Default Security Setup

This section provides information about the default security setup.

Default Security Features

Security by Default provides the following automatic security features for Cisco Unified IP Phones:

- Signing of the phone configuration files.
- Support for phone configuration file encryption.
- https with Tomcat and other Web services (Midlets)

For Unified Communications Manager Release 8.0 later, these security features are provided by default without running the CTL Client.

Trust Verification Service

There are large number of phones in a network and Cisco Unified IP Phone have limited memory. Hence, Unified Communications Manager acts as a remote trust store through TVS and so that a certificate trust store doesn't have to be placed on each phone. The Cisco Unified IP Phones contact TVS server for verification, because it cannot verify a signature or certificate through CTL or ITL files. Thus, having a central trust store is easier to manage than having the trust store on all the Cisco Unified IP Phones.

TVS enables Cisco Unified IP Phone to authenticate application servers, such as EM services, directory, and MIDlet, during HTTPS establishment.

TVS provides the following features:

- Scalability—Cisco Unified IP Phone resources are not impacted by the number of certificates to trust.
- Flexibility—Addition or removal of trust certificates are automatically reflected in the system.
- Security by Default—Non-media and signaling security features are part of the default installation and don't require user intervention.

Note When you enable secure signaling and media, create a CTL file and then set the cluster to mixed mode. To create a CTL file and set the cluster to mixed mode, use the CLI command **utils ctl set-cluster mixed-mode**.

The following are the basic concepts that describe TVS:

- TVS runs on the Unified Communications Manager server and authenticates certificates on behalf of the Cisco IP Phone.
- Cisco Unified IP Phone only needs to trust TVS, instead of downloading all the trusted certificates.
- The ITL file is generated automatically without user intervention. The ITL file is downloaded by Cisco Unified IP Phone and trust flows from there.

TVS Description

The following are the basic concepts that describe TVS:

- TVS runs on the Unified Communications Manager server and authenticates certificates on behalf of the Cisco IP Phone.
- Cisco IP Phone only needs to trust TVS, instead of downloading all the trusted certificates.
- The ITL file is generated automatically without user intervention. The ITL file is downloaded by Cisco IP Phone and trust flows from there.

Initial Trust List

The Initial Trust List (ITL) file has the same format as the CTL file. However, it is a smaller and leaner version.

The following attributes apply to the ITL file:

- The system builds the ITL file automatically when the TFTP service is activated and you install the cluster. The ITL file is updated automatically if the content is modified.
- The ITL file does not require eTokens. It uses a soft eToken (the private key associated with TFTP server's CallManager certificate).
- The Cisco Unified IP Phone download the ITL file during a reset, restart, or after downloading the CTL file.

The ITL file contains the following certificates:

- ITLRecovery Certificate—This certificate signs the ITL File.
- The CallManager certificate of the TFTP server—This certificate allows you to authenticate the ITL file signature and the phone configuration file signature.
- All the TVS certificates available on the cluster—These certificates allow the phone to communicate to TVS securely and to request certificates authentication.
- The CAPF certificate—These certificates support configuration file encryption. The CAPF certificate isn't required in the ITL File (TVS can authenticate it), however, it simplifies the connection to CAPF.

The ITL file contains a record for each certificate. Each record contains:

- A certificate
- Pre-extracted certificate fields for easy lookup by the Cisco IP Phone
- Certificate role (TFTP, CUCM, TFTP+CCM, CAPF, TVS, SAST)

The TFTP server's CallManager certificate is present in two ITL records with two different roles:

- TFTP or the TFTP and CCM role—To authenticate configuration file signature.
- SAST role—To authenticate the ITL file signature.

Initial Trust List Files

The Initial Trust List (ITL) file has the same format as the CTL file. However, it is a smaller and leaner version.

The following attributes apply to the ITL file:

- The system builds the ITL file automatically when you install the cluster. The ITL file is updated automatically if the content is modified.
- The ITL file does not require eTokens. It uses a soft eToken (the private key associated with TFTP server's CallManager certificate).
- The Cisco Unified IP Phone download the ITL file during a reset, restart, or after downloading the CTL file.

ITL File Contents

The ITL file contains the following certificates:

- The CallManager certificate of the TFTP server—This certificate allows you to authenticate the ITL file signature and the phone configuration file signature.
- All the TVS certificates available on the cluster—These certificates allow the phone to communicate to TVS securely and to request certificates authentication.
- The CAPF certificate—These certificates support configuration file encryption. The CAPF certificate isn't required in the ITL File (TVS can authenticate it), however, it simplifies the connection to CAPF.

The ITL file contains a record for each certificate. Each record contains:

- A certificate
- Pre-extracted certificate fields for easy lookup by the Cisco IP Phone
- Certificate role (TFTP, CUCM, TFTP+CCM, CAPF, TVS, SAST)

The TFTP server's CallManager certificate is present in two ITL records with two different roles:

- TFTP or the TFTP and CCM role—To authenticate configuration file signature.
- SAST role—To authenticate the ITL file signature.

ITL and CTL File Interaction

The Cisco IP Phone relies on the CTL file to know about the cluster security mode (non-secure or mixed mode). The CTL File tracks the cluster security mode by including the Unified Communications Manager certificate in the Unified Communications Manager record.

The ITL File also contains the cluster security mode indication.

Certificate Management Changes for ITLRecovery Certificate

- The validity of ITLRecovery has been extended from 5 years to 20 years to ensure that the ITLRecovery certificate remains same for a longer period.

Note The validity of ITLRecovery certificates continues to be 5 years if you upgrade Unified Communications Manager. While upgrading Unified Communications Manager, the certificates get copied to the later release. However, when you regenerate an ITLRecovery certificate or when you do a fresh install of Unified Communications Manager, the validity of ITLRecovery gets extended to 20 years.

- Before you regenerate an ITLRecovery certificate, a warning message appears on both the CLI and the GUI. This warning message displays that if you use a tokenless CTL and if you regenerate the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints.

Interactions and Restrictions

If a Unified Communications Manager cluster has more than 39 certificates, then the ITL file size on Cisco IP Phone exceeds 64 kilobytes. Increase in the ITL file size affects the ITL to load properly on the phone causing the phone registration to fail with Unified Communications Manager.

Update ITL File for Cisco Unified IP Phones

A centralized TFTP with Unified Communication Manager using Security By Default with ITL files installed on the phones does not validate TFTP configuration files.

Perform the following procedure before any phones from the remote clusters are added to the centralized TFTP deployment.

Procedure

Step 1 On the Central TFTP server, enable the Enterprise Parameter **Prepare cluster for pre CM-8.0 rollback**.

Step 2 Restart TVS and TFTP.

Step 3 Reset all phones to verify that they download the new ITL file that disables ITL signature verification.

Step 4 Configure Enterprise Parameter Secure https URLs to use HTTP instead of HTTPS.

Autoregistration

If the cluster is in nonsecure mode, the system supports autoregistration. The default configuration file will also be signed. Cisco IP Phones that do not support Security by Default will be served a nonsigned default configuration file.

Note In mixed mode, the system does not support autoregistration.

Obtain Cisco Unified IP Phone Support List

Use the Cisco Unified Reporting tool to generate a list of Cisco endpoints that support Security By Default.

Procedure

Step 1 From Cisco Unified Reporting, choose **System Reports**.

Step 2 From the **System Reports** list, choose **Unified CM Phone Feature List**.

Step 3 From the **Product** drop-down list, choose **Security By Default**.

Step 4 Click **Submit**.

A report is generated with the list of supported features for the particular phone.

ECDSA Support for Common Criteria for Certified Solutions

Unified Communications Manager supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. These certificates are stronger than the RSA-based certificates and are required for products that have Common Criteria (CC) certifications. The US government Commercial Solutions for Classified Systems (CSfC) program requires the CC certification and so, it is included in Unified Communications Manager.

The ECDSA certificates are available along with the existing RSA certificates in the following areas—Certificate Manager, SIP, Certificate Authority Proxy Function (CAPF), Transport Layer Security (TLS) Tracing, Entropy, HTTP, and computer telephony integration (CTI) Manager.

Certificate Manager ECDSA Support

In Unified Communications Manager Release 11.0, the certificate manager supports both generation of self-signed ECDSA certificates and the ECDSA certificate signing request (CSR). Earlier releases of Unified Communications Manager supported **RSA** certificate only. However, Unified Communications Manager Release 11.0 onwards, **CallManager-ECDSA** certificate has been added along with the existing **RSA** certificate.

Both the **CallManager** and **CallManager-ECDSA** certificates share the common certificate trust store—CallManager-Trust. Unified Communications Manager uploads these certificates to this trust store.

The certificate manager supports generation of ECDSA certificates having different values of key length.

When you update or install Unified Communications Manager, the self-signed certificate is generated. Unified Communications Manager Release 11.0 always has an ECDSA certificate and uses that certificate in its SIP interface. The secure Computer Telephony Integration (CTI) Manager interface also supports ECDSA certificates. As both the CTI Manager and SIP server use the same server certificate, both the interfaces work in synchronization.

SIP ECDSA Support

Unified Communications Manager Release 11.0 includes ECDSA support for SIP lines and SIP trunk interfaces. The connection between Unified Communications Manager and an endpoint phone or video device is a SIP line connection whereas the connection between two Unified Communications Managers is a SIP trunk connection. All SIP connections support the ECDSA ciphers and use ECDSA certificates.

Following are the scenarios when SIP makes (Transport Layer Security) TLS connections:

- When SIP acts as a TLS server—When the SIP trunk interface of Unified Communications Manager acts as a TLS server for incoming secure SIP connection, the SIP trunk interface determines if the CallManager-ECDSA certificate exists on disk. If the certificate exists on the disk, the SIP trunk interface uses the CallManager-ECDSA certificate if the selected cipher suite is **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** or **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**. The SIP trunk interface continues to support RSA TLS cipher suites for connections from clients that do not support ECDSA cipher suites. The **TLS Ciphers** drop-down list contains options that permit configuration of the supported cipher suites when Unified Communications Manager acts as a TLS server.

- When SIP acts as a TLS client—When the SIP trunk interface acts as a TLS client, the SIP trunk interface sends a list of requested cipher suites to the server based on the **TLS Ciphers** field (which also includes the **ECDSA ciphers** option) in the **Enterprise Parameters** window of Cisco Unified Communications Manager. The **TLS Ciphers**. This configuration determines the TLS client cipher suite list and the supported cipher suites in order of preference.

Note If you establish a TLS connection with an earlier release of the Unified Communications Manager that does not support ECDSA client certificate, the connection uses an RSA cipher suite. The client certificate sent in the TLS connection is not bound to the TLS Cipher you that you choose. Earlier releases of Unified Communications Manager also support that TLS servers receive and handle ECDSA client certificates.

Devices that use an ECDSA cipher to make a connection to Unified Communications Manager must have the CallManager-ECDSA certificate in their Identity Trust List (ITL) file. Then, the devices must incorporate the CallManager-ECDSA certificate into their local certificate store to trust the connection that is secured by the CallManager-ECDSA certificate.

CAPF ECDSA Support

Certificate Authority Proxy Function (CAPF) is a Cisco proprietary method for exchanging certificates between Cisco endpoints and Unified Communications Manager. Only Cisco endpoints use CAPF. To accomplish common criteria requirements, CAPF is updated to CAPF version 3 so that a client can be provided with ECDSA Locally Significant Certificate (LSC). A customer creates LSC locally. An LSC is an alternative to manufacturer installed certificate (MIC) that the manufacturer creates.

Use CAPF version 3 to allow Unified Communications Manager server to direct phone, CTI applications, and Jabber clients to generate EC keys to be used in their LSCs. After the EC Keys are generated, Unified Communications Manager either generates an ECDSA LSC and sends it to the Cisco endpoint or generates an ECDSA CSR.

In case the endpoint does not have CAPF version 3 support, you can configure the required EC key size and RSA key size and choose **EC Key Preferred, RSA Backup** option in **Phone Configuration** window from Cisco Unified CM Administration as a backup. This backup option is useful when CAPF server tries to send a request to EC key pair and the phone communicates to the server that it does not support EC key, the server sends the request to generate an RSA key pair instead of the EC key pair.

Note The **Endpoint Advanced Encryption Algorithms Support** parameter indicates that phones download the TFTP configuration files using advanced TLS ciphers. By default, EC ciphers have the highest priority. This solution is only supported for an on-premises deployment without MRA.

Entropy

To have strong encryption, a robust source of entropy is required. Entropy is a measure of randomness of data and helps in determining the minimum threshold for common criteria requirements. Data conversion techniques,

such as cryptography and encryption, rely on a good source of entropy for their effectiveness. If a strong encryption algorithm, such as ECDSA, uses a weak source of entropy, the encryption can be easily broken.

In Unified Communications Manager Release 11.0, the entropy source for Unified Communications Manager is improved. Entropy Monitoring Daemon is a built-in feature that does not require configuration. However, you can turn it off through the Unified Communications Manager CLI.

Use the following CLI commands to control the `Entropy Monitoring Daemon` service:

CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the `Entropy Monitoring Daemon` service.
utils service stop Entropy Monitoring Daemon	Stops the `Entropy Monitoring Daemon` service.
utils service active Entropy Monitoring Daemon	Activates the `Entropy Monitoring Daemon` service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the `Entropy Monitoring Daemon` service, which further unloads the kernel module.

HTTPS Support for Configuration Download

For secure configuration download, Unified Communications Manager Release 11.0 is enhanced to support HTTPS in addition to the HTTP and TFTP interfaces that were used in the earlier releases. Both client and server use mutual authentication, if required. Clients that are enrolled with ECDSA LSCs and Encrypted TFTP configurations are required to present their LSC.

The HTTPS interface uses both the CallManager and the CallManager-ECDSA certificates as the server certificates.

Note When you update CallManager, CallManager ECDSA, or Tomcat certificates, you must deactivate and reactivate the TFTP service. Port 6971 is used for authentication of the CallManager and CallManager-ECDSA certificates whereas port 6972 is used for the authentication of the Tomcat certificates.

CTI Manager Support

The computer telephony integration (CTI) interface is enhanced to support four new ciphers. The ciphers suites are **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**, **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** and **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**. By supporting these cipher suites, the CTI Manager interface needs to have the **CallManager-ECDSA** certificate, if it exists in Unified Communications Manager. Similar to the SIP interface, the Enterprise Parameter **TLS Ciphers** option in Unified Communications Manager is used to configure the TLS ciphers that are supported on the CTI Manager secure interface.

Certificate Regeneration

If you regenerate one of the Unified Communications Manager certificates, you must perform the steps in this section.

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate including a third party signed certificate if one was uploaded. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Regenerate CAPF Certificate

To regenerate the CAPF certificate, perform the following steps:

Note If the CAPF certificate is on the publisher, you might observe the phones restarting automatically to update their ITL file. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the CAPF certificate.

Step 2 If you have a CTL file then you must update the CTL file.

For more information see *Regenerate Certificate*, section in the Cisco Unified Communications Manager Security Guide.

Step 3 CAPF service is automatically restarted when CAPF certificate is regenerated.

See the "Activating the Certificate Authority Proxy Function Service" section, in the *Cisco Unified Communications Manager Security Guide*.

Regenerate TVS Certificate

Note If you plan to regenerate both TVS and TFTP certificates, regenerate the TVS certificate, wait for the possible phone restarts to complete, and then regenerate the TFTP certificate. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the TVS certificate.

Step 2 If you have a CTL file then you must update the CTL file.

For more information see *Regenerate Certificate*, section in the Cisco Unified Communications Manager Security Guide.

Step 3 TVS service is automatically restarted when TVS certificate is regenerated.

Regenerate TFTP Certificate

To regenerate a TFTP certificate, follow these steps:

Note If you plan to regenerate multiples certificates you must regenerate the TFTP certificate last. Wait for the possible phone restarts to complete before you regenerate the TFTP certificate. You might need to manually delete the ITL File from all Cisco IP Phones, if you do not follow this procedure. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the TFTP certificate.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If the TFTP service was activated, wait until all the phones have automatically restarted.

Step 3 If your cluster is in mixed mode, update the CTL file.

Step 4 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Tomcat Certificate Regeneration

To regenerate the Tomcat certificate, perform the following steps:

Procedure

Step 1 Regenerate the Tomcat certificate.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

System Back-Up Procedure After TFTP Certificate Regeneration

The trust anchor for the ITL File is a software entity: the TFTP private key. If the server crashes, the key gets lost, and phones will not be able to validate new ITL File.

In Unified Communications Manager Release 10.0, the TFTP certificate and private key both get backed up by the Disaster Recovery System. The system encrypts the backup package to keep the private key secret. If the server crashes, the previous certificates and keys will be restored.

Whenever the TFTP certificate gets regenerated, you must create a new system backup. For backup procedures, see the *Administration Guide for Cisco Unified Communications Manager* .

Refresh Upgrade From Cisco Unified Communications Manager Release 7.x to Release 8.6 Or Later

To upgrade your cluster from Release 7.x to Release 8.6 or later, follow this procedure:

Procedure

Step 1 Follow the normal procedure for upgrading a cluster. For more information, see *Administration Guide for Cisco Unified Communications Manager* .

Tip After you finish upgrading all nodes in the cluster to Unified Communications Manager Release 8.6 or later, you must also follow all the steps in this procedure to ensure that your Cisco Unified IP Phones register with the system.

Step 2 If you are running one of the following releases in mixed mode, you must run the CTL client:

- Unified Communications Manager Release 7.1(2)
  - All regular releases of 7.1(2)
  - All ES releases of 712 prior to 007.001(002.32016.001)
- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
  - All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see Chapter 4, “Configuring the CTL Client,”.

Step 3 Wait ten minutes for the Cisco IP Phones to automatically restart and register with Unified Communications Manager.

Caution You must back up your cluster using the Disaster Recovery System (DRS) to be able to recover the cluster.

Step 4 Back Up Your Cluster.

To backup your cluster using DRS, see the *Administration Guide for Cisco Unified Communications Manager* .

What to do next

Once the publisher is up after the upgrade, do not reboot until the CAR migration completes. You are not allowed to switch to old version or perform a DRS backup in this phase. You can monitor the CAR migration status by navigating to **Cisco Unified Serviceability** > **Tools** > **CDR Analysis and Reporting**.

Roll Back Cluster to a Pre-8.0 Release

Before you roll back a cluster to a pre-8.0 release of Unified Communications Manager, you must prepare the cluster for rollback using the Prepare Cluster for Rollback to pre-8.0 enterprise parameter.

To prepare the cluster for rollback, follow this procedure on each server in the cluster.

Procedure

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

The **Enterprise Parameters Configuration** window displays.

Set the Prepare Cluster for Rollback to pre-8.0 enterprise parameter to **True**.

Note Enable this parameter only if you are preparing to rollback your cluster to a pre-8.0 release of Unified Communications Manager. Phone services that use https (for example, extension mobility) will not work while this parameter is enabled. However, users will be able to continue making and receiving basic phone calls while this parameter is enabled.

Step 2 Wait ten minutes for the Cisco IP Phones to automatically restart and register with Unified Communications Manager.

Step 3 Revert each server in the cluster to the previous release.

For more information about reverting a cluster to a previous version, see *Administration Guide for Cisco Unified Communications Manager* .

Step 4 Wait until the cluster finishes switching to the previous version.

Step 5 If you are running one of the following releases in mixed mode, you must run the CTL client:

- Unified Communications Manager Release 7.1(2)
  - All regular releases of 7.1(2)
  - All ES releases of 712 prior to 007.001(002.32016.001)

- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
  - All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see the "Configuring the CTL Client" chapter.

Step 6 If "Prepare Cluster for Rollback to pre 8.0" is set to True in Enterprise Parameters then the following change must be made for Corporate Directories to work:

Under **Device > Device Settings > Phone Services > Corporate Directory** you must change the Service URL from Application:Cisco/CorporateDirectory to http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp.

Step 7 If "Prepare Cluster for Rollback to pre 8.0" is set to True in Enterprise Parameters then the following change must be made for Personal Directories to work:

Under **Device > Device Settings > Phone Services > Personal Directory** you must change the Service URL from Application:Cisco/PersonalDirectory to 'http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined.

Switch Back to Release 8.6 or Later After Revert

If you decide to switch back to the release 8.6 or later partition after you revert the cluster to Release 7.x, follow this procedure.

Procedure

Step 1 Follow the procedure for switching the cluster back to the inactive partition. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If you were running one of the following releases in mixed mode, you must run the CTL client:

Unified Communications Manager Release 7.1(2)

- All regular releases of 7.1(2)
- All ES releases of 712 prior to 007.001(002.32016.001)
- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
  - All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see the "Configuring the CTL Client" chapter.

Step 3 From Unified Communications Manager Administration, choose **System** > **Enterprise Parameters Configuration**.

The **Enterprise Parameters Configuration** window displays.

Set the Prepare Cluster for Rollback to pre-8.6 enterprise parameter to **False**.

Step 4 Wait ten minutes for the Cisco Unified IP Phones to automatically restart and register with Unified Communications Manager.

Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files

Unified Communications Manager 8.0(1) and later introduced the new Security By Default feature and the use of Initial Trust List (ITL) files. With this new feature, you must be careful when moving phones between different Unified CM clusters and ensure that you follow the proper steps for migration.

Caution Failure to follow the proper steps may lead to a situation where thousands of phones must manually have their ITL files deleted.

Cisco IP Phones that support the new ITL file must download this special file from their Unified CM TFTP server. Once an ITL file is installed on a phone, all future configuration files and ITL file updates must be signed by one of the following items:

- The TFTP server certificate that is currently installed on the phone or
- A TFTP certificate that can be validated TVS services on one of the clusters. You can find the certificates of TVS services within the cluster listed in the ITL file.

With this new security functionality in mind, three problems can occur when moving a phone from one cluster to another cluster:

1. The ITL file of the new cluster is not signed by the current ITL file signer, so the phone cannot accept the new ITL file or configuration files.
2. The TVS servers listed in the existing ITL of the phone may not be reachable when the phones are moved to the new cluster.
3. Even if the TVS servers are reachable for certificate verification, the old cluster servers may not have the new server certificates.

If one or more of these three problems are encountered, one possible solution is to delete the ITL file manually from all phones being moved between clusters. However, this is not a desirable solution since it requires massive effort as the number of phones increases.

The most preferred option is to make use of the Cisco Unified CM Enterprise Parameter Prepare Cluster for Rollback to pre-8.0. Once this parameter is set to True, the phones download a special ITL file that contains empty TVS and TFTP certificate sections.

When a phone has an empty ITL file, the phone accepts any unsigned configuration file (for migrations to Unified CM pre-8.x clusters), and also accepts any new ITL file (for migrations to different Unified CM 8.x clusters).

The empty ITL file can be verified on the phone by checking **Settings** > **Security** > **Trust List** > **ITL**. Empty entries appear where the old TVS and TFTP servers used to be.

The phones must have access to the old Unified CM servers only as long as it takes them to download the new empty ITL files.

If you plan to keep the old cluster online, disable the Prepare Cluster for Rollback to pre-8.0 Enterprise Parameter to restore Security By Default.

Bulk Certificate Export

If both the old and new clusters are online at the same time, you can use the Bulk Certificate migration method.

Remember that the Cisco Unified IP Phones verify every downloaded file against either the ITL file, or against a TVS server that exists in the ITL file. If the phone needs to move to a new cluster, the ITL file that the new cluster presents must be trusted by the old cluster TVS certificate store.

Note The Bulk Certificate Export method only works if both clusters are online with network connectivity while the phones are being migrated.

To use the Bulk Certificate Export method complete the following procedure:

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Security** > **Bulk Certificate Management**.

Step 2 Export certificates from new destination cluster (TFTP only) to a central SFTP server.

Step 3 Consolidate certificates (TFTP only) on the SFTP server using the Bulk Certificate interface.

Step 4 On the origination cluster use the Bulk Certificate function to import the TFTP certificates from the central SFTP server.

Step 5 Use DHCP option 150, or some other method, to point the phones to the new destination cluster.

The phones download the new destination cluster ITL file and attempt to verify it against their existing ITL file. The certificate is not in the existing ITL file so the phone requests the old TVS server to verify the signature of the new ITL file. The phone sends a TVS query to the old origination cluster on TCP port 2445 to make this request.

If the certificate export/consolidate/import process works correctly then the TVS returns success, and the phone replaces the ITL file in memory with the newly downloaded ITL file.

The phones can now download and verify the signed configuration files from the new cluster.

Generate Self-Signed Certificate

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Enter search parameters to find a certificate and view its configuration details.
The system displays the records that match all the criteria in the **Certificate List** window.

Step 3 Click **Generate Self-Signed Certificate** to generate a new self-signed certificate.
The **Generate New Self-Signed Certificate** window appears.

Step 4 From the **Certificate Purpose** drop-down box, select a system security certificate, such as **CallManager-ECDSA**.

Step 5 Configure the fields in the **Generate New Self-Signed Certificate** window. See the Related Topics section for more information about the fields and their configuration options.

Step 6 Click **Generate**.

Related Topics

Self-Signed Certificate Fields, on page 16

Self-Signed Certificate Fields

Table 1: Self-signed Certificate Fields

Field	Description
Certificate Purpose	Choose the required option from the drop-down list. When you choose any of the following options, the **Key Type** field is automatically set to **RSA**. • tomcat • ipsec • ITLRecovery • CallManager • CAPF • TVS When you choose any of the following options, the **Key Type** field is automatically set to **EC** (Elliptical Curve). • tomcat-ECDSA • CallManager-ECDSA
Distribution	Choose a Unified Communications Manager server from the drop-down list.
Key Type	This field lists the type of keys used for encryption and decryption of the public-private key pair. Unified Communications Manager supports **EC** and **RSA** key types.

Field	Description
Key Length	Choose any of the following values from the drop-down list: • 1024 • 2048 • 3072 • 4096 Depending on the key length, the self-signed certificate request, limits the hash algorithm choices. With the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. • If the key length value is 256, the supported hash algorithms are SHA256, SHA384, or SHA512. • If the key length value is 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 are chosen only for RSA certificates. These options are not available for ECDSA certificates. **Note** Some phone models might fail to register if the RSA **key length** value chosen for the CallManager **Certificate Purpose** is greater than 2048. For more information, navigate to **Unified CM Phone Feature List Report** on the Cisco Unified Reporting Tool (CURT), to check the **3072/4096 RSA key size support** for the list of supported phone models.
Hash Algorithm	Choose a value that is greater than or equal to the key length from the drop-down list: **Note** • The values in the **Hash Algorithm** drop-down list changes based on the value you have chosen in the **Key Length** field.

Generate Certificate Signing Request

If you generate a new certificate signing request for a specific certificate type, the application overwrites the existing certificate signing request for that certificate type.

Note Unified Communications Manager Release 11.0 onwards, when you choose the bulk operation units—TFTP or all, the ECDSA certificates get included with the RSA certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Generate CSR**.
The **Generate Certificate Signing Request** window appears.

Step 3 Enter search parameters to find a certificate and view its configuration details.
The system displays the records that match all the criteria in the **Certificate List** window.

Step 4 From the **Certificate Purpose** drop-down box, select a system security certificate, such as **CallManager-ECDSA**.

Step 5 Configure the fields in the **Generate Certificate Signing Request** window. See the Related Topics section for more information about the fields and their configuration options.

Step 6 Click **Generate**.

Related Topics

Certificate Signing Request Fields, on page 18

Certificate Signing Request Fields

Table 2: Certificate Signing Request Fields

Field	Description
Certificate Purpose	From the drop-down box, select a value: • **CallManager**
Distribution	Select a Unified Communications Manager server. When you select this field for multiserver for RSA, the syntax is: `Callmanager common name: <host-name>-ms.<domain>`
	Shows the name of the Unified Communications Manager application that you selected in the **Distribution** field by default.
Auto-populated Domains	This field appears in Subject Alternate Names (SANs) section. It lists the host names that are to be protected by a single certificate.
Parent Domain	This field appears in Subject Alternate Names (SANs) section. It shows the default domain name. You can modify the domain name, if required.
Key Type	This field identifies the type of key used for encryption and decryption for the public-private key pair. Unified Communications Manager supports RSA keys.

Field	Description
Key Length	From the **Key Length** drop-down box, select one of the values. Depending on the key length, the CSR request limits the hash algorithm choices. By having the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. For example, for a key length of 256, the supported hash algorithms are SHA256, SHA384, or SHA512. Similarly, for the key length of 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 can only be selected for RSA certificates. These options are not available for ECDSA certificates. **Note** Some phone models may fail to register if the RSA **key length** 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.
Hash Algorithm	Select a value from the **Hash Algorithm** drop-down box to have stronger hash algorithm as the elliptical curve key length. From the **Hash Algorithm** drop-down box, select one of the values. **Note** • The values for the **Hash Algorithm** field change based on the value you select in the **Key Length** field. • If your system is running on FIPS mode, it is mandatory that you select SHA256 as the hashing algorithm.

Interactions and Restrictions

- SIP devices that do not support **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** and **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** can still connect with **TLS_ECDHE_RSA_WITH_AES_256_SHA384**, **TLS_ECDHE_RSA_WITH_AES_128_SHA256**, or **AES128_SHA**. These options are dependent on the TLS cipher option that you choose. If you choose **ECDSA only** option, then the device that does not support the ECDSA ciphers will not be able make a TLS connection to the SIP interface. When you choose the **ECDSA only** option, the value of this parameter are **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** and **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**.
- CTI Manager Secure clients do not support **TLS_ECDHE_RSA_WITH_AES_128_SHA256** , **TLS_ECDHE_RSA_WITH_AES_256_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**, and **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384**. However, they can connect with **AES128_SHA**.

Perform Bulk Reset of ITL File

Make sure you perform this procedure only from the Unified Communications Manager publisher.

The bulk reset of the ITL file is performed, when phones no longer trust the ITL file signer and also cannot authenticate the ITL file provided by the TFTP service locally or using TVS.

To perform a bulk reset, use the CLI command **utils itl reset**. This command generates a new ITL recovery file and re-establishes the trust between phones and the TFTP service on CUCM.

Tip When you install Unified Communications Manager, use the CLI command **file get tftp** *ITLRecovery.p12*to export the ITL Recovery pair and then perform a backup through DR. You will also be prompted to enter the SFTP server (where the key is exported) and password.

Procedure

Step 1 Perform any one of the following steps:

- Run **utils itl reset localkey**.
- Run **utils itl reset remotekey**.

For **utils itl reset localkey**, the local key resides on the publisher. This step generates a new ITL file by taking the existing file on the system and replacing the signature of that file with the recovery key signature. The key is then copied to the TFTP servers in the cluster.

Step 2 Run **show itl** to verify that the reset was successful.

Step 3 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 4 Click **Reset**.

Step 5 Restart the TFTP service and restart all devices.

The devices download the ITL file that is signed with the ITLRecovery Key and register correctly to Unified Communications Manager again.

Reset CTL Localkey

When devices on a Unified Communications Manager cluster are locked and lose their trusted status, perform a reset of the Cisco Trust List (CTL) file with the CLI command **utils ctl reset localkey**. This command generates a new CTL file.

Procedure

Step 1 Run **utils ctl reset localkey**

For **utils ctl reset localkey**, the local key resides on the publisher. When issuing this command, the CTL file is temporarily signed by the ITLRecovery key. The new CTL file is then copied to the TFTP servers in the cluster.

Step 2 Run **show ctl** to verify that the reset was successful.

Step 3 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 4 Click **Reset**.

The devices restart. They are ready to download the CTL file that is signed by the ITLRecovery key and accept configuration files.

Step 5 Run the **utils ctl update CTLFile** and restart the necessary services rolling back the changes in Step 1.

The devices restart. They are ready to download the CTL file that is signed by the CallManager key and accept configuration files.

The devices download the CTL file that is signed using the required keys and register correctly to Unified Communications Manager again.

View the Validity Period of ITLRecovery Certificate

The ITLRecovery certificate has a long validity period with phones. You can navigate to the **Certificate File Data** pane to view the validity period or any other ITLRecovery certificate details.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Enter the required search parameters to find the certificate and view its configuration details.
The list of certificates that match the criteria appears in the **Certificate List** page.

Step 3 Click the **ITLRecovery** link to view the validity period.

The ITLRecovery certificate details appear in the **Certificate File Data** pane.

The validity period is 20 years from the current year.

Contact Search Authentication Task Flow

Complete the following tasks to set up Contact Search Authentication in Unified Communications Manager. When this feature is configured, users must authenticate themselves before searching the directory for other users.

Procedure

	Command or Action	Purpose
Step 1	Confirm Phone Support for Contact Search Authentication, on page 22	Confirm that your phones support this feature. Run the **Unified CM Phone Feature List** report in Cisco Unified Reporting to get a list of phone models that support the feature.
Step 2	Enable Contact Search Authentication, on page 22	Configure Unified Communications Manager for Contact Search Authentication.
Step 3	Configure Secure Directory Server for Contact Search, on page 23	Use this procedure to configure Unified Communications Manager with the URL to which phone users are directed when they search the directory for other users.

Confirm Phone Support for Contact Search Authentication

Confirm that the phones in your deployment support contact search authentication. Run a Phone Feature List report to obtain a full list of phone models that support the feature.

Procedure

Step 1 From Cisco Unified Reporting, click **System Reports**.

Step 2 Select **Unified CM Phone Feature**.

Step 3 Click the **Unified CM Phone Feature** report.

Step 4 Leave the **Product** field at the default value.

Step 5 From the **Feature** drop-down, choose **Authenticated Contact Search**.

Step 6 Click **Submit**.

Enable Contact Search Authentication

Use this procedure on Unified Communications Manager to configure contact search authentication for phone users.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils contactsearchauthentication status** command to confirm the contact search authentication setting on this node.

Step 3 If you need to configure contact search authentication:

- To enable authentication, run the **utils contactsearchauthentication enable** command.
- To disable authentication, run the **utils contactsearchauthentication disable** command.

Step 4 Repeat this procedure on all Unified Communications Manager cluster nodes.

Note You must reset phones in order for the changes to take effect.

Configure Secure Directory Server for Contact Search

Use this procedure to configure Unified Communications Manager with the directory server URL to which UDS sends user search requests. The default value is `https://<cucm-fqdn-or-ip>:port/cucm-uds/users`.

Note The default UDS port is 8443. When contact search authentication becomes enabled, the default UDS port switches to 9443. If you then disable contact search authentication, you must change the UDS port back to 8443 manually.

Procedure

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

Step 2 In the **Secure Contact Search URL** text box, enter the URL for secure UDS directory requests.

Note We recommend that for the URL, you choose a node that is not running the Cisco TFTP service. The CiscoTFTP and UDS services may disrupt each other if either service gets restarted.

Step 3 Click **Save**.