# 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.<br><br>This feature requires that you deploy an external database on which to store archived messages.<br><br>To deploy the Message Archiver, go to Message Archiver Configuration. |

| 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.<br><br>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.<br><br>To deploy this integration, go to Third-Party Compliance Server Integration. |

# 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

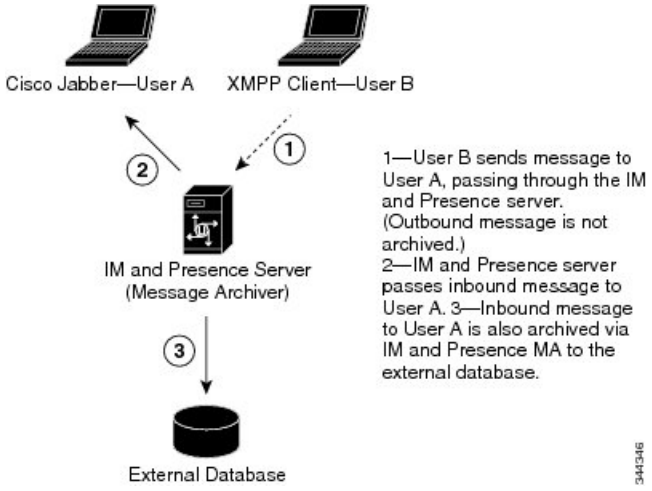
When using IM compliance in a single cluster, we highly recommend that you deploy one external database per cluster to which all incoming messages sent to users in the cluster are logged.

**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***

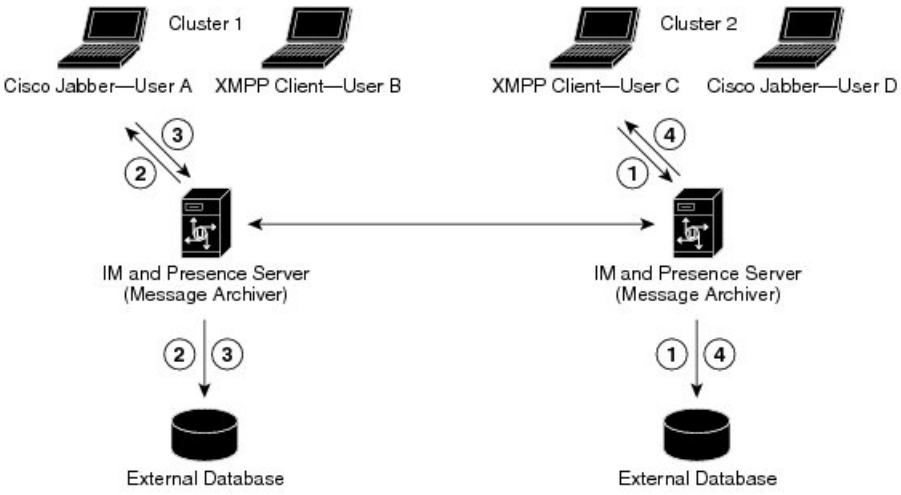



### Intercluster or Federated Network Configuration

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.