Procedura per la gestione di massa dei certificati tra cluster CUCM per la migrazione telefonica

Sommario

Introduzione

In questo documento viene descritta una procedura per la gestione di massa dei certificati tra cluster Cisco Unified Communications Manager (CUCM) per la migrazione telefonica.

Contributo di Adrian Esquillo, Cisco TAC Engineer.

> **Nota:** Questa procedura è descritta anche nella sezione relativa alla gestione dei certificati di massa del manuale Administration Guide for CUCM release 12.5(1)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:
·Server SFTP (Secure File Transfer Protocol)
·Certificati CUCM

Componenti usati

·Le informazioni fornite in questo documento si basano su CUCM 10.X.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La gestione in blocco dei certificati consente la condivisione di un insieme di certificati tra cluster CUCM. Questo passaggio è necessario per le funzioni di sistema di singoli cluster che richiedono una relazione di trust tra di essi, ad esempio per le funzionalità di mobilità di estensione tra cluster (EMCC), nonché per la migrazione telefonica tra cluster.

Come parte della procedura, viene creato un file PKCS12 (Public Key Cryptography Standards #12) contenente i certificati di tutti i nodi di un cluster. Ogni cluster deve esportare i propri certificati nella stessa directory SFTP sullo stesso server SFTP. Le configurazioni di gestione in blocco dei certificati devono essere eseguite manualmente sull'editore CUCM dei cluster di origine e di destinazione. I cluster di origine e di destinazione devono essere attivi e operativi in modo che i telefoni da migrare dispongano di connettività a entrambi i cluster. I telefoni del cluster di origine vengono migrati nel cluster di destinazione.

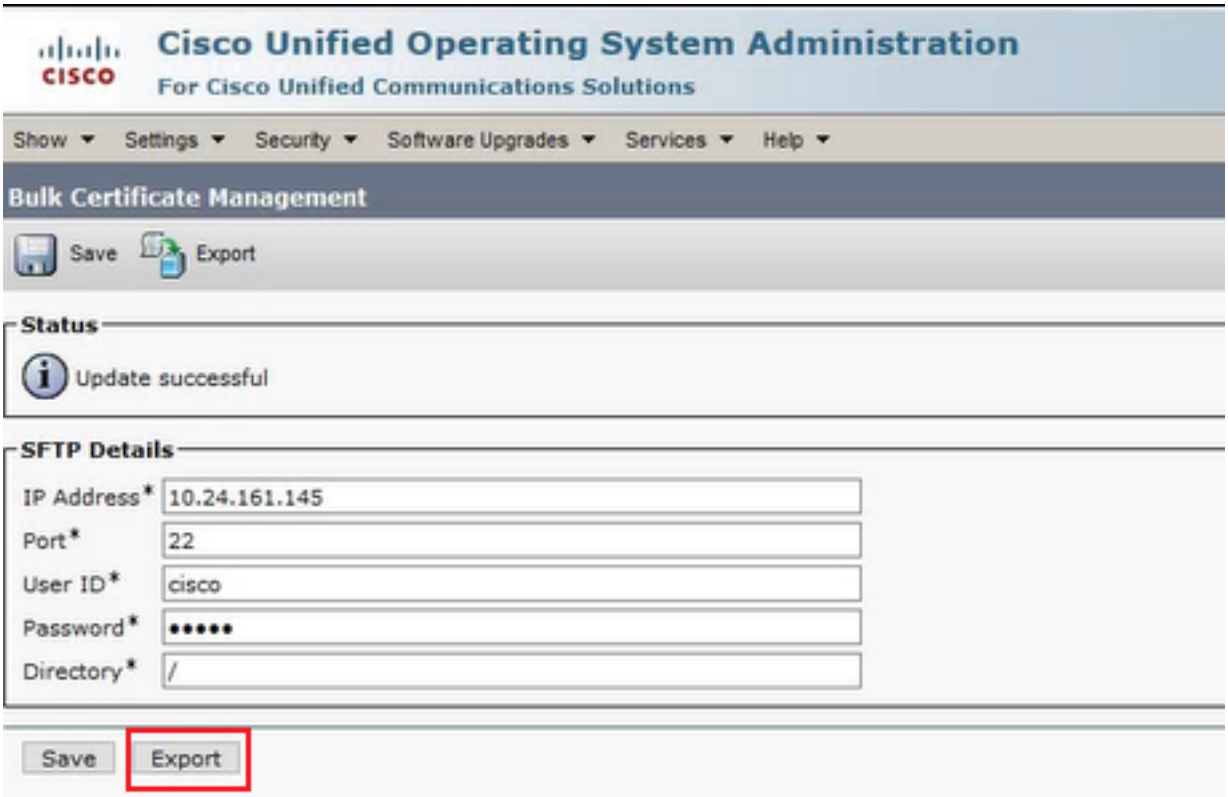
Procedura di gestione in blocco dei certificati

Esporta certificati cluster di destinazione

Passaggio 1. Configurare il server SFTP per la gestione di massa certificati sul server di pubblicazione CUCM del cluster di destinazione.

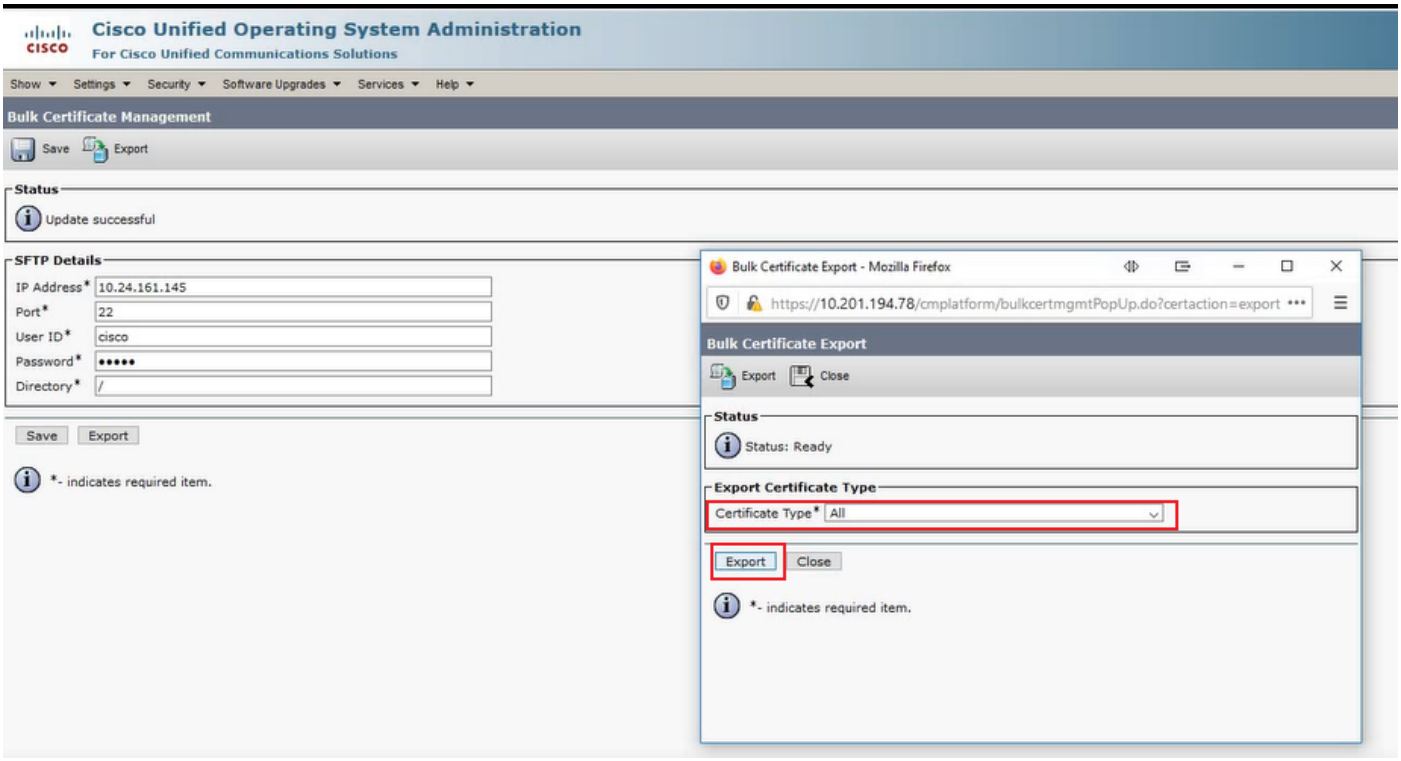
In questo esempio, la versione CUCM del cluster di destinazione è 11.5.1.

·**Passare** a **Cisco Unified OS Administration > Security > Bulk Certificate Management.** Immettere i dettagli del server SFTP e **fare clic su** Esporta, come mostrato nell'immagine.

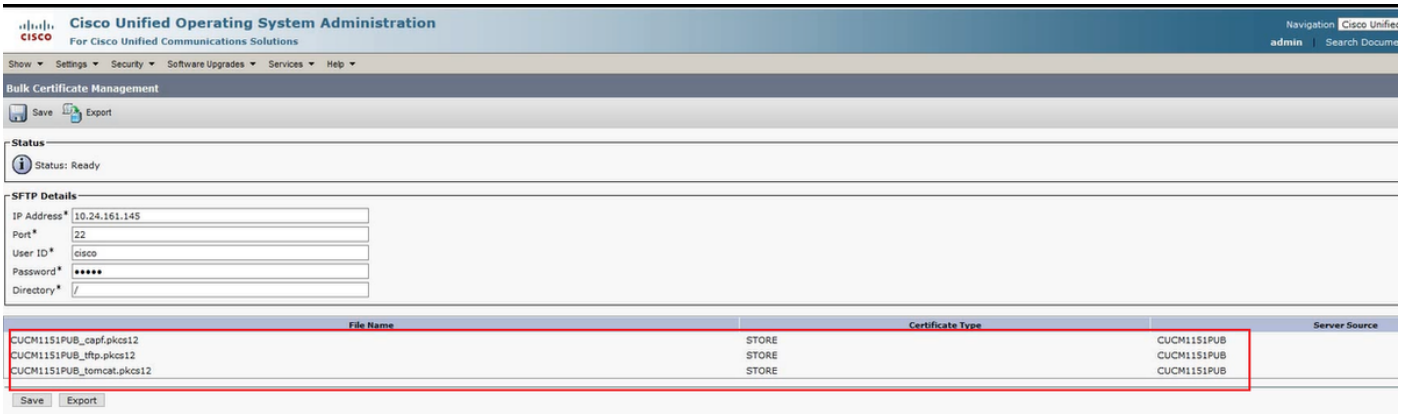


Passaggio 2. Esportare tutti i certificati da tutti i nodi nel cluster di destinazione al server SFTP.

·Nella successiva finestra popup, selezionare **All** per Certificate Type (Tipo di certificato), quindi fare clic su **Export** (Esporta), come mostrato nell'immagine.



·Chiudere la finestra popup e aggiornare Gestione bulk dei certificati con i file PKCS12 creati per ogni nodo nel cluster di destinazione. La pagina Web viene aggiornata con queste informazioni, come mostrato nell'immagine.



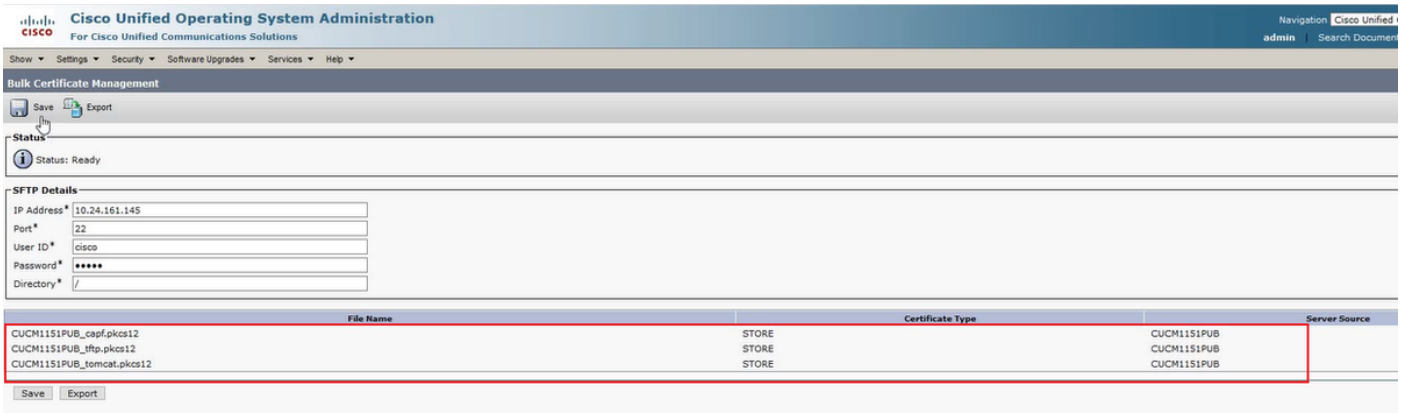
Esporta certificati cluster di origine

Passaggio 1. Configurare il server SFTP per la gestione di massa certificati sul server di pubblicazione CUCM del cluster di origine.

In questo esempio, la versione CUCM del cluster di origine è 10.5.2.

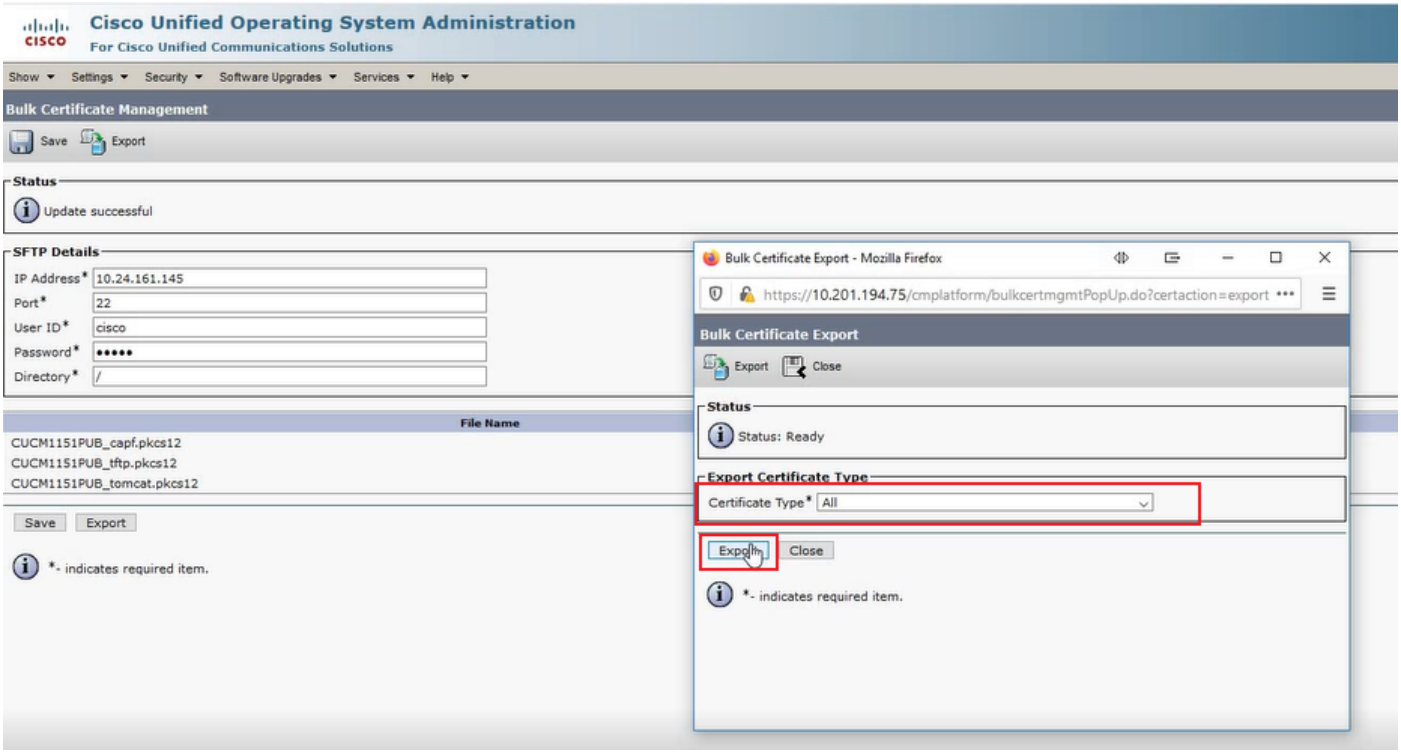
·**Passare** a **Cisco Unified OS Administration > Security > Bulk Certificate Management.** Immettere i dettagli del server SFTP e **fare clic su** Esporta, come mostrato nell'immagine.

> **Nota:** I file PKCS12 esportati dal cluster di destinazione al server SFTP vengono visualizzati nella pagina Web Bulk Certificate Management dell'editore CUCM del cluster di origine quando vi si accede.

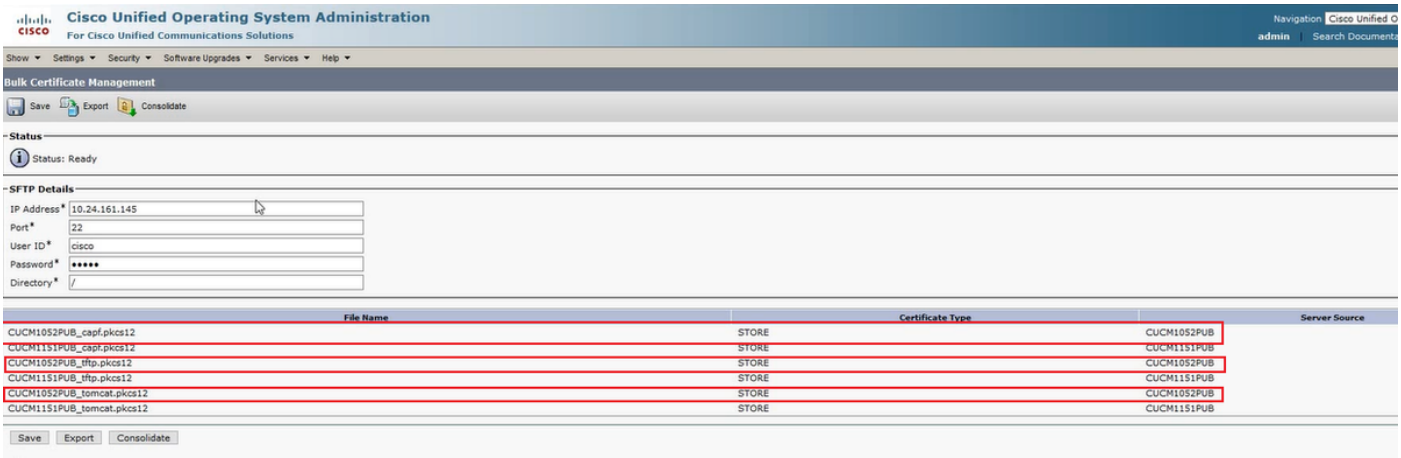


Passaggio 2. Esportare tutti i certificati da tutti i nodi nel cluster di origine al server SFTP.

·Nella successiva finestra popup, selezionare **All** per Certificate Type (Tipo di certificato), quindi fare clic su **Export** (Esporta), come mostrato nell'immagine.



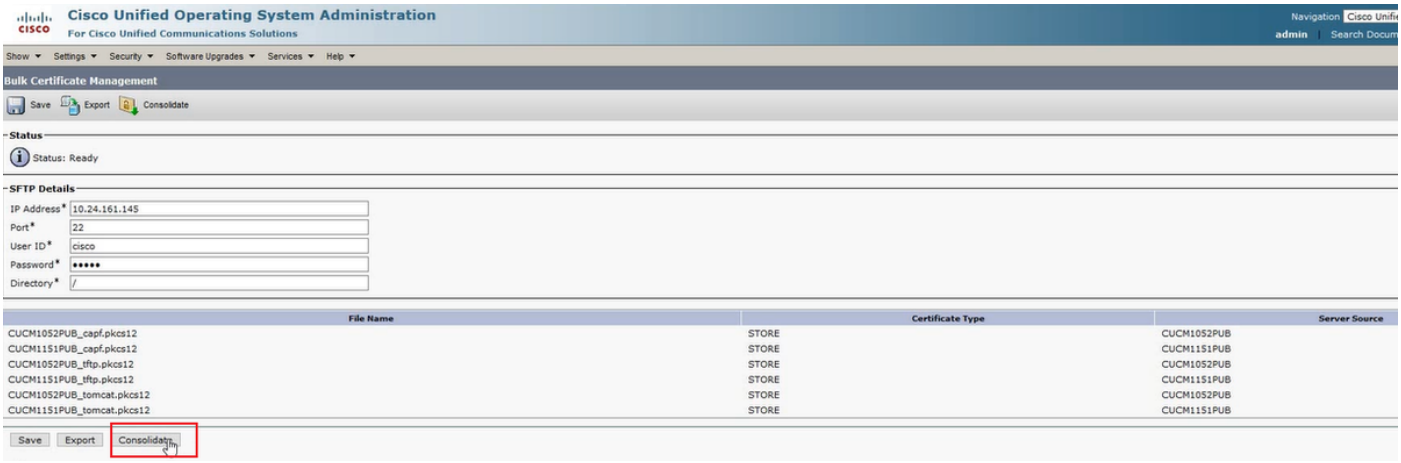
·Chiudere la finestra popup e aggiornare Gestione bulk dei certificati con i file PKCS12 creati per ogni nodo nel cluster di origine. La pagina Web viene aggiornata con queste informazioni. La pagina Web per la gestione bulk dei certificati del cluster di origine ora mostra i file PKCS12 di origine e di destinazione esportati in SFTP, come mostrato nell'immagine.



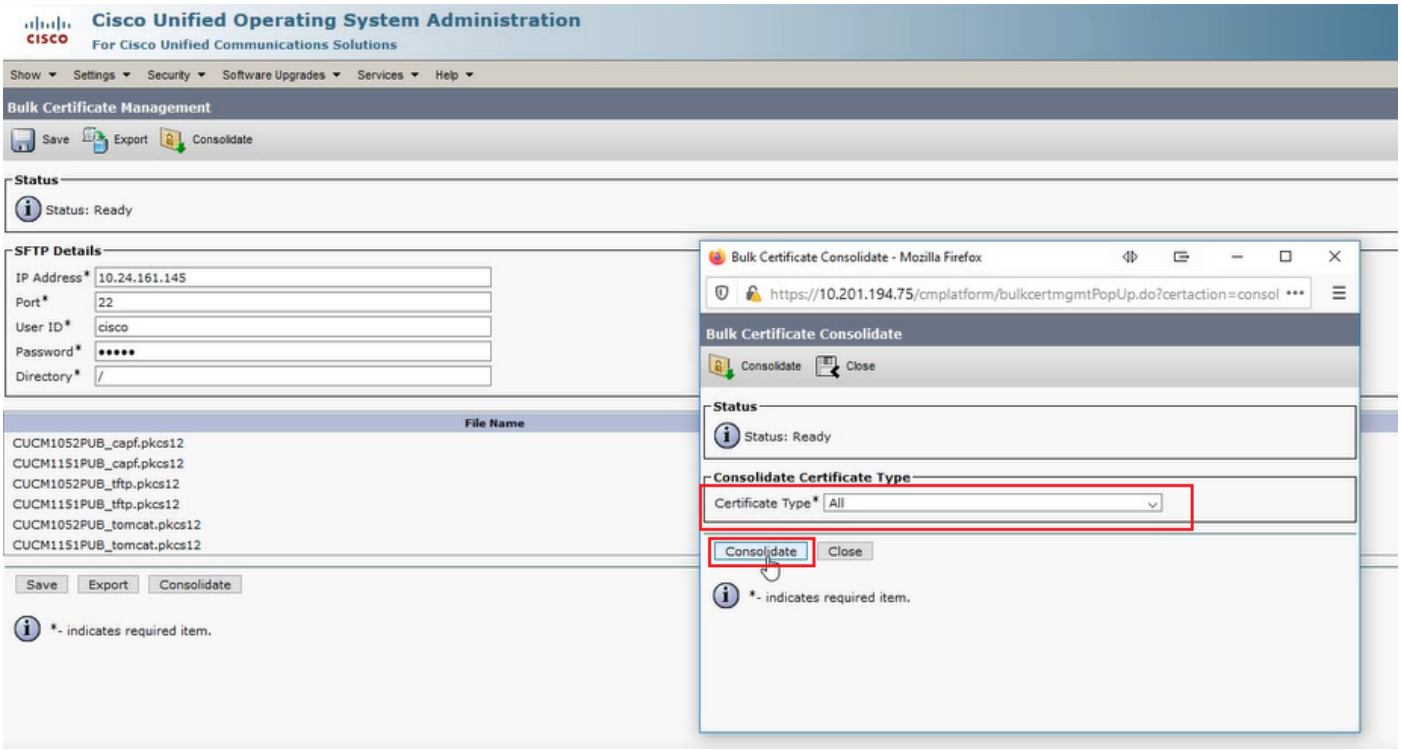
Consolidare i file PKCS12 di origine e di destinazione

> **Nota:** Mentre l'esportazione in blocco della gestione certificati viene eseguita sia sui cluster di origine che di destinazione, il consolidamento viene eseguito tramite l'editore CUCM solo su uno dei cluster.

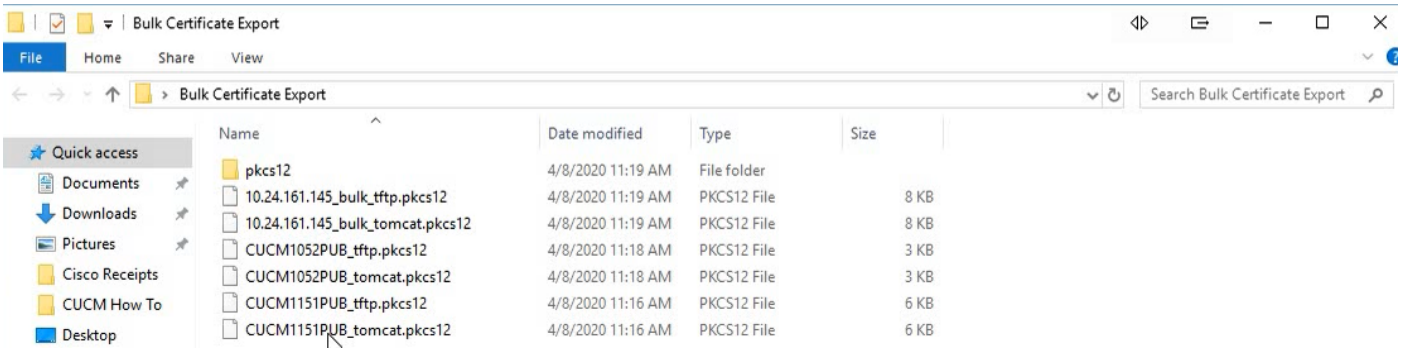
Passaggio 1. Tornare alla pagina Gestione bulk dei certificati dell'autore CUCM del cluster di origine e **fare clic** su Consolida, come mostrato nell'immagine.

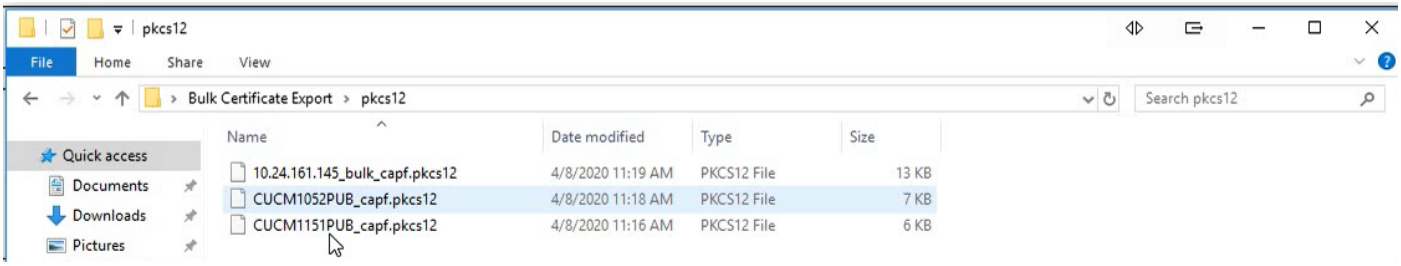


·Nella successiva finestra popup, selezionare **All** per Certificate Type (Tipo di certificato), quindi fare clic su **Consolidate** (Consolida), come mostrato nell'immagine.



· In qualsiasi momento, è possibile controllare la directory SFTP per verificare i file pkcs12 contenuti per i cluster di origine e di destinazione. Il contenuto della directory SFTP dopo l'esportazione di tutti i certificati dai cluster di destinazione e di origine è stato completato, come mostrato nelle immagini.

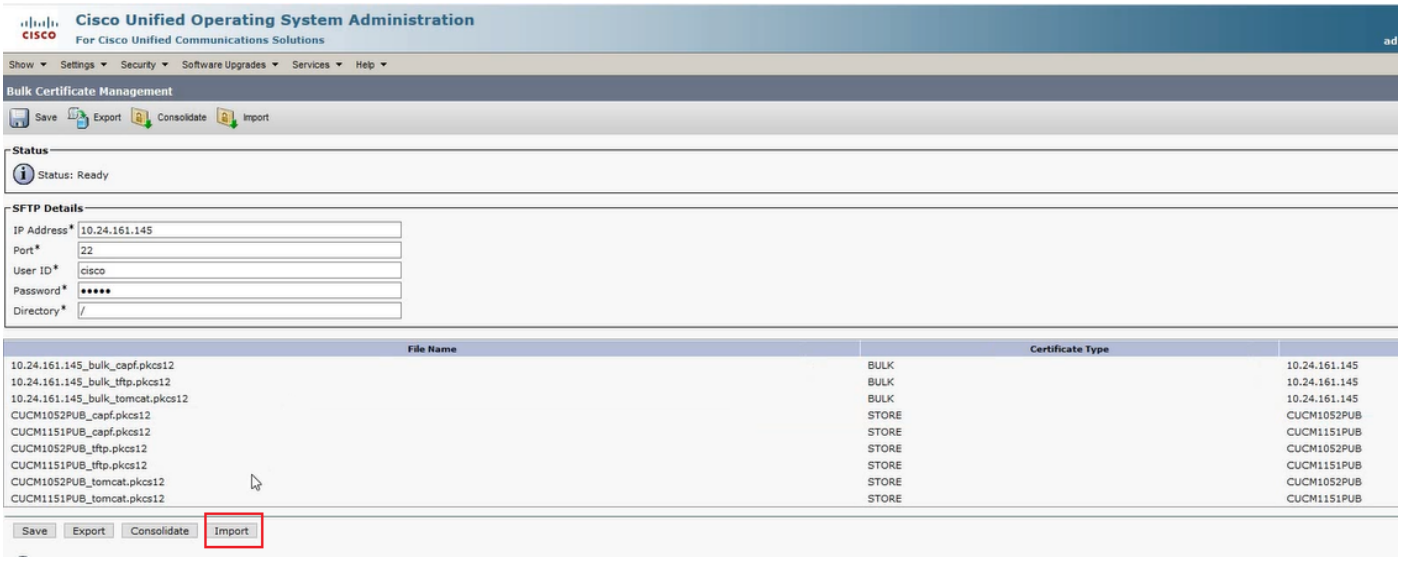




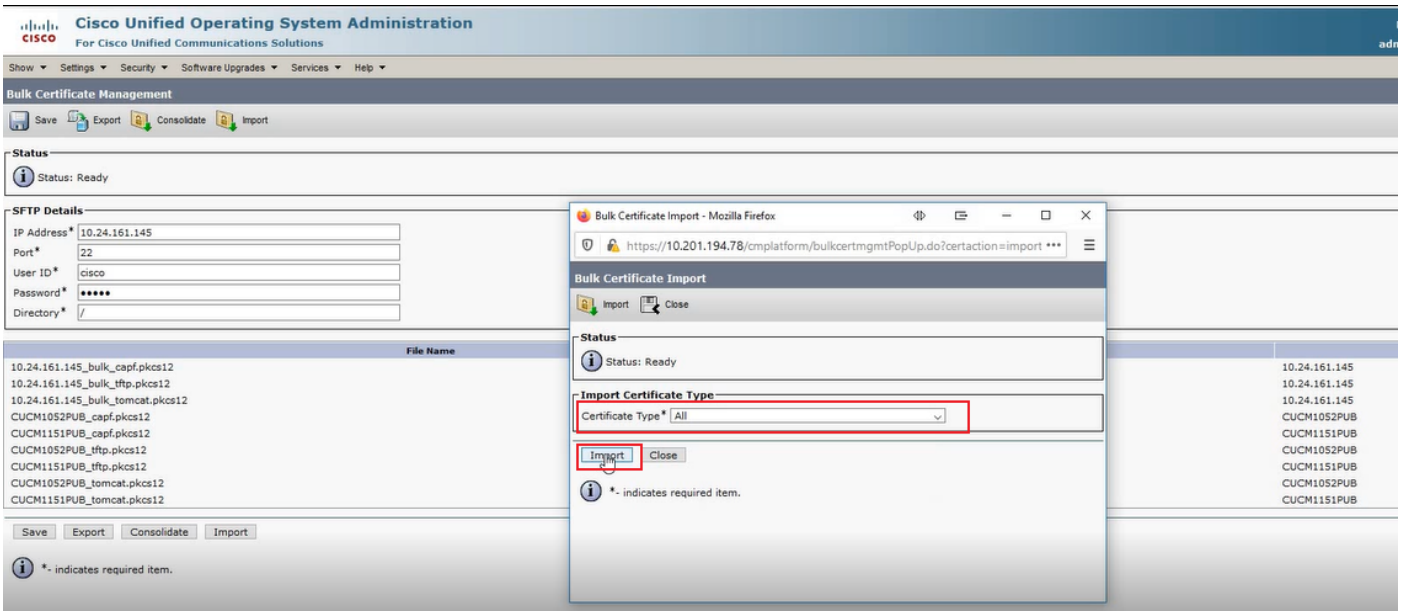
Importa certificati in cluster di destinazione e di origine

Passaggio 1. Importazione dei certificati nel cluster di destinazione

· Nell'editore CUCM del cluster di destinazione **passare** a **Cisco Unified OS Administration > Security > Bulk Certificate Management** e consentire l'aggiornamento della pagina, quindi **fare clic su** Import, come mostrato nell'immagine.



·Nella successiva finestra pop-up, selezionare **All** per Certificate Type (Tipo di certificato), quindi fare clic su **Import (Importa)**, come mostrato nell'immagine.



Passaggio 2. Ripetere il passaggio 1 per il cluster di origine.

Nota: Quando si esegue l'importazione in blocco dei certificati, i certificati vengono caricati nel cluster remoto nel modo seguente:
·Il certificato CAPF (Certificate Authority Proxy Function) viene caricato come CallManager-trust
·Il certificato Tomcat viene caricato come tomcat-trust
·Il certificato CallManager viene caricato come Phone-SAST-trust e CallManager-trust
·Il certificato di recupero dell'elenco di trust di identità (ITLRecovery) viene caricato come Phone-SAST-trust e CallManager-trust

Configurare i telefoni del cluster di origine con le informazioni sul server TFTP del cluster di destinazione

Configurare l'ambito DHCP per i telefoni del cluster di origine con l'opzione 150 TFTP (Trivial File Transfer Protocol) per puntare ai server TFTP CUCM del cluster di destinazione.

Reimposta i telefoni del cluster di origine per ottenere il file ITL/CTL del cluster di destinazione per completare il processo di migrazione

Come parte del processo di migrazione, il cluster di origine tenta di configurare una connessione sicura al servizio di verifica del trust Cisco (TVS) del cluster di origine per verificare il certificato CallManager o ITLRecovery del cluster di destinazione.

Nota: Il certificato CallManager del cluster di origine da un server CUCM che esegue il servizio TFTP (noto anche come certificato TFTP) o il relativo certificato ITLRecovery firma un file CTL (Certificate Trust List) e/o ITL (Identity Trust List) del nodo CUCM del cluster di origine. Analogamente, il certificato CallManager del cluster di destinazione da un server CUCM che esegue il servizio TFTP o il relativo certificato ITLRecovery firma un cluster di destinazione il file CTL e/o ITL del nodo CUCM. I file CTL e ITL vengono creati sui nodi CUCM che eseguono il servizio TFTP. Se il file CTL e/o ITL di un cluster di destinazione non viene convalidato dai televisori del cluster di origine, la migrazione telefonica al cluster di destinazione non riesce.

Nota: Prima di avviare il processo di migrazione dei telefoni del cluster di origine, verificare che nei telefoni sia installato un file CTL e/o ITL valido. Verificare inoltre che la funzionalità enterprise "Prepara cluster per rollback a versione precedente alla 8.0" sia impostata su False per il cluster di origine. Verificare inoltre che nei nodi CUCM del cluster di destinazione che eseguono il servizio TFTP siano installati file CTL e/o ITL validi.

Elaborazione in cluster non sicuro per i telefoni di origine per ottenere il file ITL del cluster di destinazione per completare la migrazione dei telefoni:

Passaggio 1. Per convalidare il file ITL attualmente installato non è possibile utilizzare né CallManager né il certificato ITLRecovery contenuto nel file ITL del cluster di destinazione, che viene presentato al telefono del cluster di origine al momento della reimpostazione. In questo modo, il telefono del cluster di origine stabilisce una connessione al televisore del cluster di origine per convalidare il file ITL del cluster di destinazione.
Passaggio 2. Il telefono stabilisce una connessione al cluster di origine TVS sulla porta tcp 2445.
Passaggio 3. Il TVS del cluster di origine presenta il proprio certificato al telefono. Il telefono convalida la connessione e richiede al servizio TV del cluster di origine di convalidare il certificato

CallManager o ITLRecovery del cluster di destinazione per consentire al telefono di scaricare il file ITL del cluster di destinazione.
Passaggio 4. Dopo la convalida e l'installazione del file ITL del cluster di destinazione, il telefono del cluster di origine può ora convalidare e scaricare i file di configurazione firmati dal cluster di destinazione.

Elaborazione in un cluster sicuro per i telefoni di origine per ottenere il file CTL del cluster di destinazione per completare la migrazione dei telefoni:

Passaggio 1. Il telefono si avvia e tenta di scaricare il file CTL dal cluster di destinazione.
Passaggio 2. Il file CTL è firmato dal certificato CallManager o ITLRecovery del cluster di destinazione che non si trova nel file CTL o ITL corrente del telefono.
Passaggio 3. Di conseguenza, il telefono si collega a TVS sul cluster di origine per verificare il certificato CallManager o ITLRecovery.

> **Nota:** A questo punto, il telefono ha ancora la sua configurazione precedente che contiene l'indirizzo IP del servizio TVS cluster di origine. I server TVS specificati nella configurazione phone sono gli stessi del gruppo phones Callmanager.

Passaggio 4. Il telefono configura una connessione TLS (Transport Layer Security) al televisore sul cluster di origine.
Passaggio 5. Quando la TV del cluster di origine presenta il proprio certificato al telefono, il telefono verifica il certificato della TV rispetto al certificato nel file ITL corrente.
Passaggio 6. Se sono uguali, l'handshake viene completato correttamente.
Passaggio 7. Il telefono di origine richiede che le TV del cluster di origine verifichino il certificato CallManager o ITLRecovery dal file CTL del cluster di destinazione.
Passaggio 8. Il servizio TVS di origine trova il cluster di destinazione CallManager o ITLRecovery nel proprio archivio certificati, lo convalida e il telefono del cluster di origine procede all'aggiornamento con il file CTL del cluster di destinazione.
Passaggio 9. Il telefono di origine scarica il file ITL del cluster di destinazione che viene convalidato rispetto al file CTL del cluster di destinazione che ora contiene. Poiché il file CTL del telefono di origine ora contiene il certificato CallManager o ITLRecovery del cluster di destinazione, il telefono di origine può ora verificare il certificato CallManager o ITLRecovery senza dover contattare il televisore del cluster di origine.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Video di Configuration Walkthrough

Questo collegamento consente di accedere a un video che illustra la gestione di massa dei certificati tra cluster CUCM:

Gestione in blocco dei certificati tra cluster CUCM