Encrypted Phone Configuration File Setup

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

- TFTP Encrypted Configuration Files Overview, on page 1
- Phone Models That Support Encryption, on page 3
- TFTP Encrypted Configuration Files Tips, on page 4
- Encryption for Phone Configuration File Task Flow, on page 5
- Disable TFTP Encrypted Configuration Files, on page 10
- Exclude Digest Credentials From Phone Configuration File Download, on page 11

TFTP Encrypted Configuration Files Overview

TFTP configuration protects your data during device registration by encrypting the configuration file that the phone downloads from the TFTP server during the registration process. This file contains confidential information such as usernames, passwords, IP addresses, port details, phone SSH credentials, and so on. If this feature is not configured, the configuration file is sent in cleartext. Deploying this feature ensures that an attacker cannot intercept this information during the registration process. This information is unencrypted and sent in cleartext. Hence, we recommend that you encrypt the TFTP configuration file in order to protect your data.

Warning If you have enabled the digest authentication option for SIP phones and disabled the TFTP encrypted configuration option, the digest credentials are sent in the cleartext.

After TFTP configuration, the TFTP server:

- Deletes all the cleartext configuration files on disk
- Generates encrypted versions of the configuration files

If the phone supports encrypted phone configuration files and you have performed the tasks for phone configuration file encryption, the phone requests an encrypted version of the configuration file.

Some phones don't support encrypted phone configuration files. The phone model and protocol determine the method that the system uses to encrypt the configuration file. Supported methods rely on Unified

Communications Manager functionality and a firmware load that supports encrypted configuration files. If you downgrade the phone firmware load to a version that doesn't 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.

Encryption Key Distribution

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

Unified Communications Manager supports the following methods:

- Manual key distribution
- Symmetric key encryption with a phone public key

The setup information provided for manual key distribution and symmetric key encryption with a phone public key assume that you have configured mixed mode and enabled the **TFTP Encrypted Config** option in Cisco Unified CM Administration.

Manual Key Distribution

With manual key distribution, a 128- or 256-bit symmetric key, which is stored in the Unified Communications Manager database, encrypts the phone configuration file after the phone resets. To determine the key size for your phone model.

To encrypt the configuration file, the administrator can either manually enter the key into or prompt Unified Communications Manager to generate the key in the **Phone Configuration** window. 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. After 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 Phone Models That Support Encryption, on page 3.

When the phone contains the symmetric key, the phone always requests the encrypted configuration file.Unified Communications Manager downloads the encrypted configuration file to the phone, which the TFTP server signs. Not all phone types 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 Config setting gets disabled, administrators must remove the symmetric key from the phone GUI, so the phone requests an unencrypted configuration file the next time that it is reset.

Symmetric Key Encryption with Phone Public Key

If the phone contains a manufacturing-installed certificate (MIC) or a locally significant certificate (LSC), the phone contains a public and private key pair, which are used for PKI encryption.

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). The Certificate Authority Proxy Function (CAPF) authenticates Cisco IP Phones to Unified Communications Manager and issues phone certificates (LSCs). 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 Unified Communications Manager 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 after 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 it 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 this encryption method, 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 Config setting is disabled, and Cisco IP Phones that support this encryption method request an encrypted file (.enc.sgn file), Unified Communications Manager sends a 'file not found error' to the phone. The phone then requests an unencrypted, signed file (.sgn file).

If the TFTP Encrypted Config setting is enabled but the phone requests an unencrypted configuration file for some reason, the TFTP server offers an unencrypted file that contains minimal configuration settings. After the phone receives the minimum configuration, the phone can detect error conditions, such as key mismatch, and may start a session with CAPF to synchronize the phone public key with the Unified Communications Manager database. If the error condition is resolved, the phone requests an encrypted configuration file the next time that it resets.

Phone Models That Support Encryption

You can encrypt the phone configuration file for the following Cisco Unified IP Phones:

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 7800 or 6921	Manual key distribution—Encryption algorithm: RC4Key size: 256 bits File signing support: No
Cisco Unified IP Phone 7942 or 7962 (SIP only)	Manual key distribution—Encryption algorithm: Advanced Encryption Standard (AES)128Key size: 128 bits File signing support: These phones that are running SIP receive signed, encrypted configuration files but ignore the signing information.

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, and 6961 Cisco Unified IP Phone 7970G, 7971G, 7975G; Cisco Unified IP Phone 7961G, 7962G, or 7965G;Cisco Unified IP Phone 7941G, 7942G, or 7945G;Cisco Unified IP Phone 7911G; Cisco Unified IP Phone 7906G Cisco Unified IP Phone 7971G-GE, 7961G-GE, 7941G-GE Cisco Unified IP Phone 7931G, 7921G, (SCCP only) Cisco Unified Wireless IP Phone 7925G, 7925G-EX, 7926G Cisco Unified IP Phone 8941 and 8945 Cisco Unified IP Phone 8961, 9951, and 9971 Cisco IP Phone 7811, 7821, 7841, 7861 Cisco IP Conference Phone 7832 Cisco IP Phone 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR Cisco Unified Conference Phone 8831 Cisco Conference Phone 8832 Cisco Wireless IP Phone 8821	Symmetric key encryption with phone public key (PKI encryption)—Encryption algorithm: AES128Key size: 128 bits File signing support: Yes **Note** Cisco Unified IP Phones 6901 and 6911 do not request for the ITL file as they do not support security by default. Therefore, the Unified Communications Manager cluster should be set to secure (Mixed) mode for the Cisco Unified IP Phones 6901 and 6911 to get the Cisco CTL file containing Cisco Certificate Authority Proxy Function (CAPF) details for the encrypted configuration file to work on the Cisco Unified IP Phones (6901 and 6911).

TFTP Encrypted Configuration Files Tips

We recommend that you enable the TFTP Encrypted Configuration file to secure confidential data in phone downloads. For phones that don't have PKI capabilities, you must also configure a symmetric key in Unified Communications Manager Administration and in the phone. If the symmetric key is missing from either the phone or Unified Communications Manager or if a mismatch occurs when the TFTP Encrypted Configuration file is set, the phone can't register.

Consider the following information when you configure encrypted configuration files in Unified Communications Manager:

- Only phones that support encrypted configuration files display the **TFTP Encrypted Config** check box in the **Phone Security Profile Configuration** page. You can't configure encrypted configuration files for Cisco Unified IP Phones 7800, 7942, and 7962 (SCCP only) because these phones don't receive confidential data in the configuration file download.
- By default, the **TFTP Encrypted Config** check box is unchecked. If you apply this default setting, the non secure profile to the phone, the digest credentials, and secured passwords are sent in the cleartext.
- For Cisco Unified IP Phones that use Public Key Encryption, Unified Communications Manager does not require you to set the Device Security Mode to Authenticated or Encrypted to enable encrypted

configuration files. Unified Communications Manager uses the CAPF process for downloading its Public key during registration.

- You may choose to download the unencrypted configuration files to the phones if you know that your environment is secure or to avoid manually configuring symmetric keys for phones that are not PKI-enabled. However, we don't recommend that you use this method.
- For Cisco Unified IP Phones 7800, 7942, and 7962 (SIP only), Unified Communications Manager provides a method of sending digest credentials to the phone that is easier, but less secure, than using an encrypted configuration file. This method, which uses the Exclude Digest Credential in Configuration File setting, is useful for initializing digest credentials because it doesn't require you to first configure a symmetric key and enter it on the phone. With this method, you send the digest credentials to the phone in an unencrypted configuration file. After the credentials are in the phone, we recommend that you disable the **TFTP Encrypted Config** option and then enable the **Exclude Digest Credential in Configuration File** on the **Phone Security Profile Configuration** page. This will exclude digest credentials from future downloads.
- After digest credentials exist in these phones and an incoming file doesn't contain digest credentials, the existing credentials remain in place. The digest credentials remain intact until the phone is factory reset or new credentials (including blanks) are received. If you change digest credentials for a phone or end user, temporarily disable the **Exclude Digest Credential in Configuration File** on the corresponding **Phone Security Profile Information** page to download the new digest credentials to the phone.

Encryption for Phone Configuration File Task Flow

To set up encryption for TFTP configuration files, make sure that the cluster security is in mixed mode, verify phones in your cluster that support manual key encryption and public key encryption, verify the phones that support SHA-1 and SHA-512 and complete the tasks below.

Note If you enable SHA-512 clusterwide, and your phones don't support it, those phones do not work.

Procedure

	Command or Action	Purpose
Step 1	Enable TFTP Encryption, on page 6	Enable the TFTP Configuration File option for your phones. You can enable this option in the Phone Security Profile.
Step 2	Configure SHA-512 Signing Algorithm, on page 6	When TFTP file encryption is enabled, SHA-1 is configured by default as the signing algorithm. Use this procedure to update the system to use the stronger SHA-512 algorithm.
Step 3	Verify LSC or MIC Certificate Installation, on page 9	For phones that use public keys, verify the certificate installation.
Step 4	Update CTL File, on page 9	After you complete your TFTP config file updates, regenerate the CTL file.

	Command or Action	Purpose
Step 5	Restart Services, on page 10	Restart the Cisco CallManager and Cisco TFTP services.
Step 6	Reset Phones, on page 10	After you complete your encrypted TFTP config file updates, reset your phones.

Enable TFTP Encryption

You can enable this TFTP within the phone security profile for a given phone model. Perform this procedure to enable TFTP encryption for files downloaded from the TFTP server.

Procedure

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

Step 2 Click **Find** and choose a phone security profile.

Step 3 Check the **TFTP Encrypted Config** check box.

Step 4 Click **Save**.

Step 5 Repeat these steps for any other phone security profiles that are used in the cluster.

Note To disable encryption for the phone configuration files, you must uncheck the **TFTP Encrypted Config** check box in the phone security profile in Cisco Unified Communications Manager Administration and then save your change.

Configure SHA-512 Signing Algorithm

SHA-1 is the default algorithm for TFTP file signing. You can use the below optional procedure to upgrade the system to use the stronger SHA-512 algorithm for TFTP configuration files such as digital signatures.

Note Make sure that your phones support SHA-512. If not, the phones don't work after you update your system.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Go to the **Security Parameters** pane.

Step 3 From the **TFTP File Signature Algorithm** drop-down list, choose **SHA-512**.

Step 4 Click **Save**.

Restart the affected services listed in the pop-up window to complete the procedure.

Set Up Manual Key Distribution

For phones that use manual keys, you must set up manual key distribution.

Before you begin

The following procedure assumes that:

- Your phone exists in the Unified Communications Manager database.
- A compatible firmware load exists on the TFTP server.
- You have enabled the TFTP Encrypted Config parameter in Unified Communications Manager Administration.
- Your phone supports manual key distribution.

Procedure

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

Step 2 Click **Find**.

Step 3 After the **Phone Configuration** window displays, configure the manual key distribution settings.

Note After you have configured the settings, you should not change the key.

Step 4 Click **Save**.

Step 5 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.

Manual Key Distribution Settings

The following table describes the manual distribution configuration settings in the **Phone Configuration** window.

Table 1: Manual Key Distribution Configuration Settings

Setting	Description
Symmetric Key	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). Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified Communications Manager rejects the value. Cisco Unified Communications Manager supports the following key sizes: • Cisco Unified IP Phones 7800 and (SIP only)—256 bits • Cisco Unified IP Phones 7942 and 7962 (SIP only)—128 bits After the key is configured, you should not change it.
Generate String	If you want Cisco Unified Communications Manager Administration to generate a hexadecimal string for you, click the **Generate String** button. After the key is configured, you should not change it.
Revert to Database Value	If you want to restore the value that exists in the database, click this button.

Enter Phone Symmetric Key

If you used the previous procedure to configure a manual key for your phone in Unified Communications Manager, use this procedure to enter the key on the phone.

Procedure

Step 1 Press the **Settings** button on the phone.

Step 2 If the configuration is locked, scroll down the **Settings** menu, highlight **Unlock Phone** and press the **Select** softkey. Enter the phone password and press the **Accept** softkey.

The phone accepts the password.

Step 3 Scroll down the **Settings** menu, highlight **Security Configuration**, and press the **Select** softkey.

Step 4 In the **Security Configuration** menu, highlight the **Set Cfg Encrypt Key** option and press the **Select** softkey.

Step 5 When prompted for the encryption key, enter the key (in hex). If you need to clear the key, enter 32 zero digits.

Step 6 After you have finished entering the key, press the **Accept** softkey.

The phone accepts the encryption key.

Step 7 Reset the phone.

After the phone resets, the phone requests encrypted configuration files.

Verify LSC or MIC Certificate Installation

For phones that use public keys, verify the certificate installation.

Note This procedure applies to Cisco Unified IP Phones that uses PKI encryption. To determine, if your phone supports PKI encryption, see Phone Models Supporting Encrypted Configuration File section.

The following procedure assumes that the phone exists in Unified Communications Manager database and you have enabled the TFTP Encrypted Config parameter in Unified Communications Manager.

Procedure

Step 1 Verify that a Manufacture-Installed Certificate (MIC) or a Locally Significant Certificate (LSC) exists in the phone.

Step 2 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The lists of phones appear.

Step 3 Click the **Device Name**.
The **Phone Configuration** page appears.

Tip Choose the **Troubleshoot** option in the CAPF settings section from the **Phone Configuration** page, to verify whether an LSC or MIC exists in the phone in Unified Communications Manager. The Delete and Troubleshoot options don't appear when a certificate doesn't exist in the phone.

Tip You can also verify that an LSC or MIC exists in the phone by checking the security configuration on the phone. For more information, see the administration guides for Cisco Unified IP Phones that support this version of Unified Communications Manager.

Step 4 If a certificate doesn't exist, install an LSC by using the CAPF functionality on the **Phone Configuration** window. For information on how to install an LSC, see topics related to the Certificate Authority Proxy Function.

Step 5 Click **Save** after you configure the CAPF settings.

Step 6 Click **Reset**.
The phone requests an encrypted configuration file from the TFTP server after the phone resets.

Update CTL File

Update the CTL file, when you have done any modifications to Unified Communications Manager. Since you have enabled the TFTP file encryption, you have to regenerate the CTL file.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 On the publisher node, run the **utils ctl update CTLfile** command.

Restart Services

After you have completed your encrypted TFTP configuration file updates, make sure that you restart your Cisco TFTP and Cisco CallManager services for the changes to take effect.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center – Feature Services**.

Step 2 Choose the following two services.

- Cisco CallManager
- Cisco TFTP

Step 3 Click **Restart**..

Reset Phones

Make sure that you reset your phones after you complete all your encrypted TFTP configuration file updates.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phones**.

Step 2 Click **Find**.

Step 3 Click **Select All**.

Step 4 Click **Reset Selected**.

Disable TFTP Encrypted Configuration Files

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

After you update the setting, the encryption keys for the phone remain in the Unified Communications Managerdatabase.

Cisco Unified IP Phones 7911G, 7931G (SCCP only), 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7971G, 7971G-GE, and 7975G request an encrypted file (.enc.sgn file) when the encrypted configuration setting gets updated to **False**, the phone requests an unencrypted, signed file (.sgn file).

If Cisco Unified IP Phones are running on SCCP and SIP, request an encrypted file when the encryption configuration setting gets updated to **False**. Remove the symmetric key from the phone GUI so that the phone requests an unencrypted configuration file the next time that it is reset.

- Cisco Unified IP Phones running on SCCP: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7921G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7971G, 7971G-GE, 7975G, 8941, 8945.
- Cisco Unified IP Phones running on SIP: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, 7811, 78321, 7841, 7861, 7832, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NE, 8821, 8831, 8832, 8832NR.

Procedure

	Command or Action	Purpose
Step 1	To disable encryption for the phone configuration files, Uncheck **TFTP Encrypted Config** check box in the phone security profile associated to the phone.	
Step 2	For Cisco Unified IP Phones 7942 and 7962 (SIP only), Enter a 32-byte 0 as the key value for the symmetric key at the phone screen to disable encryption.	
Step 3	For Cisco Unified IP Phones (SIP only), delete the symmetric key at the phone screen to disable encryption.	For information on how to perform these tasks, see the phone administration guide that supports your phone model.

Exclude Digest Credentials From Phone Configuration File Download

To exclude digest credentials from the configuration file that is sent to phones after the initial configuration, check the Exclude Digest Credentials in Configuration File check box for the security profile that is applied to the phone. Only Cisco Unified IP Phones 7800, 7942, and 7962 (SIP only) support this option.

You may need to uncheck this check box to update the configuration file for changes to digest credentials.