



Traces Used To Troubleshoot IM and Presence Service

- [Troubleshooting IM and Presence Service Using Trace](#), on page 1
- [Common Traces and Log File Locations for IM and Presence Service Nodes](#), on page 2
- [IM and Presence Service Login and Authentication Traces](#), on page 3
- [Availability, IM, Contact List, and Group Chat Traces](#), on page 3
- [Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues](#), on page 4
- [Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues](#), on page 5
- [Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues](#), on page 6
- [Calendaring Traces](#), on page 6
- [Intercluster Synchronization Traces and Inter-Clustering Troubleshooter](#), on page 7
- [SIP Federation Traces](#), on page 7
- [XMPP Federation Traces](#), on page 8
- [High CPU and Low VM Alert Troubleshooting](#), on page 8

Troubleshooting IM and Presence Service Using Trace

You can initiate traces using Cisco Unified IM and Presence Serviceability to help you troubleshoot issues with your IM and Presence Service deployment. After the traces are enabled, you can use either the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) to access the trace log files.

For instructions on using Serviceability traces for IM and Presence Service, see the *Cisco Unified Serviceability Administration Guide*. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands such as **file list** and **file get** to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.



Tip Use only SFTP servers for file transfers using CLI commands such as **file get**.

Common Traces and Log File Locations for IM and Presence Service Nodes

The following table lists common traces that you can perform on your IM and Presence Service node and the resulting log files. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 1: Common Traces and Trace Log Files for IM and Presence Service Nodes

Service	Trace Log Filename
Cisco AXL Web Service	/tomcat/logs/axl/log4j/axl.log
Cisco Intercluster Sync Agent	/epas/trace/epassa/log4j/icSyncAgent.log
Cisco Presence Engine	/epas/trace/epe/sdi/epe.txt
Cisco SIP Proxy	/epas/trace/esp/sdi/esp.txt
Cisco Syslog Agent	/cm/trace/syslogmib/sdi/syslogmib.txt
Cisco Tomcat Security Log	/tomcat/logs/security/log4/security*.log
Cisco XCP Authentication Service	/epas/trace/xcp/log/auth-svc-1*.log
Cisco XCP Client Connection Manager	/epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Config Manager	/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr.log
Cisco XCP Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log
Cisco XCP Text Conferencing Manager	/epas/trace/xcp/log/txt-conf-1*.log
Cisco XCP XMPP Federation Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cluster Manager	/platform/log/clustermgr*
Client Profile Agent (CPA)	/tomcat/logs/epassoap/log4j/EPASSoap*.log

Service	Trace Log Filename
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

IM and Presence Service Login and Authentication Traces

If IM and Presence Service users experience issues signing into their client software, you can run traces on the IM and Presence Service node on which the user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 2: Traces Used to Investigate Login and Authentication Issues

Service	Trace Log Filename
Cisco Client Profile Agent (CPA)	/tomcat/logs/epassoap/log4j/EPASSoap*.log
Cisco XCP Connection Manager	/epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco XCP Authentication Service	/epas/trace/xcp/logs/auth-svc-1*.log
Cisco Tomcat Security Logs	/tomcat/logs/security/log4/security*.log

Availability, IM, Contact List, and Group Chat Traces

You can run traces to troubleshoot Availability, IM, contact list, and group chat issues for your IM and Presence Service deployment.

The following table lists the recommended services to trace for commonly encountered issues.

Table 3: Recommended Traces for Availability, IM, Contact List, and Group Chat Issues

Issue/Solution	Services
End user has no availability status displayed or incorrect availability status for some or all of their contacts. Perform traces for the listed services on the IM and Presence Service node on which the end users and contacts are provisioned.	<ul style="list-style-type: none"> • Cisco XCP Connection Manager • Cisco XCP Router • Cisco Presence Engine
End user has issues with their self availability status, including on-the-phone or meeting status. Perform traces for the listed services on the IM and Presence Service node on which the end user is provisioned.	<ul style="list-style-type: none"> • Cisco XCP Connection Manager • Cisco XCP Router • Cisco Presence Engine

Issue/Solution	Services
<p>End user has issues sending or receiving instant messages.</p> <p>Perform traces for the listed services on the IM and Presence Service nodes on which the sender and recipient are provisioned.</p>	<ul style="list-style-type: none"> • Cisco XCP Connection Manager • Cisco XCP Router
<p>End user is experiencing any of the following issues:</p> <ul style="list-style-type: none"> • Difficulty creating or joining a chat room. • Chat room messages are not being delivered to all members. • Any other issues with the chat room. <p>Perform traces for the listed services on the IM and Presence Service node on which the chat room members are provisioned.</p>	<ul style="list-style-type: none"> • Cisco XCP Connection Manager • Cisco XCP Router • Cisco XCP Text Conferencing Manager
<p>The node on which the chat room that is experiencing difficulties is hosted and the node on which the creator is provisioned are not the same.</p> <p>Perform an initial trace analysis to determine which node hosted the chat room. Then perform traces for the following services on the IM and Presence Service node that hosted the chat room.</p>	<ul style="list-style-type: none"> • Cisco XCP Text Conferencing Manager • Cisco XCP Router

After the traces are complete, you can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

- Cisco Presence Engine: /epas/trace/epe/sdi/epe*.txt
- Cisco XCP Connection Manager: /epas/trace/xcp/log/client-cm-1*.log.gz
- Cisco XCP Router: /epas/trace/xcp/log/rtr-jsm-1*.log
- Cisco XCP Text Conferencing Manager: /epas/trace/xcp/log/txt-conf-1*.log

Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues

If the local IM and Presence Service user is unable to exchange availability or instant messages with an intradomain Microsoft Office Communicator (MOC) contact, you can run traces on the IM and Presence Service node on which the local user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 4: Traces Used to Investigate Availability and IM Issues with Partitioned Intradomain Federation MOC Contacts

Services	Trace Log Filename
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log
Cisco SIP Proxy	/epas/trace/esp/sdi/esp.txt
Cisco Presence Engine	/epas/trace/epe/sdi/epe.txt



Note Cisco SIP Proxy debug logging is required to see the sip message exchange.

Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues

If the local IM and Presence Service user is unable to exchange availability status or instant messages with an interdomain federation contact, you can run traces on the IM and Presence Service node on which the local user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 5: Traces Used to Investigate Availability and IM Issues for XMPP-based Interdomain Federation Contacts

Services	Trace Log Filename
Cisco XCP Connection Manager	/epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco Presence Engine	/epas/trace/epe/sdi/epe*.txt
Cisco XCP XMPP Federation Connection Manager Perform this trace on each IM and Presence Service node on which XMPP federation is enabled.	/epas/trace/xcp/log/xmpp-cm-4*.log

Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues

If the local IM and Presence Service user is unable to exchange availability status or instant messages with an interdomain federation contact, you can run traces on the IM and Presence Service node on which the local user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 6: Traces Used to Investigate Availability and IM Issues for XMPP-based Interdomain Federation Contacts

Services	Trace Log Filename
Cisco XCP Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco Presence Engine	/epas/trace/epe/sdi/epe.txt
Cisco SIP Proxy	/epas/trace/esp/sdi/esp.txt
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log

Calendaring Traces

You can run traces to troubleshoot calendaring issues for your IM and Presence Service deployment. The following table lists the service to trace.

After the trace is complete, you can view the resulting log file using the Real-Time Monitoring Tool (RTMT) and filter your search in the resulting Cisco Presence Engine log file. Look for instances of “.owa.” and “.ews.”. You can also use command line interface (CLI) commands such as **file list** and **file get** to view the log file results. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 7: Trace Used to Investigate Calendaring Issues

Service	Trace Log Filename
Cisco Presence Engine	/epas/trace/epe/sdi/epe*.txt

Intercluster Synchronization Traces and Inter-Clustering Troubleshooter

If an IM and Presence Service node generates alerts that indicate there are intercluster synchronization issues with another node in your deployment, you can run traces on the nodes that are not synchronizing to diagnose the issue. After the traces are complete, you can view the resulting log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

You can also check for synchronization errors using the Cisco Unified CM IM and Presence Administration GUI when you select **Diagnostics > System Troubleshooter** and navigate to **Inter-Clustering Troubleshooter**. You can capture a screen snap of the page.

The following table lists the services to trace for intercluster synchronization issues. Perform traces for the listed services on each IM and Presence Service node that is experiencing intercluster synchronization issues.

Table 8: Traces Used to Investigate Intercluster Synchronization Issues Between Nodes

Service	Trace Log Filename
Cisco Intercluster Sync Agent	/epas/trace/epassa/log4j/icSyncAgent*.log
Cisco AXL Web Service	/tomcat/logs/axl/log4j/axl*.log
Cisco Tomcat Security Log	/tomcat/logs/security/log4j/security*.log
Cisco Syslog Agent	/cm/trace/syslogmib/sdi/syslogmib*.txt

SIP Federation Traces

You can run traces to troubleshoot SIP federation issues for your IM and Presence Service deployment. The following table lists the services to trace.

After the traces are complete, you can view the resulting log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 9: Traces Used to Investigate Login and Authentication Issues

Service	Trace Log Filename
Cisco SIP Proxy	/epas/trace/esp/sdi/esp*.txt
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log

Service	Trace Log Filename
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log

XMPP Federation Traces

You can run traces to troubleshoot XMPP federation issues on your IM and Presence Service deployment. The following table lists the services to trace.

After the traces are complete, you can view the resulting log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Table 10: Traces Used to Investigate XMPP Federation Issues

Service	Trace Log Filename
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco XCP XMPP Federation Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log

High CPU and Low VM Alert Troubleshooting

If an IM and Presence Service node is generating high CPU or low VM availability alerts, you can collect information from the node using the Command Line Interface (CLI) to help troubleshoot the cause. You can also run traces on related services on the node, and then view the resulting log files using the Real-Time Monitoring Tool (RTMT). For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

You can also setup Cisco Unified IM and Presence Serviceability alarms to provide information about runtime status and the state of the system to local system logs. IM and Presence Service writes system errors in the Application Logs that you view using the SysLog Viewer in RTMT. For more information about setting up syslog alarms for a service, see the *Cisco Unified Serviceability Administration Guide*. For information about viewing alarm information using the SysLog Viewer, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Table 11: CLI Commands Used to Investigate High CPU and Low VM Alerts

Solution	CLI Command
Use the CLI to run the following commands on the node.	<pre>show process using-most cpu show process using-most memory utils dbrplication runtimestate utils service list</pre>

Solution	CLI Command
Use the CLI to collect all RIS (Real-time Information Service) performance logs for the node. Use only SFTP servers for file transfers using file get .	<code>file get activelog cm/log/ris/csv</code>

The following table lists the services to select when you run traces on the IM and Presence Service node to investigate high CPU and low VM alerts. Perform traces for the listed services on the IM and Presence Service node that is generating high CPU or low VM alerts.

Table 12: Traces Used to Investigate High CPU and Low VM Alerts

Services	Trace Log Filename
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log
Cisco SIP Proxy	/epas/trace/esp/sdi/esp*.txt
Cisco Presence Engine	/epas/trace/epe/sdi/epe*.txt
Cisco Tomcat Security Log	/tomcat/logs/security/log4/security*.log
Cisco Syslog Agent	/cm/trace/syslogmib/sdi/syslogmib*.txt

