

Configuración de certificados de terceros para UCS Central

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Creación del punto de confianza](#)

[Creación de Key Ring y CSR](#)

[Aplique el llavero](#)

[Validación](#)

[Resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento describe las prácticas recomendadas para configurar un certificado de terceros en Cisco Unified Computing System Central Software (UCS Central).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Cisco UCS Central
- Autoridad de certificación (CA)
- OpenSSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCS Central 2.0(1q)
- Servicios de certificados de Microsoft Active Directory
- Windows 11 Pro N
- OpenSSL 3.1.0

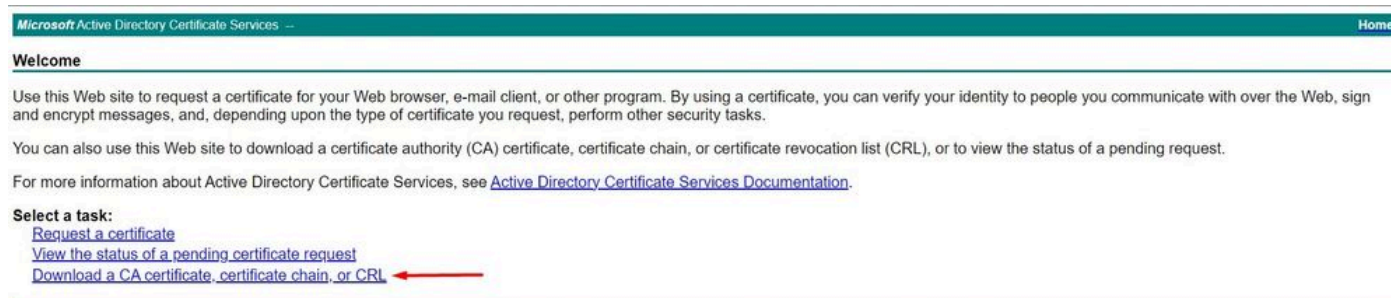
La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Descargue la cadena de certificados de la autoridad certificadora.

1. Descargue la cadena de certificados de la autoridad certificadora (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.

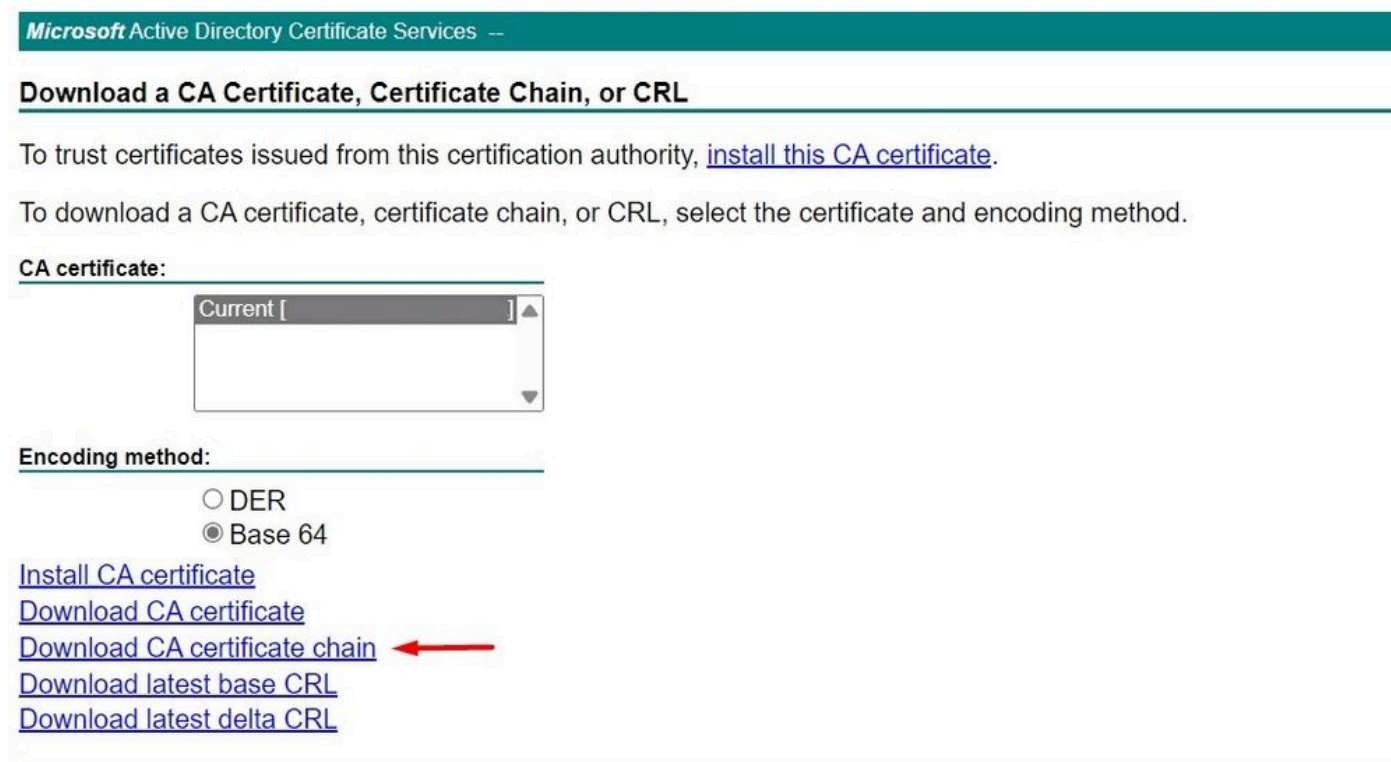
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

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

Descargar una cadena de certificados de CA

2. Establezca la codificación en Base 64 y descargue la cadena de certificados de la 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](#)

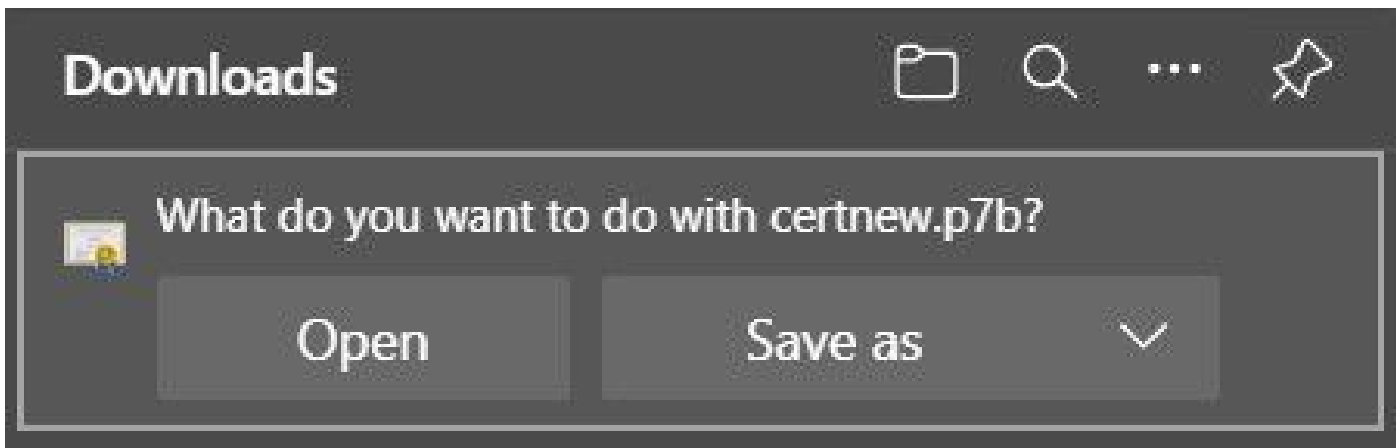
[Download CA certificate chain](#) ←

[Download latest base CRL](#)

[Download latest delta CRL](#)

Establezca la codificación en Base 64 y descargue la cadena de certificados de la CA

3. Tenga en cuenta que la cadena de certificados de la CA está en formato PB7.




El certificado está en formato PB7

4. El certificado debe convertirse al formato PEM con la herramienta OpenSSL. Para comprobar si Open SSL está instalado en Windows, utilice el 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)
```

Compruebe si OpenSSL está instalado

 Nota: La instalación de OpenSSL no está dentro del alcance de este artículo.

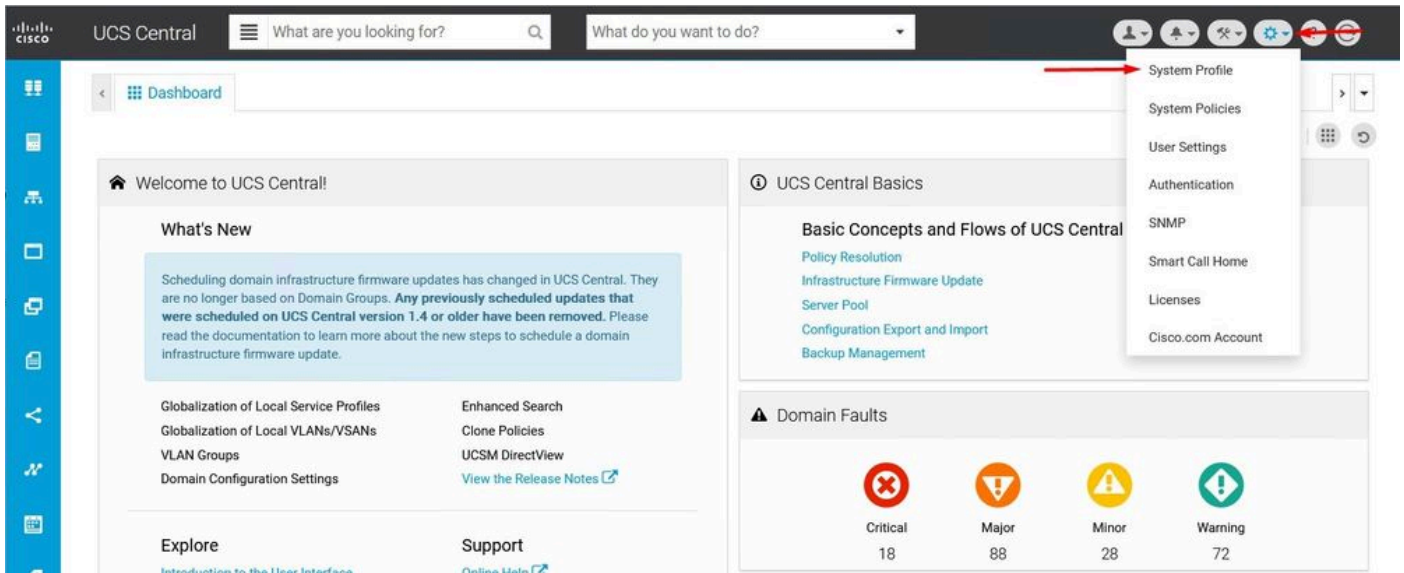
5. Si OpenSSL está instalado, ejecute el comando `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` para realizar la conversión. Asegúrese de utilizar la ruta de acceso donde se guardó el certificado.

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

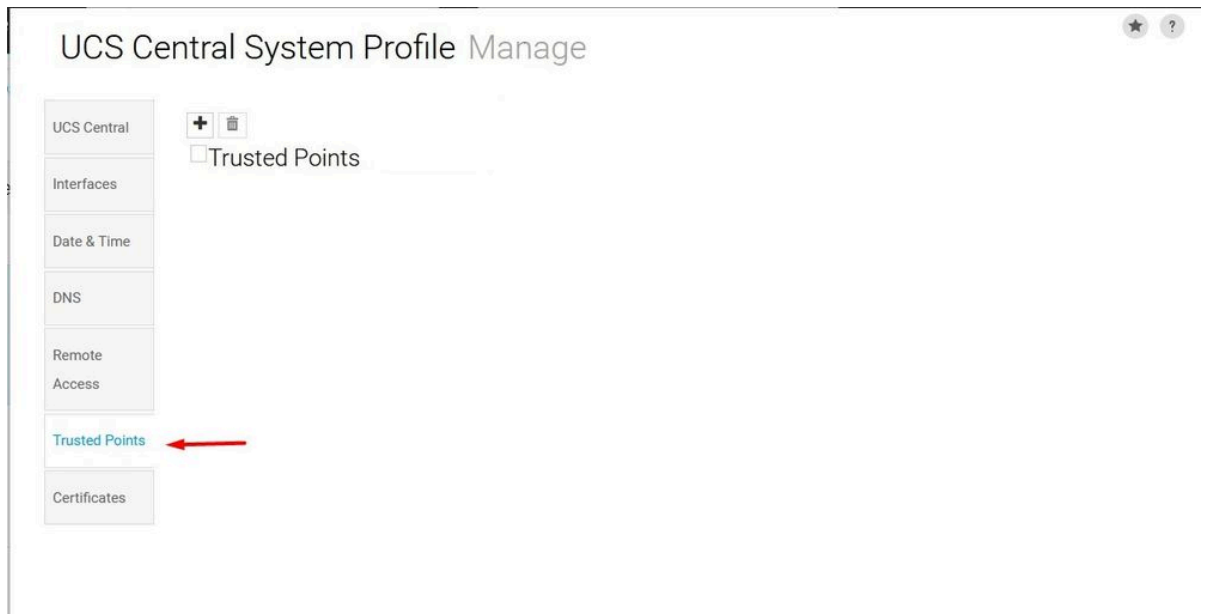
Convertir el certificado P7B al formato PEM

Creación del punto de confianza

1. Haga clic en Icono de Configuración del sistema > Perfil del sistema > Puntos de confianza.



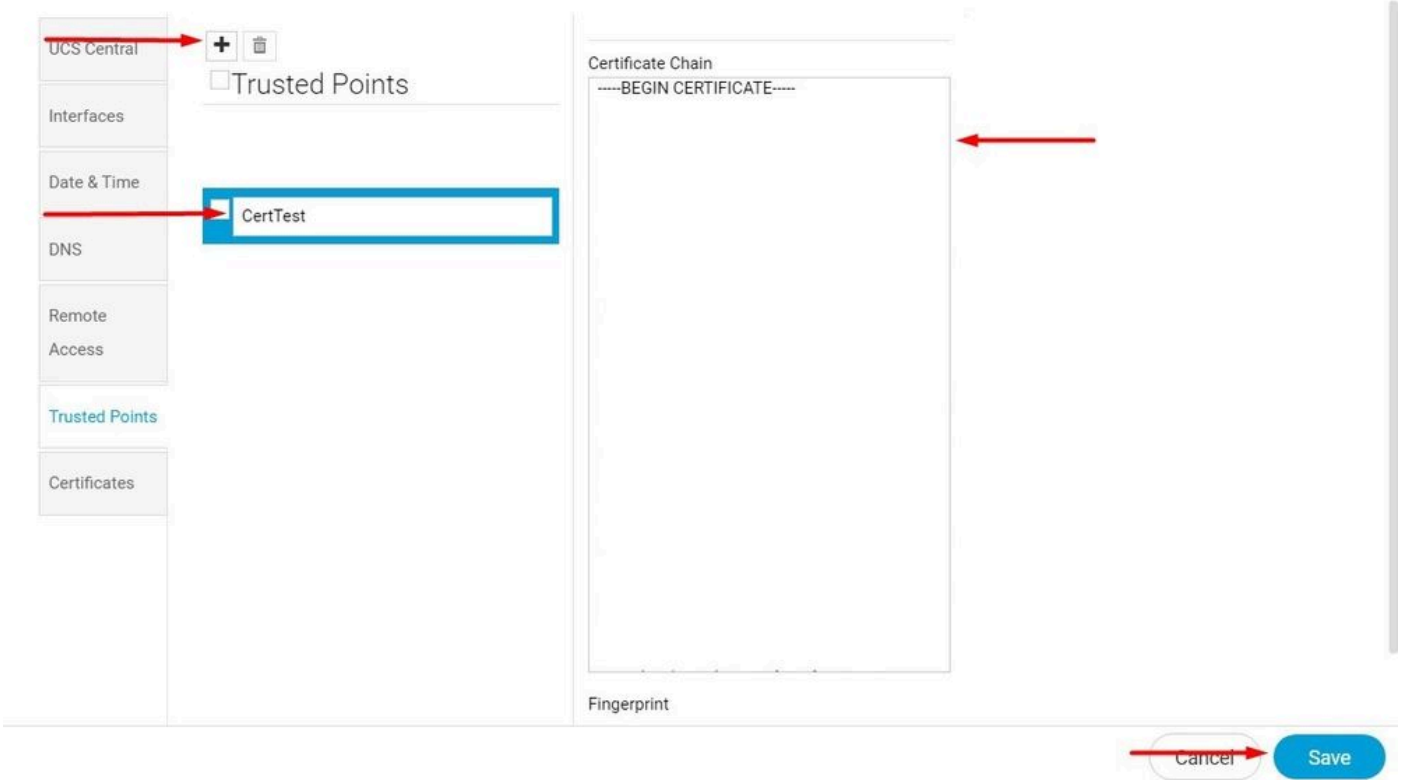
Perfil



de sistema central
de UCSPuntos de confianza de UCS Central

2. Haga clic en el icono + (más) para agregar un nuevo punto de confianza. Escriba un nombre y pegue el contenido del certificado PEM. Haga clic en Guardar para aplicar los cambios.

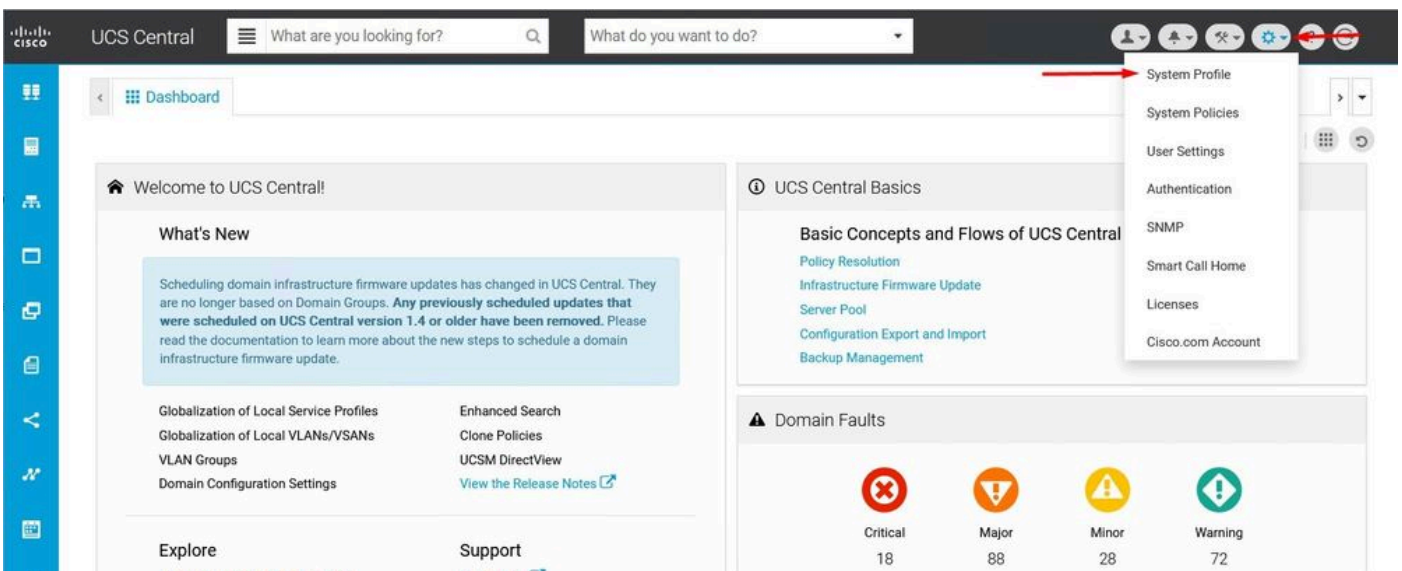
UCS Central System Profile Manage



Copiar la cadena de certificados

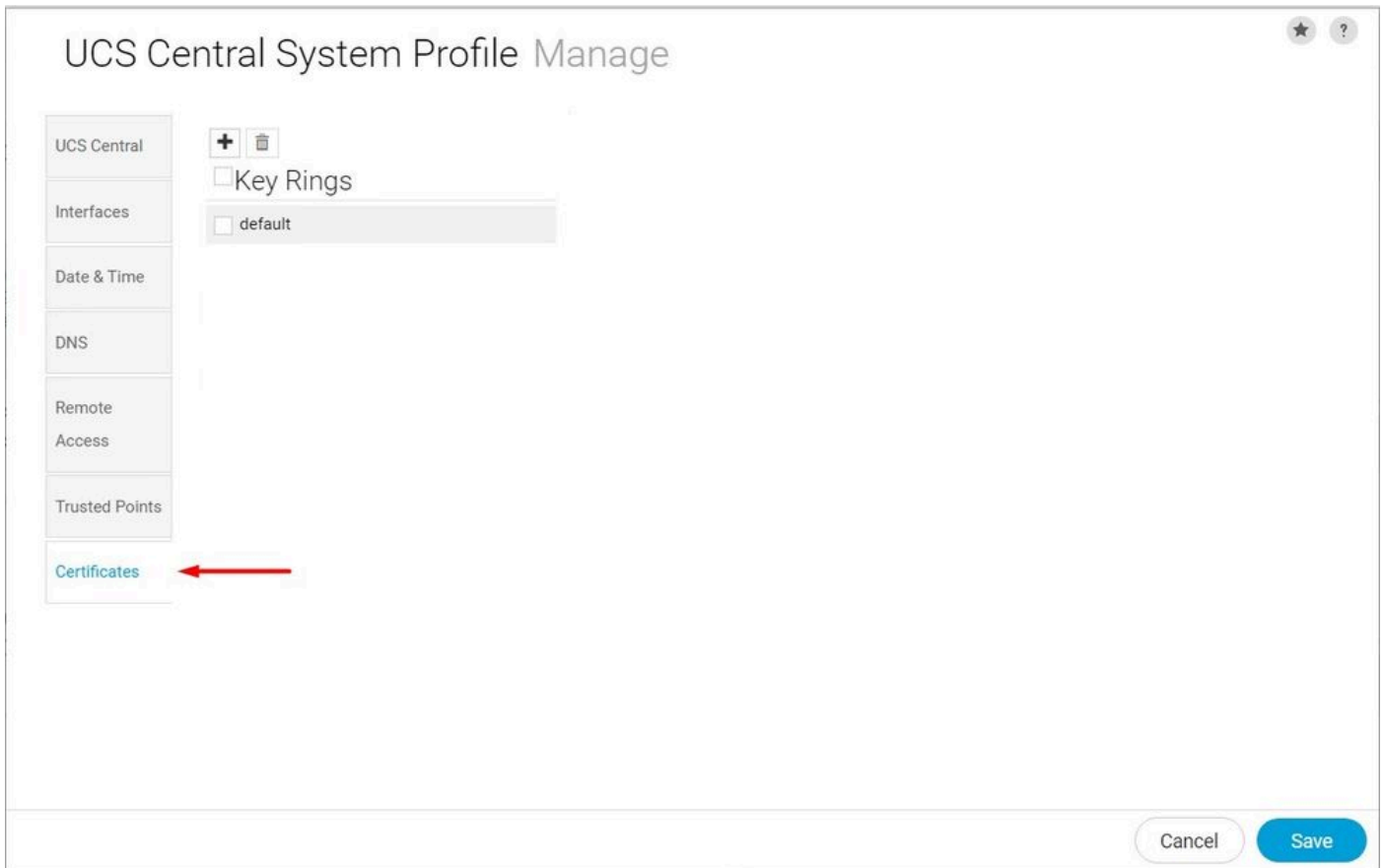
Creación de Key Ring y CSR

1. Haga clic en Icono de Configuración del sistema > Perfil del sistema > Certificados.



Perfil

de sistema central de



UCSContetos de UCS Central

2. Haga clic en el icono más para agregar un nuevo llavero. Escriba un nombre, deje el módulo con el valor predeterminado (o modifíquelo si es necesario) y seleccione el punto de confianza creado anteriormente. Después de establecer esos parámetros, pase a Solicitud 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

Crear un nuevo llavero

3. Introduzca los valores necesarios para solicitar un certificado y haga clic en Guardar.

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

Introduzca los detalles para generar un certificado

4. Vuelva al anillo de claves creado y copie el certificado generado.

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 fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.


Copiar el certificado generado

5. Vaya a la CA y solicite un certificado.

The screenshot shows the Microsoft Active Directory Certificate Services website. The page title is 'Microsoft Active Directory Certificate Services - mxsvlab-ADMXSV-CA'. The 'Welcome' section contains the following text: '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](#).' Under the 'Select a task:' section, there are three links: 'Request a certificate' (with a red arrow pointing to it), 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'.

Solicitar un certificado de CA

6. Pegue el certificado generado en UCS Central y, en la CA, seleccione la plantilla Servidor web y Cliente. Haga clic en Enviar para generar el certificado.

 **Nota:** al generar una solicitud de certificado en Cisco UCS Central, asegúrese de que el certificado resultante incluye usos de clave de autenticación de servidor y cliente SSL. Si utiliza una CA empresarial de Microsoft Windows, utilice la plantilla Equipo u otra plantilla adecuada que incluya ambos usos de clave, si la plantilla Equipo no está disponible.

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 >

Generar un certificado para utilizarlo en el anillo de claves creado

7. Convierta el nuevo certificado en PEM mediante el comando `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem`.

8. Copie el contenido del certificado PEM y vaya al anillo de claves creado para pegar el contenido. Seleccione el punto de confianza creado y guarde la configuración.

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

Pegue el certificado solicitado en el llavero

Aplique el llavero

1. Navegue hasta Perfil del sistema > Acceso remoto > Anillo de llaves, seleccione el Anillo de llaves creado y haga clic en Guardar. UCS Central cierra la sesión actual.

UCS Central System Profile Manage



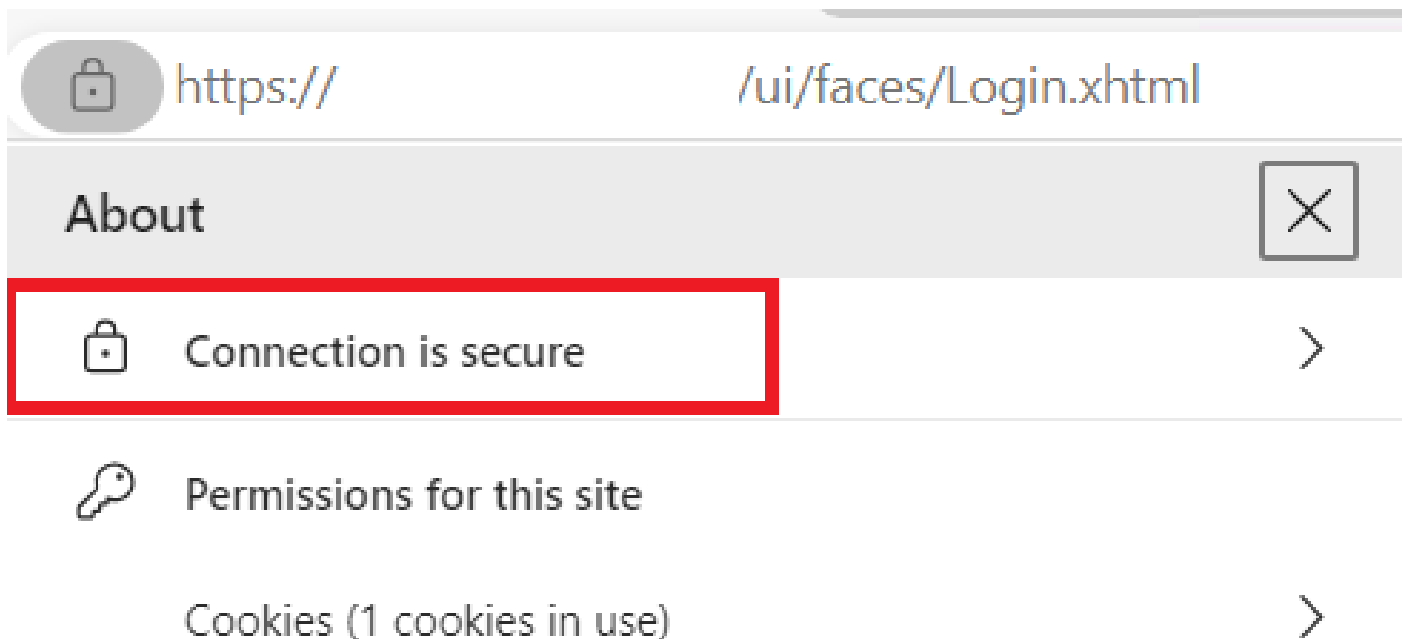
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

Cancel Save

Seleccione el llavero creado

Validación

1. Espere a que se pueda acceder a UCS Central y haga clic en el bloqueo situado junto a https://. El sitio es seguro.



UCS Central es seguro

Resolución de problemas

Compruebe si el certificado generado incluye usos de clave de autenticación de servidor y cliente SSL.

Cuando el certificado solicitado a la CA no incluye el cliente SSL y la clave de autenticación del servidor utiliza un error que dice "Certificado no válido. Este certificado no se puede utilizar para la autenticación del servidor TLS; compruebe que aparece "extensiones de uso de claves".

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

Error acerca de las claves de autorización del servidor TLS

Para verificar si el certificado en formato PEM creado a partir de la plantilla seleccionada en la CA tiene los usos correctos de clave de autenticación de servidor, puede utilizar el comando `openssl x509 -in <my_cert>.pem -text -noout`. Debe ver Autenticación de servidor web y Autenticación de cliente web en la sección Uso de clave ampliada .

```
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:

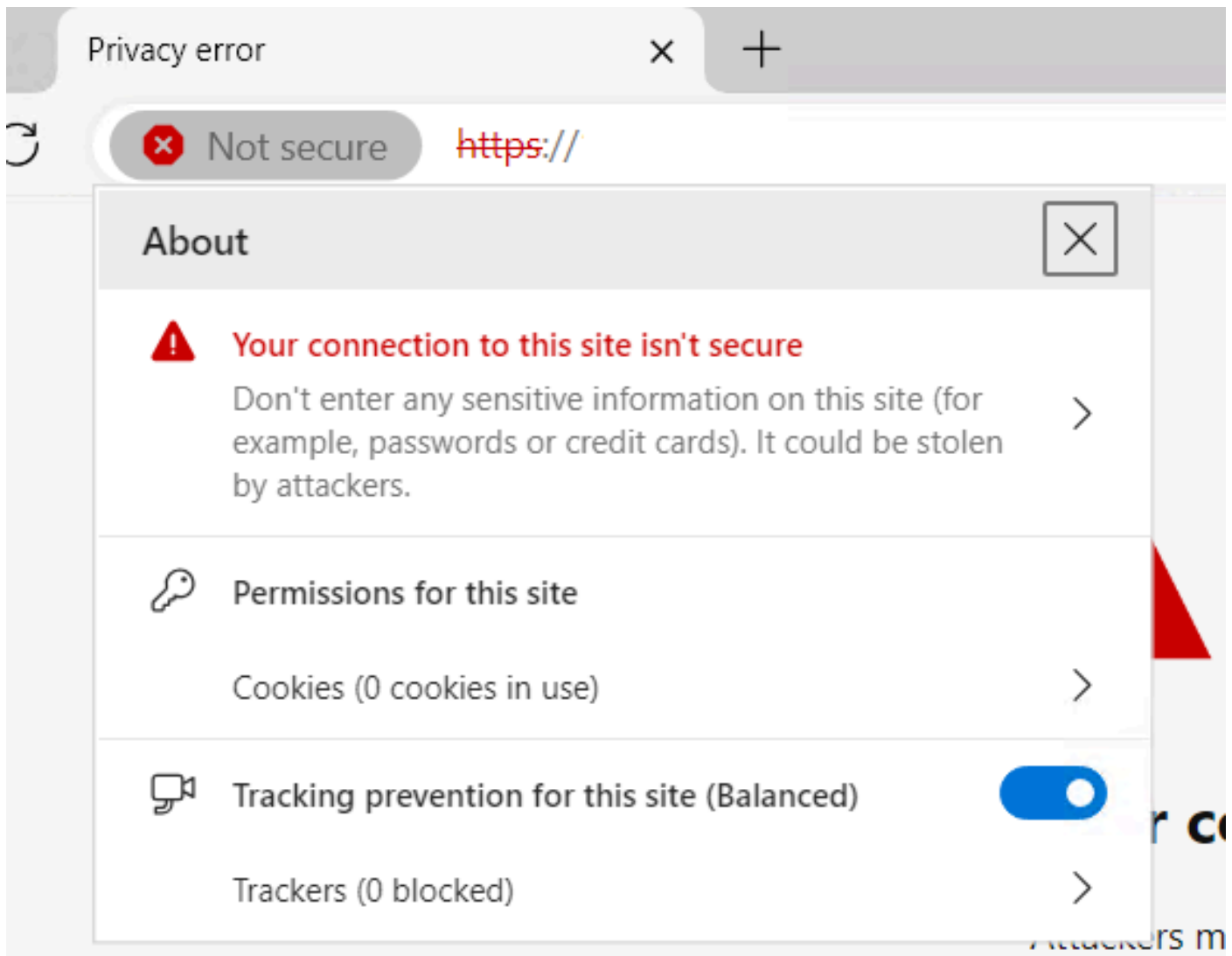
  X509v3 CRL Distribution Points:
  Full Name:

  Authority Information Access:
```

Servidor web y clave de autorización de cliente web en el certificado solicitado

UCS Central sigue marcado como sitio inseguro.

A veces, después de configurar el certificado de terceros, el explorador sigue marcando la conexión.



UCS Central sigue siendo un sitio no seguro

Para comprobar si el certificado se está aplicando correctamente, asegúrese de que el dispositivo confía en la autoridad de certificados.

Información Relacionada

- [Guía de administración central de Cisco UCS, versión 2.0](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).