Security Modes

Security Modes Overview

To implement security mechanisms to prevent tampering of data or information, Unified Communications Manager provides the following security modes:

- Non-Secure Mode—default mode
- Secure Mode or Mixed Mode—supports secure and non-secure endpoints.
- SIP Auth Mode—uses OAuth refresh tokens for Cisco Jabber authentication in secure environments

Non Secure Mode (Default Mode)

The non secure mode is the default security mode when you install Unified Communications Manager for the first time. In this mode, Unified Communications Manager doesn't provide any secure signaling or media services.

Configure Secure Mode

To apply security, configure the security mode that applies to your deployment.

Procedure

	Command or Action	Purpose
Step 1	Mixed Mode	Enable mixed mode to add security for Cisco IP Phones and Webex devices. Provides information on how to enable and verify mixed mode.

	Command or Action	Purpose
Step 2	SIP OAuth Mode	Configure SIP OAuth Mode to add security for Cisco Jabber clients and other devices.

Mixed Mode

The mixed mode or secure mode supports secure and non-secure endpoints. When you install Unified Communications Manager fresh on a cluster or server, by default it's in non-secure mode. However, you can convert the security mode from non-secure to secure or mixed mode.

To change a cluster from a non-secure mode to a mixed mode (secure mode), perform the following:

- Enable Certificate Authority Proxy Function (CAPF) service on the publisher.
- Enable Certificate Trust List (CTL) service on the publisher.

When a Call Manager certificate is self-signed, the CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

In the case of a Multi-SAN Call Manager certificate, the CTL file contains the Publisher's Call Manager certificate.

The next time that the phone initializes, it downloads the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in.sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file.

You can update the CTL file running the following commands:

- **utils ctl set-cluster mixed-mode**

  Updates the CTL file and sets the cluster to mixed mode.

- **utils ctl set-cluster non-secure-mode**

  Updates the CTL file and sets the cluster to non-secure mode.

- **utils ctl update CTLFile**

  Updates the CTL file on each node in the cluster.

Note For endpoint security, Transport Layer Security (TLS) is used for signaling and Secure RTP (SRTP) is used for media.

To enable mixed mode, log in to the Command Line Interface on the publisher node and Run the CLI command `utils ctl set-cluster mixed-mode`.

Note Make sure that Unified Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The Registration Token received from the Smart account or Virtual account has Allow Export-Controlled functionality enabled while registering with this cluster.

For the tokenless CTL file, administrators must ensure that the endpoints download the uploaded CTL file generated using USB tokens on Unified Communications Manager Release 12.0(1) or later. After the download, they can switch to tokenless CTL file. Then, they can run the util ctl update CLI command.

You can verify the security mode, if you have changed it from non-secure to secure or mixed mode. To verify the mode, navigate to the **Enterprise Parameters Configuration** page to verify if your cluster or server is in mixed mode or not. See Verify Security Mode topic for more information.

Verify Security Mode

You can verify the security mode, if you have changed it from non-secure to secure or mixed mode. To verify the mode, navigate to the **Enterprise Parameters Configuration** page to verify if your cluster or server is in mixed mode or not.

Perform the following procedure to verify the security mode:

Step 1 From Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 2 Navigate to the **Security Parameters** pane.
You'll find the **Cluster Security Mode** field with the appropriate value. If the value displays as 1, you have successfully configured Unified Communications Manager for mixed mode. You can't configure this value in Cisco Unified CM Administration page. This value displays after you have entered the CLI command `set utils cli`.

Note The cluster security mode configures the security capability for a standalone server or a cluster.

SAST Roles of CTL File

Note *Signer, mentioned in the following table, is used to sign the CTL file.

Table 1: System Administrator Security Token (SAST) Roles of CTL File

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
12.0(1)	Token 1 (Signer*) Token 2 ITLRecovery CallManager	ITLRecovery (Signer) CallManager

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
11.5(x)	Token 1 (Signer) Token 2 ITLRecovery CallManager	CallManager (Signer) ITLRecovery
10.5(2)	Token 1 (Signer) Token 2	CallManager (Signer) ITLRecovery
10.5(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
10.0(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
9.1(2)	Token 1 (Signer) Token 2	Not applicable

SIP OAuth Mode

SIP OAuth mode allows you to use OAuth refresh tokens for Cisco Jabber authentication in secure environments. Supporting OAuth on the Unified Communications Manager SIP line allows secure signalling and media without CAPF. OAuth token validation during SIP registration is completed when OAuth based authorization is enabled on Unified Communication Manager cluster and Cisco Jabber endpoints.

.OAuth support for SIP registrations is available for Cisco Jabber devices and certain Phone models.For more information on SIP OAuth, see Feature Configuration Guide for Cisco Unified Communications Manager.

SIP OAuth Configuration Through CLI

Through the CLI, you can configure the Cluster SIP OAuth mode.

Note For more information on how to configure SIP OAuth mode on Cisco Unified Communication Manager, see *Feature Configuration Guide for Cisco Unified Communications Manager, Release 14*.

Consider the following points:

- When Cluster SIP OAuth mode is enabled, Cisco Unified Communication Manager accepts SIP registrations with an OAuth token from secure devices.

  Once enabled, the following TLS ports are opened which are configurable through Cisco Unified Communications Manager user interface.

  - **SIP OAuth Port**
  - **SIP OAuth MRA Port**

You can configure the ports from Cisco Unified CM Administration, choose **System** > **Cisco Unified CM** > **CallManager** page.

- Restart the Cisco CallManager service in all the nodes for the parameter change to take effect.

The encryption option consists of the following CLI commands:

admin:utils sipOAuth-mode
Check the status of SIP OAuth mode in the cluster.

utils sipOAuth-mode enable
Enables the SIP OAuth mode in the cluster.

utils sipOAuth-mode disable
Disables the SIP OAuth mode in the cluster.

Note Run the CLI commands only on the publisher node.