Procedure for Bulk Certificate Management Between CUCM Clusters for Phone Migration

Contents

Introduction

This document provides a how-to procedure for bulk certificate management between Cisco Unified Communications Manager (CUCM) clusters for phone migration.

Contributed by Adrian Esquillo, Cisco TAC Engineer.

> **Note**: This procedure is also outlined in the Manage Bulk Certificates Section of the Administration Guide for CUCM Release 12.5(1)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:
• Secure File Transfer Protocol (SFTP) Server
• CUCM Certificates

Components Used

• The information in this document is based on CUCM 10.X.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Bulk Certificate Management allows a set of certifcates to be shared between CUCM clusters. This step is a requirement for system functions of individual clusters that need a trust to be established between them, such as for Extension Mobility Cross Cluster (EMCC), as well as for phone migration between clusters.

As part of the procedure, a Public Key Cryptography Standards #12 (PKCS12) file that contains certificates from all nodes in a cluster is created. Every cluster must export its certificates to the same SFTP directory on the same SFTP server. Bulk certificate management configurations must be done manually on the CUCM publisher of both the source and destination clusters. The source and destination clusters must be up and operational so that the phones to be migrated have connectivity to both of these clusters. The source cluster phones are migrated to the destination cluster.

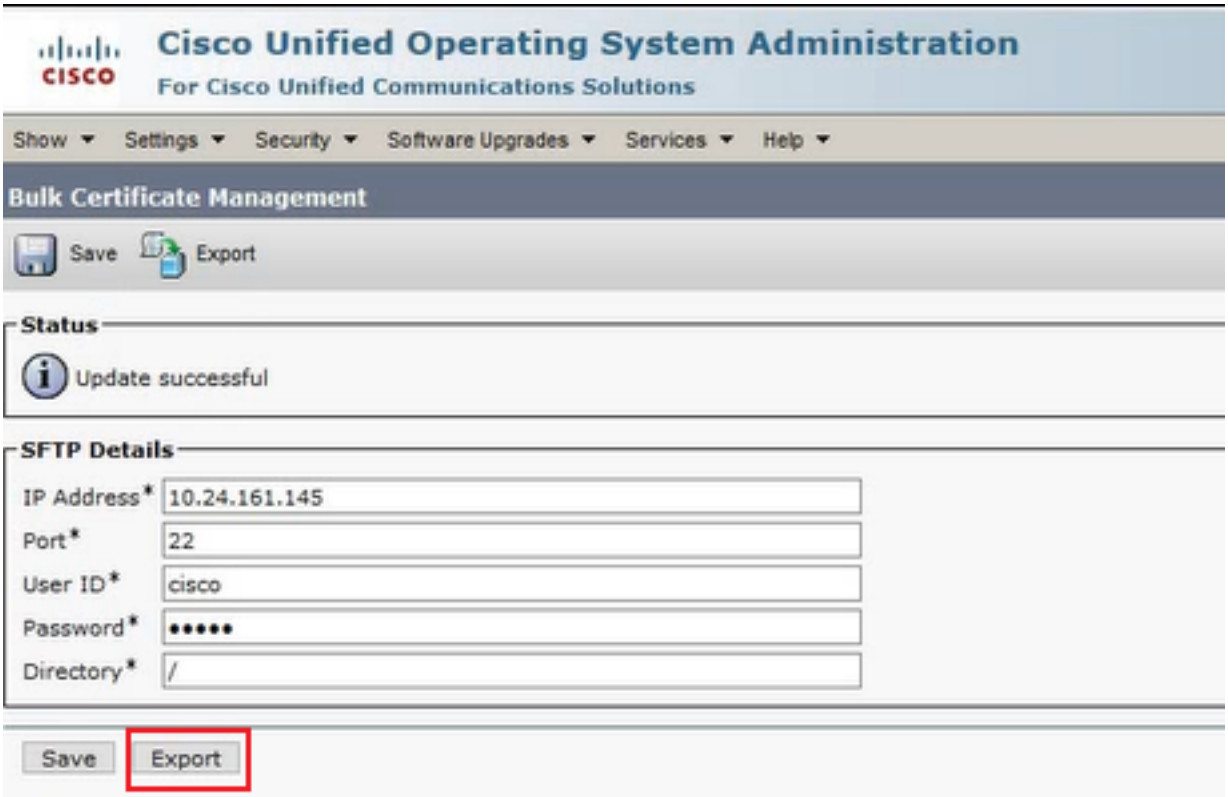
Bulk Certificate Management Procedure

Export Destination Cluster certificates

Step 1. Configure the SFTP server for Bulk Certificate Management on CUCM publisher of the destination cluster.

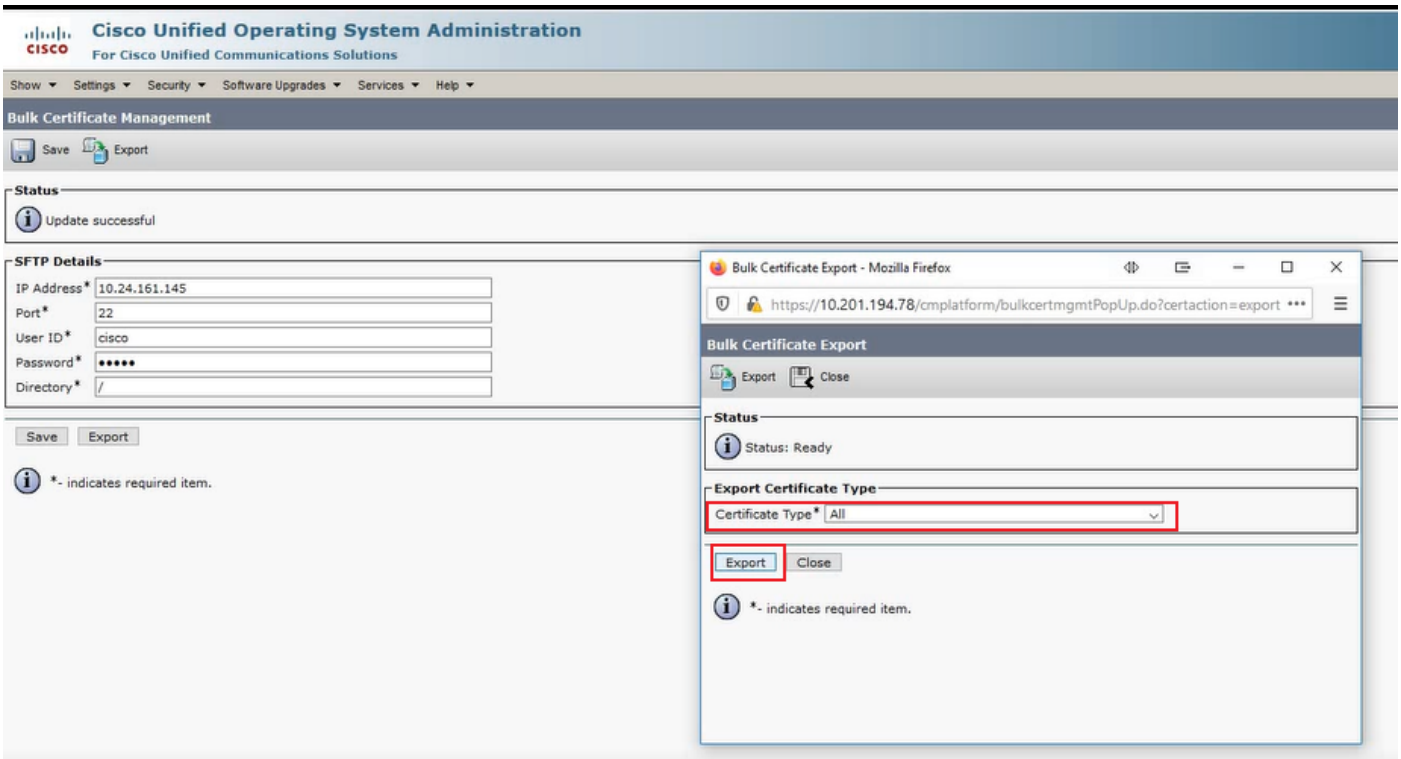
In this example, the destination cluster CUCM version is 11.5.1.

• **Navigate** to **Cisco Unified OS Adminstration > Security > Bulk Certificate Management** enter the SFTP server details and **click** Export, as shown in the image.

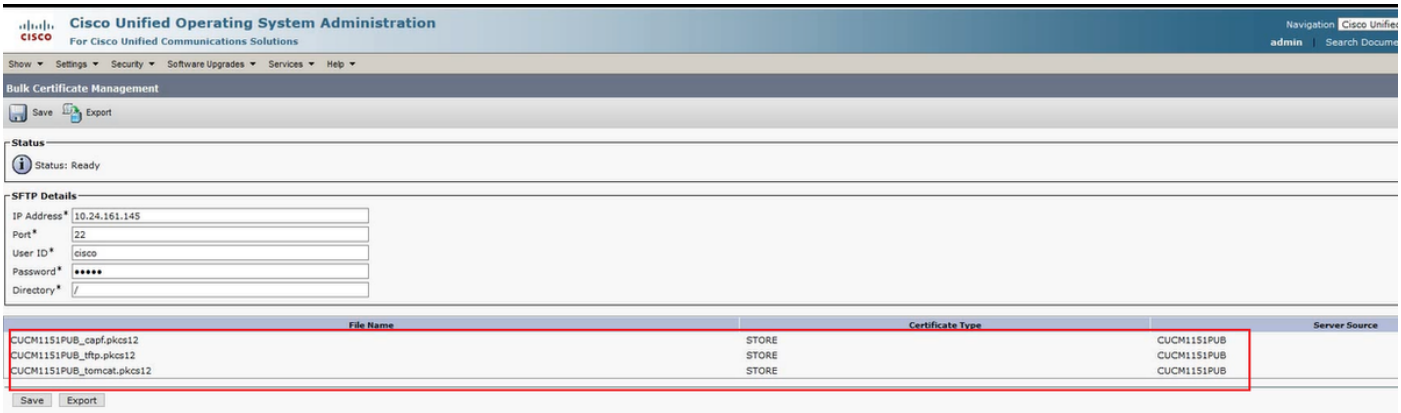


Step 2. Export all certificates from all nodes in destination cluster to SFTP server.

• In the subsequent popup window, select **All** for Certificate Type and then click **Export**, as shown in the image.



• Close the popup window and Bulk Certificate Management updates with the PKCS12 files created for each of the nodes in the destination cluster, the web page refreshes with this information, as shown in the image.



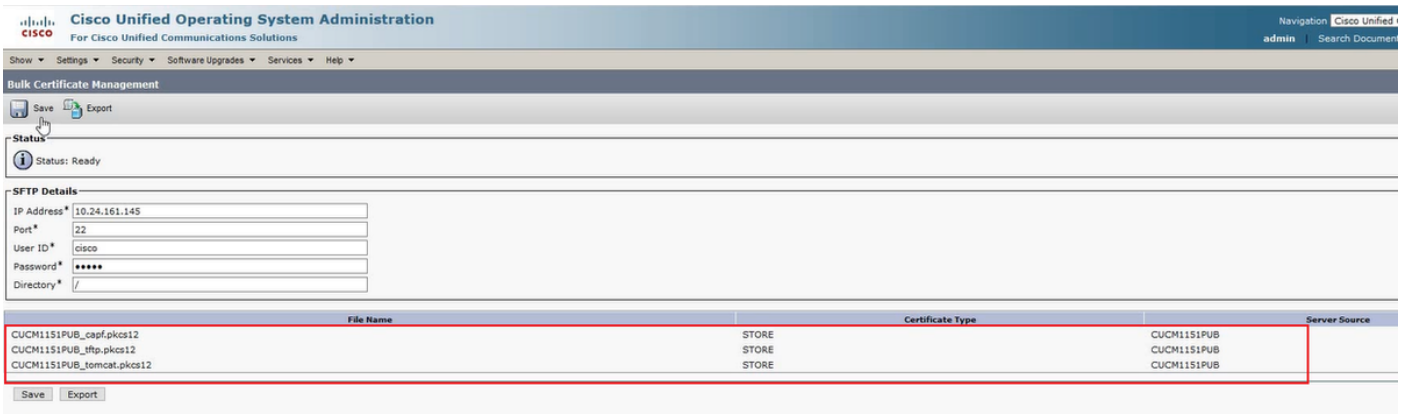
Export Source Cluster certificates

Step 1. Configure the SFTP server for Bulk Certificate Management on CUCM publisher of the source cluster.

In this example, the source cluster CUCM version is 10.5.2.

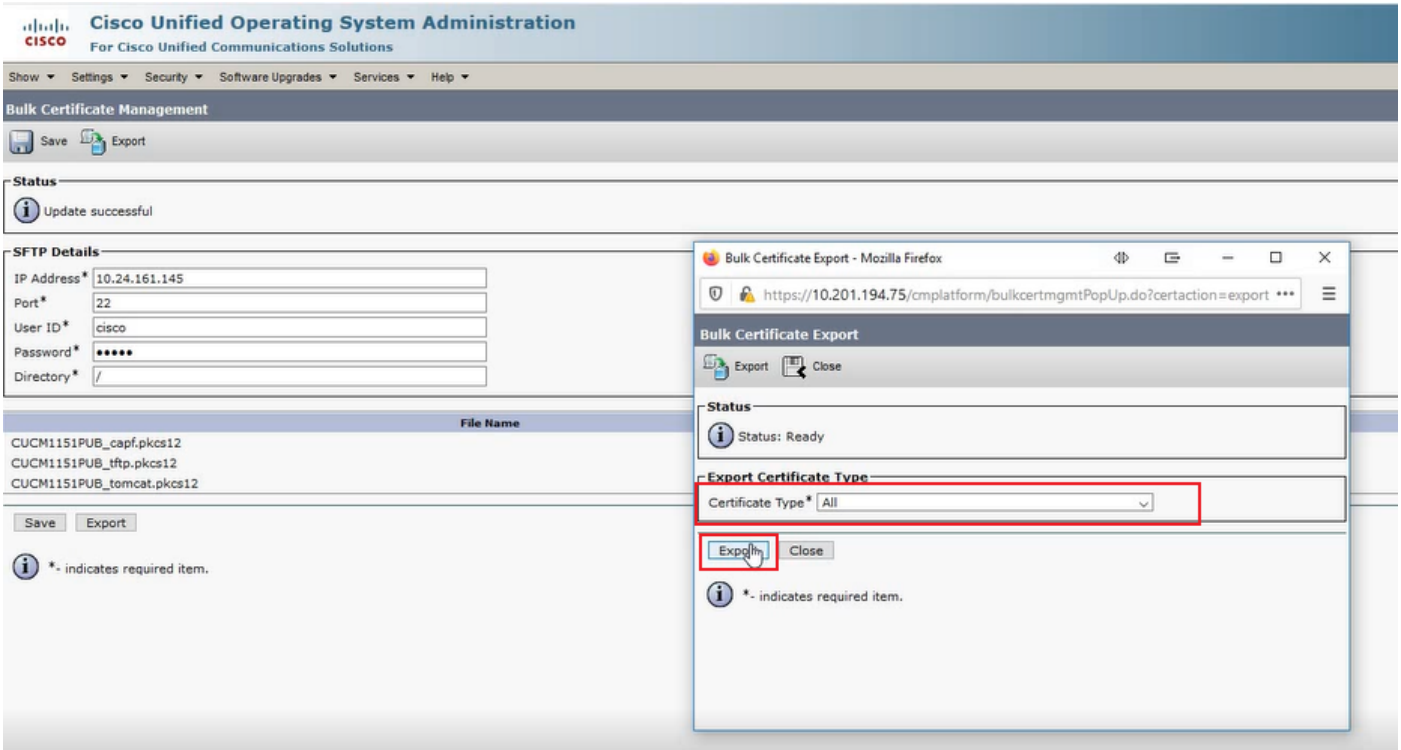
• **Navigate** to **Cisco Unified OS Adminstration > Security > Bulk Certificate Management** enter the SFTP server details and **click** Export, as shown in the image.

> **Note**: The PKCS12 files exported from the destination cluster to the SFTP server shows on the source cluster CUCM publisher's Bulk Certificate Mangement web page when accessed.

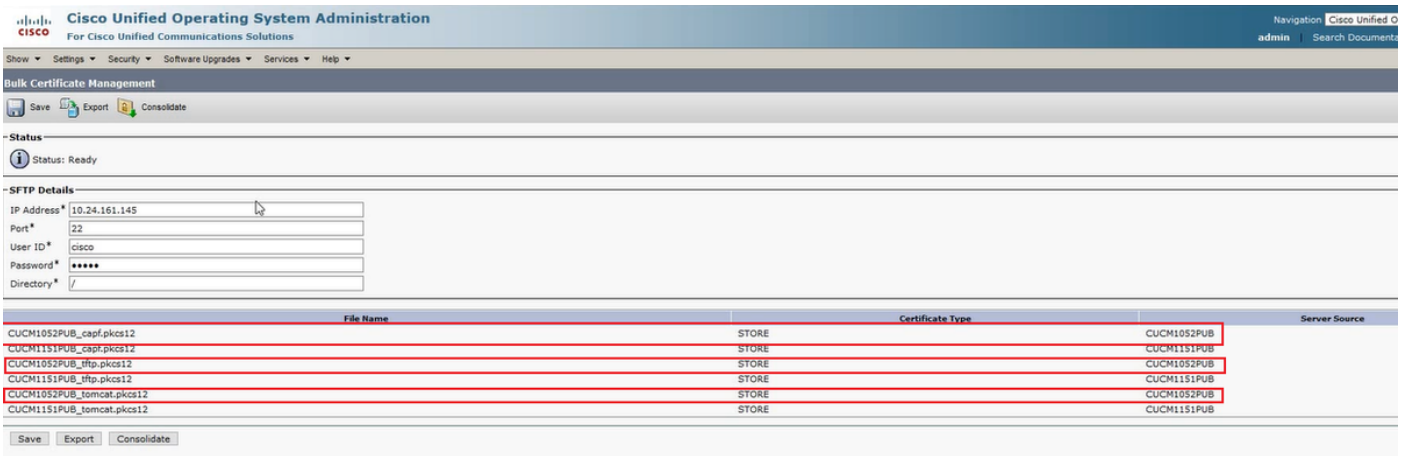


Step 2. Export all certificates from all nodes in source cluster to SFTP server.

• In the subsequent popup window, select **All** for Certificate Type and then click **Export**, as shown in the image.



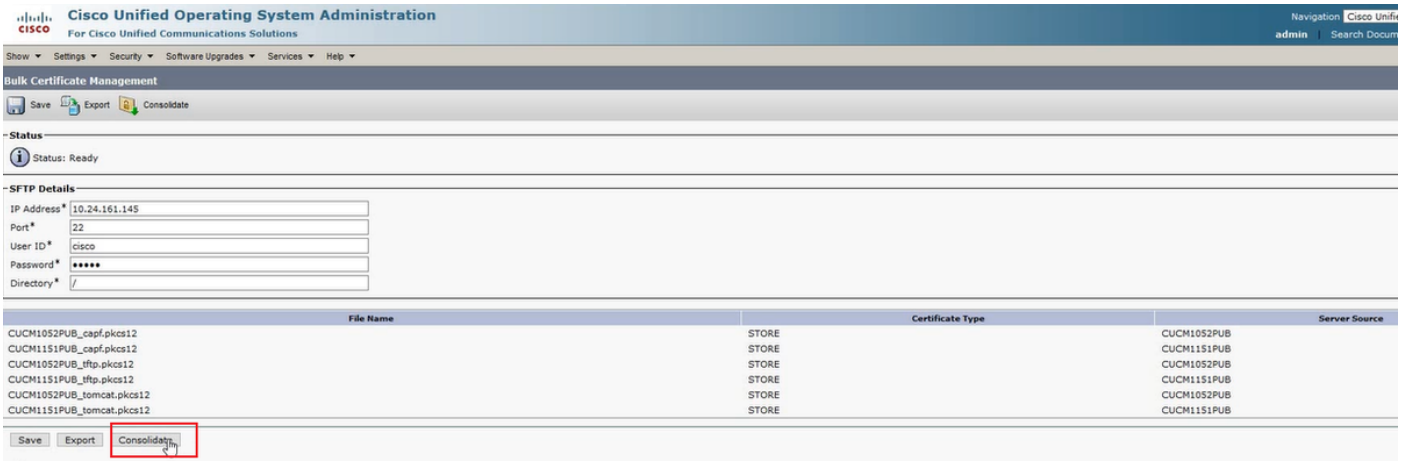
• Close the popup window and Bulk Certificate Management updates with the PKCS12 files created for each of the nodes in the source cluster, the web page refreshes with this information. The web page for Bulk Certificate Management of the source cluster now shows both source and destination PKCS12 files exported to SFTP, as shown in the image.



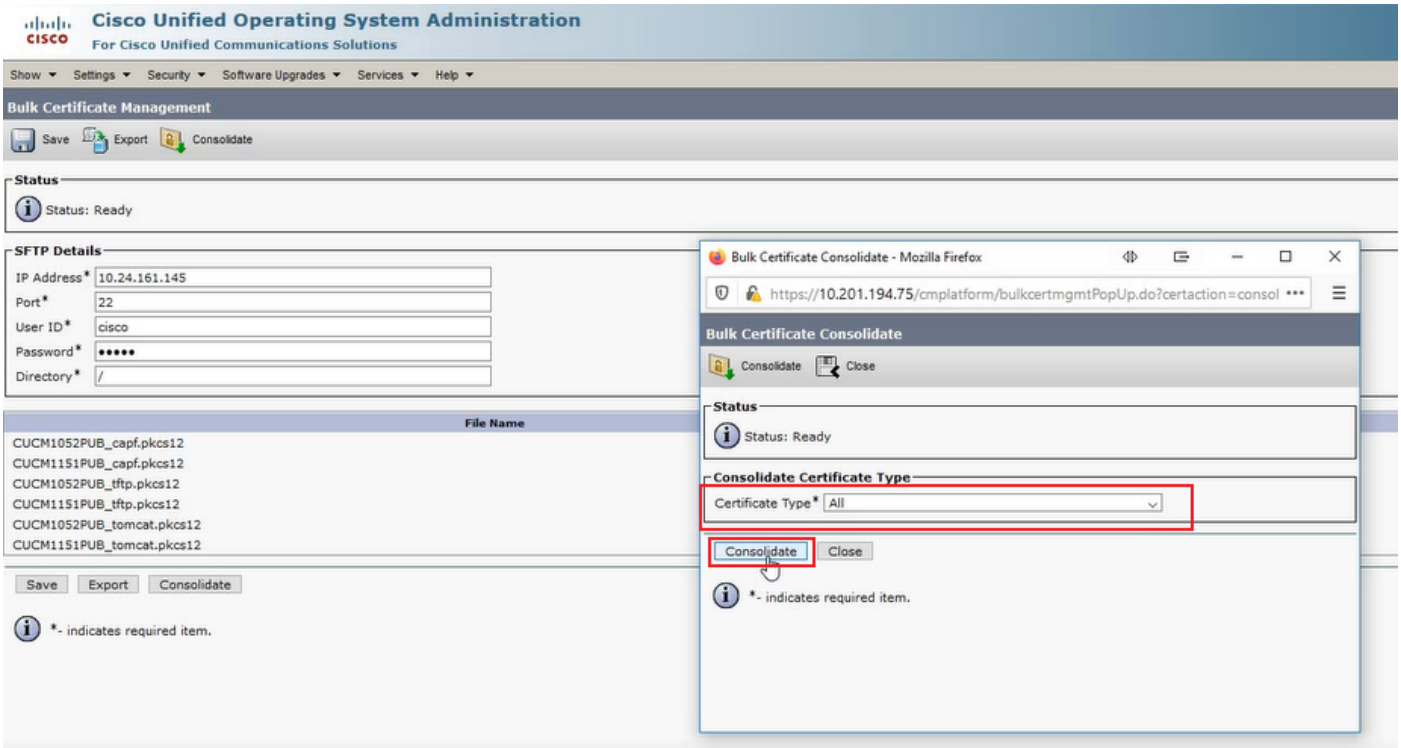
Consolidate Source and Destination PKCS12 files

> **Note**: Whereas Bulk Certificate Management export is done on both the source and destination clusters, consolidation is done through the CUCM publisher on only one of the clusters.

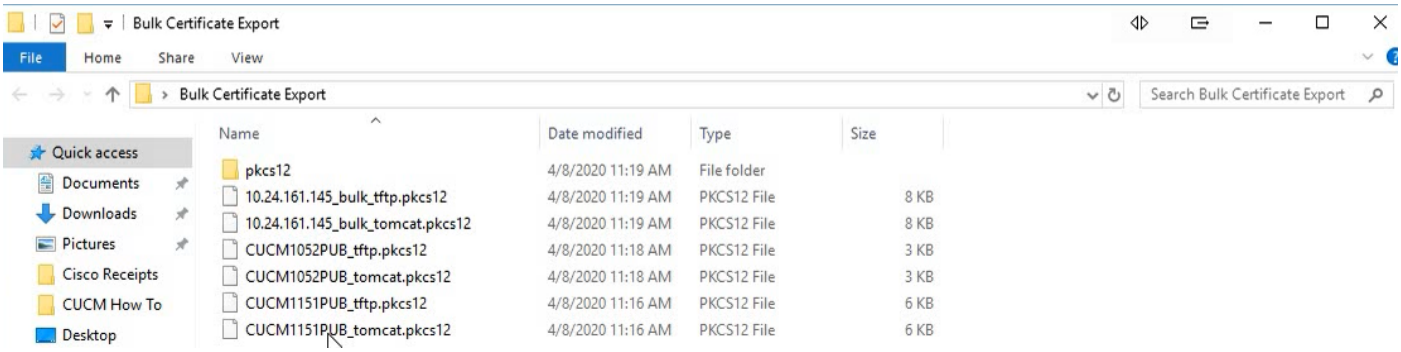
Step 1. Return to the Bulk Certificate Management Page of the CUCM publisher of the source cluster and **click** on Consolidate, as shown in the image.

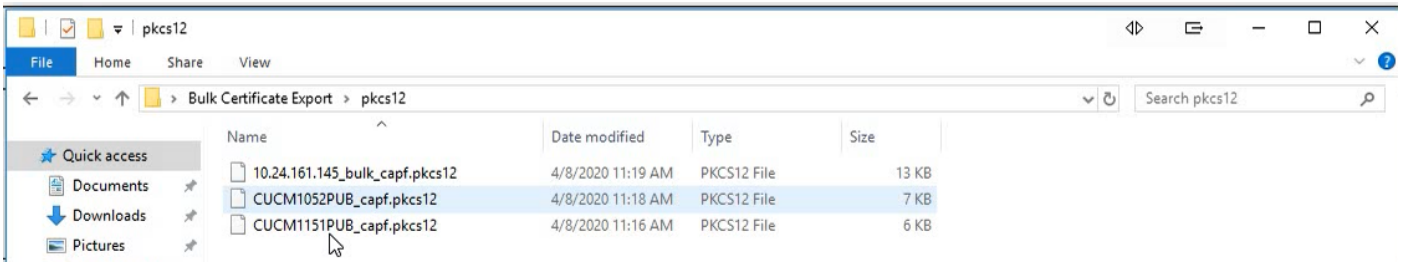


• In the subsequent popup window, select **All** for Certificate Type and then click **Consolidate**, as shown in the image.



• At any time, you can check the SFTP directory to verify the pkcs12 files that are contained for both the source and destination clusters. The contents of the SFTP directory after export of all certificates from both destination and source clusters has been completed, as shown in the images.

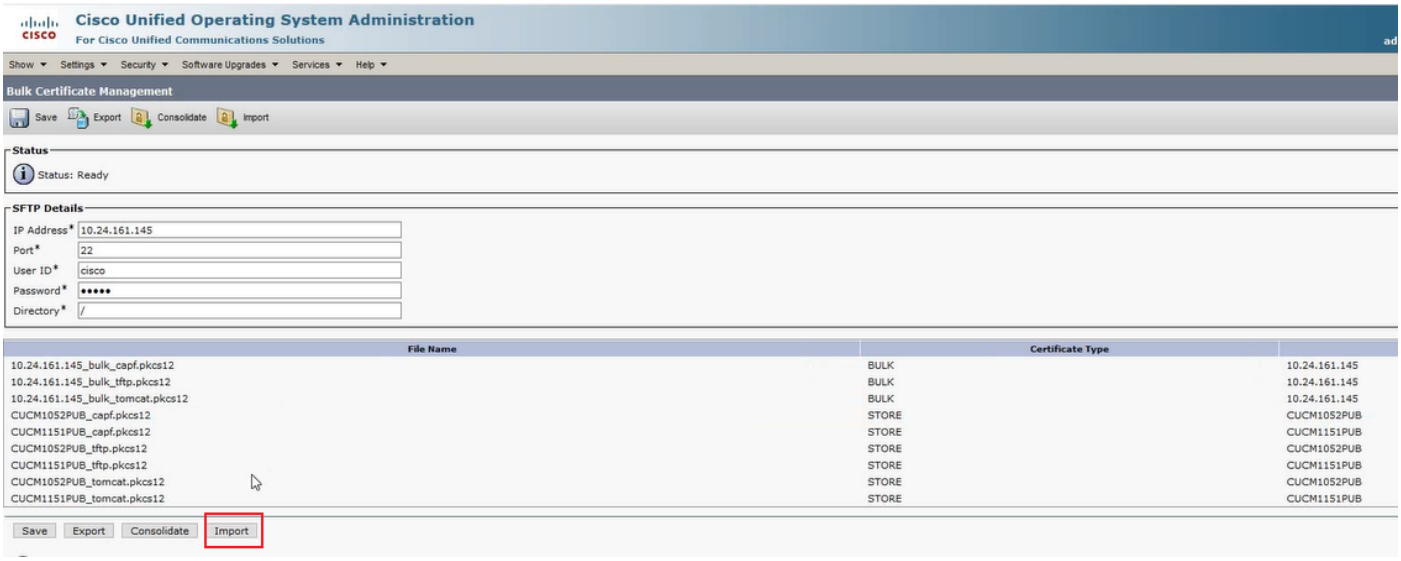




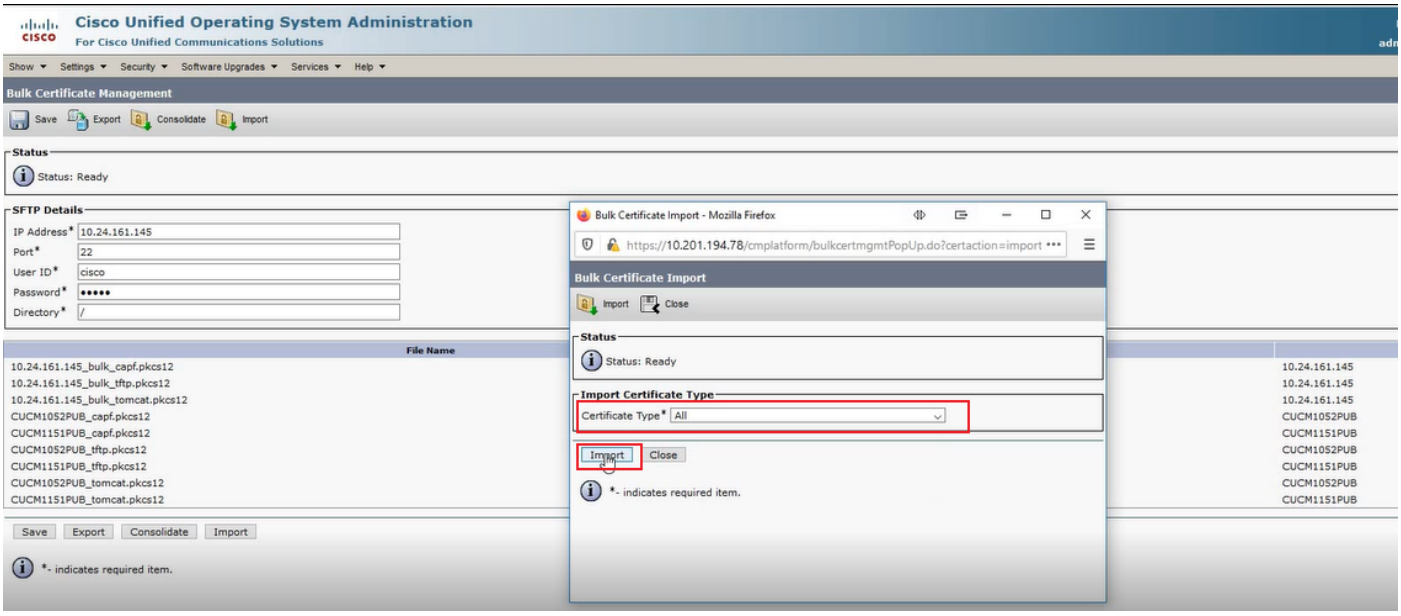
Import Certificates to Destination and Source Clusters

Step 1. Import certificates to the destination cluster

• On the CUCM publisher of the destination cluster **Navigate** to **Cisco Unified OS Adminstration > Security > Bulk Certificate Management** and let the page refresh, then **click** Import, as shown in the image.



• In the subsequent popup window, select **All** for Certificate Type and then click **Import**, as shown in the image.



Step 2. Repeat step 1 for source cluster.

Note: When bulk certificate import is performed, the certifcates are uploaded to the remote cluster as follows:
• Certificate Authority Proxy Function (CAPF) certificate gets uploaded as a CallManager-trust
• Tomcat certificate gets uploaded as a tomcat-trust
• CallManager certificate gets uploaded as Phone-SAST-trust and CallManager-trust
• Identity Trust List Recovery (ITLRecovery) certificate gets uploaded as Phone-SAST-trust and CallManager-trust

Configure Source Cluster Phones with Destination Cluster TFTP Server Information

Configure DHCP scope for source cluster phones with Trivial File Transfer Protocol (TFTP) Option 150 to point to destination cluster CUCM TFTP servers.

Reset Source Cluster Phones to Obtain Destination Cluster ITL/CTL File to Complete Migration Process

As part of the migration process, the source cluster phones attempt to setup a secure connection to the source cluster's Cisco Trust Verification Service (TVS) to verify the destination cluster's CallManager or ITLRecovery certificate.

Note: Either the source cluster's CallManager certificate from a CUCM server that runs the TFTP service (also known as TFTP certificate) or its ITLRecovery certificate signs a source cluster CUCM node's Certificate Trust List (CTL) and/or Identity Trust List (ITL) file. Similarly, either the destination cluster's CallManager certificate from a CUCM server that runs the TFTP service or its ITLRecovery certificate signs a destination cluster CUCM node's CTL and/or ITL file. CTL and ITL files are created on CUCM nodes that run the TFTP service. If a destination cluster's CTL and/or ITL file are not validated by the source cluster TVS, phone migration to the destination cluster fails.

Note: Before you start the source cluster phone migration process, confirm that these phones have a valid CTL and/or ITL file installed. Also, ensure that the enterprise feature "Prepare Cluster for Rollback to Pre 8.0" is set to False for the source cluster. Additionally, verify that the destination cluster CUCM nodes that run the TFTP service have valid CTL and/or ITL files installed.

Process in non-seucure cluster for source phones to obtain destination cluster ITL file to complete migration of phones:

Step1. Neither the CallManager nor the ITLRecovery certificate contained in the destination cluster's ITL file, that is presented to the source cluster phone on reset, can be used to validate the currently install ITL file. This causes the source cluster phone to establish a connection to the TVS of the source cluster to validate the destination cluster's ITL file.
Step 2. The phone establishes a connection to the source cluster TVS on tcp port 2445.
Step 3. The source cluster's TVS presents its certificate to the phone. The phone validates the connection and request the source cluster TVS validate the destination cluster's CallManager or ITLRecovery certificate to allow the phone to download the destination cluster's ITL file.
Step 4. After validation and installation of the destination cluster ITL file, the source cluster phone

can now validate and download signed configuration files from the destination cluster.

Process in secure cluster for source phones to obtain destination cluster CTL file to complete migration of phones:

Step 1. The phone boots and attempts to download the CTL file from the destintation cluster.
Step 2. The CTL file is signed by the destination cluster's CallManager or ITLRecovery certificate which is not in the phone's current CTL or ITL file.
Step 3. As a result, the phone reaches out to TVS on the source cluster to verify the CallManager or ITLRecovery certificate.

> **Note**: At this point, the phone still has its old configuration which contains the IP address of the source cluster TVS service. The TVS servers specified in the phones configuration is the same as the phones Callmanager group.

Step 4. The phone sets up an Transport Layer Security (TLS) connection to the TVS on the source cluster.
Step 5. When the source cluster TVS presents its certificate to the phone, the phone verifies this TVS certificate against the certificate in its current ITL file.
Step 6. If they are the same, the handshake completes successfully.
Step 7. The source phone requests that the source cluster TVS verify the CallManager or ITLRecovery certificate from the destination cluster CTL file.
Step 8. The source TVS service finds the destination cluster CallManager or ITLRecovery in its certificate store, validates it and the source cluster phone proceeds to update with the destination cluster CTL file.
Step 9. The source phone downloads the destination cluster's ITL file which is validated against the destination cluster CTL file it now contains. Since the source phone's CTL file now contains the destination cluster's CallManager or ITLRecovery certificate, the source phone can now verify the CallManager or ITLRecovery certificate without need to contact the source cluster's TVS.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Configuration Walkthrough Video

This link provides access to a video that walks through the Bulk Certificate Management Betweeen CUCM Clusters:

Bulk Certificate Management Between CUCM Clusters