Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)

First Published: July 18, 2012

Last Modified: July 18, 2012

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

Text Part Number: OL-30798-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2012-2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Planning for IM Compliance** 1

About IM Compliance 1

IM Compliance Components 1

Sample Topologies and Message Flow for IM Compliance 2

Prerequisite Configuration Tasks 4

CHAPTER 2 **IM Compliance Configuration** 7

Configure IM Compliance 7

Turning on Cisco XCP Message Archiver Service 8

CHAPTER 3 **IM Compliance Serviceability and Troubleshooting** 11

Restart Cisco XCP Router Service 11

Restart Cisco XCP Message Archiver Service 12

Set Trace Level to Info to Support IM Compliance 12

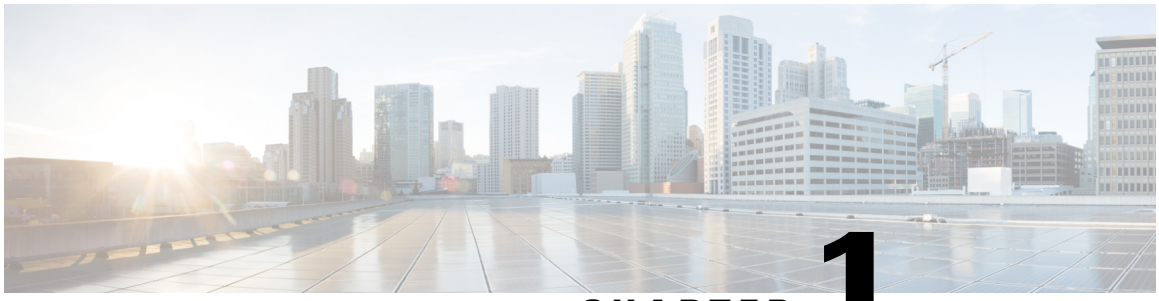
Configure Alarms for IM Compliance 12

CHAPTER 4 **Integration with Third-Party Compliance Servers** 15

About Third-Party IM Compliance 15

Configure Third-Party Compliance Server on IM and Presence Service 16

Assign Third-Party Compliance Server to IM and Presence Service Node 17



CHAPTER 1

Planning for IM Compliance

- About IM Compliance, page 1
- Prerequisite Configuration Tasks, page 4

About IM Compliance

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 the archived records must be retrievable.

The Cisco Unified Communications Manager IM and Presence Service provides support for instant messaging (IM) compliance by collecting data for the following IM activities in single cluster, intercluster, or federated network configurations:

- Point-to-point messages.
- Group chat - This includes ad-hoc, or temporary chat messages, and permanent chat messages.

IM Compliance Components

IM compliance includes these components:

- IM and Presence Service Release 9.0(1) . IM and Presence Service uses the Message Archiver component for logging messages to the external database.
- External database—For information on supported external databases, see the *Database Setup Guide for IM and Presence Service*.
- 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 The Message Archiver provides a basic IM logging solution. If you require a more granular logging solution, for example logging based on policy, use the third-party compliance solution, see the appendix module for details.

Related Topics

Database Setup for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)
Integration with Third-Party Compliance Servers, on page 15

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

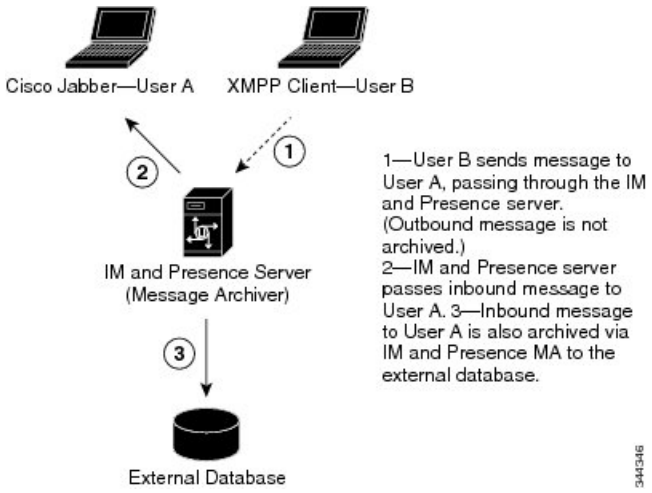
When using IM compliance in a single cluster, we highly recommend that you deploy one external database per cluster to which all incoming messages sent to users in the cluster are logged.

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 node* in a cluster. See *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .

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

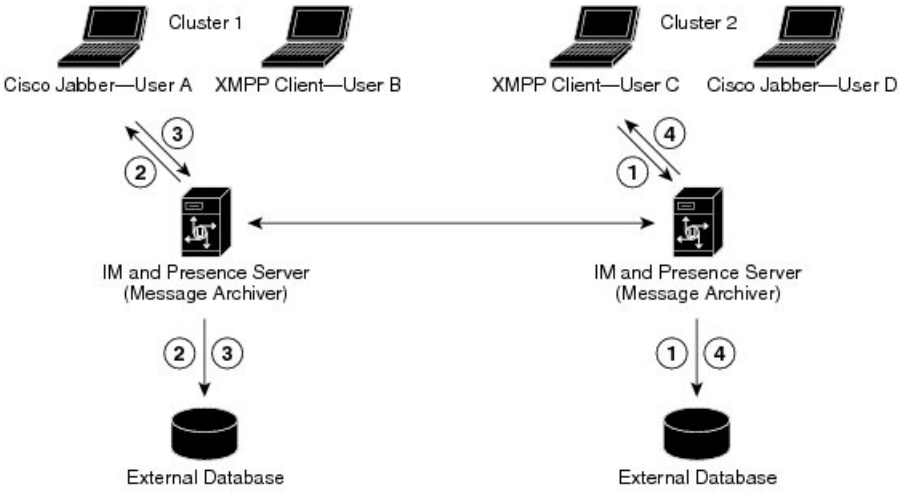


Intercluster or Federated Network Configuration

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



Prerequisite Configuration Tasks

Before you use this guide to configure IM compliance, make sure that you have performed the following tasks:

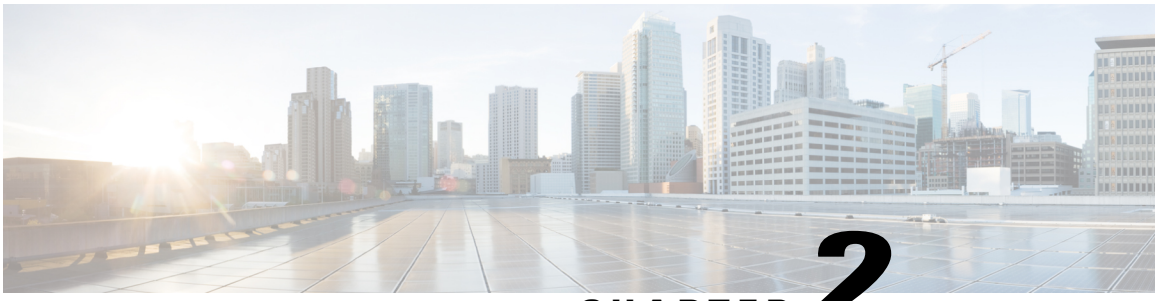
- Install the IM and Presence Service nodes as described in *Installing Cisco Unified Communications Manager*.
- Configure the IM and Presence Service nodes as described in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.
- Set up the external database as described in *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .

Support for PostgreSQL 9.1.1

To deploy PostgreSQL version 9.1.1 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 *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .



CHAPTER 2

IM Compliance Configuration

- Configure IM Compliance, page 7
- Turning on Cisco XCP Message Archiver Service, page 8

Configure IM Compliance

We recommend that you perform this configuration on the publisher node in your cluster.

Before You Begin

- Install and configure one or more supported external databases. Refer to the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .
- Configure the external databases on IM and Presence Service. Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Databases**.
- Make sure that the trace level for the Cisco XCP Router service is set to info or higher.

Procedure

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

Step 2 Choose Message Archiver from the Compliance Server Selection.

Step 3 (Optional) Check the **Enable Outbound Message Logging** checkbox.
Turning on this option can degrade IM performance. Because all inbound messages are already logged, do not enable this setting unless you are using IM compliance in intercluster or federated networks.

Step 4 For each node, assign a database from the External Database option.
If you are using one external database for your cluster, assign all nodes to the same external database. If you are using more than one external database for your cluster, assign the nodes to the external databases based on your capacity requirements.

Step 5 Click **Save**.

Step 6 Start the Cisco Message Archiver service (if this service is not already started).

Step 7 Restart the Cisco XCP Router service.
Troubleshooting Tips

a) If you make any subsequent changes to the Message Archiver configuration, restart the Cisco XCP Router service.

b) (All releases) If you switch between IM compliance deployment options (for example, switch from the Third-Party Compliance Server option to the Message Archiver option), you must restart the Cisco XCP Router service.

What to Do Next

Turning on Cisco XCP Message Archiver Service, on page 8

Related Topics

Set Trace Level to Info to Support IM Compliance, on page 12
Restart Cisco XCP Router Service, on page 11
Restart Cisco XCP Message Archiver Service, on page 12
Sample Topologies and Message Flow for IM Compliance, on page 2

Turning on Cisco XCP Message Archiver Service

The Cisco XCP Message Archiver service must be running for the compliance feature to operate correctly on IM and Presence Service.

Note If you do not assign an external database to a node for the compliance feature, IM and Presence Service does not permit you to turn on the Cisco XCP Message Archiver service.

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Step 2 Choose the server from the Server list box.

Step 3 Click Go.

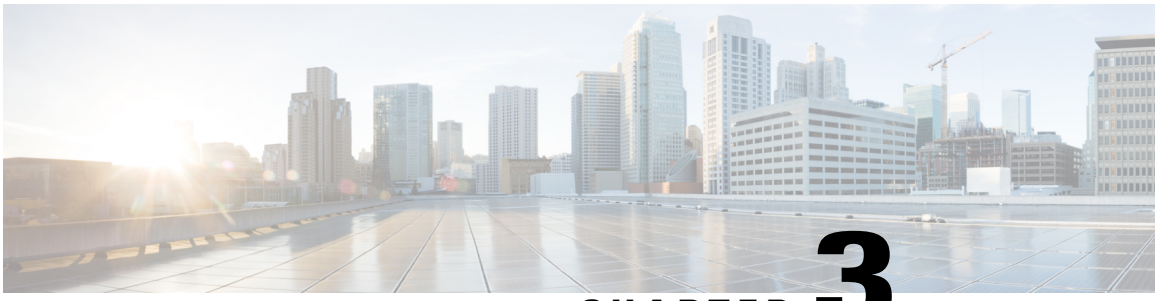
Step 4 Click the radio button next to the Cisco XCP Message Archiver service in the IM and Presence Services section.

Step 5 Click Save.
Troubleshooting Tips

If the Cisco XCP Message Archiver service fails to start, but the System Troubleshooter (**Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**) shows that the status of the external database connection is ok, we recommend that you unassign the external database from the node, and reassign it again.

Related Topics

Configure IM Compliance, on page 7



CHAPTER 3

IM Compliance Serviceability and Troubleshooting

- Restart Cisco XCP Router Service, page 11
- Restart Cisco XCP Message Archiver Service, page 12
- Set Trace Level to Info to Support IM Compliance, page 12
- Configure Alarms for IM Compliance, page 12

Restart Cisco XCP Router Service

Procedure

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

Step 2 Choose the server from the Server list box.

Step 3 Click **Go**.

Step 4 Click the **Cisco XCP Router** radio button in the IM and Presence Services section.

Step 5 Click **Restart**.

Step 6 Click **OK** when a message indicates that restarting may take a while.

Restart Cisco XCP Message Archiver Service

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services**.

Step 2 Choose the server from the Server list box.

Step 3 Click **Go**.

Step 4 Click the **Cisco XCP Message Archiver** radio button in the IM and Presence Services section.

Step 5 Click **Restart**.

Set Trace Level to Info to Support IM Compliance

The Message Archiver component uses the logging feature of the Cisco XCP Router service which requires that the trace level is set to Info or higher.

Note IM and Presence Service sets the trace level for Cisco XCP Router to Info by default. If you change the trace level to a level below Info, the compliance feature will not function correctly on IM and Presence Service.

Procedure

Step 1 Sign in to 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**Trace** > **Configuration**.

Step 4 Choose the server that is running the service for which you want to configure trace from the Server list box and click **Go**.

Step 5 Choose IM and Presence Services from the Service Group list box and click **Go**.

Step 6 Choose the Cisco XCP Router service from the Service list box and click **Go**.

Step 7 Check the **Trace On** check box.

Step 8 Choose Info as the Debug Trace Level in the **Trace Filter Settings**.

Configure Alarms for IM Compliance

If IM and Presence Service loses its connection to the external database, users will still be able to send instant messages to each other. However, these messages will not be archived, and you will no longer be satisfying

any regulatory compliance guidelines. To ensure that you are notified if this connection is lost, you should verify that its associated alarm is properly configured.

Procedure

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.

Step 5 Click **Go**.

Step 6 From the Service Group drop-down list, choose IM and Presence Services.

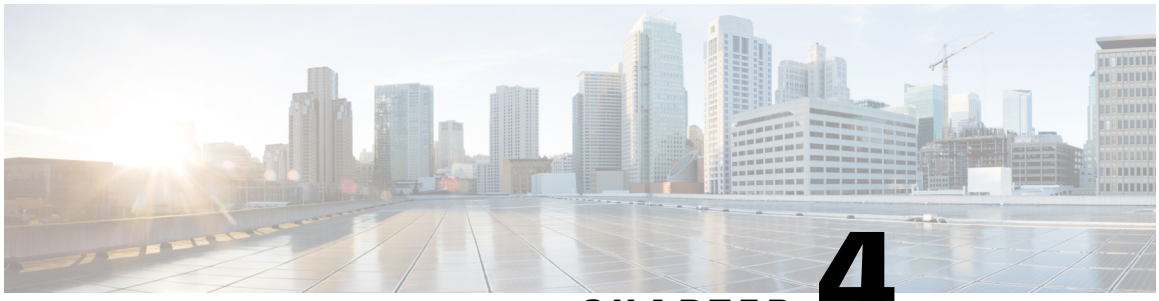
Step 7 Click **Go**.

Step 8 From the Service drop-down list, choose Cisco XCP Message Archiver.

Step 9 Click **Go**.

Step 10 Configure the alarm settings as preferred.

Step 11 Click **Save**.



CHAPTER 4

Integration with Third-Party Compliance Servers

- About Third-Party IM Compliance, page 15
- Configure Third-Party Compliance Server on IM and Presence Service, page 16
- Assign Third-Party Compliance Server to IM and Presence Service Node, page 17

About Third-Party IM Compliance

As an alternative to IM compliance, you can integrate IM and Presence Service with a third-party compliance server. With this solution, IM and Presence Service only delivers messages to users after it successfully logs the message to a third-party compliance server. If the compliance server is unavailable, IM and Presence Service does not deliver the message to the recipient.

Third-party IM compliance requires these components:

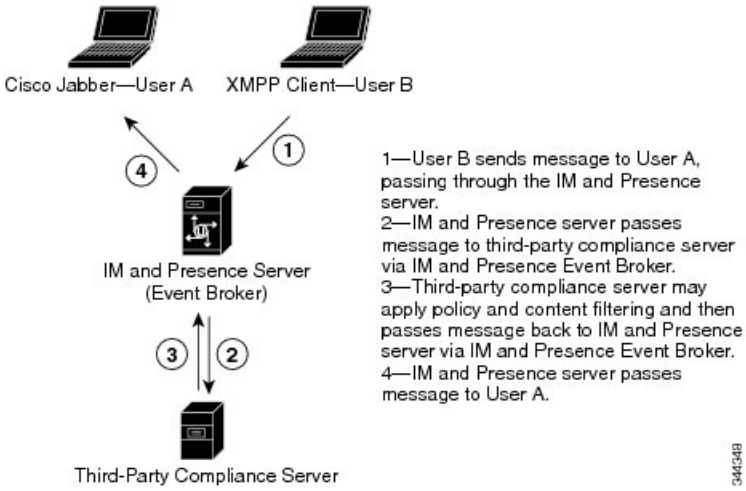
- IM and Presence Service Release 9.0(1) - IM and Presence Service uses the Event Broker component to send messages to the third-party compliance server.
- Third-party compliance server - You require a third-party compliance server for each node in the cluster.
- IM Client - Supported clients include 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.

To use the third-party compliance solution you must configure a third-party compliance server for each node in the cluster. IM and Presence Service passes all messages that are sent to or from any users associated with a node to the designated third-party compliance server for that node. The third-party compliance server applies any relevant policy or filtering to the message, and then passes the message back to IM and Presence Service. IM and Presence Service delivers the message to the recipient. Note that you may potentially experience performance delays in your network because of the volume of messages 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. The following figure highlights these components and message flow.

Figure 3: Third-Party IM Compliance



Configure Third-Party Compliance Server on IM and Presence Service

Before You Begin

- Install and configure the third-party compliance server(s)
- Install the IM and Presence Service nodes as described in *Installing Cisco Unified Communications Manager*.
- Configure the IM and Presence Service nodes as described in the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* .

Procedure

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 server details.

Step 4 Enter a value for the Restart Interval. If you want to restart the connection to the third-party compliance component if it should fail, enter the number of seconds at smaller or larger restart intervals as required. If you change this setting, you must restart the Cisco XCP Router service.

Step 5 (Optional) Check the **Enable Packet Size Limits** checkbox to restrict amount of data transferred to the third-party server.

Note During an upgrade **Enable Packet Size Limits** will be reset to the default value.

Step 6 Click **Save**.

Step 7 Restart the Cisco XCP Router service.

Troubleshooting Tip

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

You will not be able to change the name of the compliance server after it is assigned. If you change any other settings (such as the port number) without changing it on the compliance server itself, the compliance will stop working.

Related Topics

Restart Cisco XCP Router Service, on page 11
About Third-Party IM Compliance, on page 15

Assign Third-Party Compliance Server to IM and Presence Service Node

Before You Begin

Configure a third-party IM compliance server on IM and Presence Service.

Procedure

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

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

Step 3 Assign a third-party IM compliance server to a IM and Presence Service node in the Third-Party Server Assignment window.

Step 4 Click **Save**.

Step 5 Restart the Cisco XCP Router Service.

Troubleshooting Tips

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.

Related Topics

Configure Third-Party Compliance Server on IM and Presence Service, on page 16
Restart Cisco XCP Router Service, on page 11