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

Trust Verification Service (TVS) is the main component of Security by Default. TVS enables Cisco Unified IP Phones to authenticate application servers, such as EM services, directory, and MIDlet, during HTTPS establishment.

TVS provides the following features:

- Scalability— Cisco 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 do not require user intervention.

Note When you enable secure signaling and media, you must create a CTL file and set the cluster to mixed mode. You can use the CTL client to make these changes, or you can use the CLI command **utils ctl set-cluster mixed-mode** to create the CTL file and change the security mode in one step.

TVS Description

The following basic concepts describe the Trust Verification Service:

- TVS runs on the Unified Communications Manager server and authenticates certificates on behalf of the Cisco IP Phone.
- Instead of downloading all the trusted certificates, Cisco IP Phone only need to trust TVS.
- The TVS certificates and a few key certificates are bundled in a new file: the Initial Trust List file (ITL).
- The ITL file gets generated automatically without user intervention.
- The ITL file gets downloaded by Cisco IP Phones and trust flows from there.

Initial Trust List

ITL Files

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

The following attributes apply to the ITL file:

- The system builds the ITL file automatically when you install the cluster.The ITL file gets 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 IP Phones download the ITL file during a boot up time or during a reset 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 in the cluster. These certificates allow the phone to talk to TVS securely and to request certificates authentication.
- The CAPF certificate. This allows to support configuration file encryption. The CAPF certificate is not really required in the ITL File (TVS can authenticate it) but 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 look up 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 TFTP+CCM role— To authenticate configuration file signature.
- SAST role—To authenticate ITL file signature.

ITL and CTL File Interaction

The Cisco IP Phone still relies on the CTL file to know the cluster security mode (nonsecure or mixed mode). The CTL File tracks the cluster security mode by including the Unified Communications Managercertificate in the Unified Communications Manager record.

The ITL File also contains the cluster security mode indication.

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 IP Phones

A Centralized TFTP with Cisco Unified CM Release 8.0 and later using Security By Default with ITL files installed on the phones does not validate TFTP configuration files. The following procedure must be completed 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.

Note Unified Communications Manager versions 8.6 and later automatically resets phones after you enable the **Prepare cluster for pre CM-8.0 rollback** Enterprise Parameter. For Central TFTP server's Unified Communications Manager version and how to enable this parameter, see the "Roll Back Cluster to a Pre-8.0 Release" section in the *Cisco Unified Communications Manager Security Guide*.

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

You can obtain a list of the Cisco IP Phones that support security by default by using Cisco Unified Reporting. To use Cisco Unified Reporting, follow this procedure:

Procedure

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

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

Step 3 Choose the appropriate feature from the **Feature** pull-down menu.

Step 4 Click **Submit.**

What to do next

For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

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 *Cisco Unified Communications Operating System Administration Guide*.

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.

Procedure

Step 1 Regenerate the CAPF certificate.

See Chapter 6, "Security", in the *Cisco Unified Communications Operating System Administration Guide*.

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

See Chapter 4, "Configuring the Cisco CTL Client", in the *Cisco Unified Communications Operating System Administration Guide*.

Step 3 Restart the CAPF service.

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

Regenerate TVS Certificate

No manual steps are required to regenerate a 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.

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.

Procedure

Step 1 Regenerate the TFTP certificate.

See Chapter 6, “Security,” in the *Cisco Unified Communications Operating System Administration Guide*.

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, run the CTL client.

See Chapter 4, “Configuring the CTL Client,”.

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

See Chapter 6, “Security,” in the *Cisco Unified Communications Operating System Administration Guide*.

Tomcat Certificate Regeneration

To regenerate the CAPF certificate, perform the following steps:

Procedure

Step 1 Regenerate the Tomcat certificate.

See Chapter 6, “Security”, in the *Cisco Unified Communications Operating System Administration Guide*.

Step 2 Restart the Tomcat service.

See Chapter 6, “Security”, in the *Cisco Unified Communications Operating System Administration Guide*.

Step 3 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

See Chapter 6, “Security,” in the *Cisco Unified Communications Operating System Administration Guide*.

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 8.0, 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 Disaster Recovery System Administration Guide.

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 Chapter 7, "Software Upgrades," in the *Cisco Unified Communications Operating System Administration Guide*.

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 *Disaster Recovery System Administration Guide*.

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 Administration, 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 Chapter 7, “Software Upgrades” in the *Cisco Unified Communications Operating System Administration Guide*.

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 ManagerRelease 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 *Cisco Unified Communications Operating System Administration Guide*.

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.

Related Topics

Roll Back Cluster to a Pre-8.0 Release, on page 8

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.

Perform Bulk Reset of ITL File

When devices on a Unified Communications Manager cluster are locked and lose their trusted status, perform a bulk reset of the Identity Trust List (ITL) file with the CLI command **utils itl reset**. This command generates a new ITL recovery file.

Tip Whenever you perform a fresh installation of Unified Communications Manager, export the ITL key as soon as possible and perform a backup through the Disaster Recovery System.

The CLI command to export the ITL recovery pair is as follows:

file get tftp *ITLRecovery.p12*

You will be prompted to enter the SFTP server (where the key will be exported) and password.

Before you begin

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

If needed, export the key from the publisher.

Procedure

Step 1 Perform 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 Unified Communications Manager Administration, select **System** > **Enterprise Parameters**

Step 4 Select **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.