Certificaat van derden op UCSM maken en gebruiken

Inhoud

Inleiding

Dit document beschrijft de procedure om certificaten van derden op Unified Computing System (UCS) te maken en te gebruiken voor beveiligde communicatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot CA-autoriteit
- UCS M 3.1

Gebruikte componenten

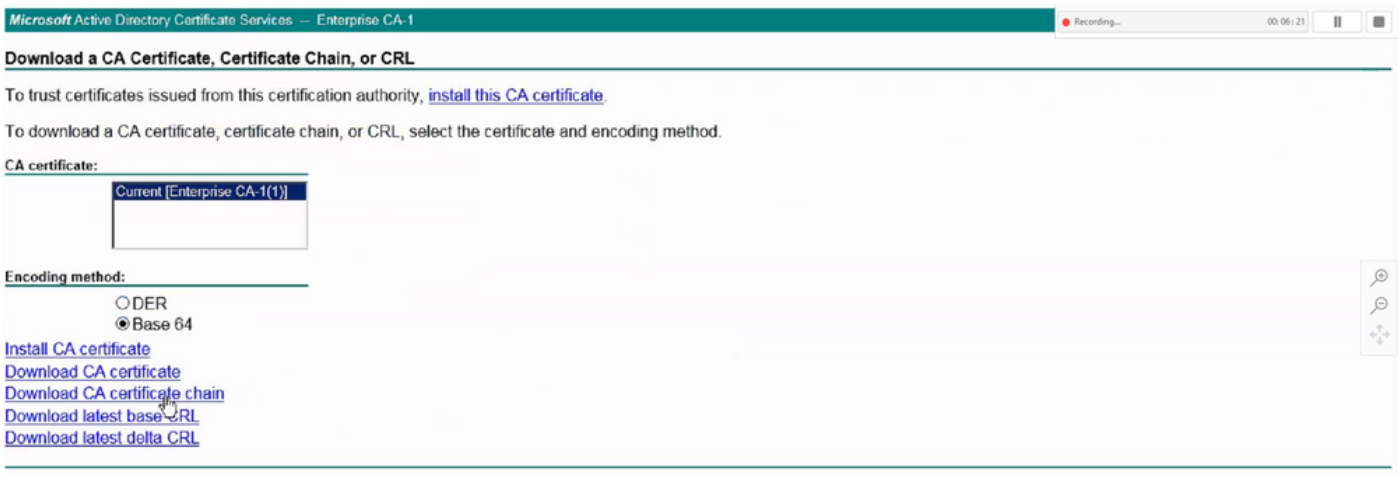
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Te configureren stappen

Vertrouwingspunt configureren

Stap 1

- Download de certificaatketen van de CA-autoriteit om Trust-Point te maken. Raadpleeg http://localhost/certsrv/Default.asp binnen Cert Server.
- Zorg ervoor dat de codering is ingesteld op Base 64.



Certificaatketen van CA-autoriteit downloaden

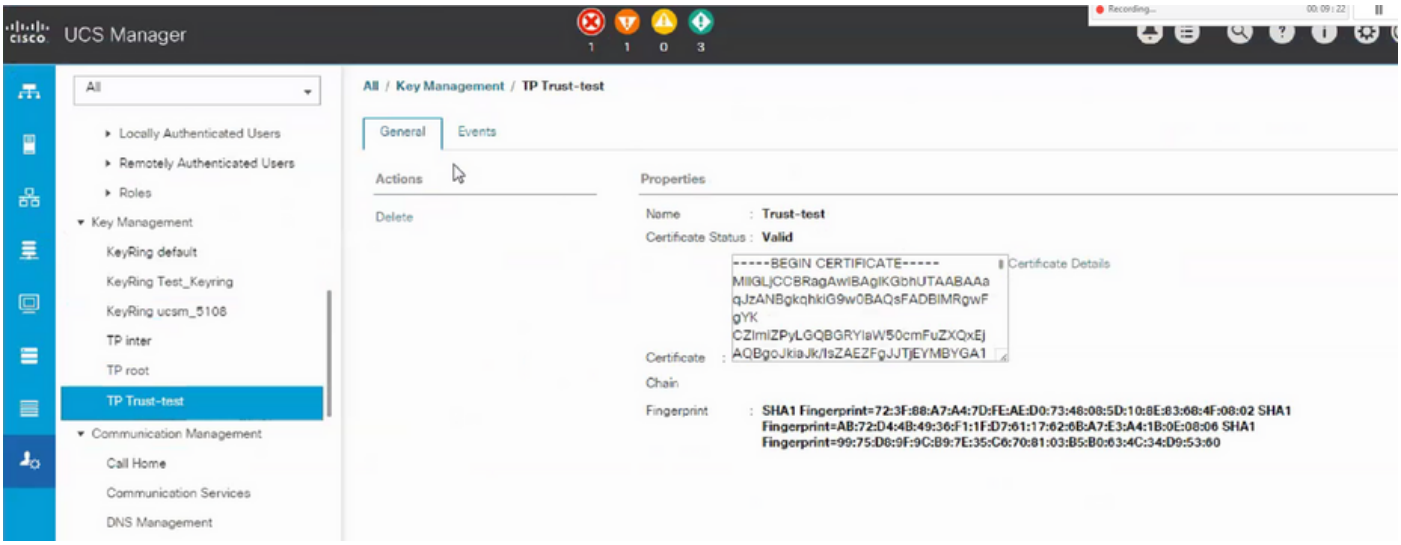
Stap 2

- De gedownloade certificaatketen is in PB7-formaat.

- Converteer het .pb7 bestand naar PEM formaat met OpenSSL tool.
- Bijvoorbeeld, in Linux, kunt u deze opdracht in terminal uitvoeren om de conversie-openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem uit te voeren.

Stap 3

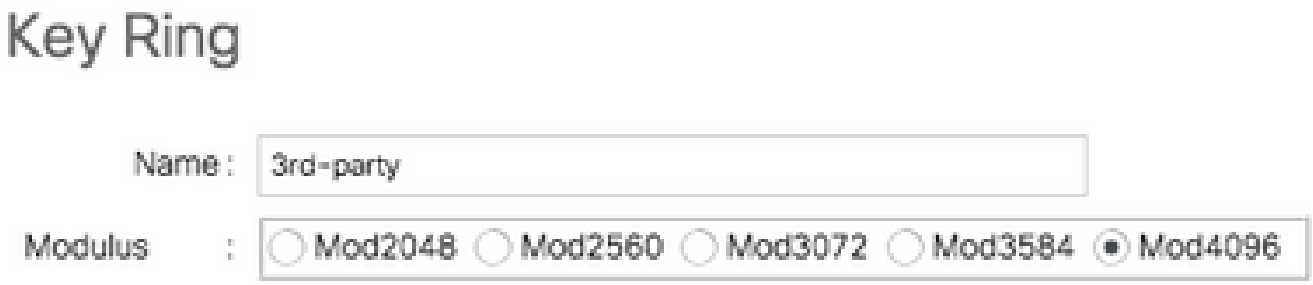
- Maak een Trust-Point op UCSM.
- Navigeer naar Beheer > Key Management > Trustpoint.
- Wanneer u het Vertrouwen-punt maakt, plakt u de volledige inhoud van het .PEM-bestand dat in stap 2 van deze sectie in de ruimte voor certificaatdetails is gemaakt.



Toetsenbord en MVO maken

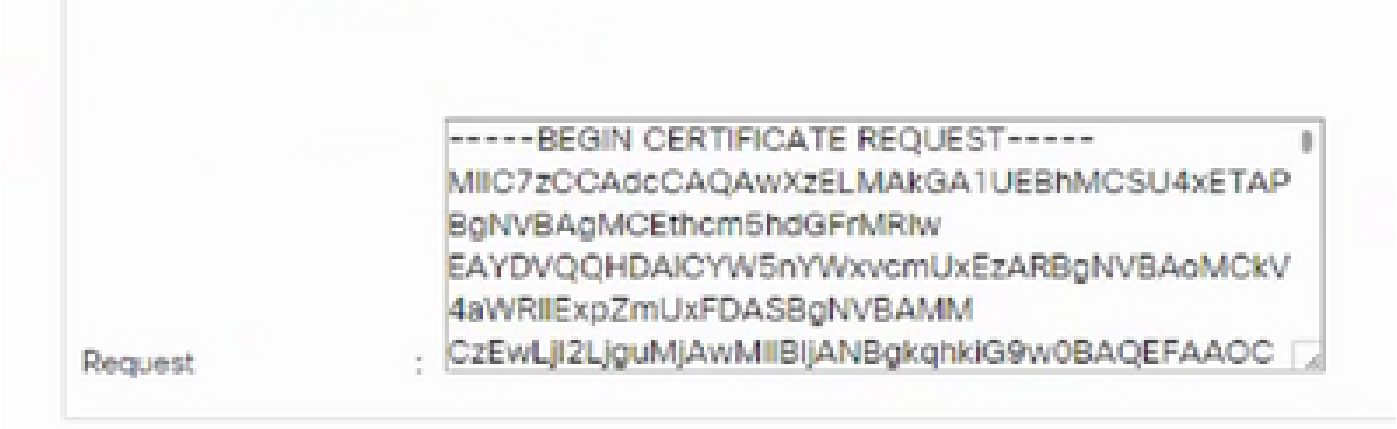
Stap 1

- Navigeer naar UCSM > Beheer > Toetsenbeheer > Toetsenbord.
- Kies de Modulus die nodig is voor het certificaat van de derde partij.



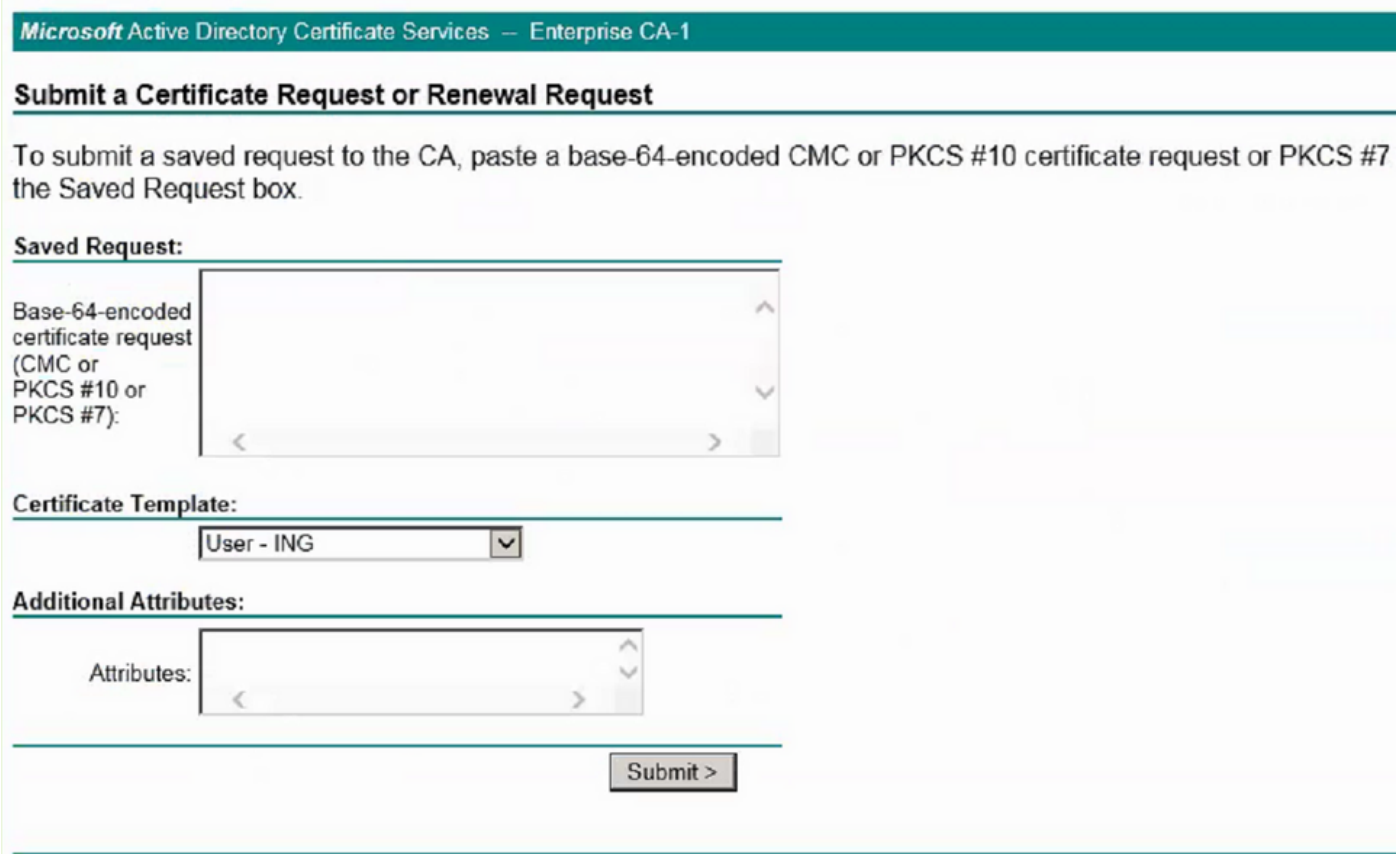
Stap 2

- Klik op certificaataanvraag maken en vul de gevraagde gegevens in.
- Kopieert de inhoud van het verzoekveld.



Stap 3

Om het certificaat te genereren, plakt u de gekopieerde aanvraag uit stap 2 in de onderstaande ruimte:



Stap 4

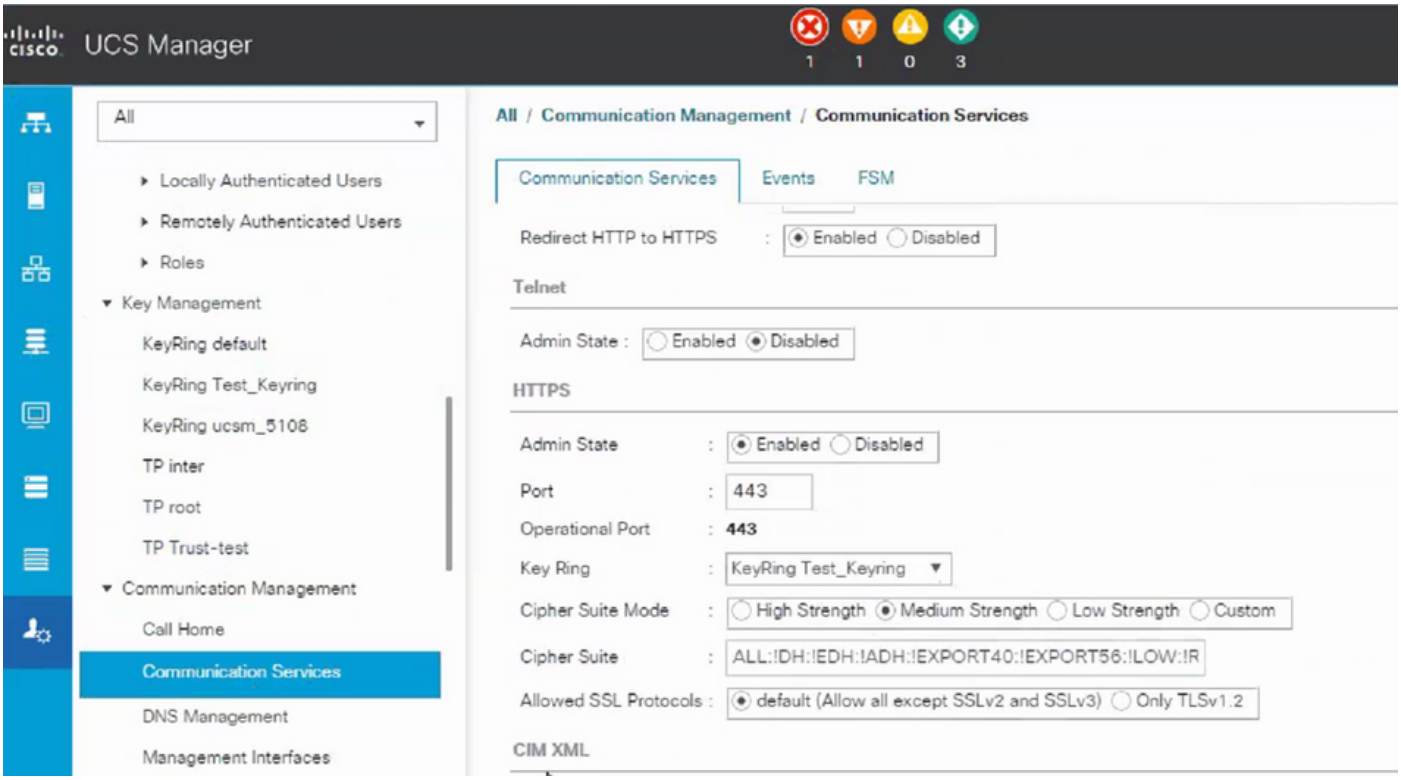
- Zodra ingediend, wordt een nieuw certificaat gegenereerd. Open het bestand en kopieer alle inhoud van het nieuwe certificaat in het veld Certificaat op de sleutelring die in stap 1 van deze sectie is gemaakt.

- Kies het vertrouwenspunt uit de vervolgkeuzelijst die is gemaakt in stap 3 van Create Keyring en CSR.

De sleutelring toepassen

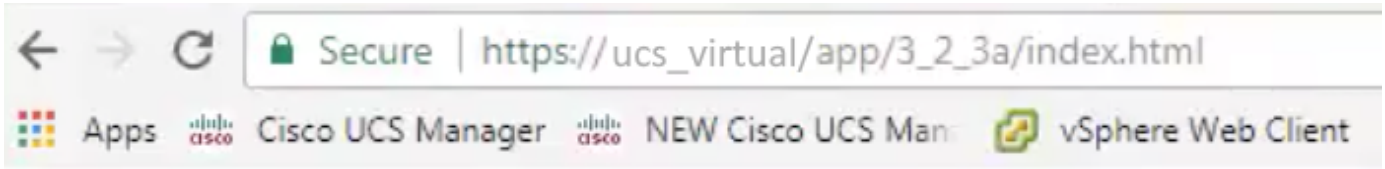
Stap 1

Kies de aangelegde sleutelring in de communicatiediensten zoals hieronder getoond:



Na de wijziging in de sleutelring wordt de HTTPS-verbinding met de UCSM in uw webbrowser even veilig weergegeven.

Opmerking: hiervoor moet het lokale bureaublad ook het certificaat van dezelfde CA-autoriteit gebruiken als de UCSM.



Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems]

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.