Set Traces and Collect Logs in CCE

Contents

Introduction

This document describes how to set and collectt traces in Cisco Unified Contact Center Enterprise (CCE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Contact Center Enterprise (UCCE)
- Package Contact Center Enterprise (PCCE)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco Virtualized Voice Browser (VVB)
- Cisco Unified Border Element (CUBE)

- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Session Initiation Protocol (SIP) Proxy (CUSP)

Components Used

The information in this document is based on these software versions:

- Cisco Finesse Release 12.5
- CVP Server Release 12.5
- UCCE/PCCE Release 12.5
- Cisco VVB Release 12.5
- CUIC Release 12.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

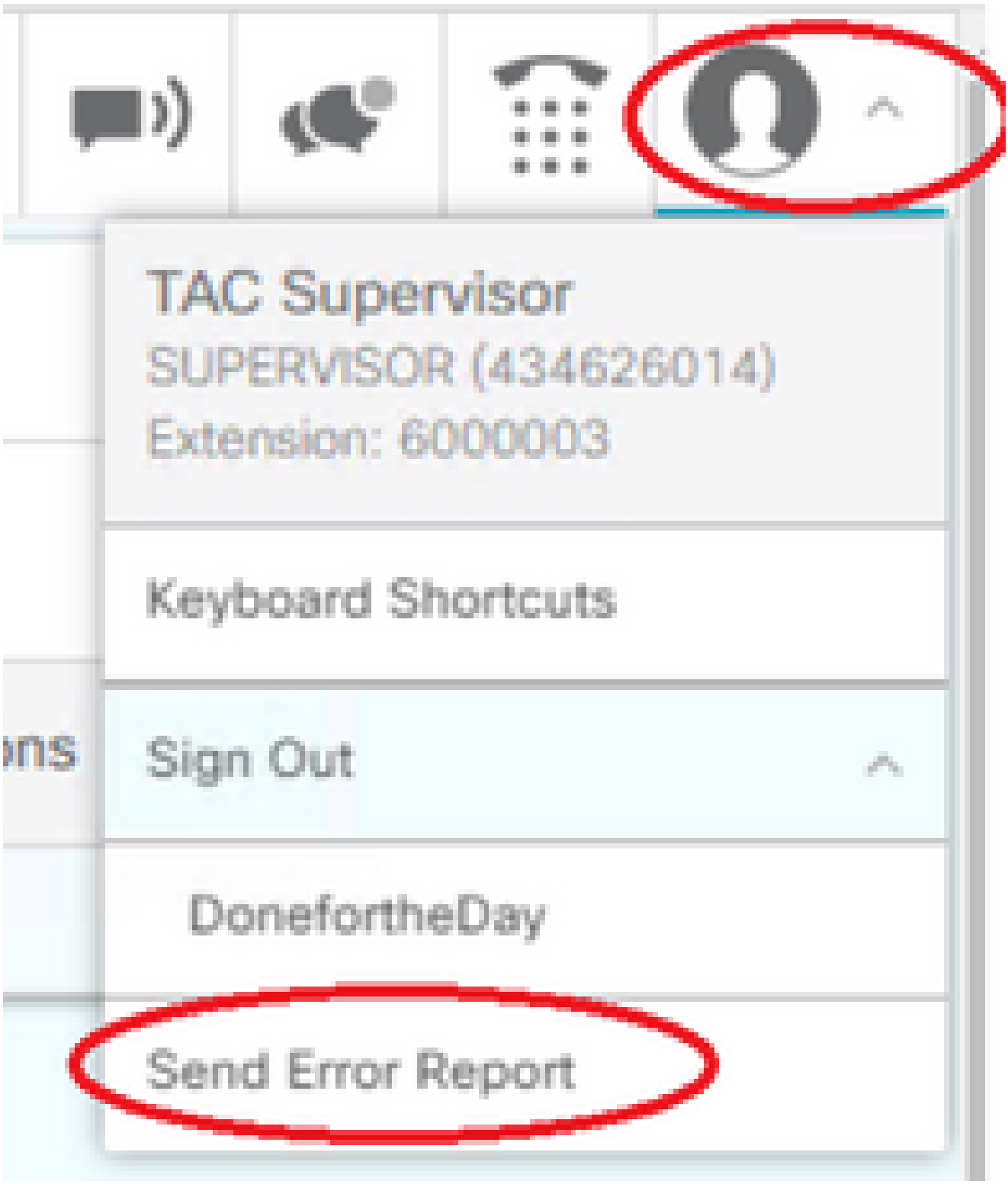
Set Traces and Collect Finesse Logs

Finesse Client

There are several options to collect Finesse client logs.

Option 1: Collect Client Logs Through the Send Error Report.

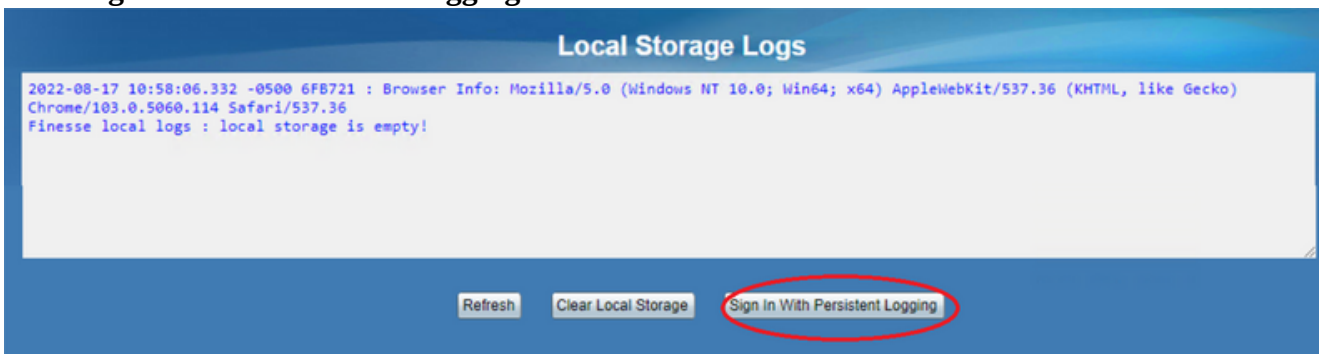
1. Log an agent in.
2. If an agent experiences any problem during a call or media event, instruct the agent to click the **Send Error Report** link on the top right-hand corner of the finesse desktop.



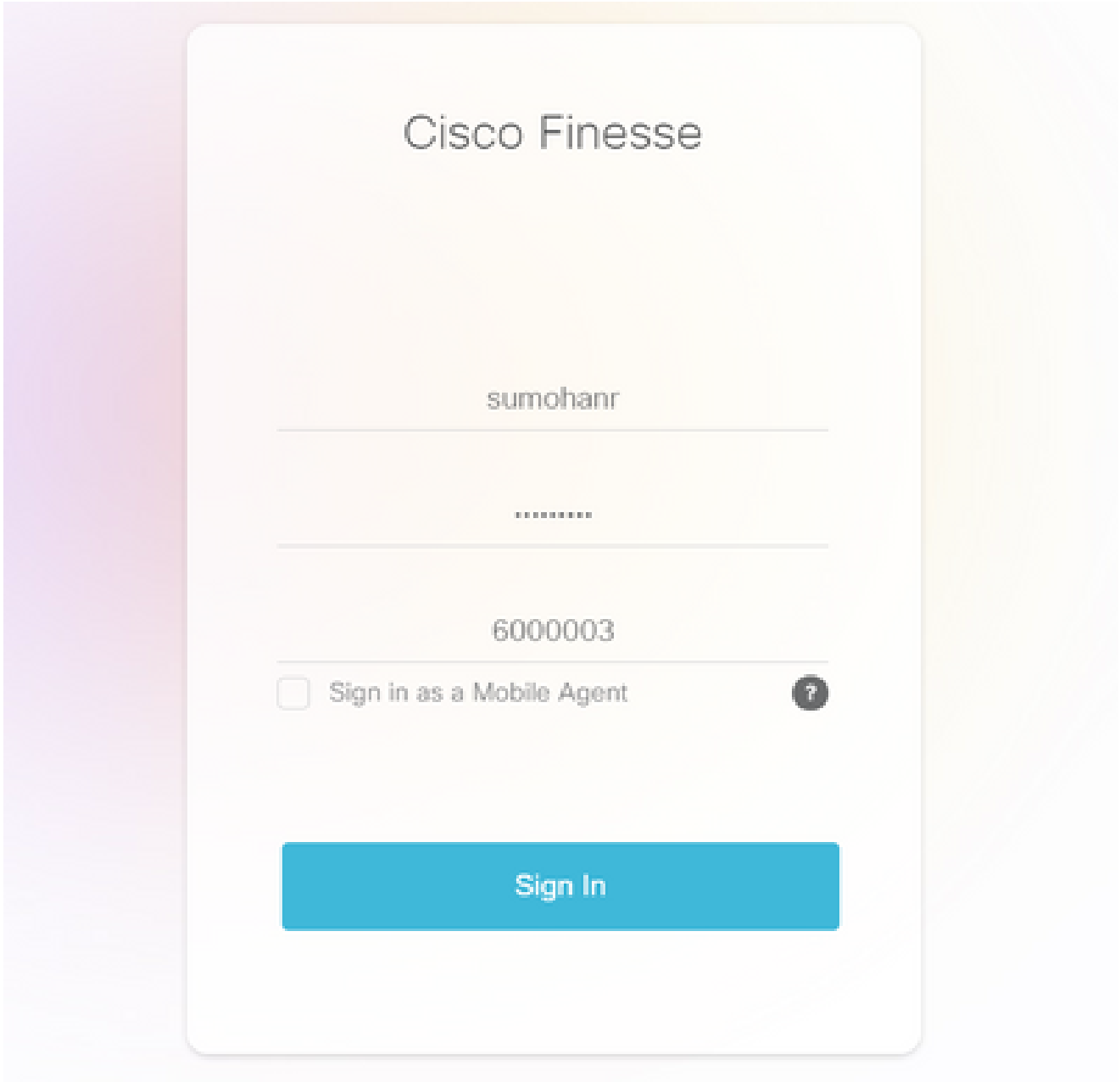
3. The agent sees the **Logs Successfully Sent!** message.
4. The client logs are sent to the Finesse server. Navigate to **https://x.x.x.x/finesse/logs** and log in with an administration account.
5. Collect the logs under the **clientlogs/** directory.

Option 2: Set Persistent Logging

1. Navigate to https://x.x.x.x:8445/desktop/locallog.
2. Click **Sign In With Persistent Logging**.



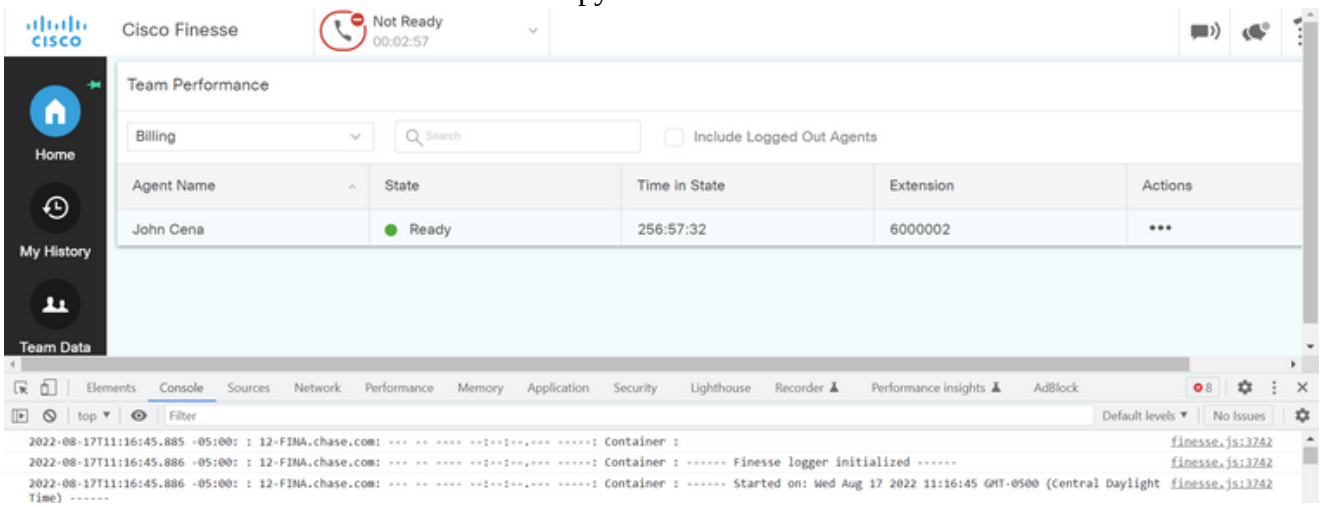
3. The Cisco Finesse agent desktop login page opens. Log the agent in.



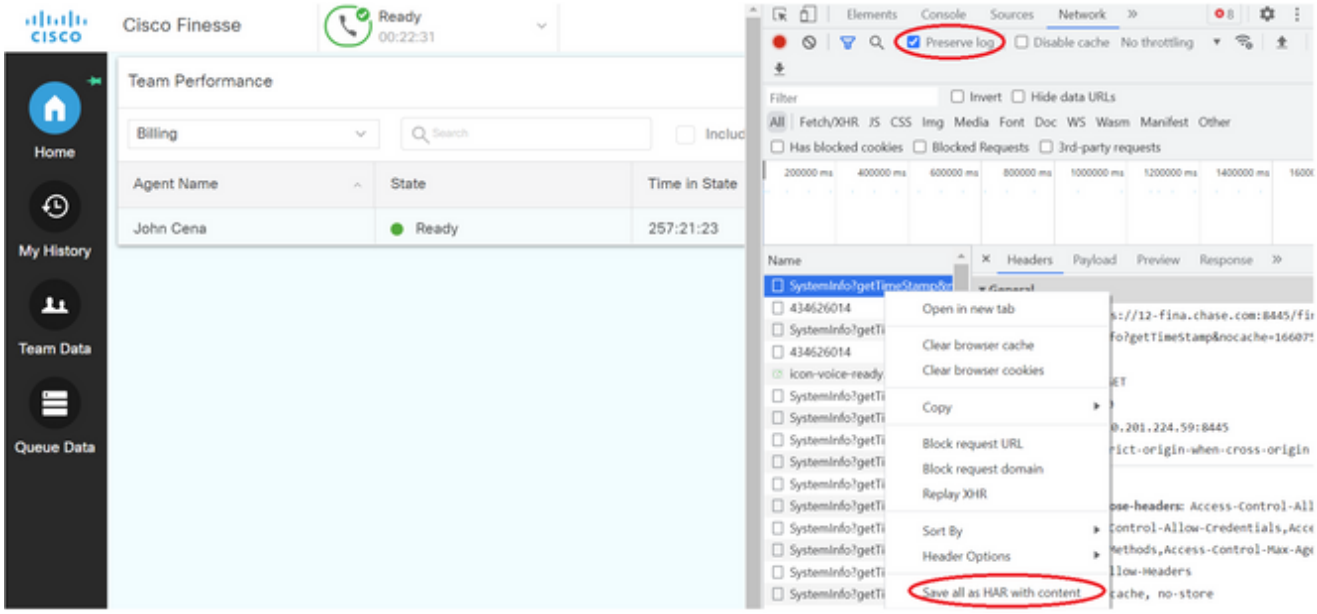
4. All the agent desktop interaction is registered and sent to the local storage logs. To collect the logs, navigate to **https://x.x.x.x:8445/desktop/locallog** and copy the content into a text file. Save the file for further analysis.

Option 3: Web Browser Console

1. After an agent logs in, press **F12** to open the browser console.
2. Select the **Console** tab.
3. Check the browser console for the errors. Copy the content into a text file and save it.



4. Select the **Network** tab, and check the Preserve log option.
5. Right-click any of the netwok name events and select **Save** as HAR with content.



Finesse Server

Option 1: Via the User Interface (UI) - Web Services (required) and additional logs

1. Navigate to **https://x.x.x.x/finesse/logs** and log in with the administration account.
2. Expand the directory **webservices/**

3. Collect the last web service logs. Select the last unzip file. For Instance, **Desktop-Webservices.201X-..log.zip**. Click the file link and you see the option to save the file.

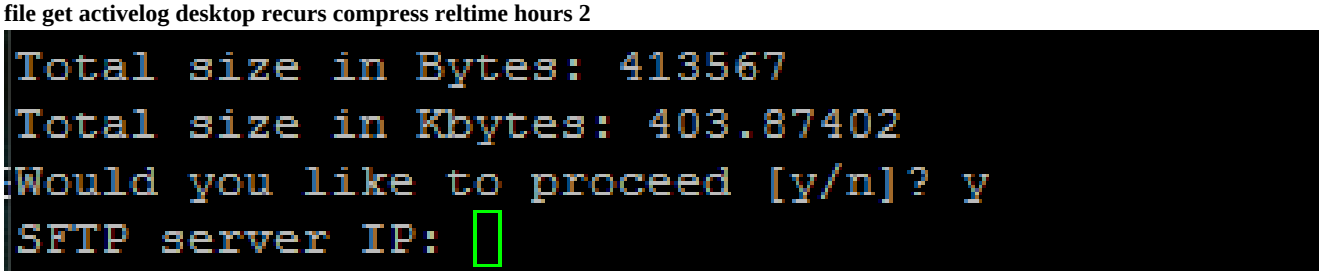
4. Collect the other required logs (depends on the scenario). For instance, openfire for notification service issues, realm logs for authentication issue and tomcatlogs for APIs issues.

Note: The recommended method to collect the Cisco Finesse server logs is via Secure Shell (SSH) and Secure File Transfer Protocol (SFTP). This method does not only allow you to collect the webservices logs but all additional logs like, Fippa, openfire, Realm, and Clientlogs.

Option 2: Via SSH and Secure File Transfer Protocol (SFTP) - Recommended Option

1. Log in to the Finesse server with the SSH.
2. Enter this command in order to collect the logs you need. The command collects the logs for 2 hours. You are prompted to identify SFTP server where the logs are uploaded.

file get activelog desktop recurs compress reltime hours 2



3. These logs are stored on the SFTP server path: <IP address>\<date time stamp>\active_nnn.tgz , where nnn is timestamp in long format.
4. To collect additional logs like tomcat, Context service, Servm and install logs, look at the Log Collection section of the Cisco Finesse Administration Guide Release 12.5(1).

Set Traces and Collect CVP and CVVB Logs

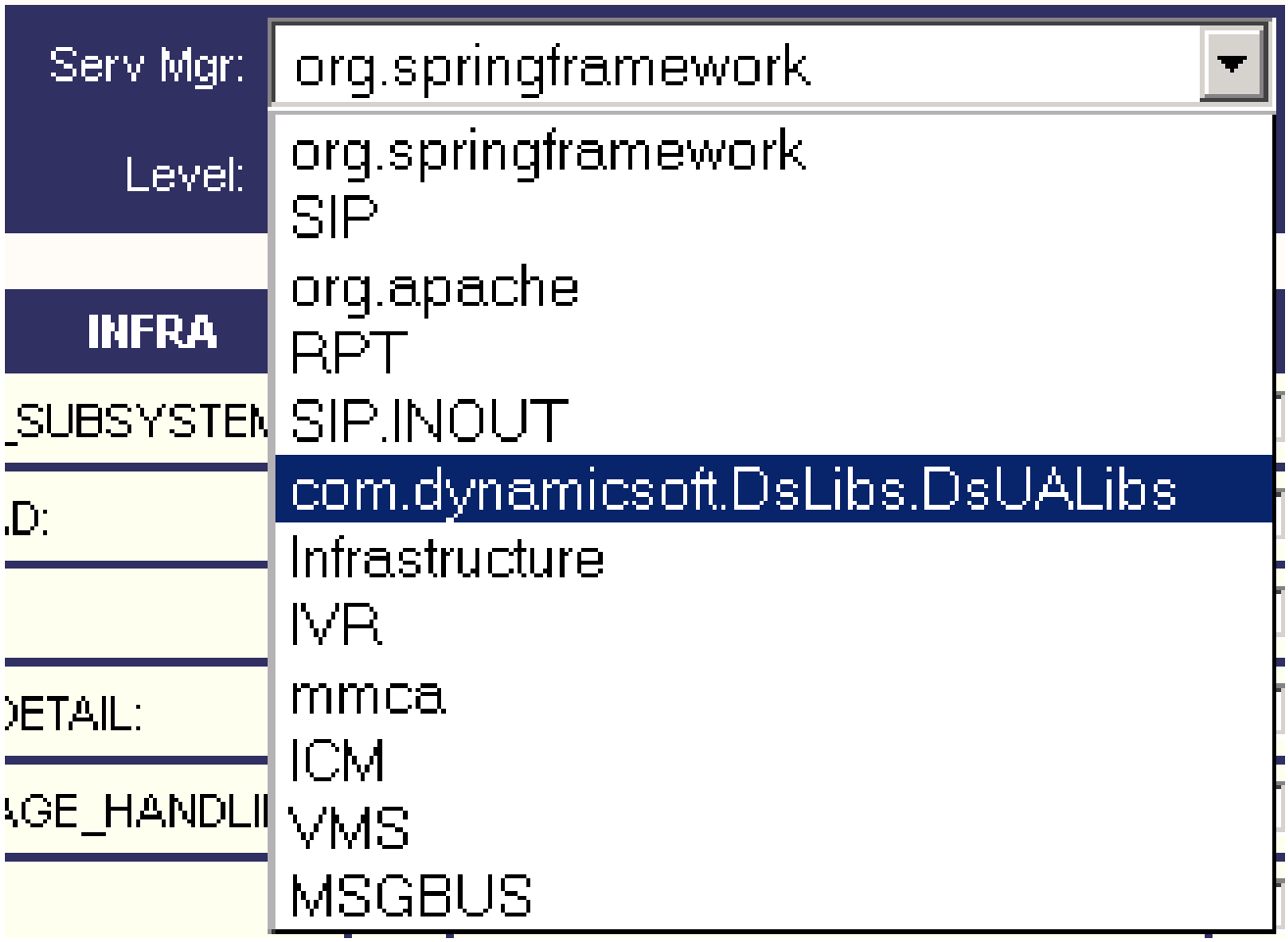
CVP Call Server

1. The CVP CallServer default level of traces is enough to troubleshoot most of the cases. However, when you need to get more detail on the Session Initiation Protocol (SIP) messages, you need to set the SIP strack traces to the DEBUG level.
2. Navigate to the CVP CallServer Diag webpage URL http:/localhost:8000/cvp/diag.

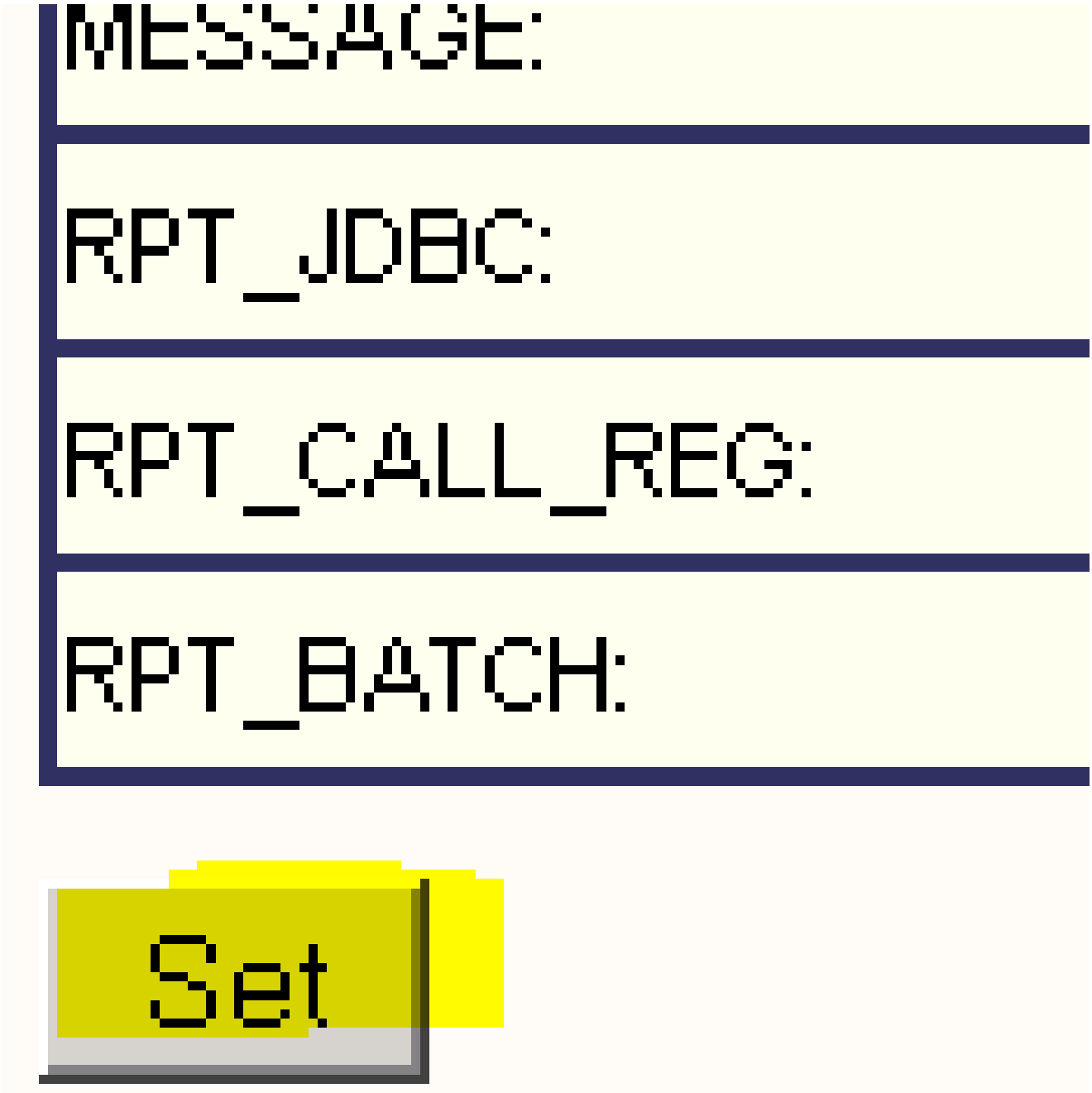
Note: This page provides good information about the CVP CallServer and it is very useful to troubleshoot certain scenarios.

---

3. Select **com.dynamicsoft.DsLibs.DsUALibs** from the **Serv. Mgr** dropdown menu at the top left-hand corner



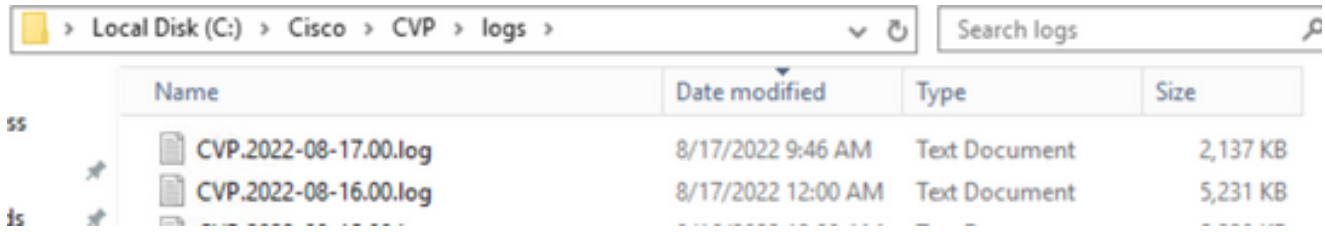
4. Click the **Set** button.



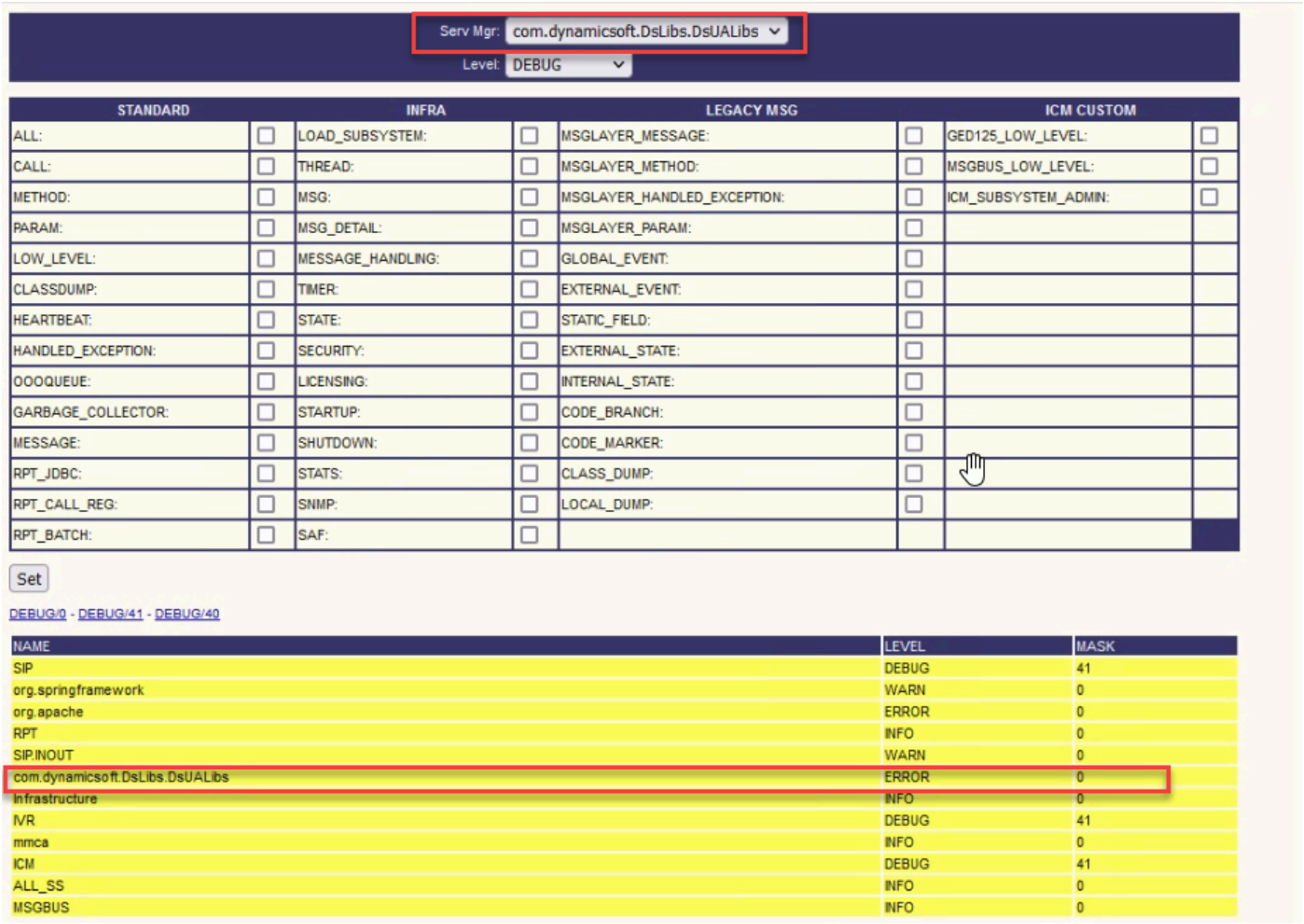
5. Scroll down in the trace window in order to ensure that the level of traces has been set correctly. These are your debug settings.

NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
SIP.INOUT	WARN	0
com.dynamicsoft.DsLibs.DsUALibs	DEBUG	0
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
MSGBUS	INFO	0

6. When you reproduce the problem, collect the logs from **C:\Cisco\CVP\logs** and select the CVP log file based on the time the problem occurred.



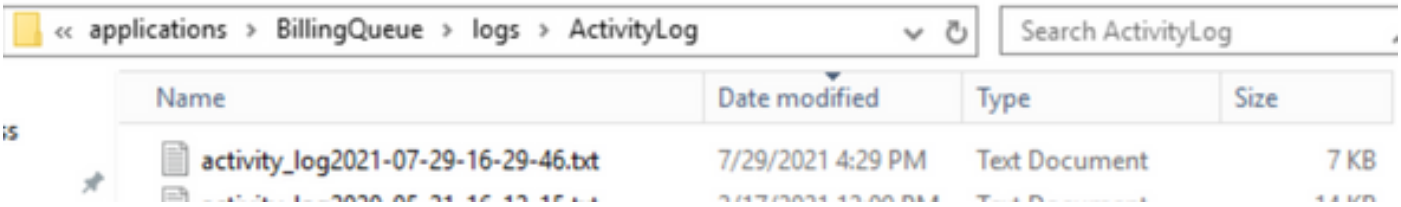
7. After you reproduce the problem, ensure to restore the traces to the default level. Select **com.dynamicsoft.DsLibs.DsUALibs** from the **Serv. Mgr** dropdown menu at the top left-hand corner and set it to error.



CVP Voice XML (VXML) Application

In very rare circumstances you need to increase the level of traces of the VXML server applications. On the other hand, it is not recommended to increase it unless a Cisco Engineer requests it.

To collect the VXML server application logs, navigate to the specific application directory under the VXML server, for example: **C:\Cisco\CVP\VXMLServer\applications\{name of application}\logs\ActivityLog** and collect the activity logs.



CVP Operations and Administration Management Portal (OAMP)

In most of the cases the default level of traces of OAMP and ORM are enough to determine the root cause of the problem. However, if the level of traces is required to be increased, here are the steps to execute this action:

1. Backup **%CVP_HOME%\conf\oamp.properties**
2. Edit **%CVP_HOME%\conf\oamp.properties**

```
omgr.traceMask=-1
omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERROR
net.sf.ehcache.logLevel=ERROR
```

3. Restart OPSConsoleServer after the modification as shown.

Trace Level Information

Trace Level	Description	Log Level	Trace Mask
0	Product install default. No or minimal performance impact expected.	INFO	None
1	Less detailed trace messages with a small performance impact.	DEBUG	DEVICE_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x01011000
2	Detailed trace messages with a medium performance impact.	DEBUG	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x05011000
3	Detailed trace message with a high performance impact.	DEBUG	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + DATABASE_MODIFY + MANAGEMENT=0x05111000

Trace Level	Description	Log Level	Trace Mask
4	Detailed trace message with a very high performance impact.	DEBUG	MISC + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + MANAGEMENT + TRACE_METHOD + TRACE_PARAM=0x17371000
5	Highest detailed trace message.	DEBUG	MISC + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + MANAGEMENT + TRACE_METHOD + TRACE_PARAM=0x17371006

Cisco Virtualized Voice Browser (CVVB)

In CVVB, a trace file is a log file that records activity from the Cisco VVB component subsystems and steps.

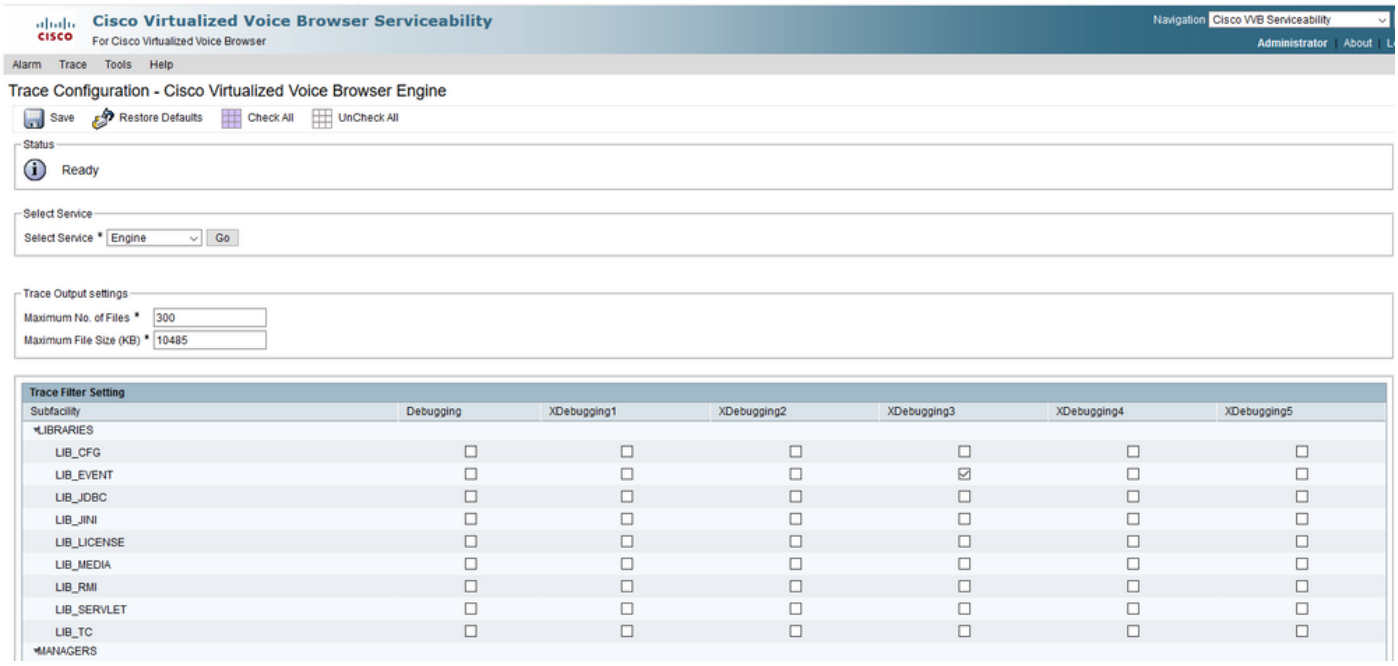
Cisco VVB has two main components:

- Cisco VVB “Administration” traces termed as MADM logs
- Cisco VVB “Engine” traces termed as MIVR logs

You can specify the components for which you want to collect information and the level of information that you want to collect.

Log Levels extend from:

- Debugging – Basic flow details to
- XDebugging 5 – Detailed level with Stack Trace



Warning: Xdebugging5 must not be enabled on production loaded system.

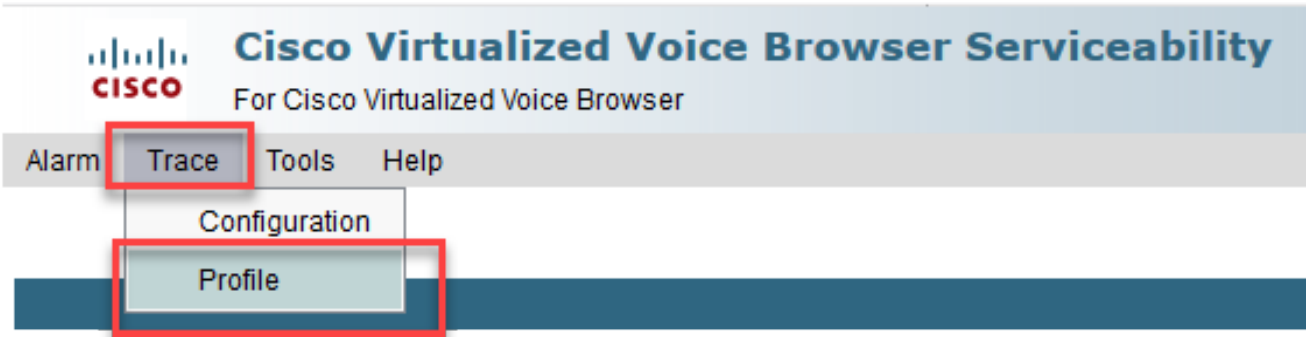
The most common logs that you need to collect are the Engine. The default level of traces for the CVVB Engine traces is enough to troubleshoot most issues. However, if you need to change the level of traces for a specific scenario, Cisco recommends that you use the pre-defined System Log Profiles.

System Log Profiles

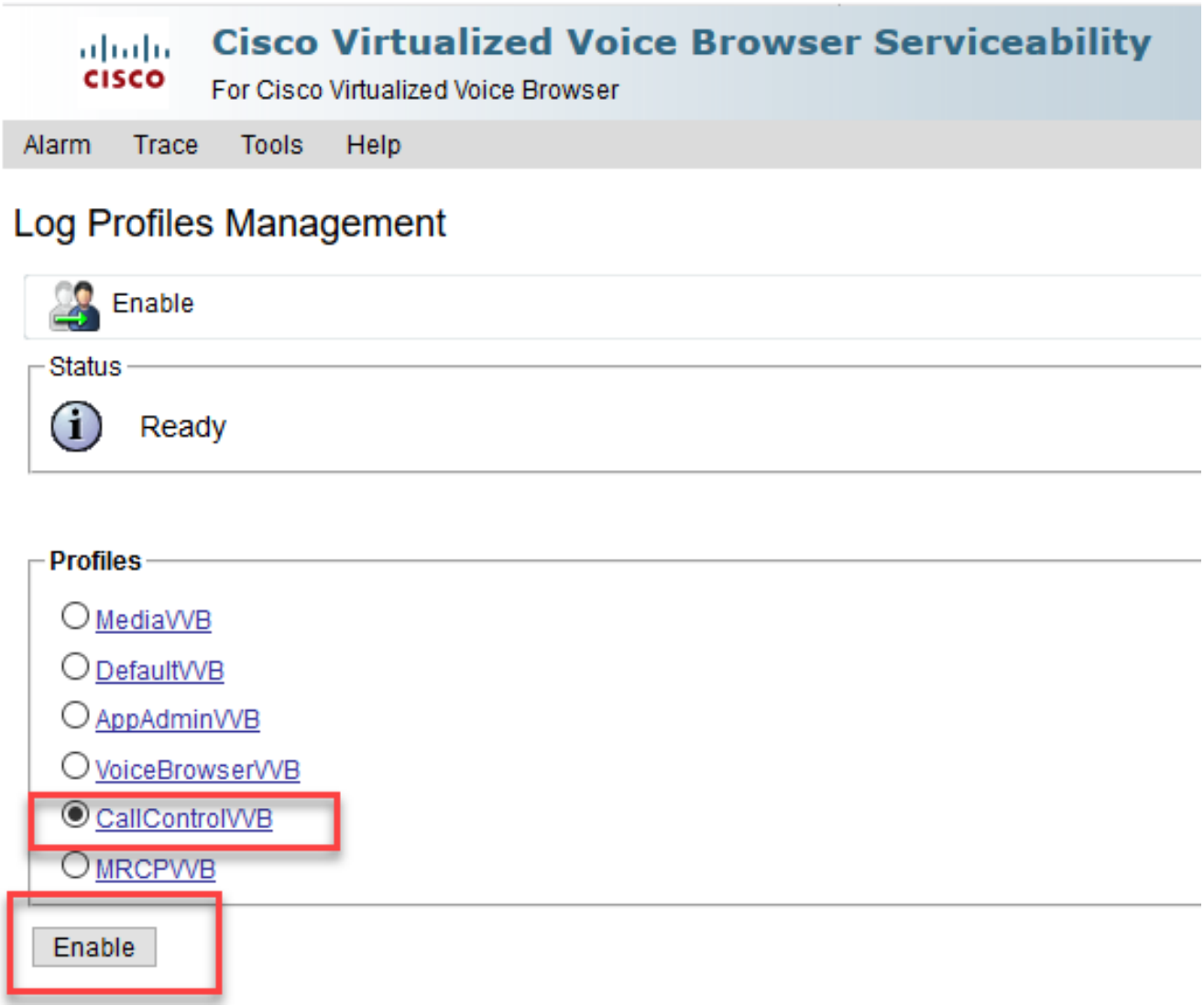
Name	**Scenario in which this profile must be activated**
DefaultVVB	Generic logs are enabled.
AppAdminVVB	For issues with web administration through AppAdmin, Cisco VVB Serviceability, and other web pages.
MediaVVB	For issues with media setup or media transmission.
VoiceBrowserVVB	For issues with calls handle.
MRCPVVB	For issues with ASR/TTS with Cisco VVB interaction.
CallControlVVB	For issues with SIP signal related are published in the log.

1. Open the CVVB main page (https://X.X.X.X/uccxservice/main.htm), and navigate to the Cisco VVB Serviceability page. Log in with the administration account

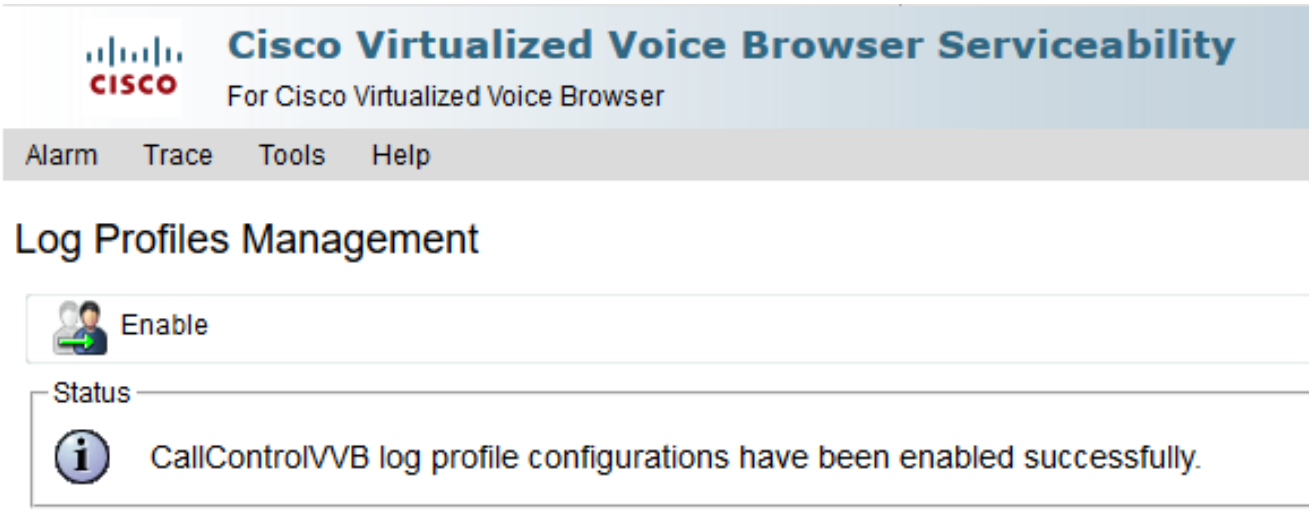
2. Select **Trace -> Profile.**



3. Check the profile that you want to enable for the specific scenario and click the **Enable** button. For example enable the profile CallControlVVB for SIP related issues or MRCPVVB for issues related to Automatic Speech Recognition and Text to Speech (ASR/TTS) interaction.

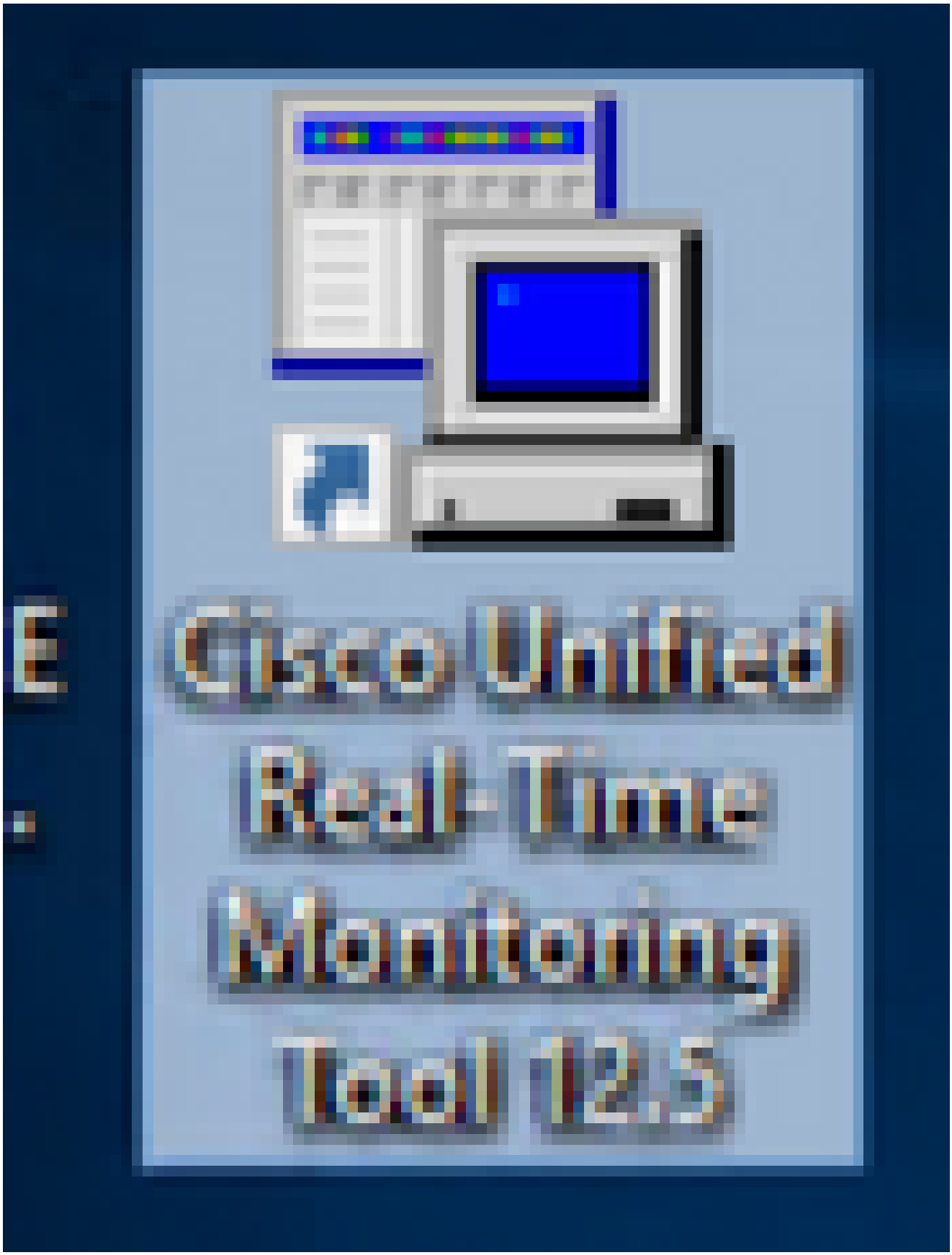


4. You see the succesful message after you click the enable button.

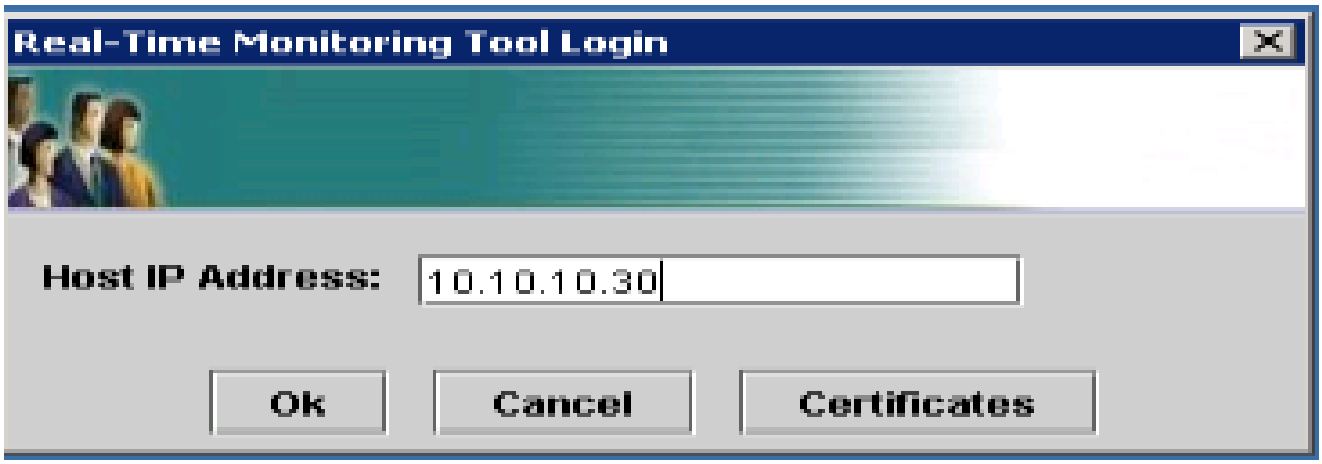


5. After the problem is reproduced, collect the logs. Use the Real Time Monitor Tool (RTMT) that comes with the CVVB to collect the logs.

6. Click on the Cisco Unified Real-Time Monitoring Tool icon on your Desktop (if needed, download this tool from the CVVB).

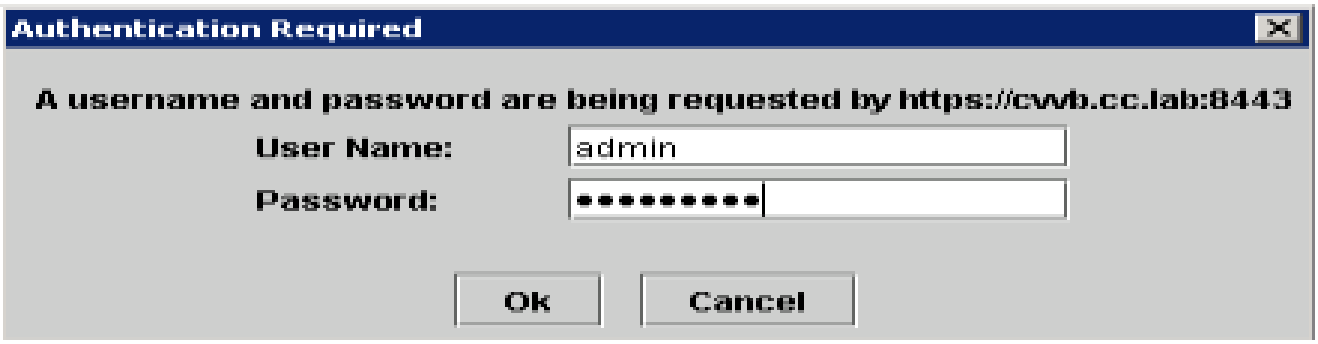


7. Provide the IP address of the VVB and click **OK**.



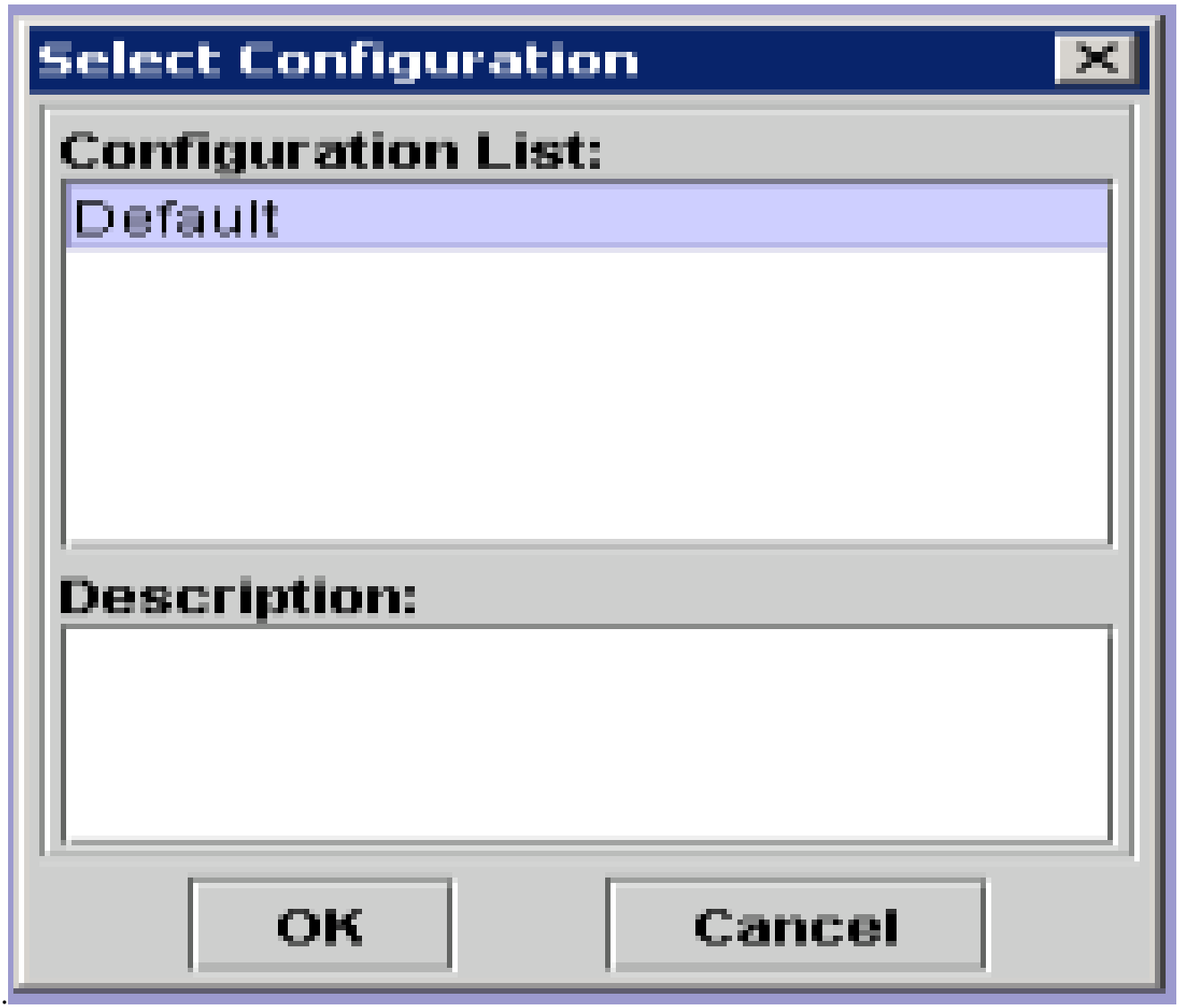
8. Accept the Certificate information if displayed

9. Provide the credential and click **OK**.

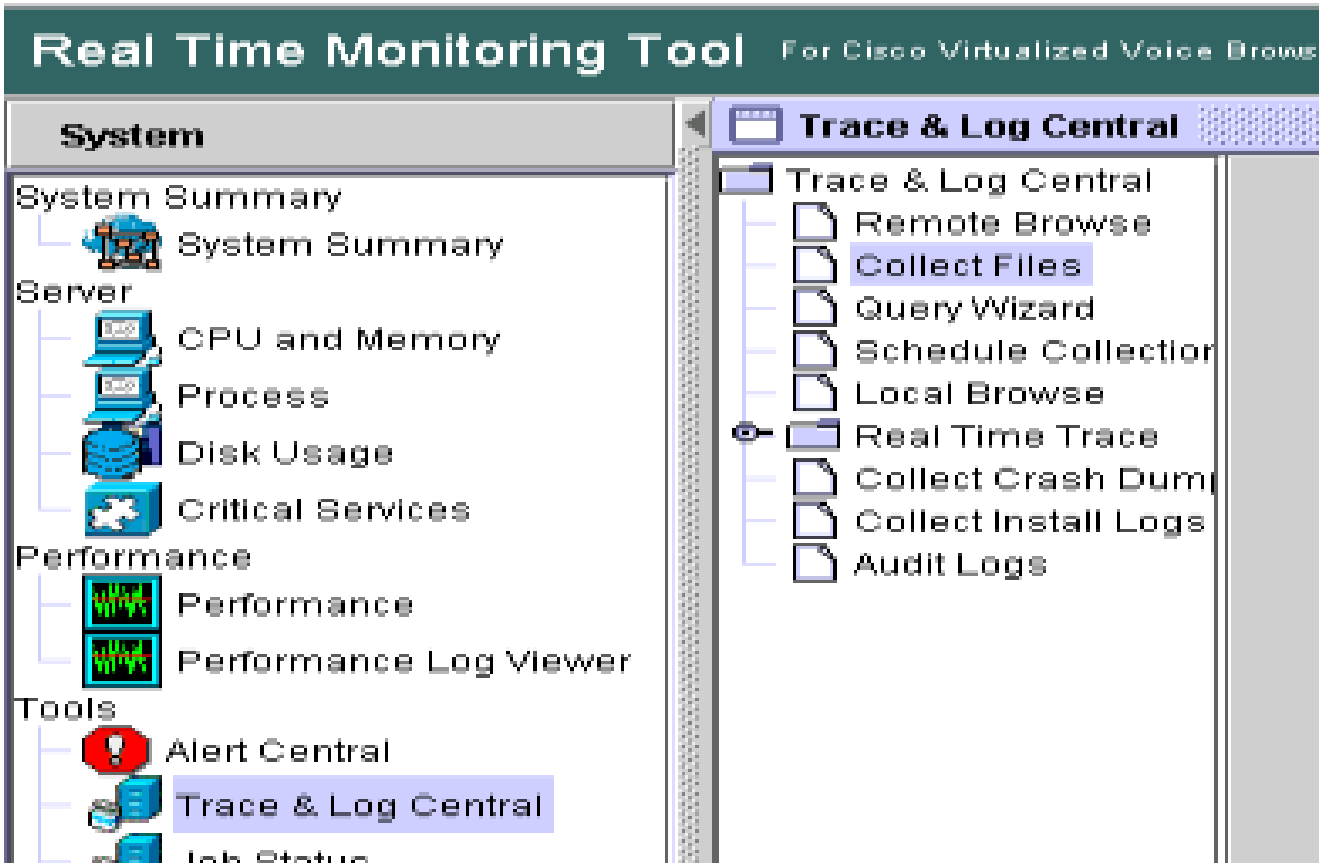


10. If you received the TimeZone error, RTMT can close after you click on the **Yes** button. Please relaunch the RTMT tool.

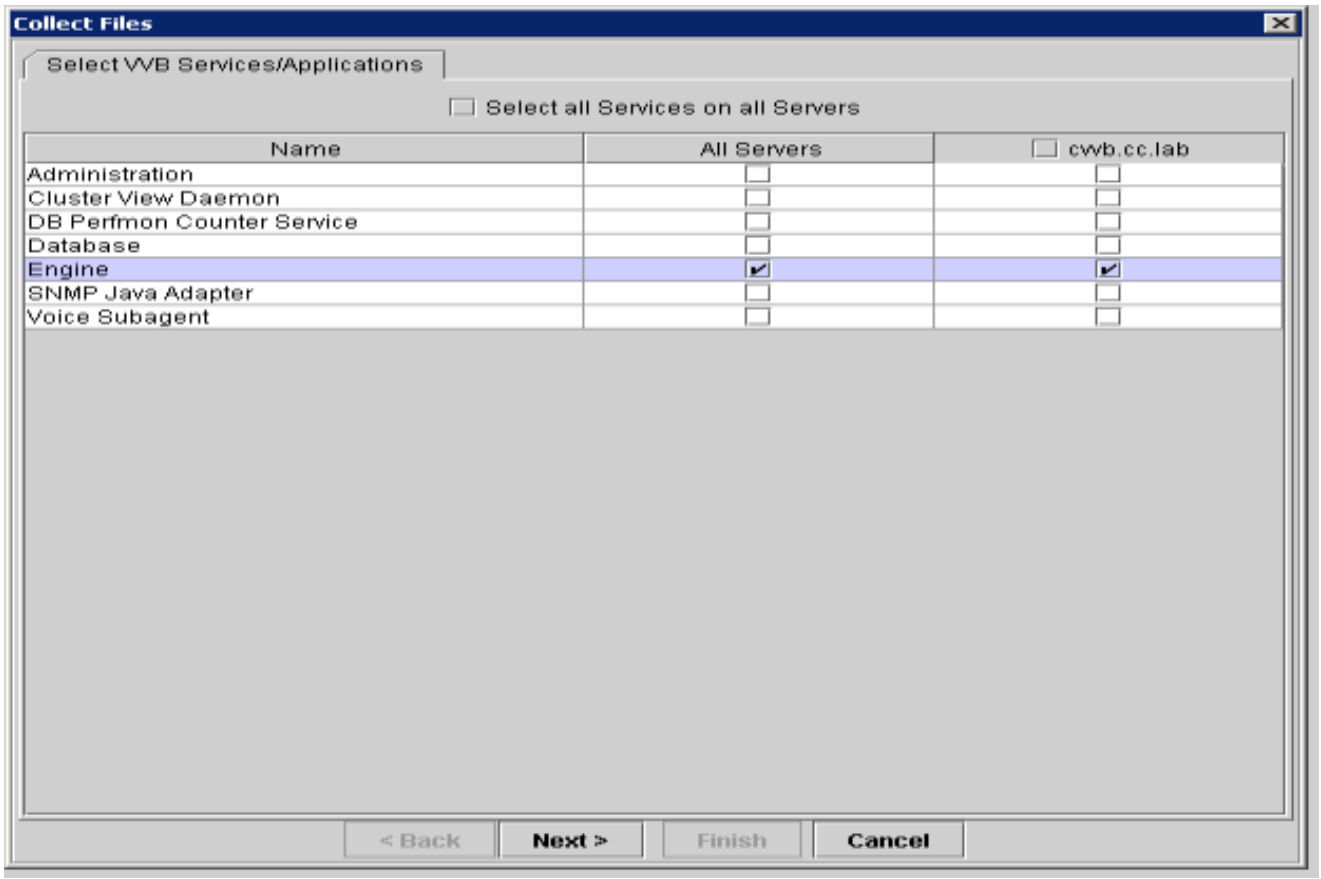
11. Leave the Default configuration selected and click on **OK**.



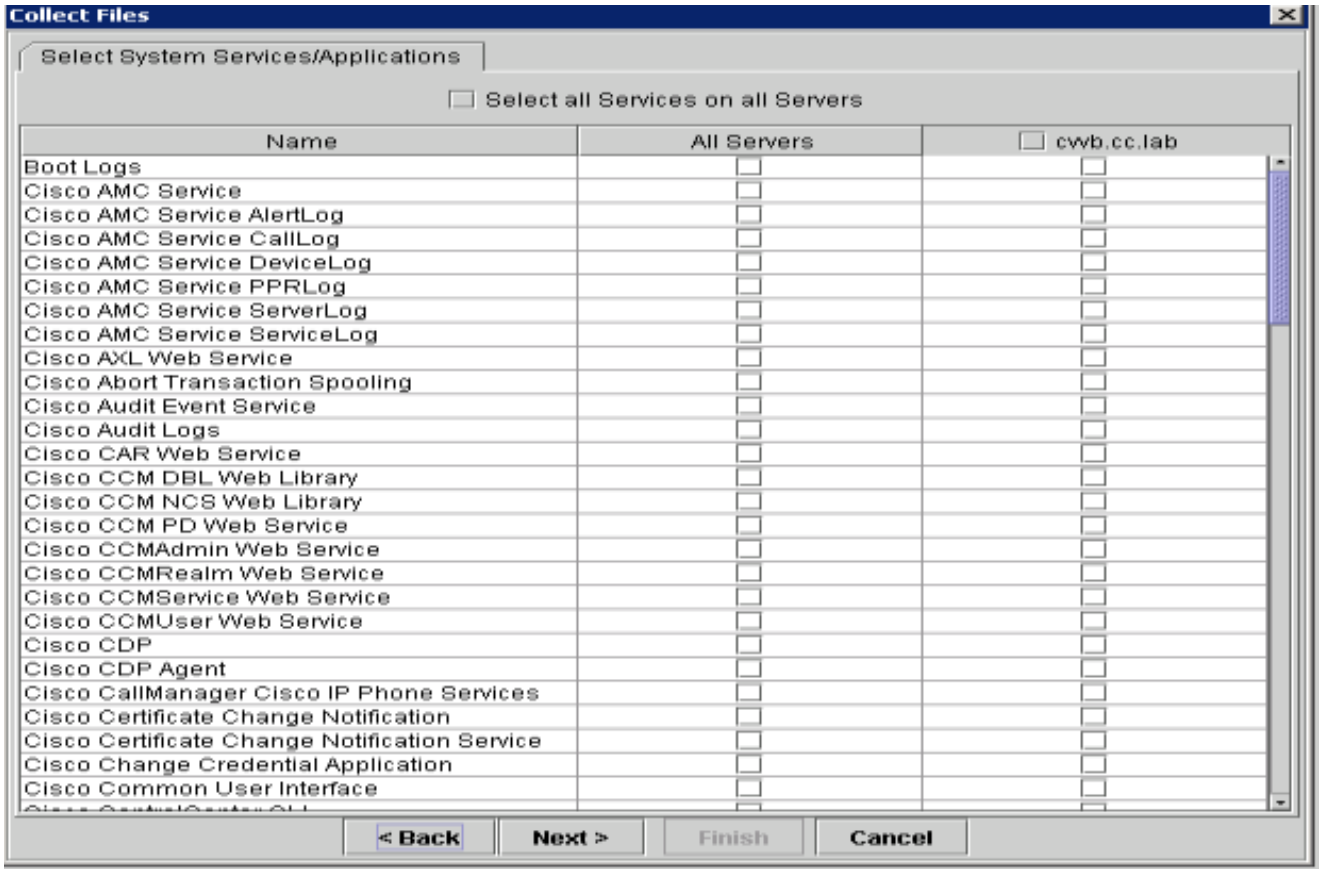
12. Select **Trace & Log Central** and then double click on **Collect Files**.



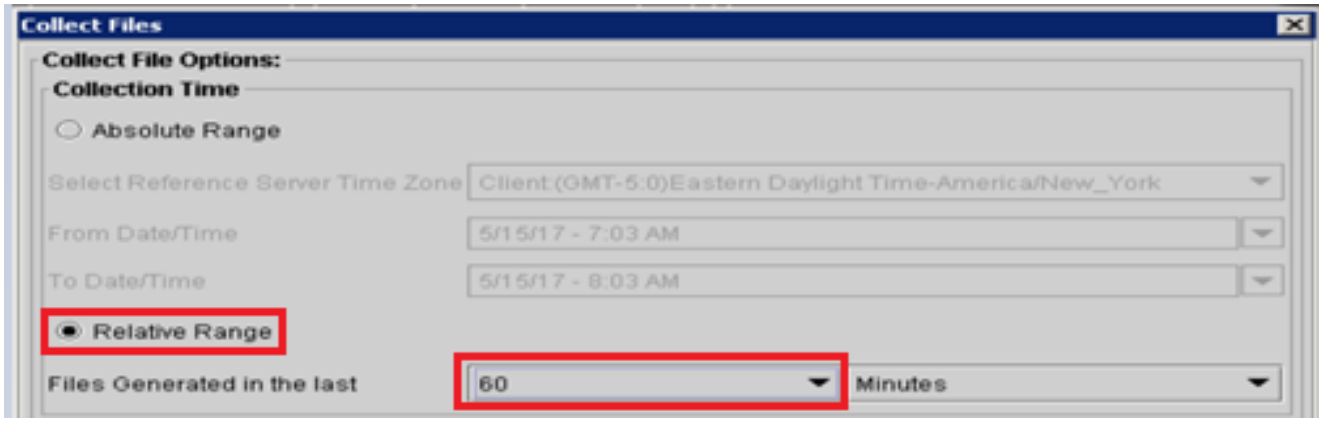
13. In the new open window, select the **Engine** and click Next.



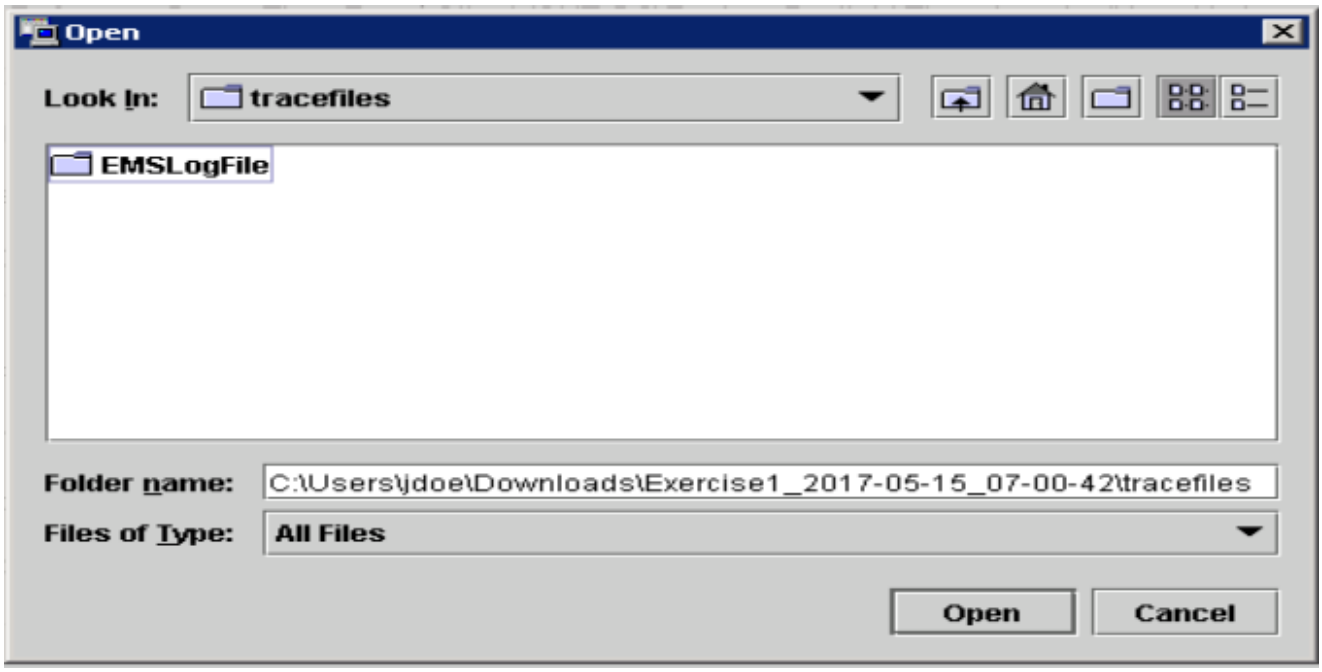
14. Click **Next** again in the next window.



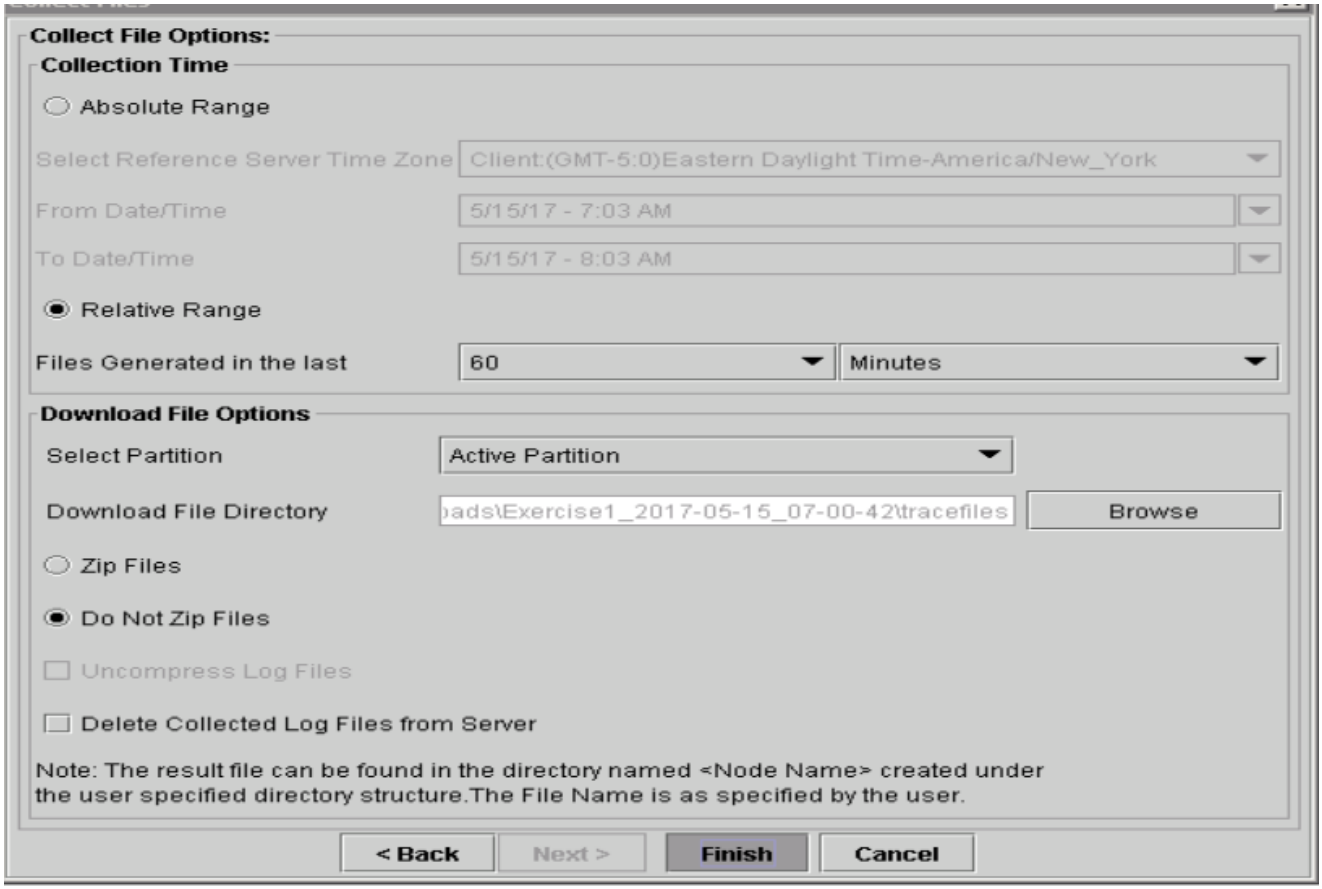
15. Select **Relative Range** and ensure you select time to cover the time of your bad call.



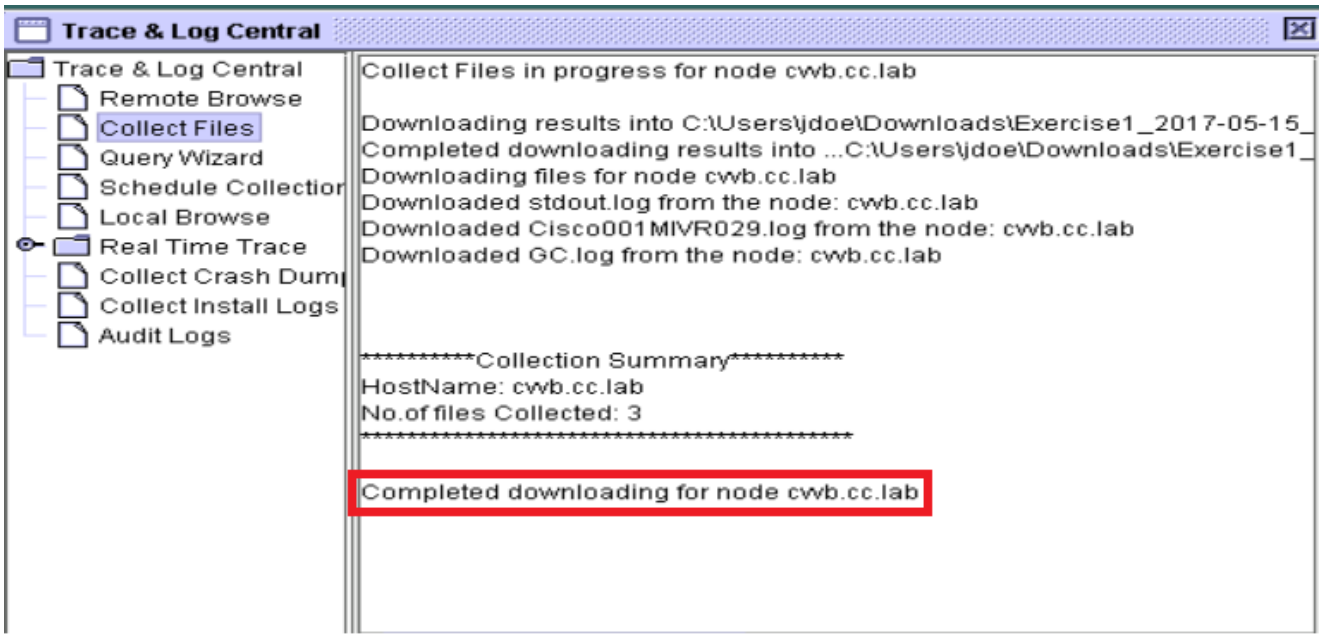
16. On the Download File Options, click **Browse** and select the directory where you want to save the file, then click **Open**.



17. Once all is selected, click on **Finish** button.



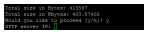
18. This collects the log files. Wait until you see confirmation message on RTMT.



19. Navigate to the folder where the traces are saved.

20. The Engine logs are all that you need. To find them navigate to **\<time stamp>\uccx\log\MIVR** folder.

Option 2: Via SSH and SFTP - Recommended Option

1. Log in to the VVB server with the Secure Shell (SSH).
2. Enter this command in order to collect the logs you need. The logs are compressed and you are prompted to identify SFTP server where the logs are uploaded. **file get activelog /uccx/log/MIVR/*** 
3. These logs are stored on the SFTP server path: *<IP address>\<date time stamp>\active_nnn.tgz* , where nnn is timestamp in long format.

Set Trace and Collect Logs for CUBE and CUSP

CUBE (SIP)

1. Set the logs timestamp and enable the logging buffer.

```
#conf  t
service timestamps debug datetime msec
service timestamps log datetime msec
service sequence-numbers
no logging console
no logging monitor
logging buffered 5000000 7
end
clear logging
```

> **Warning**: Any change on a production Cisco IOS® software GW can cause an outage.

2. This is a very robust platform that can handle the suggested debugs at the provided call volume without issue. However, Cisco recommends that you:

- Send all logs to a syslog server instead of to the logging buffer.

```
logging <syslog server ip>
logging trap debugs
```

- Apply the debug commands one at a time, and check the CPU utilization after each one.

```
show proc cpu hist
```

Warning: If the CPU gets up to 70-80% CPU utilization, the risk of a performance-related service impact is greatly increased. Thus, do not enable additional debugs if the GW hits 60%.

3. Enable these debugs:

```
debug voip ccapi inout
debug ccsip mess
After you make the call and simulate the issue, stop the debugging:
```

4. Reproduce the problem.
5. Disable the traces.

```
#undebug all
```

6. Collect the logs.

```
term len 0
show ver
show run
show log
```

CUSP

1. Turn on SIP traces on CUSP.

```
(cusp)> config
(cusp-config)> sip logging
(cusp)> trace enable
(cusp)> trace level debug component sip-wire
```

2. Reproduce the problem.
3. Turn logging off once you are done.

Collect the logs

1. Configure a user on the CUSP (for example: test).
2. Add this configuration at the CUSP prompt.

```
username <userid> create
username <userid> password <password>
username <userid> group pfs-privusers
```

3. FTP to the CUSP IP address. Use the username (test) and password as defined in the previous step.
4. Change directories to /cusp/log/trace.
5. Get the log_<filename>.

Set Trace and Collect UCCE logs

Cisco recommends to set trace levels and collect traces via Diagnostis Framework Portico or System CLI tools.

Note: For more information about Diagnostic Framework Portico and Syetem CLI, visit the chapter Diagnostic tools on the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1).

When you troubleshoot most of the UCCE scenarios, if the default level of traces does not provide enugh information, set the level of traces to 3 in the required components (with some exceptions).

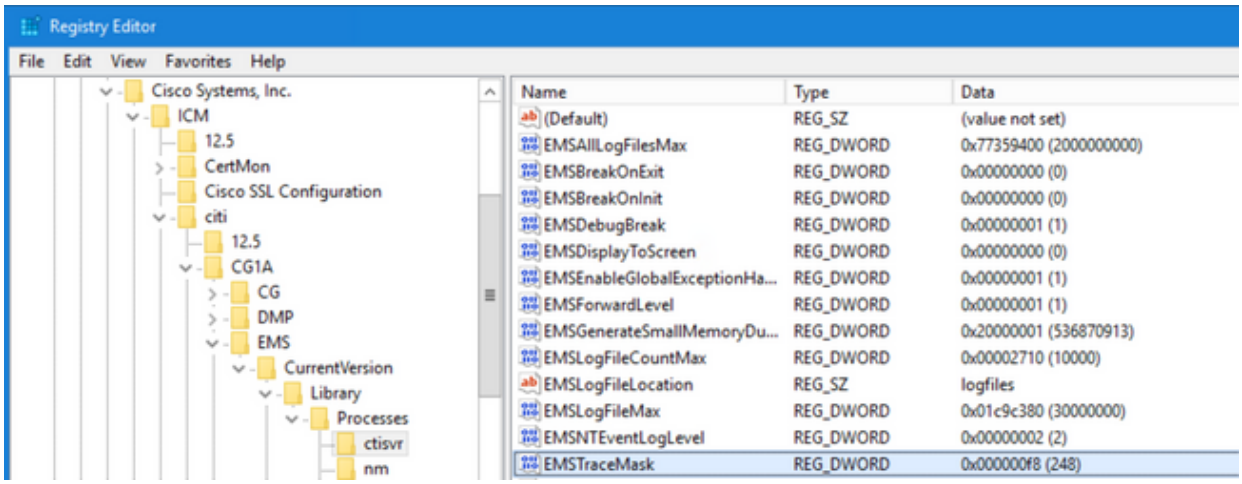
Note: Visit the Trace Level section on the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1) for more information.

For instance, if you troubleshoot Outbound Dialer issues the level of traces must be set to level 2 if the Dialer is busy.

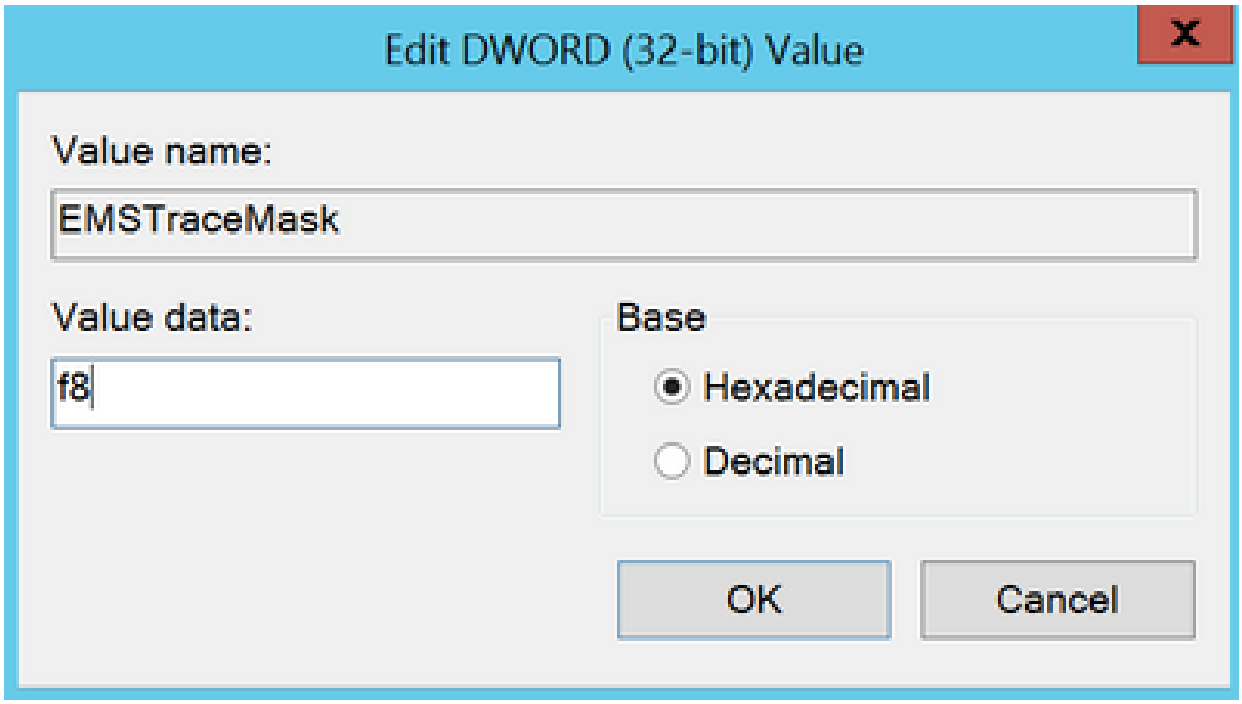
For CTISVR (CTISVR) Level 2 and level 3 does not set the exact registry level recommended by Cisco. The recommended trace registry for CTISVR is 0XF8.

1. On the UCCE Agent PG, open the Registry Editor (Regedit).

2. Navigate to HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a and b)\EMS\CurrentVersion\library\Processes\ctisvr.



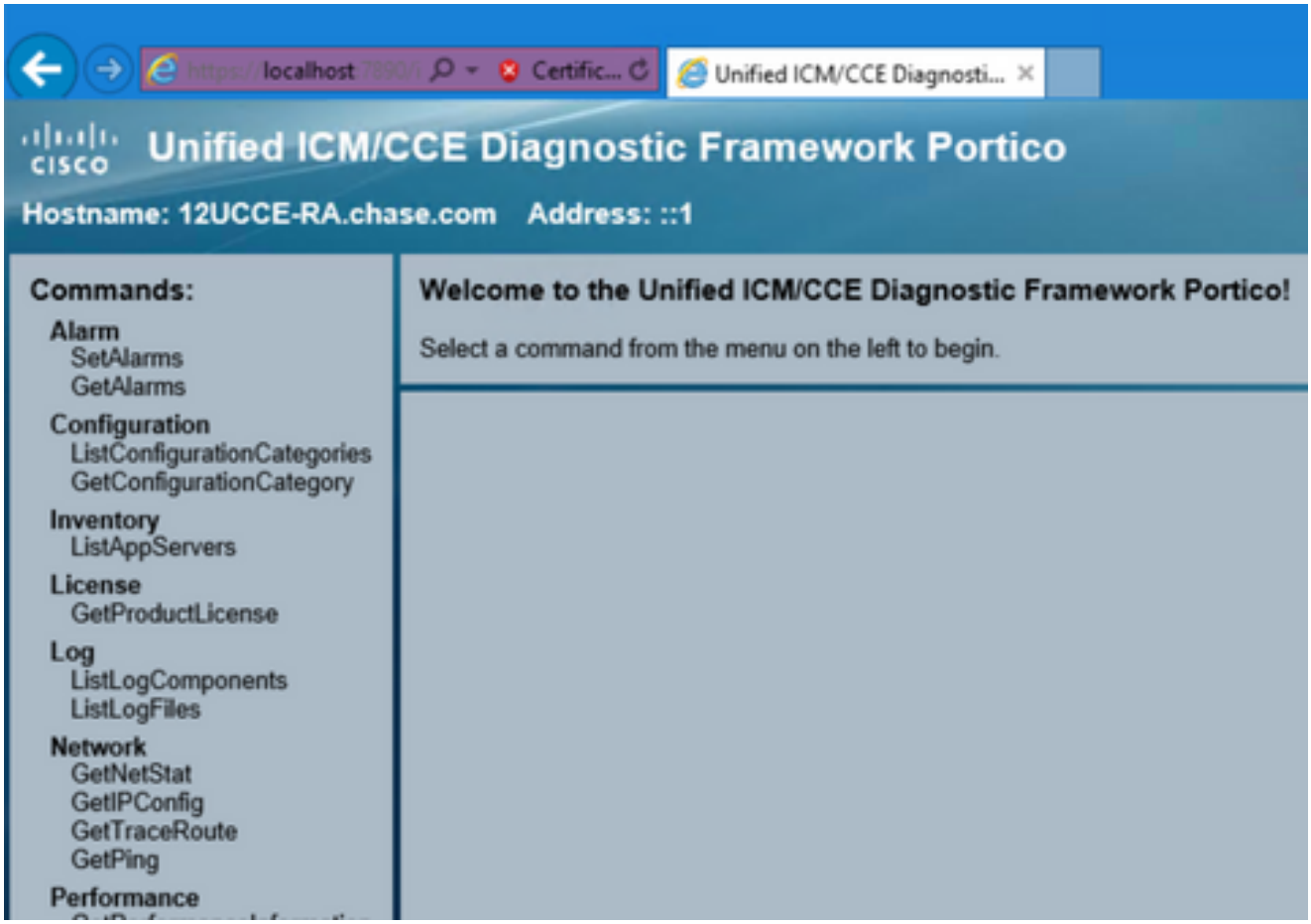
3. Double click on the **EMSTraceMask** and set the value to **f8**.



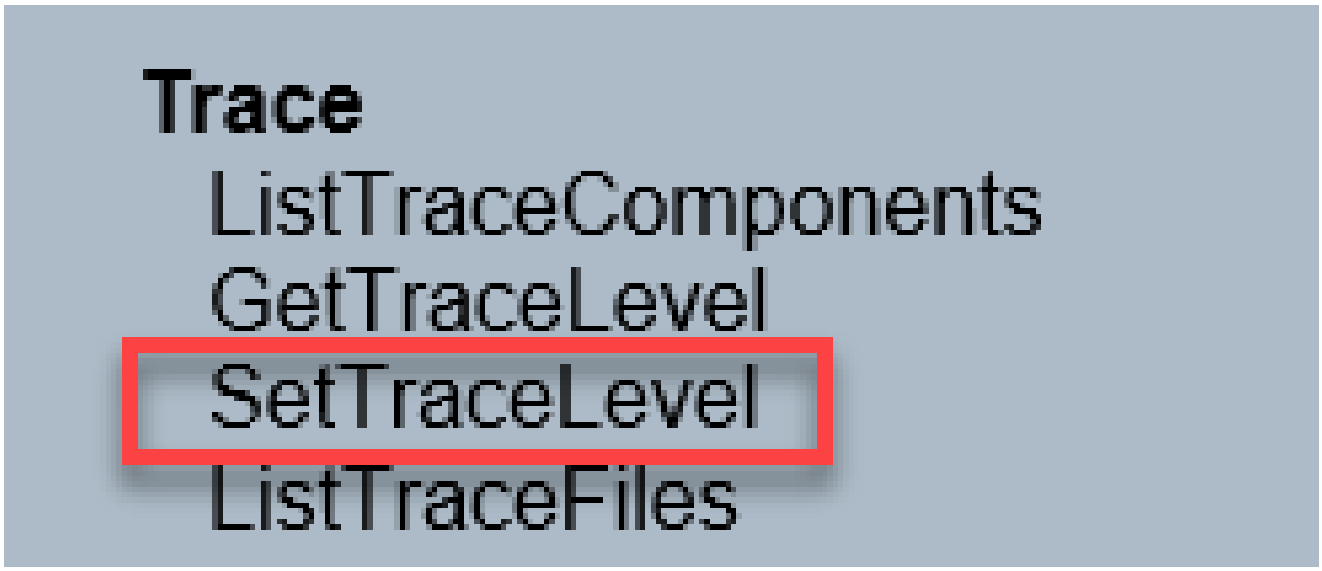
4. Click **Ok** and close the Registry Editor. These are the steps to set any of the UCCE component traces (the RTR process is used as an example).

SetTrace Level

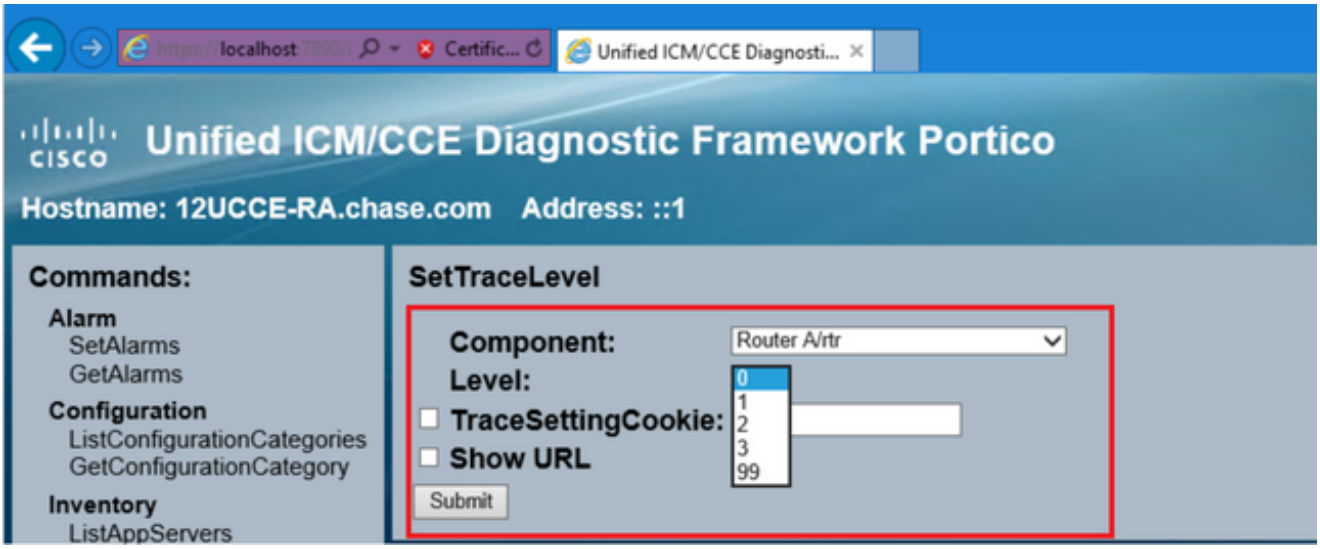
1. Open the Diagnostic Framework Portico from the server you need to set the traces, and log in as the Administrator user



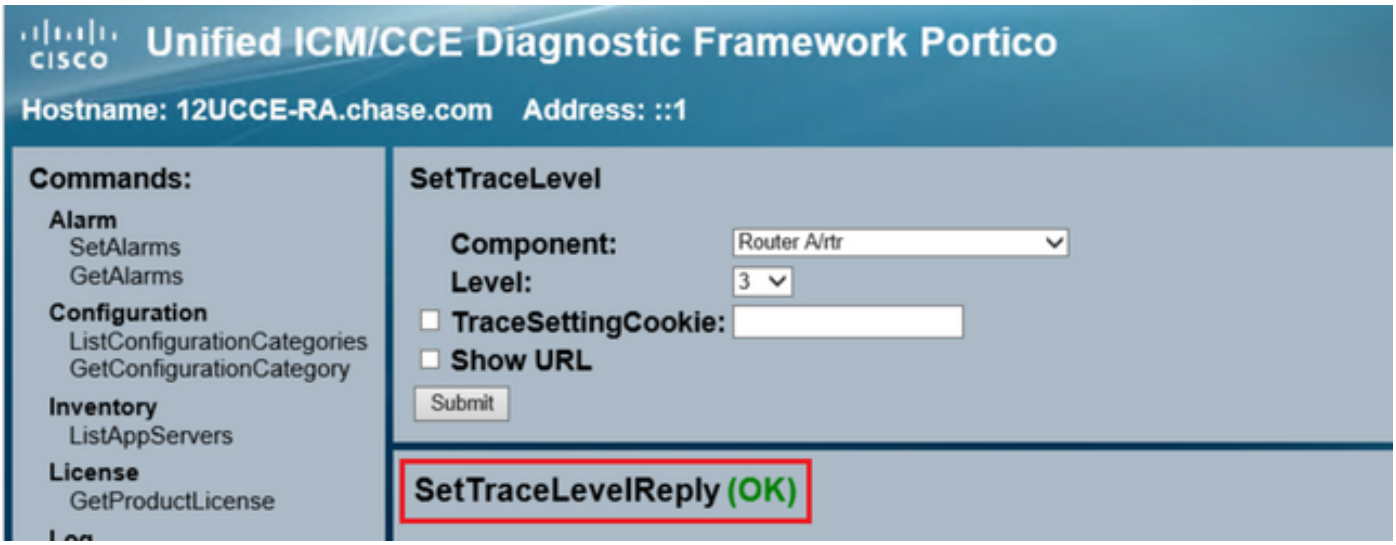
2. On the Commands section, navigate to **Trace** and select **SetTraceLevel.**



3. On the **SetTraceLevel** window, select the component and the level.



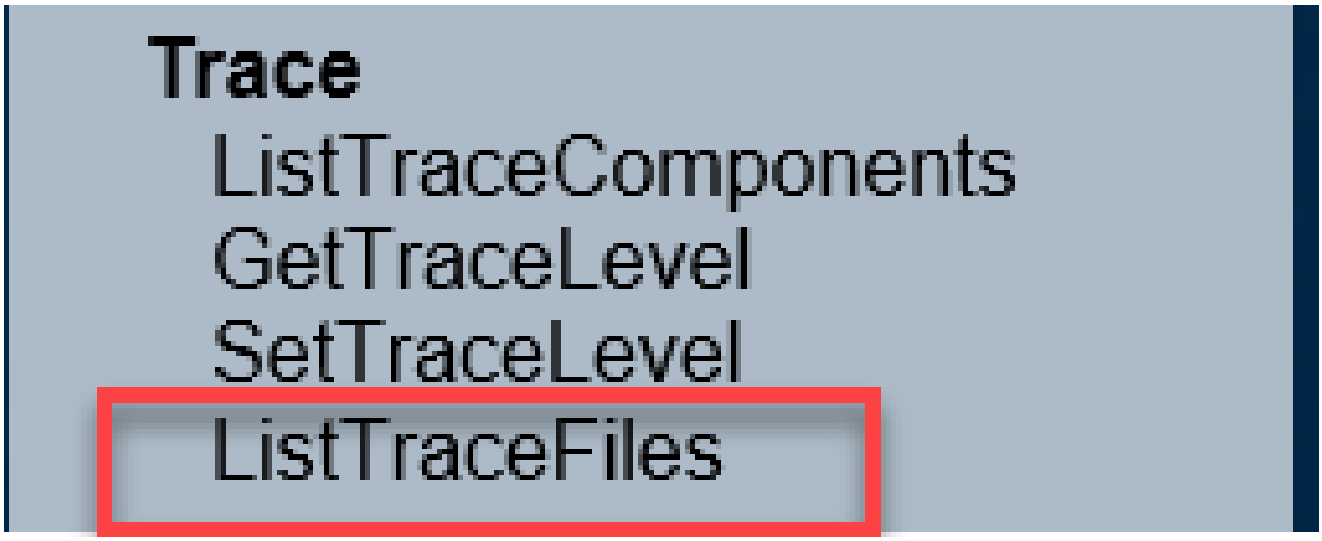
4. Click **Submit**. When finished, you see the Ok message.



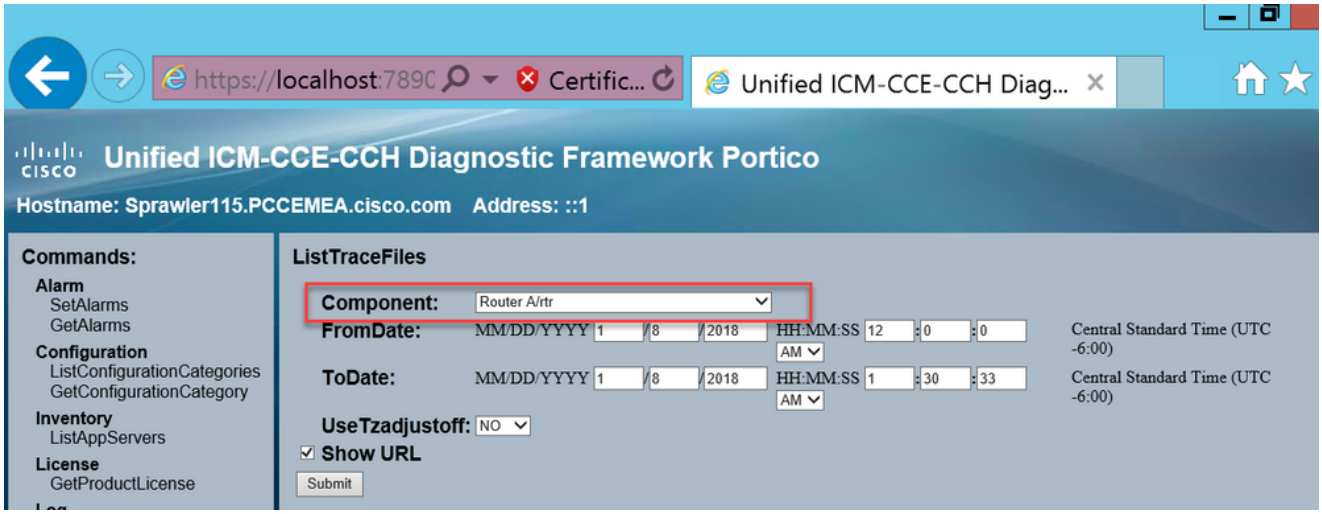
Warning: Set the level of traces to level 3 while you attempt to reproduce the problem. After the problem is reproduced, set the trace level to default. Use special cautious when you set the JTAPIGW traces, since Level 2 and Level 3 set the Low level traces and this can cause a performance impact. Set Level 2 or Level 3 in the JTAPIGW during non-production time or in a lab environment.

Log Collection

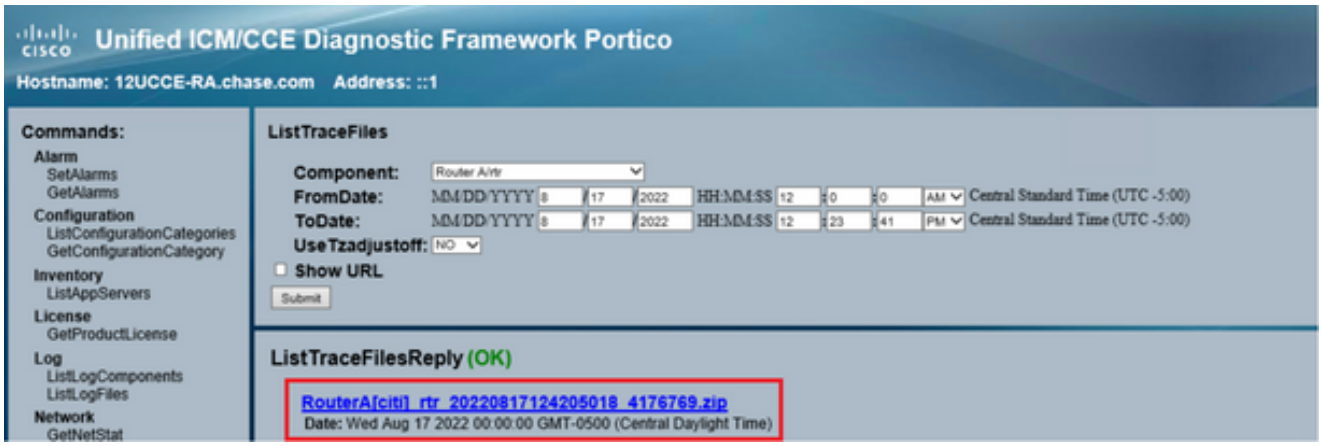
1. From the Diagnostic Framework Portico, on the **Commands** section, navigate to **Trace** and select **ListTraceFile**.



2. On the **ListTraceFile** window select the **Component**, **FromDate,** and **ToDate**. Check the **Show URL box,** and then, click on **Submit**.



3. When the request finishes, you see the OK message with the link of the ZIP log file.

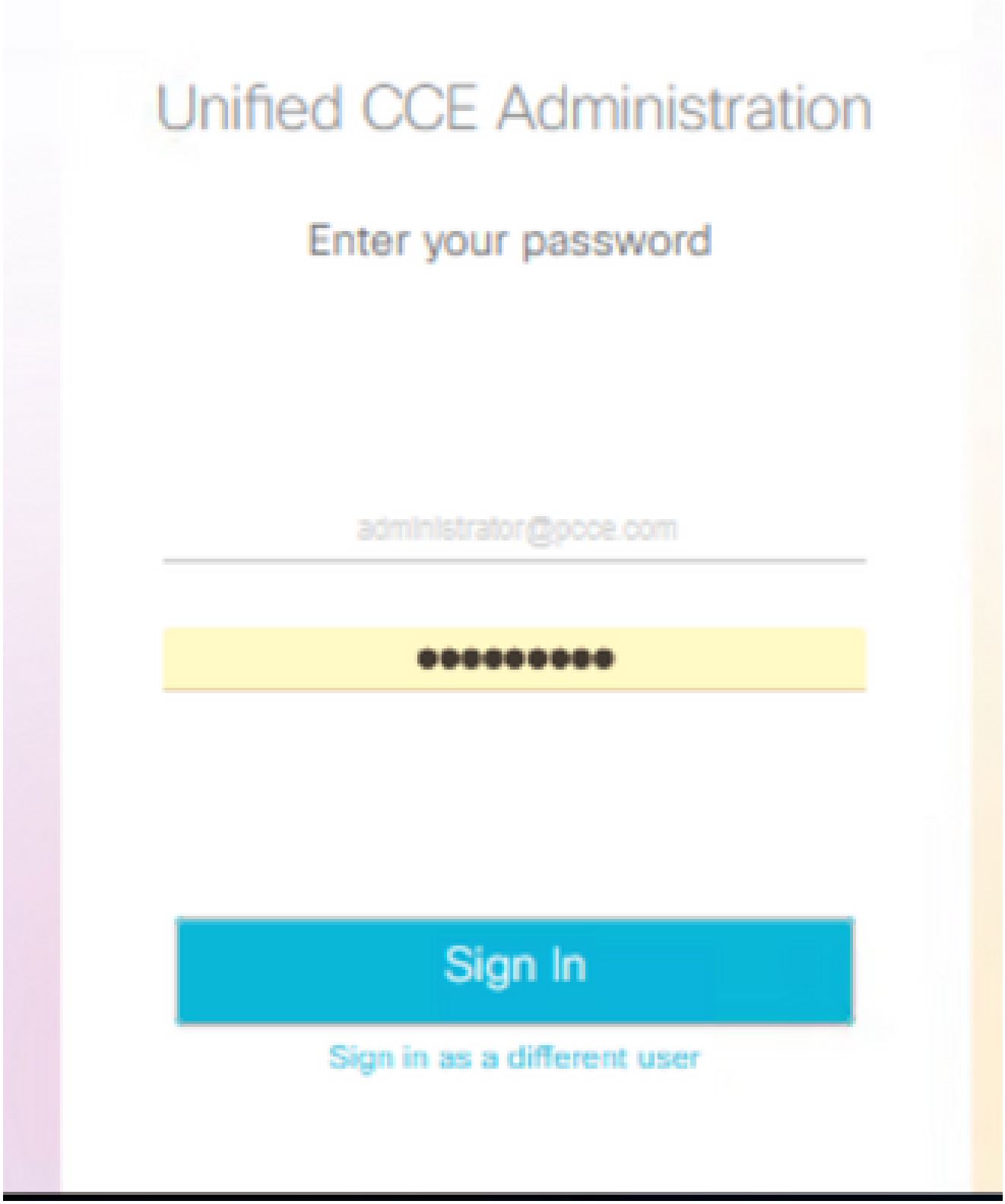


4. Click on the ZIP file link and save the file in the location you choose.

Set Trace and Collect PCCE Logs

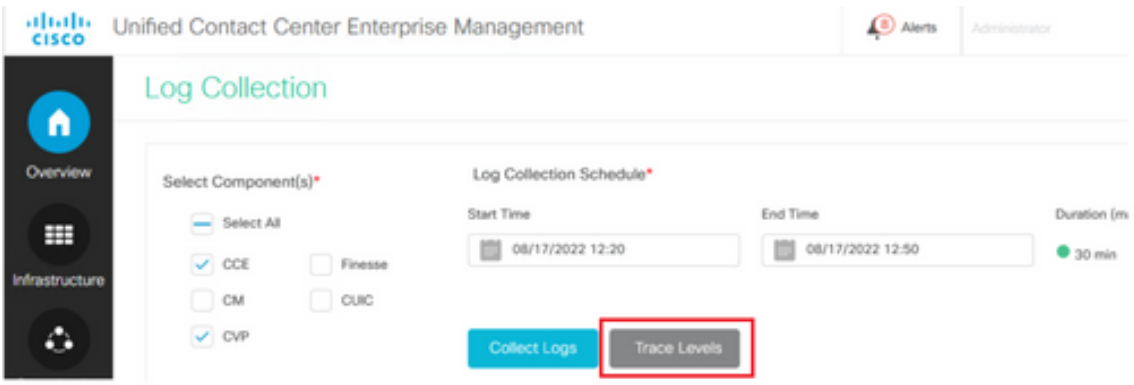
PCCE has its own tool to setup trace levels. It is not applicable to UCCE environment where Diagnostic Framework Portico or system CLI are the preferred ways to enable and collect logs.

1. From the PCCE AW server, open the Unified CCE Web Administration tool and log in to the Administrator account.

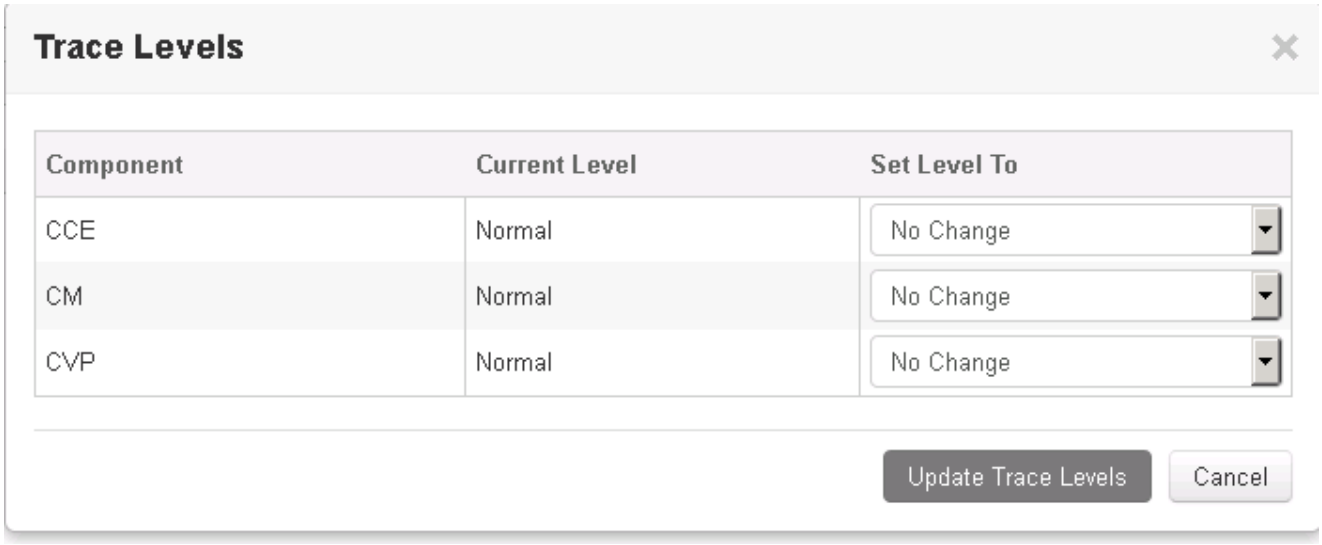


2. Navigate to **Overview->Infrastructure Settings->Log Collection** in order to open the Log Collection page.

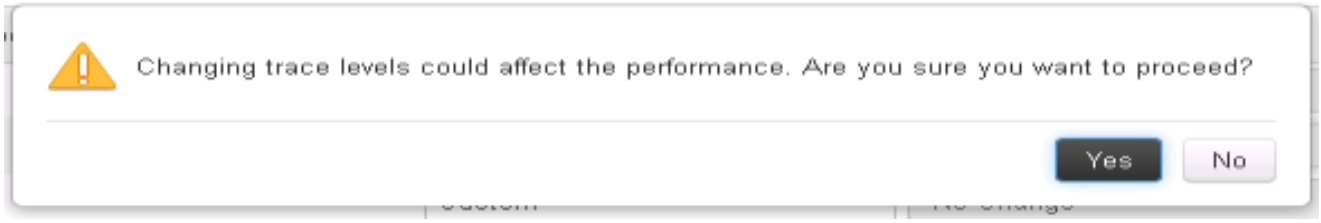
3. On the Log Collection page, click on **Trace Levels** which opens the **Trace Levels** dialog box.



4. Set the Trace Level to **Detailed** on CCE and leave it as **No Change** for CM and CVP, then click **Update Trace Levels.**



5. Click **Yes** to acknowledge the Warning.



6. After the problem is reproduced, open the **Unified CCE Administration** and navigate back to **System** > **Log Collection.**
7. Select **CCE** and **CVP** in the Components pane.
8. Select the appropriate Log Collection Time (the default is the last 30 min).
9. Click on **Collect Logs** and **Yes** to the dialog warning. The log collection starts. Wait few minutes before it finishes.

10. Once finished, click on the **Download** button in the **Actions** column to download a zipped file with all logs in it. Save the **zip** file in any location you find appropriate.

Set Trace and Collect CUIC/Live Data/IDS Logs

Download logs with SSH

1. Log in to the SSH Command Line (CLI) of CUIC, LD and IDS.

2. Run the command in order to collect CUIC related logs.

file get activelog /cuic/logs/cuic/*.* recurs compress reltime hours 1
file get activelog /cuic/logs/cuicsrvr/*.* recurs compress reltime hours 1
file get activelog tomcat/logs/*.* recurs compress

3. Run the command in order to collect LD related logs.

file get activelog livedata/logs/*.*

4. Run the command in order to collect IdS related logs.

   file get activelog ids/log/*.* recurs compress reltime days 1

5. These logs are stored on the SFTP server path: <IP address>\<date time stamp>\active_nnn.tgz , where nnn is timestamp in long format.

Download Logs with RTMT

1. Download RTMT from OAMP page. Log in to https://<HOST ADDRESS>/oamp where HOST ADDRESS is the IP address of the server.

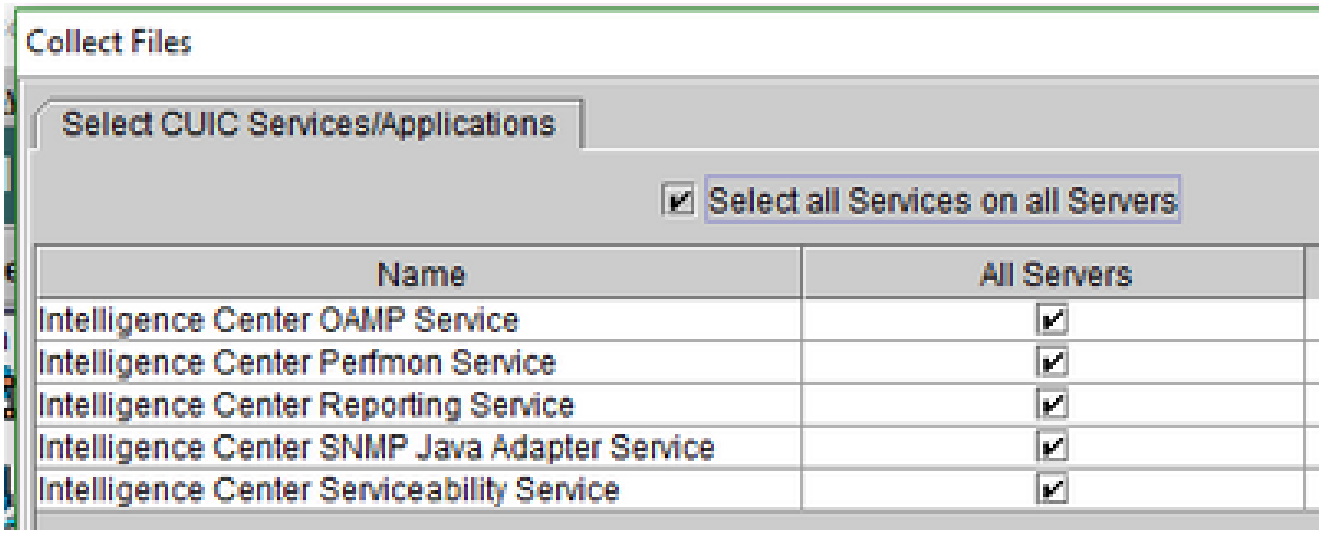
2. Navigate to **Tools > RTMT plugin download.** Download and install the plugin.

3. Launch RTMT and log in to the server with admin credentials.

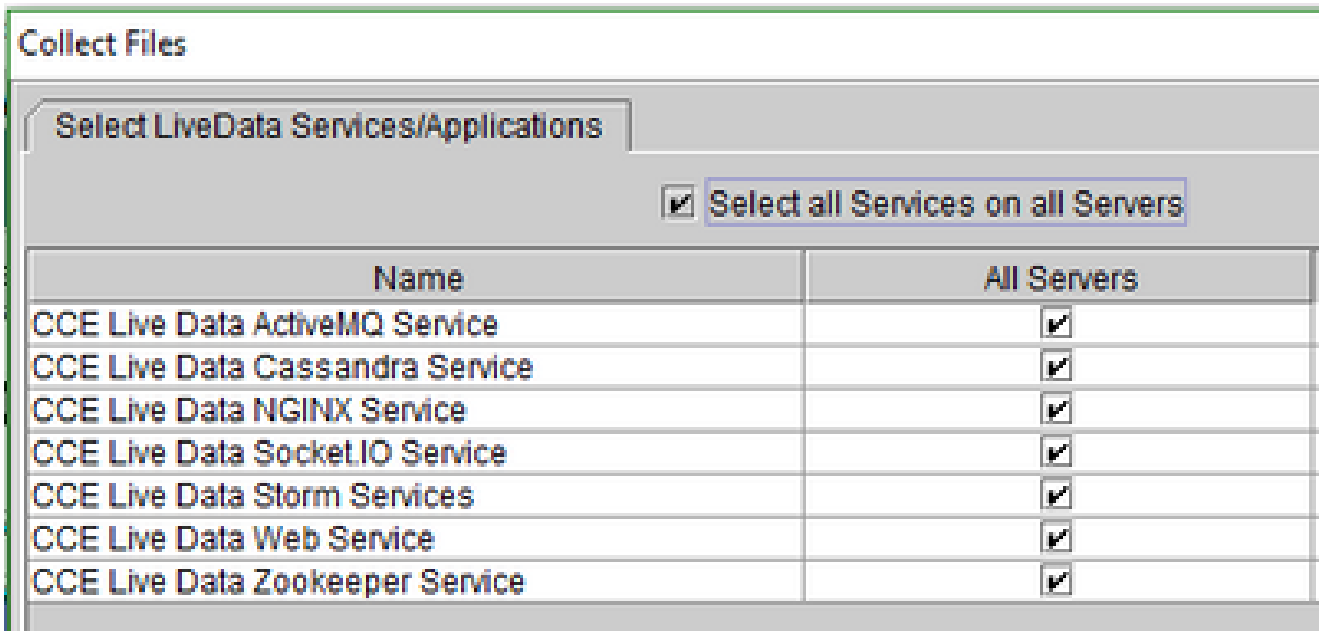
4. Double click on **Trace and Log Central** and then double click **Collect Files**.

5. You can see these tabs for the specific services. You must select all services/servers for CUIC, LD, and IDS.

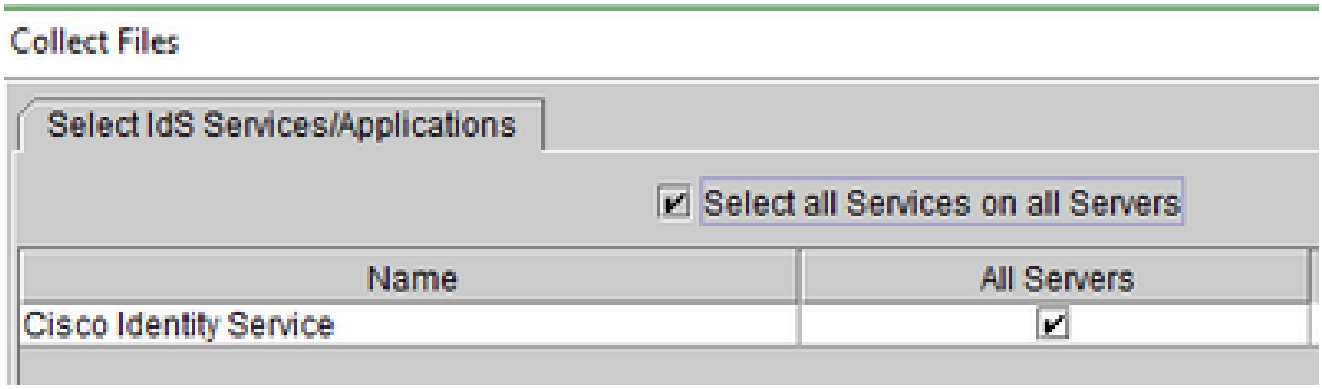
   For CUIC:



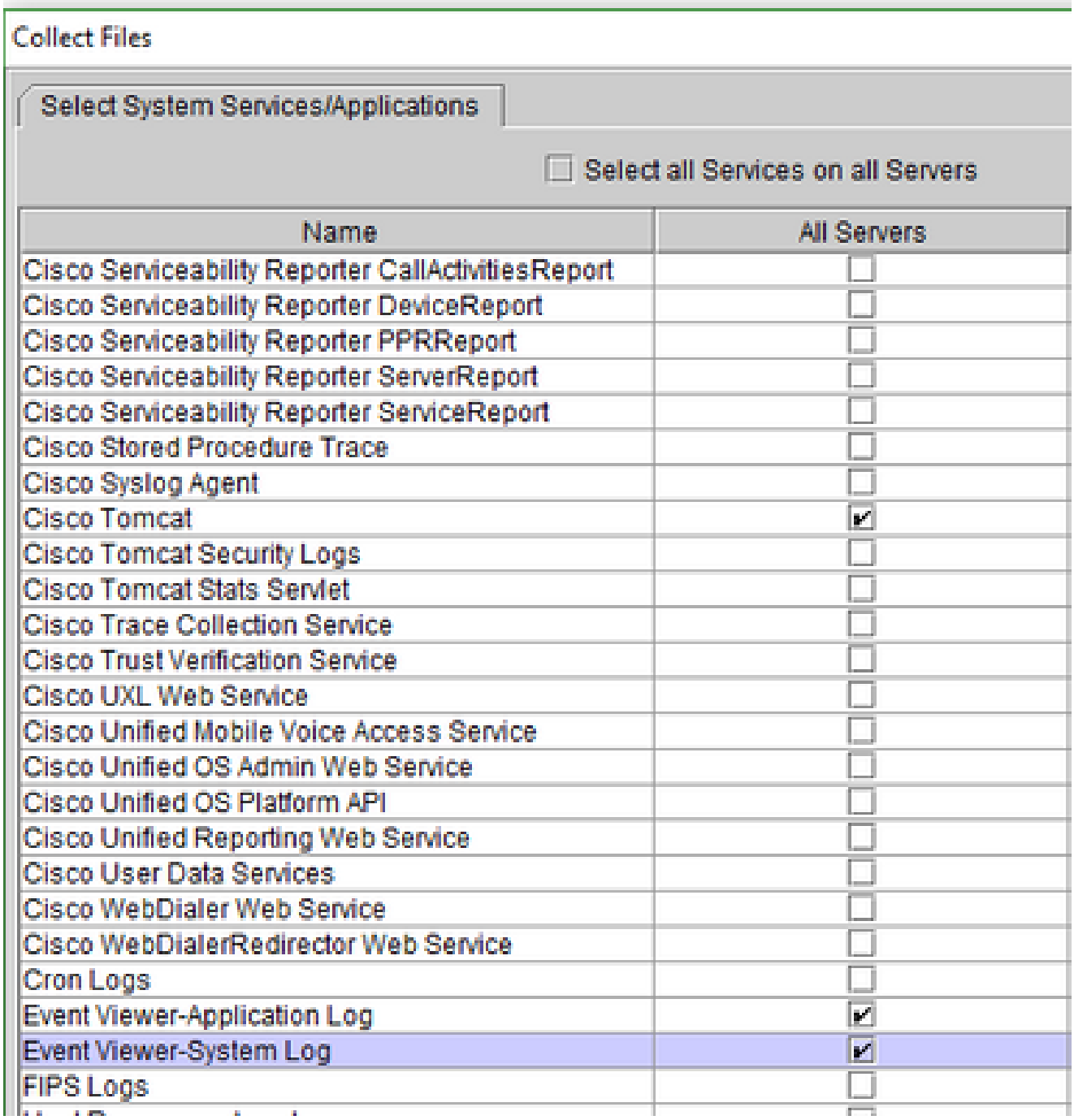
   For LD:



For IDS:



For Platform services, it is generally a good idea to select Tomcat and Event viewer logs:

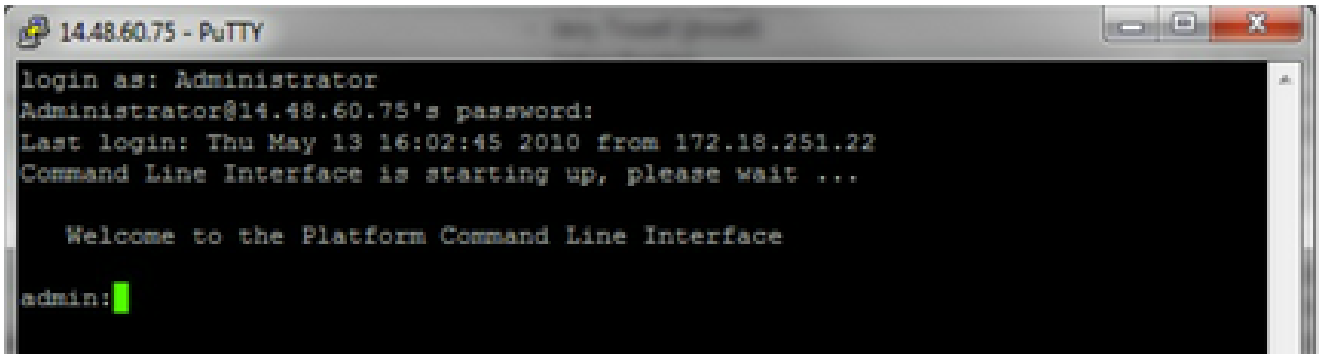


6. Select the **Date and Time** along with the destination folder in order to save the logs.

Packet Capture on VoS (Finesse, CUIC, VVB)

1. Start the Capture

   To start the capture, establish a SSH session to the VOS server authenticate with the Platform Administrator account.

2. 

1a. Command Syntax

The command is **utils network capture**and the syntax is as follows:

<#root>

Syntax:

utils network capture

[options]
options optional
page,numeric,file fname,count num,size bytes,src addr,dest addr,port
num,host protocol addr
options are:
page
- pause output
numeric - show hosts as dotted IP
addresses
file fname - output the information to a file

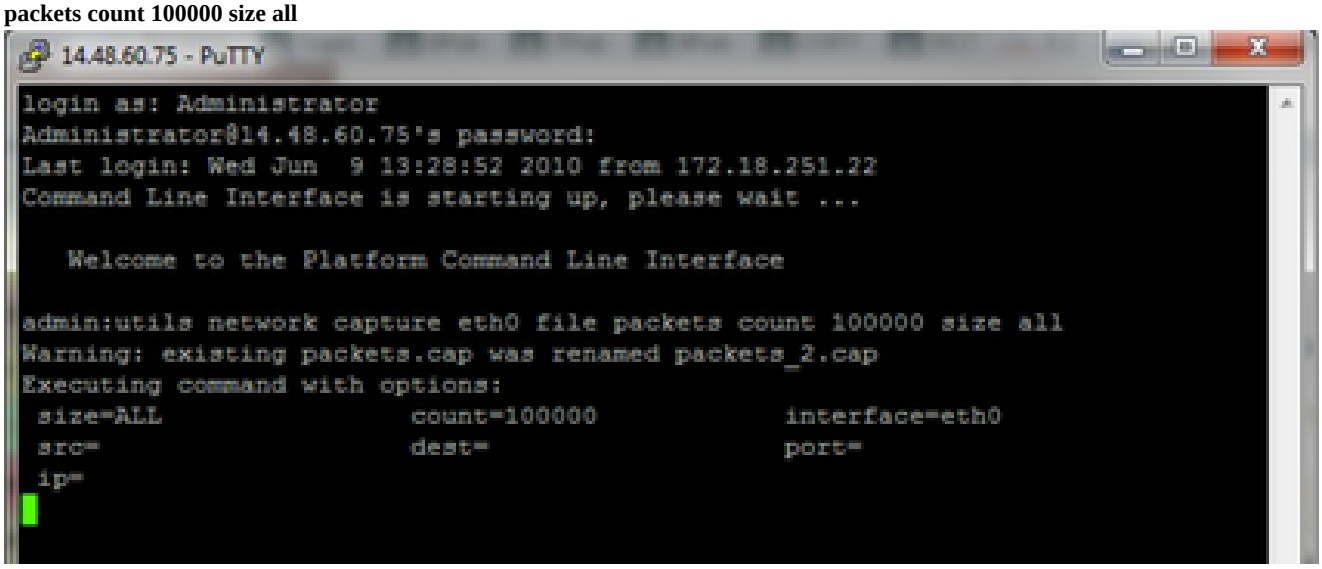
Note: The file is saved in platform/cli/fname.cap

fname should not contain the "." character
count num - a
count of the number of packets to capture
Note: The maximum count
for the screen is 1000, for a file is 100000
size bytes -
the number of bytes of the packet to capture
Note: The maximum
number of bytes for the screen is 128
For a file it can be
any number or ALL
src addr - the source address of the
packet as a host name or IPV4 address
dest addr - the
destination address of the packet as a host name or IPV4 address
port
num - the port number of the packet (either src or dest)
host
protocol addr - the protocol should be one of the following:
ip/arp/rarp/all. The host address of the packet as a host name or IPV4
address. This option will display all packets to and from that address.

Note: If "host" is provided, do not provide "src" or "dest"

1b. Capture All Traffics

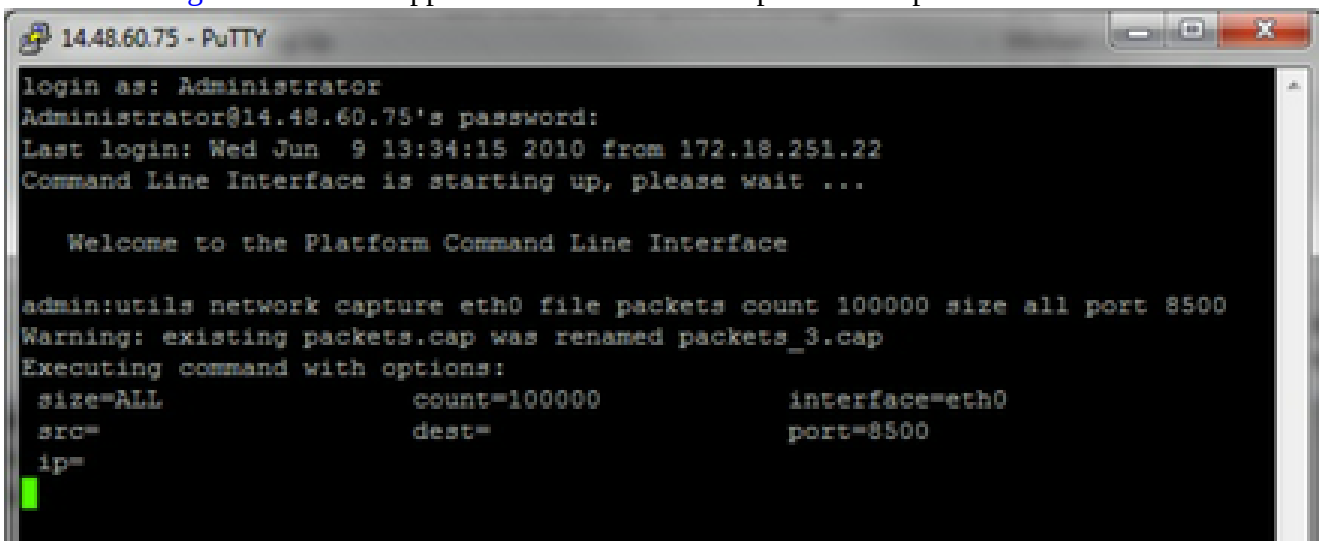
For a typical capture, one can collect ALL packets of ALL sizes from and to ALL address into a capture file called **packets.cap**. To do this simply execute on the admin CLI **utils network capture eth0 file packets count 100000 size all**



1c. Capture based on Port number

In order to troubleshoot a communications issue with the Cluster Manager, it can be desireable to use the port option to capture based on a specific port (8500).

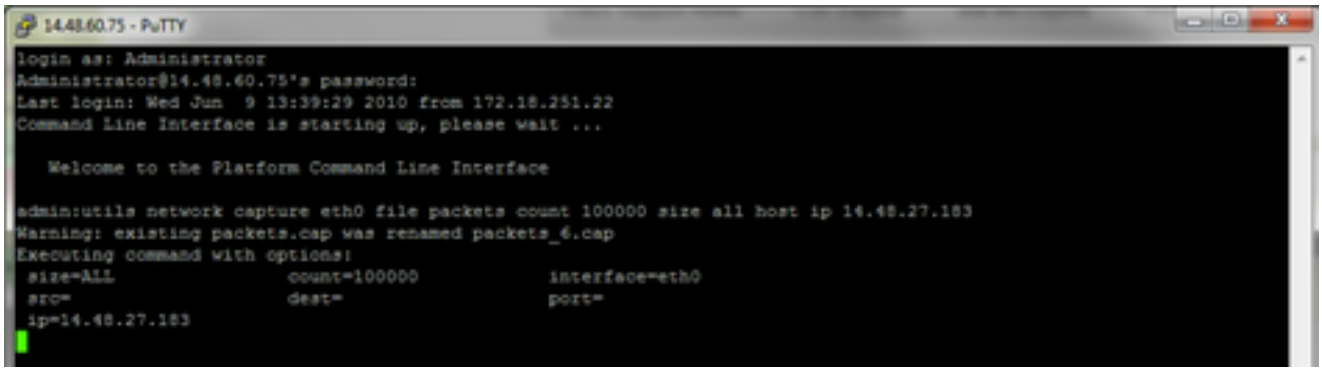
For more information about which services require communications on each port, refer to theTCP and UDP Port Usage Guidefor the applicable version of the respective component.



1d. Capture based on host

To Troubleshoot an issue with VOS and a particular host, it can be necessary to use the 'host' option to filter for traffic to and from a particular host.

It can also be necessary to exclude a particular host, in this case use a "!" in front of the IP. An example of this would be **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

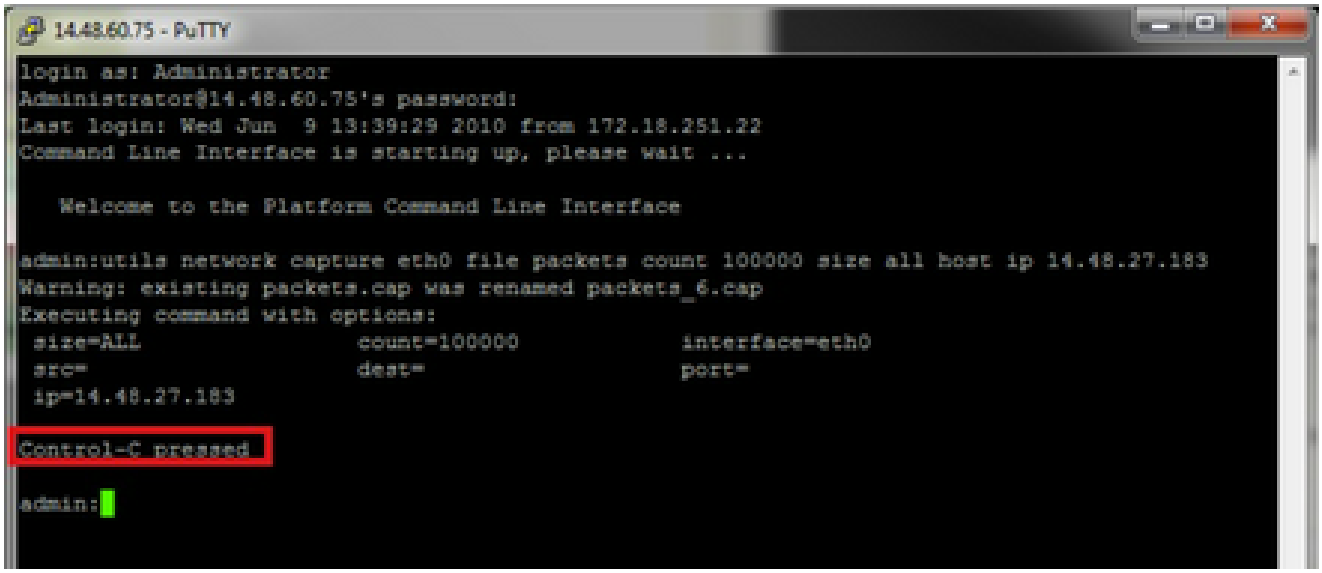


3. Reproduce the problem symptom

   While the capture is started to reproduce the problem symptom or condition so that the necessary packets are included in the capture. If the problem is intermittent it can be necessary to run the capture for an extended period. If the capture ends, it is because the buffer is filled, restart the capture and the previous capture is automatically renamed so the previous capture is not lost. If a capture is needed for an extended period of time, use a monitor session on a switch to capture at the network level.

4. Stop the capture

   To stop the capture hold the **Control** key and press **C** on the keyboard. This causes the capture process to end and no new packets are added to the capture dump.

5. 

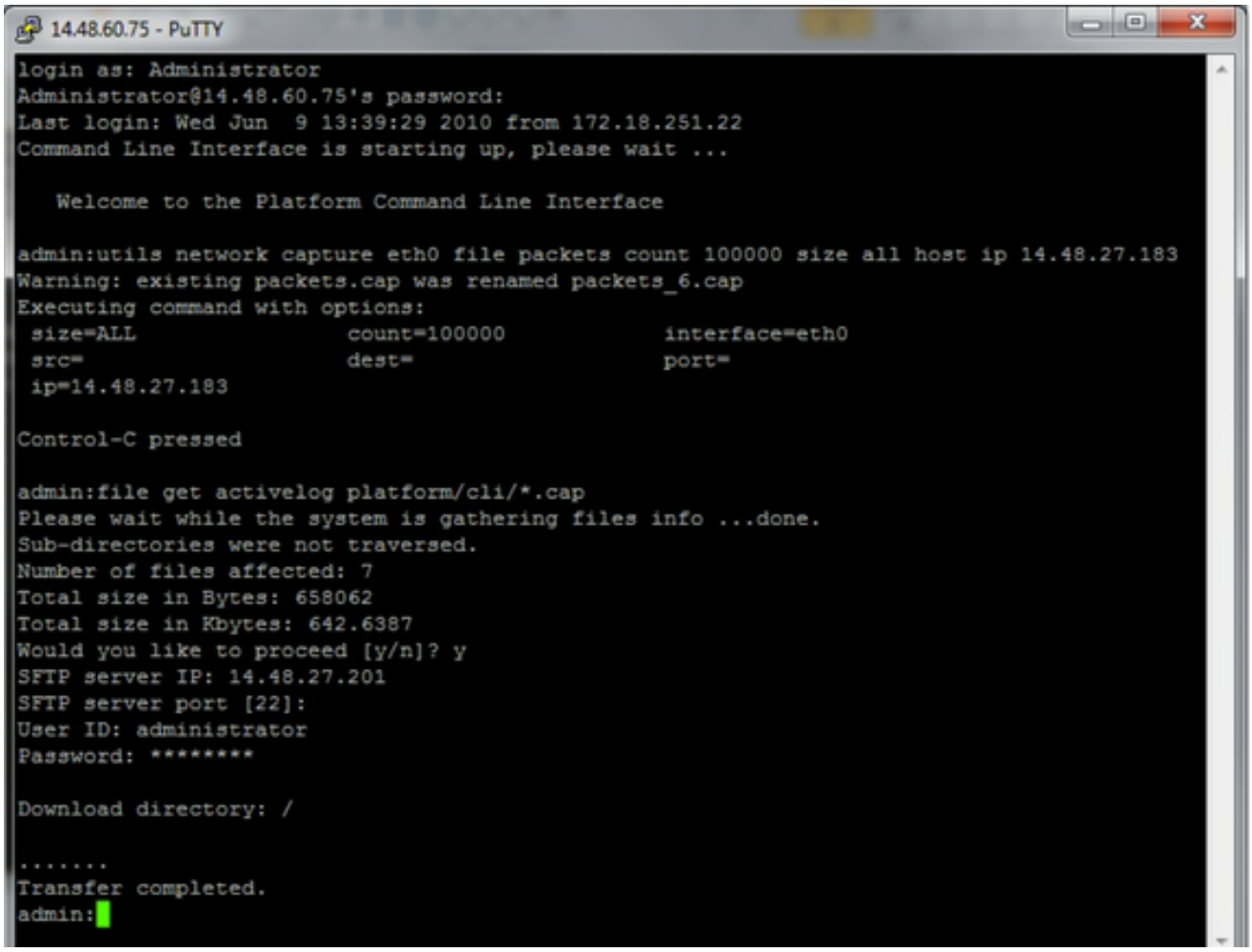
   Once this is complete, a capture file is stored on the server in the location 'activelog platform/cli/'

6. Collect the capture from the server

   The capture files are stored in "activelog platform/cli/" location on the server. You can transfer the files through CLI to an SFTP server or to the local PC with the RTMT.

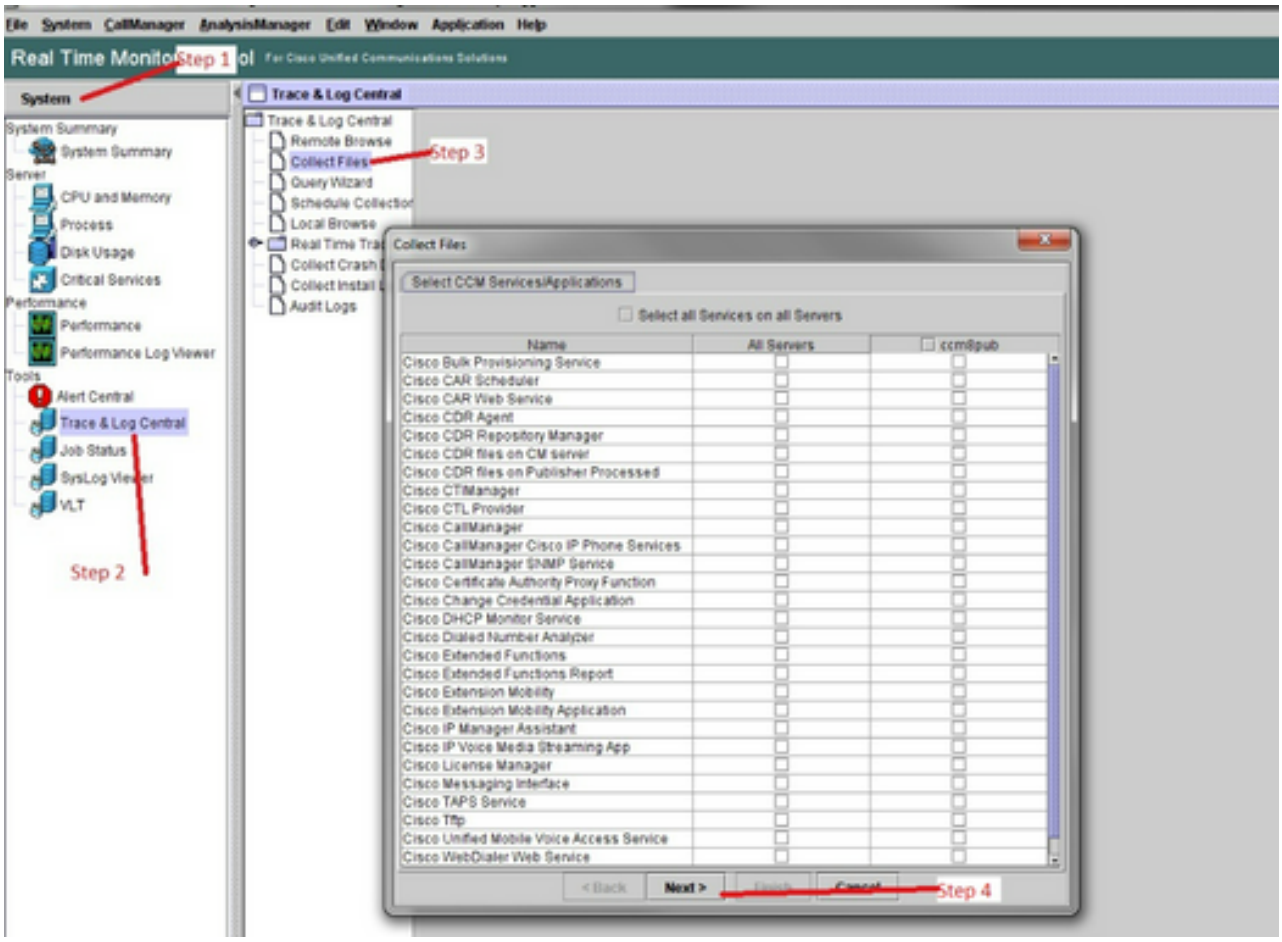
   4a. Transfer capture file through the CLI to an SFTP server

   Use the command **file get activelog platform/cli/packets.cap** to collect the packets.cap file to the SFTP server. Alternatively to collect all .cap files stored on the server, use 'file get activelog platform/cli/*.cap Finally, fill in the SFTP server IP/FQDN, port, username, password, and directory information:

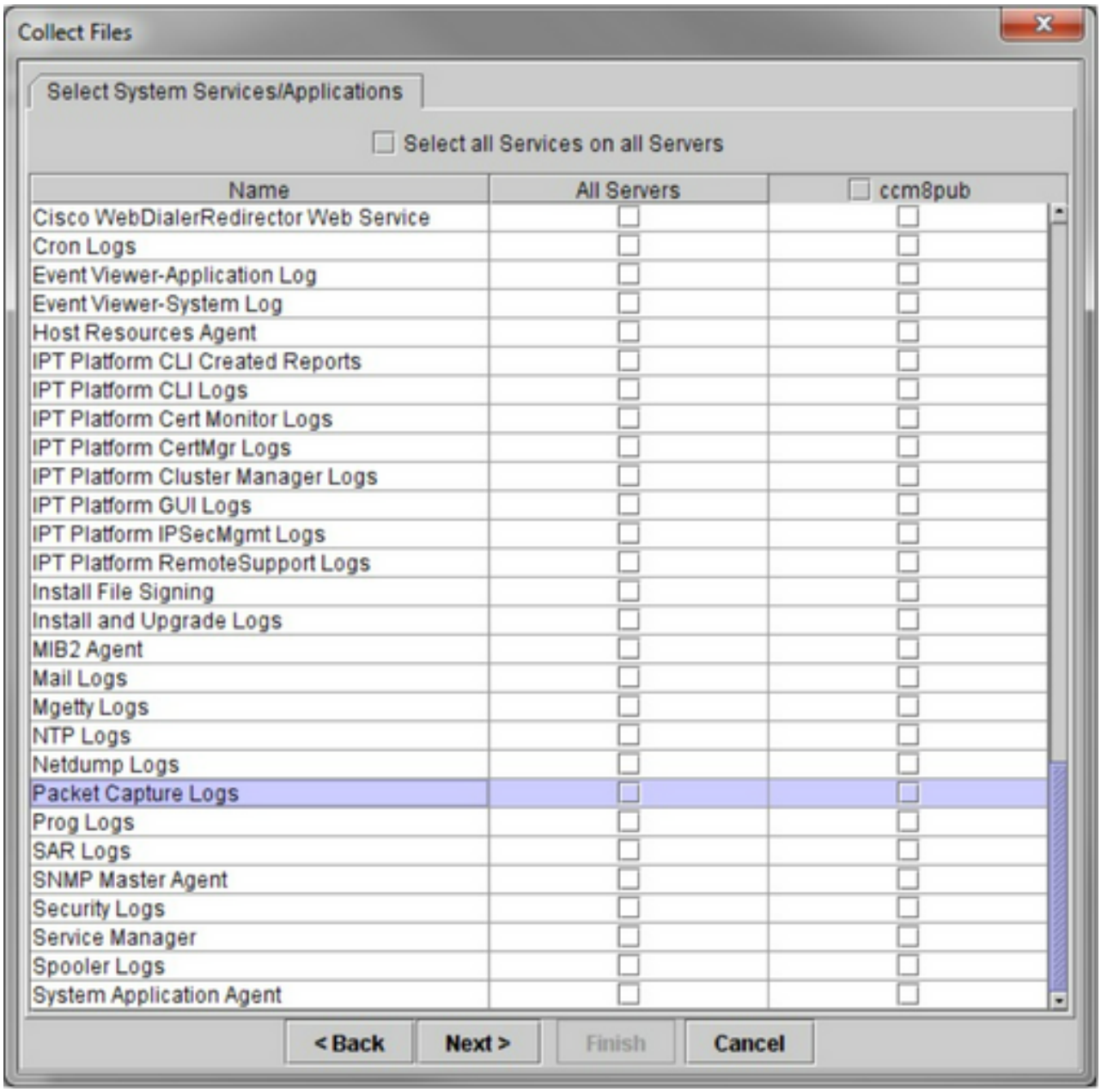


The CLI indicates success or failure of the file transfer to the SFTP server.

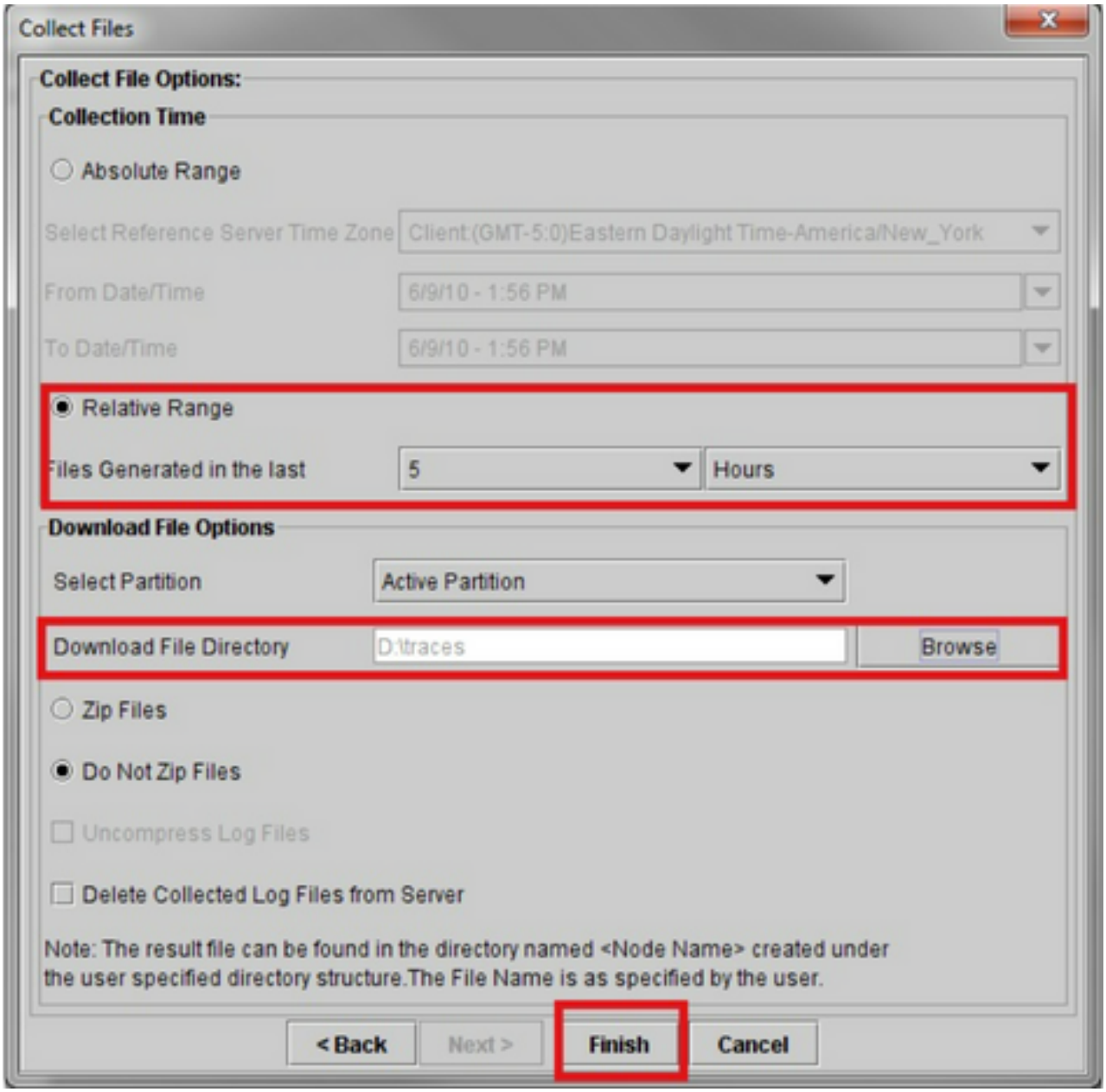
4b. Use RTMT to transfer a capture file to a local PC.
Launch the RTMT. If it is not installed on the local PC, install the appropriate version from the VOS Administration page the go to the **Applications->Plugins** menu.
Click **System**, then **Trace & Log Central**, then double click **Collect Files.** Click **Next** through the first menu.



In the second menu choose the checkbox for **Packet Capture Logs** on the server which the capture was performed, then click **Next**.



On the final screen choose a time range when the capture was performed, and a download directory on the local PC.



RTMT closes this window and proceed to collect the file and store it on the local PC in the specified location.