TFTP Encryption

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.

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 3	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 4	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 4	For phones that use public keys, verify the certificate installation.
Step 4	Update CTL File, on page 5	After you complete your TFTP config file updates, regenerate the CTL file.
Step 5	Restart Services, on page 5	Restart the Cisco CallManager and Cisco TFTP services.
Step 6	Reset Phones, on page 5	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.

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.

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.

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.

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.

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.

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**. However, after regenerating or updating CallManager certificate, you don't have to manually restart TFTP service.

Reset Phones

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

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.