Phone Security

Phone Security Overview

At installation, Unified Communications Manager boots up in nonsecure mode. When the phones boot up after the Unified Communications Manager installation, all devices register as nonsecure with Unified Communications Manager.

After you upgrade from Unified Communications Manager 4.0(1) or a later release, the phones boot up in the device security mode that you enabled prior to the upgrade; all devices register by using the chosen security mode.

The Unified Communications Manager installation creates a self-signed certificate on the Unified Communications Manager and TFTP server. You may also choose to use a third-party, CA-signed certificate for Unified Communications Manager instead of the self-signed certificate. After you configure authentication, Unified Communications Manager uses the certificate to authenticate with supported Cisco Unified IP Phones. After a certificate exists on the Unified Communications Manager and TFTP server, Unified Communications Manager does not reissue the certificates during each Unified Communications Manager upgrade. You must update the ctl file using CLI command **util ctl update CTLFile** with the new certificate entries.

Tip For information on unsupported or nonsecure scenarios, see topics related to interactions and restrictions.

Unified Communications Manager maintains the authentication and encryption status at the device level. If all devices that are involved in the call register as secure, the call status registers as secure. If one device registers as nonsecure, the call registers as nonsecure, even if the phone of the caller or recipient registers as secure.

Unified Communications Manager retains the authentication and encryption status of the device when a user uses Cisco Extension Mobility. Unified Communications Manager also retains the authentication and encryption status of the device when shared lines are configured.

Tip When you configure a shared line for an encrypted Cisco IP Phone, configure all devices that share the lines for encryption; that is, ensure that you set the device security mode for all devices to encrypted by applying a security profile that supports encryption.

Phone Hardening Overview

This section provides an overview of the phone hardening behaviours like Gratuitous ARP Disable, Web Access Disable, PC Voice VLAN Access Disable, Setting Access Disable and PC Port Disable and so on.

The following optional settings are used to harden the connection to Cisco IP Phones. These settings appear in the Product-Specific Configuration Layout of the **Phone Configuration** window.

To apply them to a set of phones, or all phones enterprise-wide, these settings also appear in the **Common Phone Profile Configuration** window and the **Enterprise Phone Configuration** window.

Table 1: Phone Hardening Behaviour

Phone Hardening Behaviour	Description	
Gratuitous ARP Disable	By default, Cisco Unified IP Phones accept Gratuitous ARP packets. Gratuitous ARP packets, which devices use, announce the presence of the device on the network. However, attackers can use these packets to spoof a valid network device; for example, an attacker could send out a packet that claims to be the default router. If you choose to do so, you can disable Gratuitous ARP in the **Phone Configuration** window. **Note** Disabling this functionality does not prevent the phone from identifying its default router.	

Phone Hardening Behaviour	Description	
Web Access Disable	Disabling the web server functionality for the phone blocks access to the phone internal web pages, which provide statistics and configuration information. Features, such as CiscoQuality Report Tool, do not function properly without access to the phone web pages. Disabling the web server also affects any serviceability application, such as CiscoWorks, that relies on web access. To determine whether the web services are disabled, the phone parses a parameter in the configuration file that indicates whether the services are disabled or enabled. If the web services are disabled, the phone does not open the HTTP port 80 for monitoring purposes and blocks access to the phone internal web pages.	
PC Voice VLAN Access Disable	By default, Cisco IP Phones forward all packets that are received on the switch port (the one that faces the upstream switch) to the PC port. If you choose to disable the PC Voice VLAN Access setting in the Phone Configuration window, packets that are received from the PC port that use voice VLAN functionality will drop. Various Cisco IP Phones use this functionality differently. • Cisco Unified IP Phones 7942 and 7962 drop any packets that are tagged with the voice VLAN, in or out of the PC port.	

Phone Hardening Behaviour	Description	
Setting Access Disable	By default, pressing the Applications button on a Cisco IP Phone provides access to a variety of information, including phone configuration information. Disabling the Setting Access parameter in the Phone Configuration window prohibits access to all options that normally display when you press the Applications button on the phone; for example, the Contrast, Ring Type, Network Configuration, Model Information, and Status settings. The preceding settings do not display on the phone if you disable the setting in Unified Communications Manager Administration. If you disable this setting, the phone user cannot save the settings that are associated with the Volume button; for example, the user cannot save the volume. Disabling this setting automatically saves the current Contrast, Ring Type, Network Configuration, Model Information, Status, and Volume settings that exist on the phone. To change these phone settings, you must enable the Setting Access setting in Unified Communications Manager Administration.	

Phone Hardening Behaviour	Description	
PC Port Disable	By default, Unified Communications Manager enables the PC port on all Cisco IP Phones that have a PC port. If you choose to do so, you can disable the PC Port setting in the Phone Configuration window. Disabling the PC port proves useful for lobby or conference room phones. **Note** The PC port is available on some phones and allows the user to connect their computer to the phone. This connection method means that the user only needs one LAN port.	

Set Up Phone Hardening

Phone Hardening consists of optional settings that you can apply to your phones in order to harden the connection. You can apply settings using one of three configuration windows:

- Phone Configuration - use **Phone Configuration** window to apply the settings to an individual phone
- Common Phone Profile - use the **Common Phone Profile** window to apply the settings to all of the phones that use this profile
- Enterprise Phone - use the **Enterprise Phone** window to apply the settings to all of your phones enterprise wide

Note If conflicting settings appear in each of these windows, following is the priority order the phone uses to determine the correct setting: 1) Phone Configuration, 2) Common Phone Profile, 3)Enterprise Phone

To setup phone hardening, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Specify the criteria to find the phone and click **Find** to display a list of all phones.

Step 3 Click the device name.

Step 4 Locate the following product-specific parameters:

a) PC Port
b) Settings Access
c) Gratuitous ARP
d) PC Voice VLAN Access
e) Web Access

Tip To review information on these settings, click the help icon that appears next to the parameters in the **Phone Configuration** window.

Step 5 Choose **Disabled** from the drop-down list for each parameter that you want to disable. To disable the speakerphone or speakerphone and headset, check the corresponding check boxes.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Trusted Devices

Unified Communications Manager allows Security icons to be enabled by phone model on Cisco IP Phones. The Security icon indicates whether the call is secure and the connected device is trusted.

A Trusted Device represents a Cisco device or a third-party device that has passed Cisco security criteria for trusted connections. This includes, but is not limited to, signaling/media encryption, platform hardening, and assurance. If a device is trusted, a Security icon displays and a secure tone plays on supported devices. Also, the device may provide other features or indicators that are related to secure calls.

Unified Communications Manager determines whether a device is trusted when you add it to your system. The security icon displays for information purposes only, and the administrator cannot configure it directly.

Unified Communications Manager also indicates whether a gateway is trusted by displaying an icon and a message in Unified Communications Manager Administration.

This section describes the behavior of the security icon for trusted devices on both the Cisco IP Phones and in Unified Communications Manager Administration.

Cisco Unified Communications Manager Administration

The following windows in Unified Communications Manager Administration indicate whether a device is trusted:

Gateway Configuration

For each gateway type, the Gateway Configuration window (**Device** > **Gateway**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Phone Configuration

For each phone device type, the Phone Configuration window (**Device** > **Phone**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Device Called Trust Determination Criteria

The type of device that a user calls affects the security icon that displays on the phone. The system considers the following three criteria to determine whether the call is secure:

- Are all devices on the call trusted?
- Is the signaling secure (authenticated and encrypted)?
- Is the media secure?

Before a supported Cisco Unified IP Phone displays the Lock Security icon, be aware that all three of these criteria must be met. For calls that involve a device that is not trusted, regardless of signaling and media security, the overall status of the call will stay unsecure, and the phone will not display the Lock icon. For example, if you include an untrusted device in a conference, the system considers its call leg, as well as the conference itself, to be unsecure.

Phone Model Support

There are two categories of phone models which support security in Unified Communications Manager: Secure Cisco phones and Secure Preferred Vendor phones. Secure Cisco phones are pre-installed with a Manufacture-Installed Certificate (MIC) and support automatic generation and exchange of Locally-Significant Certificates (LSC) using the Certificate Authority Proxy Function (CAPF). Secure Cisco phones are capable of registering with Cisco Unified CM using the MIC without additional certificate management. For additional security, you can create and install an LSC on the phone using CAPF. See topics related to phone security setup and settings for more information.

Secure Preferred Vendor phones do not come pre-installed with a MIC, and do not support CAPF for generating LSCs. In order for Secure Preferred Vendor phones to connect to Cisco Unified CM, a certificate must be provided with the device, or generated by the device. The phone supplier must provide the details on how to acquire or generate a certificate for the phone. Once you obtain the certificate, you must upload the certificate to the Cisco Unified CM using the OS Administration Certificate Management interface. See topics related to preferred vendor SIP phone security set up for more information.

For a list of security features that are supported on your phone, refer to the phone administration and user documentation that supports this Unified Communications Manager release or the firmware documentation that supports your firmware load.

You can also use Cisco Unified Reporting to list the phones that support a particular feature. For more information about using Cisco Unified Reporting, see the Cisco Unified Reporting Administration Guide.

View Phone Security Settings

You can configure and view certain security-related settings on phones that support security; for example, you can view whether a phone has a locally significant certificate or manufacture-installed certificate installed. For additional information on the security menu and icons, refer to the *Cisco IP Phone Administration Guide* and *Cisco IP Phone User Guide* that supports your phone model.

When Unified Communications Manager classifies a call as authenticated or encrypted, an icon is displayed on the phone and indicates the call state. It also determines when Unified Communications Manager classifies the call as authenticated or encrypted.

Set Up Phone Security

The following procedure describes the tasks to configure security for supported phones.

Procedure

Step 1 If you have not already done so, configure the Cisco CTL Client and ensure that the Unified Communications Manager security mode equals Mixed Mode.

Step 2 If the phone does not contain a locally significant certificate (LSC) or manufacture-installed certificate (MIC), install a LSC by using the Certificate Authority Proxy Function (CAPF).

Step 3 Configure phone security profiles.

Step 4 Apply a phone security profile to the phone.

Step 5 After you configure digest credentials, choose the Digest User from the Phone Configuration window.

Step 6 On Cisco Unified IP Phone 7962 or 7942 (SIP only), enter the digest authentication username and password (digest credentials) that you configured in the End User Configuration window.

Note This document does not provide procedures on how to enter the digest authentication credentials on the phone. For information on how to perform this task, see Administration Guide for Cisco Unified Communications Manager that supports your phone model and this version of Unified Communications Manager.

Step 7 Encrypt the phone configuration file, if the phone supports this functionality.

Step 8 To harden the phone, disable phone settings.

Preferred Vendor SIP Phone Security Set Up

Secure Preferred Vendor phones are phone types that are manufactured by third-party vendors but are installed in the Cisco Unified database via a COP file. Unified Communications Manager provides security for a preferred vendor SIP phone. In order to support security, you must enable Security Encryption or Security Authentication for the preferred vendor SIP phone in the COP file. These phone types appear in the drop-down list in the Add a New Phone window. While all preferred vendor phones support Digest Authorization, not all preferred vendor phones support TLS security. Security capabilities is based on the phone model. If the Phone Security Profile includes a “Device Security Mode” field, then it supports TLS security.

If the preferred vendor phone supports TLS security, there are two modes that are possible: per-device certificate and shared certificate. The phone supplier must specify which mode is applicable for the phone as well as instructions on generating or acquiring a certificate for the phone.

Set Up Preferred Vendor SIP Phone Security Profile Per-Device Certificates

To configure the preferred vendor SIP phone security profile with per-device certificates, perform the following procedure:

Procedure

Step 1 Upload the certificate for each phone using the OS Administration Certificate Management interface.

Step 2 In the Cisco Unified Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 3 Configure a new Phone Security Profile for the device type of this phone and in the **Device Security Mode** drop-down list, choose **Encrypted** or **Authenticated**.

Step 4 To configure the new SIP phone in the CCMAdmin interface, choose **Device** > **Phone** > **Add New**.

Step 5 Select Phone type.

Step 6 Fill in the required fields.

Step 7 In the **Device Security Profile** drop-down list, select the profile you just created.

Set Up Preferred Vendor SIP Phone Security Profile Shared Certificates

To configure the preferred vendor SIP phone security profile with shared certificates, perform the following procedure:

Procedure

Step 1 Using instructions from the phone vendor, generate a certificate with a Subject Alternate Name (SAN) string. The SAN must be of type DNS. Make a note of the SAN specified in this step. For example, X509v3 extensions:

- X509v3 Subject Alternative Name
- DNS:AscomGroup01.acme.com

Note The SAN must be of type DNS or security will not be enabled.

Step 2 Upload the shared certificate using the OS Administration Certificate Management interface.

Step 3 In the Cisco Unified Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 4 In the **Name** field, enter the name of the Subject Alt Name (SAN), which is the name on the certificate provided by the preferred vendor, or if there is no SAN enter the Certificate Name.

Note The name of the security profile must match the SAN in the certificate exactly or security will not be enabled.

Step 5 In the **Device Security Mode** drop-down list, choose **Encrypted** or **Authenticated**.

Step 6 In the Transport type drop-down list, choose **TLS**.

Step 7 To configure the new SIP phone in the CCMAdmin interface, choose **Device** > **Phone** > **Add New**.

Step 8 Select Phone type.

Step 9 Fill in the required fields

Step 10 In the **Device Security Profile** drop-down list, select the profile you just created.

Migrate Phones from One Cluster to Another Cluster

Use the following procedure to migrate phones from one cluster to another. For example, from cluster 1 to cluster 2.

Procedure

Step 1 On cluster 2, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Find**.

Step 3 From the list of Certificates, click the ITLRecovery certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 4 From the list of Certificates, click the CallManager certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 5 On cluster 1, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 6 Click **Upload Certificate Chain** to upload the downloaded certificate.

Step 7 From the **Certificate Purpose** drop-down list, choose **Phone-SAST-trust**.

Step 8 For the **Upload File** field, click **Choose File**, browse to the ITLRecovery file that you downloaded in Step 3, and then click **Upload File**.

The uploaded ITLRecovery file appears for the **Phone-SAST-Trust** certificate on **Certificate List** window of cluster 1. If the new ITL file has a ITLRecovery certificate for cluster 2, run the command `show itl`.

Step 9 If the phones in cluster 1 have Locally Significant Certificates (LSC), then the CAPF certificate from cluster 1 has to be uploaded in the CAPF-trust store of cluster 2.

Step 10 (Optional) This step is applicable only if the cluster is in mixed mode. Run the **utils ctl update CTLFile** command on the CLI to regenerate the CTL file on cluster 1.

Note
- Run the `show ctl` CLI command to ensure that the ITLRecovery certificate and CallManager certificate of cluster 2 are included in the CTL file with the role as SAST.
- Ensure that the phones have received the new CTL and ITL files. The updated CTL file has the ITLRecovery certificate of cluster 2.

The phones that you want to migrate from cluster 1 to cluster 2 will now accept the ITLRecovery certificate of cluster 2.

Step 11 Migrate the phone from one cluster to another.

Phone Security Interactions and Restrictions

This section provides the interaction and restriction on Phone Security.

Table 2: Phone Security Interactions and Restrictions

Feature	Interaction and Restriction
Certificate Encryption	Beginning from Unified Communications Manager Release 11.5(1) SU1, all the LSC certificates issued by CAPF service are signed with SHA-256 algorithm. Therefore, Cisco Unified IP Phone 7900 Series, 8900 Series, and 9900 Series supports SHA-256 signed LSC certificates and external SHA2 identity certificates (Tomcat, CallManager, CAPF, TVS, and so on). For any other cryptographic operation that require validation of signature, only SHA-1 is supported. **Note** If you use phone models which are in End of Software Maintenance or End of Life, we strongly recommend using the Unified Communications Manager before 11.5(1)SU1 release.

Phone Security Profiles

Unified Communications Manager, groups the security-related settings for phone type and protocol into security profiles. Hence, you can assign this single security profile to multiple phones. The security-related settings include device security mode, digest authentication, and some of the CAPF settings. Installing Unified Communications Manager provides a set of predefined, non-secure security profiles for auto-registration.

You can apply the configured settings to a phone by choosing the security profile in the **Phone Configuration** window. To enable security features for a phone, you must configure a new security profile for the device type and protocol, and then apply that profile to the phone. Only the security features that the selected device and protocol support are displayed in the **security profile settings** window.

Prerequisites

Consider the following information before you configure the phone security profiles:

- When you configure phones, choose a security profile in the **Phone Configuration** window. If the device does not support security or a secure profile, apply a non-secure profile.
- You cannot delete or change the predefined non-secure profiles.
- You cannot delete a security profile that is currently assigned to a device.
- If you change the settings in a security profile that is already assigned to a phone, the re-configured settings apply to all phones that are assigned that particular profile.
- You can rename security files that are assigned to devices. The phones that are assigned with the earlier profile name and settings assume the new profile name and settings.
- The CAPF settings, the authentication mode and the key size, are displayed in the **Phone Configuration** window. You must configure CAPF settings for certificate operations that involve MICs or LSCs. You can update these fields directly in the **Phone Configuration** window.
- If you update the CAPF settings in the security profile, the settings are also updated in the **Phone Configuration** window.
- If you update the CAPF settings in the Phone Configuration window and a matching profile is found, Unified Communications Manager applies the matching profile to the phone.

- If you update the CAPF settings in the Phone Configuration window, and no matching profiles are found, Unified Communications Manager creates a new profile and applies that profile to the phone.
- If you have configured the device security mode earlier to an upgrade, Unified Communications Manager creates a profile that is based on that model and protocol and applies the profile to the device.
- We recommend that you use MICs for LSC installation only. Cisco support LSCs to authenticate the TLS connection with Unified Communications Manager. Since MIC root certificates can be compromised, users who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.
- We recommend that you upgrade Cisco IP Phones to use LSCs for TLS connections and remove the MIC root certificates from the CallManager trust store to avoid compatibility issues.

Phone Security Profile Settings

The following table describes the settings for the security profile for the phone that is running SCCP.

Only settings that the selected phone type and protocol support display.

Table 3: Security Profile for Phone That Is Running SCCP

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **Device Security Profile** drop-down list in the **Phone Configuration window** for the phone type and protocol. **Tip** Include the device model and protocol in the security profile name to find the correct profile while searching for a profile or updating a profile.
Description	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Setting	Description
Device Security Mode	

Setting	Description
	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image, file, and device authentication exist for the phone. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and signalling encryption for the trunk. The following are the supported ciphers: **TLS Ciphers** This parameter defines the ciphers that are supported by the Unified Communications Manager for establishing SIP TLS and inbound CTI Manager TLS connections. Strongest- AES-256 SHA-384 only: RSA Preferred • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Strongest - AEAD AES-256 GCM cipher only'. With this option chosen, the phones will not register on authenticated mode. Strongest- AES-256 SHA-384 only: ECDSA Preferred • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` Medium- AES-256 AES-128 only: RSA Preferred **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Strongest - AEAD AES-256 GCM cipher only'. With this option chosen, the phones will not register on authenticated mode. • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256` • `TLS_ECDHE_ECDSA with AES128_GCM_SHA256` **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Medium - AEAD AES-256,AES-128 GCM ciphers only'. With this option chosen, the phones will not register on authenticated mode. Medium- AES-256 AES-128 only: ECDSA Preferred

Setting	Description
	• TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Medium - AEAD AES-256,AES-128 GCM ciphers only'. With this option chosen, the phones will not register on authenticated mode. All Ciphers, RSA Preferred: • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 All Ciphers, ECDSA Preferred: • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 **Note** If the trunks are configured with Device Security Profile option selected as Authenticated, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as Encrypted. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
TFTP Encrypted Config	When this check box is checked, Unified Communications Manager encrypts a phone downloads from the TFTP server.

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • **By Authentication String**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate without the user intervention. This option provides no security. We recommend that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If an LSC exists in the phone, authentication occurs through the LSC, regardless whether a MIC exists in the phone. If a MIC and an LSC exist in the phone, authentication occurs through the LSC. If an LSC does not exist in the phone, but a MIC exists, authentication occurs through the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF although a MIC and an LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate if an LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs through the MIC, regardless whether an LSC exists in the phone. If an LSC exists in the phone, but a MIC does not exist, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.

Setting	Description
Key Order	This field specifies the sequence of the key for CAPF. Select one of the following values from the drop-down list: • **RSA Only** • **EC Only** • **EC Preferred, RSA Backup** **Note** When you add a phone, that is based on the value in **Key Order**, **RSA Key Size**, and **EC Key Size** fields, the device security profile is associated with the phone. If you select the **EC Only** value, with the **EC Key Size** value of 256 bits, then the device security profile appends with **EC-256** value.
RSA Key Size (Bits)	From the drop-down list box, choose one of the values—**512**, **1024**, **2048, 3072**, or **4096**. **Note** Some phone models may fail to register if the RSA **key length** that is selected for the CallManager **Certificate Purpose** is greater than 2048. From the *Unified CM Phone Feature List Report* on the *Cisco Unified Reporting Tool (CURT)*, you can check the 3072/4096 RSA key size support feature for the list of supported phone models.
EC Key Size (Bits)	From the drop-down list, choose one of the values—**256**, **384**, or **521**.

The following table describes the settings for the security profile for the phone that is running SIP.

Table 4: Security Profile for Phone That Is Running SIP

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **Device Security Profile** drop-down list in the **Phone Configuration** window for the phone type and protocol. **Tip** Include the device model and protocol in the security profile name to help you find the correct profile when you are searching for or updating a profile.
Description	Enter a description for the security profile.
Nonce Validity Time	Enter the number of minutes (in seconds) that the nonce value is valid. The default value equals 600 (10 minutes). When the time expires, Unified Communications Manager generates a new value. **Note** A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.

Setting	Description
Device Security Mode	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image, file, and device authentication exist for the phone. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and encryption for the phone. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all phone calls on all SRTP-capable hops. **Note** If the trunks are configured with Device Security Profile option selected as Authenticated, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as Encrypted. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
Transport Type	When Device Security Mode is **Non Secure**, choose one of the following options from the drop-down list (some options may not display): • **TCP**—Choose the Transmission Control Protocol to ensure that packets get received in the same order as the order in which they are sent. This protocol ensures that no packets get dropped, but the protocol does not provide any security. • **UDP**—Choose the User Datagram Protocol to ensure that packets are received quickly. This protocol, which can drop packets, does not ensure that packets are received in the order in which they are sent. This protocol does not provide any security. • **TCP + UDP**—Choose this option if you want to use a combination of TCP and UDP. This option does not provide any security. When Device Security Mode is **Authenticated** or **Encrypted**, TLS specifies the Transport Type. TLS provides signaling integrity, device authentication, and signaling encryption (encrypted mode only) for SIP phones. If Device Security Mode cannot be configured in the profile, the transport type specifies UDP.

Setting	Description
Enable Digest Authentication	If you check this check box, Unified Communications Manager challenges all SIP requests from the phone. Digest authentication does not provide a device authentication, integrity, or confidentiality. Choose a security mode of authenticated or encrypted to use these features.
TFTP Encrypted Config	When this check box is checked, Unified Communications Manager encrypts the phone downloads from the TFTP server. This option exists for Cisco phones only. **Tip** We recommend that you enable this option and configure a symmetric key to secure digest credentials and administrative passwords.
Enable OAuth Authentication	This check box is available, when you choose **Encrypted** from the **Device Security Profile** drop-down list. When this check box is checked, Unified Communications Manager allows the device that is associated with the phone security profile to register on the SIP OAuth port. By default, this check box is unchecked. You can enable the SIP OAuth when: • Transport type is TLS. • Device security mode is encrypted. • Digest authentication is disabled. • Encrypted configuration is disabled. **Note** From Unified Communications Manager Release 12.5, Jabber devices support SIP OAuth authentication.
Exclude Digest Credentials in Configuration File	When this check box is checked, Unified Communications Manager omits digest credentials in the phone downloads from the TFTP server. This option exists for Cisco IP Phones, 7942, and 7962 (SIP only).

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. This option exists for Cisco phones only. From the drop-down list, choose one of the following options: • **By Authentication String**—Installs or upgrades or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**—Installs or upgrades or troubleshoots a locally significant certificate without the user intervention. This option provides no security; we recommend that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**—Installs or upgrades or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If an LSC exists in the phone, authentication occurs through the LSC, regardless whether a MIC exists in the phone. If an LSC does not exist in the phone, but a MIC does exist, authentication occurs through the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF although a MIC and an LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs or upgrades or troubleshoots a locally significant certificate if an LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs through the MIC, regardless whether an LSC exists in the phone. If an LSC exists in the phone, but a MIC does not exist, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. The default setting equals 1024. The other option for key size is 512. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.
SIP Phone Port	This setting applies to phones that are running SIP that uses UDP transport. Enter the port number for Cisco Unified IP Phone (SIP only) that use UDP to listen for SIP messages from Unified Communications Manager. The default setting equals 5060. Phones that use TCP or TLS ignore this setting.

Phone Security Configuration Task Flow

Perform the following tasks to configure phone security:

Procedure

	Command or Action	Purpose
Step 1	(Optional) Find Phone Security Profile, on page 22	Search for the phone security profile to secure a phone.
Step 2	Set Up Phone Security Profile	Set up the phone security profile to secure a phone.
Step 3	Apply Security Profiles to Phone	Apply the phone security profile to secure a phone.
Step 4	Synchronize Phone Security Profile with Phones	Synchronize all the phone security profiles with selected phones.
Step 5	(Optional) Delete Phone Security Profile	Delete all the phone security profiles associated to a phone.
Step 6	Find Phones with Phone Security Profiles	Find all phones associated with phone security profiles.
Step 7	SIP Trunk Security Profile Interactions and Restrictions	SIP trunk security profile interations and restrictions

Find Phone Security Profile

To find a phone security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 22.

To filter or search records

a) From the first drop-down list, choose a search parameter.
b) From the second drop-down list, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click **Clear Filter** to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the record that you choose.

Set Up Phone Security Profile

To setup a phone security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Security Profile > Phone Security Profile**.

Step 2 Perform one of the following tasks:

a) To add a new profile, click **Add New**.
b) To copy an existing security profile, locate the appropriate profile, click **Copy** next to the security profile that you want to copy, and continue.
c) To update an existing profile, locate the appropriate security profile and continue.

When you click **Add New**, the configuration window displays with the default settings for each field. When you click **Copy**, the configuration window displays the copied settings.

Step 3 Enter appropriate settings for phones that are running SCCP or SIP.

Step 4 Click **Save**.

Apply Security Profiles to Phone

Before you apply a security profile that uses certificates for authentication of the phone, make sure that the particular phone contains a Locally Significant Certificate (LSC) or Manufacture-Installed Certificate (MIC).

To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. However, if the phone does not contain a certificate, perform the following tasks:

- In the **Phone Configuration** window, apply a non-secure profile.
- In the **Phone Configuration** window, install a certificate by configuring the CAPF settings.
- In the **Phone Configuration** window, apply a device security profile that is configured for authentication or encryption.

To apply a phone security profile to a device, perform the following procedure:

Procedure

Step 1 Go to the **Protocol Specific Information** section in the **Phone Configuration** window.

Step 2 From the **Device Security Profile** drop-down list, choose the security profile that applies to the device. The phone security profile that is configured only for the phone type and the protocol is displayed.

Step 3 Click **Save**.

Step 4 To apply the changes to the applicable phone, click **Apply Config**.

Note To delete security profiles, check the check boxes next to the appropriate security profile in the **Find and List** window, and click **Delete Selected**.

Synchronize Phone Security Profile with Phones

To synchronize phone security profile with phones, perform the following procedure:

Procedure

Step 1 From Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

Step 2 Choose the search criteria to use and click **Find**.
The window displays a list of phone security profiles that match the search criteria.

Step 3 Click the phone security profile to which you want to synchronize the applicable phones.

Step 4 Make any additional configuration changes.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.
The **Apply Configuration Information** dialog box appears.

Step 7 Click **OK**.

Delete Phone Security Profile

Before you can delete a security profile from Unified Communications Manager, you must apply a different profile to the devices or delete all devices that use the profile.

To find out which devices use the profile, perform Step 1:

Procedure

Step 1 In the **Security Profile Configuration** window, choose **Dependency Records** from the **Related Links** drop-down list and click **Go**.

If the dependency records feature is not enabled for the system, go to **System** > **Enterprise Parameters Configuration** and change the Enable Dependency Records setting to **True**. A message displays information about high CPU consumption that relates to the dependency records feature. Save your change to activate dependency records. For more information about dependency records, see System Configuration Guide for Cisco Unified Communications Manager

This section describes how to delete a phone security profile from the Unified Communications Manager database.

Step 2 Find the security profile to delete.

Step 3 To delete multiple security profiles, check the check boxes next to the appropriate check box in the **Find and List** window; then, click **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 To delete a single security profile, perform one of the following tasks:

a) In the **Find and List** window, check the check box next to the appropriate security profile; then, click **Delete Selected**.

Step 5 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Find Phones with Phone Security Profiles

To find the phones that use a specific security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 From the first drop-down list, choose the search parameter **Security Profile**.

a) From the drop-down list, choose a search pattern.
b) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click +. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click – to remove the last added criterion or click **Clear Filter** to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the **Rows per Page** drop-down list.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the record that you choose.

SIP Trunk Security Profile Interactions and Restrictions

The following table contains feature interactions and restrictions for SIP Trunk Security Profiles.

Table 5: SIP Trunk Security Profile Interactions and Restrictions

Feature	Interactions and Restrictions
90-day Evaluation License	You cannot deploy a secure SIP trunk while running with a 90-day evaluation period. To deploy a secure SIP trunk, your system must have registered to a Smart Software Manager account with the **Allow export-controlled functionality** product registration token selected.

Digest Authentication for SIP Phones Overview

Digest authentication allows Unified Communications Manager to challenge request messages for phones that are running SIP. This includes all request messages with the exception of keepalives. Unified Communications Manager authenticates through digest credentials the end user, as configured in the **End User Configuration** window, to validate the credentials that the phone offers.

If the phone supports Extension Mobility, Unified Communications Manager uses the digest credentials for the Extension Mobility end user, as configured in the **End User Configuration** window, when the Extension Mobility user logs in.

Digest Authentication for SIP Phones Prerequisite

If you enable digest authentication for a device, the device requires a unique digest user ID and password to register. You must configure SIP digest credentials in the Unified Communications Manager database for a phone user or an application user.

Make sure that you do the following:

- For applications, specify digest credentials in the Application User Configuration window.

- For phones that are running SIP, specify the digest authentication credentials in the End User Configuration window.

  To associate the credentials with the phone after you configure the user, choose a Digest User, in the Phone Configuration window. After you reset the phone, the credentials exist in the phone configuration file that the TFTP server offers to the phone.

- For challenges received on SIP trunks, configure a SIP realm, which specifies the realm username (device or application user) and digest credentials.

Note Be aware that the cluster security mode has no effect on digest authentication.

Digest Authentication for SIP Phones Configuration Task Flow

Complete these tasks to configure Digest Authentication for SIP phones.

Procedure

	Command or Action	Purpose
Step 1	Assign Digest Credentials to Phone User	Assign the digest credentials to the end user whom owns the phone.
Step 2	Enable Digest Authentication in Phone Security Profile	Enable digest authentication in the Phone Security Profile that associates to the phone.
Step 3	Assign Digest Authentication to the Phone	In Phone Configuration, assign the user as a digest user. Make sure the digest authentication-enabled security profile is assigned.
Step 4	End User Digest Credential Settings	Set the end user digest credentials.
Step 5	Configure SIP Station Realm, on page 27	Assign the string for the Realm field that Unified CM uses to challenge a SIP request due to a 401 Unauthorized message.

Assign Digest Credentials to Phone User

Use this procedure to assign digest credentials to the end user who owns the phone. Phones use the credentials to authenticate.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

Step 2 Click **Find** and choose the end user who owns the phone.

Step 3 Enter the credentials in the following fields:

- Digest Credentials
- Confirm Digest Credentials

Step 4 Click **Save**.

Enable Digest Authentication in Phone Security Profile

Use this procedure to enable digest authentication for a phone through the Phone Security Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.
Step 2 Click **Find** and choose the phone security profile that is associated to the phone.
Step 3 Check the **Enable Digest Authentication** check box.
Step 4 Click **Save**.

Assign Digest Authentication to the Phone

Use this procedure to associate the digest user and digest authentication-enabled security profile to the phone.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device > Phone**.
Step 2 Click **Find** and choose the phone for which you want to assign digest authentication.
Step 3 From the **Digest User** drop-down list, assign the end user for whom you assigned digest credentials.
Step 4 Make sure that the phone security profile for which you enabled digest authentication is assigned through the **Device Security Profile** drop-down list.
Step 5 Click **Save**.
Step 6 Click **Reset**.

After you associate the end user with the phone, save the configuration and reset the phone.

Configure SIP Station Realm

Assign the string that Cisco Unified Communications Manager uses in the Realm field when challenging a SIP phone in the response to a 401 Unauthorized message. This applies when the phone is configured for digest authentication.

Note The default string for this service parameter is ccmsipline.

Procedure

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

Step 2 From the **Server** drop-down list, choose a node where you activated the CiscoCallManager service.

Step 3 From the **Service** drop-down list, choose the CiscoCallManager service. Verify that the word "Active" displays next to the service name.

Step 4 Update the **SIP Realm Station** parameter, as described in the help. To display help for the parameters, click the question mark or the parameter name link.

Step 5 Click **Save**.

End User Digest Credential Settings

To view the digest credentials details, perform the following procedure:

From Cisco Unified Communications Manager Administration, choose **User Management > End User** and click the User ID and the **End User Configuration** window appears. The digest credentials are available in the **User Information** pane of the **End User Configuration** window.

Table 6: Digest Credentials

Setting	Description
Digest Credentials	Enter a string of alphanumeric characters.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.