CTL Update

More Information

For information about performing a CTL update, see the “Security Basics” section in the *Cisco Unified Communications Manager Security Guide*: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Bulk Certificate Management

Bulk certificate management must be performed manually on both source nodes and destination nodes. The source nodes and destination nodes must be up and running at this point. Phones are registered with the source nodes.

Procedure

Step 1 On the Destination Cluster Publisher, navigate to Cisco Unified Operating System Administration and choose **Security** > **Bulk Certificate Management**.

Step 2 Define the Central Secure File Transfer Protocol (SFTP) server IP address, port, user, password, and directory.

Step 3 Use the **Export** button to export all Trivial File Transfer Protocol (TFTP) certificates from the destination cluster to the central SFTP server.

Step 4 On the Source Cluster Publisher, navigate to Cisco Unified Operating System Administration. Select **Security** > **Bulk Certificate Management**.

Step 5 Define the Central SFTP server with same parameters that you used in Step 2.

Step 6 Click **Export** to export all TFTP certificates from source cluster to the central SFTP server.

Step 7 Click **Consolidate** to consolidate all the TFTP certificates on the central SFTP server. You can perform this step on either the source or destination cluster, using the Bulk Certificate Management interface.

Step 8 On the Source cluster, click **Bulk Certificate Import** to import the TFTP certificates from the central SFTP server.

Step 9 On the Destination cluster, click **Bulk Certificate Import** to import the TFTP certificates from the central SFTP server.

Step 10 Use Dynamic Host Configuration Protocol (DHCP) option **150** to point the phones to the new destination cluster TFTP server.
Upon reset or power cycle, the phones will download the new destination cluster ITL file and attempt to authenticate the new Initial Trust List (ITL) file signature with the certificates in the existing ITL file.

No certificate in the existing ITL file can be used to authenticate the signature, so the phone requests the signer's certificate from the old Trust Verification Service (TVS) server on the source cluster.

The phone sends this request to the source cluster TVS service on TCP port 2445.

The bulk certificate exchange in Steps 1 through 9 provides the TVS service in the source cluster with the TFTP certificate on the destination cluster that signed the new ITL file.

TVS returns the certificate to the phone, which allows the phone to authenticate the signature and replace the old ITL file with the newly downloaded ITL file.

The phone can now download and authenticate the signed configuration files from the new destination cluster.