C H A P T E R **8**

Configuring Encrypted Phone Configuration Files

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.

This chapter contains information on the following topics:

Understanding Encryption of the Phone Configuration File

To secure digest credentials and secured passwords in phone downloads from Cisco Unified Communications Manager, you must enable the TFTP Encrypted Config option in the Phone Security Profile Configuration window and perform additional tasks in Cisco Unified Communications Manager Administration.

After you enable the TFTP Encrypt Config option, configure the required parameters in Cisco Unified Communications Manager Administration and the phone and restart required services in Cisco Unified Serviceability, the TFTP server

1. Deletes all clear text configuration files on disk
2. 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 phone that is running SIP 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 8-9 for more information.**

Some phones do not support encrypted phone configuration files, as described in "Supported Phone Models" section on page 8-4. The phone model and protocol determine the method that the system uses to encrypt the configuration file. Supported methods rely on Cisco Unified Communications Manager 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 Communications Manager supports the following methods:

- Manual Key Distribution
- Symmetric Key Encryption with Phone Public Key

The information in the "Manual Key Distribution" and "Symmetric Key Encryption with Phone Public Key" sections assumes that you configured Mixed Mode and that you enabled the TFTP Encrypted Config parameter in Cisco Unified Communications Manager Administration.

Manual Key Distribution

Tip   For a list of phones that support this method, see "Supported Phone Models" section on page 8-4.

With manual key distribution, a 128- or 256-bit symmetric key, which is stored in the Cisco Unified Communications Manager database, encrypts the phone configuration file after the phone resets. To determine the key size for your phone model, see "Supported Phone Models" section on page 8-4.

To encrypt the configuration file, the administrator can either manually enter the key into or prompt Cisco 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 "Supported Phone Models" section on page 8-4.

When the phone contains the symmetric key, the phone always requests the encrypted configuration file. Cisco 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; see "Supported Phone Models" section on page 8-4 for more information.

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

Tip   For a list of phones that support this method, see "Supported Phone Models" section on page 8-4.

For more information about The Certificate Authority Proxy Function (CAPF), see "Certificate Authority Proxy Function Overview" section on page 7-1. The Certificate Authority Proxy Function (CAPF) authenticates Cisco Unified IP Phones to Cisco Unified Communications Manager and issues phone certificates (LSCs).

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). 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 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 Unified IP Phones that support this encryption method request an encrypted file (.enc.sgn file), Cisco 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 Cisco Unified Communications Manager database. If the error condition is resolved, the phone requests an encrypted configuration file the next time that it resets.

Supported Phone Models

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

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 7905G or 7912G (SIP only)	Manual key distribution— Encryption algorithm: RC4 Key size: 256 bits File signing support: No
Cisco Unified IP Phone 7940G or 7960G (SIP only)	Manual key distribution— Encryption algorithm: Advanced Encryption Standard (AES) 128 Key size: 128 bits File signing support: These phones that are running SIP receive signed, encrypted configuration files but ignore the signing information.
Cisco Unified IP Phone 7970G, 7971G, or 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 (SCCP only)	Symmetric key encryption with phone public key (PKI encryption)— Encryption algorithm: AES 128 Key size: 128 bits File signing support: Yes

Configuration Tips for Encrypted Configuration Files

Cisco recommends that you enable the TFTP Encrypted Config flag to secure confidential data in phone downloads. For phones that do not have PKI capabilities, you must also configure a symmetric key in Cisco Unified Communications Manager Administration and in the phone. If the symmetric key is missing from either the phone or Cisco Unified Communications Manager or if a mismatch occurs when the TFTP Encrypted Config flag is set, the phone cannot register.

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

- Only phones that support encrypted configuration files display the TFTP Encrypted Config flag in the phone security profile. You cannot configure encrypted configuration files for Cisco Unified IP Phones 7905G, 7912G, 7940G, and 7960G (SCCP only) because these phones do not receive confidential data in the configuration file download.

- The default setting for TFTP Encrypted Config specifies False (not checked). If you apply the default, non-secure profile to the phone, digest credentials and secured passwords get sent in the clear.

- For Cisco Unified IP Phones that use public key encryption, Cisco Unified Communications Manager does not require you to set the Device Security Mode to authenticated or encrypted to enable encrypted configuration files. Cisco Unified Communications Manager uses the CAPF process for downloading its public key during registration.

- You may choose to download unencrypted configuration files to phones if you know your environment is secure or to avoid manually configuring symmetric keys for phones that are not PKI-enabled; however, Cisco does not recommend using this method.

- For Cisco Unified IP Phones 7905G, 7912G, 7940G, and 7960G (SIP only), Cisco Unified Communications Manager Administration 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 TFTP Exclude Digest Credential in Configuration File setting, is useful for initializing digest credentials because it does not 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, Cisco recommends that you keep the TFTP file encryption setting disabled and enable the TFTP Exclude Digest Credential in Configuration File flag on the corresponding security profile window, which will exclude digest credentials from future downloads.

  After digest credentials exist in these phones and an incoming file does not 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 Credentials flag on the corresponding security profile window to download the new digest credentials to the phone.

Encryption Configuration File Configuration Checklist

Use Table 8-1 to guide you through the configuration process for encrypted configuration files in Cisco Unified Communications Manager Administration.

Table 8-1   Encryption Configuration File Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Verify that the Cluster Security Mode is configured for Mixed Mode. **Note** Cluster security mode configures the security capability for your cluster or standalone server.	Configuring the Cisco CTL Client, page 3-1
Step 2	Check the TFTP Encrypted Config check box in the Phone Security Profile. Be sure to apply the profile to the phone.	• Configuration Tips for Encrypted Configuration Files, page 8-4 • Enabling Phone Configuration File Encryption, page 8-6 • Applying a Phone Security Profile, page 5-9
Step 3	Determine which phones support manual key distribution and which phones support symmetric key encryption with phone public key (PKI encryption).	Supported Phone Models, page 8-4

Table 8-1   Encryption Configuration File Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	If your phone supports manual key distribution, perform the manual key distribution tasks.	• Configuration Tips for Encrypted Configuration Files, page 8-4 • Configuring Manual Key Distribution, page 8-6 • Manual Key Distribution Configuration Settings, page 8-7
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 8-7
Step 6	If your phone supports the method, symmetric key encryption with phone public key (PKI encryption), verify that a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone.	• Verifying That an LSC or MIC Certificate Is Installed, page 8-8 • Using the Certificate Authority Proxy Function, page 7-1

Enabling Phone Configuration File Encryption

The TFTP server queries the database when it builds the configuration file. If the phone security profile that is applied to the phone has the TFTP encrypted configuration flag set, the TFTP server builds an encrypted configuration file.

To access the TFTP encryption flag, find the appropriate device security profile for the phone, as described in "Finding a Phone Security Profile" section on page 5-2. Check the TFTP Encrypted Config check box to enable configuration file encryption.

Additional Information

See the "Related Topics" section on page 8-10

Configuring Manual Key Distribution

To determine whether your phone supports manual key distribution, see "Supported Phone Models" section on page 8-4.

The following procedure assumes that

• The phone exists in the Cisco Unified Communications Manager database,

• A compatible firmware load exists on the TFTP server, and

• You enabled the TFTP Encrypted Config parameter in Cisco Unified Communications Manager Administration.

Procedure

Step 1   Find the phone, as described in the *Cisco Unified Communications Manager Administration Guide*.

Step 2   After the Phone Configuration window displays, configure the manual key distribution settings that are described in Table 8-2. After you have configured the settings, you should not change the key.

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 8-10.

Manual Key Distribution Configuration Settings

Table 8-2 describes the manual distribution configuration settings in the Phone Configuration window.

- For configuration tips, see the "Configuration Tips for Encrypted Configuration Files" section on page 8-4.

- For related information and procedures, see the "Related Topics" section on page 8-10.

Table 8-2   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 7905G and 7912G (SIP only)—256 bits
	• Cisco Unified IP Phones 7940G and 7960G (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.

Entering the Symmetric Key on the Phone

Follow this procedure to enter the symmetric key on the phone after you configure manual key distribution in Cisco Unified Communications Manager Administration.

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.

Verifying That an LSC or MIC Certificate Is Installed

This procedure applies to Cisco Unified IP Phones that use PKI encryption. To determine whether your phone supports the method, symmetric key encryption with phone public key (PKI encryption), see the "Supported Phone Models" section on page 8-4.

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

Procedure

Step 1 Verify that a manufacture-installed certificate (MIC) or a locally significant certificate (LSC) exists in the phone.

> **Tip** By choosing the Troubleshooting option in the CAPF settings section of the Phone Configuration window, you can verify that an LSC or MIC exists in the phone in Cisco Unified Communications Manager Administration. The Delete and Troubleshoot options do not display if a certificate does not exist in the phone.
>
> You can also verify that an LSC or MIC exists in the phone by checking the security configuration at the phone. Refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phones that support this version of Cisco Unified Communications Manager for more information.

Step 2 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 7-1.

Step 3 After you configure the CAPF settings, click **Save**.

Step 4 In the Phone Configuration window, click **Reset**. The phone requests an encrypted configuration file from the TFTP server after the phone resets

Additional Information

See the "Related Topics" section on page 8-10.

Verifying That the Phone Configuration File Is Encrypted

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

- Cisco Unified IP Phones 7905G and 7912G (SIP only)—LD <MAC>.x
- Cisco Unified IP Phones 7940G and 796G (SIP only)—SIP<MAC>.cnf.enc.sgn
- Cisco Unified IP Phones 7911G, 7931G (SCCP only), 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G,7965G, 7970G, 7971G, 7971G-GE, and 7975G—SEP<MAC>.cnf.xml.enc.sgn

To access the configuration file at the phone, refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phones that support encryption and this Cisco Unified Communications Manager release for more information.

Disabling Encryption for the Phone Configuration Files

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 save your change.

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 Cisco Unified Communications Manager database.

Cisco Unified IP Phones 7911G, 7931G (SCCP only), 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 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 7940G/7960G/7905G/7912G (SIP only) request an encrypted file when the encryption configuration setting gets updated to False, 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.

Tip For Cisco Unified IP Phones 7940G and 7960G (SIP only), enter a 32-byte 0 as the key value for the symmetric key at the phone GUI to disable encryption. For Cisco Unified IP Phones 7905G and 7912G (SIP only), 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.

Excluding 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 TFTP Exclude Digest Credentials in Configuration File check box for the security profile that is applied to the phone. Only Cisco Unified IP Phones 7905G, 7912G, 7940G, and 7960G (SIP only) support this option.

You may need to uncheck this check box to update the configuration file for changes to digest credentials. See the "Configuration Tips for Encrypted Configuration Files" section on page 8-4 for more information.

Additional Information

See the "Related Topics" section on page 8-10.

Where to Find More Information

Related Topics

Related Cisco documentation

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