Secure Access ZTNA Auto Enrollment configureren

Inhoud

Inleiding

In dit document worden de vereiste stappen beschreven voor het configureren van de ZTNA voor automatische inschrijving op basis van certificaten.

Voorwaarden

- Secure Client minimum versie 5.1.9.x

- Trusted Platform Module (TPM) voor Windows

- Secure Enclave coprocessor voor Apple apparaten

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Access
- Apparaten inschrijven in de sectie Zero Trust Access Using Certificate Guide

Gebruikte componenten

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

- Windows 11 met TPM versie 2.0
- Secure Client versie 5.1.10.17 met ZTNA en DUO-module ingeschakeld.
- Microsoft Active Directory 2022
- OpenSSL-tool voor het genereren van certificaten

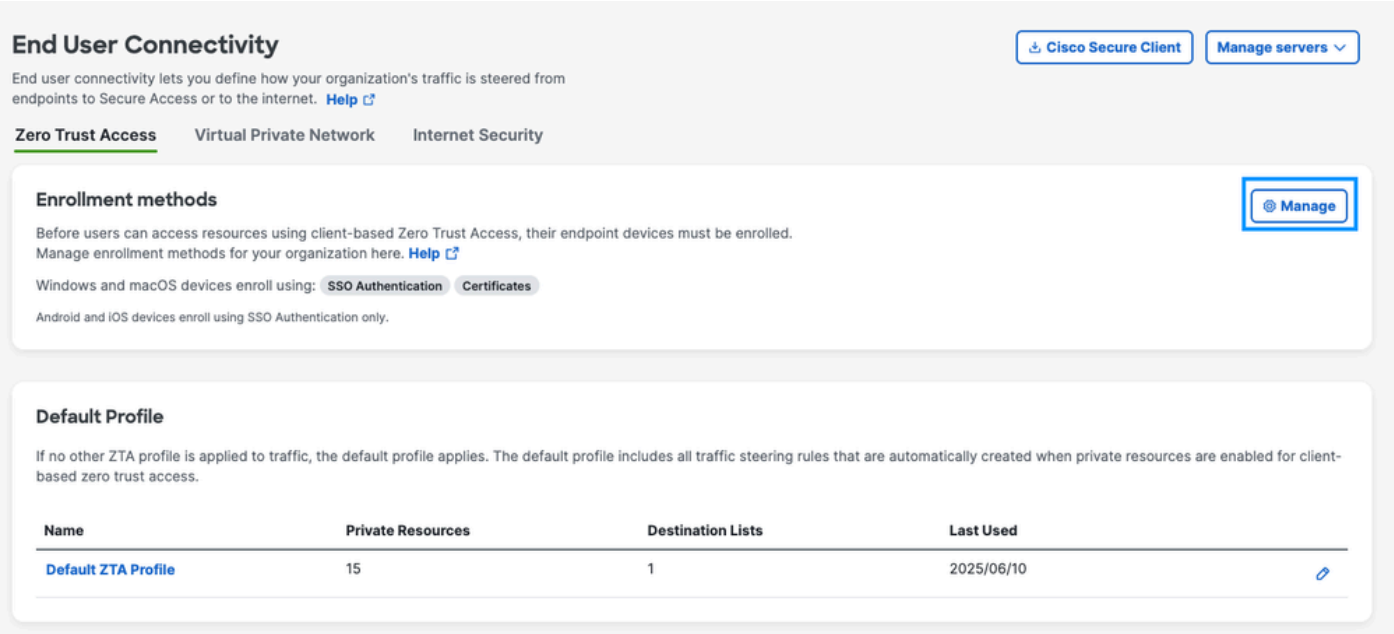
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Automatische inschrijving inschakelen op dashboard voor beveiligde toegang

De eerste stap bij het inschakelen van deze functie is het inschakelen van de functie voor automatische inschrijving voor beveiligde toegang, die het volgende omvat:

1. Navigeer naar Dashboard -> Verbinden -> Connectiviteit voor eindgebruikers -> Geen vertrouwen

2. Klik op de optie Beheren.



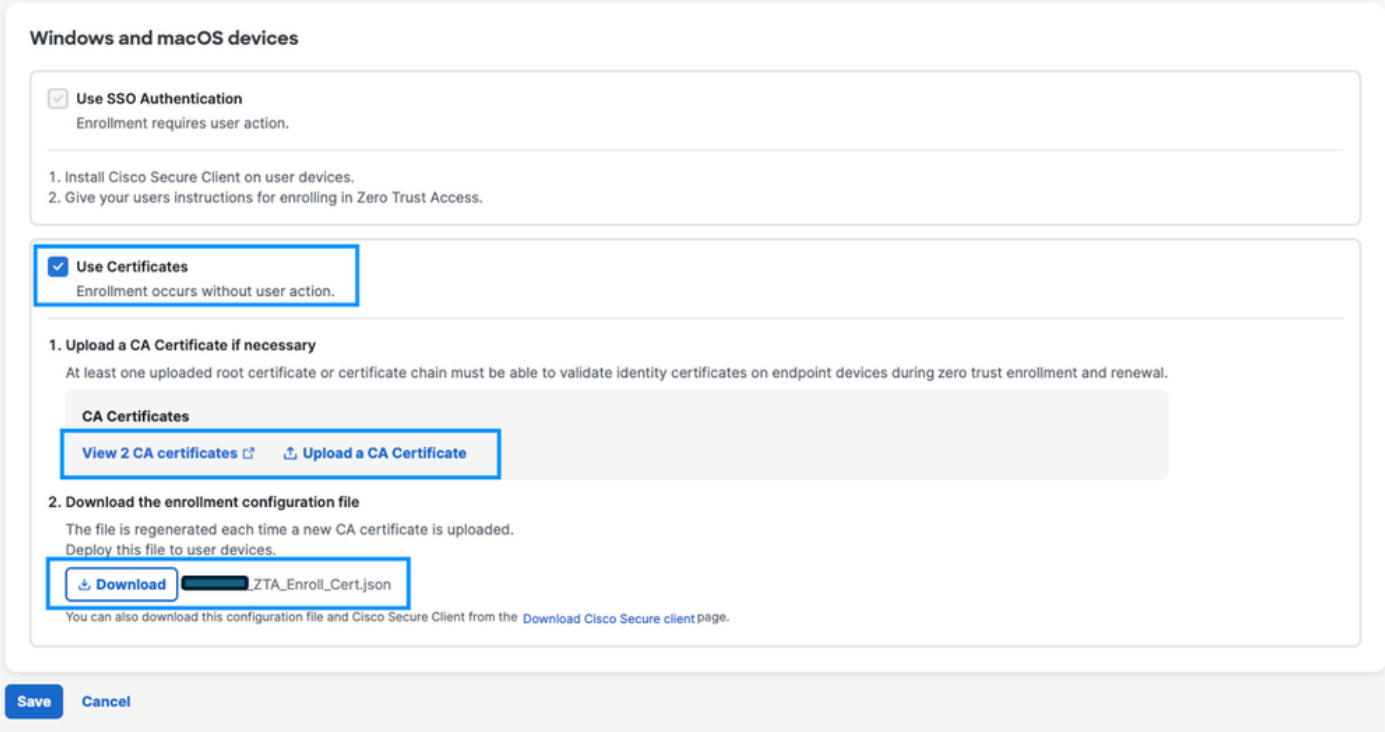
3. Gebruik van certificaten inschakelen.

4. Upload CA-certificaat door het te downloaden van uw lokale certificeringsinstantie.

5. Download de inschrijvingsconfiguratie en plaats deze in de mappen op basis van het besturingssysteem.

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices
- macOS: /opt/cisco/secureclient/zta/enrollment_choices

6. Zorg ervoor dat u uw instellingen opslaat zodra deze zijn voltooid.



Certificaatsjabloon en installatie

Veilige toegang vereist de volgende verplichte certificaatvelden:

- Alternatieve naam van het onderwerp (SAN) om het e-mailadres van de klacht van de gebruiker RFC-822 of de naam van het gebruikersbeginsel (UPN) op te nemen

Voorbeeld:

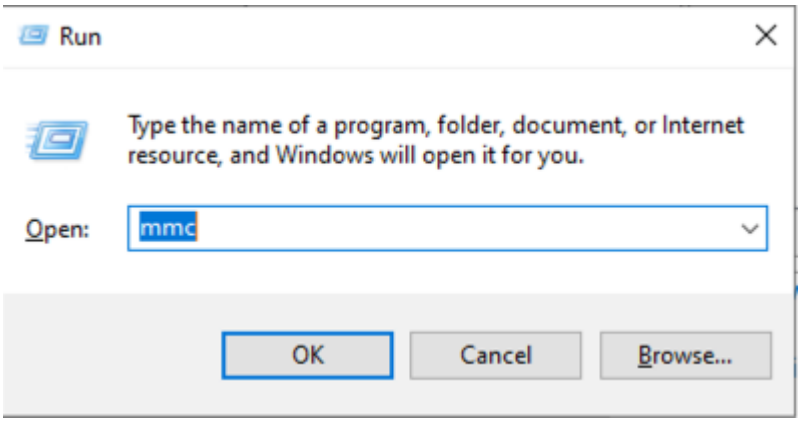
Optie 1: e-mail die voldoet aan RFC822
E-mail.1 = username@domain.local

Optie 2: (alternatief): UPN (Microsoft-specifiek)
otherName: 1.3.6.1.4.1.311.20.2.3; UTF8:username@domain.local

In dit voorbeeld gebruiken we de sjabloon voor gebruikerscertificaten in Microsoft AD om het certificaat te genereren.

Stap 1: Navigeer naar Microsoft AD en open Certificate Manager

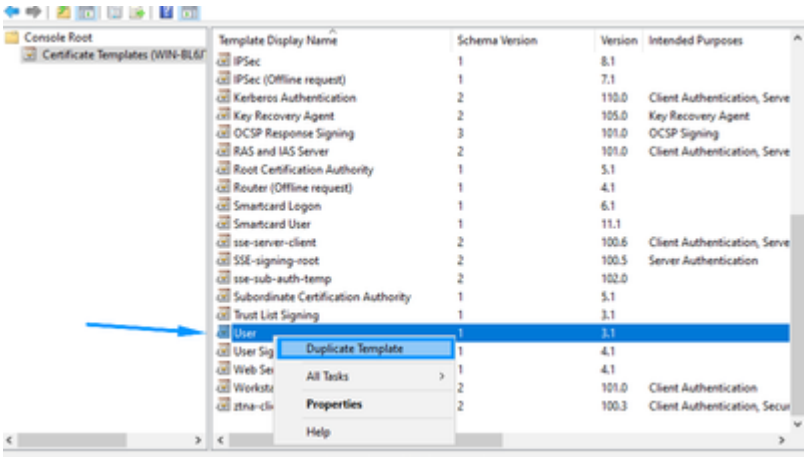
Stap 2: Open Run en voer Microsoft Management Console (mmc) in



Stap 3: Klik op Bestand en voeg Snap-in toe/verwijder

Stap 4: Certificaatsjablonen toevoegen

Stap 5: Gebruikerscertificaat dupliceren



Stap 6: Configureer de instellingen zoals beschreven

1. Nieuwe naam sjabloon: ztna-client-enroll onder (Algemeen) tabblad.

2. Selecteer (Leveren in het verzoek) op het tabblad (Onderwerpnaam).

Opmerking: Dit zorgt ervoor dat de opties die worden geboden door de openssl-sjabloon, zoals alternatieve naam voor service (SAN), worden geaccepteerd

---

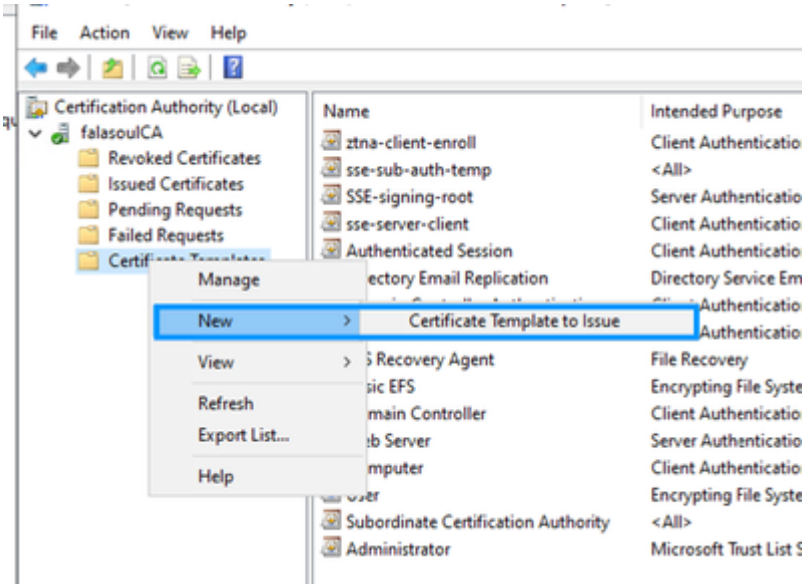
Stap 7: Klik op OK om de nieuwe template op te slaan

Stap 8: Voeg de nieuwe template toe aan de lijst met advertentiesjablonen door te doen:

1. Start certsrv.msc

2. Klik met de rechtermuisknop op Certificaatsjablonen en selecteer Nieuw -> certificaatsjabloon om uit te geven

3. Selecteer uw nieuw gemaakte sjabloon (ztna-client-enroll)



Certificaat maken met OpenSSL

Stap 1: san.cnf-bestand met inhoud maken

```
[ req ]
default_bits       = 2048
prompt             = no
default_md         = sha256
distinguished_name = dn
req_extensions     = req_ext

[ dn ]
C  = US
ST = Texas
L  = Austin
O  = exampleusername
OU = IT
CN = exampleusername

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
# Option 1: RFC822-compliant email
email.1 = user@domain.local

# Option 2 (alternative): UPN (Microsoft-specific)
#otherName:1.3.6.1.4.1.311.20.2.3;UTF8:user@domain.local
```

Stap 2: certificaat maken met behulp van de sjabloon

```
openssl genrsa -out user.key 2048
```

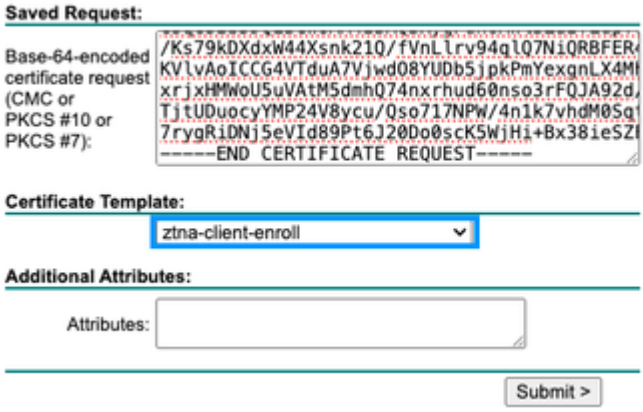
```
openssl req -new -key user.key -out user.csr
openssl req -new -key user.key -out user.csr -config san.cnf
```

Gebruikerscertificaat ondertekenen met CA ZTNA-sjabloon

Stap 1: Kopieer de inhoud van het bestand user.csr

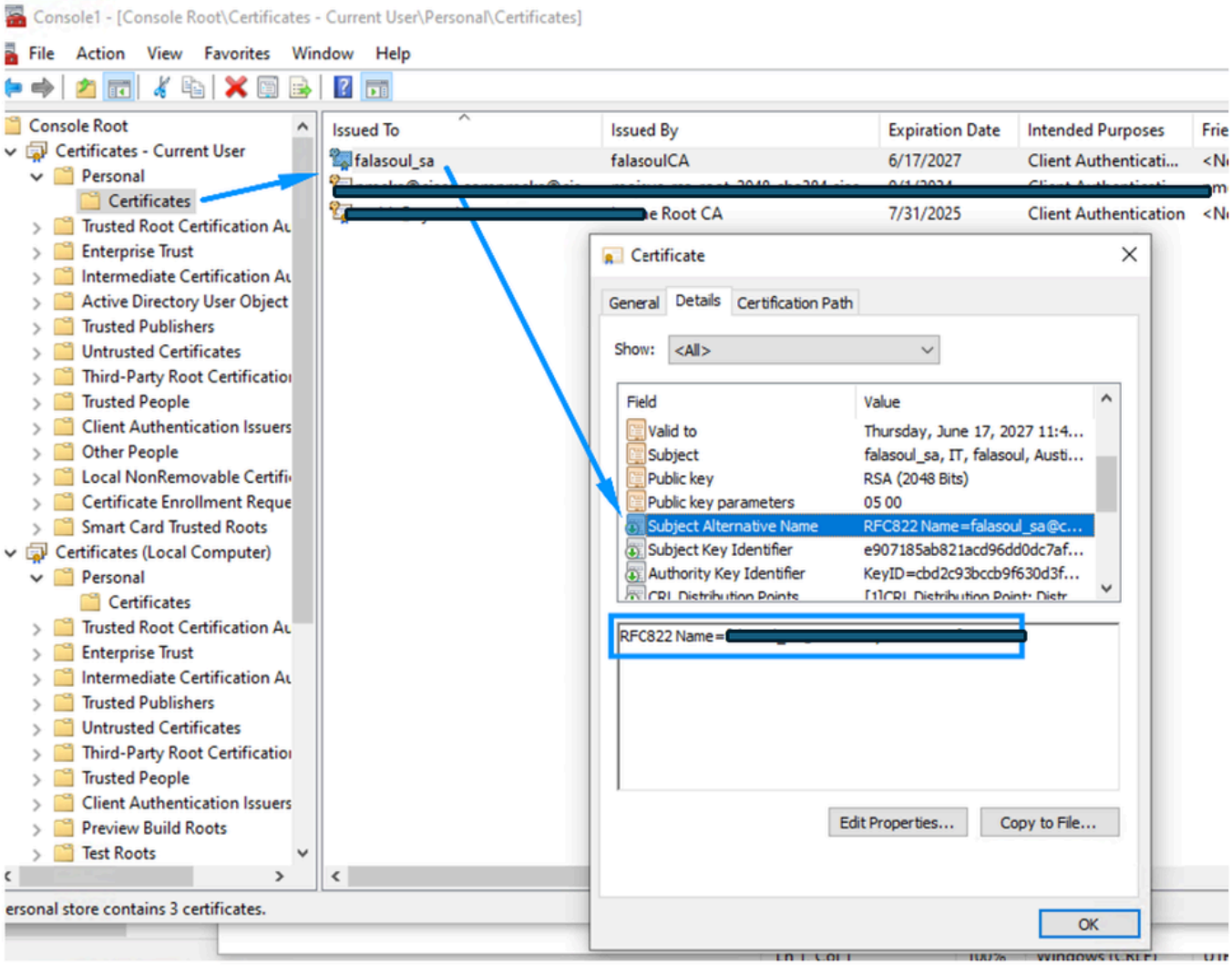
Stap 2: ga naar uw lokale AD ondertekening autoriteit (https: http://<ip-address>/certsrv/)

Stap 3: Klik op Certificaat aanvragen -> Geavanceerd certificaatverzoek -> selecteer ztna-client-enroll template



Stap 4: Download het certificaat in Base64-formaat en installeer het in het persoonlijke vertrouwde winkelcertificaat van de gebruiker.

Stap 5: Bevestig dat de juiste informatie in het certificaat aanwezig is

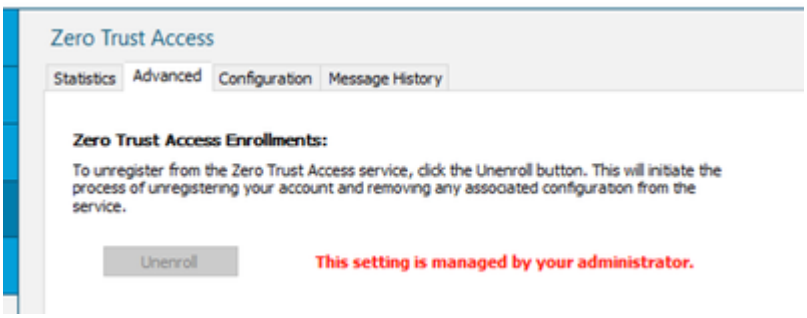


Stap 6: Start uw ZTNA-module opnieuw op zodat de inschrijving kan beginnen

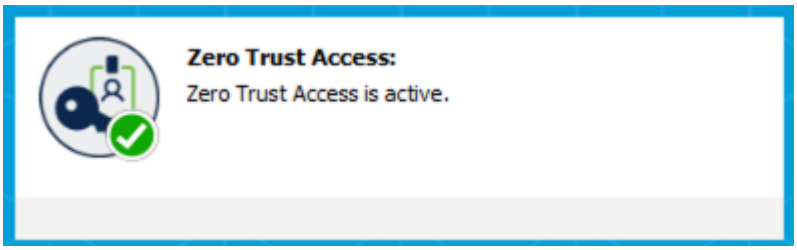
Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

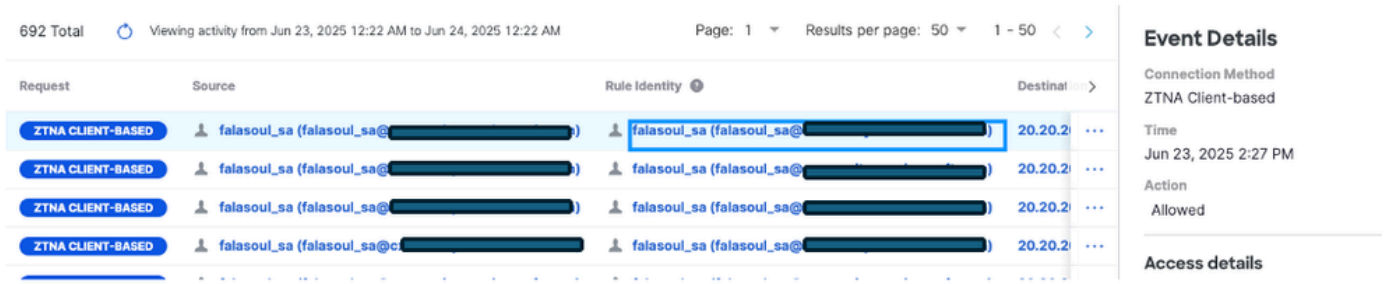
Stap 1: ZTNA-modulebericht bij het configureren van het inschrijvingskeuzebestand:



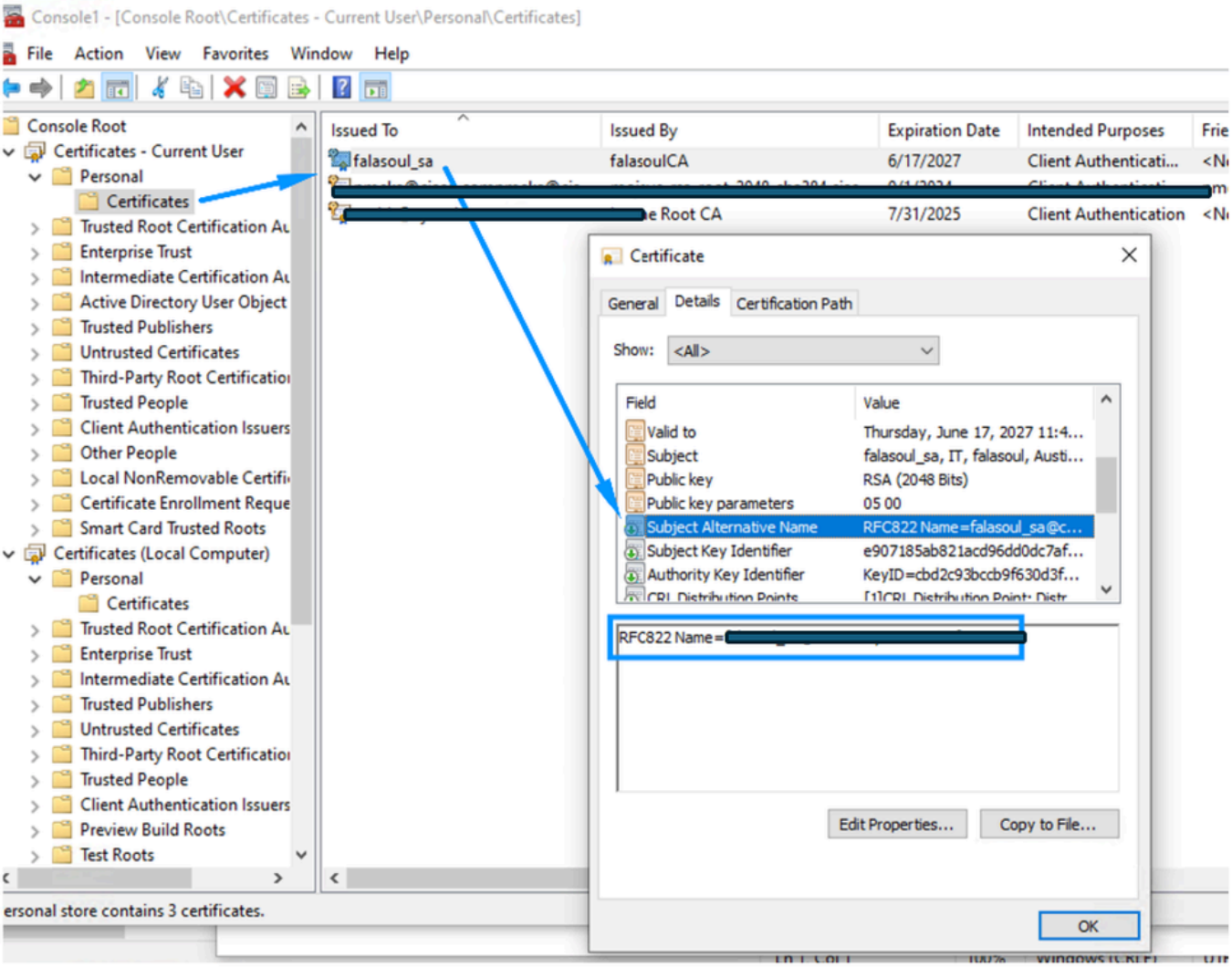
Stap 2: Nadat u de ZTNA-module voor de eerste keer opnieuw hebt gestart, kunt u zien dat u automatisch bent ingeschreven voor ZTNA



Stap 3: Controleer de juiste gebruiker die wordt weergegeven in de zoekactiviteit op basis van de SAN-informatie



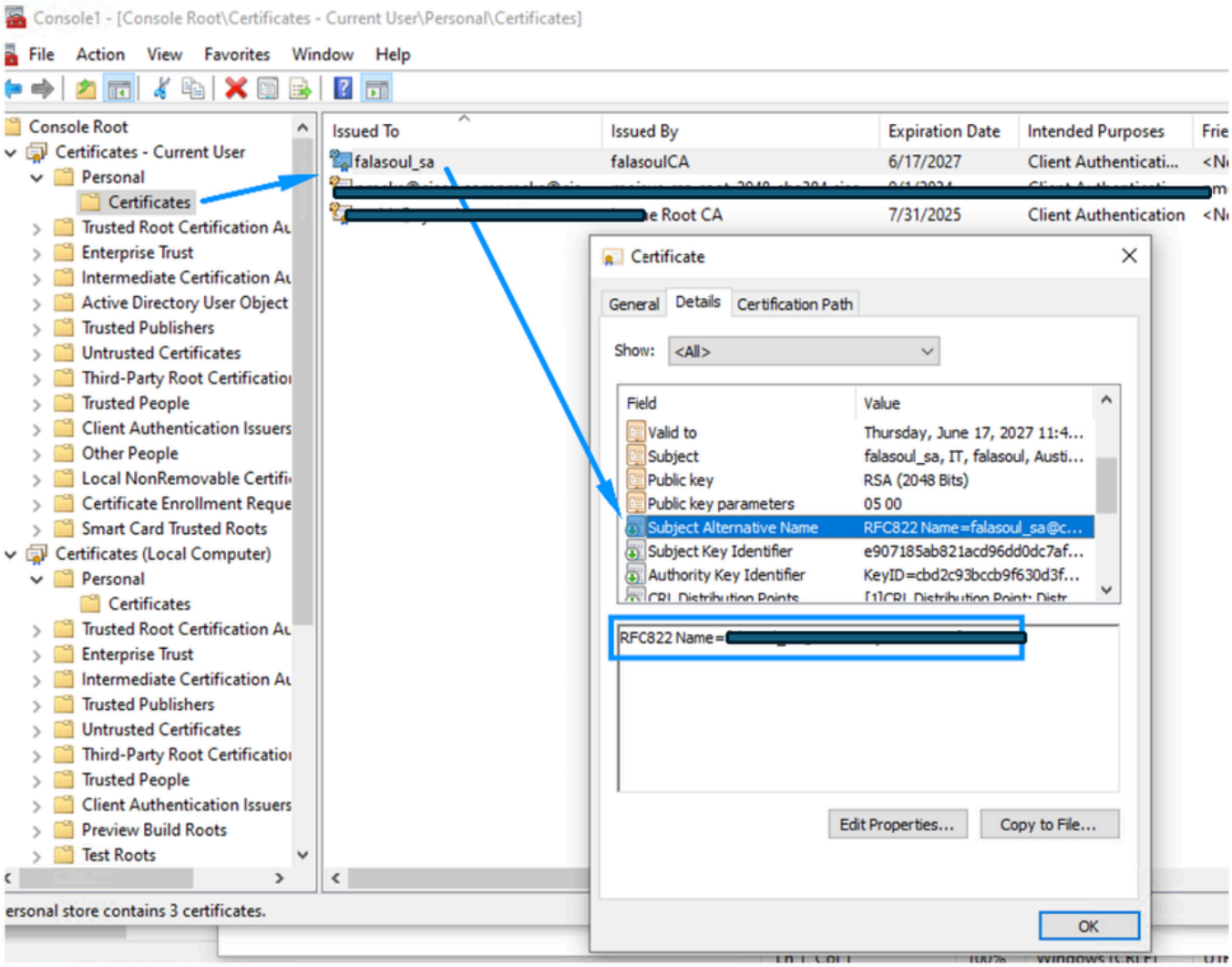
Stap 4: Bevestig dat de juiste informatie in het certificaat aanwezig is



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Stap 1: Bevestig dat de juiste informatie in het certificaat aanwezig is en dat de juiste informatie in het juiste certificaatarchief is geïnstalleerd.



Stap 2: Bevestig dat inschrijving niet tekortschiet op certificaatvereisten met behulp van DART

Stap 3: Bevestig dat u in staat bent om uw FTD-buiteninterface goed op te lossen als UZTNA wordt gebruikt.

Veelvoorkomende fout:

```
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ AppSocketTransport.cpp:231 AppSocke
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] I/ TcpTransport.cpp:114 TcpTransport::
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.610238 csc_zta_agent[0x00001638, 0x00000e58] T/ TcpTransport.cpp:150 TcpTransport::
2025-06-16 05:44:45.610238 csc_zta_agent[0x00001638, 0x00000e58] E/ TcpTransport.cpp:166 TcpTransport::
```

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.