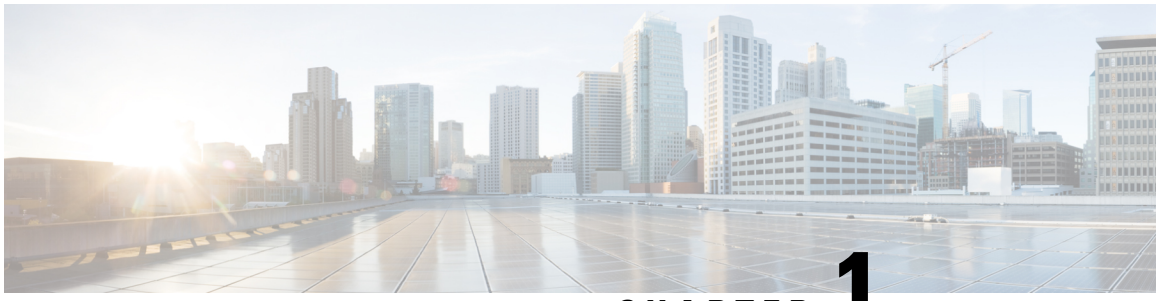
Instant Messaging Compliance for the IM and Presence Service

First Published: 2024-02-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

IM Compliance Overview

IM Compliance Overview

Many industries require that instant messages adhere to the same regulatory compliance guidelines as for all other business records. For these industries, your system must log and archive all business records, and archived records must be retrievable.

The IM and Presence Service has solutions that you can deploy to enable your system to meet compliance guidelines.

Compliance Solutions

This document describes the following two IM compliance solutions that you can deploy to enable your system to meet compliance guidelines.

Table 1: Compliance Solutions

Solution	Description
Message Archiver	The Message Archiver feature provides a basic IM compliance solution that allows your system to comply with regulations that require logging of all instant messaging traffic. The Message Archiver feature archives messages in single cluster, intercluster, or federated network configurations, including point-to-point messaging and various forms of group chat. You can configure the Message Archiver to either log all inbound instant message traffic or to log both inbound and outbound instant messaging traffic. This feature requires that you deploy an external database on which to store archived messages. To deploy the Message Archiver, go to Message Archiver Configuration, on page 5.

Solution	Description
Third-Party Compliance Server	For enhanced compliance functionality, including the ability to configure policies that determine which IMs and events are logged, you can integrate the IM and Presence Service with a third-party compliance server. With this solution, the IM and Presence Service integrates with one or more third-party compliance servers for compliance logging or ethical wall functionality. This solution allows the administrator to configure which IM, presence, or group chat events are passed to the compliance server(s), and which events are blocked. For example, the system could be configured to filter IMs between certain users, or groups of users, and block or modify content depending on the originator and recipient of the IMs. To deploy this integration, go to Third-Party Compliance Server Integration, on page 17.

Sample Topologies and Message Flow for IM Compliance

Note The external database requirements defined in this section depend on the capacity of your servers.

IM compliance provides logging of all compliance related data to an external database. All IM traffic passes through the IM and Presence Service node (via the message archiver component) and is simultaneously logged to the external database. Each IM log contains the sender and recipient information, the timestamp, and the message body.

For ad hoc group chat messages, by default IM and Presence Service logs multiple copies of the same message to the external database, one copy for each recipient. This identifies what users in the ad hoc group chat received the message.

Depending on the XMPP client you deploy, you may also notice this behavior:

- IM and Presence Service may log an incoming message to the external database twice. This occurs because some XMPP clients do not support the ability to learn the full JID, or address, of the other party in the conversation. Consequently the XMPP client forks the message to *all* active clients for the user (all clients that the user is currently signed into), and IM and Presence Service then logs all forked messages to the external database.
- IM and Presence Service may log the first message in a chat to the external database twice. This occurs until the XMPP client learns the full JID, or address, of the other party in the conversation.

If the IM and Presence Service loses its connection to the external database, it continues to send and deliver IMs to users, and users can still create (ad hoc) chat rooms. However, with no connection to the external database, the IM and Presence Service does not log any of these IMs. To maintain group chat support in this case, persistent chat should be assigned to a different database server. IM and Presence Service raises an alarm if the connection to the external database is lost.

Single Cluster Configuration

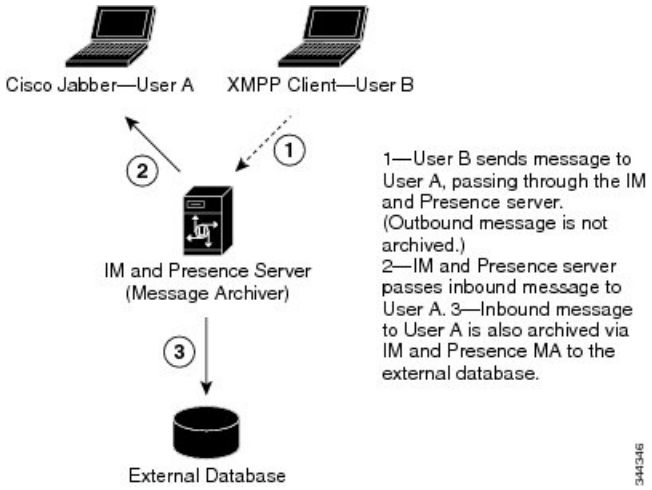
When using IM compliance in a single cluster, we highly recommend that you deploy one external database per cluster to which all incoming messages sent to users in the cluster are logged.

Note

- For IM compliance, we highly recommend that you deploy one external database per cluster. However, depending on your requirements, you can configure more than one external database per cluster, or share an external database between clusters.
- If you deploy the group chat feature, you *require* one external database *per presence redundancy group* in a cluster to support chat room failover. See *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .
- If group chat high availability is enabled, both the IM and Presence nodes on the presence redundancy group must be connected to a single external database.

The image below highlights these components and message flow. By default IM compliance logs inbound messages to the external database, however you can configure the feature to also log outgoing messages.

Figure 1: IM Compliance for a Single Cluster

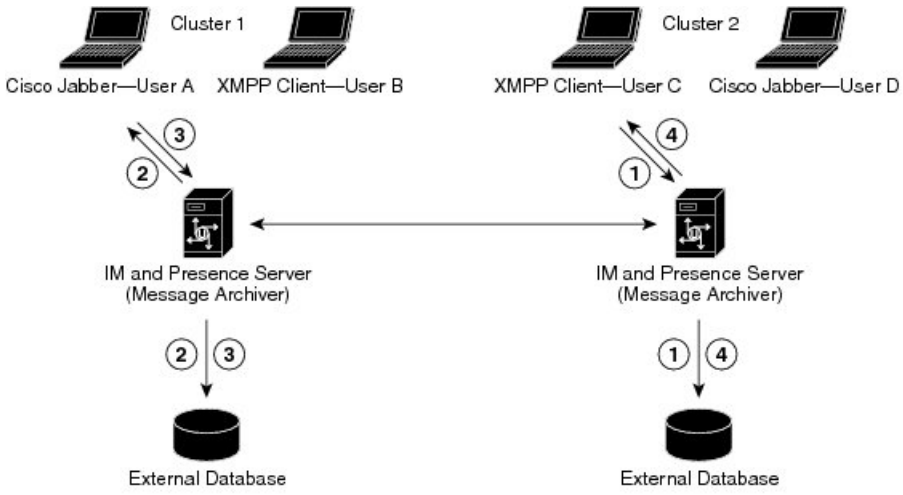


Intercluster or Federated Network Configuration

When using IM compliance in an intercluster or federated network configuration, you must configure an external database per cluster. Additionally, you should configure the IM and Presence Service node to log both incoming and outgoing messages. Otherwise, each database will retain only half of the conversation.

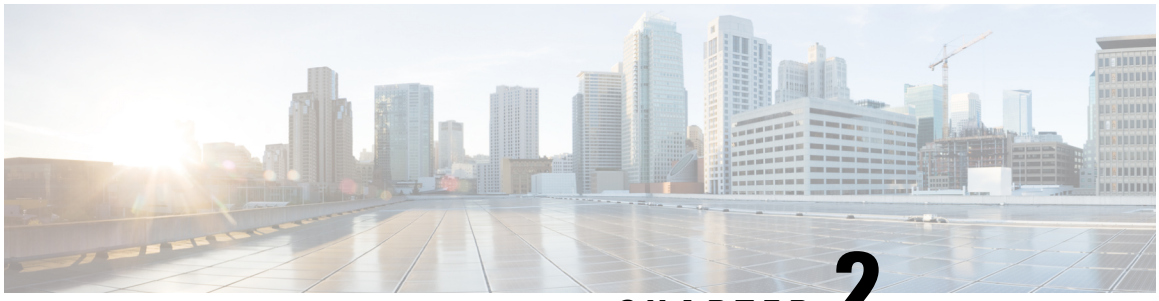
The figure below highlights these components and message flow.

Figure 2: IM Compliance for Multiple Clusters



1—User C sends message to User A, passing through the IM and Presence server (Cluster 2). Outbound message is also archived via IM and Presence MA to external database.
2—IM and Presence server (Cluster 1) passes inbound message to User A . Inbound message is also archived via IM and Presence MA to external database.
3—User A sends message to User C, passing through the IM and Presence server (Cluster 1). Outbound message is also archived via IM and Presence MA to external database.
4—IM and Presence server (Cluster 2) passes inbound message to User C. Inbound message also archived via IM and Presence MA to external database.

344347



CHAPTER 2

Message Archiver Configuration

Message Archiver Overview

The Message Archiver feature provides a basic IM compliance solution. This feature allows your system to comply with regulations that require logging of all instant messaging traffic in your company. Many industries require that instant messages adhere to the same regulatory compliance guidelines as for all other business records. To comply with these regulations, your system must log and archive all business records, and archived records must be retrievable.

The Message Archiver feature provides support for instant messaging (IM) compliance by collecting data for the following IM activities in single cluster, intercluster, or federated network configurations. This includes point-to-point messages and various forms of group chat.

This feature requires that you deploy an external database specifically for this feature

Encrypted Database for Message Archiver

For added security, you can enable an encrypted database for the Message Archiver. When this option is enabled, the IM and Presence Service encrypts IMs before archiving them in the external database. With this option, all data in the database is encrypted such that even a database administrator will be unable to read archived IMs, unless they possess the encryption key.

The encryption key can be downloaded from the IM and Presence Service and used in conjunction with whatever tool you use to view data in order to decrypt archived data.

For intercluster networks, you can enable encryption for the local cluster and any intercluster peers from a single IM and Presence Service cluster. The cluster on which you enable encryption becomes the master cluster, which controls the encryption key for its remote slave clusters. You can download the encryption key from the IM and Presence Service interface, but you must use the encryption password that was entered in the master cluster.

Encryption Standards

To ensure that archived data is not compromised, this feature uses three keys: a symmetric encryption key, along with an assymetric public-private key pair.

- Encryption key—This 256-bit symmetric key is generated and stored internally by the IM and Presence Service, which uses this key to encrypt IM compliance data before archiving the data in the compliance database. For intercluster networks, the master cluster syncs its encryption key to the remote slave clusters so that the entire intercluster network is using the same encryption key, which is controlled from the master cluster.

  You must download this key from the IM and Presence Service and use it with your data viewer to be able to decrypt archived IMs. When you download this key, the key is encrypted with the public key from the public-private key pair. You can later decrypt the encryption key with the private key.

- Public-Private key pair—You must generate this assymetric key pair in an approved key generation tool (for example, OpenSSL) and use it to encrypt the key in the IM and Presence Service and then decrypt the key with your data viewing tool. The public-private key pair secures the encryption key while in transit from the IM and Presence Service to your data viewing tool (for example, Splunk).

The encryption password is hashed with SHA2 and then encrypted with AES 256. Instant Messages are encrypted with the AES 256 algorithm

Intercluster Network Encryption

The following conditions apply for intercluster peer networks:

- An intercluster peer network can have only a single master cluster or encryption errors will result. The master cluster uses the Cisco Intercluster Sync Agent to sync encryption related information, (for example, the encryption password and encryption key) to remote peer clusters, which become slave clusters of the master cluster.
- Once you enable Message Archiver encryption within a local cluster, that cluster becomes a master cluster.
- If you checked the **Enable Encyption in Remote Clusters** check box, the remote peer clusters become slave clusters of the master cluster following the next intercluster sync, provided the Message Archiver is configured on all nodes in the remote cluster with Microsoft SQL Server as the compliance database. If this is true, the Cisco Intercluster Sync Agent syncs encryption related information, incuding the password and encryption key to the remote cluster.
- If the remote cluster does not have the Message Archiver configured on all nodes with a Microsoft SQL Server compliance database, encryption will not become enabled. However, if you later configure the Message Archiver on all nodes with a Microsoft SQL Server compliance database, encryption will be enabled automatically in the remote cluster following the next intercluster sync.
- If you configure a master cluster with the **Enable Encryption on Remote Clusters** option selected and subsequently add an intercluster peer, the peer cluster becomes a slave cluster automatically following the next intercluster sync. Encryption will be enabled on the slave provided the Message Archiver is configured on all nodes with a Micrsoft SQL Server external database.
- If you have an intercluster peer relationship between an 11.5(1)SU5 master cluster that has Message Archiver encryption enabled for remote clusters, and a peer cluster that does not support encryption (for example, 11.5(1)SU4), the peer cluster will not have encryption enabled, even if it has a Microsoft SQL

Server compliance database. However, once the peer cluster upgrades to 11.5(1)SU5, the encryption settings will be applied following the intercluster sync.

- Cisco recommends that you deploy a single external database per cluster for the Message Archiver.

Process Flow for Encryption

The following table highlights the process flow for enabling encryption and for viewing encrypted data from the database. The flow highlights each step, and the interface on which each step is completed.

Table 2: Encryption Process Flow

	IM and Presence Service Master Cluster	Key Generation Tool (e.g., OpenSSL)	Data Viewing Tool
Step 1	The administrator configures encryption for the intercluster network. The master cluster syncs encryption settings across the intercluster network. Archived data is now encrypted.		
Step 2		The administrator generates a public-private key pair for securing the encryption key.	
Step 3	The administrator downloads the encryption key from the IM and Presence Service. During the download, the public key encrypts the encryption key.		
Step 4			The administrator uses the private key to decrypt the encryption key.
Step 5			The encryption key decrypts compliance data. Authorized personnel can view archived compliance data.

Message Archiver Prerequisites

To deploy the Message Archiver feature, you must install and set up an external compliance database. This feature supports PostgreSQL, Oracle or Microsoft SQL Server databases.

For details on database requirements, see the *External Database Setup Guide for the IM and Presence Service*.

PostgreSQL Requirements

To deploy PostgreSQL version 10.0.1 as the external database, you must set the following values in the postgresql.conf file:

- escape_string_warning = off
- standard_conforming_strings = off

After you configure these parameters, you must restart PostgreSQL. For more information about how to configure the postgresql.conf file and restart PostgreSQL, see *External Database Setup Guide for the IM and Presence Service* .

Support for Oracle

In compliance with XMPP specifications, the IM and Presence Service node uses UTF8 character encoding. This allows the node to operate using many languages simultaneously and to display special language characters correctly in the client interface. If you want to use Oracle with the node, you must configure it to support UTF8.

- The value of the NLS_LENGTH_SEMANTIC parameter should be set to BYTE.
- To determine the tablespace available for your Oracle database, execute the following query as sysdba:

  SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME =

  'UPPER_CASE_USERNAME';

Encryption Requirements for Message Archiver

- For intercluster networks, intercluster peering must be configured with the **Cisco Intercluster Sync Agent** running in each cluster. The Message Archiver must be configured on all nodes in both clusters, with Microsoft SQL Server deployed as the compliance database.
- For intercluster networks, if you are enabling an encrypted database for the Message Archiver, make sure to plan which cluster in the intercluster network is going to be the master cluster. An intercluster peer network can have only a single master cluster.
- Message Archiver encrypted database is supported only if you have Microsoft SQL Server deployed as the external database.
- For 11.x releases, this feature is offered as of Release 11.5(1)SU5. For 12.x releases, this feature is supported as of 12.5(1). This feature is not supported in 12.0(1).

Message Archiver Configuration Task Flow

Complete the following tasks to configure the Message Archiver on the IM and Presence Service. You can use this feature to set up your system for instant messaging compliance by having all instant messages archived in an external compliance database.

Before you begin

Make sure that you have configured your external compliance database and set up a connection to the IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Configure the Message Archiver, on page 9	Enable the Message Archiver feature settings.
Step 2	Activate the Cisco XCP Message Archiver, on page 9	The **Cisco XCP Message Archiver** service must be running for the Message Archiver feature to work.
Step 3	Restart the Cisco XCP Router, on page 10	After you enable the Message Archiver, restart the Cisco XCP Router service on all nodes.
Step 4	Configure Alarms for IM Compliance, on page 10	Configure alarms for the Message Archiver so that any connection issues can be resolved quickly.
Step 5	Configure the Maximum Queue, on page 11	Optional. Configure the maximum queue for IMs waiting to be written to the compliance database. The default is 100,000.
Step 6	Configure Encrypted Compliance Database, on page 11	Optional. Configure encryption for the Message Archiver so that the IM and Presence Service encrypts IMs before archiving them in the compliance database.

Configure the Message Archiver

Use this procedure to enable the Message Archiver feature for IM Compliance.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 From the **Compliance Server Selection** list, check the **Message Archiver** radio button.

Step 3 Optional. Check the **Enable Outbound Message Logging** check box if you want the Message Archiver to log both inbound and outbound messages. If you leave this option unchecked, only inbound messages are archived.

Step 4 Check the **Block message delivery if unable to record in compliance database** check box if you want to block messages from being delivered if the compliance database is down.

Step 5 From the **Message Archiver Database Assignment** table, assign external compliance databases to each cluster node.

Step 6 Click **Save**.

What to do next

Activate the Cisco XCP Message Archiver, on page 9

Activate the Cisco XCP Message Archiver

To use the Message Archiver feature, you must make sure that the **Cisco XCP Message Archiver** feature service is activated on each cluster where you want to archive IMs. Use this procedure to activate the service in the local cluster.

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down, select an IM and Presence server and click **Go**.

Step 3 Under **IM and Presence Services**, check the status of the **Cisco XCP Message Archiver** service.

Step 4 If the service is not activated, check the adjacent radio button and click **Save**.
The Cisco XCP Message Archiver service starts.

What to do next

Restart the Cisco XCP Router, on page 10

Restart the Cisco XCP Router

After you configure the Message Archiver, restart the Cisco XCP Router on all nodes.

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 From the **Server** drop-down list box, choose the IM and Presence server and click **Go**.

Step 3 Under **IM and Presence Services**, select the **Cisco XCP Router** service and click **Restart**.

Configure Alarms for IM Compliance

If the IM and Presence Service loses its connection to the compliance database, messages will no longer be archived. Set up alarms that notify you of connection issues.

Note Depending on the setting of the **Block message delivery if unable to record in compliance database** setting on the IM Compliance Settings window, users may still be able to send IMs even though the compliance database is down.

Step 1 Sign into **Cisco Unified CM IM and Presence Administration**.

Step 2 Choose **Navigation** > **Cisco Unified IM and Presence Serviceability** from the menu in the upper, right corner of the IM and Presence Service main window.

Step 3 Choose **Alarm** > **Configuration**.

Step 4 From the **Server** drop-down list, choose the server for which you want to configure the alarm and click **Go**.

Step 5 From the **Service Group** drop-down list, choose IM and Presence Services and click **Go**..

Step 6 From the **Service** drop-down list, choose **Cisco XCP Message Archiver** and click **Go**..

Step 7 Configure the alarm settings as preferred.

Step 8 Click **Save**.

Configure the Maximum Queue

Use this optional procedure to configure the maximum number of messages that the system can queue for writing to the external database. The system default is 100,000 messages.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**..

Step 2 From the **Server** drop-down, select an IM and Presence cluster node.

Step 3 From the **Service** drop-down, select **Cisco XCP Message Archiver**.

Step 4 Set a value for the **Max Queue Size** parameter. The default setting is 100,000 messages.

Step 5 Click **Save**.

Configure Encrypted Compliance Database

Complete these optional tasks to configure an encrypted database for the Message Archiver. When this feature is enabled, all archived IMs are encrypted before being sent to the compliance database.

This feature is supported only if Microsoft SQL Server is the external database.

Procedure

	Command or Action	Purpose
Step 1	Enable Encryption Settings for Message Archiver, on page 11	In the IM and Presence Service, enable encryption and enter an encryption password.
Step 2	Generate Public-Private Key Pair, on page 12	Use an external key-generation tool to generate a public-private key pair. This key pair secures the encryption key while in transit from the IM and Presence Service to the data viewing tool.
Step 3	Download Encryption Key, on page 12	In the IM and Presence Service, download the symmetric encryption key. This key will itself be encrypted via the public key.
Step 4	View Archived Data, on page 13	In your data viewing tool, use the private key to decrypt the encryption key. The encryption key can then be used to decrypt archived data from the compliance database.

Enable Encryption Settings for Message Archiver

Use this procedure to enable encryption settings for your compliance database.

Note For intercluster networks, you can enable encryption for all peer clusters from a single cluster, provided the Message Archiver is already configured on each cluster with a Microsoft SQL Server compliance database.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 From the **Compliance Server Selection** list, make sure that the **Message Archiver** option is enabled.

Step 3 Make sure that the external databases that are selected for this feature are Microsoft SQL Server databases.

Step 4 Check the **Enable Encryption on this cluster** check box.

Step 5 Optional. If you have an intercluster network, and you want to enable encryption for intercluster peers as well, check the **Enable Encryption on Remote Clusters** check box.

Step 6 Enter an encryption password in the **Password** and **Confirm Password** boxes.

Step 7 Click **Save**.

Step 8 Restart the Cisco XCP Router on all nodes:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
b) From the **Server** drop-down list box, choose the IM and Presence server and click **Go**.
c) Under **IM and Presence Services**, select the **Cisco XCP Router** service, and click **Restart**.
d) Repeat this step on all cluster nodes.

What to do next

Generate Public-Private Key Pair, on page 12

Generate Public-Private Key Pair

After you enable encryption settings, use an approved tool such as OpenSSL or Python to generate an assymetric public-private key pair. This key pair will be used to secure the encryption key while it is in transit from the IM and Presence Service to whatever external data viewer you use to view archived data (for example, Splunk). Follow the below guidelines to store these keys:

- Public key—You will need to enter the public key in the IM and Presence Service interface when you download the symmetric encryption key that encrypts the database.
- Private key—The private key must be kept separate from the IM and Presence Service. You will use this key with your data viewer when you want to view archived data from the database. The private key decrypts the encryption key, which will then decrypt archived data from the database.

What to do next

Download Encryption Key, on page 12

Download Encryption Key

Use this procedure in the IM and Presence Service intercluster network to download the symmetric encryption key that encrypts archived IMs. You will need to use this key, along with the tool that you use to view compliance data in order to read encrypted data from the compliance database.

Note As a part of the download process, the IM and Presence Service uses the public key to encrypt the encryption key. This will secure the encryption key while it is in transit from the IM and Presence Service to the data viewer.

Note The encryption key can only be downloaded from a master cluster. You cannot download this key from a slave cluster.

Before you begin

Make sure that you have generated an assymetric public-private key pair with an approved key generation tool. You require the public key in this task.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 Click the **Download Encryption Key** button.

Step 3 In the popup window, complete the following fields:.

- **Password**—Enter the encryption password that was configured on the master cluster.
- **Public Key**—Copy in the public key that you generated in the external key generation tool.

Step 4 Click **Download Key** and save the encryption key to a location that you can access.

The IM and Presence Service downloads the encryption key to the location that you specify. The downloaded encryption key is itself encrypted via the public key and is unusable unless it is decrypted via the private key.

View Archived Data

All data in the compliance database is encrypted. You will need to use a data viewing tool along with the (encrypted) encryption key and the private key to extract and view archived data.

- Use the private key to decrypt the encryption key.
- Use the decrypted encryption key to decrypt archived data.

What to do next

You can now use the data viewer to read archived IMs from the database.

Change Encryption Password

Use this procedure only if you have encryption configured for the Message Archiver, and you want to change the encryption password.

Note For intercluster networks, you can only change the encryption password on the master cluster.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 Click the **Change Password** button.

Step 3 In the popup window, enter the old and new passwords.

Step 4 Click **Save**.

Disable Encryption

Use this procedure if you have encryption configured for the Message Archiver, and you want to disable it.

Note The following conditions apply for disabling encryption:

- If you disable encryption from a master cluster, it will be disabled for all slaves automatically. All encryption-related data is deleted from master and slaves automatically.
- You can disable encryption on a slave cluster provided you have the encryption password that was configured on the master cluster.
- If you want to add a node to a cluster where Message Archiver encryption is configured, you must complete this task to disable encryption before you add your node. After you add your node, you can re-enable encryption.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Settings**.
Step 2 Click the **Disable Encryption** button.
Step 3 In the popup window, enter the encryption **Password** and click **Disable**.
Step 4 Click **Yes**.

Troubleshooting for Message Archiver

For issues with the Message Archiver or Message Archiver encryption, refer to logs for the services in the below table. In addition to the services, the table displays sample CLI to build the logs as well as the log output location.

Table 3: Troubleshooting Logs for the Message Archiver

Service	CLI to Build Log	Output Location
Cisco XCP Message Archiver	`file build log msg_archiver <duration>`	`/epas/trace/log_msg_archiver_*.tar.gz`
Cisco XCP Router	`file build log cisco_xcp_router <duration>`	`/epas/trace/log_cisco_xcp_router_*.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 AXL Web Service*	For AXL, use the Real-Time Monitoring Tool:	Logs are in the following location: `/var/log/active/tomcat/logs/axl/log4j/`

*Cisco AXL Web Service and the Cisco Intercluster Sync Agent Service are used to sync encryption related information across clusters.

Troubleshooting Tips for Encryption

The following table highlights common issues with an encrypted compliance database for the Message Archiver feature.

Table 4: Troubleshooting for Encrypted Compliance Database

Error	Remedy
Encryption cannot be enabled	Do the following: • Check the external compliance database connection. Make sure the compliance database is Microsoft SQL Server. • Check that the Cisco XCP Message Archiver service is running. • Confirm that you are on a node in the master cluster. You cannot enable encryption from a slave cluster. Also, if a master cluster disables encryption, encryption gets disabled automatically for all of its slave clusters as well.
Encryption cannot be disabled	Make sure that the encryption password that you entered is correct.
Cannot update the encryption password	Make sure that your password meets complexity requirements.
Cannot download the encryption key	Do the following: • Make sure that your encryption password is correct. • Make sure that the public key was created with the proper algorithm.
Encryption successfully enabled and messages are still stored in plain text	Search the Message Archiver logs. Look for the text, "Encryption enabled". If this text is not found, check the Message Archiver xml configuration file. If encryption info is not present, restart the Cisco XCP Router.

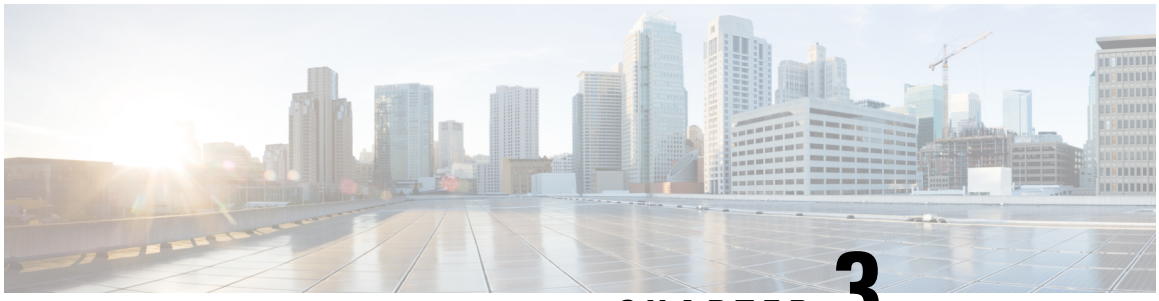
Multiple Master Cluster Alarms

An intercluster peer network can have only a single master cluster or encryption errors will result, and the **MAencryptionMultiMaster** alarm will be raised. This alarm is raised in the following scenarios:

- Connecting two master clusters as intercluster peers
- Connecting a master cluster to a slave cluster of another master.
- Connecting two clusters, which are slaves of different master clusters.

Additional Error Conditions

- If the publisher node is down on the Master cluster, encryption will not work, either within that cluster, or across clusters.
- If the publisher node is down on a slave cluster, and you subsequently disable encryption, then the slave cluster will have stale encryption data. To clear this data, you must disable Message Archiver, or wait for the publisher node to come back up.
- Removing a master cluster from network without disabling encryption will lead to stale encryption data in master and slave clusters
- Removing a slave cluster without first disabling encryption will lead to stale encryption data in the slave cluster database. In this case, you must disable the Message Archiver from the GUI.



CHAPTER 3

Third-Party Compliance Server Integration

About Third-Party Compliance

With this solution, IM and Presence Service integrates with one or more third-party compliance servers for compliance logging or ethical wall functionality. The IM and Presence Service administrator can select which IM, presence, or group chat events are passed to the compliance server(s), and which events are blocked. The events must be selected based on policy. For example, the system could be configured to filter IMs between certain users, or groups of users, and block or modify content depending on the originator and recipient of the IMs.

To use the third-party compliance solution you must configure the third-party compliance server(s) for your cluster. IM and Presence Service passes all configured events that are generated in the processing of user login, logout, presence sharing, IM exchange, or group chat activity to the third-party server(s). The third-party compliance server applies any relevant policy or filtering to the event, then instructs IM and Presence Service as to whether the event should be processed further. Note that you may potentially experience performance delays in your network because of the volume of events that pass between IM and Presence Service and the third-party compliance server. If IM and Presence Service loses its connection to the third-party server, all IM traffic stops.

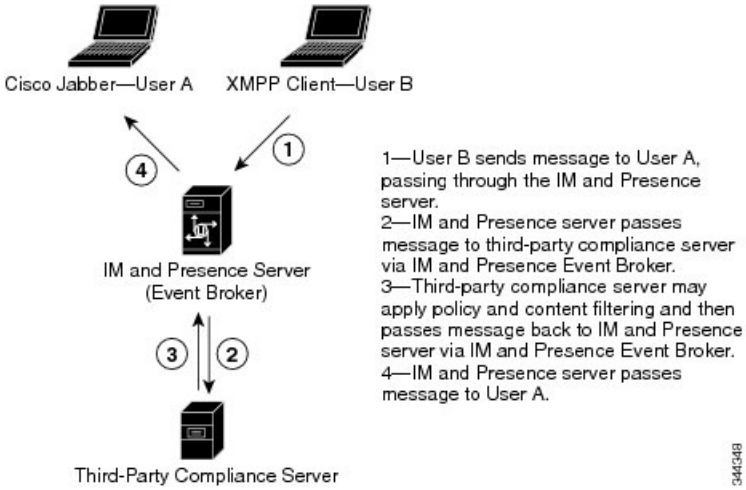
Third-party compliance requires these components:

- IM and Presence Service - IM and Presence Service uses the Event Broker component to send events to the third-party compliance server.
- Third-party compliance server - All IM and Presence Service nodes in the cluster will redirect events to the configured compliance server(s) unless you are upgrading from a system with compliance already configured.
- IM Client - Supported clients include Cisco clients such as Cisco Jabber, third-party XMPP clients, and other third-party clients used in federated networks.

Note IM and Presence Service does not provide a secure TLS/SSL connection between IM and Presence Service and the third-party compliance server.

The following figure highlights the third-party compliance components and message flow.

Figure 3: Third-Party Compliance



Compliance Profiles

A compliance profile contains a set of Jabber Session Manager (JSM) and\or Text Conferencing (TC) events that you can use to monitor for compliance. You can create a compliance profile that consists of only JSM events, only TC events, or a combination of both JSM and TC events.

When you configure a compliance profile, choose which JSM and TC events you wish to be logged to the compliance server. You can also decide what type of handling is performed by the compliance server, how IM and Presence Service handles error responses from the compliance server, and whether the IM and Presence Service node waits for a response from the compliance server before processing the event further. You can also configure how the events should be processed if no response is expected.

The following tables describe the JSM events and parameters.

Caution If a combination of Bounce, and Fire and Forget is selected, an event to which this applies will be passed to the compliance server and then discarded. This means it will not be processed further by IM and Presence Service. Use this combination with care.

Table 5: JSM Events

Event	Description
e_SESSION	Packets sent during login, which is the creation of a new session.

Event	Description
e_OFFLINE	Packets sent to users who are offline. Offline users are users who do not have an active session.
e_SERVER	Packets sent directly to the server for internal handling.
e_DELIVER	The first event for packets coming in from another server; the second event for packets coming in from a user on the same server. (The first event for packets coming in from the same server is es_IN.)
e_AUTH	IQ packets sent during authentication.
e_REGISTER	Packets generated during registration of a new account by a user.
e_STATS	Packets sent periodically that contain server statistics.
e_DISCOFEAT	Triggered when a user sends a **`disco#info`** query.
e_PRISESSION	Determines a user's primary or default session when the user has more than one session. An EventBroker component may dictate the choice of a user's primary session.
es_IN	Generated when a stanza is about to be received by a user's session.
es_OUT	Generated when a stanza is sent from a user's session.
es_END	Packets generated when a user logs out.

Table 6: JSM Parameters

Parameter	Description
Packet Type	Select one of the following XMPP packet types: • **all** - All packets • **iq** - Packets used during info-query functions • **message** - Packets containing standard IM or group chat messages • **presence** - Packets containing presence information • **subscription** - Packets sent when subscribing to another user's presence
Handling	Select **bounce** if errors returned from the compliance server should be bounced back to the originating party or component Select **pass** if they should be discarded.

Parameter	Description
Fire and Forget	Leave the check box unchecked if the IM and Presence Service node must wait for a response from the compliance server before it continues to process the event. Check the check box if the IM and Presence Service node does not require a response from the compliance server before it continues to process the event further.

The following tables describe the TC events and parameters.

Caution If a combination of Bounce, and Fire and Forget is selected, an event to which this applies will be passed to the compliance server and then discarded. This means it will not be processed further by IM and Presence Service. Use this combination with care.

Table 7: TC Events

Event	Description
onServicePacket	The system receives a packet from the router that is either addressed directly to the TC service or to a room that does not currently exist on the system.
onBeforeRoomCreate	A gear is attempting to create a room on the system.
onAfterRoomCreate	A room has been successfully created on the system. The only valid response is PASS with no modification to the original stanza.
onServiceDiscoInfo	An entity has sent a **`disco#info`** packet to the TC service. The only valid response is PASS.
onServiceReconfig	The TC service receives a signal to reconfigure itself. The only valid response is PASS. This is a notification event only. The XDB packet will be of a type="set". The external component should not respond to this packet.
onDestroy	A room owner closes a room. The only valid response is PASS.
onClose	A gear requests to close a room.
onPacket	A new XML stanza is directed at a room, or participant within a room.
onMetaInfoGet	Room configuration information is available. The only valid response is PASS.
onBeforeMetaInfoSet	A room configuration is about to be modified by a user.
onAfterMetaInfoSet	A room configuration has been modified by a user. The only valid response is PASS with nothing in it.

Event	Description
onExamineRoom	A Jabber entity requests information, either by browse or disco, from a room. The only valid response is PASS.
onBeforeChangeUser	A change has been requested of a user role, nickname, or presence. This includes on entry, exit, nick change, availability change, or any role change (granting or revoking voice, moderator privilege).
onAfterChangeUser	A user has changed. The only valid response is PASS with nothing in it.
onBeforeChangeAffiliation	A user affiliation is about to change.
onAfterChangeAffiliation	A user affiliation has changed. The only valid response is PASS with nothing in it.
onBeforeRemoveAffiliation	A user affiliation is about to be removed.
onAfterRemoveAffiliation	A user affiliation has been removed. The only valid response is PASS with no modification to the original stanza.
onBeforeJoin	A user is about to join a room.
onAfterJoin	A user has joined a room. The only valid response is PASS with nothing in it.
onLeave	A user has left a room. The only valid response is PASS.
onBeforeSubject	A room subject is about to change.
onAfterSubject	A room subject has changed. The only valid response is PASS with nothing in it.
onBeforeInvite	A user is about to be invited to a room.
onAfterInvite	A user has been invited to a room. The only valid response is PASS with nothing in it.
onHistory	A room's history has been requested. The only valid response is PASS.
onBeforeSend	A message is about to be sent in a room.
onBeforeBroadcast	A message is about to be broadcast in a room.

Table 8: TC Parameters

Parameter	Description
Handling	Select **bounce** if errors returned from the compliance server should be bounced back to the originating party or component Select **pass** if they should be discarded.

Parameter	Description
Fire and Forget	Leave the check box unchecked if the IM and Presence Service node must wait for a response from the compliance server before it continues to process the event. Check the check box if the IM and Presence Service node does not require a response from the compliance server before it continues to process the event further.

If the same compliance profile is assigned to more than one compliance server, events are load balanced across each of the compliance servers. This reduces the load on individual compliance servers. Events are routed using an algorithm that ensures that related events are routed to the same compliance server. For one to one IMs, events are routed based on the combination of the to/from address, regardless of the packet's direction. This means that the full conversation between two users is routed to one compliance server. For group chat, events for a given chat room are routed using the chat room address, so that all events for a room are routed to one compliance server.

A system default profile is available in the system after fresh install or upgrade. This profile is called SystemDefaultComplianceProfile and cannot be deleted or modified. You can assign and unassign this profile as with any other.

The SystemDefaultComplianceProfile profile has four JSM and five TC events configured. If this profile is assigned, when any of its events occur in an IM and Presence Service cluster, they are passed on to the compliance server for handling, and a response is expected. The IM and Presence Service node handles the events based on the response from the compliance server. These events are previewed in read-only format if the SystemDefaultComplianceProfile is selected from the list of available compliance profiles.

Table 9: SystemDefaultComplianceProfile Pre-Configured Events

JSM Events	TC Events
e_SESSION	onBeforeInvite
es_END	onBeforeJoin
es_IN (for message stanzas only)	onBeforeRoomCreate
es_OUT (for message stanzas only)	onBeforeSend
	onLeave

If the same event(s) are configured in multiple profiles and these profiles are assigned to different third-party compliance servers, the events are handled in order as specified by routing priority. By default, routing priority of all profiles is defined by the order in which the profiles were added to the system. The routing priority can be re-configured.

Compliance Profiles Routing Priority

You can configure routing priority when there is more than one compliance profile assigned and some or all of the events from one profile exist in the other profile(s). If each compliance profile has different events configured, routing priority is not applicable.

The default routing priority of the profiles configured in the system is the order in which they were configured.

Example

The following is an example of when you would use compliance profiles routing priority:

You have a compliance profile configured for events subject to Ethical Wall scrutiny, and another for the same events subject to IM logging. Each is assigned to a different compliance server. If you want the events subject to Ethical Wall scrutiny to be routed to the Ethical Wall server before being logged in the IM logging server, you must assign the Ethical Wall compliance profile the higher priority.

Third-Party Compliance Server Prerequisites

Install and configure the third-party compliance server. Refer to your vendor documentation for details.

Make sure to plan your compliance deployment before you configure anything. For information on designing you IM compliance setup, refer to the *Cisco Collaboration System Solution Reference Network Design*.

Third-Party Compliance Server Integration Task Flow

Before you begin

Install and configure your third-party compliance server according to your vendor documentation.

Procedure

	Command or Action	Purpose
Step 1	Add Compliance Server, on page 24	On the IM and Presence Service, add your third-party compliance server.
Step 2	Configure Compliance Profiles, on page 24	Configure Compliance Profiles for your compliance server. You can use these profiles to determine which events are logged and which are not.
Step 3	Configure Compliance Profile Routing Priority, on page 25	Configure the routing priority that the system uses to determine which compliance profile to apply.
Step 4	Assign Compliance Servers, on page 26	Assign the third-party compliance server to IM and Presence cluster nodes as a part of your compliance configuration.
Step 5	Restart Cisco XCP Router, on page 26	After you change any of the existing configurations, restart the Cisco XCP Router.
Step 6	On the compliance server, configure the corresponding open-port names generated by IM and Presence Service.	For configuration details, refer to your compliance vendor documentation.
Step 7	Configure Alarms for Compliance Server, on page 27	Optional. Configure Cisco XCP Router alarms so that the administrator can be notified if the connection to the compliance server breaks.

Add Compliance Server

Use this procedure to add a third-party compliance server to the IM and Presence Service.

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Server Setup** > **Third-Party Compliance Servers**.

Step 2 Click **Add New**.

Step 3 Enter the compliance server details. For help with the fields and their settings, refer to the online help:

- **Name**
- **Hostname/IP Address**—For the Hostname/IP Address field, allowed characters are all alphanumeric characters (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).
- **Port**
- **Password/Confirm**

Note The name is only used locally by IM and Presence Service. The IP address, port, and password must match the configuration on the compliance server itself.

Step 4 Click **Save**.

Note Use caution when changing these settings. If you save any changes, you lose all previous configuration settings.

What to do next

Configure Compliance Profiles, on page 24

Configure Compliance Profiles

Use this procedure to set up compliance profiles for a third-party compliance server. A compliance profile contains a set of Jabber Session Manager (JSM) and\or Text Conferencing (TC) events that you can use to monitor for compliance. You can use the profile to determine which events are logged by the compliance server and how error responses are handled.

Note For reference information on the JSM and TC events for which you can configure event handling policies, see Compliance Profiles, on page 18.

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Profiles**.

Step 2 Choose **Add New**.

Step 3 Enter a **Name** and **Description** for the compliance profile.

The Name supports alphanumeric characters only. Spaces are not permitted.

Note The compliance profile name cannot be modified if the profile is assigned to a compliance server.

Step 4 Configure event handling for **JSM Events** and **TC Events**. For help with the fields and their settings, see the online help:

a) From the **Event** drop-down select the JSM event for which you want to configure a policy.
b) JSM Events only. From the **Packet Type** drop-down, select a packet type.
c) From the **Handling** drop-down, configure how error responses from the compliance server should be handled. The Bounce option sends errors back to the originating party, and the pass option discards them.
d) Check the **Fire and Forget** check box if you want the IM and Presence Service to process the event without requiring a response from the compliance server. Leave the check box unchecked if you want the IM and Presence Service to wait for the compliance server response before processing the event.

Note By default, events are processed as part of the event handling chain and IM and Presence Service waits for a response from the compliance server. If an event is processed as part of the event handling chain, and the compliance server responds with HANDLE, the event is not processed further by IM and Presence Service. If the compliance server responds with PASS, IM and Presence Service continues to process the event.

e) Click **Add New Event** to add a new event.
f) Repeat this process for both JSM and TC events until you've all of the events that you want to add to this profile.

Note If you want to delete an event that you've added, select the event and click **Delete Selected**.

Step 5 Click **Save**.

Note If you update settings for events in an existing compliance profile that is assigned to a third-party compliance server, you must restart the XCP Router service.

What to do next

Configure Compliance Profile Routing Priority, on page 25

Configure Compliance Profile Routing Priority

Use this procedure to configure a routing priority for the compliance profiles that you've configured.

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Profiles Routing Priority**.

Step 2 In the **Compliance Profiles listed by routing priority (Top is highest priority)** window, use the up and down arrows to arrange the routing priority for your compliance profiles.

Step 3 Click **Save**.

What to do next

Assign Compliance Servers, on page 26

Assign Compliance Servers

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 From the **Compliance Server Selection** options list, choose **Third-Party Compliance Server**.

Step 3 Assign the third-party compliance server(s) to the IM and Presence Service nodes.

Note The same node cannot be assigned to multiple compliance servers if you have upgraded from a system that had compliance configured prior to the upgrade. In this case, if you want to be able to assign the same node to multiple compliance servers, you must enable compliance for the whole cluster.

The **Open-port Component Name** field is auto-generated based on the values in the first two columns. This is used when you configure the open-port component.

Step 4 Assign a compliance profile to each compliance server. The same compliance profile can be assigned multiple times.

Note If you have upgraded your system from pre-10.0(1), and you configured compliance prior to the upgrade, only the system default profile is available in the drop-down menu. To use custom profiles, you must enable compliance for the whole cluster.

Step 5 Click **Save**.

Note If you switch between IM compliance deployment options (for example, switch from the Message Archiver option to the Third-Party Compliance Server option), you must restart the Cisco XCP Router service. Note that you lose your third-party compliance settings if you switch between options.

What to do next

Restart the Cisco XCP Router service on all nodes if compliance is applied on all nodes in the cluster. Otherwise, it is sufficient to restart the Cisco XCP Router service on those nodes where you configured compliance.

Restart Cisco XCP Router

Use this procedure to restart the Cisco XCP Router.

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 From the **Server** drop-down list box, choose an IM and Presence node and click **Go**.

Step 3 Under **IM and Presence Services**, check the **Cisco XCP Router** service and click **Restart**.

What to do next

Optional. Configure Alarms for Compliance Server, on page 27

Configure Alarms for Compliance Server

When an IM and Presence Service node is integrated with a third-party compliance server, messages will only be delivered to users after it successfully logs the message to the third-party compliance server. If an IM and Presence Service node loses its connection to the third-party compliance server to which it is directly connected, IM and Presence Service does not deliver the message to the recipient.

Use this procedure to configure alarms to alert you when the connection to the compliance server is lost.

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Alarm** > **Configuration**.

Step 2 From the **Server** drop-down, choose the node on which you want to configure the alarm and click **Go.**

Step 3 From the **Service Group** drop-down, choose **IM and Presence Services** and click **Go**.

Step 4 From the **Service** drop-down, choose **Cisco XCP Router** and click **Go**.

Step 5 Configure the alarm settings. For help with the fields, see the online help.

Step 6 Click **Save**.

Enable Compliance Logging for all Nodes Following Upgrade

Caution When you enable this setting, you cannot change it back.

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 Choose Third-Party Compliance Server from the Compliance Server Selection.

Step 3 Check the **Enable compliance logging for all nodes in the cluster. Once enabled, this setting cannot be reverted back. Please refer to the documentation for optimal configuration** check box and click Save.

A warning message appears.

Step 4 Click OK.

Step 5 Restart the Cisco XCP Router service on all nodes in the cluster.

What to do next

After you enable compliance for all nodes, the component name used by IM and Presence Service changes to an auto-generated format. Update your compliance server(s) with the new component name to continue using the feature.

Related Topics

Restart Cisco XCP Router Service

Troubleshooting for Third-Party Compliance Server

If the compliance integration is not operating as expected and you are experiencing problems such as:

- Slow user login
- Blocked IMs
- Blocked group chat events when IM and Presence Service is configured to use third-party compliance.

Then carry out the following list of checks to troubleshoot the compliance integration:

1. Check the Troubleshooter in the Compliance Server Settings window. If the Troubleshooter is red continue with step 2. If the troubleshooter is green go to step 3.
2. Check the connection settings for the third-party compliance server in the third-party compliance server settings window.
3. To verify that the Cisco XCP Router service has established a connection to the third-party compliance server, check the Cisco XCP Router service logs using RTMT. Scan the logs for entries such as the following:
   - `Component op-gwydlvm131.gwydlvm1153-cisco-com is CONNECTED`

     This entry shows that the Cisco XCP Router service has established a network connection to the third-party compliance server.
   - `Component op-gwydlvm131.gwydlvm1153-cisco-com is ACTIVE`

     This entry shows that the Cisco XCP Router service and the third-party compliance server have completed authentication.
4. If the logs show `CONNECTED` but not `ACTIVE`, verify that:
   - The correct password has been configured on IM and Presence Service and on the third-party compliance server.
   - The correct component name has been configured on the third-party compliance server.

   If the Cisco XCP Router service is unable to connect to the third-party compliance server, the Cisco XCP Router service logs will show output similar to the following:

   ```
   Connecting on fd 22 to host '10.53.52.205', port 7999
   Unable to connect to host '10.53.52.205', port 7999:(111) Connection refused
   Component op-gwydlvm131.gwydlvm1153-cisco-com is GONE
   ```
5. If the Cisco XCP Router Service is unable to establish a connection to the third-party compliance server, check that:
   - The correct IP/FQDN and port have been configured on IM and Presence Service and on the third-party compliance server.
   - The third-party compliance server is running and listening on the specified port.
6. If the logs show `CONNECTED` and `ACTIVE` when IM and Presence Service passes events to the compliance server for processing, the third-party compliance server must respond to each event before IM and Presence

Service can continue to process the event. If you suspect that the compliance server is not responding, check the compliance server logs.

Third-Party Compliance Server Failure Event Handling

About Third-Party Compliance Server Failure Event Handling

This chapter describes the behavior IM and Presence Service users will experience when problems occur with compliance integration or during HA failover.

Note The sections in this chapter assume that compliance profiles include the following events (except where otherwise stated):

- e_SESSION (recording user logins)
- es_END (recording user logouts)
- es_OUT/es_IN for message (recording IM conversations)
- One or more TC events (recording chat room interactions)

Event handling during a Compliance Server or Service Outage

A Single Compliance Server or Service Shutdown

Assumed deployment:

- One or more IM and Presence Service node(s) deployed in a sub-cluster.
- One IM and Presence Service node is configured with a single third-party compliance server.

If the compliance server or service is shut down gracefully users will be affected as follows:

- Users will continue to log in and log out of IM and Presence Service using their XMPP clients as normal, but login and logout events will not be logged to the compliance server.
- Users will be blocked from sending IMs or interacting with chat rooms, and in each case users will receive a server error response.

A Single Compliance Server or Service Ungraceful Failure or Network Disruption

Assumed deployment:

- One or more IM and Presence Service node(s) deployed in a sub-cluster.
- One IM and Presence Service node is configured with a single third-party compliance server.

For an initial period of up to 5 minutes, if the compliance server or service fails ungracefully or if there is a disruption to the network between an IM and Presence Service node and the compliance server, the node will attempt to queue events for that compliance server. Individual events will be queued for 30 seconds before being processed or bounced.

After 5 minutes, if the compliance server or network has not recovered, the connection to the server will be dropped and events will no longer be queued. In this situation, events will be processed or bounced immediately. Users will be affected as follows:

- Users will experience up to 30 seconds delay on logging in to IM and Presence Service, but there will be no delay when logging out. Login and logout events will not be logged to the compliance server.
- Users will be blocked from sending IMs or interacting with chat rooms. In each case users will receive a server error response, but there may be a delay of up to 30 seconds before the error is received.
- Users may experience delays of up to 30 seconds while presence status updates are being processed.

Compliance Server or Service Graceful Outage with Multiple Compliance Servers

Assumed deployment:

- One IM and Presence Service node deployed in a sub-cluster.
- One IM and Presence Service node is configured with multiple third-party compliance servers.

Where an IM and Presence Service node is connected to multiple compliance servers, normal behavior is for events to be load-balanced across the compliance servers using a JID-based algorithm. Events for different users may be routed to different compliance servers.

If one of the compliance servers or services is shut down gracefully, then events that would have been routed to that server will instead be routed to the remaining compliance server(s).

Compliance Server or Service Ungraceful Outage with Multiple Compliance Servers

Assumed deployment:

- One IM and Presence Service node deployed in a sub-cluster.
- One IM and Presence Service node is configured with multiple third-party compliance servers.

Where an IM and Presence Service node is connected to multiple compliance servers, normal behavior is for events to be load-balanced across the compliance servers using a JID-based algorithm. Events for different users may be routed to different compliance servers.

If one of the compliance servers or services fails ungracefully, or if there is a disruption to the network between an IM and Presence Service node and that server, then users will be affected as follows:

- Some users will experience up to 30 seconds delay in logging in to IM and Presence Service, but there will be no delay when logging out. Login and logout events will not be logged to the compliance server.
- Some users will be blocked from sending IMs or interacting with chat rooms for a period of up to 5 minutes. After this period, affected users can continue to send IMs or interact with chat rooms, and the events will be routed to one of the remaining compliance servers.
- Some users may experience delays of up to 30 seconds for presence status updates to be processed.

Compliance Server or Service Outage with Multiple Compliance Servers and Profiles

Where an IM and Presence Service node is configured to connect to multiple compliance servers, each of which uses a different compliance profile, and the profiles contain one or more identical events, normal behavior is for these events to be routed in turn to the compliance server associated with each compliance profile according to each profile's priority.

This behavior is explained in more detail in the following example:

Assumed deployment:

- One IM and Presence Service node deployed in a sub-cluster with multiple profiles containing one or more identical events.
- The IM and Presence Service node is configured with multiple third-party compliance servers and profiles.

Each compliance profile has the following events configured:

Profile 1:

- e_SESSION (recording user logins)
- es_OUT/es_IN for message (recording IM conversations)
- es_END (recording user logouts)

Profile 2:

- es_OUT/es_IN for message (recording IM conversations)

Profile assignments:

- Profile 1 is assigned to Compliance Server 1
- Profile 2 is assigned to Compliance Server 2
- Profile 1 has the highest priority

During normal behavior:

When a user sends an IM, the es_OUT event for Profile 1 is routed to Compliance Server 1. When Compliance Server 1 acknowledges the event, the es_OUT event for Profile 2 is routed to Compliance Server 2.

If Compliance Server 1 experiences an ungraceful outage then the following sequence will take place:

1. User A sends IM to user B.
2. The es_OUT event (Profile 1) is queued for Compliance Server 1.
3. The es_OUT event (Profile 1) times out after 30 seconds.
4. The es_OUT event (Profile 1) is bounced, and the IM sender receives an error response.
5. The es_OUT (Profile 2) event is not processed and the event is not sent to Compliance Server 2.

In this case users will be affected as follows:

- Users will be blocked from sending IMs. Users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events associated with the IM conversation will not be routed to the remaining compliance servers.
- Users may experience delays of up to 30 seconds for presence status updates to be processed.

Compliance Handling During an IM and Presence Service Node Failure

Compliance Handling during Manual Node Failover

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA enabled.
- Each IM and Presence Service node is configured with a different third-party compliance server using the same compliance profile.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to a compliance server are routed via the IM and Presence Service node to which it is connected.

If an IM and Presence Service node manual failover occurs, events normally routed to its associated compliance server will be handled as follows:

- Login and logout events will not be logged to the compliance server. Some users will experience a delay of up to 30 seconds when logging in to IM and Presence Service, but there will be no delay when logging out.
- During failover, some users will be blocked from sending IMs or interacting with chat rooms. In this case users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events which are blocked will not be logged to the compliance server.
- When failover has been completed, IM or group chat events will be processed by the compliance server connected to the other IM and Presence Service node and stanzas will be delivered normally.

Compliance Handling during Automated Node Failover

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA enabled.
- Each IM and Presence Service node is configured with a different compliance server using the same compliance profile.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to each compliance server are routed via the IM and Presence Service node to which it is connected.

Note If the failover is not caused by a failure or shutdown of the Cisco XCP Router service, compliance events will continue to be routed to the compliance servers as normal. Events routed to the compliance server connected to the IM and Presence Service node that has failed over will continue to be routed to the compliance server.

Compliance Handling during Network Outage Between Multiple Nodes

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA enabled.
- Each IM and Presence Service node is configured with a different compliance server using the same compliance profile.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to each compliance server are routed via the IM and Presence Service node to which it is connected.

If a network outage between the IM and Presence Service nodes occurs, events for users that are normally routed to the compliance server associated with the other IM and Presence Service node will be handled as follows:

- Some users will experience a delay of up to 30 seconds when logging in to IM and Presence Service, but there will be no delay when logging out. Login and logout events will not be logged to the compliance server.
- During the outage, some users will be blocked from sending IMs or interacting with chat rooms. Users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events which are blocked will not be logged to the compliance server.
- If the outage continues for longer than 2 minutes, events will be processed by another compliance server in the deployment and stanzas will be delivered normally.

Compliance Handling during Cisco XCP Router Service Failure

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA not enabled.
- Each IM and Presence Service node is configured with a different compliance server using the same compliance profile.

Note In this section, consequences when HA is enabled will also be highlighted.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to each compliance server are routed via the IM and Presence Service node to which it is connected.

The difference in effects that users will experience when HA is either enabled or not enabled are as follows:

- When HA is enabled users will remain logged in and will be moved to the remaining node.
- When HA is not enabled, users on the failed node will be logged out and will not get any service.

More general effects include:

- Events normally routed to the compliance server connected to the failed IM and Presence Service node, will be routed to the compliance server connected to the other IM and Presence Service node.
- If the failure is transient, some users will initially be blocked from sending IMs or interacting with chat rooms. Users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events which are blocked will not be logged to the compliance server.
- If the failure lasts for a longer period, IMs will be processed normally and be routed to the compliance server connected to the other IM and Presence Service node.