An Overview

System Requirements

The following are the system requirements to authenticate or encrypt the Unified Communications Manager:

- Login to Cisco Unified Communications Manager Administration CLI of the Unified Communications Manager publisher and run **util ctl** command to set the cluster to mixed mode (Secure Mode).

- Locally Significant Certificates (LSC) exist in all phones to authenticate the TLS connection with Unified Communications Manager.

Note A few Endpoints also use MICs if the LSC is not present but we always recommend you to use LSCs.

Best Practices

Cisco strongly recommends the following best practices:

- Always perform installation and configuration tasks in a secure lab environment before you deploy to a wide-scale network.

- Use IPSec for gateways and other application servers at remote locations.

Warning Failure to use IPSec in these instances results in session encryption keys getting transmitted in the clear.

- To prevent toll fraud, configure conference enhancements that are described in the System Configuration Guide for Cisco Unified Communications Manager. Likewise, you can perform configuration tasks to

restrict external transferring of calls. For more information on how to perform this task, see Feature Configuration Guide for Cisco Unified Communications Manager.

Device Resets, Server and Cluster Reboots, and Service Restarts

The following table lists the security actions with reset, restart, and reboot details:

Table 1: Security Actions with Reset, Restart, and Reboot details:

SI No	Action	Reset (Yes / No)	Restart (Yes / No)
1	Apply Security Profile	Yes	No
2	Apply Phone Hardening	—	—
3	Security Mode Changes	Yes. All devices	Yes. Restart CallManager service.
4	CTL File Update	—	Yes.All encrypted and authenticated phones need to be reset to ensure they get an updated CTL file.
5	Update Ports for TLS Connection	—	Yes. Restart the CTL Provider Service.
6	Update /Configure CAPF service parameters	—	Yes. Restart the Cisco Certificate Authority Proxy Function service
7	Start or Stop the CTL Provider service	—	Yes. Restart all Cisco CallManager and Cisco TFTP services
7	Configure secure SRST references	Yes. Reset dependent devices	—
8	Change the Smart Card service to Started and Automatic	—	Yes
9	Configure security-related service parameters that are associated with the application User CAPF Profile.	—	Yes. Restart the Cisco IP Manager Assistant service, Cisco Web Dialer Web Service, and the Cisco Extended Functions service after

To restart the Unified Communications Manager service, see Administration Guide for Cisco Unified Communications Manager.

To reset a single device after you update the phone configuration, see topics related to applying the phone security profile.

Reset Devices, Servers, Clusters, and Services

This section provides information on when to reset devices, servers, clusters, and services in Cisco Unified Serviceability.

To reset all devices in a cluster, perform the following procedure:

Step 1   From Unified Communications Manager, choose **System** > **CiscoUnifiedCM**.

Step 2   Click **Find**.

A list of configured Unified Communications Manager servers appears.

Step 3   Choose the Unified Communications Manager on which you want to reset devices.

Step 4   Click **Reset**.

Step 5   Perform Step 2 and Step 4 for each server in the cluster.

Media Encryption with Barge Setup

Configure barge for Cisco Unified IP Phones 7962 and 7942 for encryption and perform the following tasks in Cisco Unified Communications Manager Administration.

• Update the Cluster Security Mode using CLI commands (utils ctl set cluster mixed-mode).

• Update the Builtin Bridge Enable parameter in the **Service Parameter** window.

On completion of the tasks, the following message appears.

> ⚠️
>
> **Attention**   If you configure encryption for Cisco Unified IP Phone models 7962 and 7942, the encrypted devices can't accept a barge request when they are participating in an encrypted call. The barge attempt fails when the call is encrypted.

Cisco Unified IP Phones 7962 and 7942 configured with an encrypted security profile doesn't display the message in the **Phone Configuration** window. You choose **Default** for the Built In Bridge setting or the default setting equals Default. The same restriction applies for either selection.

> 🔍
>
> **Tip**   Reset the dependent CiscoIP devices for changes to take effect.

Common Icons

Unified Communications Manager provides a security status for calls based on security levels configured for all servers and devices participating in the call.

All phones that support security icons display call security level.

• A shield icon appears for calls with authenticated level of signaling security. A shield identifies a secured connection between CiscoIP devices, which means that the devices are authenticated and are using encrypted signaling.

• A lock icon appears for calls with encrypted media, which means that the devices are using encrypted signaling and encrypted media.

Note Some phone models only display the lock icon.

The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints.

The audio and video call provide basis for the call security status. The call is secure only if both the audio and video are secure.

Note The "Override BFCP Application Encryption Status When Designating Call Security Status" service parameter displays a lock icon when the parameter value is True and audio is secure. This condition ignores the security statuses of all other media channels. The default parameter value is False.

For conference and barge calls, the security icon displays the security status for the conference.