



Troubleshooting Tools

This chapter addresses the tools and utilities that you use to configure, monitor, and troubleshoot Cisco CallManager 3.3 and provides general guidelines for collecting information to avoid repetitive testing and recollection of identical data.



Note

To access some of the URL sites listed this document, you must be a registered user and you must be logged in.

This chapter contains the following topics:

- [Sniffer Traces](#)
- [Debugs](#)
- [Cisco CallManager Troubleshooting Tools](#)
- [Troubleshooting Tips](#)
- [Where to Find More Information](#)

Sniffer Traces

Typically, you collect sniffer traces by connecting a laptop or other sniffer-equipped device on a Catalyst port that is configured to span the VLAN or port(s) (CatOS, Cat6K-IOS, XL-IOS) that contains the trouble information. If no free port is available, connect the sniffer-equipped device on a hub that is inserted between the switch and the device.

**Tip**

To help facilitate reading and interpreting the traces by the TAC engineer, Cisco recommends using Sniffer Pro software because it is widely used within the TAC.

Have available the IP/MAC addresses of all equipment that is involved, such as IP phones, gateways, Cisco CallManagers, and so on.

Debugs

The output from **debug** privileged EXEC commands provides diagnostic information concerning a variety of internetworking events relating to protocol status and network activity in general.

Set up your terminal emulator software (such as HyperTerminal), so it can capture the debug output to a file. In HyperTerminal, click **Transfer**; then, click **Capture Text**, and choose the appropriate options.

Before running any IOS voice gateway debugs, make sure that `service timestamps debug datetime msec` is globally configured on the gateway.

**Note**

Avoid collecting debugs in a live environment during operation hours.

Preferably, collect debugs during non-working hours. If debugs must be collected in a live environment, configure `no logging console` and `logging buffered`. To collect the debugs, use `show log`.

Some debugs can be lengthy, so collect them directly on the console port (default **logging console**) or on the buffer (**logging buffer**). Collecting debugs over a Telnet session may have an impact on the device performance, and the result could be incomplete debugs, which requires that you recollect them.

To stop a debug, use the `no debug all` or `undebug all` commands. Verify that the debugs have been turned off by using the command `show debug`.

Cisco CallManager Troubleshooting Tools

Cisco CallManager supports the troubleshooting tools listed in [Table 2-1](#).

Table 2-1 Troubleshooting Tools.

Tool Name	What it does	For more information
Cisco CallManager Administration Serviceability Tool	Monitors real-time behavior of the components in a Cisco CallManager cluster. AST monitors device status, system performance, and device discovery.	See Cisco CallManager Administration Serviceability Tool and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Alarms	Provides information about a Cisco CallManager service to a destination that you configure. Also provides definitions of alarms and the recovery procedure.	See Alarms and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Trace	Configures, collects, and analyzes information in log files for Cisco CallManager services.	See Traces and refer to the <i>Cisco CallManager Administration Guide</i> and the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Real-Time Monitoring	Monitors real-time behavior of the components in a Cisco CallManager cluster.	See Real-Time Monitoring and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.

Table 2-1 Troubleshooting Tools. (continued)

Tool Name	What it does	For more information
Service Activation	Views activation status of Cisco CallManager services. You can also activate and deactivate services.	See Service Activation and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Control Center	Views status and starts and stops Cisco CallManager services for a particular server or all servers in a cluster.	See Alarms and refer to the <i>Cisco CallManager Administration Guide Release</i> and the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Microsoft Performance Monitor (Perfmon)	Collects and displays system and device statistics for a local or remote Cisco CallManager installation.	See Microsoft Performance Monitor and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> and microsoft.com for detailed information.
Microsoft Event Viewer	Enables you to identify problems at the system level, such as a gateway.	See Microsoft Event Viewer and refer to microsoft.com for detailed information.
Show Command	Displays the contents of the Cisco CallManager configuration database, configuration file, and memory statistics.	See Show Command and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.
Cisco Secure Telnet	Provides transparent firewall access to Cisco CallManagers servers on the customer site.	See Cisco Secure Telnet and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> for detailed information.

Table 2-1 Troubleshooting Tools. (continued)

Tool Name	What it does	For more information
CiscoWorks2000	Manages the remote Cisco CallManager network	See CiscoWorks2000 and refer to the <i>Cisco CallManager Serviceability Administration Guide</i> and the CiscoWorks2000 documentation for detailed information.
Other tools, such as the Dick Tracy utility	The Dick Tracy utility provides additional information that is not available using the Show command.	See Other Tools and refer to http://www-tac/Teams/AVVID/sj/Ttools/ttools.htm for detailed information.

Cisco CallManager Administration Serviceability Tool

The Cisco CallManager Administration Serviceability Tool (AST), a web-based tool available with the Cisco CallManager Serviceability program, monitors real-time behavior of the components in a Cisco CallManager cluster. The AST uses HTTP and TCP to monitor device status, system performance, and device discovery.

Refer to the *Cisco CallManager Serviceability Administration Guide* for more information on the AST.

Alarms

Alarms, a web-based tool available with the Cisco CallManager Serviceability program, provides two functions:

- Configure alarms and events
- Provide alarm message definitions.

Alarms contain information such as explanation and recommended action. Alarm information includes application name, machine name, and cluster name to help you perform troubleshooting for problems that are not on your local Cisco CallManager.

Refer to the *Cisco CallManager Serviceability Administration Guide* for configuration procedures to view definitions and alarm information.

Traces

For IP telephony issues, Cisco CallManager traces prove very important in the troubleshooting process. A TAC engineer may ask you to capture traces to troubleshoot the problem.

This section contains information for the following trace items:

- [Trace Configuration](#)
- [Trace Analysis](#)
- [Trace Collection](#)
- [Q931 Translator](#)

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Trace Configuration

You can configure the following Cisco CallManager services for Trace Configuration and to specify the parameters that you want to trace.

- Cisco CallManager
- Cisco CTIManager (release 3.1 only)
- Cisco Database Layer Monitor
- Cisco IP Voice Media Streaming Application
- Cisco Messaging Interface
- Cisco RIS Data Collector (release 3.1 only)
- Cisco TFTP

Trace Analysis

The Trace Analysis tool, a post-processing tool that displays XML files, provides greater trace detail to help narrow system problems.

Cisco CallManager traces are located at

C:\program files\cisco\traces\ccm

SDL traces are located at

C:\program files\cisco\traces\sdl\ccm

Using the Trace Analysis tool, you can specify an SDI or SDL trace, a device name, or an IP address for the following Cisco CallManager services:

- Cisco CallManager
- Cisco CTIManager
- Cisco TFTP

Trace Collection

The Trace Collection tool collects trace information for any of the following Cisco CallManager services, the time and date of the trace for that service, and the trace type (SDI or SDL):

- Cisco CallManager
- Cisco CTIManager
- Cisco Database Layer Monitor
- Cisco IP Voice Media Streaming Application
- Cisco Messaging Interface
- Cisco RIS Data Collector
- Cisco TFTP
- server_x: Cisco Call Manager

Use the following procedure to collect Cisco CallManager traces and SDL traces.

Procedure

-
- Step 1** Set the service parameter `SDLTraceTypeFlags` to **0x8000EB15**.

- Step 2** Set CCM and SDL traces to **On**.
- Step 3** Set CCM trace setting to **Arbitrary**.
-

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Q931 Translator

You can use the Q931 Translator for a Cisco CallManager server for which you want to translate Q931 messages in the following formats:

- XML trace file format
- Text trace file format

Real-Time Monitoring

Cisco CallManager Serviceability provides a web-based tool, Real-Time Monitoring Tool (RTMT), that monitors real-time behavior of the components in a Cisco CallManager cluster. RTMT uses HTTP and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP for troubleshooting system problems.

Performance monitoring provides the following services:

- Monitors performance counters from the Cisco CallManager cluster, including Cisco CallManager nodes, TFTP servers, and database servers.
- Presents counters hierarchically for easy navigation.
- Associates counter threshold settings to alert notification. An email or popup message provides notification to the administrator.
- Permits saving and restoring settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Displays up to three counters in one chart for performance comparisons.

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Service Activation

Cisco CallManager Serviceability provides a web-based Service Activation tool that is used to activate or deactivate multiple services and to choose default services to activate.

Activate or deactivate services in the Service Activate web pages by checking the check boxes beside the service names and clicking the **Update** button.

The Service Activation tool activates services in automatic mode and checks for service dependencies. When you click the **Set Default** button, the Service Activation tool chooses those services that are required to run Cisco CallManager. For example, if you choose one service, all the other services that depend on that service to run Cisco CallManager, if any, also automatically get chosen.



Caution

Only deactivate services from the Service Activation pages. If you deactivate services from the Service Control Manager on the Cisco CallManager system, you will get an error message saying that some of the services are not configured properly. This occurs because deactivating services from the Service Control Manager does not remove the entries from the database tables; therefore, the services get out of sync with the database.



Note

Access the Control Center web pages from a link on the Service Activation pages.

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Control Center

Control Center views status and starts and stops Cisco CallManager services for a particular server or all servers in a cluster. An icon indicates the status of the service. Control Center supports the following Cisco CallManager services:

- Cisco CallManager
- Cisco TFTP
- Cisco Messaging Interface

- Cisco IP Voice Media Streaming Application
- Cisco CTIManager
- Cisco Telephony Call Dispatcher
- Cisco MOH Audio Translator
- Cisco RIS Data Collector
- Cisco Extension Mobility
- Cisco Database Layer Monitor
- Cisco CDR Insert
- Cisco Call Back
- Cisco IP Manager Assistant

Microsoft Performance Monitor

Microsoft Performance Monitor application monitors and logs resource counters from the Cisco CallManager nodes in the network and displays the system activities and status information in real time.



Tip

Use the following procedure to collect and display system and device statistics for any Cisco CallManager installation.

Procedure

- Step 1** Access Performance Monitor by choosing **Start > Programs > Administration Tools > Performance**.
- Step 2** Choose **Action > New log settings** and enter a name for the counter log.
- Step 3** Click **Counters**.
- Step 4** Click **Add**.
- Step 5** Click **Performance Object**.
- Step 6** Click **Process**.
- Step 7** In **Select Counters from List** and **Select Instances from List**, choose the following counters and associated instances:

- % Processor Time/_Total
- % Processor Time/ccm
- % Processor Time/AudioTranslator
- % Processor Time/Aupair
- % Processor Time/CiscoMessagingI
- % Processor Time/ctftp
- % Processor Time/CTIManager
- % Processor Time/DLLHOST
- % Processor Time/sqlservr
- % Processor Time/TcdSrv
- % Processor Time/RisDC
- % Processor Time/snmp
- % Processor Time/CallBackService
- % Processor Time/LogoutService
- % Processor Time/InsertCDR
- Virtual Bytes/_Total
- Virtual Bytes/AudioTranslator
- Virtual Bytes/Aupair
- Virtual Bytes/ccm
- Virtual Bytes/CiscoMessagingI
- Virtual Bytes/ctftp
- Virtual Bytes/CTIManager
- Virtual Bytes/DLLHOST
- Virtual Bytes/sqlservr
- Virtual Bytes/TcdSrv
- Virtual Bytes/RisDC
- Virtual Bytes/snmp
- Virtual Bytes/CallBackService
- Virtual Bytes/LogoutService

- Virtual Bytes/InsertCDR
- Private Bytes/_Total
- Private Bytes/ccm
- Private Bytes/AudioTranslator
- Private Bytes/Aupair
- Private Bytes/CiscoMessagingI
- Private Bytes/ctftp
- Private Bytes/CTIManager
- Private Bytes/DLLHOST
- Private Bytes/sqlservr
- Private Bytes/TcdSrv
- Private Bytes/RisDC
- Private Bytes/snmp
- Private Bytes/CallBackService
- Private Bytes/LogoutService
- Private Bytes/InsertCDR

Step 8 Click the **General** tab.

Step 9 Enter the collection interval of **60** and for Units choose **seconds**, so the data is averaged and collected over 60-second intervals.

Step 10 Click **Apply**.

Step 11 Click the **Schedule** tab.

Step 12 Choose the **At** option for Start log and enter the current time and date to enable the logging to continue after a reboot.

Step 13 Click **Save** to save your settings, such as the *objects* that you chose.

This allows you to load the same data again, if necessary.



Note

The log files will expand in size. Manually purge the log files to maintain optimal disk space.

Performance Monitor can simultaneously collect data from multiple installed systems and store the information in a single log file. You can export the log file into a Tab Separated Value (TSV) file or a Comma Separated Value (CSV) file. View the TSV file or CSV file in a spreadsheet application.

**Note**

You must enable Statistics in Cisco CallManager Administration for the Performance Monitor to collect data.

Cisco CallManager directly updates Microsoft Performance Monitor counters. The call perfmon counters as call-processing-related counters contain simple, useful counts such as number of registered phones, number of active calls, and number of available conference bridge resources.

The following list identifies the Cisco CallManager performance counters:

- Cisco CallManager
- Cisco Phones
- Cisco Lines
- Cisco H323
- Cisco MGCP Gateways
- Cisco MOH Device
- Cisco Analog Access
- Cisco MGCP FXS Device
- Cisco MGCP FXO Device
- Cisco MGCP T1CAS Device
- Cisco MGCP PRI Device

Customize Performance Monitor to view the Cisco CallManager-related parameters that you want to monitor by choosing the object, counter, and the instance.

Refer to microsoft.com for more information on Performance Monitor.

Microsoft Event Viewer

Microsoft Event Viewer tool can help you identify problems at the system level, such as events regarding a specific gateway.

Access Event Viewer by choosing

Start > Programs > Administration Tools > Event Viewer.

The Event Viewer displays the following types of logs:

- Application log—Contains events logged by applications or programs, such as Cisco CallManager.
- System log—Reports events logged by Windows 2000 system components, such as the failure of a component.
- Security log—Holds information records regarding security events. Cisco CallManager does not report events in this log.

The Event Viewer displays the following event types:

- Error—Indicates a problem, such as the loss of data or functionality.
- Warning—Indicates a potential problem, such as when a service is stopped or started. This event type does not necessarily signal an error.
- Information—Indicates the availability of system information, such as host names or the version of the currently used database.

Cisco Secure Telnet

Cisco Secure Telnet allows Cisco Service Engineers (CSE) transparent firewall access to the Cisco CallManager node on your site. Using strong encryption, Cisco Secure Telnet enables a special Telnet client from Cisco Systems to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and troubleshooting of your Cisco CallManager nodes, without requiring firewall modifications.



Note

Cisco provides this service only with your permission. You must ensure that a network administrator is available at your site to help initiate the process.

Command Line Tools

Command Line Tools prove useful in troubleshooting. The following list gives the available command line tools:

- **show**—Displays the Cisco CallManager database content, the .ini config file, memory statistics, and Windows diagnostic information and runs from a DOS shell or from a Telnet session into the Cisco CallManager.
- **nslookup *hostname***—Checks for a host-name-to-IP-address resolution.
- **netstat - a | more**—Checks for socket listens on the correct port number.
- **ping *hostname***—Checks that the machine can be reached via an IP.
- **net start**—Checks to see whether services are running.

Show Command

Use the Show command line tool to display the contents of the system memory statistics and the Windows diagnostic information. You can run the show command from a DOS shell or from a Telnet session if Telnet server software is enabled. You can display the output data on the console or save it as a text file.

The following syntax applies for the show command:

show [-f <filename>] [-c <column width>] [-w <console width>] [-v] [command]

Use the following parameters with the show command:

- **show ?**—Show help message
- **show db**—Show configuration database
- **show db tables**—Show database table names
- **show db t <tablename>**—Show content of the database table
- **show win**—Report Windows diagnostics

Refer to the *Cisco CallManager Serviceability Administration Guide* for more information on the show command.

CiscoWorks2000

CiscoWorks2000 serves as the network management system of choice for all Cisco devices including Cisco CallManager. Because CiscoWorks2000 is not bundled with Cisco CallManager, you must purchase it separately. Use the following tools with CiscoWorks2000 for remote serviceability:

- System Log
- Path Analysis
- Cisco Discovery Protocol
- Simple Network Management Protocol

Refer to the *Cisco CallManager Serviceability Administration Guide* and the CiscoWorks2000 documentation for more information on CiscoWorks2000 at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>

Other Tools

Access other available tools, such as the Dick Tracy utility, at the following URL:

<http://www-tac/Teams/AVVID/sj/Ttools/ttools.htm>

Troubleshooting Tips

The following tips may help you when troubleshooting the Cisco CallManager.

**Tip**

Check the release notes for Cisco CallManager for known problems.

The release notes provide descriptions and workaround solutions for known problems.

**Tip**

Know where your devices are registered.

Each Cisco CallManager log traces files locally. If a phone or gateway is registered to a particular Cisco CallManager, then the call processing gets done on that Cisco CallManager if the call is initiated there. You will need to capture traces on that Cisco CallManager to debug a problem.

A common mistake involves having devices registered on a subscriber server, but capturing traces on the publisher server. These trace files will be near empty (and most definitely will not have the call in them).

Another common problem involves having Device 1 registered to CM1 and Device 2 registered to CM2. If Device 1 calls Device 2, the call trace occurs in CM1 and if Device 2 calls Device 1 the trace occurs in CM2. If you are troubleshooting a two-way calling issue, you need both traces from both Cisco CallManagers to obtain all the information needed to troubleshoot.

**Tip**

Know the approximate time of the problem.

Multiple calls may have been made, so knowing the approximate time of the call helps TAC quickly locate the trouble.

You can obtain phone statistics on a Cisco IP Phone 79xx by pressing the **i** button twice during an active call.

When you are running a test to reproduce the issue and produce information, knowing the following data is crucial to understanding the issue:

- Calling number/called number
- Any other number that is involved in the specific scenario
- Time of call

**Note**

Remember that time synchronization of all equipment is important for troubleshooting.

If you are reproducing a problem, make sure to choose the file for the timeframe by looking at the modification date and the timestamps in the file. The best way to collect the right trace is to reproduce a problem and then quickly locate the most recent file and copy it from the Cisco CallManager server.

**Tip**

Save the log files to prevent them from being overwritten.

Files will be overwritten after some time. The only way to know which file is being logged to is to choose **View > Refresh** on the menu bar and look at the dates and times on the files.

**Tip**

Verify that the Cisco CallManager services are running.

Use the following procedure to verify that the Cisco CallManager service is active on a server.

Procedure

-
- Step 1** From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.
The Cisco CallManager Serviceability window displays.
- Step 2** Choose **Tools > Service Activation**.
- Step 3** From the Servers column, choose the server.
The server that you chose displays next to the Current Server title, and a box with configured services displays.
Activation Status column displays either Activated or Deactivated in the Cisco CallManager line.
If Activated, the Cisco CallManager is active on the chosen server.
If Deactivated, continue with the following steps.
- Step 4** Check the check box for Cisco CallManager.
- Step 5** Click the **Update** button.
The Activation Status column displays Activated in the Cisco CallManager line.
Cisco CallManager is now active for the chosen server.
-

Perform the following procedure if the Cisco CallManager has been in service and you want to verify if it is currently active.

Procedure

-
- Step 1** From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.
The Cisco CallManager Serviceability window displays.

Step 2 Choose **Tools > Control Center**.

Step 3 From the Servers column, choose the server.

The server that you chose displays next to the Current Server title, and a box with configured services displays.

Activation Status column displays Activated in the CallManager line.

Cisco CallManager is active for the chosen server.



Tip

Start and stop the Internet Information Server.

Use either of the following procedures to start or stop the Internet Information Server (IIS).

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing the services.

To Stop Services

Step 2 Choose **IIS Admin Service**.

Step 3 Click the stop button (black square box at the top of the window).

Step 4 Click **Yes**.

To start Services

Step 5 Click the **Start** button.

Step 6 Choose **World Wide Web Publishing**.

Step 7 Click the start button (black square box with right arrow at the top of the window).
The IIS starts.

Procedure

- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
- A window displays listing the services.

To Stop Services

- Step 2** Right-click **IIS Admin Service**.
- Step 3** Choose **Stop**.
- The IIS stops.

To start Services

- Step 4** Click the **Start** button.
- Step 5** Right-click **World Wide Web Publishing**.
- Step 6** Choose **Start**.
- The IIS starts.
-

Procedure

-
- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
- A window displays listing IIS Administration Service.
- Step 2** Right-click **IIS Admin Service** and choose **Stop**.
- The IIS stops.
- Step 3** To start the IIS server:
- Right-click **IIS Admin Service** and choose **Start**.
- The IIS starts.
-

Where to Find More Information

Additional Cisco Documentation

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Administration Guide*
- *Installation Guide for Cisco CallManager*
- CiscoWorks2000 user documentation at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>