Configure Third Party Certificate for UCS Central

Contents

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:

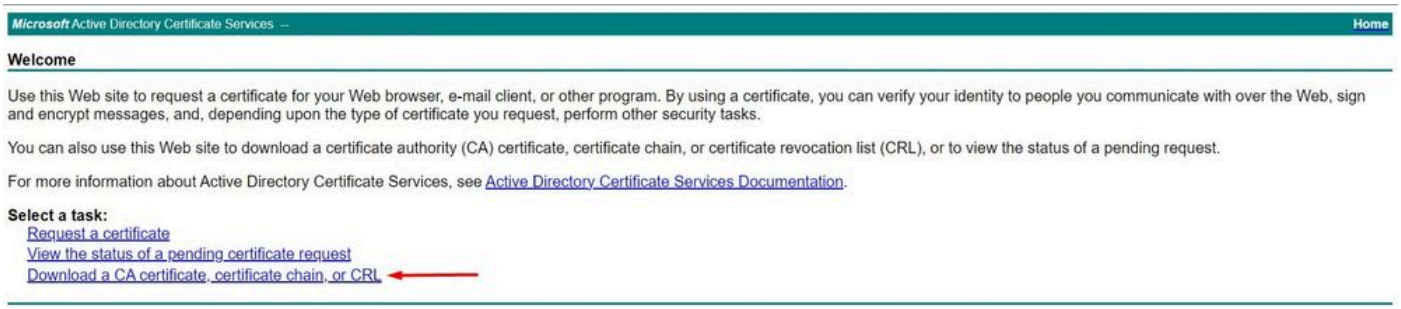
- UCS Central 2.0(1q)
- Microsoft Active Directory Certificate Services
- Windows 11 Pro N
- OpenSSL 3.1.0

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

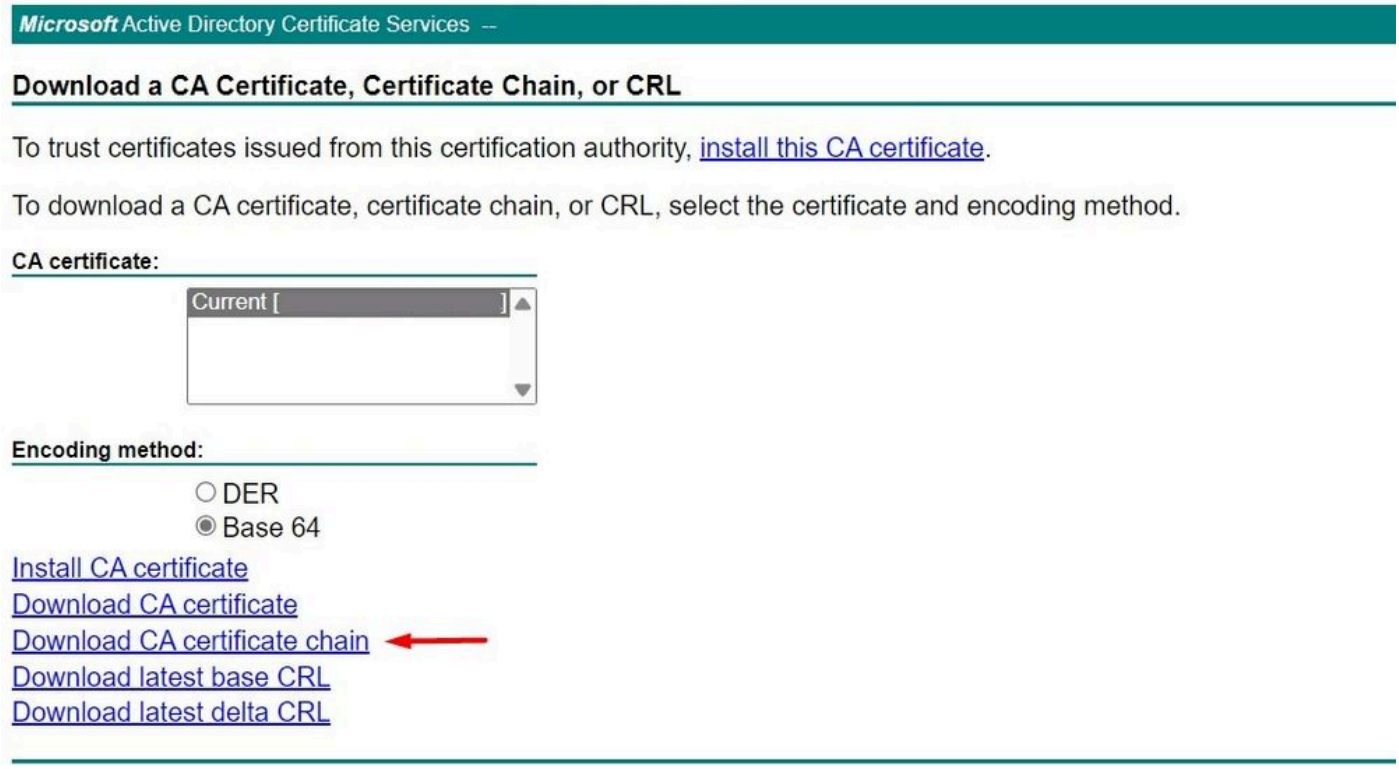
Download the Certificate Chain from the Certificate Authority.

1. Download the certificate chain from the Certificate Authority (CA).



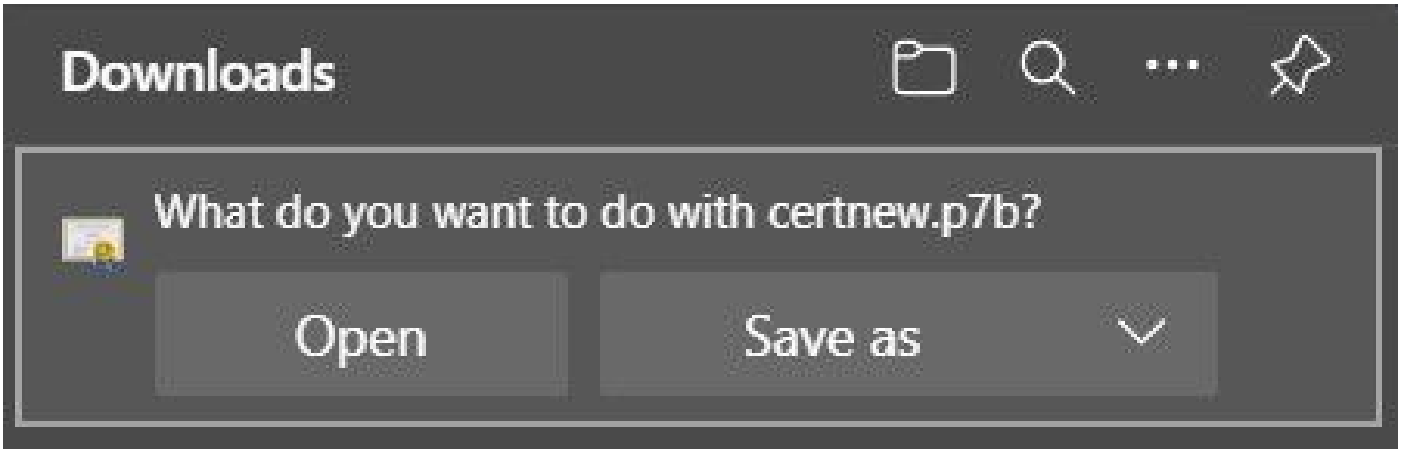
Download a certificate chain from CA

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



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.

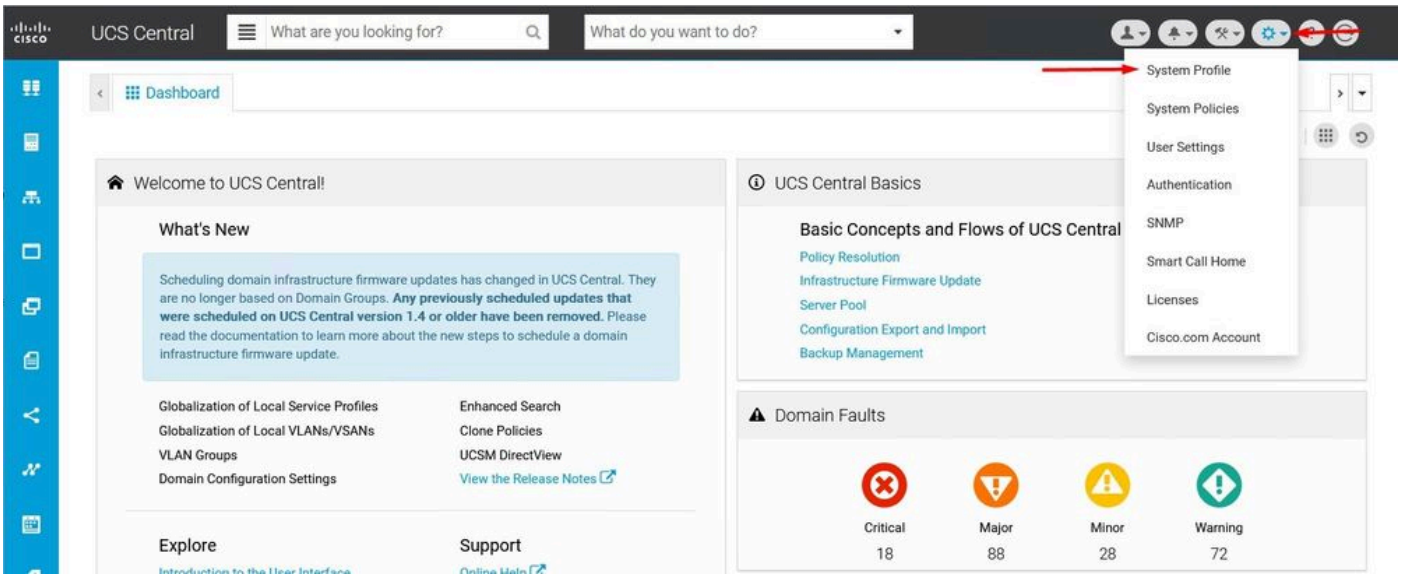
5.If OpenSSL is installed, run the command **openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem** to perform the conversion. Make sure to use the path were the certificate is saved.

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

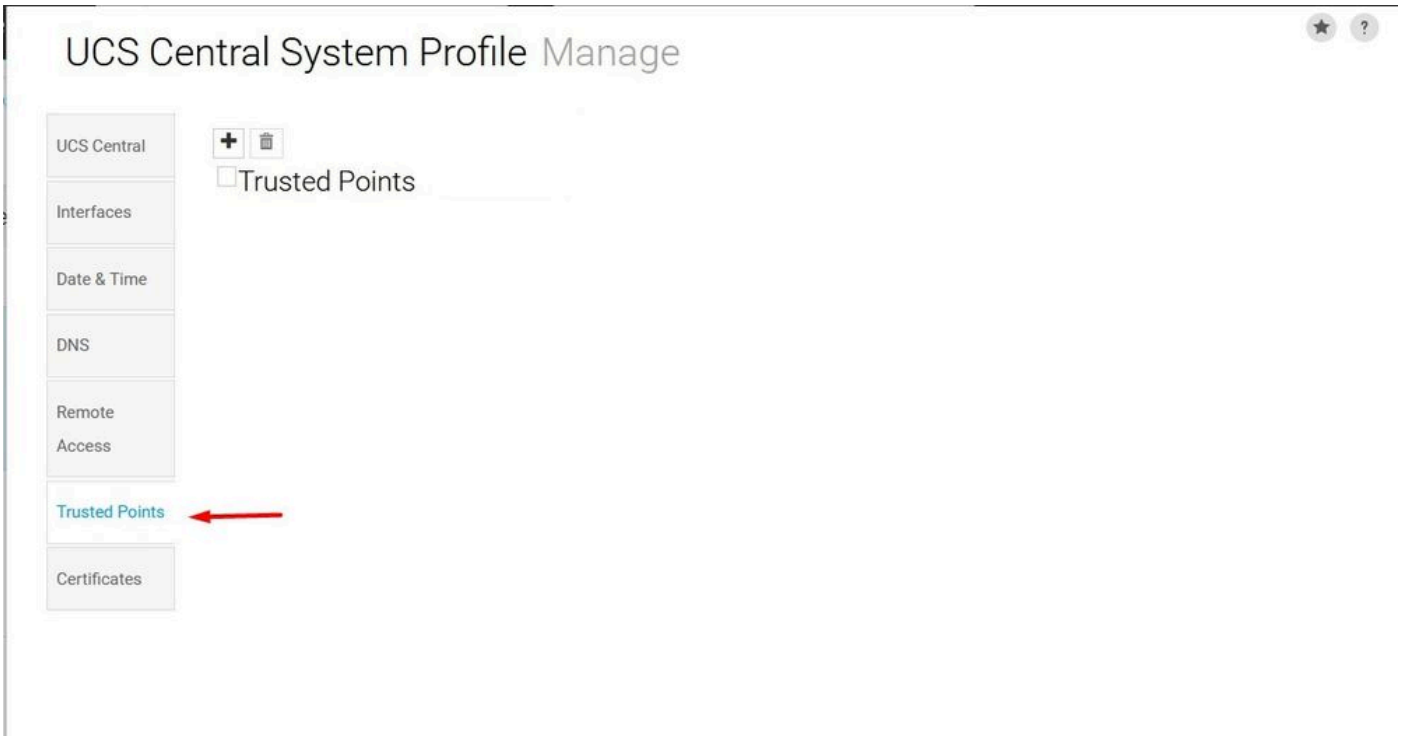
Convert the P7B certificate to PEM format

Create the Trusted Point

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

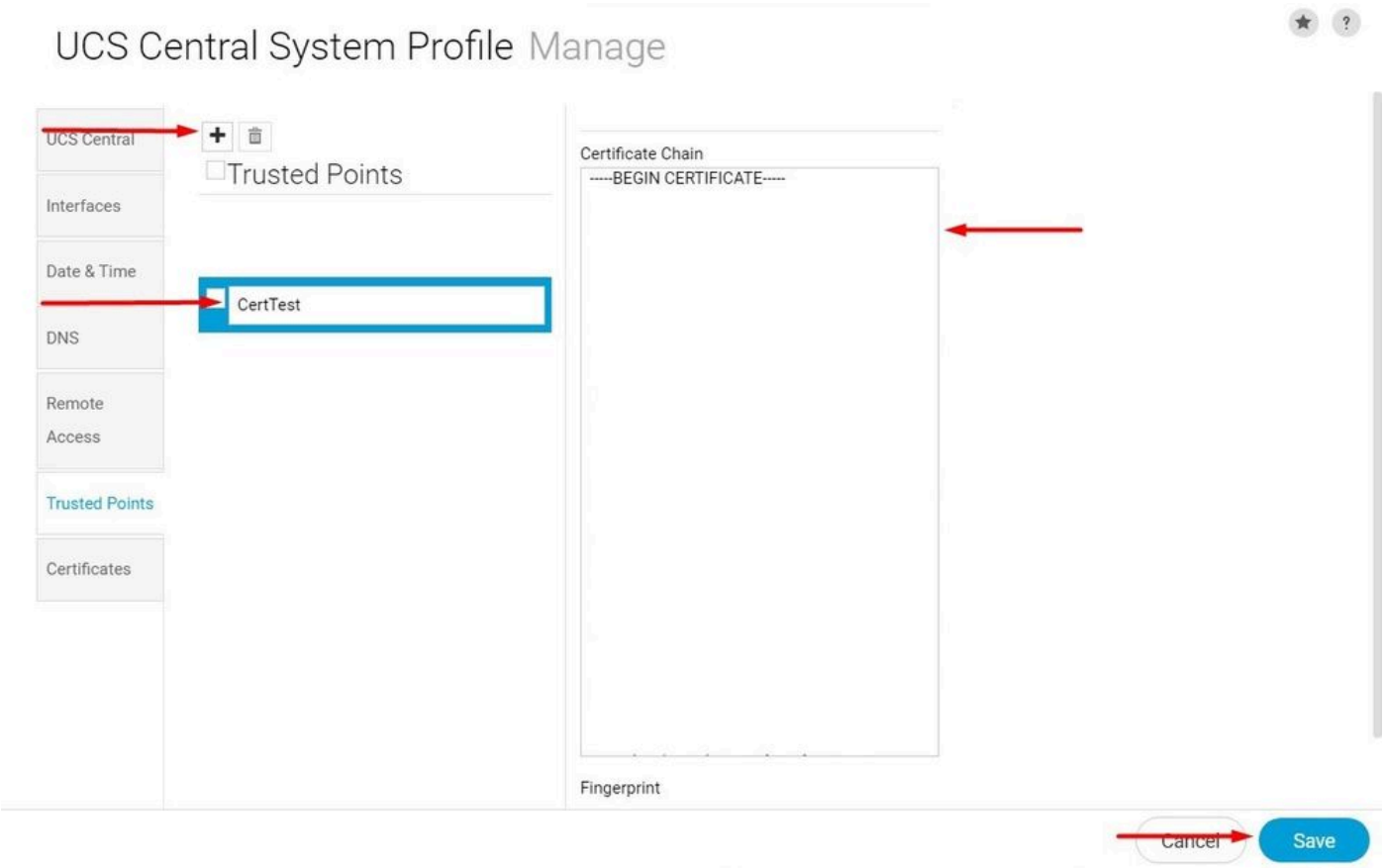


UCS Central System Profile



UCS Central Trusted Points

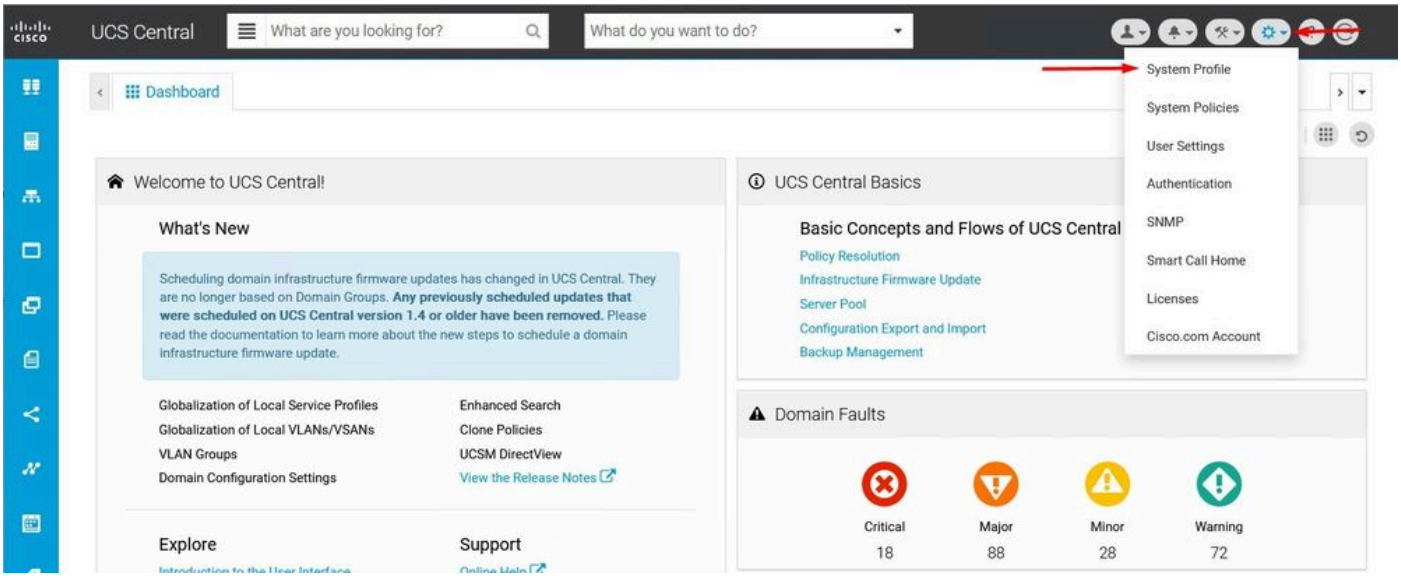
2. Click the + (plus) icon to add a new Trusted Point. Write a name and paste in the contents of the PEM certificate. Click **Save** to apply the changes.



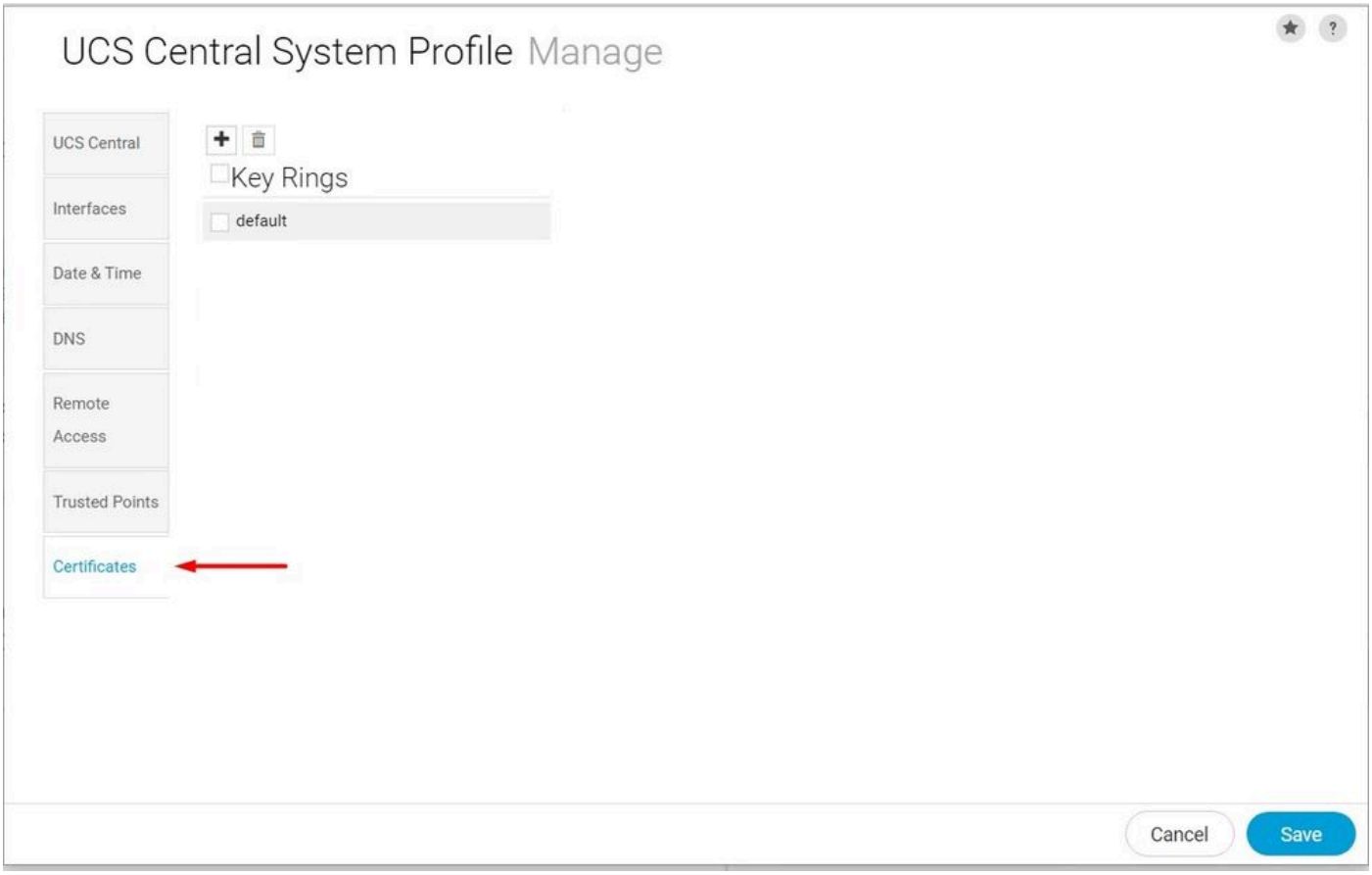
Copy the certificate chain

Creating Key Ring and CSR

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

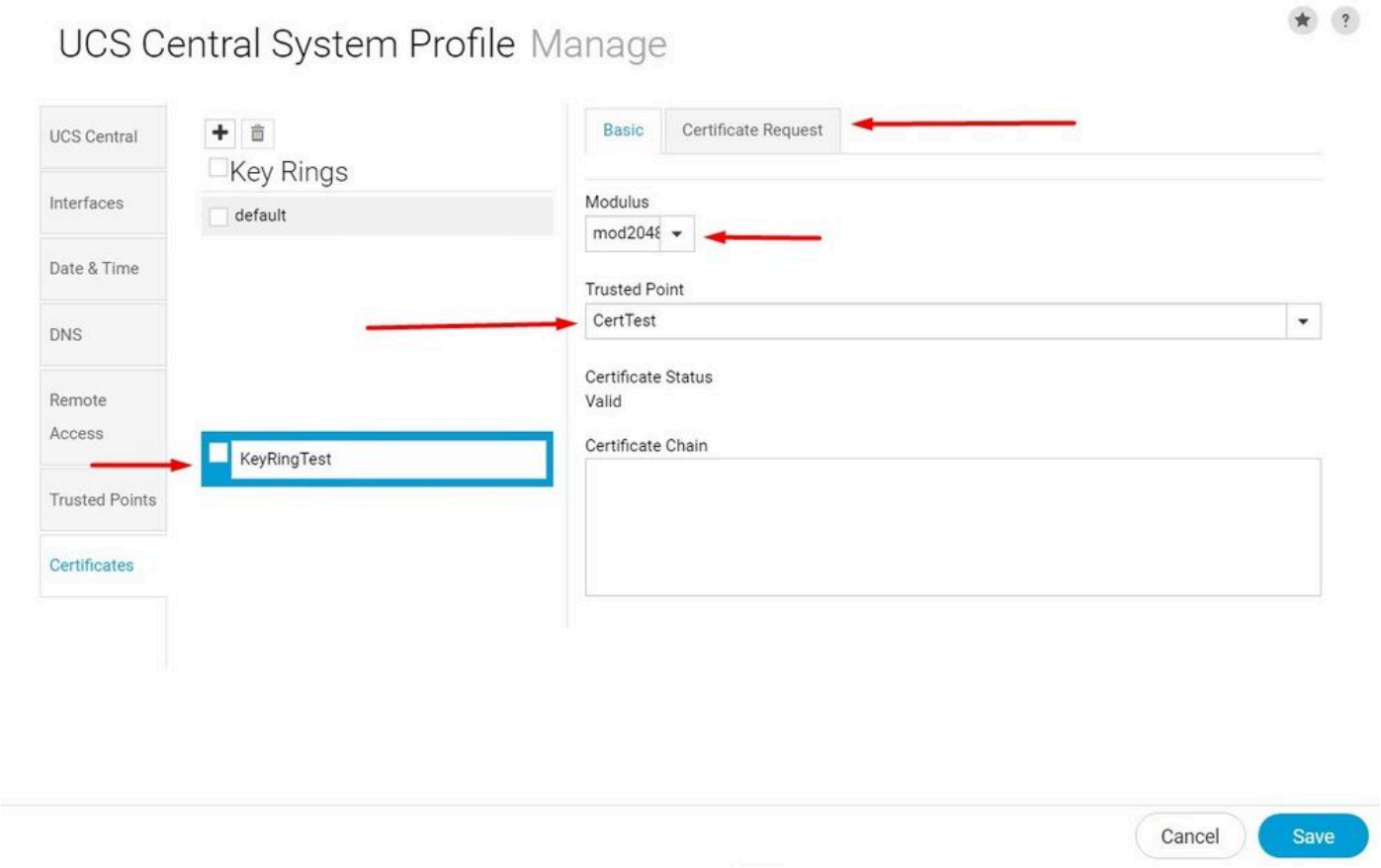


UCS Central System Profile



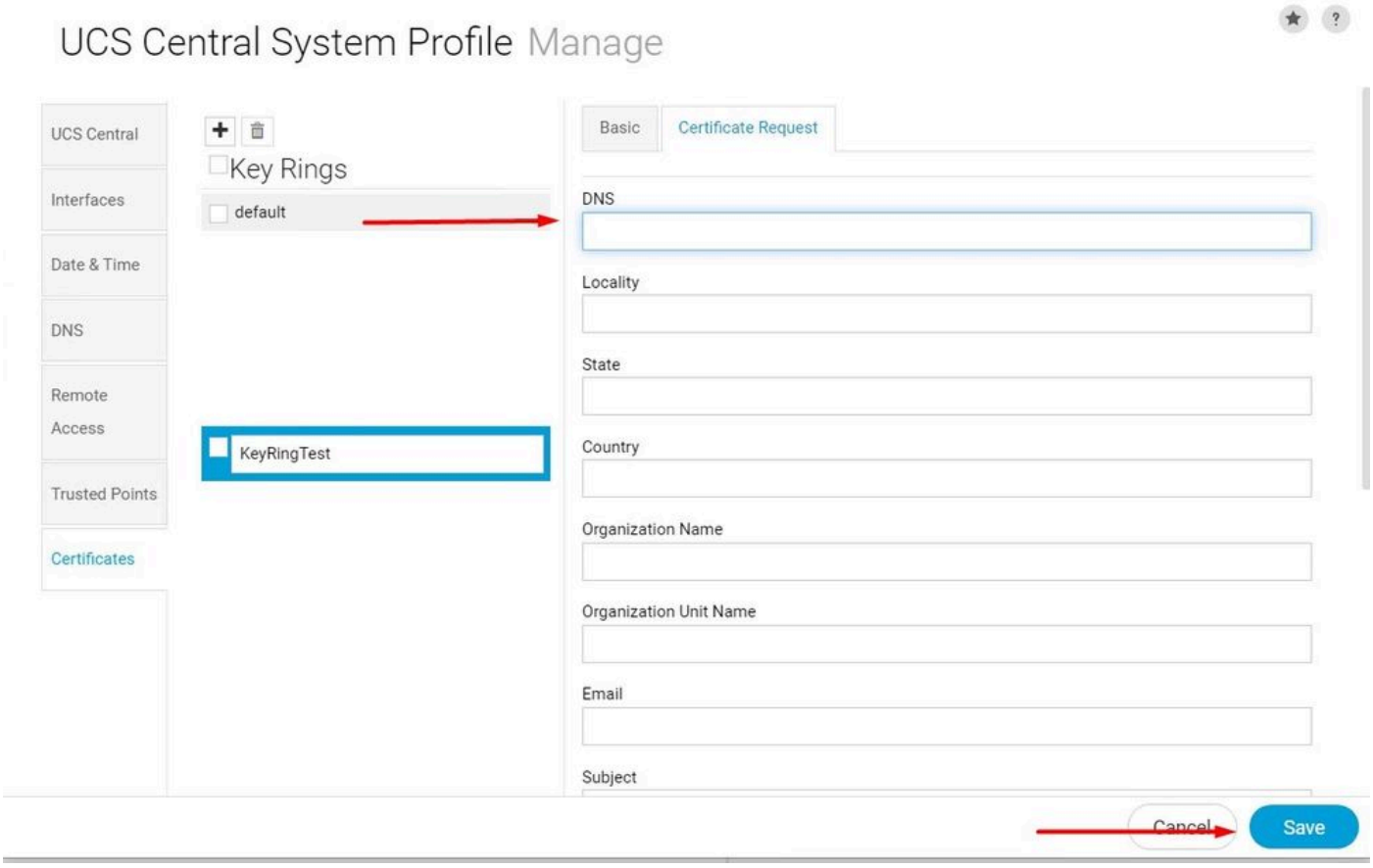
UCS Central Certificates

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**.



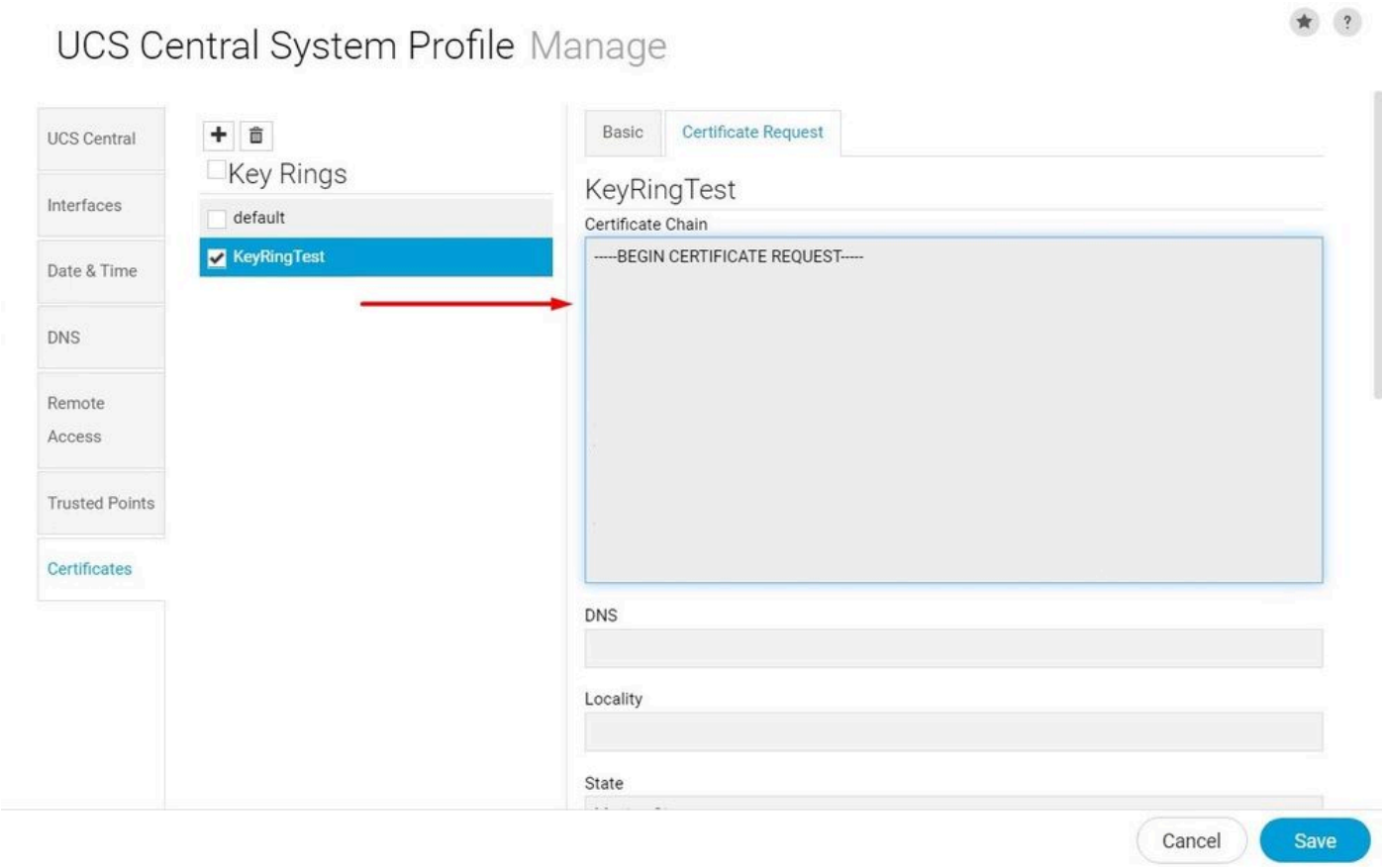
Create a new Key Ring

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



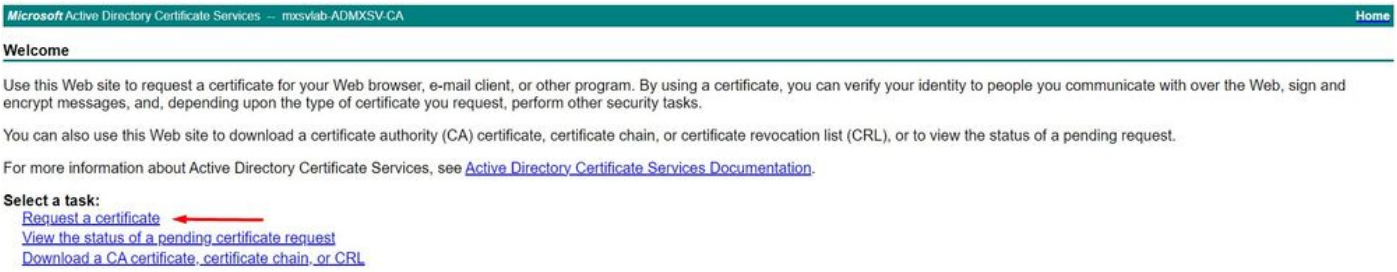
Enter the details to generate a certificate

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



Copy the certificate generated

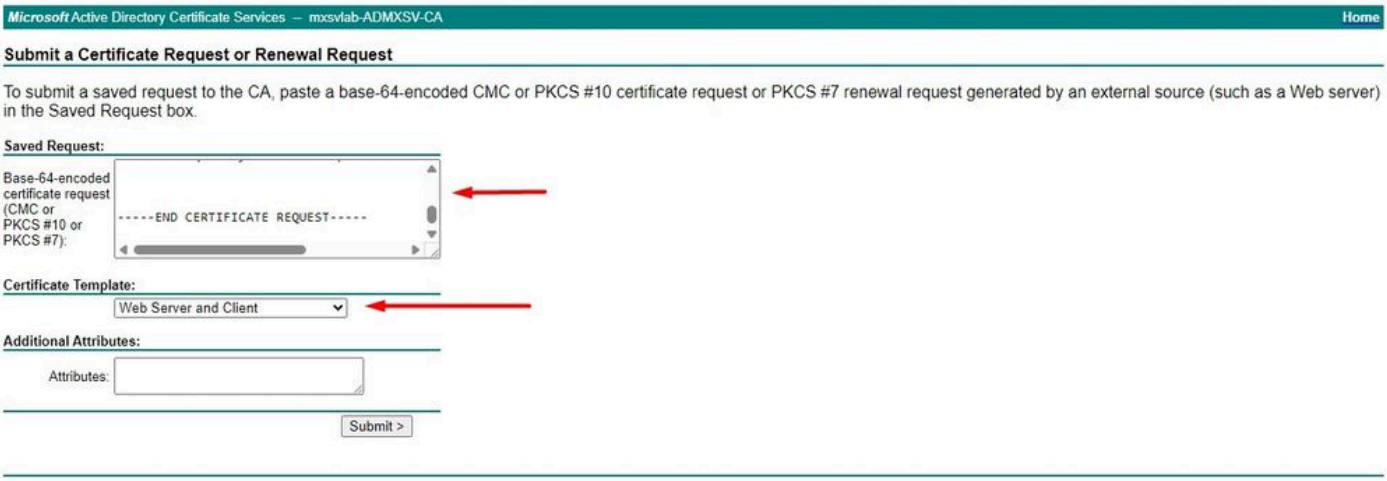
5. Go to the CA and request a certificate.



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.

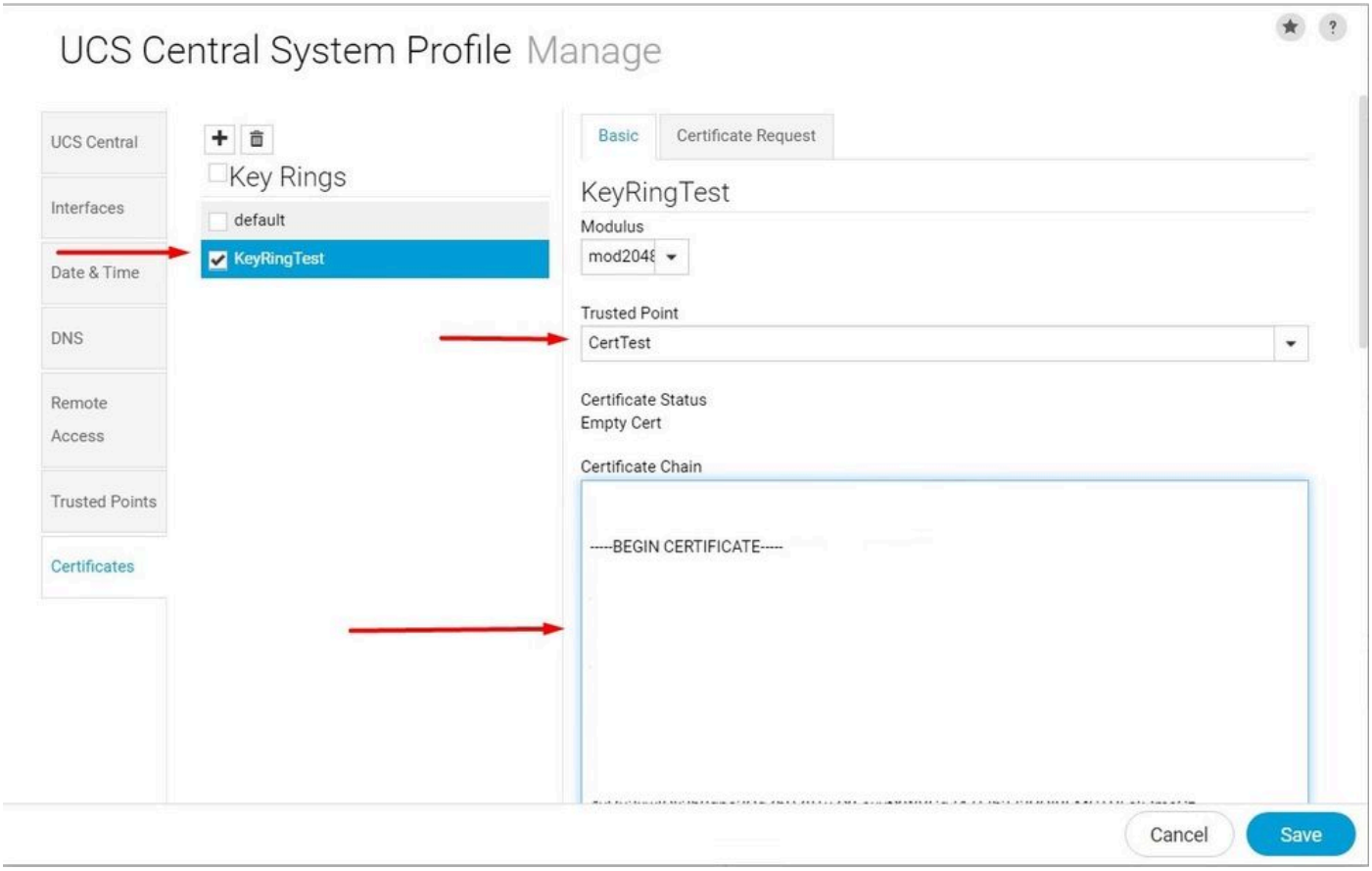
Note: When generating a certificate request in Cisco UCS Central, ensure the resulting certificate includes SSL Client and Server Authentication key usages. If using a Microsoft Windows Enterprise CA, utilize the Computer template, or another appropriate template that includes both key usages, if the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



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**.

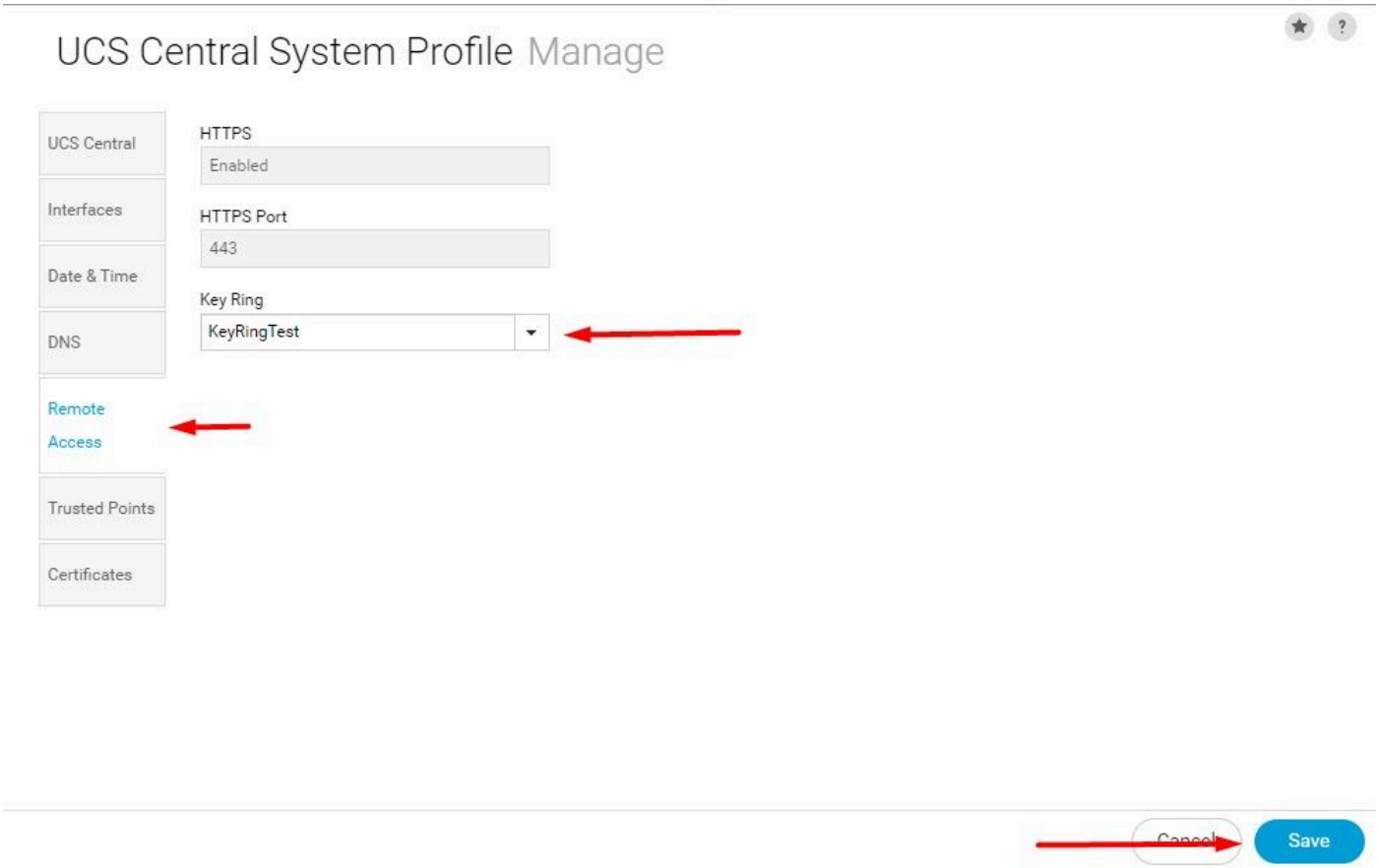
8. Copy the contents of the PEM certificate and go to the Key ring created to paste the contents. Select the **Trusted Point** created and save the configuration.



Paste the certificate requested in the key ring

Apply the Key Ring

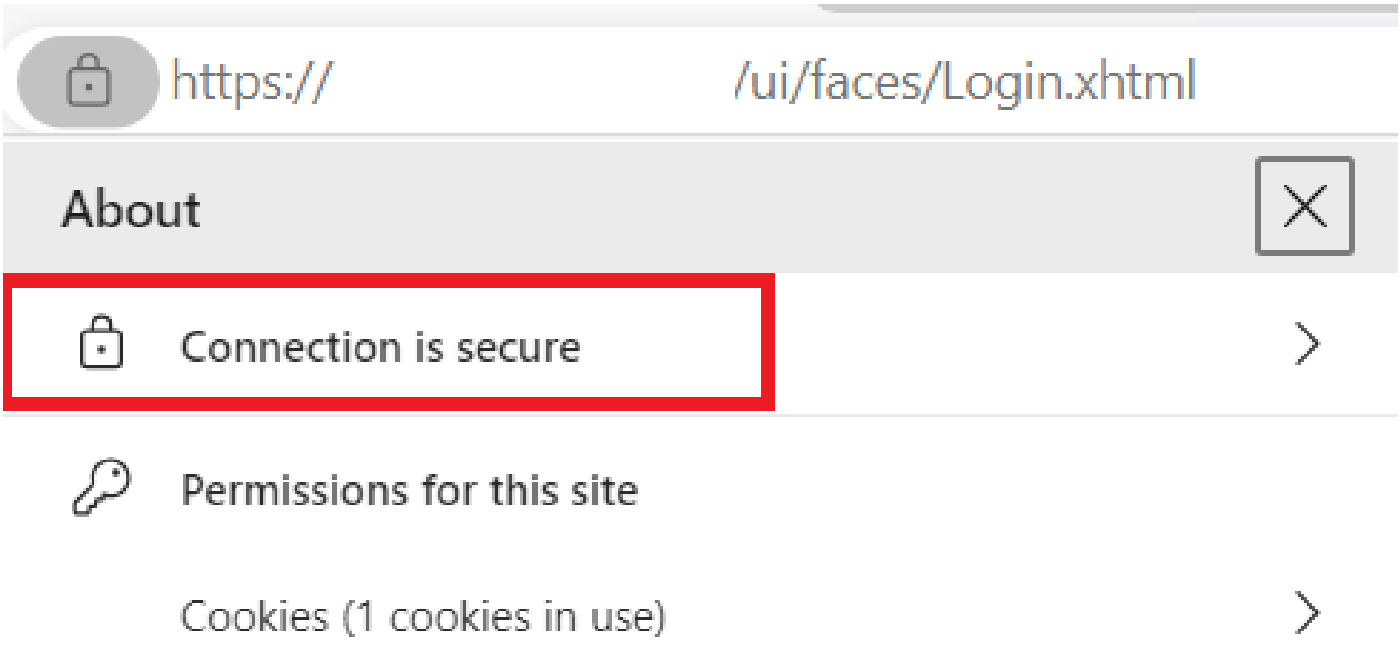
1. Navigate to **System Profile > Remote Access > Keyring**, select the Key ring created, and click **Save.** UCS Central closes the current session.



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

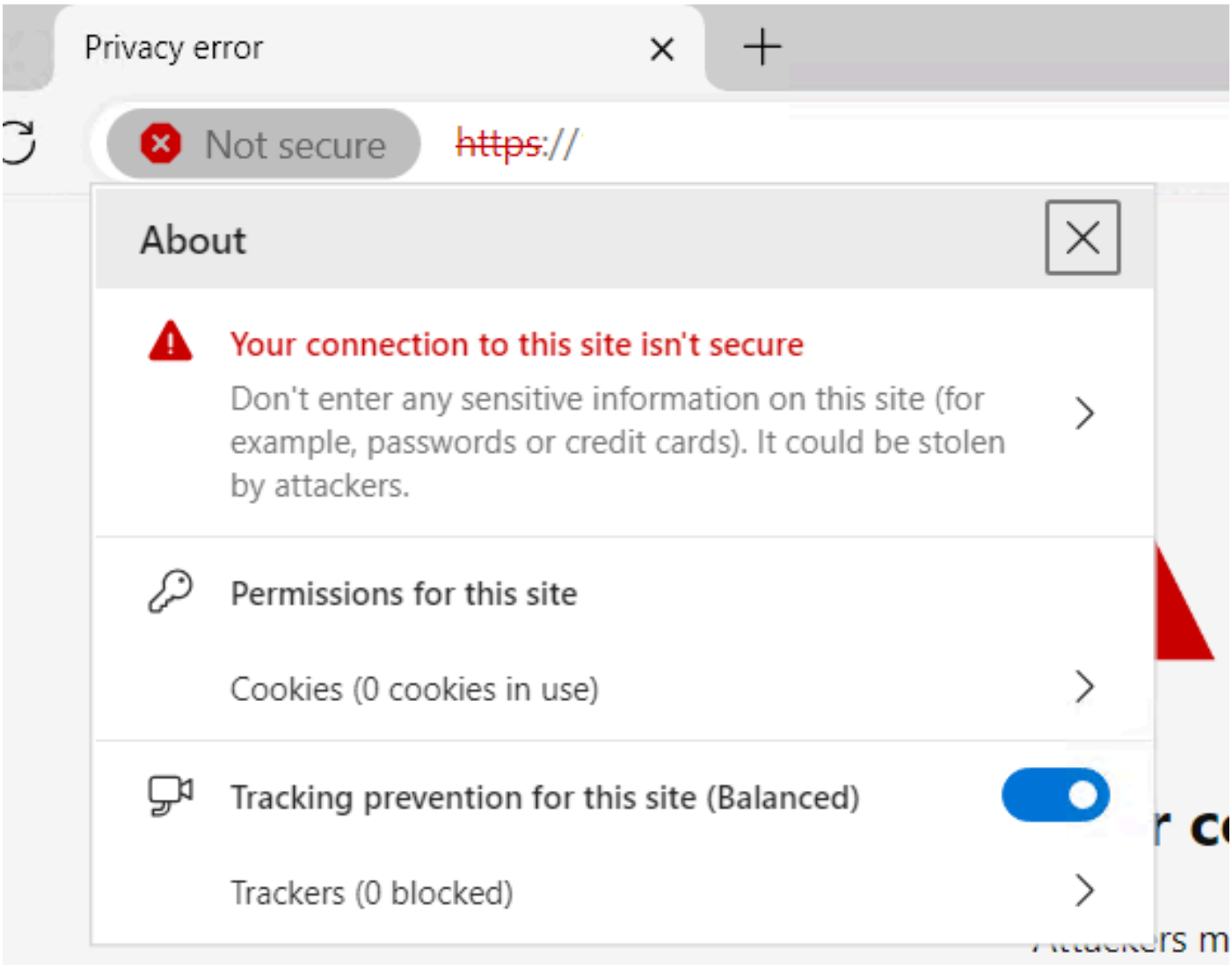
To verify if the certificate in PEM format created from the template selected in the CA has the correct Server Authentication key usages you can use the command **openssl x509 -in <my_cert>.pem -text -noout**. You must see **Web Server Authentication** and **Web Client Authentication** under the **Extended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

```
        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