Procédure de gestion des certificats en masse entre les clusters CUCM pour la migration des téléphones

Contenu

Introduction

Ce document fournit une procédure d'instructions pour la gestion de certificats en bloc entre les clusters Cisco Unified Communications Manager (CUCM) pour la migration de téléphones.

Avec la collaboration d'Adrian Esquillo, ingénieur TAC Cisco.

> **Note**: Cette procédure est également décrite dans la section Gestion des certificats en vrac du Guide d'administration de CUCM version 12.5(1)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :
Serveur · SFTP (Secure File Transfer Protocol)
Certificats CUCM ·

Components Used

·Les informations de ce document sont basées sur 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La gestion des certificats en bloc permet de partager un ensemble de certificats entre les clusters CUCM. Cette étape est requise pour les fonctions système de clusters individuels qui nécessitent une confiance à établir entre eux, comme pour les clusters EMCC (Extension Mobility Cross Cluster), ainsi que pour la migration des téléphones entre les clusters.

Dans le cadre de cette procédure, un fichier PKCS12 (Public Key Cryptography Standards #12) contenant des certificats de tous les noeuds d'un cluster est créé. Chaque cluster doit exporter ses certificats vers le même répertoire SFTP sur le même serveur SFTP. Les configurations de gestion des certificats en bloc doivent être effectuées manuellement sur l'éditeur CUCM des clusters source et de destination. Les clusters source et de destination doivent être actifs et opérationnels afin que les téléphones à migrer aient une connectivité avec ces deux clusters. Les téléphones du cluster source sont migrés vers le cluster de destination.

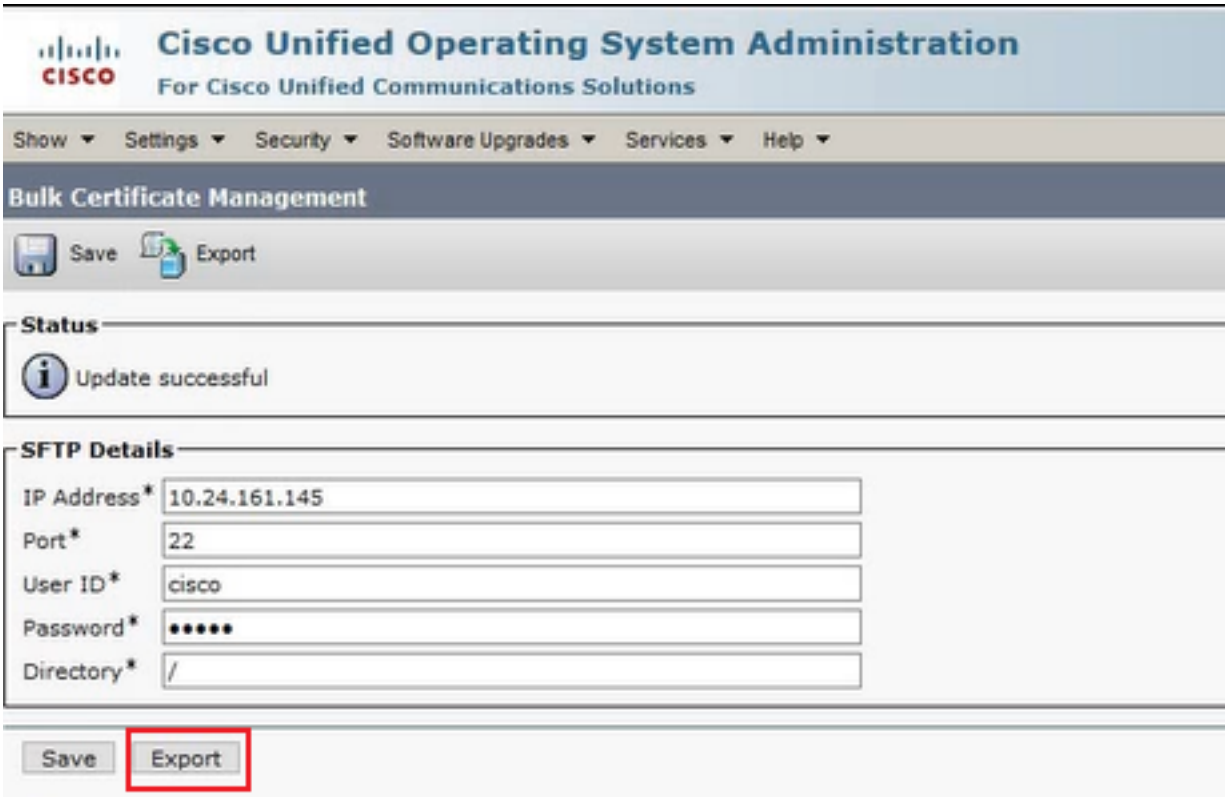
Procédure de gestion des certificats en bloc

Exporter les certificats de cluster de destination

Étape 1. Configurez le serveur SFTP pour Bulk Certificate Management sur l'éditeur CUCM du cluster de destination.

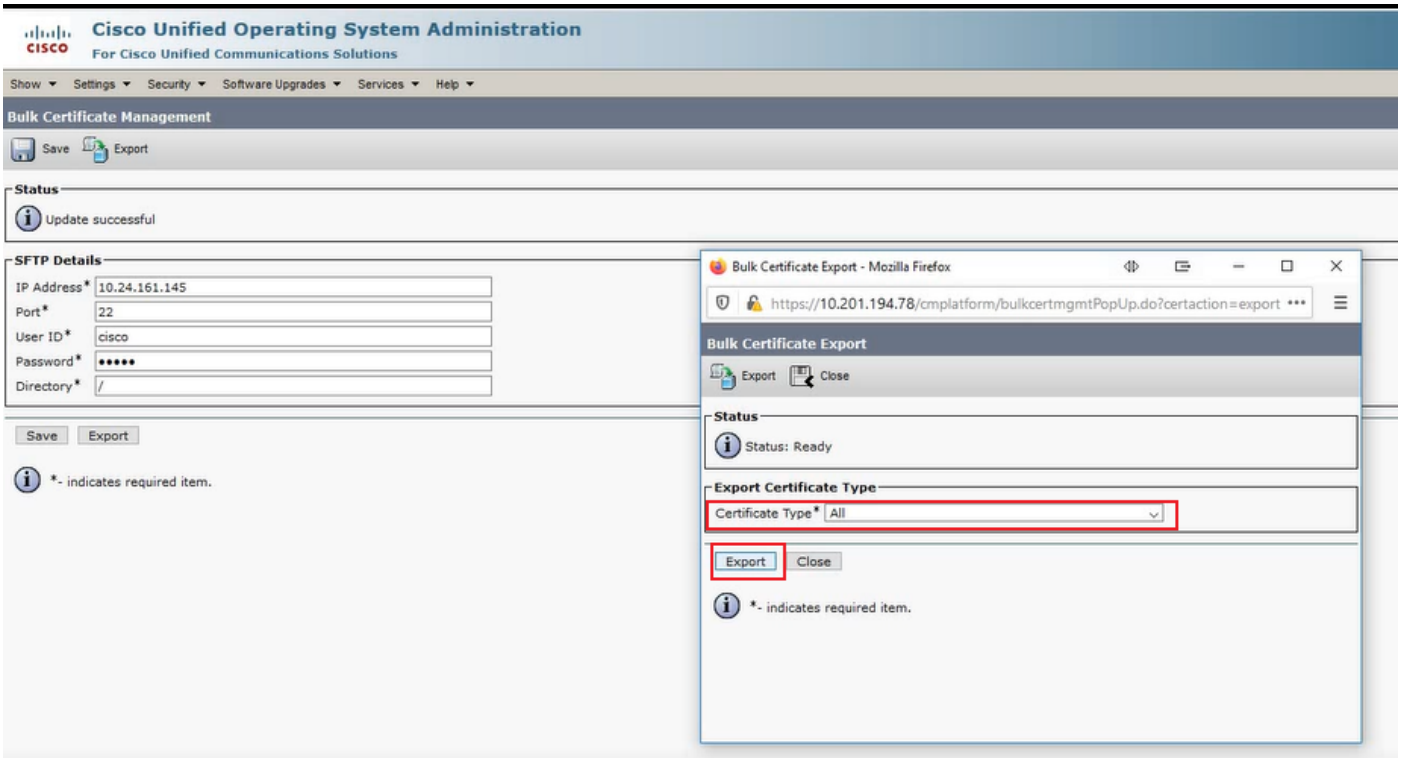
Dans cet exemple, la version CUCM du cluster de destination est 11.5.1.

·**Accédez** à **Cisco Unified OS Administration > Security > Bulk Certificate Management** pour entrer les détails du serveur SFTP et **cliquez sur** Export, comme illustré dans l'image.

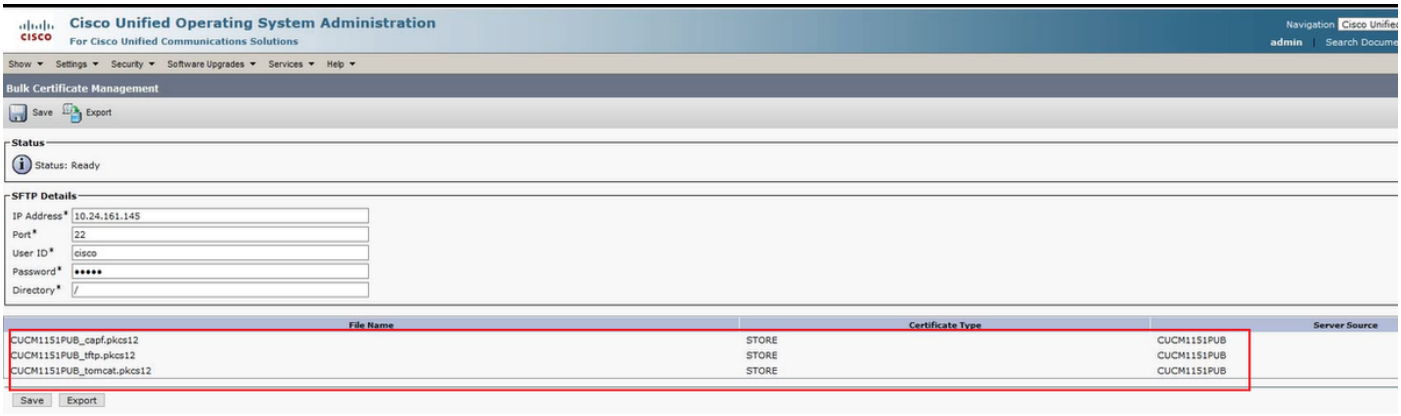


Étape 2. Exporter tous les certificats de tous les noeuds du cluster de destination vers le serveur SFTP.

·Dans la fenêtre contextuelle suivante, sélectionnez **Tout** pour le type de certificat, puis cliquez sur **Exporter**, comme indiqué dans l'image.



·fermez la fenêtre contextuelle et les mises à jour Bulk Certificate Management avec les fichiers PKCS12 créés pour chacun des noeuds du cluster de destination, la page Web est actualisée avec ces informations, comme illustré dans l'image.



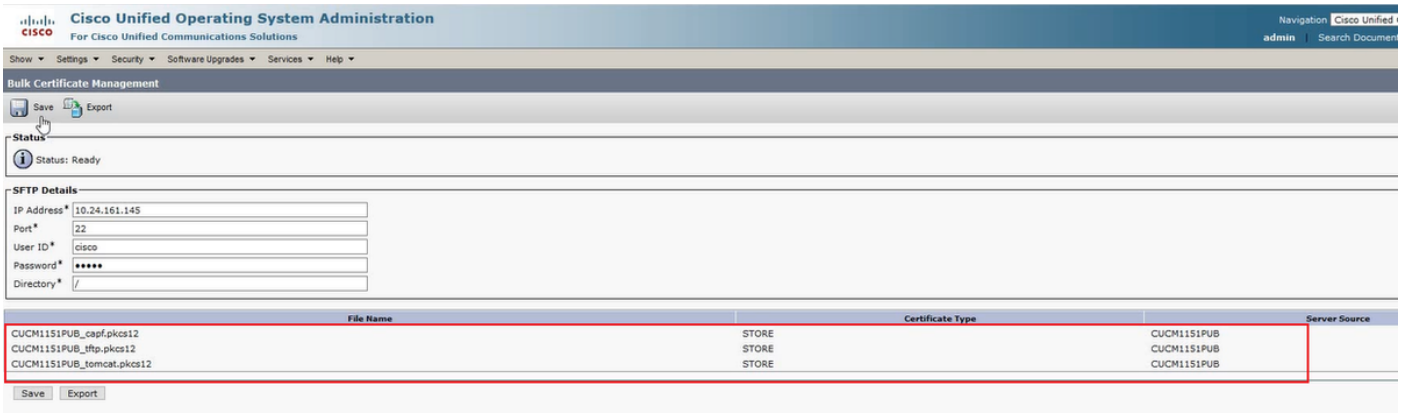
Exporter les certificats de cluster source

Étape 1. Configurez le serveur SFTP pour Bulk Certificate Management sur l'éditeur CUCM du cluster source.

Dans cet exemple, la version CUCM du cluster source est 10.5.2.

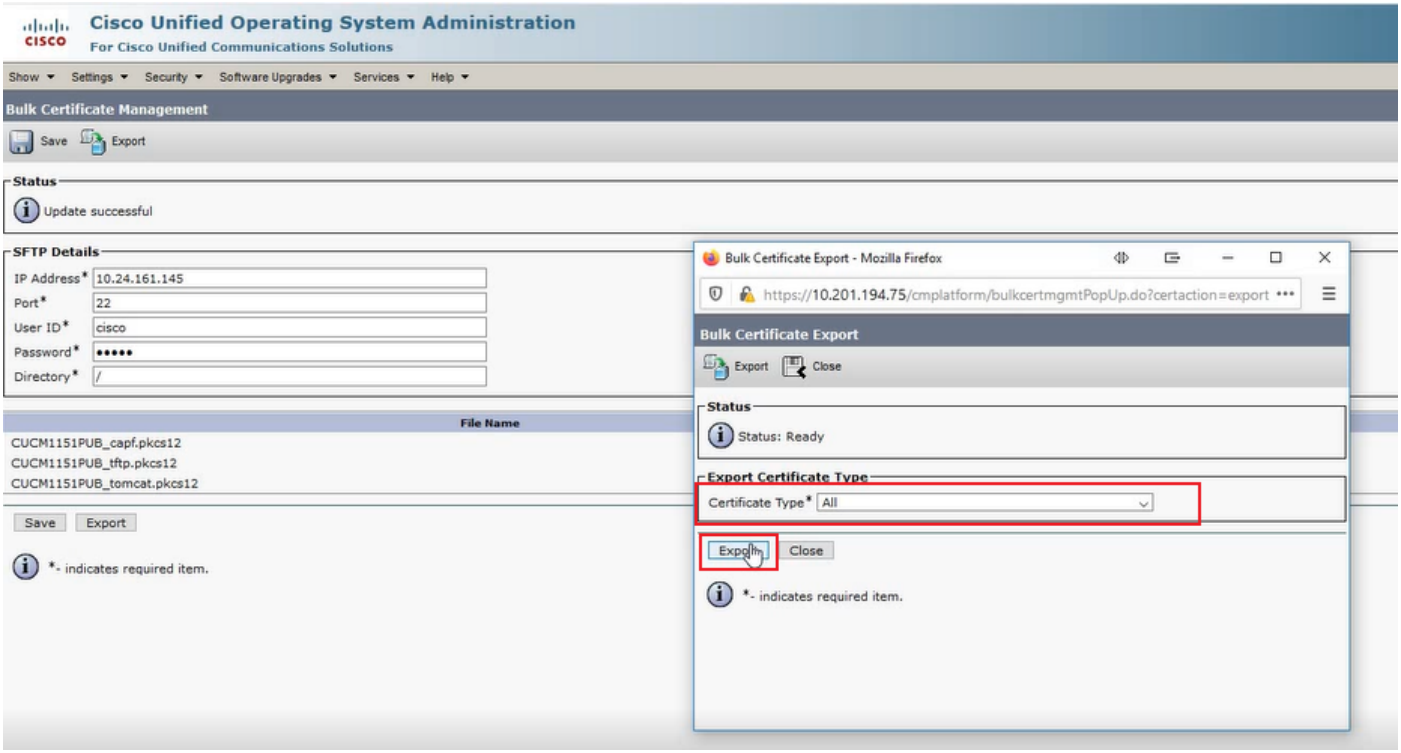
·**Accédez** à **Cisco Unified OS Administration > Security > Bulk Certificate Management** pour entrer les détails du serveur SFTP et **cliquez sur** Export, comme illustré dans l'image.

> **Note**: Les fichiers PKCS12 exportés du cluster de destination vers le serveur SFTP s'affichent sur la page Web Gestion des certificats en bloc de l'éditeur CUCM du cluster source lorsqu'ils sont accessibles.

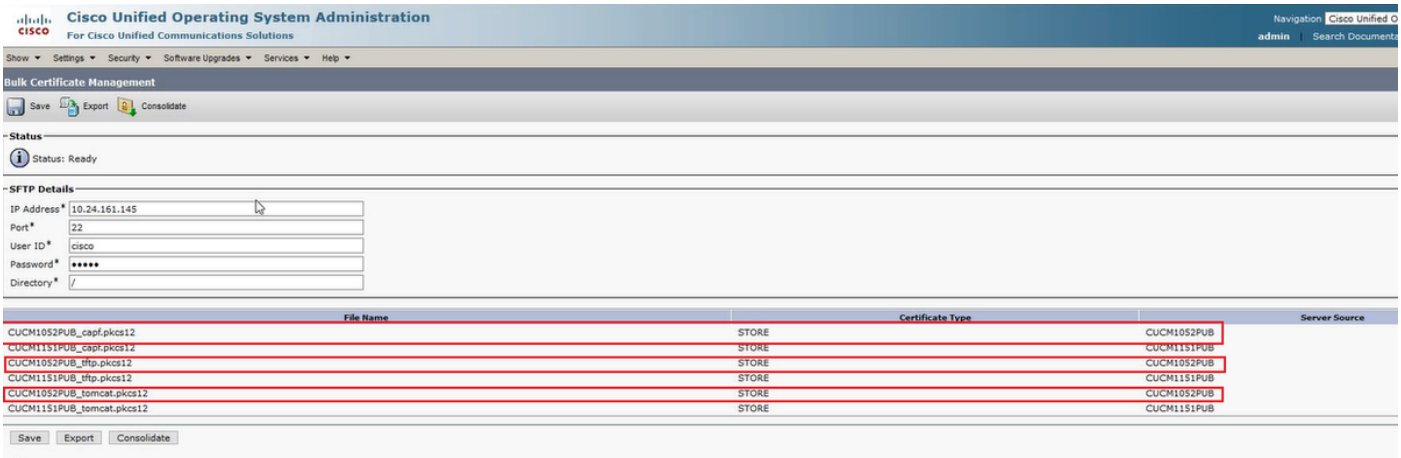


Étape 2. Exporter tous les certificats de tous les noeuds du cluster source vers le serveur SFTP.

·Dans la fenêtre contextuelle suivante, sélectionnez **Tout** pour le type de certificat, puis cliquez sur **Exporter**, comme indiqué dans l'image.



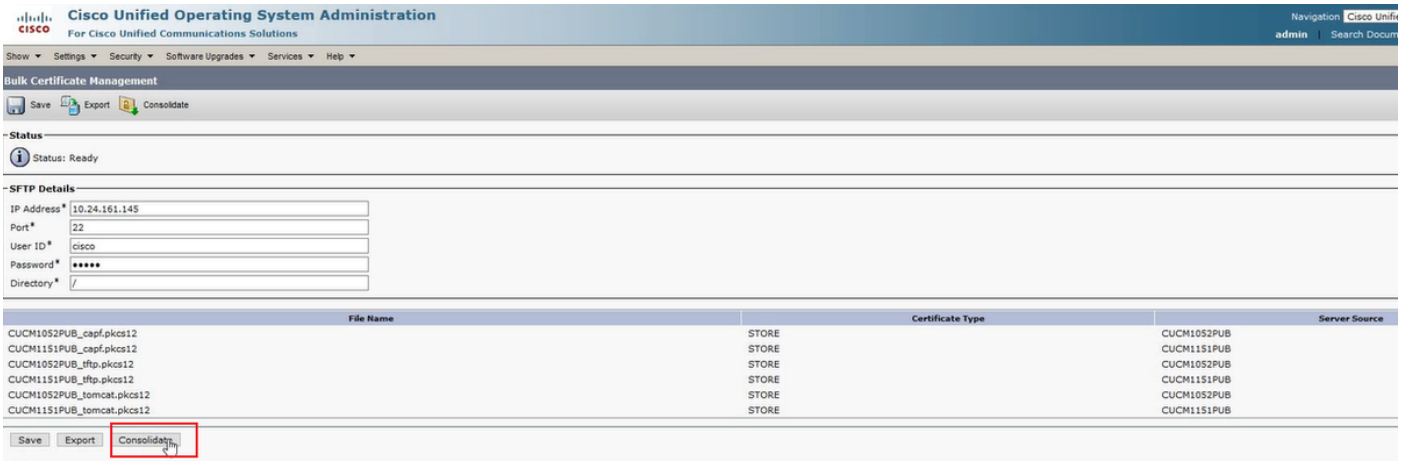
·fermez la fenêtre contextuelle et les mises à jour Bulk Certificate Management avec les fichiers PKCS12 créés pour chacun des noeuds du cluster source, la page Web est actualisée avec ces informations. La page Web Gestion des certificats en bloc du cluster source affiche désormais les fichiers PKCS12 source et de destination exportés vers SFTP, comme l'illustre l'image.



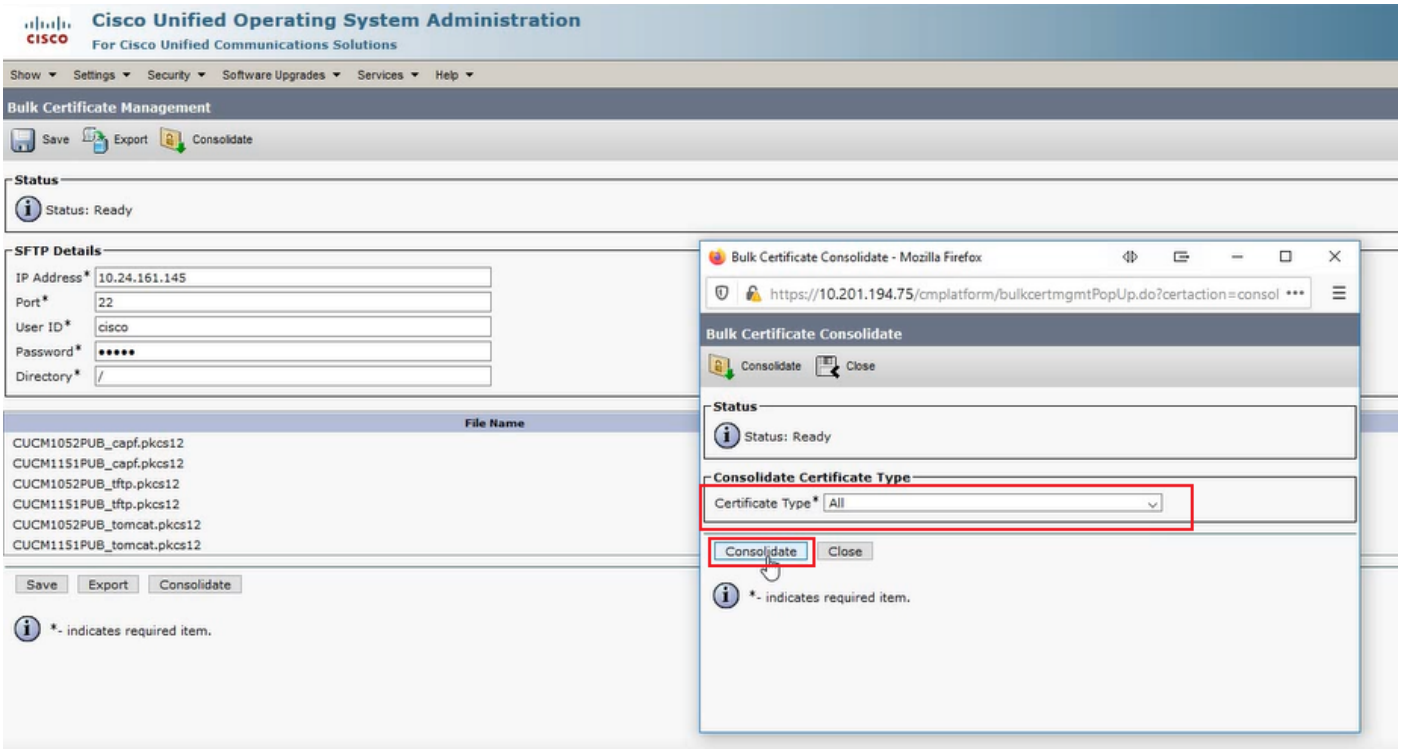
Consolider les fichiers PKCS12 source et de destination

> **Note**: Alors que l'exportation Bulk Certificate Management est effectuée sur les clusters source et de destination, la consolidation est effectuée par l'intermédiaire de l'éditeur CUCM sur un seul des clusters.

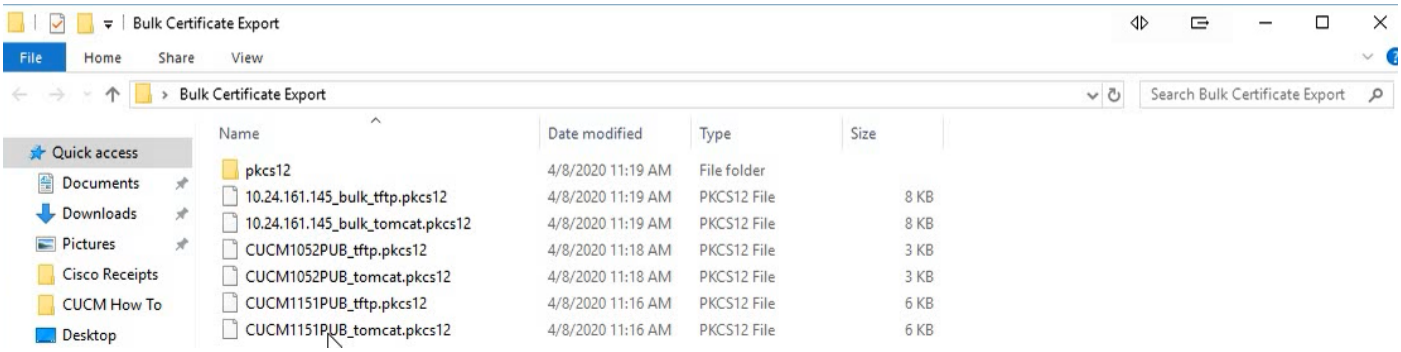
Étape 1. Revenez à la page Bulk Certificate Management de l'éditeur CUCM du cluster source et **cliquez** sur Consolider, comme illustré dans l'image.

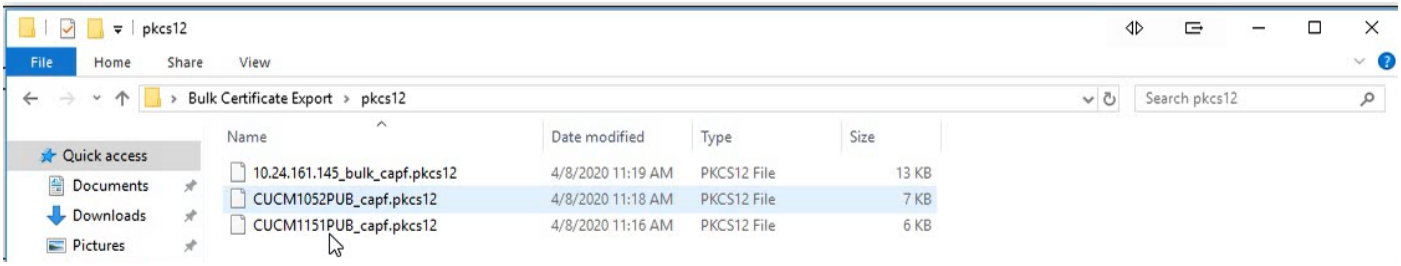


·Dans la fenêtre contextuelle suivante, sélectionnez **Tout** pour le type de certificat, puis cliquez sur **Consolider**, comme illustré dans l'image.



· À tout moment, vous pouvez vérifier le répertoire SFTP pour vérifier les fichiers pkcs12 qui sont contenus pour les clusters source et de destination. Le contenu du répertoire SFTP après l'exportation de tous les certificats des clusters de destination et source a été terminé, comme le montrent les images.

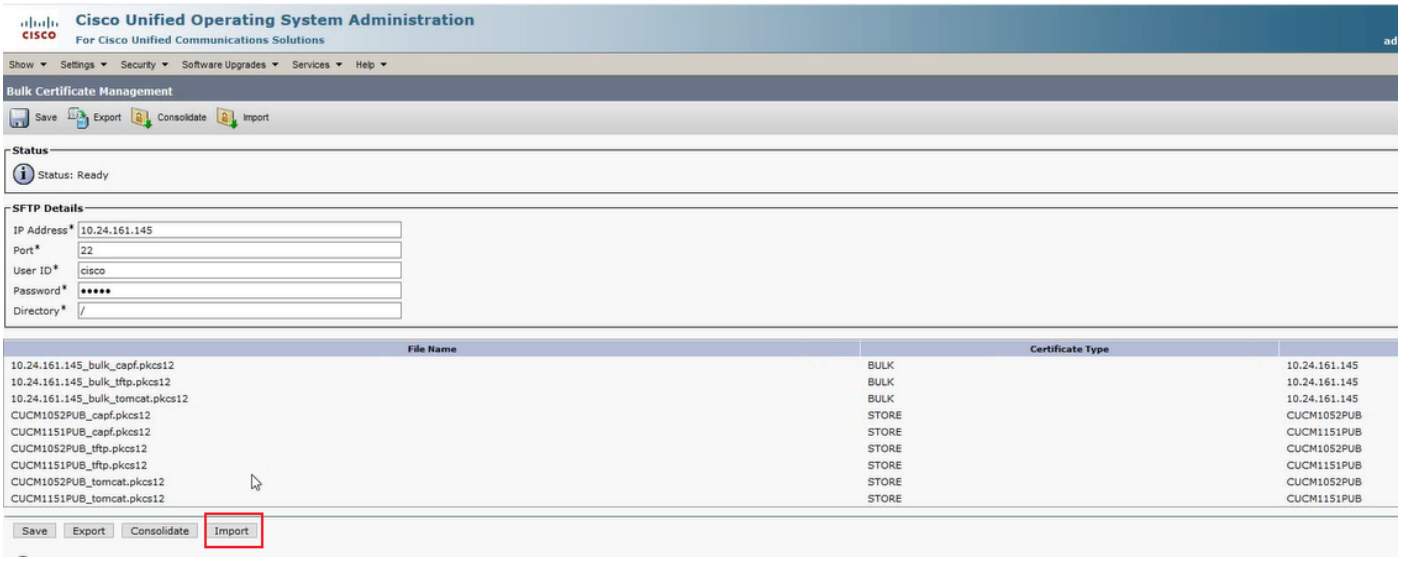




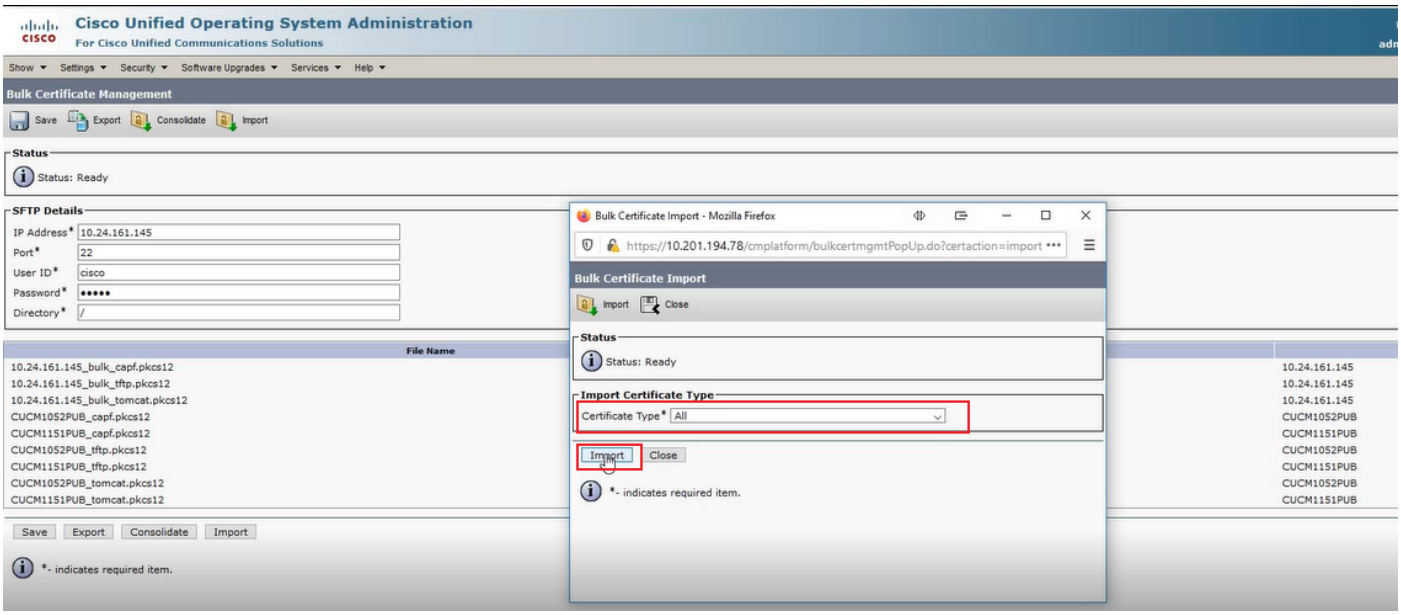
Importer des certificats dans les clusters de destination et source

Étape 1. Importer des certificats dans le cluster de destination

· Sur l'éditeur CUCM du cluster de destination **Accédez** à **Cisco Unified OS Administration > Security > Bulk Certificate Management** et laissez la page s'actualiser, puis **cliquez sur** Import, comme illustré dans l'image.



·Dans la fenêtre contextuelle suivante, sélectionnez **Tout** pour le type de certificat, puis cliquez sur **Importer**, comme indiqué dans l'image.



Étape 2. Répétez l'étape 1 pour le cluster source.

Note: Lorsque l'importation de certificats en bloc est effectuée, les certificats sont téléchargés vers le cluster distant comme suit :
·certificat CAPF (Certificate Authority Proxy Function) est téléchargé en tant que CallManager-trust
·certificat Tomcat est téléchargé en tant que tomcat-trust
·certificat CallManager est téléchargé en tant que Phone-SAST-trust et CallManager-trust
Le certificat · Identity Trust List Recovery (ITLRecovery) est téléchargé en tant que Phone-SAST-trust et CallManager-trust

Configurer les téléphones de cluster source avec les informations du serveur TFTP du cluster de destination

Configurez l'étendue DHCP pour les téléphones de cluster source avec l'option TFTP (Trivial File Transfer Protocol) 150 pour pointer vers les serveurs TFTP CUCM du cluster de destination.

Réinitialiser les téléphones de cluster source pour obtenir le fichier ITL/CTL du cluster de destination afin de terminer le processus de migration

Dans le cadre du processus de migration, les téléphones du cluster source tentent de configurer une connexion sécurisée au service de vérification de confiance (TVS) du cluster source pour vérifier le certificat CallManager ou ITLRecovery du cluster de destination.

Note: Soit le certificat CallManager du cluster source d'un serveur CUCM qui exécute le service TFTP (également appelé certificat TFTP), soit son certificat ITLRecovery signe une liste CTL (Certificate Trust List) et/ou un fichier ITL (Identity Trust List) du noeud CUCM du cluster source. De même, soit le certificat CallManager du cluster de destination d'un serveur CUCM qui exécute le service TFTP, soit son certificat ITLRecovery signe un fichier CTL et/ou ITL du noeud CUCM du cluster de destination. Les fichiers CTL et ITL sont créés sur les noeuds CUCM qui exécutent le service TFTP. Si le fichier CTL et/ou ITL d'un cluster de destination n'est pas validé par le TVS du cluster source, la migration du téléphone vers le cluster de destination échoue.

Note: Avant de démarrer le processus de migration des téléphones du cluster source, vérifiez que ces téléphones ont un fichier CTL et/ou ITL valide installé. Assurez-vous également que la fonction Enterprise « Prepare Cluster for Rollback to Pre 8.0 » a la valeur False pour le cluster source. En outre, vérifiez que les noeuds CUCM du cluster de destination qui exécutent le service TFTP ont des fichiers CTL et/ou ITL valides installés.

Processus dans un cluster non sécurisé pour les téléphones sources afin d'obtenir le fichier ITL du cluster de destination pour terminer la migration des téléphones :

Étape 1. Ni CallManager ni le certificat ITLRecovery contenu dans le fichier ITL du cluster de destination, qui est présenté au téléphone du cluster source lors de la réinitialisation, ne peuvent être utilisés pour valider le fichier ITL actuellement installé. Cela entraîne l'établissement d'une connexion au TVS du cluster source pour valider le fichier ITL du cluster de destination.
Étape 2. Le téléphone établit une connexion à la TVS du cluster source sur le port tcp 2445.
Étape 3. La TVS du cluster source présente son certificat au téléphone. Le téléphone valide la connexion et demande que les TVS du cluster source valident le certificat CallManager ou ITLRecovery du cluster de destination pour permettre au téléphone de télécharger le fichier ITL du

cluster de destination.
Étape 4. Après validation et installation du fichier ITL du cluster de destination, le téléphone du cluster source peut désormais valider et télécharger les fichiers de configuration signés à partir du cluster de destination.

Processus dans le cluster sécurisé pour les téléphones sources afin d'obtenir le fichier CTL du cluster de destination pour terminer la migration des téléphones :

Étape 1. Le téléphone démarre et tente de télécharger le fichier CTL à partir du cluster de destination.
Étape 2. Le fichier CTL est signé par le certificat CallManager ou ITLRecovery du cluster de destination qui ne figure pas dans le fichier CTL ou ITL actuel du téléphone.
Étape 3. Par conséquent, le téléphone communique avec TVS sur le cluster source pour vérifier le certificat CallManager ou ITLRecovery.

> **Note**: À ce stade, l'ancienne configuration du téléphone contient toujours l'adresse IP du service TVS du cluster source. Les serveurs TVS spécifiés dans la configuration des téléphones sont identiques au groupe Callmanager des téléphones.

Étape 4. Le téléphone configure une connexion TLS (Transport Layer Security) à TVS sur le cluster source.
Étape 5. Lorsque le cluster source TVS présente son certificat au téléphone, le téléphone vérifie ce certificat TVS par rapport au certificat dans son fichier ITL actuel.
Étape 6. S'ils sont identiques, la connexion s'effectue correctement.
Étape 7. Le téléphone source demande que les TVS du cluster source vérifient le certificat CallManager ou ITLRecovery à partir du fichier CTL du cluster de destination.
Étape 8. Le service TVS source trouve CallManager ou ITLRecovery du cluster de destination dans son magasin de certificats, le valide et le téléphone du cluster source procède à la mise à jour avec le fichier CTL du cluster de destination.
Étape 9. Le téléphone source télécharge le fichier ITL du cluster de destination qui est validé par rapport au fichier CTL du cluster de destination qu'il contient maintenant. Étant donné que le fichier CTL du téléphone source contient désormais le certificat CallManager ou ITLRecovery du cluster de destination, le téléphone source peut désormais vérifier le certificat CallManager ou ITLRecovery sans avoir à contacter la TVS du cluster source.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Vidéo pas à pas de configuration

Ce lien permet d'accéder à une vidéo qui passe en revue la gestion des certificats en masse entre les clusters CUCM :

Gestion des certificats en masse entre les clusters CUCM