Troubleshooting

Enabling Cisco Unified SIP Proxy Traces

Procedure

Step 1 Choose **Troubleshoot** > **Cisco Unified SIP Proxy** > **Traces**.

The system displays the Cisco Unified SIP Proxy Traces page.

Step 2 To capture the network traffic on Cisco Unified SIP Proxy interfaces, check the **Packet Capture** check box.

a) Click **Start** to start packet capture.

b) Click **Stop** to stop packet capture.

Each packet capture request is limited to 40 MB. When the buffer size of the packet goes beyond 40 MB, the packet captures are overwritten, that is, the packet capture will always provide information of the last packet capture done. This prevents disk space over utilization. You can capture two packets of 20 MB each. This log file is located at: `/opt/CUSP/dsnrs/log/packetcapture`. The Cisco Unified SIP Proxy administrator must download the latest packetcapture.zip file before starting the next packet capture request.

Step 3 To enable tracing on your system, check the **Enable Tracing** check box.

Step 4 Set the trace values for the following components (For details on the level to chose for each component, see Component Levels, on page 2):

- Base Tracing
- Routing
- Proxy-Core
- SIP-Wire-Log
- Normalization
- Proxy-Transactions
- SIP-Ping
- License-Mgmt
- Trigger-Conditions
- Accounting
- SIP-Search
- Config-Mgmt

Step 5 Click **Update** to save your changes.

Related Topics

Component Levels, on page 2

Component Levels

For each component, you can choose one of the following levels:

Component Levels

Level	Description
default	Uses the trace level of the parent.
debug	Logs messages of debug severity or higher.
info	Logs messages of info severity or higher.
warn	Logs messages of warning severity or higher.
error	Logs messages of error severity or higher.
fatal	Logs messages of fatal severity or higher.
off	Does not log messages.

Viewing the Cisco Unified SIP Proxy Log File

Procedure

Step 1 Choose **Troubleshoot** > **Cisco Unified SIP Proxy** > **Log File**.

The system displays the Cisco Unified SIP Proxy Trace Log File page and shows the contents of the trace log file.

Step 2 To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

Step 3 To save the trace log file information, do the following:

a) Click **Download Log File**.
b) Save the file to a convenient location.
c) Click **Close** when done.

Configuring Trace Settings

Use this procedure to enable traces, or debug message output, for components in the Cisco Unified SIP Proxy system. Components are entities and activities in the system. You can review the output by selecting **Troubleshoot > View > Trace Buffer**.

Restriction Enabling too many traces can adversely affect the system performance.

Procedure

Step 1 Choose **Troubleshoot** > **Traces**.

The system displays the Traces page, with a hierarchical listing of the system components.

Step 2 To enable a trace on a system component, check the check box next to the name of the component.

- To expand the list of components, click the + sign next to any upper-level component. To condense the list of components, click the - sign next to any upper-level component.
- Check the check box next to any upper-level component to enable the traces for all of the components under that component. Uncheck the check box next to any upper-level component to disable the traces for all of the components under that component.

Step 3 Click **Apply** to save your changes.

Step 4 Click **OK** in the confirmation window.

Related Topics

Viewing a Trace Buffer, on page 4

Viewing Tech Support Information

Procedure

Step 1 Choose **Troubleshoot** > **View** > **Tech Support**.

The system displays the Tech Support page and shows a collection of configuration data.

Step 2 To save the tech support information, click **Download Tech Support**.

Step 3 Save the file to a convenient location.

Step 4 Click **Close** when finished.

Viewing a Trace Buffer

Procedure

Step 1 Choose **Troubleshoot** > **View** > **Trace Buffer**.

The system displays the Trace Buffer page and shows the contents of the trace buffer.

Step 2 To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

Step 3 To save the trace buffer information, do the following:

a) Click **Download Trace Buffer**.
b) Save the file to a convenient location.
c) Click **Close** when done.

Step 4 To clear the trace buffer, do the following:

a) Click **Clear Trace Buffer**.
b) Click **OK** at the confirmation prompt.

Viewing a Log File

Procedure

Step 1 Choose **Troubleshoot** > **View** > **Log File**.

The system displays the Log File page and shows the contents of the log file.

Step 2 To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

Step 3 To save the log file, do the following:

a) Click **Download Log File**.
b) Save the file to a convenient location.
c) Click **Close** when done.

Enabling SIP Message Logging

Use the SIP message log to capture and troubleshoot SIP calls handled by Cisco Unified SIP Proxy. By default, the SIP message log is disabled. When the SIP message log is enabled, you can enter an optional expression to filter the messages that are stored.

Note If record-route is not configured for a network, the system does not display mid-dialog SIP messages in the SIP message log.

Caution Enabling the SIP message logging feature can have a significant performance impact on your system. We recommend that you limit the volume of calls processed by Cisco Unified SIP Proxy to less than 15 calls per second before you enable SIP message logging. We also recommend using the SIP message log filter whenever possible to limit the number of SIP messages that the system logs every second.

Procedure

Step 1 Choose **Troubleshoot** > **SIP Message Log** > **Controls**.

The system displays the SIP Message Logging page.

Step 2 Select if you want to enable or disable SIP message logging.

Step 3 (Optional) Enter a regular expression filter. This reduces the number of calls that are written to the SIP message log. An example of a regular expression filter is **999…1020**. If you enter this, the system will match any number beginning with 999 and ending with 1020. Only messages that match the regular expression will pass through the filter and be stored.

Step 4 Click **Update**.

Note In the event of a reload, the log control option in SIP message logging reverts to disabled state and the selected preferences are reset. The user needs to re-assign the preferences.

Searching SIP Message Calls

You can search the SIP message log for certain calls by entering search parameters. If you enter multiple search parameters, the system only returns values that match all the criteria. If you enter no parameters, the system returns all the calls.

There are many SIP messages within each call; if any individual SIP message matches the search criteria, the system displays that call in the search results.

Restriction The system returns a maximum of 500 calls. You can refine the results by entering more search parameters.

Procedure

Step 1 Choose **Troubleshoot** > **SIP Message Log** > **Search Calls**.

The system displays the SIP Message Log Search page.

Step 2 Enter data on which to search. See Data for Call Search, on page 6.

Step 3 Click **Search**.

The system refreshes the page and displays any calls that match the search criteria.

Step 4 To clear the SIP message log, click **Clear SIP Message Log**.

Step 5 To see more information about a call that the system returned, click it. The system displays the Call Log page with details about the call.

Data for Call Search

Data for Call Search

Field	Description
Called Party—The following parameters apply to the party initiating the call:	
Request-URI contains	Matches the supplied string against the SIP Request-URI field in each SIP message
Remote Party ID contains	Matches the supplied string against the SIP Remote Party-ID field in each SIP message
P-Asserted ID contains	Matches the supplied string against the SIP P-Asserted ID field in each SIP message
To header contains	Matches the supplied string against the SIP To Header field in each SIP message
Calling Party—The following parameters apply to the party receiving the call:	

Field	Description
From: header contains	Matches the supplied string against the SIP From Header field in each SIP message
Date and Time—The following parameters limit the search results to an inclusive window of time:	
Start Time	Calls before this time are excluded. **Note** If you enter a value in this field, it must include a time and not just a date. If you do not enter a time, the system returns nothing.
End Time	Calls after this time are excluded. **Note** If you enter a value in this field, it must include a time and not just a date. If you do not enter a time, the system returns nothing.

Viewing SIP Message Calls

The Call Log page displays the individual SIP messages that were processed by the Cisco Unified SIP Proxy during the dialog. It shows the time the message was handled and the direction relative to the Cisco Unified SIP Proxy.

Procedure

Step 1 Choose **Troubleshoot** > **SIP Message Log** > **Search Calls**.

The system displays the SIP Message Log Search page.

Step 2 Enter data on which to search. See Searching SIP Message Calls, on page 6.

Step 3 Click **Search**.

The system refreshes the page and displays any calls that match the search criteria.

Step 4 Click on any call.

The system displays the Call Log page with details about the call.

Related Topics

Searching SIP Message Calls, on page 6

Enabling the Failed Calls Log

Use the failed calls log to capture and troubleshoot calls that either fail during initial call setup or that do not terminate normally.

The failed calls log is disabled by default. After you enable it, the system automatically generates a log entry for call setup requests that result in a non-successful status. Similarly, calls that do not terminate properly, including calls exceeding the configured session timeout (when call admission control is enabled), will generate a failed calls log entry.

Note You enable the failed calls log independently from the SIP message log. If you want to review the SIP message details for a failed call, enable the SIP message log. See Enabling SIP Message Logging, on page 5.

Procedure

Step 1 Choose **Troubleshoot** > **Failed Calls Log** > **Controls**.

The system displays the Failed Call Logging page.

Step 2 Select **Enable** to enable the failed call log.

Step 3 If you want to include calls that failed due to license limitations, check **Log failed calls due to license limit**.

Step 4 Click **Update**.

Related Topics

Enabling SIP Message Logging, on page 5

Viewing the Failed Calls Log

Use the failed calls log to capture and troubleshoot calls that either fail during initial call setup or that do not terminate normally.

Procedure

Step 1 Choose **Troubleshoot** > **Failed Calls Log** > **Search Calls**.

The system displays the Failed Calls Log page and shows the contents of the log file.

Step 2 To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

Step 3 To see a different number of failed calls on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, or 100 failed calls.

Step 4 To clear the log, click **Clear All Calls**.

Viewing the History of a Failed Call

Procedure

Step 1 Choose **Troubleshoot** > **Failed Calls Log**.

The system displays the Failed Calls Log page and shows the contents of the log file.

Step 2 To see more information about a particular failed call, click the underlined call ID.

The system displays the Failed Call Session History page containing more information about the call.