電話機の移行のためのCUCMクラスタ間の一括証明書管理の手順

内容

概要

このドキュメントでは、電話機の移行のためにCisco Unified Communications Manager(CUCM)クラスタ間で証明書を一括管理する手順について説明します。

著者：Cisco TACエンジニア、Adrian Esquillo

> **注**：この手順については、『Administration Guide for CUCM Release 12.5(1)』の「Manage Bulk Certificates」の項でも説明します

前提条件

要件

次の項目に関する知識があることが推奨されます。
・ Secure File Transfer Protocol(SFTP)サーバ
・ CUCM証明書

使用するコンポーネント

・ このドキュメントの情報は、CUCM 10.Xに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Bulk Certificate Managementでは、一連の証明書をCUCMクラスタ間で共有できます。この手順は、クラスタ間のExtension Mobility Cross Cluster(EMCC)などの信頼を確立する必要がある個々のクラスタのシステム機能、およびクラスタ間の電話の移行に必要です。

この手順の一部として、クラスタ内のすべてのノードからの証明書を含むPublic Key Cryptography Standards #12(PKCS12)ファイルが作成されます。すべてのクラスタは、同じSFTPサーバ上の同じSFTPディレクトリに証明書をエクスポートする必要があります。証明書の一括管理設定は、送信元クラスタと宛先クラスタの両方のCUCMパブリッシャで手動で行う必要があります。移行元と移行先のクラスタが稼働していて、移行対象の電話機がこれらのクラスタの両方に接続できる必要があります。移行元クラスタの電話機が移行先クラスタに移行されます。

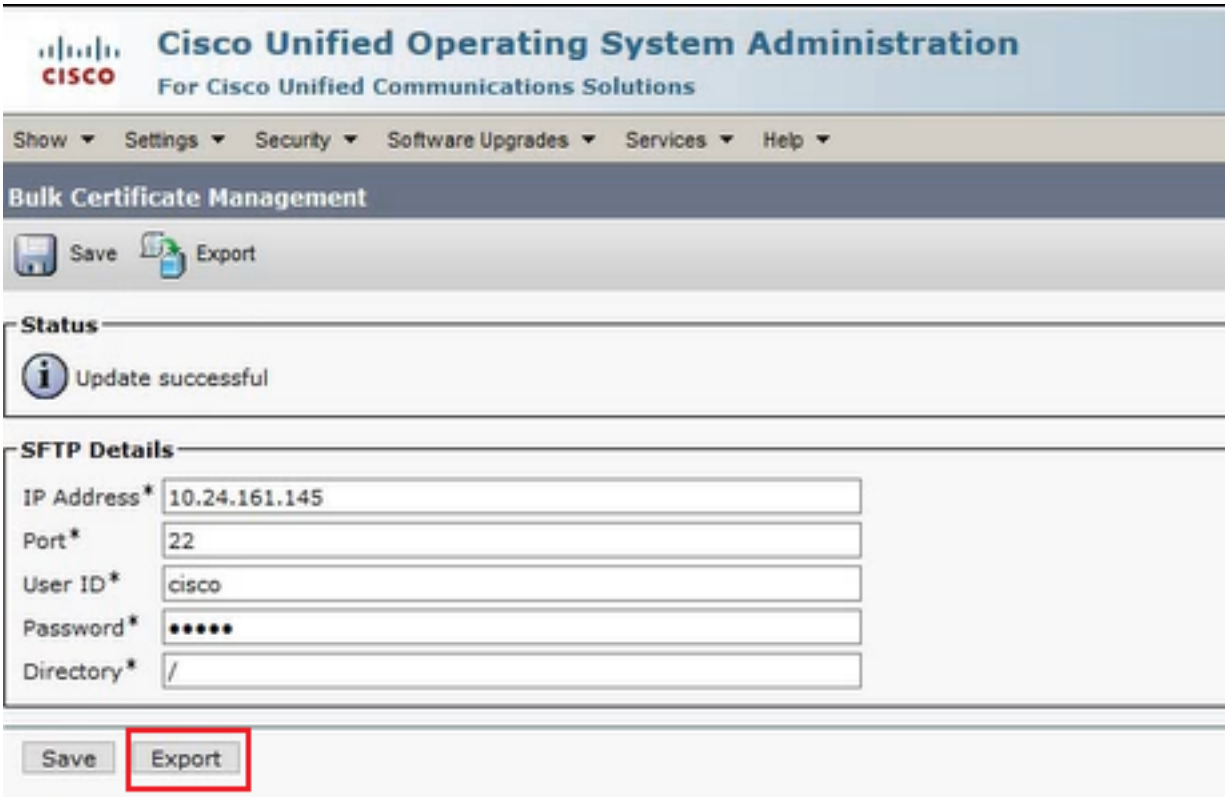
証明書の一括管理手順

宛先クラスタ証明書のエクスポート

ステップ1：宛先クラスタのCUCMパブリッシャでBulk Certificate Management用にSFTPサーバを設定します。

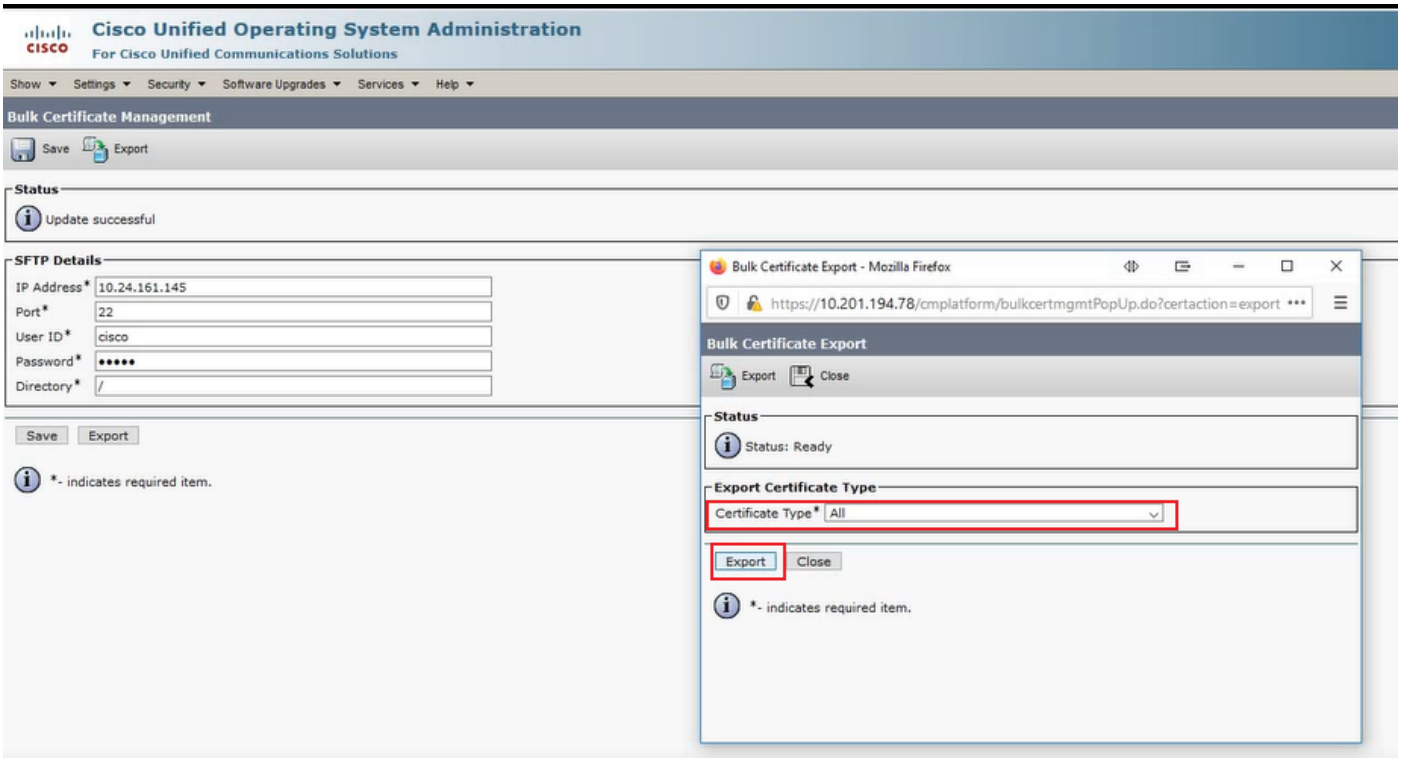
この例では、宛先クラスタのCUCMバージョンは11.5.1です。

・ [Cisco Unified OS Administration] > [Security] > [Bulk Certificate Management] に移動し、SFTPサーバの詳細を入力し、図に示すように[Export]**をクリックします。**

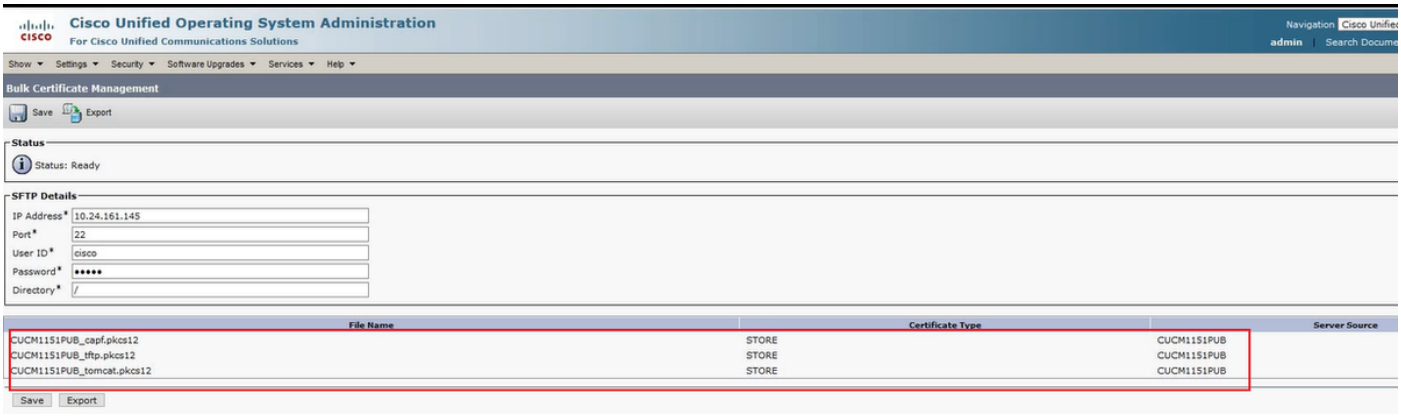


ステップ2：宛先クラスタ内のすべてのノードからすべての証明書をSFTPサーバにエクスポートします。

・次のポップアップウィンドウで、[証明書の種類]**に[すべて]**を選択し、図に示すように[エクス**ポート]**をクリックします。



・ポップアップウィンドウを閉じ、宛先クラスタ内の各ノードに対して作成されたPKCS12ファイルを使用して証明書の一括管理(BAT)の更新を行います。図に示すように、Webページが更新されます。



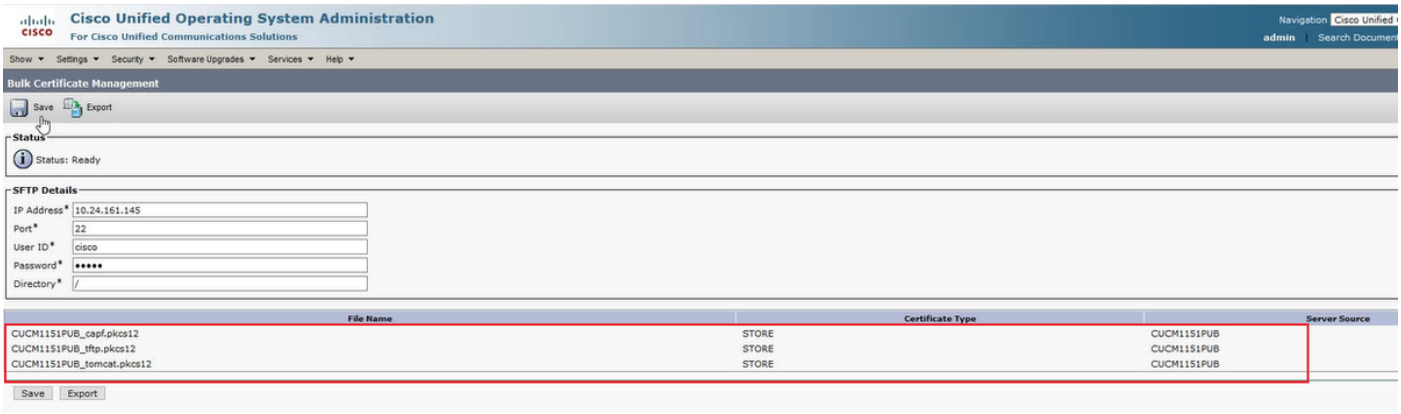
ソースクラスタ証明書のエクスポート

ステップ1：ソースクラスタのCUCMパブリッシャでBulk Certificate Management用にSFTPサーバを設定します。

この例では、ソースクラスタCUCMのバージョンは10.5.2です。

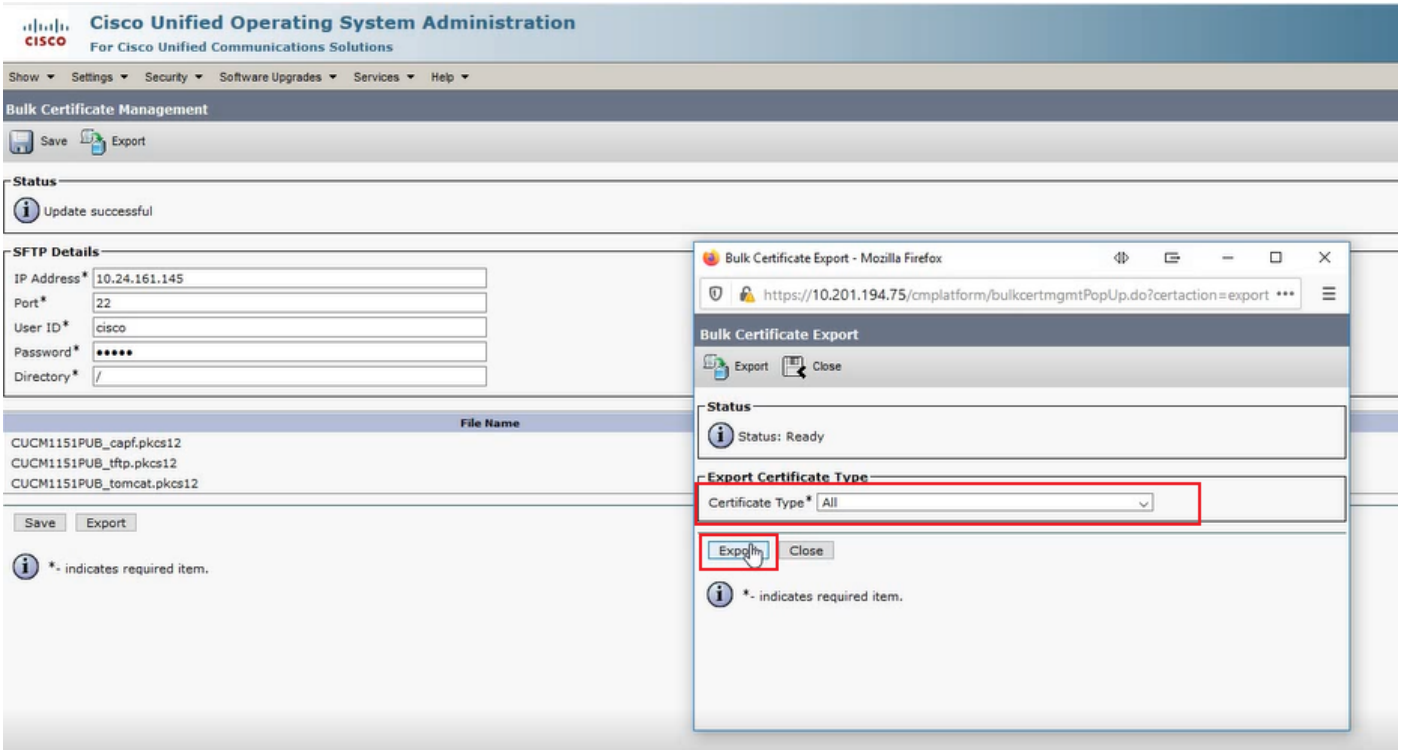
・ [Cisco Unified OS Administration] > [Security] > [Bulk Certificate Management] に移動し、SFTPサーバの詳細を入力し、図に示すように[Export]**をクリックします。**

> **注**：宛先クラスタからSFTPサーバにエクスポートされたPKCS12ファイルは、ソースクラスタのCUCMパブリッシャのBulk Certificate Management Webページ（アクセス時）に表示されます。

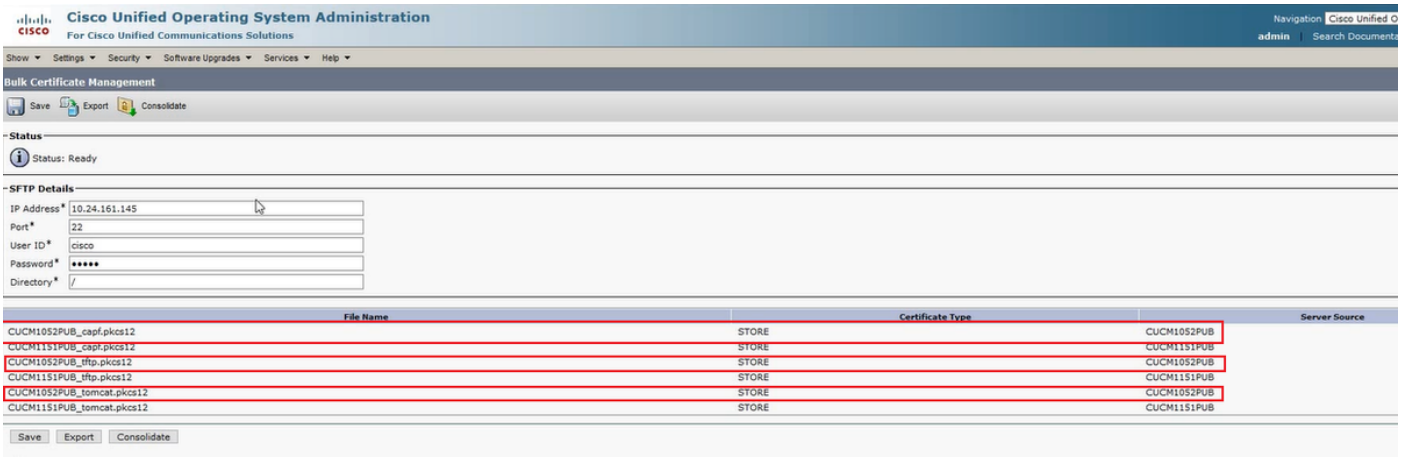


ステップ2：ソースクラスタ内のすべてのノードからすべての証明書をSFTPサーバにエクスポートします。

・ 次のポップアップウィンドウで、[証明書の種類]**に[すべて]**を選択し、図に示すように[エクス**ポート]**をクリックします。



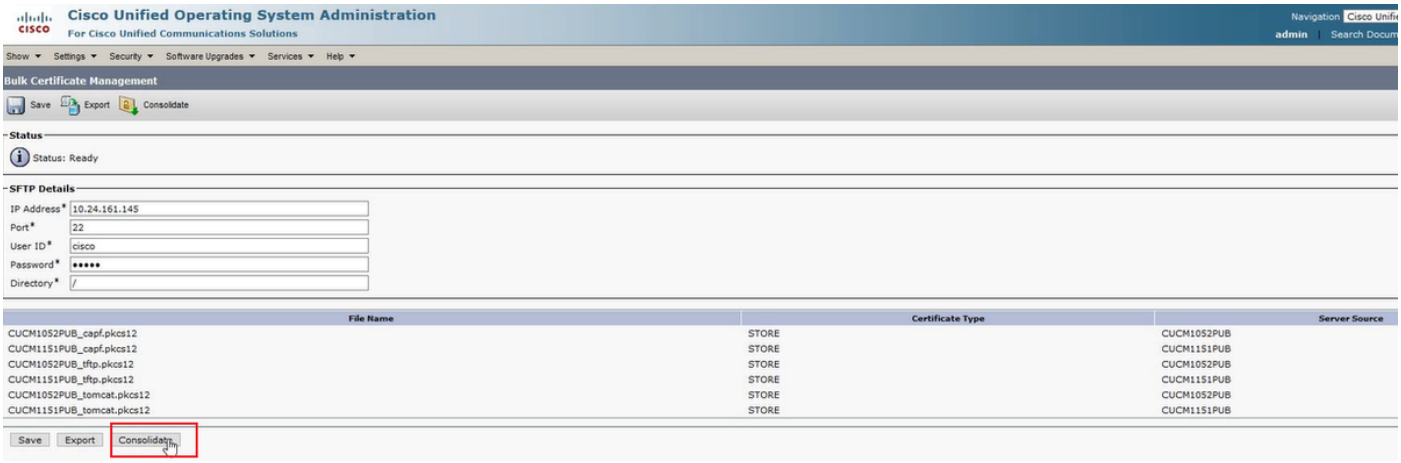
・ポップアップウィンドウを閉じ、ソースクラスタ内の各ノードに対して作成されたPKCS12ファイルを使用して証明書の一括管理(BAT)の更新を行います。Webページが更新され、この情報が表示されます。図に示すように、ソースクラスタのBulk Certificate Management（BAT；一括証明書管理）のWebページに、SFTPにエクスポートされた送信元と宛先の両方のPKCS12ファイルが表示されます。



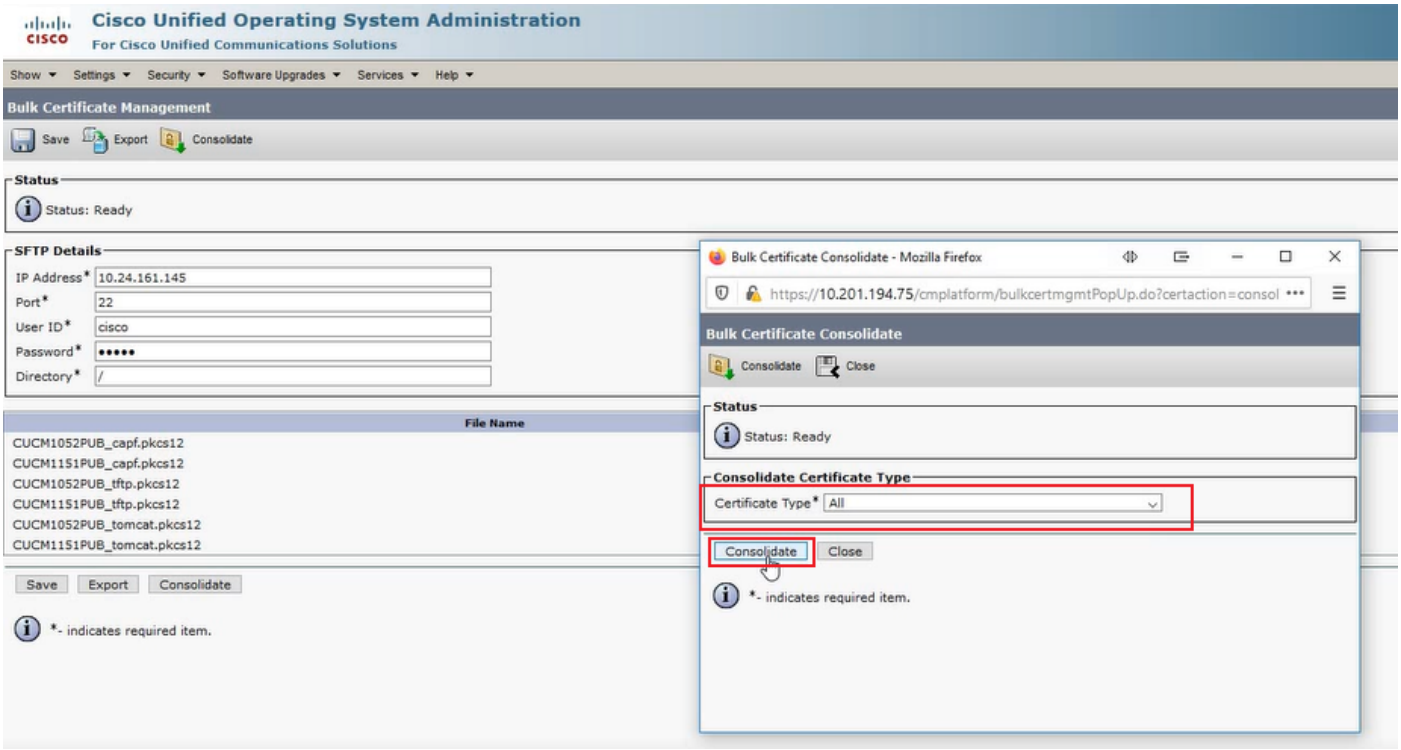
送信元および宛先PKCS12ファイルの統合

> **注：**Bulk Certificate Management（BAT；一括証明書管理）エクスポートは送信元クラスタと宛先クラスタの両方で実行されますが、統合はクラスタの1つでのみCUCMパブリッシャを介して実行されます。

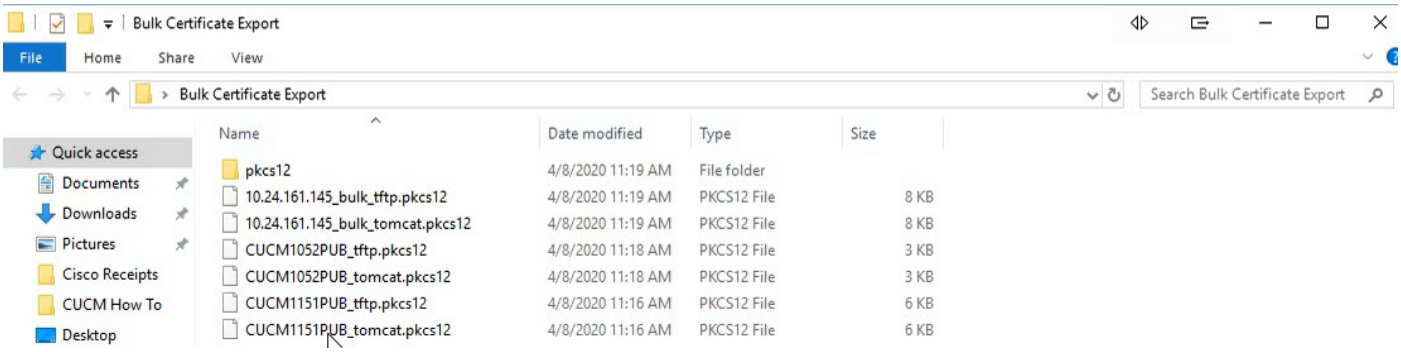
ステップ 1： 図に示すように、ソースクラスタのCUCMパブリッシャの[Bulk Certificate Management]ページに戻り、[Consolidate]をクリックします。

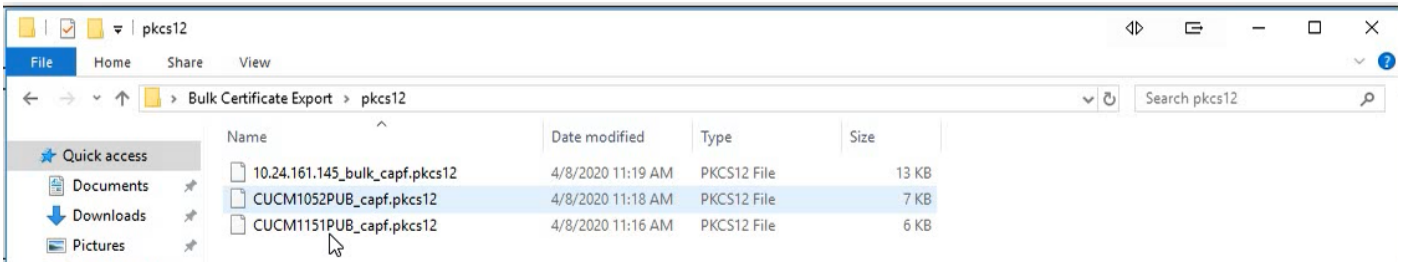


・次のポップアップウィンドウで、[証明書の種類]**に[すべて]**を選択し、図に示すように**[統合]**をクリックします。



・SFTPディレクトリをチェックして、送信元クラスタと宛先クラスタの両方に含まれるpkcs12ファイルをいつでも確認できます。図に示すように、宛先クラスタと送信元クラスタのすべての証明書のエクスポートが完了した後のSFTPディレクトリの内容。

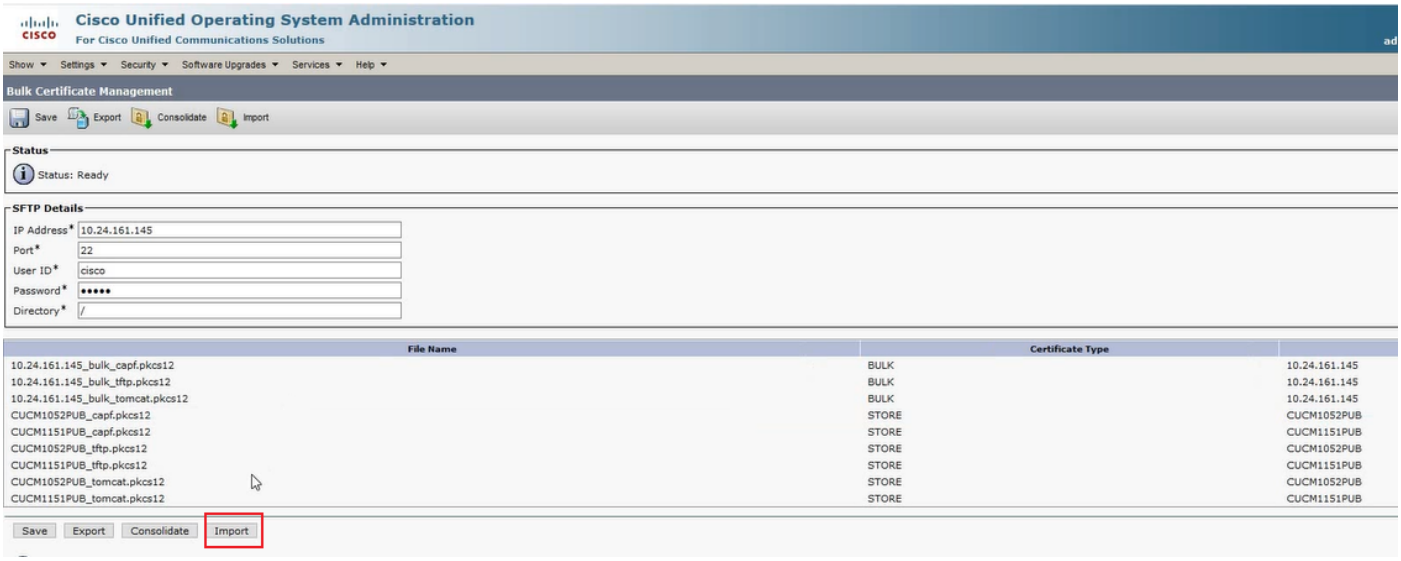




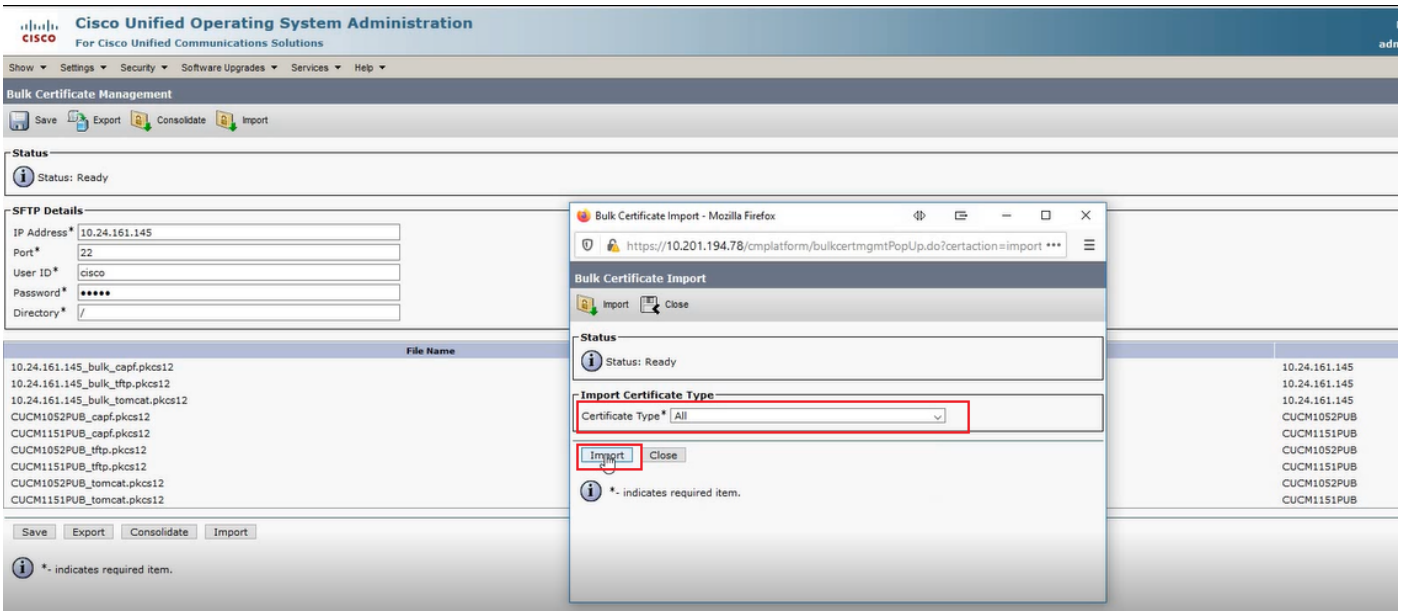
宛先クラスタと送信元クラスタへの証明書のインポート

ステップ1：宛先クラスタへの証明書のインポート

・ 宛先クラスタのCUCMパブリッシャで、[Cisco Unified OS Administration] > [Security] > [Bulk Certificate Management]に移動し、ページを更新してから、図に示すように[Import]をクリックします。



・ 次のポップアップウィンドウで、[Certificate Type]に[All]を選択し、図に示すように[Import]をクリックします。



ステップ 2： ソースクラスタに対して手順1を繰り返します。

注：証明書の一括インポートを実行すると、証明書は次のようにリモートクラスタにアップロードされます。
・ Certificate Authority Proxy Function(CAPF)証明書がCallManager-trustとしてアップロードされます
・ Tomcat証明書がtomcat-trustとしてアップロードされます
・ CallManager証明書がPhone-SAST-trustおよびCallManager-trustとしてアップロードされる
・ Identity Trust List Recovery (ITLRecovery)証明書がPhone-SAST-trustおよびCallManager-trustとしてアップロードされます

宛先クラスタTFTPサーバ情報を使用したソースクラスタ電話機の設定

Trivial File Transfer Protocol(TFTP)オプション150を使用してソースクラスタ電話機のDHCPスコープを設定し、宛先クラスタのCUCM TFTPサーバをポイントするようにします。

移行元クラスタ電話機をリセットして移行先クラスタITL/CTLファイルを取得し、移行プロセスを完了する

移行プロセスの一環として、ソースクラスタの電話機は、ソースクラスタのCisco Trust Verification Service(TVS)へのセキュアな接続をセットアップして、宛先クラスタのCallManagerまたはITLRecovery証明書を確認しようとします。

注：TFTPサービスを実行するCUCMサーバからのソースクラスタのCallManager証明書（TFTP証明書とも呼ばれる）またはそのITLRecovery証明書が、ソースクラスタCUCMノードの証明書信頼リスト(CTL)および/またはアイデンティティ信頼リスト(ITL)ファイルに署名します。同様に、TFTPサービスを実行するCUCMサーバからの宛先クラスタのCallManager証明書またはそのITLRecovery証明書のいずれかが、宛先クラスタのCUCMノードのCTLおよび/またはITLファイルに署名します。CTLファイルとITLファイルは、TFTPサービスを実行するCUCMノードに作成されます。宛先クラスタのCTLおよび/またはITLファイルが送信元クラスタTVSによって検証されない場合、電話機の宛先クラスタへの移行が失敗します。

注：移行元クラスタの電話機の移行プロセスを開始する前に、これらの電話機に有効なCTLファイルまたはITLファイルがインストールされていることを確認します。また、ソースクラスタのエンタープライズ機能[Prepare Cluster for Rollback to Pre 8.0]が[False]に設定されていることを確認します。また、TFTPサービスを実行する宛先クラスタのCUCMノードに、有効なCTLファイルやITLファイルがインストールされていることを確認します。

電話機の移行を完了するために、移行元の電話機の非セキュアクラスタで移行先クラスタITLファイルを取得するプロセス：

ステップ1：リセット時に移行元クラスタ電話機に提示される、移行先クラスタのITLファイルに含まれるCallManagerおよびITLRecovery証明書を使用して、現在インストールされているITLファイルを検証することはできません。これにより、送信元クラスタの電話機は、宛先クラスタのITLファイルを検証するために、送信元クラスタのTVSへの接続を確立します。
ステップ2：電話機がTCPポート2445でソースクラスタTVSへの接続を確立します。
ステップ3：ソースクラスタのTVSは、電話機にその証明書を提示します。電話機は接続を検証し、送信元クラスタTVSに、宛先クラスタのCallManagerまたはITLRecovery証明書を検証して、電話機が宛先クラスタのITLファイルをダウンロードできるようにします。

ステップ4：宛先クラスタのITLファイルの検証とインストールが完了すると、送信元クラスタの電話機は、宛先クラスタから署名付き設定ファイルを検証し、ダウンロードできるようになります。

移行元の電話機のセキュアなクラスタ内のプロセスで、移行先のクラスタCTLファイルを取得し、電話機の移行を完了します。

ステップ1：電話機が起動し、宛先クラスタからCTLファイルをダウンロードしようとします。
ステップ2:CTLファイルは、電話機の現在のCTLファイルまたはITLファイルにない宛先クラスタのCallManagerまたはITLRecovery証明書によって署名されます。
ステップ3：その結果、電話機はソースクラスタのTVSに到達し、CallManagerまたはITLRecovery証明書を確認します。

> **注：**この時点で、電話機には引き続き元のクラスタTVSサービスのIPアドレスを含む古い設定があります。電話機の設定で指定されたTVSサーバは、電話機のCallmanagerグループと同じです。

ステップ4：電話機は、ソースクラスタのTVSへのTransport Layer Security(TLS)接続をセットアップします。
ステップ5：ソースクラスタTVSが電話機に証明書を提示すると、電話機は現在のITLファイルの証明書に対してこのTVS証明書を検証します。
ステップ6：同じ場合、ハンドシェイクは正常に完了します。
ステップ7：送信元の電話機は、宛先クラスタCTLファイルから送信元クラスタTVSにCallManagerまたはITLRecovery証明書を確認するように要求します。
ステップ8：送信元TVSサービスは、その証明書ストアで宛先クラスタCallManagerまたはITLRecoveryを検出し、検証し、送信元クラスタ電話機は宛先クラスタCTLファイルで更新を続行します。
ステップ9：送信元の電話機が、現在含まれている宛先クラスタCTLファイルと照合して検証された宛先クラスタのITLファイルをダウンロードします。送信元の電話機のCTLファイルに宛先クラスタのCallManagerまたはITLRecovery証明書が含まれるため、送信元の電話機は送信元クラスタのTVSに連絡しなくてもCallManagerまたはITLRecovery証明書を確認できます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

設定ウォークスルービデオ

このリンクを使用すると、CUCMクラスタ間のBulk Certificate Management（BAT；証明書の一括管理）を閲覧するビデオにアクセスできます。

CUCMクラスタ間の一括証明書管理