Troubleshoot the System

Troubleshooting Overview

Use the procedures in this chapter to troubleshoot issues with your IM and Presence deployment. With your IM and Presence Service deployment, you can:

- Use the Command Line Interface (CLI) to build trace logs that you can use to check to resolve issues.
- Run diagnostics, to check for issues with your system.
- Run the system troubleshooter to confirm the health of your system.
- Troubleshoot duplicate directory URI issues.

Run the System Troubleshooter

Run the troubleshooter to diagnose issues with your IM and Presence Service deployment. The troubleshooter checks automatically for a wide range of issues with your deployment including:

- System Issues
- Sync Agent Issues
- Presence Engine Issues
- SIP Proxy Issues
- Microsoft RCC Issues
- Calendaring Issues
- Inter-clustering Issues
- Topology Issues

- Cisco Jabber Redundancy Assignments
- External Database entries
- Third-Party Compliance Server
- Third-Party LDAP Connection
- LDAP Connection
- XCP Staus
- User Configuration

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. The troubleshooter runs a series of automated checks against your system. The results display in the **System Configuration Troubleshooter** window.

Step 2 Resolve any issues that the troubleshooter highlights.

Run Diagnostics

When administering an up and running system, you may encounter problems which affect the normal running of the system. You can use the IM and Presence Service Diagnostic tools to help determine the root causes of these problems.

Use this procedure to access the Diagnostic tools on IM and Presence Service.

These tools can be accessed in **Cisco Unified CM IM and Presence Administration** by clicking **Diagnostics** and choosing from one of these options:

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Diagnostics**.

Step 2 Click the Diagnostic tool you want to use from the drop-down list.

See Diagnostic Tools Overview for more on the purpose of these tools.

Diagnostic Tools Overview

Diagnostic Tool	Purpose
System Dashboard	Use the System Dashboard to acquire a snapshot of the state of your IM and Presence Service system including a summary data view of these system components - number of devices, number of users, per-user data such as contacts, and primary extension.
System Configuration Troubleshooter	Use the System Configuration Troubleshooter to diagnose IM and Presence Service configuration issues after your initial configuration or whenever you make configuration changes. The Troubleshooter performs a set of tests on both the IM and Presence Service cluster and on the Cisco Unified Communications Manager cluster to validate the IM and Presence Service configuration. After the Troubleshooter finishes testing, it reports one of three possible states for each test: • Test Passed • Test Failed • Test Warning, which indicates a possible configuration issue For each test that fails or that results in a warning, the Troubleshooter provides a description of the problem and a possible solution. For any test failures or test warnings, click the fix link in the solution column to go to the Cisco Unified Communications Manager IM and Presence Administration window where the Troubleshooter found the problem. Correct any configuration errors that you find and rerun the Troubleshooter.
Microsoft RCC Troubleshooter	Use the Microsoft Remote Call Control (RCC) Troubleshooter to diagnose integration issues between IM and Presence Service and the Microsoft Lync or Microsoft Office client application after your initial configuration or whenever you make configuration changes. The Troubleshooter validates user-related and connectivity-related issues between Microsoft Lync, LCS, or OCS servers and the IM and Presence Service, and between the Microsoft Lync or Microsoft Office client and the IM and Presence Service.

Using Trace Logs for Troubleshooting

Use traces to troubleshoot system issues with IM and Presence services and features. You can configure automated system tracing for a variety of services, features, and system components. The results are stored in system logs that you can browse and view using the Cisco Unified Real-Time Monitoring Tool. Alternatively, you can use the Command Line Interface to pull a subset of the system log files and upload them to your own PC or laptop for further analysis.

To use traces, you must first configure the system for tracing. For details on how to configure system tracing, refer to the "Traces" chapter of the *Cisco Unified Serviceability Administration Guide*.

Once tracing is configured, you can use one of two methods to view the contents of trace files:

- Real-Time Monitoring Tool—With the Real-Time Monitoring Tool, you can browse and view the individual log files that are created as a result of system tracing. For details on how to use the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.
- Command Line Interface (CLI)—If system tracing is configured, use the CLI to build customized traces from your system logs. With the CLI, you can specify the specific days that you want to include in a customized trace file. The CLI pulls the associated trace files from your system and saves them in a compressed zip file that you can copy to a PC or laptop for further analysis, thereby ensuring that the logs don't get overwritten by the system.

  The susequent tables and tasks in this section describe how to use CLI commands to build trace log files for the IM and Presence Service.

Common IM and Presence Issues via Trace

The following table lists common issues with the IM and Presence Service and which traces you can run to troubleshoot the issue.

Table 1: Common IM and Presence Issue Troubleshooting

Issues with...	View Traces for These Services	Additional Instructions
Login and Authentication Traces	Client Profile Agent Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Authentication Service Cisco Tomcat Security Logs	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.
Availability Status	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.
Sending and Receiving IMs	Cisco XCP Connection Manager Cisco XCP Router	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.

Issues with...	View Traces for These Services	Additional Instructions
Contact Lists	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.
Chat Rooms	Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Text Conferencing Manager	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.
Partitioned Intradomain Federation	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations. **Note** Cisco SIP Proxy debug logging is required to see the SIP message exchange
Availability and IMs for XMPP Based Interdomain Federation Contact	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco XCP XMPP Federation Connection Manager	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations. Perform trace on each IM and Presence node on which XMPP Federation is enabled
Availability and IMs for SIP Interdomain Federation Contact	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco SIP Proxy Cisco XCP SIP Federation Connection Manager	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.
Calendaring Traces	Cisco Presence Engine	See Common Traces via CLI, on page 6 for CLI commands to build logs and output locations.
Intercluster Synchronization Traces and Intercluster Troubleshooter	Cisco Intercluster Sync Agent Cisco AXL Web Service Cisco Tomcat Security Log Cisco Syslog Agent	Run the system troubleshooter at **Diagnostics** > **System Troubleshooter** to check for interclustering errors.

Issues with...	View Traces for These Services	Additional Instructions
SIP Federation Traces	Cisco SIP Proxy Cisco XCP Router Cisco XCP SIP Federation Connection Manager	See Common Traces via CLI, on page 6 for CLI commands to build logs and file output locations.
XMPP Federation Traces	Cisco XCP Router Cisco XCP XMPP Federation Connection Manager	See Common Traces via CLI, on page 6 for CLI commands to build logs and file output locations.
High CPU and Low VM Alert Troubleshooting	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine Cisco Tomcat Security Log Cisco Syslog Agent	For additional troubleshooting, run the following CLI commands: • `show process using-most cpu` • `show process using-most memory` • `utils dbreplication runtimestate` • `utils service list` Run the following CLI to get RIS (Real-Time Information Service) data: • `file get activelog cm/log/ris/csv` 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.

Common Traces via CLI

Use the Command Line Interface to build trace log files to troubleshoot your system. With the CLI, you can choose the component for which you want to run a trace and specify the <duration>, which is the number of days looking backwards from today that you want to include in your log file.

The following two tables contain the CLI commands that you can use to build trace log files and the log output locations for:

- IM and Presence Services
- IM and Presence Features

Note The CLI pulls a subset of the same individual traces files that you can view with the Cisco Unified Real-Time Monitoring Tool (RTMT), but groups and stores them in a single compressed zip file. For RTMT traces, see Common Traces via RTMT, on page 11.

Table 2: Common Traces for IM and Presence Services using CLI

Service	CLI to Build Log	CLI Output File
Cisco Audit Logs	file build log cisco_audit_logs <duration>	`/epas/trace/log_cisco_audit_logs_*.tar.gz`
Cisco Client Profile Agent	file build log cisco_client_profile_agent <duration>	`/epas/trace/log_cisco_client_profile_agent_*.tar.gz`
Cisco Cluster Manager	file build log cisco_config_agent <duration>	`/epas/trace/log_cisco_cluster_manager_*.tar.gz`
Cisco Config Agent	file build log cisco_config_agent<duration>	`/epas/trace/log_cisco_config_agent_*.tar.gz`
Cisco Database Layer Monitor	file build log cisco_database_layer_monitor <duration>	`/epas/trace/log_cisco_database_layer_monitor_*.tar.gz`
Cisco Intercluster Sync Agent	file build log cisco_inter_cluster_sync_agent <duration>	`/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz`
Cisco OAM Agent	file build log cisco_oam_agent <duration>	`/epas/trace/log_cisco_oam_agent_*.gz`
Cisco Presence Engine	file build log cisco_presence_engine <duration>	`/epas/trace/log_cisco_presence_engine_*.tar.gz`
Cisco RIS (Real-time Information Service) Data Collector	file build log cisco_ris_data_collector <duration>	`/epas/trace/log_cisco_ris_data_collector_*.tar.gz`
Cisco Service Management	file build log cisco_service_management <duration>	`/epas/trace/log_cisco_service_management_*.tar.gz`
Cisco SIP Proxy	file build log cisco_sip_proxy <duration>	`/epas/trace/log_cisco_sip_proxy_*.tar.gz`
Cisco Sync Agent	file build log cisco_sync_agent <duration>	`/epas/trace/log_cisco_sync_agent_*.tar.gz`

Service	CLI to Build Log	CLI Output File
Cisco XCP Config Manager	file build log cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP Router	file build log cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

Table 3: Common Traces for IM and Presence Features using CLI

Feature Name	CLI to Build Log	CLI Output File
Administration GUI	file build log admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
Bulk Administration	file build log bat <duration>	/epas/trace/log_bat_*.tar.gz
Bidirectional Streams over Synchronous HTTP	file build log bosh <duration>	/epas/trace/log_bosh_*.tar.gz
Certificates	file build log certificates <duration>	/epas/trace/log_certificates_*.tar.gz
Config Agent Core	file build log cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
Customer Voice Portal	file build log cvp <duration>	/epas/trace/log_cvp_*.tar.gz
Directory Groups	file build log directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
Disaster Recovery	file build log disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
Flexible IM address	file build log flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz
General core	file build log general_core <duration>	/epas/trace/log_general_core_*.tar.gz
High Availability	file build log ha <duration>	/epas/trace/log_ha_*.tar.gz
High CPU	file build log high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz
High Memory	file build log high_memory <duration>	/epas/trace/log_high_memory_*.tar.gz
Instant Messaging Database Core	file build log imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz
Intercluster Peering	file build log inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz

Feature Name	CLI to Build Log	CLI Output File
Managed File Transfer	file build log managed_file_transfer <duration>	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	file build log msft_exchange <duration>	/epas/trace/log_msft_exchange_*.tar.gz
Message Archiver	file build log msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz
Presence Engine Core	file build log pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
Presence and IM Message Exchange	file build log presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP Login Issues	file build log pws <duration>	/epas/trace/log_pws_*.tar.gz
Remote Call Control	file build log remote_call_control <duration>	/epas/trace/log_remote_call_control_*.tar.gz
Security Vulnerabilities	file build log sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
Serviceability GUI	file build log serviceability_ui <duration>	/epas/trace/log_serviceability_ui_*.tar.gz
SIP Interdomain Federation	file build log sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_*.tar.gz
SIP Partitioned Intradomain Federation	file build log sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_*.tar.gz
SIP Proxy Core	file build log sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz
Persistent Chat High Availability	file build log tc_ha <duration>	/epas/trace/log_tc_ha_*.tar.gz
Persistent Chat	file build log text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
Upgrade Issues	file build log upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
User Connectivity	file build log user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
Rosters	file build log user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz

Feature Name	CLI to Build Log	CLI Output File
XCP Router Core	file build log xcp_core <duration>	`/epas/trace/log_xcp_core_*.tar.gz`
XMPP Interdomain Federation	file build log xmpp_inter_federation <duration>	`/epas/trace/log_xmpp_inter_federation_*.tar.gz`
Deployment Info	file build log deployment_info <duration>	`/epas/trace/log_deployment_info_*.tar.gz`

Run Traces via CLI

Use this procedure to create a customized trace file via the Command Line Interface (CLI). With the CLI, you can specify, via the duration parameter, the number of days looking backwards that you want to include in your trace. The CLI pulls a subset of the system logs.

Note Make sure to use SFTP servers only to transfer files.

Before you begin

You must have trace configured for your system. For details on setting up trace, see the "Trace" chapter of the *Cisco Unified Serviceability Administration Guide*.

Review Common Traces via CLI, on page 6 for a list of traces that you can run.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 To build the log, run the `file build log <name of service> <duration>` CLI command where duration is the number of days to include in the trace.

For example, `file build log cisco_cluster_manager 7` to view Cisco Cluster Manager logs for the past week.

Step 3 To get the log, run the `file get activelog <log filepath>` CLI command to get the trace files.

For example, **file get activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz**.

Step 4 To maintain a stable system, delete the log after you retrieve it. Run the `file delete activelog <filepath>` command to delete the log.

For example, `file delete activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`.

Common Traces via RTMT

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).

Note The CLI can be used to pull a subset of the same individual traces files that you can view with RTMT, but groups and stores them in a single compressed zip file. For CLI traces, see Common Traces via CLI, on page 6.

Note The following table shows the output locations for 11.5(1). Please note that automatic log file compression with gzip was introduced for many of these services as of release 11.5(1)SU2. For 11.5(1)SU2 and later details, see Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)SU2.

Table 4: Common Traces and Log Files for IM and Presence Nodes

Service	Trace Log Filename
Cisco AXL Web Services	`/tomcat/logs/axl/log4j/axl*.log`
Cisco Intercluster Sync Agent	`/epas/trace/cupicsa/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 Config Manager	`/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.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 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*.log`

Service	Trace Log Filename
Cisco Client Profile Agent (CPA)	`/tomcat/logs/epassoap/log4j/EPASSoap*.log`
dbmon	`/cm/trace/dbl/sdi/dbmon*.txt`

Troubleshooting UserID and Directory URI Errors

Received Duplicate UserID Error

Problem I received an alarm indicating that there are duplicate user IDs and I have to modify the contact information for those users.

Solution Perform the following steps.

1. Use the **utils users validate { all | userid | uri }** CLI command to generate a list of all users. For more information about using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

   The UserID is entered in the result set and is followed by the list of servers where the duplicate UserIDs are homed. The following sample CLI output shows UserID errors during output:

   ```
   Users with Duplicate User IDs
   ---------------------------------------------
    User ID: user3
     Node Name
     cucm-imp-1
     cucm-imp-2
   ```

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.
3. If different users on different clusters have the same User ID assigned to them, then rename the UserID value for one of the users to ensure there is no longer any duplication.
4. If the user information is invalid or empty, proceed to correct the user ID information for that user using the Cisco Unified Communications Manager Administration GUI.
5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

   Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate user ID errors.

Received Duplicate or Invalid Directory URI Error

Problem I received an alarm indicating that there are duplicate or invalid user Directory URIs and I have to modify the contact information for those users.

Solution Perform the following steps.

1. Use the **utils users validate { all | userid | uri }** CLI command to generate a list of all users. For more information about using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

   The Directory URI value is entered in the result set and is followed by the list of servers where the duplicate or invalid Directory URIs are homed. The following sample CLI output shows Directory URI errors detected during a validation check:

   ```
   Users with No Directory URI Configured
   ------------------------------------------------------
    Node Name: cucm-imp-2
    User ID
    user4

   Users with Invalid Directory URI Configured
   ------------------------------------------------------
    Node Name: cucm-imp-2
    User ID   Directory URI
    user1     asdf@ASDF@asdf@ADSF@cisco

   Users with Duplicate Directory URIs
   ------------------------------------------------------
   Directory URI: user1@cisco.com
    Node Name   User ID
    cucm-imp-1  user4
    cucm-imp-2  user3
   ```

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.
3. If different users on different clusters have the same Directory URI value assigned to them, then rename the Directory URI value for one of the users to ensure there is no longer any duplication.
4. If the user information is invalid or empty, proceed to correct the user's Directory URI information.
5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate or invalid Directory URI errors.