CHAPTER 31

Configuring the Cisco CTL Client

This chapter contains information on the following topics:

Cisco CTL Client Overview

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) client on a single Windows workstation or server that has a USB port.

Note Supported Windows versions for Cisco CTL client include Windows 2000 and Windows XP. Do not use Terminal Services to install the Cisco CTL client. Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote troubleshooting and configuration tasks.

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

- Site Administrator Security Token (SAST)
- Cisco Unified CallManager and Cisco TFTP that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TLS proxy server such as a firewall

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 CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster. 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 display the certificate in the CTL client GUI.

When you configure a TLS proxy server in the CTL file, you can secure a Cisco PIX Firewall as part of a secure Cisco Unified CallManager system. The Cisco CTL client displays the firewall certificate as a “CCM” certificate.

Cisco Unified CallManager Administration uses an etoken to authenticate the TLS connection between the Cisco CTL client and provider.

Configuration Tips for Cisco CTL Client Configuration

Consider the following information when you configure the Cisco CTL client in Cisco Unified CallManager Administration:

- Ensure that Cisco Unified CallManager node hostnames are resolvable on the remote PC where the Cisco CTL client is installed, or the Cisco CTL client will not function correctly.
- You must activate the Cisco CTL Provider service on all servers in the cluster.
- When the Cisco CTL client contains entries for off-cluster servers, such as alternate or centralized TFTP server, you must also run the CTL Provider service on these servers.
- In the Alternate TFTP Server Tab Settings section of the CTL client GUI, alternate TFTP server designates a Cisco TFTP server that exists in a different cluster. Use these setting to configure alternate and centralized TFTP servers in the CTL client.

Note See "Cisco TFTP" for information about configuring off-cluster (alternate and centralized) TFTP servers by using TFTP service parameters.

- For centralized TFTP configurations, all off-cluster TFTP servers that are operating in mixed mode must add the Master TFTP server or Master TFTP server IP address to the off-cluster CTL file. The master TFTP server serves configuration files from all alternate TFTP servers in the alternate file list that is configured for the master TFTP server. All clusters in a centralized TFTP configuration do not need to use the same security mode; each cluster can select its own mode.
- After you create or update the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.

Cisco CTL Client Configuration Checklist

Table 31-1 provides a list of configuration tasks that you perform to install and configure the Cisco CTL client for the first time. See Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7, for more information about configuring the CTL file when you upgrade Cisco Unified CallManager.

Table 31-1 Cisco CTL Client Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	On each Cisco Unified CallManager in the cluster, activate the Cisco CTL Provider service in Cisco Unified CallManager Serviceability. **Tip** If you activated this service prior to a Cisco Unified CallManager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.	Activating the Cisco CTL Provider Service, page 31-4
Step 2	On the first node, activate the Cisco Certificate Authority Proxy service in Cisco Unified CallManager Serviceability. **Timesaver** Performing this task before you install and configure the Cisco CTL client ensures that you do not have to update the CTL file to use CAPF.	Activating the Certificate Authority Proxy Function Service, *Cisco Unified CallManager Security Guide, Release 5.0(4)*
Step 3	If you do not want to use the default settings, configure ports for the TLS connection. **Tip** If you configured these settings prior to a Cisco Unified CallManager upgrade, the settings migrate automatically.	Configuring Ports for the TLS Connection, page 31-5
Step 4	Obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the Cisco CTL client.	Configuring the Cisco CTL Client, page 31-8

Table 31-1 Cisco CTL Client Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Install the Cisco CTL client.	• System Requirements, page 30-4 • Installation, page 30-12 • Installing the Cisco CTL Client, page 31-6
Step 6	Configure the Cisco CTL client.	Configuring the Cisco CTL Client, page 31-8

Activating the Cisco CTL Provider Service

After you configure the Cisco CTL client, this service changes the cluster 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 Cisco Unified CallManager and Cisco TFTP servers.

If you activate the service and then upgrade Cisco Unified CallManager, Cisco Unified CallManager 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 CallManager Serviceability, choose **Tools > Service Activation**.

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

Step 3 Click the **Cisco CTL Provider** service radio button.

Step 4 Click **Save**.

Step 5 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 “Configuring Ports for the TLS Connection” in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

Step 6 Verify that the service runs on all servers in the cluster. In Cisco Unified CallManager Serviceability, choose **Tools > Control Center - Feature Services** to verify the state of the service.

Additional Information

See the “Related Topics” section on page 31-18.

Activating the Cisco CAPF Service

For information on activating this service, see the "Activating the Certificate Authority Proxy Function Service" section in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

Timesaver Performing this task before you install and configure the Cisco CTL client ensures that you do not have to update the CTL file to use CAPF.

Configuring Ports for the TLS Connection

You may have to configure a different port number if the 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 clusterwide security mode, saving the CTL file to TFTP servers, and retrieving a list of Cisco Unified CallManager and TFTP servers in the cluster.

The Ethernet Phone Port monitors registration requests from the SCCP phone. In nonsecure mode, the phone connects through port 2000. In mixed mode, the Cisco Unified CallManager port for TLS connection equals the value for the Cisco Unified CallManager port number added to (+) 443; therefore, the default TLS connection for Cisco Unified CallManager 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 Cisco Unified CallManager to listen for SIP messages from SIP phones. The default value equals 5061. If you change this port, you must restart the Cisco CallManager service in Cisco Unified CallManager Serviceability and reset the SIP phones.

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

You must open the CTL ports to the data VLAN from where the CTL client runs. Phones that are running TLS for signaling back to Cisco Unified CallManager also use the ports that the CTL client uses. Ensure that you open these ports to all VLANs where phones are configured for authenticated or encrypted status.

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 through Step 6.
- To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform Step 7 through Step 11.

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

Step 3 In the Server drop-down list box, 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 CallManager** in Cisco Unified CallManager Administration.

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

Step 9 After the Cisco Unified CallManager 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 CallManager Serviceability.

Step 11 Click **Save**.

Additional Information

See the "Related Topics" section on page 31-18.

Installing the Cisco CTL Client

You must use the client and update the CTL file when the following events occur:

- The first time you set the security mode of the cluster
- The first time you create the CTL file
- After the Cisco Unified CallManager installation
- After you restore a Cisco Unified CallManager server or Cisco Unified CallManager data
- After you change the IP address or hostname of the Cisco Unified CallManager server
- After you add or remove a security token, TFTP server, PIX firewall, or Cisco Unified CallManager server
- After you upload a third-party, CA-signed certificate to the platform

Tip If the Smart Card service is not set to started and automatic on the server or workstation where you plan to install the client, the installation fails.

To install the Cisco CTL client, perform the following procedure:

Procedure

Step 1 From the Windows workstation or server where you plan to install the client, browse to Cisco Unified CallManager Administration, as described in the *Cisco Unified CallManager Administration Guide*.

Step 2 In Cisco Unified CallManager Administration, choose **Application > Plugins.**

The Find and List Plugins window displays.

Step 3 From the Plugin Type equals drop-down list box, choose **Installation** and click **Find**.

Step 4 Locate the Cisco CTL Client.

Step 5 To download the file, click **Download** on the right side of the window, directly opposite the Cisco CTL Client plug-in name.

Step 6 Click **Save** and save the file to a location that you will remember.

Step 7 To begin the installation, double-click **Cisco CTL Client** (icon or executable depending on where you saved the file).

Note You can also click **Open** from the Download Complete box.

Step 8 The version of the Cisco CTL client displays; click **Continue**.

Step 9 The installation wizard displays. Click **Next**.

Step 10 Accept the license agreement and click **Next**.

Step 11 Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click **Next**.

Step 12 To begin the installation, click **Next**.

Step 13 After the installation completes, click **Finish**.

Additional Information

See the "Related Topics" section on page 31-18.

Upgrading the Cisco CTL Client and Migrating the Cisco CTL File

If you want to make changes to the CTL file after a Cisco Unified CallManager Release 5.0 to 5.1 upgrade, you must uninstall the Cisco CTL client that you installed prior to the upgrade, install the latest Cisco CTL client, as described in the "Installing the Cisco CTL Client" section on page 31-6, and regenerate the CTL file. If you did not remove or add any servers before the Cisco Unified CallManager upgrade, you do not need to reconfigure the Cisco CTL client after the upgrade. The Cisco Unified CallManager upgrade automatically migrates the data in the CTL file.

When you upgrade from a 4.x release to a 5.x release and security is enabled on the cluster, you must uninstall the Cisco CTL client that you installed prior to the upgrade, install the latest Cisco CTL client, and regenerate the CTL file. Follow this procedure to enable security on the upgraded cluster:

Procedure

Step 1 Uninstall the existing Cisco CTL client.

Step 2 Install the new Cisco CTL client as described in the "Installing the Cisco CTL Client" section on page 31-6.

Step 3 Run the Cisco CTL client by using at least one of the previously used USB keys, as described in "Configuring the Cisco CTL Client" section on page 31-8.

Step 4 Restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.

Additional Information

See the "Related Topics" section on page 31-18.

Configuring the Cisco CTL Client

Tip Configure the Cisco CTL client during a scheduled maintenance window because you must restart the Cisco Unified CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.

The Cisco CTL client performs the following tasks:

- Sets the Cisco Unified CallManager cluster security mode.

  Tip You cannot set the Cisco Unified CallManager clusterwide parameter to mixed mode through the Enterprise Parameters window of Cisco Unified CallManager Administration. You must configure the CTL client to set the clusterwide mode. For more information, see the "Cisco CTL Client Configuration Settings" section on page 31-12.

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

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

  The security tokens that you insert during the configuration sign the CTL file.

Before You Begin

Tip See Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7 for more information about configuring the CTL file when you upgrade Cisco Unified CallManager.

Before you configure the Cisco CTL client, verify that you activated the Cisco CTL Provider service and the Cisco Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability. Obtain at least two security tokens; the Cisco certificate authority issues these security tokens. The security tokens must come from Cisco. You will insert the tokens one at a time into the USB port on the server/workstation. If you do not have a USB port on the server, you may use a USB PCI card.

Obtain the following passwords, hostnames/IP addresses, and port numbers:

- Administrative username and password for Cisco Unified CallManager
- Security token administrative password
- Administrative username and password for the PIX firewall

See Table 31-2 for a description of the preceding information.

Tip Before you install the Cisco CTL client, verify that you have network connectivity to each server in the cluster. To ensure that you have network connectivity to all servers in the cluster, issue a ping command, as described in the *Cisco Unified Communications Operating System Administration Guide*.

If you installed multiple Cisco CTL clients, Cisco Unified CallManager only accepts CTL configuration information on one client at a time, but you can perform configuration tasks on up to five Cisco CTL clients simultaneously. While you perform configuration tasks on one client, Cisco Unified CallManager automatically stores the information that you entered on the other clients.

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

- Writes the CTL file to all Cisco Unified CallManager servers in the cluster.
- Writes CAPF capf.cer to all Cisco Unified CallManager subsequent nodes (not first node) in the cluster.
- Writes CAPF certificate file in PEM format to all Cisco Unified CallManager subsequent nodes (not first node) in the cluster.
- Writes the file to all configured TFTP servers
- Writes the file to all configured PIX 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.

To configure the client, perform the following procedure:

Procedure

Step 1 Obtain at least two security tokens that you purchased.

Step 2 Perform one of the following tasks:

- Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.
- Choose **Start > Programs > Cisco CTL Client**.

Step 3 Enter the configuration settings for the Cisco Unified CallManager server, as described in Table 31-2; click **Next**.

Step 4 Click **Set Cisco Unified CallManager Cluster to Mixed Mode**, as described in Table 31-2; click **Next**.

Step 5 Perform the following tasks, depending on what you want to accomplish:

- To add a security token, see Step 6 through Step 12.

- To complete the Cisco CTL client configuration, see Step 17 through Step 21.

Caution You need a minimum of two security tokens the first time that you configure the client. Do not insert the tokens until the application prompts you to do so. If you have two USB ports on the workstation or server, do not insert two security tokens at the same time.

Step 6 When the application prompts you to do so, insert one security token in an available USB port on the workstation or server where you are currently configuring the Cisco CTL client; click **OK**.

Step 7 The security token information displays for the token that you inserted; click **Add**.

Step 8 The detected certificate entries display in the pane.

Step 9 To add other security token(s) to the certificate trust list, click **Add Tokens**.

Step 10 If you have not already done so, remove the token that you inserted into the server or workstation. When the application prompts you to do so, insert the next token and click **OK**.

Step 11 The security token information for the second token displays; click **Add**.

Step 12 For all security tokens, repeat Step 9 through Step 11.

Step 13 The certificate entries display in the pane.

Step 14 Enter the configuration settings, as described in Table 31-2.

Step 15 Click **Next**.

Step 16 Enter the configuration settings, as described in Table 31-2; click **Next**.

Step 17 When you have added all security tokens and servers, click **Finish**.

Step 18 Enter the username password for the security token, as described in Table 31-2; click **OK**.

Step 19 After the client creates the CTL file, a window displays the server, file location, and status of the CTL file on each server. Click **Finish**.

Step 20 Reset all devices in the cluster. See the "Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster" section on page 30-10.

Step 21 In Cisco Unified CallManager Serviceability, restart the Cisco Unified CallManager and Cisco TFTP services on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.

Step 22 After you create the CTL file, you may remove the security token from the USB port. Store all security tokens in a safe place that you will remember.

Additional Information

See the "Related Topics" section on page 31-18.

Updating the CTL File

You must update the CTL file if the following scenarios occur:

- If you add a new Cisco Unified CallManager server to the cluster
- If you change the name or IP address of the Cisco Unified CallManager server in the cluster
- If you change the IP address or hostname for any configured TFTP servers or PIX firewall

- If you enabled the Cisco Certificate Authority Function service in Cisco Unified CallManager Serviceability
- If you need add or remove a security token, TFTP server, PIX firewall, or Cisco Unified CallManager server
- If you restore a Cisco Unified CallManager server or Cisco Unified CallManager data
- After you upload a third-party, CA-signed certificate to the platform

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

To update the information that exists in CTL file, perform the following procedure:

Procedure

Step 1 Obtain one security token that you inserted to configure the latest CTL file.

Step 2 Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.

Step 3 Enter the configuration settings for the Cisco Unified CallManager server, as described in Table 31-2; click **Next**.

Tip You make updates in this window for the Cisco Unified CallManager server.

Step 4 To update the CTL file, click **Update CTL File**, as described in Table 31-2; click **Next**.

Caution For all CTL file updates, you must insert one security token that already exists in the CTL file into the USB port. The client validates the signature of the CTL file through this token. You cannot add new tokens until the CTL client validates the signature. If you have two USB ports on the workstation or server, do not insert both security tokens at the same time.

Step 5 If you have not already inserted one security token in an available USB port on the workstation or server where you are currently updating the CTL file, insert one of the security tokens; click **OK**.

Step 6 The security token information displays for the token that you inserted; click **Next**.

The detected certificate entries display in the pane.

Tip You cannot update the Cisco Unified CallManager or Cisco TFTP entries from this pane. To update the Cisco Unified CallManager entry, click **Cancel** and perform Step 2 through Step 6 again.

Step 7 To update existing Cisco CTL entries or to add or delete security tokens, consider the following information:

- To update servers settings or to add new security tokens, see "Configuring the Cisco CTL Client" section on page 31-8.

- To delete a security token, see the "Deleting a CTL File Entry" section on page 31-12.

Additional Information

See the "Related Topics" section on page 31-18.

Deleting a CTL File Entry

At any time, you can delete some CTL entries that display in the CTL Entries window of the Cisco CTL client. After you open the client and follow the prompts to display the CTL Entries window, highlight the item to delete and click **Delete Selected** to delete the entry.

You cannot delete servers that run Cisco Unified CallManager, Cisco TFTP, PIX firewall, or Cisco CAPF from the CTL file.

Two security token entries must exist in the CTL file at all times. You cannot delete all security tokens from the file.

Additional Information

See the "Related Topics" section on page 31-18.

Updating the Clusterwide Security Mode

You must use the Cisco CTL client to configure the clusterwide security mode. You cannot change the clusterwide security mode from the Enterprise Parameters window in Cisco Unified CallManager Administration.

To change the clusterwide security mode after the initial configuration of the Cisco CTL client, you must update the CTL file. Navigate to the Cluster Security Mode window, change the mode setting, and click **Next**, then **Finish**, as described in the "Updating the CTL File" section on page 31-10 and Table 31-2.

If you change the clusterwide security mode from mixed to nonsecure mode, the CTL file still exists on the servers in the cluster, but the CTL file does not contain any certificates. Because no certificates exist in the CTL file, the phone requests an unsigned configuration file and registers as nonsecure with Cisco Unified CallManager.

Cisco CTL Client Configuration Settings

The cluster can exist in one of two modes, as described in Table 31-2. Only mixed mode supports authentication. When you configure the Cisco CTL client for authentication, you must choose Set Cisco Unified CallManager Cluster to Mixed Mode.

Use Table 31-2 to configure the Cisco CTL client for the first time, to update the CTL file, or to change the mode from mixed to nonsecure.

- For configuration tips, see the "Configuration Tips for Cisco CTL Client Configuration" section on page 31-2.
- For related information and procedures, see the "Related Topics" section on page 31-18.

Table 31-2 Configuration Settings for CTL Client

Setting	Description
Cisco Unified CallManager Server	
Hostname or IP Address	Enter the hostname or IP address for the first node.
Port	Enter the port number, which equals the CTL port for the Cisco CTL Provider service that runs on the specified Cisco Unified CallManager server. The default port number equals 2444.
Username and Password	Enter the same username and password that has administrative privileges on the first node.
Security Mode Radio Buttons	
Set Cisco Unified CallManager Cluster to Mixed Mode	Mixed mode allows authenticated or encrypted Cisco Unified IP Phones and nonauthenticated Cisco Unified IP Phones to register with Cisco Unified CallManager. In this mode, Cisco Unified CallManager ensures that authenticated or encrypted devices use a secure port. **Note** Cisco Unified CallManager disables auto-registration if you configure the cluster for mixed mode.
Set Cisco Unified CallManager Cluster to Non-Secure Mode	All devices register as unauthenticated with Cisco Unified CallManager, and Cisco Unified CallManager supports image authentication only. When you choose this mode, the 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 Cisco Unified CallManager. **Tip** To revert the phone to the default nonsecure mode, you must delete the CTL file from the phone and all Cisco Unified CallManager servers. You can use auto-registration in this mode.
Update CTL File	After you have created the CTL file, you must choose this option to make any changes to the CTL file. Choosing this option ensures that the Cluster Security mode does not change.
CTL Entries Radio Buttons	
Add Tokens	Click this button to add additional security token(s) to the certificate trust list. 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.

Table 31-2 Configuration Settings for CTL Client (continued)

Setting	Description
Add Firewall	Click this button to add a firewall (TLS proxy server) 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.
Alternate TFTP Server	
Hostname or IP Address	Enter the hostname or IP address for the TFTP server. Alternate TFTP server designates a Cisco TFTP server that exists in a different cluster. If you use two different clusters for the alternate TFTP server configuration, both clusters must use the same clusterwide security mode, which means that you must install and configure the Cisco CTL client in both clusters. Likewise, both clusters must run the same version of Cisco Unified CallManager. Ensure that the path in the TFTP service parameter, FileLocation, is the same for all servers in the cluster.
Port	Not required with this release of Cisco Unified CallManager.
Username and Password	Not required with this release of Cisco Unified CallManager.
TLS Proxy Server	
Hostname or IP Address	Enter the hostname or IP address for the TLS proxy.
Port	Enter the port number, which equals the CTL port for the Cisco CTL Provider service that runs on the firewall. The default port number equals 2444.
Username and Password	Enter the same username and password that has administrative privileges on the first node.
Security Token	
User Password	The first time that you configure the Cisco CTL client, enter **Cisco123**, the case-sensitive default password, to retrieve the private key of the certificate and ensure that the CTL file gets signed.

Verifying the Security Mode for the Cisco Unified CallManager Cluster

To verify the security mode for the Cisco Unified CallManager cluster, perform the following procedure:

Procedure

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

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

Tip You cannot configure this value in Cisco Unified CallManager Administration. This value displays after you configure the Cisco CTL client.

Additional Information

See the "Related Topics" section on page 31-18.

Setting the Smart Card Service to Started and 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 plug-in.

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

After you upgrade the operating system, apply service releases, upgrade Cisco Unified CallManager, 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.

Additional Information

See the "Related Topics" section on page 31-18.

Changing the Security Token Password (Etoken)

This administrative password retrieves the private key of the certificate and ensures that the CTL file gets signed. Each security token comes with a default password. You can change the security token password at any time. If the Cisco CTL client prompts you to change the password, you must change the password before you can proceed with the configuration.

To review pertinent information on setting passwords, click the **Show Tips** button. If you cannot set the password for any reason, review the tips that display.

To change the security token password, perform the following procedure:

Procedure

Step 1 Verify that you have installed the Cisco CTL client on a Windows server or workstation.

Step 2 If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL client.

Step 3 Choose **Start > Programs > etoken > Etoken Properties**; right-click **etoken** and choose **Change etoken password**.

Step 4 In the Current Password field, enter the password that you originally created for the token.

Step 5 Enter a new password.

Step 6 Enter the new password again to confirm it.

Step 7 Click **OK**.

Additional Information

See the "Related Topics" section on page 31-18.

Deleting the CTL File on the Cisco Unified IP Phone

Caution Cisco recommends that you perform this task in a secure lab environment, especially if you do not plan to delete the CTL file from the Cisco Unified CallManager servers in the cluster.

Delete the CTL file on the Cisco Unified IP Phone if the following cases occur:

- You lose all security tokens that signed the CTL file.
- The security tokens that signed the CTL file appear compromised.

- You move a phone out of a secure cluster; for example, to a storage area, to a nonsecure cluster, or to another secure cluster in a different domain.
- You move a phone from an area with an unknown security policy to a secure cluster.
- You change the alternate TFTP server address to a server that does not exist in the CTL file.

To delete the CTL file on the Cisco Unified IP Phone, perform the tasks in Table 31-3.

Table 31-3 Deleting the CTL File on the Cisco Unified IP Phone

Cisco Unified IP Phone Model	Tasks
Cisco Unified IP Phones 7960 and 7940	Under the Security Configuration menu on the phone, press **CTL file**, **unlock** or ****#**, and **erase**.
Cisco Unified IP Phone 7970	Perform one of the following methods: • Unlock the Security Configuration menu, as described in *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*. Under the CTL option, press the **Erase** softkey. • Under the Settings menu, press the **Erase** softkey. **Note** Pressing the Erase softkey under the Settings menu deletes other information besides the CTL file. For additional information, refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager.*

Additional Information

See the "Related Topics" section on page 31-18.

Determining the Cisco CTL Client Version

To determine which version of the Cisco CTL client you are using, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Double-click the **Cisco CTL Client** icon that exists on the desktop.
- Choose **Start > Programs > Cisco CTL Client**.

Step 2 In the Cisco CTL client window, click the icon in the upper, left corner of the window.

Step 3 Choose **About Cisco CTL Client**. The version of the client displays.

Additional Information

See the "Related Topics" section on page 31-18.

Verifying or Uninstalling the Cisco CTL Client

Uninstalling the Cisco CTL client does not delete the CTL file. Likewise, the clusterwide security mode and the CTL file do not change when you uninstall the client. If you choose to do so, you can uninstall the CTL client, install the client on a different Windows workstation or server, and continue to use the same CTL file.

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

Procedure

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

Step 2 Double-click **Add Remove Programs**.

Step 3 To verify that the client installed, locate **Cisco CTL Client**.

Step 4 To uninstall the client, click **Remove**.

Additional Information

See the "Related Topics" section on page 31-18.

Where to Find More Information

Related Topics

- System Requirements, page 30-4
- Cisco CTL Client Overview, page 31-2
- Cisco CTL Client Configuration Checklist, page 31-3
- Activating the Cisco CTL Provider Service, page 31-4
- Activating the Cisco CAPF Service, page 31-5
- Configuring Ports for the TLS Connection, page 31-5
- Installing the Cisco CTL Client, page 31-6
- Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7
- Configuring the Cisco CTL Client, page 31-8
- Updating the CTL File, page 31-10
- Deleting a CTL File Entry, page 31-12
- Updating the Clusterwide Security Mode, page 31-12
- Cisco CTL Client Configuration Settings, page 31-12
- Verifying the Security Mode for the Cisco Unified CallManager Cluster, page 31-15
- Setting the Smart Card Service to Started and Automatic, page 31-15
- Deleting the CTL File on the Cisco Unified IP Phone, page 31-16
- Determining the Cisco CTL Client Version, page 31-17
- Verifying or Uninstalling the Cisco CTL Client, page 31-18

- Using the Certificate Authority Proxy Function, *Cisco Unified CallManager Security Guide, Release 5.0(4)*

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

Troubleshooting Guide for Cisco Unified CallManager