Certificaat van derden voor UCS Central configureren

Inhoud

Inleiding

Dit document beschrijft de beste praktijken om een certificaat van derden in Cisco Unified Computing System Central-software (UCS Central) te configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Cisco UCS Central-software
- Certificaatautoriteit (CA)
- OpenSSL

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

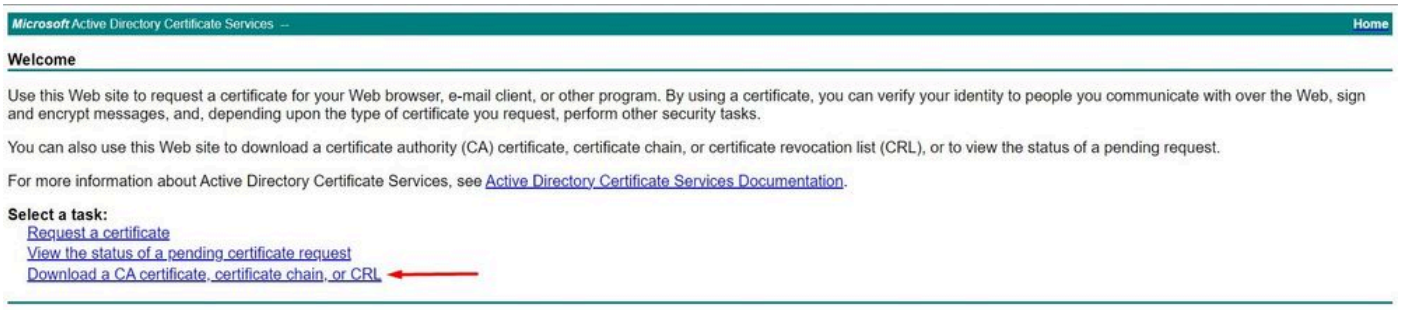
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

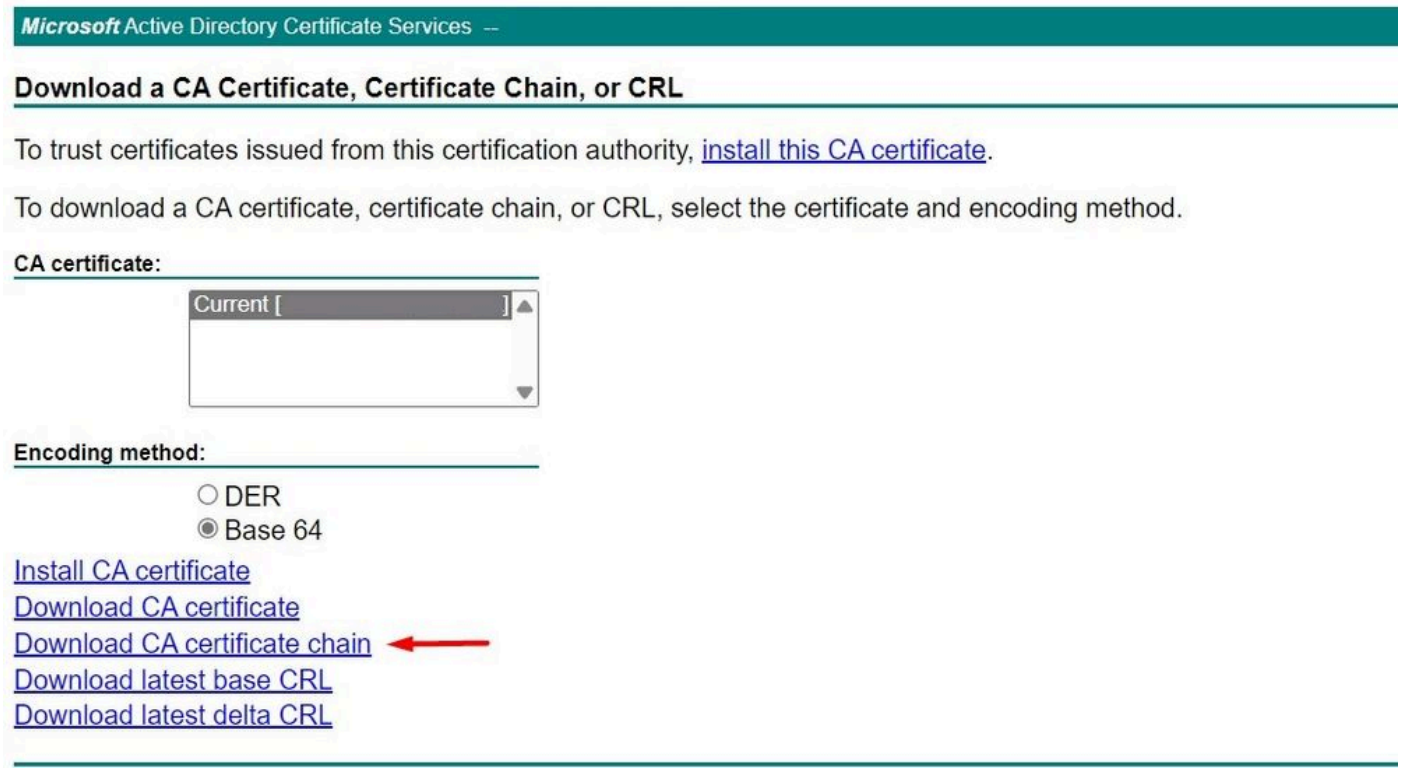
Download de certificaatketen van de certificeringsinstantie.

1. Download de certificaatketen van de certificeringsinstantie (CA).



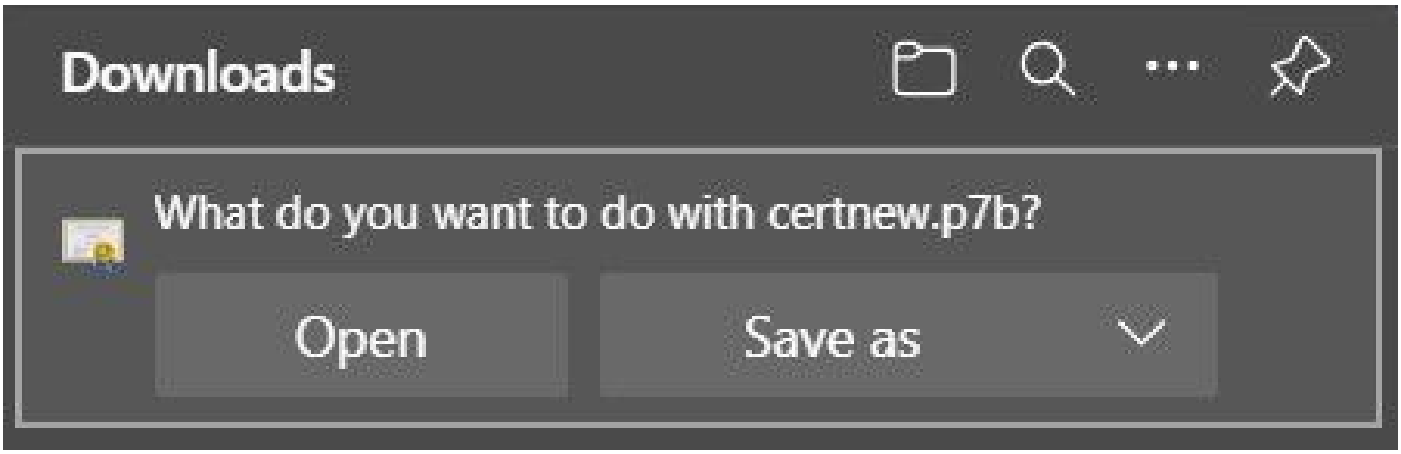
Download een certificaatketen van CA

2. Stel de codering in op Base 64 en download de CA-certificaatketen.



Stel de codering in op Base 64 en download de CA-certificaatketen

3. Merk op dat de CA certificaatketting in PB7 formaat is.



Certificaat in PB7-indeling

4. Het certificaat moet worden geconverteerd naar PEM-indeling met OpenSSL-tool. Gebruik de opdracht openssl versie om te controleren of Open SSL in Windows is geïnstalleerd.

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

Controleer of OpenSSL is geïnstalleerd

Opmerking:OpenSSL-installatie valt buiten het toepassingsgebied van dit artikel.

---

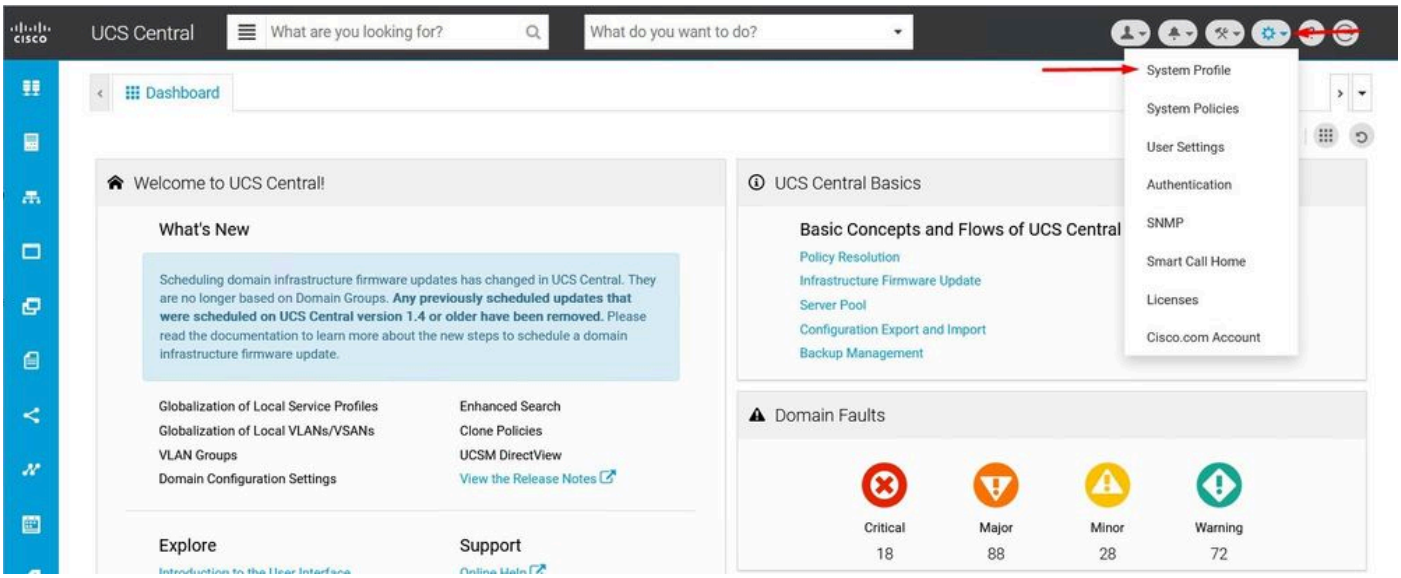
5. Als OpenSSL is geïnstalleerd, voer dan de opdracht openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem uit om de conversie uit te voeren. Zorg ervoor dat het pad wordt gebruikt als het certificaat wordt opgeslagen.

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

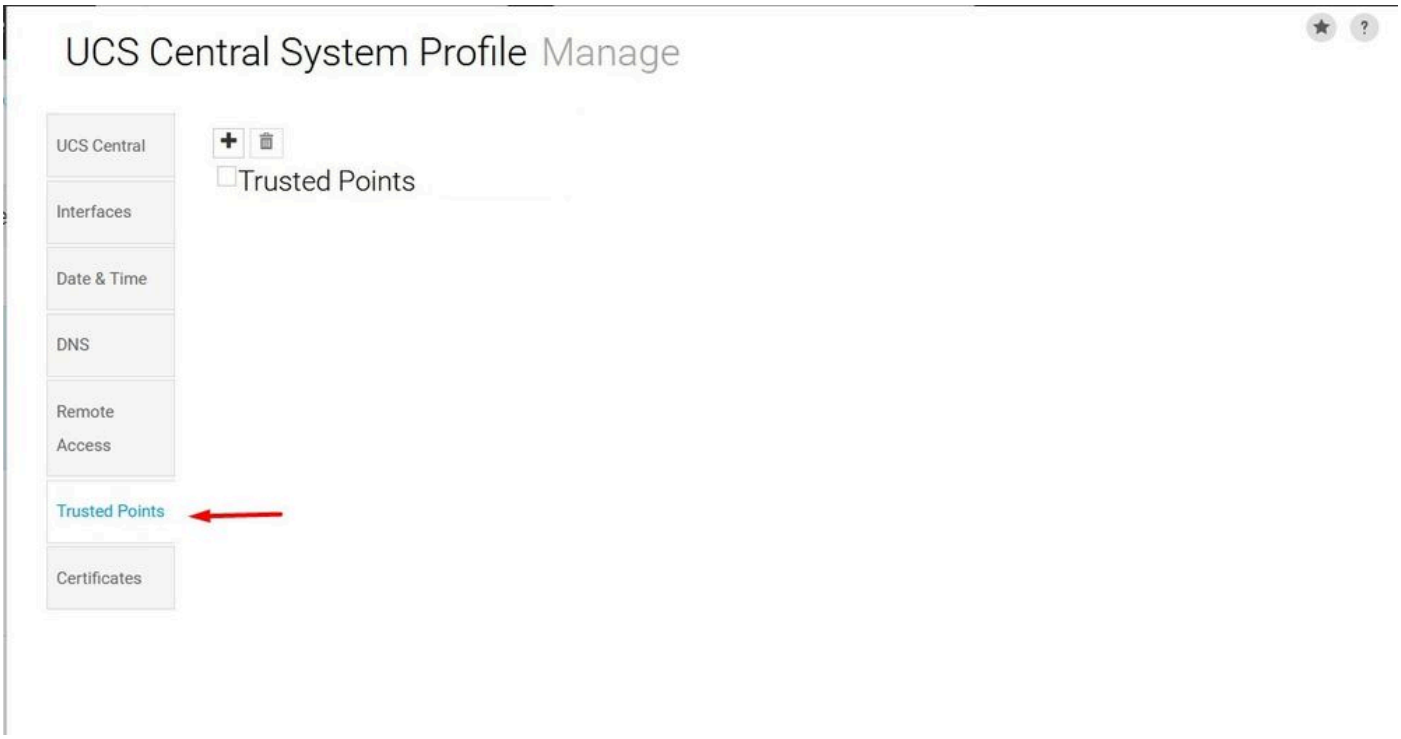
Converteer het P7B-certificaat naar PEM-formaat

Het vertrouwde punt maken

1. Klik op het pictogram Systeemconfiguratie > Systeemprofiel > Vertrouwde punten.

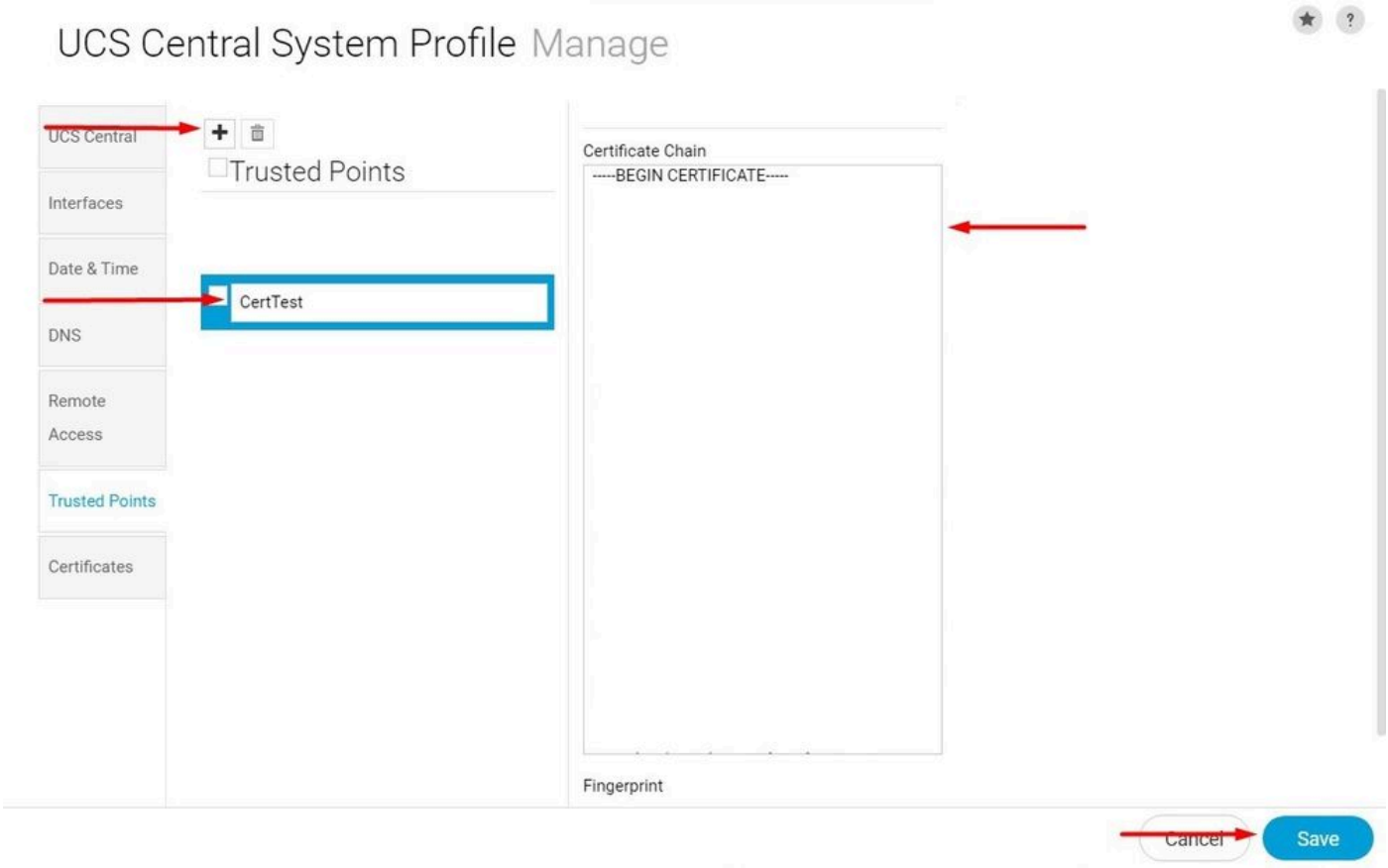


UCS Central System



ProfileUCS Central Trusted Points

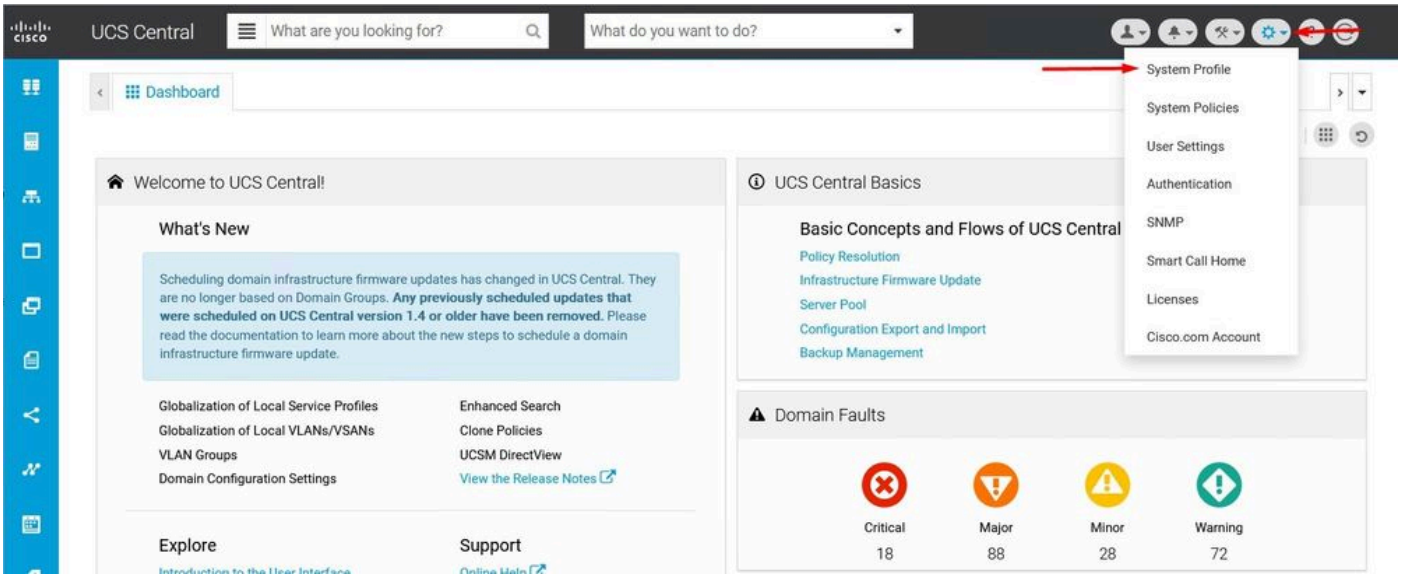
2. Klik op het pictogram + (plus) om een nieuw Trusted Point toe te voegen. Schrijf een naam en plak in de inhoud van het PEM-certificaat. Klik op Opslaan om de wijzigingen toe te passen.



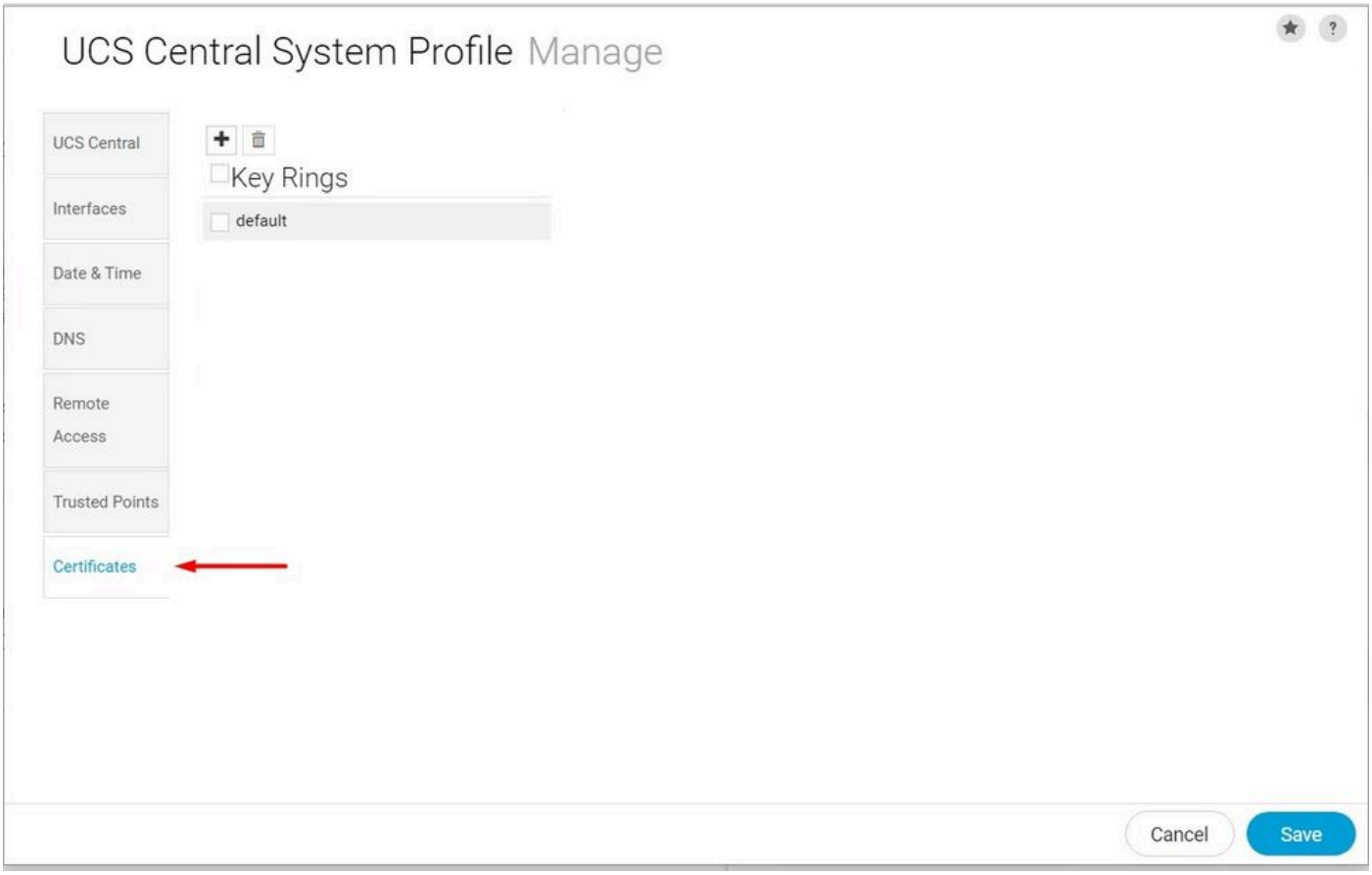
Kopieert de certificaatketen.

Key Ring en CSR maken

1. Klik op het pictogram Systeemconfiguratie > Systeemprofiel > Certificaten.

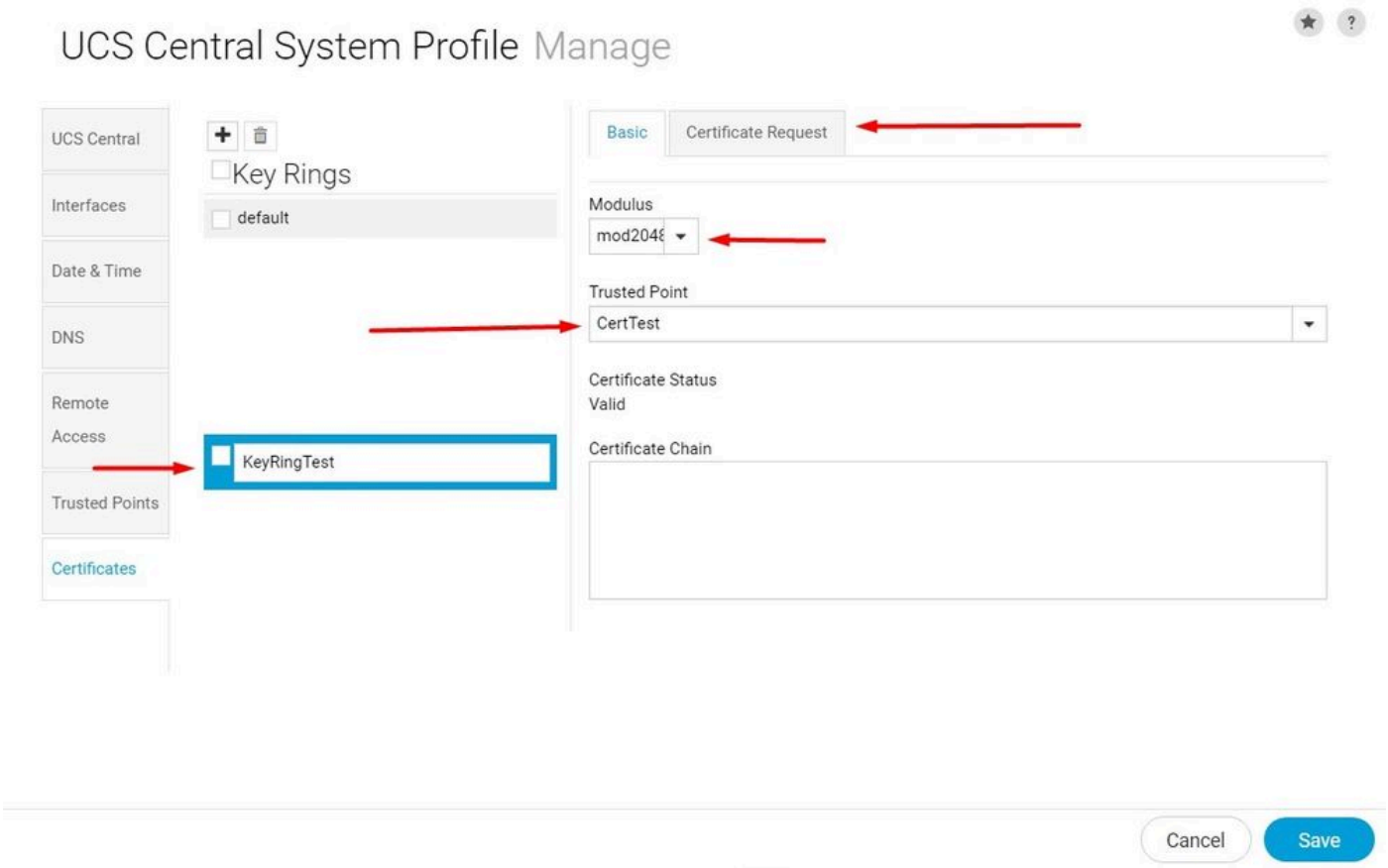


UCS Central System



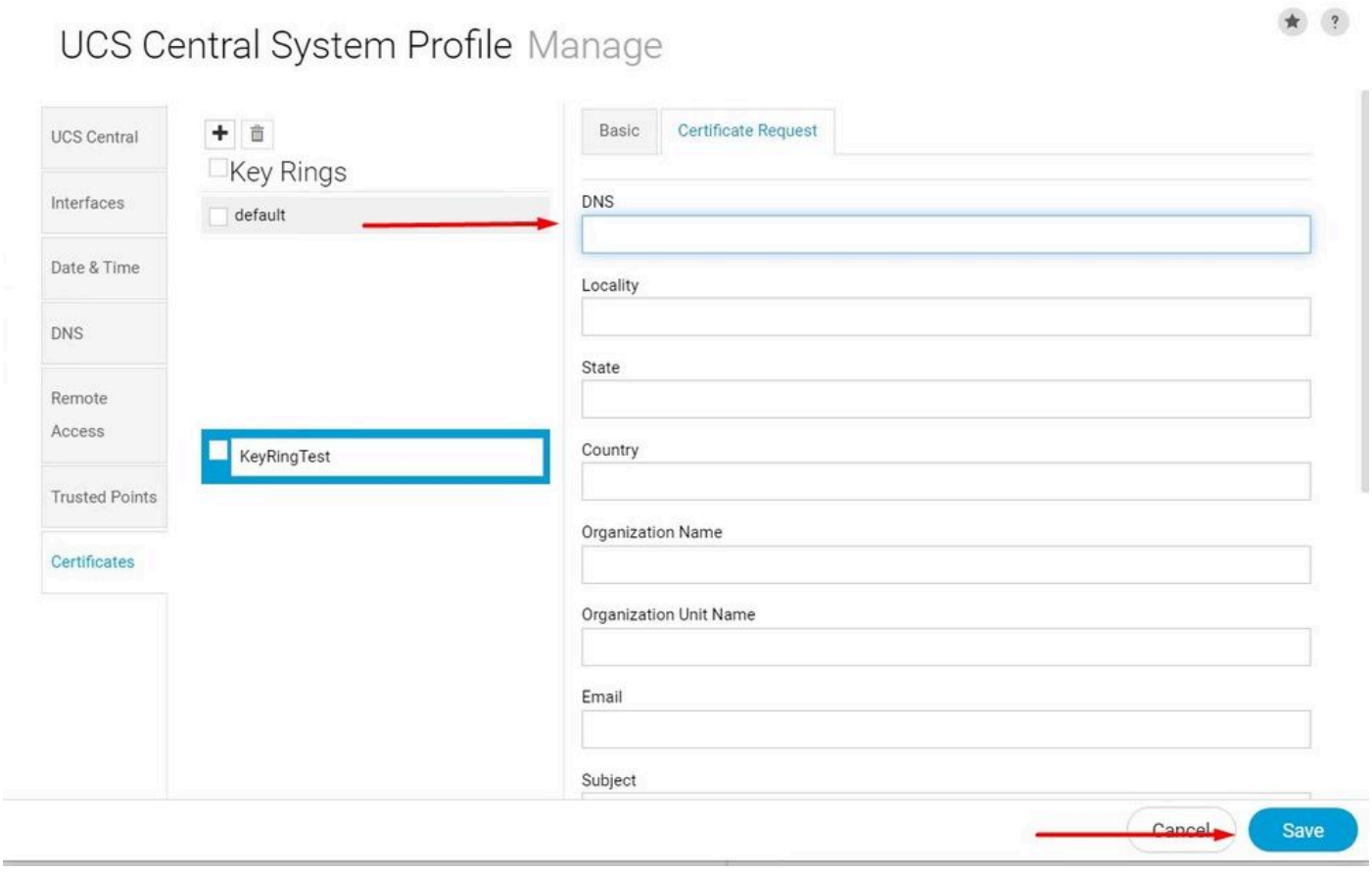
ProfileUCS Central-certificaten

2. Klik op het plus-pictogram om een nieuwe sleutelring toe te voegen. Schrijf een naam, laat de modulus met de standaardwaarde (of wijzig indien nodig) en selecteer het Vertrouwde punt dat eerder gemaakt is. Nadat u deze parameters hebt ingesteld, gaat u naar Certificaataanvraag.



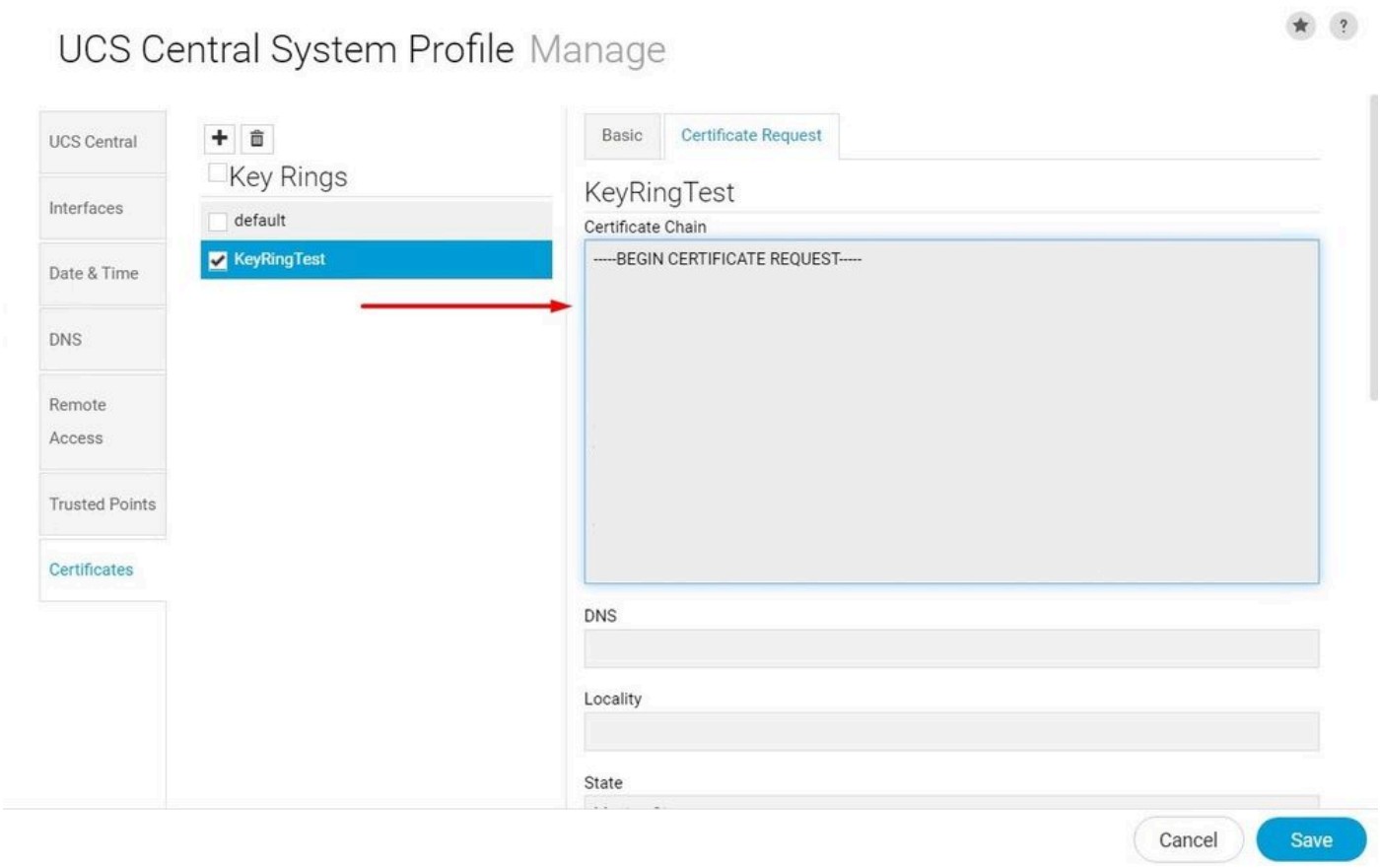
Een nieuwe sleutelring maken

3. Voer de gewenste waarden in voor het aanvragen van een certificaat en klik op Opslaan.



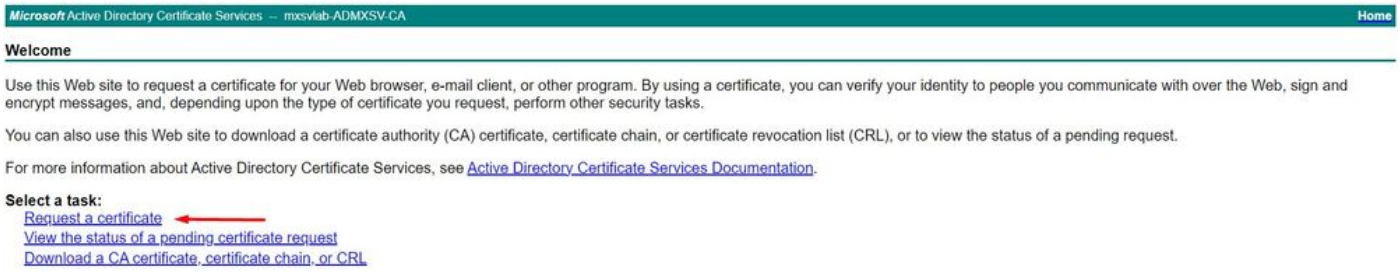
Voer de gegevens in om een certificaat te genereren

4. Ga terug naar de sleutelring die is gemaakt en kopieer het gegenereerde certificaat.



Het gegenereerde certificaat kopiëren

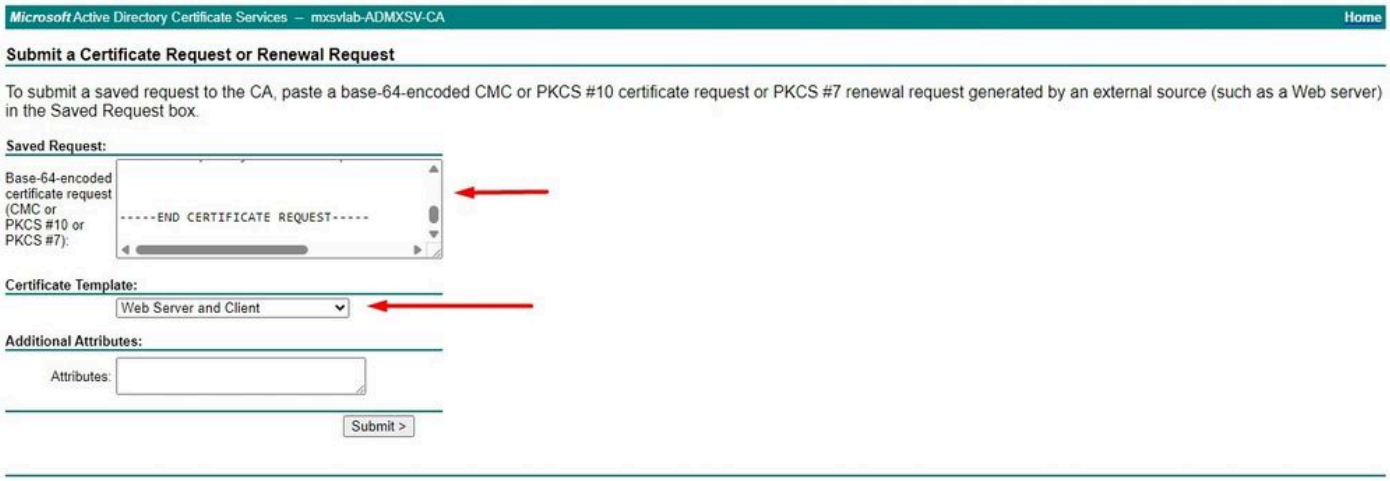
5. Ga naar de CA en vraag een certificaat aan.



Vraag een certificaat aan bij CA

6. Plakt het certificaat dat in UCS Central en in de CA is gegenereerd, en selecteer de sjabloon voor de webserver en client. Klik op Indienen om het certificaat te genereren.

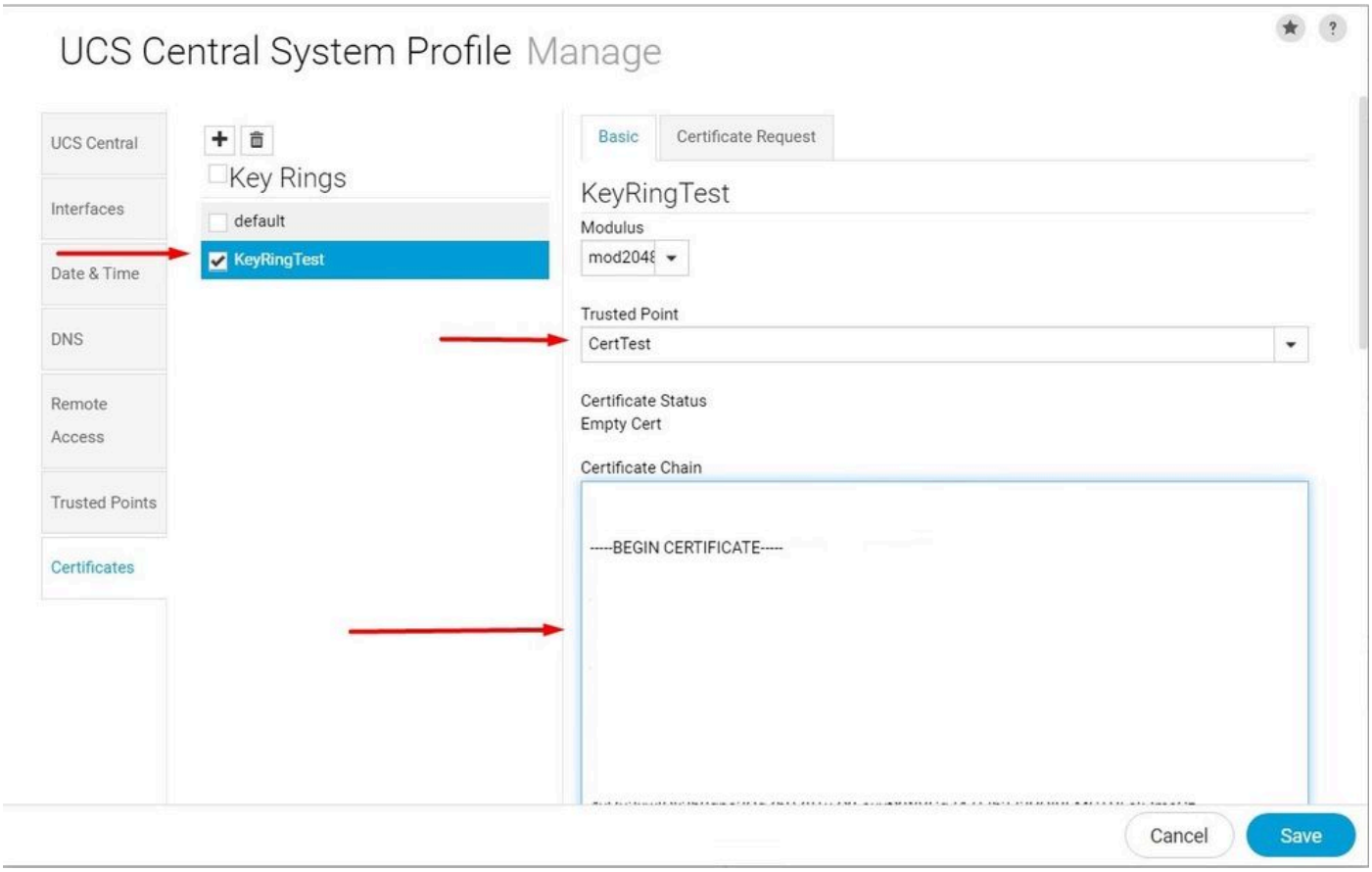
Opmerking: wanneer u een certificaataanvraag in Cisco UCS Central genereert, zorg er dan voor dat het resulterende certificaat SSL-client- en serververificatie bevat. Als u een Microsoft Windows Enterprise CA gebruikt, gebruikt u de Computersjabloon of een andere geschikte sjabloon met beide sleuteltoepassingen als de Computersjabloon niet beschikbaar is.



Genereert een certificaat voor gebruik in de sleutelring

7. Converteer het nieuwe certificaat naar PEM met de opdracht openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

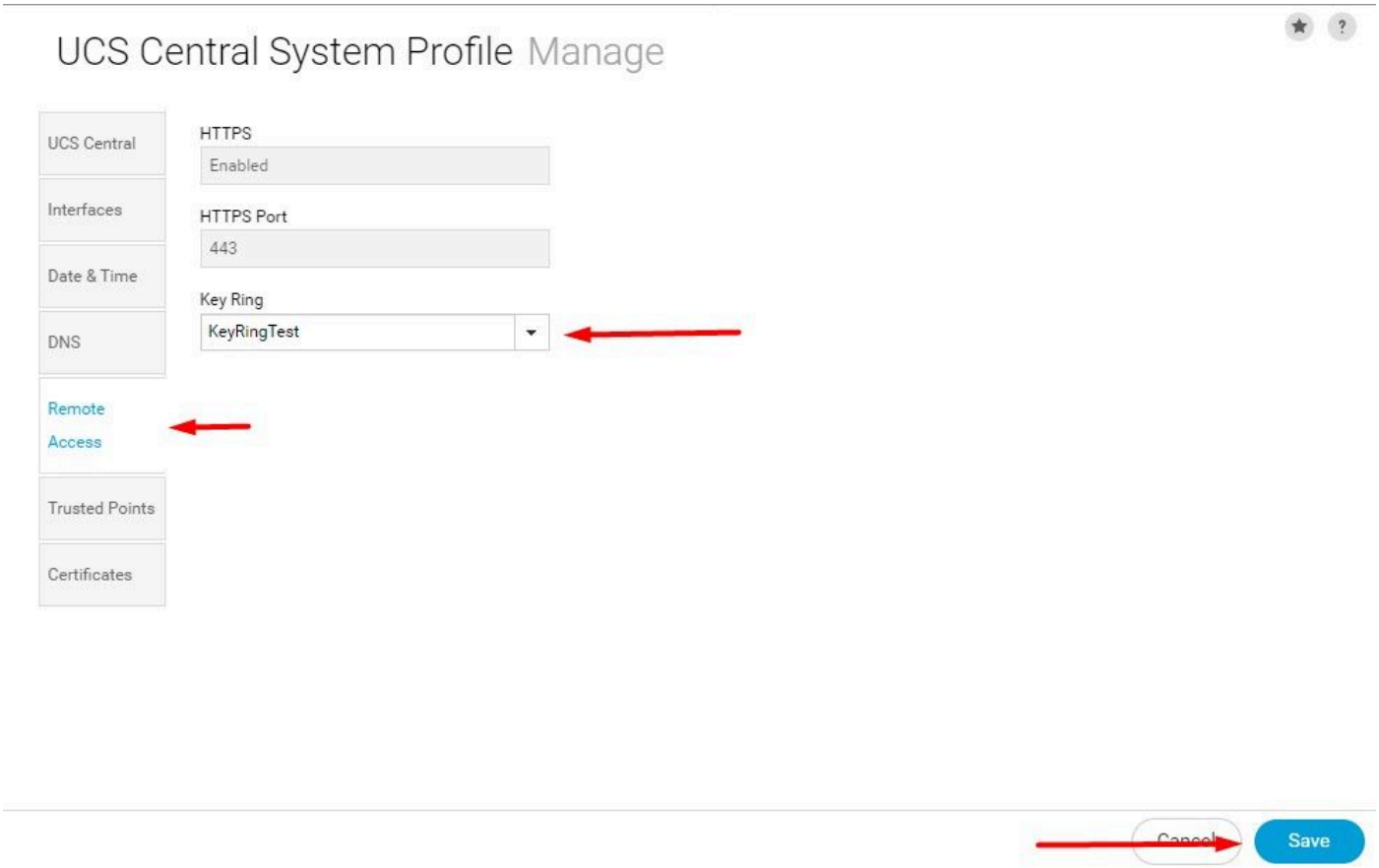
8. Kopieer de inhoud van het PEM-certificaat en ga naar de sleutelring die is gemaakt om de inhoud te plakken. Selecteer het vertrouwde punt dat is gemaakt en sla de configuratie op.



Plakt het gevraagde certificaat in de sleutelring.

De sleutelring toepassen

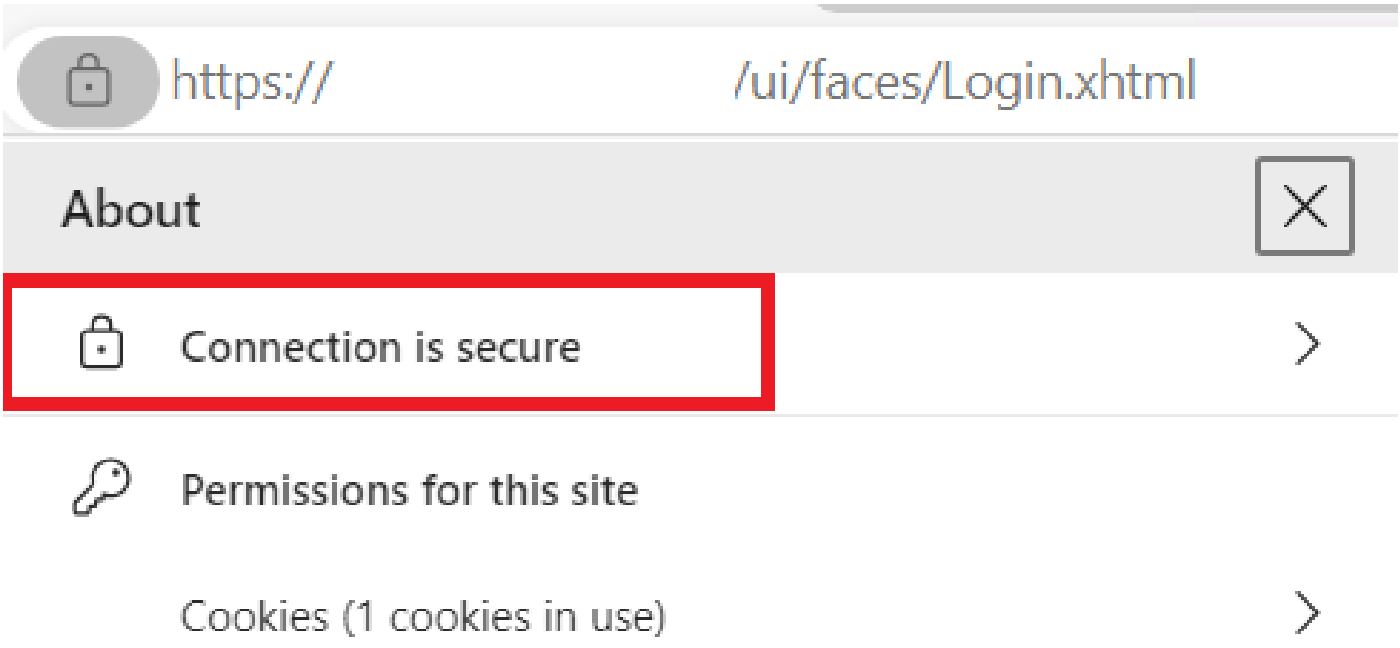
1. Navigeer naar Systeemprofiel > Externe toegang > Toetsenring, selecteer de sleutelring die is gemaakt en klik op Opslaan. UCS Central sluit de huidige sessie.



Selecteer de sleutelring die is gemaakt

Validatie

1. Wacht tot UCS Central toegankelijk is en klik in het slot naast https://. De site is veilig.



UCS Central is veilig

Probleemoplossing

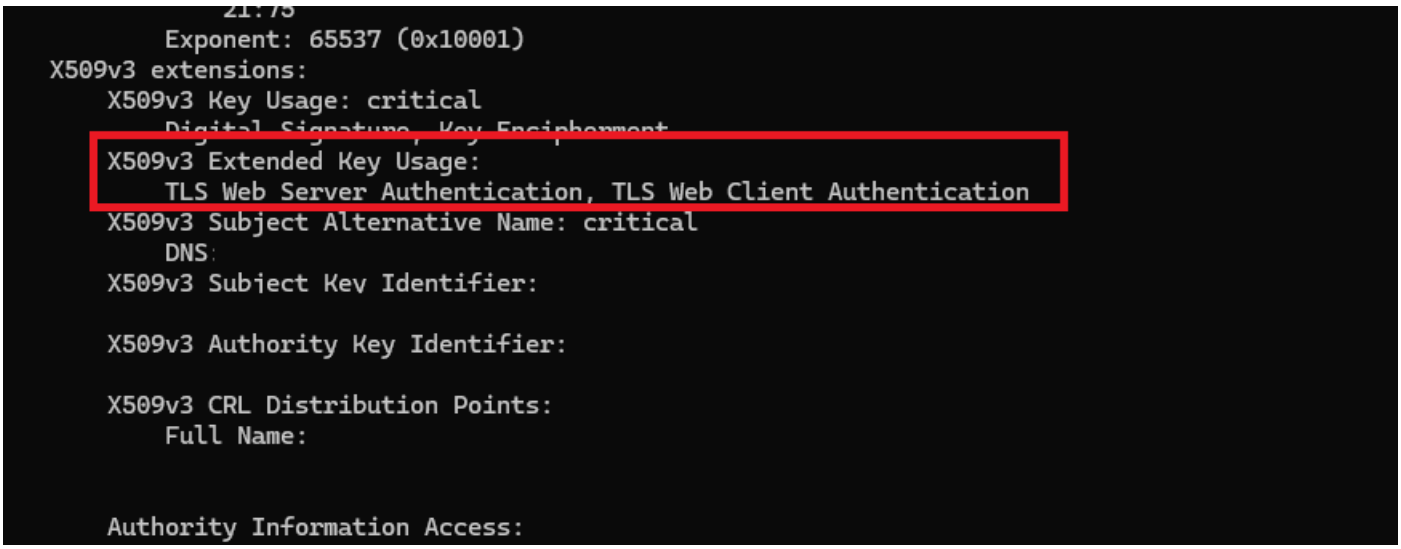
Controleer of het gegenereerde certificaat SSL-client- en serververificatie bevat.

Wanneer het certificaat dat is aangevraagd bij CA niet de SSL-client- en serververificatiesleutel bevat, wordt een fout gebruikt met de tekst "Ongeldig certificaat. Dit certificaat kan niet worden gebruikt voor TLS-serververificatie; "check key use extensions" verschijnt.

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

Fout bij autorisatiesleutels voor TLS-servers

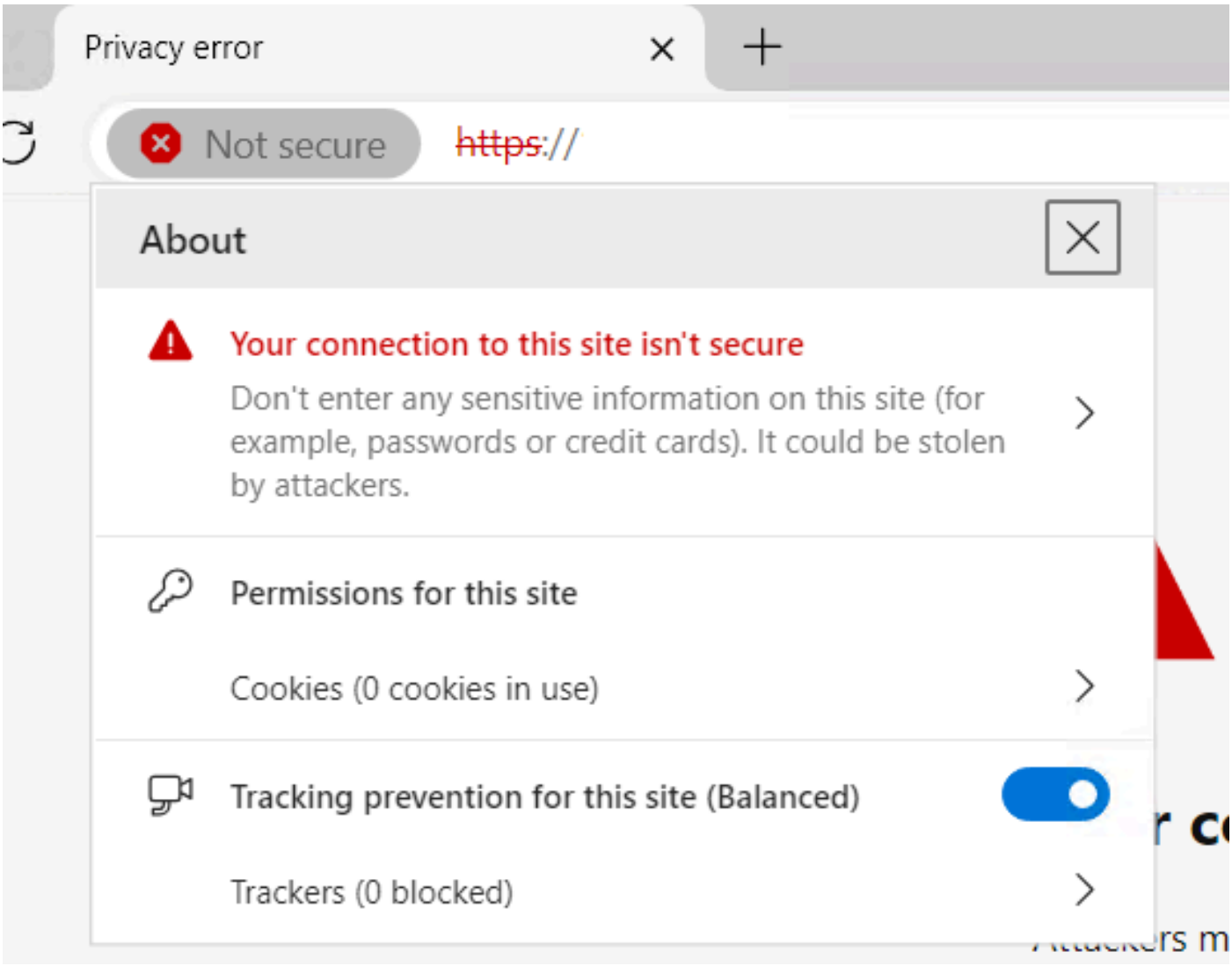
Om te verifiëren of het certificaat in PEM-formaat dat is gemaakt op basis van de sjabloon die in de CA is geselecteerd, de juiste serververificatie heeft gebruikt, kunt u de opdracht openssl x509 -in <my_cert>.pem -text -no gebruiken. U moet Web Server Verification en Web Clientverificatie zien onder de sectie Uitgebreid sleutelgebruik.



Webserver- en webclientautorisatiesleutel in aangevraagd certificaat

UCS Central wordt nog steeds gemarkeerd als een onveilige site.

Soms wordt de verbinding na het configureren van het certificaat van derden nog steeds gemarkeerd door de browser.



UCS Central is een onveilige site

Om te controleren of het certificaat correct wordt toegepast, moet u ervoor zorgen dat het apparaat de certificeringsinstantie vertrouwt.

Gerelateerde informatie

- Cisco UCS Central-beheergids, release 2.0
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.