Implementatiegids voor draadloze BYOD voor FlexConnect

Inhoud

Inleiding

Mobiele apparaten worden steeds krachtiger en populairder onder consumenten. Miljoenen van deze apparaten worden verkocht aan consumenten met snelle Wi-Fi zodat gebruikers kunnen communiceren en samenwerken. Consumenten zijn nu gewend aan de productiviteitsverbetering die deze mobiele apparaten in hun leven brengen en proberen hun persoonlijke ervaring in de werkruimte te brengen. Dit creëert de functionaliteitsbehoeften van een Bring Your Own Device (BYOD) oplossing op de werkplek.

Dit document biedt de implementatie van de branch voor de BYOD-oplossing. Een medewerker

verbindt zich met een corporate service set identifier (SSID) met zijn/haar nieuwe iPad en wordt doorgestuurd naar een zelfregistratieportal. De Cisco Identity Services Engine (ISE) verifieert de gebruiker aan de hand van de Active Directory (AD) van het bedrijf en downloadt een certificaat met een ingesloten iPad-MAC-adres en -gebruikersnaam naar de iPad, samen met een profiel van de aanvrager waarmee het gebruik van EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) als methode voor dot1x-connectiviteit wordt afgedwongen. Gebaseerd op het autorisatiebeleid in ISE kan de gebruiker vervolgens verbinding maken met het gebruik van dot1x en toegang krijgen tot de juiste bronnen.

ISE-functies in softwarereleases van Cisco draadloze LAN-controllers eerder dan 7.2.10.0 boden geen ondersteuning voor lokale switching-clients die worden geassocieerd met FlexConnect-access points (AP's). Release 7.2.10.0 ondersteunt deze ISE-functies voor FlexConnect AP's voor lokale switching- en centraal geverifieerde clients. Bovendien biedt release 7.2.10.0, geïntegreerd met ISE 1.1.1, (maar is niet beperkt tot) deze BYOD-oplossingsfuncties voor draadloos:

- Apparaatprofilering en -houding
- Registratie van apparaten en levering van applicaties
- Onboarding van persoonlijke apparaten (iOS- of Android-apparaten)

Opmerking: hoewel ondersteund, zijn andere apparaten, zoals PC of Mac draadloze laptops en werkstations, niet meegeleverd in deze handleiding.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

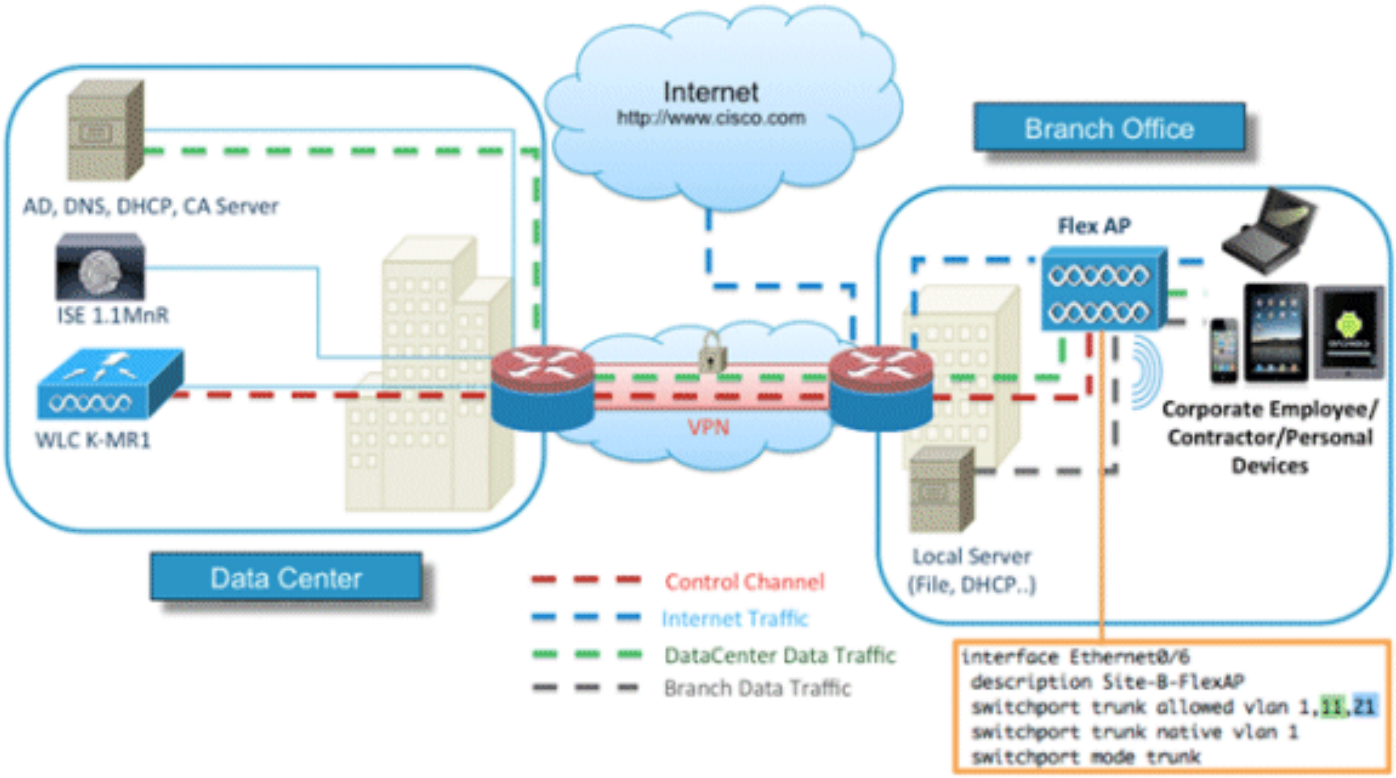
- Cisco Catalyst 6500-switches
- Cisco draadloze LAN (WLAN)-controllers
- Cisco WLAN controller (WLC) softwarerelease 7.2.10.0 en hoger
- 802.11n access points in FlexConnect-modus
- Cisco ISE-softwarerelease 12.1 en hoger
- Windows 2008 AD met certificeringsinstantie (CA)
- DHCP-server
- Domain Name System (DNS)-server
- Network Time Protocol (NTP)
- Draadloze client laptop, smartphone en tablets (Apple iOS, Android, Windows en Mac)

Opmerking: Raadpleeg Releaseopmerkingen voor Cisco draadloze LAN-controllers en lichtgewicht access points voor release 7.2.10.0 voor belangrijke informatie over deze softwarerelease. Log in op de Cisco.com site voor de laatste release notities voordat u de software laadt en test.

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 de potentiële impact van elke opdracht begrijpen.

Topologie

Een minimale netwerkinstallatie, zoals in dit diagram wordt getoond, is vereist om deze functies correct te kunnen implementeren en testen:



Voor deze simulatie hebt u een netwerk nodig met een FlexConnect AP, een lokale/externe site met lokale DHCP, DNS, de WLC en de ISE. FlexConnect AP is verbonden met een trunk om lokale switching met meerdere VLAN's te testen.

Apparaatregistratie en probleemprovisioning

Een apparaat moet worden geregistreerd, zodat de native supplicant kan provisioneren voor dot1x-verificatie. Gebaseerd op het juiste verificatiebeleid wordt de gebruiker omgeleid naar de gastenpagina en geverifieerd door werknemersreferenties. De gebruiker ziet de pagina van de apparatenregistratie, die om hun apparateninformatie vraagt. Het proces voor apparaatprovisioning wordt vervolgens gestart. Als het besturingssysteem (OS) niet wordt ondersteund voor provisioning, wordt de gebruiker doorgestuurd naar het Asset Registration Portal om dat apparaat te markeren voor toegang tot MAC-verificatie-omzeiling (MAB). Als het besturingssysteem wordt ondersteund, wordt het inschrijvingsproces gestart en wordt de native supplicant van het apparaat voor dot1x-verificatie geconfigureerd.

Asset Registration Portal

De Asset Registration Portal is het onderdeel van het ISE-platform dat werknemers in staat stelt het onboarding van endpoints te initiëren via een verificatie- en registratieproces.

De beheerders kunnen activa van de pagina van de endpointidentiteiten verwijderen. Elke medewerker kan de activa die hij heeft geregistreerd bewerken, verwijderen en op een zwarte lijst zetten. De eindpunten op de zwarte lijst worden toegewezen aan een zwarte lijst identiteitsgroep, en een vergunningsbeleid wordt gecreëerd om netwerktoegang door de op de zwarte lijst geplaatste eindpunten te verhinderen.

Portal voor zelfregistratie

In de Central Web Verification (CWA)-stroom worden werknemers omgeleid naar een portal waar ze hun referenties kunnen invoeren, authenticeren en de specifieke kenmerken kunnen invoeren van het specifieke actief dat ze willen registreren. Dit portaal heet de Self Provisioning Portal en is vergelijkbaar met de Device Registration Portal. Het staat de werknemers toe om het adres van MAC evenals een zinvolle beschrijving van het eindpunt in te gaan.

Verificatie en provisioning

Zodra werknemers selecteren de Self-Registration Portal, worden ze uitgedaagd om een reeks geldige werknemersreferenties te verstrekken om verder te gaan naar de provisioningfase. Na succesvolle verificatie kan het eindpunt worden geprovisioneerd in de endpointdatabase en wordt er een certificaat gegenereerd voor het eindpunt. Via een link op de pagina kan de medewerker de Supplicant Pilot Wizard (SPW) downloaden.

> **Opmerking**: raadpleeg het artikel FlexConnect Feature Matrix Cisco om de nieuwste FlexConnect-functiematrix voor BYOD te bekijken.

Provisioning voor iOS (iPhone/iPad/iPod)

Voor de EAP-TLS-configuratie volgt ISE het inschrijvingsproces voor Apple Over-the-Air (OTA):

- Na succesvolle verificatie evalueert de evaluatie-engine het beleid voor client-provisioning, wat resulteert in een profiel van de aanvrager.
- Als het profiel van de aanvrager betrekking heeft op de EAP-TLS-instelling, bepaalt het OTA-proces of de ISE gebruik maakt van zelfondertekening of ondertekend door een onbekende CA. Als een van de voorwaarden waar is, wordt de gebruiker gevraagd om het certificaat van ofwel ISE of CA te downloaden voordat het inschrijvingsproces kan beginnen.
- Voor andere EAP-methoden, wordt het definitieve profiel na succesvolle verificatie gedrukt.

Provisioning voor Android

Om veiligheidsredenen moet de Android-agent worden gedownload van de Android-marktplaats en kan hij niet worden geleverd via ISE. Cisco uploadt een versie van de wizard naar de Android-marktplaats via de Cisco Android-marktplaats-uitgeversaccount.

Dit is het Android-provisioningproces:

1. Cisco gebruikt de Software Development Kit (SDK) om het Android-pakket met de extensie .apk te maken.
2. Cisco uploadt een pakket naar de Android-markt.
3. De gebruiker configureert het beleid in de client provisioning met de juiste parameters.
4. Na registratie van het apparaat wordt de eindgebruiker doorgestuurd naar de client provisioning service wanneer dot1x-verificatie mislukt.
5. De Provising Portal pagina biedt een knop die de gebruiker omleidt naar de Android marktplaats portal waar ze de SPW kunnen downloaden.
6. Cisco SPW wordt gestart en voert provisioning van de aanvrager uit: SPW ontdekt de ISE en downloadt het profiel van ISE.SPW maakt een combinatie van zekerheid en sleutel voor EAP-TLS.SPW doet een Simple Certificate Enrollment Protocol (SCEP) proxyverzoek naar ISE en krijgt het certificaat.SPW past de draadloze profielen toe.SPW activeert opnieuw verificatie als de profielen met succes worden toegepast.SPW-uitgangen.

Dubbele SSID draadloze BYOD zelfregistratie

Dit is het proces voor dubbele SSID draadloze BYOD zelfregistratie:

1. De gebruiker associeert met de Guest SSID.
2. De gebruiker opent een browser en wordt doorgestuurd naar het ISE CWA Guest Portal.
3. De gebruiker voert een gebruikersnaam en wachtwoord voor de werknemer in het Guest Portal in.
4. ISE verifieert de gebruiker, en, gebaseerd op het feit dat ze een werknemer zijn en geen gast, leidt de gebruiker naar de Gastpagina voor de registratie van het apparaat van de werknemer.
5. Het MAC-adres is vooraf ingevuld in de gastenpagina voor apparaatregistratie voor de DeviceID. De gebruiker voert een beschrijving in en accepteert indien nodig het beleid voor aanvaardbaar gebruik (Acceptable Use Policy of AUP).
6. De gebruiker selecteert **Akkoord** en begint de SPW te downloaden en te installeren.
7. De aanvrager voor het apparaat van die gebruiker wordt geleverd samen met eventuele certificaten.
8. CoA treedt op, en het apparaat koppelt terug aan de corporate SSID (CORP) en authenticeert met EAP-TLS (of een andere autorisatiemethode die gebruikt wordt voor die aanvrager).

Single SSID draadloze BYOD zelfregistratie

In dit scenario is er één SSID voor bedrijfstoegang (CORP) die zowel Protected Extensible Verification Protocol (PEAP) als EAP-TLS ondersteunt. Er is geen gast SSID.

Dit is het proces voor single SSID draadloze BYOD zelfregistratie:

1. De gebruiker associeert met CORP.
2. De gebruiker voert een werknemersgebruikersnaam en wachtwoord in in de aanvrager voor de PEAP-verificatie.

3. De ISE verifieert de gebruiker en biedt op basis van de PEAP-methode een autorisatiebeleid voor acceptatie met doorverwijzing naar de gastenpagina voor apparaatregistratie voor werknemers.
4. De gebruiker opent een browser en wordt doorgestuurd naar de gastenpagina voor de registratie van het apparaat van de werknemer.
5. Het MAC-adres is vooraf ingevuld in de gastenpagina voor apparaatregistratie voor de DeviceID. De gebruiker voert een beschrijving in en accepteert de AUP.
6. De gebruiker selecteert **Akkoord** en begint de SPW te downloaden en te installeren.
7. De aanvrager voor het apparaat van die gebruiker wordt geleverd samen met eventuele certificaten.
8. CoA treedt op, en het apparaat koppelt terug naar de CORP-SSID en verificeert met EAP-TLS.

Functieconfiguratie

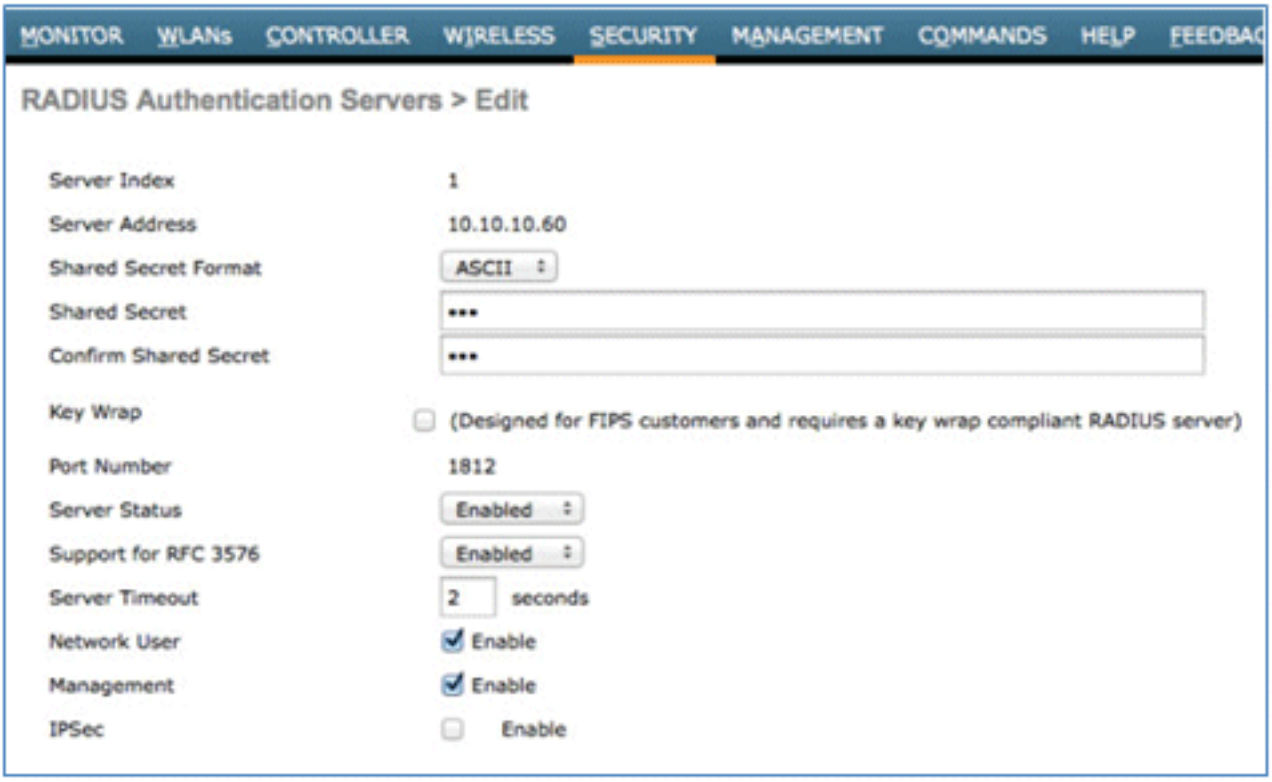
Voltooi de volgende stappen om te beginnen met de configuratie:

1. Zorg voor deze handleiding dat de WLC-versie 7.2.10.0 of hoger is.

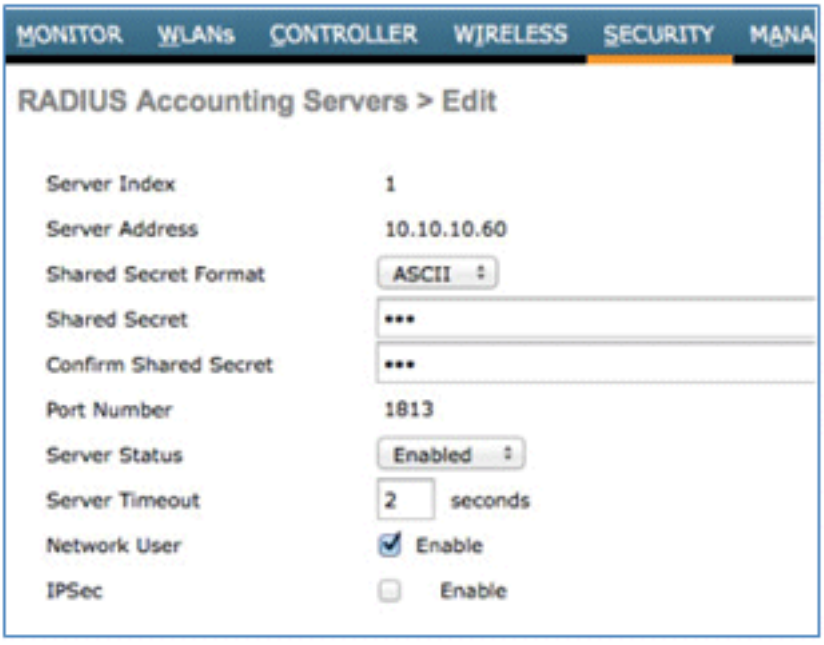
2. Navigeer naar **Security** > **RADIUS** > **Verificatie** en voeg de RADIUS-server toe aan de WLC.

3. Voeg de ISE 1.1.1 toe aan de WLC:

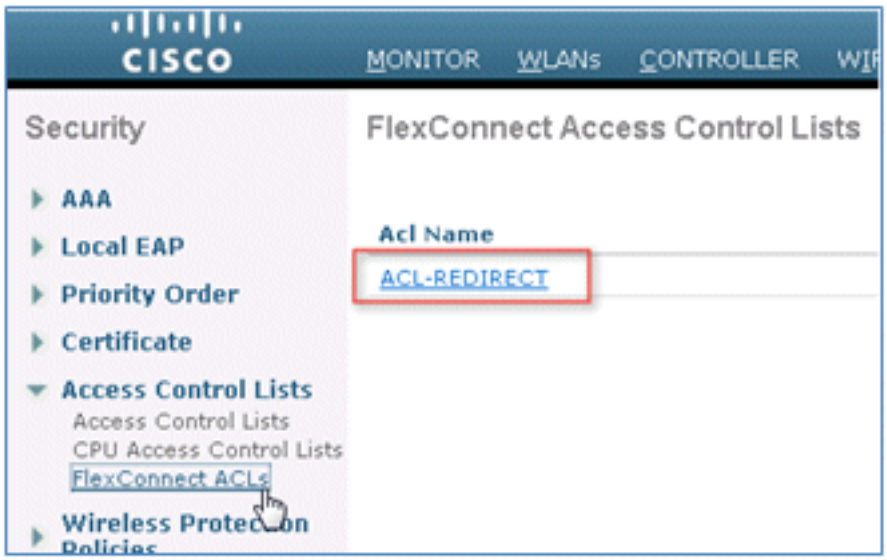
   Voer een gedeeld geheim in.Stel ondersteuning voor RFC 3576 in op **Ingeschakeld**.



4. Voeg dezelfde ISE-server toe als een RADIUS-accountserver.



5. Maak een WLC Pre-Autation ACL om later in het ISE-beleid te gebruiken. Navigeer naar WLC > **Security** > **Toegangscontrolelijsten** > **FlexConnect ACL's**, en maak een nieuwe FlexConnect ACL met de naam **ACL-REDIRECT** (in dit voorbeeld).

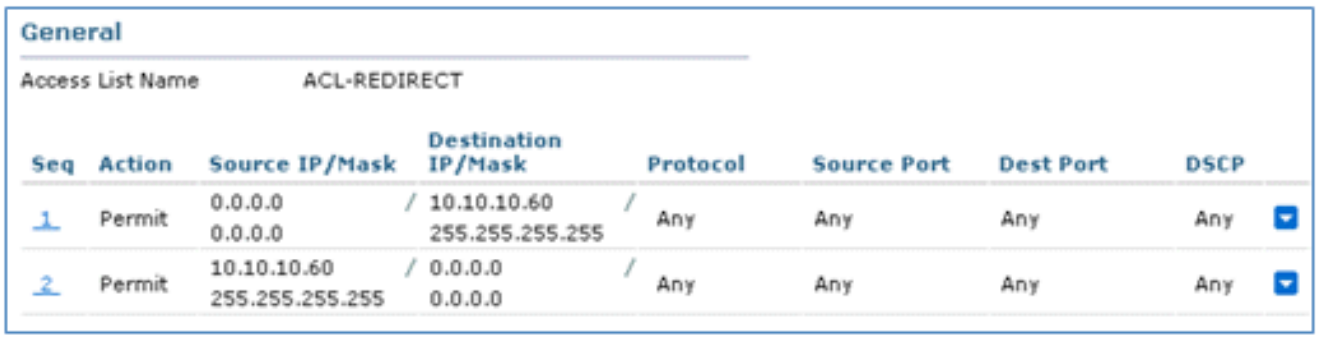


6. In de ACL-regels kunt u al het verkeer toestaan naar/van de ISE en verkeer van clients toestaan tijdens levering door de aanvrager.

   Voor de eerste regel (vervolg 1):

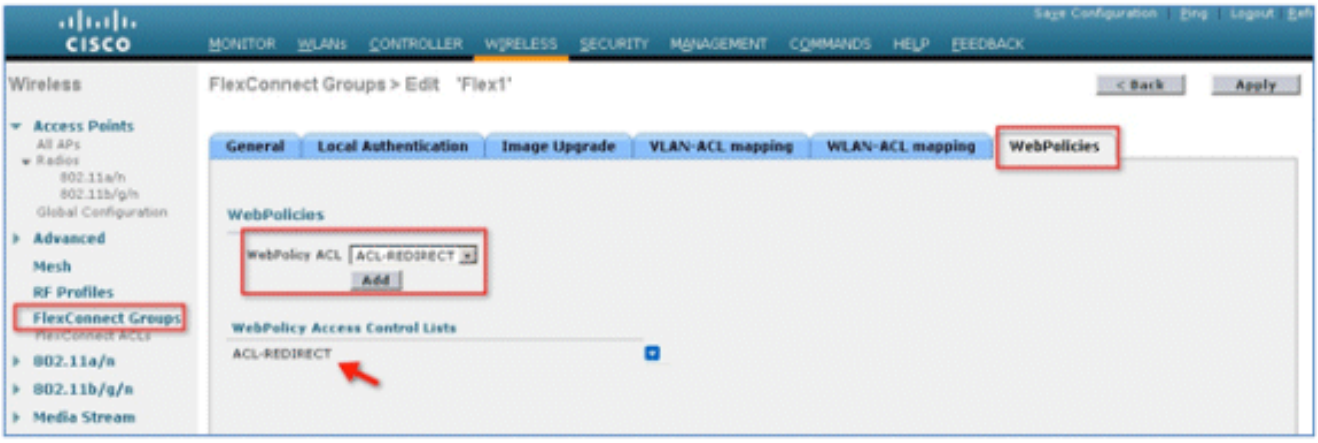
   Bron instellen op **Any**.IP (ISE-adres) instellen/ Netmasker **255.255.255.255**.Stel actie in op **Permit**.

   Voor de tweede regel (opeenvolging 2), plaats bron IP (het adres van ISE)/ masker 255.255.255.255 aan **om het even welke** en Actie om **toe** te **staan**.



7. Maak een nieuwe FlexConnect-groep met de naam Flex1 (in dit voorbeeld):

   Navigeer naar **FlexConnect Group** > tabblad **WebPolicies**.Klik onder het veld Web Policy ACL op **Add** en selecteer **ACL-REDIRECT** of de eerder gemaakte FlexConnect ACL.Bevestig dat het veld **Web Policy Access Control Lists** wordt ingevuld.



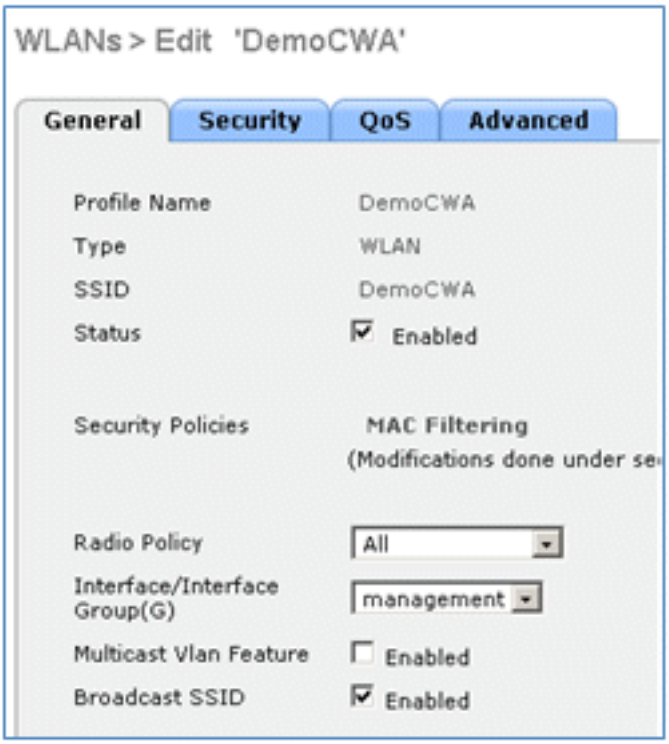
8. Klik op **Toepassen** en **Configuratie opslaan**.

WLAN-configuratie

Voltooi de volgende stappen om het WLAN te configureren:

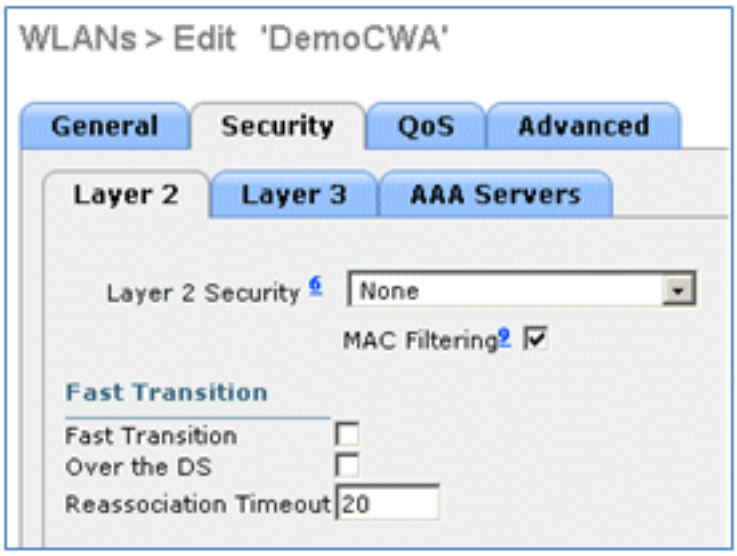
1. Maak een Open WLAN-SSID voor het voorbeeld van de dubbele SSID:

   Voer een WLAN-naam in: **DemoCWA** (in dit voorbeeld).Selecteer de **Enabled** optie voor Status.



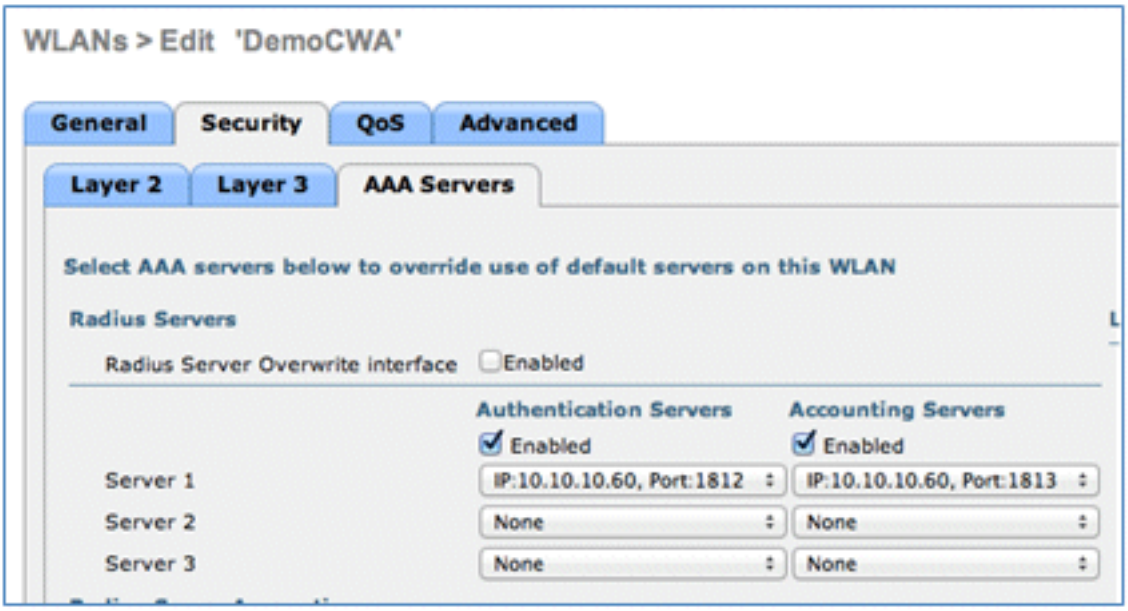
2. Navigeer naar het tabblad **Beveiliging** > **Layer 2**-tabblad en stel deze kenmerken in:

Layer 2 Security: **geen**MAC-filtering: **ingeschakeld** (aangevinkt)Snelle overgang: **uitgeschakeld** (dit vakje is niet aangevinkt)



3. Ga naar het tabblad **AAA-servers** en stel deze kenmerken in:

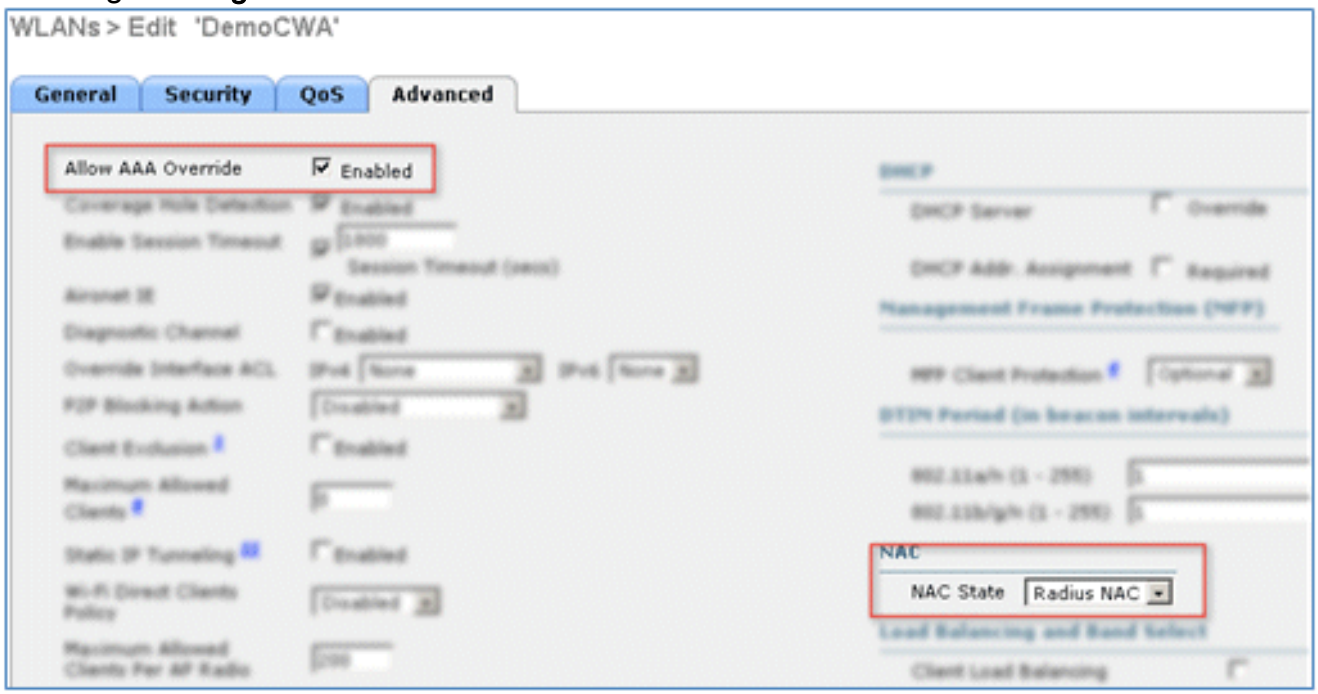
   Verificatie- en accountservers: **ingeschakeld**Server 1: *<ISE/IP-adres>*



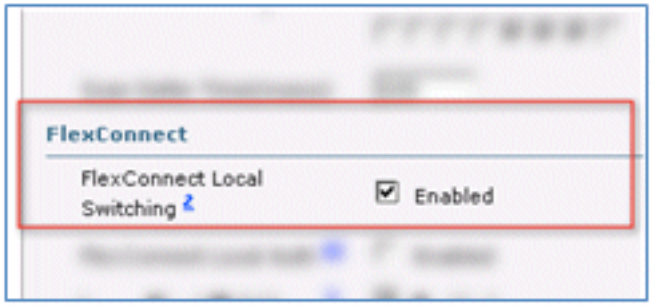
4. Blader omlaag vanaf het tabblad **AAA-servers**. Zorg er onder Verificatieprioriteit voor webautorisatiegebruiker voor dat **RADIUS** voor verificatie wordt gebruikt en dat de andere niet worden gebruikt.

5. Ga naar het tabblad **Geavanceerd** en stel deze kenmerken in:

   AAA negeren: **ingeschakeld**NAC-status: **straal NAC**

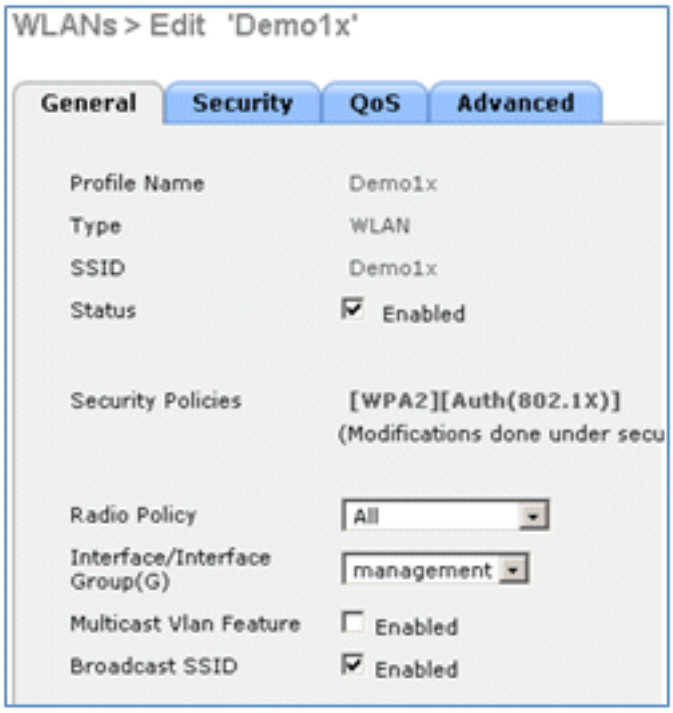


   Opmerking: RADIUS Network Admission Control (NAC) wordt niet ondersteund wanneer FlexConnect AP zich in de losgekoppelde modus bevindt. Als de FlexConnect AP zich dus in de standalone modus bevindt en de verbinding met de WLC verliest, worden alle clients losgekoppeld en wordt de SSID niet meer geadverteerd.
6. Blader naar beneden in het tabblad Geavanceerd en stel FlexConnect Local Switching in op **Enabled**.



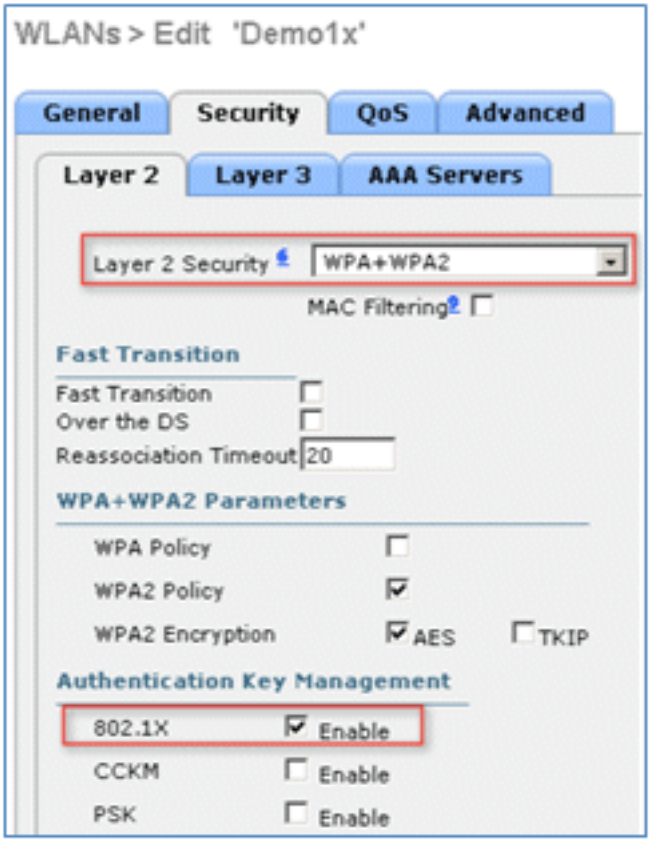
7. Klik op **Toepassen** en **Configuratie opslaan**.

8. Maak een 802.1X WLAN SSID met de naam **Demo1x** (in dit voorbeeld) voor enkele en dubbele SSID-scenario's.



9. Navigeer naar het tabblad **Beveiliging > Layer 2**-tabblad en stel deze kenmerken in:

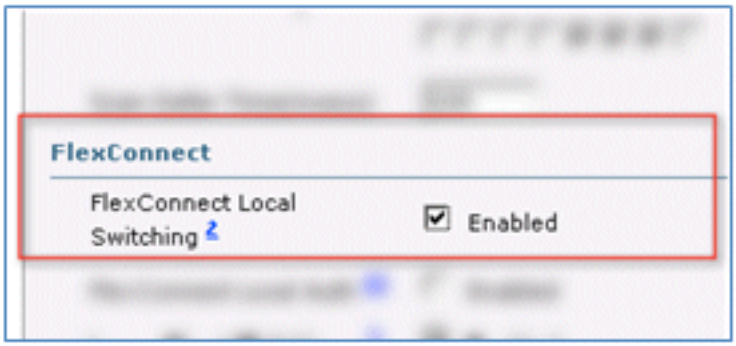
   Layer 2-beveiliging: **WPA+WPA2**Snelle overgang: **uitgeschakeld** (dit vakje is niet aangevinkt)Verificatie Key Management: 802.lX: **inschakelen**



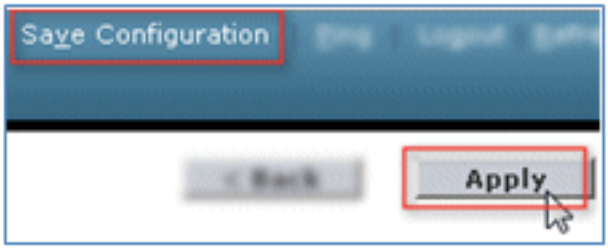
10. Ga naar het tabblad **Geavanceerd** en stel deze kenmerken in:

    AAA negeren: **ingeschakeld**NAC-status: **straal NAC**

11. Blader naar beneden in het tabblad **Geavanceerd** en stel FlexConnect Local Switching in op **Enabled**.



12. Klik op **Toepassen** en **Configuratie opslaan**.



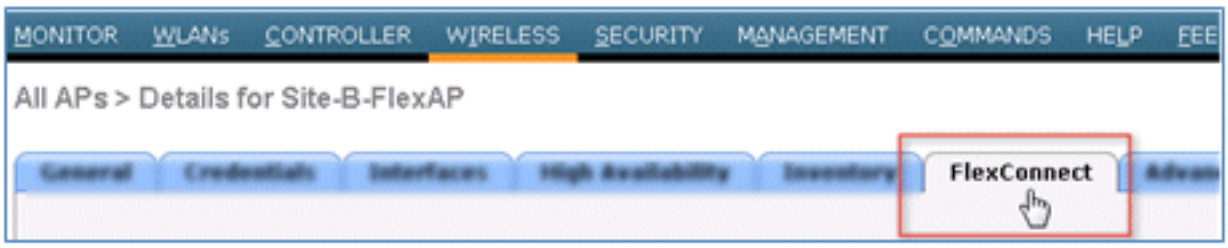
13. Bevestig dat beide nieuwe WLAN's zijn gemaakt.

Configuratie FlexConnect AP

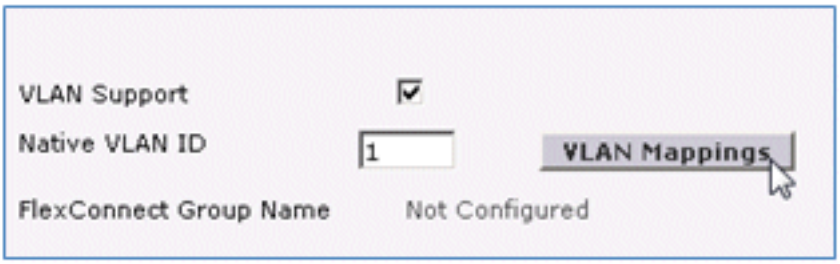
Voltooi de volgende stappen om FlexConnect AP te configureren:

1. Navigeer naar **WLC > Wireless** en klik op het doel FlexConnect AP.

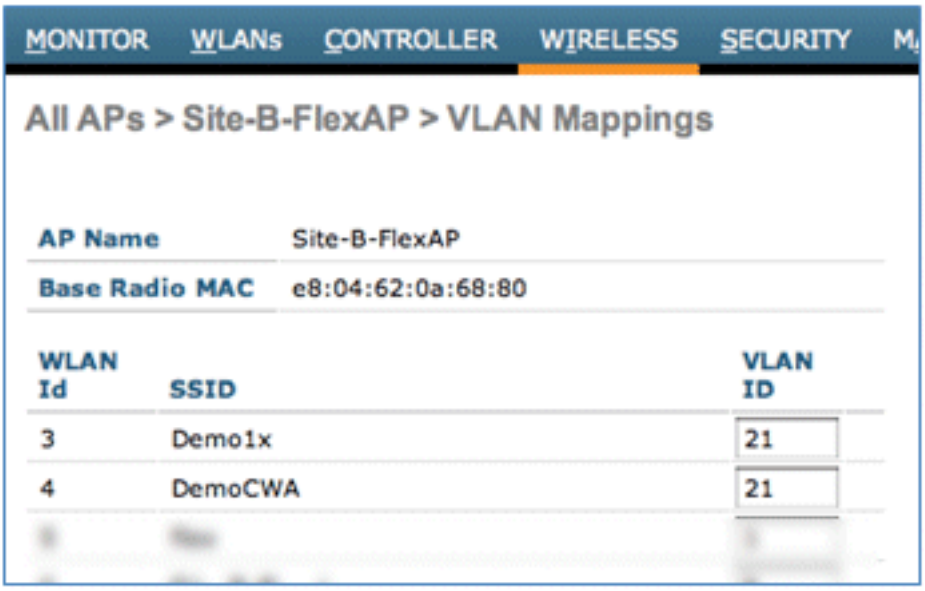
2. Klik op het tabblad **FlexConnect**.



3. Schakel VLAN-ondersteuning in (dit vakje is ingeschakeld), stel de native VLAN-id in en klik op **VLAN-toewijzingen**.



4. Stel de VLAN-id in op **21** (in dit voorbeeld) voor de SSID voor lokale switching.



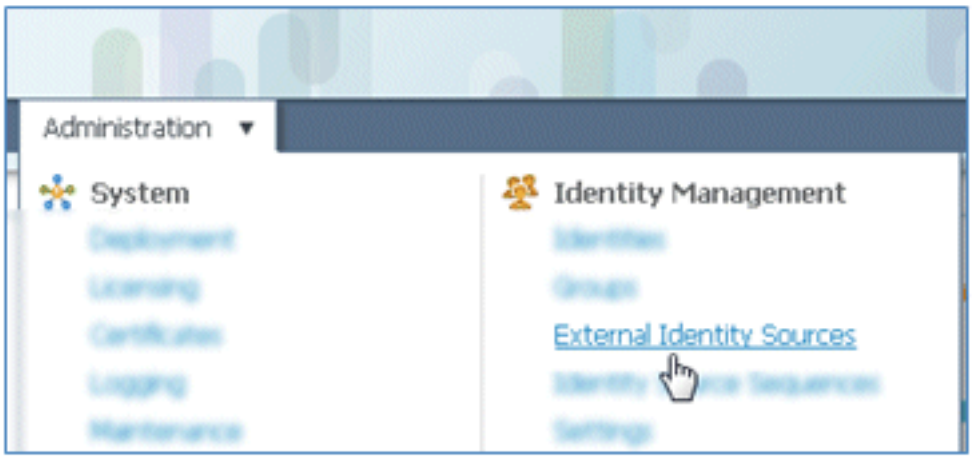
5. Klik op **Toepassen** en **Configuratie opslaan**.

ISE-configuratie

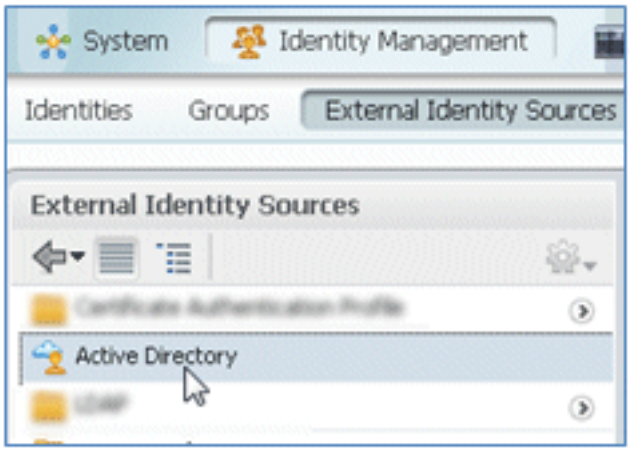
Voltooi de volgende stappen om de ISE te configureren:

1. Log in op de ISE-server: <*https://ise*>.

2. Ga naar **Beheer > Identiteitsbeheer > Externe Identiteitsbronnen**.

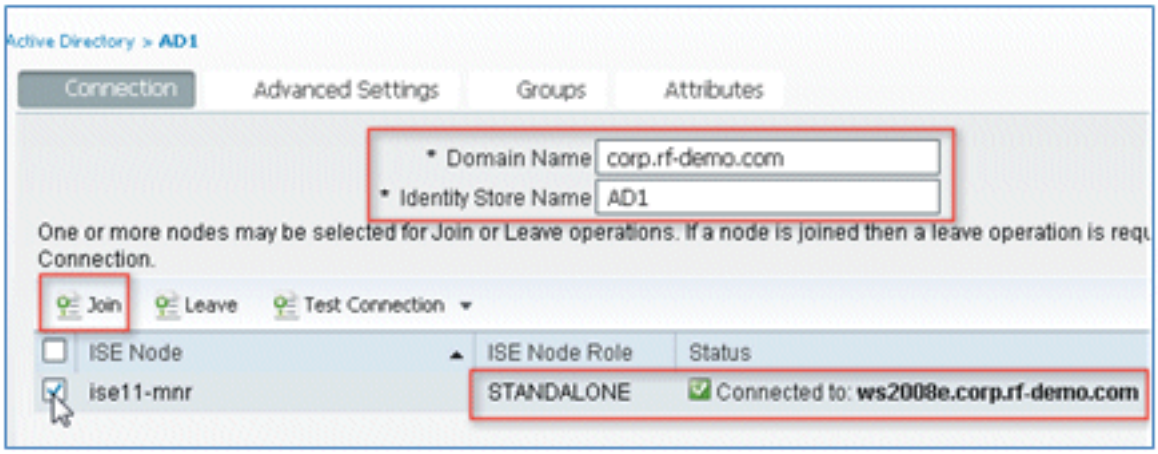


3. Klik op **Active Directory**.

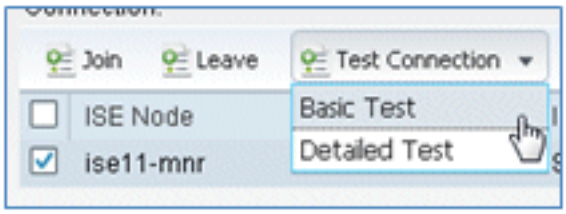


4. Op het tabblad Verbinding:

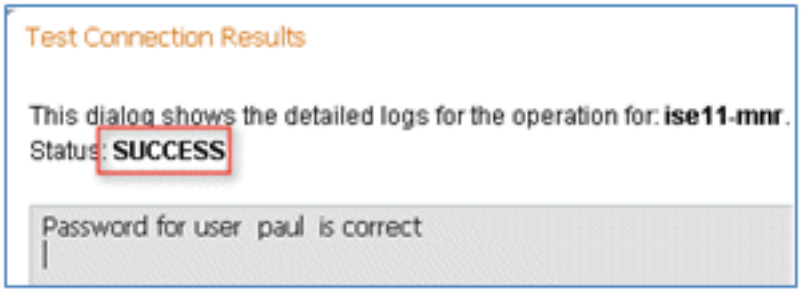
   Voeg de domeinnaam van **corp.rf-demo.com toe** (in dit voorbeeld) en verander de standaard Identity Store Name in **AD1**.Klik op **Configuratie opslaan**.Klik op **Lid worden** en geef de gebruikersnaam en het wachtwoord voor de AD Administrator-account op die vereist zijn om lid te worden.De status moet groen zijn. **Verbinding met** inschakelen**:** (dit vakje is ingeschakeld).



5. Voer met een huidige domeingebruiker een basisverbindingstest uit voor de advertentie.

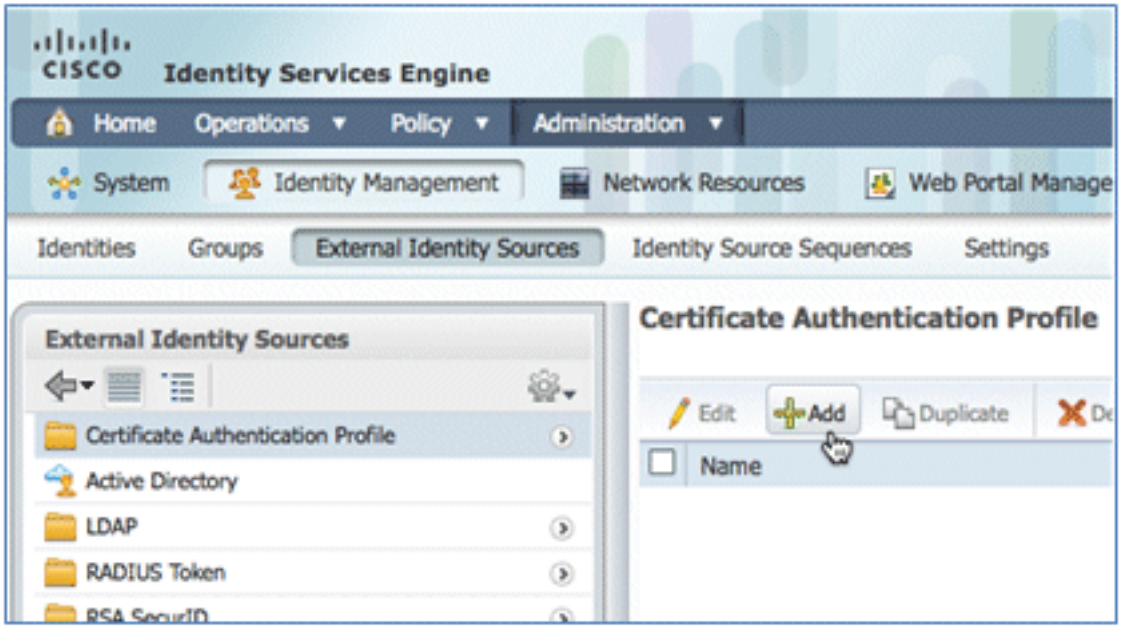


6. Als de verbinding met de AD succesvol is, wordt in een dialoogvenster bevestigd dat het wachtwoord correct is.

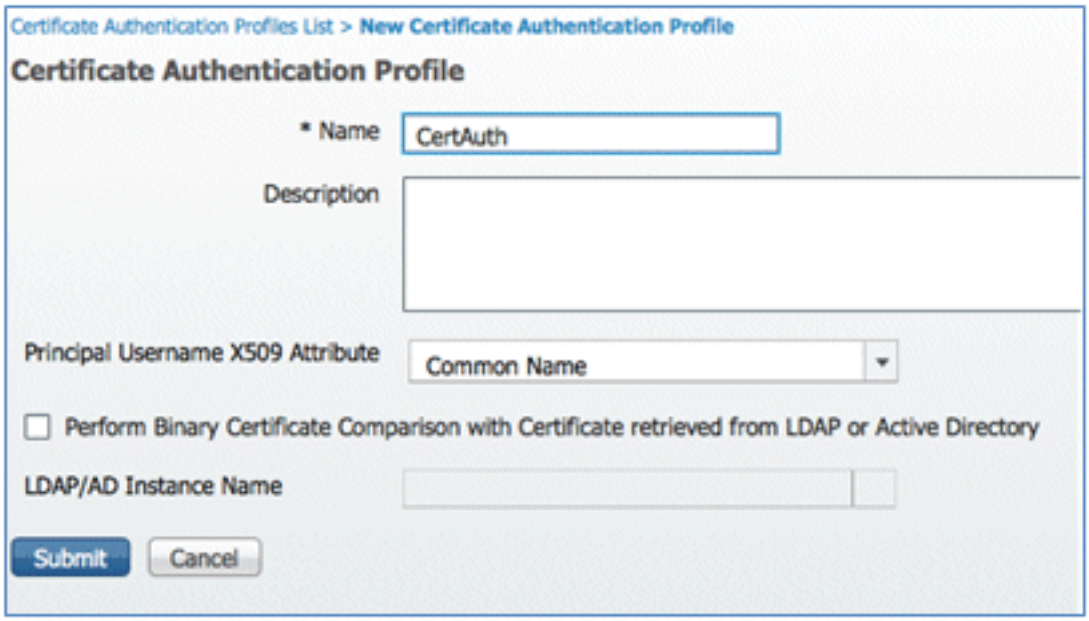


7. Ga naar **Administratie > Identiteitsbeheer > Externe Identiteitsbronnen**:

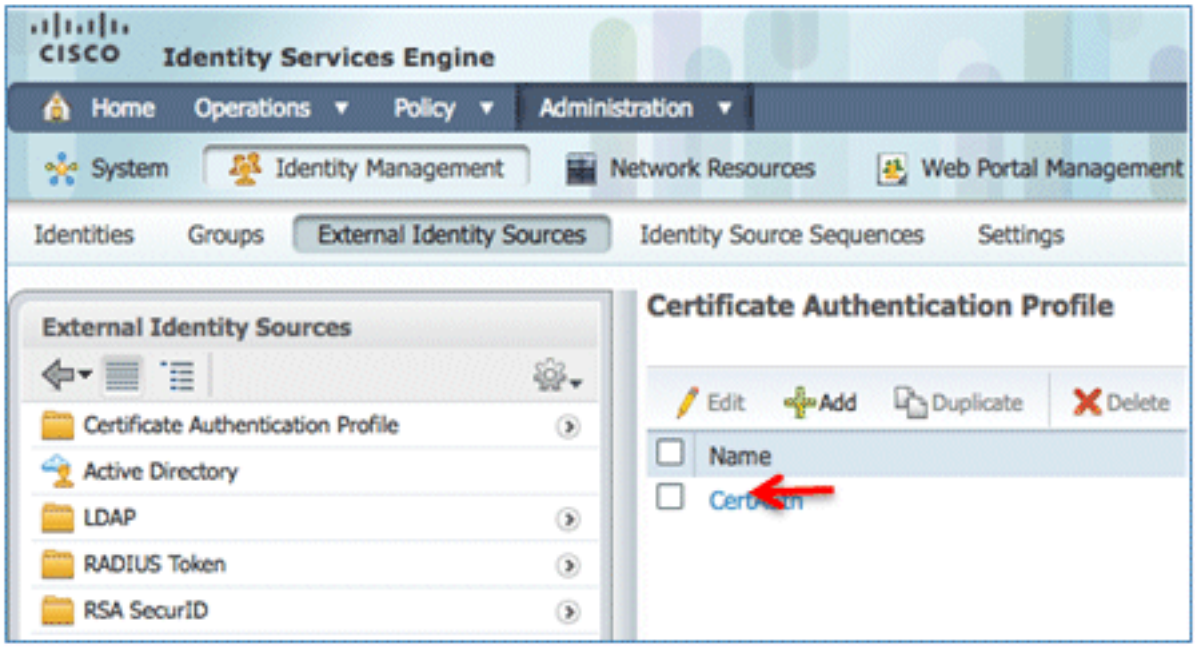
   Klik op **Certificaatverificatieprofiel**.Klik op **Add** om een nieuw certificaatverificatieprofiel (CAP) te selecteren.



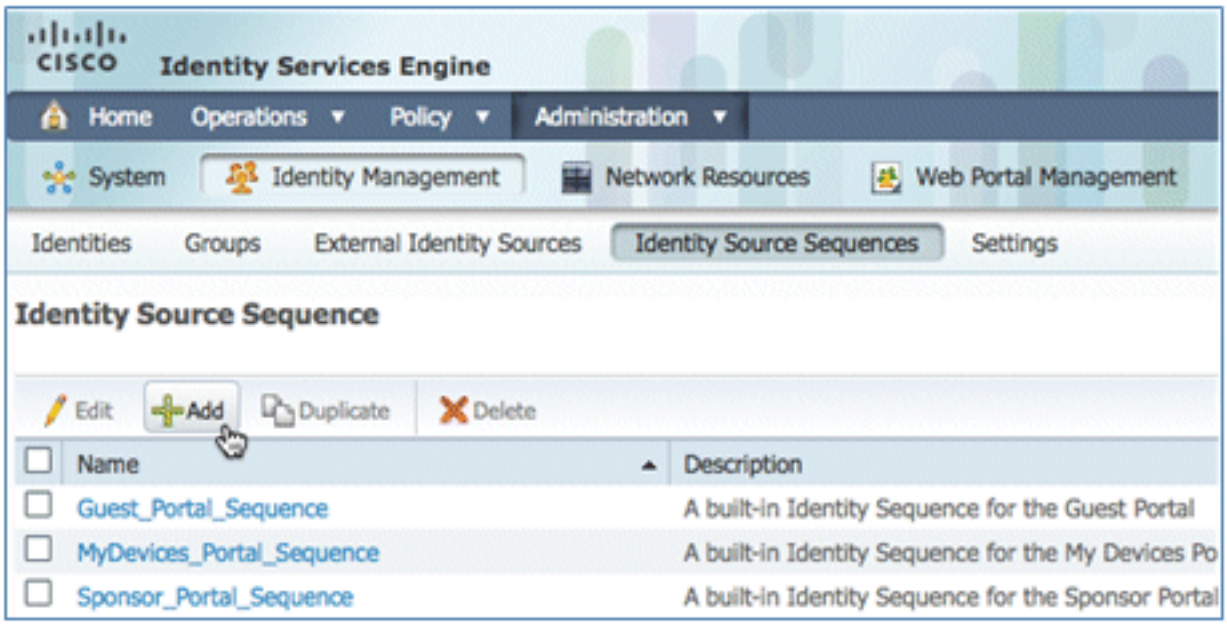
8. Voer een naam in van **CertAuth** (in dit voorbeeld) voor de CAP; voor het hoofdkenmerk X509 selecteert u **algemene naam**; klik vervolgens op **Indienen**.



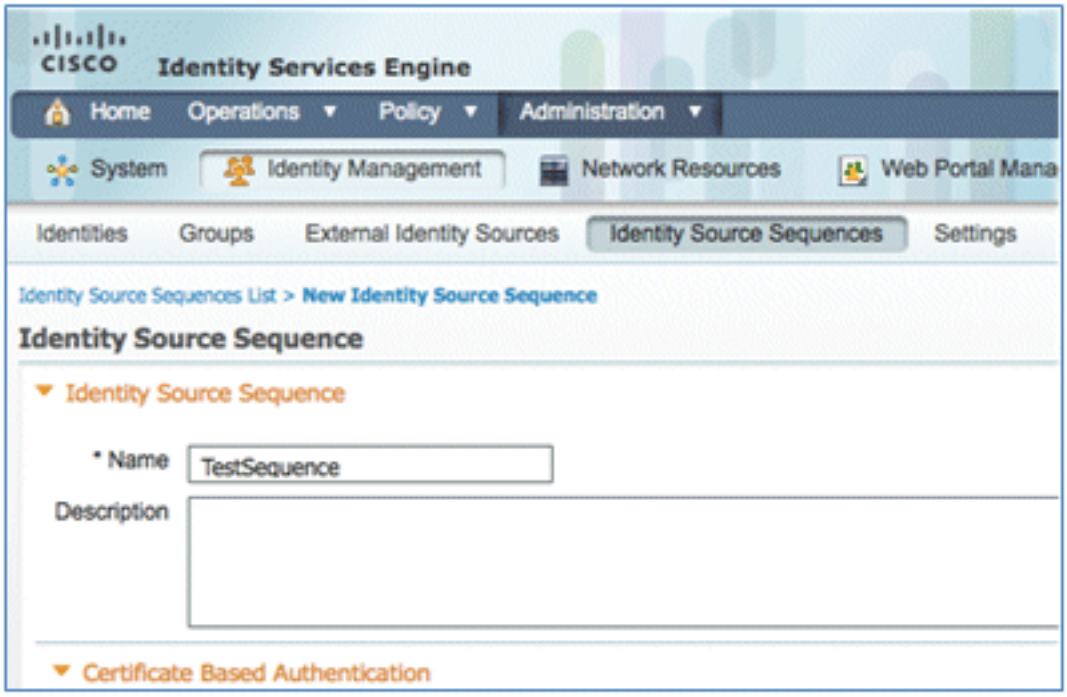
9. Bevestig dat het nieuwe GLB wordt toegevoegd.



10. Navigeer naar **Beheer > Identity Management > Identity Source Sequences** en klik op **Add** .

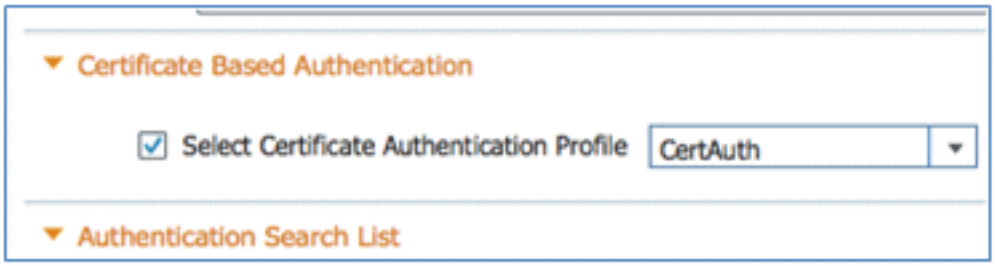


11. Geef de sequentie een naam van **TestSequence** (in dit voorbeeld).



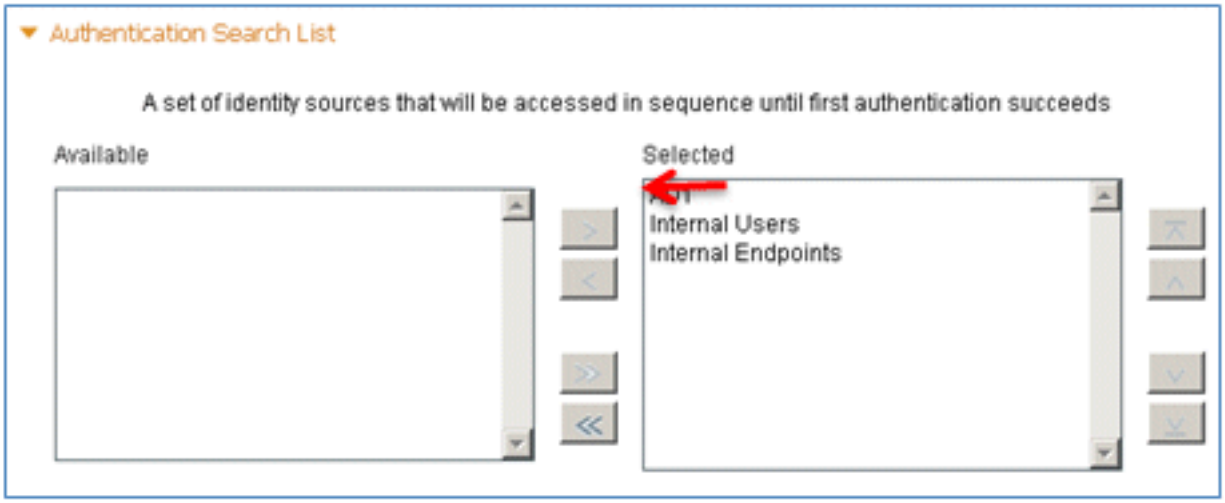
12. Blader naar beneden naar **op certificaat gebaseerde verificatie**:

    Schakel **de optie Certificaatverificatieprofiel** in (aangevinkt).Selecteer **Automatisch** (of een ander eerder gemaakt CAP-profiel).

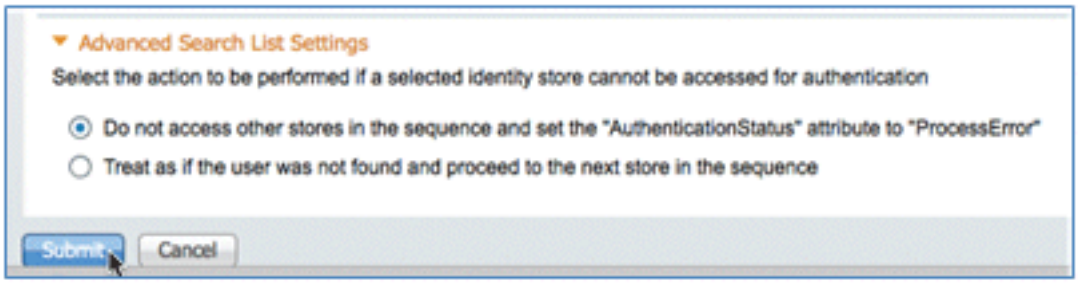


13. Scroll naar beneden naar **de zoeklijst voor verificatie**:

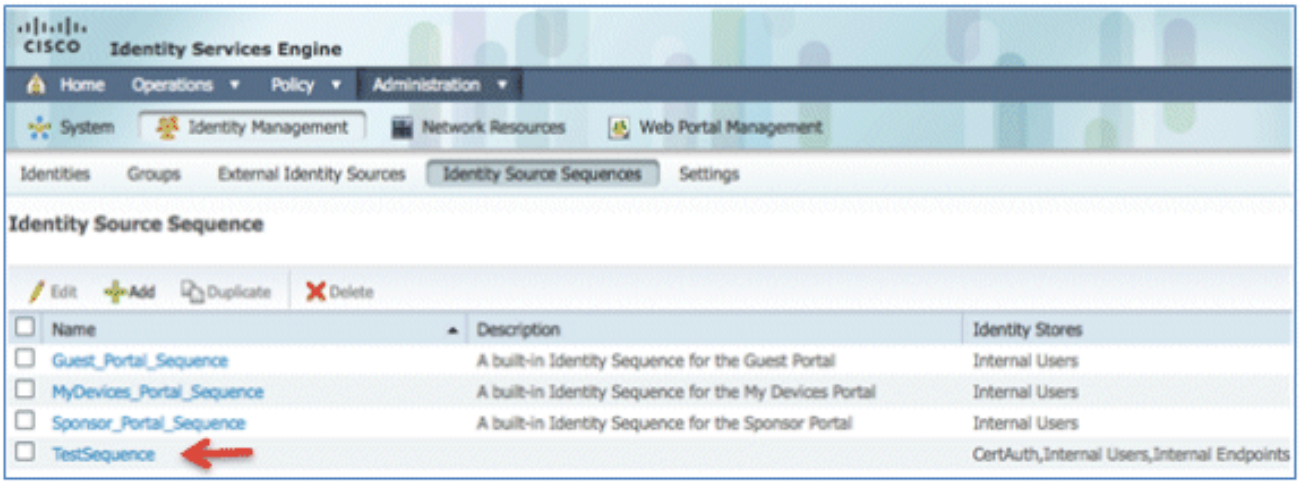
Verplaats AD1 van Beschikbaar naar Geselecteerd.Klik op de knop omhoog om AD1 naar de hoogste prioriteit te verplaatsen.



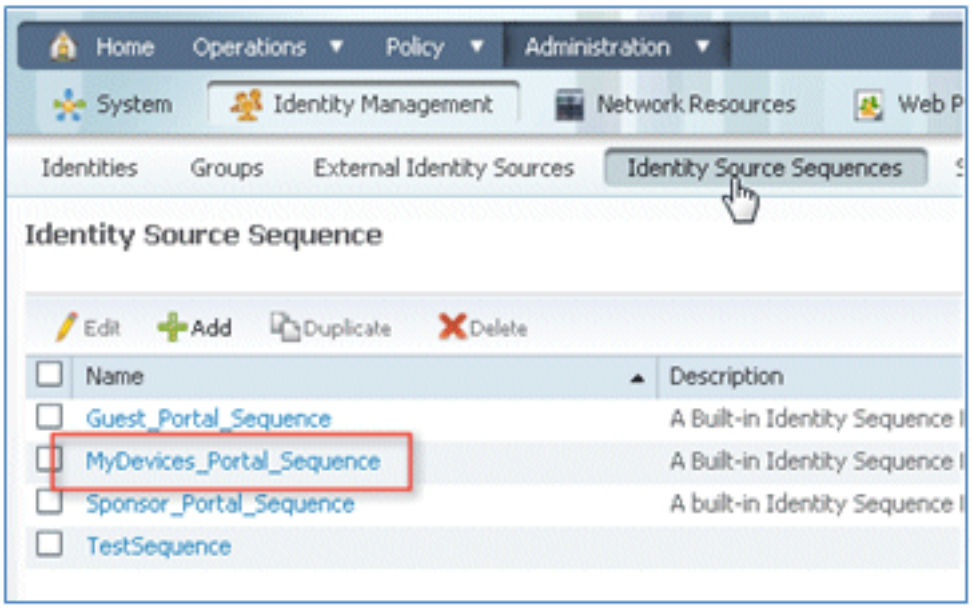
14. Klik op **Indienen** om op te slaan.



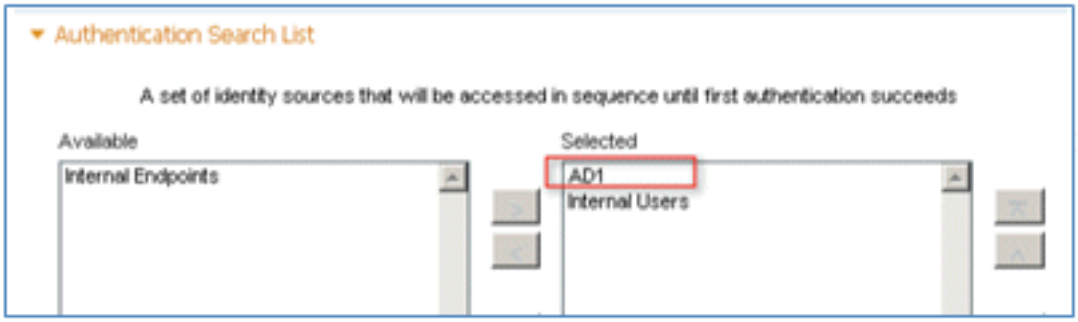
15. Bevestig dat de nieuwe Identity Source Sequence is toegevoegd.



16. Gebruik de AD om het My Devices Portal te verifiëren. Navigeer naar ISE > **Administration** > **Identity Management** > **Identity Source Sequence**, en bewerk **MyDevices_Portal_Sequence**.



17. Voeg **AD1** toe aan de geselecteerde lijst en klik op de knop omhoog om AD1 naar de hoogste prioriteit te verplaatsen.

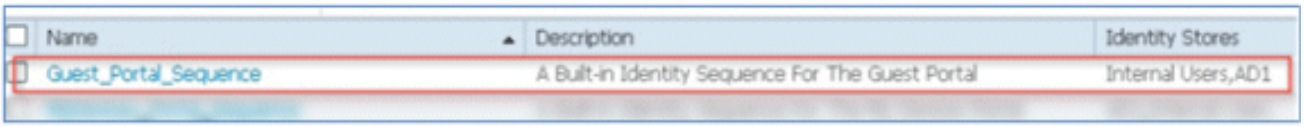


18. Klik op **Save** (Opslaan).

19. Bevestig dat de Identity Store-sequentie voor MyDevices_Portal_Sequence **AD1** bevat.

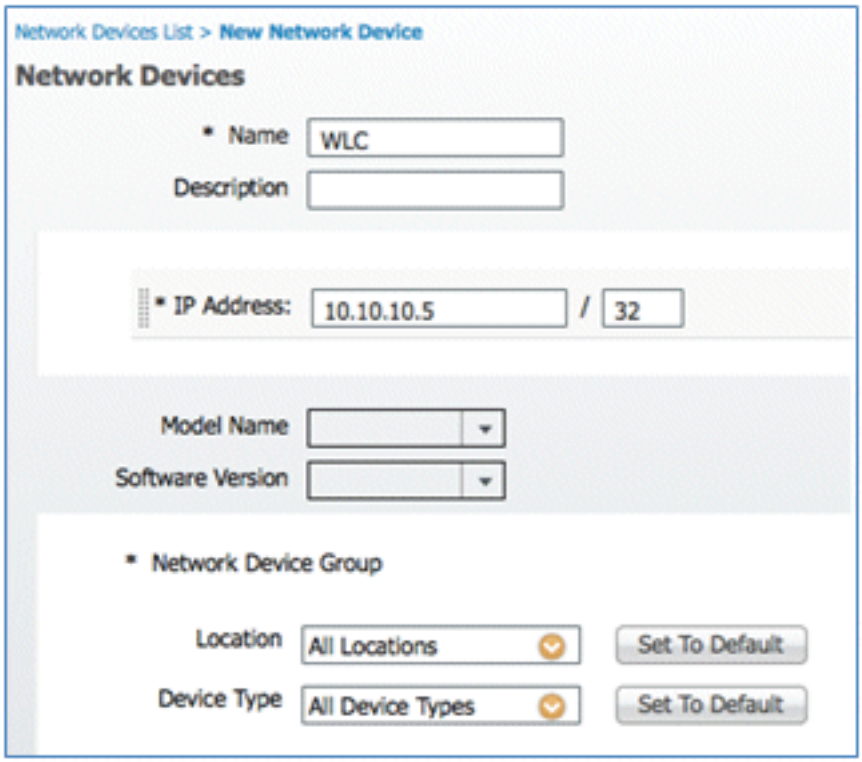
20. Herhaal stap 16-19 om AD1 voor Guest_Portal_Sequence toe te voegen en klik op **Opslaan**.

21. Bevestig dat Guest_Portal_Sequence **AD1** bevat.

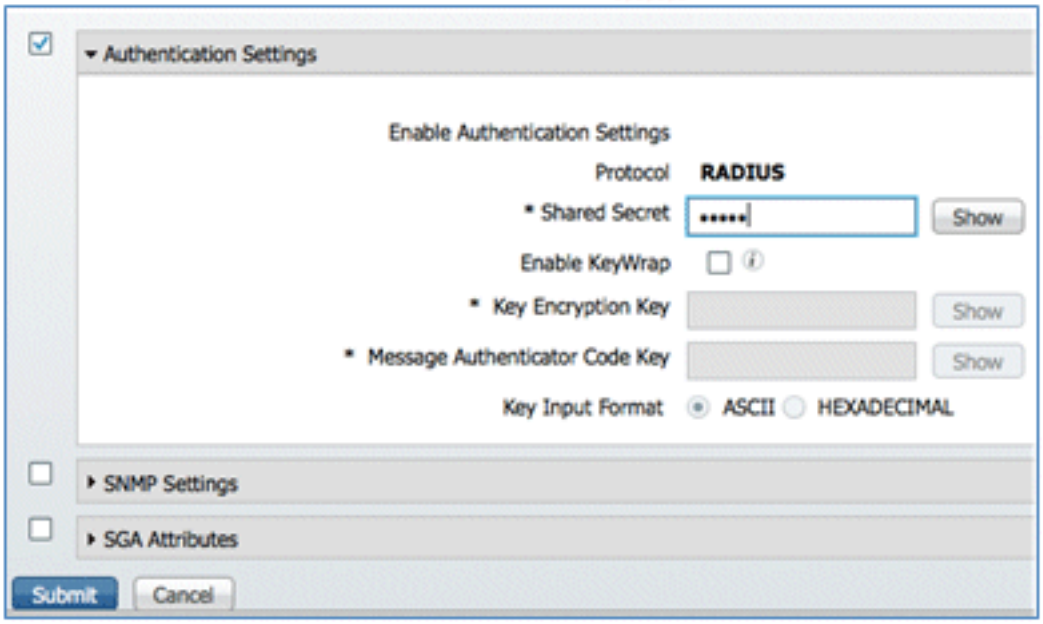


22. Als u WLC wilt toevoegen aan Network Access Device (WLC), navigeert u naar **Beheer > Network Resources > Network Devices** en klikt u op **Add**.

23. Voeg de WLC-naam, IP-adres, subnetmasker toe, enzovoort.

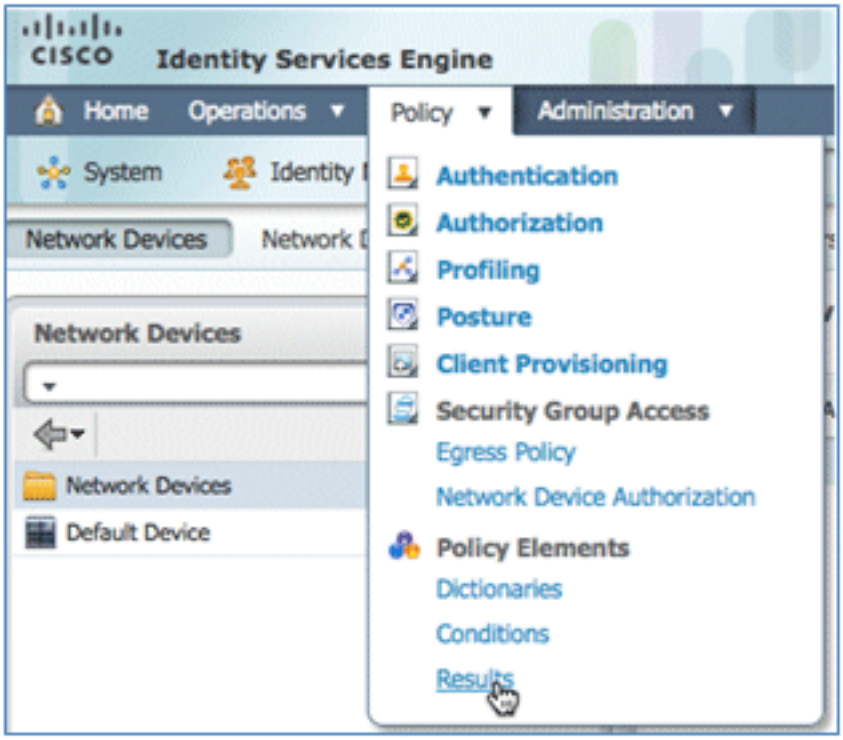


24. Blader naar beneden naar Verificatie-instellingen en voer het gedeelde geheim in. Dit moet overeenkomen met het gedeelde geheim van de WLC RADIUS.

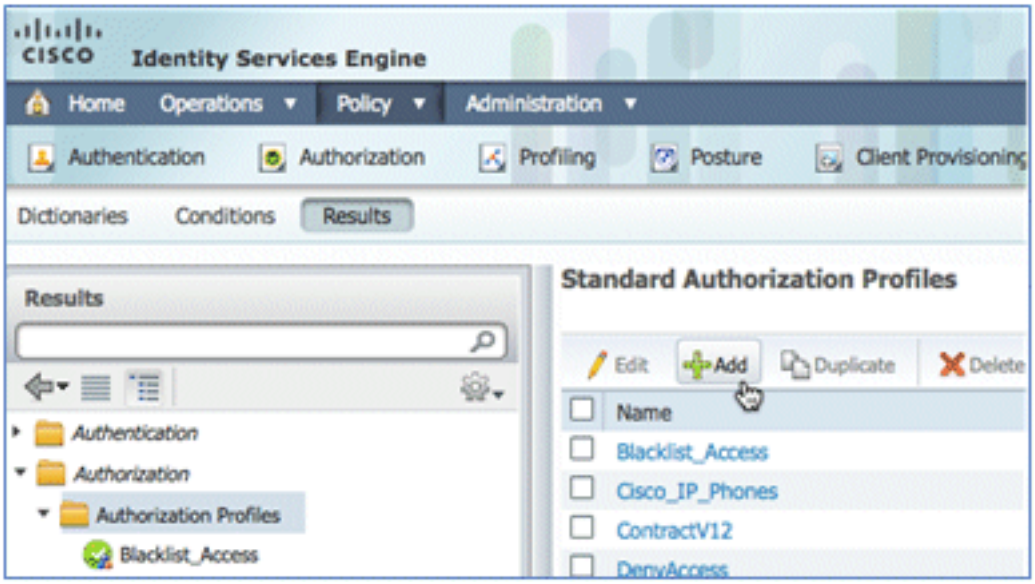


25. Klik op **Verzenden**.

26. Ga naar **ISE > Policy > Policy Elements > Results**.

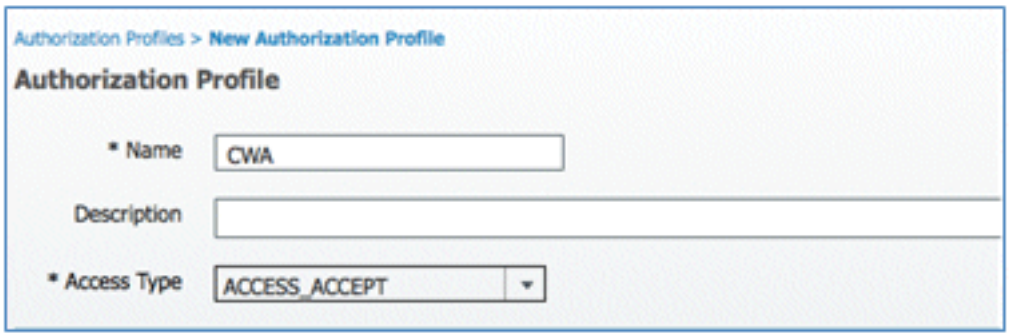


27. **Resultaten** en **autorisatie** uitvouwen, klik op **Autorisatieprofielen** en klik op **Toevoegen** voor een nieuw profiel.



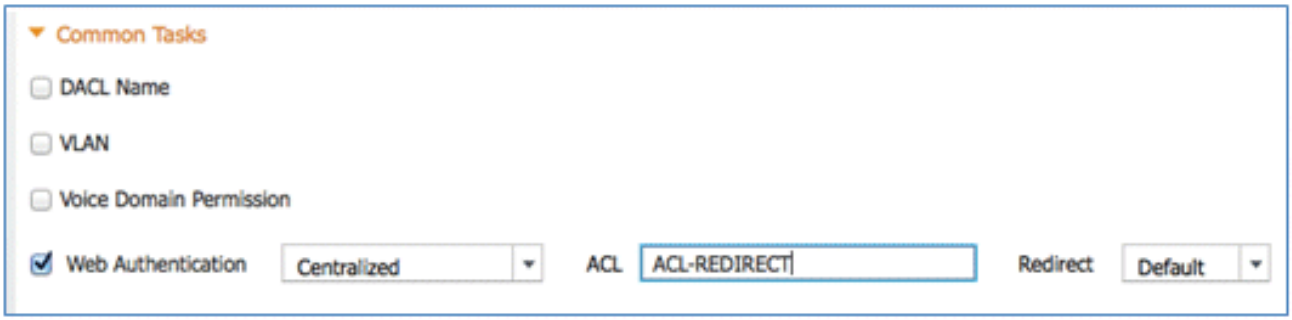
28. Geef dit profiel de volgende waarden:

    Naam: **CWA**

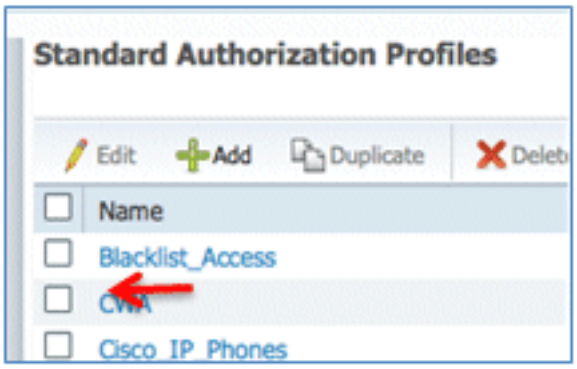


Webverificatie inschakelen (aangevinkt):

Web verificatie: **gecentraliseerd**ACL: **ACL-REDIRECT** (dit moet overeenkomen met de vooraf ingestelde WLC ACL-naam.)Omleiden: **standaard**



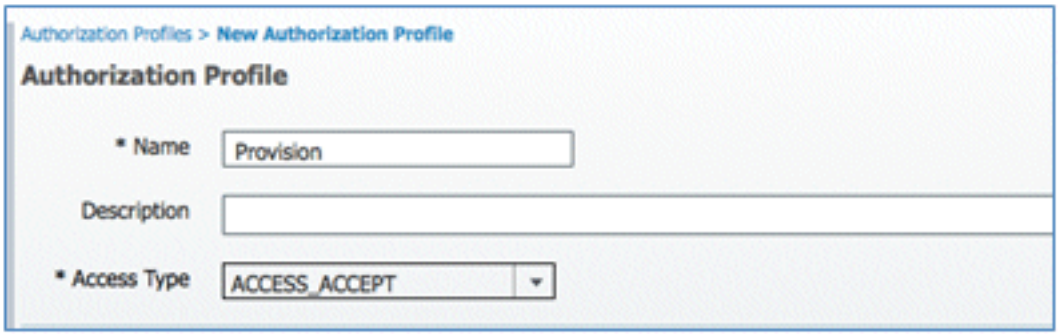
29. Klik op **Indienen** en bevestig dat het CWA-autorisatieprofiel is toegevoegd.



30. Klik op **Add** om een nieuw autorisatieprofiel te maken.

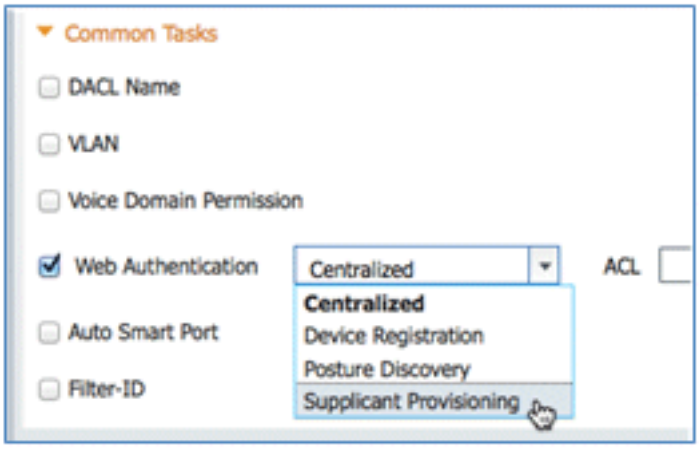
31. Geef dit profiel de volgende waarden:

    Naam: **Voorziening**

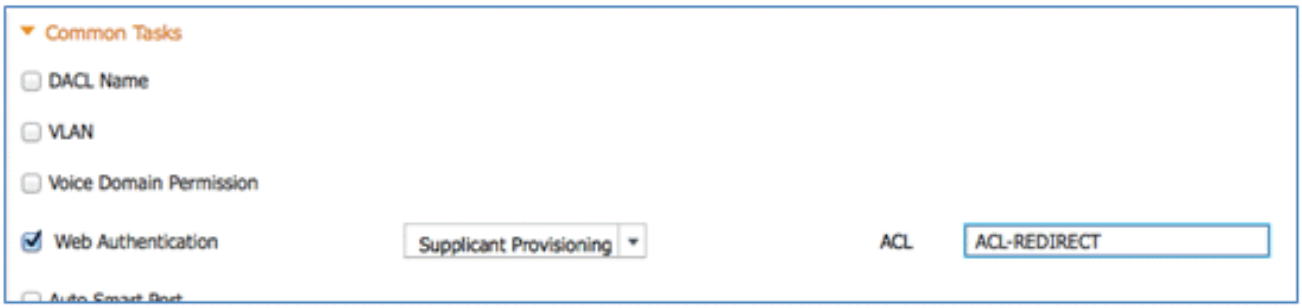


    Webverificatie inschakelen (aangevinkt):

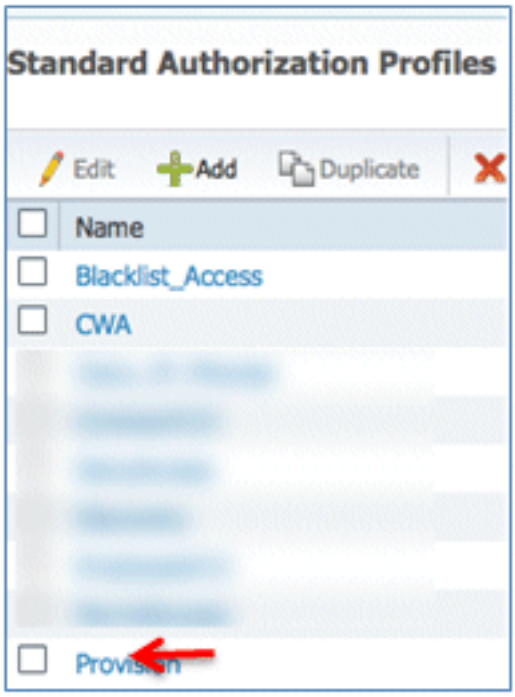
    Web verificatie Value: **Supplicant Provisioning**



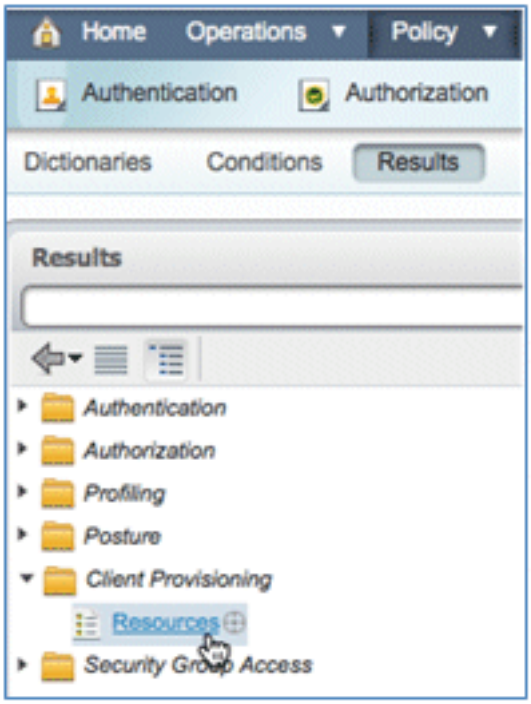
    ACL: **ACL-REDIRECT** (dit moet overeenkomen met de vooraf ingestelde WLC ACL-naam.)



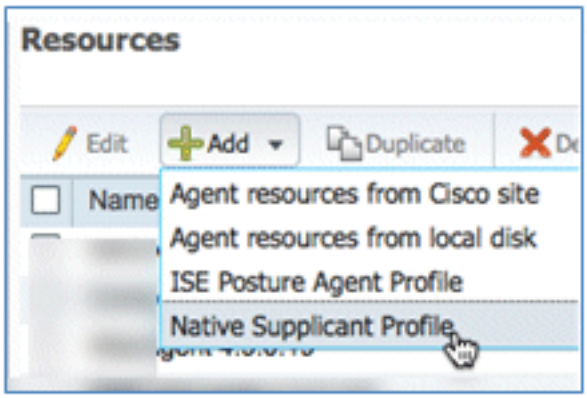
32. Klik op **Indienen** en bevestig dat het Provision-autorisatieprofiel is toegevoegd.



33. Scroll naar beneden in Resultaten, vouw **Clientprovisioning** uit en klik op **Resources**.



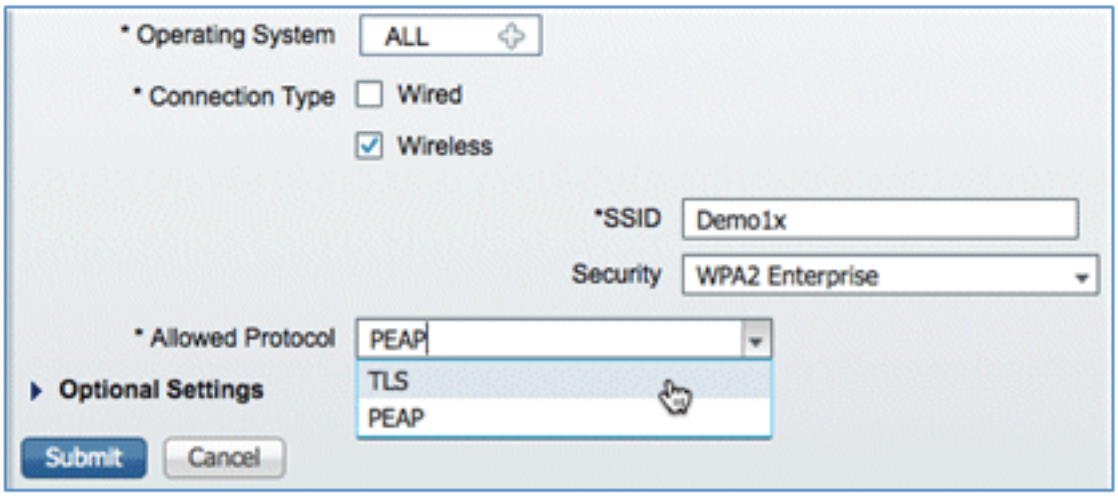
34. Selecteer het **profiel van de native aanvrager**.



35. Geef het profiel een naam voor **WirelessSP** (in dit voorbeeld).

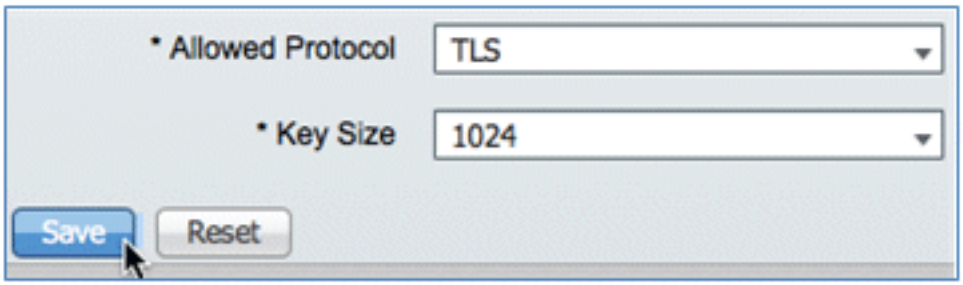
36. Voer deze waarden in:

    Type verbinding: **draadloos**SSID: **Demo1x** (deze waarde is afkomstig van de WLC 802.1x WLAN-configuratie)Toegestaan protocol: **TLS**Sleutelgrootte: **1024**

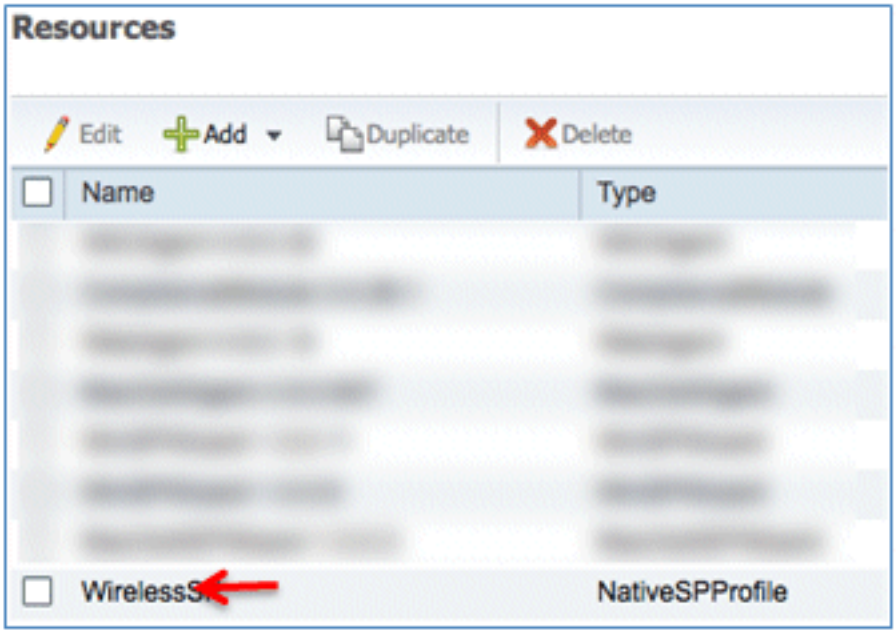


37. Klik op **Verzenden**.

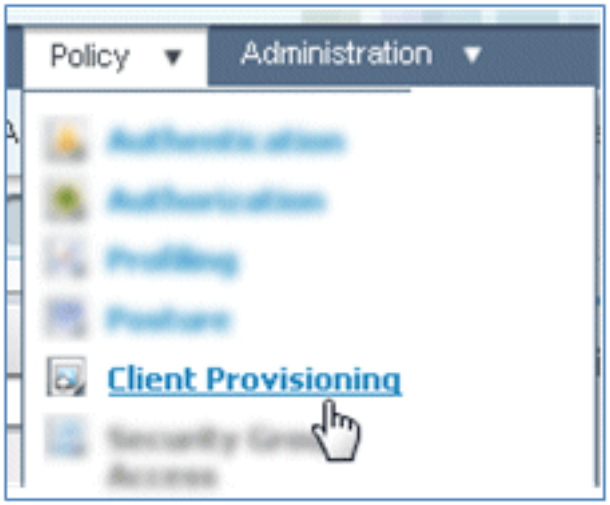
38. Klik op **Save** (Opslaan).



39. Controleer of het nieuwe profiel is toegevoegd.

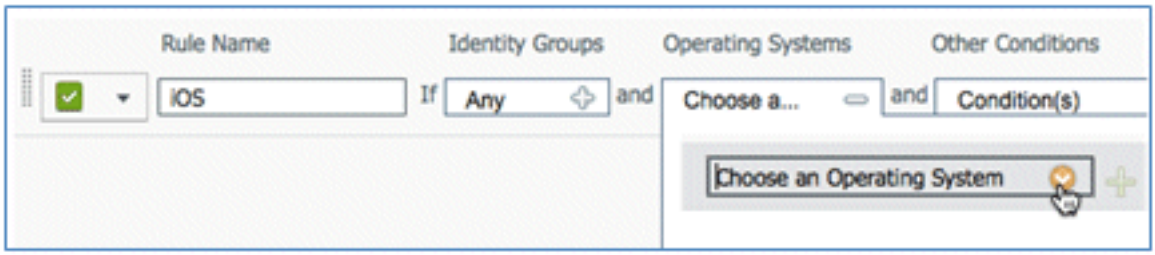


40. Ga naar **Beleid > Clientprovisioning**.

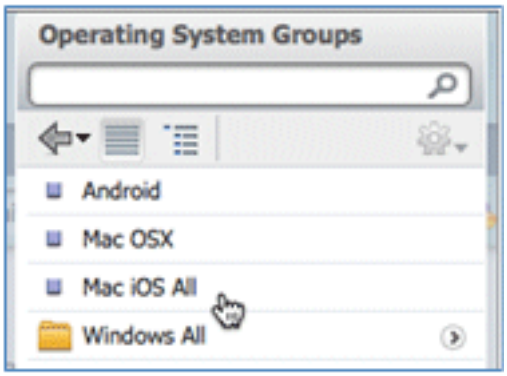


41. Geef deze waarden op voor de provisioningregel van iOS-apparaten:

    Regel Naam: **iOS**Identiteitsgroepen: **alle**

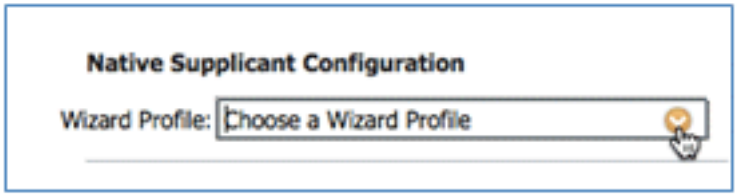


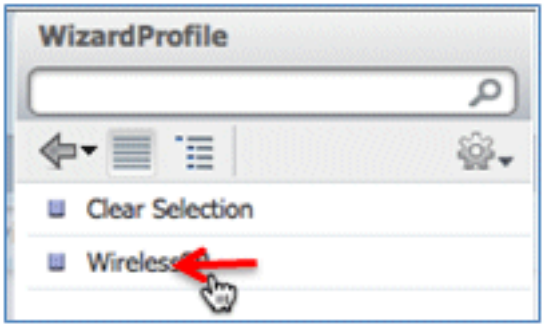
Besturingssystemen: **Mac iOS All**



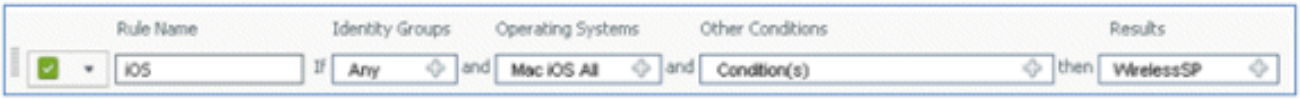
Resultaten: **WirelessSP** (dit is het Native Supplicant Profile dat eerder is gemaakt)

Navigeer naar **Resultaten** > **Wizard Profiel** (vervolgkeuzelijst) > **WirelessSP**.

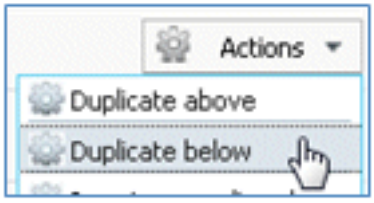




42. Bevestig dat het iOS Provisioning Profile is toegevoegd.

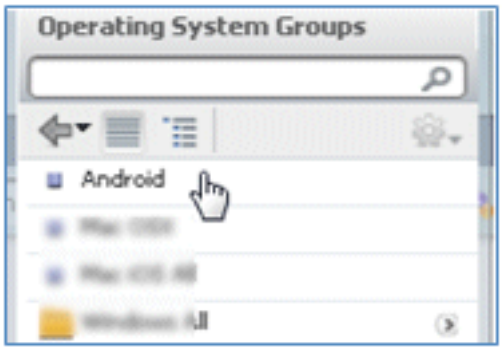


43. Zoek in de rechterkant van de eerste regel de vervolgkeuzelijst Acties en selecteer **hieronder** (of hierboven) **Dupliceren**.



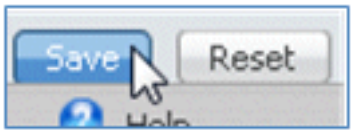
44. Wijzig de naam van de nieuwe regel in **Android**.

45. Verander de besturingssystemen naar **Android**.

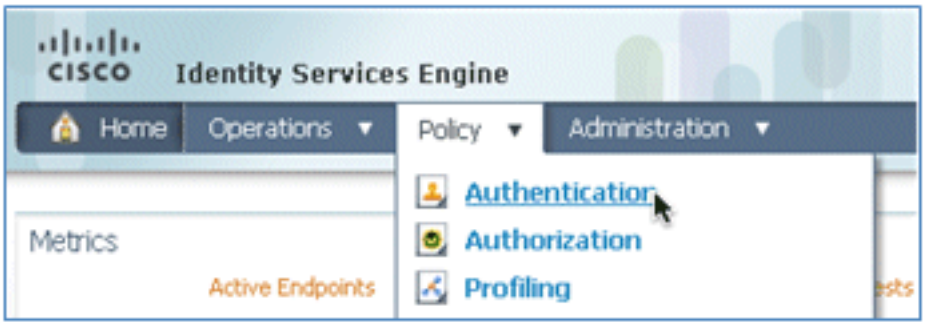


46. Laat andere waarden ongewijzigd.

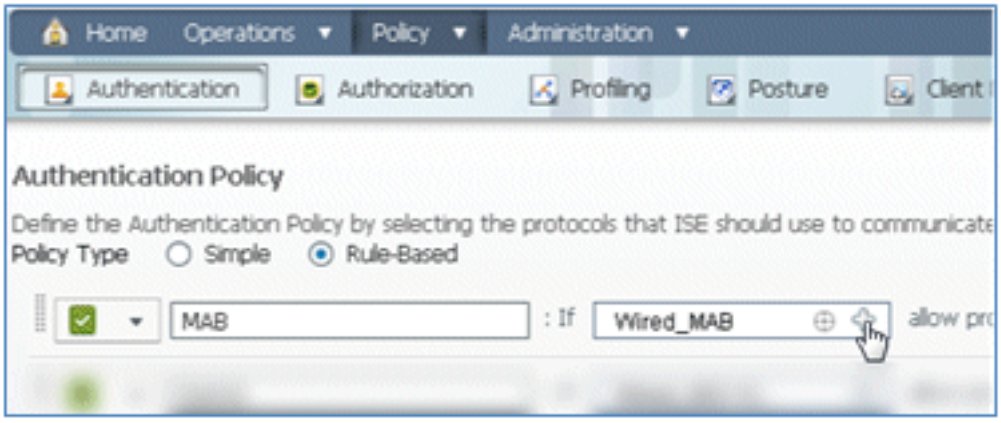
47. Klik op **Opslaan** (linkerbenedenscherm).



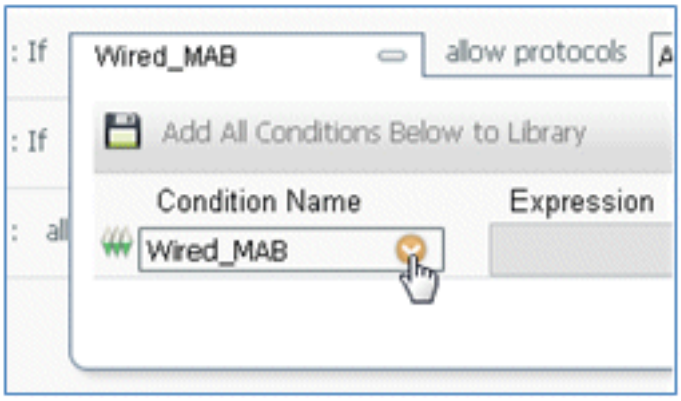
48. Navigeer naar **ISE > Policy > Authenticatie**.



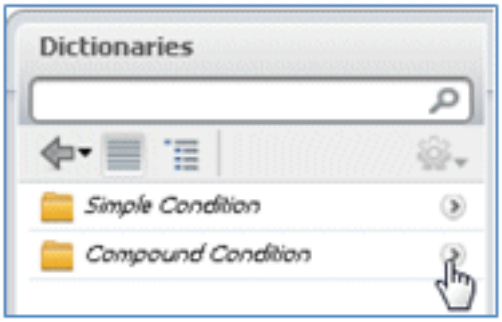
49. Wijzig de voorwaarde om Wireless_MAB te omvatten, en breid **Wired_MAB** uit.



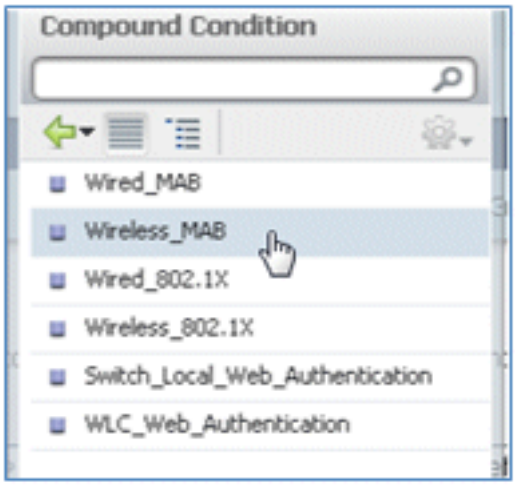
50. Klik op de vervolgkeuzelijst **Condition Name**.



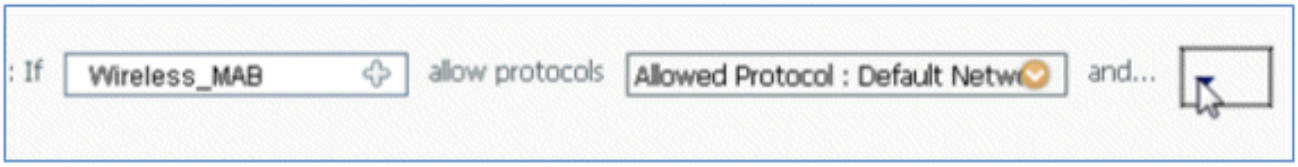
51. Selecteer **Woordenboeken** > **Samengestelde staat**.



52. Selecteer **Wireless_MAB**.

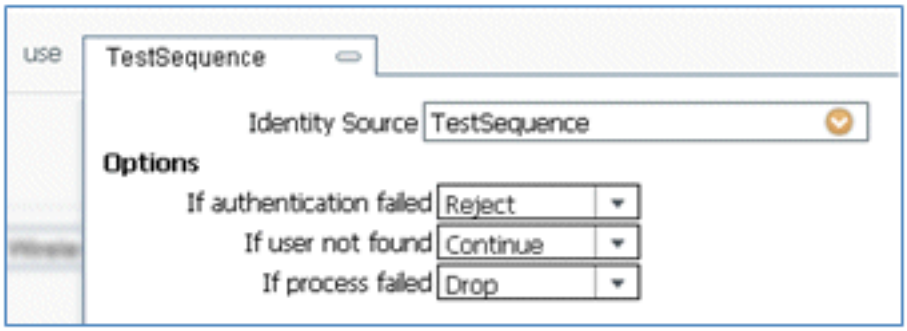


53. Selecteer de pijl rechts van de regel die u wilt uitvouwen.

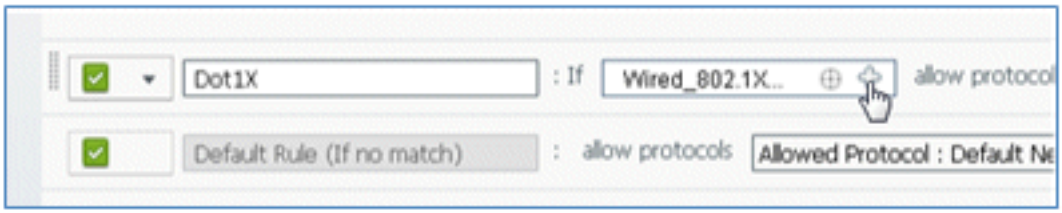


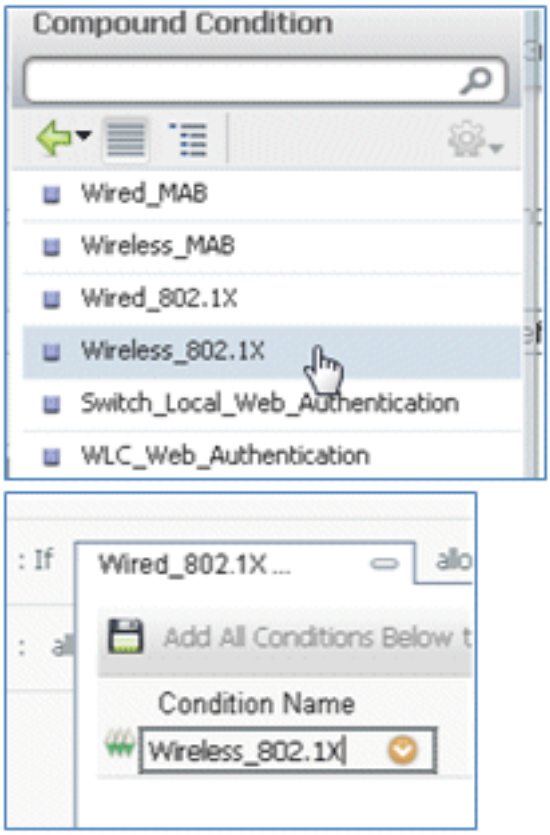
54. Selecteer deze waarden in de vervolgkeuzelijst.

    Identiteitsbron: **TestSequence** (dit is de waarde die eerder is gemaakt)Indien verificatie mislukt: **Afwijzen**Als gebruiker niet gevonden: **Doorgaan**Als proces is mislukt: **Drop**



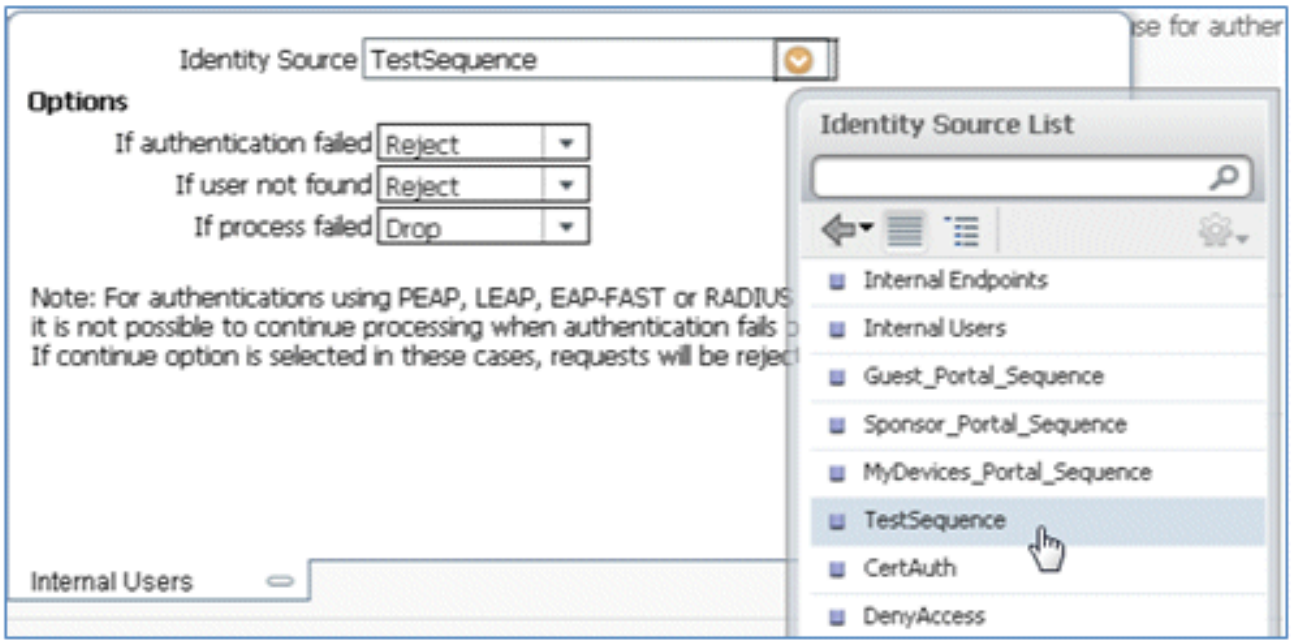
55. Ga naar de **Dot1X-**regel en wijzig deze waarden:





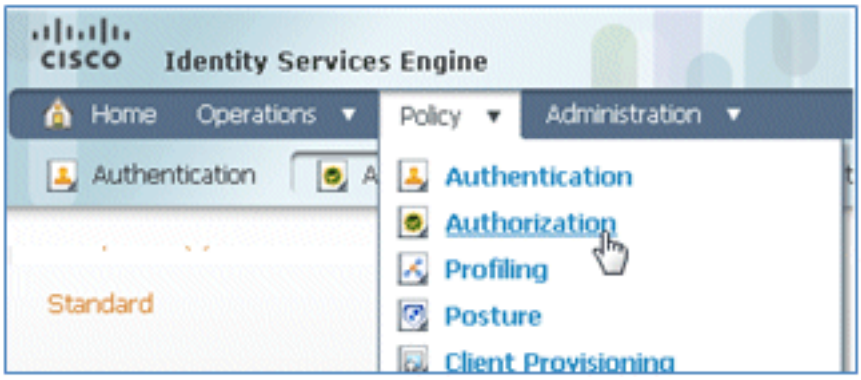
Voorwaarde: **Wireless_802.1X**

Identiteitsbron: **TestSequence**

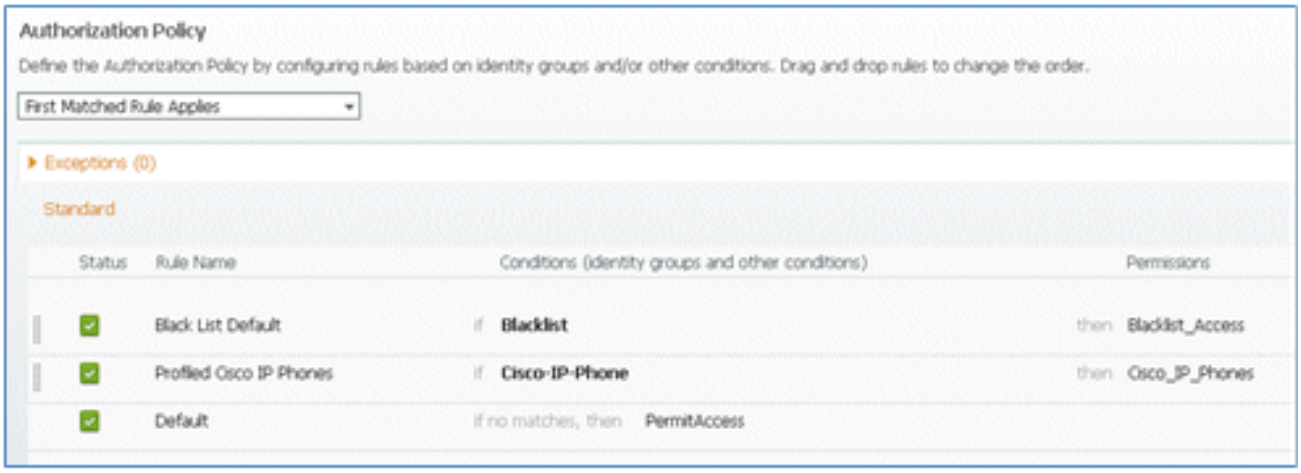


56. Klik op **Save** (Opslaan).

57. Blader naar **ISE > Policy > Authorisation**.



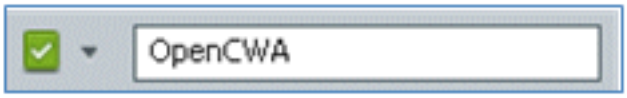
58. Standaardregels (zoals Standaard zwarte lijst, Profiled en Standaard) zijn al vanaf de installatie geconfigureerd; de eerste twee kunnen worden genegeerd; de Standaardregel wordt later bewerkt.



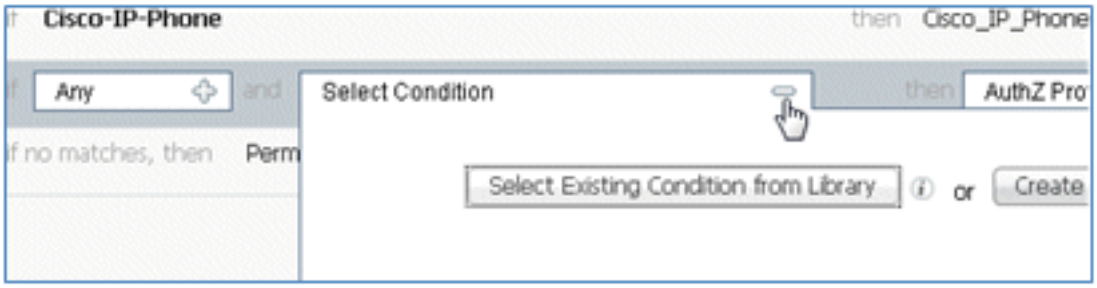
59. Klik rechts van de tweede regel (geprofileerde Cisco IP-telefoons) op het pijltje omlaag naast Bewerken en selecteer **Hieronder nieuwe regel invoegen**.

Er wordt een nieuwe standaardregel # toegevoegd.

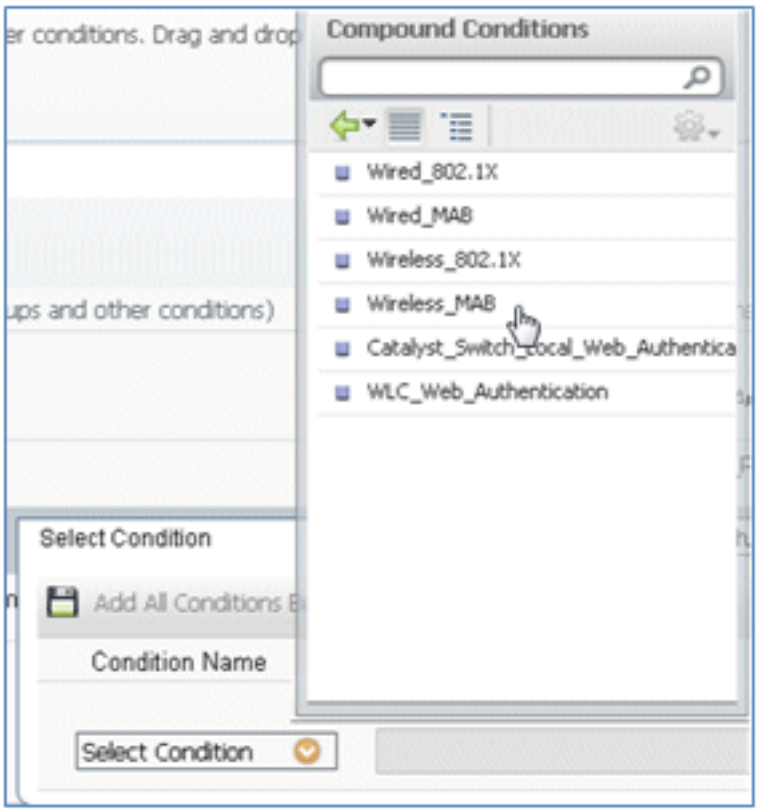
60. Verander de naam van de regel van Standaardregel # in **OpenCWA**. Deze regel start het registratieproces op het open WLAN (dual SSID) voor gebruikers die naar het gastnetwerk komen om apparaten te hebben geleverd.



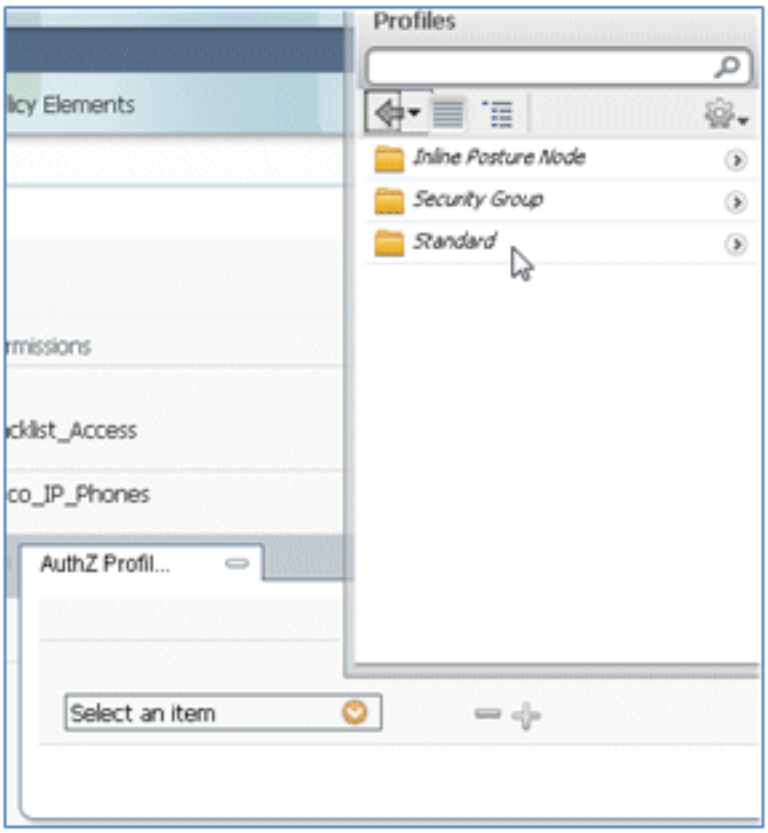
61. Klik op het plusteken (**+**) voor Voorwaarde(n) en klik op **Bestaande Voorwaarde uit bibliotheek selecteren**.



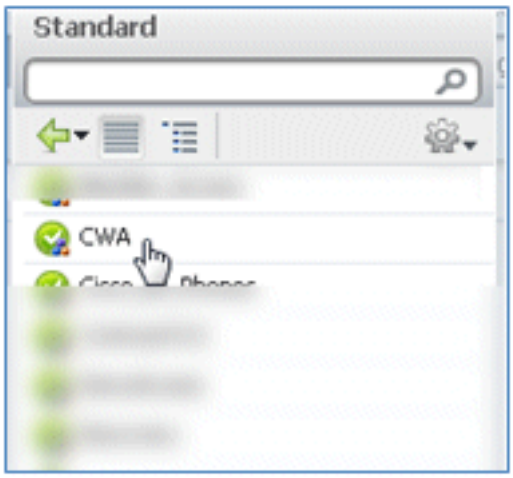
62. Selecteer **Samengestelde voorwaarden > Wireless_MAB**.



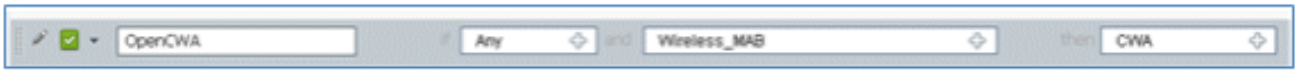
63. Klik in het AuthZ-profiel op het plusteken (**+**) en selecteer **Standaard**.



64. Selecteer de standaard **CWA** (dit is het autorisatieprofiel dat eerder is gemaakt).



65. Bevestig dat de regel wordt toegevoegd met de juiste voorwaarden en autorisatie.



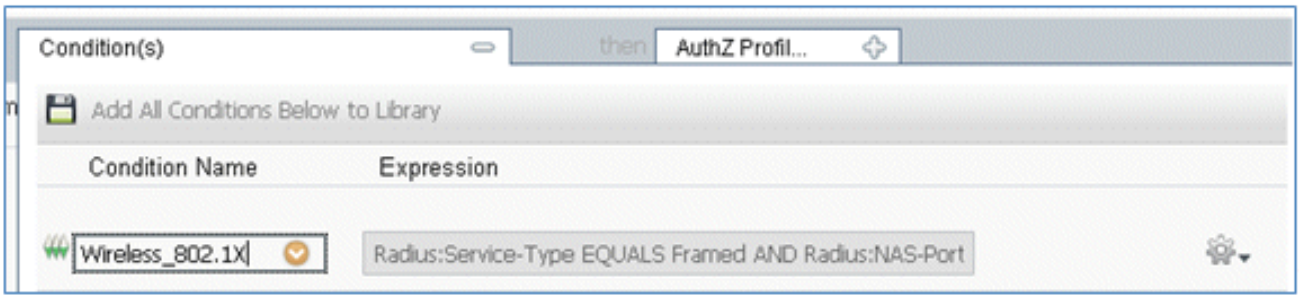
66. Klik op **Gereed** (rechts van de regel).

67. Klik rechts van dezelfde regel op het pijltje omlaag naast Bewerken en selecteer **Hieronder**

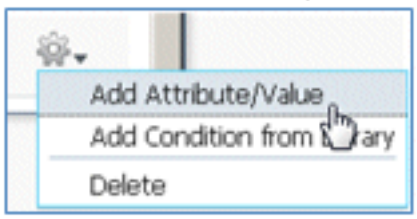
nieuwe regel invoegen.

68. Wijzig de naam van de regel van standaardregel # in **PEAP-regel** (in dit voorbeeld). Deze regel is voor PEAP (ook gebruikt voor één SSID-scenario) om te controleren dat verificatie van 802.1X zonder Transport Layer Security (TLS) en dat netwerkprovider-provisioning wordt gestart met het eerder gemaakte provisioningprofiel.

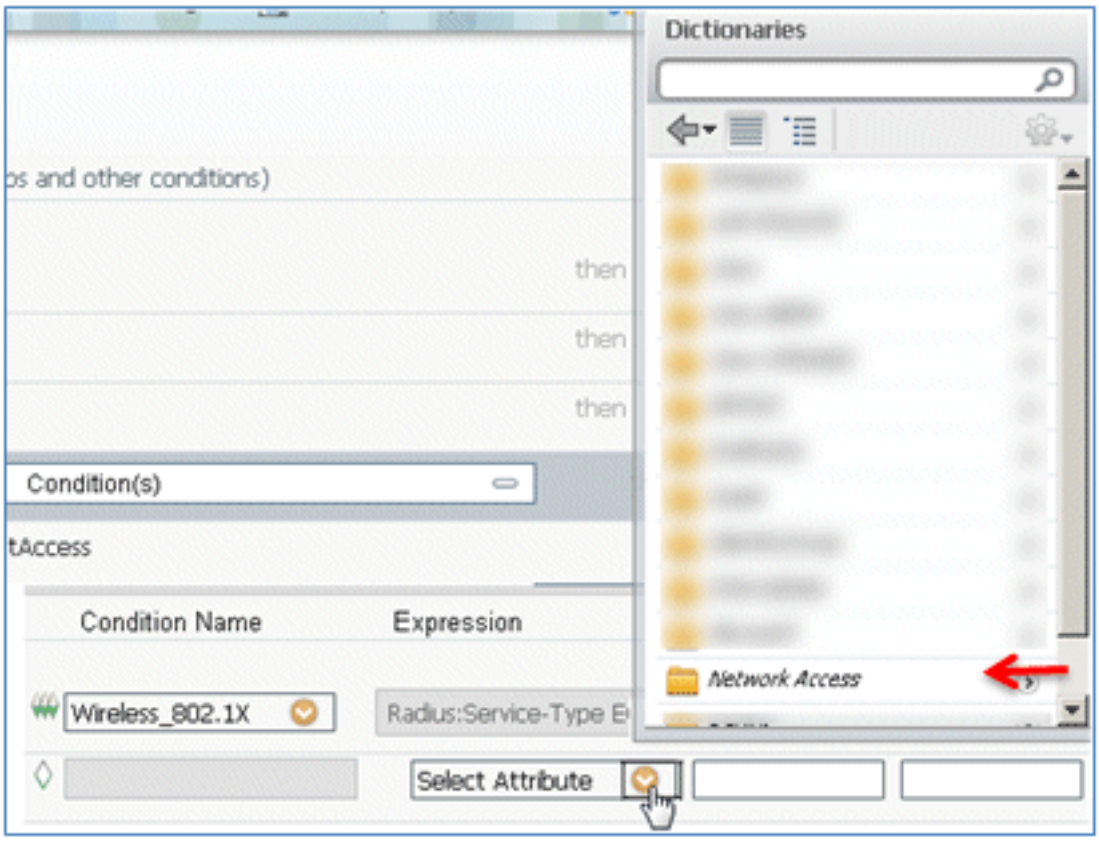
69. Verander de Voorwaarden in **Wireless_802.1X**.



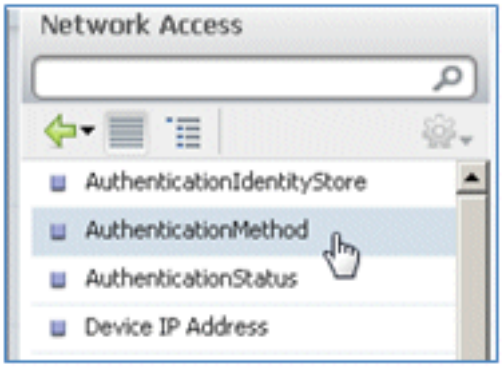
70. Klik op het tandwielpictogram aan de rechterkant van de voorwaarde en selecteer **Kenmerk/waarde toevoegen**. Dit is een 'en'-voorwaarde, geen 'of'-voorwaarde.



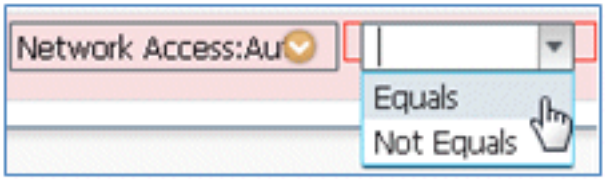
71. Zoek en selecteer **Netwerktoegang**.



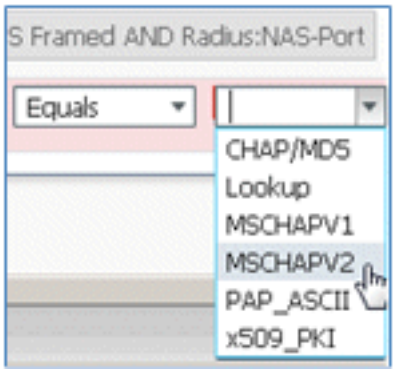
72. Selecteer **Verificatiemethode** en voer deze waarden in:



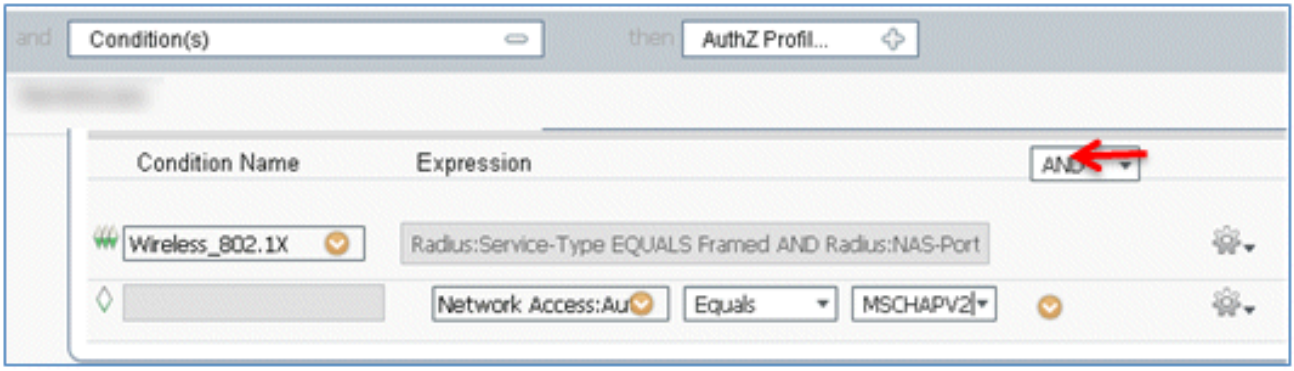
Authenticatiemethode: **Gelijk**



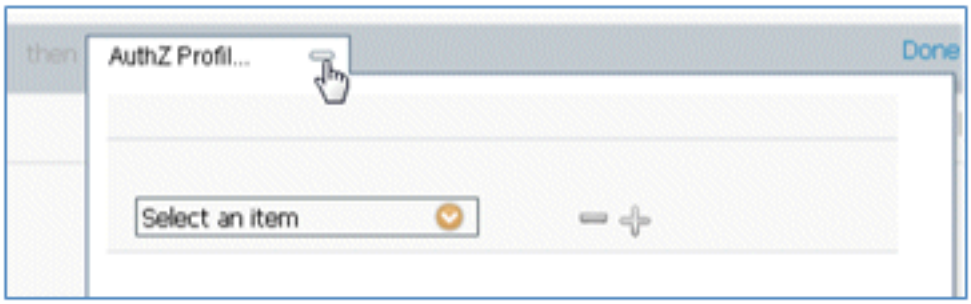
Selecteer **MSCHAPV2**.

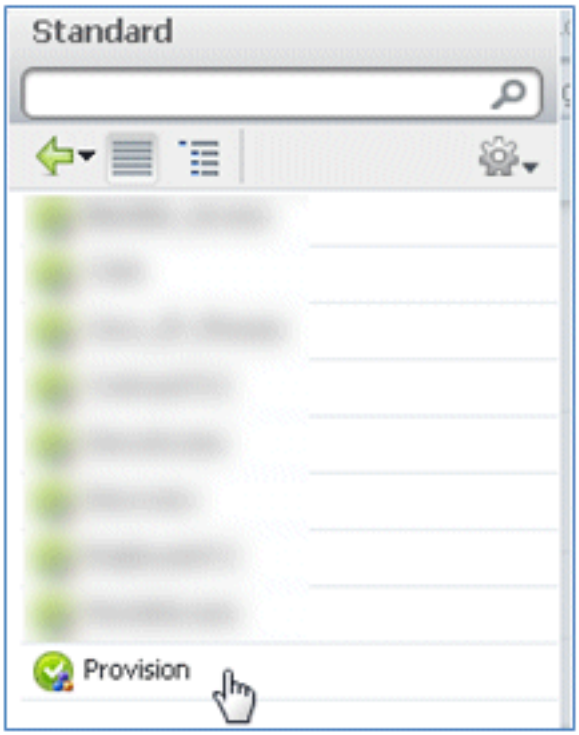


Dit is een voorbeeld van de regel; ben zeker om te bevestigen dat de voorwaarde een EN is.



73. Selecteer in het profiel AuthZ de optie **Standaard > Voorziening** (dit is het profiel voor autorisatie dat eerder is gemaakt).

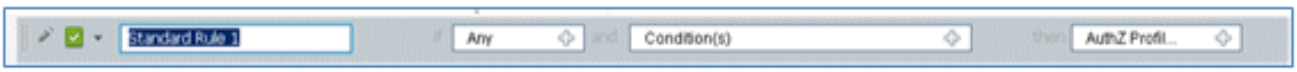




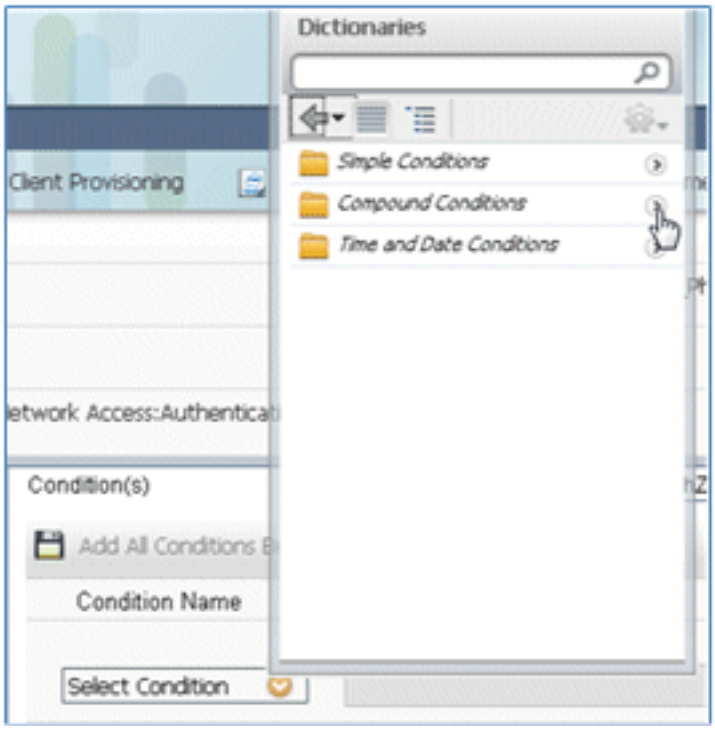
74. Klik op **Gereed**.

75. Klik rechts van de PEAP-regel op het pijltje-omlaag naast Bewerken en selecteer **Nieuwe regel invoegen hieronder**.

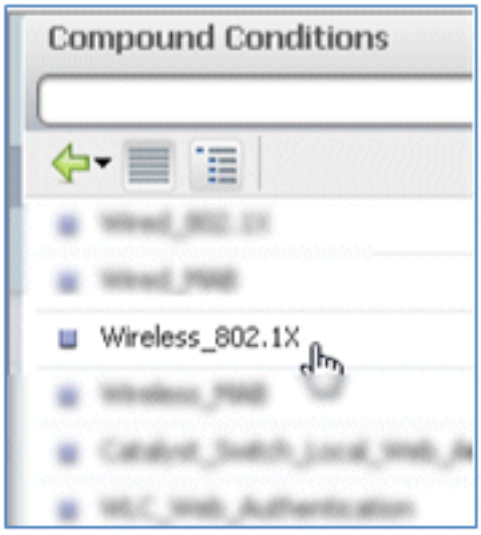
76. Verander de naam van de regel van Standaardregel # om **Regel toe** te **staan** (in dit voorbeeld). Deze regel zal worden gebruikt om toegang tot geregistreerde apparaten met geïnstalleerde certificaten toe te staan.



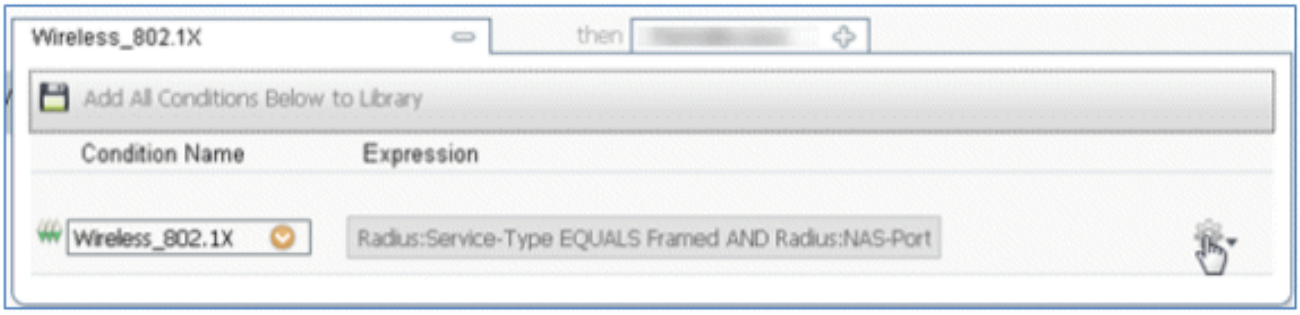
77. Selecteer onder Conditie(s) de optie **Samengestelde voorwaarden**.



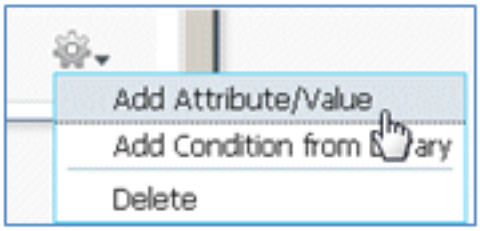
78. Selecteer **Wireless_802.1X**.



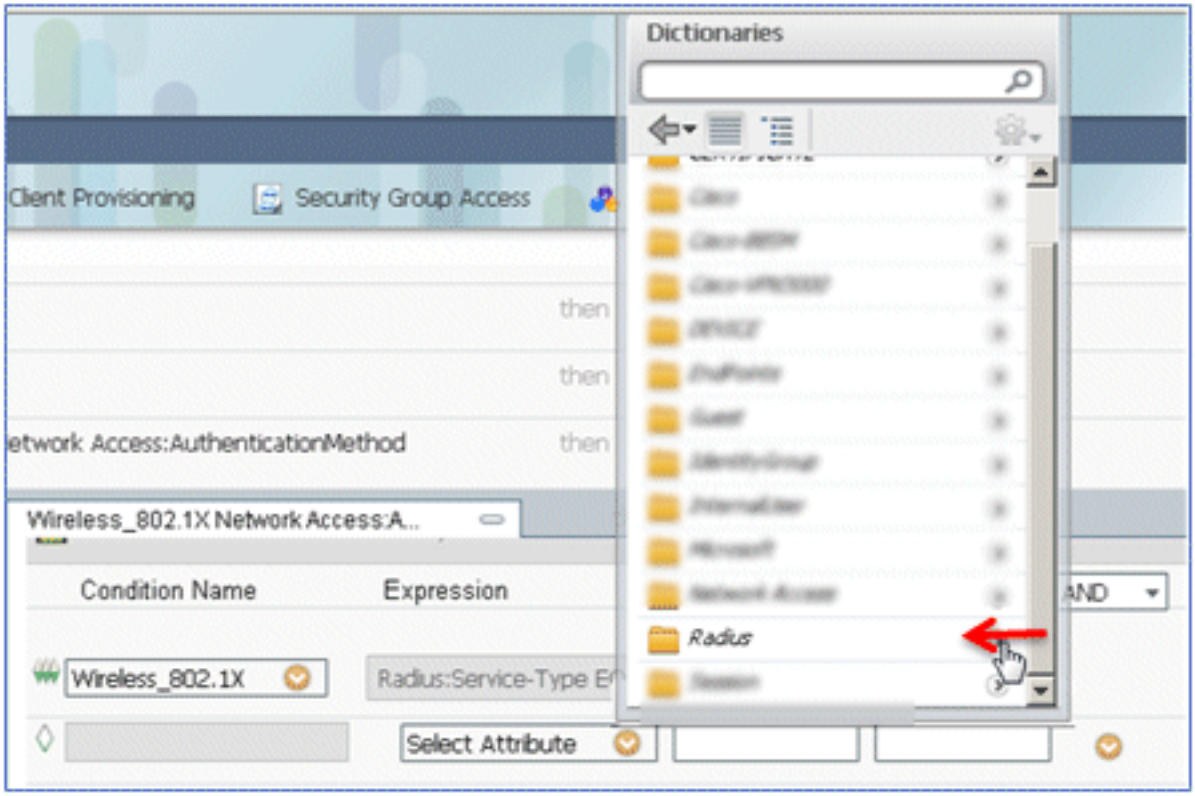
79. Voeg een EN-kenmerk toe.



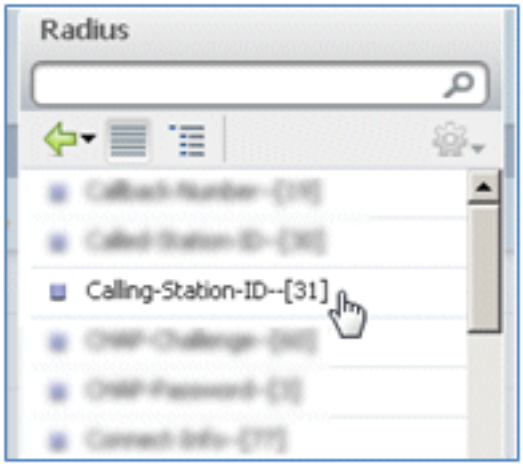
80. Klik op het tandwielpictogram aan de rechterkant van de voorwaarde en selecteer **Kenmerk/waarde toevoegen**.



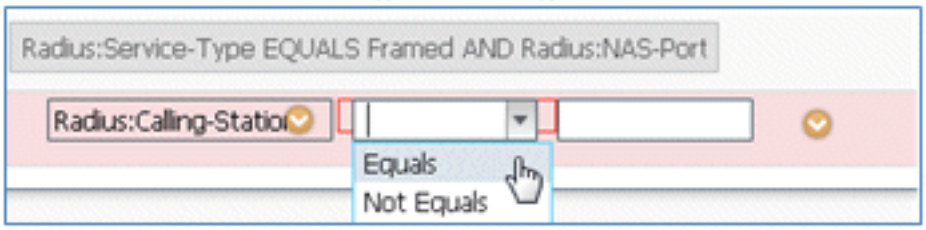
81. Zoek en selecteer **Straal**.



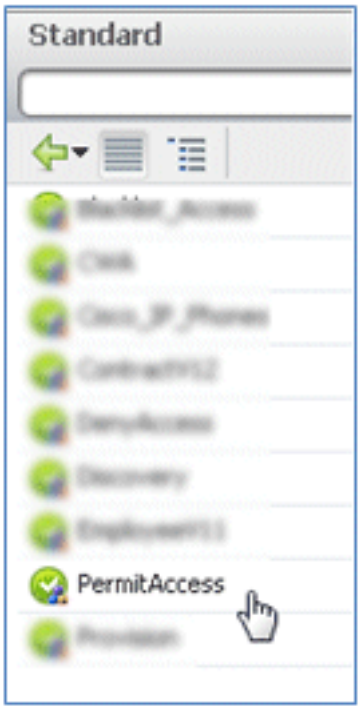
82. Selecteer **Calling-Station-ID—[31]**.



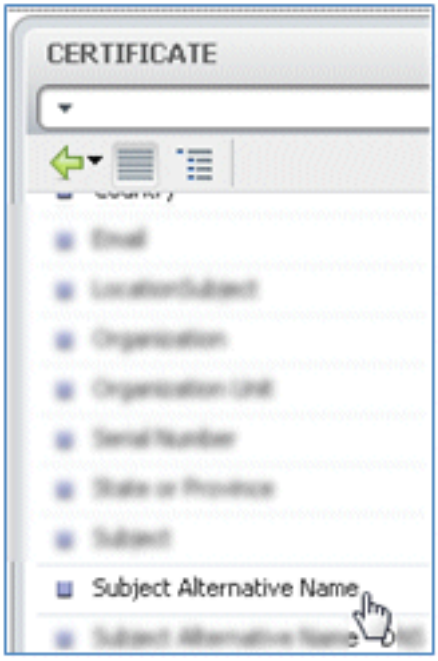
83. Selecteer **Gelijken**.



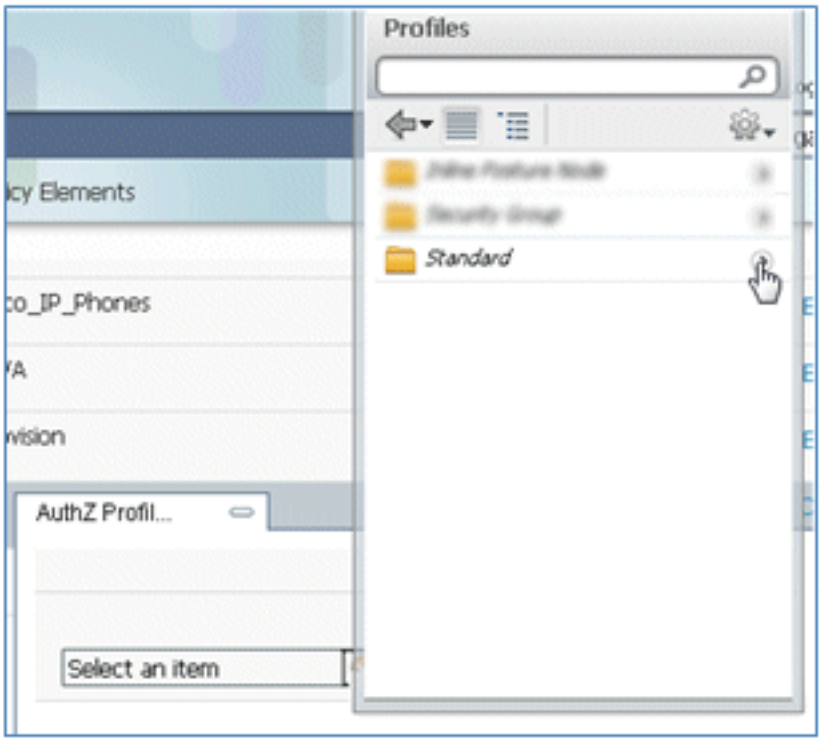
84. Ga naar **CERTIFICAAT** en klik op het pijltje rechts.



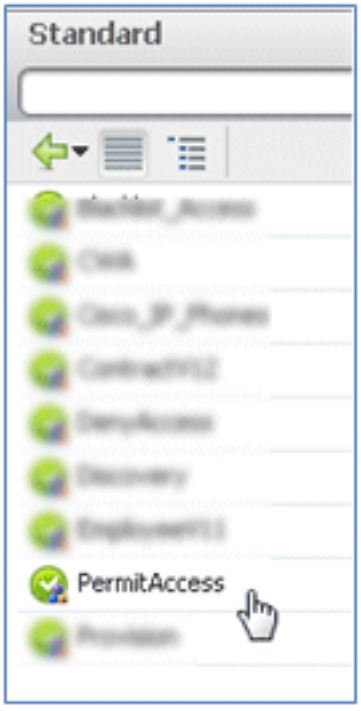
85. Selecteer **Onderwerp alternatieve naam**.



86. Selecteer **Standaard** voor het AuthZ-profiel.



87. Selecteer **Toegang toestaan**.

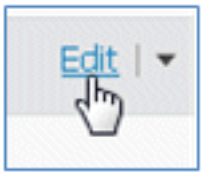


88. Klik op **Gereed**.

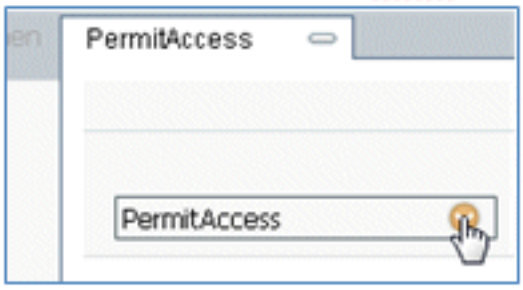
Dit is een voorbeeld van de regel:

89. Bepaal de plaats van de Standaardregel om PermitAccess in DenyAccess te veranderen.

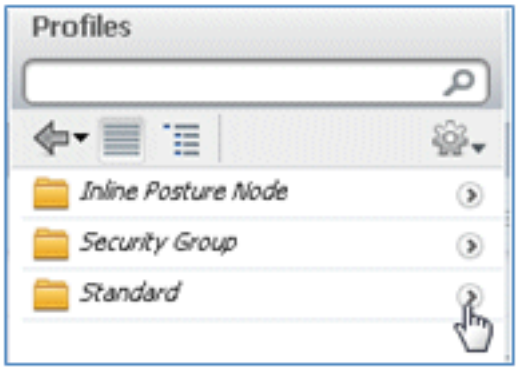
90. Klik op **Bewerken** om de standaardregel te bewerken.



91. Ga naar het bestaande AuthZ-profiel van PermitAccess.



92. Selecteer **Standaard**.



93. Selecteer **Toegang weigeren**.

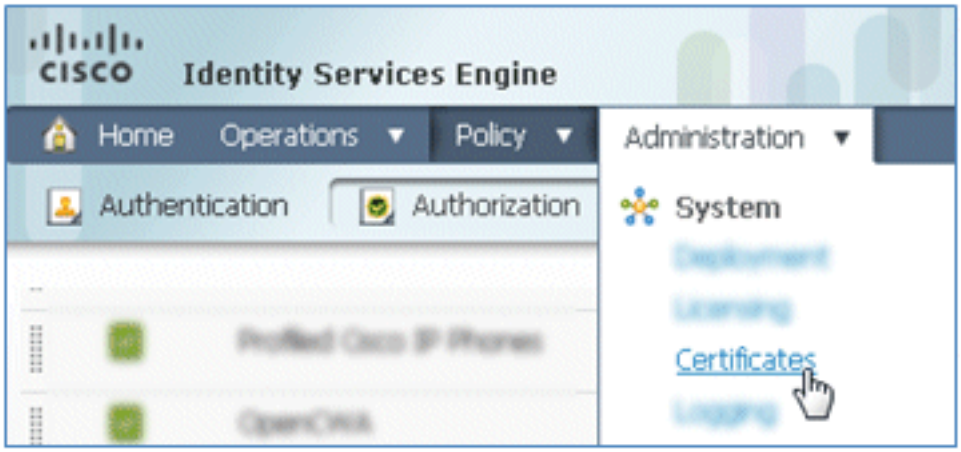
94. Bevestig dat de standaardregel DenyAccess heeft als er geen overeenkomsten worden gevonden.

95. Klik op **Gereed**.

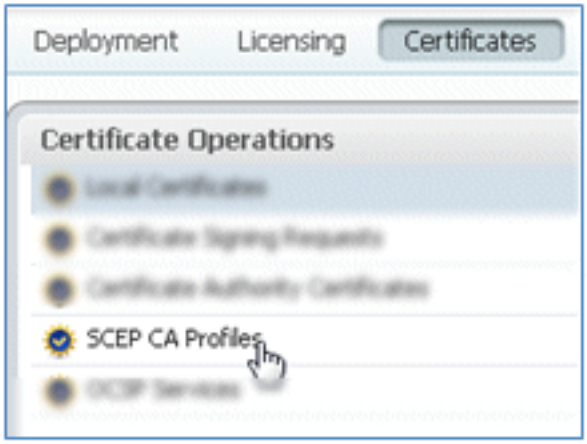
Dit is een voorbeeld van de belangrijkste regels die voor deze test vereist zijn; deze zijn van toepassing op een scenario met één of twee SSID's.

96. Klik op **Save** (Opslaan).

97. Navigeer naar **ISE > Administration > System > Certificates** om de ISE-server te configureren met een SCEP-profiel.



98. Klik in Certificaatbewerkingen op **SCEP CA-profielen**.



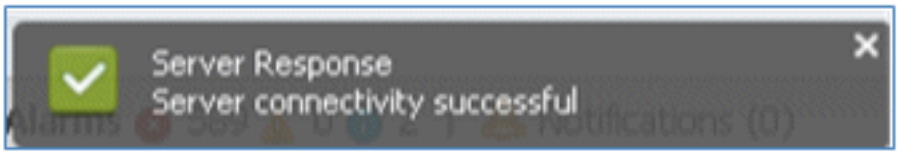
99. Klik op **Add** (Toevoegen).

100. Voer deze waarden in voor dit profiel:

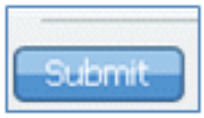
Naam: **mySCEP** (in dit voorbeeld)URL: **https://*<ca-server>*/CertServ/mscep/**(Controleer de configuratie van uw CA-server op het juiste adres.)

101. Klik op **Connectiviteit testen** om de connectiviteit van de SCEP-verbinding te testen.

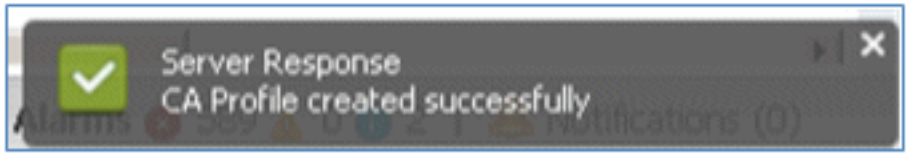
102. Deze respons laat zien dat de serverconnectiviteit succesvol is.



103. Klik op **Verzenden**.



104. De server reageert dat het CA-profiel is gemaakt.



105. Bevestig dat het SCEP CA-profiel is toegevoegd.

Gebruikerservaring - Provisioning iOS

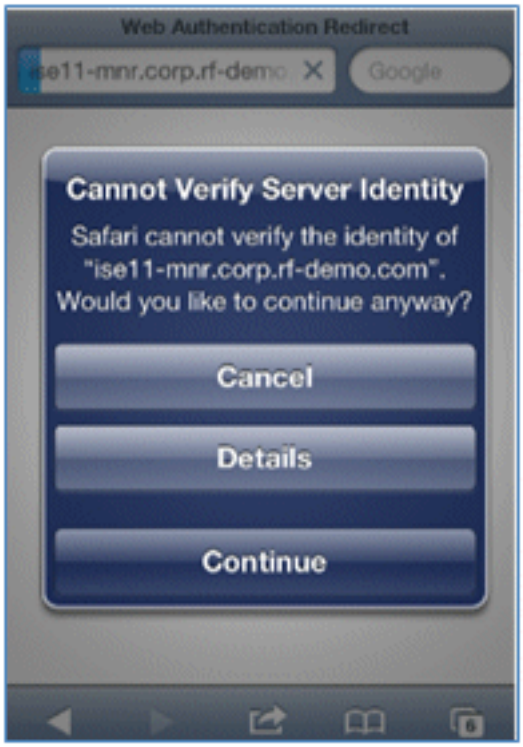
Dubbele SSID

In dit gedeelte worden dubbele SSID's besproken en wordt beschreven hoe u verbinding kunt maken met de te leveren gast en hoe u verbinding kunt maken met een 802.1x WLAN.

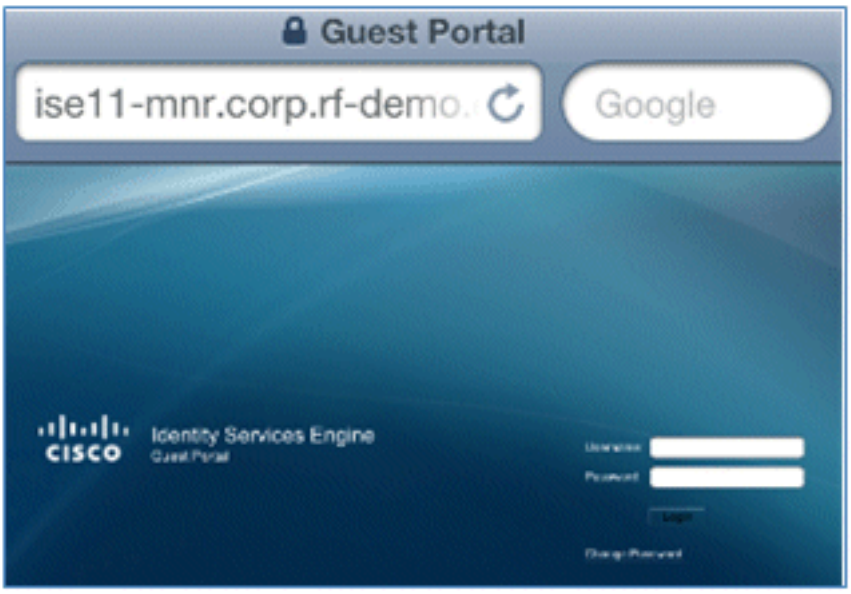
Voltooi deze stappen om iOS in het dubbele scenario van SSID te voorzien:

1. Ga op het iOS-apparaat naar **Wi-Fi Networks** en selecteer **DemoCWA** (geconfigureerd, open WLAN op WLC).

2. Open de Safari-browser op het iOS-apparaat en bezoek een bereikbare URL (bijvoorbeeld een interne/externe webserver). De ISE leidt u naar de portal. Klik op **Continue** (Doorgaan).



3. U wordt doorgestuurd naar het Guest Portal voor aanmelding.



4. Log in met een AD-gebruikersaccount en wachtwoord. Installeer het CA-profiel als hierom wordt gevraagd.

5. Klik op **Install** vertrouwde certificaat van de CA-server.

6. Klik op **Gereed** als het profiel volledig is geïnstalleerd.

7. Ga terug naar de browser en klik op **Registreren**. Maak een notitie van de Apparaat-ID die het MAC-adres van het apparaat bevat.

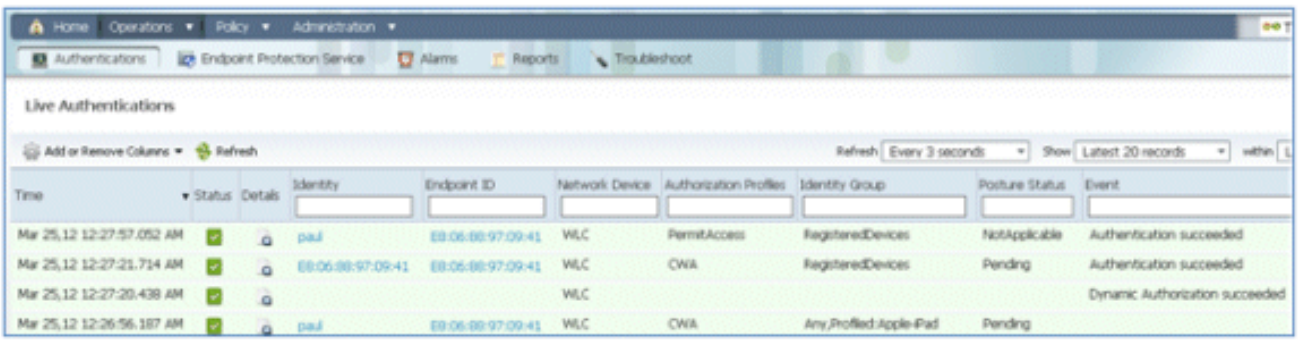
8. Klik op **Installeren** om het geverifieerde profiel te installeren.

9. Klik op **Nu installeren**.

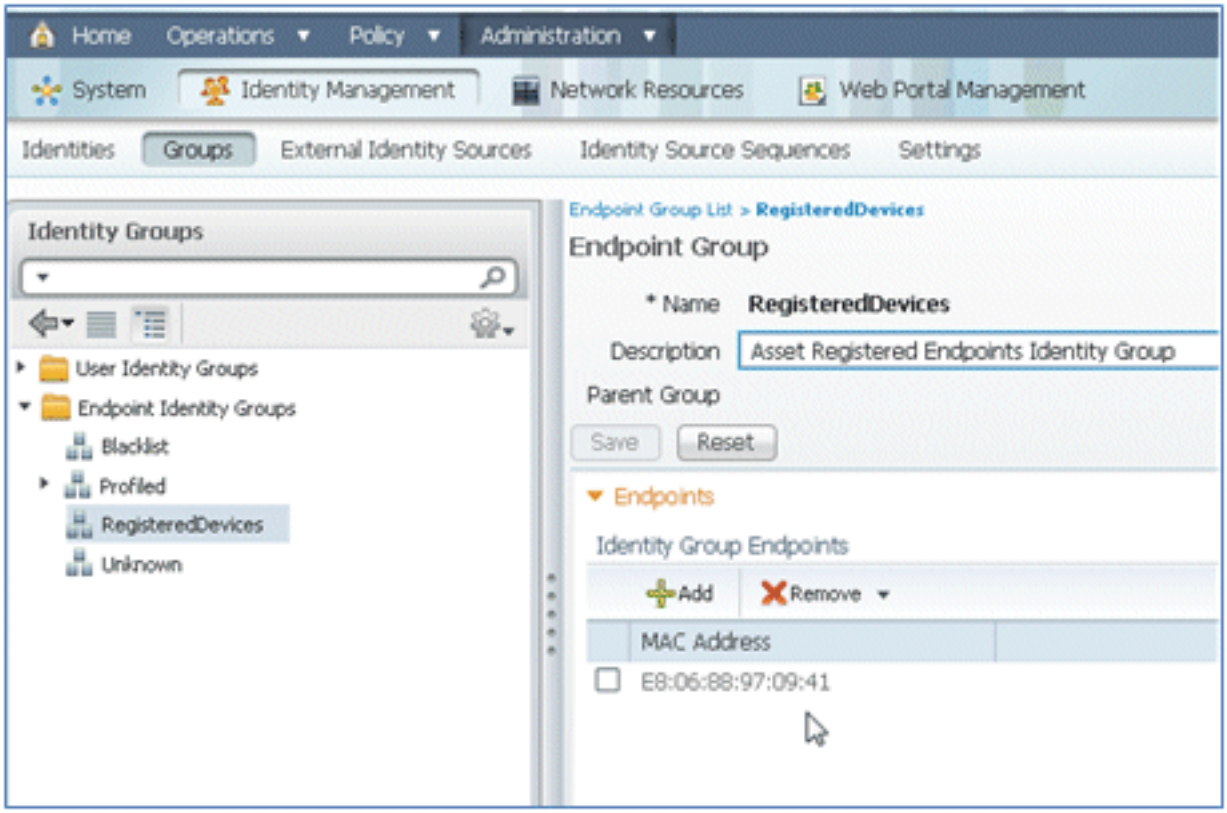
10. Nadat het proces is voltooid, bevestigt het WirelessSP-profiel dat het profiel is geïnstalleerd. Klik op **Gereed**.

11. Ga naar **Wi-Fi Networks** en wijzig het netwerk in **Demo1x**. Uw apparaat is nu verbonden en gebruikt TLS.

12. Ga op de ISE naar **Operations > Authentications**. De gebeurtenissen tonen het proces waarin het apparaat is verbonden met het open gastennetwerk, gaat door het registratieproces met de levering van de aanvrager, en wordt toegestaan vergunningstoegang na registratie.



13. Navigeer naar ISE > Administration > Identity Management > **Groepen** > **Endpoint Identity Groups** > **RegisteredDevices**. Het MAC-adres is toegevoegd aan de database.

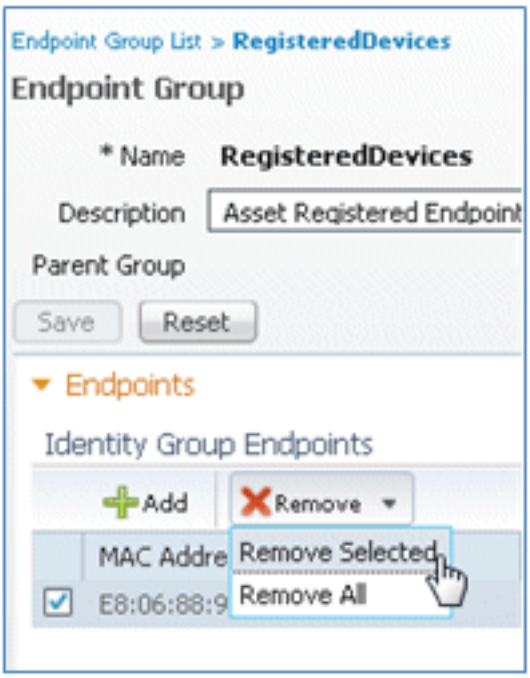


Enkelvoudige SSID

In deze sectie wordt beschreven hoe u rechtstreeks verbinding kunt maken met een 802.1x WLAN, kunt u een AD-gebruikersnaam/wachtwoord opgeven voor PEAP-verificatie, kunt u gebruikmaken van een gastaccount en opnieuw verbinding kunt maken met TLS.

Voltooi deze stappen om iOS in het enige scenario van SSID te voorzien:

1. Als u hetzelfde iOS-apparaat gebruikt, verwijdert u het eindpunt uit de geregistreerde apparaten.



2. Ga op het iOS-apparaat naar **Instellingen** > **Algemeen** > **Profielen**. Verwijder de profielen die in dit voorbeeld zijn geïnstalleerd.

3. Klik op **Verwijderen** om de vorige profielen te verwijderen.

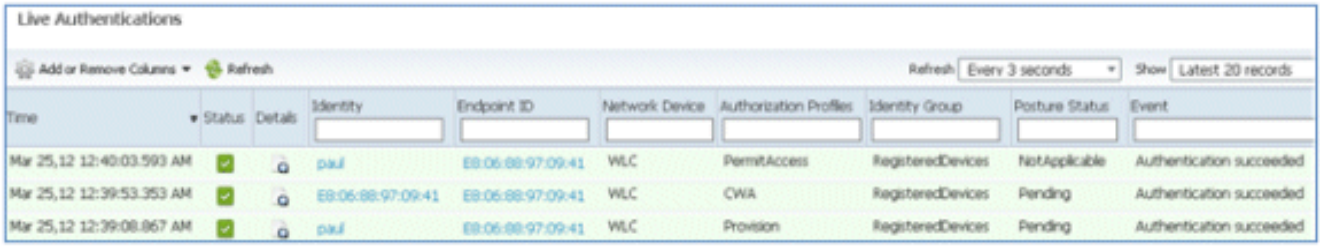
4. Sluit rechtstreeks aan op de 802.1x met het bestaande (ontruimde) apparaat of met een nieuw iOS-apparaat.

5. Verbind met **Dot1x**, voer een gebruikersnaam en wachtwoord in en klik op **Join**.

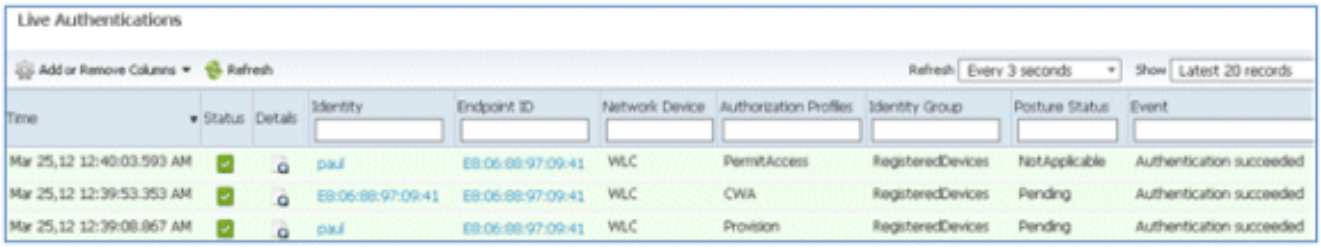
6. Herhaal stap 90 en verder van het gedeelte ISE-configuratie totdat de juiste profielen volledig

zijn geïnstalleerd.

7. Navigeer naar **ISE > Operations > Authentications** om het proces te bewaken. Dit voorbeeld toont de client die rechtstreeks is verbonden met 802.1X WLAN omdat deze is provisioned, verbinding verbreekt en opnieuw verbinding maakt met hetzelfde WLAN met behulp van TLS.



8. Navigeer naar **WLC > Monitor > [Client MAC]**. Houd er rekening mee dat de client zich in de toestand RUN bevindt, dat de gegevensswitching is ingesteld op lokaal en dat de verificatie centraal staat. Dit geldt voor clients die verbinding maken met FlexConnect AP.



Gebruikerservaring - Provisioning Android

Dubbele SSID

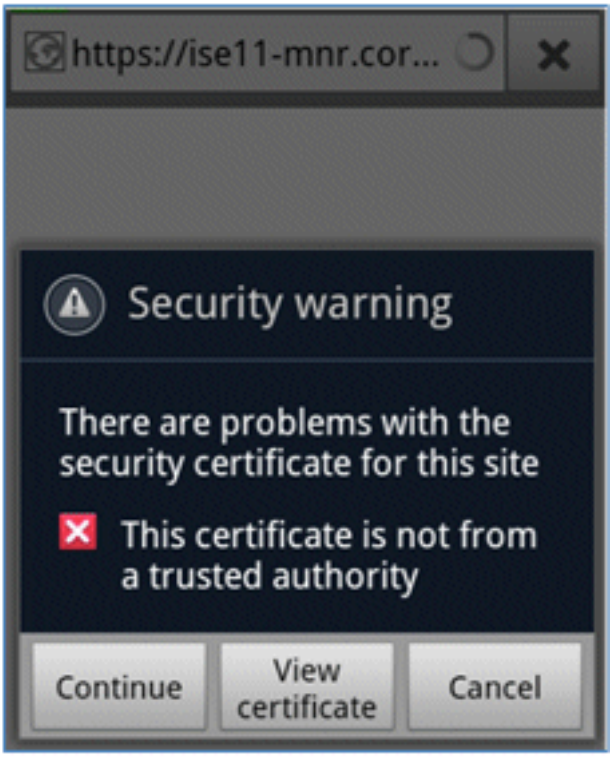
In dit gedeelte worden dubbele SSID's besproken en wordt beschreven hoe u verbinding kunt maken met de te leveren gast en hoe u verbinding kunt maken met een 802.1x WLAN.

Het verbindingsproces voor het Android-apparaat is zeer vergelijkbaar met dat voor een iOS-apparaat (enkele of dubbele SSID). Een belangrijk verschil is echter dat het Android-apparaat toegang tot het internet nodig heeft om toegang te krijgen tot Google Marketplace (nu Google Play) en om de verzoeker-agent te kunnen downloaden.

Voltooi deze stappen om een Android-apparaat (zoals de Samsung Galaxy in dit voorbeeld) in het dual SSID-scenario te voorzien:

1. In het Android-apparaat, gebruik Wi-Fi om verbinding te maken met **DemoCWA**, en open de gast WLAN.

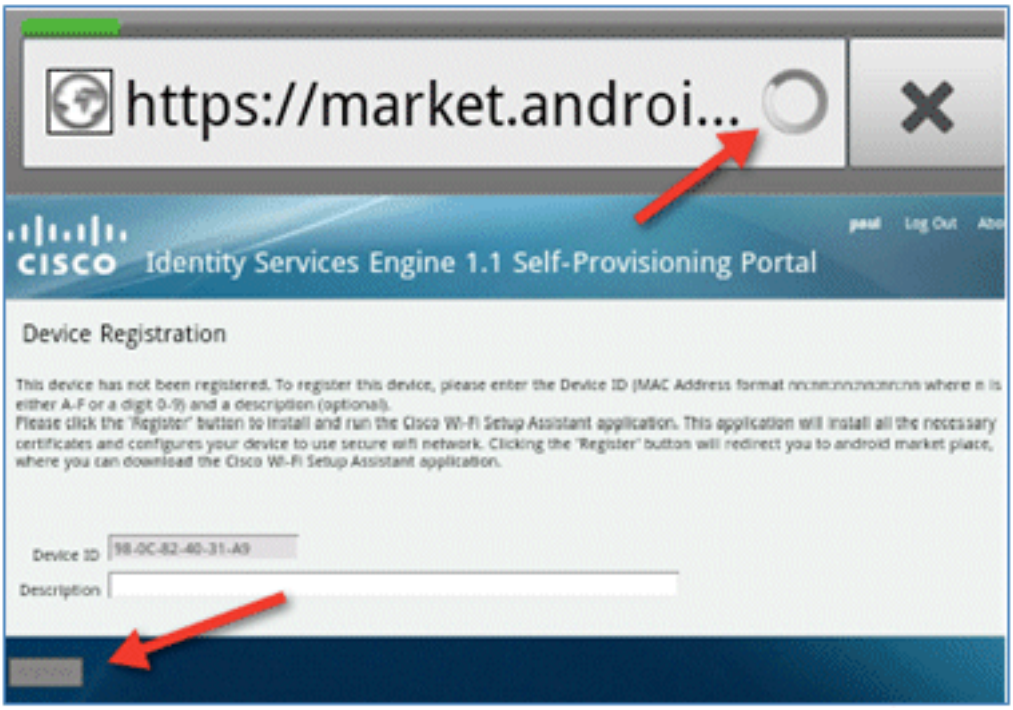
2. Accepteer een certificaat om verbinding met de ISE te maken.



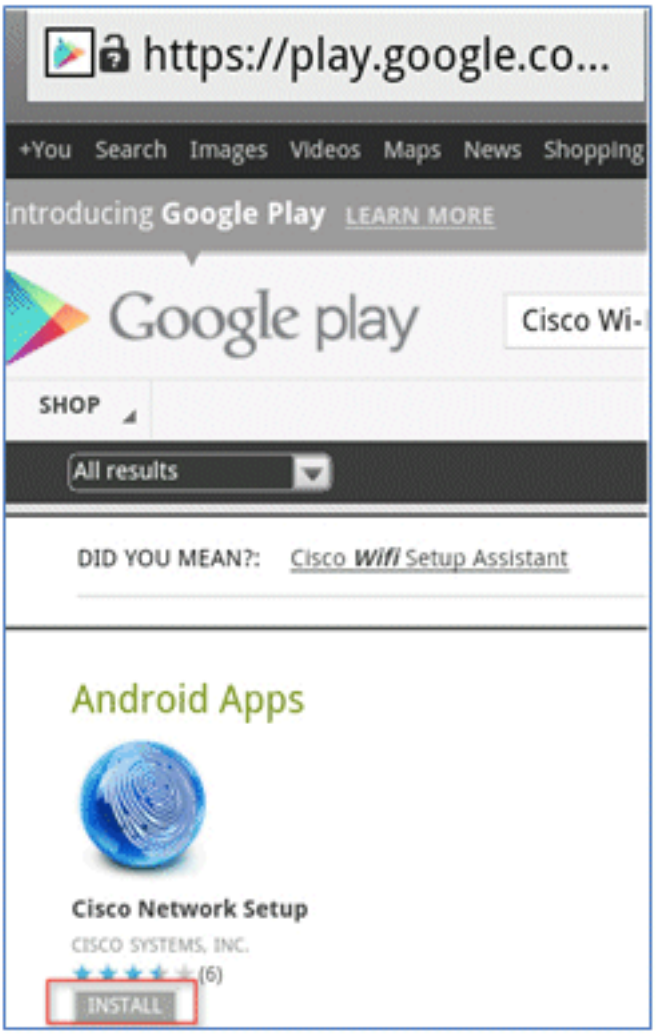
3. Voer een gebruikersnaam en wachtwoord in bij de Guest Portal om in te loggen.

4. Klik op **Registreren**. Het apparaat probeert het internet te bereiken om toegang te krijgen tot

Google Marketplace. Voeg eventuele aanvullende regels toe aan de pre-autorisatiefilm (zoals ACL-REDIRECT) in de controller om toegang tot het internet mogelijk te maken.

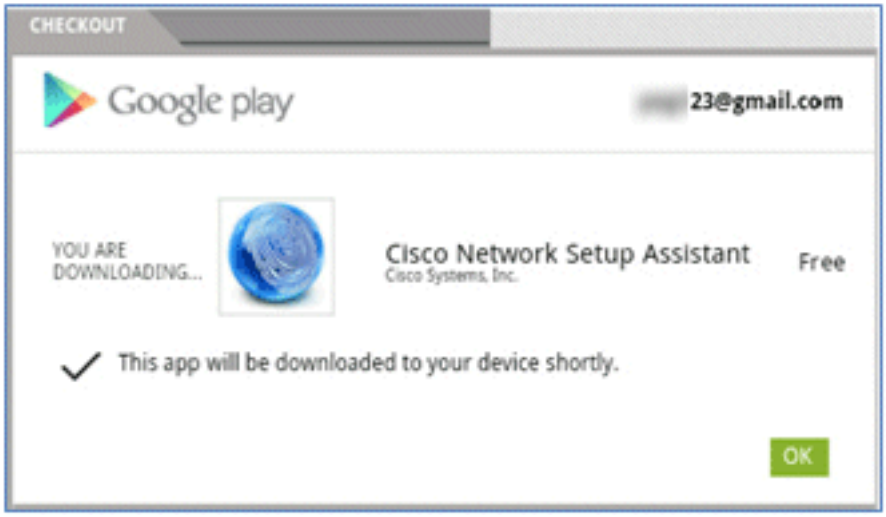


5. Google noemt Cisco Network Setup als een Android-app. Klik op **Install** (Installeren).

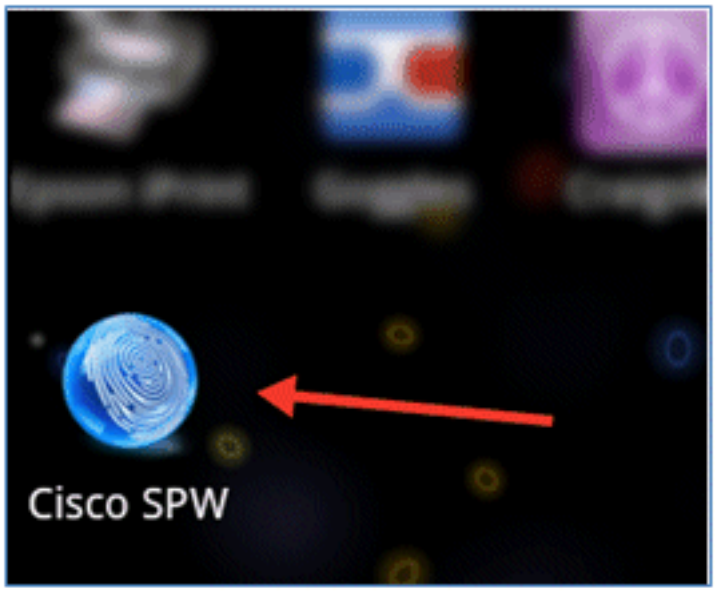


6. Meld u aan bij Google en klik op **INSTALL**.

7. Klik op **OK**.



8. Zoek op het Android-apparaat de geïnstalleerde **Cisco SPW-**app en open deze.



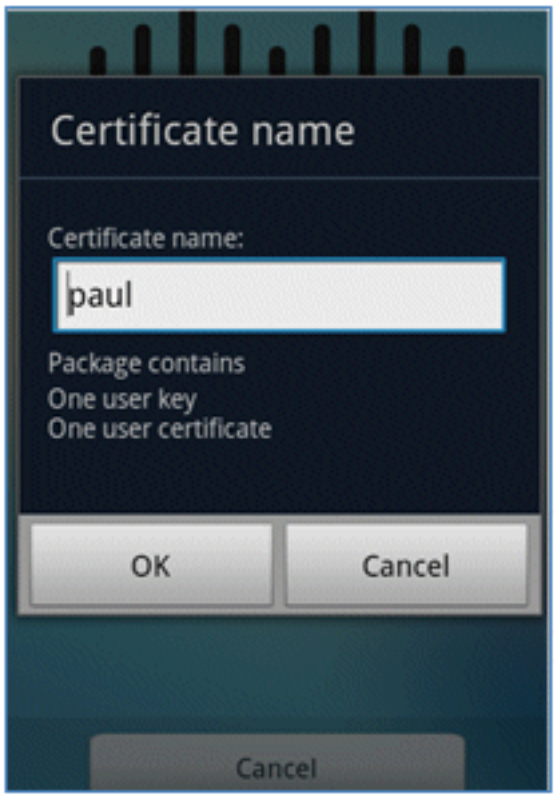
9. Zorg ervoor dat je nog steeds ingelogd bent op het Guest Portal vanaf je Android-apparaat.

10. Klik op **Start** om de Wi-Fi Setup Assistant te starten.

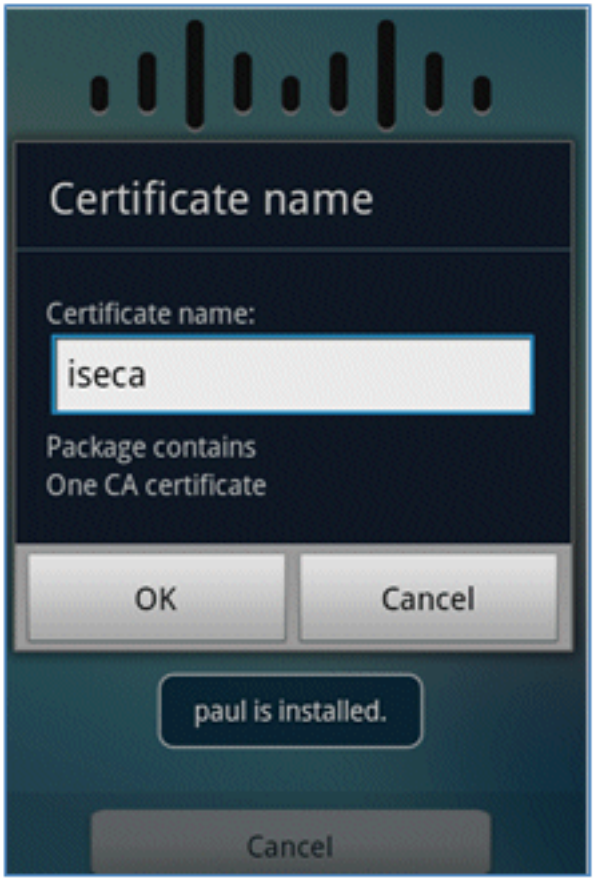
11. Cisco SPW begint certificaten te installeren.

12. Stel desgevraagd een wachtwoord in voor het opslaan van de referenties.

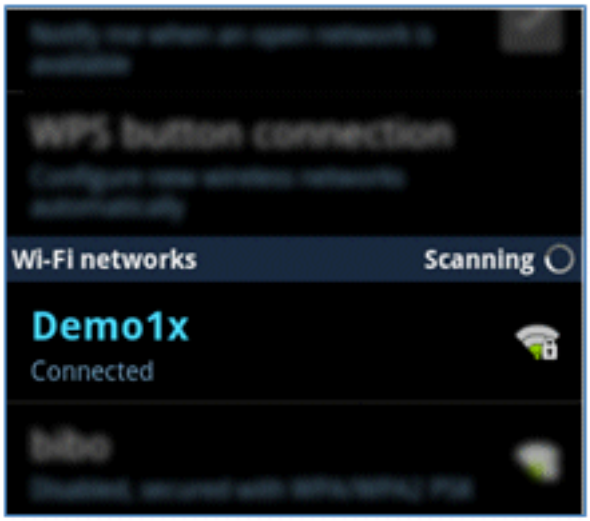
13. Cisco SPW keert met een certificaatnaam terug, die de gebruikerssleutel en het gebruikerscertificaat bevat. Klik op **OK** om het te bevestigen.



14. Cisco SPW gaat verder en vraagt om een andere certificaatnaam die het CA-certificaat bevat. Voer de naam **iseca** in (in dit voorbeeld) en klik vervolgens op **OK** om door te gaan.



15. Het Android-apparaat is nu verbonden.

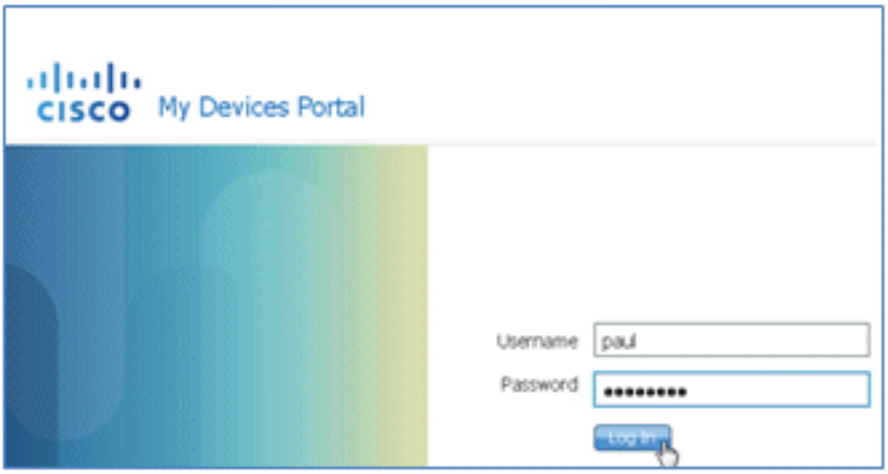


Mijn apparaatportal

Mijn Apparatenportal staat gebruikers toe om eerder geregistreerde apparaten te verduisteren in het geval dat een apparaat verloren of gestolen is. Hiermee kunnen gebruikers indien nodig ook opnieuw inschrijven.

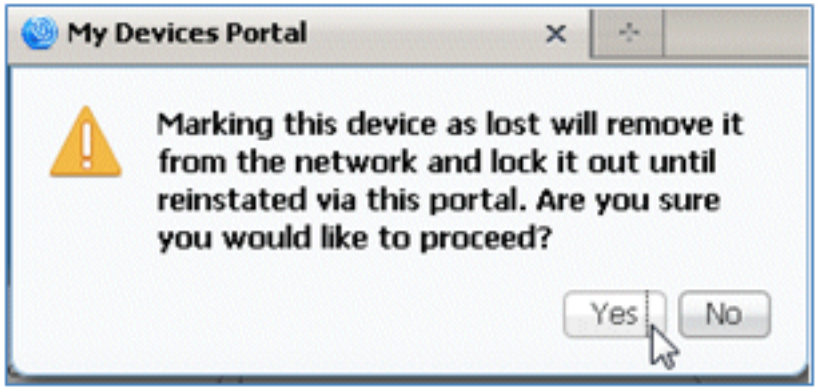
Voltooi de volgende stappen om een apparaat op een zwarte lijst te zetten:

1. Om in te loggen op My Devices Portal, open een browser, maak verbinding met https://ise-server:8443/mydevices (noteer het poortnummer 8443) en log in met een AD-account.



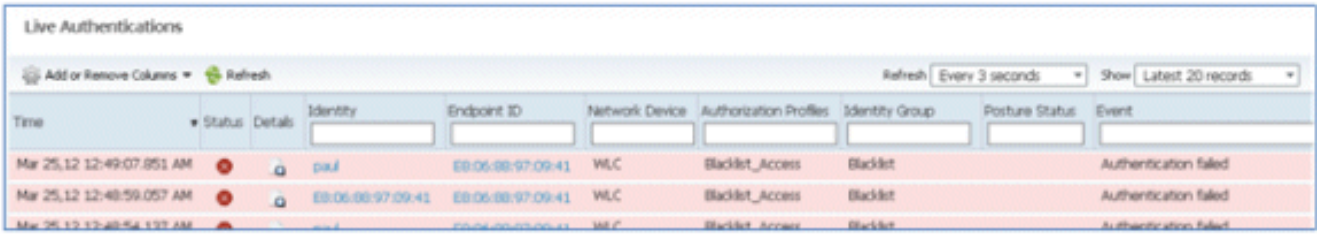
2. Zoek het apparaat onder Apparaat-ID en klik op **Lost?** om een zwarte lijst van een apparaat te starten.

3. Wanneer de ISE om een waarschuwing vraagt, klikt u op **Ja** om verder te gaan.



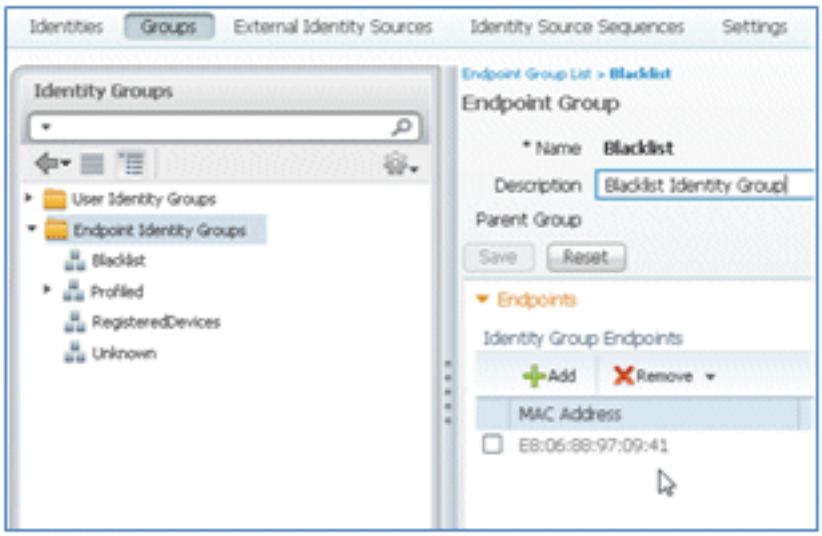
4. ISE bevestigt dat het apparaat is gemarkeerd als **verloren**.

5. Elke poging om verbinding te maken met het netwerk met het eerder geregistreerde apparaat wordt nu geblokkeerd, zelfs als er een geldig certificaat is geïnstalleerd. Dit is een voorbeeld van een apparaat op de zwarte lijst dat niet kan worden geverifieerd:



6. Een beheerder kan navigeren naar ISE > Administration > Identity Management > **Groups**, klikken op **Endpoint Identity Groups** > **Blacklist** en zien dat het apparaat op een zwarte lijst

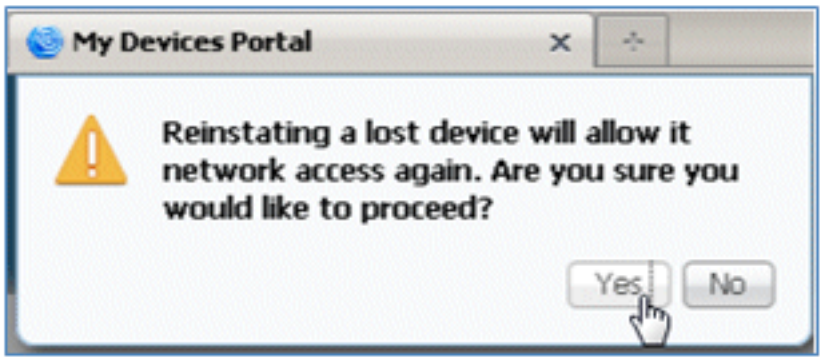
staat.



Voltooi deze stappen om een apparaat op de zwarte lijst te herstellen:

1. Klik vanuit het My Devices Portal op **Reinstate** voor dat apparaat.

2. Wanneer ISE om een waarschuwing vraagt, klikt u op **Ja** om verder te gaan.



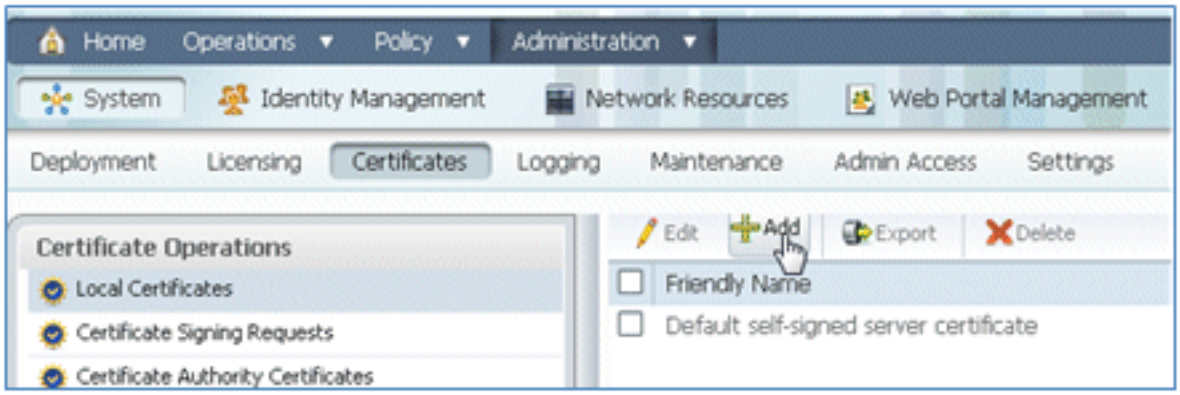
3. ISE bevestigt dat het apparaat met succes is hersteld. Sluit het opnieuw geïnstalleerde apparaat aan op het netwerk om te testen of het apparaat nu zal worden toegestaan.

Referentie - Certificaten

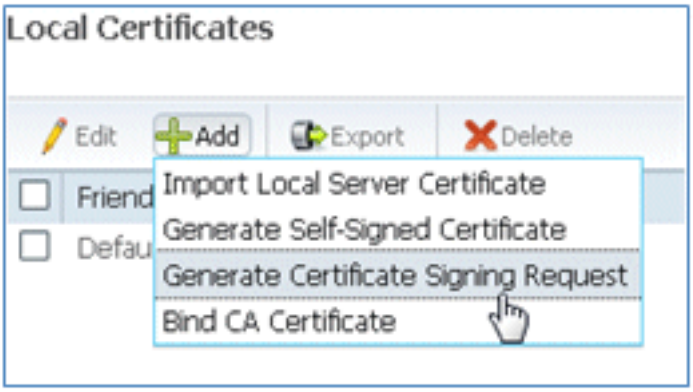
ISE vereist niet alleen een geldig CA-basiscertificaat, maar heeft ook een geldig certificaat nodig dat is ondertekend door CA.

Voltooi deze stappen om een nieuw vertrouwd CA-certificaat toe te voegen, te binden en te importeren:

1. Navigeer naar ISE > Beheer > Systeem > **Certificaten**, klik op **Local Certificates** en klik op **Add**.



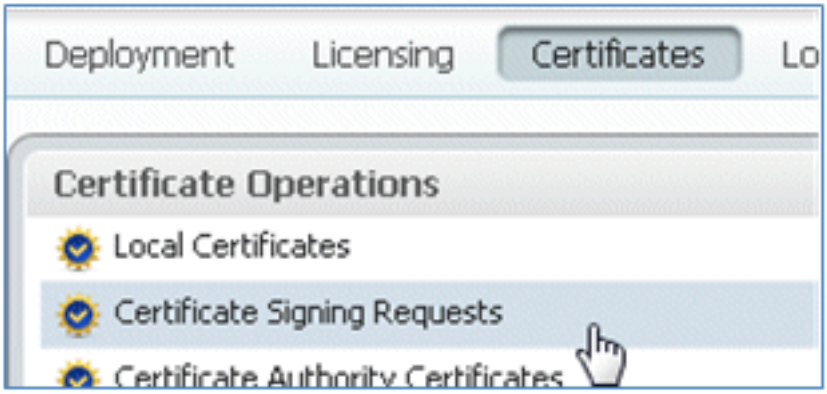
2. Selecteer **Generate Certificate Signing Aanvraag** (CSR).



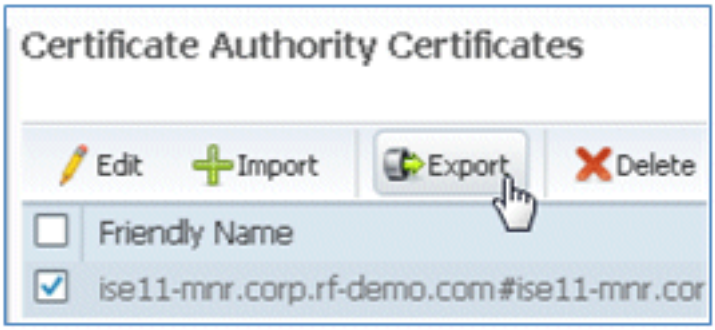
3. Voer het certificaatonderwerp **CN=<*ISE-SERVER hostname.FQDN*>in**. Voor de andere velden kunt u de standaardinstelling of de waarden gebruiken die zijn vereist bij de CA-instelling. Klik op **Verzenden**.

4. ISE verifieert dat de MVO is opgesteld.

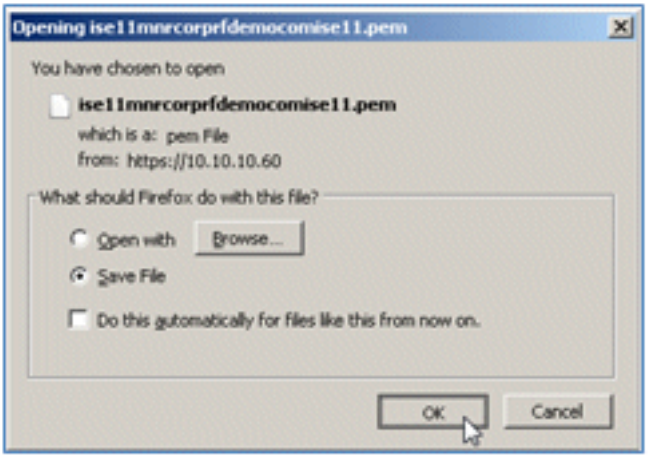
5. Klik op de verwerkingen voor het **ondertekenen** van het **certificaat** om toegang te krijgen tot de MVO.



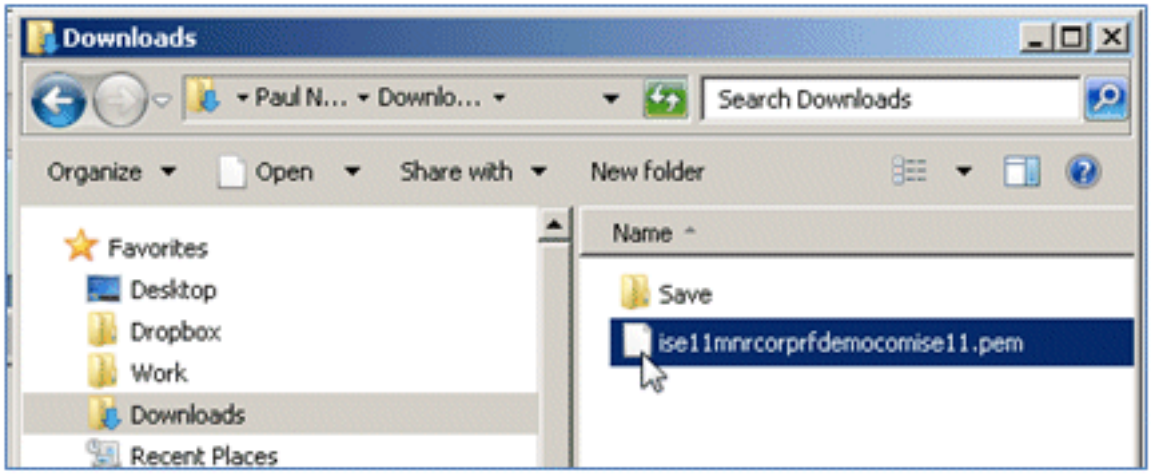
6. Selecteer de onlangs gemaakte MVO en klik op **Exporteren**.



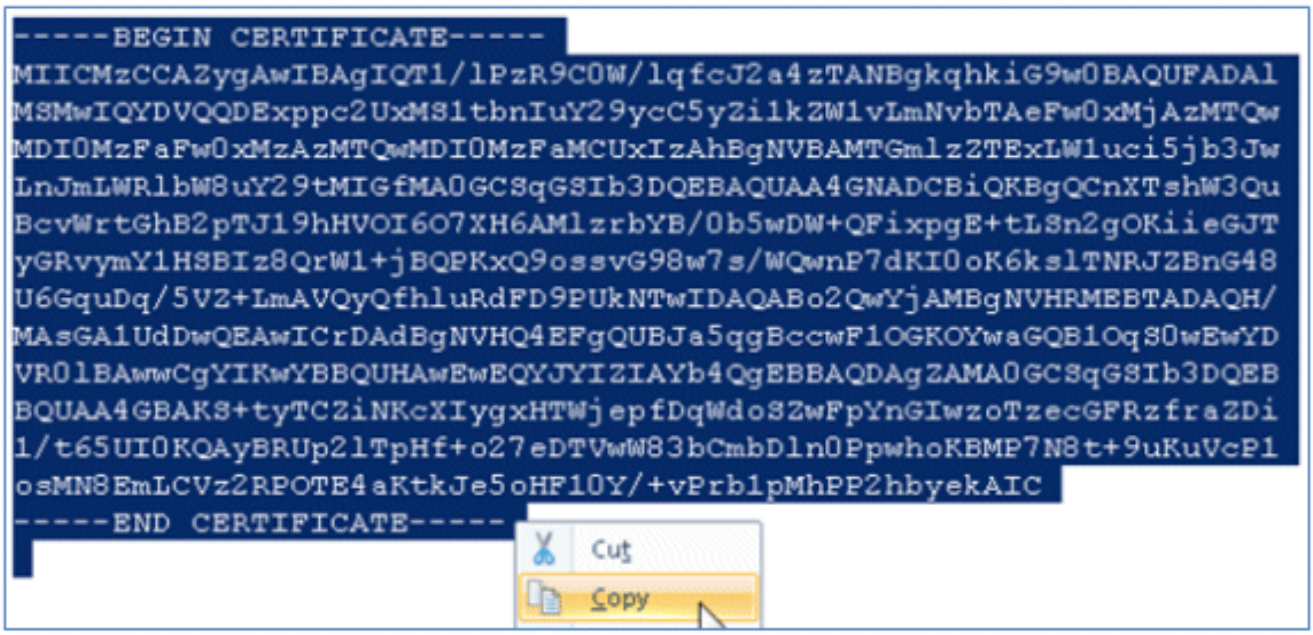
7. ISE exporteert de CSR naar een .pem bestand. Klik op **Bestand opslaan** en vervolgens op **OK** om het bestand op te slaan op de lokale computer.



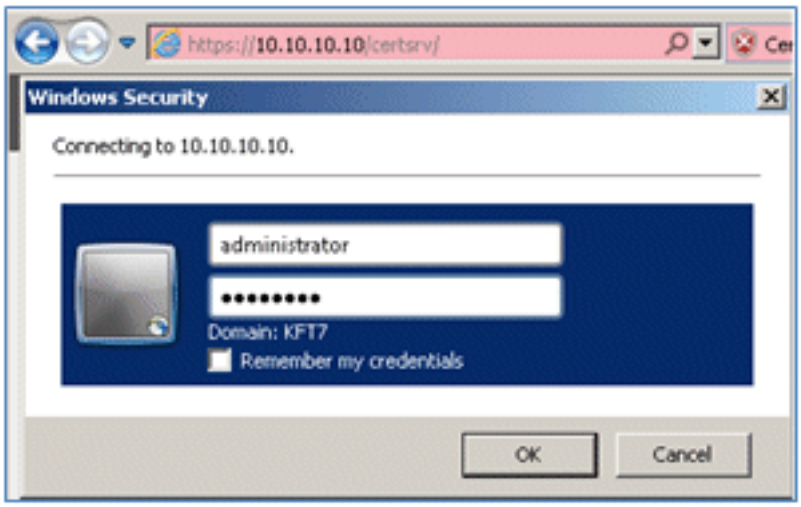
8. Lokaliseer en open het ISE-certificaatbestand met een teksteditor.



9. Kopieert de gehele inhoud van het certificaat.

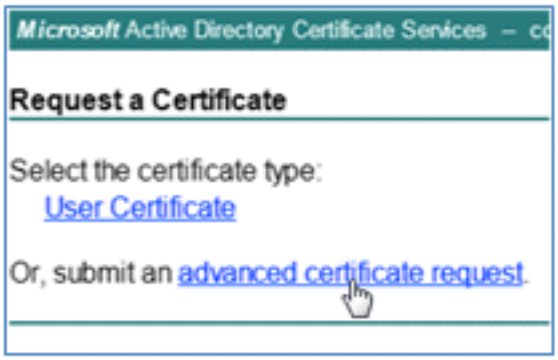


10. Maak verbinding met de CA-server en log in met een Administrator-account. De server is een Microsoft 2008 CA op https://10.10.10.10/certsrv (in dit voorbeeld).

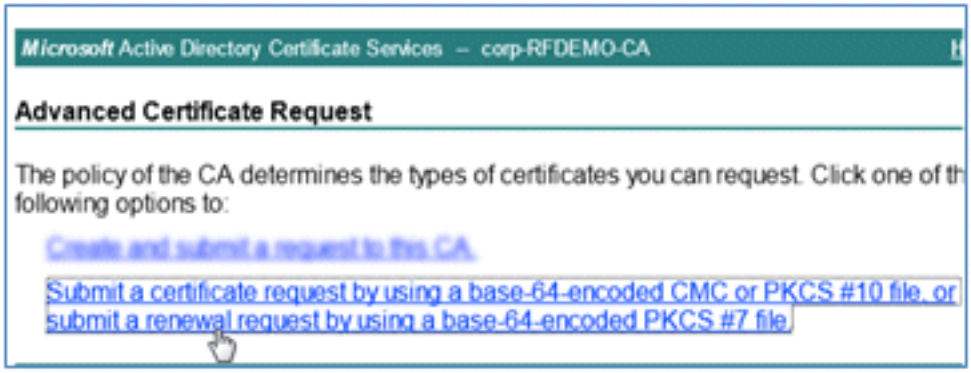


11. Klik op **Certificaat aanvragen**.

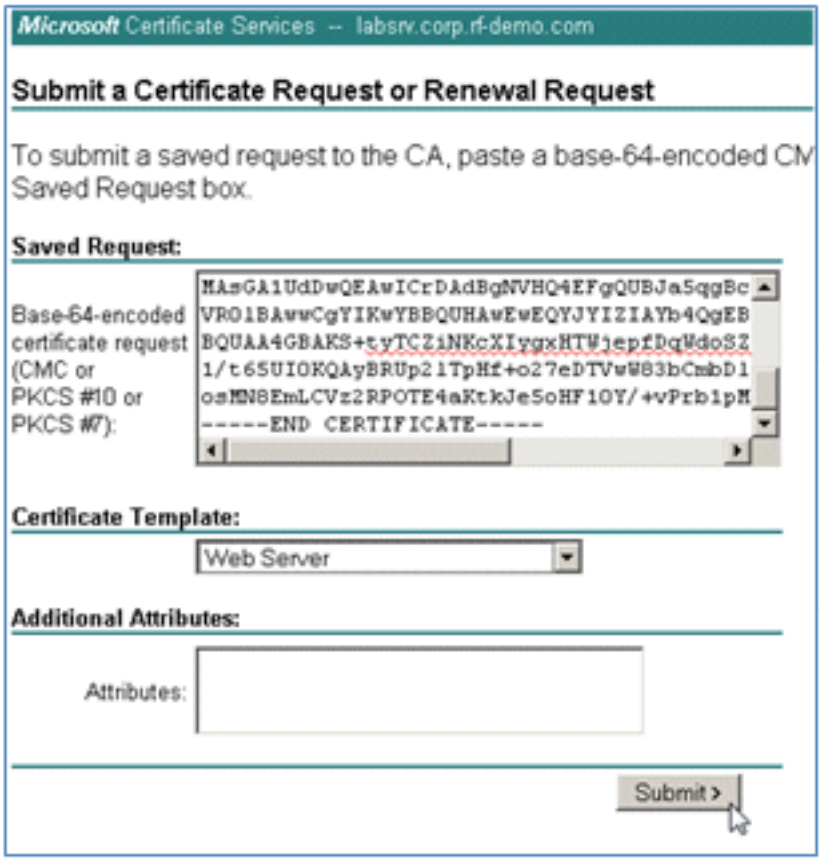
12. Klik op **Geavanceerd certificaatverzoek**.



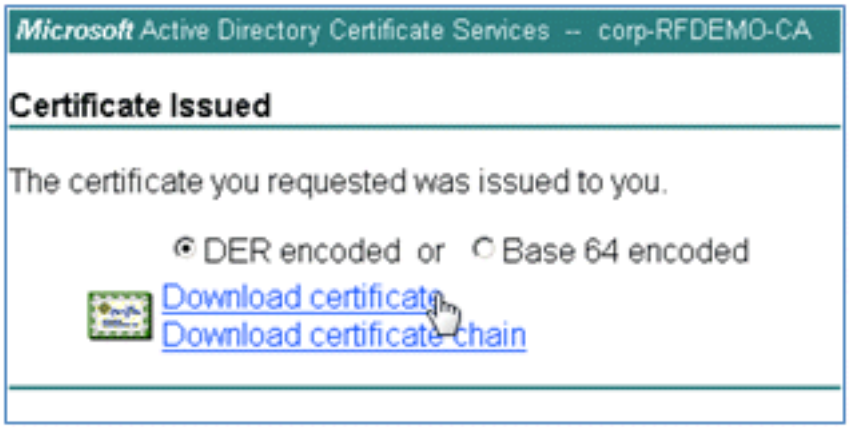
13. Klik op de tweede optie om **een certificaataanvraag in** te **dienen met behulp van een basis-64-gecodeerde CMC of ...** .



14. Plakt de inhoud van het ISE-certificaatbestand (.pem) in het veld Opgeslagen aanvraag, zorg ervoor dat de certificaatsjabloon **webserver** is en klik op **Indienen**.

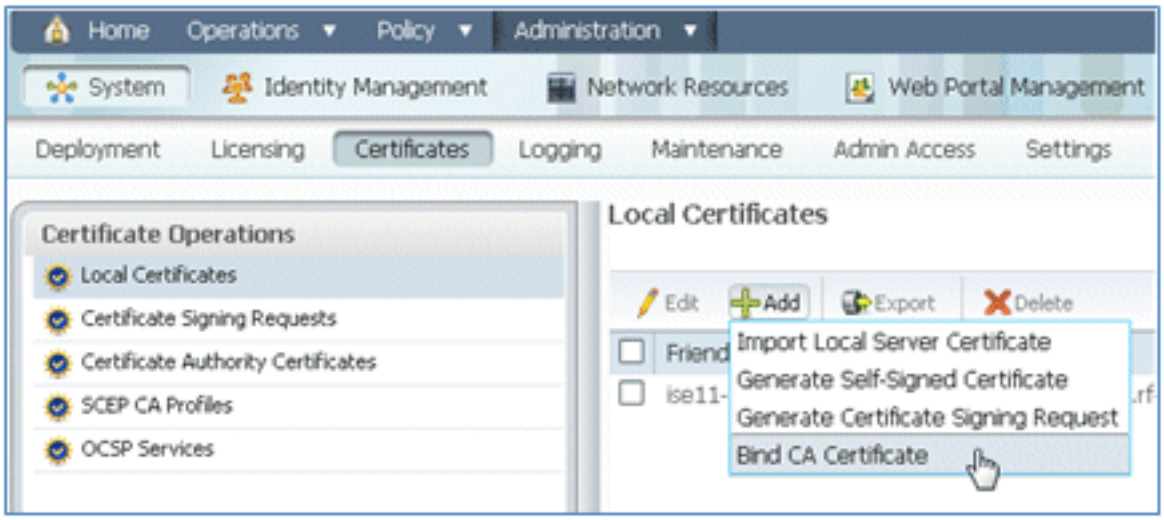


15. Klik op **Certificaat downloaden**.

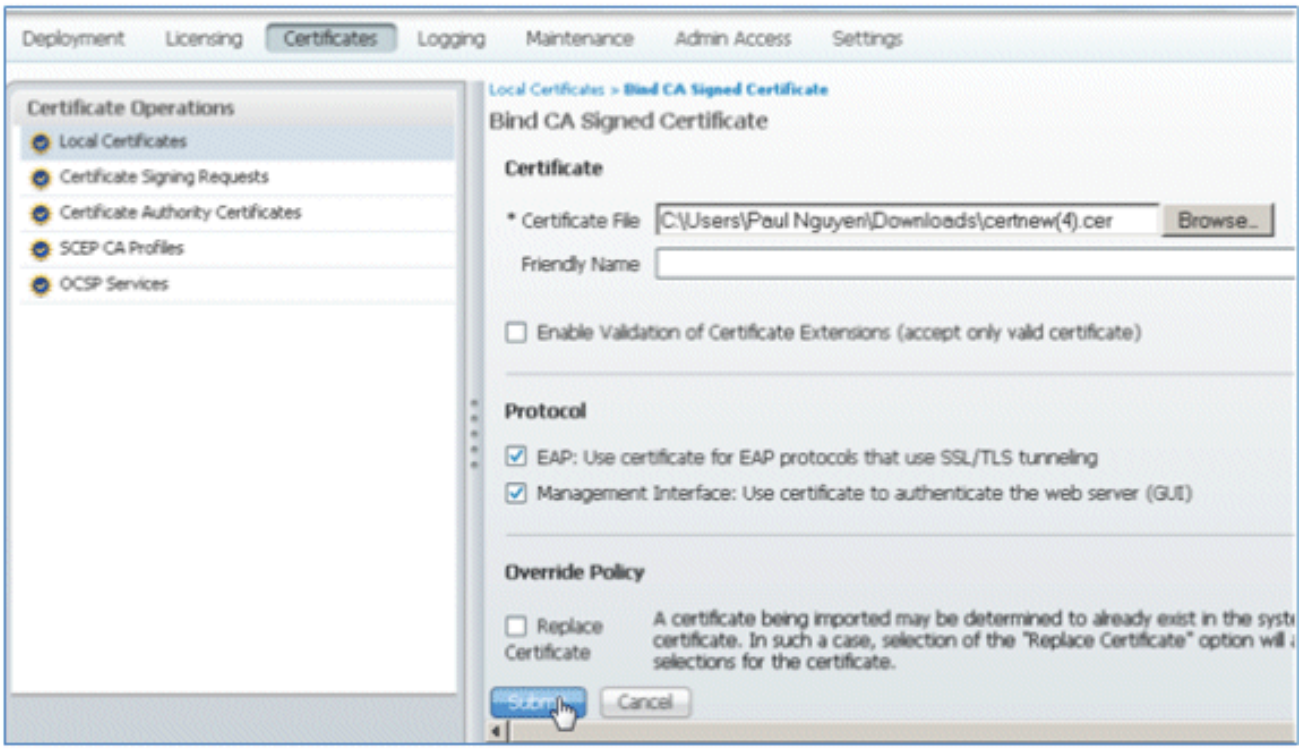


16. Sla het bestand certnew.cer op. Het wordt later gebruikt om met de ISE te verbinden.

17. Ga van ISE-**certificaten** naar **Local Certificates** en klik op **Add > Bind CA-certificaat**.



18. Blader naar het certificaat dat in de vorige stap is opgeslagen op de lokale machine, schakel de protocollen **EAP** en **Management Interface in** (selectievakjes zijn ingeschakeld) en klik op **Indienen**. ISE kan enkele minuten of langer duren om de services opnieuw te starten.

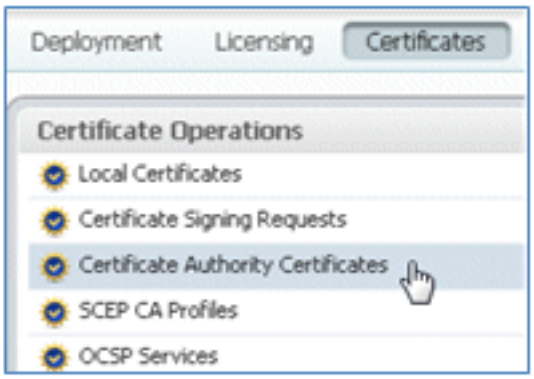


19. Ga terug naar de landingspagina van de CA (https://CA/certsrv/) en klik op **Een CA-certificaat, certificaatketen of CRL downloaden**.

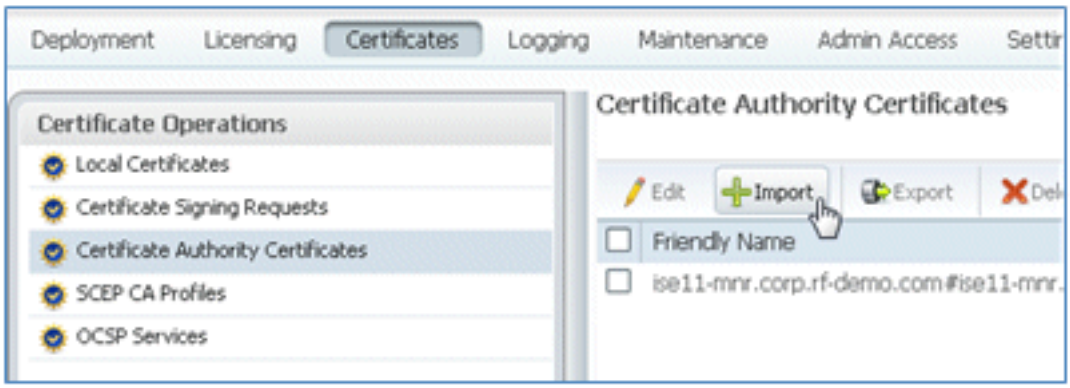
20. Klik op **CA-certificaat downloaden**.

21. **Sla** het bestand op de lokale computer op.

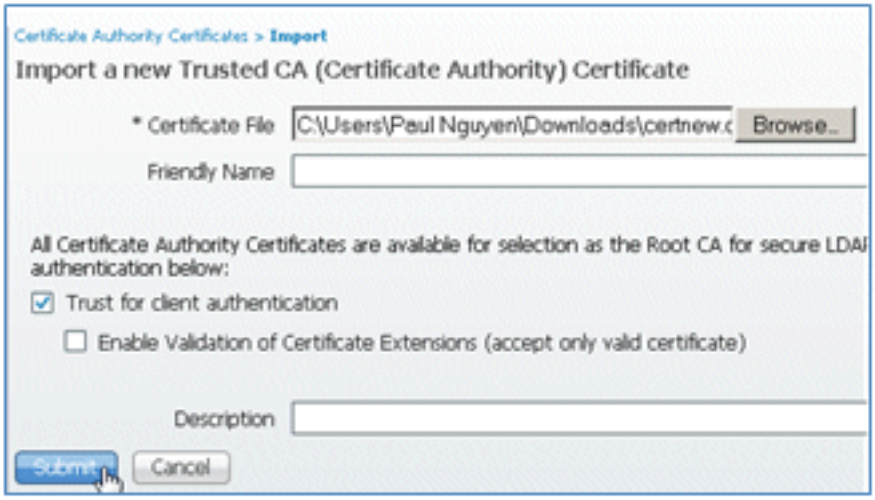
22. Ga met de ISE-server online naar **Certificaten** en klik op **Certificaatverleningscertificaten**.



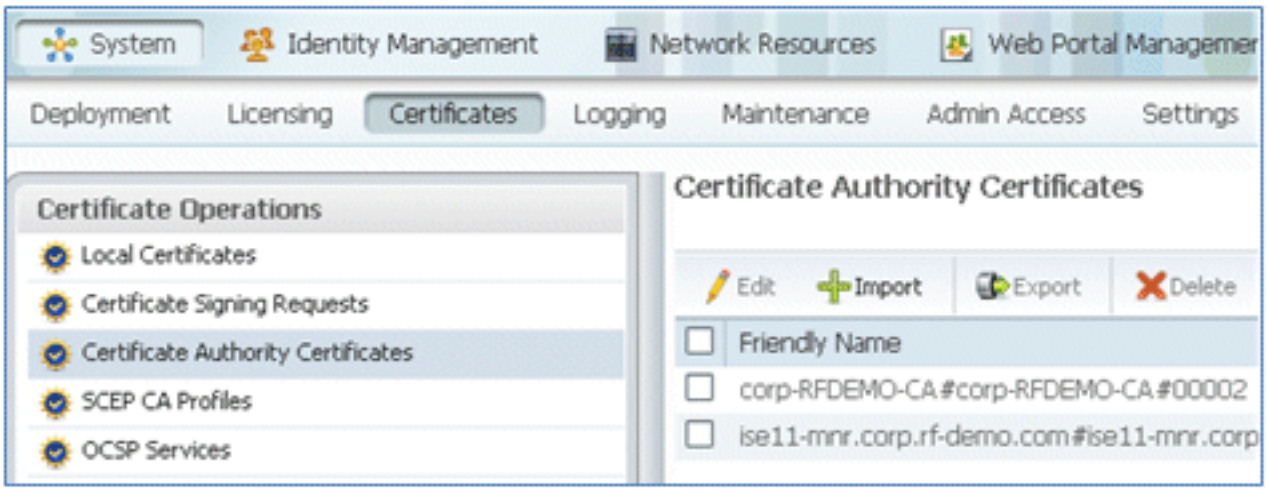
23. Klik op **Import** (Importeren).



24. Blader naar het CA-certificaat, schakel **Vertrouwen voor clientverificatie in** (aangevinkt) en klik op **Indienen**.



25. Bevestig dat het nieuwe vertrouwde CA-certificaat wordt toegevoegd.



Gerelateerde informatie

- Hardware-installatiehandleiding voor Cisco Identity Services Engine, release 1.0.4
- Cisco 2000 Series draadloze LAN-controllers
- Cisco 4400 Series draadloze LAN-controllers
- Cisco Aironet 3500 Series
- Implementatiehandleiding voor Flex 7500 Wireless Branch Controller
- Breng uw eigen apparaat - Unified device verificatie en consistente access ervaring
- Draadloze BYOD met Identity Services Engine
- 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.