Procedimiento para la administración masiva de certificados entre clústeres de CUCM para la migración del teléfono

Contenido

Introducción

Este documento proporciona un procedimiento de procedimientos para la gestión masiva de certificados entre los clústeres de Cisco Unified Communications Manager (CUCM) para la migración del teléfono.

Colaborado por Adrian Esquillo, Ingeniero del TAC de Cisco.

> **Nota:** Este procedimiento también se describe en la sección Administrar certificados masivos de la Guía de administración de la versión 12.5(1) de CUCM

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:
Servidor · Secure File Transfer Protocol (SFTP)
Certificados · CUCM

Componentes Utilizados

·La información de este documento se basa en 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Bulk Certificate Management permite compartir un conjunto de certificados entre clústeres de CUCM. Este paso es un requisito para las funciones del sistema de los clústeres individuales que necesitan que se establezca una confianza entre ellos, como para Extension Mobility Cross Cluster (EMCC), así como para la migración telefónica entre clústeres.

Como parte del procedimiento, se crea un archivo de estándares de criptografía de clave pública nº 12 (PKCS12) que contiene certificados de todos los nodos de un clúster. Cada clúster debe exportar sus certificados al mismo directorio SFTP del mismo servidor SFTP. Las configuraciones de administración de certificados masivos se deben realizar manualmente en el editor de CUCM de los clústeres de origen y de destino. Los clústeres de origen y de destino deben estar activos y operativos para que los teléfonos que se migrarán tengan conectividad a ambos clústeres. Los teléfonos del clúster de origen se migran al clúster de destino.

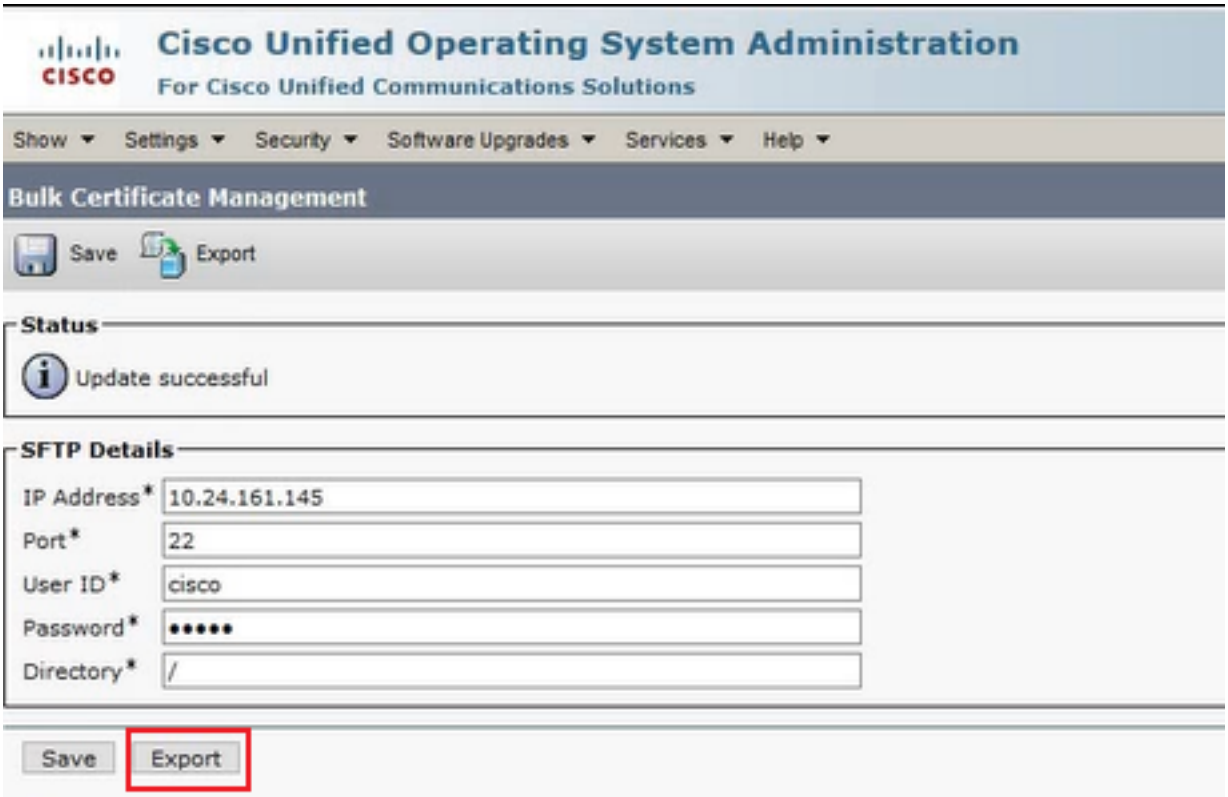
Procedimiento de administración de certificados masivos

Exportar certificados de clúster de destino

Paso 1. Configure el servidor SFTP para Bulk Certificate Management en el editor CUCM del clúster de destino.

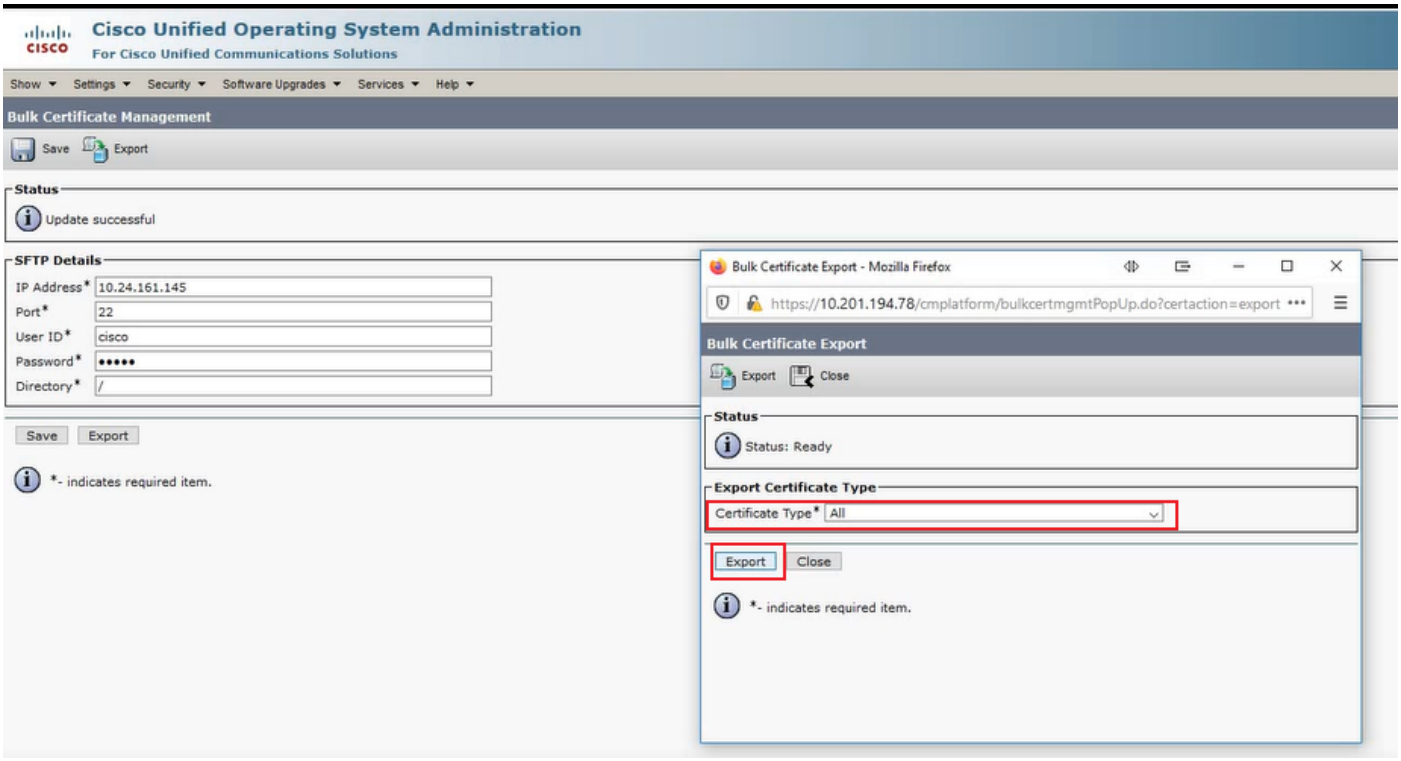
En este ejemplo, la versión de CUCM del clúster de destino es 11.5.1.

·**Vaya** a **Administración de Cisco Unified OS > Seguridad > Administración de certificados masivos** introduzca los detalles del servidor SFTP y **haga clic en** Exportar, como se muestra en la imagen.

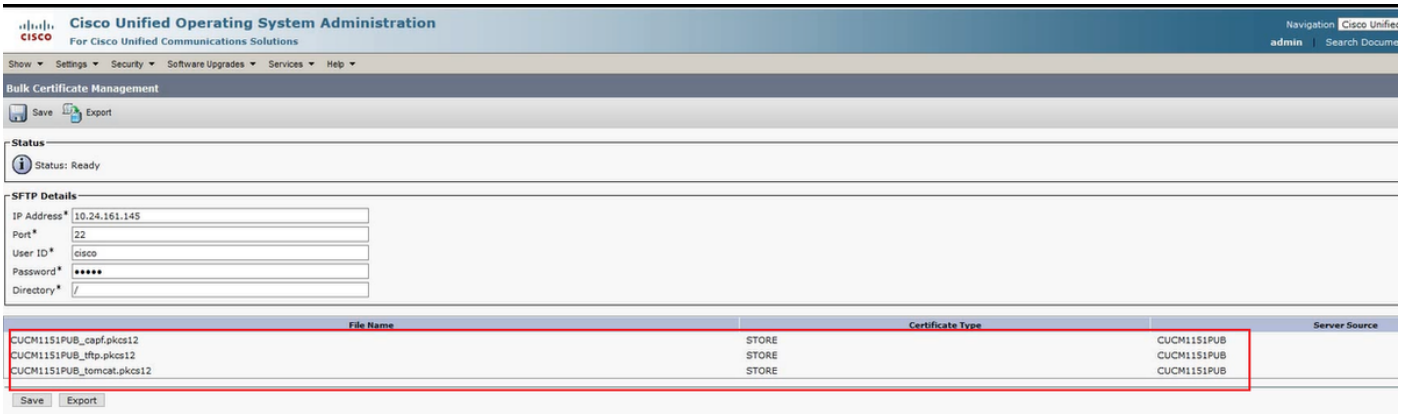


Paso 2. Exportar todos los certificados de todos los nodos del clúster de destino al servidor SFTP.

·En la siguiente ventana emergente, seleccione **Todo** para Tipo de certificado y luego haga clic en **Exportar**, como se muestra en la imagen.



·Cerrar la ventana emergente y las actualizaciones de Bulk Certificate Management con los archivos PKCS12 creados para cada uno de los nodos del clúster de destino, la página web se actualiza con esta información, como se muestra en la imagen.



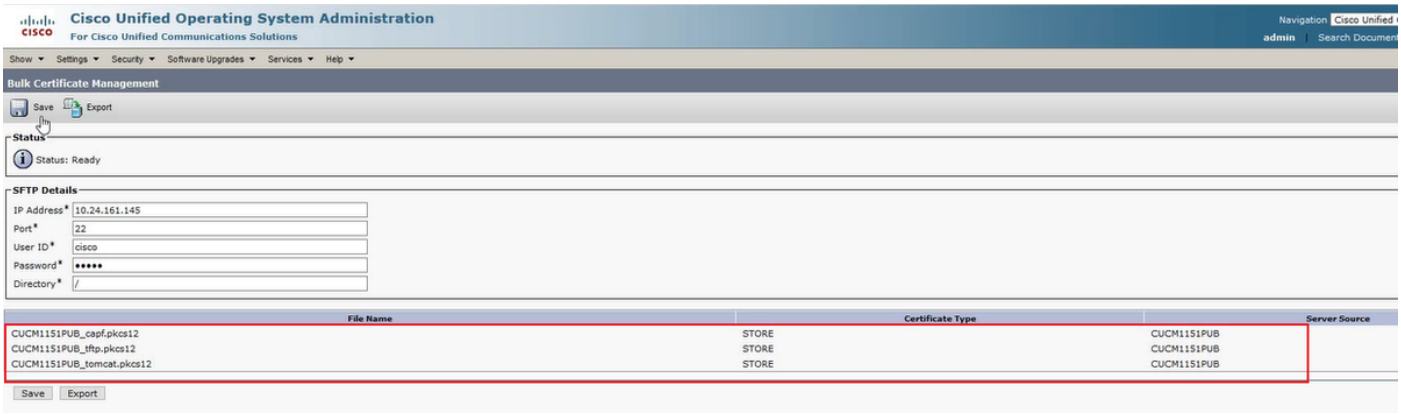
Exportar certificados de clúster de origen

Paso 1. Configure el servidor SFTP para Bulk Certificate Management en el editor CUCM del clúster de origen.

En este ejemplo, la versión de CUCM del clúster de origen es 10.5.2.

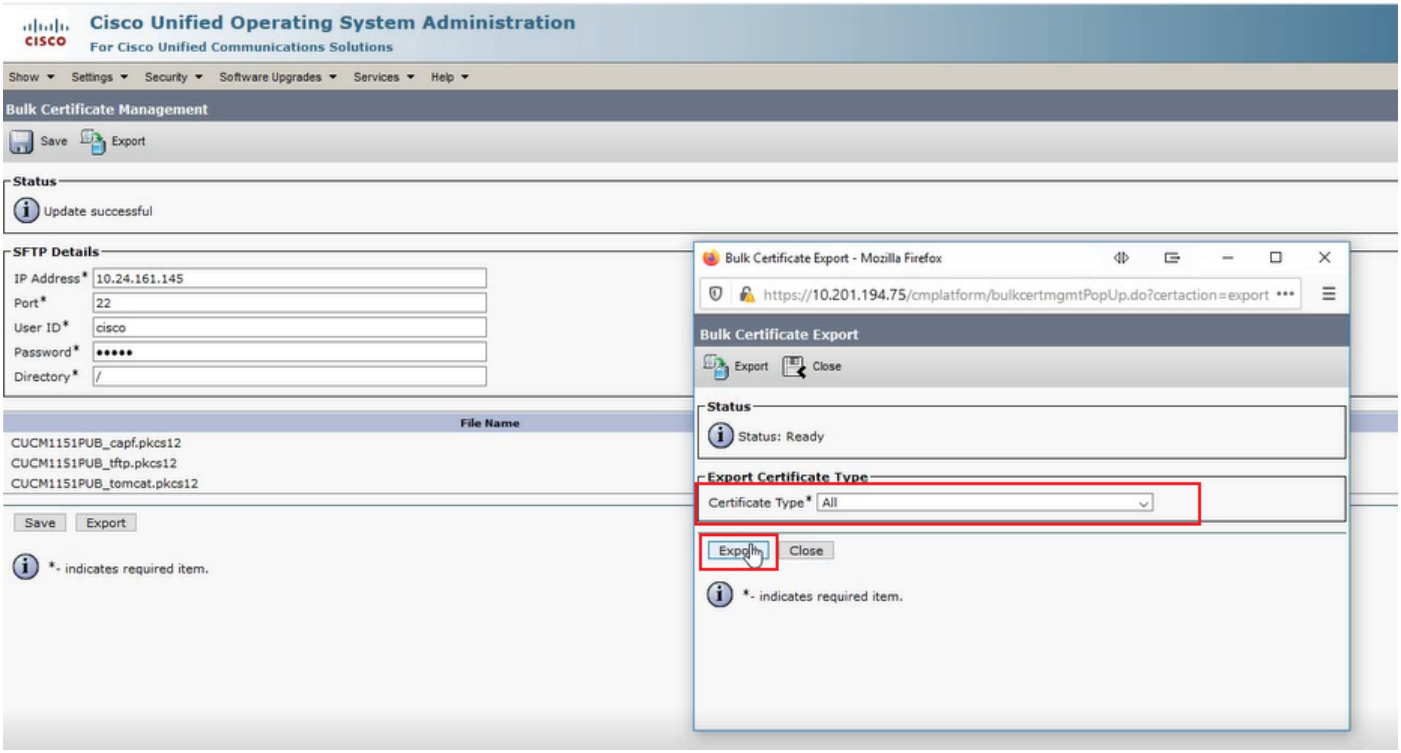
·**Vaya** a **Administración de Cisco Unified OS > Seguridad > Administración de certificados masivos** introduzca los detalles del servidor SFTP y **haga clic en** Exportar, como se muestra en la imagen.

> **Nota:** Los archivos PKCS12 exportados desde el clúster de destino al servidor SFTP se muestran en la página web Bulk Certificate Management del editor de CUCM del clúster de origen cuando se accede a ellos.

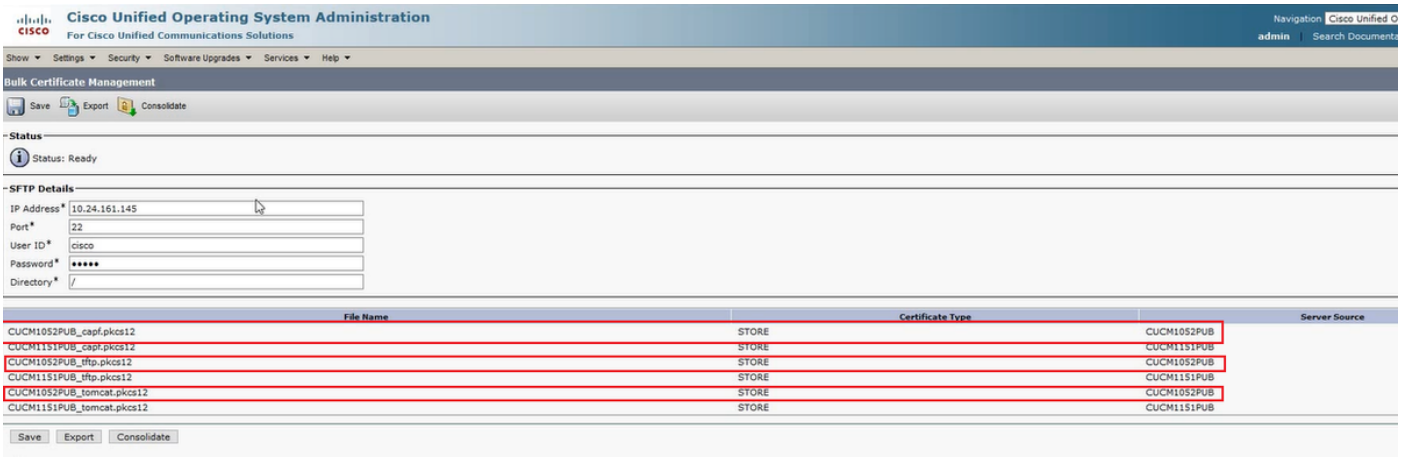


Paso 2. Exportar todos los certificados de todos los nodos del clúster de origen al servidor SFTP.

·En la siguiente ventana emergente, seleccione **Todo** para Tipo de certificado y luego haga clic en **Exportar**, como se muestra en la imagen.



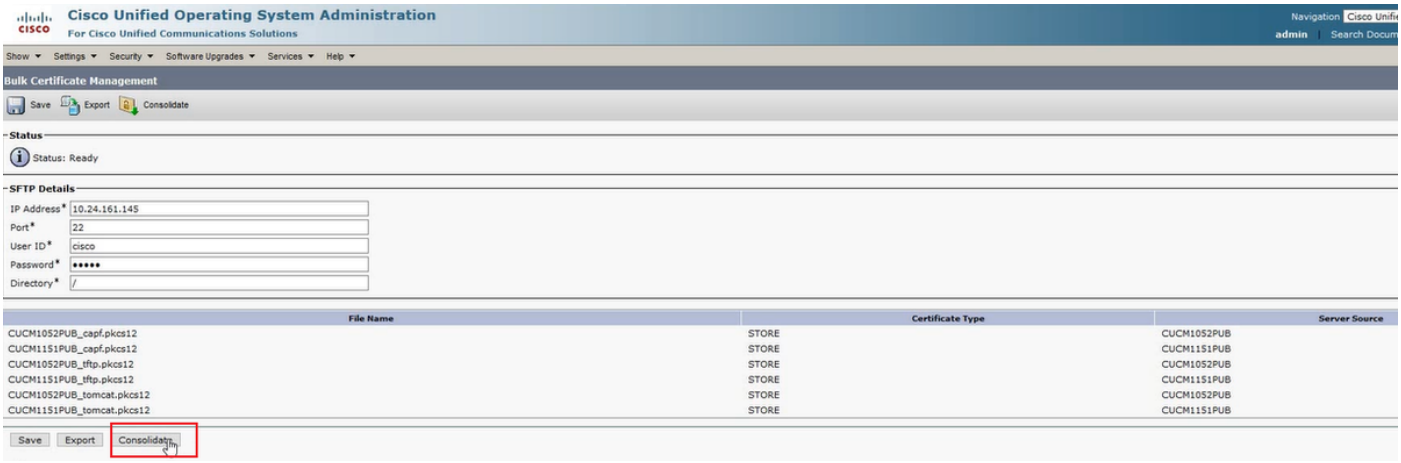
·Cerrar la ventana emergente y las actualizaciones de Bulk Certificate Management con los archivos PKCS12 creados para cada uno de los nodos del clúster de origen, la página web se actualiza con esta información. La página web para Bulk Certificate Management del clúster de origen ahora muestra los archivos PKCS12 de origen y de destino exportados a SFTP, como se muestra en la imagen.



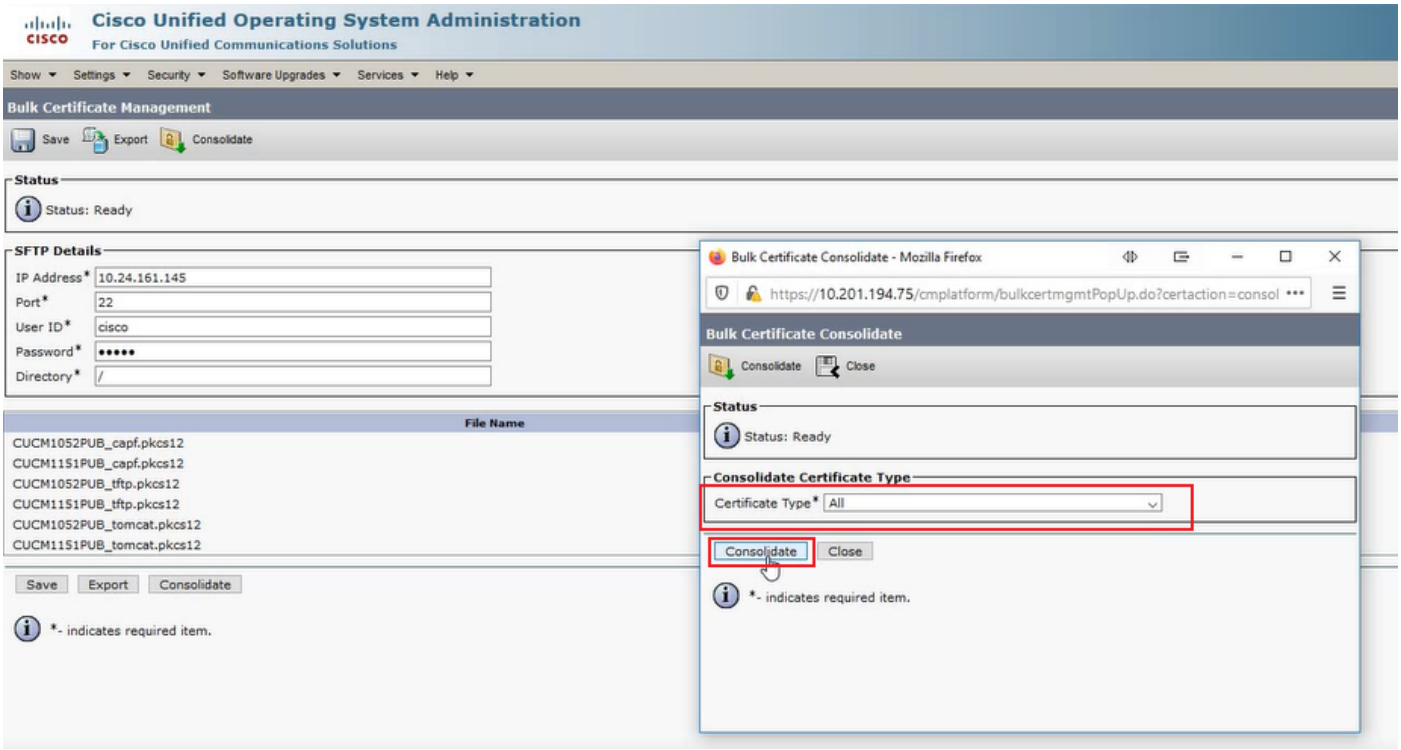
Consolidación de archivos PKCS12 de origen y destino

> **Nota:** Mientras que la exportación de Administración de certificados masivos se realiza tanto en los clústeres de origen como de destino, la consolidación se realiza a través del editor de CUCM en uno solo de los clústeres.

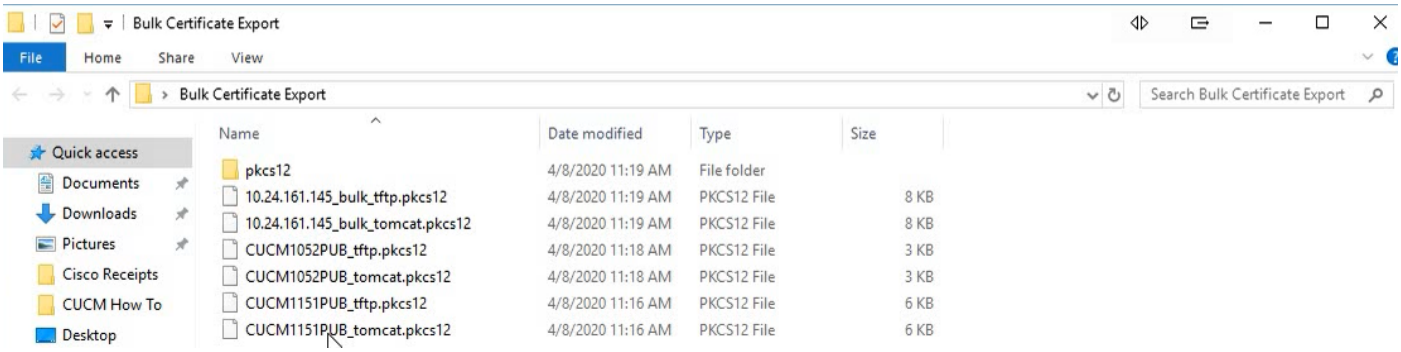
Paso 1. Vuelva a la página Bulk Certificate Management (Administración de certificados masivos) del editor de CUCM del clúster de origen y **haga clic** en Consolidar, como se muestra en la imagen.

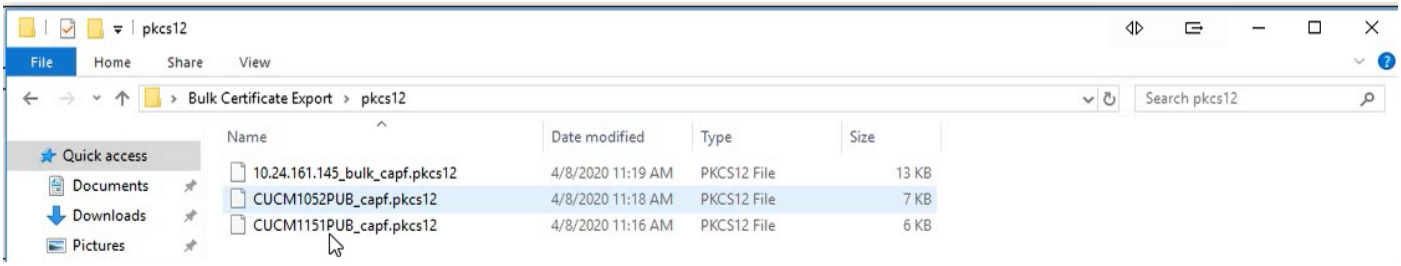


·En la siguiente ventana emergente, seleccione **Todo** para el tipo de certificado y, a continuación, haga clic en **Consolidar**, como se muestra en la imagen.



· En cualquier momento, puede verificar el directorio SFTP para verificar los archivos pkcs12 que están contenidos tanto para los clústeres de origen como de destino. Se ha completado el contenido del directorio SFTP después de exportar todos los certificados de los clústeres de destino y de origen, como se muestra en las imágenes.

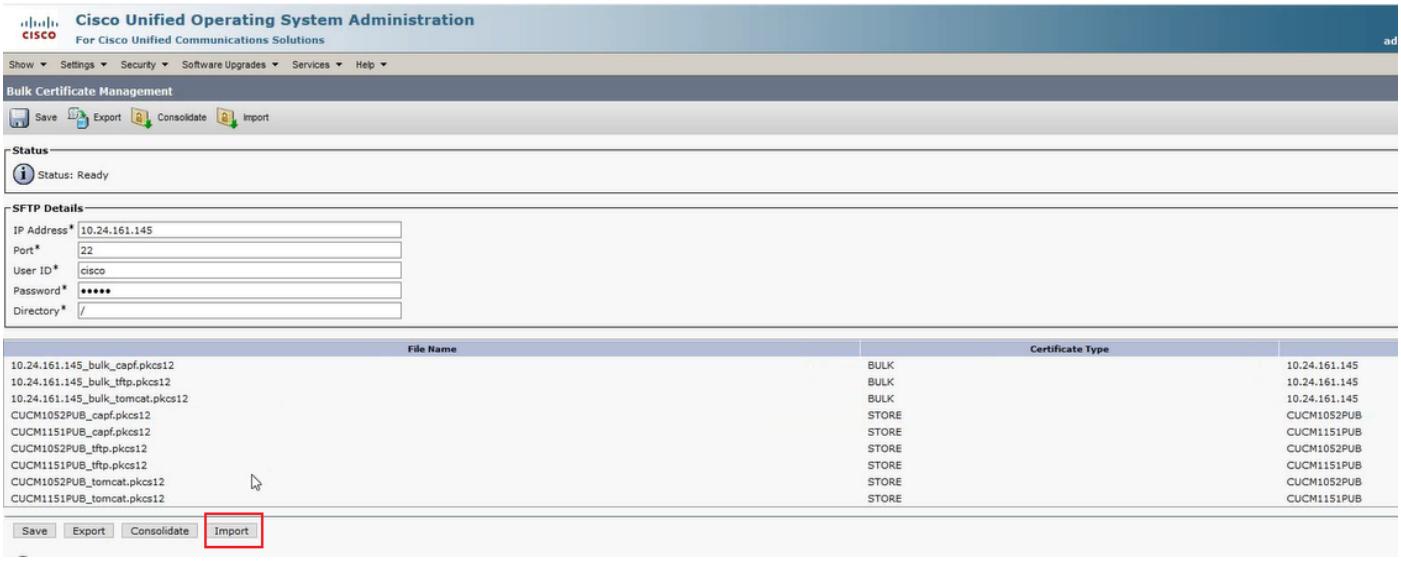




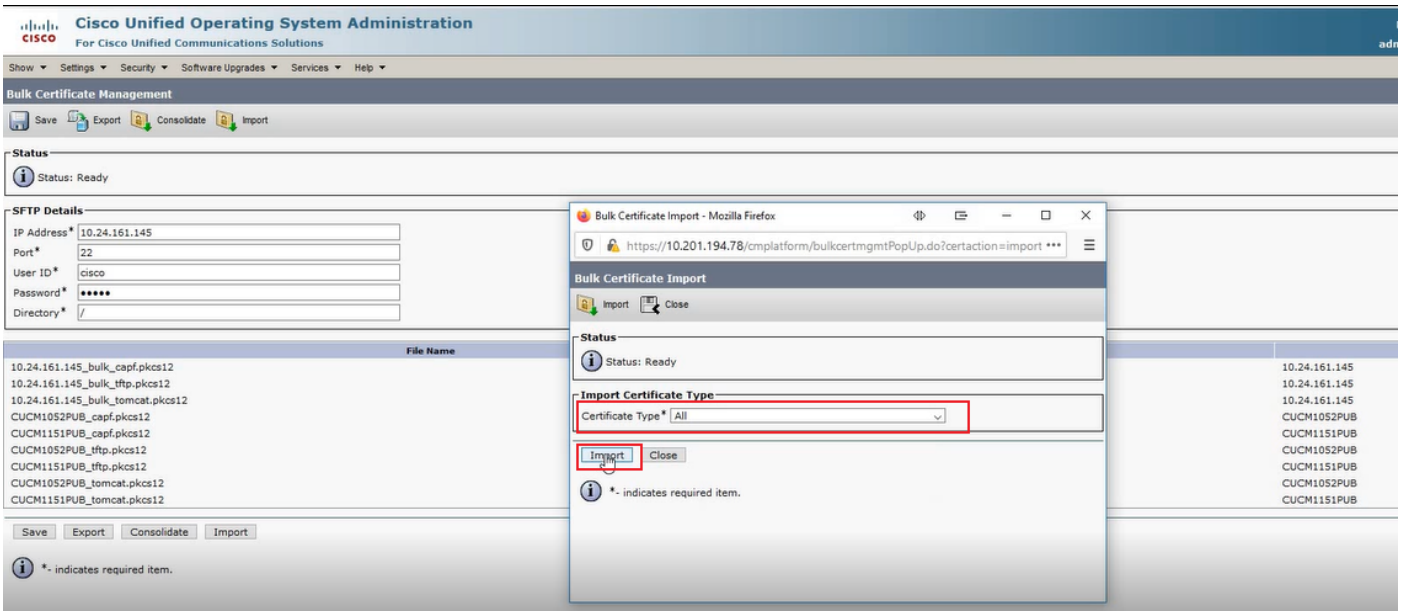
Importar certificados a clústeres de destino y de origen

Paso 1. Importar certificados al clúster de destino

· **en el editor de CUCM del clúster de destino Navegue** a **Administración de Cisco Unified OS > Seguridad > Gestión de certificados masivos** y deje que la página se actualice y, a continuación, haga clic en Importar, como se muestra en la imagen.



·En la siguiente ventana emergente, seleccione **Todo** para Tipo de certificado y luego haga clic en **Importar**, como se muestra en la imagen.



Paso 2. Repita el paso 1 para el clúster de origen.

Nota: Cuando se realiza la importación masiva de certificados, los certificados se cargan en el clúster remoto de la siguiente manera:
Se carga el certificado de función de proxy de autoridad de certificados · (CAPF) como CallManager-trust
·el certificado Tomcat se carga como tomcat-trust
·certificado de CallManager se carga como Phone-SAST-trust y CallManager-trust
El certificado de recuperación de la lista de confianza de identidad · (ITLRecrecovery) se carga como Phone-SAST-trust y CallManager-trust

Configuración de los Teléfonos del Clúster de Origen con Información del Servidor TFTP del Clúster de Destino

Configure el alcance DHCP para los teléfonos de clúster de origen con la opción 150 del protocolo trivial de transferencia de archivos (TFTP) para apuntar a los servidores TFTP de CUCM de clúster de destino.

Restablecer los teléfonos del clúster de origen para obtener el archivo ITL/CTL del clúster de destino para completar el proceso de migración

Como parte del proceso de migración, los teléfonos de clúster de origen intentan configurar una conexión segura al Servicio de verificación de confianza de Cisco (TVS) del clúster de origen para verificar el certificado de recuperación de ITLR o CallManager del clúster de destino.

Nota: El certificado CallManager del clúster de origen de un servidor CUCM que ejecuta el servicio TFTP (también conocido como certificado TFTP) o su certificado ITLRecrecovery firma un archivo de lista de confianza de certificados (CTL) o lista de confianza de identidad (ITL) del nodo CUCM de clúster de origen. De manera similar, el certificado CallManager del clúster de destino de un servidor CUCM que ejecuta el servicio TFTP o su certificado ITLRecrecovery firma un archivo CTL y/o ITL del nodo CUCM del clúster de destino. Los archivos CTL e ITL se crean en los nodos CUCM que ejecutan el servicio TFTP. Si la TVS del clúster de origen no valida el archivo CTL o ITL de un clúster de destino, la migración del teléfono al clúster de destino falla.

Nota: Antes de iniciar el proceso de migración del teléfono del clúster de origen, confirme que estos teléfonos tienen instalado un archivo CTL o ITL válido. Además, asegúrese de que la función empresarial "Prepare Cluster for Rollback to Pre 8.0" esté establecida en False para el clúster de origen. Además, verifique que los nodos CUCM del clúster de destino que ejecutan el servicio TFTP tengan instalados archivos CTL o ITL válidos.

Procesar en clúster no seguro para que los teléfonos de origen obtengan el archivo ITL del clúster de destino para completar la migración de los teléfonos:

Paso 1. Ni el CallManager ni el certificado ITLRecrecovery contenido en el archivo ITL del clúster de destino, que se presenta al teléfono del clúster de origen al restablecer, se pueden utilizar para validar el archivo ITL de instalación actual. Esto hace que el teléfono del clúster de origen establezca una conexión con la TVS del clúster de origen para validar el archivo ITL del clúster de destino.
Paso 2. El teléfono establece una conexión con la TVS del clúster de origen en el puerto TCP 2445.

Paso 3. La TVS del clúster de origen presenta su certificado al teléfono. El teléfono valida la conexión y solicita que la TVS del clúster de origen valide el certificado de recuperación de ITLR o CallManager del clúster de destino para permitir que el teléfono descargue el archivo ITL del clúster de destino.
Paso 4. Después de la validación e instalación del archivo ITL del clúster de destino, el teléfono del clúster de origen ahora puede validar y descargar los archivos de configuración firmados del clúster de destino.

Procesar en clúster seguro para que los teléfonos de origen obtengan el archivo CTL del clúster de destino para completar la migración de los teléfonos:

Paso 1. El teléfono arranca e intenta descargar el archivo CTL del clúster de destino.
Paso 2. El archivo CTL está firmado por el certificado CallManager o ITLRecrecovery del clúster de destino que no está en el archivo CTL o ITL actual del teléfono.
Paso 3. Como resultado, el teléfono llega a TVS en el clúster de origen para verificar el certificado de CallManager o ITLRecrecovery.

> **Nota:** En este momento, el teléfono todavía tiene su configuración antigua que contiene la dirección IP del servicio TVS del clúster de origen. Los servidores TVS especificados en la configuración de teléfonos son los mismos que el grupo Callmanager de teléfonos.

Paso 4. El teléfono configura una conexión de seguridad de la capa de transporte (TLS) a la TVS en el clúster de origen.
Paso 5. Cuando el clúster de origen TVS presenta su certificado al teléfono, el teléfono verifica este certificado TVS con el certificado en su archivo ITL actual.
Paso 6. Si son iguales, el intercambio de señales se completa correctamente.
Paso 7. El teléfono de origen solicita que la TVS del clúster de origen verifique el certificado de CallManager o ITLRecrecovery del archivo CTL del clúster de destino.
Paso 8. El servicio TVS de origen encuentra el clúster de destino CallManager o ITLRecrecovery en su almacén de certificados, lo valida y el teléfono del clúster de origen continúa actualizándose con el archivo CTL del clúster de destino.
Paso 9. El teléfono de origen descarga el archivo ITL del clúster de destino que se valida con el archivo CTL del clúster de destino que ahora contiene. Dado que el archivo CTL del teléfono de origen ahora contiene el certificado de CallManager o ITLRecrecovery del clúster de destino, el teléfono de origen ahora puede verificar el certificado de CallManager o ITLRecrecovery sin necesidad de ponerse en contacto con la TVS del clúster de origen.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Vídeo del tutorial de configuración

Este enlace proporciona acceso a un vídeo que recorre la Administración masiva de certificados entre clústeres de CUCM:

Gestión masiva de certificados entre clústeres de CUCM