Configure Security Settings

- Security Overview, on page 1
- Security Settings Configuration Task Flow , on page 1

Security Overview

This chapter contains procedures for configuring security settings on the IM and Presence Service. On the IM and Presence Service, you can configure secure TLS connections and enable enhanced security settings such as FIPS mode.

The IM and Presence Service shares a platform with Cisco Unified Communications Manager. For information on how to configure security in Cisco Unified Communications Manager, refer to the *Security Guide for Cisco Unified Communications Manager*.

Security Settings Configuration Task Flow

Complete these optional tasks to set up security with the IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Create Login Banner, on page 2	Create a login banner that users must acknowledge when they log in to any IM and Presence Service interface.
Step 2	Configure Secure XMPP Connections , on page 2	Complete these tasks to configure XMPP security.
Step 3	Configure TLS Peer Subject, on page 3	Configure these tasks if you want to set up TLS peers.
Step 4	Configure TLS Context, on page 4	Configure a TLS Context and TLS ciphers for your TLS peers.
Step 5	FIPS Mode, on page 5	If you want your deployment to be FIPS-compliant, you can enable FIPS mode.

	Command or Action	Purpose
		For added security, you can also enable Enhanced Security mode and Common Compliance mode.

Create Login Banner

You can create a banner that users acknowledge as part of their login to any IM and Presence Service interface. You create a .txt file using any text editor, include important notifications they want users to be made aware of, and upload it to the Cisco Unified IM and Presence OS Administration page.

This banner will then appear on all IM and Presence Service interfaces notifying users of important information before they login, including legal warnings and obligations. The following interfaces will display this banner before and after a user logs in: Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Operating System Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, and IM and Presence Disaster Recovery System.

Procedure

Step 1 Create a .txt file with the contents you want to display in the banner.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 3 Choose **Software Upgrades** > **Customized Logon Message**.

Step 4 Click **Browse** and locate the .txt file.

Step 5 Click **Upload File**.

The banner will appear before and after login on most IM and Presence Service interfaces.

Note
The .txt filemust be uploaded to each IMand Presence Service node separately.

Configure Secure XMPP Connections

Use this procedure to enable secure XMPP connections using TLS.

Procedure

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

Step 2 Check the appropriate check box to enable the following XMPP security settings:

Table 1: XMPP Security Settings for the IM and Presence Service

Settings	Description
Enable XMPP Client To IM/P Service Secure Mode	When enabled, the IM and Presence Service establishes a secure TLS connection with XMPP client applications in a cluster. This setting is enabled by default. We recommend that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.
Enable XMPP Router-to-Router Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between XMPP routers in the same cluster, or in different clusters. IM and Presence Service automatically replicates the XMPP certificate within the cluster and across clusters as an XMPP trust certificate. An XMPP router will attempt to establish a TLS connection with any other XMPP router that is in the same cluster or a different cluster, and is available to establish a TLS connection.
Enable Web Client to IM/P Service Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP-based API client applications. If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence Service.

Step 3 Click **Save**.

What to do next

If you updated the **Enable XMPP Client To IM/P Service Secure Mode** setting, restart the Cisco XCP Connection Manager.

SIP Security Settings Configuration on IM and Presence Service

Configure TLS Peer Subject

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Security** > **TLS Peer Subjects**.

Step 2 Click **Add New**.

Step 3 Perform one of the following actions for the Peer Subject Name:

a) Enter the subject CN of the certificate that the node presents.

b) Open the certificate, look for the CN and paste it here.

Step 4 Enter the name of the node in the Description field.

Step 5 Click **Save**.

What to do next

Proceed to configure the TLS context.

Configure TLS Context

Use this procedure to assign a TLS context and TLS ciphers to your TLS peer subjects.

Note When you import an IM and Presence Service certificate, the IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list.

Before you begin

Configure TLS Peer Subject, on page 3

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, **System** > **Security** > **TLS Context Configuration**.

Step 2 Click **Find**.

Step 3 Choose **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 4 From the list of available TLS peer subjects, select the TLS peer subject that you configured.

Step 5 Use the > arrow to move this TLS peer subject to **Selected TLS Peer Subjects**.

Step 6 Configure the **TLS Cipher Mapping** options:

a) Review the list of TLS ciphers that are available in the **Available TLS Ciphers** and **Selected TLS Ciphers** boxes.

b) If you want to enable a TLS cipher that isn't currently selected, use the > arrow to move the cipher to **Selected TLS Ciphers**.

Step 7 Click **Save**.

Step 8 Restart the Cisco SIP Proxy service:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**.

b) From the **Server** drop-down list box, select an IM and Presence Service cluster node and click **Go**.

c) Select the **Cisco SIP Proxy** service and click **Restart**.

FIPS Mode

The IM and Presence Service contains a set of enhanced system security modes that allows your system to operate in a stricter set of security guidelines and risk management controls around items such as cryptography, data and signaling encryption, and audit logging.

- FIPS Mode—The IM and Presence Service can be configured to operate in FIPS mode, which allows your system to comply with FIPS or Federal Information Processing Standards, a US and Canadian government standard for cryptographic modules.
- Enhanced Security Mode—Enhanced Security Mode runs on a FIPS-enabled system and provides additional risk management controls such as data encryption requirements, a stricter credential policy, user authentication for contact searches, and stricter audit logging requirements.
- Common Criteria Mode—Common Criteria mode also runs on a FIPS-enabled system providing additional controls that allows your system to comply with Common Criteria guidelines such as TLS and the use of X.509 v3 certificates.

Note If the external database is MSSQL, for the services like Message Archiver, Text Conference Manager, and File Transfer Manager to work in the Common Criteria mode, you must perform the following:

1. Configure the server hosting the MSSQL database to support TLS 1.1 or higher.
2. Re-upload the database certificate to the IM and Presence service.
3. Check the **Enable SSL** checkbox in the **External Database Configuration** page. Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Server Setup** > **External Databases** to configure the external database.

Important This note is applicable for Release 12.5(1)SU7 only.

If you have multiserver SAN certificate configuration on the cluster, and move the cluster to FIPS and Common Criteria mode. It will convert multiserver SAN certificates to self-signed certificates.

If the old multiserver SAN certificate remains on Unified Communications Manager servers in the FIPS and Common Criteria mode, it needs to be deleted manually.

For details on how to enable FIPS Mode, Enhanced Security Mode, and Common Criteria Mode in Cisco Unified Communications Manager and the IM and Presence Service, refer to the "FIPS Mode Setup" chapter of the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

FIPS for Outlook Calendar Integration

When FIPS mode is enabled on IM and Cisco Presence Service server, only NTLMv2 is supported to get the Exchange Web Services information. If FIPS mode is disabled, then both NTLMv1 and NTLMv2 are supported

as per the existing behavior. Basic Authentication is supported in both the cases regardless of enabling or disabling FIPS mode.

A new service parameter for Presence Engine service named **FIPS Mode Exchange Server Authentication** is introduced to validate the type of authentication used by the Presence Engine to establish a connection with Exchange Server through the Microsoft Outlook Calendar Integration feature.

You can set the **FIPS Mode Exchange Server Authentication** service parameter to either **Auto** or **Basic Only**.

Service parameter set to **Auto**: The Presence Engine negotiates NTLMv2 first and falls back to "Basic Authentication" only if NTLMv2 negotiation fails. NTLMv1 will not be negotiated in FIPS Mode.

Service parameter set to **Basic Only**: The Presence Engine is forced to use "Basic Authentication" even though the Exchange Server is configured to allow both NTLM and Basic Authentication.

Note Any changes in the service parameter setting requires restart of the Cisco Presence Engine.