Enable and Collect Trace Logs in Cisco Unified SIP Proxy (CUSP)

Contents

[Introduction](#)
[Enable Trace Logs](#)
[From the GUI](#)
[From the CLI](#)
[Trace Log Collection](#)
[From the GUI](#)
[From the CLI](#)
[From the Public File System (PFS)](#)
[SIP Message Logging](#)
[Log Storage Information](#)
[CUSP 9.0 and Later](#)
[CUSP Versions Earlier than 9.0](#)
[Log collection on CUSP Version 10.2.1](#)
[Related Information](#)

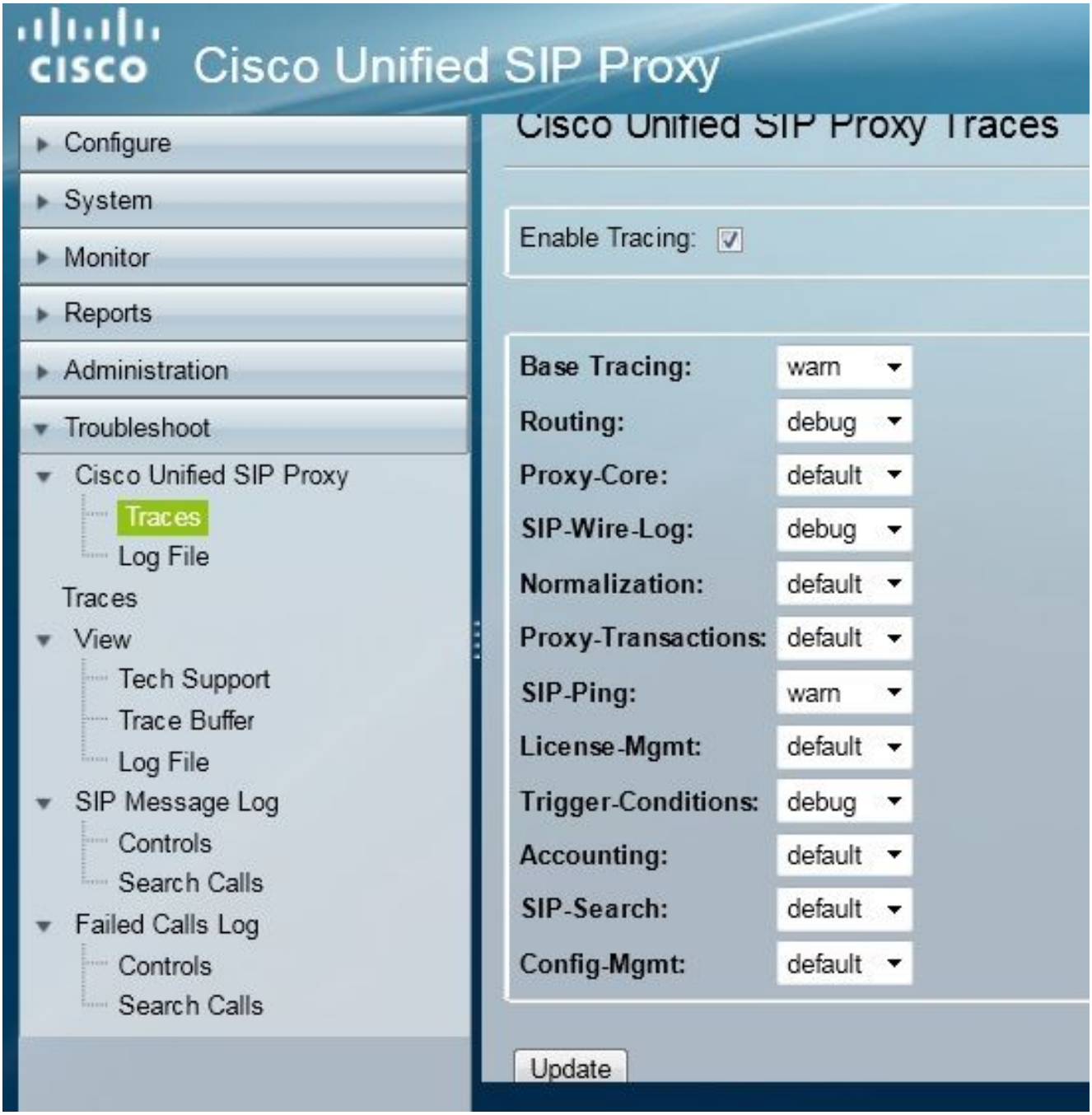
Introduction

This document describes the various options available in Cisco Unified SIP Proxy (CUSP) to enable and collect trace logs. Traces can be enabled and collected either from the GUI or the CLI. This document explains each procedure in detail.

Enable Trace Logs

From the GUI

1. Log into the CUSP GUI (http://<IP Address of CUSP Module>/).
2. Navigate to **Troubleshoot < Traces**.



3. Check the **Enable Tracing** box, and then select the required component(s) to troubleshoot the issue and set the level to debug.
4. Click **Update** after you make the required changes.

From the CLI

1. Access the CUSP module and go to the CUSP mode.

```
Router#service-module sM 2/0 session
Trying 10.106.122.8, 2131 ... Open
CUSP# cusp
CUSP(cusp)#
```

2. In order to enable tracing, execute the **trace enable** command:

```
CUSP(cusp)# trace enable
```

3. Select the required CUSP component and set the trace level to debug.

```
MyCUSP-9(cusp)# trace level debug component ?
  routing              Routing component
  proxy-core           Proxy Core Component
  sip-wire-log         SIP Wire Log Component
  normalization        Normalization Component
  proxy-transactions   Proxy Transaction Layer Component
  sip-ping             Servergroup SIP Ping Component
  license-mgmt         License Management Component
  trigger-conditions   Trigger Conditions Component
  accounting           Accounting Component
  sip-search           SIP Search/Forking Component
  config-mgmt          Configuration Management Component
```

4. You need to repeat the previous command in order to enable debug for multiple components.

5. You can view the current trace setting with the **show trace options** command.

```
MyCUSP-9(cusp)# show trace options
Trace is enabled.

Category                                                    Level
root                                                        warn
sip-wire-log                                                debug
sip-ping                                                    warn
MyCUSP-9(cusp)#
```

Trace Log Collection

From the GUI

1. Log into the CUSP GUI.

2. Navigate to **Troubleshoot > Log File**. This displays the collected logs. You can either view or download the file.

Note: CUSP Version 8.5(5) and later provide the option to clear the log buffer from GUI. If the CUSP version is earlier than Version 8.5(5), the logs must be cleared manually with the CLI.

3. In order to clear the logs with the CLI, enter this command:

```
CUSP(cusp)# clear trace log
```

From the CLI

1. Use this command in order display the content of log:

```
MyCUSP-9(cusp)# show trace log ?
  tail              Tail the log
  <1-100000>        Dump specified number of lines from end of log
  <cr>
  |                 Pipe output to another command
```

2. Press **CTRL+C** in order to break the scrolling.
3. Use the **show trace log | p command** in order to show the trace output page-by-page**.**

From the Public File System (PFS)

There is another way to collect the trace logs. This is from the PFS, which is the file system on which CUSP runs. PFS can be accessed with FTP.

1. Create a username and assign the PFS privilege to this user.

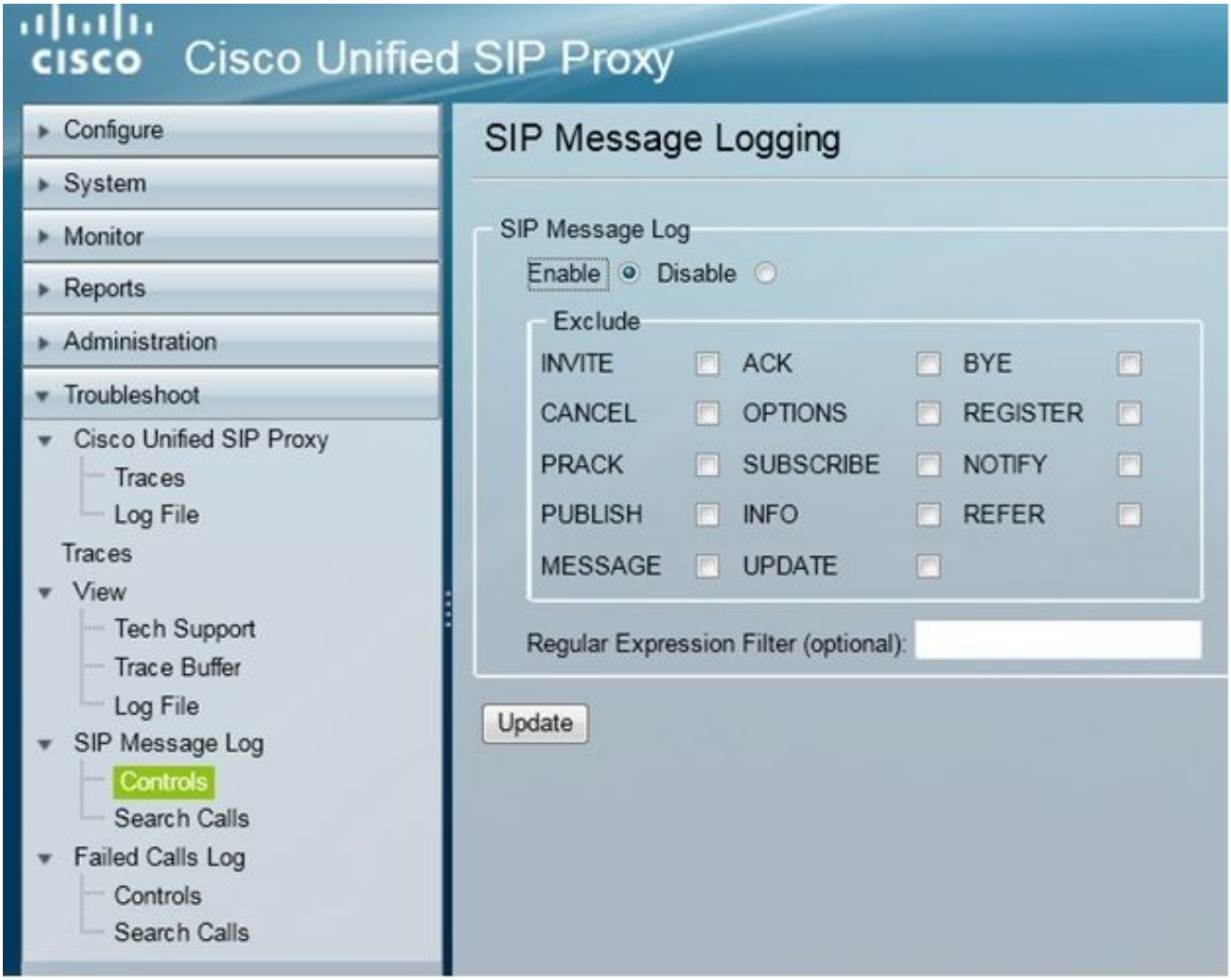
```
MyCUSP-9# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MyCUSP-9(config)# username cisco create
MyCUSP-9(config)# exit
MyCUSP-9# username cisco password cisco
MyCUSP-9# username cisco group pfs-privusers
MyCUSP-9#
```

2. Access this URL with the credentials defined in the previous step. You can download **.log** files that contain the trace log. ftp://<IP of CUSP>/cusp/log/trace/

SIP Message Logging

Apart from the trace logs mentioned in the previous sections, Session Initiation Protocol (SIP) message logs are also available in CUSP. This log only shows the SIP messages that come into and go out from the CUSP. You can enable SIP message logs from the GUI.

1. Navigate to **Troubleshoot > SIP Message Logs > Controls**.



2. In order to view the SIP message logs, navigate to **Troubleshoot > SIP Message Logs > Search Calls**.

   Note: In order to view how CUSP processes the SIP methods, such as the route tables and normalization, trace logs are required.

Log Storage Information

CUSP 9.0 and Later

In CUSP Version 9 (Virtual CUSP) and later, the log buffer size can be increased up to 5 GB. In this version, you can provision disk space in order to store logs and the number of log files.

Here is the configuration that sets the log size to 5 GB and the file count to 500.

```
MyCUSP-9# cusp
MyCUSP-9(cusp)# trace logsize 5000 filecount 500
MyCUSP-9(cusp)#
MyCUSP-9(cusp)# show trace size

Configured Log Size: 5000
Configured file Count: 500

Default Log Size is 200MB and File Count is 20

MyCUSP-9(cusp)#
```

Cisco recommends that each log file must be 10 MB for better performance.

CUSP Versions Earlier than 9.0

In older versions of CUSP, the log buffer size is set to 200MB, In CUSP 8.5.8 and later you can use the trace logsize command to increase it to up to 5Gb:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel8_5/cli_commands/cli_commands/cusp_exec_cmds.html#63802

Log collection on CUSP Version 10.2.1

On version 10.2.1, there is a software limitation with the log rotation.
New logs are not written if the buffer gets full on CUSP version 10.2.1.
Cisco bug ID CSCvs47162 Refer 10.2.1v1 Release Notes for this defect fix.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel10_2/releasenotes/cusprn102.html#Cisco_Concept.dita_4e7c4d6b-10ed-4bcf-901c-019500ba20c7

This issue has been fixed on 10.2.1 v1 or later patches.

Once the upgrade is done to v1 or later version, to collect the latest logs use CLI or GUI only, as the SFTP (PFS user) does not reflect in the latest logs.

Collecting Logs through CLI:

1. Use the command "show logs" to show latest log files

```
se-10-65-105-44# show logs
     SIZE            LAST_MODIFIED_TIME                    NAME
    26552   Wed Aug 17 01:19:01 IST 2022              atrace.log
        0   Tue Mar 22 15:55:16 IST 2022           pmessages.log
        0   Mon Mar 07 11:19:04 IST 2022                yum.log
   100618   Wed Aug 17 01:16:46 IST 2022                dmesg
    14741   Wed Aug 17 01:16:55 IST 2022              boot.log
  2078001   Mon Sep 05 13:32:34 IST 2022          messages.log
```

2. Copy the file to a SFTP server

```
CUSP# copy log <logfilename> url sftp://<username>:<password>@<ftphost>/path/to/filename
```

Collecting Logs through GUI:

CUSP GUI: Troubleshoot > Cisco Unified SIP Proxy > Log File > Download Log File

If the user installs a new vCUSP and upgardes to version 10.2.1v1 or later before the buffer is full, logs can be collected through any log collection mechanism and the issue is never encountered.

Related Information

- **CUSP Configuration Example**
- **Technical Support & Documentation - Cisco Systems**