Cisco Unified CallManager System Issues

Updated7-3-2007

This section covers solutions for the following most common issues that relates to a Cisco Unified CallManager system.

Cisco Unified CallManager System Not Responding

This section covers the following issues for a Cisco Unified CallManager system that is not responding:

Cisco Unified CallManager System Stops Responding

Symptom

The Cisco Unified CallManager system does not respond.

When the Cisco CallManager service crashes, the following message displays in the System Event log:

```
The Cisco CallManager service terminated unexpectedly.
It has done this 1 time. The following corrective action
will be taken in 60000 ms. Restart the service.
```

Other messages you may see in the event of a crash follow:

```
Timeout 3000 milliseconds waiting for
Cisco CallManager service to connect.
```

The Cisco CallManager failed to start due to the following error:

```
The service did not respond to the start or control request in a timely fashion.
```

At this time, when devices such as the Cisco Unified IP Phones and gateways unregister from the Cisco Unified CallManager, users receive delayed dial tone, and/or the Cisco Unified CallManager server freezes due to high CPU usage. For event log messages that are not included here, view the Cisco Unified CallManager Event Logs.

Possible Cause

The Cisco CallManager service can crash because the service does not have enough resources such as CPU or memory to function. Generally, the CPU utilization in the server is 100 percent at that time.

Recommended Action

Depending on what type of crash you experience, you will need to gather different data that will help determine the root cause of the crash.

Use the following procedure if a lack of resources crash occurs.

Procedure

Step 1 Collect Cisco CallManager traces 15 minutes before and after the crash.

Step 2 Collect SDL traces 15 minutes before and after the crash.

Step 3 Collect perfmon traces if available.

Step 4 If the traces are not available, start collecting the perfmon traces and track memory and CPU usage for each process that is running on the server. These will help in the event of another lack of resources crash.

Cisco Unified CallManager Administration Does Not Display

Symptom

Cisco Unified CallManager Administration does not display.

Possible Cause

The Cisco CallManager service stopped.

Recommended Action

Verify that the Cisco CallManager service is active and running on the server, as described in "Verify Cisco Unified CallManager Services Are Running" section on page 2-21 or in the *Cisco Unified CallManager Serviceability Administration Guide*.

Error When Attempting to Access Cisco Unified CallManager Administration

Symptom

One of the following messages displays when you are trying to access Cisco Unified CallManager Administration.

- Internet Explorer—The page cannot be displayed.
- Netscape—Warning box displays: There was no response. The server could be down or is not responding.

Possible Cause

The services did not start automatically as expected. One of the services stopping represents the most frequent reason for Cisco Unified CallManager Administration not displaying.

Recommended Action

Try starting the other services.

Error When Attempting to Access Cisco Unified CallManager Administration on a Subsequent Node

Symptom

One of the following error messages displays when you are trying to access the Cisco Unified CallManager Administration.

Possible Cause

If the IP address of the first Cisco Unified CallManager node gets changed while a subsequent node is offline, you may not be able to log in to Cisco Unified CallManager Administration on the subsequent node.

Recommended Action

If this occurs, follow the procedure for changing the IP address on a subsequent Cisco Unified CallManager node in the *Cisco Unified Communications Operating System Administration Guide*.

You Are Not Authorized to View

Symptom

When accessing the Cisco Unified CallManager Administration, one of the following messages displays.

- You Are Not Authorized to View This Page
- You do not have permission to view this directory or page using the credentials you supplied.
- Server Application Error. The server has encountered an error while loading an application during the processing of your request. Please refer to the event log for more detailed information. Please contact the server administrator for assistance.
- Error: Access is Denied.

Possible Cause

Unknown

Recommended Action

Contact TAC for further assistance.

Problems Displaying or Adding Users with Cisco Unified CallManager

Symptom

You cannot add a user or conduct a search in Cisco Unified CallManager Administration.

Possible Cause

You may encounter the following problems if you are working with Cisco Unified CallManager that is installed on a server that has a special character (such as an underscore) in its hostname or Microsoft Internet Explorer 5.5 with SP2 and a Q313675 patch or above.

- When you conduct a basic search and hit submit, the same page redisplays.
- When you try to insert a new user, the following message displays.

```
The following error occurred while trying to execute the command.
Sorry, your session object has timed out.
Click here to Begin a New Search
```

Recommended Action

You may not be able to add a user or do a search on Cisco Unified CallManager Administration, if your Cisco Unified CallManager hostname contains any special characters such as underscore or period (for example, Call_Manager). Domain Name System (DNS)-supported characters include all letters (A-Z, a-z), numbers (0-9), and hyphen (-); any special characters are not allowed. If the Q313675 patch is installed on your browser, make sure that the URL does not contain any non-DNS supported characters.

For more information about the Q313675 patch, refer to MS01-058: File Vulnerability Patch for Internet Explorer 5.5 and Internet Explorer 6.

To resolve this problem, you have the following options:

- Access Cisco Unified CallManager Administration by using the IP address of the server.
- Do not use non-DNS characters in the Server Name.
- Use the localhost or IP address in the URL.

Name to Address Resolution Failing

Symptom

One of the following messages displays when you try to access the following URL:

http://your-cm-server-name/ccmadmin

- Internet Explorer—This page cannot be displayed
- Netscape—Not Found. The requested URL /ccmadmin was not found on this server.

If you try to access the same URL by using the Cisco CallManager IP address (http://10.48.23.2/ccmadmin) instead of the name, the window displays.

Possible Cause

The name that you entered as "your-cm-server-name" maps to the wrong IP address in DNS or hosts file.

Recommended Action

If you have configured the use of DNS, check in the DNS to see whether the entry for the *your-cm-server-name* has the correct IP address of the Cisco Unified CallManager server. If it is not correct, change it.

If you are not using DNS, your local machine will check in the "hosts" file to see whether an entry exists for the *your-cm-server-name* and an IP address that is associated to it. Open the file and add the Cisco Unified CallManager server name and the IP address. You can find the "hosts" file at **C:\WINNT\system32\drivers\etc\hosts**.

Port 80 Blocked Between Your Browser and the Cisco Unified CallManager Server

Symptom

One of the following messages displays when a firewall blocks the port that is used by the web server or the http traffic:

- Internet Explorer—This page cannot be displayed
- Netscape—There was no response. The server could be down or is not responding

Possible Cause

For security reasons, the system blocked the http access from your local network to the server network.

Recommended Action

1. Verify whether other types of traffic to the Cisco Unified CallManager server, such as ping or Telnet, are allowed. If any are successful, it will show that http access to the Cisco Unified CallManager web server has been blocked from your remote network.
2. Check the security policies with your network administrator.
3. Try again from the same network where the server is located.

Improper Network Setting Exists in the Remote Machine

Symptom

No connectivity exists, or no connectivity exists to other devices in the same network as the Cisco Unified CallManager.

When you attempt the same action from other remote machines, Cisco Unified CallManager Administration displays.

Possible Cause

Improper network configuration settings on a station or on the default gateway can cause a web page not to display because partial or no connectivity to that network exists.

Recommended Action

1. Try pinging the IP address of the Cisco Unified CallManager server and other devices to confirm that you cannot connect.
2. If the connectivity to any other device out of your local network is failing, check the network setting on your station, as well as the cable and connector integrity. Refer to the appropriate hardware documentation for detailed information.

   If you are using TCP-IP over a LAN to connect, continue with the following steps to verify the network settings on the remote station.
3. Choose **Start > Setting > Network and Dial-up connections**.
4. Choose **Local Area Connection**, then **Properties**.

   The list of communication protocols displays as checked.
5. Choose **Internet Protocol (TCP-IP)** and click **Properties** again.
6. Depending on your network, choose either **Obtain an ip address automatically** or **set manually your address, mask and default Gateway**.

   The possibility exists that a browser-specific setting could be improperly configured.
7. Choose the Internet Explorer browser **Tools > Internet Options**.
8. Choose the **Connections** tab and then verify the LAN settings or the dial-up settings.

   By default, the LAN settings and the dial-up settings do not get configured. The generic network setting from Windows gets used.
9. If the connectivity is failing only to the Cisco Unified CallManager network, a routing issue probably exists in the network. Contact the network administrator to verify the routing that is configured in your default gateway.

Note If you cannot browse from the remote server after following this procedure, contact TAC to have the issue investigated in more detail.

Replication Fails Between the Publisher and the Subscriber

Replicating the database is a core function of Cisco Communications Manager clusters. The server with the master copy of the database is called the publisher, while the servers replicating the database are called subscribers.

Symptom

Changes made on the publisher are not reflected on phones that are registered with the subscriber.

Possible Cause

Replication fails between the publisher and subscriber.

Recommended Action

Complete the following steps to reestablish the relationship between the two systems.

1. Verify the Replication.
   a. Open Cisco Unified Communications Manager Real-Time Monitoring Too (RTMT).
   b. Choose System > Performance > Open Peformance Monitoring.
   c. Double-click the publisher node to expand the performance monitors.
   d. Double-click Replication Counters.
   e. Double-click Number of Replicates Created.
   f. Choose ReplicateCount from the Object Instances dialog box and click Add.
   g. Double-click Replication Status.
   h. Choose ReplicateCount from the Object Instances dialog box and click Add.

Note Right click the counter name and choose Counter Description to view the definition of the counter.

2. Check State of Replication via CLI.
   a. Access the platform CLI and use the following command to check repliaction:

      ```
      utils dbreplication status file view activelog <filename_output_above>
      ```

   b. Review the Summary information and counts for each node to verify replication.

3. To repair replication, use the following procedure:
   a. Access the platform CLI.
   b. Repair replication by using the following command:

      ```
      utils dbreplication repair usage:utils dbreplicatoin repair [nodename]|all
      ```

Slow Server Response

This section addresses a problem that relates to a slow response from the server due to mismatched duplex port settings.

Symptom

Slow response from the server occurs.

Possible Cause

Slow response could result if the duplex setting of the switch does not match the duplex port setting on the Cisco Unified CallManager server.

Recommended Action

1. For optimal performance, set both switch and server to **100/Full**.

   Cisco does not recommend using the Auto setting on either the switch or the server.

2. You must restart the Cisco Unified CallManager server for this change to take effect.

JTAPI Subsystem Startup Problems

The JTAPI (Java Telephony API) subsystem represents a very important component of the Cisco Customer Response Solutions (CRS) platform. JTAPI communicates with the Cisco Unified CallManager and has responsibility for telephony call control. The CRS platform hosts telephony applications, such as Cisco Unified AutoAttendant, Cisco IP ICD, and Cisco Unified IP-IVR. Although this section is not specific to any of these applications, keep in mind that the JTAPI subsystem is an underlying component that all of them use.

Before starting the troubleshooting process, ensure that the software versions that you are using are compatible. To verify compatibility, read the Cisco Unified CallManager Release Notes for the version of Cisco Unified CallManager that you are using.

To check the version of CRS, log in to the AppAdmin page by typing http://servername/appadmin, where *servername* is the name of the server on which CRS is installed. The current version is located in the lower-right corner of the main menu.

JTAPI Subsystem is OUT_OF_SERVICE

Symptom

The JTAPI subsystem does not start.

Possible Cause

One of the following exceptions displays in the trace file:

- MIVR-SS_TEL-4-ModuleRunTimeFailure
- MIVR-SS_TEL-1-ModuleRunTimeFailure

MIVR-SS_TEL-4-ModuleRunTimeFailure

Search for the **`MIVR-SS_TEL-1-ModuleRunTimeFailure`** string in the trace file. At the end of the line, an exception reason appears.

The following list gives the most common errors:

- Unable to create provider—bad login or password
- Unable to create provider—Connection refused
- Unable to create provider—login=
- Unable to create provider—hostname

Unable to create provider—bad login or password

Possible Cause

Administrator entered an incorrect user name or password in the JTAPI configuration.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI
Subsystem,Failure Cause=7,Failure
Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- bad login or password.
%MIVR-SS_TEL-7-
EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- bad login or password.
```

Recommended Action

Verify that the user name and password are correct. Try logging into the Unified CMuser page (http://servername/ccmuser) on the Cisco Unified CallManager to ensure that the Cisco Unified CallManager cannot authenticate correctly.

Unable to create provider—Connection refused

Possible Cause

The Cisco Unified CallManager refused the JTAPI connection to the Cisco Unified CallManager.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
to create provider -- Connection refused
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Connection refused
```

Recommended Action

Verify that the CTI Manager service is running in the Cisco Unified CallManager Control Center.

Unable to create provider—login=

Possible Cause

Nothing has been configured in the JTAPI configuration window.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
```

```
Unable to create provider -- login=
```

Recommended Action

Configure a JTAPI provider in the JTAPI configuration window on the CRS server.

Unable to create provider—hostname

Possible Cause

The CRS engine cannot resolve the host name of the Cisco Unified CallManager.

Full Text of Error Message

```
%M%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
```

Recommended Action

Verify that DNS resolution is working correctly from the CRS engine. Try using an IP address instead of the DNS name.

Unable to create provider—Operation timed out

Possible Cause

The CRS engine does not have IP connectivity with the Cisco Unified CallManager.

Full Text of Error Message

```
101: Mar 24 11:37:42.153 PST
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
102: Mar 24 11:37:42.168 PST %MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
```

Recommended Action

Check the IP address that is configured for the JTAPI provider on the CRS server. Check the default gateway configuration on the CRS server and the Cisco Unified CallManager. Make sure no IP routing problems exist. Test connectivity by pinging the Cisco Unified CallManager from the CRS server.

Unable to create provider—null

Possible Cause

No JTAPI provider IP address or host name get configured, or the JTAPI client is not using the correct version.

Full Text of Error Message

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
```

```
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- null
```

Recommended Action

Verify that a host name or IP address is configured in the JTAPI configuration. If the JTAPI version is incorrect, download the JTAPI client from the Cisco Unified CallManager Plugins window and install it on the CRS server.

MIVR-SS_TEL-1-ModuleRunTimeFailure

Symptom

This exception usually occurs when the JTAPI subsystem is unable to initialize any ports.

Possible Cause

The CRS server can communicate with the Cisco Unified CallManager, but is unable to initialize any CTI ports or CTI route points through JTAPI. This error occurs if the CTI ports and CTI route points are not associated with the JTAPI user.

Full Text of Error Message

```
255: Mar 23 10:05:35.271 PST %MIVR-SS_TEL-1-ModuleRunTimeFailure:
Real-time failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_SS,Exception=null
```

Recommended Action

Check the JTAPI user on the Cisco Unified CallManager and verify that CTI ports and CTI route points that are configured on the CRS server associate with the user.

JTAPI Subsystem is in PARTIAL_SERVICE

Symptom

The following exception displays in the trace file:

MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT

Possible Cause

The JTAPI subsystem cannot initialize one or more CTI ports or route points.

Full Text of Error Message

```
1683: Mar 24 11:27:51.716 PST
%MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT:
Unable to register CTI Port: CTI Port=4503,
Exception=com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
1684: Mar 24 11:27:51.716 PST %MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
```

Recommended Action

The message in the trace tells you which CTI port or route point cannot be initialized. Verify that this device exists in the Cisco Unified CallManager configuration and also associates with the JTAPI user on the Cisco Unified CallManager.

Security Issues

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

Note This section 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 the *Cisco Unified CallManager Security Guide* or the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* that matches the model of the phone.

Security 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).

Security 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 3-1 lists the performance counters that apply to security features.

Table 3-1 Security Performance Counters

Object	Counters
Cisco Unified CallManager	AuthenticatedCallsActive
	AuthenticatedCallsCompleted
	AuthenticatedPartiallyRegisteredPhone
	AuthenticatedRegisteredPhones
	EncryptedCallsActive
	EncryptedCallsCompleted
	EncryptedPartiallyRegisteredPhones
	EncryptedRegisteredPhones
	SIPLineServerAuthorizationChallenges
	SIPLineServerAuthorizationFailures
	SIPTrunkServerAuthenticationChallenges
	SIPTrunkServerAuthenticationFailures
	SIPTrunkApplicationAuthorization
	SIPTrunkApplicationAuthorizationFailures
	TLSConnectedSIPTrunk
SIP Stack	StatusCodes4xxIns
	StatusCodes4xxOuts
	For example:
	401 Unauthorized (HTTP authentication required)
	403 Forbidden
	405 Method Not Allowed
	407 Proxy Authentication Required
TFTP Server	BuildSignCount
	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 Security Log and Trace Files

Cisco Unified CallManager stores log and trace files in multiple directories (cm/log, cm/trace, tomcat/logs, tomcat/logs/security, and so on).

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

You can use the trace collection feature of Cisco Unified CallManager Real Time Monitoring Tool or CLI commands to find, view, and manipulate log and trace files.

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 3-15
- Troubleshooting If You Lose One Security Token (Etoken), page 3-16

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 the *Cisco Unified CallManager Security Guide*. 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 *Cisco Unified CallManager Security Guide*.

Step 3 Reset all phones, as described in the *Cisco Unified CallManager Security Guide*.

Troubleshooting CAPF

This section contains information on the following topics:

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 3-17

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, H.323/H.245/H.225 trunk, or SIP 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), see the "Packet Capture" section on page 2-5.

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.

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.

CAPF Error Codes

The following table contains CAPF error codes that may appear in CAPF log files and the corresponding corrective actions for those codes:

Table 3-2 CAPF Error Codes

Error Code	Description	Corrective Action
0	CAPF_OP_SUCCESS /*Success */	No correction action required.
1	CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */	Install a certificate on the phone. For more information, refer to the *Cisco Unified CallManager Security Guide*.
2	CAPF_OP_FAIL /* Fail */	No corrective action available.
3	CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */	Enter the correct authentication string on phone. For more information, refer to the *Cisco Unified CallManager Security Guide*.
4	CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */	Update the locally significant certificate (LSC) on the phone. For more information, refer to the *Cisco Unified CallManager Security Guide*.

Table 3-2 CAPF Error Codes (continued)

Error Code	Description	Corrective Action
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	The manufacture-installed certificate (MIC) has been invalidated. You must install a LSC. For more information, refer to the *Cisco Unified CallManager Security Guide*.
6	CAPF_OP_FAIL_INVALID_CRENDENTIALS, /* Invalid credential */	Enter correct credentials.
7	CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure*/	No corrective action available.
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	Reschedule the operation.
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	Reschedule the CAPF operation.