



Troubleshooting

This chapter provides information about security-related measurements and general guidelines for troubleshooting security-related problems. This chapter contains information on the following topics:

- [Using the CLI, page 16-2](#)
- [Using Alarms, page 16-2](#)
- [Using Performance Monitor Counters, page 16-2](#)
- [Reviewing Log and Trace Files, page 16-4](#)
- [Backing Up and Restoring Security Files, page 16-4](#)
- [Troubleshooting Certificates, page 16-4](#)
- [Troubleshooting CTL Security Tokens, page 16-4](#)
- [Troubleshooting CAPF, page 16-5](#)
- [Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways, page 16-7](#)
- [Where to Find More Information, page 16-8](#)

For detailed information about Cisco Unified CallManager alarms, performance monitors, logs, and traces or error messages and corrective actions, refer to the following documents (or use the online help):

- For more information about alarms at the GUI and performance monitors in Cisco Unified CallManager Real Time Monitoring Tool, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.
- For more information about error messages, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.
- For more information about viewing logs and traces in Cisco Unified CallManager Real Time Monitoring Tool, refer to the *Cisco Unified CallManager Serviceability System Guide*.
- For more information about using or configuring packet capturing and about analyzing captured packets, refer to the *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(2)*.
- For troubleshooting instructions and corrective actions, refer to the *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(2)*.



Note

This chapter does not describe how to reset the Cisco Unified IP Phone if it has been corrupted by bad loads, security bugs, and so on. For information on resetting the phone, refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* that matches the model of the phone.

For information about how to delete the CTL file from Cisco Unified IP Phone models 7970, 7960, and 7940 only, see [Table 3-3](#) or the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* that matches the model of the phone.

Using the CLI

The command line interface (CLI) gives administrators access to system functions for troubleshooting purposes if a problem occurs when using the Cisco Unified Communications Platform Administration GUI.

You must have SSH access and a login ID and password to use the CLI interface. For information about using the CLI to view logs, traces, and performance monitors, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Using Alarms

Cisco Unified CallManager Serviceability generates security-related alarms for X.509 name mismatches, authentication errors, and encryption errors. The Serviceability GUI provides the alarm definitions.

Alarms may get generated on the phone for TFTP server and CTL file errors. For alarms that get generated on the phone, refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* for your phone model and type (SCCP or SIP) and to the [“Deleting the CTL File on the Cisco Unified IP Phone”](#) section on page 3-14.

Using Performance Monitor Counters

Performance monitor counters monitor the number of authenticated phones that register with Cisco Unified CallManager, the number of authenticated calls that are completed, and the number of authenticated calls that are active at any time. [Table 16-1](#) lists the performance counters that apply to security features.

Table 16-1 Security Performance Counters

Object	Counters
Cisco Unified CallManager	AuthenticatedCallsActive AuthenticatedCallsCompleted AuthenticatedPartiallyRegisteredPhone AuthenticatedRegisteredPhones EncryptedCallsActive EncryptedCallsCompleted EncryptedPartiallyRegisteredPhone EncryptedRegisteredPhones CMSIPLineServerAuthChallenges CMSIPLineServerAuthFailures CMSIPTrunkServerAuthChallenges CMSIPTrunkServerAuthFailures CMSIPTrunkClientAuthResponses CMSIPTrunkClientAuthRejects CMSIPPresenceAuthorizations CMSIPPresenceAuthorizationsFailure CMSIPTrunkMethodAuthorization CMSIPTrunkMethodAuthorizationFailure TLSConnectedSIPTrunk
SIP Stack	StatusCodes4xxIns (for example, 405 Method Not Allowed) StatusCodes4xxOuts (for example, 405 Method Not Allowed)
TFTP Server	BuildSigCount EncryptCount

Refer to the *CallManager Serviceability System Guide* for accessing performance monitors in RTMT, configuring perfmon logs, and for more details about counters.

The CLI command **show perf** displays performance monitoring information. For information about using the CLI interface, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Reviewing Log and Trace Files

Before you contact the team that provides technical assistance for this product, for example, your Cisco Partner or the Cisco Technical Assistance Center (TAC), review the log and trace files for the node in the Cisco Unified CallManager Real Time Monitoring Tool.

The administrator can download log and trace files from the server by using the trace collection feature in the Cisco Unified CallManager Real Time Monitoring Tool. After collecting the files, you can view them in the appropriate viewer within Cisco Unified CallManager Real Time Monitoring Tool.

**Note**

For devices that support encryption, the SRTP keying material does not display in the trace file.

For information about using the trace collection tool and using filtering to review log file records, refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide*.

Cisco Unified CallManager stores log and trace files in multiple directories (cm/log, cm/trace, tomcat/logs, tomcat/logs/security, and so on). CLI commands for **activelog** and **inactivelog** allow you to find, view, and manipulate log and trace files.

For more information about using the CLI interface, refer to the *Cisco Unified Communications Operating System Administration Guide*.

**Tip**

If you do not know the directory and filename for the log or trace file, contact TAC for further assistance.

Backing Up and Restoring Security Files

Refer to the *Cisco IP Telephone Disaster Recovery Framework Administration Guide* for backup and restore procedures for security files, such as CAPF data.

Troubleshooting Certificates

The certificate management tool in Cisco Unified Communications Platform Administration allows you to display certificates, delete and regenerate certificates, monitor certificate expirations, and download and upload certificates and CTL files (for example, to upload updated CTL files to Unity). The CLI allows you to list and view self-signed and trusted certificates and to regenerate self-signed certificates.

The CLI commands **show cert**, **show web-security**, **set cert regen**, and **set web-security** allow you to manage certificates at the CLI interface; for example, **set cert regen tomcat**. For information about how to use the GUI or CLI to manage certificates, refer to *Cisco Unified Communications Operating System Administration Guide*.

Troubleshooting CTL Security Tokens

The section contains information on the following topics:

- [Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password](#), page 16-5

- [Troubleshooting If You Lose One Security Token \(Etoken\), page 16-5](#)

If you lose all security tokens (etokens), contact Cisco TAC for further assistance.

Troubleshooting a Locked Security Token After You Consecutively Enter an Incorrect Security Token Password

Each security token contains a retry counter, which specifies the number of consecutive attempts to log in to the etoken Password window. The retry counter value for the security token equals 15. If the number of consecutive attempts exceeds the counter value, that is, 16 unsuccessful consecutive attempts occur, a message indicates that the security token is locked and unusable. You cannot re-enable a locked security token.

Obtain additional security token(s) and configure the CTL file, as described in [“Configuring the Cisco CTL Client” section on page 3-7](#). If necessary, purchase new security token(s) to configure the file.



Tip

After you successfully enter the password, the counter resets to zero.

Troubleshooting If You Lose One Security Token (Etoken)

If you lose one security token, perform the following procedure:

Procedure

-
- Step 1** Purchase a new security token.
- Step 2** Using a token that signed the CTL file, update the CTL file by performing the following tasks:
- a. Add the new token to the CTL file.
 - b. Delete the lost token from the CTL file.
- For more information on how to perform these tasks, see the [“Updating the CTL File” section on page 3-9](#).
- Step 3** Reset all phones, as described in [“Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster” section on page 1-10](#).
-

Troubleshooting CAPF

This section contains information on the following topics:

- [Troubleshooting the Authentication String on the Phone, page 16-6](#)
- [Troubleshooting If the Locally Significant Certificate Validation Fails, page 16-6](#)
- [Verifying That the CAPF Certificate Installed on All Servers in the Cluster, page 16-6](#)
- [Verifying That a Locally Significant Certificate Exists on the Phone, page 16-6](#)
- [Verifying That a Manufacture-Installed Certificate \(MIC\) Exists in the Phone, page 16-7](#)

Troubleshooting the Authentication String on the Phone

If you incorrectly enter the authentication string on the phone, a message displays on the phone. Enter the correct authentication string on the phone.



Tip

Verify that the phone is registered to the Cisco Unified CallManager. If the phone is not registered to the Cisco Unified CallManager, you cannot enter the authentication string on the phone.

Verify that the device security mode for the phone equals nonsecure.

Verify authentication mode in the security profile that is applied to the phone is set to By Authentication String.

CAPF limits the number of consecutive attempts in which you can enter the authentication string on the phone. If you have not entered the correct authentication string after 10 attempts, wait at least 10 minutes before you attempt to enter the correct string again.

Troubleshooting If the Locally Significant Certificate Validation Fails

On the phone, the locally significant certificate validation may fail if the certificate is not the version that CAPF issued, the certificate has expired, the CAPF certificate does not exist on all servers in the cluster, the CAPF certificate does not exist in the CAPF directory, the phone is not registered to Cisco Unified CallManager, and so on. If the locally significant certificate validation fails, review the SDL trace files and the CAPF trace files for errors.

Verifying That the CAPF Certificate Installed on All Servers in the Cluster

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific for CAPF. The CAPF certificate, which the Cisco CTL client copies to all servers in the cluster, uses the .0 extension. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications platform GUI or use the CLI:

- In DER encoded format—CAPF.cer
- In PEM encoded format—.0 extension file that contains the same common name string as the CAPF.cer

Verifying That a Locally Significant Certificate Exists on the Phone

You can verify that the locally significant certificate is installed on the phone at the Model Information or Security Configuration phone menus and by viewing the LSC setting. Refer to the *Cisco Unified IP Phone Administration Guide* for your phone model and type (SCCP or SIP) for additional information.

Verifying That a Manufacture-Installed Certificate (MIC) Exists in the Phone

You can verify that a MIC exists in the phone at the Model Information or Security Configuration phone menus and by viewing the MIC setting. Refer to the *Cisco Unified IP Phone Administration Guide* for your phone model and type (SCCP or SIP) for additional information.

Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways

This section contains information on the following topics:

- [Using Packet Capturing, page 16-7](#)
- [Configuring BAT for Phone Packet Capturing, page 16-7](#)

Using Packet Capturing

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable SRTP encryption, you must use Cisco Unified CallManager Administration to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Cisco Unified CallManager and the device (Cisco Unified IP Phone, Cisco SIP IP Phone, Cisco IOS MGCP gateway, H.323 gateway, or H.323/H.245/H.225 trunk).



Note

SIP trunks do not support SRTP.

- Capture the SRTP packets between the devices.
- Extract the media encryption key material from messages and decrypt the media between the devices.

For information about using or configuring packet capturing and about analyzing captured packets for SRTP-encrypted calls (and for all other call types), refer to the *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(2)*.



Tip

Performing this task for several devices at the same time may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

Configuring BAT for Phone Packet Capturing

By using the Bulk Administration Tool that is compatible with this Cisco Unified CallManager release, you can configure the packet capture mode for phones. For information about how to perform this task, refer to the *Cisco Unified CallManager Bulk Administration Guide*.

**Tip**

Performing this task in Cisco Unified CallManager Bulk Administration may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

Where to Find More Information

Related Topics

- [Interactions and Restrictions, page 1-5](#)
- [Certificate Types, page 1-12](#)
- [Configuring Media Encryption with Barge, page 1-11](#)
- [Using the CLI, page 16-2](#)
- [Using Alarms, page 16-2](#)
- [Using Performance Monitor Counters, page 16-2](#)
- [Reviewing Log and Trace Files, page 16-4](#)
- [Backing Up and Restoring Security Files, page 16-4](#)
- [Troubleshooting Certificates, page 16-4](#)
- [Troubleshooting CTL Security Tokens, page 16-4](#)
- [Troubleshooting CAPF, page 16-5](#)
- [Troubleshooting Encryption for Phones and Cisco IOS MGCP Gateways, page 16-7](#)

Related Cisco Documentation

- *Cisco IP Telephony Disaster Recovery Administration Guide*
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(2)*
- *Cisco Unified Communications Operating System Administration Guide*
- Cisco Unified IP Phone administration guide for the phone model and protocol