

Configure Third Party Certificate for UCS Central

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Create the Trusted Point](#)

[Creating Key Ring and CSR](#)

[Apply the Key Ring](#)

[Validation](#)

[Troubleshooting](#)

[Related Information](#)

Introduction

This document describes the best practice to configure a third-party certificate in Cisco Unified Computing System Central Software (UCS Central).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco UCS Central
- Certificate Authority (CA)
- OpenSSL

Components Used

The information in this document is based on these software and hardware versions:

- UCS Central 2.0(1q)
- Microsoft Active Directory Certificate Services
- Windows 11 Pro N
- OpenSSL 3.1.0

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Download the Certificate Chain from the Certificate Authority.

1. Download the certificate chain from the Certificate Authority (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](#) ←

Download a certificate chain from CA

2. Set the encoding to Base 64 and download the CA certificate chain.

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](#)

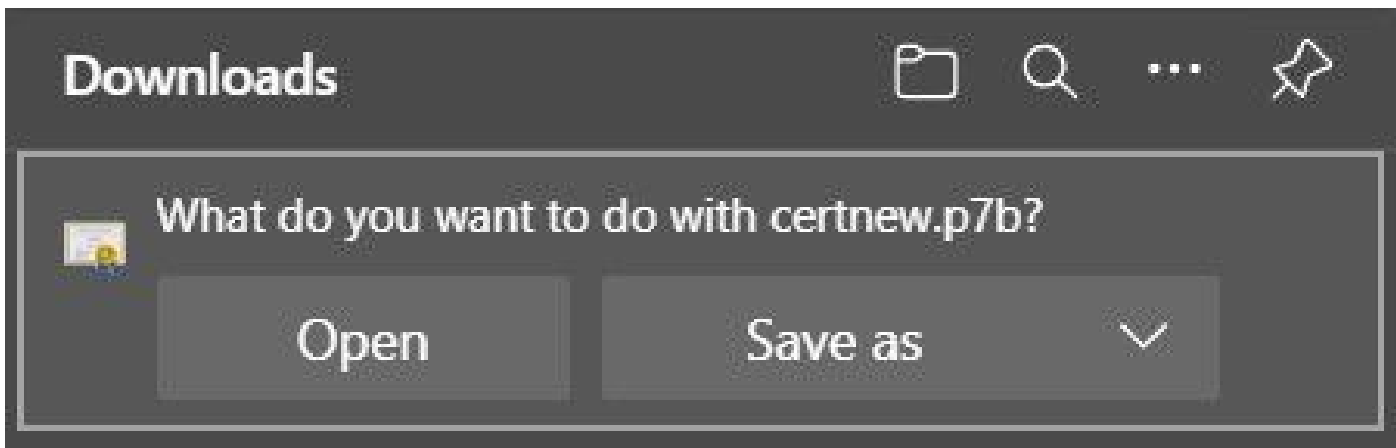
[Download CA certificate chain](#) ←

[Download latest base CRL](#)

[Download latest delta CRL](#)

Set the encoding to Base 64 and download the CA certificate chain

3. Note that the CA certificate chain is in PB7 format.




Certificate is in PB7 format

4. The certificate has to be converted to PEM format with OpenSSL tool. To check if Open SSL is installed in Windows use the command **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)
```

Check if OpenSSL is installed

 **Note:**OpenSSL installation is out of the scope of this article.

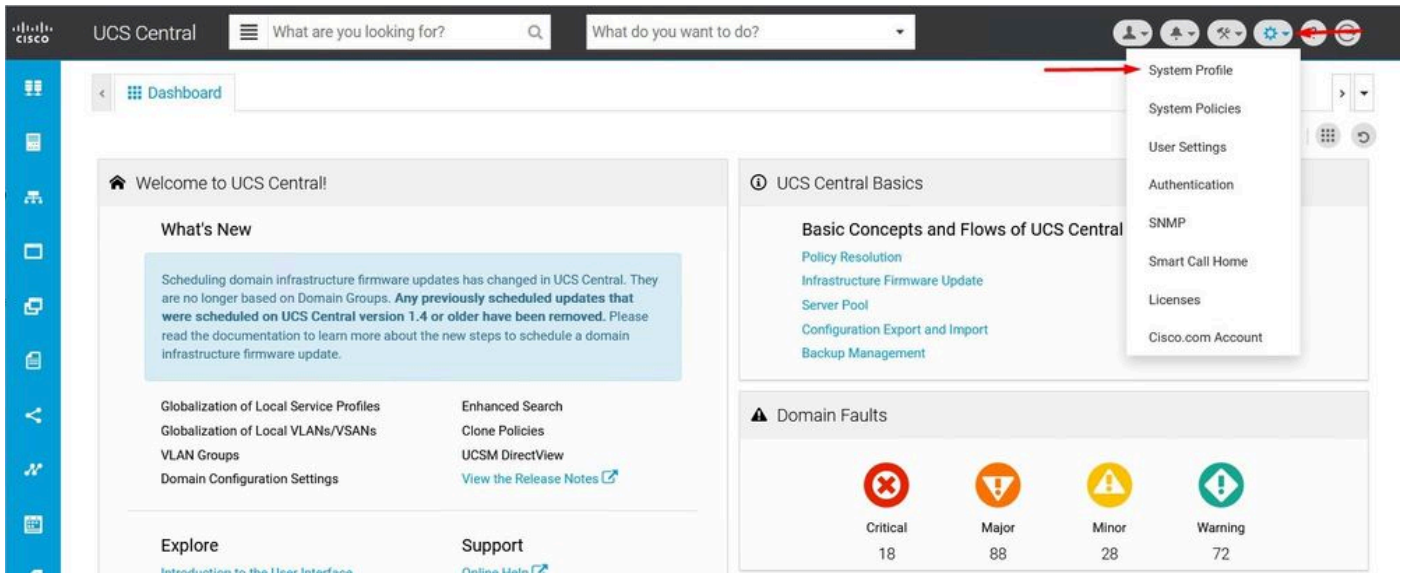
5.If OpenSSL is installed, run the command **openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem** to perform the conversion. Make sure to use the path were the certificate is saved.

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

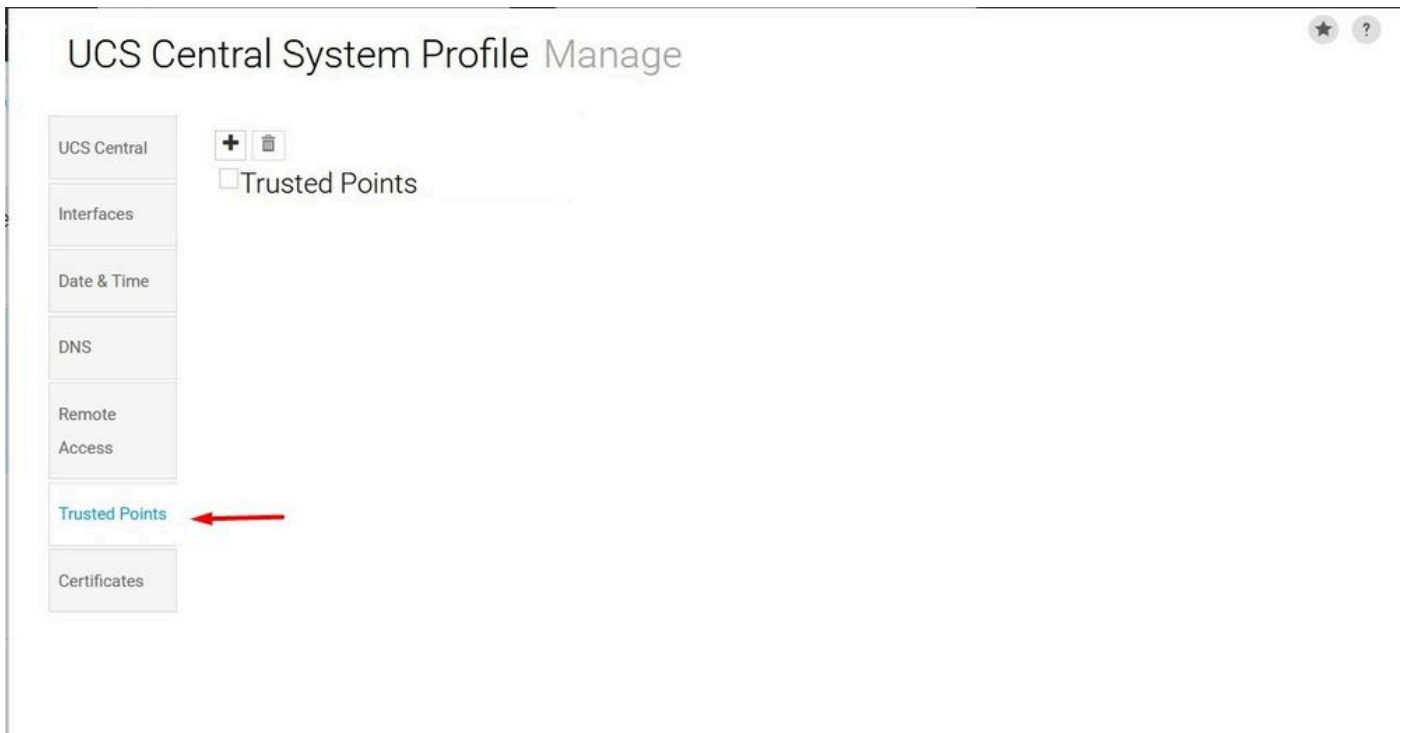
Convert the P7B certificate to PEM format

Create the Trusted Point

1. Click **System Configuration icon > System Profile > Trusted Points**.



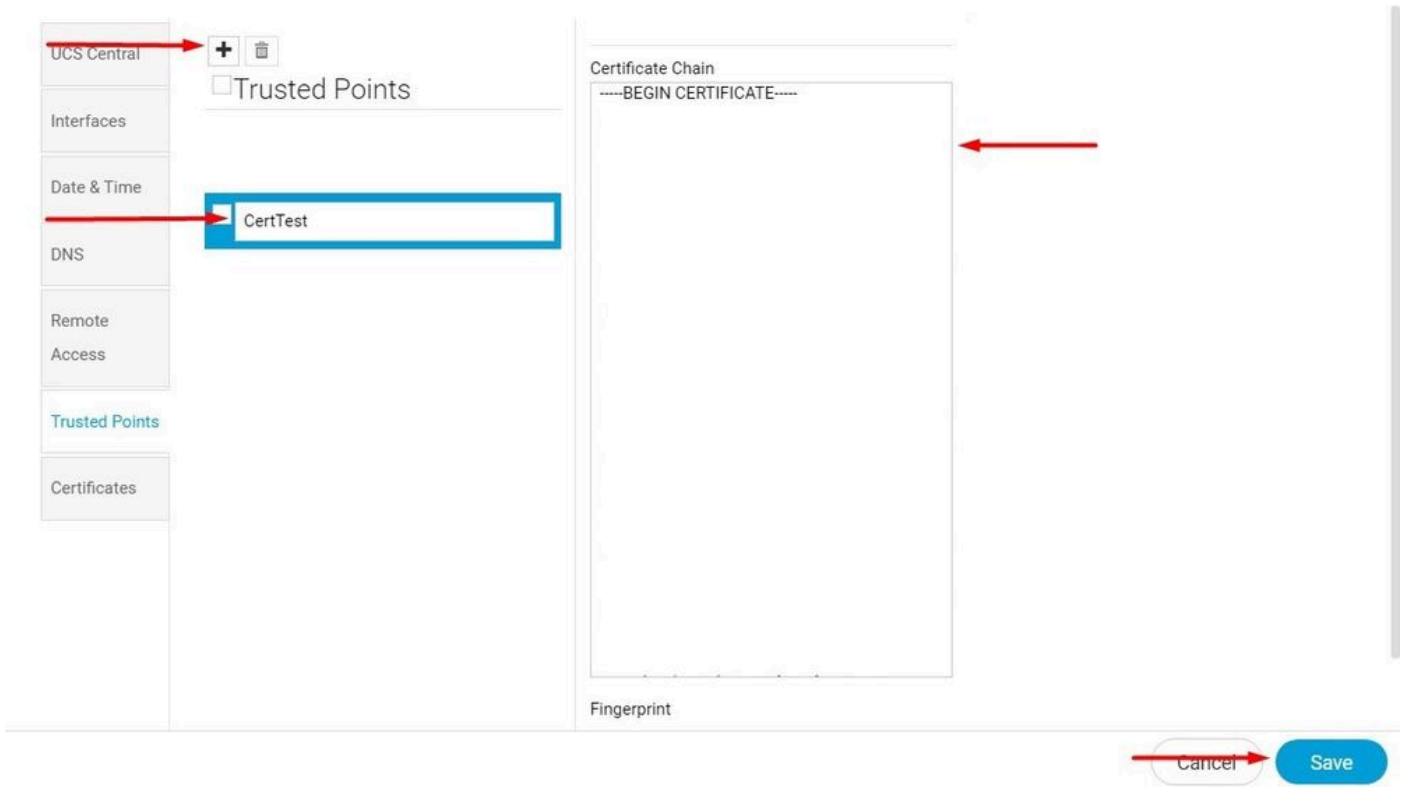
UCS Central System Profile



UCS Central Trusted Points

2. Click the + (plus) icon to add a new Trusted Point. Write a name and paste in the contents of the PEM certificate. Click **Save** to apply the changes.

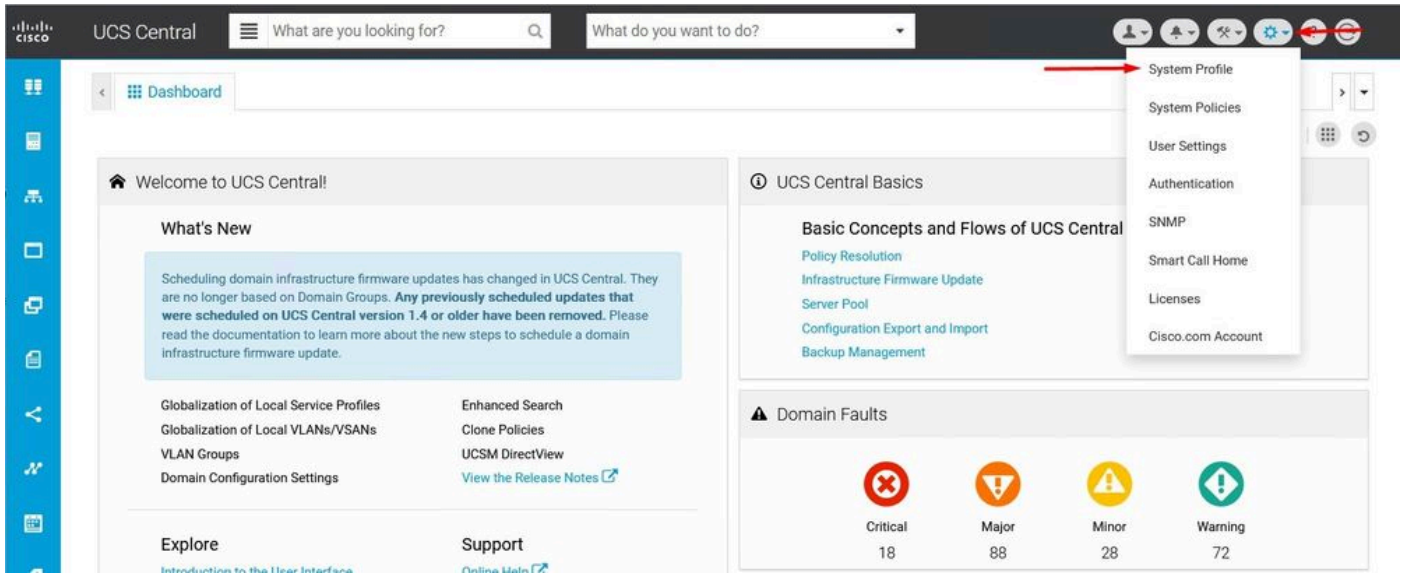
UCS Central System Profile Manage



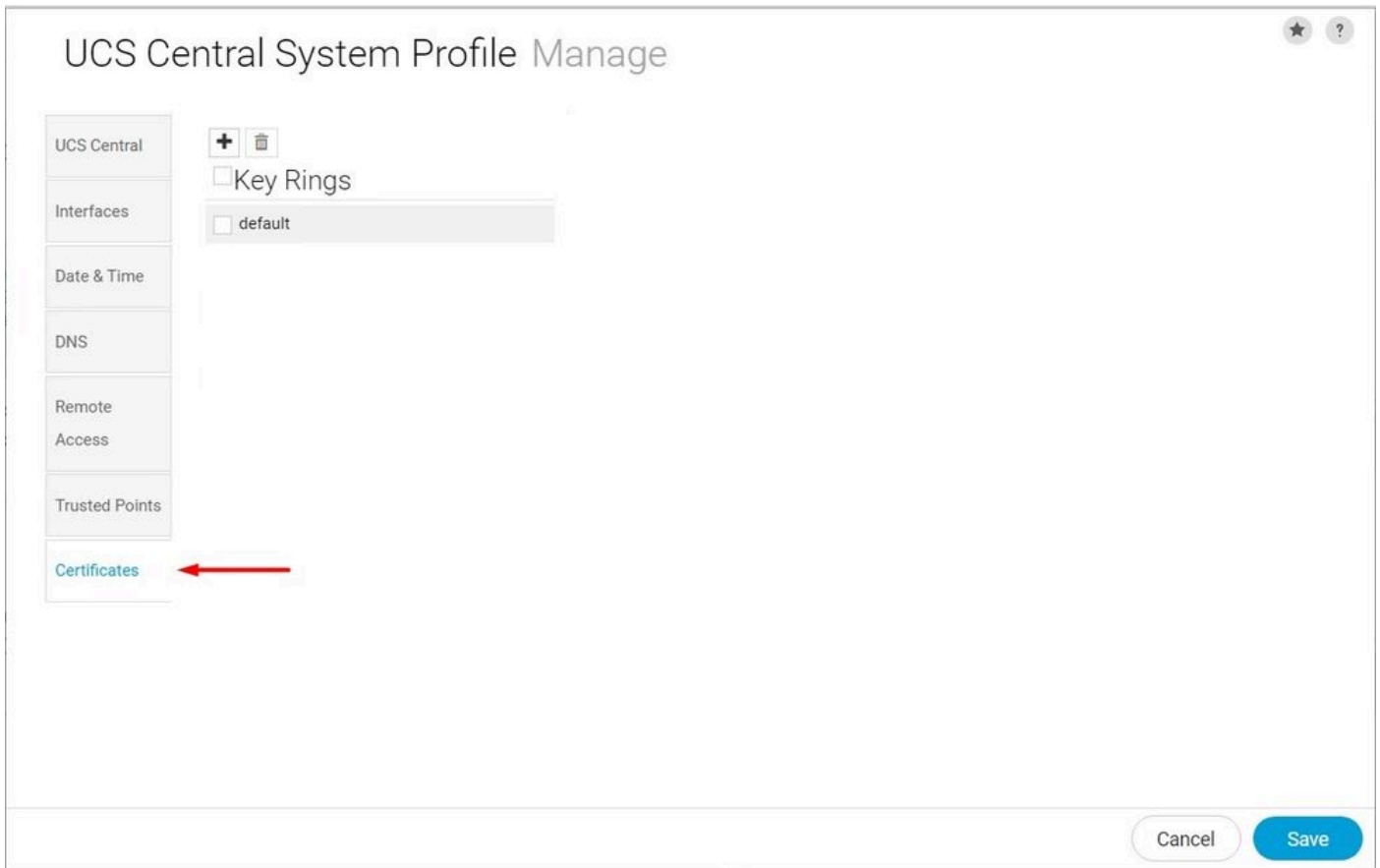
Copy the certificate chain

Creating Key Ring and CSR

1. Click **System Configuration icon** > **System Profile** > **Certificates**.



UCS Central System Profile



UCS Central Certificates

2. Click the **plus** icon to add a new Key Ring. Write a name, leave the modulus with the default value (or modify if needed) and select the Trusted Point created before. After setting those parameters move to **Certificate Request**.

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

Create a new Key Ring

3. Enter the necessary values to request a certificate and click **Save**.

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

Enter the details to generate a certificate

4. Go back to the Key ring created and copy the certificate generated.

The screenshot shows the 'UCS Central System Profile Manage' interface. On the left, a sidebar lists various system profiles: UCS Central, Interfaces, Date & Time, DNS, Remote Access, Trusted Points, and Certificates. Under 'Key Rings', 'KeyRingTest' is selected and highlighted in blue. 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 form for 'KeyRingTest'. The 'Certificate Chain' field is a large text area containing the text '-----BEGIN CERTIFICATE REQUEST-----'. Below this are fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.


Copy the certificate generated

5. Go to the CA and request a certificate.

The screenshot shows the Microsoft Active Directory Certificate Services website. The browser title bar reads 'Microsoft Active Directory Certificate Services - mxsvlab-ADMXSV-CA'. The page has a 'Welcome' header. Below it, there is a paragraph of 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.' Another paragraph follows: '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.' A third paragraph says: 'For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).' Under the heading 'Select a task:', 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'.

Request a certificate from CA

6. Paste the certificate generated in UCS Central and in the CA select the **Web Server and Client** template. Click **Submit** to generate the certificate.

 **Note:** When generating a certificate request in Cisco UCS Central, ensure the resulting certificate includes SSL Client and Server Authentication key usages. If using a Microsoft Windows Enterprise CA, utilize the Computer template, or another appropriate template that includes both key usages, if the Computer template is unavailable.

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 >

Generate a certificate to use in the Key ring created

7. Convert the new certificate to PEM using the command **openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem**.

8. Copy the contents of the PEM certificate and go to the Key ring created to paste the contents. Select the **Trusted Point** created and save the configuration.

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

Paste the certificate requested in the key ring

Apply the Key Ring

1. Navigate to **System Profile > Remote Access > Keyring**, select the Key ring created, and click **Save**. UCS Central closes the current session.

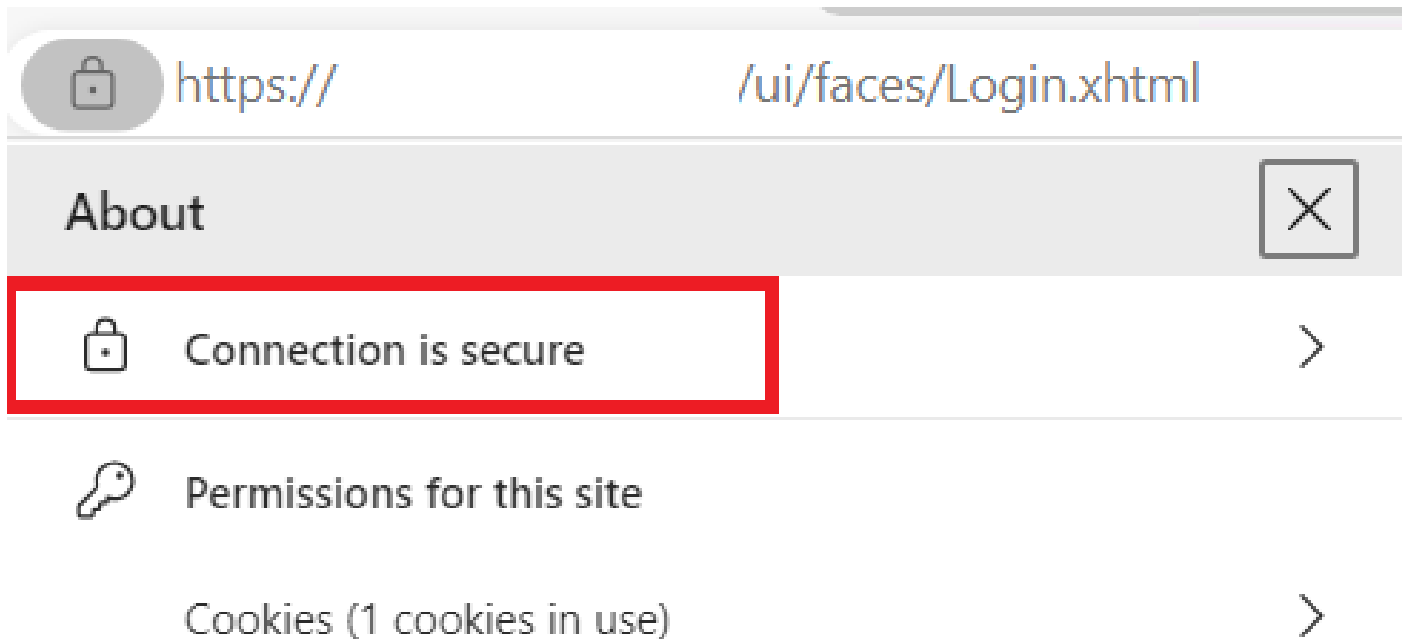
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

Select the key ring created

Validation

1. Wait until UCS Central is accessible and click in the lock next to **https://**. The site is secure.



UCS Central is secure

Troubleshooting

Check if certificate generated includes SSL Client and Server Authentication key usages.

When the certificate requested to CA does not include the SSL Client and Server Authentication key usages an error saying "Invalid certificate. This certificate cannot be used for TLS server authentication, check key usage extensions" appears.

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

Error about TLS Server Authorization Keys

To verify if the certificate in PEM format created from the template selected in the CA has the correct Server Authentication key usages you can use the command **openssl x509 -in <my_cert>.pem -text -noout**. You must see **Web Server Authentication** and **Web Client Authentication** under the **Extended Key Usage** section.

```
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:

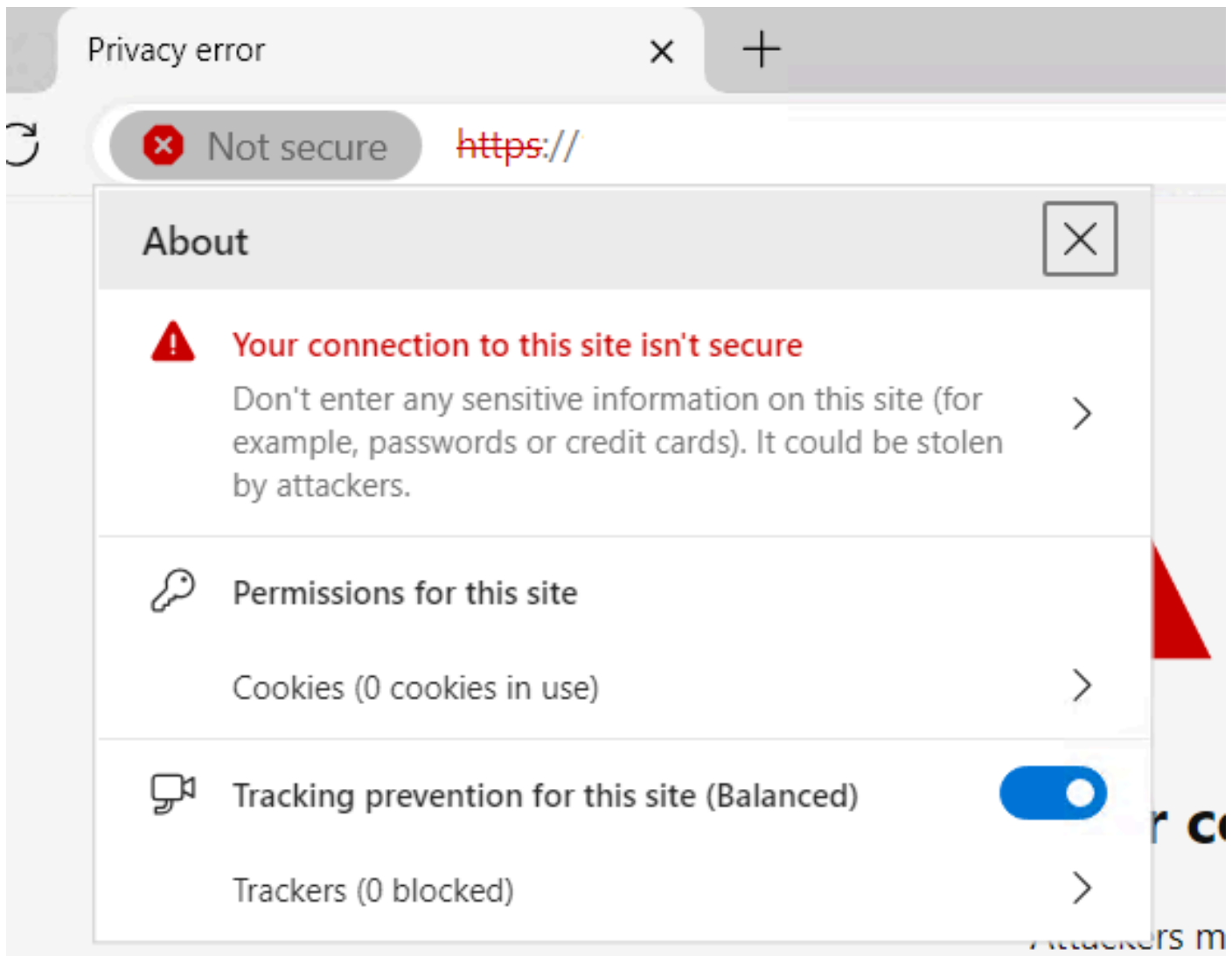
    X509v3 CRL Distribution Points:
        Full Name:

    Authority Information Access:
```

Web Server and Web Client Authorization Key in certificate requested

UCS Central is still flagged as an insecure site.

Sometimes after configuring the Third Party Certificate the connection is still flagged by the browser.



UCS Central is a unsecure site still

To verify if the certificate is being applied correctly, ensure the device trust the Certificate Authority.

Related Information

- [Cisco UCS Central Administration Guide, Release 2.0](#)
- [Cisco Technical Support & Downloads](#)