

Collect Trace Data for CUCM 9.X or Later

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Install the RTMT Application](#)

[Configure or Confirm Detailed Tracing for the CallManager Service](#)

[Configure or Confirm Detailed Tracing for the CTI Manager Service](#)

[Reproduce the Issue and Take Notes](#)

[Gather the Requested Traces](#)

[Verify Trace File Coverage](#)

[Attach a Trace Package to Your Service Request](#)

[Analysis](#)

Introduction

This document describes how to use the trace collection process of the Cisco Unified Communications Manager (CUCM/CallManager).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Real-Time Monitoring Tool (RTMT) application
- Detailed tracing for the CallManager service
- Detailed tracing for the computer-telephony integration (CTI) Manager service

Note: You must be a registered Cisco client to use these tools.

Components Used

The information in this document is based CUCM 9.X and later versions.

Note: For information on the earlier version CUCM 8.6.2, see [Collecting CUCM Traces from CUCM 8.6.2 for a TAC SR](#).

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.

Background Information

If you work with a Technical Assistance Engineer (TAC) engineer on a Communications Manager issue, you need to collect CUCM traces. This could be a task you do infrequently or have never done before.

In this scenario, you troubleshoot a call that has not been recorded even though the CUCM-side configuration appears to be correct. The administrator receives an alarm message for each call that failed to record, so the TAC engineer has asked you to reproduce the issue and gather detailed CallManager traces, detailed CTI Manager traces, and Event Viewer logs from the CUCM side. These logs capture the call signaling events, the CTI messages that are exchanged with the server that records the calls, and the alarms from the call that failed to be recorded.

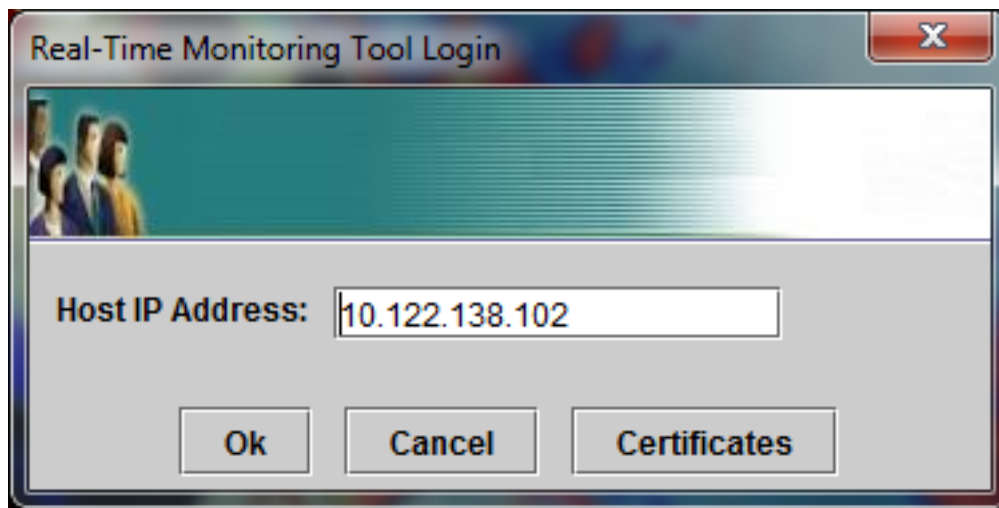
To complete this task:

- Install the RTMT application
- Configure or confirm detailed traces for the CallManager service
- Configure or confirm detailed traces for the CTI Manager service
- Reproduce the issue and take notes
- Gather the requested traces
- Verify trace file coverage
- Attach a trace package to your service request

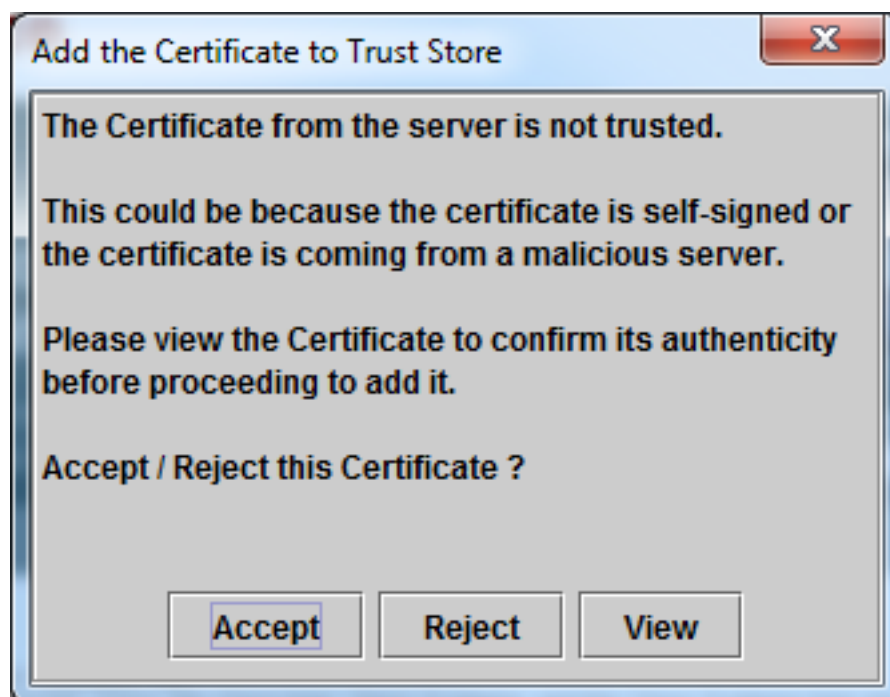
Install the RTMT Application

In CUCM, the RTMT application is used to gather traces for most types of issues. Every major and minor version of CUCM has an associated version of the RTMT application. If, on your PC, you do not see a **Unified RTMT** program group under **Start > Programs > Cisco**, or if the RTMT version does not match your CUCM cluster, you must install the RTMT tool for your CUCM version before you move forward.

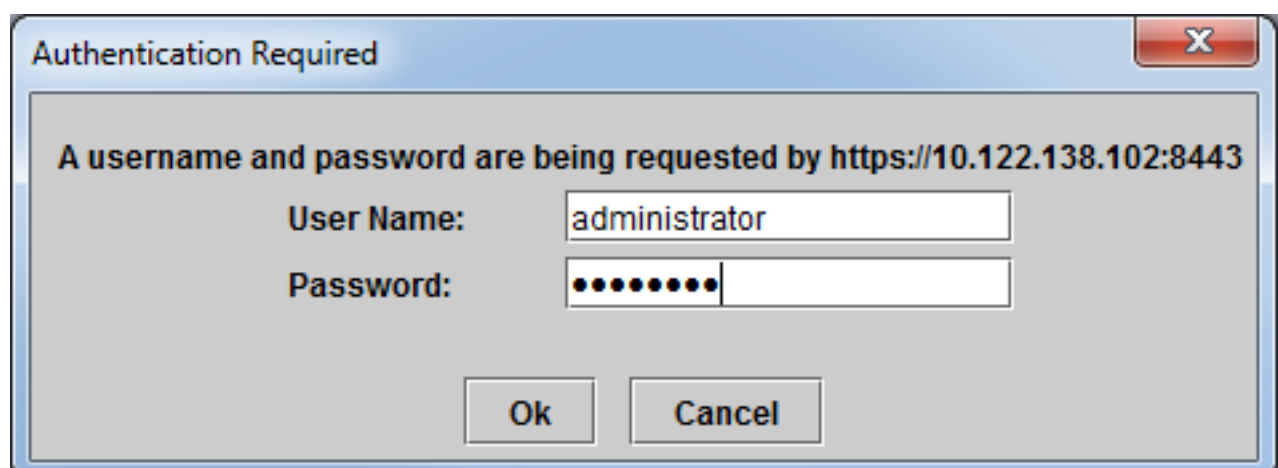
1. Log in to the Cisco Unified CM Administration Page.
2. Choose **Application > Plugins**.
3. Click **Find**.
4. Click the **Download** link for the Cisco Unified Real-Time Monitoring Tool – Windows plugin.
5. Save the CcmServRtmtPlugin.exe file.
6. Run CcmServRtmtPlugin.exe.
7. Step through the directions of the InstallAnywhere installation wizard, accept the License Agreement and install to the default folder location. If you had an old version of RTMT installed, the installation wizard directs you to uninstall the old version before you proceed.
8. Choose **Start > Programs > Cisco > Unified RTMT** and launch Cisco Unified Real-Time Monitoring Tool.
9. In the Real-Time Monitoring Tool Login window, enter the IP address for your CUCM Publisher.



10. In the Add the Certificate to Trust Store window, click **Accept**.

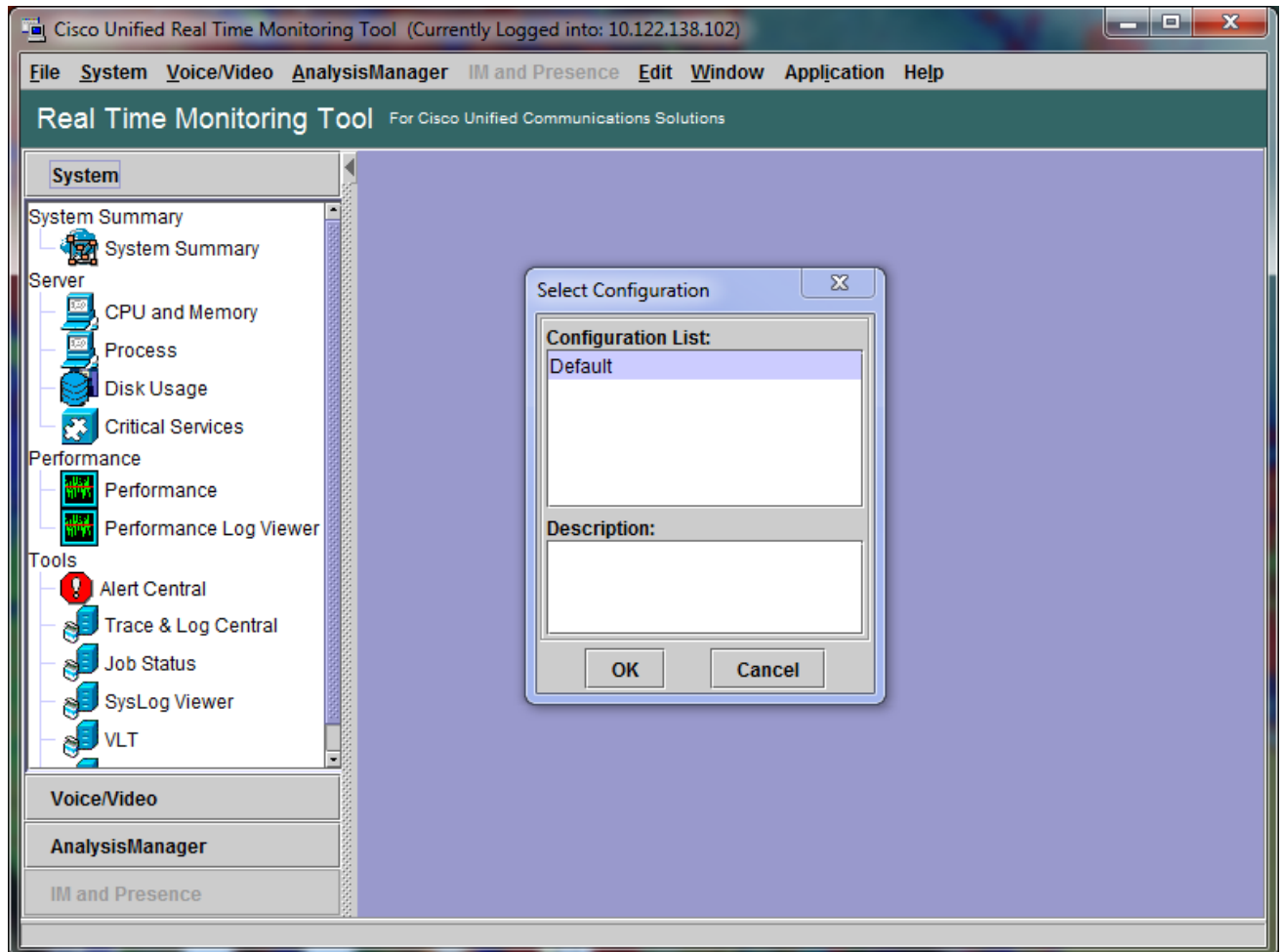


11. In the Authentication Required window, enter the same User Name and Password as you do to log on to the CUCM Administration page.

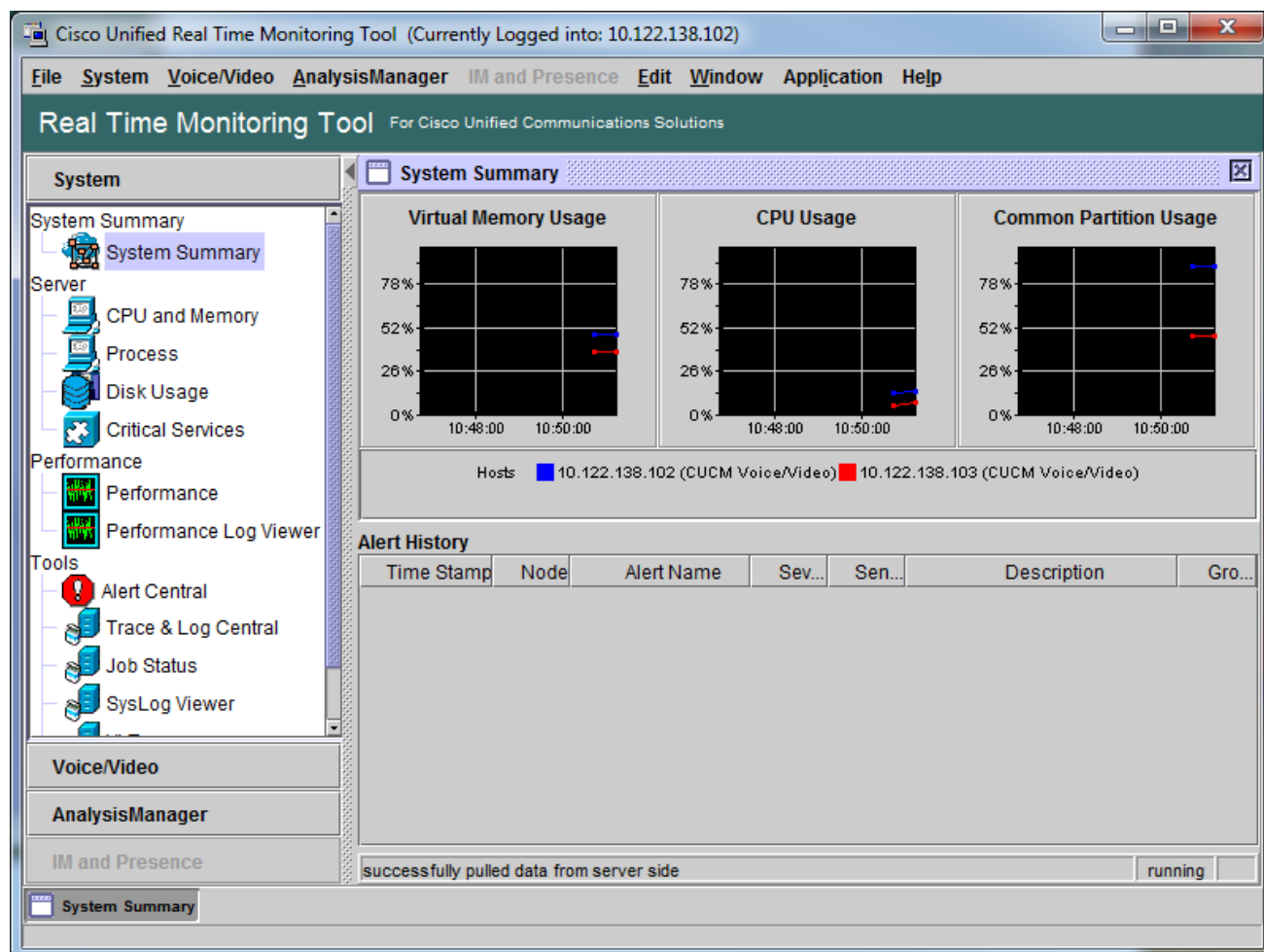


If you are unable to log on, add theRealtime and TraceCollection permissions to your user account, or use the application administrator account created when the system was installed and try again.

12. The application opens, and you can see a Select Configuration window. Click **OK** in order to select the Default configuration.



The System Summary page opens.



You have now verified that RTMT is installed, and that you are able to log on to your CUCM cluster with the tool.

Configure or Confirm Detailed Tracing for the CallManager Service

In CUCM 9.X and later, detailed tracing is enabled by default for the CallManager service. Before you proceed, confirm that detailed tracing is still configured. If not, configure it.

1. Log on to the Cisco Unified Serviceability page.
2. Choose **Trace > Configuration**.
3. From the Server drop-down list, choose the CUCM Publisher and click **Go**.
4. From the Service Group drop-down list, choose **CM Services** and click **Go**.
5. From the Service drop-down list, choose **Cisco CallManager** and click **Go**.
6. The system is configured for the default detailed tracing, as shown in this image:

The screenshot shows the Cisco Unified Serviceability administrator interface. The browser address bar displays `https://10.122.138.102/ccmservice`. The page title is "Cisco Unified Serviceability For Cisco Unified Communications Solutions". The user is logged in as "administrator".

Trace Configuration

Related Links: [SDL Configuration](#)

Buttons: Save, Set Default

Status:

Ready

Select Server, Service Group and Service

Server*: 10.122.138.102--CUCM Voice/Video [Go]

Service Group*: CM Services [Go]

Service*: Cisco CallManager (Active) [Go]

☐ Apply to All Nodes

☒ Trace On

Trace Filter Settings

Debug Trace Level: Detailed

<input checked="" type="checkbox"/> Enable H245 Message Trace	<input checked="" type="checkbox"/> Enable CDR Trace
<input checked="" type="checkbox"/> Enable DT-24+/DE-30+ Trace	<input checked="" type="checkbox"/> Enable Analog Trunk Trace
<input checked="" type="checkbox"/> Enable PRI Trace	<input checked="" type="checkbox"/> Enable All Phone Device Trace
<input checked="" type="checkbox"/> Enable ISDN Translation Trace	<input checked="" type="checkbox"/> Enable MTP Trace
<input checked="" type="checkbox"/> Enable H225 & Gatekeeper Trace	<input type="checkbox"/> Enable All GateWay Trace
<input type="checkbox"/> Enable Miscellaneous Trace	<input checked="" type="checkbox"/> Enable Forward & Miscellaneous Trace
<input checked="" type="checkbox"/> Enable Conference Bridge Trace	<input checked="" type="checkbox"/> Enable MGCP Trace
<input checked="" type="checkbox"/> Enable Music On Hold Trace	<input checked="" type="checkbox"/> Enable Media Resource Manager Trace
<input checked="" type="checkbox"/> Enable CM Real-Time Information Server Trace	<input checked="" type="checkbox"/> Enable SIP Call Processing Trace
<input checked="" type="checkbox"/> Enable SIP Stack Trace	<input type="checkbox"/> Enable SCCP Keep Alive Trace
<input checked="" type="checkbox"/> Enable Annunciator Trace	<input type="checkbox"/> Enable SpeedDial Trace
<input type="checkbox"/> Enable SoftKey Trace	<input type="checkbox"/> Enable SIP Keep Alive (REGISTER Refresh) Trace
<input type="checkbox"/> Enable Route or Hunt List Trace	<input checked="" type="checkbox"/> Enable IVR Trace

Trace Output Settings

Traces for this service are written into the SDL trace files. File settings are found in the SDL Configuration page reached via Related Links above.

Buttons: Save, Set Default

* - indicates required item.

Trace On is enabled. The Debug Trace Level is set to Detailed. All Trace Filters are enabled, with the exception of: Enable Miscellaneous Trace, Enable SoftKey Trace, Enable Route or Hunt List Trace, Enable All GateWay Trace, Enable SCCP Keep Alive Trace, Enable SpeedDial Trace, Enable SIP Keep Alive (REGISTER Refresh) Trace.

- If the system is not configured with at least the default detailed tracing settings, and if you use CUCM 9.x or later:

Click **Set Default**. This reverts trace configuration for this service to default settings. Choose **Apply to All Nodes**. Click **Save**.

- Confirm trace configuration on the other servers in the cluster.

If you use an earlier version of CUCM, you need to manually configure your trace settings to

match the illustration. The **Set Default** button on earlier versions sets the Debug Trace Level to Error, and not the Detailed.

Configure or Confirm Detailed Tracing for the CTI Manager Service

In CUCM 9.X and later, detailed tracing is also enabled by default for the CTI Manager service. Before you proceed, confirm or configure this capability.

1. Log in to the Cisco Unified Serviceability page.
2. Choose **Trace > Configuration**.
3. From the Server drop-down list, choose the CUCM Publisher and click **Go**.
4. From the Service Group drop-down list, choose **CM Services** and click **Go**.
5. From the Service drop-down list, choose **Cisco CallManager** and click **Go**.

The system is configured for the default detailed tracing, as shown in this image:

The screenshot shows the Cisco Unified Serviceability web interface. The browser address bar displays `https://10.122.138.102/ccmservice`. The page title is "Cisco Unified Serviceability For Cisco Unified Communications Solutions". The user is logged in as "administrator". The navigation menu includes "Alarm", "Trace", "Tools", "Snmp", "CallHome", and "Help". The "Trace Configuration" section is active, showing "Related Links: SDL Configuration" and "Go". The "Status" section indicates "Ready". The "Select Server, Service Group and Service" section shows the following configuration: Server* is "10.122.138.102--CUCM Voice/Video", Service Group* is "CM Services", and Service* is "Cisco CTIManager (Active)". The "Apply to All Nodes" checkbox is unchecked. The "Trace On" checkbox is checked. The "Trace Filter Settings" section shows "Debug Trace Level" set to "Detailed" and "Enable All Trace" checked. The "Trace Output Settings" section contains a message: "Traces for this service are written into the SDL trace files. File settings are found in the SDL Configuration page reached via Related Links above." At the bottom, there are "Save" and "Set Default" buttons, and a note: "* - indicates required item."

- Trace On is enabled.
- The Debug Trace Level is set to Detailed.

- Enable All Trace is enabled.
6. If these settings were modified, and if you use CUCM version 9.x or later:
 1. Click **Set Default** in order to revert trace configuration to default settings.
 2. Check the **Apply to All Nodes** check box.
 3. Click **Save**.
 7. Confirm trace configuration on the other servers in the cluster.

As with the CallManager trace settings, if you use an earlier version of CUCM you need to manually configure your trace settings to match the settings in the previous illustration. Click **Set Default** on earlier versions if you need to set the Debug Trace Level to Error.

Note: But what about the Event Viewer logs? You do not need to change debug levels for either the Event Viewer, Application logs or the Event Viewer, nor the System logs. You need to proceed with issue reproduction.

Reproduce the Issue and Take Notes

In this scenario, you can place test calls to generate a failure. It helps the TAC Engineer to analyze the call if you provide information on the set of traces that have no information about the test calls. Also, you risk the collection of data for the wrong time frame and if that happens, you have to start over.

For each test call, record this information:

- The phone number for the party that called.
- The called party phone number.
- The call start time.
- The call end time.
- Time and description for any issues you experienced during the call

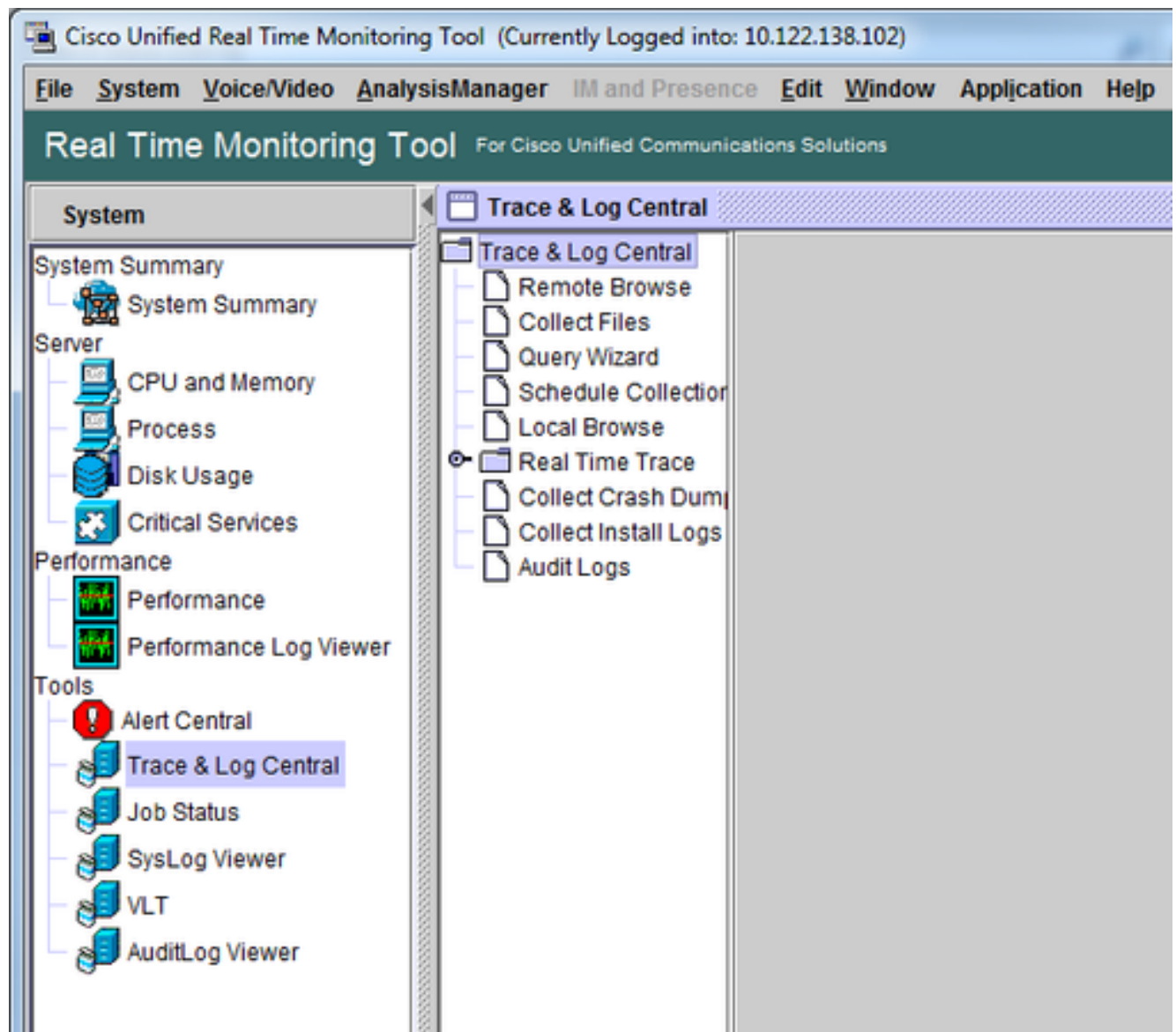
As CUCM traces can be very lengthy, TAC needs those call details in order to find your test calls in the data.

Gather the Requested Traces

After the issue was reproduced, gather the traces requested by TAC immediately. If you do, the files are not overwritten before you can gather them.

In this scenario, you need to collect CallManager traces, CTI Manager traces, and all Event Viewer logs. Unless TAC has given you other instructions, you need to collect those files from all servers for the complete time range that covers your test call or calls. This prevents the lost of traces from a server that you did not know was in the call flow.

1. Launch the RTMT.
2. Connect to the IP address of your CUCM Publisher.
3. Log on with the same credentials you use for the CUCM Administration web page.
4. Choose **System > Tools > Trace & Log Central**.



5. Double-click **Collect Files**. The Collect Files window opens to Select UCM Services/Applications.
6. In Select UCM Services/Applications, click the check box in the All Servers column for: Cisco CTIManagerCisco CallManager

Collect Files

Select UCM Services/Applications

☐ Select all Services on all Servers

Name	All Servers	<input type="checkbox"/> goesto11pub	
Cisco AXL Web Service	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Bulk Provisioning Service	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CAR Web Service	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CDR Agent	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CDR Repository Manager	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CDR files on CM server	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CDR files on Publisher Processed	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CTIManager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Cisco CTL Provider	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco CallManager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Cisco CallManager SNMP Service	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Certificate Authority Proxy Function	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Change Credential Application	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco DHCP Monitor Service	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Dialed Number Analyzer	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Dialed Number Analyzer Server	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Directory Number Alias Lookup	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Directory Number Alias Sync	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Extended Functions	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Extended Functions Report	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Extension Mobility	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Extension Mobility Application	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco IP Manager Assistant	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco IP Voice Media Streaming App	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Intercluster Lookup Service	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco License Manager	<input type="checkbox"/>	<input type="checkbox"/>	
Cisco Location Bandwidth Manager	<input type="checkbox"/>	<input type="checkbox"/>	

< Back **Next >** Finish Cancel

7. Click **Next**. The Collect Files window advances to Select System Services/Applications.
8. In Select System Services/Applications, click the check box in the All Servers column for:
Event Viewer-Application LogEvent Viewer-System Log

Collect Files

Select System Services/Applications

☐ Select all Services on all Servers

Name	All Servers	<input type="checkbox"/> goesto11pub
Cisco Serviceability Reporter ServiceReport	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Stored Procedure Trace	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Syslog Agent	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Tomcat	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Tomcat Security Logs	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Tomcat Stats Servlet	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Trace Collection Service	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Unified OS Admin Web Service	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Unified OS Platform API	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Unified Reporting Web Service	<input type="checkbox"/>	<input type="checkbox"/>
Cisco WebDialerRedirector Web Service	<input type="checkbox"/>	<input type="checkbox"/>
Cron Logs	<input type="checkbox"/>	<input type="checkbox"/>
Event Viewer-Application Log	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Event Viewer-System Log	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FIPS Logs	<input type="checkbox"/>	<input type="checkbox"/>
Host Resources Agent	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CLI Created Reports	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CLI Logs	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform Cert Monitor Logs	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CertMgr Logs	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform Cluster Manager Logs	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform GUI Logs	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform IPSecMgmt Logs	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform RemoteSupport Logs	<input type="checkbox"/>	<input type="checkbox"/>
Install File Signing	<input type="checkbox"/>	<input type="checkbox"/>
Install and Upgrade Logs	<input type="checkbox"/>	<input type="checkbox"/>
Kerneldump Logs	<input type="checkbox"/>	<input type="checkbox"/>

< Back Next > Finish Cancel

9. Click **Next**. The Collect Files window advances to the Collect File Options screen.
10. Configure your Collection Time: As you have timestamps for your test call(s), click the **Absolute Range** radio button. From the **From Date/Time** drop-down list, choose the time for one minute before your first test call. From the **To Date/Time** drop-down list, choose the time for one minute after your last test call.
11. Configure your Download File Options. Click **Browse** in order to configure your Download File Directory and specify a new directory for each trace file collection. For example, when you want to download these files to Desktop\TAC\callrectest01. Traces for a later test could go to Desktop\TAC\callrectest02. This keeps the collected file sets for each issue reproduction organized and separated. Leave all other settings set to the defaults.

Collect Files

Collect File Options:

Collection Time

☒ Absolute Range

Select Reference Server Time Zone: Client:(GMT-5:0)Eastern Daylight Time-America/New_York

From Date/Time: 7/22/16 - 1:05 PM

To Date/Time: 7/22/16 - 1:15 PM

☐ Relative Range

Files Generated in the last: 5 Minutes

Download File Options

Select Partition: Active Partition

Download File Directory: c:\Desktop\TAC\07222016_106_PM_callrec_fail **Browse**

☐ Zip Files

☒ Do Not Zip Files

☐ Uncompress Log Files

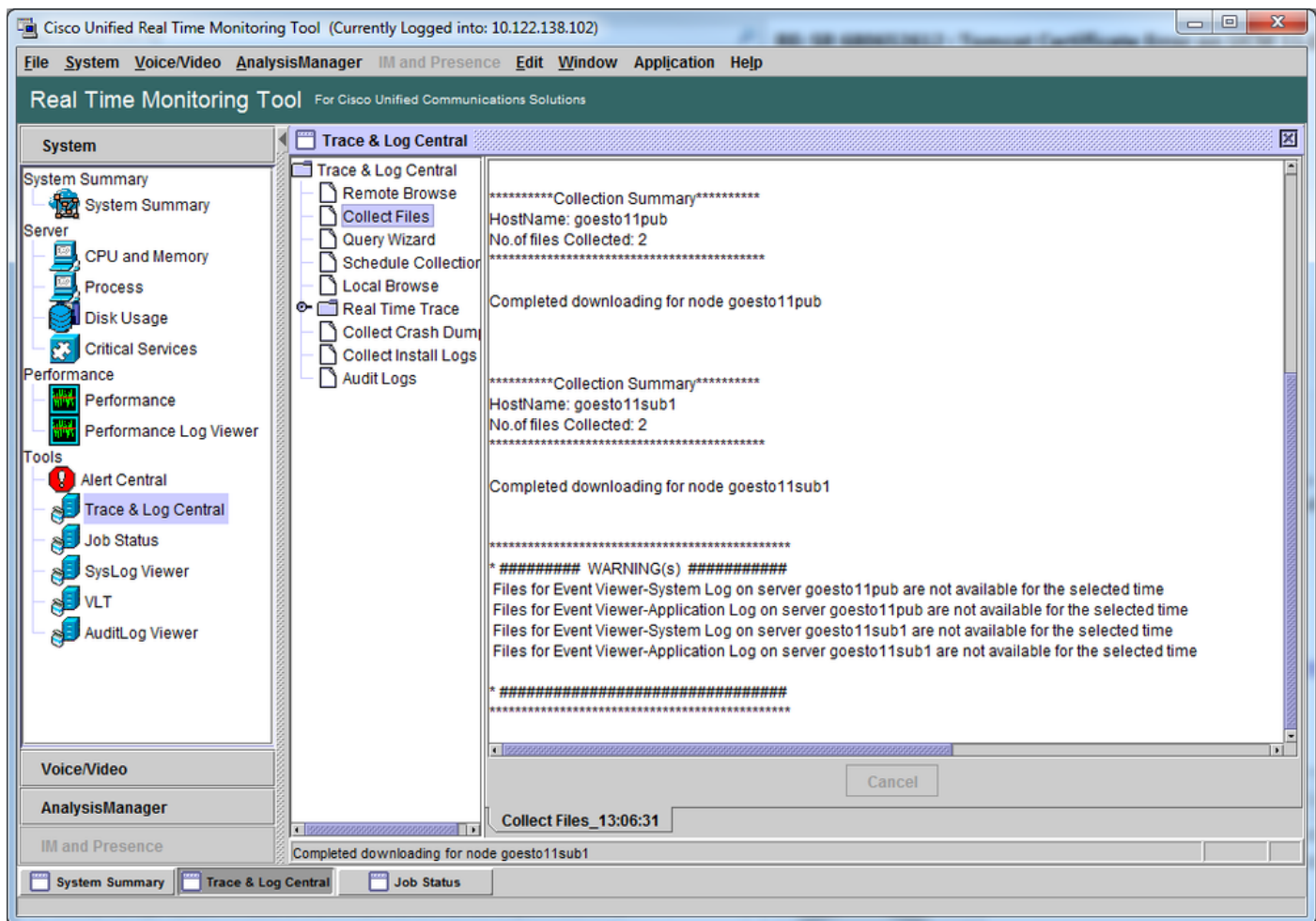
☐ Delete Collected Log Files from Server

Note: The result file can be found in the directory named <Node Name> created under the user specified directory structure. The File Name is as specified by the user.

< Back Next > Finish Cancel

12. Click **Finish**.

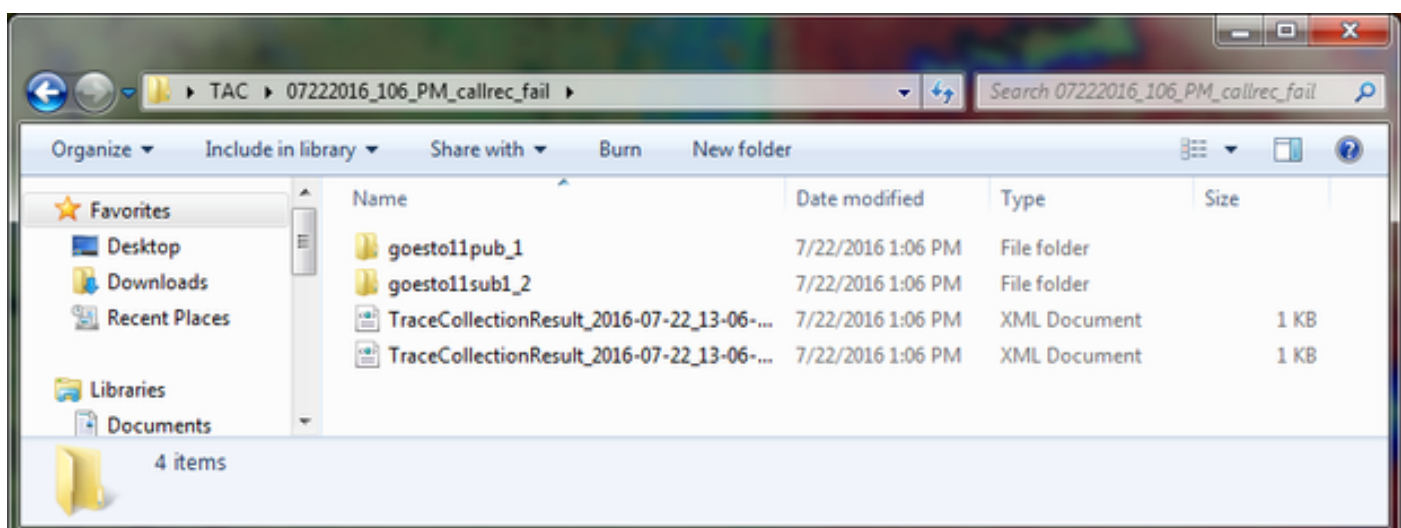
The Collect Files window updates with the status of trace collection. While trace collection continues, you can see a **Cancel** button is available. When collection is complete, the **Cancel** button is grayed out.



Verify Trace File Coverage

Review the files that you have gathered in order to ensure they cover the problem time frame. The simplest way to do this is to review the **TraceCollectionResult*.xml** files.

When RTMT collects a set of files, it writes a **TraceCollectionResult*.xml** file to the download file directory for each server that it collects data from. You can see these files along with subdirectories for each CUCM server. The **TraceCollectionResult*.xml** files state which files were successfully downloaded from each server. The subdirectories contain the actual trace and log files.



Open each TraceCollectionResult file and observe whether the modified date for the listed file or files maps to the date and time range for your trace collection. If trace files could not be collected, for example, they are overwritten, then they are lost.



If you are familiar with earlier versions of CUCM, this version differs in that the Cisco CallManager traces are a single set of SDL* traces, not a set of SDL* traces and a set of ccm* traces. This is because, in CUCM 9.X and later, traces are interwoven into a single set of files which makes analysis easier. The same is true for the Cisco CTI Manager service. Instead of both the SDL* traces and cti* traces, all of the data is in the SDL* traces for that service.

Trace collection issues can usually be avoided if you collect traces immediately after an issue reproduction.

Note: The TraceCollectionResult*.xml files simply contain a list of files which were successfully collected from each CUCM server. TAC needs to review the actual trace and log files that were collected.

Attach a Trace Package to Your Service Request

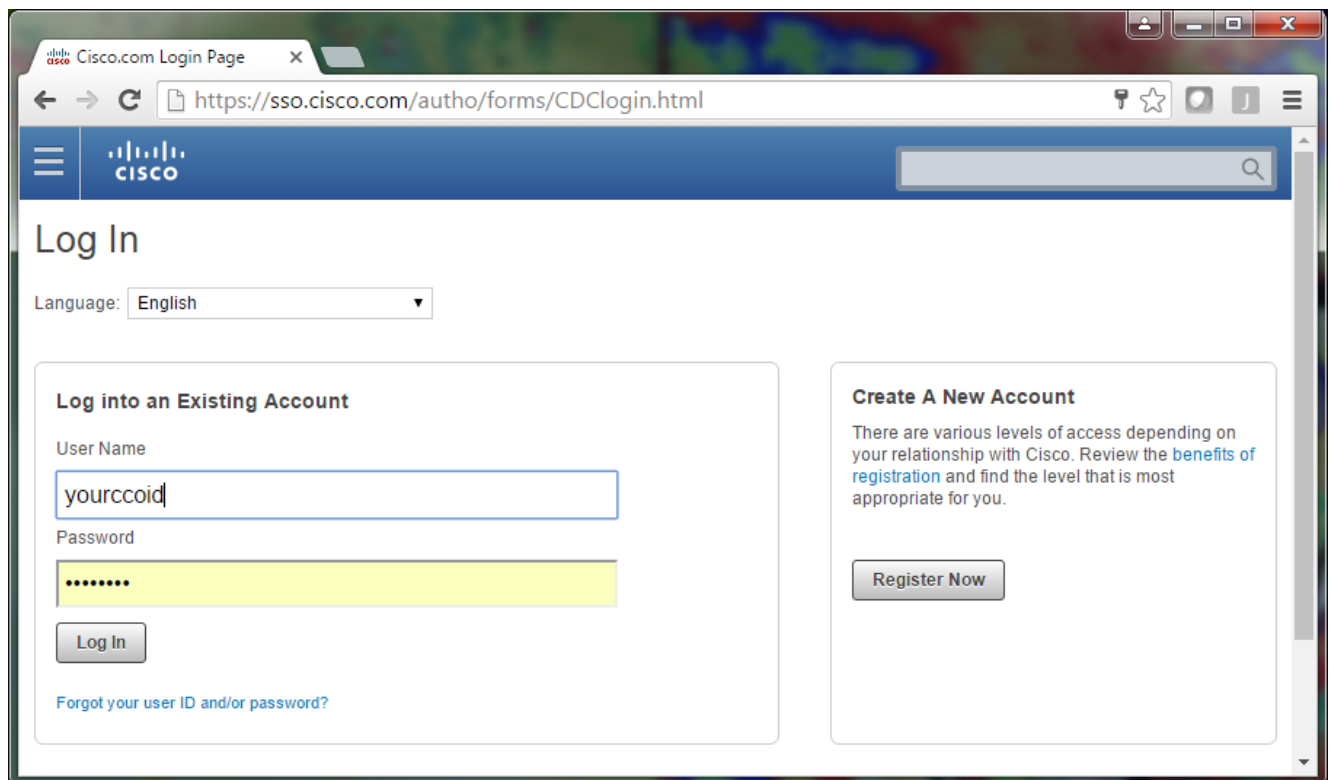
Now that you have a complete set of traces for your issue reproduction call, you need send them to your TAC engineer.

When you downloaded the traces, you specified a new download file directory. This directory now contains all of the log and trace files, as well as the TraceCollectionResult*.xml files. TAC requires you to send all of the contents of the download file directory, not just one or two files.

In order to make this simple, upload a single .zip file with the Case File Uploader tool:

1. Compress the entire download file directory to a single .zip archive file.
2. Browse to the [Support Case Manager](#).

You are redirected to a log in page. Log in with your CCO username and password.



The screenshot shows the Cisco.com Login Page in a web browser. The address bar displays `https://sso.cisco.com/autho/forms/CDClogin.html`. The page features the Cisco logo and a search bar at the top. Below the header, the "Log In" section includes a language dropdown set to "English". There are two main options: "Log into an Existing Account" and "Create A New Account". The "Log into an Existing Account" section contains fields for "User Name" (with the text "yourccoid" entered) and "Password" (masked with dots). A "Log In" button is positioned below these fields, along with a link for "Forgot your user ID and/or password?". The "Create A New Account" section provides information about access levels and a "Register Now" button.

Cisco.com Login Page

https://sso.cisco.com/autho/forms/CDClogin.html

Log In

Language: English

Log into an Existing Account

User Name

yourccoid

Password

.....

Log In

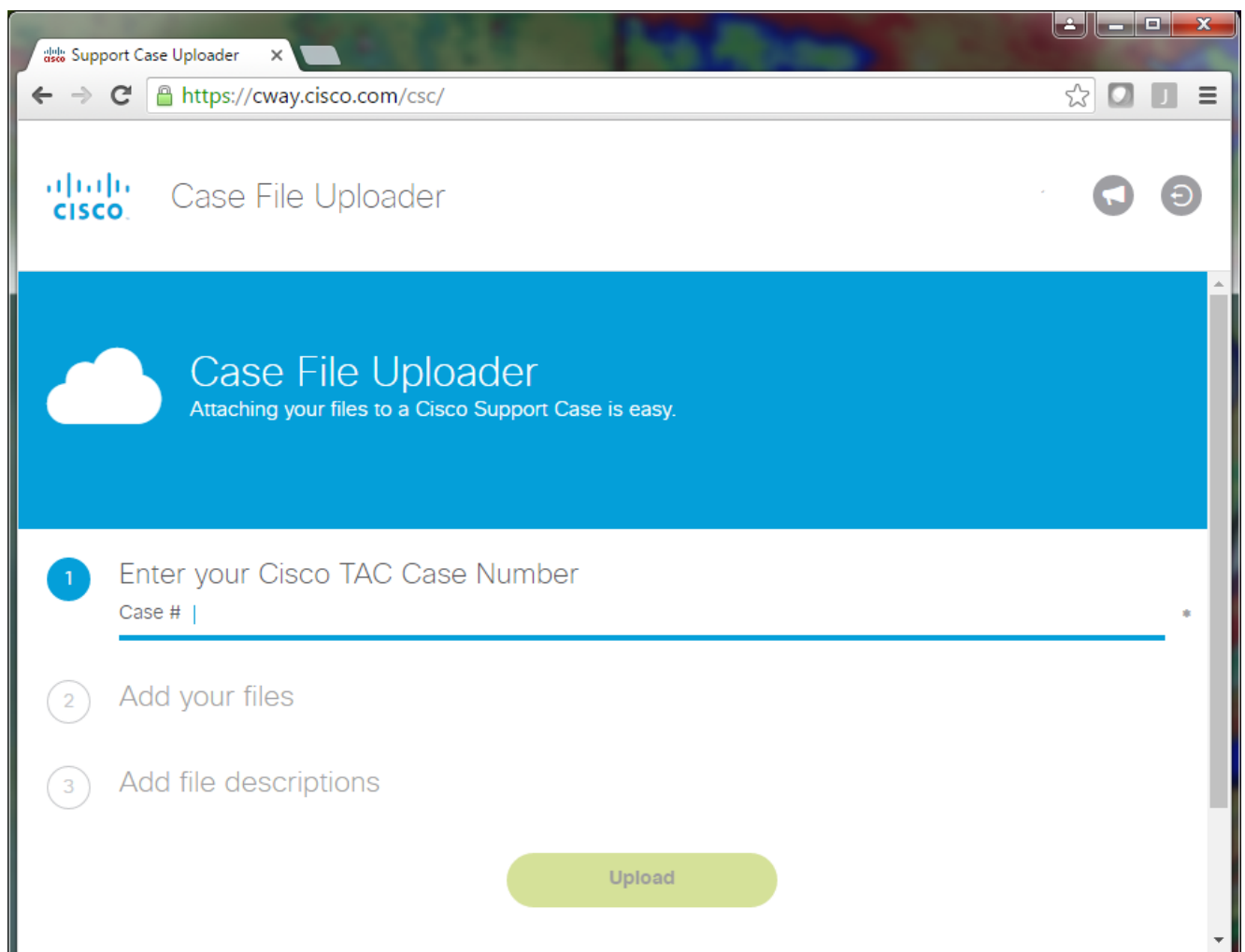
[Forgot your user ID and/or password?](#)

Create A New Account

There are various levels of access depending on your relationship with Cisco. Review the [benefits of registration](#) and find the level that is most appropriate for you.

Register Now

This brings you to the Case File Uploader tool.



The screenshot shows the Case File Uploader tool in a web browser. The address bar displays `https://cway.cisco.com/csc/`. The page features the Cisco logo and the title "Case File Uploader". Below the header, there is a blue banner with a cloud icon and the text "Case File Uploader" and "Attaching your files to a Cisco Support Case is easy." Below the banner, there are three numbered steps: 1. Enter your Cisco TAC Case Number (with a "Case #" input field), 2. Add your files, and 3. Add file descriptions. At the bottom, there is a green "Upload" button.

Support Case Uploader

https://cway.cisco.com/csc/

Case File Uploader

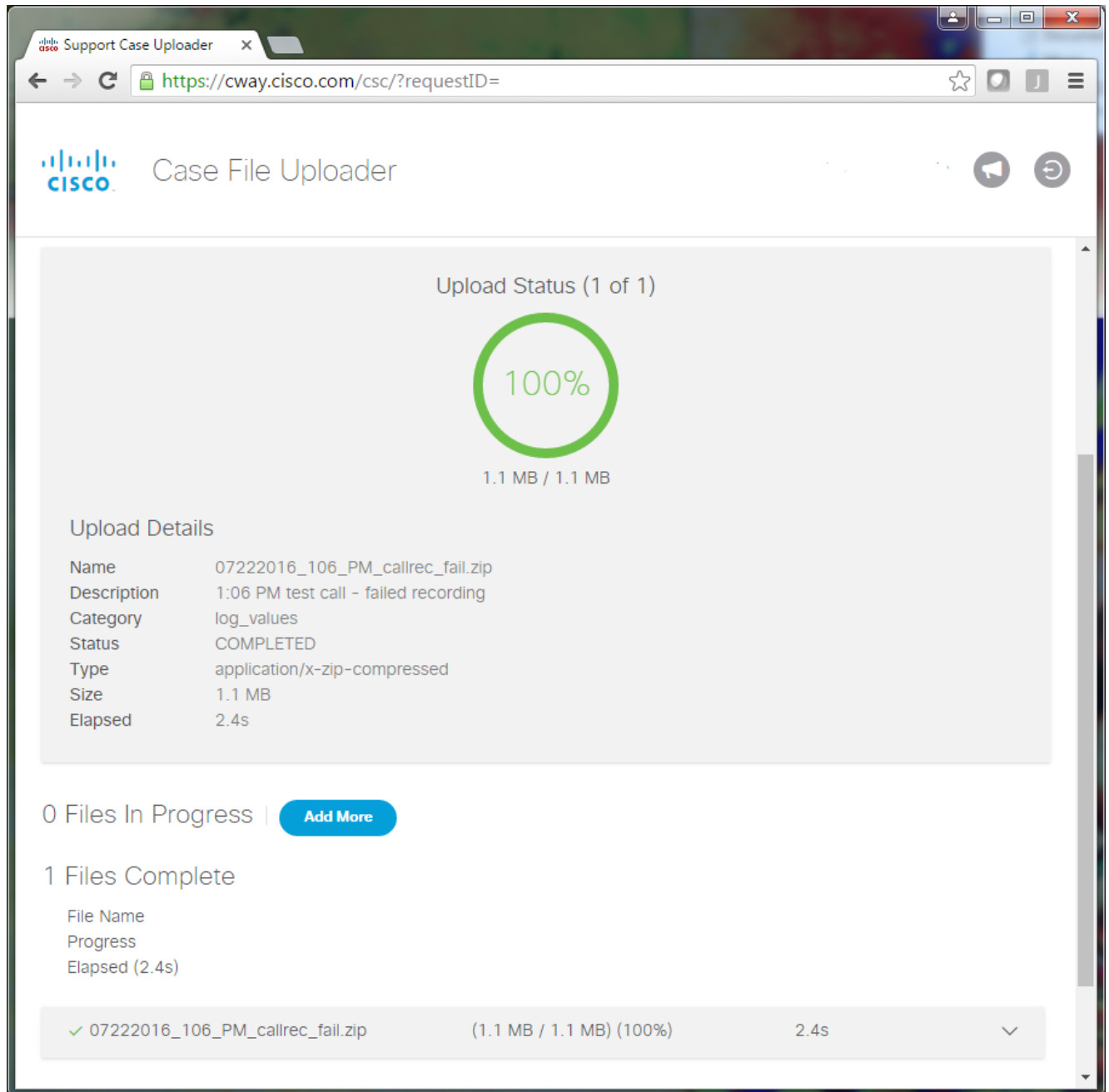
Case File Uploader

Attaching your files to a Cisco Support Case is easy.

- 1 Enter your Cisco TAC Case Number
Case # |
- 2 Add your files
- 3 Add file descriptions

Upload

3. Enter your service request number.
4. Add your .zip file.
5. Add a file description for your TAC engineer. This is a good opportunity to communicate your issue reproduction notes.
6. Click **Upload**. The Case File Uploader tool displays the upload status. Wait for the upload to complete.



7. Close the browser window.
8. Ensure that you have communicated to your TAC engineer all of your issue reproduction notes whether this was through the upload tool, via email, or verbally. This allows them to start to analyze the data for you.

Analysis

The Cisco CallManager/CTI Manager traces related to the specific call can be analyzed by the

Collaboration Solutions Analyzer tool (ladder diagram/annotations/filtered logs/diagnostic signatures). Check the documentation on how to use the tool:

- [Collaboration Solutions Analyzer User Documentation](#)
- [Collaboration Solutions Analyzer](#)