Proxy TFTP Server

The Cisco Proxy TFTP Server allows all the endpoints in a large-scale deployment to download the configuration file and get registered to the Cisco Unified Communications Manager.

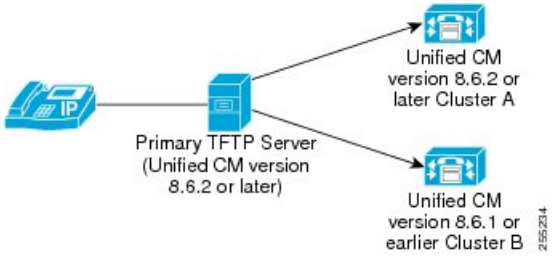
Cisco Proxy TFTP Server Deployment Models

Cisco Proxy TFTP Server supports two deployment models.

Cisco Proxy TFTP Server Deployment Model 1

For the deployment model illustrated in the following figure, the Primary TFTP Server should have Unified CM version 8.6 (2) or later.

Figure 1: Cisco Proxy TFTP Server Deployment Model 1



The two remote clusters, Cluster A and Cluster B, are configured to the Primary TFTP Server. However, you can configure any number of remote clusters to the Primary TFTP Server. Whenever an endpoint sends a request for configuration file, the Primary TFTP Server looks into the local cache and the configured remote

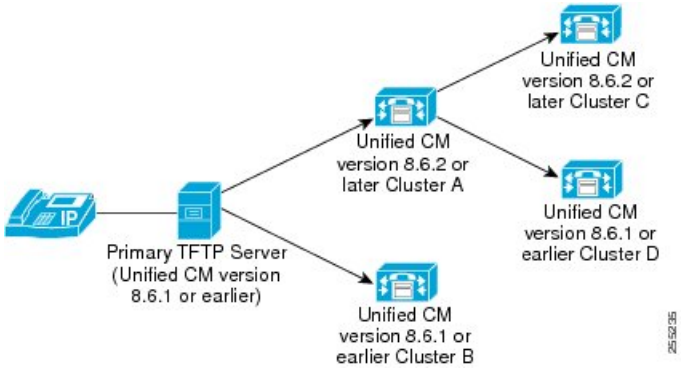
clusters. So, an endpoint that is configured to the Primary TFTP Server Cluster, Cluster A, and Cluster B can retrieve the configuration file and register to the Cisco Unified Communications Manager.

Note Cisco recommends that you use deployment model 1 for better system performance. However, if you do not wish to change your existing Centralized TFTP (8.6 (1) or earlier), you can use deployment model 2.

Cisco Proxy TFTP Server Deployment Model 2

In the deployment model illustrated in the following figure, the centralized Unified CM TFTP server acts as a Primary TFTP server.

Figure 2: Cisco Proxy TFTP Server Deployment Model 2



The two remote clusters - Cluster A and Cluster B have been configured to the Primary TFTP Server. However, you can configure any number of remote clusters to the Primary TFTP Server. Two more remote clusters have been added to the Cluster A. Whenever an endpoint sends a request for configuration file, the Primary TFTP Server looks into the local cache and the configured remote clusters (Cluster A and Cluster B). Cluster A further looks into its configured remote clusters (Cluster C and Cluster D). Thus, all the endpoints configured to the Primary TFTP Server Cluster, Cluster A, Cluster B, Cluster C and Cluster D can get the configuration file and get registered to the Cisco Unified Communications Manager.

Use Cases and Best Practices

Consider the following scenarios that detail how Proxy TFTP can be used and the best practices for implementation.

1. The cluster can act as just a proxy TFTP cluster with no other purpose. In this case, the cluster has no relationship with the other clusters, and does not process calls. For this scenario, the Remote Cluster TFTP is manually defined and rollback to pre-8.0 is recommended.

Note Autoregistration will not work in this scenario.

2. The cluster is a remote cluster that is also acting as a Proxy TFTP server for remote clusters. The remote cluster is manually defined, and Autoregistration should not be enabled.

TFTP Setup

Cisco Proxy TFTP Server can be configured manually as well as dynamically. This section provides configuration procedures for TFTP.

Set Up TFTP Manually

Follow this procedure to configure Cisco Proxy TFTP Server manually in your network.

Procedure

Step 1 Create a new cluster.
a) In Cisco Unified Communications Manager Administration, choose **Advanced Features > Cluster View**.
b) Enter the **Cluster Id** and **Fully Qualified Domain Name**.

Step 2 Check the **Enable** check box for the TFTP service.

Step 3 Click **TFTP** hyperlink.

The Remote Cluster Manually Override Configuration window appears.

Step 4 Choose **Manually Configure Remote Service addresses**.

Step 5 Enter IP addresses for the TFTP servers of the remote clusters.

Step 6 Click **Save**.

Set Up TFTP Dynamically

Perform the following steps to dynamically configure Cisco Proxy TFTP Server in your network.

- Configure EMCC.
- In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **Cluster View** > **Update Remote Cluster Now**.

Proxy TFTP Server and Centralized TFTP Server

For large scale deployments, the Centralized TFTP server has the following limitations:

- Sometimes, endpoints are unable to download the configuration file because the primary TFTP server takes more time to get the configuration file from the alternate TFTP servers. By the time the primary TFTP server gets the file, the endpoints get timed out. As a result, endpoints never get registered to their Unified CM.
- Only 10 alternate TFTP servers can be added.

These limitations are not applicable to Cisco Proxy TFTP Server.

Note When a phone requests a common file from a central or proxy TFTP server and that file has a common name such as `ringlist.xml.sgn` or is a locale file, the TFTP server sends its own local copy of the file instead of the file from the home cluster of the phone. The phone rejects the file due to a signature verification failure because the file has the signature of the TFTP server's local cluster, which does not match the Initial Trust List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the phone or perform the bulk certificate export procedure to make the Trust Verification System (TVS) return a success when the phone verifies a signature from a different cluster. See the procedure in the "Default Security Setup" section of the *Cisco Unified Communications Manager Security Guide* for performing a bulk certificate export when migrating IP phones between clusters to perform the bulk certificate export. To disable Security by Default, see the procedure to update the ITL file for IP Phones in the *Cisco Unified Communications Manager Security Guide*.

Phone Behavior with Proxy TFTP Server

For phones configured to remote clusters, first-time phone registration may take a few minutes. The time delay is due to Proxy TFTP Server searching for the configuration file in the remote clusters. The delay will vary based on the number of end points and the number of remote clusters configured. However, subsequent registrations will not have any delay.

Cisco Proxy TFTP Server System Requirements

The following system requirements exist for Cisco Proxy TFTP Server:

- Cisco Unified Communications Manager, Release 8.6 (2) or higher
- Cisco TFTP service - should be activated and in running state

Cisco Proxy TFTP Server Interactions and Restrictions

This section provides the details of interactions and restrictions for Cisco Proxy TFTP Server.

Cisco Proxy TFTP Server Interactions

Cisco TFTP service of the Proxy TFTP server interacts with the TFTP services of the remote clusters. In the Cluster View window (**Advanced Features > Cluster View**), for a particular remote cluster, TFTP service can have a maximum of three IP addresses, and Proxy TFTP server will interact with all three IP addresses if they are configured.

Note You must ensure that the Cisco TFTP service is active and in running state on the configured IP addresses.

When a phone requests a common file from a central or proxy TFTP server and that file has a common name such as `ringlist.xml.sgn` or is a locale file, the TFTP server sends its own local copy of the file instead

of the file from the home cluster of the phone. The phone rejects the file due to a signature verification failure because the file has the signature of the TFTP server's local cluster, which does not match the Initial Trust List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the phone or perform the bulk certificate export procedure to make the Trust Verification System (TVS) return a success when the phone verifies a signature from a different cluster. See the procedure in the "Default Security Setup" section of the *Cisco Unified Communications Manager Security Guide* for performing a bulk certificate export when migrating IP phones between clusters to perform the bulk certificate export. To disable Security by Default, see the procedure to update the ITL file for IP Phones in the *Cisco Unified Communications Manager Security Guide*.

Cisco Proxy TFTP Server Restrictions

This section describes the restrictions and limitations of the Cisco Proxy TFTP Server with other Cisco Unified Communications Manager Administration components.

Phones Unable to Register with Cluster

Follow these steps if phones in your cluster are no longer able to register correctly with the cluster.

1. Verify that full security mesh is established between the home and Proxy TFTP clusters:
   a. Perform a bulk import of the CallManager certificates from the Proxy TFTP server to the home cluster.
   b. Perform a bulk import of the CallManager certificates from the home clustser to the Proxy TFTP server.
2. On the home cluster, keep the **Prepare Cluster for Rollback to pre 8.0** set to **False**. This makes sure that phones will have Security by Default (SBD) enabled during normal operation.
3. On the Proxy TFTP cluster, set the **Prepare Cluster for Rollback to pre 8.0** to **False**. This step makes sure that SBD is enabled on the Proxy TFTP server as well.

Caution When the Proxy TFTP cluster is set up, do not remove the cluster view configuration from the Proxy TFTP configuration. Removing the cluster view from the Proxy TFTP configuration can result in phones receiving a 404 file not found error, which sends the phones a default ITL file from the Proxy TFTP server. This scenario requires that the ITL files be manually deleted from the phones to correctly register back to the home cluster.

Registration Problems for Phones with SBD Loads for Previous Versions of Cisco Unified Communications Manager 8.0

For remote cluster TFTP servers that are running on Cisco Unified Communications Manager 8.0 and later, the phones with SBD load can register to these remote cluster Unified Communications Managers through a Proxy TFTP server. However, for the remote cluster TFTP servers that running on a version that is earlier than Cisco Unified Communications Manager 8.0, the phones with SBD load are unable to register to the remote cluster Unified Communications Managers through a Proxy TFTP server, because the Identity Trust List (ITL) file is unavailable in versions that are earlier than Unified Communications Manager 8.0.

Use the following procedure to resolve this problem.

1. Connect the endpoint directly to the remote cluster Unified Communications Manager:
   a. Disable the DHCP option.

b. Enter the TFTP IP address on the phone manually.

The phone gets the required SBD load and registers to the Unified Communications Manager.

2. Enable the DHCP option and reset the phone manually.

The phone gets registered to the remote cluster through Proxy TFTP.

Note This procedure is applicable only if you have new phones with SBD load or if you plan to move the phones from a Unified Communications Manager with SBD support to a Unified Communications Manager without SBD support. This procedure is not applicable if the number of phones in a cluster is large.

Problems When You Move a Device From One Remote Cluster to Another

When you move a device from one cluster to another, the device may lose its trusted status. For a secure cluster, you must re-run the CTL Client.

The following procedures show actions you can take to restore the trusted status for devices in various deployments:

10.0 Proxy TFTP deployments

1. Export the TFTP certificate from the Proxy TFTP.
2. Import the certificate to all the slave SBD-aware clusters.
3. Add the TFTP certificate from the Proxy TFTP to the CTL file for all of the mixed-mode 7.x slave clusters.

8.6 and 9.0 Proxy TFTP deployments

1. If the Proxy TFTP is not on the highest release, export the locale and ring list files from the cluster with the highest Unified Communications Manager release.
2. Import the TFTP certificate from the Proxy TFTP to all the SBD-aware slave clusters.
3. Add the TFTP certificate from the Proxy TFTP to the CTL file of all the mixed-mode 7.x slave clusters.

8.0 and 8.5 Centralized TFTP deployments

1. If the Centralized TFTP is not on the highest release, export the locale and ring list files from the cluster with the highest Unified Communications Manager release.
2. Import the TFTP certificate from the Centralized TFTP to all the slave SBD aware clusters.
3. Add the TFTP certificate form the Centralized TFTP in the CTL Files of all the mixed-mode 7.x slave clusters.

The following procedures detail the best practices for successfully moving endpoints between clusters.

Move Endpoints From an 8.0+ Cluster to a Cluster with a CTL File

Note If the second cluster is in mixed mode, the first cluster must have a CTL file.

1. Run the CTL client if needed (with desired cluster security mode).
2. If the two clusters have CTL files signed by USB eTokens that are trusted by endpoints in both clusters, no action is required; go to Step 4.
3. Physically ship the USB eTokens from the second cluster to the first cluster and add the USB eTokens in the CTL file of the first cluster.
4. Point the endpoints in the first cluster to the second cluster, for example, through DHCP.

Move Endpoints From a 7.x Cluster with a CTL File to Another Cluster with a CTL File

1. If the two clusters have CTL files that are signed by trusted USB eTokens in both clusters, no action is required; go to Step 3.
2. Physically ship the USB eTokens from the second cluster to the first cluster and add the USB eTokens in the CTL file of the first cluster.
3. Point the endpoints in the first cluster to the second cluster, for example, through DHCP.

Moving Endpoints From an 8.0+ Cluster with a CTL File to Another Cluster

1. If the two clusters have CTL files that are signed by trusted USB eTokens in both clusters, no action is required.
2. Physically ship the USB eTokens from the second cluster to the first cluster and add the USB eTokens in the CTL file of the first cluster.

Phones Take Time to Register While Upgrading the Remote Cluster

When a remote cluster is upgraded, phones request the new load file, which must be downloaded to the Proxy TFTP local cache. If you plug in an Ethernet cable to a phone and then set up the phone on the Unified Communications Manager, the phone takes about 30 minutes to register. However, if you set up the phone on the Unified Communications Manager and then plug in the Ethernet cable, the phone is registered immediately.

Proxy TFTP and Security

Endpoints in a Cisco Unified Communications Manager cluster are configured with Proxy TFTP (for example, through Dynamic Host Configuration Protocol, or DHCP). Proxy TFTP can find the target cluster of the endpoint.

Note It is recommended that you keep the Proxy TFTP on the current release while you upgrade the rest of the clusters, as well as have a combination of nonsecure and mixed-mode clusters.

The Proxy TFTP server does not have to be on the highest Unified Communications Manager release, and clusters in a Proxy TFTP deployment can be either nonsecure or in mixed-mode.

Proxy TFTP can find the target cluster of endpoints because the MAC address of the endpoints is part of the filename in the TFTP GET request (for example, `SEP001956A3A472.cnf.xml.sgn`). Proxy TFTP discovers the target in the following way:

1. Proxy TFTP polls all the clusters that it controls for the requested file, starting from its own database.
2. The cluster where the endpoint is configured returns the file.
3. The locale and ring list file requests do not contain a MAC address, so Proxy TFTP returns its own copies of these files.

Note The locale and ring list files are backward compatible for Unified Communications Manager releases.

When Security-by-Default (SBD) was introduced for Unified Communications Manager, Proxy TFTP (and TFTP servers in general) served both signed and nonsigned requests.

If the home cluster of an endpoint does not accept the ITL file request, the endpoint requests a default ITL file which the Proxy TFTP serves. After the endpoint receives the configuration file from its home cluster, the endpoint cannot validate the signature, because the endpoint has the ITL file from the Proxy TFTP and not its home cluster.

10.0(1) Proxy TFTPs perform the following steps for signing files and serving them to endpoints:

- Automatically discover the cluster in the deployment that is on the highest release
- Get the locale and ring list files from the cluster
- Strip the signature of the locale or ring list file
- Sign the files with their own TFTP private key before serving them to endpoints that are requesting the files

Cisco Proxy TFTP Server Installation and Activation

After you install Cisco Unified Communications Manager, your network can support the Cisco Proxy TFTP Server feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the TFTP Setup, on page 3

Remote Cluster Settings

In Cisco Unified Communications Manager Administration, use the **Advanced Features > Cluster View** menu path to configure remote clusters.

Tips About Finding Remote Clusters

The Find operation locates only those remote clusters that you added previously. The Find operation does not locate the clusters that belong to the enterprise automatically.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Navigating the Cisco Unified Communications Manager Administration Application" section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

The following table provides detailed descriptions of the remote cluster settings that you configure in the Cluster View window (**Advanced Features > Cluster View**).

Table 1: Remote Cluster Settings

Field	Description
Remote Cluster Information	
Cluster Id	Enter the cluster ID of the remote cluster. Valid values include alphanumeric characters, period (.), and hyphen (-).
Description	Enter a description for the remote cluster. This field accepts up to 128 characters. You may use any character except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), dash (-), ampersand (&), and percent sign (%).
Fully Qualified Name	Enter the fully qualified name of the remote cluster/IP address. This field accepts up to 50 characters and allows the following characters: alphanumeric (a through z, A through Z, and 0 through 9), period (.), dash (-), asterisk (*), and space ( ).
Remote Cluster Service Information	

Field	Description
EMCC	For the EMCC service, the following column headings detail the configuration for this service: • Enabled—If the EMCC service is enabled, this box gets checked. • Service—This entry specifies the EMCC service. • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
PSTN Access	For the PSTN access, the following column headings detail the configuration for this service: • Enabled—If the PSTN access is enabled, this box gets checked. • Service—This entry specifies the PSTN access • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.

Field	Description
RSVP Agent	For the RSVP agent, the following column headings detail the configuration for this service: • Enabled—If the RSVP agent is enabled, this box gets checked. • Service—This entry specifies the RSVP agent • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.

Field	Description
TFTP	For the TFTP service, the following column headings detail the configuration for this service: • Enabled—If the TFTP service is enabled, this box gets checked. • Service—This entry specifies the EMCC service. • Remote Activated—Valid values specify true or false. **Note** The value of the Remote Activated column is set to true whenever remote IP addresses are configured either manually or dynamically. • Address 1—This column lists the first address for this service. **Note** When you upgrade from Cisco Unified Communications Manager 8.6 (1) to Cisco Unified Communications Manager 8.6 (2) or later, Address 1 is automatically updated by the system. However, if this field is blank after the upgrade due to some reason such as DNS lookup failure, you must manually update it with the appropriate IP address of the TFTP service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
Enabled All Services	Click this button to enable all services (EMCC, PSTN Access, and RSVP Agent).
Disabled All Services	Click this button to disable all services (EMCC, PSTN Access, and RSVP Agent).
Update Remote Cluster Now	Click this button to update the remote cluster immediately.

Remote Cluster Manually Override Settings

The following table provides detailed descriptions of the remote cluster settings that you configure in the Remote Cluster Manually Override Configuration window (**Advanced Features > Cluster View > TFTP**).

Field	Description
Use automatically determined remote server addresses	Choose this option to use automatically-determined remote server addresses.
Manually configure remote server addresses	Choose this option to manually configure remote server addresses.
Address 1	Enter the first address of the TFTP service.
Address 2	Enter the second address of the TFTP service.
Address 3	Enter the third address of the TFTP service.