existing endpoints will be downgraded to non-secure.`	A non-secure Cisco TelePresence endpoint, an audio-only call that is added in, or an endpoint that is running Cisco TelePresence System software that is release 1.5 or lower has joined a Best-Effort meeting after a meeting has been started as secure.	No action is required, but be aware that the best-effort meeting is now non-secure.
Log Message `Conf Id xxxxxxxxxx: will start as non-secure`	A non-secure Cisco TelePresence endpoint started a Best-Effort meeting.	No action is required, but be aware that the best-effort meeting is now non-secure.
Log Message `Could not connect to Cisco Unified CM`	The secure port numbers that are used by either CTMS, Cisco TelePresence Manager or the Cisco TelePresence system software do not match the port number for Cisco Unified CM.	Check the port numbers between the Cisco TelePresence elements to make sure that they match.
Log Message `Dialing xxxxx received 403 Forbidden from Cisco Unified CM. Check SIP trunk config.`	The Subject Names for the LSCs do not match.	Check the Subject Name that you created in the "Downloading LSCs onto an Infrastructure Device" section on page 3-5 and make sure that is matches the Subject name in the "Configuring a CTMS or a CTRS for SIP Security" section on page 3-12
Log Message `Dialing xxxxx received 488 Not Acceptable Here from Cisco Unified CM. Check SIP trunk config`	The **SRTP Allowed** check box is not selected in the Cisco Unified CM configuration.	Follow the instructions in the "Configuring an Existing Trunk for SIP Security" section on page 3-10 and make sure that you check the **SRTP Allowed** check box.
Log Message `TLS error: Error loading Private key file`	The key file is from a different CTMS or Cisco Unified CM than the one that is being configured.	Make sure that the CTMS.key file being used is from the CTMS or Cisco Unified CM that is being configured.

Table 6-1 Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch (continued)

Message Type	Possible Cause	Solution
Log Message `TLS error: TLS connect failed because client side post-connection verification failed` `TLS error: TLS: didn't find matching cert`	The certificates from Cisco Unified CM are not valid.	Download new certificates by following the procedure in the "Downloading Certificates from Cisco Unified CM" section on page 1-9, then upload those certificates to CTMS by following the procedure in the "Installing Downloaded Security Certificates to an Infrastructure Device" section on page 3-3.
Log Message `Media Timeout occurred for call : called num = 13105`	Multiplexer negotiation has failed. One possible cause of this failure is that CTMS did not received an ACK message from the Cisco TelePresence System.	Recheck your security settings and the procedures you followed in Chapter 3, "Configuring Inter-device Security for the Cisco TelePresence Infrastructure Devices."
Log Message *`SPIMAP timeout, Dropping the call`*	An ACK message for Group Security Parameters (GSPs) was not received by CTMS. The Cisco TelePresence System will either end the meeting or downgrade the meeting to non-secure.	Recheck your security settings and the procedures you followed in Chapter 3, "Configuring Inter-device Security for the Cisco TelePresence Infrastructure Devices."
Log Message "`606 Not acceptable`" message in the system log.	The most likely cause of this error is that your system uses Cisco Unified CM Cisco Unified CM release 6.1.x, but you selected **Encrypted with SDP keys** in the CTMS setup.	Check your Cisco Unified CM release. If your system is running Cisco Unified CM release 6.1.x, complete the steps in the "Creating and Configuring a New Trunk for SIP Security" section on page 3-11, and in the "Configuring a CTMS or a CTRS for SIP Security" section on page 3-12, select **Encrypted without SDP keys**.

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.