



Trace

Use trace configuration to specify the type and level of trace information reported by Cisco CallManager and its associated services. You can configure trace options for each of the following system services:

- Cisco CallManager
- Cisco Database Layer Monitor
- Cisco IP Voice Media Streaming Application
- Cisco Messaging Interface (CMI)
- Cisco Telephony Call Dispatcher (TCD)
- Cisco Trivial File Transfer Protocol (TFTP)

The following sections provide details about configuring trace settings:

- Understanding Trace Configuration, page 32-2
- Recommended Trace Settings, page 32-9
- Adding a New Service and Trace Configuration, page 32-9
- Updating a Trace Configuration, page 32-11
- Deleting a Trace Configuration, page 32-11

Understanding Trace Configuration

Traces provide information that can be used for system performance monitoring, troubleshooting, and debugging. It is important that you select the proper level and amount of trace information for your needs. Too little trace information will prevent you from debugging the system, but too much trace information can overload the system and degrade performance.

You can set the following parameters in Cisco CallManager Administration to control the type and amount of trace information generated:

- Trace Levels, page 32-2
- Date and Time, page 32-3
- User Mask, page 32-4
- Event Type, page 32-6
- Trace Log Components, page 32-7

The hexadecimal number in the Trace Mask field changes as you change the settings of trace level, date, time, and user mask.

Trace Levels

Table 32-1 lists the available trace levels used by the Cisco CallManager service. The Error level provides the least amount of trace information, and the Detailed level provides the most. The levels are cumulative, which means that a more detailed level includes all the same information as the lower level plus some additional information.

Table 32-1 Trace Levels

Level	Description
Error	Traces alarm conditions and events.
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation.

Table 32-1 Trace Levels (continued)

Level	Description
Significant	Traces all State Transition conditions plus media events that occur during normal operation.
Entry/Exit	Traces all Significant conditions plus entry and exit points of routines. Not all services use this trace level.
Arbitrary	Traces all Entry/Exit conditions plus low-level debugging information. <i>Do not use this trace level with the Cisco CallManager service or the Cisco IP Voice Media Streaming Application service during normal operation.</i>
Detailed	Traces all Arbitrary conditions plus detailed debugging information. <i>Do not use this trace level with the Cisco CallManager service or the Cisco IP Voice Media Streaming Application service during normal operation.</i>

Date and Time

You can enable the Show Date and Show Time options to record the date and time of each trace event. Cisco recommends that you enable the Show Time option for all traces.

User Mask

The user mask is a series of flags, or bits, that enable and disable specific types of trace information. As you click on the bits to turn them on and off, the hexadecimal value in the Mask field changes. The function of each mask bit depends on the service you are tracing, as indicated in Table 32-2.

Table 32-2 User Mask Bits

Service	Mask Bits	Type of Trace Enabled by This Bit
Cisco CallManager	0	Protocol layer 1 information.
	1	Protocol layer 2 information.
	2	Digital gateway information.
	3	Analog gateway information.
	4	Primary Rate Interface (PRI) information.
	5	Skippy Station protocol information.
	6	Message translation information for ISDN messages.
	7	Media Termination Point (MTP) information.
	8	H.225 and Gatekeeper information.
	9	Gateway traces (used in conjunction with bits 2, 3, and 4)
	10	Detailed debugging information. <i>Do not set this flag during normal system operation.</i>
	11	Subsystem information not covered by one of the other user mask bits.
	12	Conference bridge information.
	13	MGCP gateway information.
14-15	Not used.	

Table 32-2 User Mask Bits (continued)

Service	Mask Bits	Type of Trace Enabled by This Bit
Cisco Database Layer Monitor	0	Detailed database information such as SQL statements.
	1	Detailed information about the business rules.
	2	Information about DBLX.dll relating to the web administration pages and Visual Basic applications. Tracing this information from web administration requires that you enable the debug settings on IISAdmin service and the web service from the IIS Management console. After enabling this bit, you must stop and restart all applications that use this DLL before tracing will begin.
	3	Information about database change notification messages.
	4-7	Not used.
	8	Information about DBL.dll relating to any application programs that access the database. After enabling this bit, you must stop and restart all applications that use this DLL before tracing will begin.
	9	Information about all code in the database.
	10-15	Not used.
	Cisco IP Voice Media Streaming Application	0
1		Service and database manager information.
2		Media Termination Point (MTP) device information.
3		Conference bridge device information.
4		MTP and conference bridge device recovery information.
5		Device driver information.
6		Message information from Skinny Station protocol.
7		High-level WinSock information.
8		Not used.
9		Low-level WinSock information.
10-15		Not used.

Table 32-2 User Mask Bits (continued)

Service	Mask Bits	Type of Trace Enabled by This Bit
Cisco Messaging Interface (CMI)	0-15	Not used.
Cisco Trivial File Transfer Protocol (TFTP)	0	All TFTP event information.
	1-15	Not used.

Event Type

The event type applies only to Error traces, and it specifies what types of error events are traced. The available event types are:

- Debug
- Information
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

The Emergency event type traces only the most severe Error events, and it provides the least amount of trace information. The Debug event type provides trace information on all types of events, including events that occur during normal system operation. The event types between Emergency and Debug provide increasingly greater amounts of trace information. For traces during normal system use, select an event type between Warning (minimum) and Debug (maximum).

Trace Log Components

The trace log components let you specify where the trace information is collected or stored.

**Caution**

Creating a large number of trace files, or letting a single trace file grow too large, can severely degrade the performance of your system.

Table 32-3 describes the trace log components.

Table 32-3 Components of the Trace Log

Component	Description
EventLog	Enable this option to send trace information to the Windows 2000 EventLog.
Output Debug String	This option is for Cisco development use only. <i>Do not enable this option unless instructed to do so by Cisco Technical Assistance Center (TAC).</i>

Table 32-3 Components of the Trace Log (continued)

Component	Description
File	<p>Enable this option to store trace information in a file. You can also set the following file parameters:</p> <ul style="list-style-type: none"> • Name is the fully qualified path name of the trace file. Each service requires a unique trace file name. Cisco recommends that you leave the file names set to their default values. • # of Files specifies the total number of trace files for a given service. A sequence number is automatically appended to the file name to indicate which file it is. When the last file in the sequence is full, the trace data begins writing over the first again. • # of Lines specifies the maximum number of lines of data stored in each trace file. • # of Minutes specifies the maximum number of minutes worth of data stored in each trace file. <p>When the trace data exceeds either the maximum number of lines or the maximum number of minutes for one file, that file is closed and the remaining trace data is written to the next file in the sequence. For example, you can set up trace files to store a full week of data, with one day of data in each file. To do this, you can set the number of files to 7, the number of minutes to 1440 (one day), and the number of lines to a large value such as 10000 (or larger for a busy system).</p>
System Log	<p>Enable this option to send trace information to the Cisco Syslog Collector. The System Log parameters are:</p> <ul style="list-style-type: none"> • Debug Enabled causes all trace data to be sent to the Cisco Syslog Collector. If you do not enable this option, only alarm (Error) traces are sent to the Cisco Syslog Collector. • System Server is the name of the Cisco Syslog Collector. Do not change this field unless instructed to do so by Cisco Technical Assistance Center (TAC).

Recommended Trace Settings

In general, it is best to start with a small amount of tracing so that system resources are not overloaded by the trace data. If the initial traces are not sufficient for your purposes, you can gradually increase the level of tracing until you get the desired data. If system performance begins to degrade during tracing, decrease the trace level until the performance returns to normal.

During normal system operation, it is customary to trace alarm conditions and to respond to them as quickly as possible. Alarm tracing is considered to be the minimum level of tracing for a fully operational system. To configure this minimum level of alarm tracing, set the trace parameters as follows for each service on each Cisco CallManager in the cluster:

- Enable Trace On.
- Set the trace level to Error.
- Enable the Show Time option.
- Enable the appropriate user mask bits for each service, as described in Table 32-2.
- Set the event type to Error.
- Enable EventLog.

Adding a New Service and Trace Configuration

This section describes how to add a new service and trace configuration to the Cisco CallManager database. Normally you do not have to use this procedure because each service receives a default trace configuration when you install the Cisco CallManager software. You can then modify this default trace configuration by following the procedure described in the “Updating a Trace Configuration” section on page 32-11.

However, you can also add a new service and trace configuration before installing an additional (subscriber) Cisco CallManager in a cluster. If you then install a Cisco CallManager with the same name specified in the new trace configuration, that trace configuration becomes the default for the specified service on the specified Cisco CallManager.

Procedure

- Step 1** Open Cisco CallManager Administration.
 - Step 2** Select **Service > Trace**.
 - Step 3** From the list of IP addresses at the left of the screen, select the IP address of the Cisco CallManager server whose trace parameters you want to configure.
 - Step 4** Click **New** to create a trace configuration for a new service.
 - Step 5** From the Service Type drop-down list box, select the service for which you want to add a trace configuration, then click **Insert**.
 - Step 6** Click **Trace On** to enable trace.
 - Step 7** Select the desired trace level. For details, see the “Trace Levels” section on page 32-2.
 - Step 8** If desired, enable the Show Time and Show Date options to record the time and date of each event. Cisco recommends that you enable the Show Time option.
 - Step 9** Set the appropriate user mask bits for the service. For details, see the “User Mask” section on page 32-4.
 - Step 10** Select the desired event type. For details, see the “Event Type” section on page 32-6.
 - Step 11** Set the desired trace log components. For details, see the “Trace Log Components” section on page 32-7.
 - Step 12** If you want to reset all trace parameters to their previous value, click **Cancel**. If you want to reset all trace parameters to their initial default value, click **SetDefault**.
 - Step 13** When you are finished setting the trace parameters, click **Update** to save the changes in the database.
-

Updating a Trace Configuration

This section describes how to update an existing trace configuration for a service.

Procedure

- Step 1** Open Cisco CallManager Administration.
 - Step 2** Select **Service > Trace**.
 - Step 3** From the list of IP addresses at the left of the screen, select the IP address of the Cisco CallManager server whose trace configuration you want to update.
 - Step 4** From the list of Configured Services, select the service whose trace configuration you want to update.
 - Step 5** Make the desired changes in the fields you want to update. Before saving the changes, you can click **Cancel** to reset all fields to their previous value or click **SetDefault** to reset all fields to their default value.
 - Step 6** Click **Update** to save the changes in the database.
-

Deleting a Trace Configuration

This section describes how to delete a trace configuration.

Procedure

- Step 1** Open Cisco CallManager Administration.
- Step 2** Select **Service > Trace**.
- Step 3** From the list of IP addresses at the left of the screen, select the IP address of the Cisco CallManager server whose trace configuration you want to delete.
- Step 4** From the list of Configured Services, select the service whose trace configuration you want to delete.
- Step 5** Click **Delete** to delete the trace configuration for this service. If you want to delete all trace services for the selected Cisco CallManager, click **Delete Service**.

**Caution**

Turning off all trace services also disables Simple Network Management Protocol (SNMP).

Step 6

When asked to confirm the delete operation, click either **OK** to delete or **Cancel** to cancel the delete operation.
