用於電話遷移的CUCM群集之間的批次證書管理過程

目錄

簡介

本文檔提供了在思科統一通訊管理器(CUCM)集群之間進行批次證書管理的操作步驟，以便進行電話遷移。

作者：思科TAC工程師Adrian Esquillo。

> **附註**：CUCM版本12.5(1)的《管理指南》的管理批次證書一節中還介紹了此過程

必要條件

需求

思科建議您瞭解以下主題：
·安全檔案傳輸通訊協定(SFTP)伺服器
·CUCM證書

採用元件

·本文檔中的資訊基於CUCM 10.X。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

批次證書管理允許在CUCM群集之間共用一組證書。此步驟要求各個群集的系統功能需要在它們之間建立信任，例如跨群集分機移動(EMCC)以及群集之間的電話遷移。

在此過程中，會建立一個包含來自群集中所有節點的證書的公鑰加密標準#12(PKCS12)檔案。每個群集都必須將其證書匯出到同一SFTP伺服器上的同一SFTP目錄中。必須在源群集和目標群集的CUCM發佈伺服器上手動完成批次證書管理配置。源集群和目的集群必須啟動且正常運行，以便要遷移的電話可以同時連線到這兩個集群。源群集電話將遷移到目標群集。

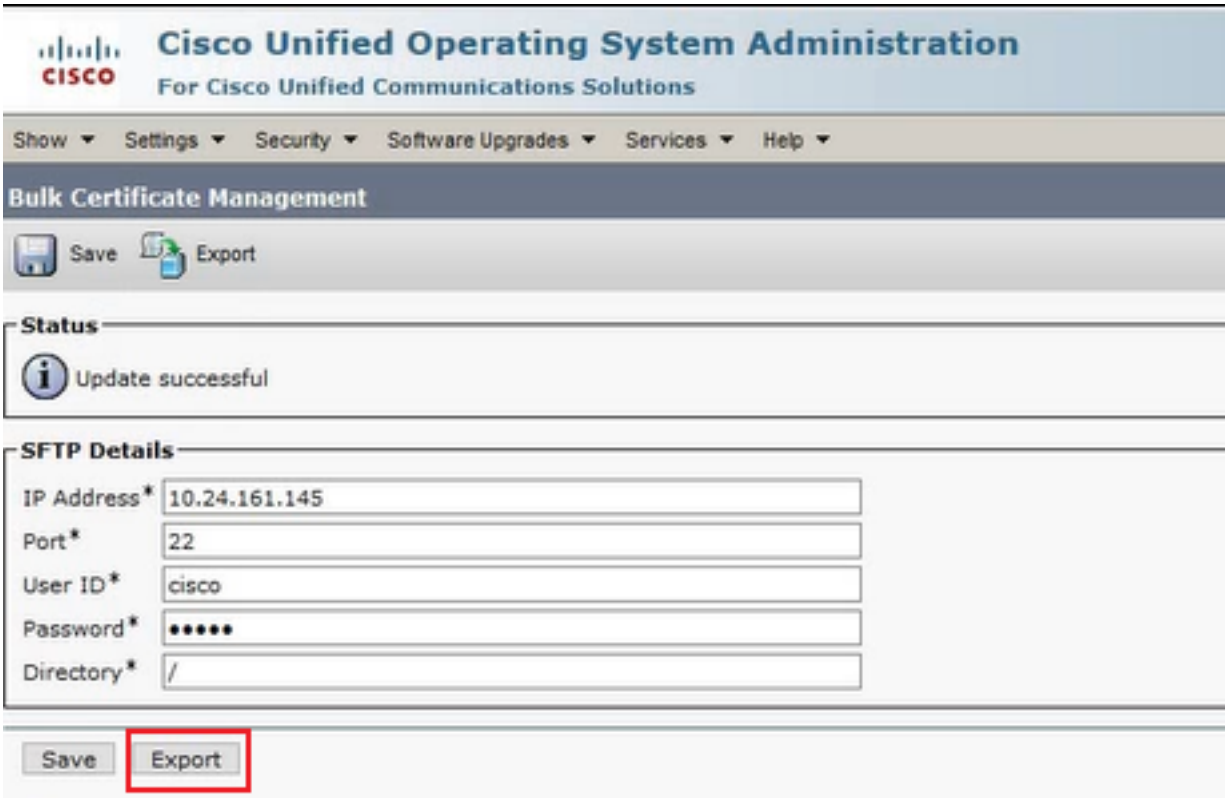
批次證書管理過程

匯出目標群集證書

步驟1.在目標群集的CUCM發佈伺服器上配置SFTP伺服器進行批次證書管理。

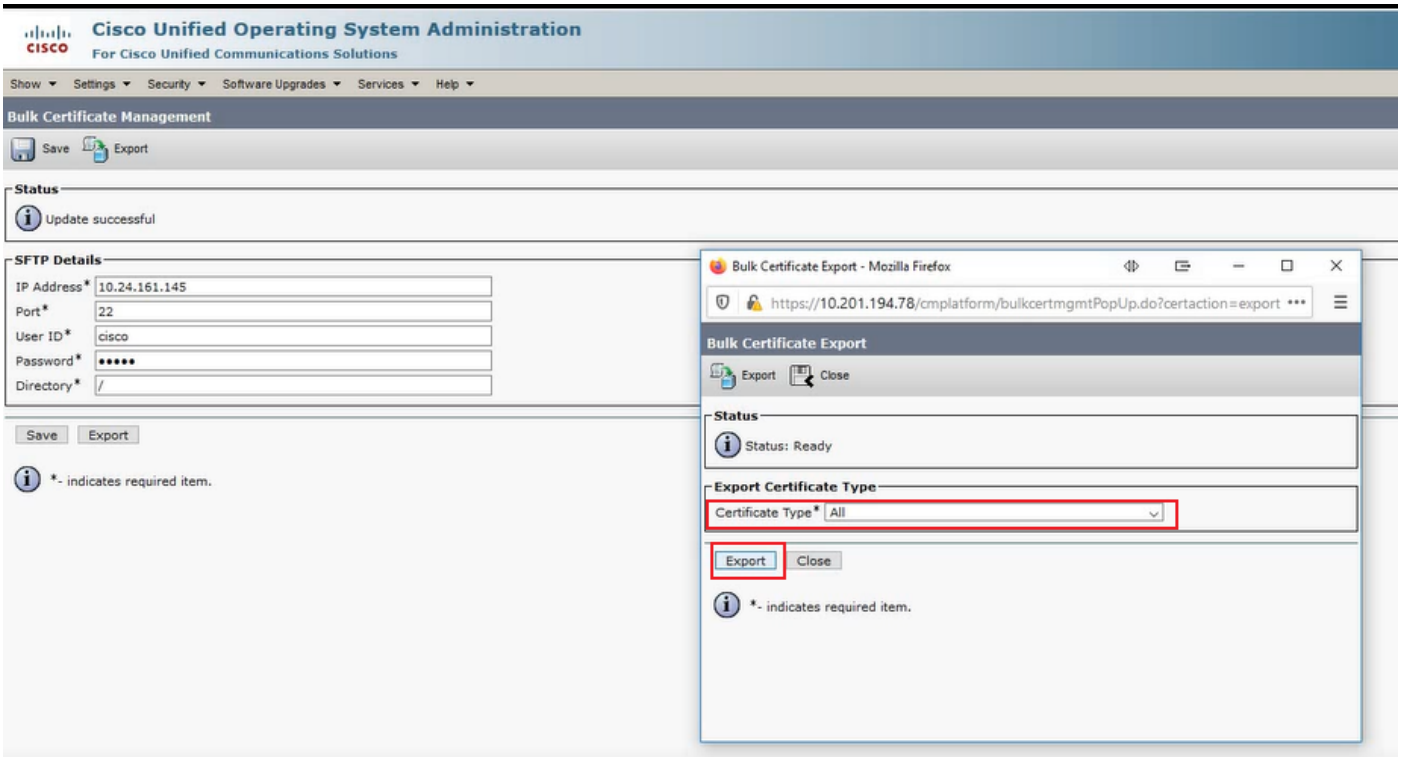
在本示例中，目標群集CUCM版本為11.5.1。

·導覽至**Cisco Unified OS Administration > Security > Bulk Certificate Management**，輸入SFTP伺服器詳細資訊，然後按一下Export，如下圖所示。

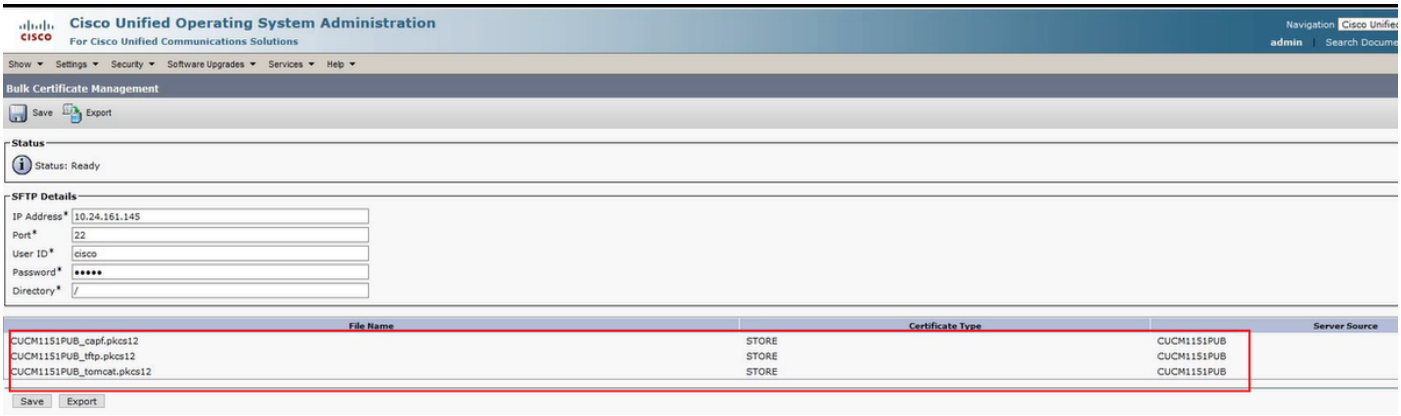


步驟2.將所有證書從目標群集中的所有節點匯出到SFTP伺服器。

·在後續的彈出視窗中，為「Certificate Type」選擇**All**，然後按一下**Export**，如下圖所示。



·關閉彈出視窗，使用為目標群集中的每個節點建立的PKCS12檔案更新Bulk Certificate Management更新，網頁將使用此資訊刷新，如下圖所示。



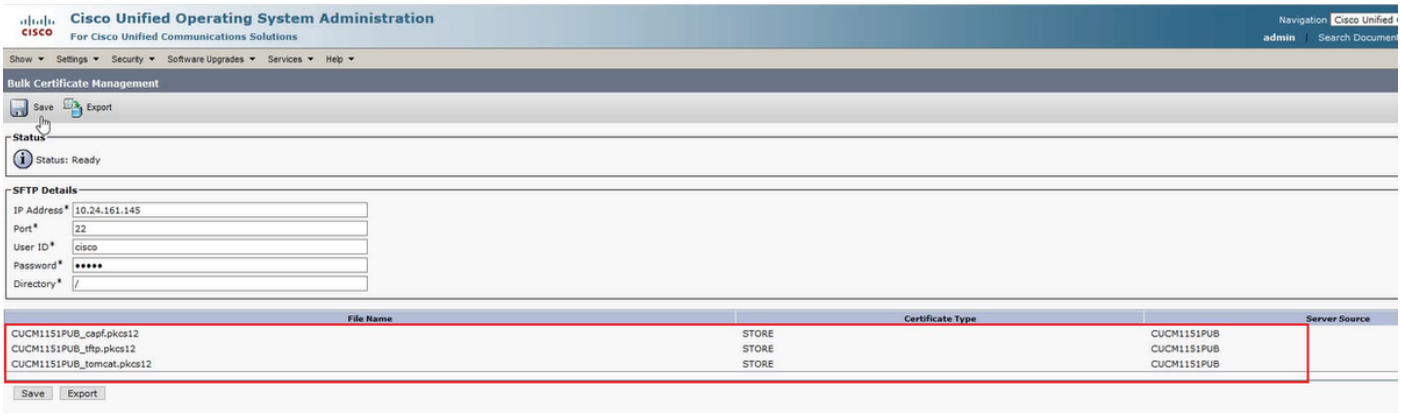
匯出源群集證書

步驟1.在源群集的CUCM發佈伺服器上配置SFTP伺服器進行批次證書管理。

在本示例中，源群集CUCM版本為10.5.2。

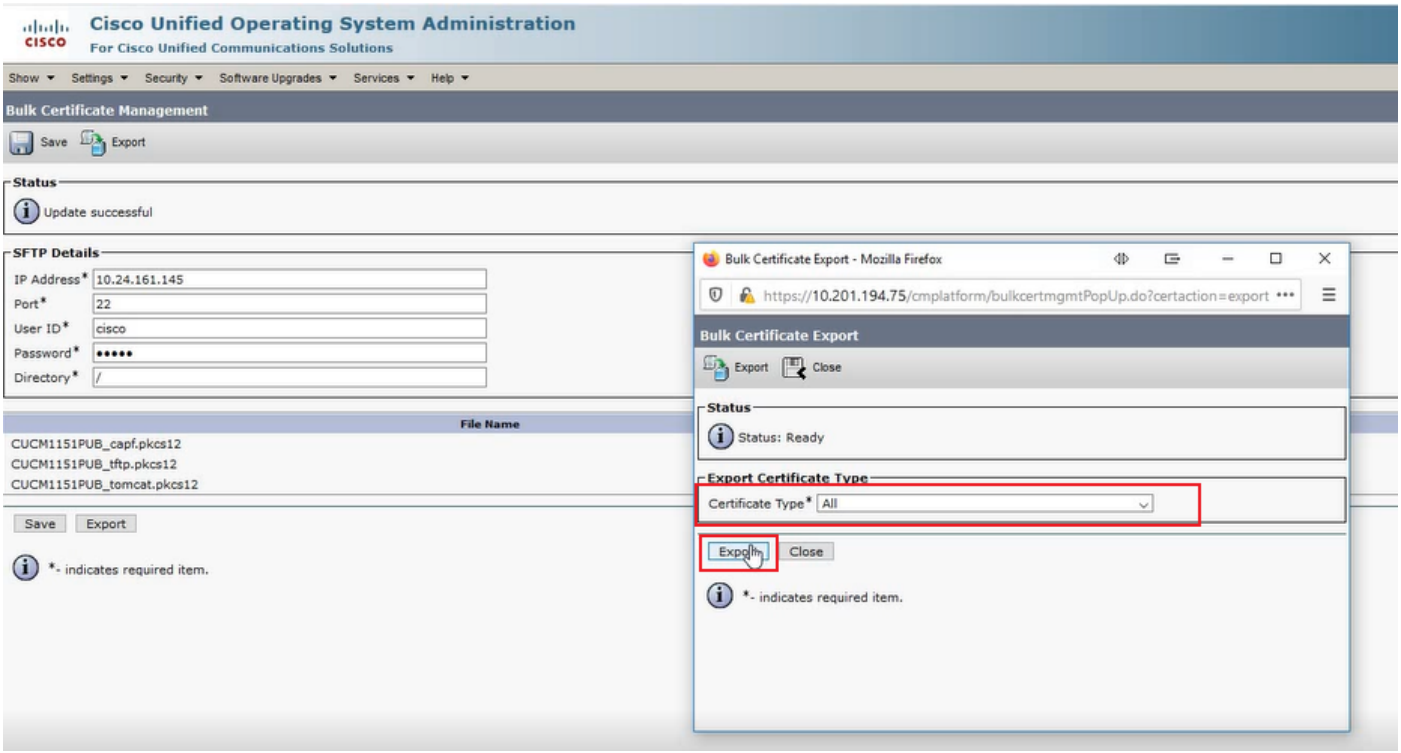
·導覽至**Cisco Unified OS Administration > Security > Bulk Certificate Management**，輸入SFTP伺服器詳細資訊，然後按一下Export，如下圖所示。

> **附註**：從目標群集匯出到SFTP伺服器的PKCS12檔案在訪問時顯示在源群集CUCM發佈伺服器的「批次證書管理」網頁上。

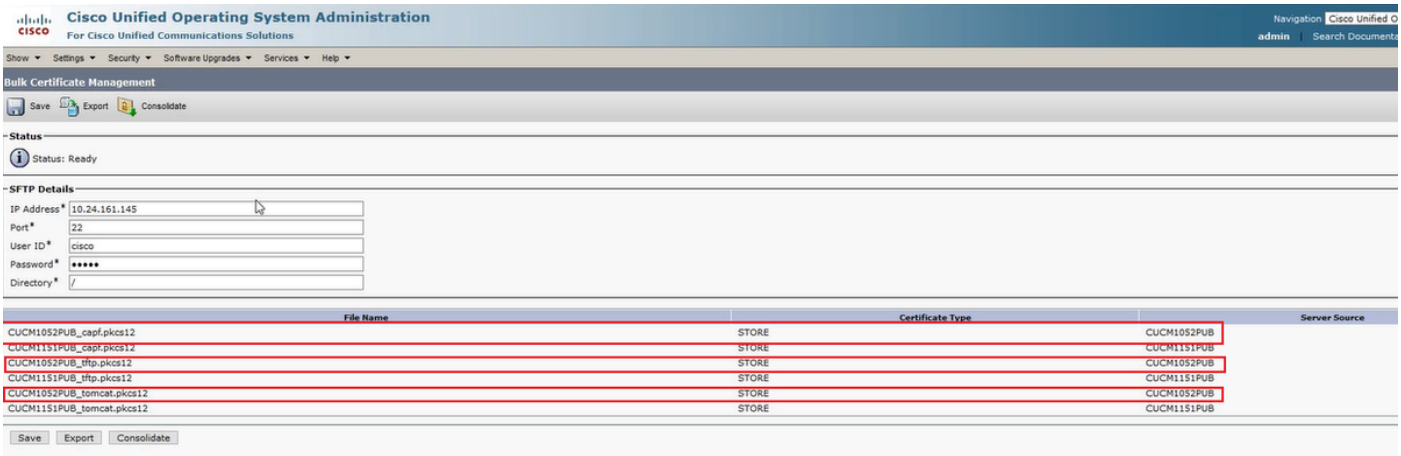


步驟2.將所有證書從源群集中的所有節點匯出到SFTP伺服器。

·在後續的彈出視窗中，為「Certificate Type」選擇**All**，然後按一下**Export**，如下圖所示。



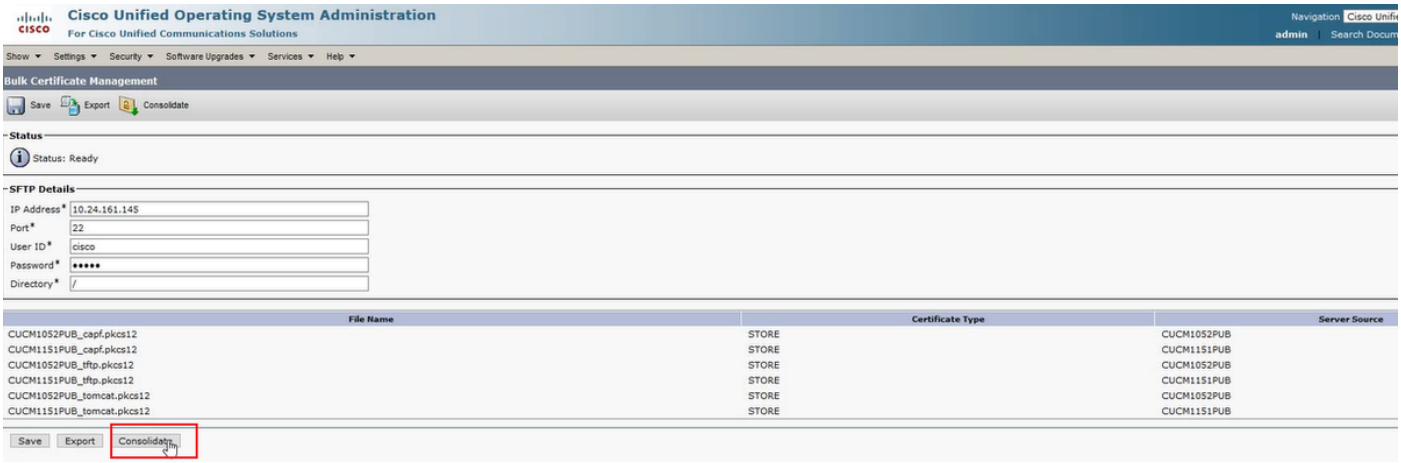
·關閉彈出視窗並使用為源群集中的每個節點建立的PKCS12檔案更新Bulk Certificate Management更新，網頁將使用此資訊刷新。現在，源群集的「批次證書管理」網頁將顯示匯出到SFTP的源和目標PKCS12檔案，如下圖所示。



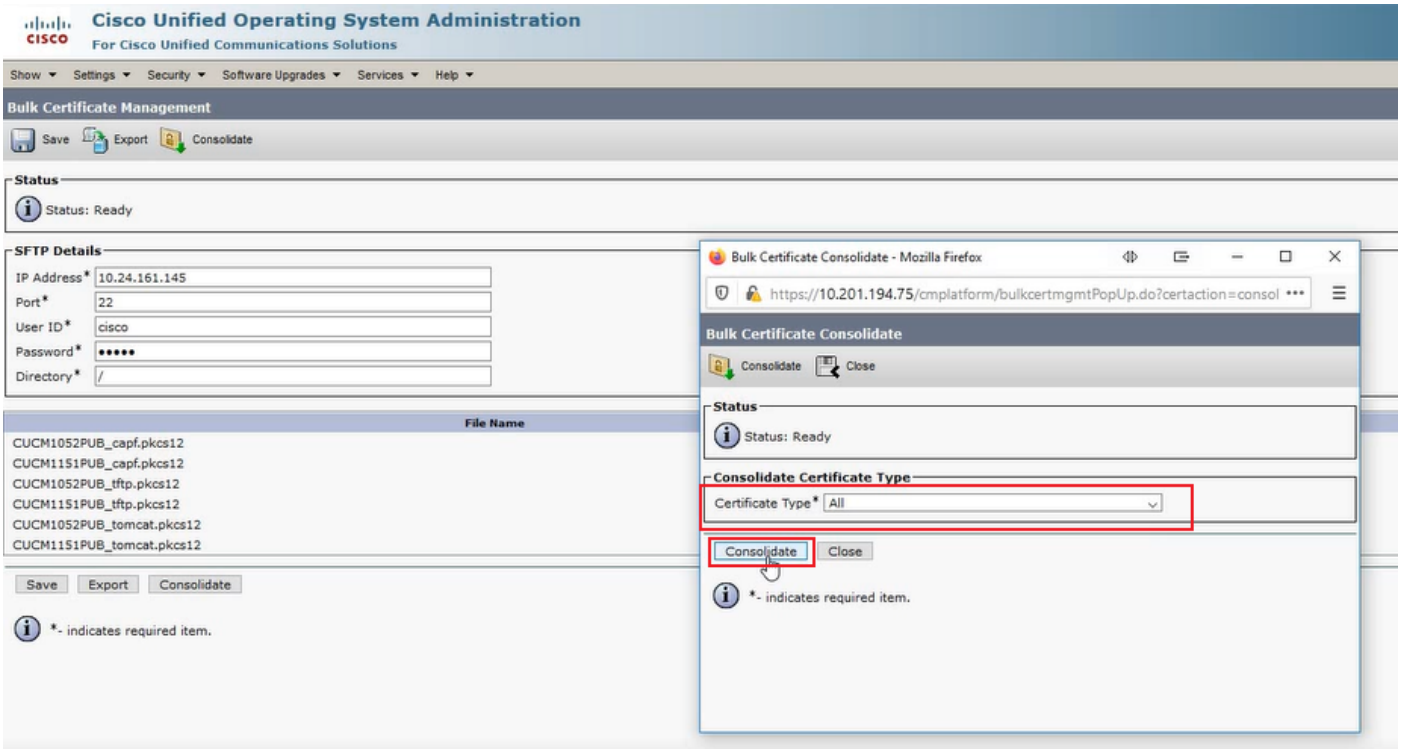
合併源和目標PKCS12檔案

> **附註**：批次證書管理匯出在源群集和目標群集上完成，而整合僅通過其中一個群集上的CUCM發佈器完成。

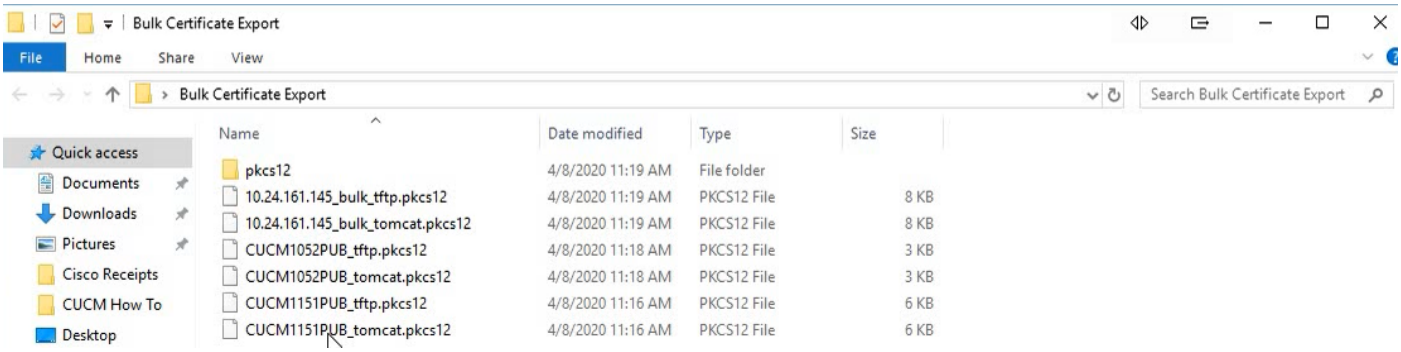
步驟1. 返回源群集的CUCM發佈者的Bulk Certificate Management頁面，然後單擊Consolidate（合併），如下圖所示。

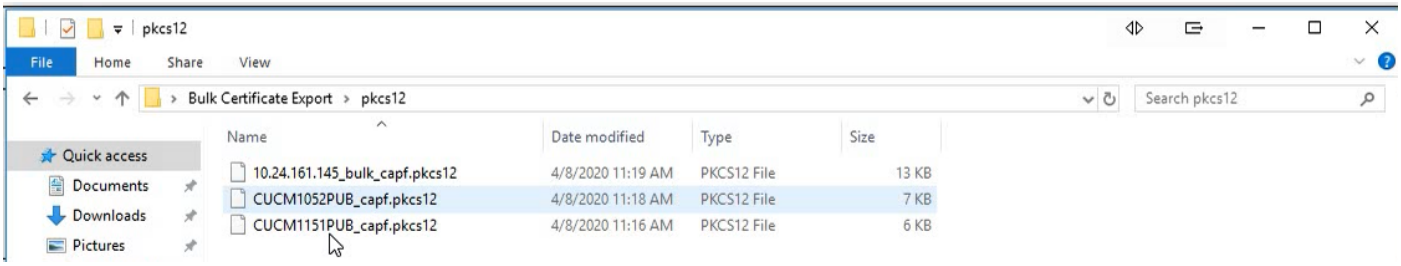


·在後續的彈出視窗中，為Certificate Type選擇**All**，然後按一下**Consolidate**，如下圖所示。



·您可以隨時檢查SFTP目錄，以驗證源群集和目標群集所包含的pkcs12檔案。從目標和源群集匯出所有證書後，SFTP目錄的內容已完成，如下圖所示。

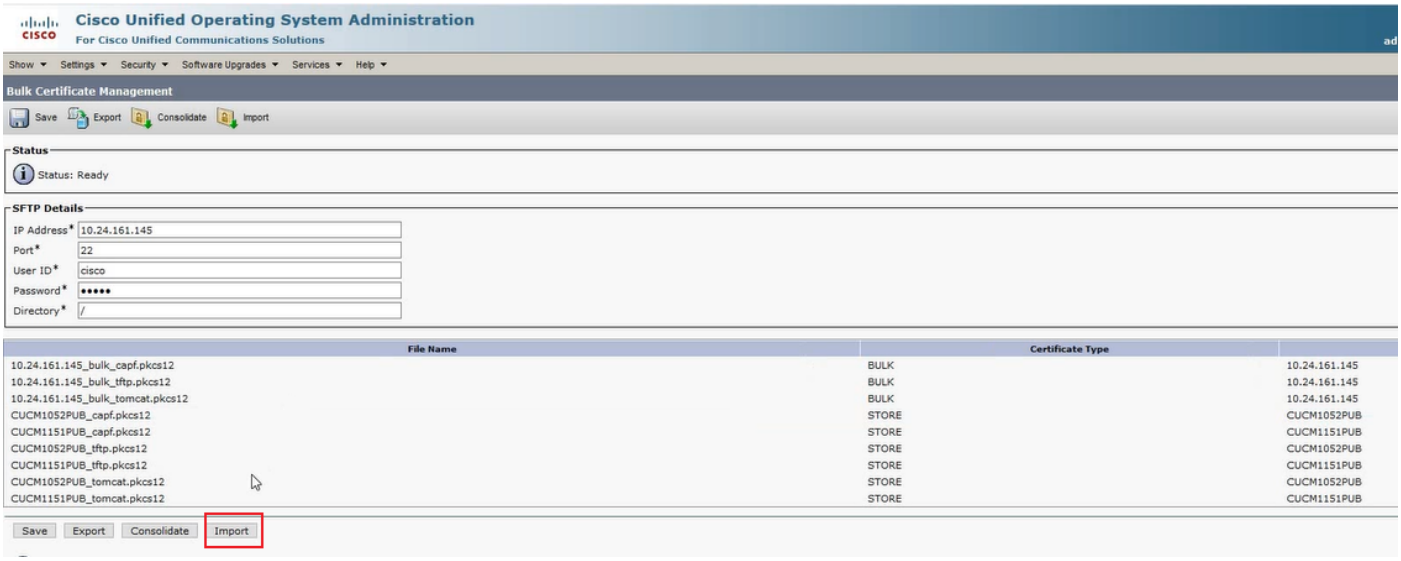




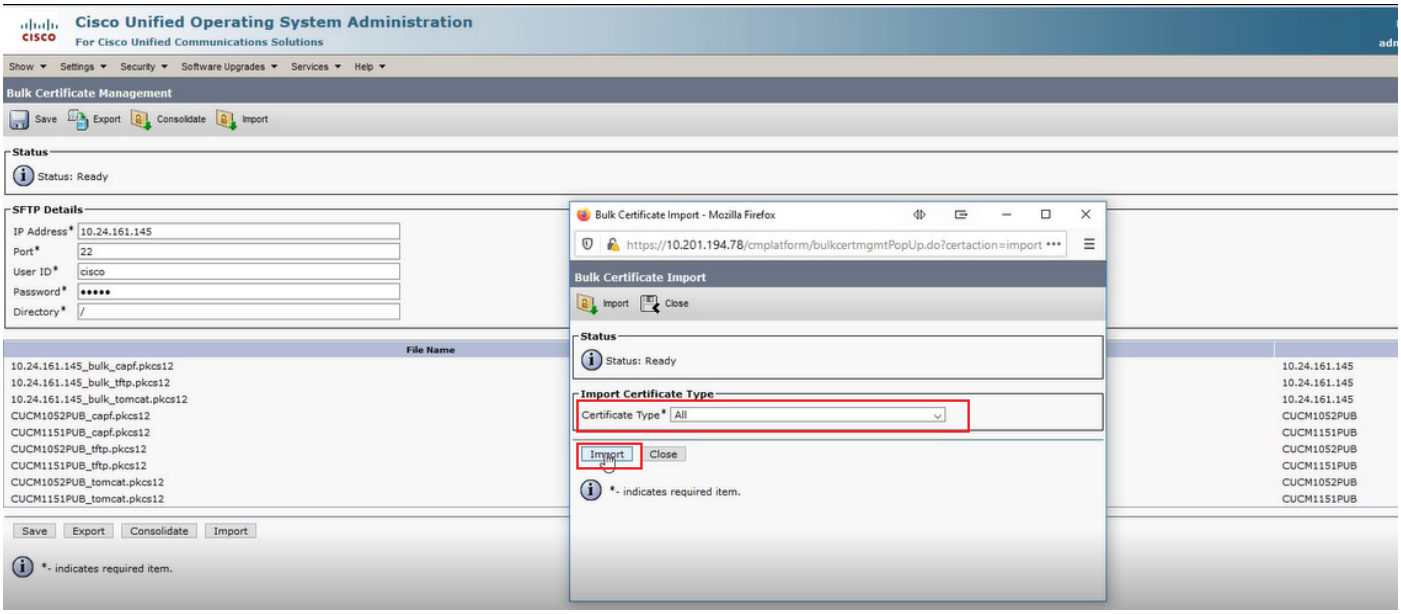
將證書匯入到目標和源群集

步驟1.將證書匯入目標群集

·在目標群集的CUCM發佈伺服器上，導航到Cisco Unified OS Administration > Security > Bulk Certificate Management，然後刷新頁面，然後按一下 Import，如下圖所示。



·在後續彈出視窗中，為**Certificate Type選擇All**，然後按一下**Import**，如下圖所示。



步驟2. 對源群集重複步驟1。

附註：執行批次證書匯入時，證書將按以下方式上傳到遠端群集：
·證書頒發機構代理函式(CAPF)證書以CallManager-trust形式上傳
·以tomcat-trust身份上傳Tomcat證書
·將CallManager證書上傳為Phone-SAST-trust和CallManager-trust
·身份信任清單恢復(ITLRecovery)證書作為Phone-SAST-trust和CallManager-trust上傳

使用目標群集TFTP伺服器資訊配置源群集電話

使用簡單檔案傳輸協定(TFTP)選項150配置源群集電話的DHCP作用域，以指向目標群集CUCM TFTP伺服器。

重置源群集電話以獲取目標群集ITL/CTL檔案以完成遷移過程

作為遷移過程的一部分，源群集電話嘗試建立與源群集的Cisco信任驗證服務(TVS)的安全連線，以驗證目標群集的CallManager或ITLRecovery證書。

附註：來自運行TFTP服務的CUCM伺服器的源群集的CallManager證書（也稱為TFTP證書）或其ITLRecovery證書在源群集CUCM節點的證書信任清單(CTL)和/或身份信任清單(ITL)檔案中簽名。同樣，來自運行TFTP服務的CUCM伺服器的目標群集的CallManager證書或其ITLRecovery證書將簽署目標群集CUCM節點的CTL和/或ITL檔案。CTL和ITL檔案是在運行TFTP服務的CUCM節點上建立的。如果目標集群的CTL和/或ITL檔案未被源集群TVS驗證，則到目標集群的電話遷移將失敗。

附註：在開始源群集電話遷移過程之前，請確認這些電話已安裝有效的CTL和/或ITL檔案。此外，請確保將源群集的企業功能「準備群集以回滾到8.0之前的版本」設定為False。此外，驗證運行TFTP服務的目標群集CUCM節點是否安裝了有效的CTL和/或ITL檔案。

在非安全集群中處理源電話獲取目標集群ITL檔案以完成電話遷移：

步驟1.在重置時提供給源集群電話的目標集群ITL檔案中包含的CallManager和ITLRecovery證書均不能用於驗證當前安裝的ITL檔案。這會導致源群集電話建立到源群集的TVS的連線，以驗證目標群

集的ITL檔案。
步驟2.電話在TCP埠2445上建立到源群集TVS的連線。
步驟3.源群集的TVS向電話顯示其證書。電話驗證連線並請求源集群TVS驗證目標集群的CallManager或ITLRecovery證書以允許電話下載目標集群的ITL檔案。
步驟4.在驗證和安裝目標集群ITL檔案之後，源集群電話現在可以驗證和下載目標集群中已簽名的配置檔案。

在安全群集中為源電話獲取目標群集CTL檔案以完成電話遷移的過程：

步驟1.電話啟動並嘗試從目標群集下載CTL檔案。
步驟2. CTL檔案由目標集群的CallManager或ITLRecovery證書簽名，該證書不在電話的當前CTL或ITL檔案中。
步驟3.因此，電話會連線到源群集上的TVS以驗證CallManager或ITLRecovery證書。

> **附註**：此時，電話仍舊有包含源群集TVS服務的IP地址的舊配置。電話配置中指定的TVS伺服器與電話Callmanager組相同。

步驟4.電話建立到源群集上TVS的傳輸層安全(TLS)連線。
步驟5.當源群集TVS向電話顯示其證書時，電話根據其當前ITL檔案中的證書驗證此TVS證書。
步驟6.如果相同，則握手成功完成。
步驟7.源電話請求源群集TVS驗證目標群集CTL檔案中的CallManager或ITLRecovery證書。
步驟8.源TVS服務在其證書儲存中找到目標群集CallManager或ITLRecovery，對其進行驗證，並且源群集電話繼續使用目標群集CTL檔案進行更新。
步驟9.源電話下載目標集群的ITL檔案，該檔案根據它現在包含的目標集群CTL檔案進行驗證。由於源電話的CTL檔案現在包含目標群集的CallManager或ITLRecovery證書，因此源電話現在可以驗證CallManager或ITLRecovery證書，而無需聯絡源群集的TVS。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

配置演練影片

此連結提供對CUCM集群間批次證書管理的影片的訪問：

CUCM群集之間的批次證書管理