Criar e usar certificado de terceiros no UCSM

Contents

Introdução

Este documento descreve o procedimento para criar e usar certificados de terceiros no Unified Computing System (UCS) para comunicação segura.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à autoridade de certificação
- UCSM 3.1

Componentes Utilizados

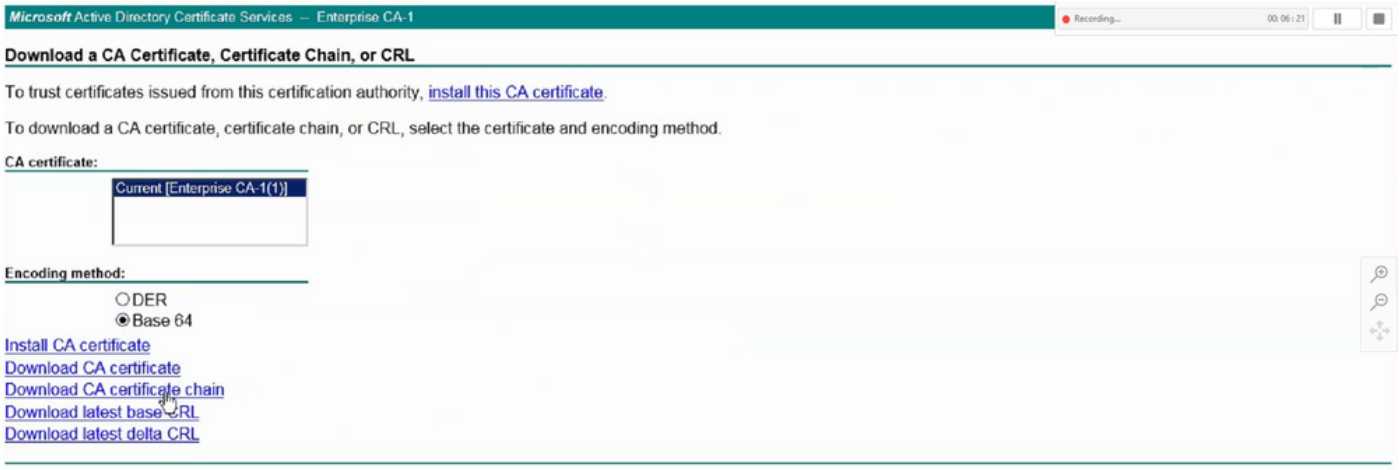
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Etapas para configurar

Configurar Ponto de Confiança

Passo 1

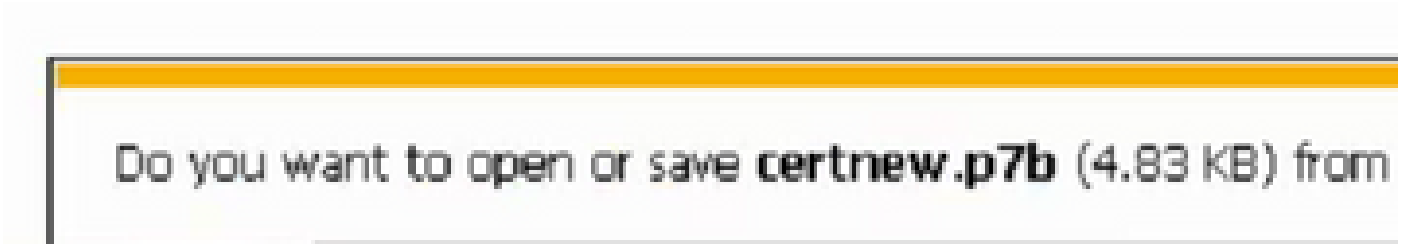
- Baixe a cadeia de certificados da autoridade de certificação para criar um Ponto de Confiança. Consulte http://localhost/certsrv/Default.asp no Servidor Cert.
- Verifique se a codificação está definida como Base 64.



Baixar cadeia de certificados da autoridade de certificação

Passo 2

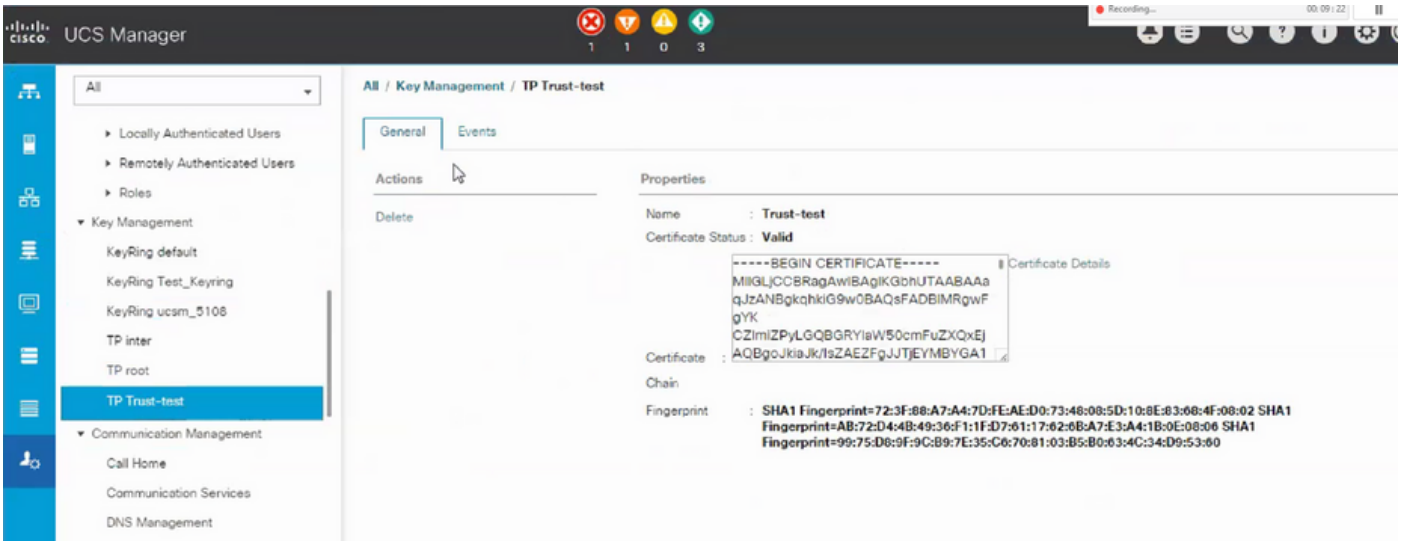
- A cadeia de certificados baixada está no formato PB7.



- Converta o arquivo .pb7 para o formato PEM com a ferramenta OpenSSL.
- Por exemplo, no Linux, você pode executar esse comando no terminal para executar a conversão- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

Etapa 3

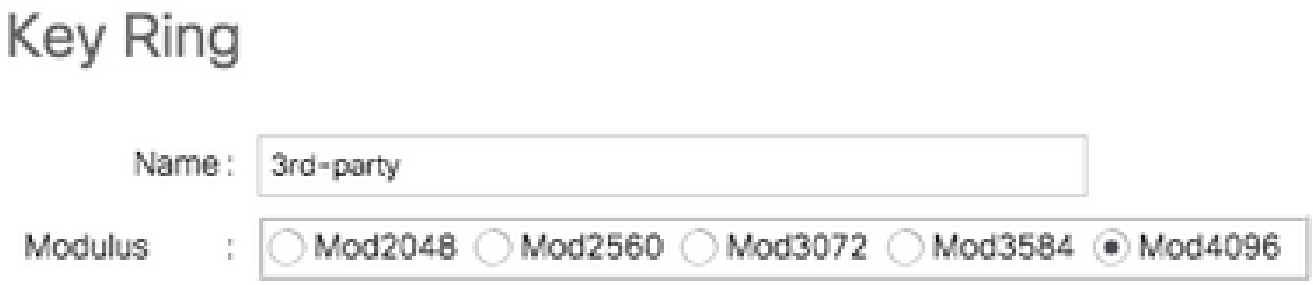
- Crie um ponto de confiança no UCSM.
- Navegue até Admin > Gerenciamento de chaves > Trustpoint.
- Ao criar o ponto de confiança, cole o conteúdo completo do arquivo .PEM criado na etapa 2 desta seção no espaço de detalhes do certificado.



Criar chaveiro e CSR

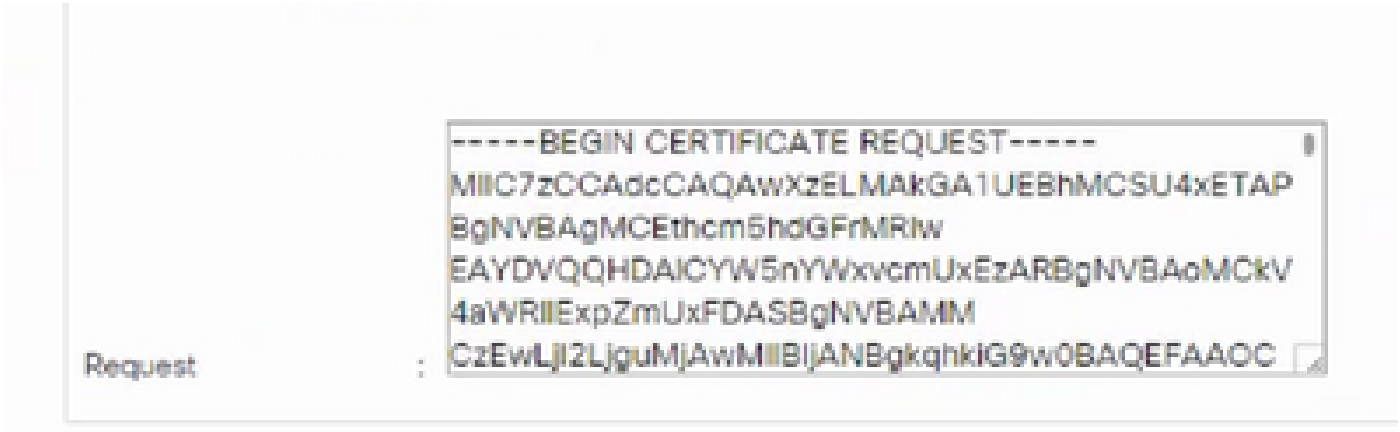
Passo 1

- Navegue até UCSM > Admin > Key Management > Keyring.
- Escolha o Módulo necessário para o certificado de terceiros.



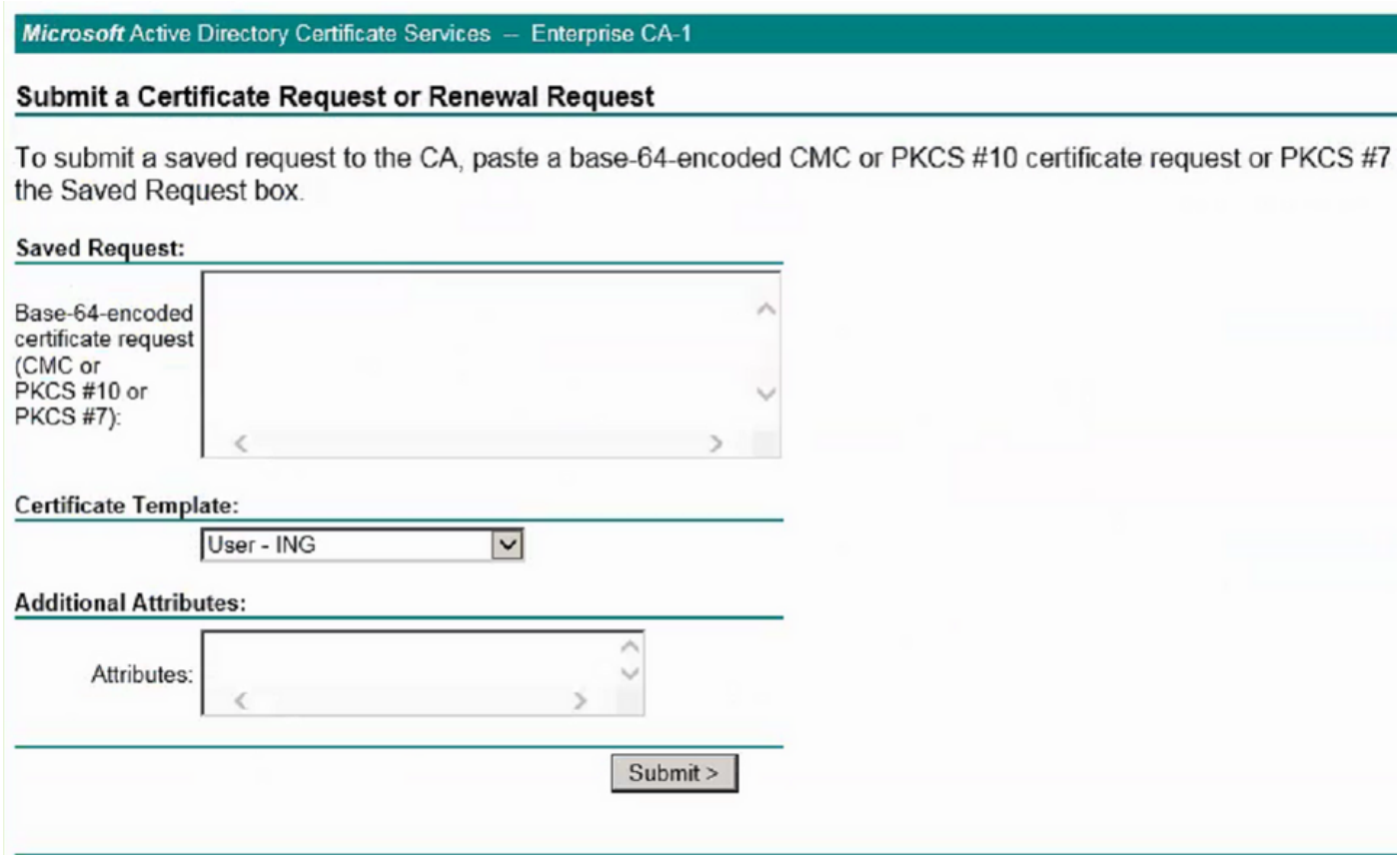
Passo 2

- Clique em criar solicitação de certificado e preencha os detalhes solicitados.
- Copie o conteúdo do campo de solicitação.



Etapa 3

Para gerar o certificado, cole a solicitação copiada da etapa 2 no espaço mostrado abaixo:



Passo 4

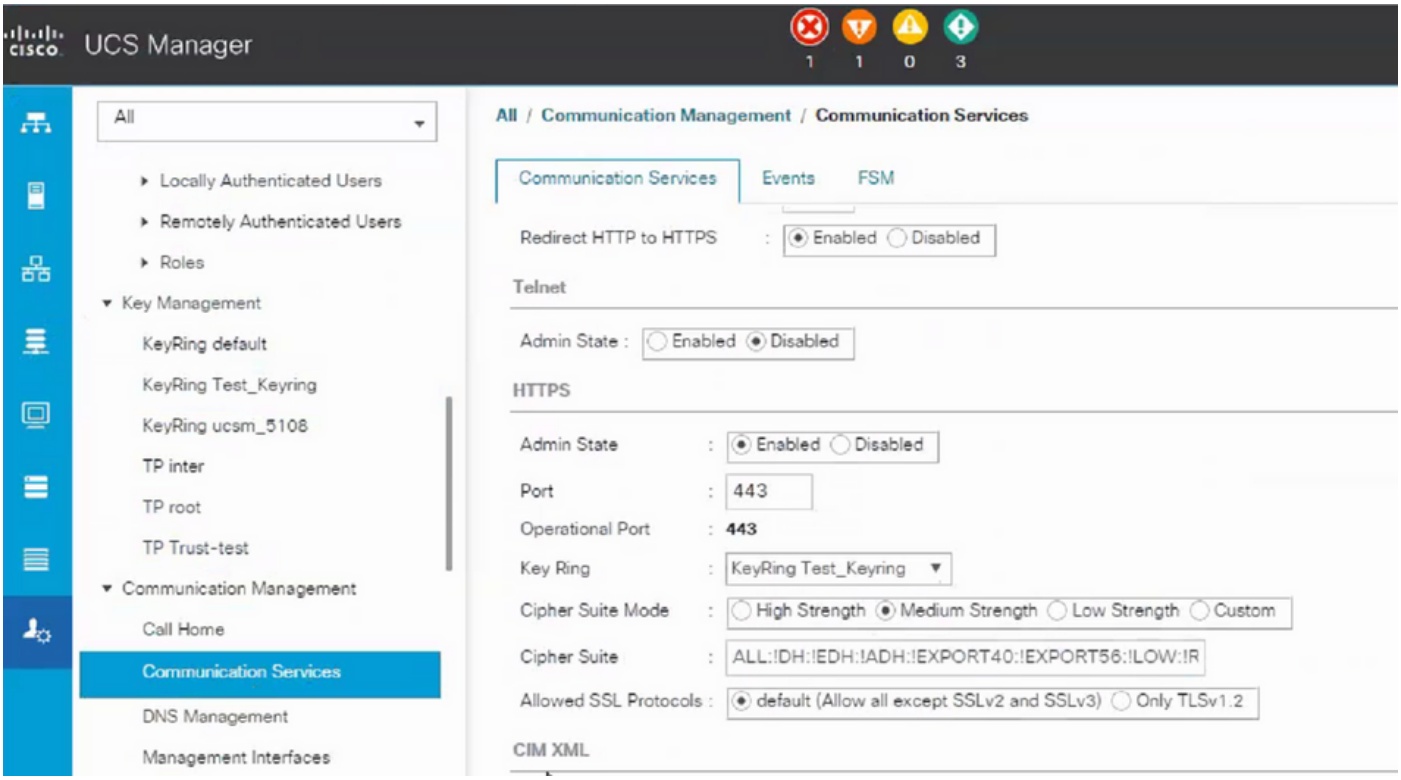
- Depois de enviado, um novo certificado é gerado. Abra o arquivo e copie todo o conteúdo do certificado recém-gerado no campo do certificado no keyring criado na etapa 1 desta seção.

- Escolha o ponto de confiança no menu suspenso criado na etapa 3 de Criar chaveiro e CSR.

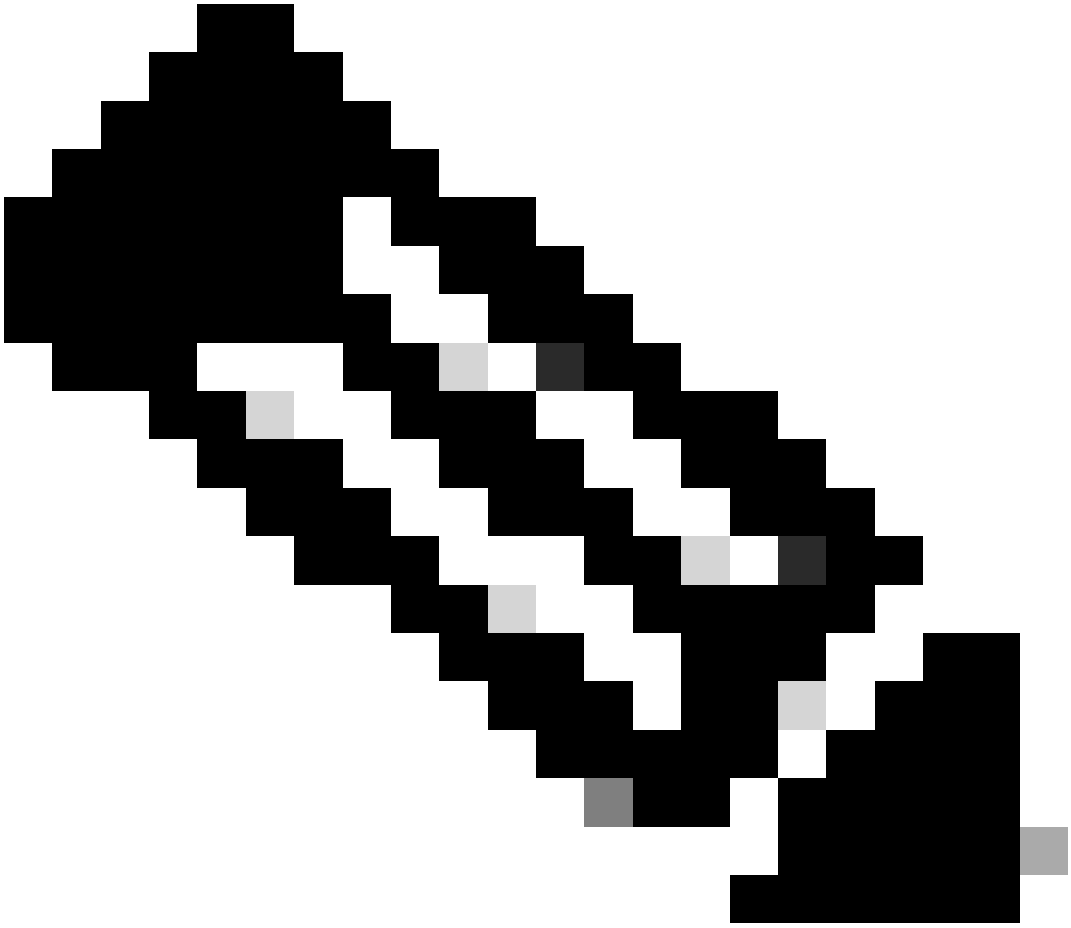
Aplicar o toque de tecla

Passo 1

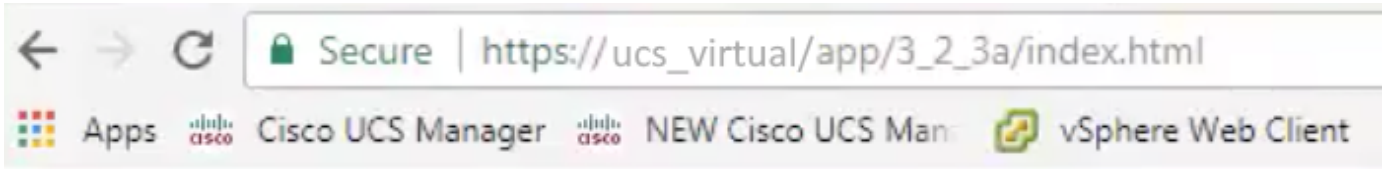
Escolha o chaveiro criado nos serviços de comunicação como mostrado abaixo:



Após a alteração no chaveiro, a conexão HTTPS com o UCSM aparece como segura em seu navegador da Web.



Observação: isso exige que a área de trabalho local também use o certificado da mesma autoridade CA que o UCSM.



Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.