Verfahren für die Verwaltung von Massenzertifikaten zwischen CUCM-Clustern für die Telefonmigration

Inhalt

Einführung

Dieses Dokument enthält eine Anleitung zur Verwaltung der Massenzertifikate zwischen Cisco Unified Communications Manager (CUCM)-Clustern für die Telefonmigration.

Mitarbeiter: Adrian Esquillo, Cisco TAC Engineer.

> **Hinweis**: Dieses Verfahren ist auch im Abschnitt "Massenzertifikate verwalten" des Administrationsleitfadens für CUCM 12.5(1) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:
·Secure File Transfer Protocol (SFTP)-Server
·CUCM-Zertifikate

Verwendete Komponenten

·Die Informationen in diesem Dokument basieren auf CUCM 10.X.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das Massenzertifikatmanagement ermöglicht die gemeinsame Nutzung einer Reihe von Zertifikaten durch CUCM-Cluster. Dieser Schritt ist eine Voraussetzung für Systemfunktionen einzelner Cluster, die eine Vertrauensstellung zwischen ihnen benötigen, z. B. für das Extension Mobility Cross Cluster (EMCC) sowie für die Telefonmigration zwischen Clustern.

Im Rahmen des Verfahrens wird eine PKCS12-Datei (Public Key Cryptography Standards #12) erstellt, die Zertifikate aller Knoten in einem Cluster enthält. Jeder Cluster muss seine Zertifikate in dasselbe SFTP-Verzeichnis auf demselben SFTP-Server exportieren. Massenkonfigurationen der Zertifikatsverwaltung müssen manuell auf dem CUCM-Publisher der Quell- und Ziel-Cluster ausgeführt werden. Die Quell- und Ziel-Cluster müssen betriebsbereit sein, damit die zu migrierenden Telefone über Verbindungen zu beiden Clustern verfügen. Die Quell-Cluster-Telefone werden zum Ziel-Cluster migriert.

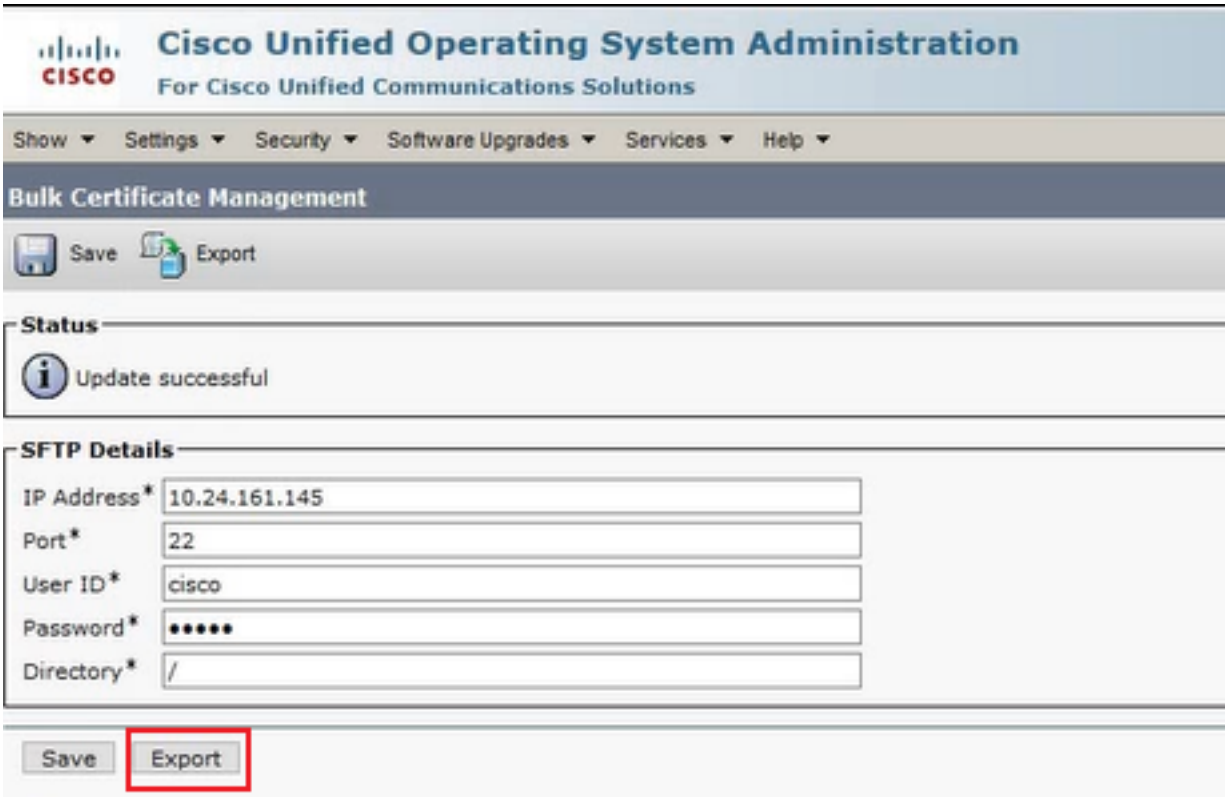
Massenzertifikatmanagement-Verfahren

Export-Ziel-Cluster-Zertifikate

Schritt 1: Konfigurieren Sie den SFTP-Server für die Verwaltung mehrerer Zertifikate auf dem CUCM-Publisher des Ziel-Clusters.

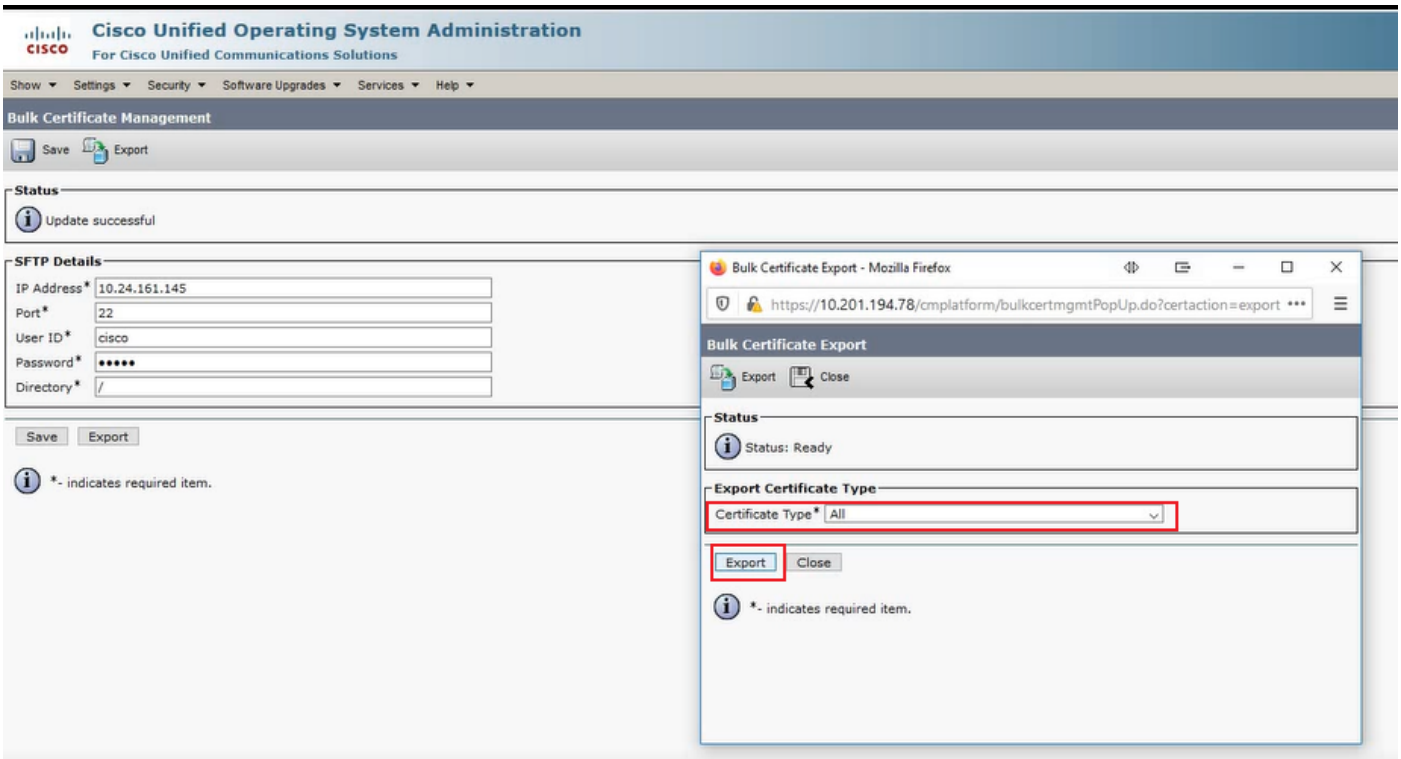
In diesem Beispiel ist die CUCM-Version des Zielclusters 11.5.1.

·**Navigieren Sie** zu **Cisco Unified OS Administration > Security > Bulk Certificate Management**, geben Sie die SFTP-Serverdetails ein, und **klicken Sie** auf Export (Exportieren), wie im Bild gezeigt.

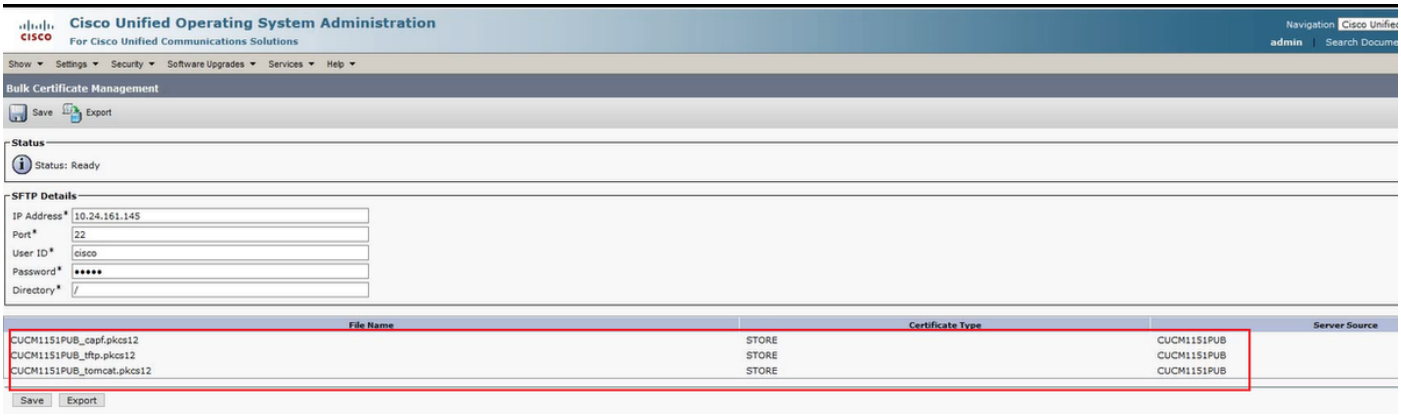


Schritt 2: Exportieren Sie alle Zertifikate von allen Knoten im Ziel-Cluster auf den SFTP-Server.

·Wählen Sie im nachfolgenden Popup-Fenster **All** for Certificate Type (Alle für Zertifikatstyp) aus, und klicken Sie dann auf **Exportieren**, wie im Bild gezeigt.



·Schließen Sie das Popup-Fenster und die Aktualisierung der Massenzertifikatverwaltung mit den PKCS12-Dateien, die für die einzelnen Knoten im Ziel-Cluster erstellt wurden. Die Webseite wird mit diesen Informationen aktualisiert, wie im Bild gezeigt.



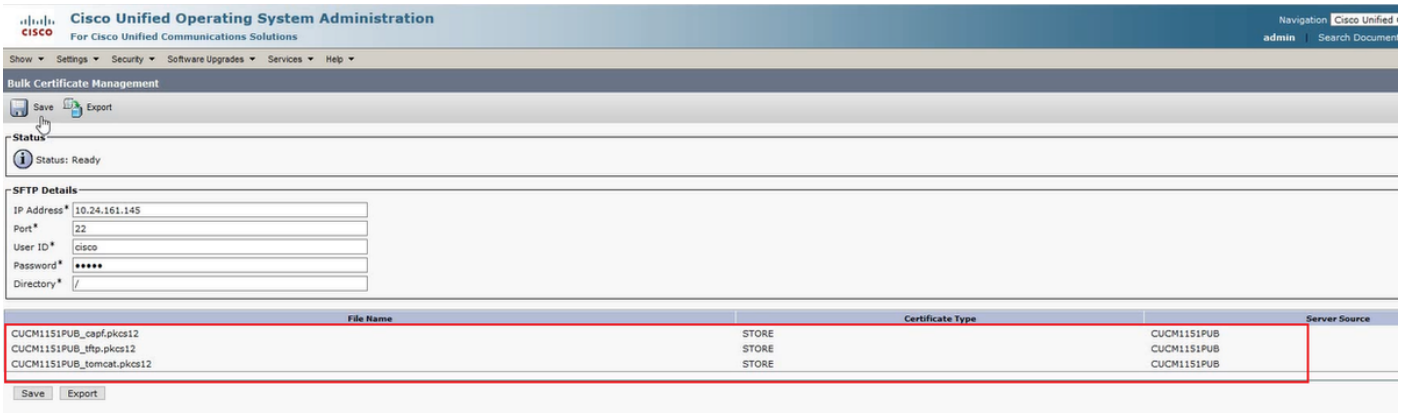
Exportieren von Cluster-Zertifikaten

Schritt 1: Konfigurieren Sie den SFTP-Server für die Verwaltung mehrerer Zertifikate auf dem CUCM-Publisher des Quell-Clusters.

In diesem Beispiel ist die CUCM-Version des Quellclusters 10.5.2.

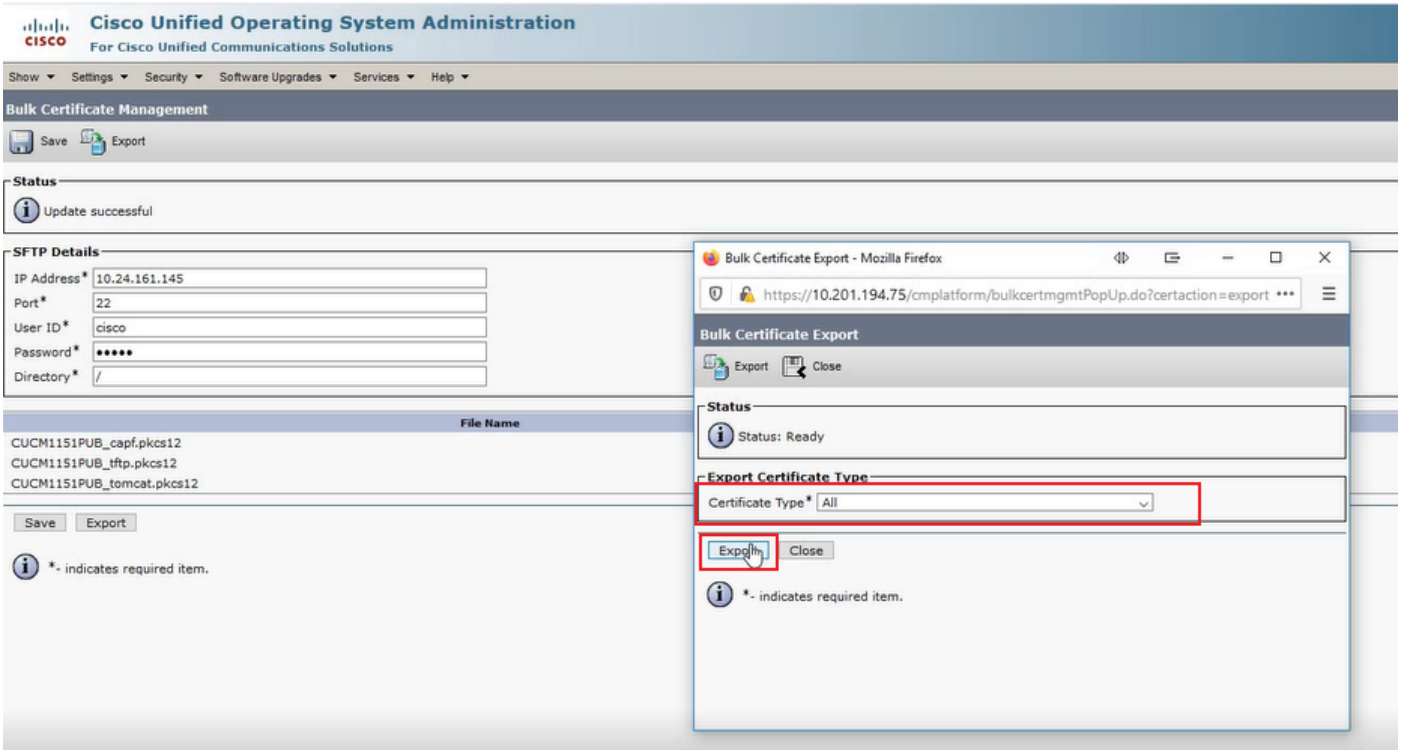
·**Navigieren Sie** zu **Cisco Unified OS Administration > Security > Bulk Certificate Management**, geben Sie die SFTP-Serverdetails ein, und **klicken Sie** auf Export (Exportieren), wie im Bild gezeigt.

> **Hinweis**: Die vom Ziel-Cluster auf den SFTP-Server exportierten PKCS12-Dateien werden beim Zugriff auf die Bulk Certificate Management-Webseite des CUCM-Herausgebers des Quellclusters angezeigt.

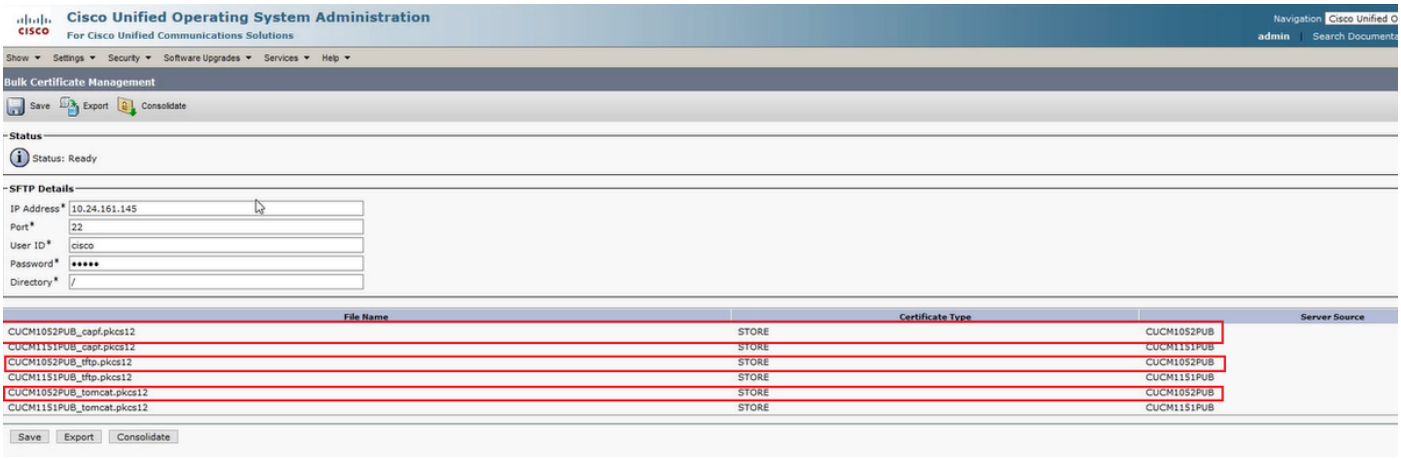


Schritt 2: Exportieren Sie alle Zertifikate von allen Knoten im Quell-Cluster auf den SFTP-Server.

·Wählen Sie im nachfolgenden Popup-Fenster **All** for Certificate Type (Alle für Zertifikatstyp) aus, und klicken Sie dann auf **Exportieren**, wie im Bild gezeigt.



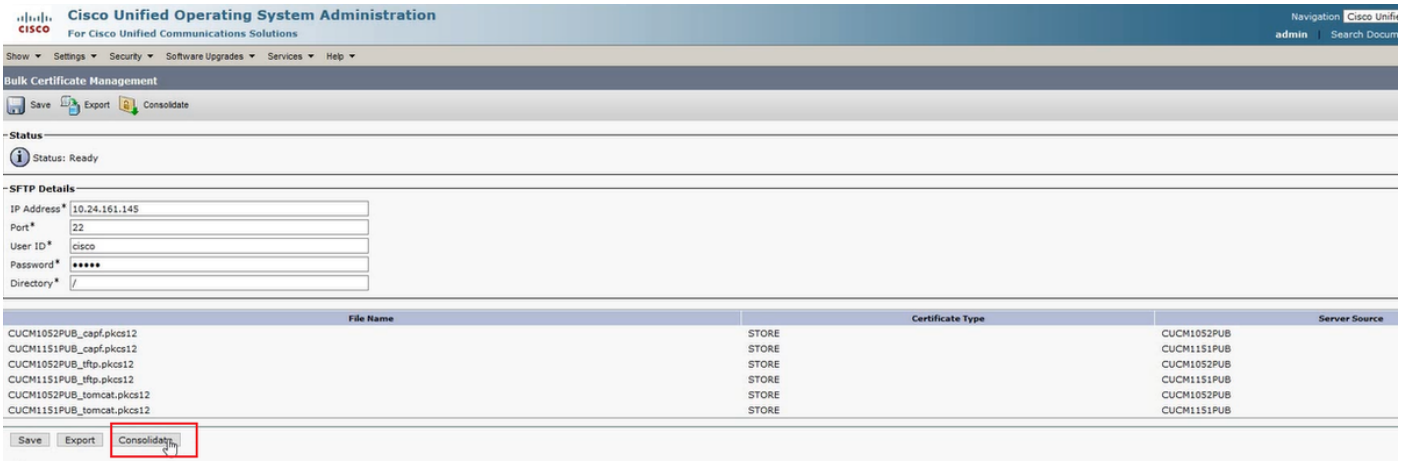
·Schließen Sie das Popup-Fenster, und aktualisieren Sie das Bulk Certificate Management mit den PKCS12-Dateien, die für jeden Knoten im Quellcluster erstellt wurden. Die Webseite wird mit diesen Informationen aktualisiert. Auf der Webseite für das Bulk Certificate Management des Quell-Clusters werden nun sowohl Quell- als auch Ziel-PKCS12-Dateien angezeigt, die nach SFTP exportiert werden, wie im Bild gezeigt.



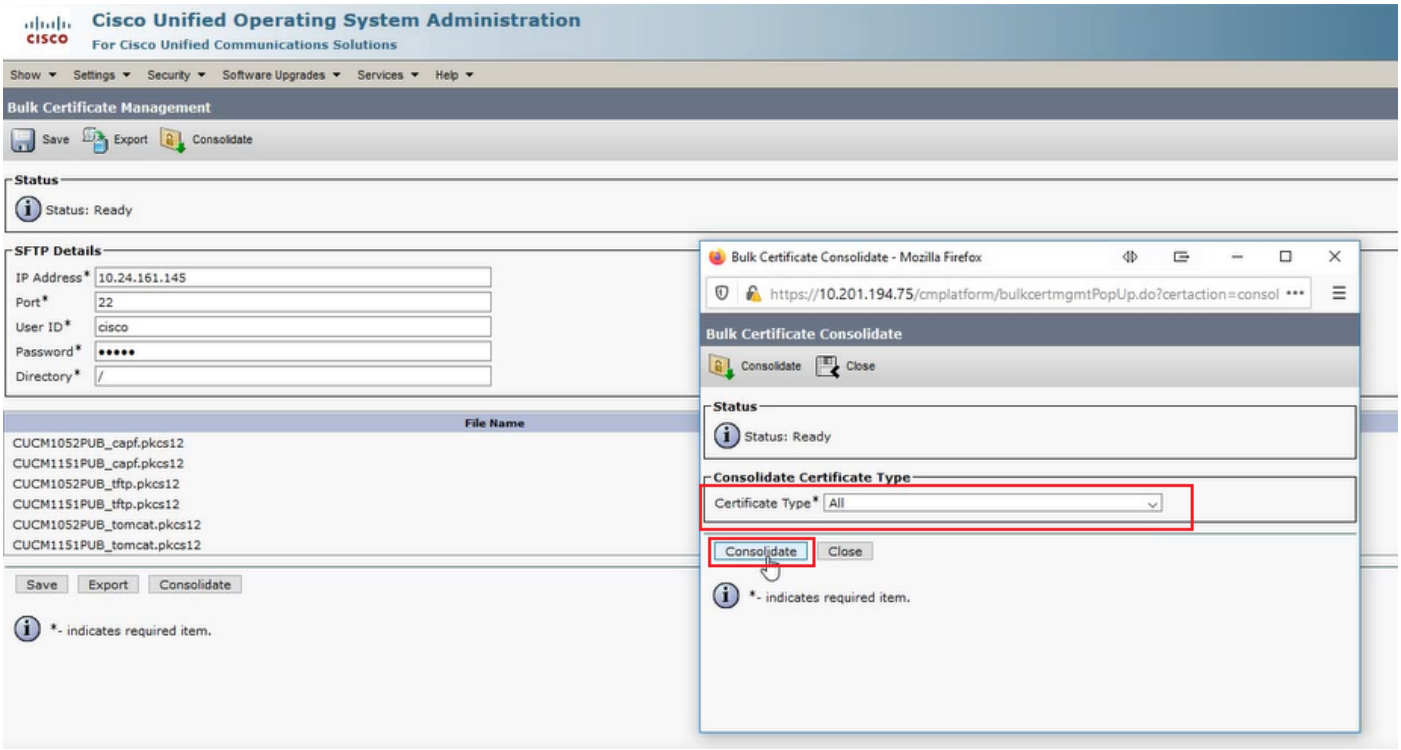
Konsolidieren von Quell- und Ziel-PKCS12-Dateien

> **Hinweis**: Während der Export der Massenzertifikatverwaltung sowohl für die Quell- als auch für die Ziel-Cluster erfolgt, erfolgt die Konsolidierung über den CUCM-Publisher auf nur einem der Cluster.

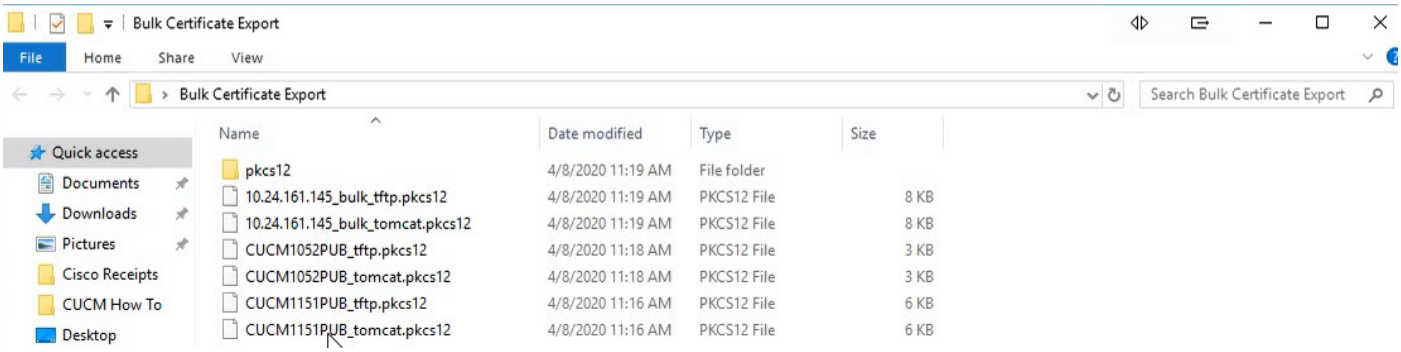
Schritt 1: Kehren Sie zur Seite "Bulk Certificate Management" (Massenzertifikatverwaltung) des CUCM-Herausgebers des Quellclusters zurück, und **klicken Sie** wie im Bild gezeigt auf Consolidate (Konsolidierung).

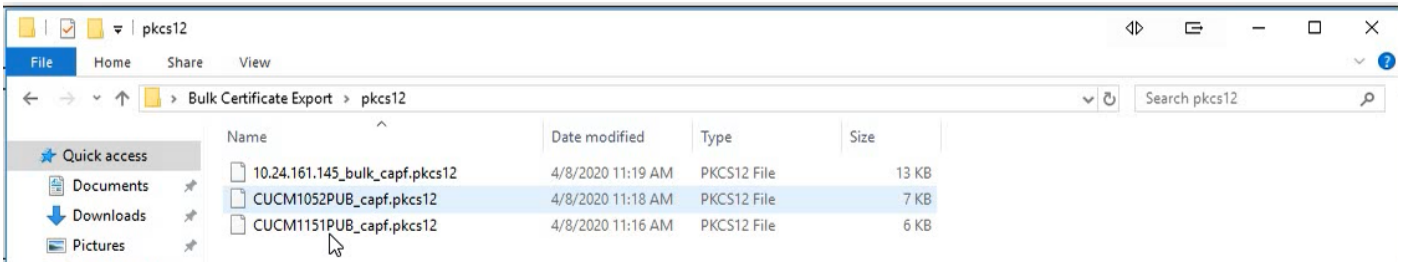


·Wählen Sie im nachfolgenden Popup-Fenster **All** for Certificate Type (Alle für Zertifikatstyp) aus, und klicken Sie dann auf **Consolidate (Konsolidierung)**, wie im Bild gezeigt.



· Sie können jederzeit das SFTP-Verzeichnis überprüfen, um die pkcs12-Dateien zu überprüfen, die sowohl für die Quell- als auch für die Ziel-Cluster enthalten sind. Der Inhalt des SFTP-Verzeichnisses nach dem Exportieren aller Zertifikate aus den Ziel- und Quellclustern wurde abgeschlossen, wie in den Bildern gezeigt.

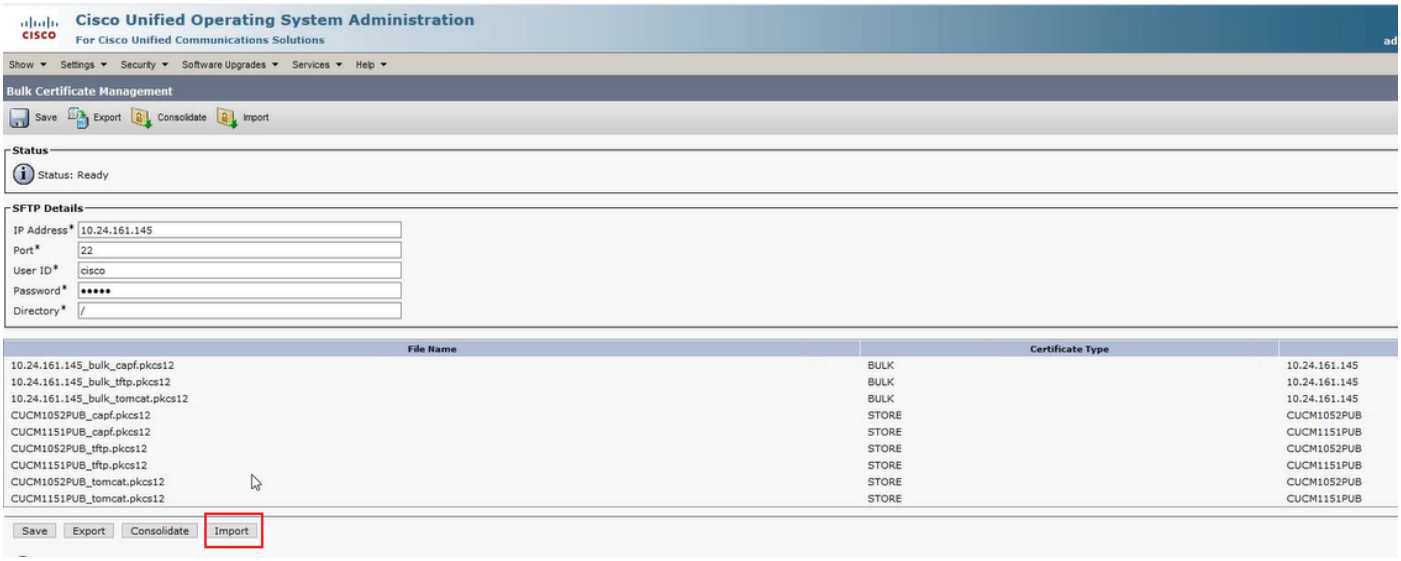




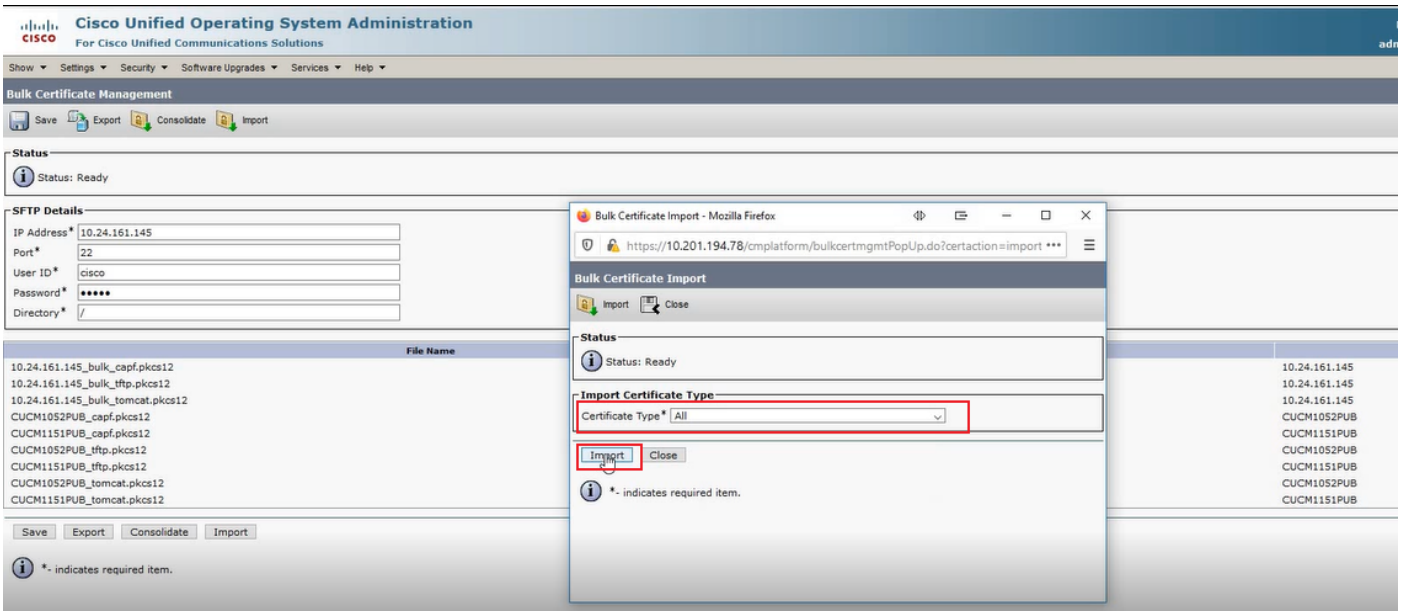
Importieren von Zertifikaten in Ziel- und Quell-Cluster

Schritt 1: Importieren von Zertifikaten in das Ziel-Cluster

· **Navigieren Sie** im CUCM-Publisher des Zielclusters zu **Cisco Unified OS Administration > Security > Bulk Certificate Management** und lassen Sie die Seite aktualisieren. Klicken Sie anschließend **auf** Import (Importieren), wie im Bild gezeigt.



·Wählen Sie im nachfolgenden Popup-Fenster **All** for Certificate Type (Alle für Zertifikatstyp) aus, und klicken Sie dann auf **Importieren**, wie im Bild gezeigt.



Schritt 2: Wiederholen Sie Schritt 1 für das Quell-Cluster.

Hinweis: Beim Importieren von Massenzertifikaten werden die Zertifikate wie folgt in das entfernte Cluster hochgeladen:
·CAPF-Zertifikat (Certificate Authority Proxy Function) wird als CallManager-Vertrauenswürdigkeit hochgeladen
·Tomcat-Zertifikat wird als tomcat-trust hochgeladen
·Das CallManager-Zertifikat wird als Phone-SAST-trust und CallManager-trust hochgeladen.
·Identity Trust List Recovery (ITLRecovery)-Zertifikat wird als Phone-SAST-trust und CallManager-trust hochgeladen

Konfigurieren von Quell-Cluster-Telefonen mit TFTP-Serverinformationen des Ziel-Clusters

Konfigurieren Sie den DHCP-Bereich für Quell-Cluster-Telefone mit der TFTP-Option 150, um auf CUCM-TFTP-Server des Ziel-Clusters zu verweisen.

Zurücksetzen von Quell-Cluster-Telefonen zum Abrufen der ITL-/CTL-Zieldatei für den vollständigen Migrationsprozess

Im Rahmen des Migrationsprozesses versuchen die Quell-Cluster-Telefone, eine sichere Verbindung zum Cisco Trust Verification Service (TVS) des Quell-Clusters herzustellen, um das CallManager- oder ITLR-Wiederherstellungszertifikat des Ziel-Clusters zu überprüfen.

Hinweis: Entweder das CallManager-Zertifikat des Quell-Clusters von einem CUCM-Server, der den TFTP-Dienst ausführt (auch als TFTP-Zertifikat bezeichnet) oder das ITLR-Wiederherstellungszertifikat signiert die CTL-Datei (Certificate Trust List) und/oder die ITL-Datei (Identity Trust List) eines CUCM-Quellknotens. Ebenso signiert entweder das CallManager-Zertifikat des Zielclusters von einem CUCM-Server, der den TFTP-Dienst ausführt, oder das entsprechende ITLRecovery-Zertifikat die CTL- und/oder ITL-Datei eines Ziel-CUCM-Knotens. CTL- und ITL-Dateien werden auf CUCM-Knoten erstellt, auf denen der TFTP-Dienst ausgeführt wird. Wenn die CTL- und/oder ITL-Datei eines Ziel-Clusters nicht vom Quell-Cluster-TVS validiert wird, schlägt die Telefonmigration zum Ziel-Cluster fehl.

Hinweis: Bevor Sie den Migrationsprozess für das Quellclustertelefon starten, stellen Sie sicher, dass auf diesen Telefonen eine gültige CTL- und/oder ITL-Datei installiert ist. Stellen Sie außerdem sicher, dass für das Quell-Cluster die Enterprise-Funktion "Cluster für Rollback auf Pre 8.0 vorbereiten" auf False festgelegt ist. Überprüfen Sie außerdem, ob für die CUCM-Zielcluster-Knoten, die den TFTP-Dienst ausführen, gültige CTL- und/oder ITL-Dateien installiert sind.

Prozess in einem nicht sicheren Cluster für Quelltelefone, um die ITL-Zieldatei des Clusters abzurufen, um die Migration der Telefone abzuschließen:

Schritt 1: Weder der CallManager noch das ITLR-Wiederherstellungszertifikat, das in der ITL-Datei des Zielclusters enthalten ist und dem Quellclustertelefon beim Zurücksetzen angezeigt wird, können zur Validierung der aktuell installierten ITL-Datei verwendet werden. Dies veranlasst das Quell-Cluster-Telefon, eine Verbindung zum TVS des Quell-Clusters herzustellen, um die ITL-Datei des Ziel-Clusters zu validieren.
Schritt 2: Das Telefon stellt eine Verbindung mit dem Quell-Cluster-TVS am TCP-Port 2445 her.

Schritt 3: Das TVS des Quell-Clusters legt dem Telefon sein Zertifikat vor. Das Telefon validiert die Verbindung und fordert das Quell-Cluster-TVS auf, das CallManager- oder ITLR-Wiederherstellungszertifikat des Ziel-Clusters zu validieren, damit das Telefon die ITL-Datei des Ziel-Clusters herunterladen kann.
Schritt 4: Nach der Validierung und Installation der ITL-Datei des Ziel-Clusters kann das Quell-Cluster-Telefon signierte Konfigurationsdateien validieren und vom Ziel-Cluster herunterladen.

Verarbeiten Sie in einem sicheren Cluster für Quelltelefone, um die CTL-Zieldatei des Clusters abzurufen, um die Telefone vollständig zu migrieren:

Schritt 1: Das Telefon startet und versucht, die CTL-Datei vom Ziel-Cluster herunterzuladen.
Schritt 2: Die CTL-Datei wird vom CallManager- oder ITLR-Wiederherstellungszertifikat des Zielclusters signiert, das sich nicht in der aktuellen CTL- oder ITL-Datei des Telefons befindet.
Schritt 3: Daher erreicht das Telefon das TVS im Quell-Cluster, um das CallManager- oder ITLR-Wiederherstellungszertifikat zu überprüfen.

> Hinweis: Zu diesem Zeitpunkt verfügt das Telefon noch über seine alte Konfiguration, die die IP-Adresse des Quell-Cluster-TVS-Dienstes enthält. Die in der Telefonkonfiguration angegebenen TVS-Server entsprechen denen der CallManager-Telefongruppe.

Schritt 4: Das Telefon richtet eine TLS-Verbindung (Transport Layer Security) zum TVS im Quell-Cluster ein.
Schritt 5: Wenn der Quell-Cluster TVS dem Telefon sein Zertifikat vorlegt, überprüft das Telefon dieses TVS-Zertifikat anhand des Zertifikats in der aktuellen ITL-Datei.
Schritt 6: Wenn sie identisch sind, wird der Handshake erfolgreich abgeschlossen.
Schritt 7: Das Quelltelefon fordert vom Quell-Cluster-TVS die Überprüfung des CallManager- oder ITLR-Wiederherstellungszertifikats aus der CTL-Datei des Zielclusters an.
Schritt 8: Der Quell-TVS-Dienst findet den Ziel-Cluster-CallManager oder die ITLR-Wiederherstellung in seinem Zertifikatsspeicher, validiert diesen und das Quell-Cluster-Telefon wird mit der CTL-Datei des Ziel-Clusters aktualisiert.
Schritt 9: Das Quelltelefon lädt die ITL-Datei des Ziel-Clusters herunter, die anhand der CTL-Zieldatei des Zielclusters validiert wird, die es jetzt enthält. Da die CTL-Datei des Quelltelefons jetzt das CallManager- oder ITLR-Wiederherstellungszertifikat des Zielclusters enthält, kann das Quelltelefon jetzt das CallManager- oder ITLRecovery-Zertifikat überprüfen, ohne dass eine Verbindung zum TVS des Quellclusters hergestellt werden muss.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Exemplarische Konfigurationsanleitung - Video

Dieser Link bietet Zugriff auf ein Video, das die Verwaltung mehrerer Zertifikate zwischen CUCM-Clustern durchläuft:

Massenzertifikatverwaltung zwischen CUCM-Clustern