



Cisco CTL Client Setup

This chapter provides information about Cisco CTL client setup.

- [About Cisco CTL Setup, on page 1](#)
- [Activate Cisco CTL Provider Service, on page 2](#)
- [Cisco CAPF Service Activation, on page 3](#)
- [Set up Secure Ports, on page 3](#)
- [Set Up Cisco CTL Client, on page 4](#)
- [Update CTL File, on page 5](#)
- [Update Cisco Unified Communications Manager Security Mode, on page 6](#)
- [Cisco CTL File Details, on page 7](#)
- [Verify Cisco Unified Communications Manager Security Mode, on page 8](#)
- [Set Up Smart Card Service to Started or Automatic, on page 9](#)
- [Verify or Uninstall Cisco CTL Client, on page 10](#)

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)
- Cisco CallManager and Cisco TFTP services that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TFTP server(s)
- ASA firewall
- ITLRecovery

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.

After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability on all nodes that run these services. 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 Manager 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.

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 Cisco TFTP 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 Cisco CTL 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 **Cisco CTL 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 Cisco CTL 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 Cisco CallManager 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:
- To change the Port Number parameter for the Cisco CTL Provider service, perform [Step 2, on page 4](#) through [Step 6, on page 4](#).
 - To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform [Step 7, on page 4](#) through [Step 11, on page 4](#).
- 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 Cisco CTL 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.
- Step 6** Click **Save**.
- Step 7** To change the Ethernet Phone Port or SIP Phone Secure Port settings, choose **System > Cisco Unified CM** in Unified Communications Manager Administration.
- Step 8** Find a server where the Cisco CallManager service runs, as described in the *Cisco Unified Communications Manager Administration Guide*; 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 Cisco CallManager 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; however, you must restart the TFTP services and then the CallManager services 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.
-

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.

- If you change the name or IP address of a Unified Communications Manager server
- If you change the IP address or hostname for any configured TFTP servers

- If you change the IP address or hostname for any configured ASA firewall
- If you enabled the Cisco Certificate Authority Function service in Cisco Unified Serviceability
- If you need to add or remove a security token
- If you need to add or remove a TFTP server
- If you need to add or remove a Unified Communications Manager server
- If you need to add or remove an ASA firewall
- If you restore a Unified Communications Manager server or Unified Communications Manager data
- If you 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.
- If you update from a Unified Communications Manager version prior to 7.1.5 to a version 7.1.5 or later.
- If you 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.
- After you 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 Cisco 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 1: CTL Configuration Settings

Setting	Description
Unified Communications Manager Server	
Security Mode	
Set Unified Communications Manager Cluster to Mixed Mode	<p>Mixed mode allows authenticated, encrypted, and nonsecure Cisco IP Phones to register with Unified Communications Manager. In this mode, Unified Communications Manager ensures that authenticated or encrypted devices use a secure port.</p> <p>Note Unified Communications Manager disables auto-registration if you configure mixed mode.</p>

Setting	Description
Set Unified Communications Manager Cluster to Non-Secure Mode	<p>If you configure nonsecure mode, all devices register as unauthenticated, and Unified Communications Manager supports image authentication only.</p> <p>When you choose this mode, the Cisco CTL Client removes the certificates for all entries that are listed in the CTL file, but the CTL file still exists in the directory that you specified. The phone requests unsigned configuration files and registers as nonsecure with Unified Communications Manager.</p> <p>Tip To revert the phone to the default nonsecure mode, you must delete the CTL file from the phone and all Unified Communications Manager servers.</p> <p>You can use auto-registration in this mode.</p>
CTL Entries	
Tokens	If you have not already done so, remove the token that you initially inserted into the server or workstation. When the application prompts you to do so, insert the next token and click OK . When the security token information for the additional 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 trust list. For information on the settings, click the Help button after the Alternate TFTP Server tab settings display. After you enter the settings, click Next .
Add Firewall	Click this button to add an ASA firewall to the certificate trust list. For information on the settings, click the Help button after the Firewall tab settings display. After you enter the settings, click Next .

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**.
-