Certificaat of smartcard-gebaseerde verificatie configureren voor ISE-beheer

Inhoud

Inleiding

In dit document wordt beschreven hoe u clientadapterverificatie op basis van certificaten voor de toegang tot Identity Services Engine (ISE) kunt configureren. In dit voorbeeld, authenticeert de ISE-beheerder aan de hand van het gebruikerscertificaat om Admin-toegang te verkrijgen tot de Cisco Identity Services Engine (ISE) Management GUI.

Voorwaarden

Vereisten

Cisco adviseert om kennis van deze onderwerpen te hebben:

- ISE-configuratie voor wachtwoord- en certificeringsverificatie.
- Microsoft Active Directory (AD)

Gebruikte componenten

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

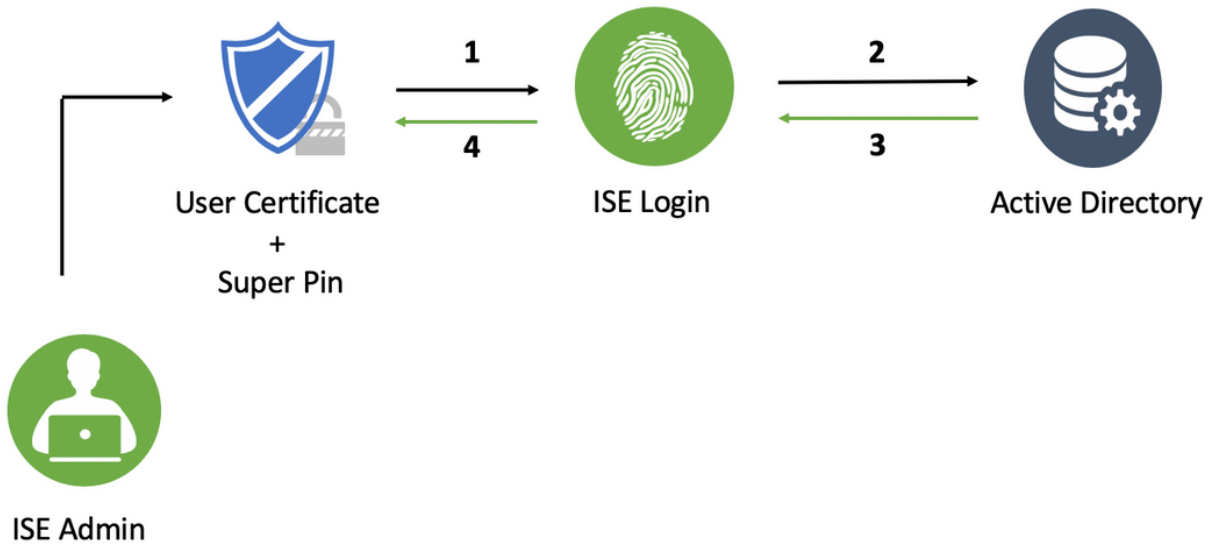
- Cisco Identity Services Engine (ISE) versie 2.6
- Windows Active Directory (AD) Server 2008 release 2
- Certificaat

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 het netwerk live is, zorg er dan voor dat u de mogelijke impact van elke configuratie begrijpt.

Configureren

Gebruik dit gedeelte om het clientcertificaat of de slimme kaart te configureren als een externe identiteit voor beheertoegang tot de Cisco ISE-beheerGUI.

Netwerkdiagram

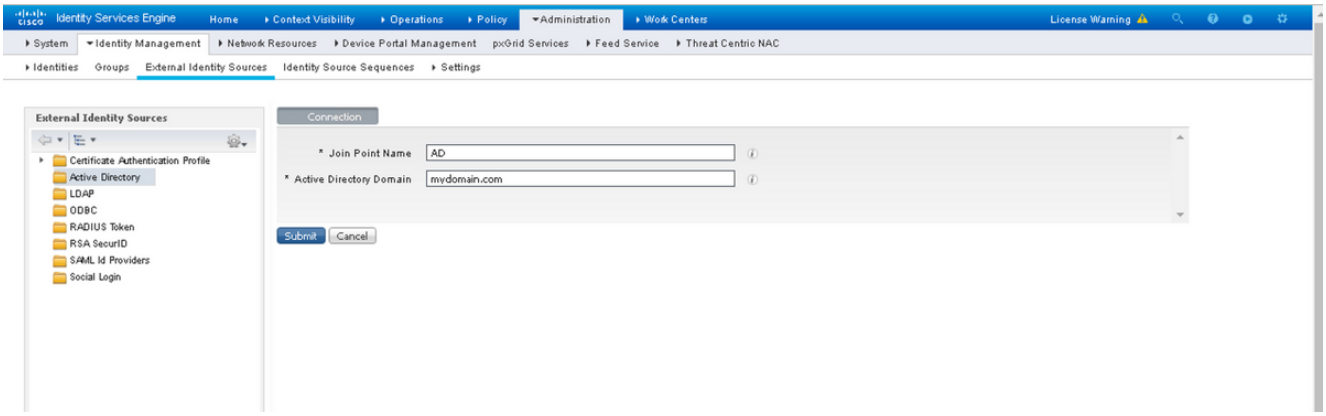


ISE samenvoegen in actieve map

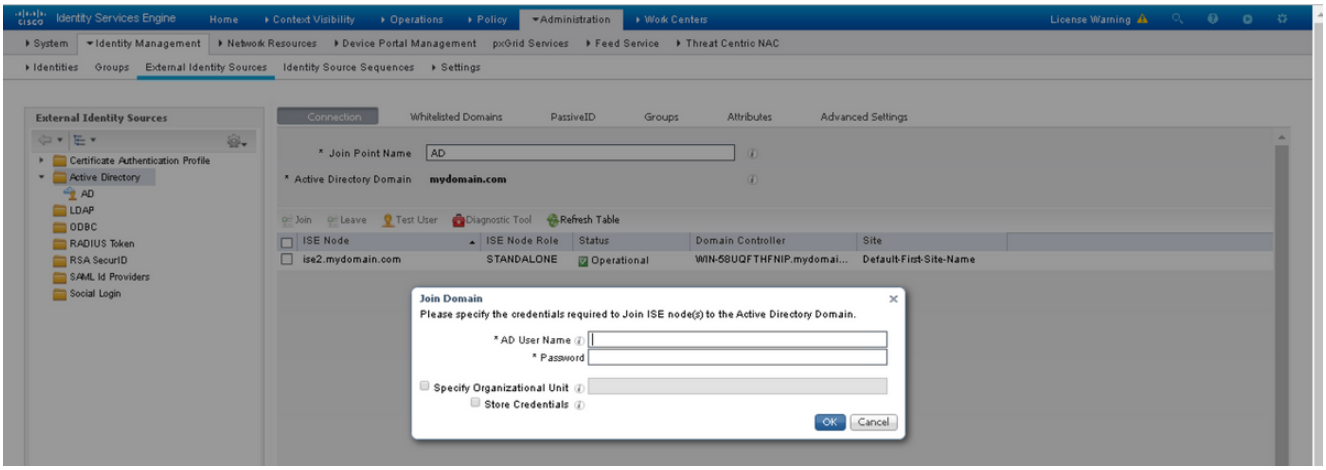
1. Kies **Administratie > Identity Management > Externe identiteitsbronnen > Actieve map**

2. Maak een instantie van de Actieve Map met de **naam van het Punt samen** te voegen en **AD domein** in Cisco ISE.

3. Klik op **Inzenden**.



4. Sluit alle knooppunten aan op de juiste **gebruikersnaam** en **wachtwoord** in de melding.



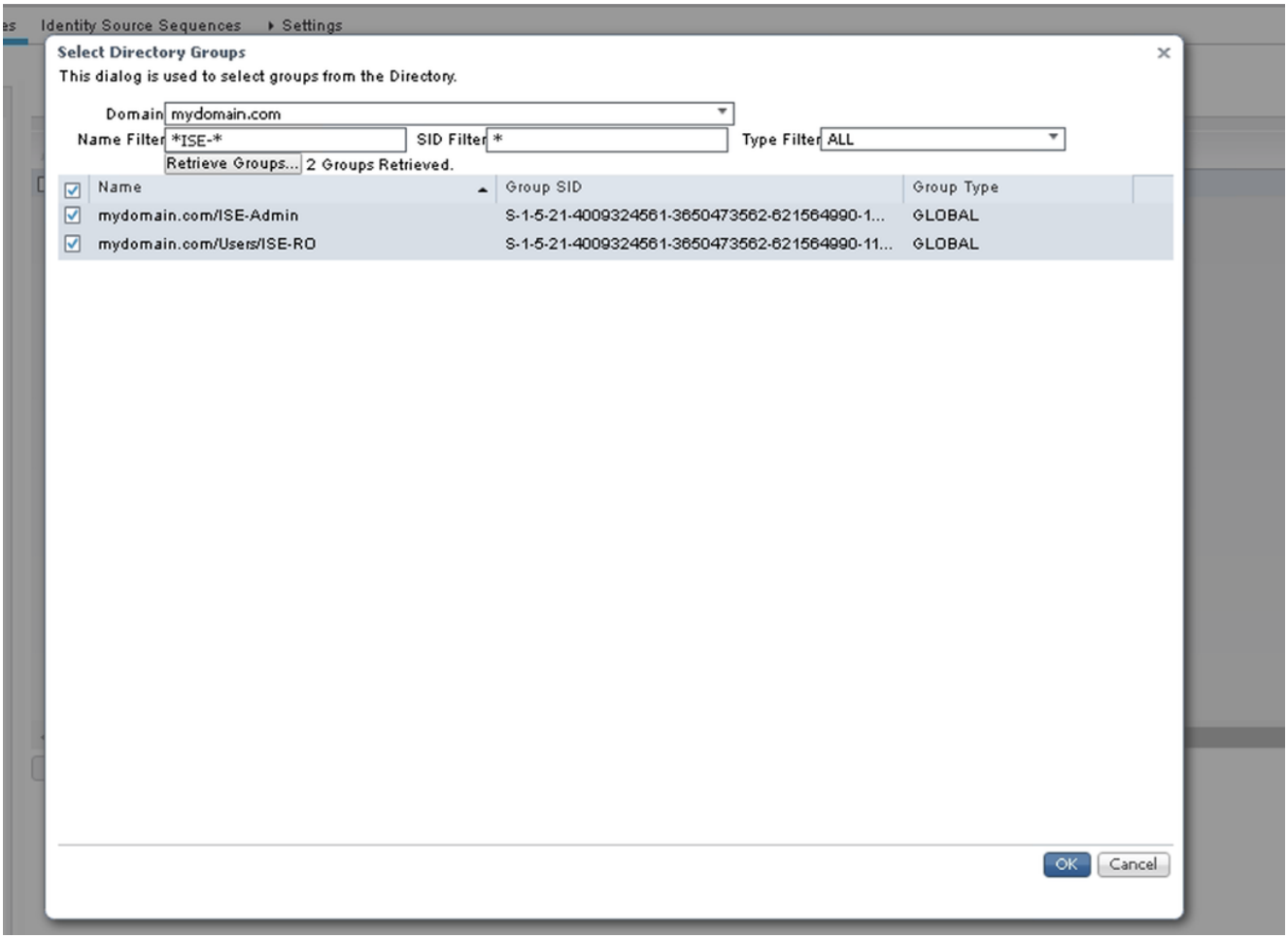
5. Klik op **Opslaan**.

Map-groepen selecteren

1. Maak een externe Administrator-groep en stuur het naar de actieve directory groep.

2. Kies **Administratie >identiteitsbeheer > Externe identiteitsbronnen > Actieve map > Groepen > Groepen uit Map selecteren.**

3. Neem ten minste één AD-groep op waartoe de beheerder behoort.

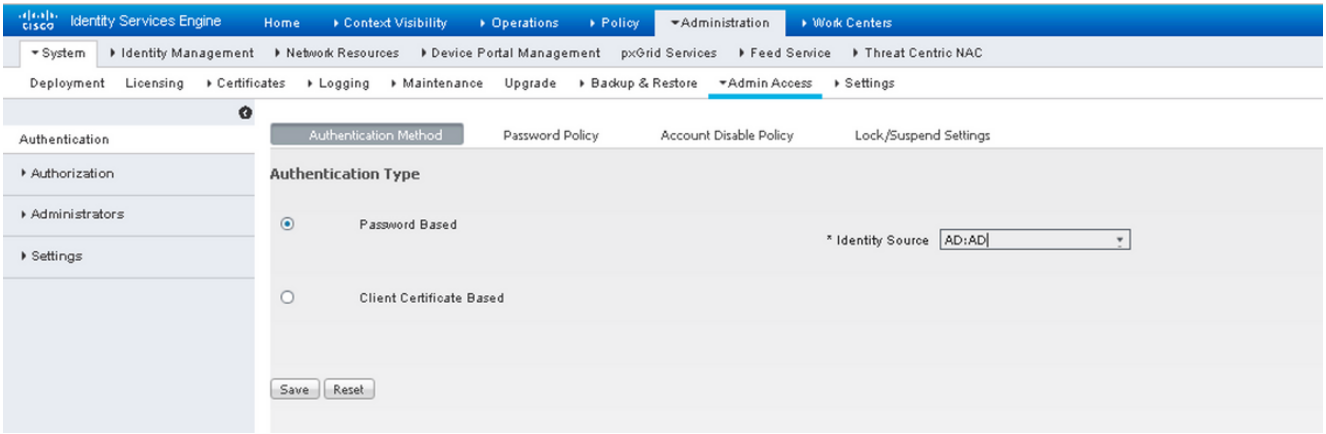


4. Klik op **Opslaan**.

Wachtwoord voor actieve map inschakelen voor beheertoegang

1. Actieve directory-instantie inschakelen als op een wachtwoord gebaseerde verificatiemethode die eerder tot ISE is toegetreden.

2. Kies **Beheer > Systeem > Admin toegang > Verificatie**, zoals in de afbeelding.



3. Klik op **Opslaan**.

Opmerking: De op wachtwoord gebaseerde echtheidsconfiguratie is vereist om op certificaat gebaseerde verificatie mogelijk te maken. Deze configuratie moet worden omgekeerd na

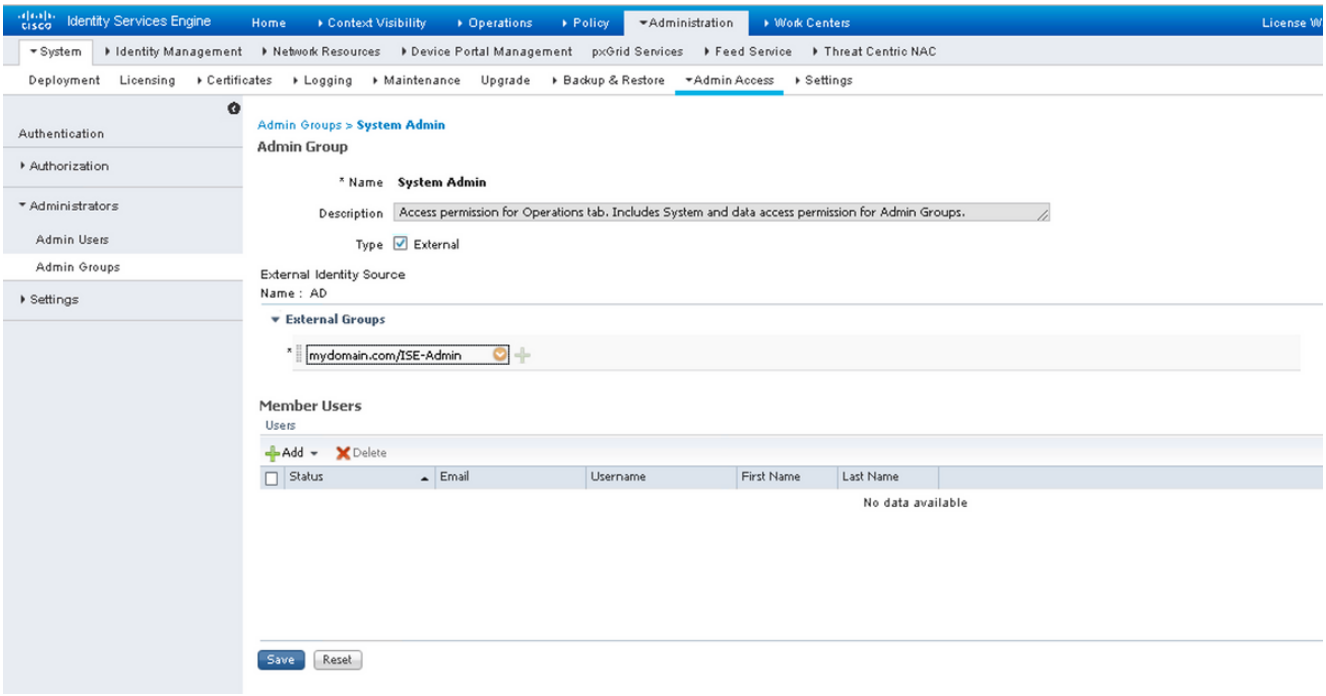
een succesvolle configuratie van op certificaten gebaseerde verificatie.

Geef externe identiteitsgroepen aan beheergroepen op

In dit voorbeeld wordt de externe AD-groep toegewezen aan de standaard Admin-groep.

1. Kies **Beheer > Systeem > Admin Toegang >Beheerders >Admin Groepen > Super Admin.**

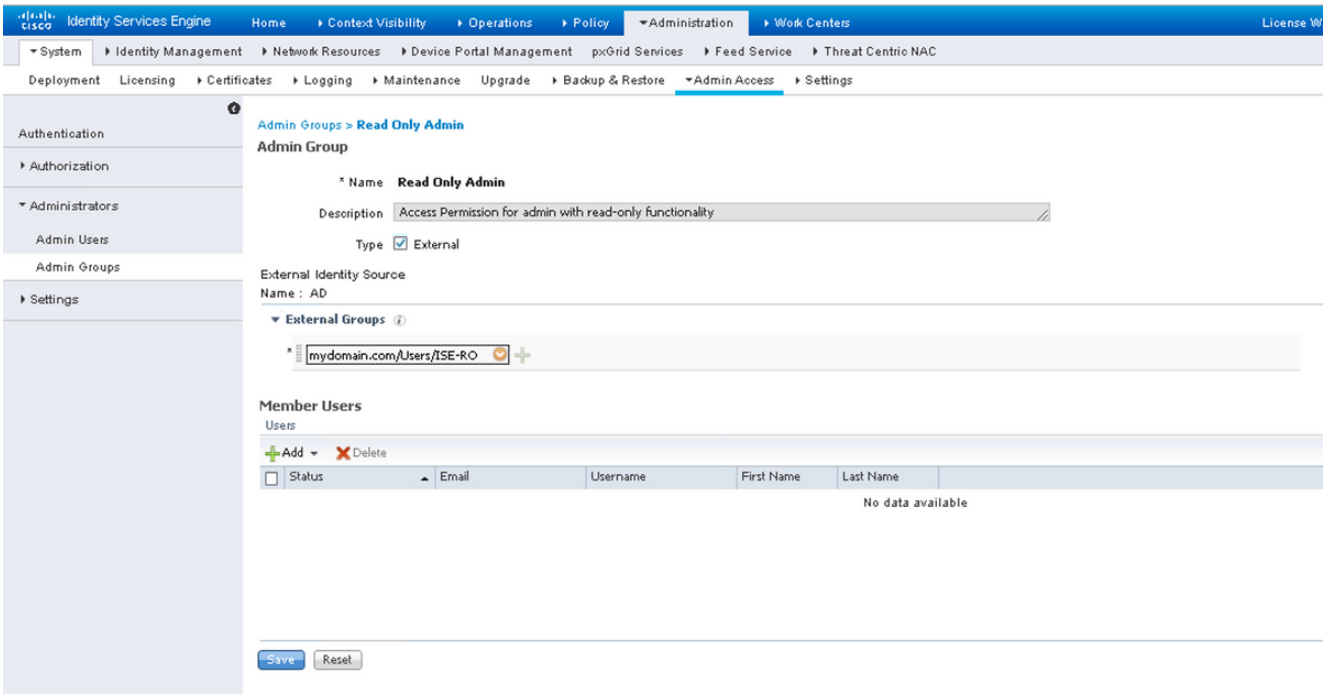
2. Controleer het type als **extern** en selecteer de AD groep onder **Externe groepen**.



3. Klik op **Opslaan**.

4. Kies **Beheer > Systeem > Admin Access > Administrators > Admin Groepen > Alleen lezen Admin**.

5. Controleer het type als **extern** en selecteer de AD groep onder **Externe groepen**, zoals in de afbeelding weergegeven.



6. Klik op **Opslaan**.

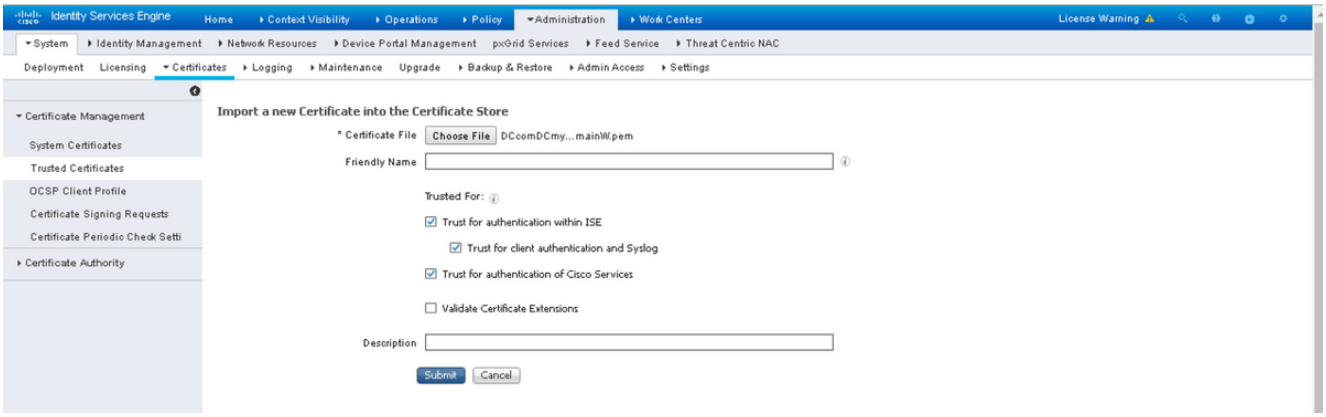
Vertrouwd certificaat importeren

1. Importeer het certificaat van de certificaatautoriteit (CA) dat het certificaat van de klant bevestigt.

2. Kies **beheerder > Systeem > Certificaten > Vertrouwd certificaat > Importeren.**

3. Klik op Blader en kies het CA-certificaat.

4. Controleer het **Vertrouwen op clientverificatie en het selectieteken Syslog**, zoals in de afbeelding wordt weergegeven.



5. Klik op **Inzenden.**

Certificaatverificatieprofiel instellen

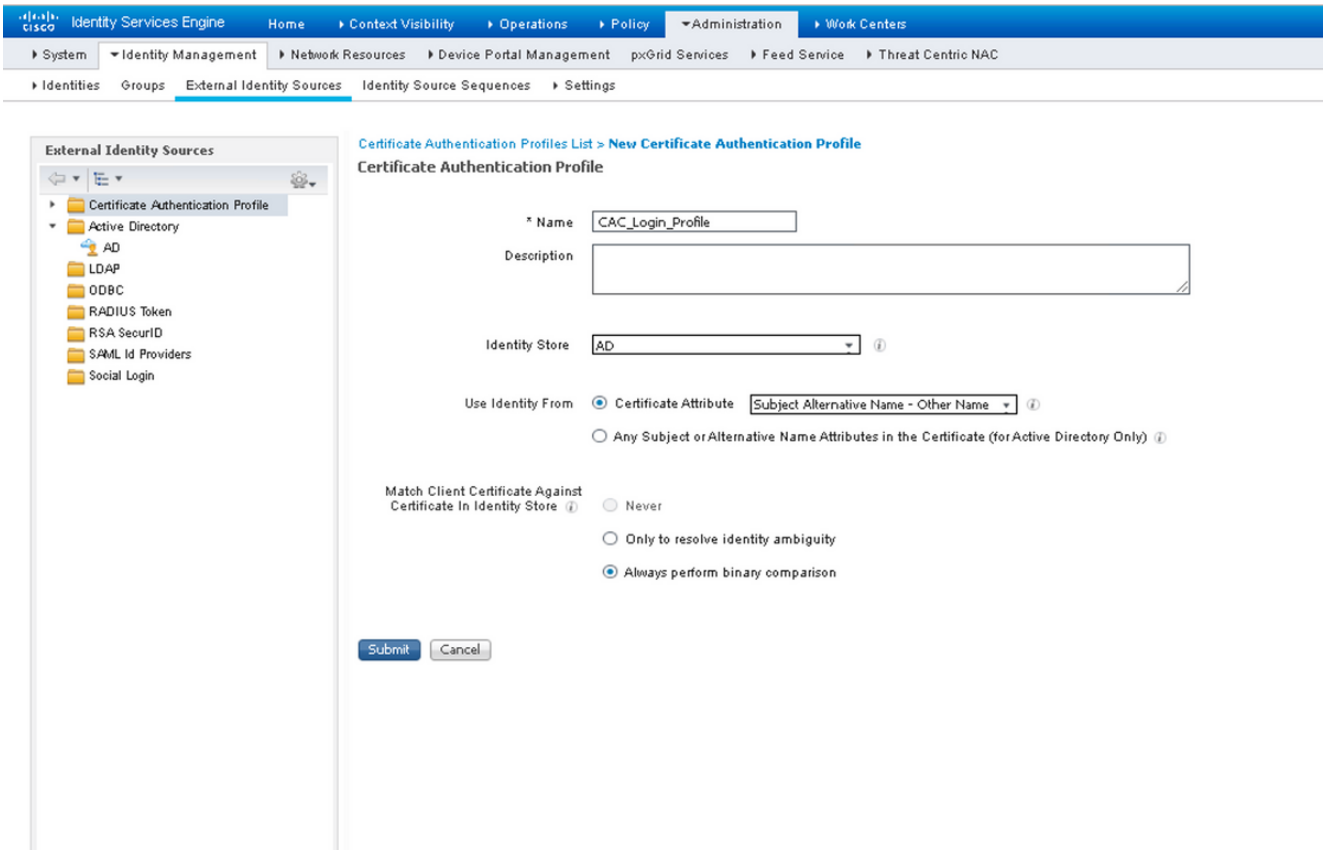
1. Kies **Administratie >identiteitsbeheer > Externe identiteitsbronnen > Facebook-**

verificatieprofiel > Toevoegen.

2. Naam profiel toevoegen.

3. Selecteer de gewenste eigenschap die de gebruikersnaam voor de beheerder in de certificaateigenschap bevat.

4. Als het AD-record voor de gebruiker het certificaat van de gebruiker bevat en het certificaat dat van de browser wordt ontvangen, wilt vergelijken met het certificaat in AD, **voert** u **altijd binaire vergelijking** uit en selecteert u de naam van de instantie die van de Active Directory is opgegeven.

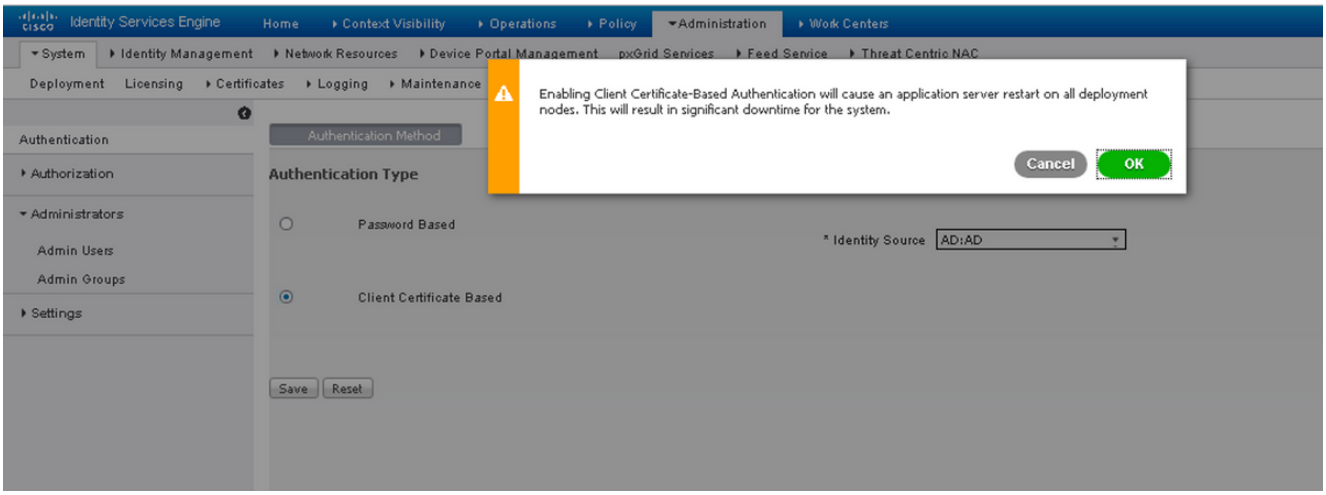


5. Klik op **Inzenden.**

Opmerking: Hetzelfde certificatieprofiel kan ook worden gebruikt voor de op identiteit gebaseerde verificatie van het eindpunt.

Op client gebaseerde verificatie inschakelen

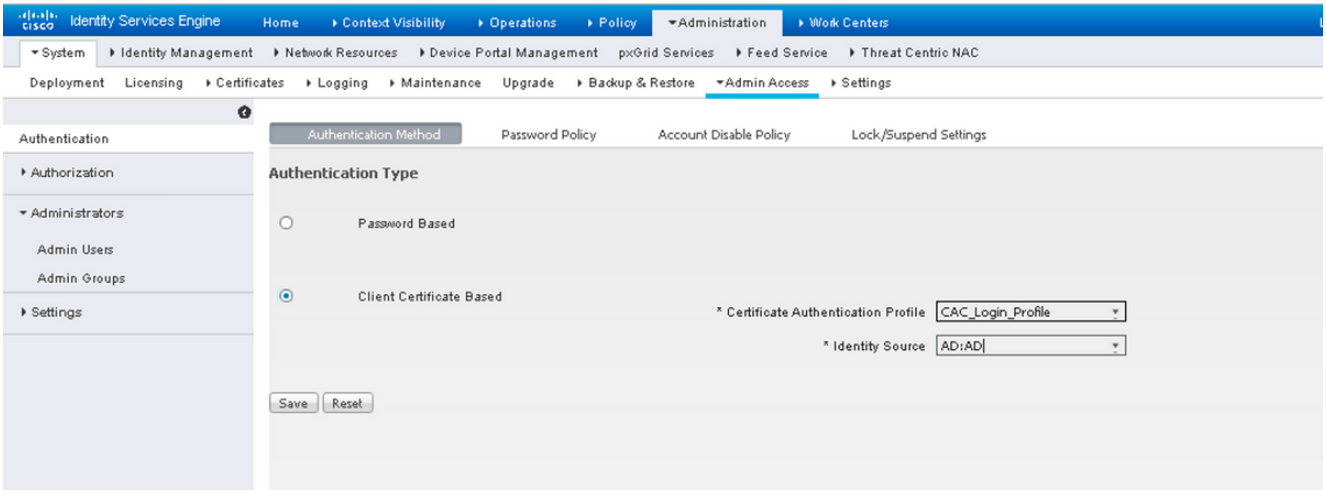
1. Kies **Toediening > Systeem > Admin Access > Verificatie > Clientcertificaat voor verificatiemethode.**



2. Klik op **OK**.

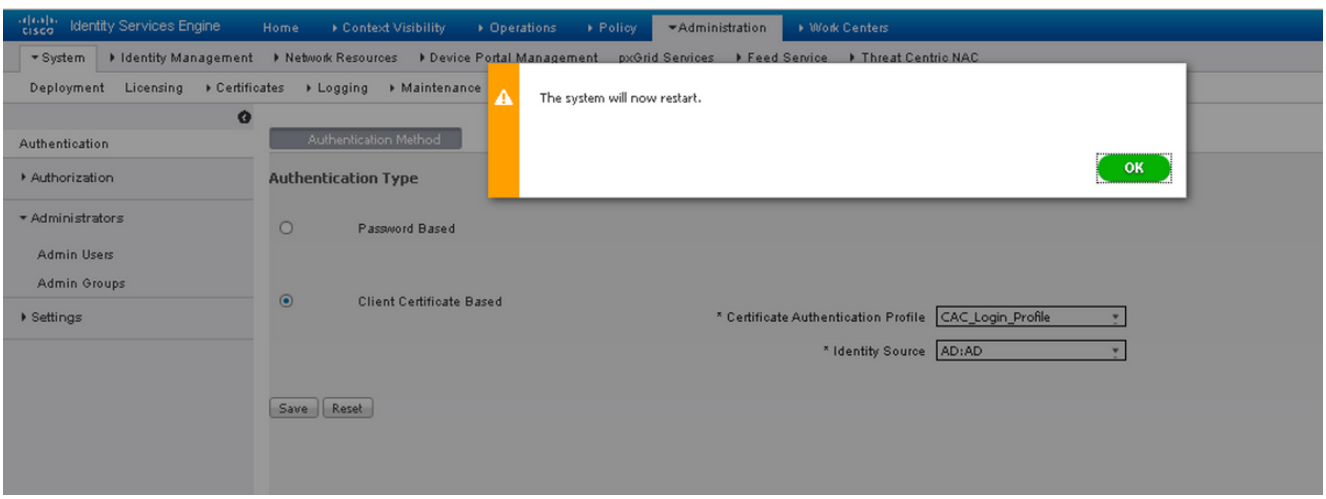
3. Kies het **profiel** van de **certificaatverificatie** dat eerder is ingesteld.

4. Selecteer de naam van de instantie Active Directory.



5. Klik op **Opslaan**.

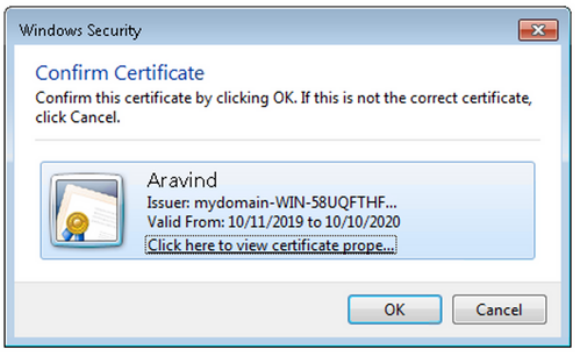
6. ISE-services op alle knooppunten in de implementatieherstart.

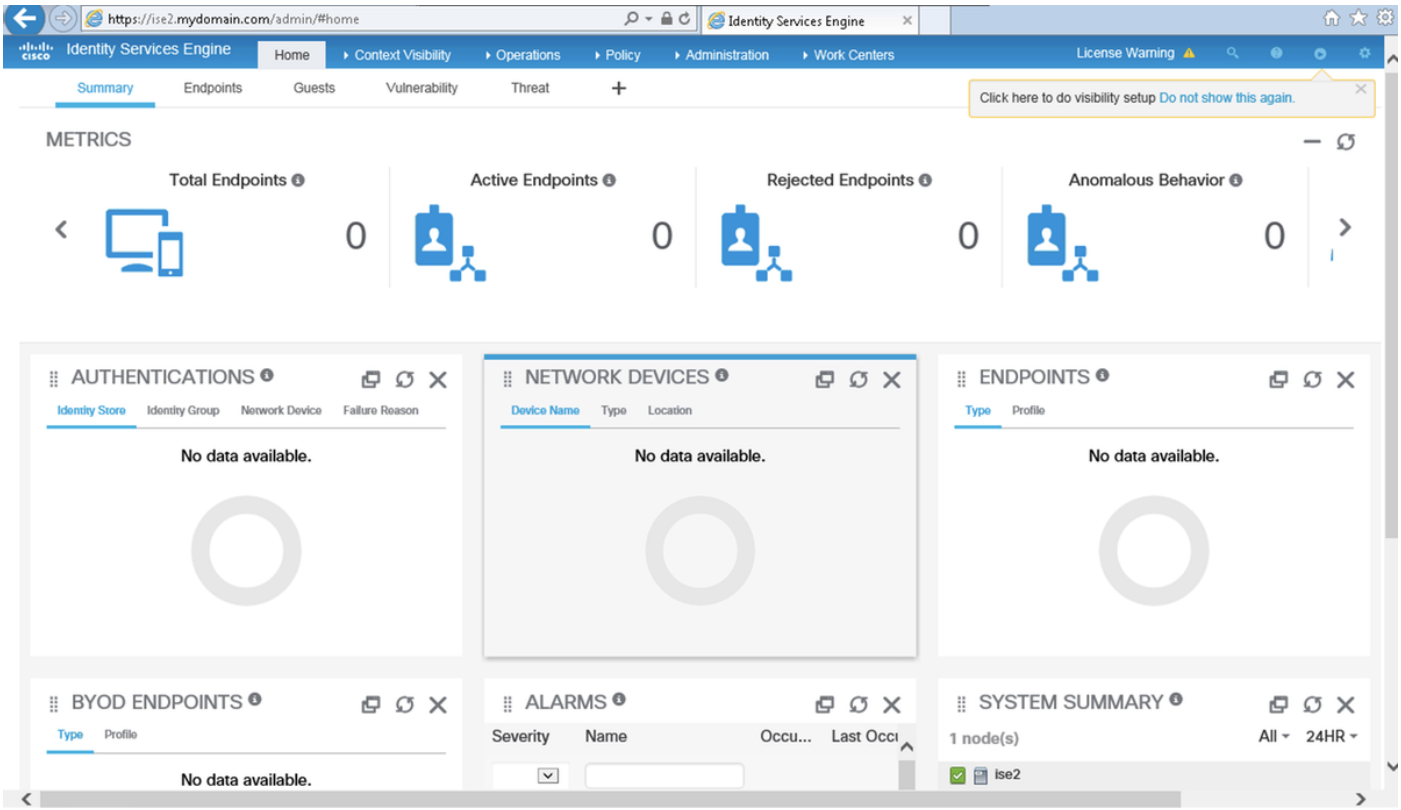


Verifiëren

Controleer de toegang tot de ISE GUI nadat de servicestatus van de **Application Server** verandert in **gebruik.**

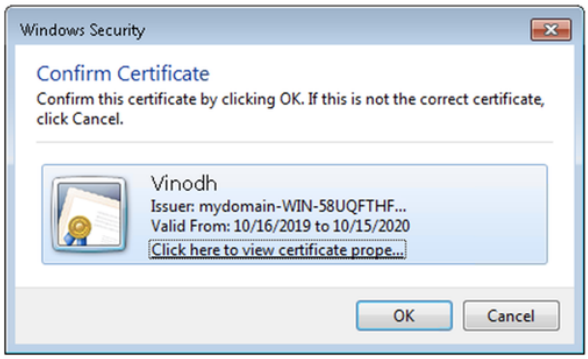
Super Admin Gebruiker: Controleer dat de gebruiker wordt gevraagd een certificaat te kiezen om in te loggen op de ISE GUI en krijgt Super Admin-rechten als het certificaat van een gebruikersdeel van de Super Admin Externe Identity Group is.

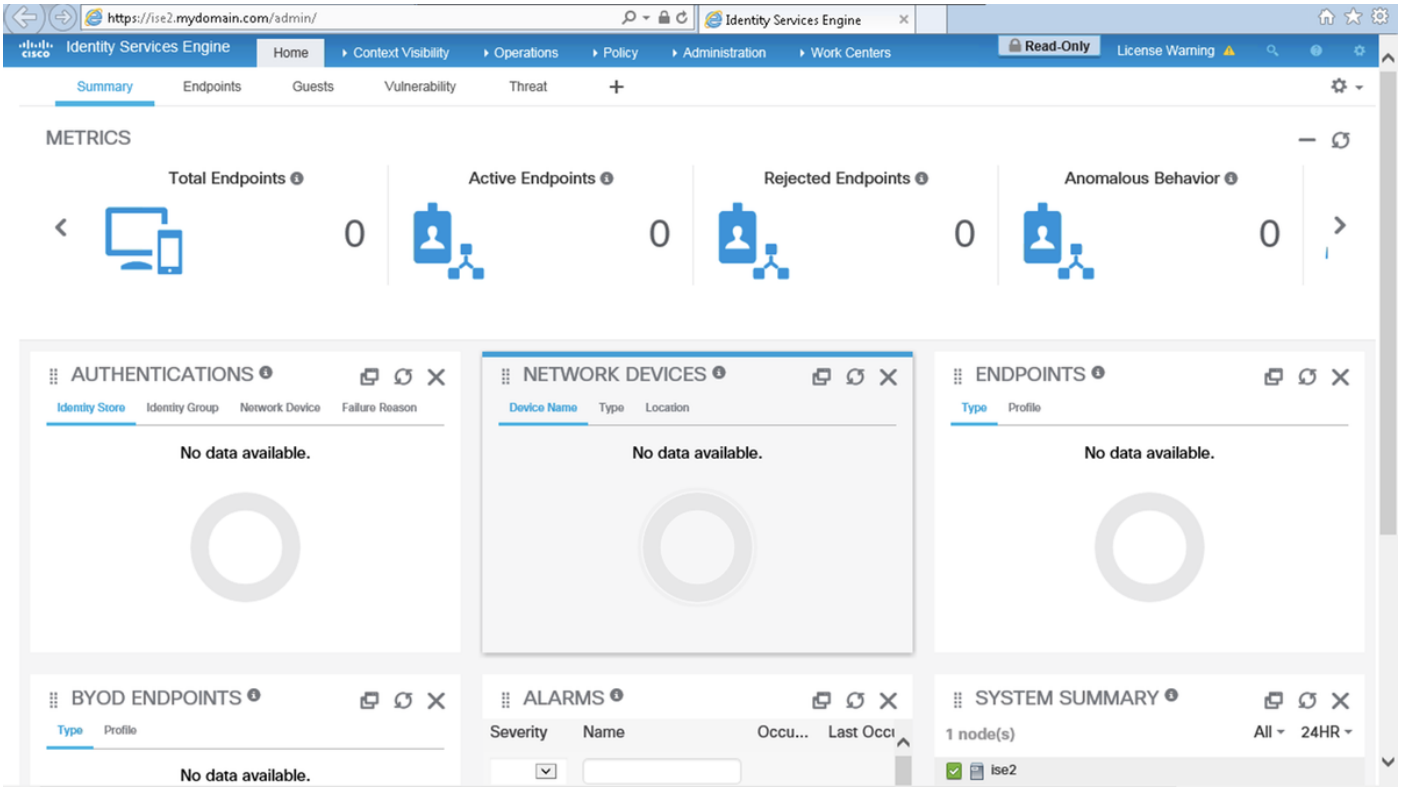




Alleen-lezen beheerder: controleer of de gebruiker een certificaat heeft gevraagd om in te loggen

op de ISE GUI en alleen Lezen-only Admin rechten heeft als het certificaat deel uitmaakt van een gebruikersgroep van de alleen-lezen Admin Externe Identity.





Opmerking: Als Common Access Card (CAC) in gebruik is, geeft Smartcard het gebruikerscertificaat aan ISE nadat de gebruiker hun geldige superpin heeft ingevoerd.

Problemen oplossen

1. Gebruik de **app start veilige** opdracht om Cisco ISE te starten in een veilige modus die

tijdelijk toegangscontrole naar het Admin-portal **toestaat** en de configuratie en het opnieuw opstarten van de services van ISE **toestaat** met de **optie** van de opdrachttoepassing **stop** gevolgd door **ingang van de toepassing..**

2. De veilige optie biedt een manier van herstel als een beheerder onopzettelijk de toegang tot het Cisco ISE Admin-portal voor alle gebruikers sluit. Deze gebeurtenis kan voorkomen als de beheerder een onjuiste **IP-toegangslijst** instelt in het **Beheer > Toegang > Instellingen > Access-pagina**. De **veilige** optie **omzeilt op certificaat gebaseerde verificatie** en keert terug naar de standaard gebruikersnaam en wachtwoordverificatie voor loggen naar het Cisco ISE Admin-portaal.