Installeer een CA-certificaat van derden in ISE 2.0

Inhoud

Inleiding

Dit document beschrijft de installatie van een CA-ondertekend certificaat van derden in Cisco Identity Services Engine (ISE). Dit proces is hetzelfde ongeacht de uiteindelijke certificeringsrol (EAP-verificatie, Portal, Admin en PxGrid).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Basisinfrastructuur van de Openbare Sleutel.

Gebruikte componenten

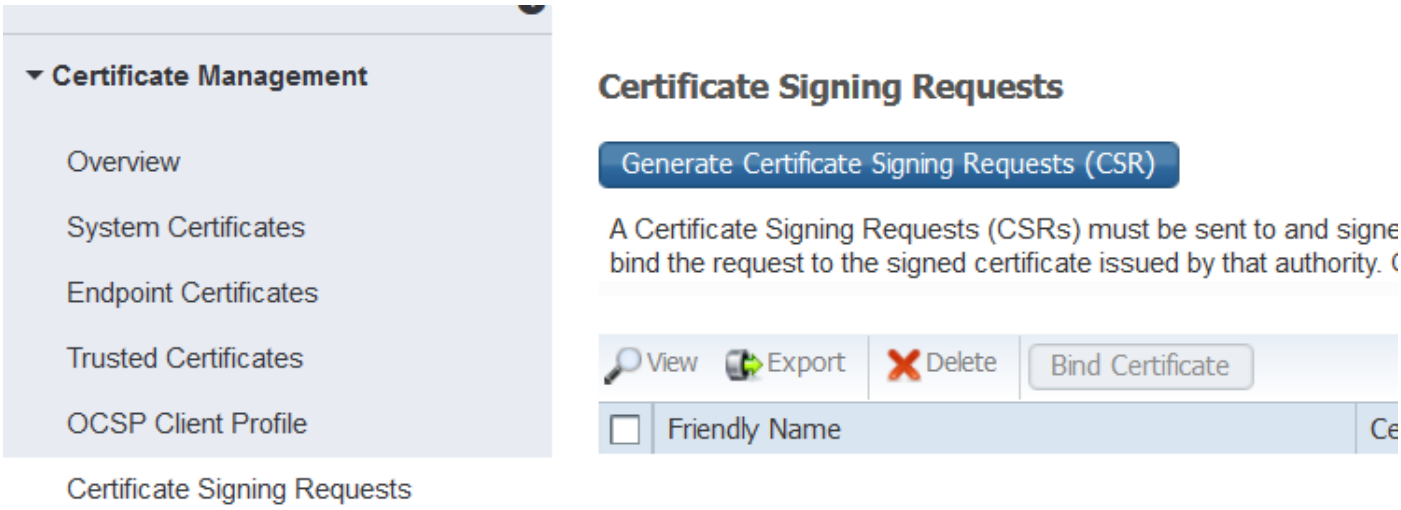
De informatie in dit document is gebaseerd op Cisco Identity Services Engine (ISE) release 2.0. Dezelfde configuratie is van toepassing op de releases 12.3 en 1.4.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap 1. Generate certificaataanvraag (CSR).

Om de CSR te genereren, navigeer dan naar **Administratie > Certificaten > Aanvragen van certificaatsignalering** en klik op **Aanvragen van** certificaatsignalering **genereren** (CSR).



1. Selecteer onder het gedeelte Gebruik de rol die u wilt gebruiken in het vervolgkeuzemenu. Als het certificaat wordt gebruikt voor meerdere rollen, kunt u Meervoudig gebruik selecteren. Zodra het certificaat is gegenereerd kunnen de rollen indien nodig worden gewijzigd.

2. Selecteer het knooppunt waarvoor het certificaat wordt gegenereerd.

3. Vul de vereiste informatie in (organisatie-eenheid, organisatie, stad, staat en land).

   Opmerking: Onder Common Name (CN) - veld ISE vult de Full Qualified Domain Name (FQDN) van het knooppunt automatisch in.

Wildcards:

- Als het doel is om een certificaat met jokerteken te genereren, controleer dan het vakje **Wildcard Certificaten toestaan**.

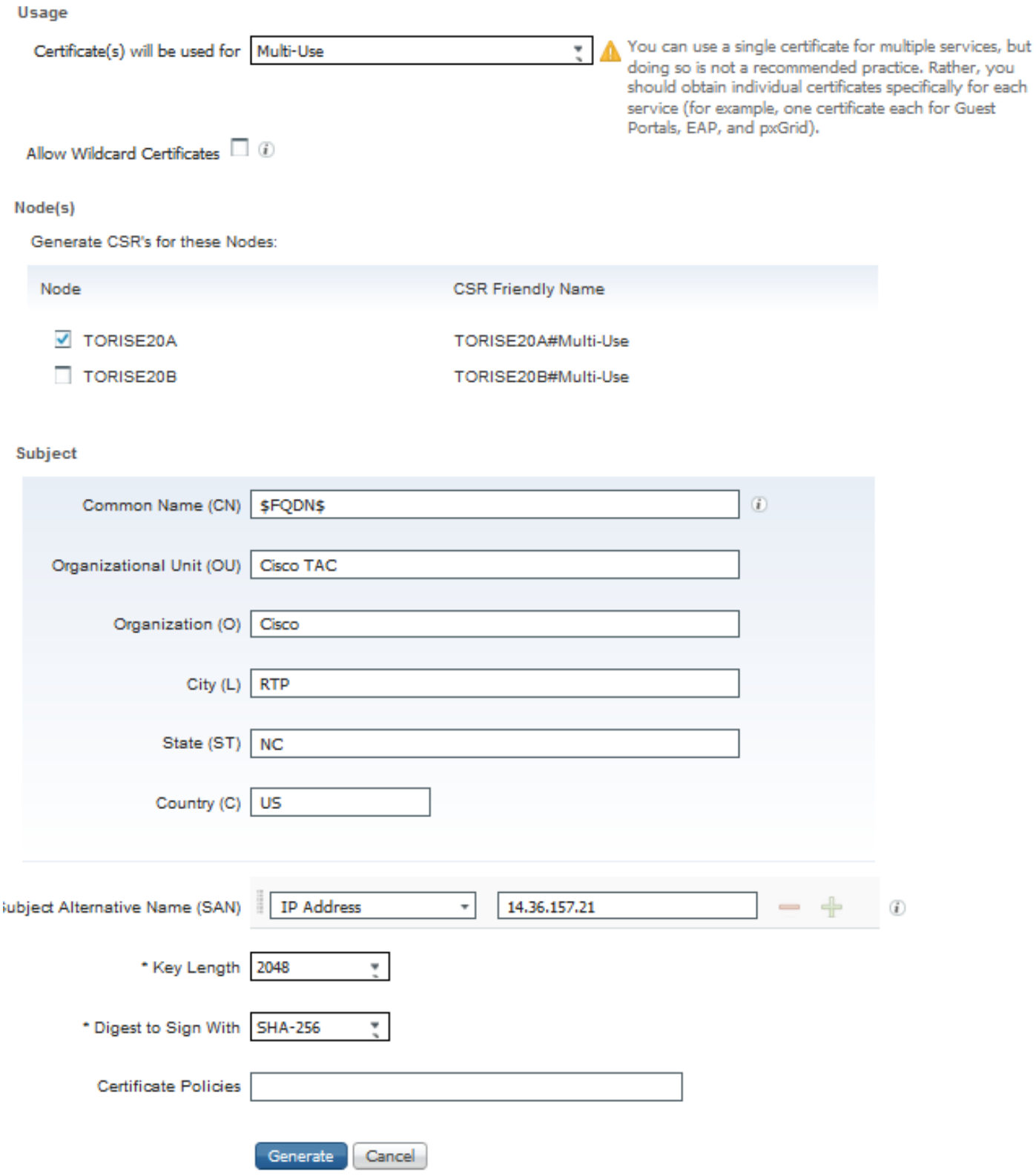
- Indien het certificaat wordt gebruikt voor MAP-authenticaties, mag het*****-symbool niet in het veld Onderwerp GN worden aangebracht, aangezien Windows-aanvragers het servercertificaat afwijzen.

- Zelfs wanneer **Validering Server Identity** op de aanvrager uitgeschakeld is, kan de SSL-handdruk falen wanneer de ***** in het GN-veld staat.

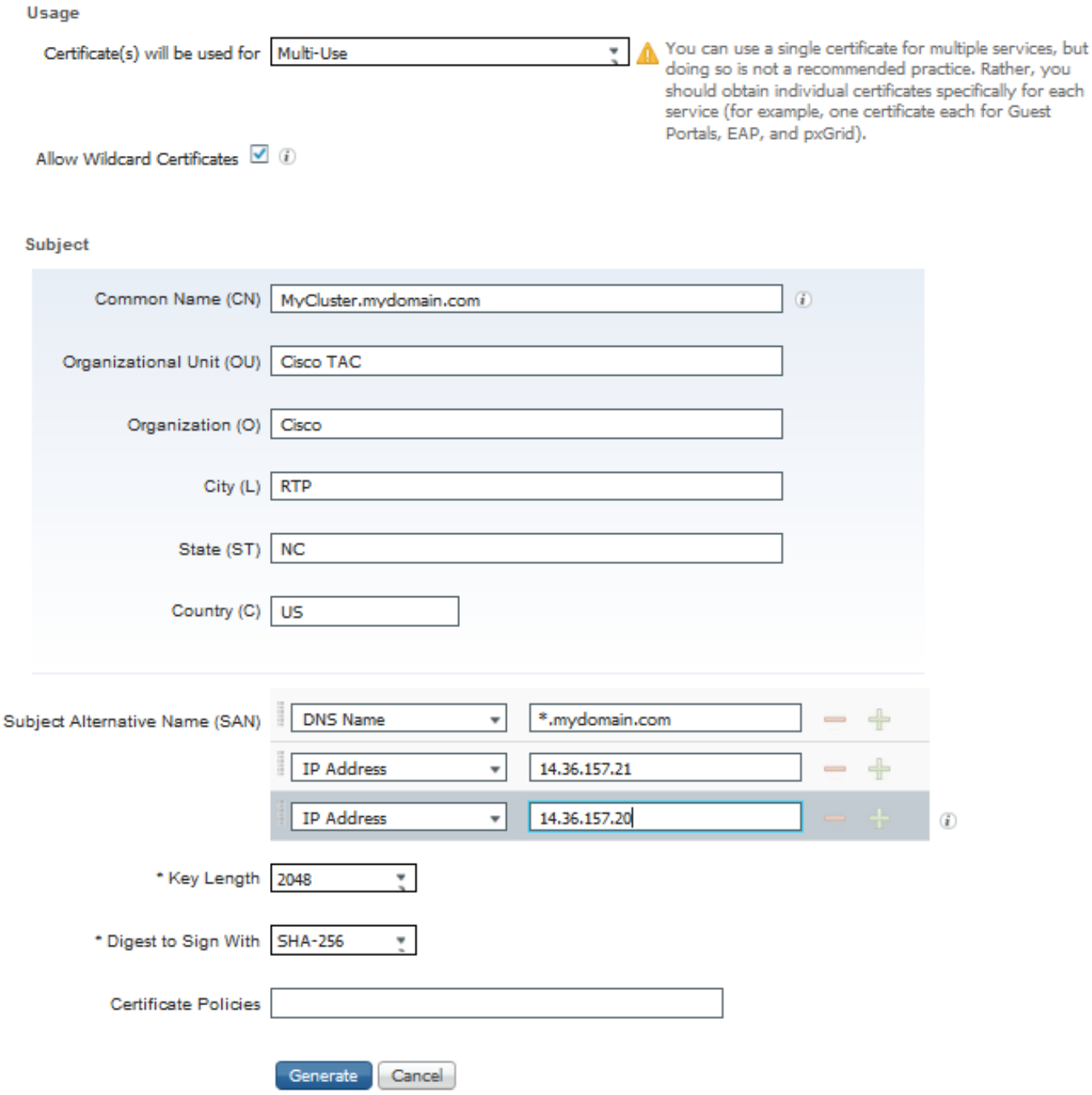
- In plaats daarvan kan een generieke FQDN in het GN-veld worden gebruikt, en vervolgens kan het ***.domain.com** worden gebruikt in het veld Naam Onderwerp Alternative Name (SAN) DNS Name.

  Opmerking: Sommige certificaatinstanties (CA) kunnen de wildkaart (*) automatisch toevoegen aan de GN van het certificaat, zelfs als deze niet in het CSR aanwezig is. In dit geval is een speciaal verzoek vereist om deze actie te voorkomen.

Individueel servercertificaat CSR voorbeeld:

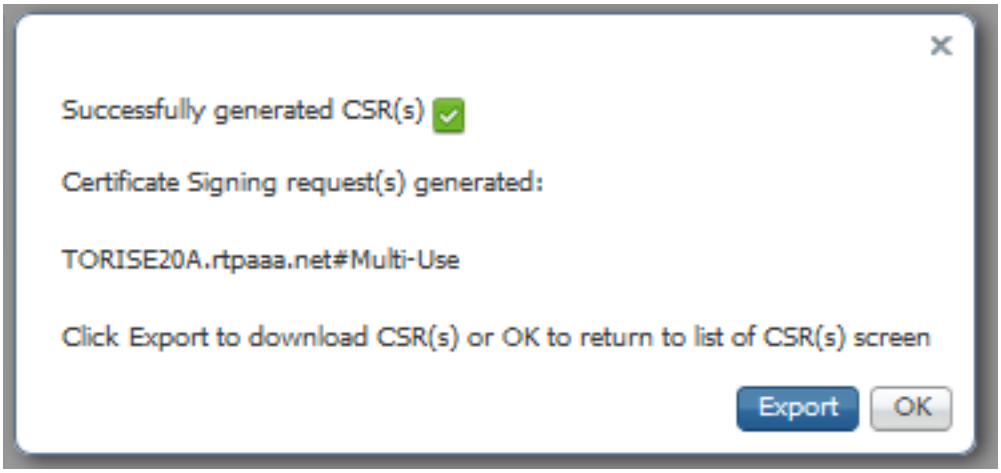


Voorbeeld van jokerteken CSR:



Opmerking: Het IP-adres van elk van de implementatieknooppunten kan aan het SAN-veld worden toegevoegd om een certificaatwaarschuwing te voorkomen wanneer u de server via het IP-adres benadert.

Zodra de CSR is gemaakt, geeft ISE een pop-upvenster weer met de optie om deze te exporteren. Als dit bestand eenmaal geëxporteerd is, moet dit naar de CA worden verzonden voor het ondertekenen.



Stap 2. Voer een nieuwe certificaatketen in.

De certificaatinstantie geeft het ondertekende servercertificaat terug samen met de volledige ondertekeningsketen (Root/Intermediate). Nadat u de certificaten hebt ontvangen, volgt u de onderstaande stappen om deze in uw ISE-server te importeren.

1. Om alle door de CA verstrekte wortelcertificaten en (of) certificaten via tussenweg in te voeren, navigeer dan naar **Administratie > Certificaten > Vertrouwde certificaten**.

2. Als u het servercertificaat wilt importeren, navigeer dan naar **Administratie > Certificaten > Aanvragen voor certificaatsignalering**.

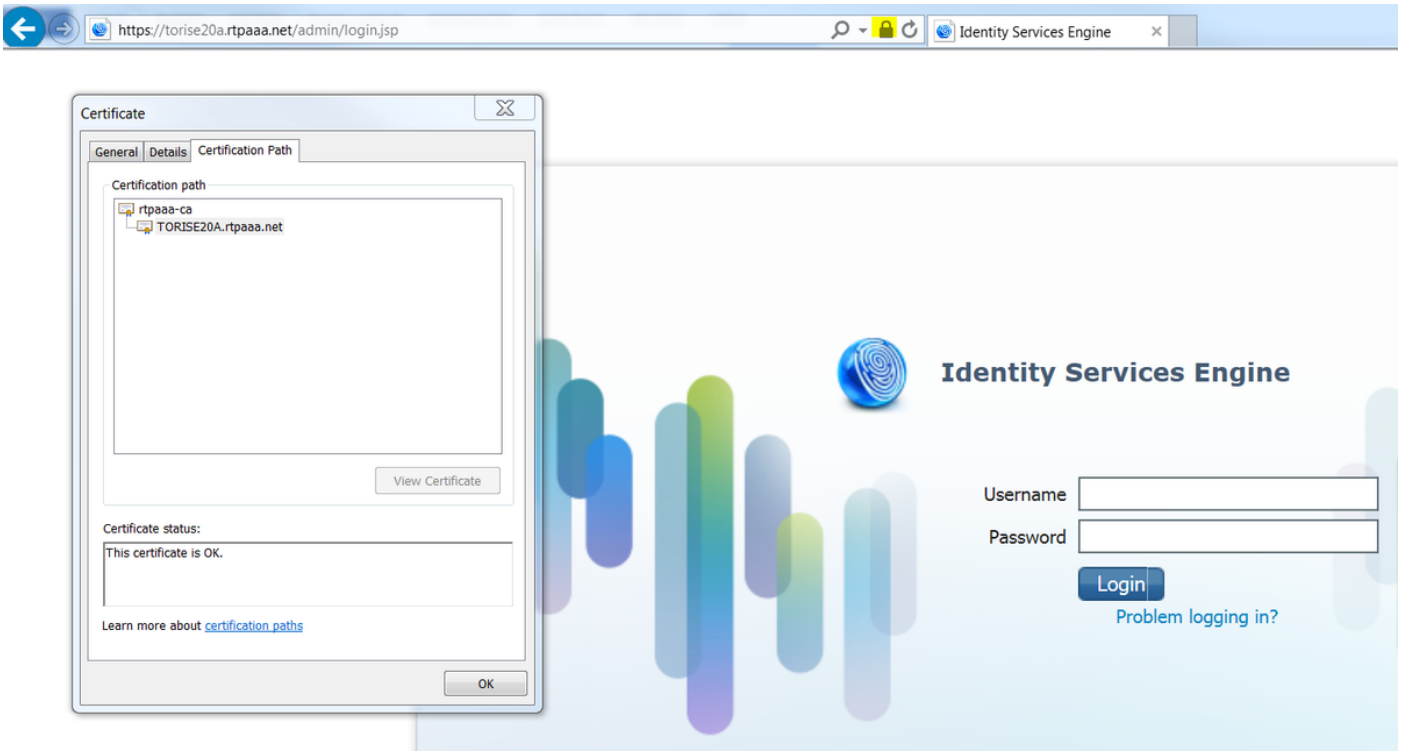
3. Selecteer de CSR die eerder is gemaakt en klik op **Bind-certificaat**.

4. Selecteer de nieuwe certificaatlocatie en ISE bindt het certificaat aan de privé sleutel die in de database gecreëerd en opgeslagen wordt.

   Opmerking: Als de Admin Rol voor dit certificaat is geselecteerd, start ISE de services opnieuw.

Verifiëren

Als de admin-rol is geselecteerd tijdens de certificaatinvoer, kunt u controleren of het nieuwe certificaat is geïnstalleerd door de admin-pagina in de browser te laden. De browser dient het nieuwe admin certificaat te vertrouwen zolang de keten correct gebouwd is en als de certificeringsketen door de browser wordt vertrouwd.



Selecteer voor extra verificatie het symbool van het slot in de browser en controleer of de volledige keten aanwezig is en betrouwbaar is in de machine. Dit is geen directe indicator dat de volledige keten correct door de server werd doorgegeven maar een indicator van de browser die het servercertificaat kan vertrouwen op basis van zijn lokale vertrouwenswinkel.

Problemen oplossen

Leverancier heeft geen vertrouwen in het ISE Local Server Certificate tijdens een dot1x-verificatie

Controleer of ISE tijdens het SSL-handschudproces de volledige certificatieketen passeert.

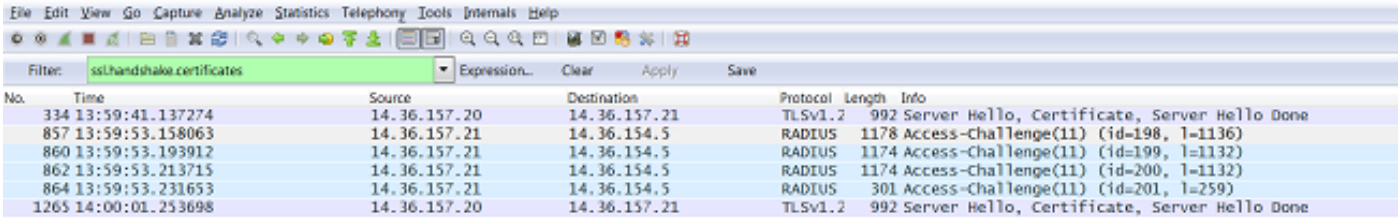
Bij het gebruik van MAP-methoden waarbij een servercertificaat (d.w.z. PEAP) vereist is en **de** naam **van de** bevestigde **serveridentiteit** wordt geselecteerd, bevestigt de aanvrager de certificeringsketen met behulp van de certificaten die hij in zijn lokale trustwinkel heeft als onderdeel van het verificatieproces. Als onderdeel van het SSL-handdrukproces presenteert ISE zijn certificaat en ook alle Root- en (of) intermediaire certificaten die in zijn keten aanwezig zijn. De aanvrager kan de serveridentiteit niet valideren als de keten niet volledig is. U kunt de volgende stappen uitvoeren om te controleren of de certificeringsketen naar uw client is teruggestuurd:

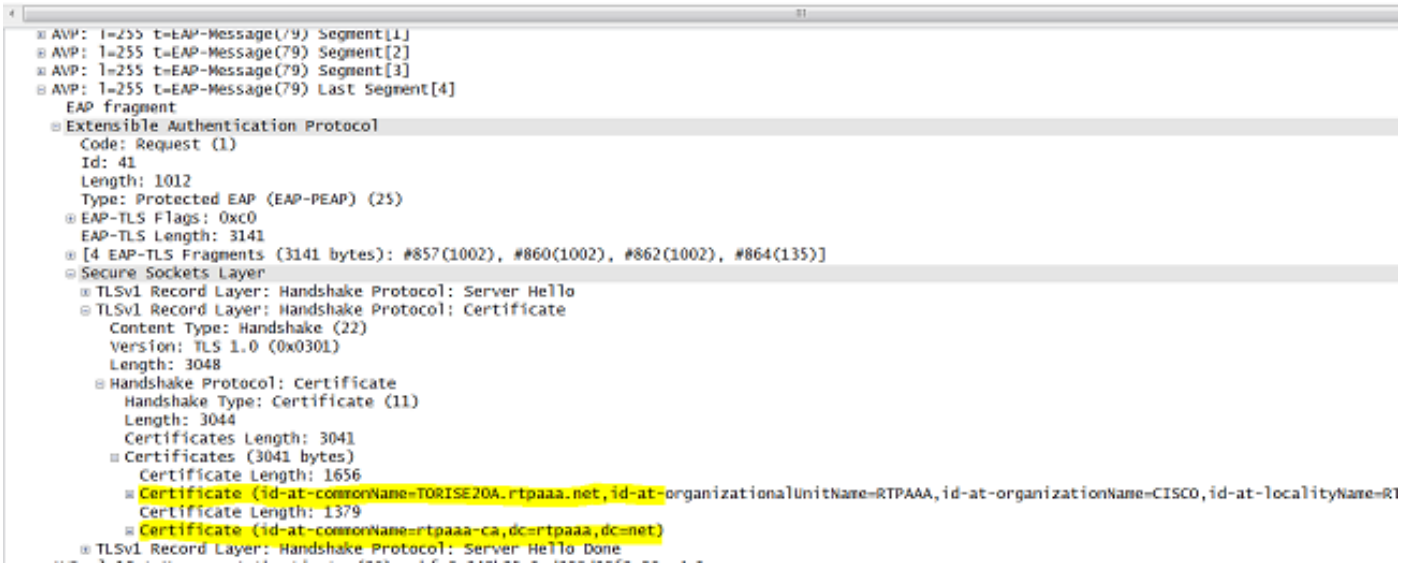
1. Om een opname van ISE (TCPDump) te nemen tijdens de authenticatie, navigeer naar **Operations > diagnostische tools > General Tools > TCP dump**.

2. Download/open de opname en pas het filter **toe.**sl.**handshake.certificaten** in Wireshark en vind een access-challenge.

3. Nadat u deze optie hebt geselecteerd, navigeer u om **Radius Protocol uit** te **vouwen > Waarde van kenmerken > EAP-Message Laatste segment > Extensible Authentication Protocol > Secure Socket Layer > Certificate > Certificates**.

certificaatketen in de opname.

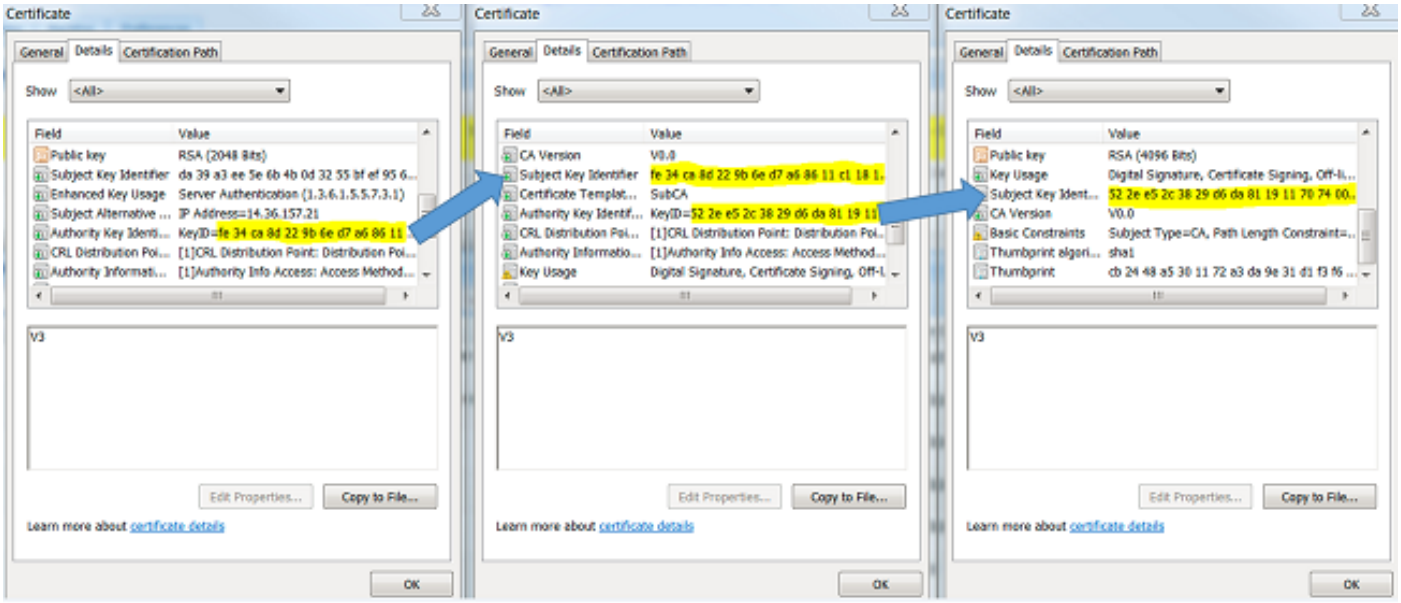




Als de ketting niet volledig is, navigeer dan naar **ISE-administratie > Certificaten > Trusted Certificates** en controleer of de Root en (of) Intermediate certificaten aanwezig zijn. Indien de certificeringsketen succesvol is doorlopen, moet de keten zelf als geldig worden gecontroleerd met behulp van de hier beschreven methode.

Open elk certificaat (server, intermediair en wortel) en controleer de vertrouwensketen door de onderwerpsleutel (SKI) van elk certificaat te koppelen aan de doorsnede van de Autoriteit (AKI) van het volgende certificaat in de keten.

Voorbeeld van een certificeringsketen.

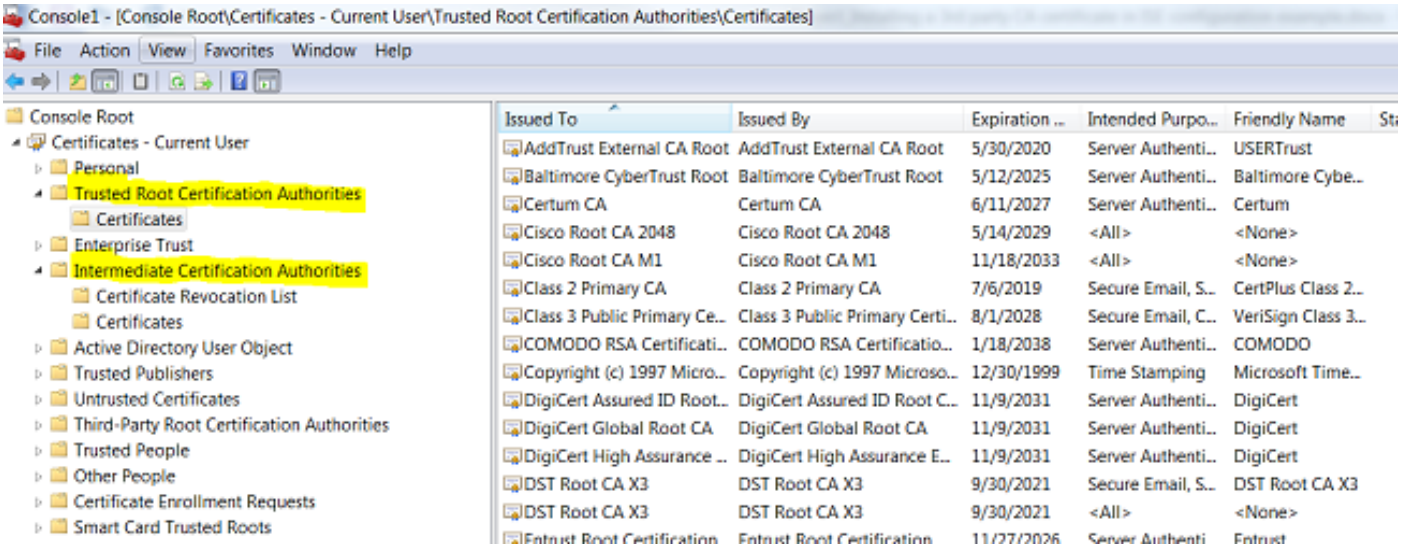


ISE certificaatketen is correct maar endpoint wijst ISE's servercertificaat tijdens verificatie af

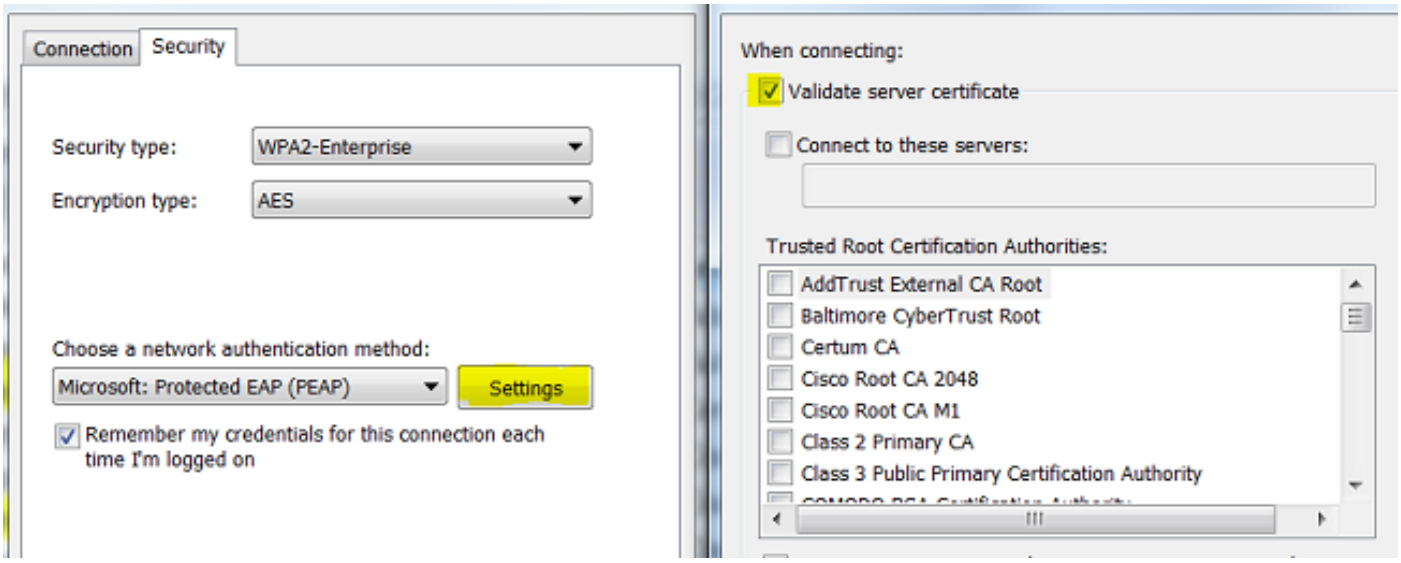
indien ISE tijdens de SSL-handdruk haar volledige certificatieketen presenteert en de aanvrager de certificeringsketen nog steeds afwijst; de volgende stap is te verifiëren dat de Root- en/of Intermediate-certificaten zich in de client Local Trust Store bevinden.

Om dit vanuit een Windows-apparaat te controleren, navigeer naar **mmc.exe File > Add-Remove Magnetisch-in**. Selecteer in de kolom Beschikbare invoegtoepassingen **Certificaten** en klik op **Toevoegen**. Selecteer **Mijn gebruikersaccount** of **computeraccount**, afhankelijk van het gebruikte verificatietype (gebruiker of machine), en klik vervolgens op **OK**.

Selecteer onder de console-weergave de **Trusted Root-certificeringsinstanties** en de **Intermediate Certified-certificeringsinstanties** om de aanwezigheid van een certificaat voor wortel en tussenkomst in de plaatselijke trustwinkel te controleren.



Een makkelijke manier om te controleren of dit een probleem is met de identiteitscontrole van de server, **valideren van het servercertificaat** uit te schakelen onder de configuratie van het flexibele profiel en het opnieuw testen.



> Opmerking: ISE ondersteunt momenteel geen verwerkingscertificaten die RSASSA-PSS als signatuur gebruiken. Dit omvat het servercertificaat, het certificaat Root, het certificaat Intermediate of client (d.w.z. EAP-TLS, PEAP (TLS) enz.). Raadpleeg CSCug22137 als insect.

Gerelateerde informatie

- Administrator-gids voor Cisco Identity Services Engine, release 2.0
- Technische ondersteuning en documentatie – Cisco Systems