Procedimento para gerenciamento de certificado em massa entre clusters CUCM para migração de telefone

Contents

Introduction

Este documento fornece um procedimento de instruções para o gerenciamento de certificados em massa entre clusters do Cisco Unified Communications Manager (CUCM) para migração de telefone.

Contribuído por Adrian Esquillo, engenheiro do TAC da Cisco.

> **Note**: Este procedimento também está descrito na [seção Gerenciar certificados em massa do Guia de administração do CUCM versão 12.5(1)](#)

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:
Servidor Secure File Transfer Protocol (SFTP)
Certificados CUCM

Componentes Utilizados

As informações neste documento são baseadas no 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Gerenciamento de Certificados em Massa permite que um conjunto de certificados seja compartilhado entre clusters CUCM. Esta etapa é um requisito para as funções do sistema de clusters individuais que precisam ser estabelecidos entre eles, como para o Cluster da Mobilidade de Ramal (EMCC), bem como para a migração de telefones entre clusters.

Como parte do procedimento, um arquivo PKCS12 (Public Key Cryptography Standards #12) que contém certificados de todos os nós em um cluster é criado. Cada cluster deve exportar seus certificados para o mesmo diretório SFTP no mesmo servidor SFTP. As configurações de gerenciamento de certificado em massa devem ser feitas manualmente no editor do CUCM dos clusters de origem e de destino. Os clusters de origem e destino devem estar ativos e operacionais para que os telefones a serem migrados tenham conectividade com ambos os clusters. Os telefones do cluster de origem são migrados para o cluster de destino.

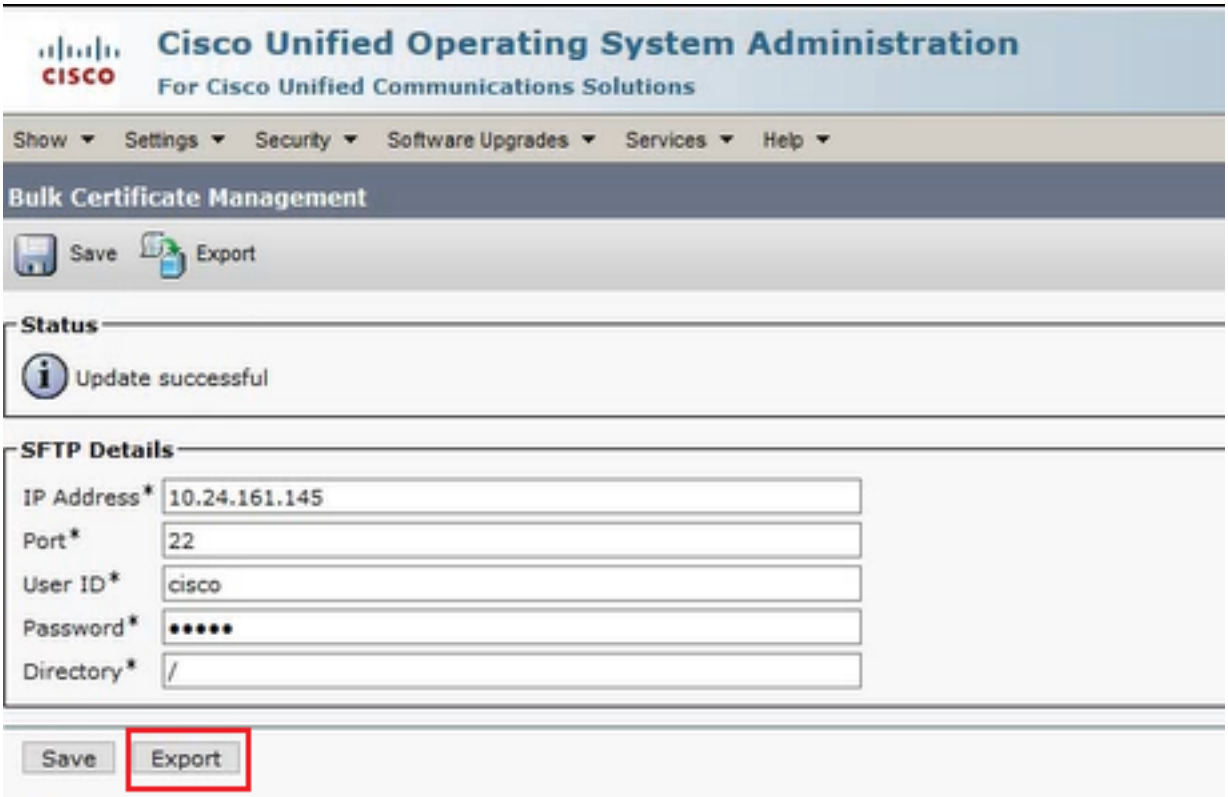
Procedimento de gerenciamento de certificado em massa

Exportar certificados de cluster de destino

Etapa 1. Configure o servidor SFTP para Gerenciamento de Certificados em Massa no editor CUCM do cluster de destino.

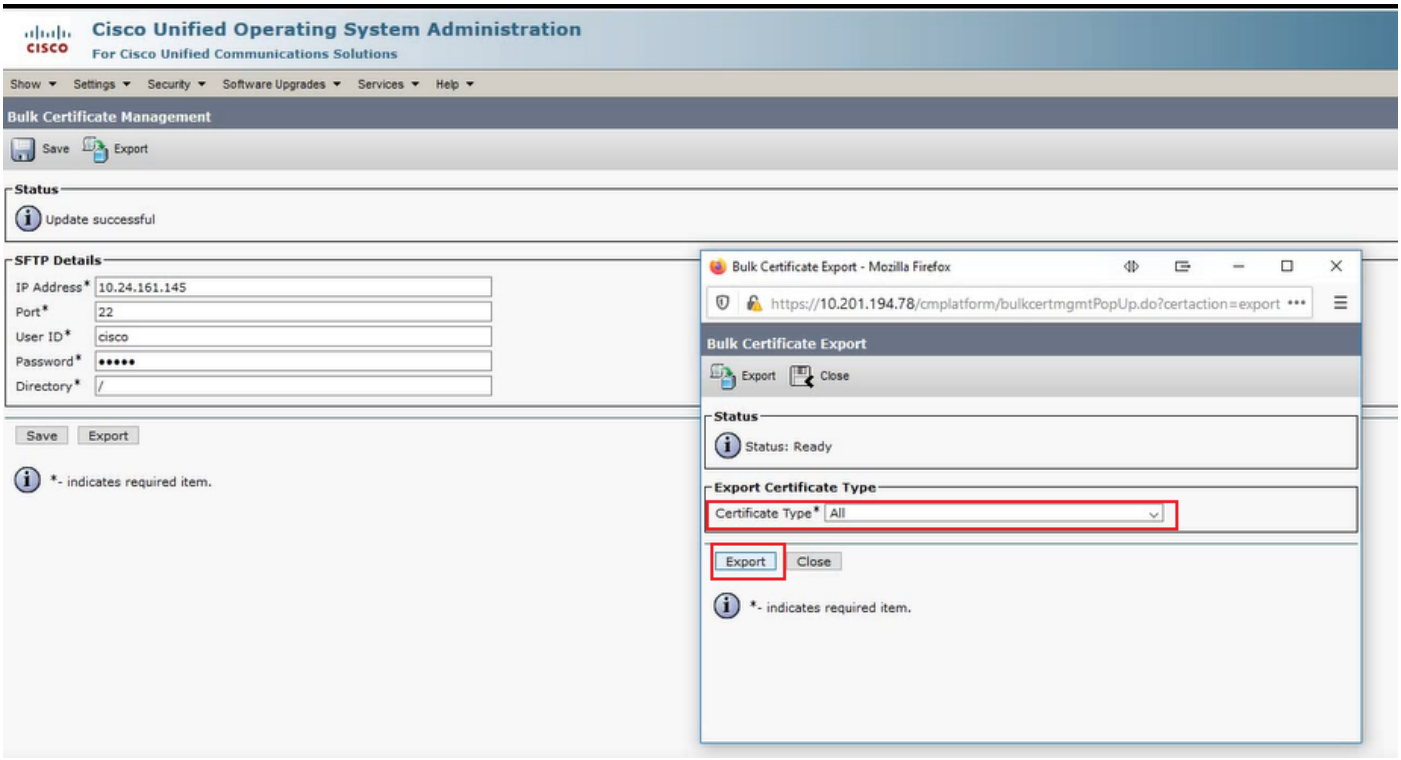
Neste exemplo, a versão do CUCM do cluster de destino é 11.5.1.

·**Navegue** até **Cisco Unified OS Administration > Security > Bulk Certificate Management** insira os detalhes do servidor SFTP e **clique em** Export, como mostrado na imagem.

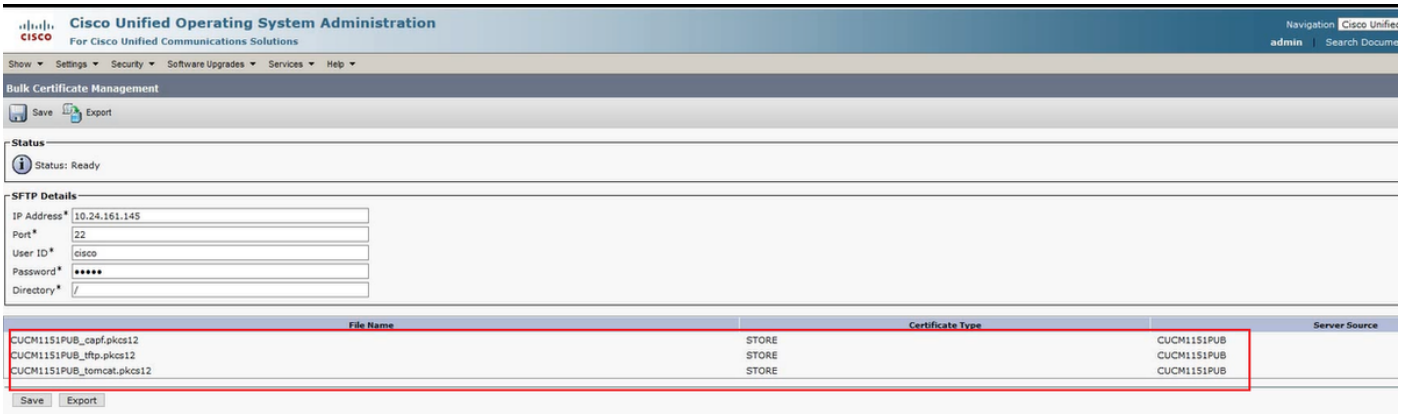


Etapa 2. Exportar todos os certificados de todos os nós no cluster de destino para o servidor SFTP.

·Na janela pop-up subsequente, selecione **All** for Certificate Type e clique em **Export**, como mostrado na imagem.



Feche a janela pop-up e as atualizações do Bulk Certificate Management com os arquivos PKCS12 criados para cada um dos nós no cluster de destino, a página da Web é atualizada com essas informações, como mostrado na imagem.



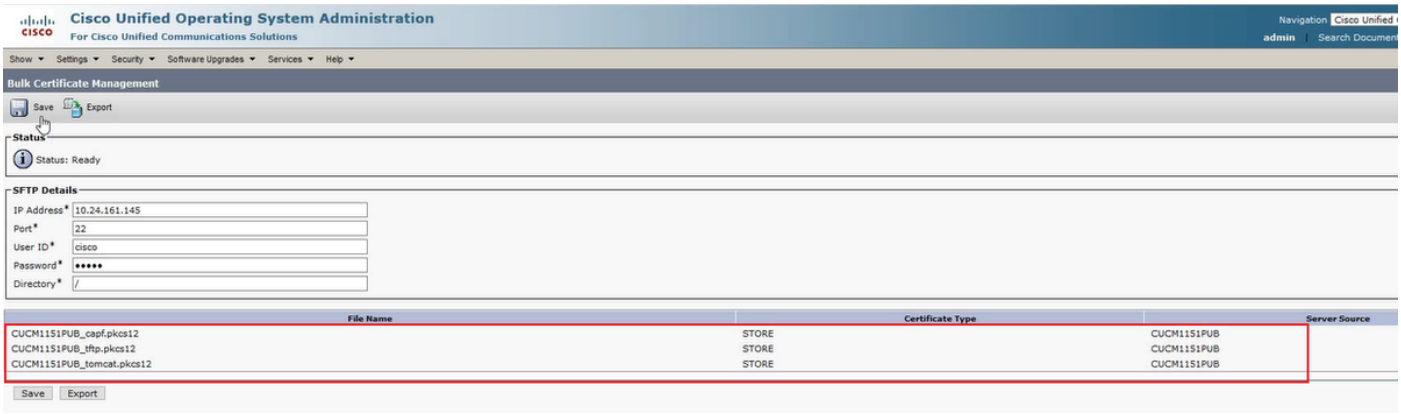
Exportar certificados do cluster de origem

Etapa 1. Configure o servidor SFTP para Gerenciamento de Certificados em Massa no editor CUCM do cluster de origem.

Neste exemplo, a versão do CUCM do cluster de origem é 10.5.2.

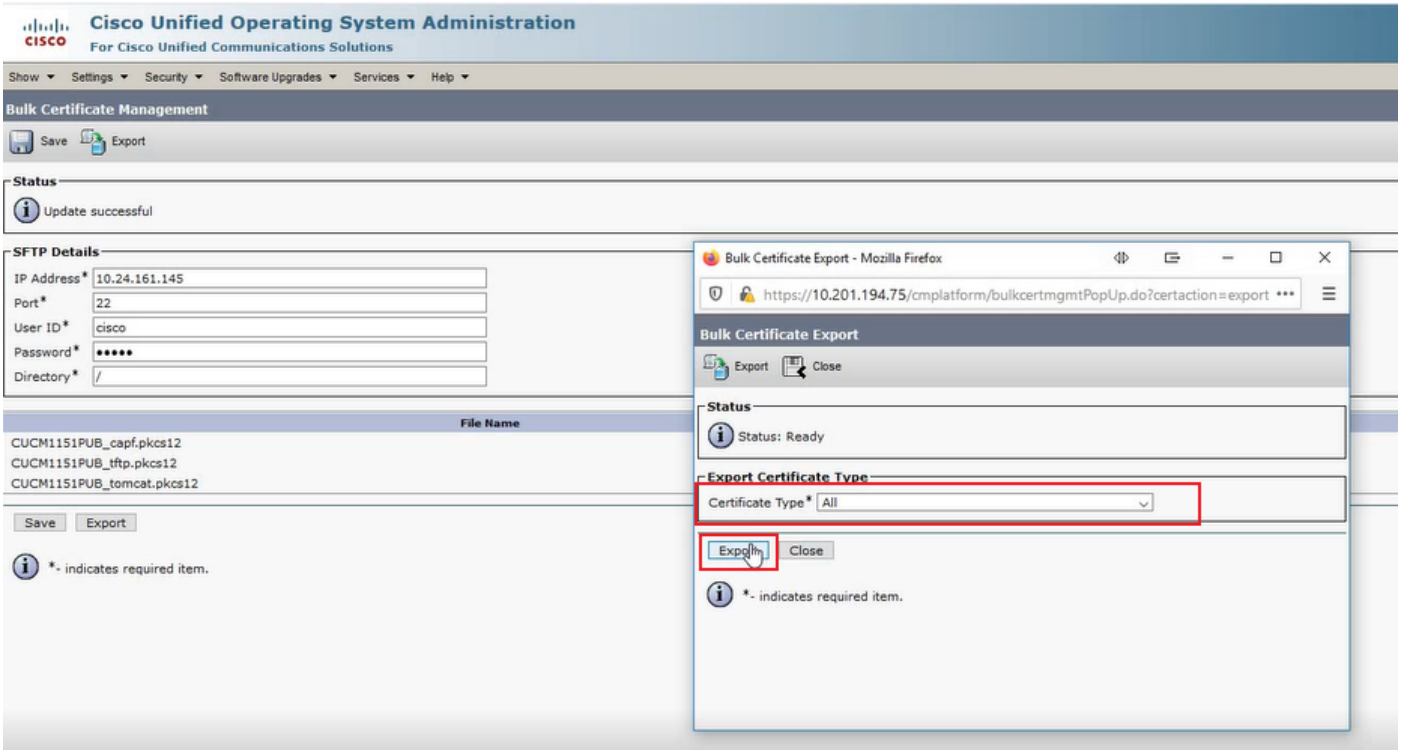
·**Navegue** até **Cisco Unified OS Administration > Security > Bulk Certificate Management** insira os detalhes do servidor SFTP e **clique em** Export, como mostrado na imagem.

> **Note**: Os arquivos PKCS12 exportados do cluster de destino para o servidor SFTP são mostrados na página da Web Bulk Certificate Management do editor CUCM do cluster de origem quando acessados.

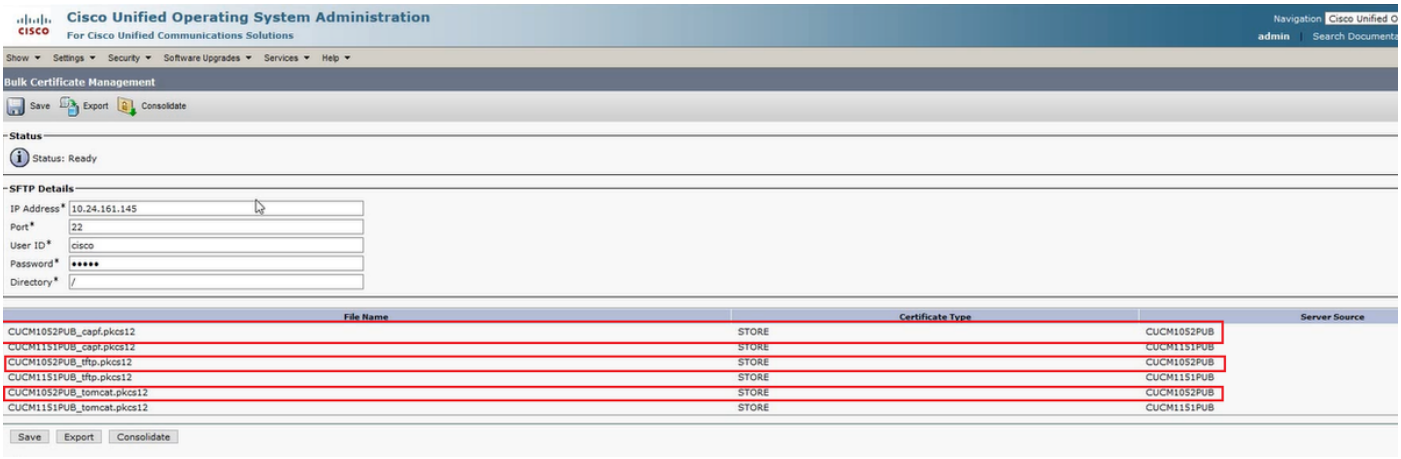


Etapa 2. Exportar todos os certificados de todos os nós no cluster de origem para o servidor SFTP.

·Na janela pop-up subsequente, selecione **All** for Certificate Type e clique em **Export**, como mostrado na imagem.



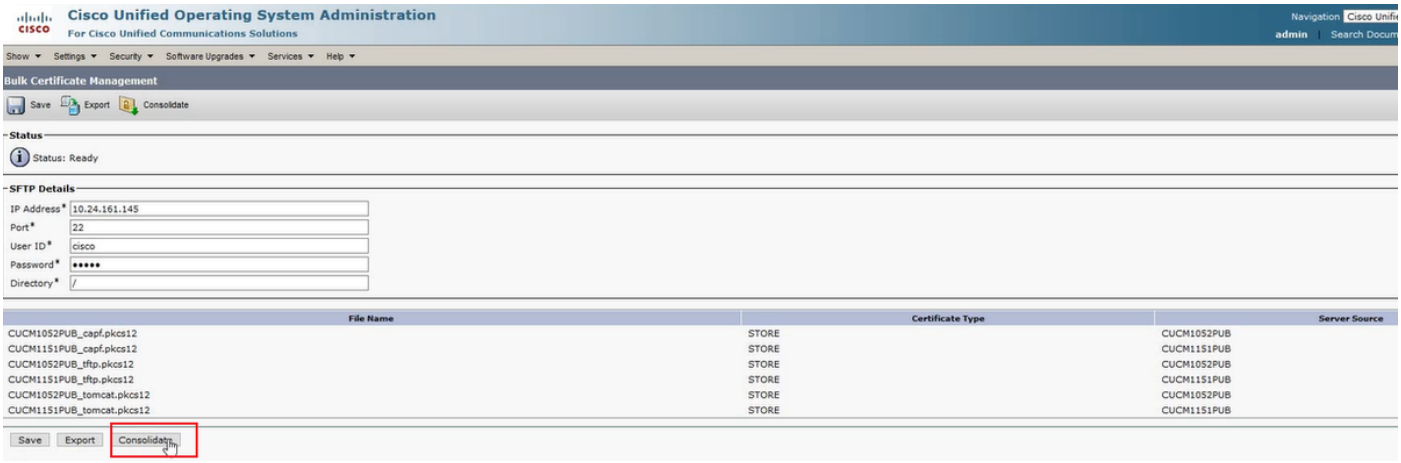
Feche a janela pop-up e as atualizações do Bulk Certificate Management com os arquivos PKCS12 criados para cada um dos nós no cluster de origem, a página da Web é atualizada com essas informações. A página da Web do Bulk Certificate Management do cluster de origem agora mostra os arquivos PKCS12 de origem e de destino exportados para SFTP, como mostrado na imagem.



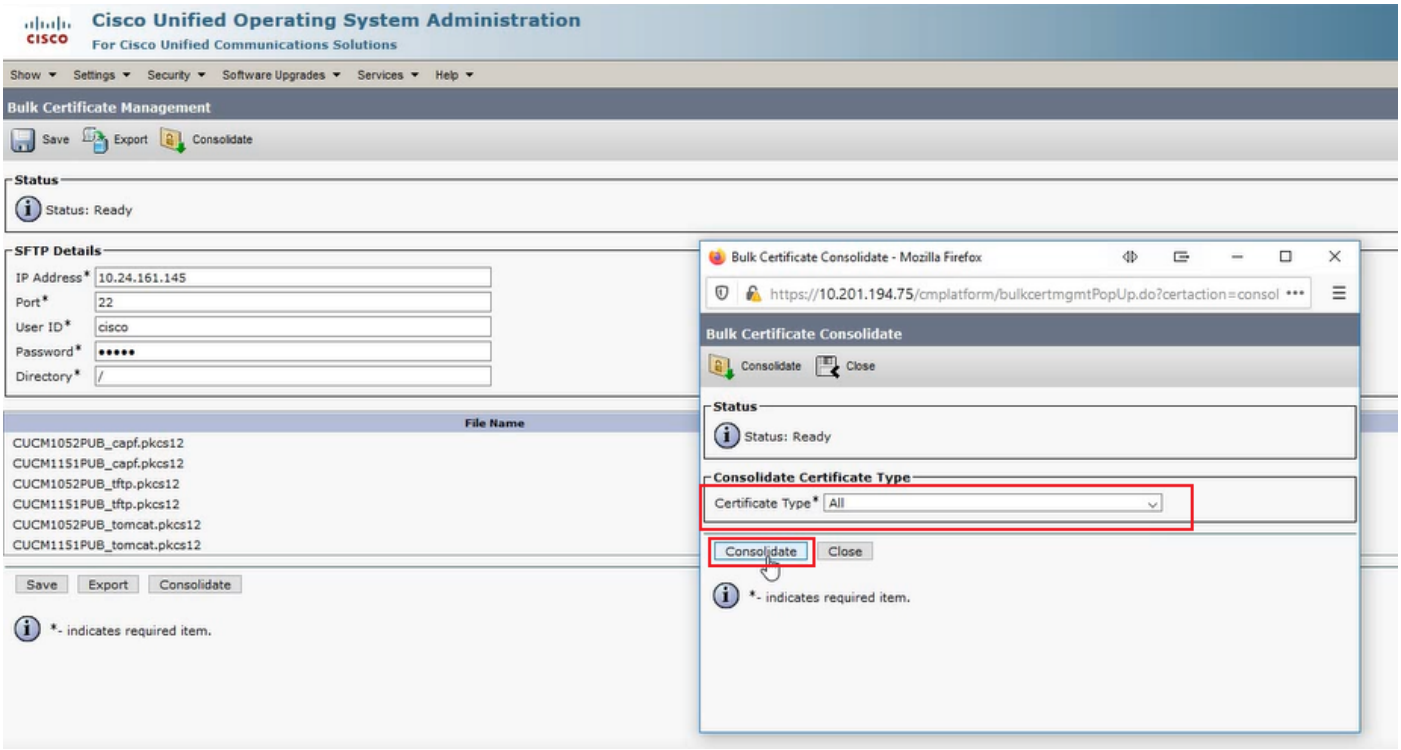
Consolidar arquivos PKCS12 de origem e destino

> **Note**: Enquanto a exportação do Bulk Certificate Management é feita nos clusters de origem e de destino, a consolidação é feita através do editor do CUCM em apenas um dos clusters.

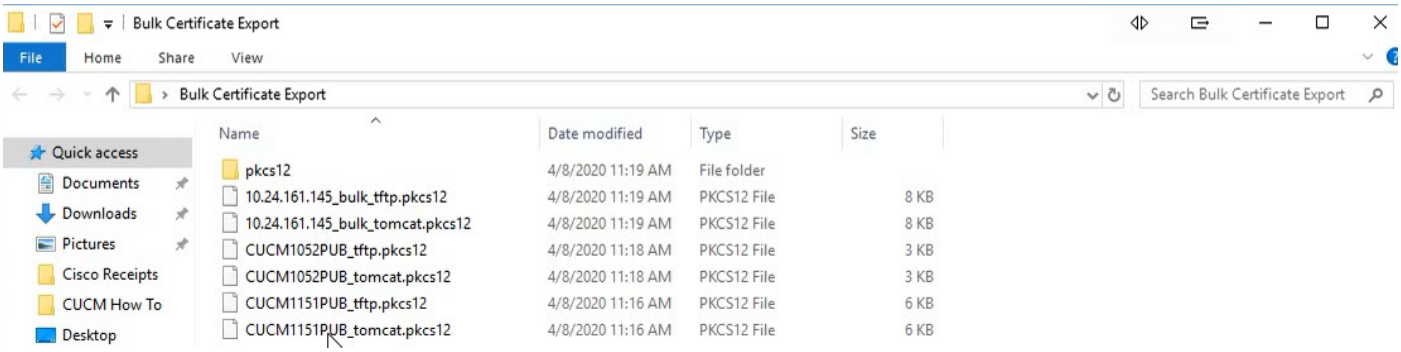
Etapa 1. Retorne à página Gerenciamento de certificado em massa do editor do CUCM do cluster de origem e **clique** em Consolidar, como mostrado na imagem.

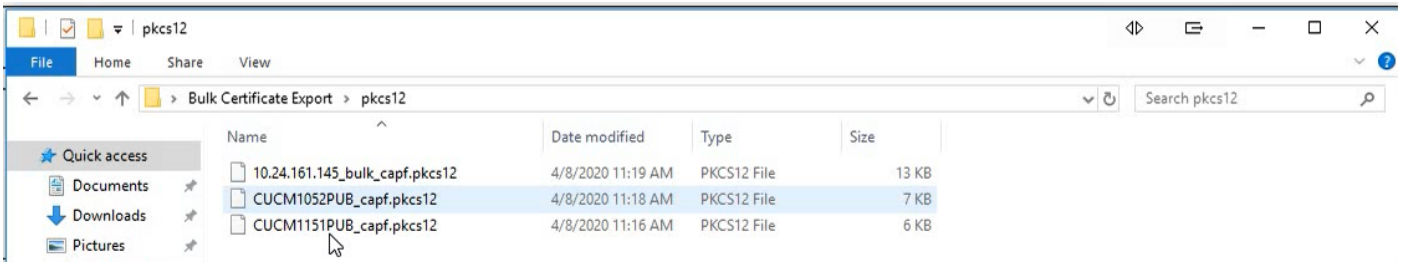


·Na janela pop-up subsequente, selecione **All** for Certificate Type e clique em **Consolidate**, como mostrado na imagem.



· A qualquer momento, você pode verificar o diretório SFTP para verificar os arquivos pkcs12 contidos nos clusters de origem e de destino. O conteúdo do diretório SFTP após a exportação de todos os certificados dos clusters de origem e de destino foi concluído, como mostrado nas imagens.

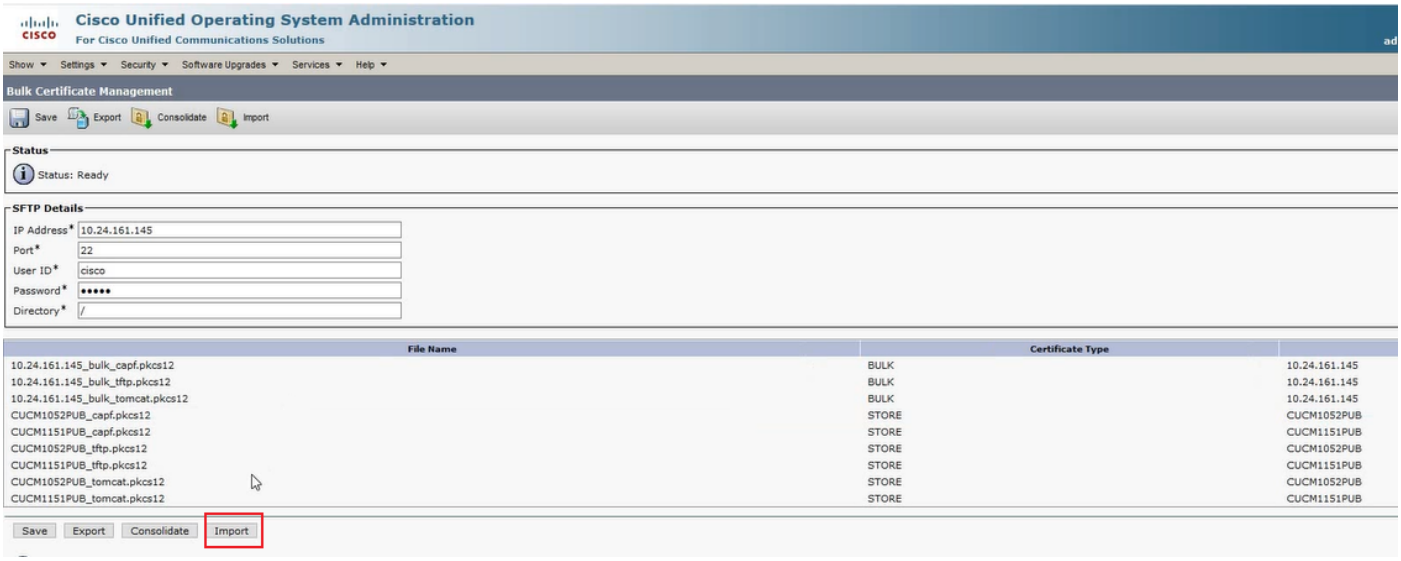




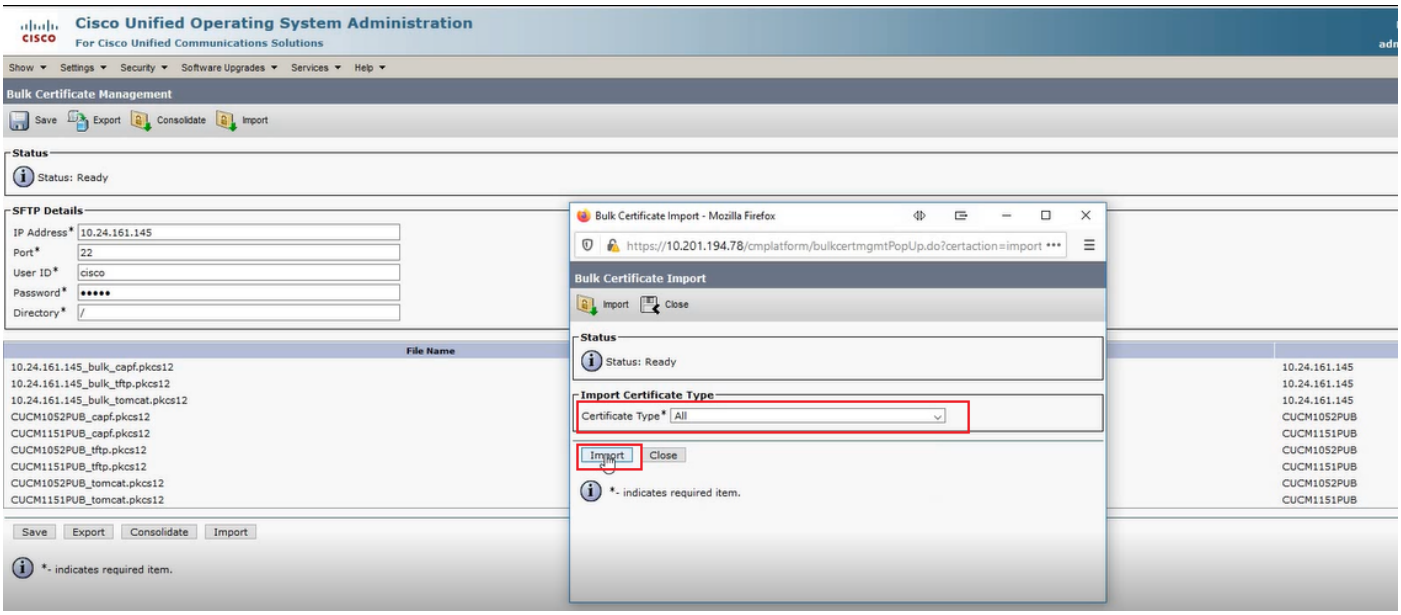
Importar certificados para clusters de destino e origem

Etapa 1. Importar certificados para o cluster de destino

· No editor do CUCM do cluster de destino **Navegue** para **Cisco Unified OS Administration > Security > Bulk Certificate Management** e deixe a página atualizar e, em seguida, **clique em** Import, como mostrado na imagem.



·Na janela pop-up subsequente, selecione **All** for Certificate Type e clique em **Import**, conforme mostrado na imagem.



Etapa 2. Repita a etapa 1 para o cluster de origem.

Note: Quando a importação de certificado em massa é executada, os certificados são carregados para o cluster remoto da seguinte maneira:
O certificado CAPF (Certificate Authority Proxy Function) é carregado como um CallManager-trust
O certificado Tomcat é carregado como um tomcat-trust
O certificado do CallManager é carregado como Phone-SAST-trust e CallManager-trust
O certificado do Identity Trust List Recovery (ITLRecovery) é carregado como Phone-SAST-trust e CallManager-trust

Configurar telefones do cluster de origem com informações do servidor TFTP do cluster de destino

Configure o escopo de DHCP para telefones de cluster de origem com a Opção 150 do Trivial File Transfer Protocol (TFTP) para apontar para servidores TFTP CUCM de cluster de destino.

Redefinir telefones de cluster de origem para obter o arquivo ITL/CTL do cluster de destino para concluir o processo de migração

Como parte do processo de migração, os telefones do cluster de origem tentam configurar uma conexão segura com o Cisco Trust Verification Service (TVS) do cluster de origem para verificar o certificado de recuperação do CallManager ou ITLR do cluster de destino.

Note: O certificado CallManager do cluster de origem de um servidor CUCM que executa o serviço TFTP (também conhecido como certificado TFTP) ou seu certificado ITLRecovery assina um arquivo de lista de confiança de certificado (CTL) e/ou lista de confiança de identidade (ITL) do nó CUCM do cluster de origem. Da mesma forma, o certificado CallManager do cluster de destino de um servidor CUCM que executa o serviço TFTP ou seu certificado de recuperação ITLR assina um arquivo CTL e/ou ITL do nó CUCM do cluster de destino. Os arquivos CTL e ITL são criados em nós CUCM que executam o serviço TFTP. Se um arquivo CTL e/ou ITL do cluster de destino não for validado pelo TVS do cluster de origem, a migração do telefone para o cluster de destino falhará.

Note: Antes de iniciar o processo de migração do telefone do cluster de origem, confirme se esses telefones têm um arquivo CTL e/ou ITL válido instalado. Além disso, certifique-se de que o recurso corporativo "Prepare o cluster para reversão para Pre 8.0" esteja definido como False para o cluster de origem. Além disso, verifique se os nós CUCM do cluster de destino que executam o serviço TFTP têm arquivos CTL e/ou ITL válidos instalados.

Processo no cluster não seguro para telefones de origem para obter o arquivo ITL do cluster de destino para concluir a migração de telefones:

Etapa1. Nem o certificado de recuperação ITLR ou CallManager contido no arquivo ITL do cluster de destino, apresentado ao telefone do cluster de origem na redefinição, pode ser usado para validar o arquivo ITL atualmente instalado. Isso faz com que o telefone do cluster de origem estabeleça uma conexão com o TVS do cluster de origem para validar o arquivo ITL do cluster de destino.
Etapa 2. O telefone estabelece uma conexão com o cluster de origem TVS na porta tcp 2445.
Etapa 3. O TVS do cluster de origem apresenta seu certificado ao telefone. O telefone valida a conexão e solicita que o TVS do cluster de origem valide o certificado do CallManager ou

ITLRecovery do cluster de destino para permitir que o telefone baixe o arquivo ITL do cluster de destino.
Etapa 4. Após a validação e instalação do arquivo ITL do cluster de destino, o telefone do cluster de origem agora pode validar e baixar arquivos de configuração assinados do cluster de destino.

Processo no cluster seguro para telefones de origem para obter o arquivo CTL do cluster de destino para concluir a migração de telefones:

Etapa 1. O telefone é inicializado e tenta baixar o arquivo CTL do cluster de destino.
Etapa 2. O arquivo CTL é assinado pelo certificado CallManager ou ITLRecovery do cluster de destino que não está no arquivo CTL ou ITL atual do telefone.
Etapa 3. Como resultado, o telefone chega ao TVS no cluster de origem para verificar o certificado de recuperação do CallManager ou ITLR.

> **Note**: Neste ponto, o telefone ainda tem sua configuração antiga que contém o endereço IP do serviço TVS do cluster de origem. Os servidores TVS especificados na configuração dos telefones são os mesmos que o grupo do Callmanager dos telefones.

Etapa 4. O telefone configura uma conexão TLS (Transport Layer Security) para o TVS no cluster de origem.
Etapa 5. Quando o cluster de origem TVS apresenta seu certificado ao telefone, o telefone verifica esse certificado TVS em relação ao certificado em seu arquivo ITL atual.
Etapa 6. Se forem iguais, o handshake é concluído com êxito.
Passo 7. O telefone de origem solicita que o cluster de origem TVS verifique o certificado de recuperação do CallManager ou ITLR a partir do arquivo CTL do cluster de destino.
Etapa 8. O serviço TVS de origem localiza o cluster de destino CallManager ou ITLRecovery em seu repositório de certificados, o valida e o telefone do cluster de origem continua a ser atualizado com o arquivo CTL do cluster de destino.
Etapa 9. O telefone de origem faz o download do arquivo ITL do cluster de destino, validado em relação ao arquivo CTL do cluster de destino que ele agora contém. Como o arquivo CTL do telefone de origem agora contém o certificado de recuperação do CallManager ou ITLR do cluster de destino, o telefone de origem agora pode verificar o certificado de recuperação do CallManager ou ITLR sem precisar entrar em contato com o TVS do cluster de origem.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Vídeo de acompanhamento da configuração

Este link fornece acesso a um vídeo que passa pelo Gerenciamento de Certificados em Massa entre Clusters CUCM:

Gerenciamento de certificado em massa entre clusters CUCM