# 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 1: 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 5 | Enable the Message Archiver feature settings. |
| **Step 2** | Activate the Cisco XCP Message Archiver, on page 5 | 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 6 | After you enable the Message Archiver, restart the Cisco XCP Router service on all nodes. |
| **Step 4** | Configure Alarms for IM Compliance, on page 6 | Configure alarms for the Message Archiver so that any connection issues can be resolved quickly. |
| **Step 5** | Configure the Maximum Queue, on page 7 | 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 7 | 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 5

# 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 6

# 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 7 | In the IM and Presence Service, enable encryption and enter an encryption password. |
| **Step 2** | Generate Public-Private Key Pair, on page 8 | 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 8 | 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 9 | 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 8

## 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 8

## 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 2: 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 3: Troubleshooting for Encrypted Compliance Database***

| Error | Remedy |
|---|---|
| Encryption cannot be enabled | Do the following:<br>• Check the external compliance database connection. Make sure the compliance database is Microsoft SQL Server.<br>• Check that the Cisco XCP Message Archiver service is running.<br>• Confirm that you are on a node in the master cluster. You cannot enable encryption from a slave cluster.<br>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:<br>• Make sure that your encryption password is correct.<br>• 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.