



Troubleshooting Tools

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



Note

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

This section contains the following topics:

- [Sniffer Traces](#)
- [Debugs](#)
- [Cisco Unified 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 of 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 Unified CallManagers, and so on.

Debugs

The output from **debug** privileged EXEC commands provides diagnostic information about a variety of internetworking event that relate 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 you must collect debugs in a live environment, configure `no logging console` and `logging buffered`. To collect the debugs, use `show log`.

Because some debugs can be lengthy, collect them directly on the console port (default `logging console`) or on the buffer (`logging buffer`). Collecting debugs over a Telnet session may impact the device performance, and the result could be incomplete debugs, which requires that you re-collect 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 Unified CallManager Troubleshooting Tools

Refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide* for detailed information of the following different types of tools that Cisco Unified CallManager Serviceability provides to monitor and analyze the various Cisco Unified CallManager systems.

Table 2-1 **Serviceability Tools**

Term	Definition
Real-Time Monitoring Tool (RTMT)	<p>This term identifies a program in Serviceability that provides real-time information about Cisco Unified CallManager devices and performance counters as well as enables administrators to collect traces.</p> <p>Performance counters can be system specific or Cisco Unified CallManager specific. Objects comprise the logical groupings of like counters for a specific device or feature, such as Cisco Unified IP Phones or Cisco Unified CallManager System Performance. Counters measure various aspects of system performance. Counters measure statistics such as the number of registered phones, calls that are attempted and calls in progress.</p>
Alarms	<p>Administrators use alarms to obtain run-time status and state of the Cisco Unified CallManager system. Alarms contain information about system problems such as explanation and recommended action.</p> <p>Administrators search the alarm definitions database for alarm information. The alarm definition contains a description of the alarm and recommended actions.</p>

Table 2-1 Serviceability Tools (continued)

Term	Definition
Trace	<p>Administrators and Cisco engineers use trace files to obtain specific information about Cisco CallManager service problems. Cisco Unified CallManager Serviceability sends configured trace information to the trace log file. Two types of trace log files exist: SDI and SDL.</p> <p>Every Cisco CallManager service includes a default trace log file. The system traces system diagnostic interface (SDI) information from the services and logs run-time events and traces to a log file.</p> <p>The SDL trace log file contains call-processing information from services such as Cisco CallManager and Cisco CTIManager. The system traces the signal distribution layer (SDL) of the call and logs state transitions into a log file.</p> <p>Note In most cases, you will only gather SDL traces when Cisco Technical Assistance Center (TAC) requests you to do so.</p>
Trace Analysis	This program presents trace information in a format that allows you to filter the results.
Quality Report Tool	This term designates voice quality and general problem-reporting utility in Cisco Unified CallManager Serviceability.

Cisco Secure Telnet

Cisco Secure Telnet allows Cisco Service Engineers (CSE) transparent firewall access to the Cisco Unified 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 Unified 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 Unified 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 Unified 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 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.

**Note**

Because the show command uses a temporary file in the \Temp directory for the output, check to ensure that you have enough disk space available to receive it. The amount that you will need varies depending on a number of factors; for example, the number of users and devices being used and the size of the database being used by the system.

Alternatively, you can run **show.exe** from a Telnet session if Telnet server software is enabled.

The following syntax applies for the show command:

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

Table 2-2 lists options that the **show** command supports.

Table 2-2 Show Command Options

Command	Description
-f <filename>	Name of file to print the report
-c <col width>	Width of each column in the database report (default 15)
-w <con width>	Width of the database report area (default 80)
-v	Verbose mode

Use the following parameters with the **show** command:

- **?**—Show help message.
- **db**—Show configuration database.
- **db tables**—Show database table names.
- **db t <tablename>**—Show content of the database table.
- **inst [apps | elem | all]**—Show information about installed applications and elements.
- **isdn [cluster | local | specific]**—Show D channel status on gateway.
- **ps**—Show all processes running on the local system.
- **win**—Report windows diagnostics. The **win** parameter includes, but is not limited to, information such as system statistics, storage information, software environment, and summary statistics.



Note **Show win** consumes a significant part of CPU resources to get the windows system information and takes a long time to display. Execute it only when Cisco Unified CallManager is not busy.

- **tech | (none)**—Report database and Windows system information.



Note **Show tech** reports the same multireport output as **show** command without a parameter

Example:

```
show -f output.txt -v -w480 db
show tech
show db t ProcessNode
```

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

Cisco Unified CallManager System Performance Monitoring

Use Windows 2000 Performance to collect and display system and device statistics for any local or remote Cisco Unified CallManager installation. This administrative tool allows you to gain a full understanding of a system without studying the operation of each of its components. It reports both general and specific information in real time.

After adding the Cisco CallManager parameters, you can define the terms under which Cisco Unified CallManager will display statistics generated by the system.

For more information about Performance, refer to the Microsoft Windows 2000 documentation.

Path Analysis Operation

Path Analysis, a diagnostic application, traces connectivity between two specified points on a network. It analyzes both physical and logical paths (Layer 2 and Layer 3) that are taken by packets that flow between those points.

After a call completes, PathTool traces the route of audio packets by specifying the directory number of the calling and called parties. This applies to calls among any of the following endpoints: Cisco Unified IP Phones, analog devices that are connected to a station gateway, or trunk gateways (analog or digital).

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

System Log Management Process

Although it can be adapted to other network management systems, Cisco Syslog Analysis, which is packaged with CiscoWorks2000 Resource Manager Essentials, provides the best method to manage Syslog messages from Cisco devices.

Cisco Syslog Analyzer serves as the component of Cisco Syslog Analysis that provides a common storage and analysis of the system log for multiple applications. The other major component, Syslog Analyzer Collector, gathers log messages from Cisco Unified CallManager servers.

These two Cisco applications work together to provide a centralized system logging service for Cisco Unified Communications Solutions.

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

Simple Network Management Protocol Support

Network management systems (NMS) use SNMP, an industry-standard interface, to exchange management information between network devices. A part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
- An agent, as network management software, resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

- A network management system comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. The following NMSs share compatibility with Cisco Unified CallManager:
 - CiscoWorks2000
 - HP OpenView
 - Third-party applications that support SNMP and Cisco Unified CallManager SNMP interfaces

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

CiscoWorks2000

CiscoWorks2000 serves as the network management system of choice for all Cisco devices including Cisco Unified CallManager. Because CiscoWorks2000 is not bundled with Cisco Unified 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 Unified 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>

Cisco Discovery Protocol Support

The Cisco Discovery Protocol Support enables discovery of Cisco Unified CallManager servers and management of those servers by CiscoWorks2000.

Refer to the *Cisco Unified 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>

SQL Query Analyzer

The SQL Query Analyzer to find devices, such as endpoints, IP phones, and gateways, that are associated with a location. To use the SQL Query, perform the following steps.

**Note**

If the value **None** appears in the Location field in the Cisco Unified CallManager Configuration window, the device has not been assigned to a specific location. Therefore, devices not assigned to a location do not get returned by the SQL Query.

Procedure

-
- Step 1** Choose **Start > Programs > Microsoft SQL Server > Query Analyzer** on the Windows 2000 server console of the Cisco Unified CallManager server to run the SQL Server Query Analyzer application.
- The Connect to SQL Server window appears. (The SQL Query Analyzer window is dimmed in the background.)
- Step 2** In the SQL Server field, type a period character.
- Step 3** Uncheck the **Start SQL Server if it is Stopped** option.
- Step 4** Click the **Windows Authentication** button.
- Step 5** Click **OK**.
- Step 6** The Query (local) window appears. (The SQL Query Analyzer window gets dimmed in the background.)

Step 7 From the DB field, click the drop-down arrow and choose the highest numbered Cisco Unified CallManager database.

Cisco Unified CallManager databases are labeled with the following format: **ccm03xx** (where **xx** is the number of the database).

Step 8 Enter the following SQL query in the body of the Query (local) window.

```
SELECT Device.name, Device.description
FROM Device, Location
WHERE Device.fkLocation=Location.pkid
AND Location.name="enter location name between these quotes"
```

Step 9 Choose **Query > Execute** from the main Query Analyzer window to run the query.

You can also click the green arrow from the toolbar or press **F5** to run the query.

Step 10 When the results are done, close the SQL Server Query Analyzer window.

Troubleshooting Tips

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

**Tip**

Check the release notes for Cisco Unified CallManager for known problems.

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

**Tip**

Know where your devices are registered.

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

A common mistake involves having devices that are registered on a subscriber server but are capturing traces on the publisher server. These trace files will be nearly 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 Unified CallManagers to obtain all the information that is needed to troubleshoot.

**Tip**

Know the approximate time of the problem.

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

You can obtain phone statistics on a Cisco Unified 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, know the following data that 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 time stamps in the file. The best way to collect the right trace means that you reproduce a problem and then quickly locate the most recent file and copy it from the Cisco Unified CallManager server.



Tip Save the log files to prevent them from being overwritten.

Files will get overwritten after some time. The only way to know the file that 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 Unified CallManager Administration, choose **Application > Cisco Unified CallManager Serviceability**.

The Cisco Unified 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 Unified CallManager line.

If the **Activated** status displays, the Cisco Unified CallManager remains active on the chosen server.

If the **Deactivated** status displays, continue with the following steps.

Step 4 Check the check box for Cisco Unified CallManager.

Step 5 Click the **Update** button.

The Activation Status column displays **Activated** in the Cisco Unified CallManager line.

Cisco Unified CallManager is now active for the chosen server.

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

Procedure

Step 1 From Cisco Unified CallManager Administration, choose **Application > Cisco Unified CallManager Serviceability**.

The Cisco Unified 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 Unified CallManager is active for the chosen server.



Tip

Start and stop the Internet Information Server.

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

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