

Configurar certificado de terceiros para UCS Central

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Criar o Ponto Confiável](#)

[Criação de Key Ring e CSR](#)

[Aplicar o toque de tecla](#)

[Validação](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as práticas recomendadas para configurar um certificado de terceiros no Cisco Unified Computing System Central Software (UCS Central).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Cisco UCS Central
- autoridade de certificado (CA)
- OpenSSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- UCS Central 2.0(1q)
- Serviços de Certificados do Microsoft Active Directory
- Windows 11 Pro N
- OpenSSL 3.1.0

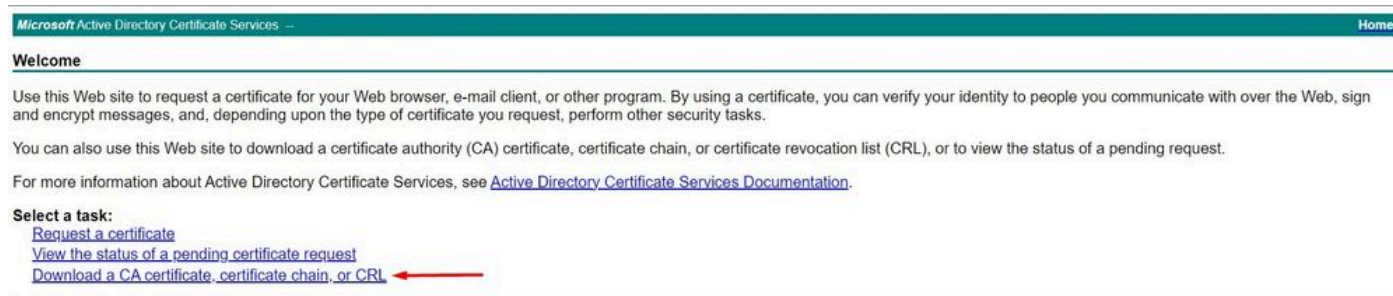
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Faça o download da cadeia de certificados da autoridade de certificação.

1. Faça o download da cadeia de certificados da Autoridade de Certificação (CA).



Microsoft Active Directory Certificate Services -- Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

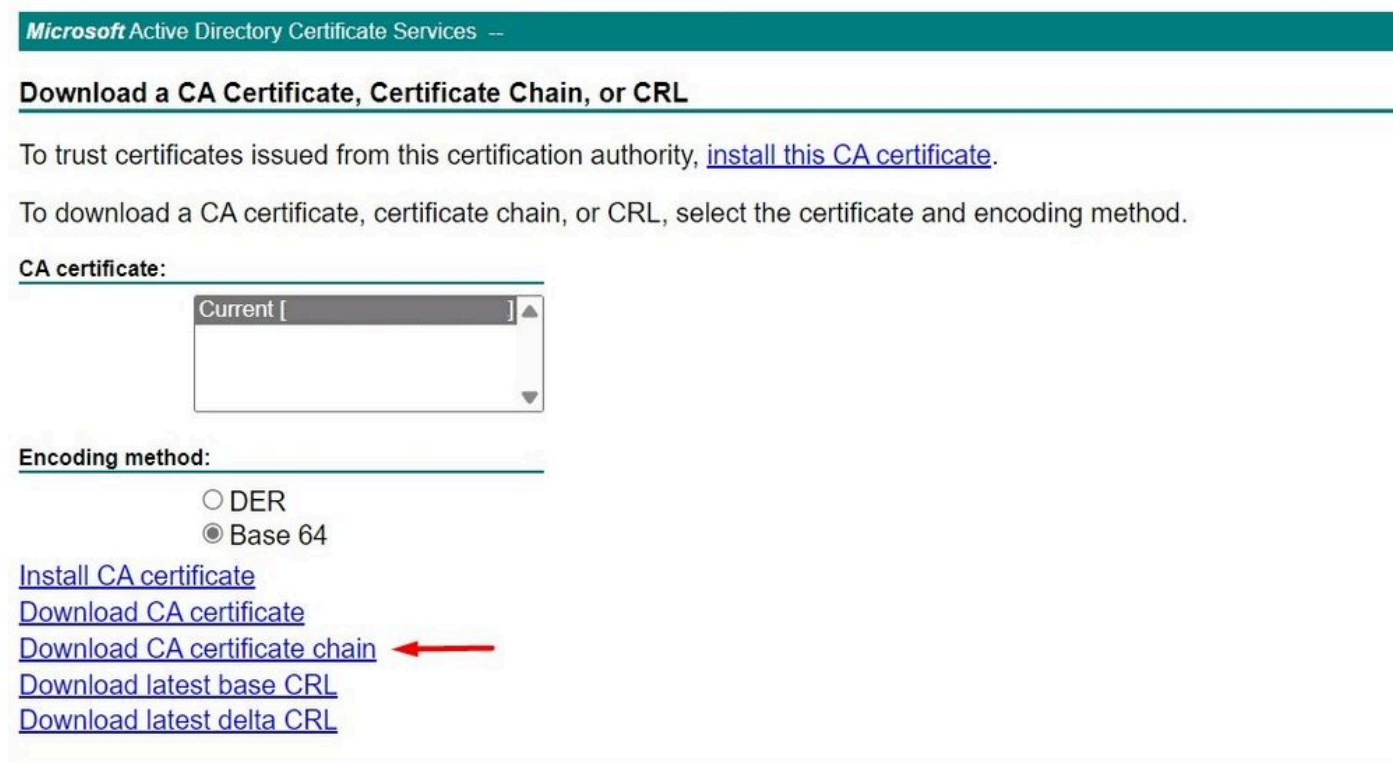
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Baixar uma cadeia de certificados da autoridade de certificação

2. Defina a codificação como Base 64 e baixe a cadeia de certificados da CA.



Microsoft Active Directory Certificate Services --

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current []

Encoding method:

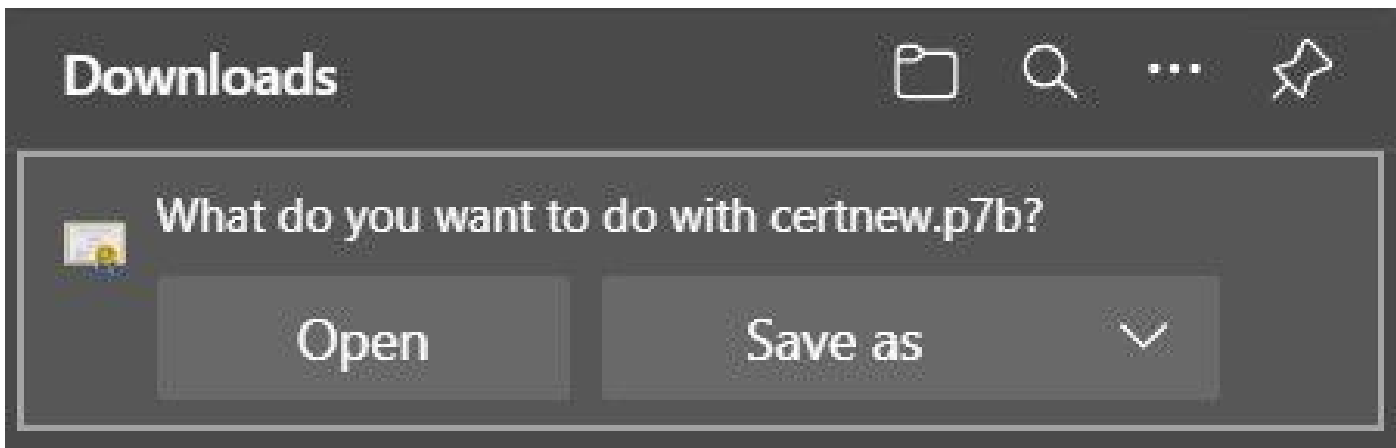
DER

Base 64

- [Install CA certificate](#)
- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

Defina a codificação como Base 64 e baixe a cadeia de certificados da CA

3. Observe que a cadeia de certificados da autoridade de certificação está no formato PB7.



O certificado está no formato PB7

4. O certificado tem de ser convertido para o formato PEM com a ferramenta OpenSSL. Para verificar se o Open SSL está instalado no Windows, use o comando `openssl version`.

```
C:\Program Files\OpenSSL-Win64\bin>openssl version
OpenSSL 3.1.0 14 Mar 2023 (Library: OpenSSL 3.1.0 14 Mar 2023)
```

Verificar se o OpenSSL está instalado

 Nota: A instalação do OpenSSL está fora do escopo deste artigo.

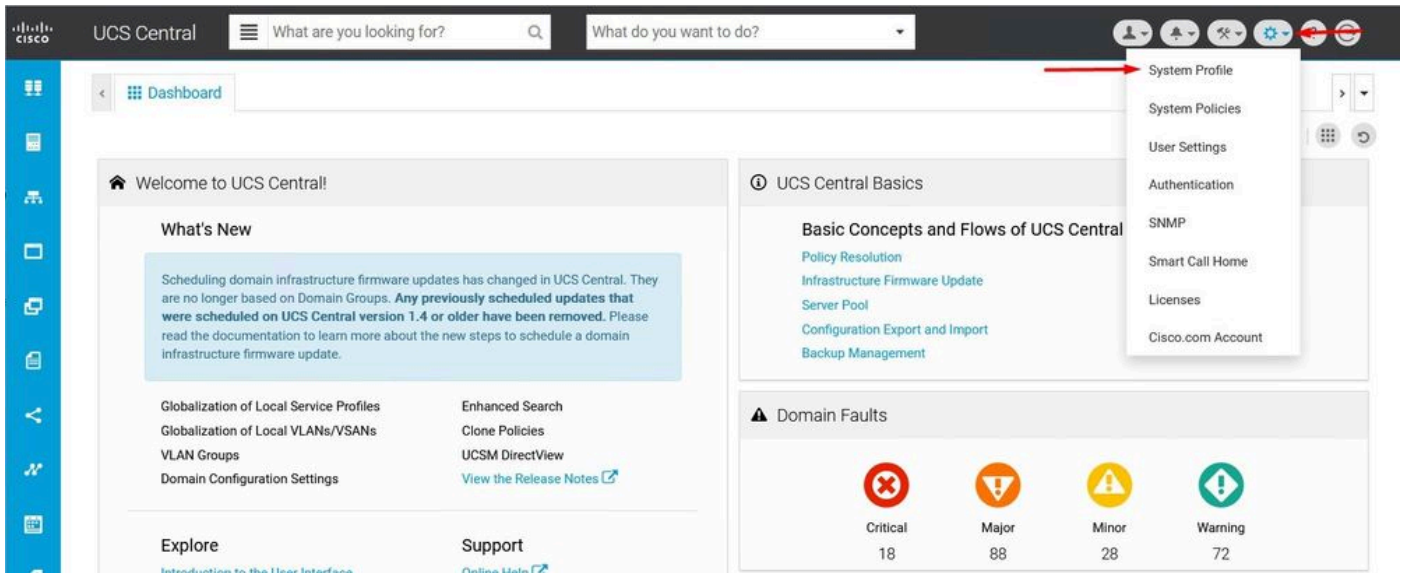
5. Se o OpenSSL estiver instalado, execute o comando `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` para executar a conversão. Certifique-se de usar o caminho onde o certificado foi salvo.

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkcs7 -print_certs -in C://Users/ /Desktop/certnew.p7b -out C://Users/ /Desktop/certnew.pem
```

Converter o certificado P7B para o formato PEM

Criar o Ponto Confiável

1. Clique no ícone Configuração do Sistema > Perfil do Sistema > Pontos Confiáveis.

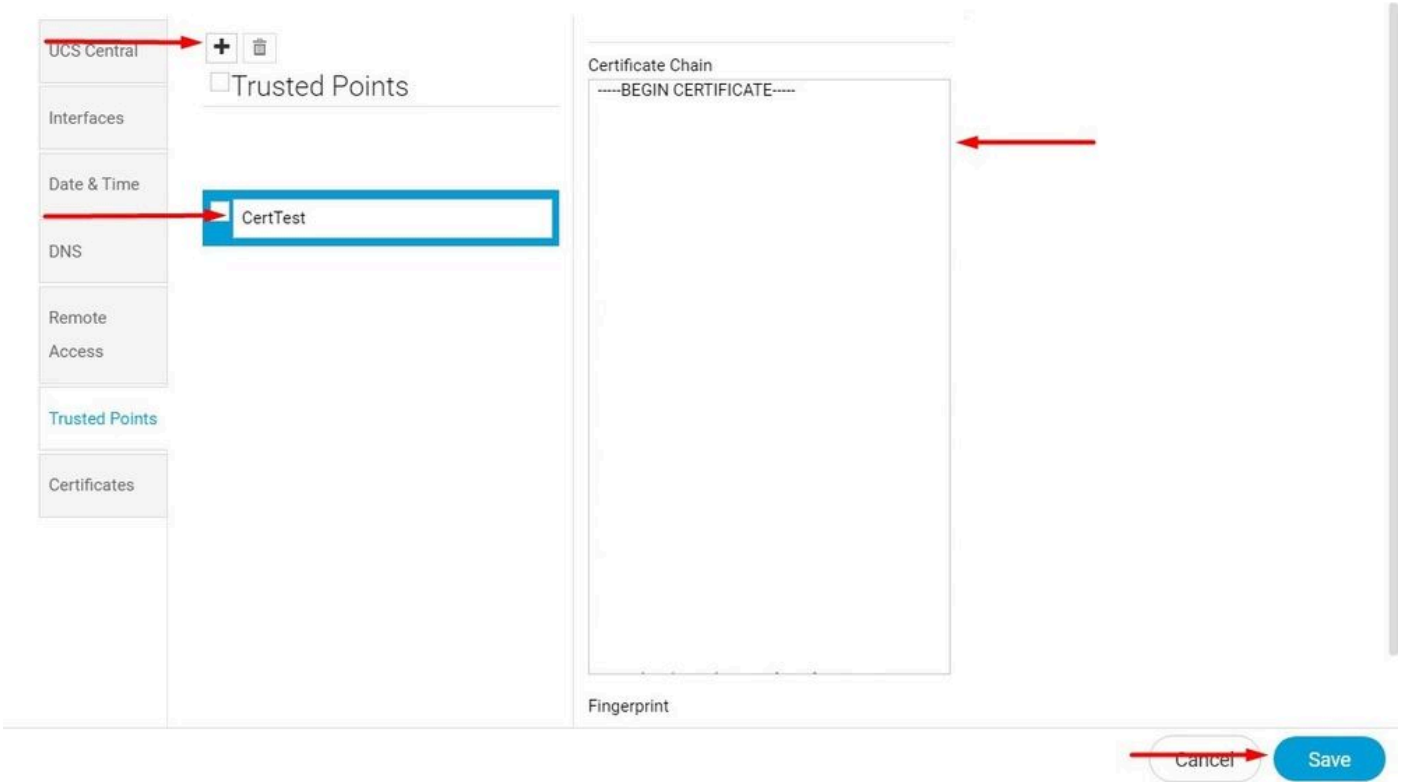


Perfil

do sistema central do UCSProdutos confiáveis do sistema central do UCS

2. Clique no ícone + (sinal de adição) para adicionar um novo Ponto Confiável. Escreva um nome e cole no conteúdo do certificado PEM. Clique em Salvar para aplicar as alterações.

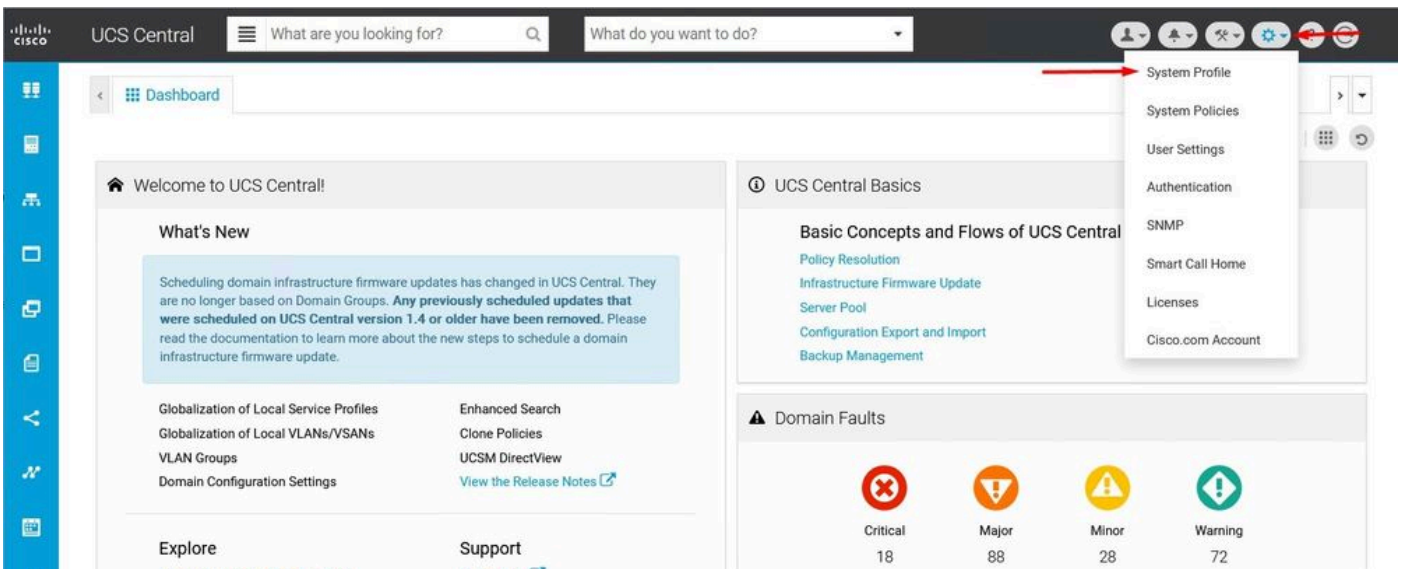
UCS Central System Profile Manage

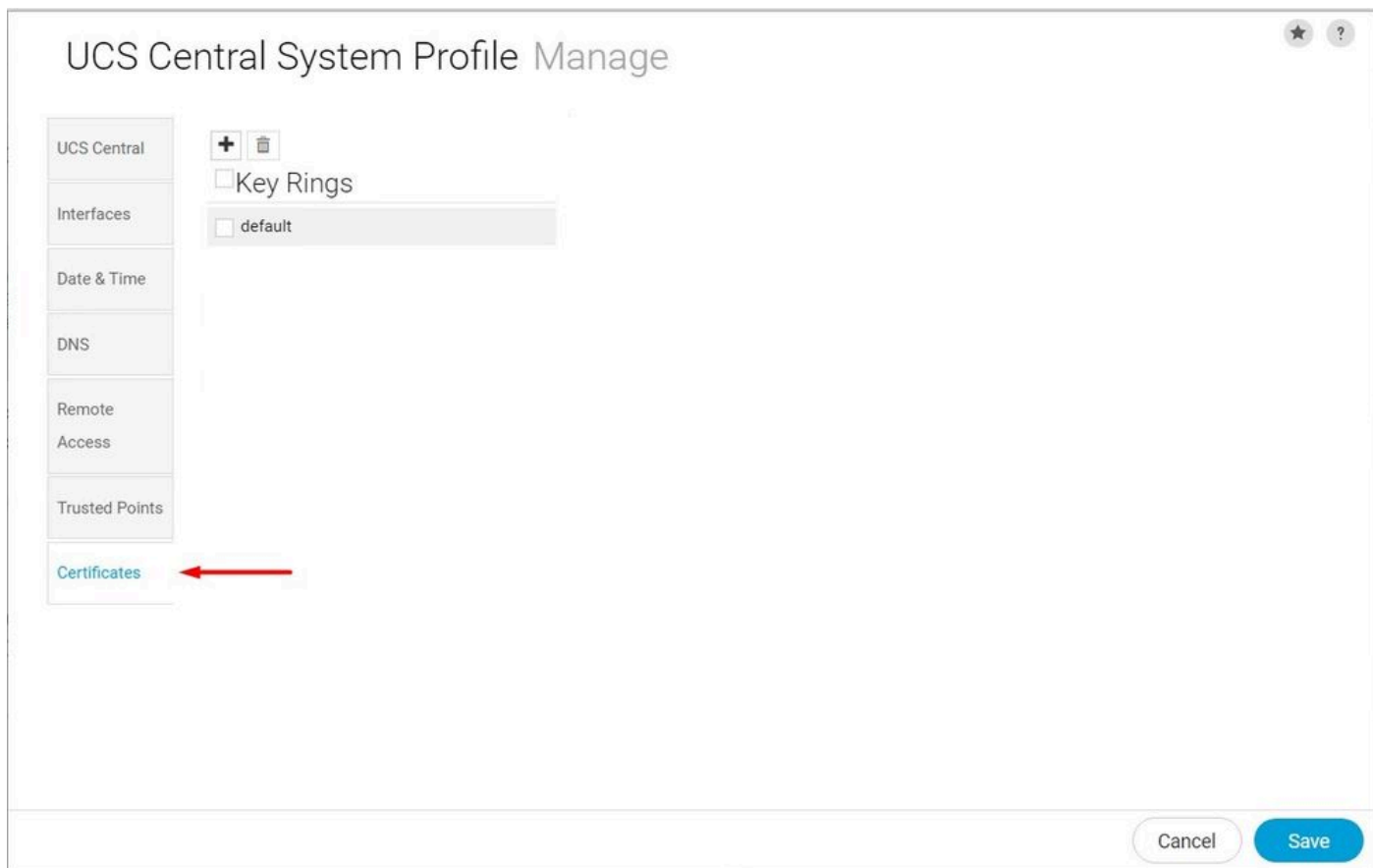


Copiar a cadeia de certificados

Criação de Key Ring e CSR

1. Clique no ícone Configuração do Sistema > Perfil do Sistema > Certificados.





Perfil

do sistema central do UCSConfirmação do sistema central do UCS

2. Clique no ícone do sinal de mais para adicionar um novo Toque de Tecla. Escreva um nome, deixe o módulo com o valor padrão (ou modifique se necessário) e selecione o ponto confiável criado antes. Depois de definir esses parâmetros, vá para Solicitação de certificado.

UCS Central System Profile Manage



UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+ Key Rings

default

KeyRingTest

Basic Certificate Request

Modulus: mod2048

Trusted Point: CertTest

Certificate Status: Valid

Certificate Chain

Cancel Save

Criar um novo Toque de Tecla

3. Informe os valores necessários para solicitar um certificado e clique em Salvar.

UCS Central System Profile Manage



UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+ Key Rings

default

KeyRingTest

Basic Certificate Request

DNS

Locality

State

Country

Organization Name

Organization Unit Name

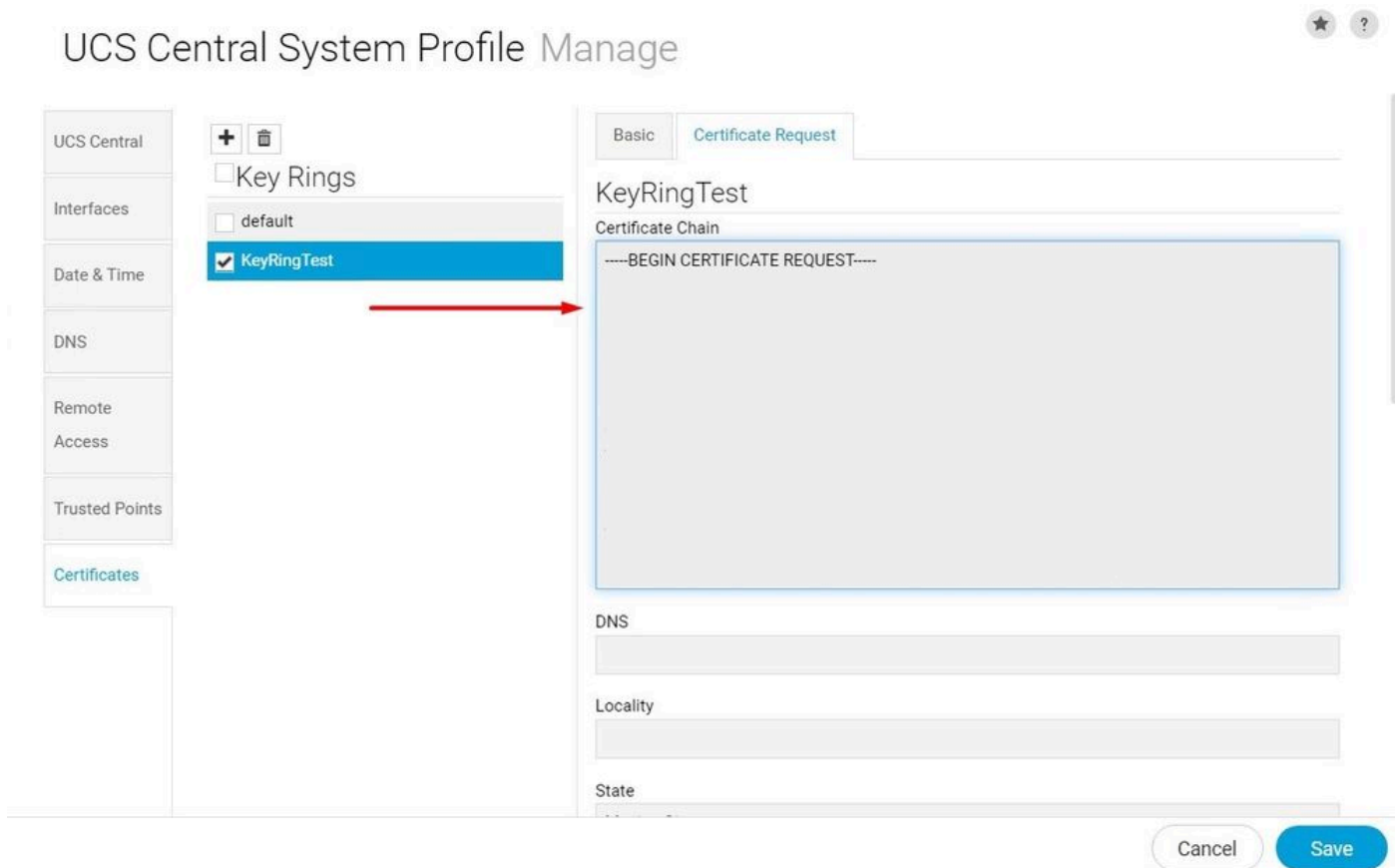
Email

Subject

Cancel Save

Insira os detalhes para gerar um certificado

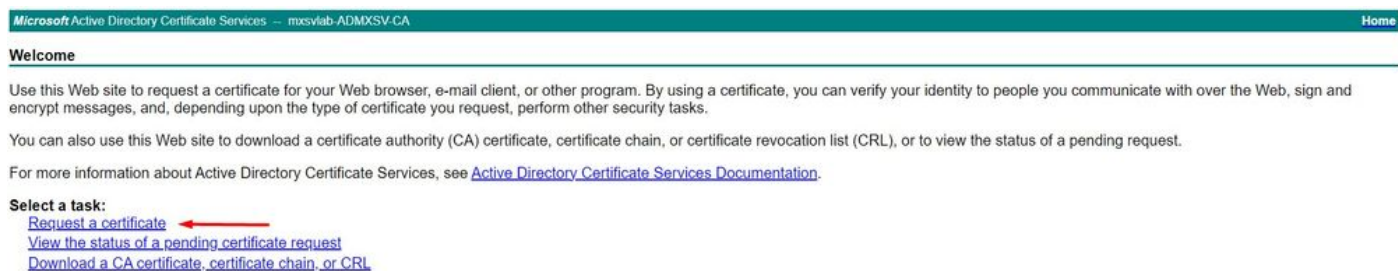
4. Volte para o Toque de chave criado e copie o certificado gerado.



The screenshot shows the 'UCS Central System Profile Manage' interface. On the left, a sidebar lists various system settings: UCS Central, Interfaces, Date & Time, DNS, Remote Access, Trusted Points, and Certificates. Under 'Key Rings', 'KeyRingTest' is selected. A red arrow points from this selection to the main content area. The main area has two tabs: 'Basic' and 'Certificate Request'. The 'Certificate Request' tab is active, showing a 'Certificate Chain' section with a text area containing '-----BEGIN CERTIFICATE REQUEST-----'. Below this are input fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Copiar o certificado gerado


5. Vá para a CA e solicite um certificado.



The screenshot shows the Microsoft Active Directory Certificate Services website. The header includes 'Microsoft Active Directory Certificate Services - mxslab-ADMXSV-CA' and a 'Home' link. The main content area has a 'Welcome' section with instructions on how to use the site to request a certificate, download a CA certificate, or view the status of a pending request. A 'Select a task:' section lists three links: 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'. A red arrow points to the 'Request a certificate' link.

Solicitar um certificado da autoridade de certificação

6. Cole o certificado gerado no UCS Central e, na CA, selecione o modelo Servidor Web e Cliente. Clique em Enviar para gerar o certificado.

 **Observação:** ao gerar uma solicitação de certificado no Cisco UCS Central, certifique-se de que o certificado resultante inclua o cliente SSL e os usos de chave de autenticação de servidor. Se estiver usando uma autoridade de certificação empresarial do Microsoft Windows, utilize o modelo Computador ou outro modelo apropriado que inclua ambos os usos principais, caso o modelo Computador não esteja disponível.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

-----END CERTIFICATE REQUEST-----

Certificate Template:

Web Server and Client

Additional Attributes:

Attributes:

Submit >

Gerar um certificado para usar no anel de chave criado

7. Converta o novo certificado em PEM usando o comando openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

8. Copie o conteúdo do certificado PEM e vá para o Toque de chave criado para colar o conteúdo. Selecione o Ponto confiável criado e salve a configuração.

UCS Central System Profile Manage

UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+ -

Key Rings

default

KeyRingTest

Basic Certificate Request

KeyRingTest

Modulus

mod2048

Trusted Point

CertTest

Certificate Status

Empty Cert

Certificate Chain

-----BEGIN CERTIFICATE-----

Cancel
Save

Colar o certificado solicitado no toque de chave

Aplicar o toque de tecla

1. Navegue até Perfil do sistema > Acesso remoto > Toque de chave, selecione o Toque de chave criado e clique em Salvar. O UCS Central fecha a sessão atual.

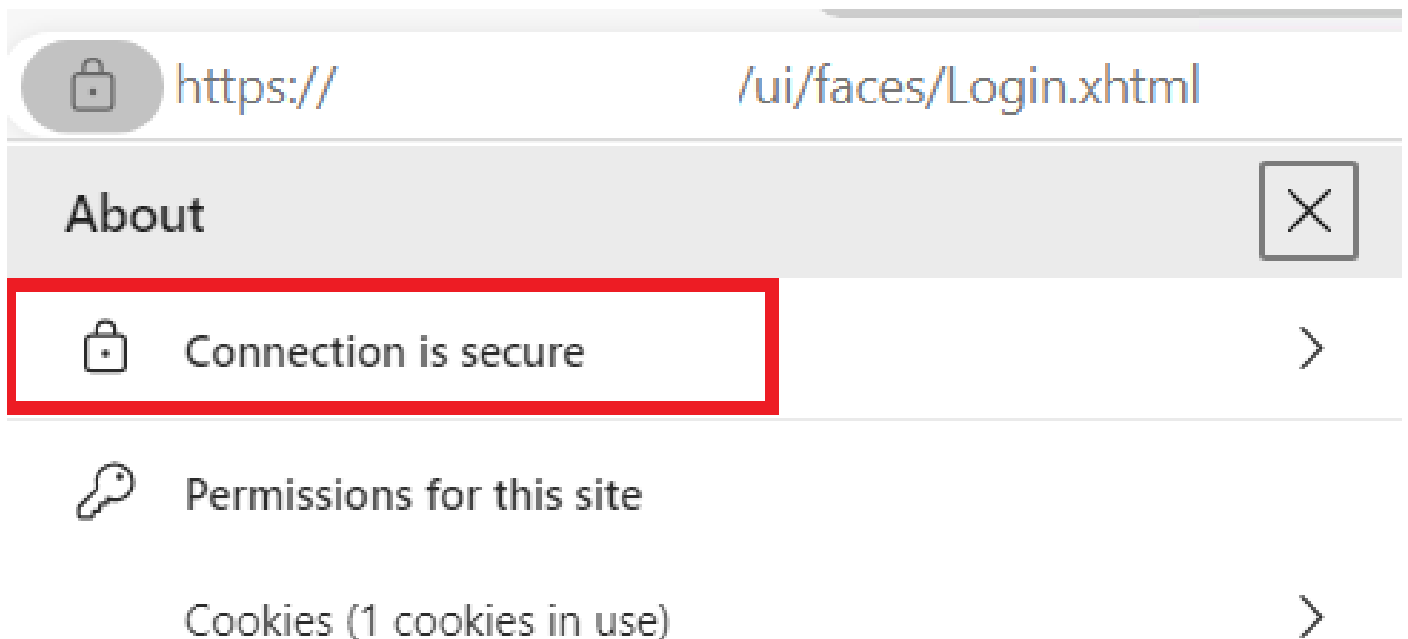
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

Selecionar o toque de chave criado

Validação

1. Aguarde até que o UCS Central esteja acessível e clique no cadeado ao lado de https://. O site é seguro.



O UCS Central é seguro

Troubleshooting

Verifique se o certificado gerado inclui o cliente SSL e os usos da chave de autenticação de servidor.

Quando o certificado solicitado para a CA não inclui a chave de Autenticação de Cliente e Servidor SSL usa um erro dizendo "Certificado inválido. Este certificado não pode ser usado para autenticação do servidor TLS. Verifique as extensões de uso da chave" aparece.

Invalid certificate: This certificate cannot be used for TLS server authentication, check key usage extensions.

Erro sobre chaves de autorização do servidor TLS

Para verificar se o certificado no formato PEM criado a partir do modelo selecionado na CA tem os usos de chave de autenticação de servidor corretos, você pode usar o comando `openssl x509 -in <my_cert>.pem -text -noout`. Você deve ver Web Server Authentication e Web Client Authentication na seção Extended Key Usage .

```
21:75
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Subject Alternative Name: critical
    DNS:
  X509v3 Subject Key Identifier:

  X509v3 Authority Key Identifier:

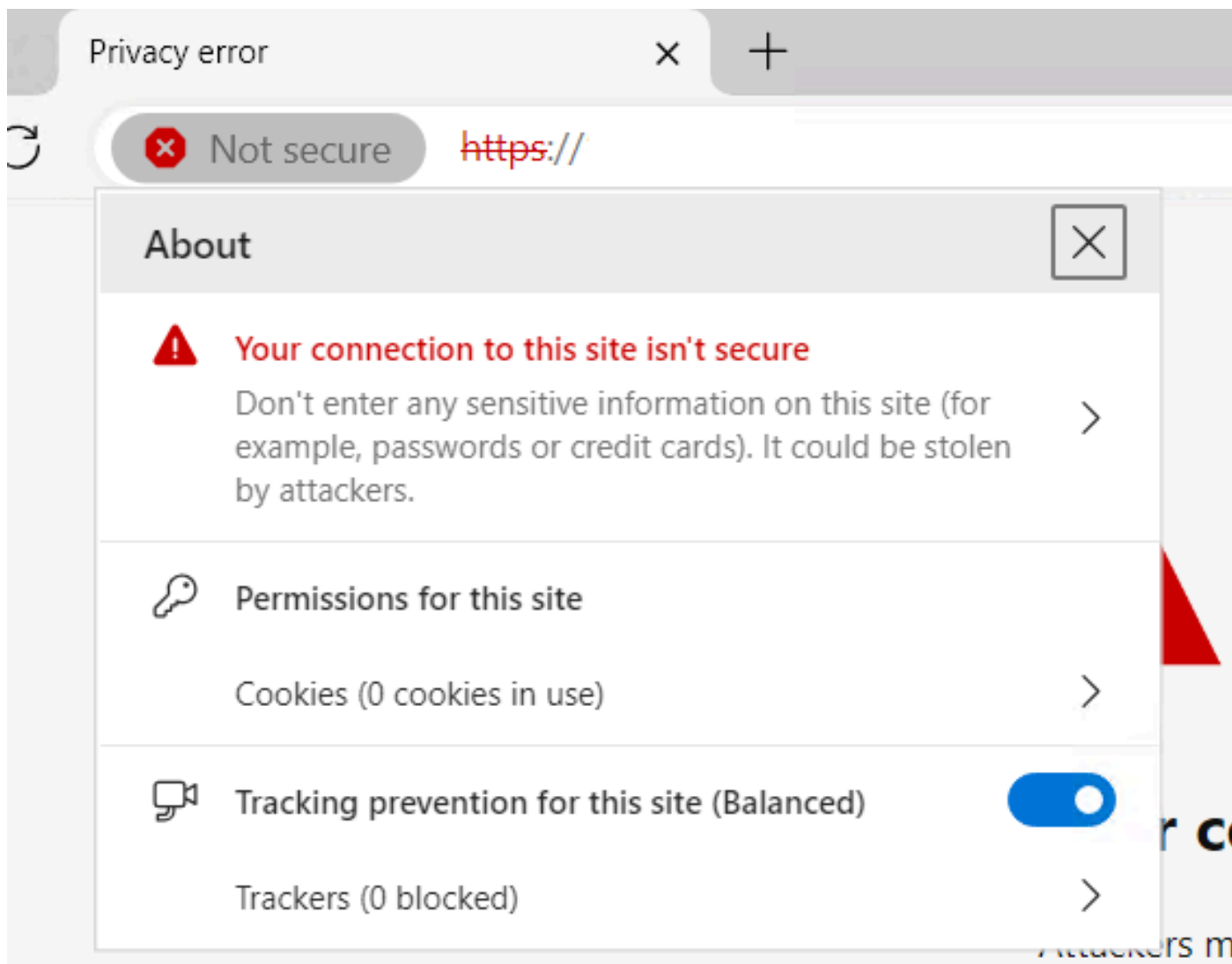
  X509v3 CRL Distribution Points:
    Full Name:

Authority Information Access:
```

Foi solicitada a chave de autorização do servidor Web e do cliente Web no certificado

O UCS Central ainda está sinalizado como um site não seguro.

Às vezes, após a configuração do Certificado de Terceiros, a conexão ainda é sinalizada pelo navegador.



O UCS Central ainda é um site não seguro

Para verificar se o certificado está sendo aplicado corretamente, verifique se o dispositivo confia na Autoridade de Certificação.

Informações Relacionadas

- [Guia de administração central do Cisco UCS, versão 2.0](#)
- [Suporte técnico e downloads da Cisco](#)

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.