Configure TFTP Servers

Proxy TFTP Deployment Overview

Use a proxy Trivial File Transfer Protocol (TFTP) server to provide the configuration files that endpoints in your network need, such as: dial plans, ringer files, and device configuration files. A TFTP server can be installed in any cluster in your deployment and can service requests from endpoints on multiple clusters. The DHCP scope specifies the IP address of the proxy TFTP server to use to get the configuration files.

Redundant and Peer Proxy TFTP Servers

In a single cluster deployment, the cluster must have at least one proxy TFTP server. You can add another proxy TFTP server to the cluster for redundancy. The second proxy TFTP server is added in option 150 for IPv4. For IPv6, you add the second proxy TFTP server to TFTP Server Addresses sub-option type 1 in the DHCP scope.

In a multiple cluster deployment, you can specify up to three remote proxy TFTP servers as peer clusters of the primary proxy TFTP server. This is useful if you want to configure only one proxy TFTP server for many DHCP scopes, or have only one DHCP scope. The primary proxy TFTP server provides the configuration files for all phones and devices in the network.

You must create a peer relationship between each remote proxy TFTP server and the primary proxy TFTP server.

Tip When you configure peer relationships between the remote proxy TFTP servers in your network, keep the relationships hierarchical. Ensure that the peer proxy TFTP servers on the remote clusters do not point to each other to avoid possible looping. For example, if the primary node A has a peer relationship with nodes B and C. You should not create a peer relationship between nodes B and C. If you do, then you have created a loop.

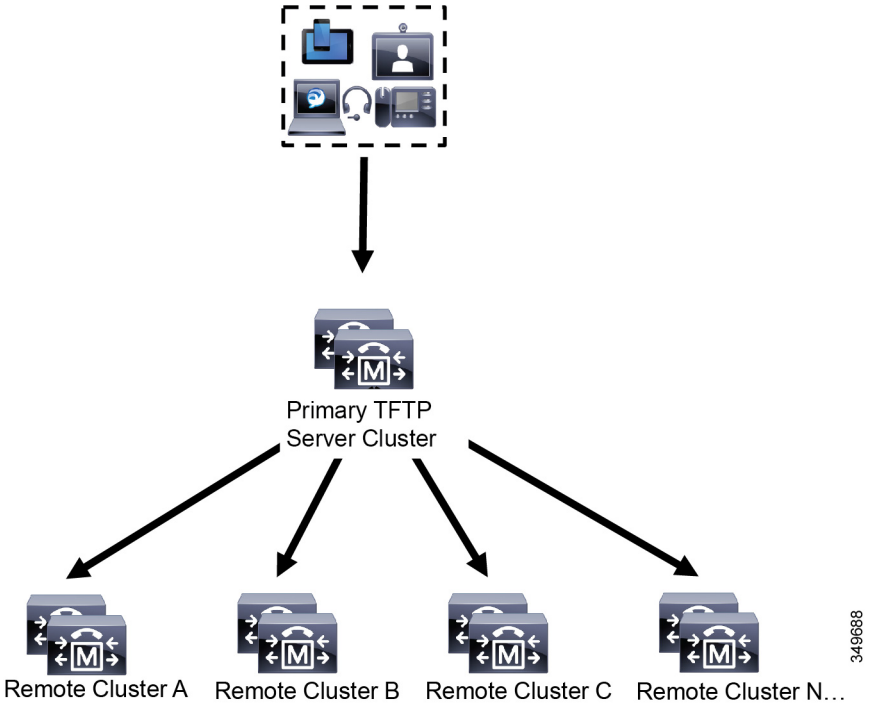
Proxy TFTP

In multi-cluster systems, the proxy TFTP service is able provide TFTP files from multiple clusters via a single primary TFTP server. The proxy TFTP can serve as a single TFTP reference for scenarios where a single

subnet or VLAN contains phones from multiple clusters or in any scenario where multiple clusters share the same DHCP TFTP option (150).

The Proxy TFTP service functions as a single-level hierarchy is as illustrated. More complicated multi-level hierarchies are not supported.

Figure 1: Proxy TFTP Single-Level Hierarchy



In the above illustration, a group of devices contacts the Primary TFTP server for their configuration files. When it receives a request for TFTP from a device, the primary TFTP looks into its own local cache for the configuration file as well as any other remotely configured clusters such as Remote Cluster A, B, C, or N (any other remote clusters configured).

It is possible to configure any number of remote clusters on the primary TFTP server; however, each remote cluster may contain only up to 3 TFTP IP addresses. The recommended design for redundancy is 2 TFTP servers per cluster, and thus 2 IP addresses per remote cluster on the Primary TFTP server for redundancy.

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 Support for IPv4 and IPv6 Devices

We recommend that you enable IPv4 phones and gateways to use the DHCP custom option 150 to discover the TFTP server IP address. Using option 150, gateways and phones discover the TFTP server IP address. For more information, see the documentation that came with your device.

In an IPv6 network, we recommend that you use the Cisco vendor-specific DHCPv6 information to pass the TFTP server IPv6 address to the endpoint. With this method, you configure the TFTP server IP address as the option value.

If you have some endpoints that use IPv4 and some that use IPv6, we recommend that you use DHCP custom option 150 for IPv4 and use the TFTP Server Addresses sub-option type 1, a Cisco vendor-specific information option, for IPv6. If the endpoint obtains an IPv6 address and sends a request to the TFTP server while the TFTP server is using IPv4 to process requests, the TFTP server does not receive the request because the TFTP server is not listening for the request on the IPv6 stack. In this case, the endpoint cannot register with Cisco Unified Communications Manager.

There are alternative methods that you could use for your IPv4 and IPv6 devices to discover the IP address of the TFTP server. For example, you could use DHCP option 066 or CiscoCM1 for your IPv4 devices. For your IPv6 devices, other methods include using TFTP Service sub-option type 2 or configuring the IP address of the TFTP server on the endpoint. These alternative methods are not recommended. Consult your Cisco service provider before using any alternative methods.

Endpoints and Configuration Files for TFTP Deployments

SCCP phones, SIP phones and gateways, request a configuration file when they initialize. An updated configuration file gets sent to the endpoint whenever you change the device configuration.

The configuration file contains information such as a prioritized list of Unified Communications Manager nodes, the TCP ports used to connect to those nodes, as well other executables. For some endpoints, the configuration file also contains locale information and URLs for phone buttons, such as: messages, directories, services, and information. Configuration files for gateways contain all the configuration information that the device requires.

Security Considerations for Proxy TFTP

Cisco Proxy TFTP servers handle both signed and unsigned requests and run in either nonsecure mode or mixed mode. The Proxy TFTP Server searches the local file system or database when a phone requests for a file and if not found, sends a request to remote clusters. When the phone requests the server for a common file with names such as `ringlist.xml.sgn, locale file`, and so on, the server sends a local copy of the file instead of the file itself from the home cluster of the phone.

When receiving files from Proxy TFTP, the phone rejects the file due to a signature verification failure because the file has the signature of the proxy server which doesn't 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 import Proxy TFTP's callmanager certificate to new (remote/home) clusters phone-sast-trust. Then the phones can reachout to Trust Verification Service (TVS) and trust the Proxy TFTP certificats. Bulk certificate exchange is needed if EMCC is enabled on the deployment

To disable Security by Default, see "Update ITL File for Cisco Unified IP Phones" section the Security Guide for Cisco Unified Communications Manager.

Proxy TFTP in Mixed Mode

TFTP servers on remote clusters that are running in mixed mode must have the primary Proxy TFTP server certificates added to their Cisco Certificate Trust List (CTL) file. Otherwise, endpoints that are registered to a cluster where security is enabled will be unable to download the files that they need. To achieve this update CTL file after performing bulk import-export of certificates.

For more information, see "Bulk Certificate Export" section in the Security Guide for Cisco Unified Communications Manager when migrating IP phones between clusters to perform the bulk certificate export.

Moving Phones Between Clusters in Proxy TFTP Environment

When moving phones from one Remote Cluster to another in a Proxy TFTP environment, perform the following:

1. Add Phone details to Remote Cluster B (destination cluster).
2. Delete Phone details from Remote Cluster A (source cluster).

Note The phone's configuration in the Proxy TFTP takes 30 minutes to expire. To avoid any file not found response, you can restart Proxy Cluster's TFTP services.

3. Reset Phones to download configuration files from Remote Cluster B and register to Remote Cluster B.

TFTP Server Configuration Task Flow

You can let the system dynamically configure the proxy TFTP server if you have Extension Mobility Cross Cluster (EMCC) configured for your cluster. If you don't, then you can set up the TFTP server and set the security mode manually.

Procedure

	Command or Action	Purpose
Step 1	Set up the TFTP server using one of the following methods: • Configure TFTP Server Dynamically, on page 5 • Configure TFTP Server Manually, on page 6	If you have Intercluster Lookup Service (ILS) configured, you can set up your TFTP server dynamically. If you don't have EMCC configured, set up your TFTP server manually. You must indicate if the cluster is secured or non-secured. The cluster is treated as non-secure by default.
Step 2	(Optional) Update the CTL File for TFTP Servers, on page 7	Install the CTL client plug-in and add the primary proxy TFTP server to the Cisco Certificate Trust List (CTL) file of all proxy TFTP servers in all remote clusters that are operating in mixed-mode.

	Command or Action	Purpose
Step 3	(Optional) See the documentation that supports your endpoint device.	Add the proxy TFTP servers to the Trust Verification List (TVL) of all remote endpoints if your proxy TFTP deployment has remote clusters.
Step 4	(Optional) Modify Non-Configuration Files for the TFTP Server, on page 7	You can modify non-configuration files that the end points request from the proxy TFTP server.
Step 5	(Optional) Stop and Start the TFTP service, on page 8	Stop and restart the TFTP service on the proxy TFTP node if you have uploaded modified non-configuration files for your endpoints.
Step 6	(Optional) See the documentation that supports your DHCP server.	For multiple cluster deployments, modify the DHCP scope for individual remote nodes to include the IP address of the primary proxy TFTP server.

Configure TFTP Server Dynamically

You can configure a Cisco proxy TFTP server dynamically if you have Intercluster Lookup Service (ILS) configured for your network.

Before you begin

Configure EMCC for your network. For more information, see the *Features and Services Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Important From Release 14SU1 onwards, when SIP OAuth is enabled, you must copy the root CA certificate of off clusters Tomcat certificates to proxy phone edge trust.

Procedure

In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **Cluster View** > **Update Remote Cluster Now**. The TFTP server is automatically configured for the cluster.

What to do next

You must add any remote proxy TFTP servers to the Trust Verification Lists (TVL) of the endpoints; otherwise, they will not accept the configuration files from the proxy TFTP server that is on a remote cluster. See the documentation that supports your endpoint device for instructions.

Configure TFTP Server Manually

To configure TFTP in your network when you don't have EMCC configured, you must use the manual procedure.

You set up peer relationships between the primary proxy TFTP server and other TFTP servers from the Cluster View. You can add up to three peer TFTP servers.

Each remote TFTP server in the proxy TFTP deployment must include a peer relationship to the primary proxy TFTP server. To avoid creating a loop, ensure that the peer TFTP servers on the remote clusters do not point to each other.

Before you begin

Important From Release 14SU1 onwards, when SIP OAuth is enabled, you must copy the root CA certificates of off clusters Tomcat certificates to proxy phone edge trust.

Procedure

Step 1 Create a remote cluster. Perform the following actions:

a) From Cisco Unified CM Administration, select **Advanced Features** > **Cluster View**.

b) Click **Add New**. The **Remote Cluster Configuration** window appears.

c) Enter a cluster ID and a Fully Qualified Domain Name (FQDN) of up to 50 characters for the TFTP server, then click **Save**.

Valid values for the cluster ID include alphanumeric characters, period (.), and hyphen (-). Valid values for the FQDN include alphanumeric characters, period (.), dash (-), asterisk (*), and space.

d) (Optional) In the **Remote Cluster Service Configuration** window, enter a description of up to 128 characters for the remote cluster.

Do not use quotes (“), closed or open angle brackets (> <), backslash (\), dash (-), ampersand (&), or the percent sign (%).

Step 2 Check the **TFTP** check box to enable TFTP for the remote cluster.

Step 3 Click **TFTP**.

Step 4 In the **Remote Cluster Service Manually Override Configuration** window, select **Manually configure remote service addresses**.

Step 5 Enter the IP addresses of the TFTP server to create a peer relationships to those TFTP servers.

You can enter up to three TFTP server IP addresses.

Step 6 (Optional) Check the **Cluster is Secure** check box if the proxy TFTP server is deployed in a secured cluster.

Step 7 Click **Save**.

What to do next

You must add any remote TFTP servers to the Trust Verification Lists (TVL) of the endpoints; otherwise, they will not accept the configuration files from the proxy TFTP server that is on a remote cluster. See the documentation that supports your endpoint device for instructions.

Update the CTL File for TFTP Servers

Update the CTL file from publisher node by running `utils ctl` in each cluster which is in mixed mode. Make sure that a complete security network is attained between the Proxy TFTP server and all the clusters, that is bulk import and export exchange of certificates between Proxy and remote clusters.

While using CTLClient, you must add the primary TFTP server or the IP address of the primary TFTP server to the Cisco Certificate Trust List (CTL) file of all TFTP servers in remote clusters that are running in mixed mode. This is necessary so that endpoints in security-enabled clusters can successfully download their configuration files.

For more information about security and using the Cisco CTL CLI, see the "About Cisco CTL Setup" section in the Security Guide for Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Application** > **Plugins**.

Step 2 Click **Find** to list of all the plug-ins that you can install.

Step 3 Click the **Download** link for the Cisco CTL Client.
The system installs the client that digitally signs certificates stored on the TFTP server.

Step 4 Reboot the TFTP server.

Modify Non-Configuration Files for the TFTP Server

You can modify a non-configuration file, such as a load file or `RingList.xml`, that the endpoints request from the proxy TFTP server. After you complete this procedure, upload the modified files to the TFTP directory of the proxy TFTP server.

Procedure

Step 1 In Cisco Unified Communications Operating System Administration, select **Software Upgrades** > **TFTP File Management**.
The **TFTP File Management** window appears.

Step 2 Click **Upload File**.
The **Upload File** pop-up appears.

Step 3 Perform one of the following actions:

- Click **Browse** to browse to the directory location of the file to upload.
- Paste the full directory path of the updated file in to the **Directory** field.

Step 4 Click **Upload File** or click **Close** to exit without uploading the file.

What to do next

Stop and restart the Cisco TFTP service on the proxy TFTP node using Cisco Unified Serviceability Administration.

Stop and Start the TFTP service

Use the following procedure to stop and restart the TFTP service on the proxy TFTP node.

For more information about service activation, deactivation, and restarts, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Procedure

Step 1 In Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**.

Step 2 In the **Control Center–Feature Services** window, select the proxy TFTP node in the **Server** drop-down list.

Step 3 Select the TFTP service in the **CM Services** area and click **Stop**.

The status changes to reflect the updated status.

Tip To see the latest status of services, click **Refresh**.

Step 4 Select the TFTP service in the **CM Services** area, then click **Start**.

The status changes to reflect the updated status.