Cisco CTL Client Setup

This chapter provides information about Cisco CTL client setup.

About Cisco CTL Setup

Device, file, and signaling authentication rely on the creation of the Certificate Trust List (CTL) file, which is created when you install and configure the Cisco Certificate Trust List (CTL).

The CTL file contains entries for the following servers or security tokens:

- System Administrator Security Token (SAST)
- CiscoCallManager and CiscoTFTP services that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TFTP server(s)
- ASA firewall
- ITLRecovery

When a Call Manager certificate is self-signed, the CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

In the case of a Multi-SAN Call Manager certificate, the CTL file contains the Publisher's Call Manager certificate.

The next time that the phone initializes, it downloads the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in.sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file.

After the Cisco CTL Client adds a server certificate to the CTL file, you can update the CTL file by running the following CLI commands:

utils ctl set-cluster mixed-mode
Updates the CTL file and sets the cluster to mixed mode.
utils ctl set-cluster non-secure-mode
Updates the CTL file and sets the cluster to non-secure mode.
utils ctl update CTLFile
Updates the CTL file on each node in the cluster.

When you configure a firewall in the CTL file, you can secure a Cisco ASA Firewall as part of a secure Unified Communications Manage system. It displays the firewall certificate as a “CCM” certificate.

Note

- You must run the CLI commands on the publisher node.
- Be aware that regenerating the CallManager certificate changes the signer of the file. Phones that do not support Security by Default will not accept the new CTL file unless CTL files are manually deleted from the phone. For information on deleting the CTL files on the phone, see the *Cisco IP Phone Administration Guide* for your phone model.

Addition of Second SAST Role in the CTL File for Recovery

Earlier releases of Unified Communications Manager has tokenless approach where endpoints trusted only one Cisco site administrator security token (SAST). This SAST is the CallManager certificate. In this approach, the certificate trust list (CTL) file contained only one SAST record that was used to sign the CTL file. As only one SAST was used, any update in the SAST signer caused the endpoints to get locked out. Following points list the scenarios when endpoints or devices locked out due to update in SAST signer:

- The endpoints accepted the CTL file that is signed by using the CallManager certificate during registration.
- An administrator regenerated the CallManager certificate and updated the CTL file. This regeneration implied that the updated CTL file was signed by updated CallManager certificate instead of the existing CallManager certificate.
- The endpoints did not trust the updated CallManager certificate because the updated certificate was unavailable in the endpoints trust list. So, the endpoints rejected the CTL file instead of downloading it.
- The endpoints tried to connect with the ccm service securely over Transport Layer Security (TLS), ccmservice offered its updated CallManager certificate to the endpoints as part of TLS exchange. Because the updated certificate was unavailable in the endpoints trust list, endpoints rejected the CTL file instead of downloading it.

- The endpoints no longer talk to ccmservice and get locked out as a result.

For easier recovery from the endpoint lock out, the tokenless approach for endpoints is enhanced by addition of second SAST in the CTL File for recovery. In this feature, the tokenless CTL file contains two SAST tokens—the CallManager record and the ITLRecovery record.

The ITLRecovery certificate is chosen over other certificates because of the following reasons:

- Does not change because of secondary reasons, such as change in hostname.
- Already being used in the ITL file.

SIP OAuth Configuration Through CLI

Through the CLI, you can configure the Cluster SIP OAuth mode.

Note For more information on how to configure SIP OAuth mode on Cisco Unified Communication Manager, see *Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)*.

Consider the following points:

- When Cluster SIP OAuth mode is enabled, Cisco Unified Communication Manager accepts SIP registrations with an OAuth token from secure devices.

  Once enabled, the following TLS ports are opened which are configurable through Cisco Unified Communications Manager user interface.

  - **SIP OAuth Port**
  - **SIP OAuth MRA Port**

  You can configure the ports from Cisco Unified CM Administration, choose **System** > **Cisco Unified CM** > **CallManager** page.

- Restart the Cisco CallManager service in all the nodes for the parameter change to take effect.

The encryption option consists of the following CLI commands:

admin:utils sipOAuth-mode
Check the status of SIP OAuth mode in the cluster.
utils sipOAuth-mode enable
Enables the SIP OAuth mode in the cluster.
utils sipOAuth-mode disable
Disables the SIP OAuth mode in the cluster.

Note Run the CLI commands only on the publisher node.

Activate Cisco CTL Provider Service

After you configure the Cisco CTL Client, the Cisco CTL Provider service changes the security mode from nonsecure to mixed mode and transports the server certificates to the CTL file. The service then transports the CTL file to all Unified Communications Manager and CiscoTFTP servers.

If you activate this service and then upgrade Unified Communications Manager, Unified Communications Manager automatically reactivates the service after the upgrade.

Tip You must activate the CiscoCTL Provider service on all servers in the cluster.

To activate the service, perform the following procedure:

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 In the Servers drop-down list box, choose a server where you have activated the Cisco CallManager or Cisco TFTP services.

Step 3 Click the **CiscoCTL Provider** service radio button.

Step 4 Click **Save.**

Tip Perform this procedure on all servers in the cluster.

Note You can enter a CTL port before you activate the CiscoCTL Provider service. If you want to change the default port number, see topics related to setting up ports for a TLS connection.

Step 5 Verify that the service runs on the servers. In Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to verify the state of the service.

Cisco CAPF Service Activation

Warning Activating the Cisco certificate authority proxy function service before you install and configure the Cisco CTL Client ensures that you do not have to update the CTL file to use CAPF.

Set up Secure Ports

You may have to configure a different TLS port number if the default port is currently being used or if you use a firewall and you cannot use the port within the firewall.

- The Cisco CTL Provider default port for the TLS connection equals 2444. The Cisco CTL Provider port monitors requests from the Cisco CTL Client. This port processes Cisco CTL Client requests, such as retrieving the CTL file, setting the cluster security mode, and saving the CTL file to the TFTP server.

Note Cluster security mode configures the security capability for your standalone server or a cluster.

- The Ethernet Phone Port monitors registration requests from the phone that is running SCCP. In nonsecure mode, the phone connects through port 2000. In mixed mode, the Unified Communications Manager port for TLS connection equals the value for the Unified Communications Manager port number added to (+) 443; therefore, the default TLS connection for Unified Communications Manager equals 2443. Update this setting only if the port number is in use or if you use a firewall and you cannot use the port within the firewall.
- The SIP Secure Port allows Unified Communications Manager to listen for SIP messages from phones that are running SIP. The default value equals 5061. If you change this port, you must restart the CiscoCallManager service in Cisco Unified Serviceability and reset the phones that are running SIP.

Tip After you update the port(s), you must restart the Cisco CTL Provider service in Cisco Unified Serviceability.

Tip You must open the CTL ports to the data VLAN from where the CTL Client runs.

To change the default setting, perform the following procedure:

Procedure

Step 1 Perform the following tasks, depending on the port that you want to change:

a) To change the Port Number parameter for the Cisco CTL Provider service, perform Step 2, on page 5 through Step 6, on page 6.

b) To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform Step 7, on page 6 through Step 11, on page 6.

Step 2 To change the Cisco CTL Provider port, choose **System** > **Service Parameters** in Unified Communications Manager Administration.

Step 3 In the Server drop-down list, choose a server where the CiscoCTL Provider service runs.

Step 4 In the Service drop-down list box, choose Cisco CTL Provider service.

Tip For information on the service parameter, click the question mark or the link name.

Step 5 To change the value for the Port Number parameter, enter the new port number in the Parameter Value field.

Note Starting 12.X onwards, you cannot change the value for the Port Number parameter in the Parameter Value field.

Step 6 Click **Save.**

Step 7 To change the Ethernet Phone Port or SIP Phone Secure Port settings, choose **System** > **CiscoUnifiedCM** in Unified Communications Manager Administration.

Step 8 Find a server where the CiscoCallManager service runs, as described in the *Administration Guide for Cisco Unified Communications Manager*; after the results display, click the **Name** link for the server.

Step 9 After the Unified Communications Manager Configuration window displays, enter the new port numbers in the Ethernet Phone Port or SIP Phone Secure Port fields.

Step 10 Reset the phones and restart the CiscoCallManager service in Cisco Unified Serviceability.

Step 11 Click **Save**.

Set Up Cisco CTL Client

Important You can set up encryption by using the **utils ctl** CLI command set. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions.*

The Cisco CTL CLI performs the following tasks:

- Sets the Unified Communications Manager security mode for a cluster or standalone server.

Note You cannot set the Unified Communications Manager cluster security parameter to mixed mode through the Enterprise Parameters Configuration window of Unified Communications Manager Administration. You can set the cluster security mode through the Cisco CTL Client or the CLI command set **utils ctl**.

- Creates the Certificate Trust List (CTL), which is a file that contains certificate entries for security tokens, Unified Communications Manager, ASA firewall, and CAPF server.

  The CTL file indicates the servers that support TLS for the phone connection. The client automatically detects the Unified Communications Manager, Cisco CAPF, and ASA firewall and adds certificate entries for these servers.

Note The Cisco CTL Client also provides supercluster support: up to 16 call processing servers, 1 publisher, 2 TFTP servers, and up to 9 media resource servers.

Tip You can update the CTL file during a scheduled maintenance window becaus you must restart the TFTP services and then the CallManager on all the serve that run these services in the cluster.

After you complete the Cisco CTL configuration, the CTL performs the following tasks:

- Writes the CTL file to the Unified Communications Manager server(s).
- Writes CAPF capf.cer to all Unified Communications Manager subsequent nodes (not first node) in the cluster.
- Writes CAPF certificate file in PEM format to all Unified Communications Manager subsequent nodes (not first node) in the cluster.
- Writes the file to all configured TFTP servers.
- Writes the file to all configured ASA firewalls.
- Signs the CTL file with the private key of the security token that exists in the USB port at the time you create the CTL file.

SAST Roles of CTL File

Note *Signer, mentioned in the following table, is used to sign the CTL file.

Table 1: System Administrator Security Token (SAST) Roles of CTL File

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
12.0(1)	Token 1 (Signer*) Token 2 ITLRecovery CallManager	ITLRecovery (Signer) CallManager

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
11.5(x)	Token 1 (Signer) Token 2 ITLRecovery CallManager	CallManager (Signer) ITLRecovery
10.5(2)	Token 1 (Signer) Token 2	CallManager (Signer) ITLRecovery
10.5(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
10.0(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
9.1(2)	Token 1 (Signer) Token 2	Not applicable

Migrate Phones from One Cluster to Another Cluster

Use the following procedure to migrate phones from one cluster to another. For example, from cluster 1 to cluster 2.

Procedure

Step 1 On cluster 2, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Find**.

Step 3 From the list of Certificates, click the ITLRecovery certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 4 From the list of Certificates, click the CallManager certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 5 On cluster 1, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 6 Click **Upload Certificate Chain** to upload the downloaded certificate.

Step 7 From the **Certificate Purpose** drop-down list, choose **Phone-SAST-trust**.

Step 8 For the **Upload File** field, click **Choose File**, browse to the ITLRecovery file that you downloaded in Step 3, and then click **Upload File**.

The uploaded ITLRecovery file appears for the **Phone-SAST-Trust** certificate on **Certificate List** window of cluster 1. If the new ITL file has a ITLRecovery certificate for cluster 2, run the command `show itl`.

Step 9 If the phones in cluster 1 have Locally Significant Certificates (LSC), then the CAPF certificate from cluster 1 has to be uploaded in the CAPF-trust store of cluster 2.

Step 10 (Optional) This step is applicable only if the cluster is in mixed mode. Run the **utils ctl update CTLFile** command on the CLI to regenerate the CTL file on cluster 1.

Note
- Run the `show ctl` CLI command to ensure that the ITLRecovery certificate and CallManager certificate of cluster 2 are included in the CTL file with the role as SAST.
- Ensure that the phones have received the new CTL and ITL files. The updated CTL file has the ITLRecovery certificate of cluster 2.

The phones that you want to migrate from cluster 1 to cluster 2 will now accept the ITLRecovery certificate of cluster 2.

Step 11 Migrate the phone from one cluster to another.

Migration from eToken-based CTL File to Tokenless CTL File

For the tokenless CTL file, administrators must ensure that the endpoints download the uploaded CTL file generated using USB tokens on Unified Communications Manager Release 12.0(1) or later. After the download, they can switch to tokenless CTL file. Then, they can run the `util ctl update` CLI command.

Update CTL File

Note This procedure is not required if you manage cluster security through the CLI command set **utils ctl**.

You must update the CTL file if the following scenarios occur. If you:

- Add a new Unified Communications Manager server to the cluster

Note To add a node to a secure cluster, see *Installing Unified Communications Manager*, which describes how to add a node and how to configure security for the new node.

- Change the name or IP address of a Unified Communications Manager server
- Change the IP address or hostname for any configured TFTP servers
- Change the IP address or hostname for any configured ASA firewall
- Enable the Cisco Certificate Authority Function service in Cisco Unified Serviceability
- Add or remove a security token
- Add or remove a TFTP server

- Add or remove a Unified Communications Manager server
- Add or remove an ASA firewall
- Manually regenerate CallManager, CAPF, or ITL Recovery certificate on any node on the Cisco Unified Communications Manager cluster that contains a CTL file, you must re-run the CTL wizard. This step is not required for the generation of other certificates.
- Update from a Unified Communications Manager version prior to 7.1.5 to a version 7.1.5 or later.
- Update from a Unified Communications Manager version prior to 10.5 to a version 10.5 or later, refer to the migration section from Hardware eTokens to Tokenless Solution.
- Upload a third-party, CA-signed certificate to the platform.

Note When a domain name is added or changed on a Unified Communications Manager cluster in mixed mode, you must update the CTL file for the phone configuration files to take effect.

Tip We strongly recommends that you update the file when minimal call-processing interruptions will occur.

Caution If Unified Communications Manager is integrated with Unity Connection 10.5 or later using secure SIP or SCCP, then the secure calls may stop working with Unity Connection. You must reset the corresponding port groups on Unity Connection to resolve this issue.

To reset the port group through the Unity Connection Administration interface, navigate to **Telephony Integrations** > **Port Group**, select the port group that you want to reset, and click **Reset** on the **Port Group Basics** page.

Update Cisco Unified Communications Manager Security Mode

You must use the Cisco CTL to configure the cluster security mode. You cannot change the Unified Communications Manager security mode from the Enterprise Parameters Configuration window in Unified Communications Manager Administration.

Note Cluster security mode configures the security capability for a standalone server or a cluster.

To change the cluster security mode after the initial configuration of the Cisco CTL Client, you must update the CTL file.

Procedure

Step 1 Run the CLI command `utils ctl set-cluster mixed-mode` to change the cluster security mode to secure.

Step 2 Run the CLI command `utils ctl set-cluster non-secure-mode` to change the cluster security mode to non-secure.

Cisco CTL File Details

Note You can set up encryption by using the **utils ctl** CLI command set, which does not require security tokens. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions.*

You can set the cluster security mode to nonsecure or mixed mode, as described in the following table. Only mixed mode supports authentication, encrypted signaling, and encrypted media.

Note Cluster security mode configures the security capability for a standalone server or a cluster.

Table 2: CTL Configuration Settings

Setting	Description
Unified Communications Manager Server	
Security Mode	
Set Unified Communications Manager Cluster to Mixed Mode	Mixed mode allows authenticated, encrypted, and nonsecure Cisco Manager. In this mode, Unified Communications Manager ensures t
Set Unified Communications Manager Cluster to Non-Secure Mode	If you configure nonsecure mode, all devices register as unauthenti image authentication only. When you choose this mode, the Cisco CTL Client removes the cer the CTL file still exists in the directory that you specified. The pho nonsecure with Unified Communications Manager. **Tip** To revert the phone to the default nonsecure mode, you Communications Manager servers.
CTL Entries	
Tokens	If you have not already done so, remove the token that you initially application prompts you to do so, insert the next token and click **OK** token displays, click **Add**. For all security tokens, repeat these tasks
Add TFTP Server	Click this button to add an Alternate TFTP server to the certificate t button after the Alternate TFTP Server tab settings display. After yo
Add Firewall	Click this button to add an ASA firewall to the certificate trust list. after the Firewall tab settings display. After you enter the settings, c

Verify Cisco Unified Communications Manager Security Mode

To verify the cluster security mode, perform the following procedure:

Note Cluster security mode configures the security capability for a standalone server or a cluster.

Procedure

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

Step 2 Locate the **Cluster Security Mode** field. If the value in the field displays as **1**, you correctly configured Unified Communications Manager for mixed mode. (Click the field name for more information.)

Tip You cannot configure this value in Unified Communications Manager Administration. This value displays after you configure the Cisco CTL Client.

Set Up Smart Card Service to Started or Automatic

If the Cisco CTL Client installation detects that the Smart Card service is disabled, you must set the Smart Card service to automatic and started on the server or workstation where you are installing the Cisco CTL Client plug-in.

Tip You cannot add the security tokens to the CTL file if the service is not set to started and automatic.

Tip After you upgrade the operating system, apply service releases, upgrade Cisco Unified Communications Manager, and so on, verify that the Smart Card service is started and automatic.

To set the service to started and automatic, perform the following procedure:

Procedure

Step 1 On the server or workstation where you installed the Cisco CTL Client, choose **Start** > **Programs** > **Administrative Tools** > **Services** or **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 From the Services window, right-click the **Smart Card** service and choose Properties.

Step 3 In the Properties window, verify that the **General** tab displays.

Step 4 From the Startup type drop-down list box, choose **Automatic**.

Step 5 Click **Apply**.

Step 6 In the Service Status area, click **Start**.

Step 7 Click **OK**.

Step 8 Reboot the server or workstation and verify that the service is running.

Verify or Uninstall Cisco CTL Client

Uninstalling the Cisco CTL Client does not delete the CTL file. Likewise, the cluster security mode and the CTL file do not change when you uninstall the client. If you choose to do so, you can uninstall the Cisco CTL using the CLI option.

To verify that the Cisco CTL Client installed, perform the following procedure:

Procedure

Step 1 Choose **Start** > **Control Panel** > **Add Remove Programs**.

Step 2 To verify that the client installed, locate **Cisco CTL Client**.

Step 3 To uninstall the client, click **Remove**.