**Main page:** Cisco Unified Presence, Release 7.x

## Contents



**Previous Topic**

- How to Configure Trace and Log Central in RTMT

# About Trace Collection

You can use Trace and Log Central, an option in the Cisco Unified Presence Real-Time Monitoring Tool (RTMT), to collect, view, and zip various service traces and/or other log files. With the Trace and Log Central option, you can collect SDI traces, Application Logs, System Logs (such as Event View Application, Security, and System logs), and crash dump files.

The Trace and Log Central feature allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or collect a crash dump file. After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

Consider the following recommendations:

- To collect CSA logs, check **Cisco Security Agent** in the Select System Services/Applications tab in RTMT. To access user logs that provide information about users that are logging in and out, check **Security Logs** in the Select System Services/Applications tab.
- For devices that support encryption, the SRTP keying material does not display in the trace file.
- From RTMT, you can also edit the trace setting for the traces on the server that you have specified. Enabling trace settings decreases system performance; therefore, enable Trace only for troubleshooting purposes.
- Do not use NotePad to view collected trace files.

- Time Zone and Date Range for Trace Collection

- Logs for Trace Collection

## Time Zone and Date Range for Trace Collection

The time zone of the client computer provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone list box.

The trace or crash dump files that get modified in the date range (between the From date and the To date), get collected if the chosen time zone matches the time zone settings of the server (for example Server 1). If another server exists in the same Cisco Unified Presence cluster (Server 2), but that server resides in a different time zone, then the files that get modified in the corresponding date range in Server 2 will get collected from Server 2.

- **Absolute Range**-Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.
- **Relative Range**-Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

**Related Topics**

- Getting More Information

## Logs for Trace Collection

Cisco Unified Serviceability stores logs for up to two Linux-based versions of Cisco Unified Presence. Cisco Unified Serviceability stores the logs for the version of Cisco Unified Presence that you are logged in to in the active partition and stores the logs for the other version of Cisco Unified Presence (if installed) in the inactive directory.

When you upgrade from one version of Cisco Unified Presence that is running on the Linux platform to another and log in to the new version of Cisco Unified Presence that is running on the Linux platform, Cisco Unified Serviceability moves the logs from the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version of Cisco Unified Presence, Cisco Unified Serviceability moves the logs for the newer version of Cisco Unified Presence to the inactive partition and stores the logs for the older version in the active directory.

**Note:** Cisco Unified Serviceability does not retain logs from Cisco Unified Presence versions that ran on the Windows platform.

**Related Topics**

- Getting More Information