



Configuring Encrypted Phone Configuration Files

After you configure security-related settings, the phone configuration file contains sensitive configuration information, such as digest passwords and phone administrator passwords. To ensure privacy of the configuration file, you must configure the configuration files for encryption.

This chapter contains information on the following topics:

- [Understanding Encryption of the Phone Configuration File, page 7-1](#)
- [Supported Phone Models, page 7-3](#)
- [Encryption Configuration File Configuration Checklist, page 7-4](#)
- [Enabling Phone Configuration File Encryption Enterprise Parameters, page 7-4](#)
- [Configuring Manual Key Distribution, page 7-5](#)
- [Manual Key Distribution Configuration Settings, page 7-6](#)
- [Entering the Symmetric Key on the Phone, page 7-6](#)
- [Using Symmetric Key Encryption with Phone Public Key, page 7-6](#)
- [Verifying That the Phone Configuration File Is Encrypted, page 7-7](#)
- [Disabling Encryption for the Phone Configuration Files, page 7-7](#)
- [Where to Find More Information, page 7-8](#)

Understanding Encryption of the Phone Configuration File

To encrypt the phone configuration file, you must enable an enterprise parameter in Cisco Unified CallManager Administration and perform additional tasks in Cisco Unified CallManager Administration. After you enable the parameter and restart required services in Cisco Unified CallManager Serviceability, the TFTP server deletes all clear text configuration files and then generates encrypted versions of the configuration files. If the phone supports encrypted phone configuration files and if you performed the necessary tasks for phone configuration file encryption, the phone requests an encrypted version of the configuration file.



Warning

If digest authentication is True for the SIP phone when the TFTP encrypted configuration setting is False, digest credentials may get sent in the clear. See [“Disabling Encryption for the Phone Configuration Files”](#) section on page 7-7 for more information.

Some phone models do not support encrypted phone configuration files, as described in the “[Supported Phone Models](#)” section on page 7-3. The phone model determines the method that the system uses to encrypt the configuration file; supported methods rely on Cisco Unified CallManager functionality and a firmware load that supports encrypted configuration files. If you downgrade the phone firmware load to a version that does not support encrypted configuration files, the TFTP server offers an unencrypted configuration file that provides minimal configuration settings, and the phone may not perform as expected.

To ensure that you maintain the privacy of the key information, Cisco strongly recommends that you perform the tasks that are associated with encrypted phone configuration files in a secure environment.

Cisco Unified CallManager supports the following methods:

- [Manual Key Distribution](#), page 7-2
- [Symmetric Key Encryption with Phone Public Key](#), page 7-3

The information in the “[Manual Key Distribution](#)” and “[Symmetric Key Encryption with Phone Public Key](#)” sections assumes that you configured the cluster for Secure Mode and that you enabled the TFTP Encrypted Configuration parameter in Cisco Unified CallManager Administration.

Manual Key Distribution



Tip

For a list of phone models that support this method, see the “[Supported Phone Models](#)” section on page 7-3.

With manual key distribution, a 128- or 256-bit symmetric key, which gets entered into the Cisco Unified CallManager database, encrypts the phone configuration file after the phone resets. To determine the key size for your phone model, see the “[Supported Phone Models](#)” section on page 7-3.

To update the configuration file, the administrator can either manually enter the key into Cisco Unified CallManager Administration or prompt Cisco Unified CallManager Administration to generate the key. After the key exists in the database, the administrator or user must enter the key into the phone by accessing the user interface on the phone; the phone stores the key in flash as soon as you press the **Accept** softkey. Once the key is entered, the phone requests an encrypted configuration file after it is reset. After the required tasks occur, the symmetric key uses RC4 or AES 128 encryption algorithms to encrypt the configuration file. To determine which phones use the RC4 or AES 128 encryption algorithms, see the “[Supported Phone Models](#)” section on page 7-3.

When the phone contains the symmetric key, the phone requests the encrypted configuration file. The phone downloads the encrypted configuration file, which the TFTP server signs.

The Cisco Unified SIP IP Phone models 7960 and 7940 do not validate the signer of the configuration file. The phone decrypts the file contents by using the symmetric key that is stored in flash. If decryption fails, the configuration file does not get applied to the phone.



Tip

If the TFTP Encrypted Configuration enterprise parameter gets disabled, administrators must remove the symmetric key from the phone GUI so that the phone requests an unencrypted configuration file the next time that it is reset.

Symmetric Key Encryption with Phone Public Key

**Tip**

For a list of phone models that support this method, see the [“Supported Phone Models”](#) section on page 7-3.

If the phone contains a manufacturing-installed certificate (MIC) or a locally significant certificate (LSC), the phone contains a public and private key pair. If you are using this method for the first time, the phone compares the MD5 hash of the phone certificate in the configuration file to the MD5 hash of the LSC or MIC. If the phone does not identify a problem, the phone requests an encrypted configuration file from the TFTP server after the phone resets. If the phone identifies a problem, for example, the hash does not match, the phone does not contain a certificate, or the MD5 value is blank, the phone attempts to initiate a session with CAPF unless the CAPF authentication mode equals By Authentication String (in which case, you must manually enter the string). CAPF extracts the phone public key from the LSC or MIC, generates a MD5 hash, and stores the values for the public key and certificate hash in the Cisco Unified CallManager database. After the public key gets stored in the database, the phone resets and requests a new configuration file.

After the public key exists in the database and the phone resets, the symmetric key encryption process begins once the database notifies TFTP that the public key exists for the phone. The TFTP server generates a 128-bit symmetric key, which encrypts the configuration file with the Advanced Encryption Standard (AES) 128 encryption algorithm. Then, the phone public key encrypts the symmetric key, which includes in the signed envelope header of the configuration file. The phone validates the file signing, and, if the signature is valid, the phone uses the private key from the LSC or MIC to decrypt the encrypted symmetric key. The symmetric key then decrypts the file contents.

Every time that you update the configuration file, the TFTP server automatically generates a new key to encrypt the file.

**Tip**

For phones that support symmetric key encryption using phone public key, the phone uses the encryption configuration flag in the configuration file to determine whether to request an encrypted or unencrypted file. If the TFTP Encrypted Configuration enterprise parameter is disabled, and Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 request an encrypted file (.enc.sgn file), Cisco Unified CallManager sends a ‘file not found error’ to the phone. The phone then requests an unencrypted, signed file (.sgn file).

If the TFTP Encrypted Configuration enterprise parameter is enabled but the phone requests an unencrypted configuration file for some reason, the TFTP server offers an unencrypted file that contain minimal configuration settings.

Supported Phone Models

You can encrypt the phone configuration file for the following phone models:

- Cisco Unified SIP IP Phone 7905 or 7912—Supports manual key distribution
The symmetric key uses the RC4 encryption algorithm and a key size of 256 bits. These SIP phone models do not support file signing.
- Cisco Unified SIP IP Phone 7940 or 7960—Supports manual key distribution

The symmetric key uses the Advanced Encryption Standard (AES) 128 encryption algorithm and a key size of 128 bits. These SIP phones receive signed, encrypted configuration files, but ignore the signing information

- Cisco Unified SIP IP Phone 7970 or 7971; Cisco Unified SIP IP Phone 7941 or 7961; Cisco Unified SIP IP Phone 7911; Cisco Unified IP Phone 7970 or 7971; Cisco Unified IP Phone 7941 or 7961; Cisco Unified IP Phone 7911—Supports symmetric key encryption with phone public key

The symmetric key uses the AES 128 encryption algorithm and a key size of 128 bits. These phones support file signing.

Encryption Configuration File Configuration Checklist

To encrypt the phone configuration file, you must perform the tasks in [Table 7-1](#):

Table 7-1 Encryption Configuration File Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Verify that the Cluster Security Mode is configured for Secure Mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	In Cisco Unified CallManager Administration, enable the TFTP Encrypted Configuration enterprise parameter.	Enabling Phone Configuration File Encryption Enterprise Parameters, page 7-4
Step 3	Determine which phones support manual key distribution and which phones support symmetric key encryption with phone public key.	Supported Phone Models, page 7-3
Step 4	If your phone supports manual key distribution, perform the manual key distribution tasks in Cisco Unified CallManager Administration.	<ul style="list-style-type: none"> • Configuring Manual Key Distribution, page 7-5 • Manual Key Distribution Configuration Settings, page 7-6
Step 5	If your phone supports manual key distribution, enter the symmetric key on the phone; reset the phone.	Entering the Symmetric Key on the Phone, page 7-6
Step 6	If your phone supports the method, symmetric key encryption with phone public key, verify that a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone.	<ul style="list-style-type: none"> • Using Symmetric Key Encryption with Phone Public Key, page 7-6 • Understanding Encryption of the Phone Configuration File, page 7-1 • Using the Certificate Authority Proxy Function, page 6-1

Enabling Phone Configuration File Encryption Enterprise Parameters

Before you can encrypt phone configuration files, you must enable the TFTP Encrypted Configuration enterprise parameter in Cisco Unified CallManager Administration. The TFTP server queries the database when it builds the configuration file. If the enterprise parameter is enabled, the TFTP server builds an encrypted configuration file.

To access the enterprise parameter in Cisco Unified CallManager Administration, choose **System > Enterprise Parameters**.

For information on the enterprise parameter, including information on the default value, click the TFTP Encrypted Configuration link that displays in the Enterprise Parameters Configuration window.

Configuring Manual Key Distribution

To determine whether your phone supports manual key distribution, see the [“Supported Phone Models” section on page 7-3](#).

To configure manual key distribution, perform the following procedure, which assumes that the phone exists in the Cisco Unified CallManager database, that a compatible firmware load exists on the TFTP server, and that you enabled the TFTP Encrypted Configuration enterprise parameter in Cisco Unified CallManager Administration:

Procedure

- Step 1** Find the phone, as described in the *Cisco Unified CallManager Administration Guide*.
 - Step 2** After the Phone Configuration window displays, configure the manual key distribution settings that are described in [Table 7-2](#). Once configured, the key should not be changed.
 - Step 3** Click **Save**.
 - Step 4** Enter the symmetric key on the phone and then reset the phone. For information on how to perform these tasks, refer to the phone administration guide that supports your phone model.
-

Additional Information

See the [“Related Topics” section on page 7-8](#).

Manual Key Distribution Configuration Settings

Table 7-2 describes the manual distribution configuration settings in the Phone Configuration window. For related procedures, see the “[Related Topics](#)” section on page 7-8.

Table 7-2 Manual Key Distribution Configuration Settings

Setting	Description
Symmetric Key	<p>Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and uppercase /lowercase characters, A-F (or a-f).</p> <p>Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified CallManager rejects the value. Cisco Unified CallManager supports the following key sizes:</p> <ul style="list-style-type: none"> • Cisco Unified IP Phone models 7905 and 7912 (SIP Protocol only)—256 bits • Cisco Unified IP Phone models 7940 and 7960 (SIP Protocol only)—128 bits <p>Once configured, the key should not be changed.</p>
Generate String	<p>If you want Cisco Unified CallManager Administration to generate a hexadecimal string for you, click the Generate String button.</p> <p>Once generated, the key should not be changed</p>
Revert to Database Value	<p>If you want to restore the value that exists in the database, click this button.</p>

Entering the Symmetric Key on the Phone

For information on how to enter the symmetric key on the phone after you configure manual key distribution in Cisco Unified CallManager Administration, refer to the Cisco Unified IP Phone administration guide that supports your phone model and protocol.

Using Symmetric Key Encryption with Phone Public Key

To determine whether your phone supports the method, symmetric key encryption with phone public key, see the “[Supported Phone Models](#)” section on page 7-3. To use this method, perform the following tasks, which assume that the phone exists in the Cisco Unified CallManager database and that you enabled the TFTP Encrypted Configuration enterprise parameter in Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Verify that a manufacture-installed certificate (MIC) or a locally significant certificate (LSC) exists in the phone. If a certificate does not exist, install an LSC by using the CAPF functionality in the Phone Configuration window. For information on how to install a LSC, see the “[Using the Certificate Authority Proxy Function](#)” section on page 6-1.
- Step 2** After you configure the CAPF settings, click **Save**.

Step 3 In the Phone Configuration window, click **Reset**.

Additional Information

See the “[Related Topics](#)” section on page 7-8.

Verifying That the Phone Configuration File Is Encrypted

When the phone configuration file is encrypted, it uses the following format:

- Cisco Unified IP Phone models 7905 and 7912 (SIP protocol only)—LD <MAC>.x
- Cisco Unified IP Phone models 7940 and 7960 (SIP protocol only)—SIP<MAC>.cnf.enc.sgn
- Cisco Unified IP Phone models 7970 and 7971 (SIP protocol only)—SIP<MAC>.cnf.xml.enc.sgn
- Cisco Unified IP Phone models 7970 and 7971 (SCCP protocol only)—SEP<MAC>.cnf.xml.enc.sgn

Disabling Encryption for the Phone Configuration Files

To disable encryption for the phone configuration files, you must update the TFTP Encrypted Configuration enterprise parameter in Cisco Unified CallManager Administration.



Warning

If digest authentication is True for the SIP phone when the TFTP encrypted configuration setting is False, digest credentials may get sent in the clear.

After you update the enterprise parameter, the keys for the phone remain in the Cisco Unified CallManager database.

If Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 request an encrypted file (.enc.sgn file) when the encrypted configuration setting gets updated to false, the phone requests a unencrypted, signed file (.sgn file).

If Cisco Unified IP SIP Phone models 7940/7960/7905/7912 request an encrypted file when the encryption configuration setting gets updated to false, administrators must remove the symmetric key from the phone GUI so that the phone requests an unencrypted configuration file the next time that it is reset.



Tip

For Cisco Unified IP SIP Phone models 7940 and 7960, enter a 32-byte 0 as the key value for the symmetric key at the phone GUI to disable encryption. For Cisco Unified IP SIP Phone models 7905 and 7912, delete the symmetric key at the phone GUI to disable encryption. For information on how to perform these tasks, refer to the phone administration guide that supports your phone model.

Where to Find More Information

Related Topics

- [Understanding Encryption of the Phone Configuration File, page 7-1](#)
- [Supported Phone Models, page 7-3](#)
- [Encryption Configuration File Configuration Checklist, page 7-4](#)
- [Enabling Phone Configuration File Encryption Enterprise Parameters, page 7-4](#)
- [Configuring Manual Key Distribution, page 7-5](#)
- [Manual Key Distribution Configuration Settings, page 7-6](#)
- [Entering the Symmetric Key on the Phone, page 7-6](#)
- [Using Symmetric Key Encryption with Phone Public Key, page 7-6](#)
- [Verifying That the Phone Configuration File Is Encrypted, page 7-7](#)
- [Disabling Encryption for the Phone Configuration Files, page 7-7](#)
- [Using the Certificate Authority Proxy Function, page 6-1](#)

Related Cisco documentation

- *Cisco Unified CallManager Bulk Administration Guide*
- Cisco Unified IP Phone administration guide for the phone model and protocol