

Draadloze BYOD met Identity Services Engine

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie](#)

[Conventies](#)

[Overzicht van draadloze LAN-controllers voor RADIUS, NAC en CoA](#)

[Functiestroom voor draadloze LAN-controller voor RADIUS, NAC en CoA](#)

[ISE-profilering - Overzicht](#)

[Interne identiteitsgebruikers maken](#)

[Voeg draadloze LAN-controller toe aan ISE](#)

[Configureren ISE voor draadloze verificatie](#)

[Bootstrap draadloze LAN-controller](#)

[WLC aansluiten op een netwerk](#)

[Voeg verificatieservers \(ISE\) toe aan WLC](#)

[Dynamische interface voor WLC-werknemers maken](#)

[WLC Guest Dynamic interface maken](#)

[Voeg 802.1x WLAN toe](#)

[Dynamische interfaces WLC testen](#)

[Draadloze verificatie voor iOS \(iPhone/iPad\)](#)

[Add Positie Redirect ACL naar WLC](#)

[Profieltests op ISE inschakelen](#)

[ISE-profielbeleid voor apparaten inschakelen](#)

[ISE-autorisatieprofiel voor Posture Discovery Redirect](#)

[ISE-autorisatieprofiel voor werknemers maken](#)

[ISE-autorisatieprofiel voor contractant maken](#)

[Autorisatiebeleid voor apparaatpositie/profielen](#)

[Beleid voor herstel van houding testen](#)

[Autorisatiebeleid voor gedifferentieerde toegang](#)

[CoA testen voor gedifferentieerde toegang](#)

[WLC Guest WLAN](#)

[Het testen van het WLAN en het gastenportal](#)

[ISE draadloze gesponsorde gasttoegang](#)

[Gast sponsoren](#)

[Toegang tot gastenportal testen](#)

[Certificaatconfiguratie](#)

[Integratie van Windows 2008 Active Directory](#)

[Active Directory-groepen toevoegen](#)

[Identity Source Sequence toevoegen](#)

[ISE draadloze gesponsorde gasttoegang met geïntegreerde AD](#)

[SPAN op de Switch configureren](#)

[Referentie: Draadloze verificatie voor Apple MAC OS X](#)

[Referentie: Draadloze verificatie voor Microsoft Windows XP](#)

[Referentie: Draadloze verificatie voor Microsoft Windows 7](#)

[Gerelateerde informatie](#)

Inleiding

Cisco Identity Services Engine (ISE) is de next-generation beleidserver van Cisco die verificatie- en autorisatieinfrastructuur voor de Cisco TrustSec-oplossing biedt. Daarnaast levert zij twee andere essentiële diensten:

- De eerste service is om een manier te bieden om het type apparaat voor eindpunten automatisch te benaderen op basis van de kenmerken die Cisco ISE uit verschillende informatiebronnen ontvangt. Deze service (genaamd Profiler) biedt functies die equivalent zijn aan die welke Cisco eerder heeft aangeboden met het Cisco NAC Profiler-apparaat.
- Een andere belangrijke service die Cisco ISE biedt, is het scannen van endpointcompatibiliteit; bijvoorbeeld AV/AS-softwareinstallatie en de geldigheid van het definitiebestand (bekend als Posture). Cisco heeft deze exacte poortfunctie voorheen alleen geleverd met de Cisco NAC-applicatie.

Cisco ISE biedt een equivalent niveau van functionaliteit en is geïntegreerd met 802.1X-verificatiemechanismen.

Cisco ISE geïntegreerd met Wireless LAN-controllers (WLC's) kan voorzien in profileringsmechanismen van mobiele apparaten zoals Apple iDevices (iPhone, iPad en iPod), Android-gebaseerde smartphones en andere apparaten. Voor 802.1X-gebruikers kan Cisco ISE hetzelfde serviceniveau leveren, zoals profilering en postuur scannen. Gastservices op Cisco ISE kunnen ook worden geïntegreerd met Cisco WLC door webverificatieaanvragen naar Cisco ISE te sturen voor verificatie.

Dit document introduceert de draadloze oplossing voor Bring Your Own Device (BYOD), zoals het bieden van gedifferentieerde toegang op basis van bekende endpoints en het gebruikersbeleid. Dit document biedt niet de volledige oplossing van BYOD, maar dient om een eenvoudig gebruikgeval van dynamische toegang aan te tonen. Andere configuratievoorbeelden omvatten het gebruik van het ISE-sponsorportaal, waar een geprivilegieerde gebruiker een gast kan sponsoren voor de levering van draadloze gasttoegang.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

de RADIUS NAC-instelling ingeschakeld. Wanneer het Cisco AV-paar voor URL-omleiding is ontvangen, wordt de client in de POSTURE_REQD-status gezet. Dit is in principe hetzelfde als de WEBAUTH_REQD status intern in de controller.

Wanneer de ISE RADIUS-server van mening is dat de client Posture_Compliant is, geeft het een CoA-herautorisatie af. Session_ID wordt gebruikt om het aan elkaar te koppelen. Met deze nieuwe AuthC (re-Auth) wordt de URL-Redirect AV-Paren niet verzonden. Omdat er geen URL Redirect AV-Paren zijn, weet de WLC dat de client geen Posture meer nodig heeft.

Als de RADIUS NAC-instelling niet is ingeschakeld, negeert WLC de URL Redirect VSA's.

CoA-ReAuth: Dit is ingeschakeld met de RFC 3576-instelling. De herautorisatiemogelijkheden zijn toegevoegd aan de bestaande CoA-opdrachten die eerder werden ondersteund.

De RADIUS NAC-instelling sluit deze mogelijkheid wederzijds uit, hoewel de CoA deze instelling nodig heeft om te werken.

Pre-Posture ACL: Wanneer een client in de Posture_REQ staat, het standaardgedrag van de WLC is om al verkeer te blokkeren behalve DHCP/DNS. De Pre-Posture ACL (die het in het url-redirect-acl AV-paar wordt genoemd) wordt toegepast op de cliënt, en wat in dat ACL wordt toegelaten is wat de cliënt kan bereiken.

Pre-Auth ACL vs. VLAN Override: een Quarantaine of AuthC VLAN dat verschilt van het Access-VLAN wordt niet ondersteund in 7.0MR.1. Als u een VLAN instelt vanaf de beleidserver, wordt het het VLAN voor de gehele sessie. Na de eerste autorisatie zijn geen VLAN-wijzigingen nodig.

[Functiestroom voor draadloze LAN-controller voor RADIUS, NAC en CoA](#)

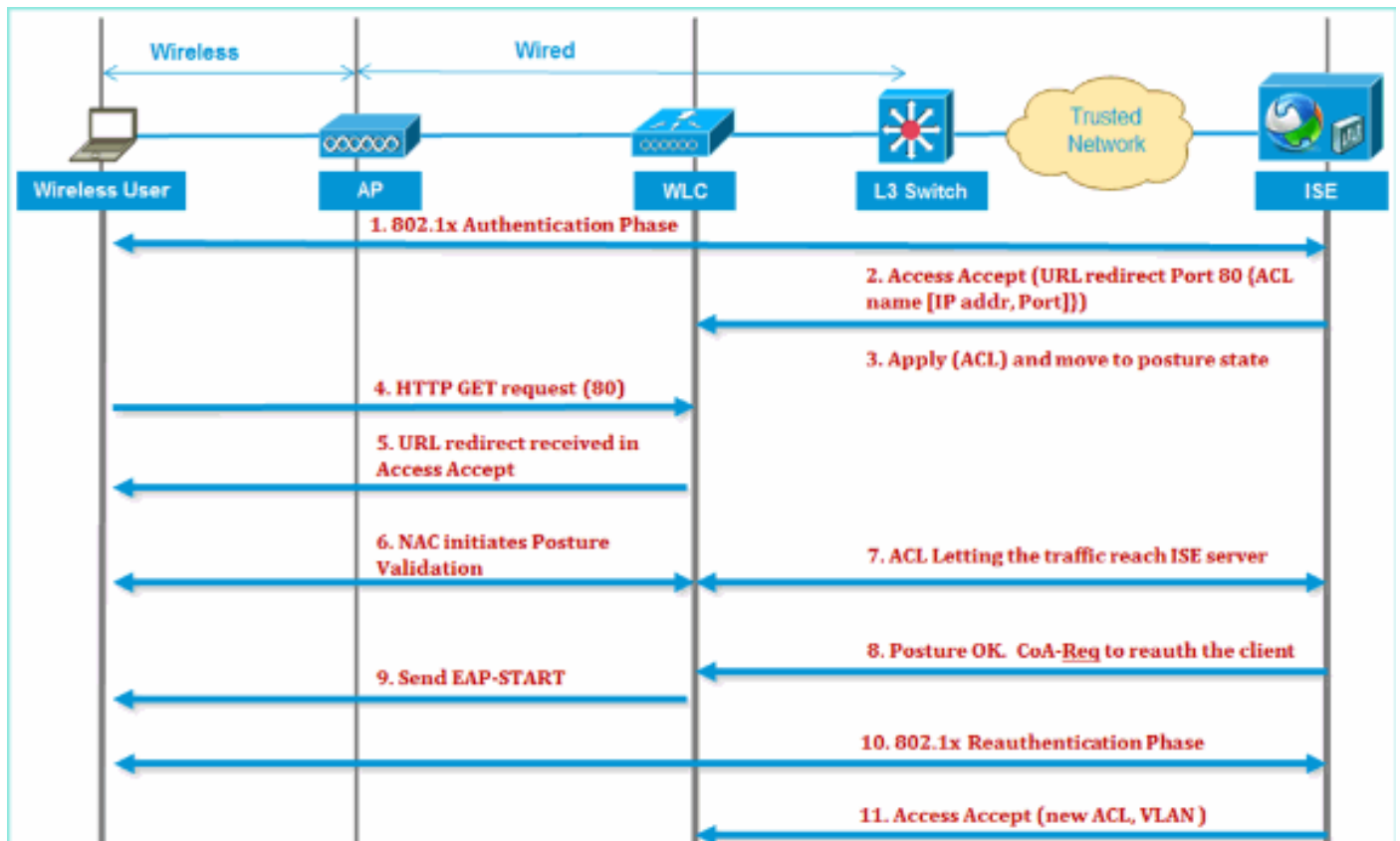
De onderstaande [figuur](#) geeft details over de berichtenuitwisseling wanneer de client wordt geverifieerd naar de backend server en NAC-posture validatie.

1. De client wordt geverifieerd met behulp van dot1x-verificatie.
2. RADIUS-toegangsgoedkeuring bevat omgeleide URL voor poort 80 en pre-auth ACL's die het toestaan van IP-adressen en poorten of quarantaine-VLAN omvatten.
3. De client zal worden omgeleid naar de URL die in toegang accepteert wordt geleverd en in een nieuwe status worden geplaatst tot de posture validatie is uitgevoerd. De client in deze staat praat met de ISE-server en valideert zichzelf tegen de beleidsregels die op de ISE NAC-server zijn geconfigureerd.
4. NAC-agent op client initieert posture validatie (verkeer naar poort 80): Agent stuurt HTTP-detectieaanvraag naar poort 80 die controller omleidt naar URL die in toegang wordt verstrekt accepteert. De ISE weet dat de klant probeert te bereiken en direct op de klant reageert. Op deze manier leert de client over de ISE-server IP en van nu af aan spreekt de client direct met de ISE-server.
5. WLC staat dit verkeer toe omdat ACL wordt gevormd om dit verkeer toe te staan. In het geval van VLAN-overschrijving wordt het verkeer overbrugd zodat het de ISE-server bereikt.
6. Zodra de ISE-client de evaluatie heeft voltooid, wordt er een RADIUS CoA-Req met basisservice naar de WLC verzonden. Hiermee wordt de verificatie van de client opnieuw gestart (door EAP-START te verzenden). Zodra de herverificatie slaagt, stuurt de ISE

toegang accepteren met een nieuwe ACL (indien van toepassing) en geen URL doorsturen, of toegang tot VLAN.

7. WLC heeft ondersteuning voor CoA-Req en Disconnect-Req zoals per RFC 3576. De WLC moet CoA-Req ondersteunen voor opnieuw opstarten, zoals per RFC 5176.
8. In plaats van downloadbare ACL's worden voorgeconfigureerde ACL's op de WLC gebruikt. De ISE-server verstuurt alleen de ACL-naam, die al in controller is geconfigureerd.
9. Dit ontwerp moet voor zowel VLAN- als ACL-cases werken. In het geval van VLAN override, we gewoon de poort 80 wordt omgeleid en staat (bridge) rest van het verkeer op het quarantaine VLAN toe. Voor ACL wordt de pre-auth ACL die in toegang wordt ontvangen, toegepast.

Dit cijfer geeft een visuele weergave van deze functiestroom:



ISE-profilering - Overzicht

Cisco ISE-profilerservice biedt de functionaliteit voor het detecteren, lokaliseren en bepalen van de functies van alle aangesloten endpoints op uw netwerk, ongeacht hun apparaattypen, om adequate toegang tot uw ondernemingsnetwerk te garanderen en te behouden. Het verzamelt voornamelijk een attribuut of een set attributen van alle endpoints op uw netwerk en classificeert ze op basis van hun profielen.

De profiler bestaat uit deze componenten:

- De sensor bevat een aantal sondes. De sondes vangen netwerkpakketten door netwerktoegangsapparaten te vragen, en door:sturen de attributen en hun attributenwaarden die van de eindpunten aan de analyser worden verzameld.
- Een analyzer evalueert eindpunten met behulp van het ingestelde beleid en de identiteitsgroepen om de kenmerken en hun verzamelde attribuutwaarden aan te passen,

waarbij eindpunten worden geclassificeerd naar de gespecificeerde groep en eindpunten worden opgeslagen met het bijbehorende profiel in de Cisco ISE-database.

Voor de detectie van mobiele apparaten wordt aanbevolen een combinatie van deze sondes te gebruiken voor een juiste identificatie van het apparaat:

- RADIUS (Calling-Station-ID): biedt het MAC-adres (OUI)
- DHCP (host-name): Hostname - standaard hostname kan apparaattype omvatten; bijvoorbeeld: jsmith-ipad
- DNS (reverse IP lookup): FQDN - standaard hostnaam kan apparaattype omvatten
- HTTP (User-Agent): gegevens over specifiek type mobiel apparaat

In dit voorbeeld van een iPad, vangt de profiler de webbrowser informatie van de User-Agent attributen, evenals andere eigenschappen van HTTP van de verzoekberichten, en voegt hen aan de lijst van endpointattributen toe.



Is the MAC Address
from Apple?



Does the Hostname
contain "iPad"?



Is the Safari Browser
on an iPad?



I am
certain it
is an iPad!

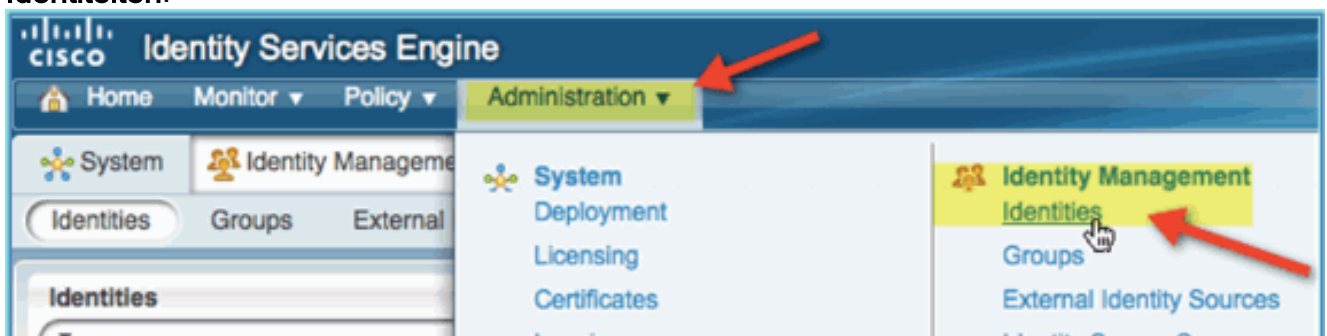
[Interne identiteitsgebruikers maken](#)

MS Active Directory (AD) is niet vereist voor een eenvoudig proof-of-concept. ISE kan worden gebruikt als de enige identiteitswinkel, waaronder het differentiëren van gebruikers toegang voor toegang en granulaire beleidscontrole.

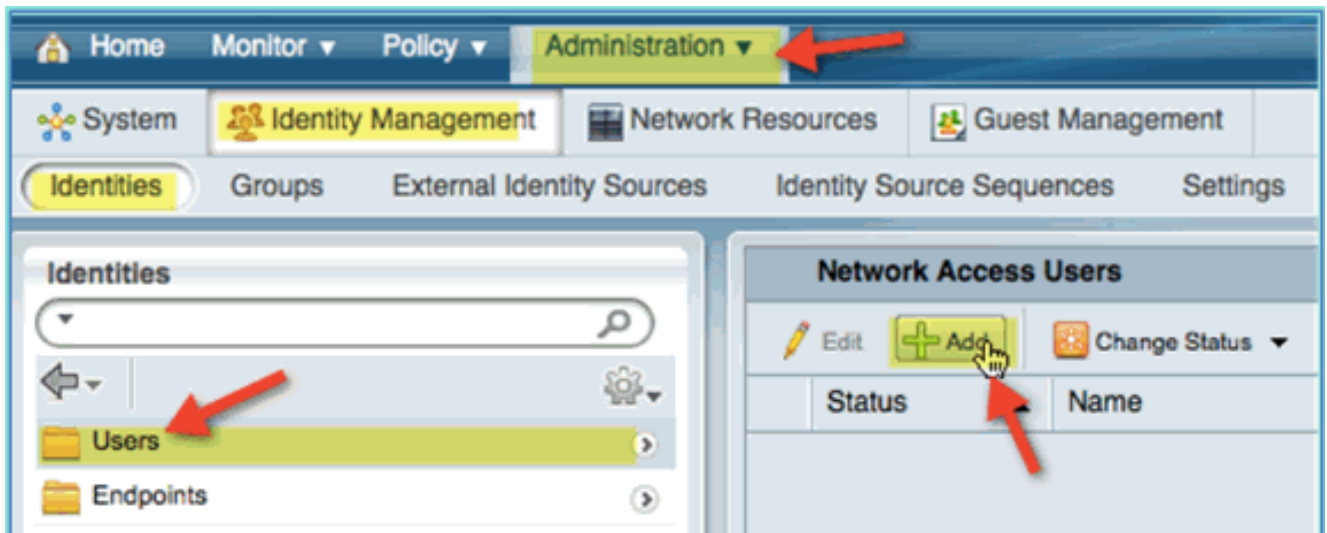
Bij de release van ISE 1.0, met AD-integratie, kan de ISE AD-groepen gebruiken in het autorisatiebeleid. Als de interne gebruikerswinkel van ISE wordt gebruikt (geen AD-integratie), kunnen groepen niet worden gebruikt in beleid in combinatie met apparaatidentiteitsgroepen (een geïdentificeerd bug die in ISE 1.1 moet worden opgelost). Daarom kan alleen onderscheid worden gemaakt tussen individuele gebruikers, zoals werknemers of aannemers, wanneer deze naast de apparaatidentiteitsgroepen worden gebruikt.

Voer de volgende stappen uit:

1. Open een browservenster naar het https://ISEip-adres.
2. Ga naar **Administratie > Identiteitsbeheer > Identiteiten**.

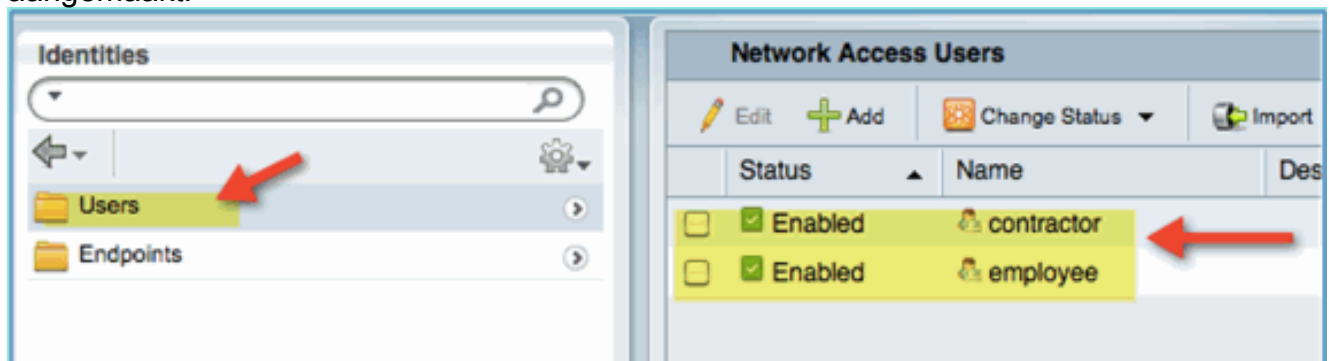


3. Selecteer **Gebruikers** en klik op **Toevoegen** (Gebruiker van netwerktoegang). Voer deze gebruikerswaarden in en wijs toe aan werknemersgroep: Naam: medewerker Wachtwoord: XXXX





4. Klik op **Verzenden**. Naam: contractant Wachtwoord: XXXX
5. Controleer of beide accounts zijn aangemaakt.



Voeg draadloze LAN-controller toe aan ISE

Elk apparaat dat RADIUS-verzoeken naar de ISE initieert, moet een definitie in ISE hebben. Deze netwerkapparaten worden gedefinieerd op basis van hun IP-adres. ISE-netwerkapparaatdefinities kunnen IP-adresbereiken specificeren, zodat de definitie meerdere werkelijke apparaten kan vertegenwoordigen.

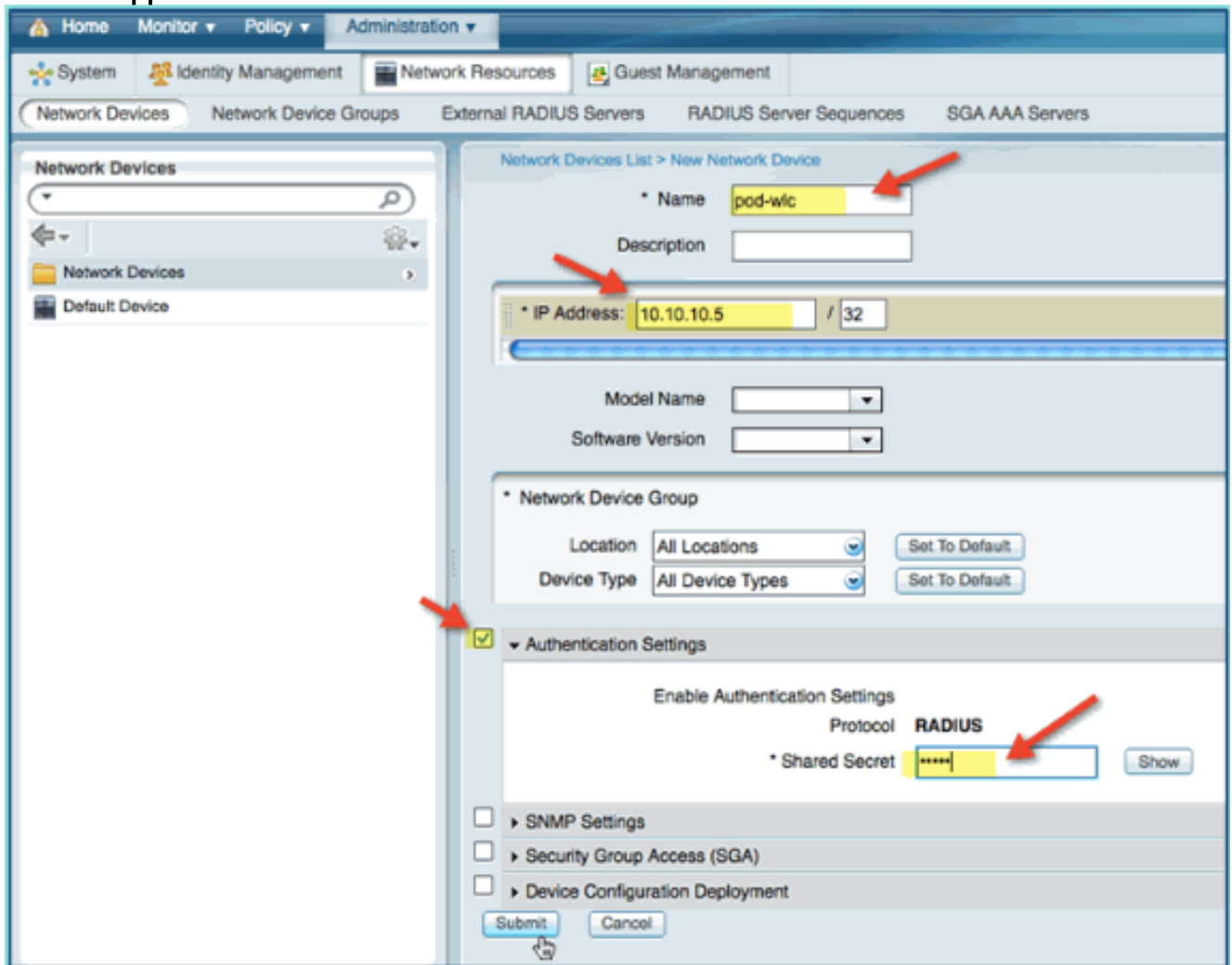
Buiten wat nodig is voor RADIUS-communicatie, bevatten de definities van ISE-netwerkapparaten instellingen voor andere ISE-communicatie/communicatie met apparaten, zoals SNMP en SSH.

Een ander belangrijk aspect van de definitie van netwerkapparaten is het op de juiste wijze groeperen van apparaten zodat deze groepering in het beleid van de netwerktoegang kan worden leveraged.

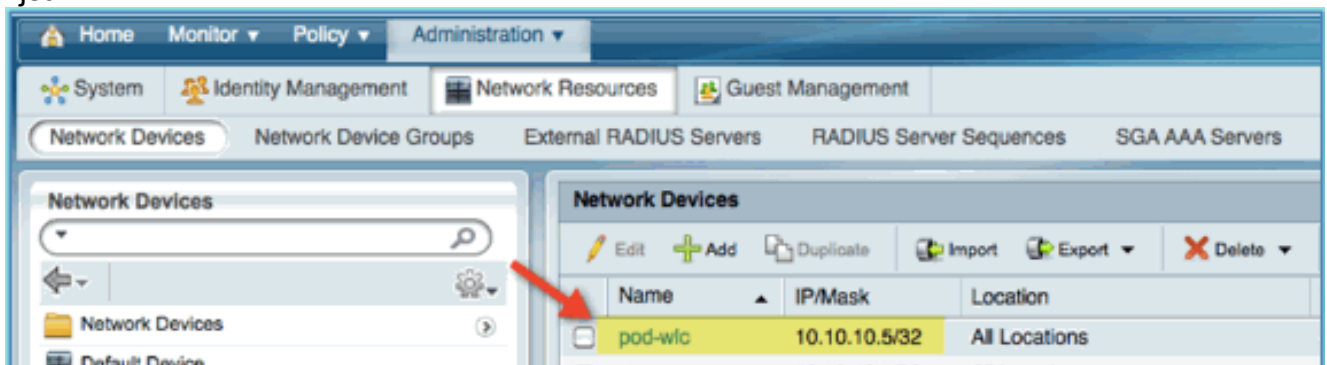
In deze oefening, worden de apparatendefinities die voor uw laboratorium worden vereist gevormd.

Voer de volgende stappen uit:

1. Ga van ISE naar **Beheer > Netwerkbronnen > Netwerkapparaten**.



2. Klik op **Toevoegen** op Netwerkapparaten. Voer het IP-adres in, controleer de verificatieinstelling en voer vervolgens "cisco" in voor gedeeld geheim.
3. Sla de WLC-vermelding op en bevestig de controller in de lijst.

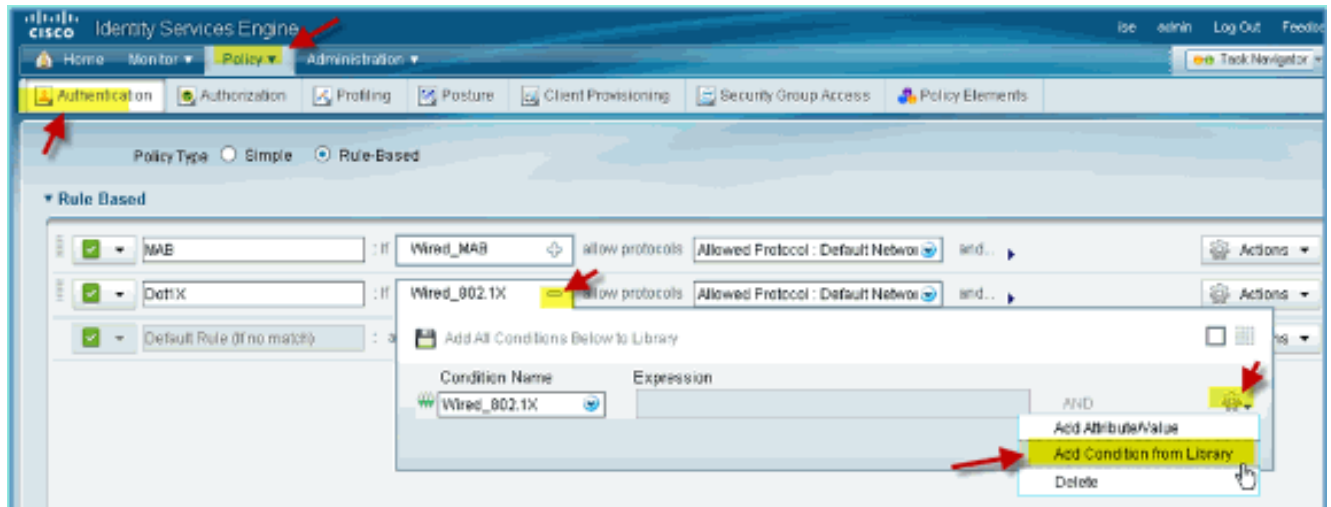


[Configureren ISE voor draadloze verificatie](#)

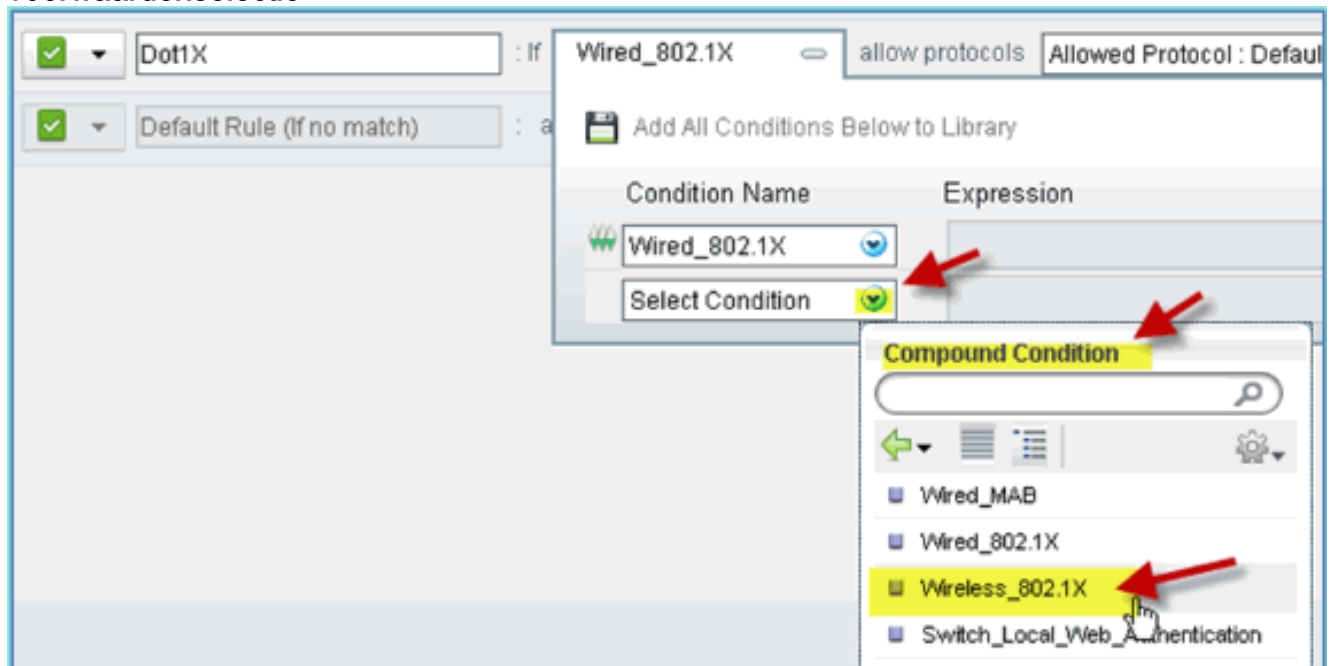
De ISE moet worden geconfigureerd voor het authenticeren van 802.1x draadloze clients en voor het gebruik van Active Directory als identiteitsopslag.

Voer de volgende stappen uit:

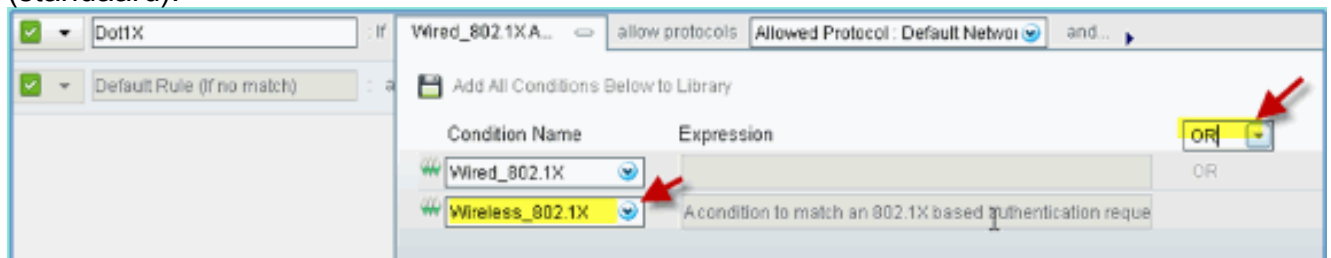
1. Ga van ISE naar **Policy > Verificatie**.
2. Klik hierop om Dot1x > Wired_802.1X (-) uit te vouwen.
3. Klik op het tandwielpictogram om **Conditie toe te voegen uit bibliotheek**.

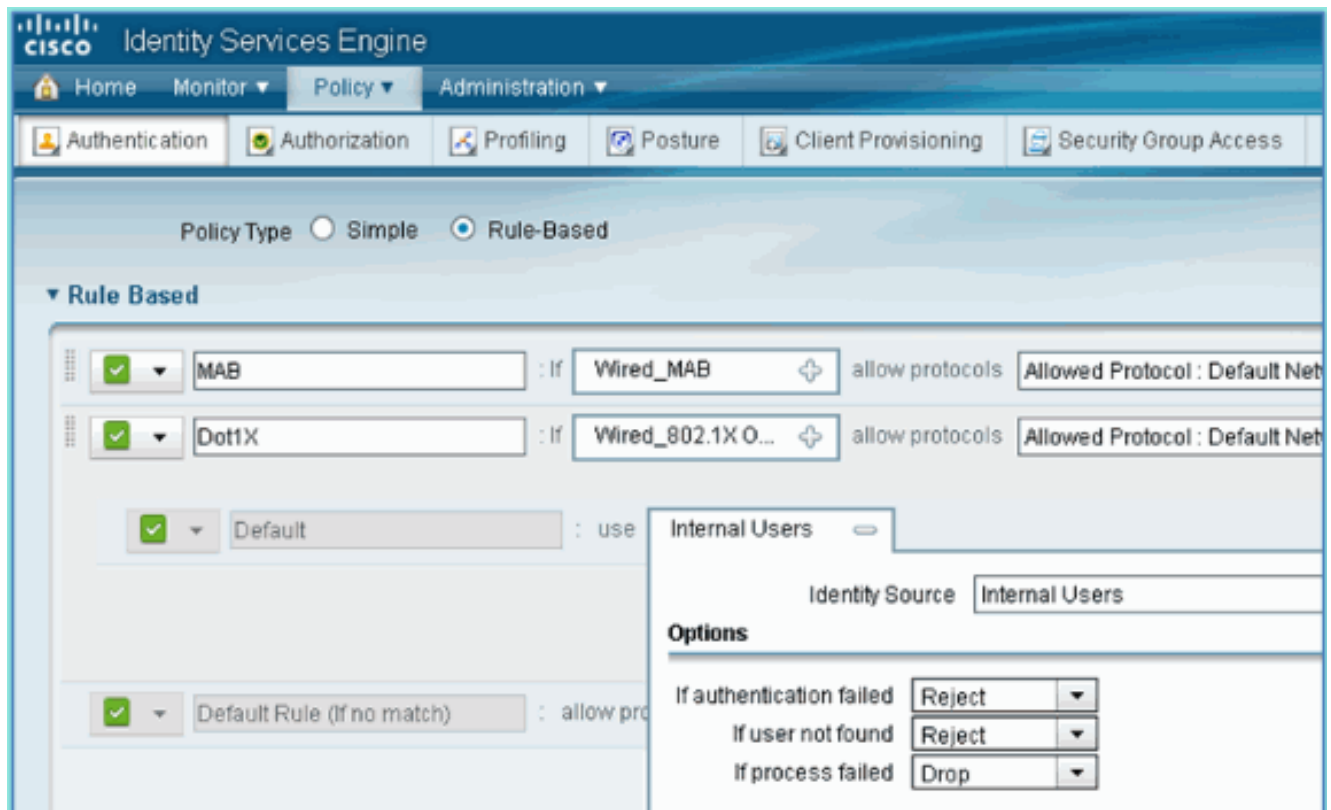


4. Kies **Samengestelde toestand > Wireless_802.1X** in de vervolgkeuzelijst voorwaardenselectie.



5. Stel de Express voorwaarde in op **OR**.
6. Breid de optie achteraf toegestane protocollen uit en accepteer de standaard interne gebruikers (standaard).





7. Laat de rest bij default. Klik op **Opslaan** om de stappen te voltooien.

[Bootstrap draadloze LAN-controller](#)

[WLC aansluiten op een netwerk](#)

Een implementatiegids voor Cisco 2500 draadloze LAN-controllers is ook beschikbaar in de [implementatiegids voor Cisco 2500 Series draadloze controllers](#).

De controller configureren met de opstartwizard

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
(3 to 24 characters): Cisco123
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes

Enable 802.11a Network [YES][no]: yes

Enable 802.11g Network [YES][no]: yes

Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no

Configure the ntp system time now? [YES][no]: yes

Enter the date in MM/DD/YY format: mm/dd/yy

Enter the time in HH:MM:SS format: hh:mm:ss

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!

Resetting system with new configuration...

Restarting system.

Configuratie buurman Switch

De controller is aangesloten op de Ethernet-poort op de naburige switch (Fast Ethernet 1). De buurpoort voor switch is geconfigureerd als een 802.1Q-trunk en maakt alle VLAN's in de trunk mogelijk. Met de native VLAN 10 kan de beheerinterface van de WLC worden aangesloten.

De configuratie van de 802.1Q-switch is als volgt:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

[Voeg verificatieservers \(ISE\) toe aan WLC](#)

De ISE moet aan de WLC worden toegevoegd om 802.1X en de CoA-functie voor draadloze endpoints mogelijk te maken.

Voer de volgende stappen uit:

1. Open een browser, dan verbinding met de pod WLC (met behulp van beveiligde HTTP) > <https://wlc>.
2. Navigeer naar **Beveiliging > Verificatie > Nieuw**.

MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User Enable

Management Enable

IPSec Enable

- Voer deze waarden in: IP-adres server: 10.10.10.70 (controletoewijzing) Gedeeld geheim: cisco
Ondersteuning voor RFC 3576 (CoA): ingeschakeld (standaard) Alle andere: Standaard
- Klik op **Toepassen** om door te gaan.
- Selecteer **RADIUS-accounting > NIEUW toevoegen**.

CISCO MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT

Security RADIUS Accounting Servers > New

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies
- Local EAP
- Priority Order
- Certificate

Server Index (Priority) 2

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Port Number 1813

Server Status Enabled

Server Timeout 2 seconds

Network User Enable

IPSec Enable

- Voer deze waarden in: IP-adres server: 10.10.10.70 Gedeeld geheim: cisco Alle andere: Standaard
- Klik op **Toepassen** en sla vervolgens de Configuration op voor de WLC.

Dynamische interface voor WLC-werknemers maken

Voltooi deze stappen om een nieuwe dynamische interface voor WLC toe te voegen en het in kaart te brengen aan de Werknemer VLAN:

1. Van WLC, navigeer aan **Controlemechanisme > Interfaces**. Klik vervolgens op **Nieuw**.



2. Van WLC, navigeer aan **Controlemechanisme > Interfaces**. Voer het volgende in: Interface naam: WerknemerVLAN-id:
11



3. Voer het volgende in voor werknemersinterface: Poortnummer: 1 VLAN-identificatiecode: 11 IP-adres: 10.10.11.5 Netmasker: 255.255.255.0 Gateway: 10.10.11.1 DHCP: 10.10.10.10

Configuration

Quarantine

Quarantine Vlan Id

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

4. Bevestig dat de nieuwe dynamische interface voor werknemers is gemaakt.

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMUNITY

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

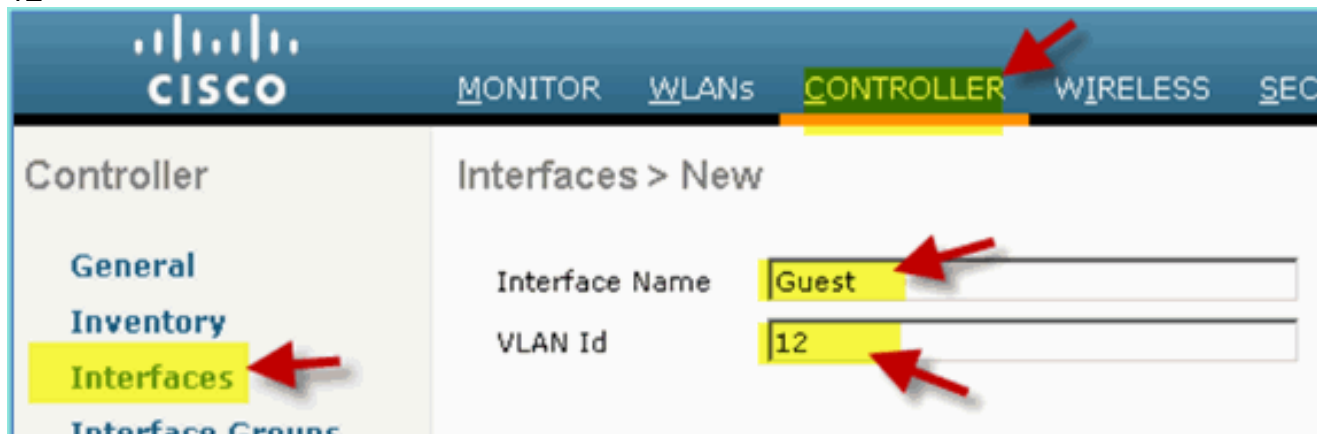
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

WLC Guest Dynamic interface maken

Voltooi deze stappen om een nieuwe dynamische interface voor WLC toe te voegen en het in kaart te brengen aan de Gast VLAN:

1. Van WLC, navigeer aan **Controlemechanisme > Interfaces**. Klik vervolgens op **Nieuw**.
2. Van WLC, navigeer aan **Controlemechanisme > Interfaces**. Voer het volgende in: Interfacenaam: Gast VLAN-id: 12



3. Voer deze in voor de gastinterface: Poortnummer: 1 VLAN-id: 12 IP-adres: 10.10.12.5 Netmasker: 255.255.255.0 Gateway: 10.10.12.1 DHCP: 10.10.10.10

Configuration

Quarantine
Quarantine Vlan Id

Physical Information

Port Number
Backup Port
Active Port
Enable Dynamic AP Management

Interface Address

VLAN Identifier
IP Address
Netmask
Gateway

DHCP Information

Primary DHCP Server
Secondary DHCP Server

Access Control List

ACL Name

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. Bevestig dat de gastinterface is toegevoegd.

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
quest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Voeg 802.1x WLAN toe

Vanaf de eerste bootstrap van WLC, kan er een standaard WLAN gecreëerd zijn. Als dit het geval is, wijzig deze of maak een nieuw WLAN om de draadloze 802.1X-verificatie te ondersteunen, zoals beschreven in de handleiding.

Voer de volgende stappen uit:

1. Van WLC, navigeer aan **WLAN > creëer Nieuw**.



2. Voer voor het WLAN het volgende in: Profielnaam: pod1x SSID: hetzelfde



3. Gebruik voor de WLAN-instellingen > tabblad Algemeen het volgende: Radiobeleid: AlleInterface/groep: beheerAl het andere: standaard

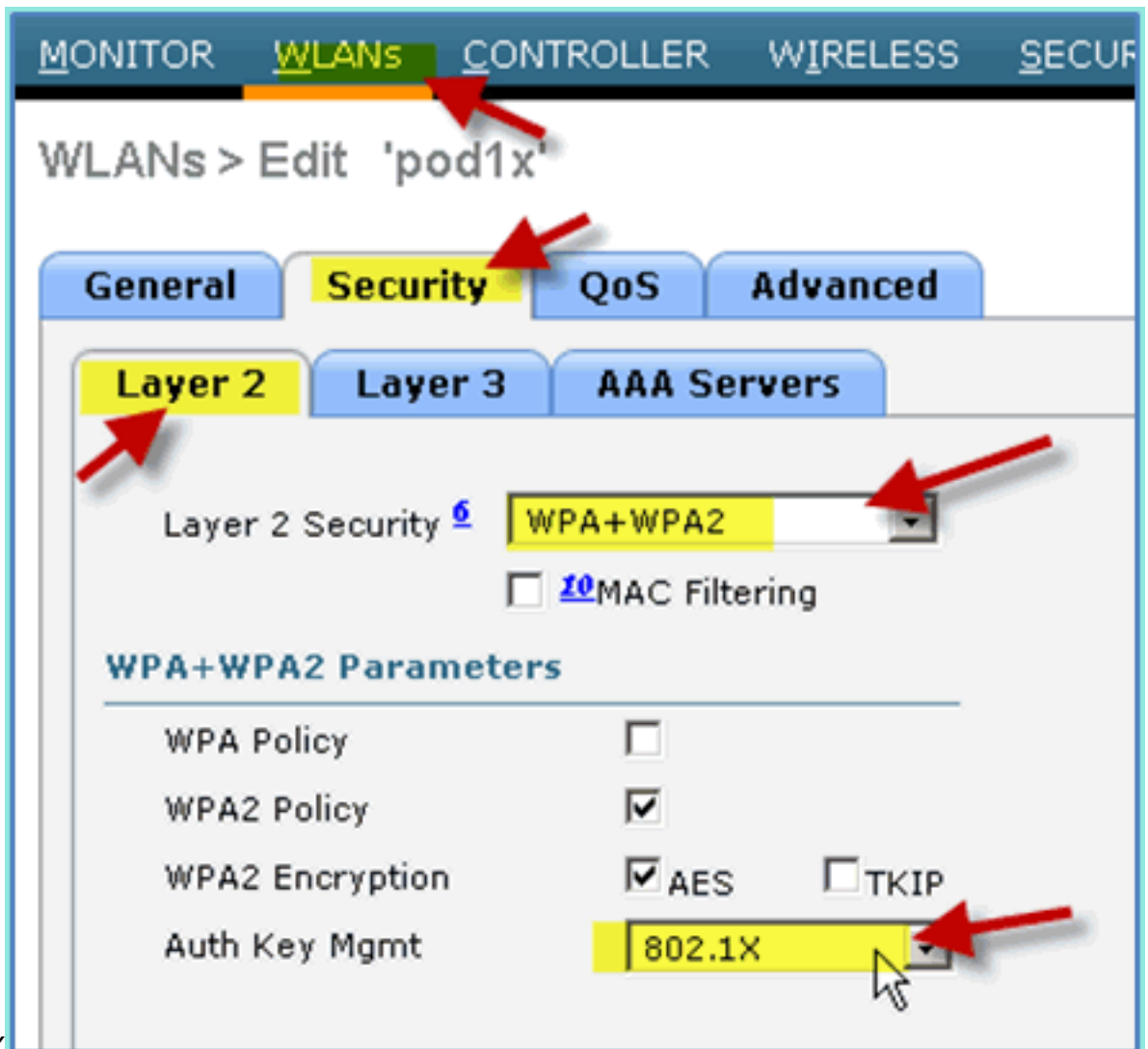
MONITOR WLANS CONTROLLER WIRELESS SECURITY

WLANs > Edit 'pod1x'

General Security QoS Advanced

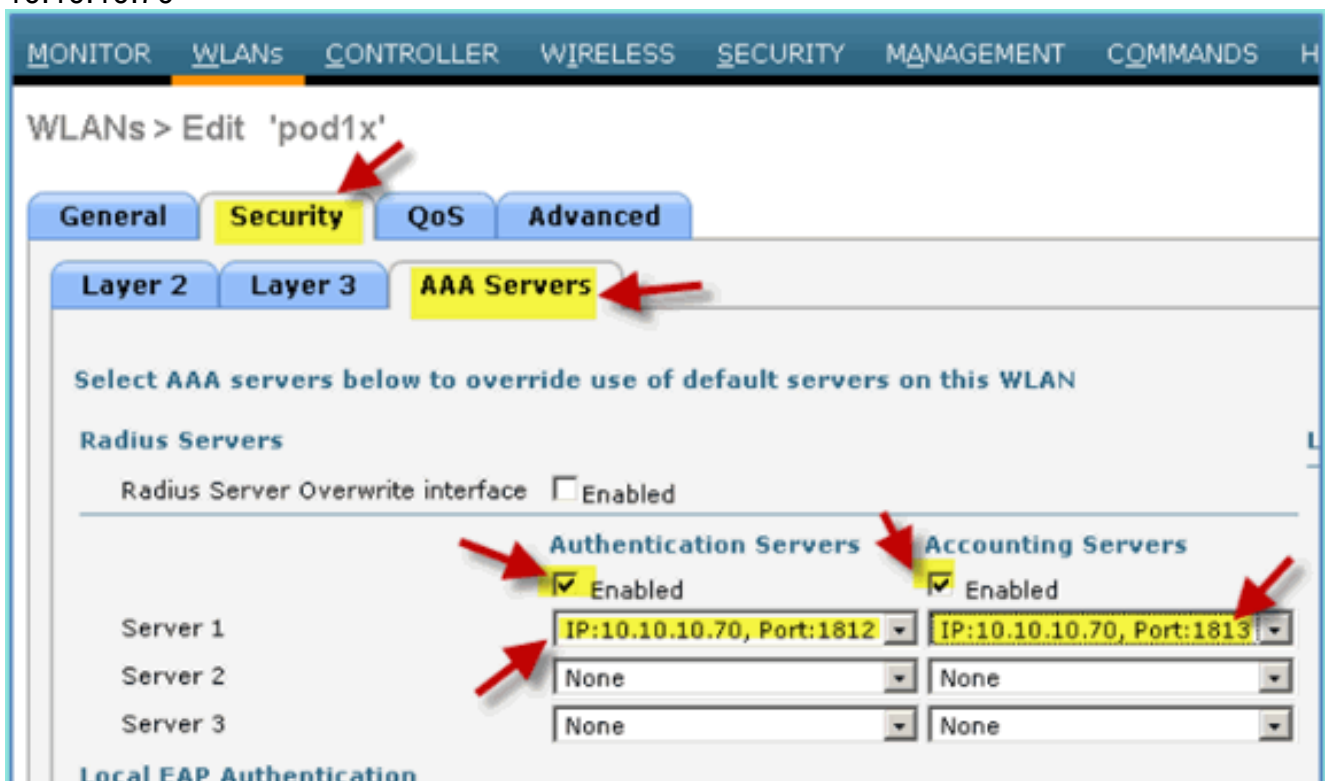
Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab w
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

4. Stel voor het WLAN > Beveiligingstabblad > Layer 2 het volgende in: Layer 2-beveiliging: WPA+WPA2 WPA2-beleid/encryptie: ingeschakeld/AES Beheer autorisatiesleutel:



802.1X

5. Stel voor WLAN > Beveiligingstabblad > AAA-servers het volgende in: Interface voor overschrijven van radioserver: uitgeschakeld
 Verificatie-/boekhoudservers: ingeschakeld
 Server 1: 10.10.10.70



6. Geef op het tabblad WLAN > Geavanceerd het volgende op:AAA negeren: ingeschakeld
toestaanNAC-status: straal NAC
(geselecteerd)

The screenshot shows the 'WLANs > Edit 'pod1x'' configuration page. The 'Advanced' tab is selected and highlighted in yellow. A red arrow points to the 'Advanced' tab. Below it, the 'Allow AAA Override' checkbox is checked and highlighted in yellow, with another red arrow pointing to it. In the 'NAC' section, the 'NAC State' dropdown menu is set to 'Radius NAC' and is also highlighted in yellow with a red arrow. Other visible settings include 'Coverage Hole Detection' (checked), 'Enable Session Timeout' (checked, 1800 secs), 'Aironet IE' (checked), 'Diagnostic Channel' (unchecked), 'IPv6 Enable' (unchecked), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (checked, 60 secs), 'Maximum Allowed Clients' (0), and 'Static IP Tunneling' (unchecked). The right-hand side shows 'DHCP' settings (DHCP Server, DHCP Addr. Assignment), 'Management Frame Protection (MFP)' (MFP Client Protection: Optional), and 'DTIM Period (in beacon intervals)' (802.11a/n: 1, 802.11b/g/n: 1).

7. Terug naar het tabblad WLAN > Algemeen > WLAN inschakelen
(aanvinkvakje).

WLANs > Edit 'pod1x'

General Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

[Dynamische interfaces WLC testen](#)

U moet snel controleren of er geldige werknemer- en gasteninterfaces zijn. Gebruik een willekeurig apparaat om te koppelen aan het WLAN en verander vervolgens de WLAN-interfacetaak.

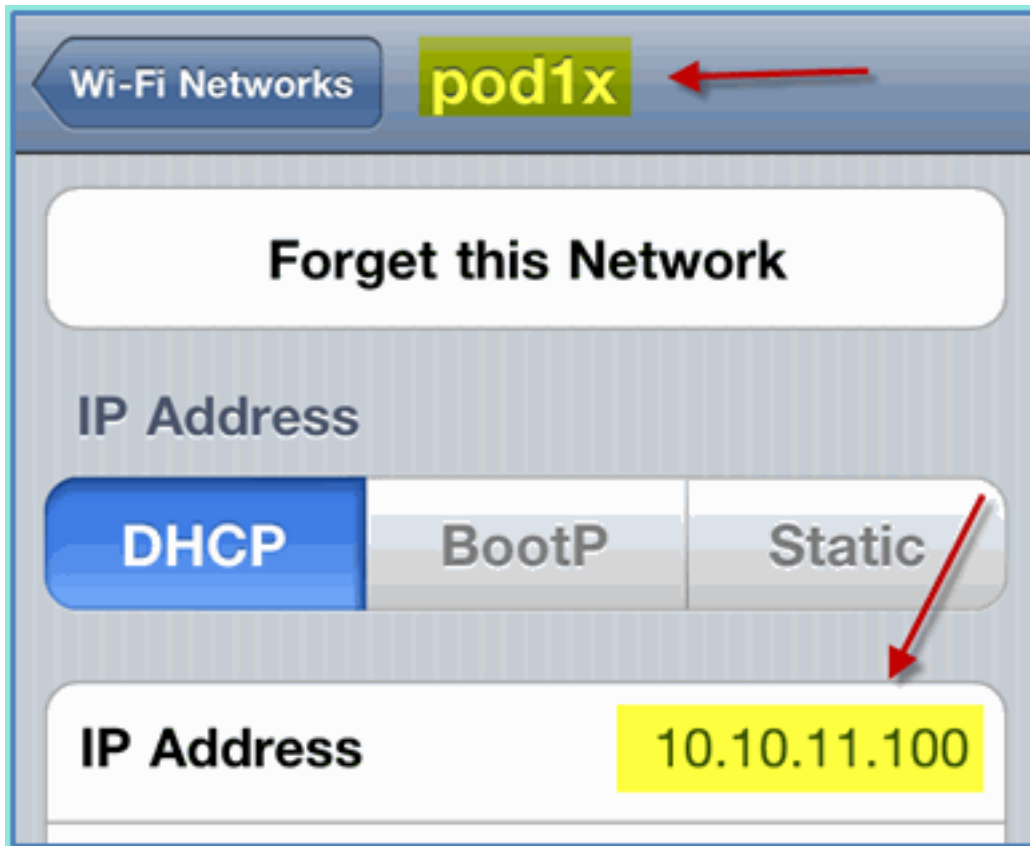
1. Van WLC, navigeer aan **WLAN > WLAN's**. Klik om uw beveiligde SSID die in de eerdere oefening is gemaakt, te bewerken.
2. Wijzig de interface/interfacegroep in **Werknemer** en klik vervolgens op **Toepassen**.

The screenshot displays the Cisco WLAN configuration interface. At the top, the Cisco logo is on the left, and navigation tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY are on the right. The main content area is titled 'WLANs > Edit 'pod1x''. On the left sidebar, there is a tree view with 'WLANs' and 'Advanced' folders. The 'WLANs' folder is expanded, and the 'WLANs' sub-item is selected. The main configuration area has four tabs: General, Security, QoS, and Advanced. The 'General' tab is active. The configuration details are as follows:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security to
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	guest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Red arrows point to the 'WLANs' tab in the top navigation, the 'WLANs' folder in the sidebar, the 'General' tab, and the 'management' dropdown menu in the 'Interface/Interface Group(G)' field. The dropdown menu is open, showing options: 'management', 'employee', 'guest', and 'management'. A mouse cursor is pointing at the 'employee' option.

3. Indien correct geconfigureerd, ontvangt een apparaat een IP-adres van de werknemer VLAN (10.10.11.0/24). Dit voorbeeld toont een iOS-apparaat dat een nieuw IP-adres



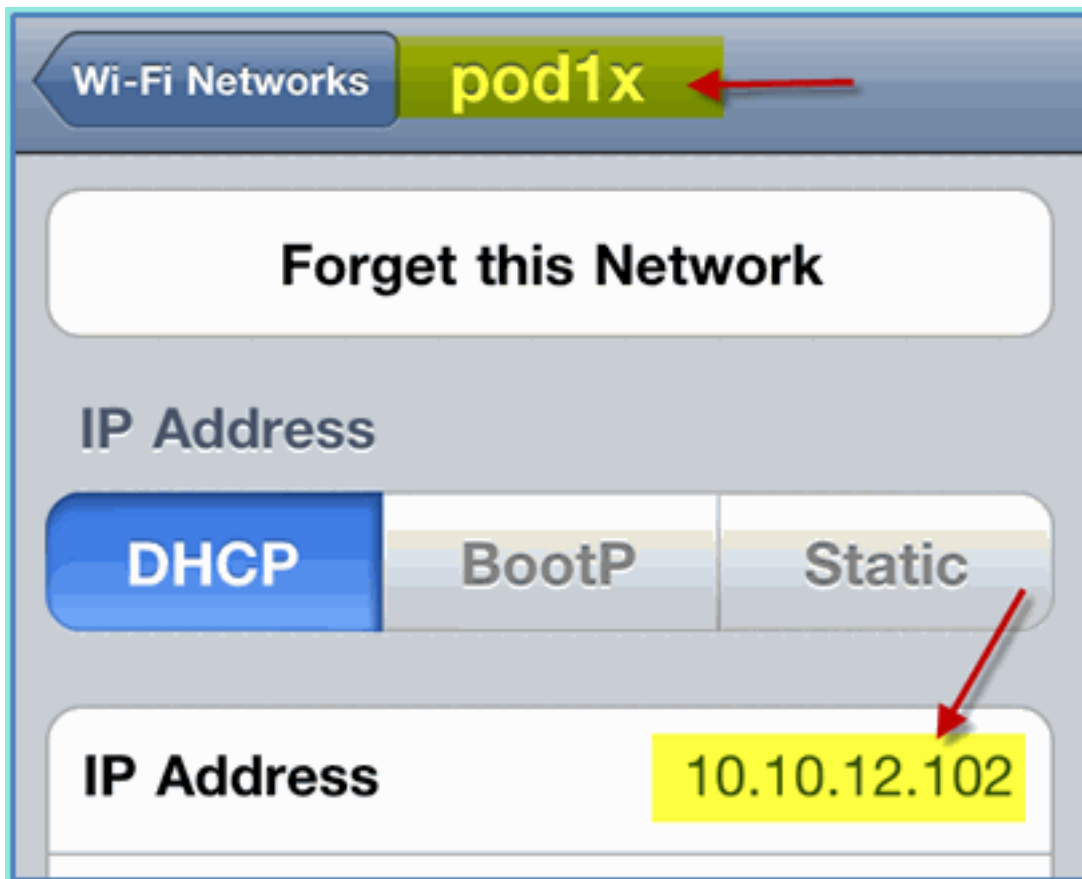
krijgt.

4. Nadat de vorige interface is bevestigd, wijzigt u de WLAN-interfacetaak in **Gast** en klikt u op **Toepassen**.

The screenshot shows the Cisco configuration interface for WLANs. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The main content area is titled 'WLANs > Edit 'pod1x''. Below this, there are four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active. The configuration details are as follows:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	quest
Multicast Vlan Feature	quest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. Indien correct geconfigureerd, ontvangt een apparaat een IP-adres van de gast VLAN (10.10.12.0/24). Dit voorbeeld toont een iOS-apparaat dat een nieuw IP-adres



krijgt.

6. **BELANGRIJK:** Verander de interfacetaak terug naar het oorspronkelijke beheer.
7. Klik op **Toepassen** en opslaan van de Configuration voor de WLC.

[Draadloze verificatie voor iOS \(iPhone/iPad\)](#)

Associeer aan de WLC via een geverifieerde SSID een INTERNE gebruiker (of geïntegreerd, AD-gebruiker) met behulp van een iOS-apparaat zoals een iPhone, iPad of iPod. Sla deze stappen over als dit niet van toepassing is.

1. Ga voor het iOS-apparaat naar de WLAN-instellingen. Schakel WIFI in en selecteer vervolgens de 802.1X-compatibele SSID die in de vorige paragraaf is gemaakt.
2. Geef deze informatie op om verbinding te maken met: Gebruikersnaam: werknemer (intern - werknemer) of aannemer (intern - aannemer) Wachtwoord:



XXXX

3. Klik om het ISE-certificaat te



accepteren.

4. Bevestig dat het iOS-apparaat een IP-adres krijgt van de beheerinterface



(VLAN10).

5. Controleer op de WLC > Monitor > Clients de endpointinformatie, waaronder gebruik, status en EAP-type.

The screenshot displays the Cisco ISE Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar shows a menu with 'Monitor' selected, and sub-items like 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients', and 'Multicast'. The main content area is titled 'Clients > Detail' and is divided into two sections: 'Client Properties' and 'Security Information'.

Client Properties

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN

AAA Override ACL Name none



6. Op dezelfde manier kan de cliëntinformatie door ISE > Monitor > de pagina van de Verificatie worden verstrekt.

CISCO Identity Services Engine

Home Monitor Policy Administration

Authentications Alarms Reports Troubleshoot

Add or Remove Columns Refresh

Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:36.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7. Klik op het pictogram **Details** om naar beneden te boren naar de sessie voor uitgebreide informatie over de sessie.



Showing Page 1 of 1

First Prev

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45

AAA session ID : ise/99967658/11

Date : July 13, 2011

Generated on July 13, 2011 4:41:11 PM PDT

Authentication Summary

Logged At: July 13, 2011 4:39:36.573 PM

RADIUS Status: Authentication succeeded

NAS Failure:

Username: aduser

MAC/IP Address: 5C:59:48:40:82:8D

Network Device: WLC : 10.10.10.5 :

Allowed Protocol: Default Network Access

Identity Store: AD1

Authorization Profiles: PermitAccess

SGA Security Group:

Authentication Protocol : PEAP(EAP-MSCHAPv2)

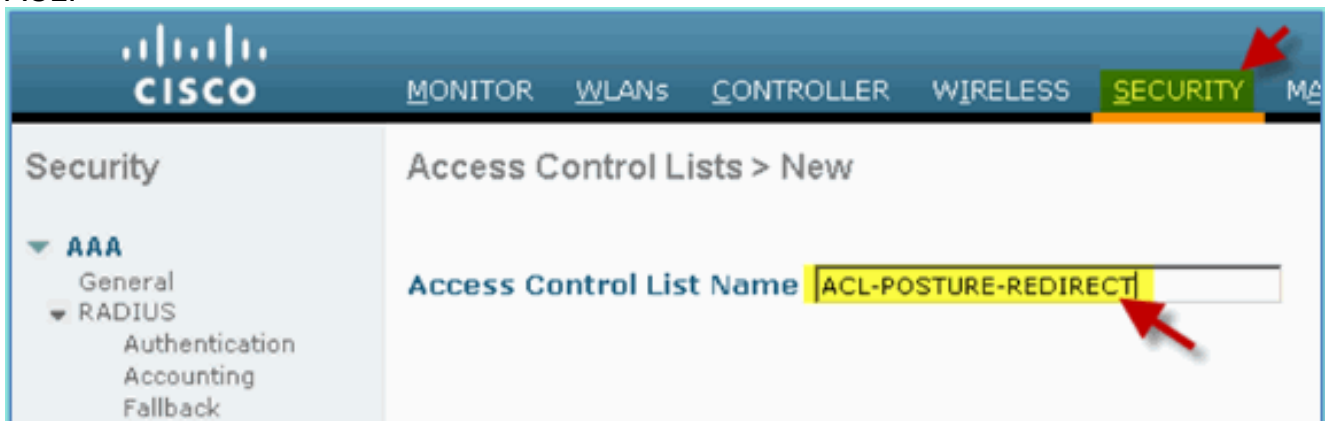
Add Positie Redirect ACL naar WLC

Posture redirect ACL is geconfigureerd op de WLC, waar ISE zal gebruiken om client voor postuur te beperken. De ACL maakt verkeer tussen ISE effectief en op zijn minst mogelijk. Optionele regels kunnen indien nodig worden toegevoegd in deze ACL.

1. Navigeer naar **WLC > Security > Access Control Lists > Access Control Lists**. Klik op **New (Nieuw)**.



2. Geef een naam (ACL-POSTURE-REDIRECT) op voor de ACL.



3. Klik op **Nieuwe regel toevoegen** voor de nieuwe ACL. Stel de volgende waarden in op ACL-sequentie #1. Klik op **Toepassen** na voltooiing. Bron: AlleBestemming: IP-adres 10.10.10.70, 255.255.255.255 Protocol: alleActie: Permit

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Access Control Lists > Rules > Edit

Sequence: 1

Source: Any

Destination: IP Address

IP Address: 10.10.10.70

Netmask: 255.255.255.255

Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

4. Bevestig de volgorde is toegevoegd.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. Klik op **Nieuwe regel toevoegen**. Stel de volgende waarden in op ACL-sequentie #2. Klik op **Toepassen** na voltooiing. Bron: IP-adres 10.10.10.70, 25.255.255.255 Bestemming: alle Protocol: alle Actie: Permit

Sequence: 2

Source: IP Address

IP Address: 10.10.10.70

Netmask: 255.255.255.255

Destination: Any

Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

6. Bevestig de volgorde is toegevoegd.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0					

7. Stel de volgende waarden in op ACL-sequentie #3. Klik op **Toepassen** na voltooiing. Bron: AlleBestemming: alleProtocol: UDPBronpoort: DNSBestemmingspoort: AnyActie:

Sequence: 3

Source: Any

Destination: Any

Protocol: UDP

Source Port: DNS

Destination Port: Any

DSCP: Any

Direction: Any

Action: Permit

Permit

8. Bevestig de volgorde is toegevoegd.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0					
<u>3</u>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0 /	0.0.0.0					

9. Klik op **Nieuwe regel toevoegen**. Stel de volgende waarden in op ACL-sequentie #4. Klik op **Toepassen** na voltooiing. Bron: AlleBestemming: alleProtocol: UDPBronpoort:

AnyResDoelpoort: DNSActie:

Sequence: 4

Source: Any

Destination: Any

Protocol: UDP

Source Port: Any

Destination Port: DNS

DSCP: Any

Direction: Any

Action: Permit

Permit

10. Bevestig de volgorde is toegevoegd.

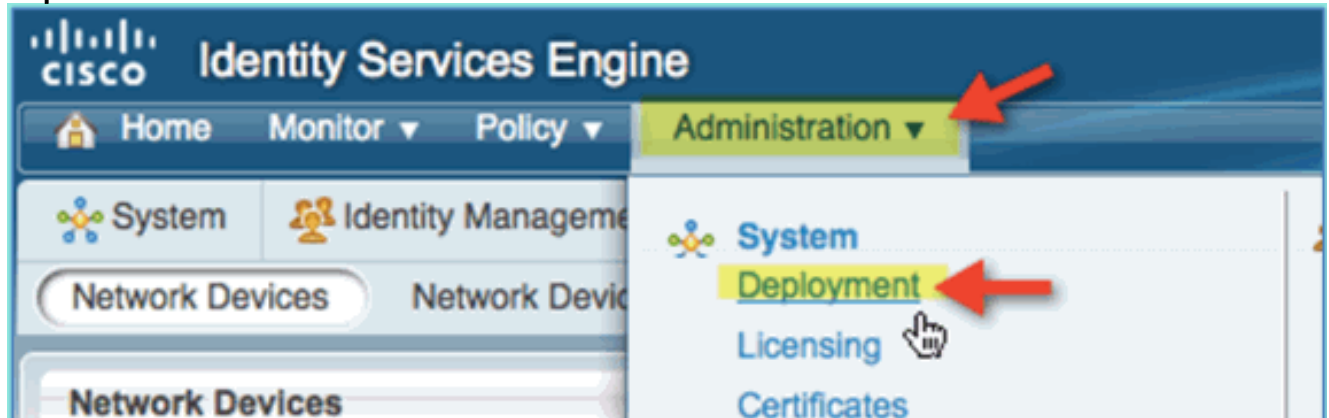
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any

11. Sla de huidige WLC-configuratie op.

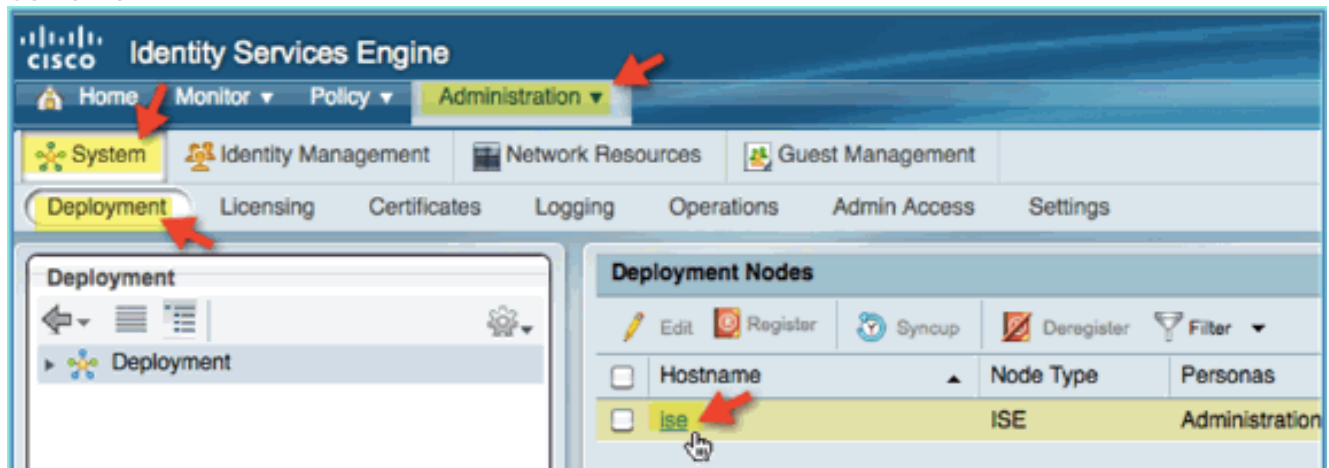
[Profieltests op ISE inschakelen](#)

De ISE moet als probes worden geconfigureerd om effectief eindpunten te profileren. Deze opties zijn standaard uitgeschakeld. Deze paragraaf laat zien hoe u ISE kunt configureren als probes.

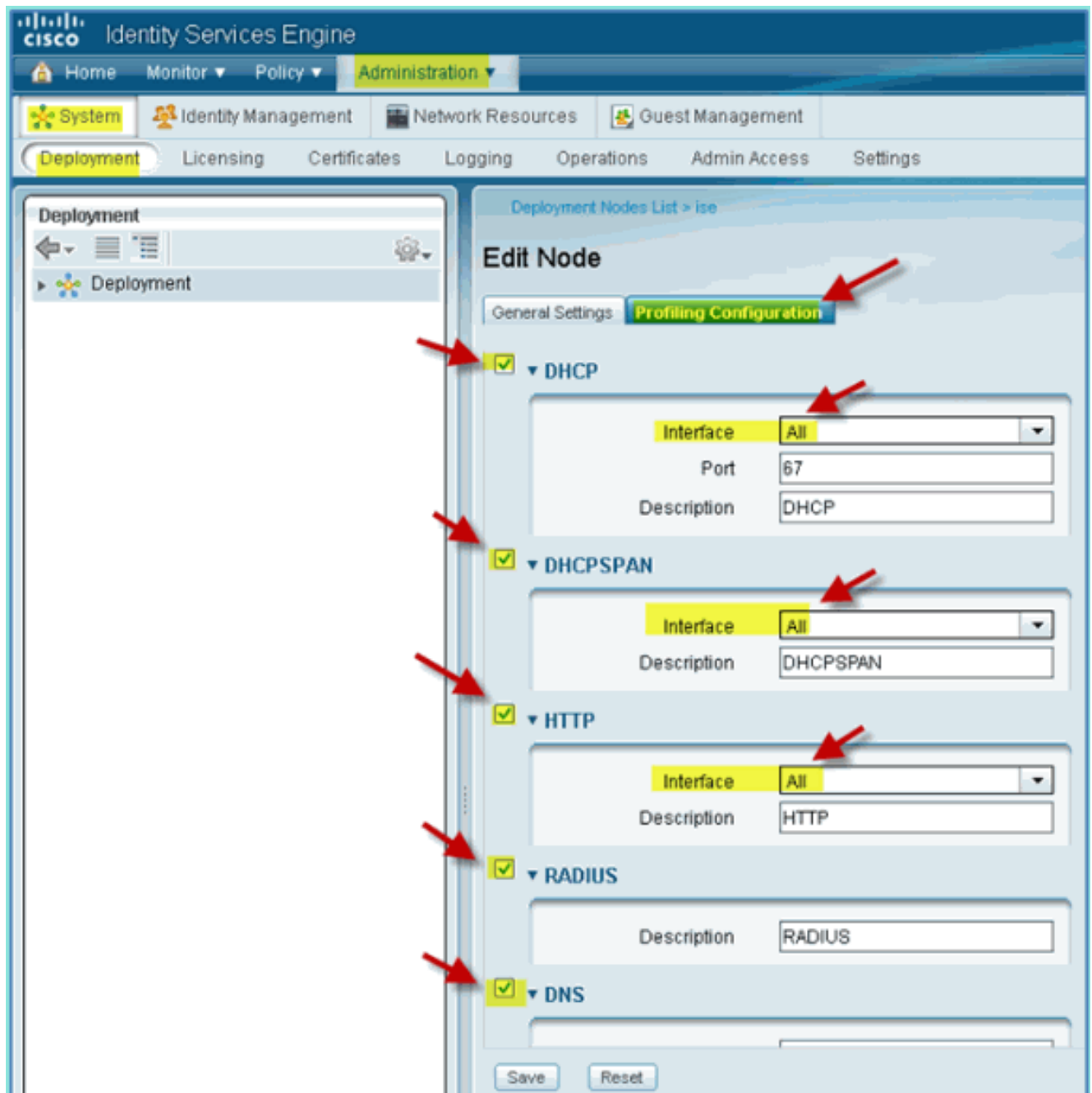
1. Ga van ISE-beheer naar **Beheer > Systeem > Implementatie**.



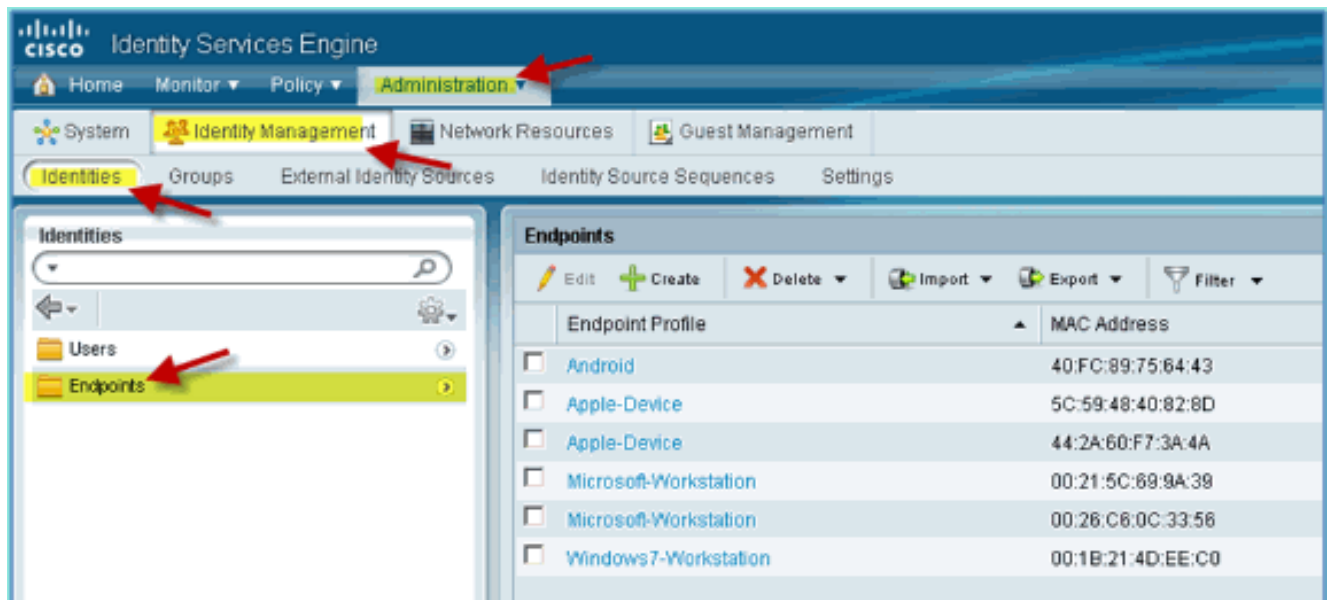
2. Kies ISE. Klik op ISE-host bewerken.



3. Selecteer op de pagina Knooppunt bewerken de profielconfiguratie en configureer de volgende instellingen: DHCP: Ingeschakeld, Alle (of standaard) DHCP-SPAN: ingeschakeld, alles (of standaard) HTTP: ingeschakeld, alles (of standaard) RADIUS: ingeschakeld, n.v.t. DNS: ingeschakeld, N/A



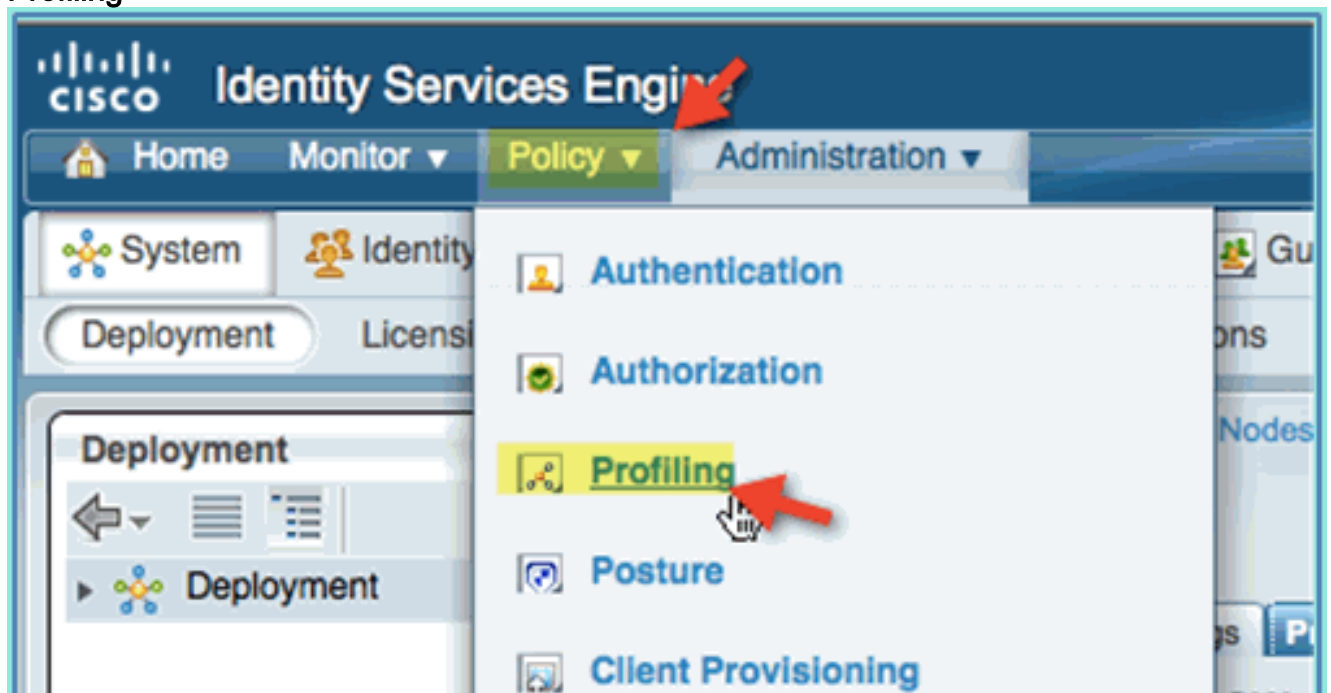
4. Herassocieer de apparaten (iPhone/iPads/Droids/Mac, etc.).
5. Bevestig de ISE-endpointidentiteiten. Ga naar **Administratie > Identiteitsbeheer > Identiteiten**. Klik op Endpoints om aan te geven wat er is geprofileerd. **Opmerking**: De eerste profilering is van RADIUS-probes.



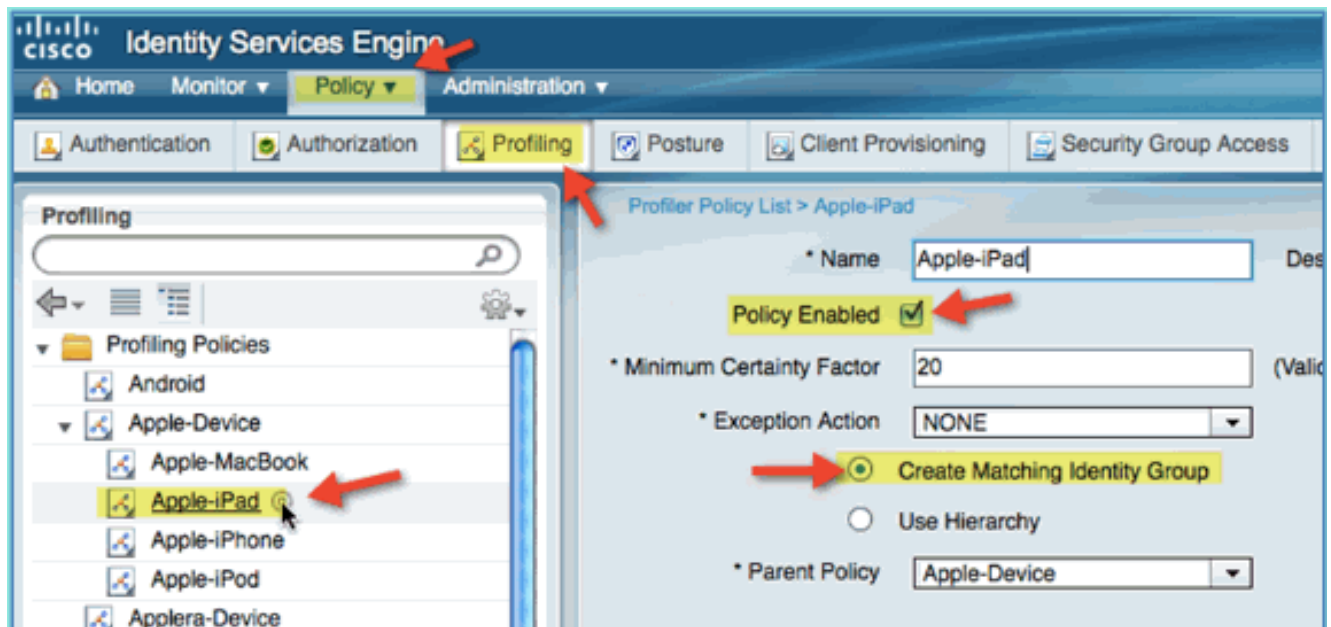
ISE-profielbeleid voor apparaten inschakelen

Vanuit het vak biedt ISE een bibliotheek met verschillende endpointprofielen. Voltooi deze stappen om profielen voor apparaten in te schakelen:

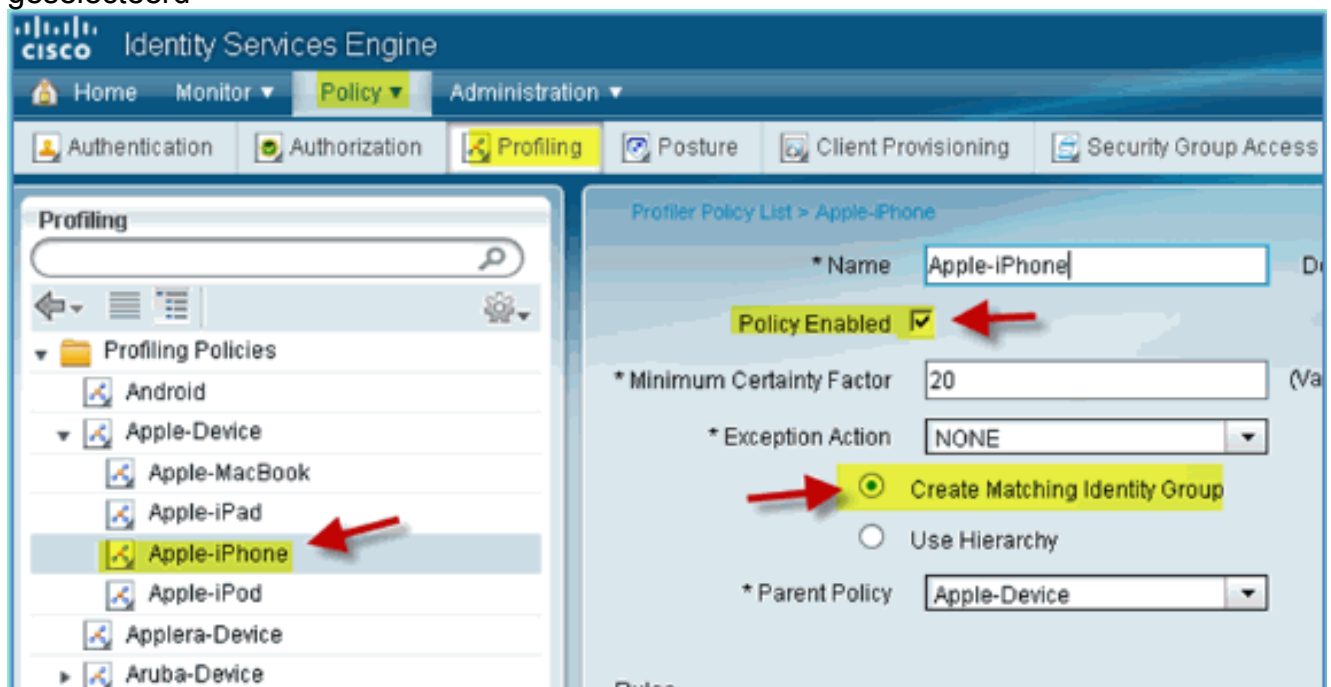
1. Ga van ISE naar **Policy > Profiling**.



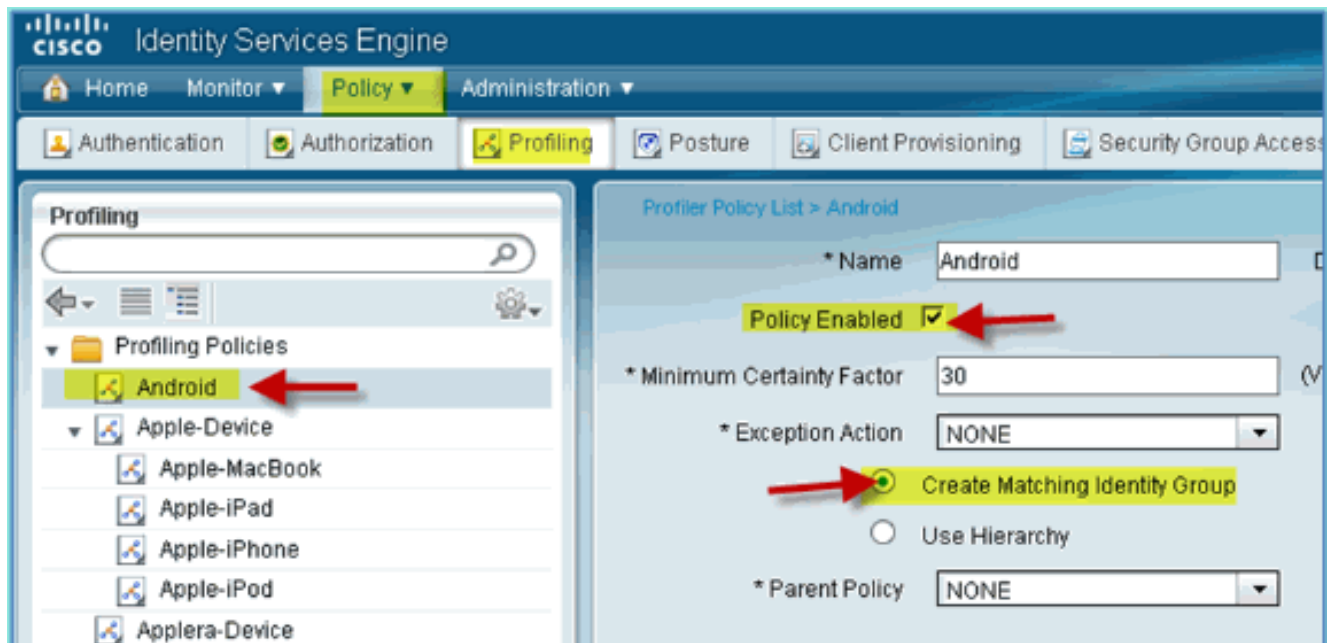
2. Vouw vanuit het linker deelvenster het **profielbeleid uit**.
3. Klik op **Apple Device > Apple iPad** en stel het volgende in: Toegelaten beleid: Ingeschakeld
Overeenkomende identiteitsgroep maken: geselecteerd



4. Klik op **Apple Device > Apple iPhone**, stel het volgende in: Toegelaten beleid: Ingeschakeld
Overeenkomende identiteitsgroep maken: geselecteerd



5. Klik op **Android** en stel het volgende in: Toegelaten beleid: Ingeschakeld
Overeenkomende identiteitsgroep maken: geselecteerd



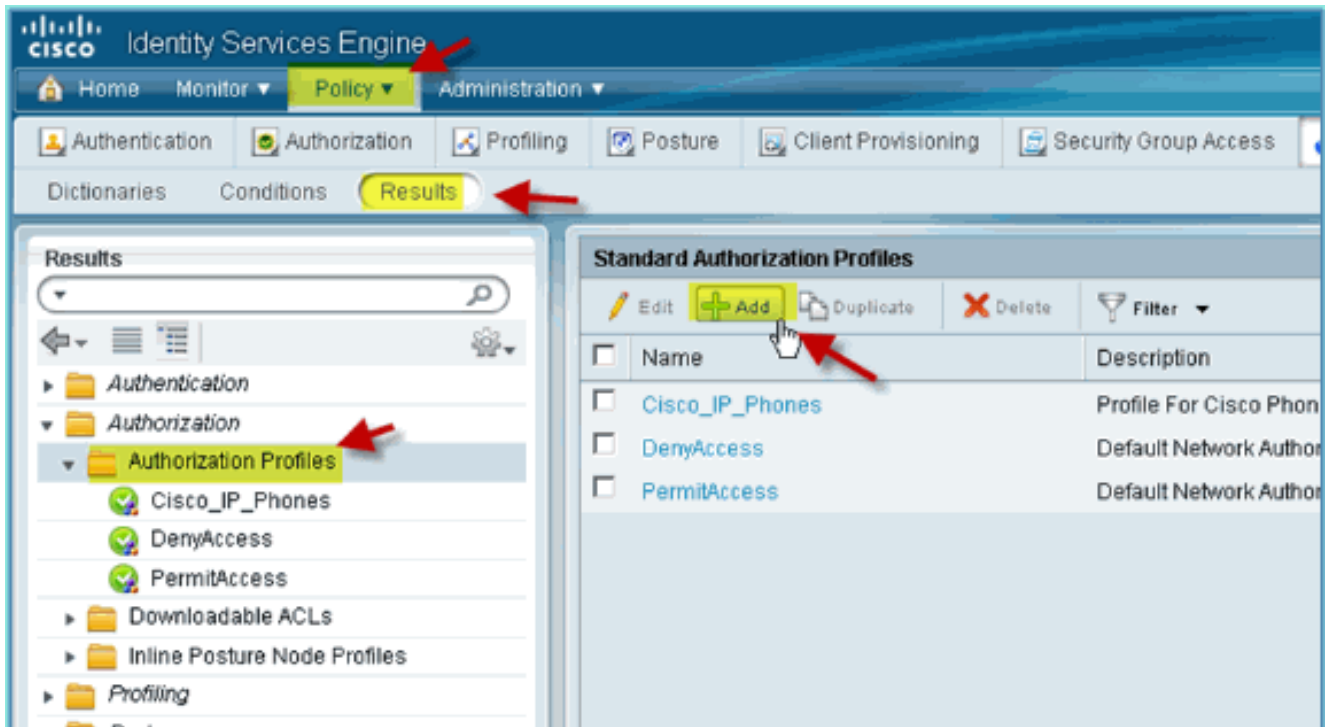
[ISE-autorisatieprofiel voor Posture Discovery Redirect](#)

Voltooi deze stappen om een postuur van het vergunningsbeleid te vormen toelaat nieuwe apparaten om aan ISE voor juiste ontdekking en het profileren worden opnieuw gericht:

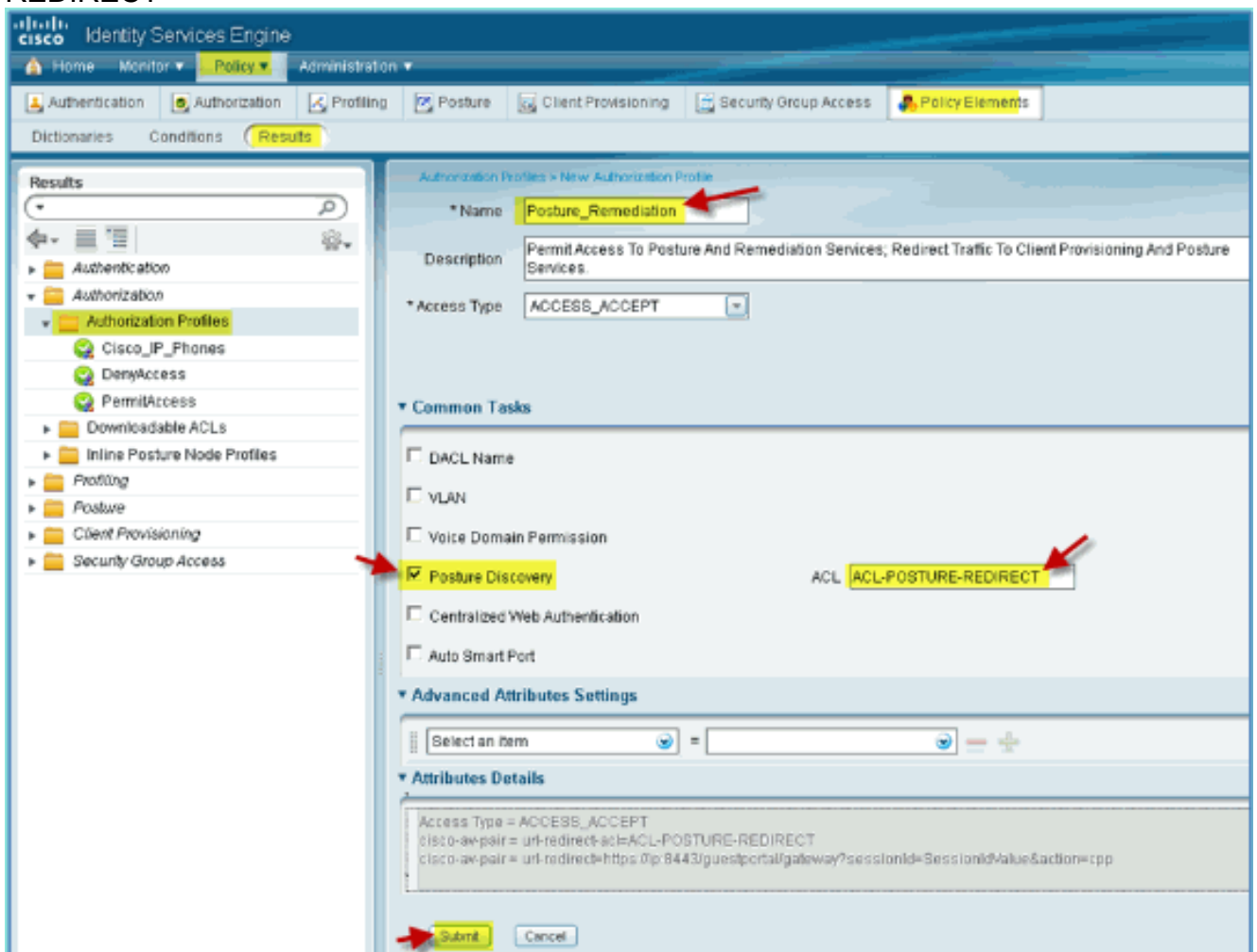
1. Ga van ISE naar **Policy > Policy Elements > Results**.



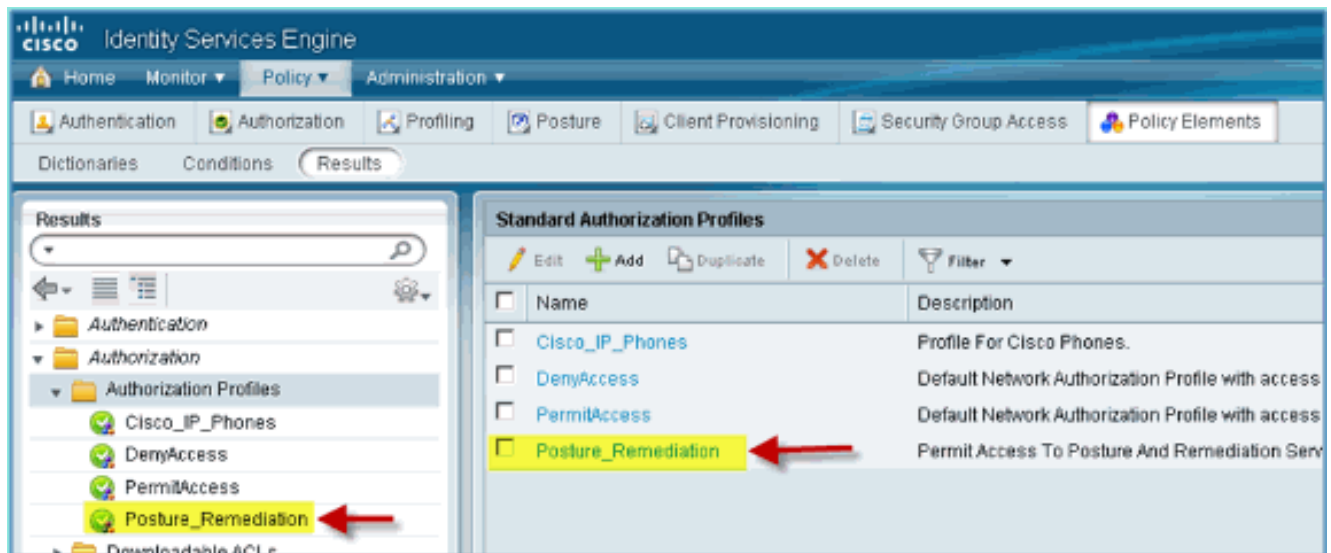
2. Vergunning uitvouwen. Klik op **Autorisatieprofielen** (linkerdeelvenster) en klik op **Toevoegen**.



- Maak het autorisatieprofiel aan met de volgende opties: Naam: Posture_Remediation Toegangstype: Access_Accept Gemeenschappelijke tools: Detectie van houding, ingeschakeld Detectie van houding, ACL-POSTURE-REDIRECT



- Klik op **Indienen** om deze taak te voltooien.
- Bevestig dat het nieuwe autorisatieprofiel wordt toegevoegd.

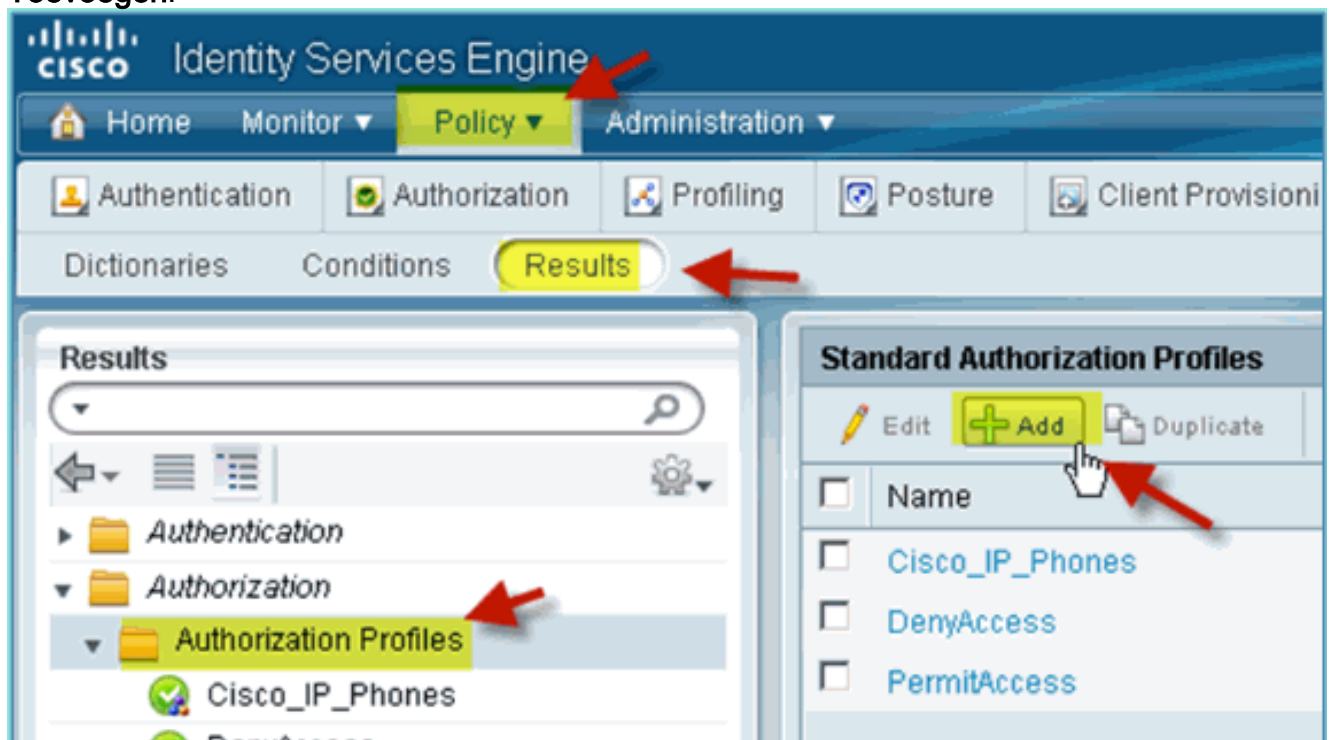


ISE-autorisatieprofiel voor werknemers maken

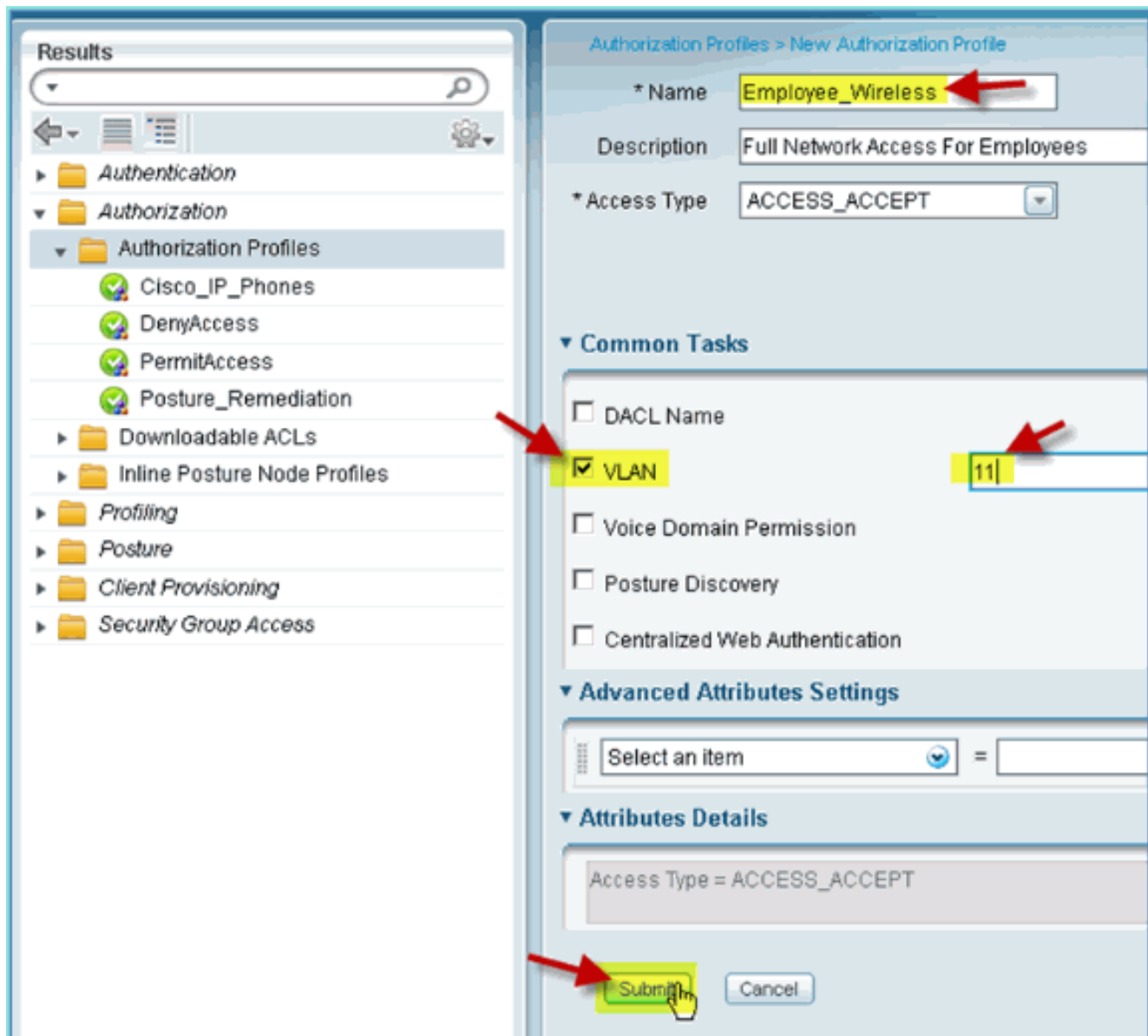
Door een autorisatieprofiel voor een werknemer toe te voegen, kan ISE toegang toestaan en autoriseren met de toegewezen kenmerken. Werknemer VLAN 11 is in dit geval toegewezen.

Voer de volgende stappen uit:

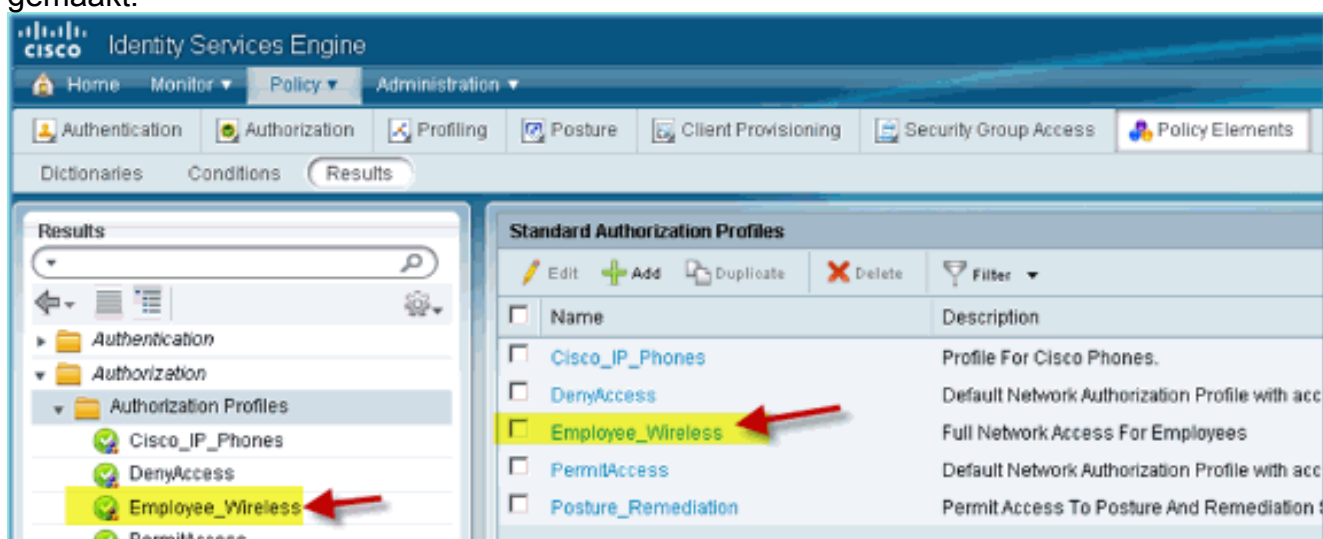
1. Ga van ISE naar **Policy > Results**. Breid **Autorisatie** uit, klik vervolgens op **Autorisatieprofielen** en klik op **Toevoegen**.



2. Voer het volgende in voor een profiel voor werknemersautorisatie: Naam: Werknemer_DraadloosGemeenschappelijke taken:VLAN, ingeschakeldVLAN, subwaarde 11
3. Klik op **Indienen** om deze taak te voltooien.



4. Bevestig dat het nieuwe profiel voor de werknemersautorisatie is gemaakt.

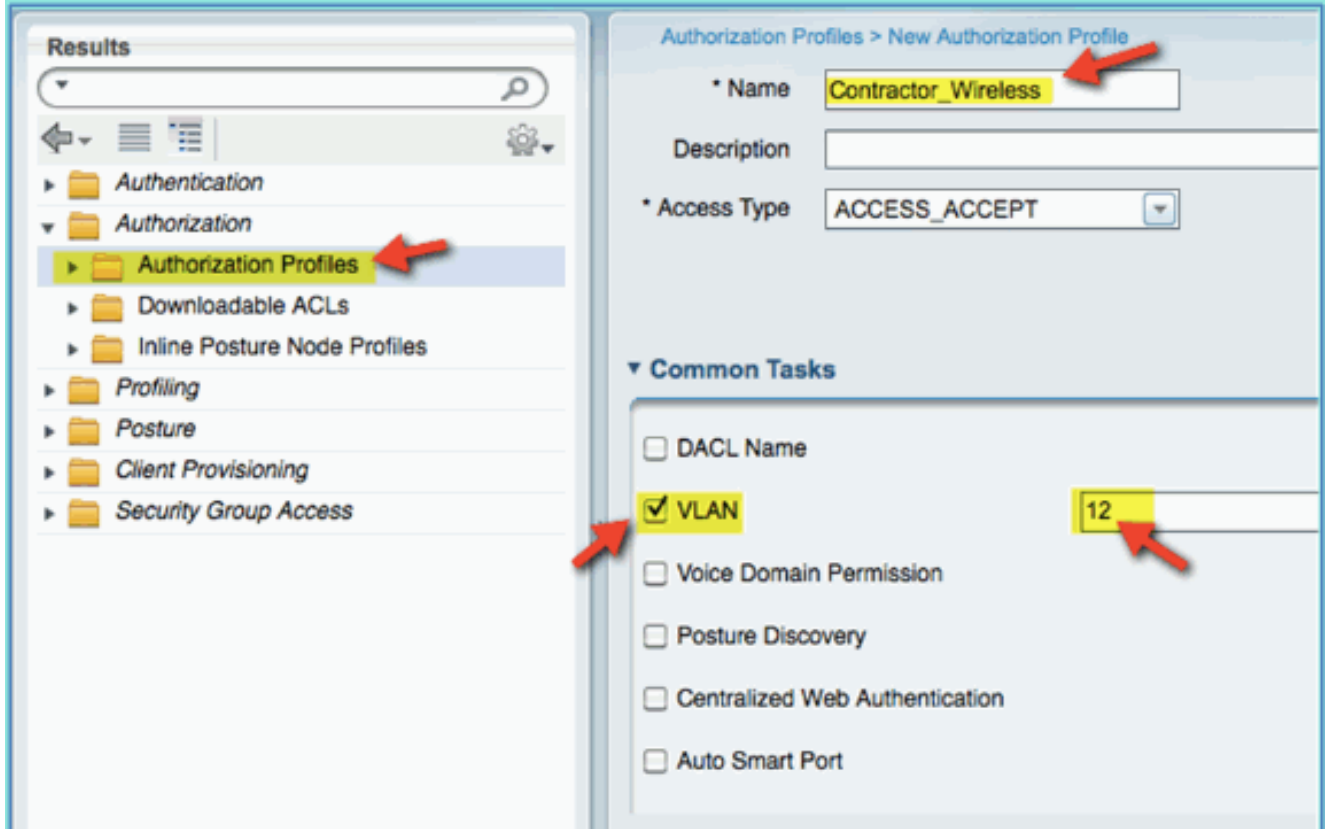


ISE-autorisatieprofiel voor contractant maken

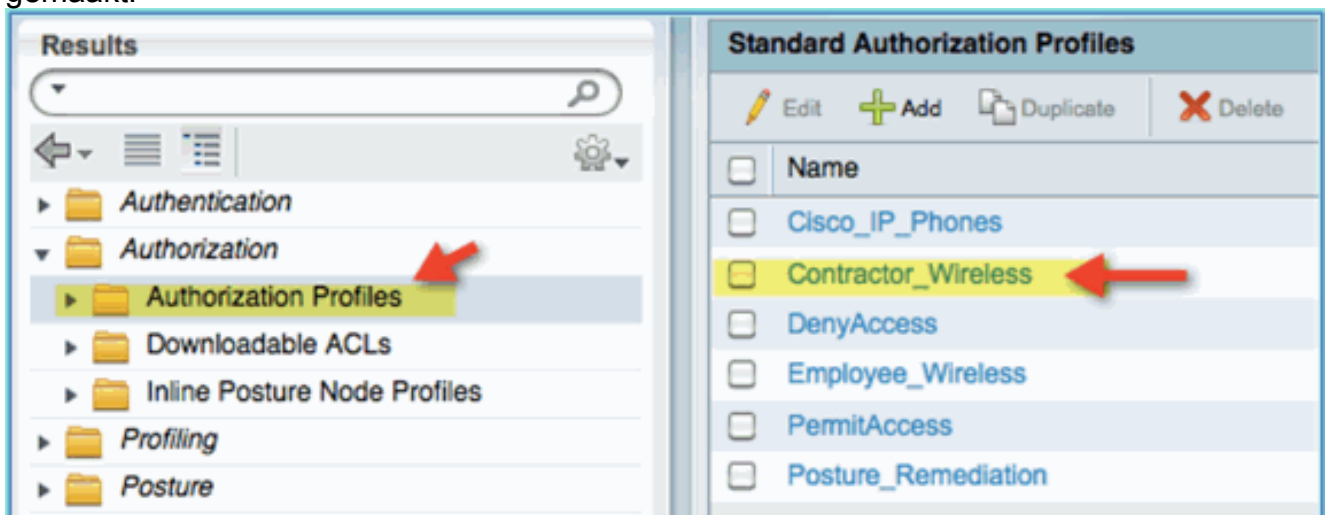
Door een autorisatieprofiel voor een contractant toe te voegen, kan ISE toegang toestaan en toestaan met de toegewezen attributen. Contractor VLAN 12 wordt in dit geval toegewezen.

Voer de volgende stappen uit:

1. Ga van ISE naar **Policy > Results**. Breid **Autorisatie** uit, klik vervolgens op **Autorisatieprofielen** en klik op **Toevoegen**.
2. Voer het volgende in voor een profiel voor werknemersautorisatie: Naam: **Werknemer_DraadloosGemeenschappelijke taken:VLAN**, ingeschakeld **VLAN**, subwaarde **12**



3. Klik op **Indienen** om deze taak te voltooien.
4. Bevestig dat het profiel voor de machtiging van de contractant is gemaakt.



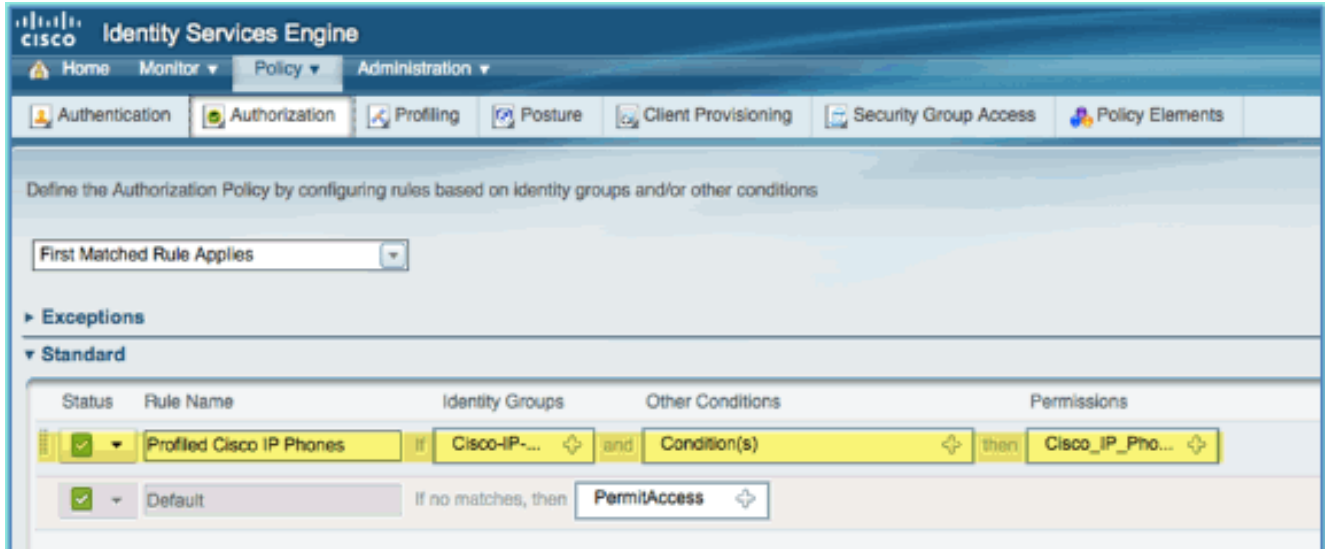
[Autorisatiebeleid voor apparaatpositie/profielen](#)

Er is weinig informatie bekend over een nieuw apparaat wanneer het voor het eerst op het netwerk komt, een beheerder zal het juiste beleid aanmaken om onbekende eindpunten te kunnen identificeren alvorens toegang toe te staan. In deze oefening zal het vergunningsbeleid worden

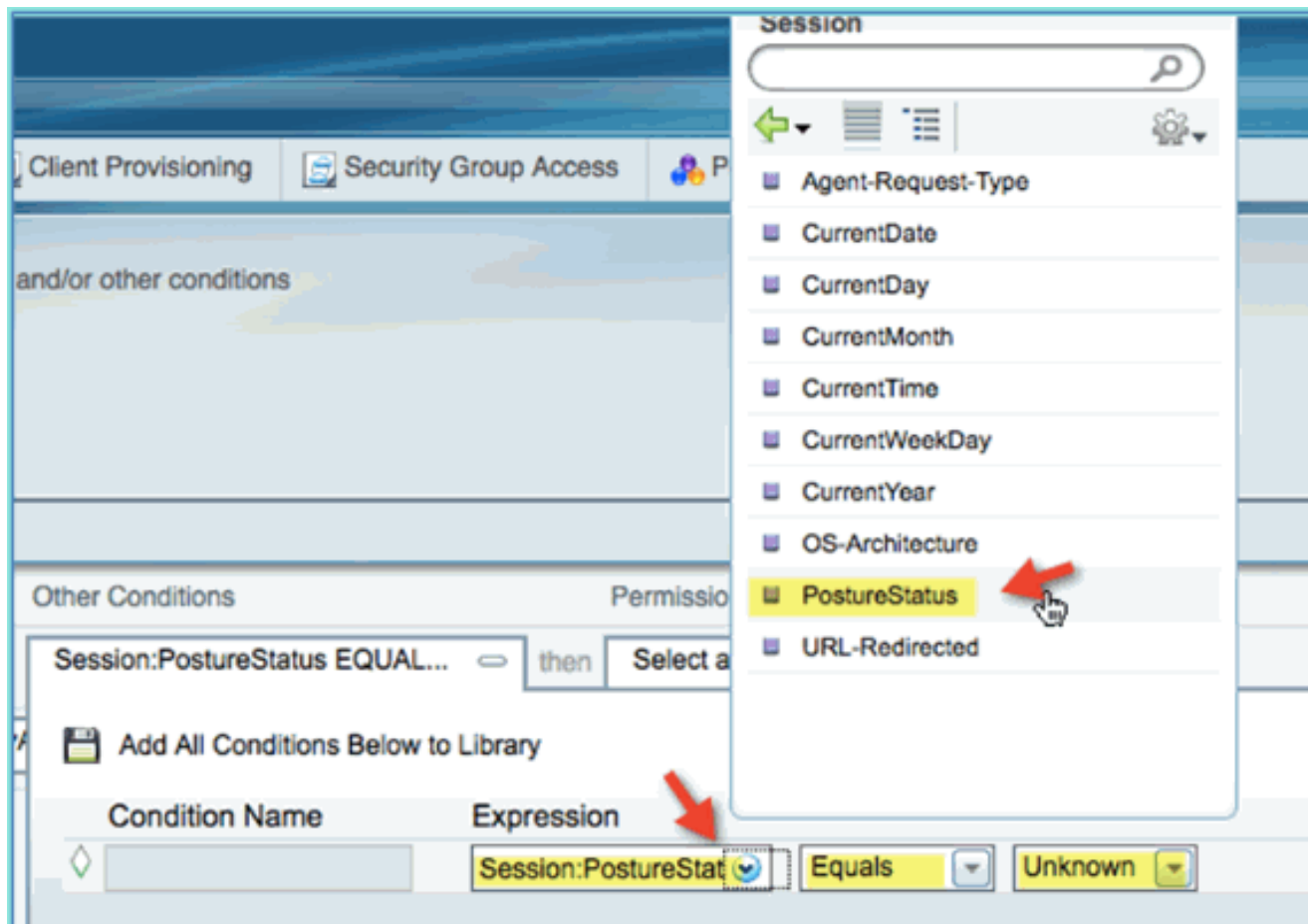
gecreëerd zodat een nieuw apparaat aan ISE voor de beoordeling van de houding zal worden opnieuw gericht (voor mobiele apparaten zijn agentless, daarom is alleen profileren relevant); endpoints zullen aan het ISE captive portaal worden opnieuw gericht en geïdentificeerd.

Voer de volgende stappen uit:

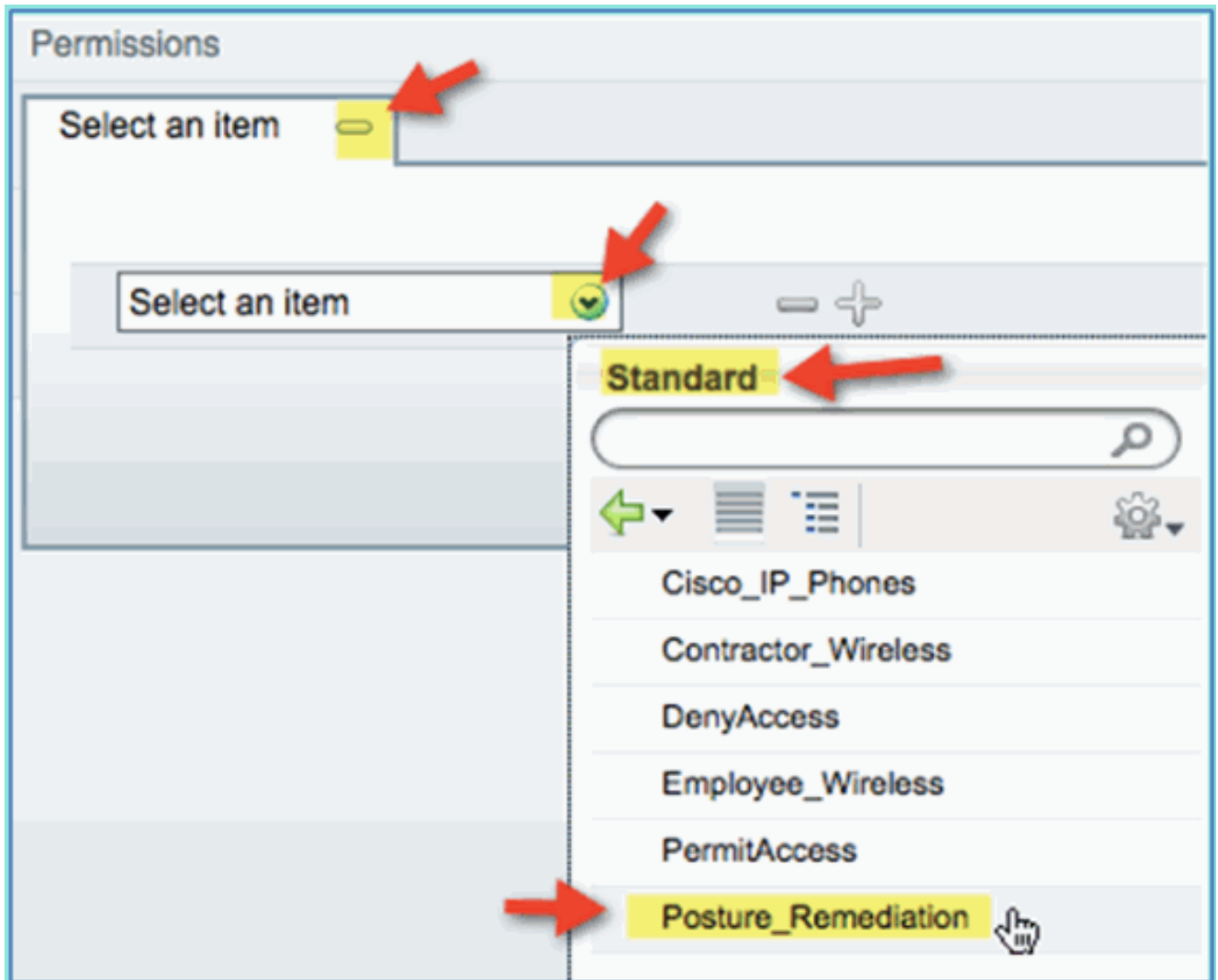
1. Ga van ISE naar **Policy > Authorisation**.



2. Er is een beleid voor geprofileerde Cisco IP-telefoons. Dit is uit de doos. Bewerk dit als een postuur beleid.
3. Voer de volgende waarden voor dit beleid in: Regel Naam: Posture_RemediationIdentiteitsgroepen: alleAndere voorwaarden > Nieuw maken: (geavanceerde) sessie > PostureStatusPositie Status > Gelijk: Onbekend



4. Geef de volgende rechten op: Rechten > Standaard: Posture_Remediation

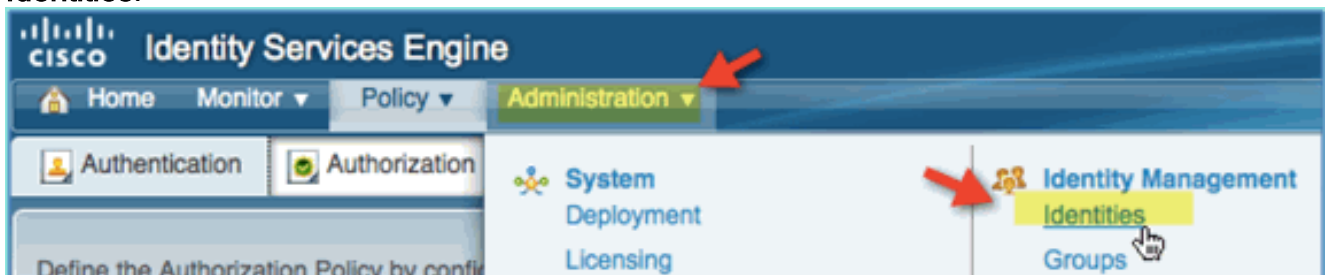


5. Klik op **Save** (Opslaan). **Opmerking:** U kunt ook aangepaste beleidselementen maken om gebruiksgemak toe te voegen.

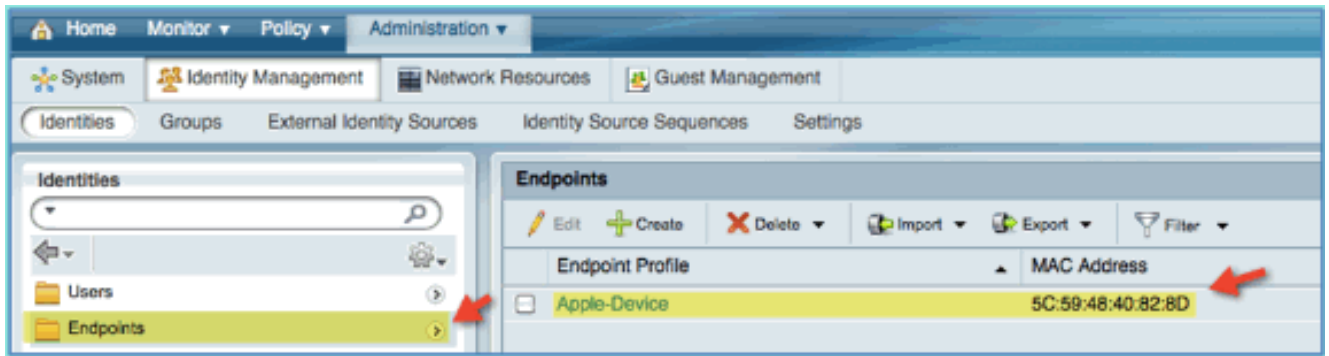
[Beleid voor herstel van houding testen](#)

Om eenvoudig te demonstreren kan worden uitgevoerd om aan te tonen dat ISE een nieuw apparaat correct profileert op basis van het postuur beleid.

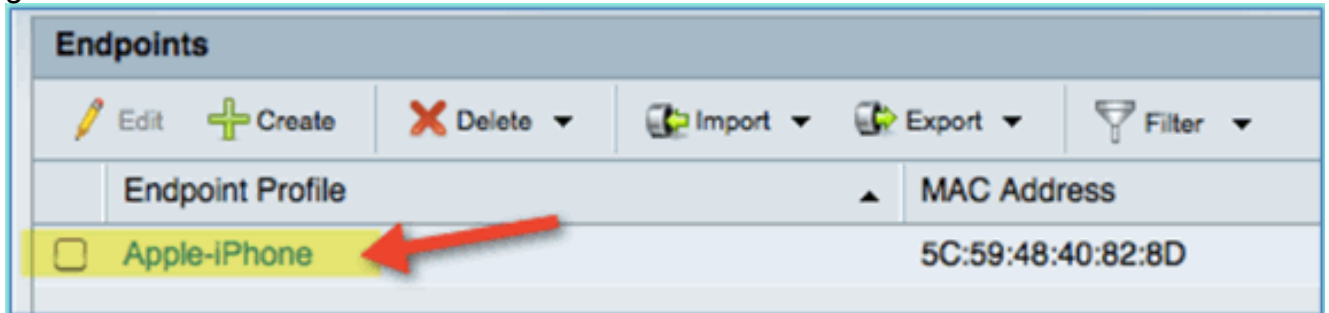
1. Ga van ISE naar **Administration > Identity Management > Identity Identities**.



2. Klik op **Endpoints**. Koppel een apparaat aan en sluit het aan (in dit voorbeeld een iPhone).



3. Verfris de lijst Endpoints. Neem in acht welke informatie wordt gegeven.
4. Blader van het eindpuntapparaat naar:URL: http://www (of 10.10.10.10)Het apparaat wordt omgeleid. Aanvaard elke prompt voor certificaten.
5. Nadat het mobiele apparaat volledig is omgeleid, van ISE verfris de Endpoints lijst opnieuw. Kijk wat er is veranderd. Het vorige eindpunt (bijvoorbeeld Apple-Device) moet zijn veranderd in 'Apple-iPhone' etc. De reden is dat de HTTP sonde effectief gebruiker-agent informatie verkrijgt, als deel van het proces om aan het gevangen portaal worden opnieuw gericht.

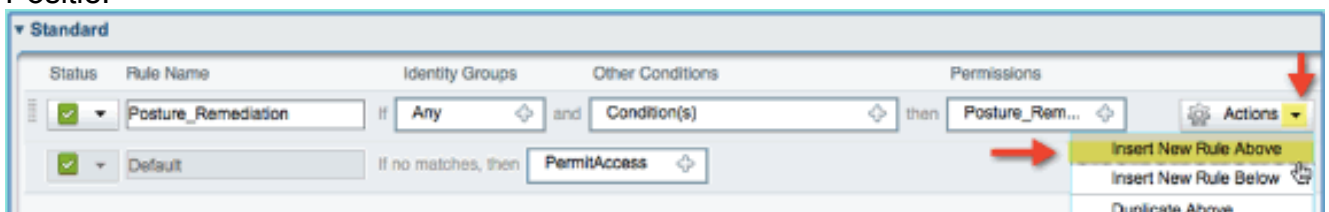


Autorisatiebeleid voor gedifferentieerde toegang

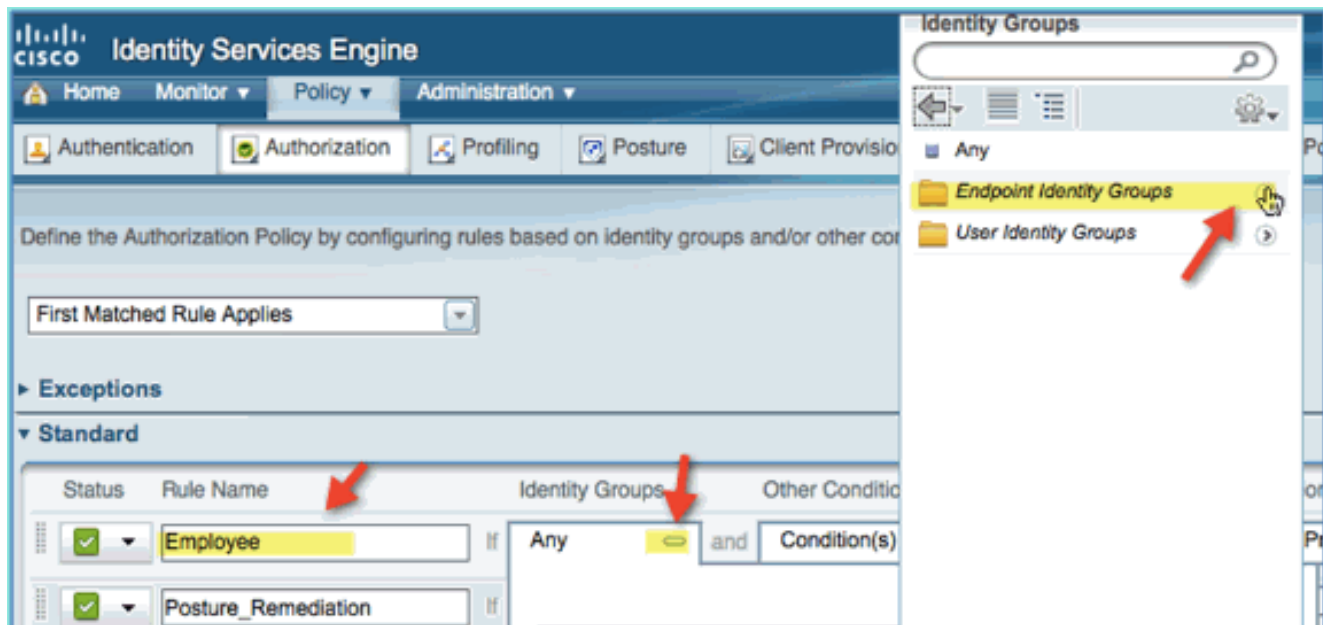
Na met succes het testen van de postuur autorisatie, blijven bouwen beleid om gedifferentieerde toegang voor de werknemer en contractant met bekende apparaten en verschillende VLAN-toewijzing specifiek voor de gebruikersrol (in dit scenario, werknemer en contractant) te ondersteunen.

Voer de volgende stappen uit:

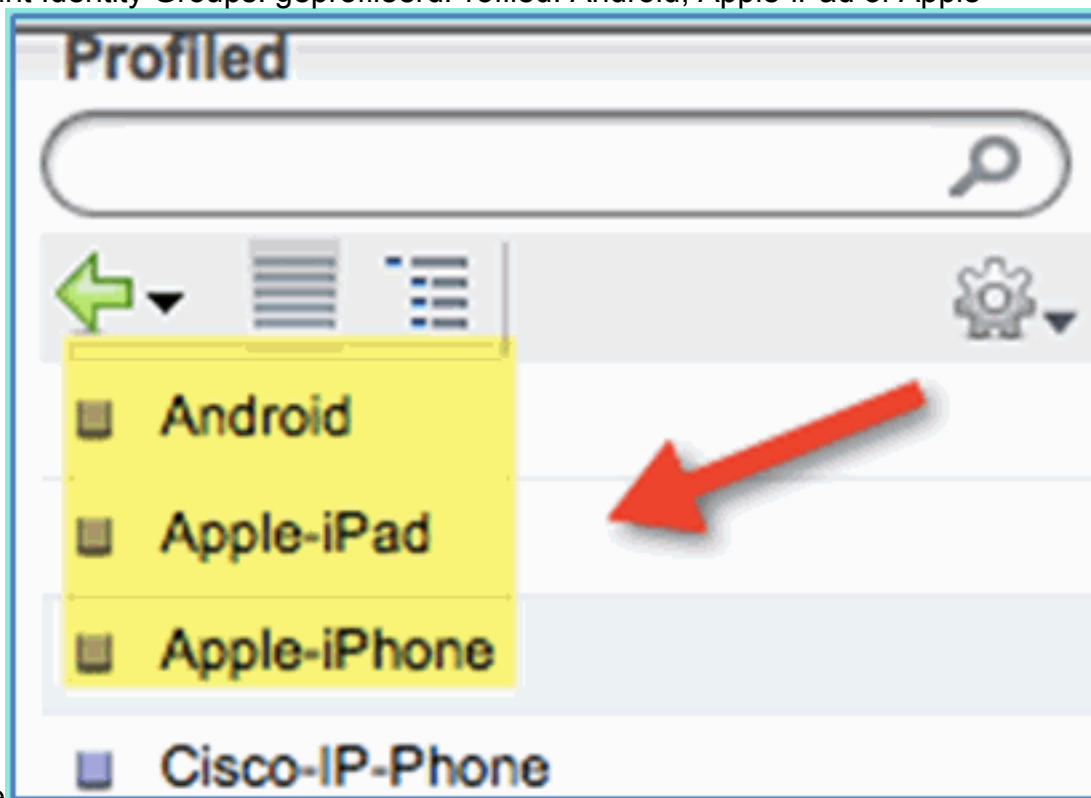
1. Ga naar **ISE > Policy > Autorisatie**.
2. Voeg/voeg een nieuwe regel toe boven het beleid/de lijn van de Oplossing van de Positie.



3. Voer de volgende waarden voor dit beleid in:Regel Naam: WerknemerIdentiteitsgroepen (uitvouwen): Endpoint Identity Groups

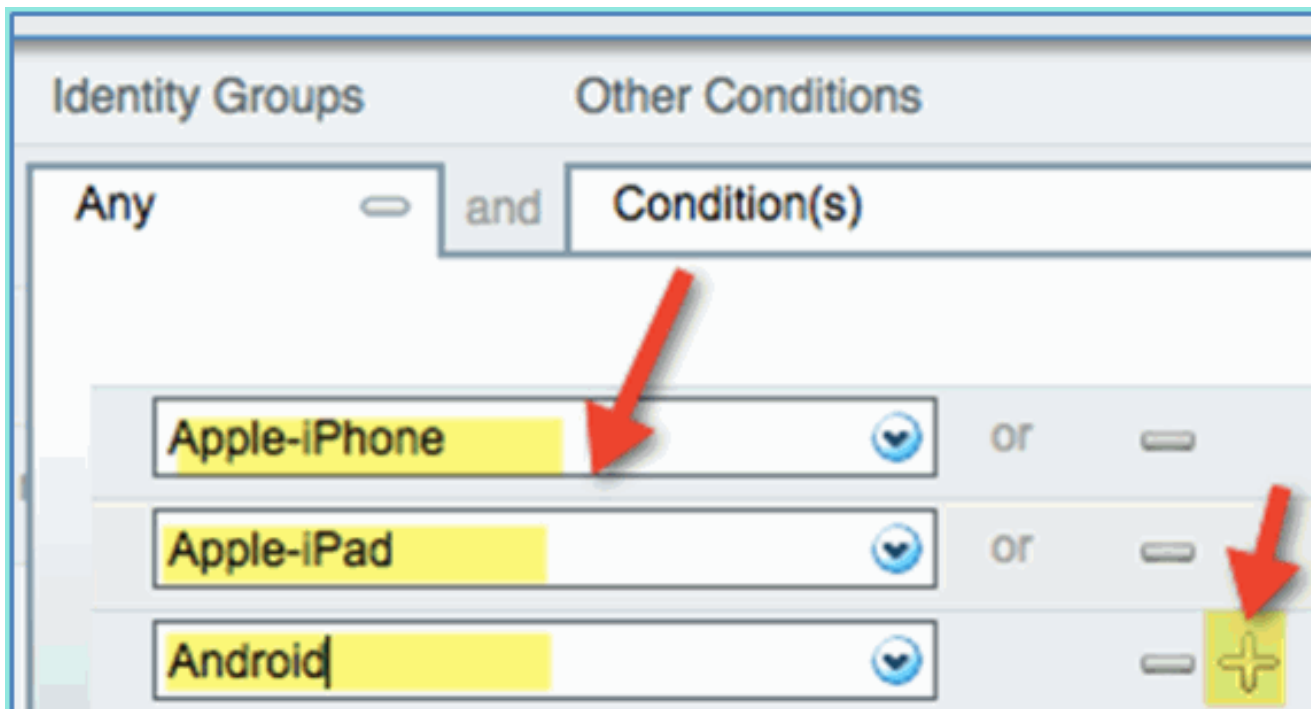


Endpoint Identity Groups: geprofileerdProfiled: Android, Apple-iPad of Apple-

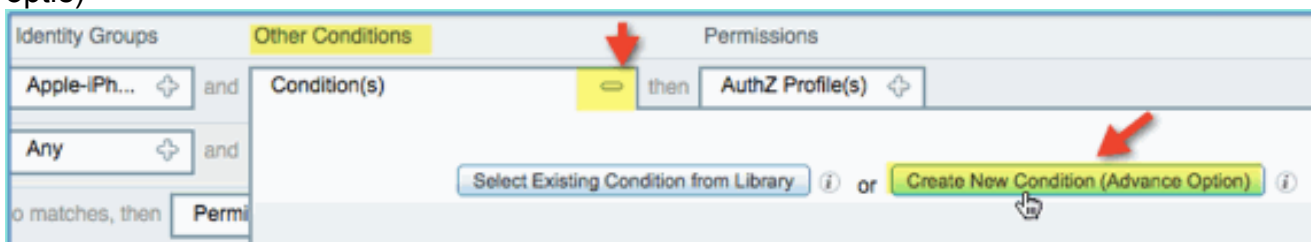


iPhone

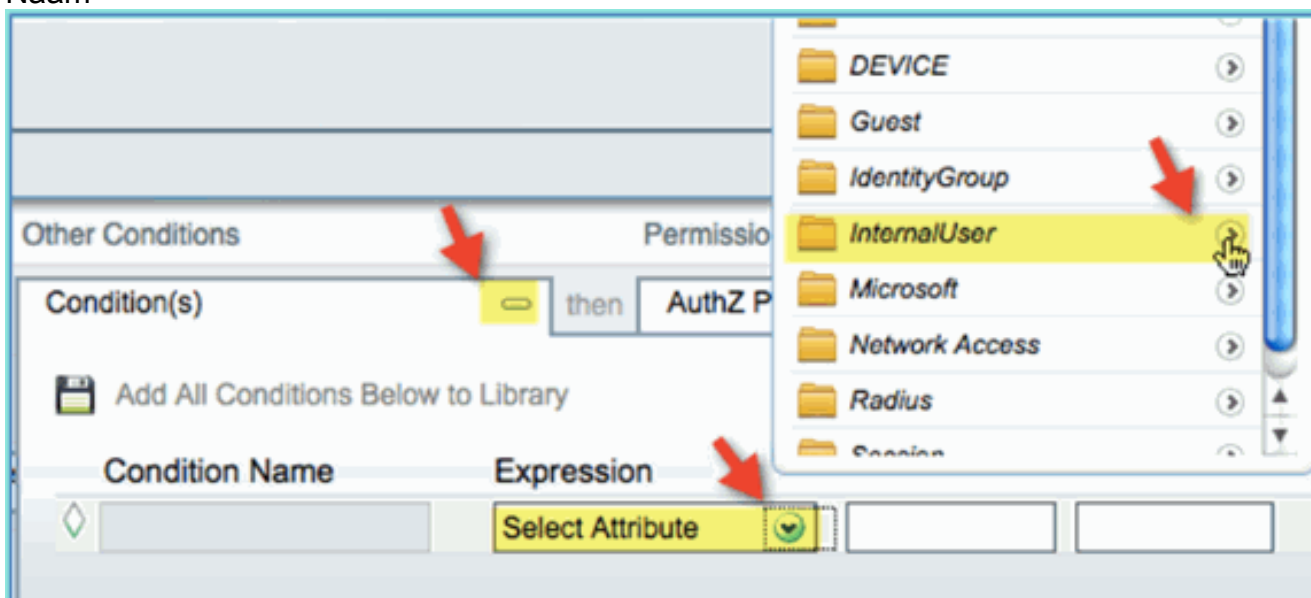
4. Als u extra apparaattypen wilt opgeven, klikt u op de +-toets en voegt u meer apparaten toe (indien nodig): Endpoint Identity Groups: geprofileerdProfiled: Android, Apple-iPad of Apple-iPhone



5. Specificeer de volgende waarden voor toegangsrechten voor dit beleid: Andere voorwaarden (uitbreiden): Nieuwe voorwaarde maken (geavanceerde optie)



Voorwaarde > Expressie (van lijst): Interne Gebruiker > Naam



Interne Gebruiker > Naam:
medewerker

Other Conditions Permissions

Select Attribute then AuthZ Profile(s)

Add All Conditions Below to Library

Condition Name Expression

InternalUser:Name Equals employee

6. Voeg een voorwaarde toe voor posture sessie Voldoet:Rechten > Profielen > Standaard: Werknemer_Draadloos

Permissions

AuthZ Profile(s)

Select an item

Standard

Cisco_IP_Phones

Contractor_Wireless

DenyAccess

Employee_Wireless

PermitAccess

Posture_Remediation

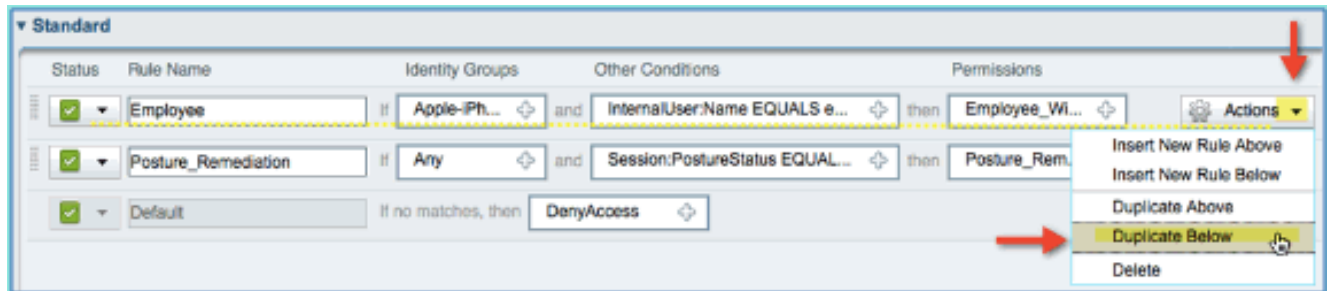
7. Klik op **Save** (Opslaan). Bevestig dat het beleid goed is toegevoegd.

▼ Standard

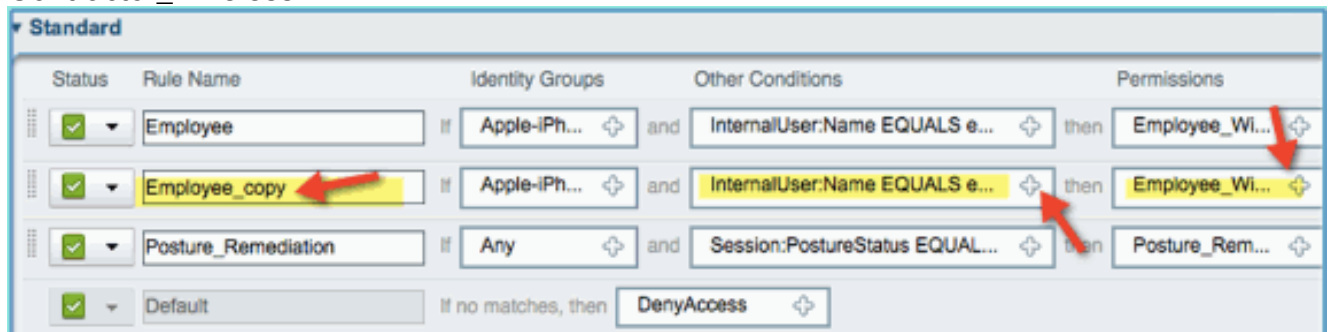
Status	Rule Name	Identity Groups	Other Conditions	Permissions
	Employee	Apple-iPh...	and InternalUser:Name EQUALS e...	then Employee_Wi...
	Posture_Remediation	If Any	and Session:PostureStatus EQUAL...	then Posture_Rem...
	Default	If no matches, then	DenyAccess	

8. Doorgaan door het Contractor-beleid toe te voegen. In dit document wordt het vorige beleid gedupliceerd om het proces te versnellen (of, u kunt handmatig configureren voor goede

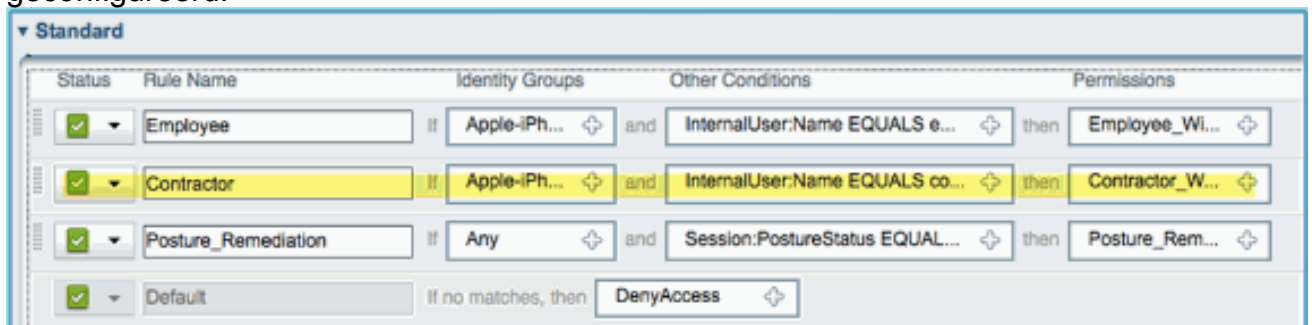
praktijken).Klik vanuit het werknemersbeleid > Handelingen op **Dupliceren** hieronder.



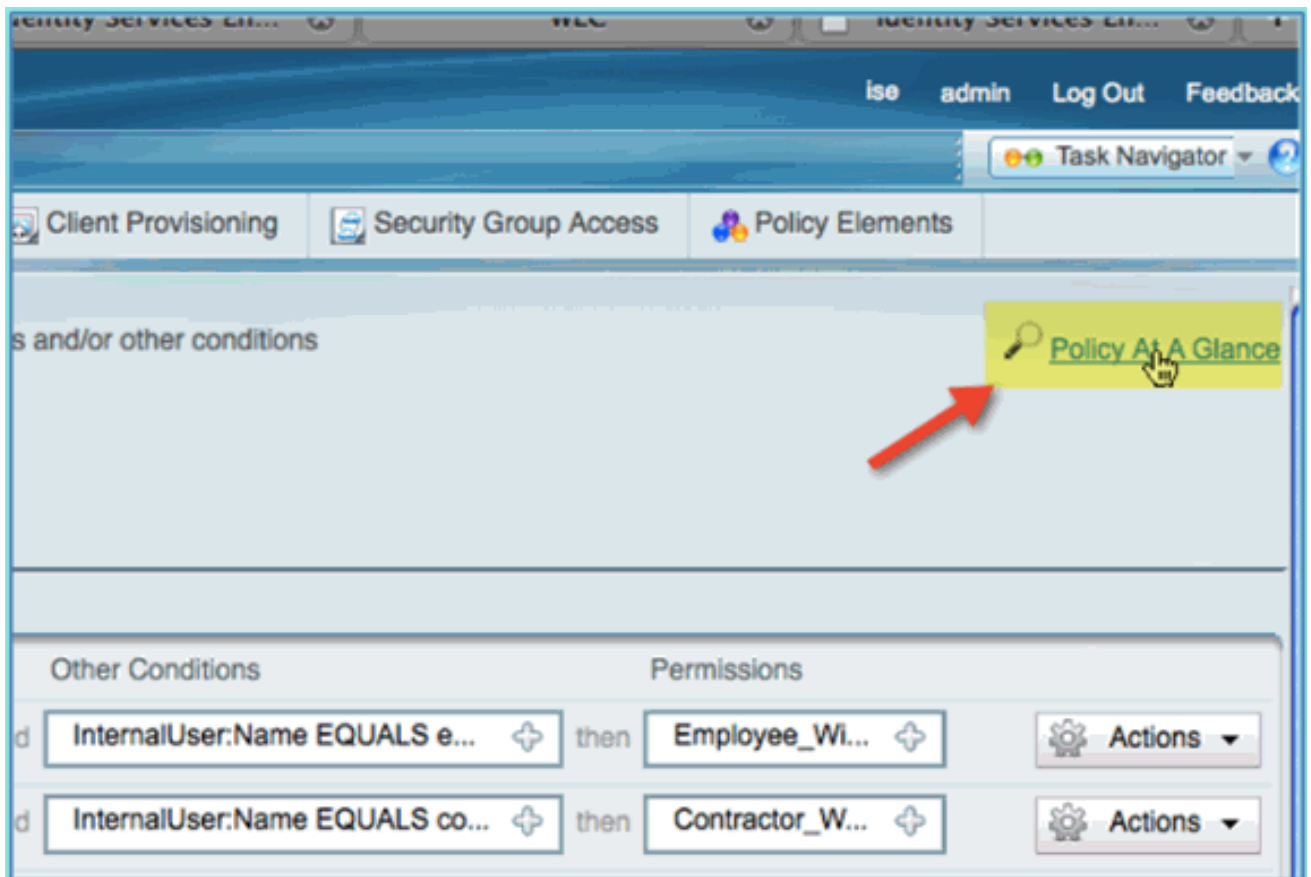
9. Bewerk de volgende velden voor dit beleid (kopie dupliceren):Regel Naam: AannemerAndere voorwaarden > Interne Gebruiker > Naam: contractantRechten: Contractor_Wireless



10. Klik op **Save** (Opslaan). Bevestig dat de vorige geduplicateerde kopie (of het nieuwe beleid) goed is geconfigureerd.



11. Klik op **Beleid** in één oogopslag om een voorbeeld van het beleid te bekijken.



Policy at A Glance-weergave biedt een geconsolideerde samenvatting en gemakkelijk te zien beleid.

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No rules available	
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
<input checked="" type="checkbox"/> Enabled	Employee	Android OR Apple-iPad OR Apple- iPhone	InternalUser.Name EQUALS employee	Employee_Wireless
<input checked="" type="checkbox"/> Enabled	Contractor	Android OR Apple-iPad OR Apple- iPhone	InternalUser.Name EQUALS contractor	Contractor_Wireless
<input checked="" type="checkbox"/> Enabled	Posture_Remediation	Any	Session.PostureStatus EQUALS Unknown	Posture_Remediation
<input checked="" type="checkbox"/> Enabled	Default	Any		DenyAccess

CoA testen voor gedifferentieerde toegang

Nu de machtigingsprofielen en het beleid zijn voorbereid op het differentiëren van de toegang, is het tijd om te testen. Met één beveiligd WLAN wordt een werknemer toegewezen aan de werknemer VLAN en een contractor wordt toegewezen aan de contractor VLAN. Een Apple iPhone/iPad wordt gebruikt in de volgende voorbeelden.

Voer de volgende stappen uit:

1. Verbind met het beveiligde WLAN (POD1x) met het mobiele apparaat en gebruik deze referenties: Gebruikersnaam: medewerker Wachtwoord: XXXXX



2. Klik op **Samenvoegen**. Bevestig dat de werknemer VLAN 11 (medewerker VLAN) krijgt toegewezen.



3. Klik op Dit netwerk vergeten. Bevestig door op Vergeten te



klikken.

4. Ga naar WLC en verwijder bestaande client verbindingen (als hetzelfde werd gebruikt in vorige stappen). Navigeer naar **Monitor > Clients > MAC-adres** en klik vervolgens op **Verwijderen**.

Monitor

Clients 

Summary

Current Filter

▶ Access Points

▶ Cisco CleanAir

▶ Statistics

▶ CDP

▶ Rogues

Clients 


Multicast

Client MAC Addr

[44:2a:60:f7:3a:4a](#)

[5c:59:48:40:82:8d](#)


Status	Auth	Port	WGB
--------	------	------	-----

Associated	Yes	1	No 
------------	-----	---	---

Associated	No	1	
------------	----	---	--

LinkTest

Disable

Remove 

802.11aTSM

802.11b/gTSM



5. Een andere veilige manier om vorige clientsessies te wissen is door het WLAN uit te schakelen/in te schakelen. Ga naar **WLC > WLAN's > WLAN** en klik vervolgens op het WLAN om te bewerken. Schakel **Ingeschakeld > Toepassen** (uitschakelen) uit. Schakel het selectievakje **Ingeschakeld > Toepassen** (opnieuw inschakelen) in.



6. Ga terug naar het mobiele apparaat. Sluit opnieuw aan op hetzelfde WLAN met deze referenties: Gebruikersnaam: aannemer Wachtwoord:

Enter the password for "pod1x"

Cancel **Enter Password**

Username contractor ←

Password ●●●●●●●● | ←

Mode Automatic >

1 2 3 4 5 6 7 8 9 0

XXXX

7. Klik op **Samenvoegen**. Bevestig dat de contractorgebruiker VLAN 12 (Contractor/guest VLAN) krijgt toegewezen.



8. U kunt de real-time logweergave van ISE bekijken in **ISE > Monitor > Autorisaties**. U moet zien dat individuele gebruikers (werknemer, contractant) gedifferentieerde autorisatieprofielen (Employee_Wireless vs Contractor_Wireless) in verschillende VLAN's krijgen.

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Aug 02,11 03:40:18.331 PM	✓		employee	5C:59:48:40:82:8D		wlc		Employee_Wireless
Aug 02,11 03:36:33.663 PM	✓		contractor	5C:59:48:40:82:8D		wlc		Contractor_Wireless

WLC Guest WLAN

Voltooi deze stappen om een gast WLAN toe te voegen om gasten toegang te geven tot het ISE

Sponsor Guest Portal:

1. Van WLC, navigeer aan **WLANS > WLANS > Voeg nieuw toe**.
2. Voer het volgende in voor de nieuwe gast WLAN:Profielnaam: pod1guestSSID: pod1guest



3. Klik op **Apply** (Toepassen).
4. Voer het volgende in onder het tabblad Gast WLAN > Algemeen:Status: UitgeschakeldInterface/interfacegroep: gast

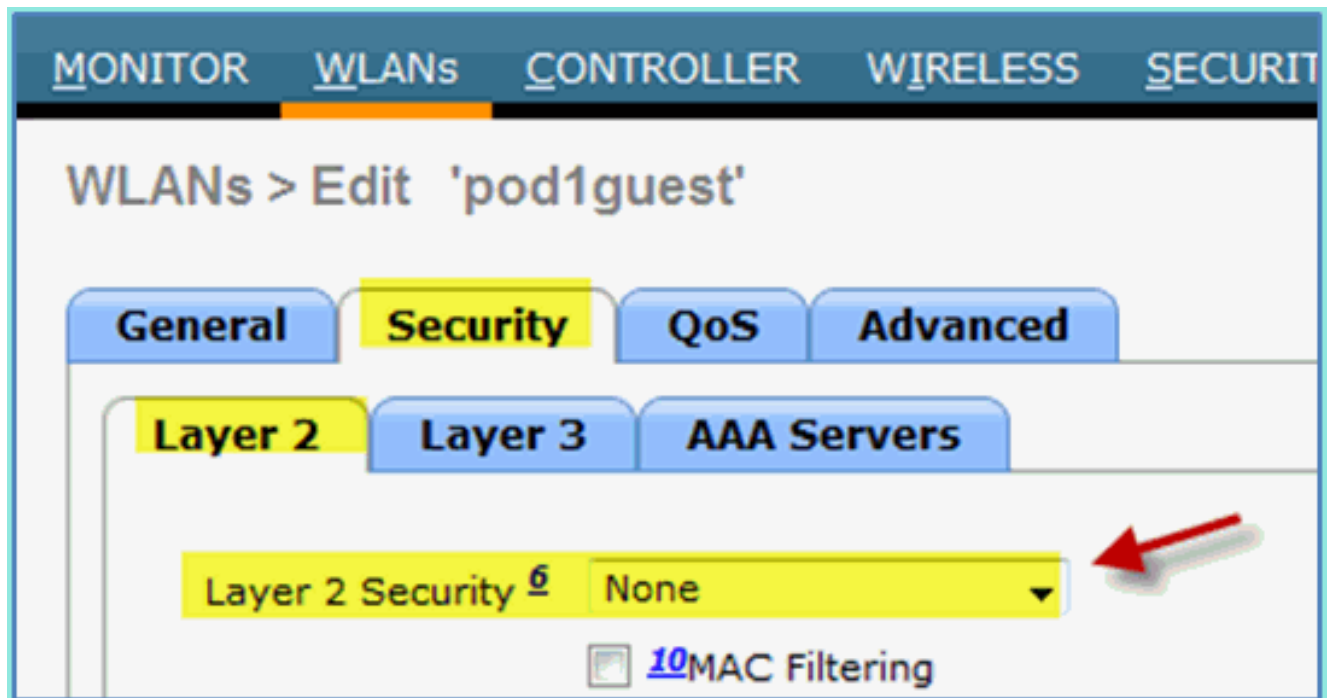
MONITOR **WLANs** CONTROLLER WIRELESS SECUR

WLANs > Edit 'pod1guest'

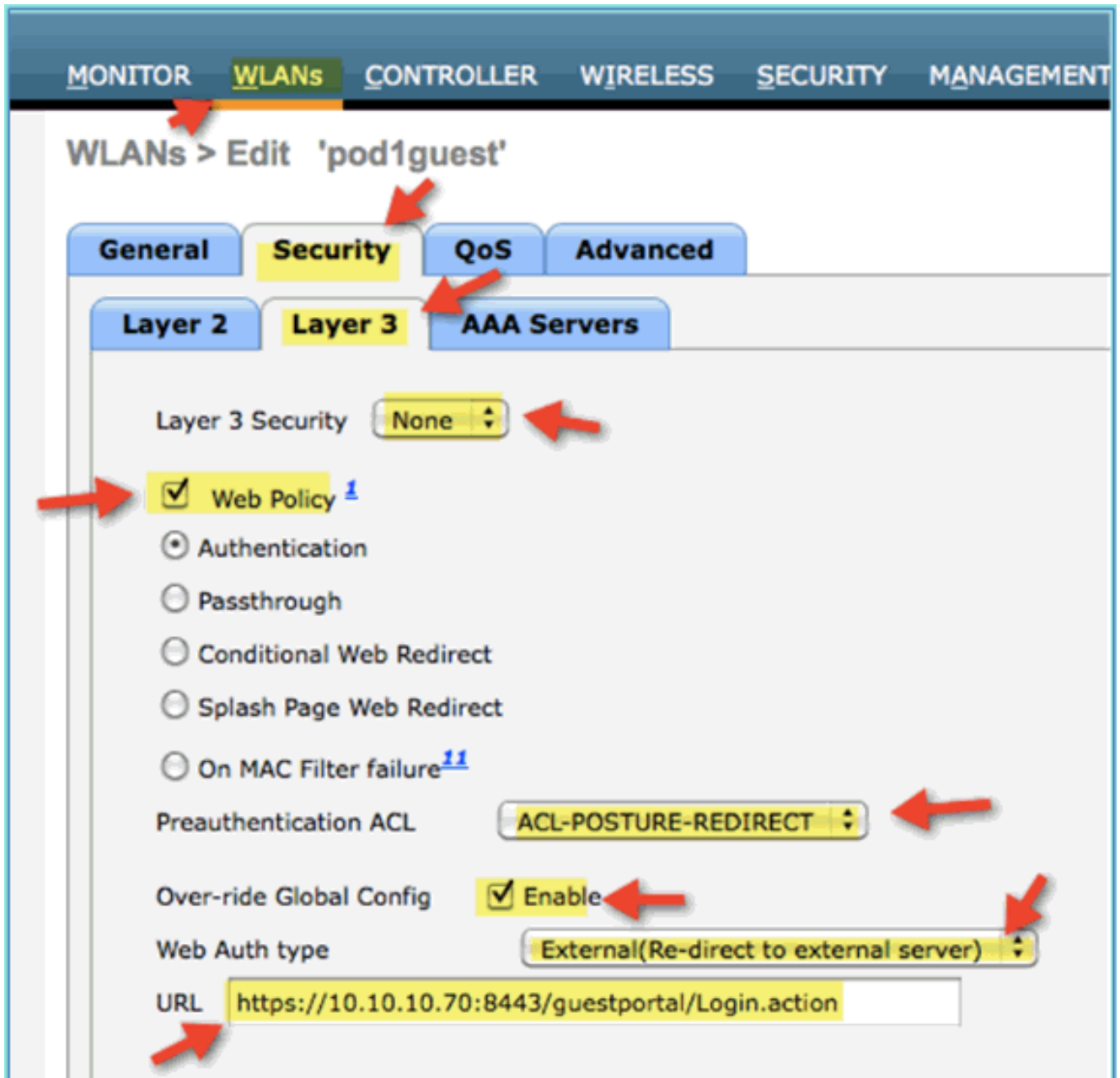
General Security QoS Advanced

Profile Name	pod1guest
Type	WLAN
SSID	pod1guest
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security)
Radio Policy	All
Interface/Interface Group(G)	guest
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. Navigeer naar gast WLAN > Beveiliging > Layer 2 en voer het volgende in: Layer 2 Security: geen



6. Navigeer naar gast WLAN > Security > Layer 3-tabblad en voer het volgende in: Layer 3-beveiliging: geen Webbeleid: ingeschakeld Web Policy subwaarde: Verificatie Verificatie vooraf: ACL-POST-REDIRECT Web Auth type: Extern (omleiden naar externe server) URL: <https://10.10.10.70:8443/guestportal/Login.action>



7. Klik op **Apply** (Toepassen).

8. Zorg ervoor dat u de **WLC-configuratie** opslaat.

Het testen van het WLAN en het gastenportal

U kunt nu de configuratie van de WLAN-gast testen. Het moet de gasten omleiden naar de ISE guest portal.

Voer de volgende stappen uit:

1. Navigeer vanaf een iOS-apparaat, zoals een iPhone, naar **Wi-Fi-netwerken > Inschakelen**. Selecteer vervolgens het POD-



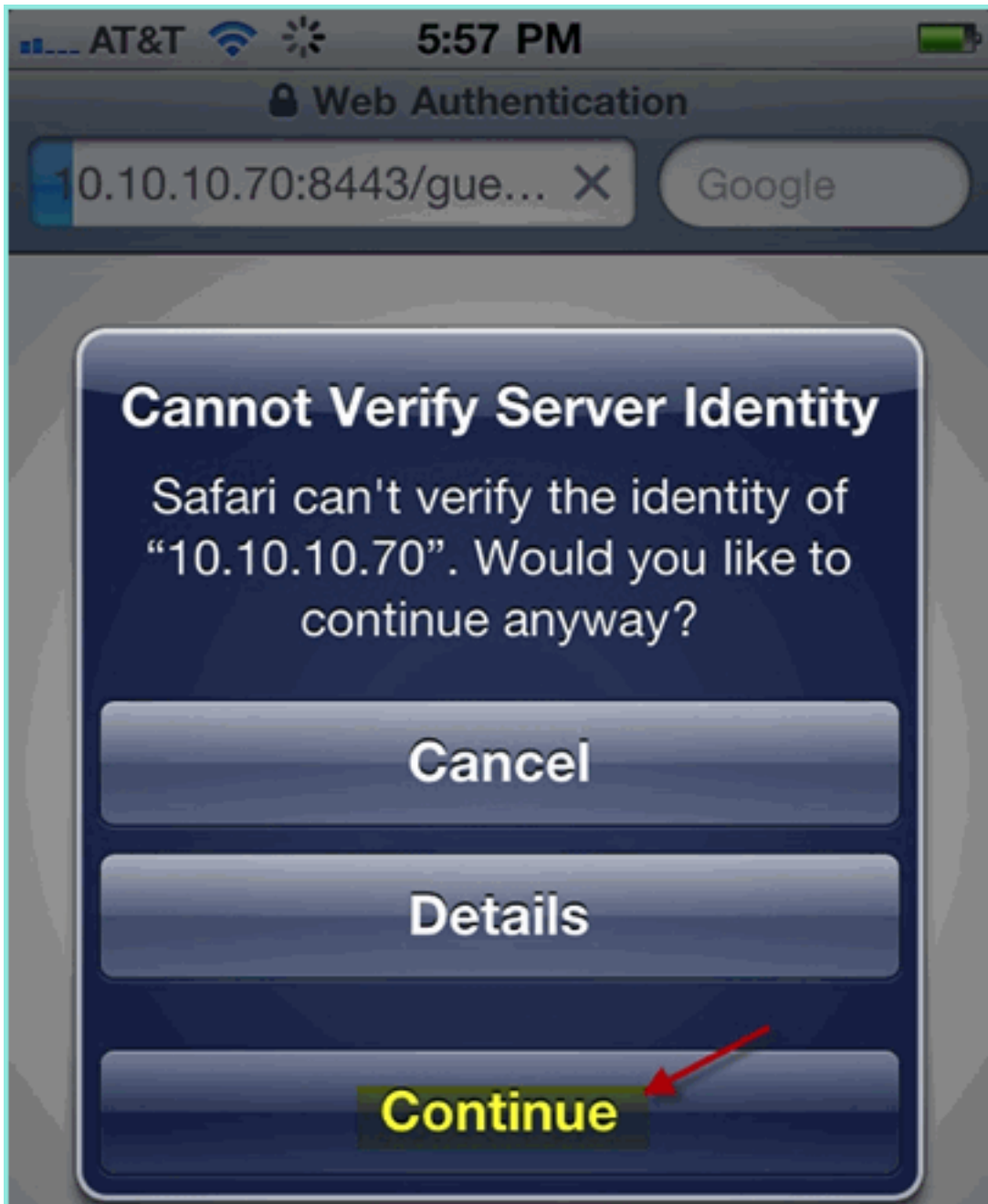
gastennetwerk.

2. Uw iOS-apparaat moet een geldig IP-adres van de gast VLAN (10.10.12.0/24)

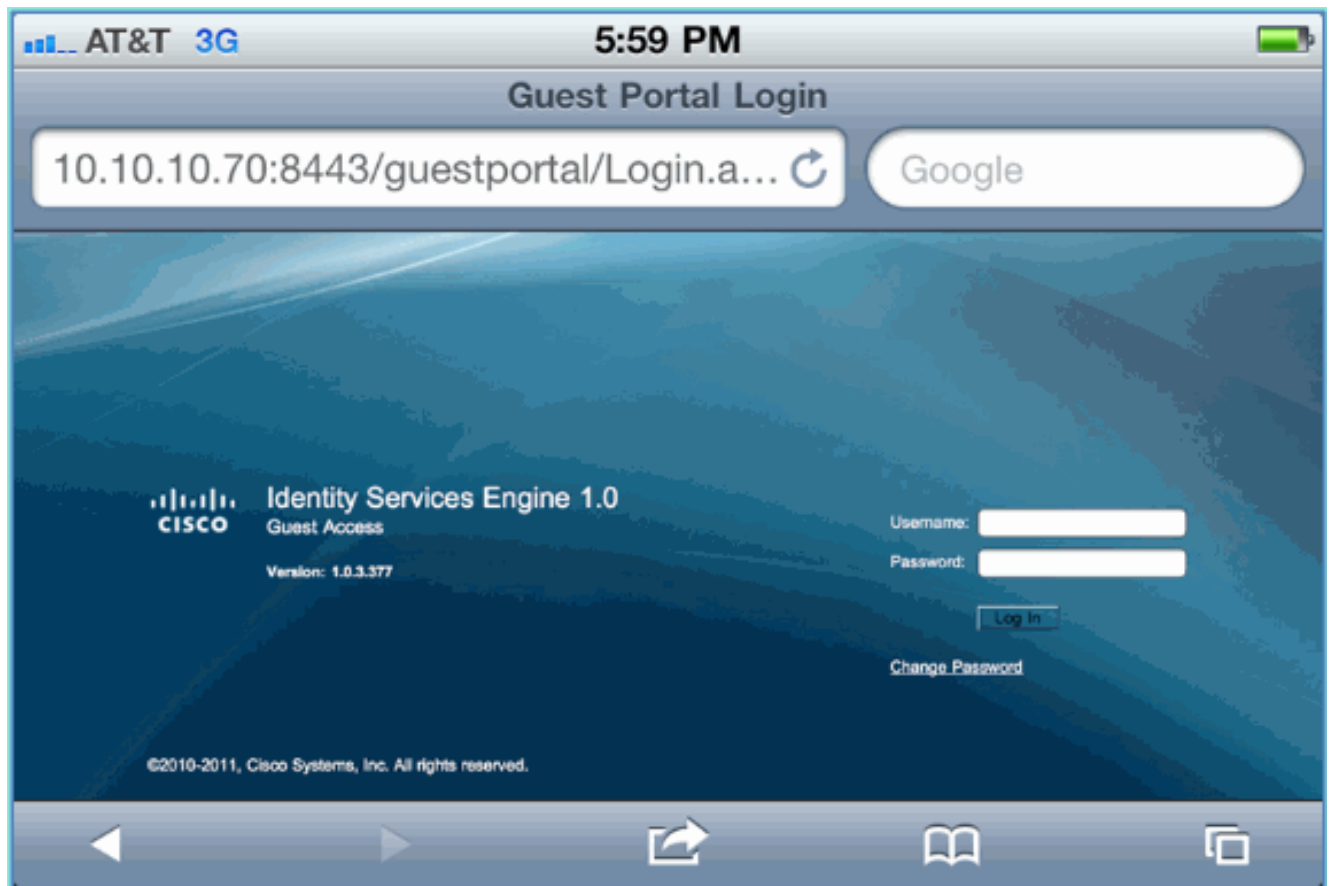


tonen.

3. Open de Safari browser en maak verbinding met:URL: <http://10.10.10.10>Er wordt een webverificatie-omleiding weergegeven.
4. Klik op **Doorgaan** tot u bent gearriveerd op de pagina van het ISE Guest



Portal. De
De volgende voorbeeldscreenshot toont het iOS-apparaat op een Guest Portal Login. Dit bevestigt dat de juiste installatie voor het WLAN en ISE Guest Portal actief is.

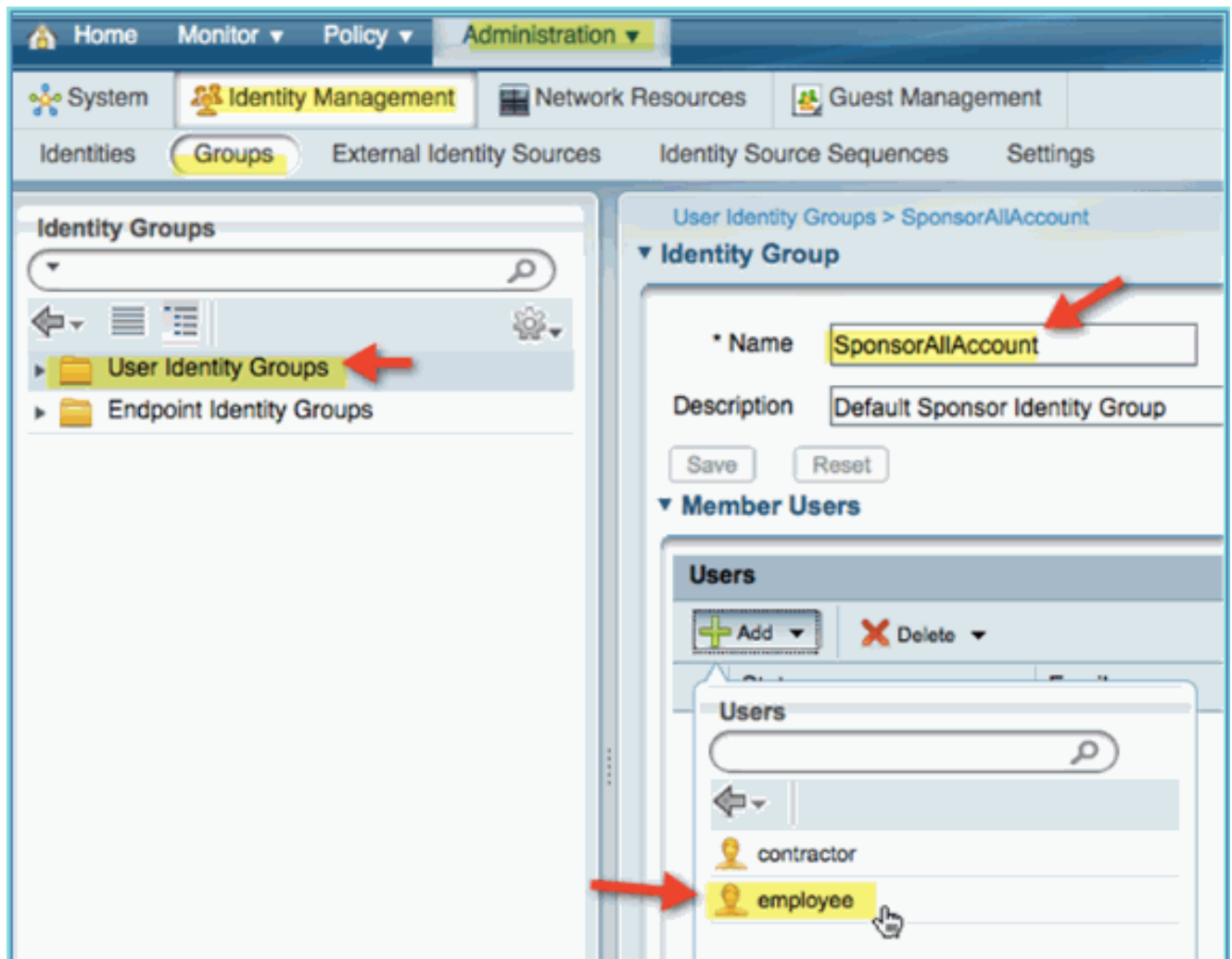


ISE draadloze gesponsorde gasttoegang

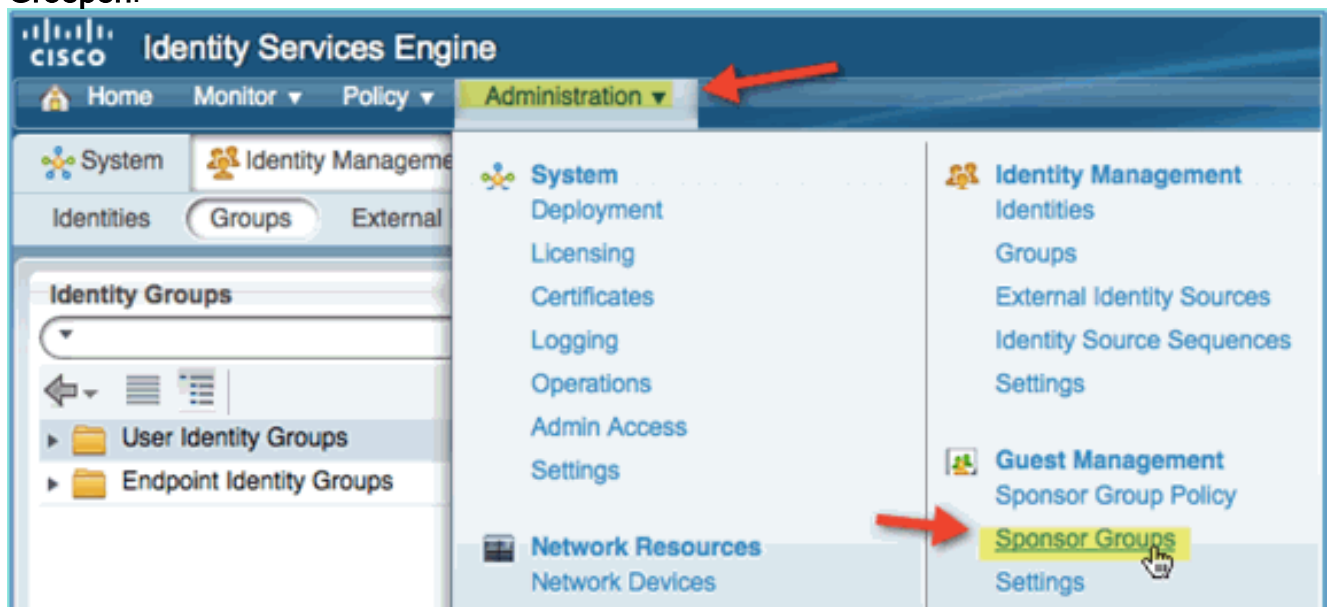
ISE kan zo worden geconfigureerd dat gasten kunnen worden gesponsord. In dit geval zal u ISE-gastbeleid configureren om interne of AD-domeingebruikers (indien geïntegreerd) de toegang tot gasten te kunnen sponsoren. U zal ook ISE configureren om sponsors toe te staan om gastwachtwoord te bekijken (optioneel), wat nuttig is voor dit lab.

Voer de volgende stappen uit:

1. Werknemergebruiker toevoegen aan de SponsorAllAccount groep. Er zijn verschillende manieren om dit te doen: rechtstreeks naar de groep gaan, of de gebruiker bewerken en een groep toewijzen. Ga bij dit voorbeeld naar **Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen**. Klik vervolgens op **SponsorAllAccount** en voeg een werknemersgebruiker toe.



2. Ga naar **Beheer > Gastenbeheer > Sponsor Groepen**.



3. Klik op **Bewerken** en kies vervolgens **SponsorAllAccounts**.





CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy **Sponsor Groups** Settings

Guest Sponsor Groups

 Edit  Add  Delete  Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

4. Selecteer Autorisatieniveaus en stel het volgende in:Wachtwoord voor gasten weergeven:
Ja

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb trail is "Sponsor Group List > SponsorAllAccounts". The "Authorization Levels" tab is selected and highlighted in green. A red arrow points to the "View Guest Password" dropdown menu, which is currently set to "Yes" and is also highlighted in yellow. Other settings include "Allow Login", "Create Accounts", "Create Bulk Accounts", "Create Random Accounts", "Import CSV", "Send Email", "Send SMS", "Allow Printing Guest Details", "View/Edit Accounts", and "Suspend/Reinstate Accounts". At the bottom, there are "Save" and "Reset" buttons.

5. Klik op **Opslaan** om deze taak te voltooien.

[Gast sponsoren](#)

Eerder hebt u het juiste gastenbeleid en de juiste gastengroepen ingesteld zodat AD-domeingebruikers tijdelijke gasten kunnen sponsoren. Vervolgens krijgt u toegang tot het Sponsor Portal en maakt u een tijdelijke gasttoegang.

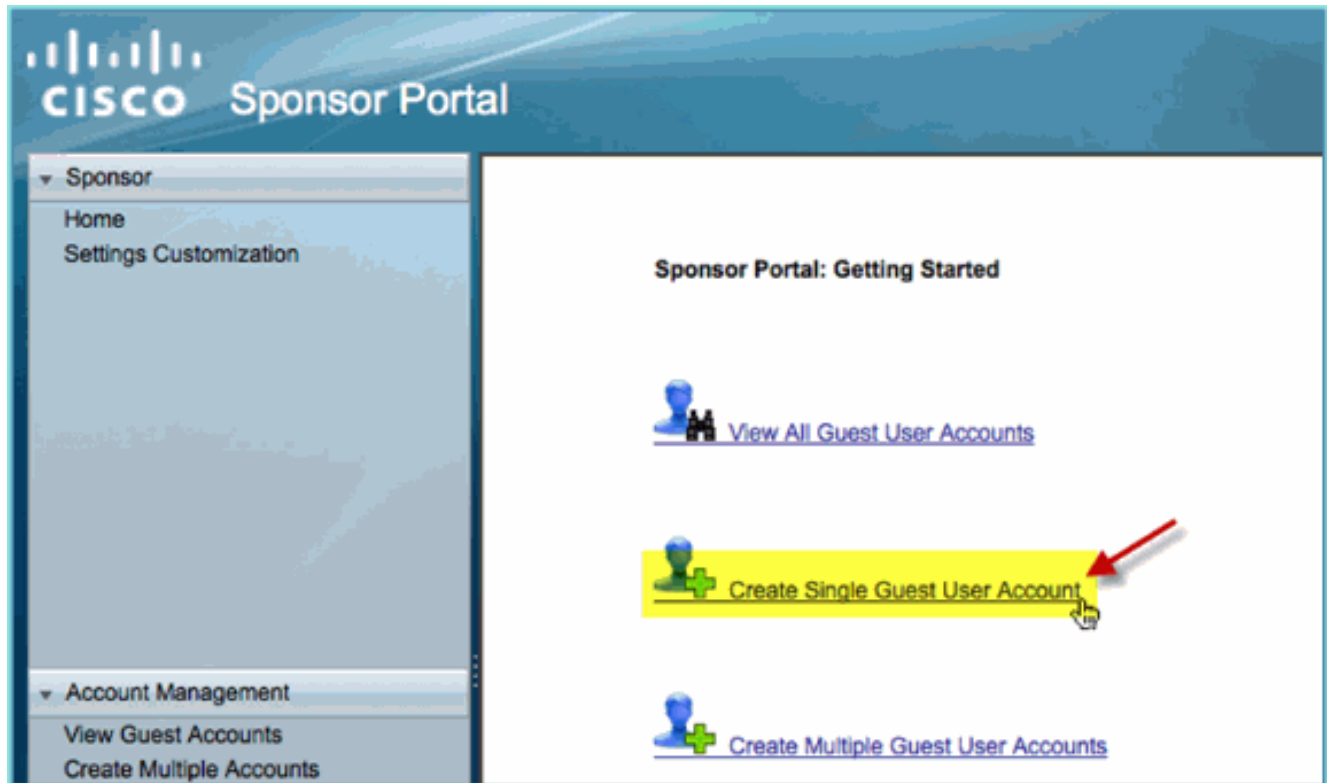
Voer de volgende stappen uit:

1. Ga vanuit een browser naar een van deze URL's: <http://<ip>:8080/sponsorportal/> of <https://<ip>:8443/sponsorportal/>. Log dan in met het volgende: Gebruikersnaam: aduser (Active Directory), medewerker (interne gebruiker)Wachtwoord:

XXXX



2. Klik op de pagina Sponsor op **Enkelgastengebruikersaccount** maken.



3. Voor een tijdelijke gast, voeg het volgende toe: Voornaam: Vereist (bijvoorbeeld Sam) Achternaam: Vereist (bijvoorbeeld Jones) Groepsrol: GastTijdprofiel: DefaultOneHourTijdzone: Any/Default

Sponsor Portal

Account Management > [View All Guest Accounts](#) > Create Guest Account

Create Guest Account

First Name:

Last Name:

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:

Time Profile:

Timezone:

= Required fields

4. Klik op **Verzenden**.
5. Er wordt een gastaccount aangemaakt op basis van uw vorige boeking. Merk op dat het wachtwoord zichtbaar is (van vorige oefening) in plaats van ***.
6. Laat dit venster open met de gebruikersnaam en het wachtwoord voor de gast. Je zal ze gebruiken om te testen Guest Portal Login (volgende).



Successfully Created Guest Account **siam0002**

Username: **siam0002** ←

Password: **5_5g6d7Kx** ←

First Name: Sam ←

Last Name: iAm

Email Address:

Phone Number:

Company:

Status: AWAITING INITIAL LOGIN

Suspended: false

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role: Guest

Time Profile: DefaultOneHour

Timezone: EST

Account Start Date: 2011-07-15 13:56:04 EST

Account Expiration Date: 2011-07-15 14:56:04 EST

Email

Print

Create Another Account

View All Accounts

[Toegang tot gastenportal testen](#)

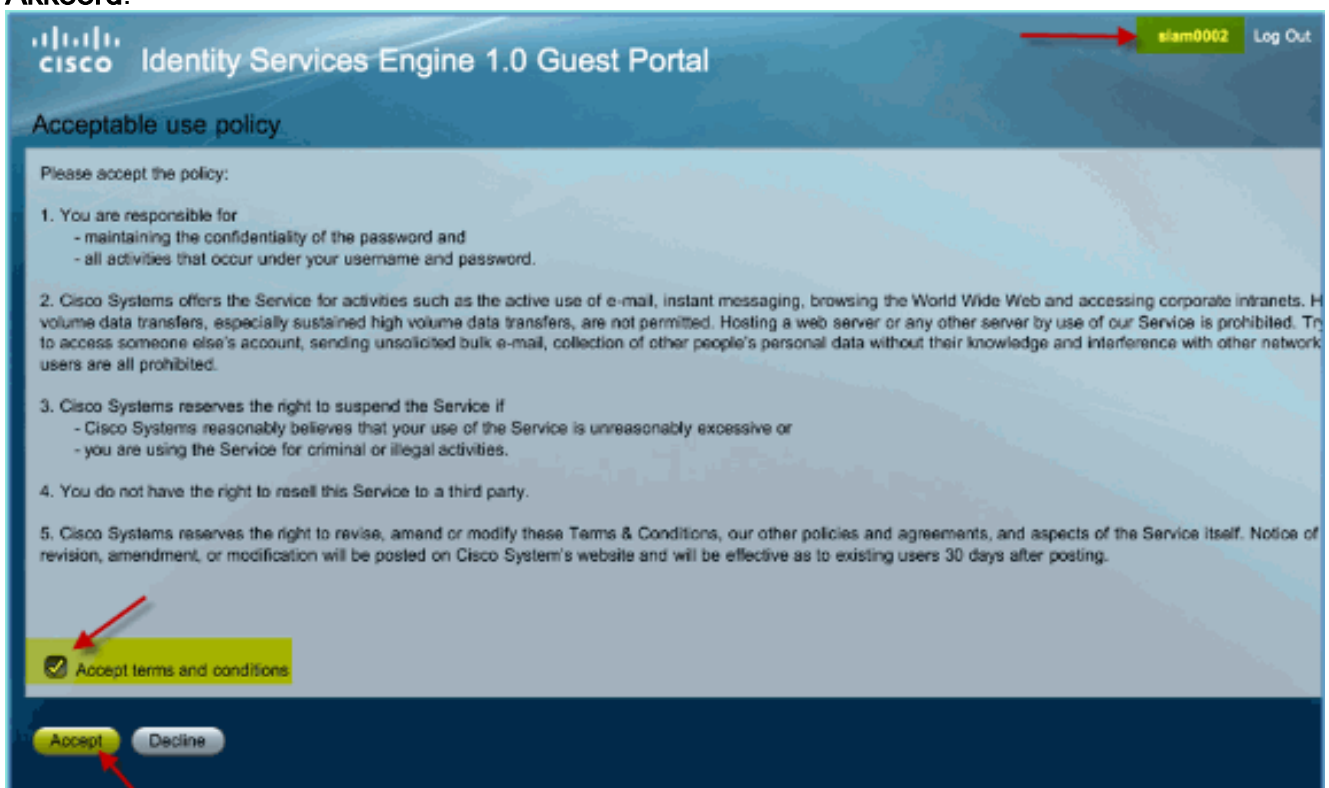
Met het nieuwe gastaccount dat door een AD-gebruiker/sponsor is gemaakt, is het tijd om het gastportaal en de toegang te testen.

Voer de volgende stappen uit:

1. Op een voorkeursapparaat (in dit geval een Apple iOS / iPad), maak verbinding met de Pod Guest SSID en controleer het IP-adres / de connectiviteit.
2. Gebruik de browser en probeer te navigeren naar <http://www>. Je wordt doorgestuurd naar de inlogpagina van het Guest Portal.



3. Log in met de gastaccount die in de vorige oefening is gemaakt. Indien geslaagd, verschijnt de pagina Acceptable Use Policy (Beleid voor aanvaardbaar gebruik).
4. Controleer de **voorwaarden en bepalingen accepteren** en klik vervolgens op **Akkoord**.



De originele URL is voltooid en het eindpunt is geautoriseerd als gast.

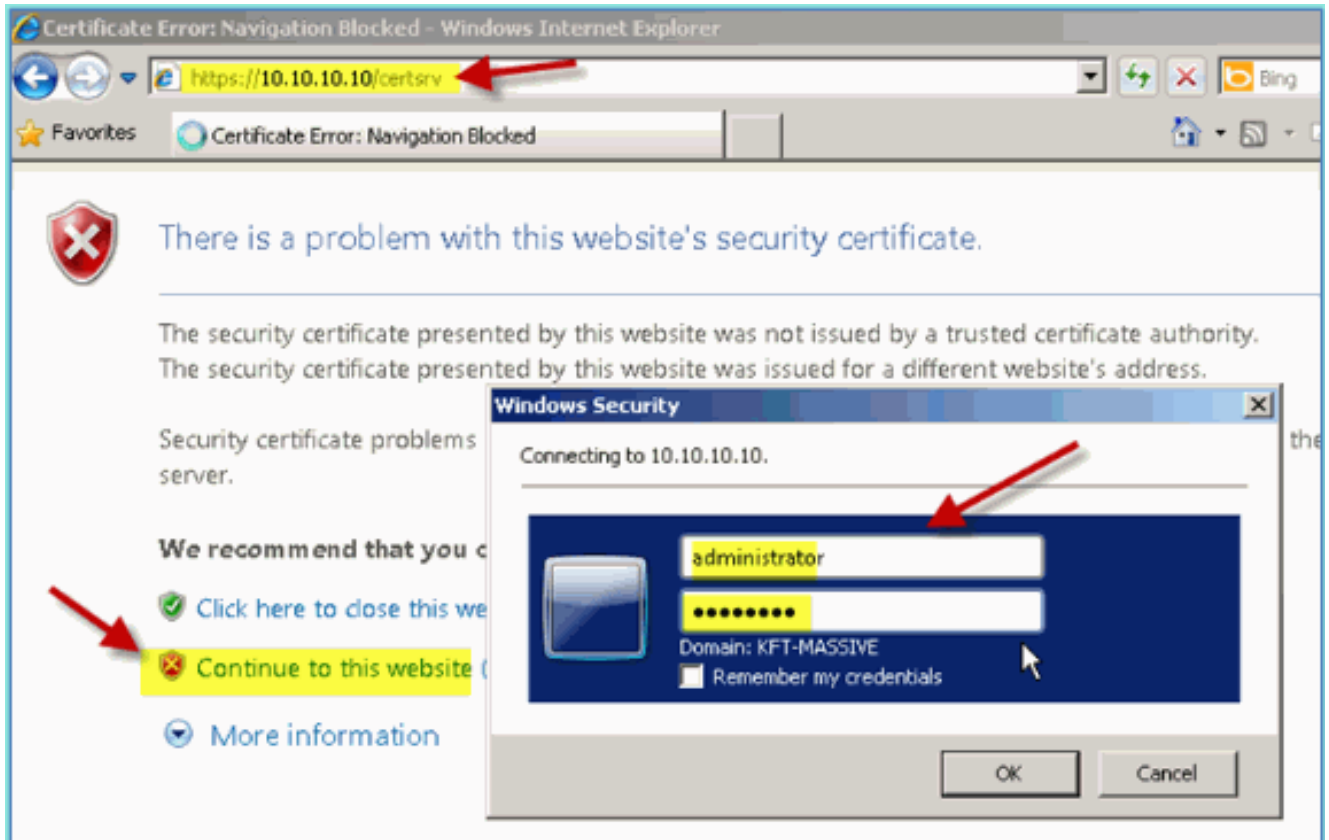
Certificaatconfiguratie

Om de communicatie met ISE te beveiligen, moet u bepalen of de communicatie betrekking heeft op authenticatie of voor ISE-beheer. Bijvoorbeeld, voor configuratie met behulp van de ISE web UI, X.509 certificaten en certificaat trust ketens moeten worden geconfigureerd om asymmetrische encryptie mogelijk te maken.

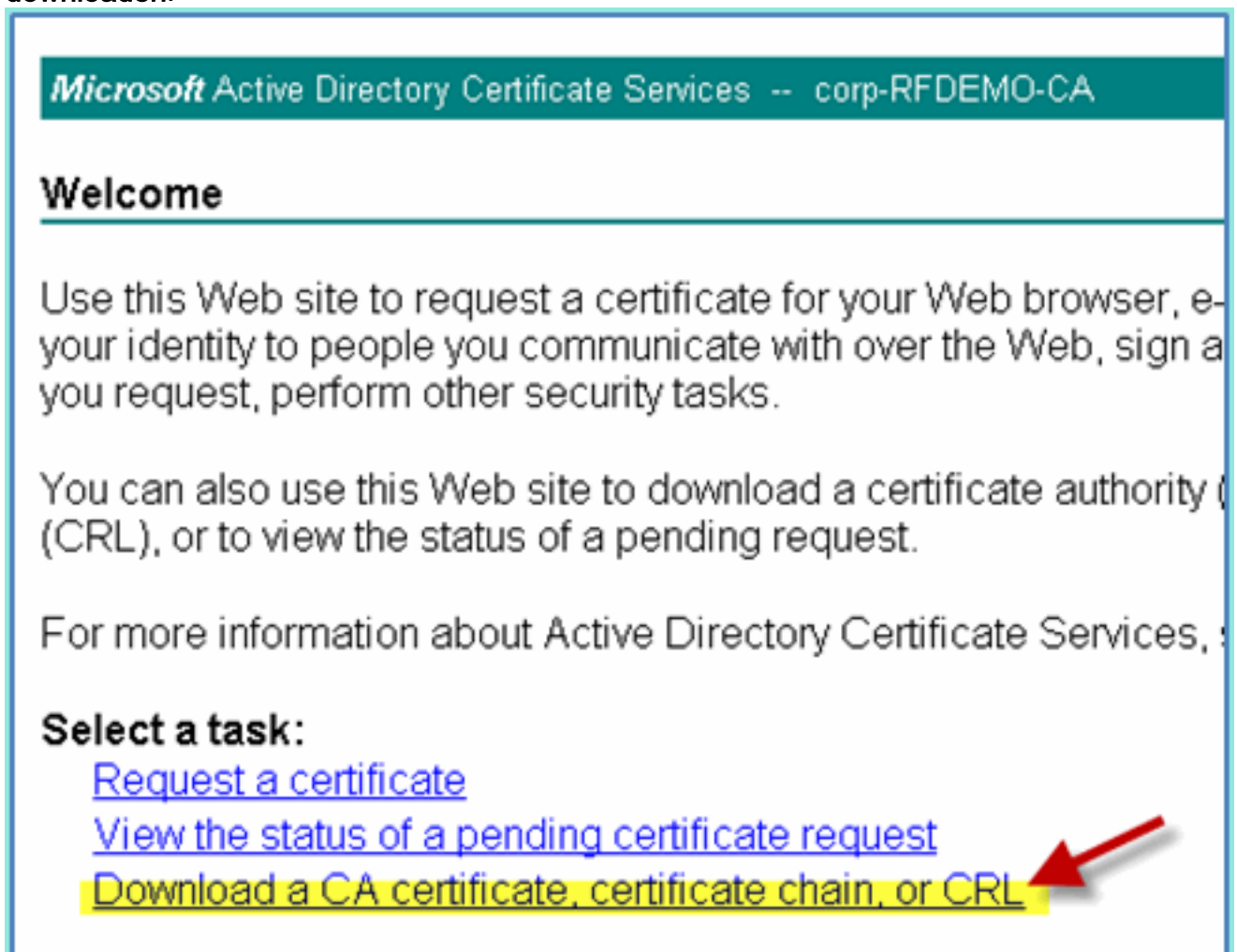
Voer de volgende stappen uit:

1. Open vanuit uw bekabelde verbonden pc een browservenster op <https://AD/certsrv>. **Opmerking:** gebruik de beveiligde HTTP. **Opmerking:** gebruik Mozilla Firefox of MS Internet Explorer om toegang tot ISE te krijgen.
2. Log in als

beheerder/Cisco123.



3. Klik op Een CA-certificaat, certificaatketen of CRL downloaden.



4. Klik op CA-certificaat downloaden en bewaar het (let op de

opslaglocatie).

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install the CA certificate on your computer. To download a CA certificate, certificate chain, or CRL, select the type of file you want to download.

CA certificate:

Current [corp-RFDEMO-CA]

Encoding method:

DER
 Base 64

[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)
[Download latest delta CRL](#)

5. Open een browservenster op <https://<Pod-ISE>>.
6. Ga naar **Beheer > Systeem > Certificaten > Certificaten van de Autoriteit Certificaten**.

CISCO Identity Services Engine

Home Monitor Policy Administration

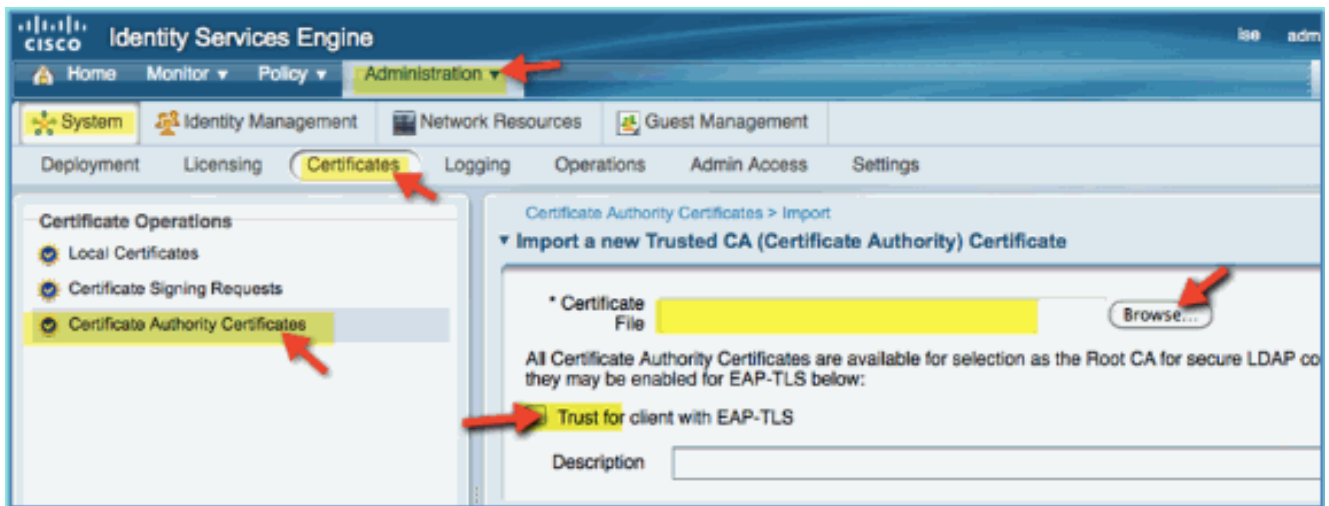
System
Deployment
Licensing
Certificates
Logging

Metrics

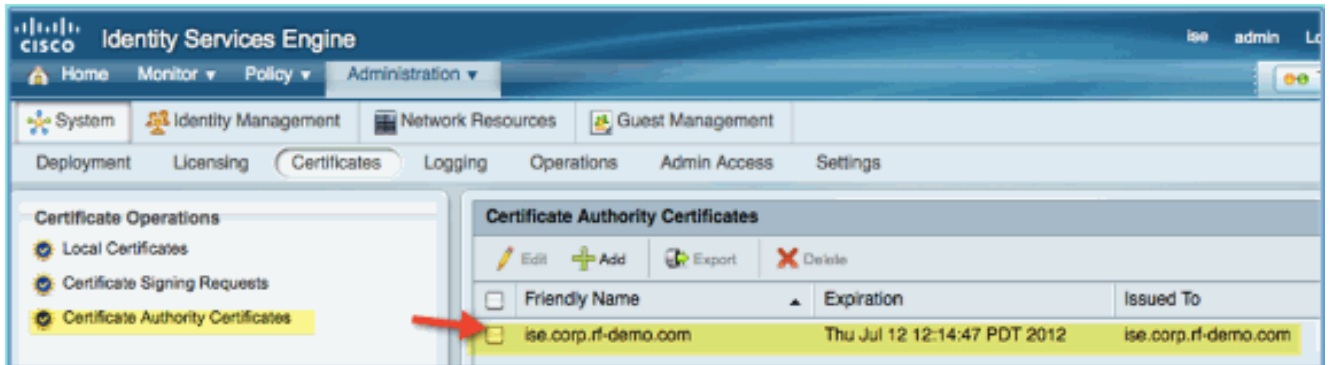
Active Endpoints

0 -

7. Selecteer **Certificaatautoriteit Certificaten** en blader naar de eerder gedownloade CA cert.
8. Selecteer **Vertrouwen voor client met EAP-TLS** en vervolgens indienen.

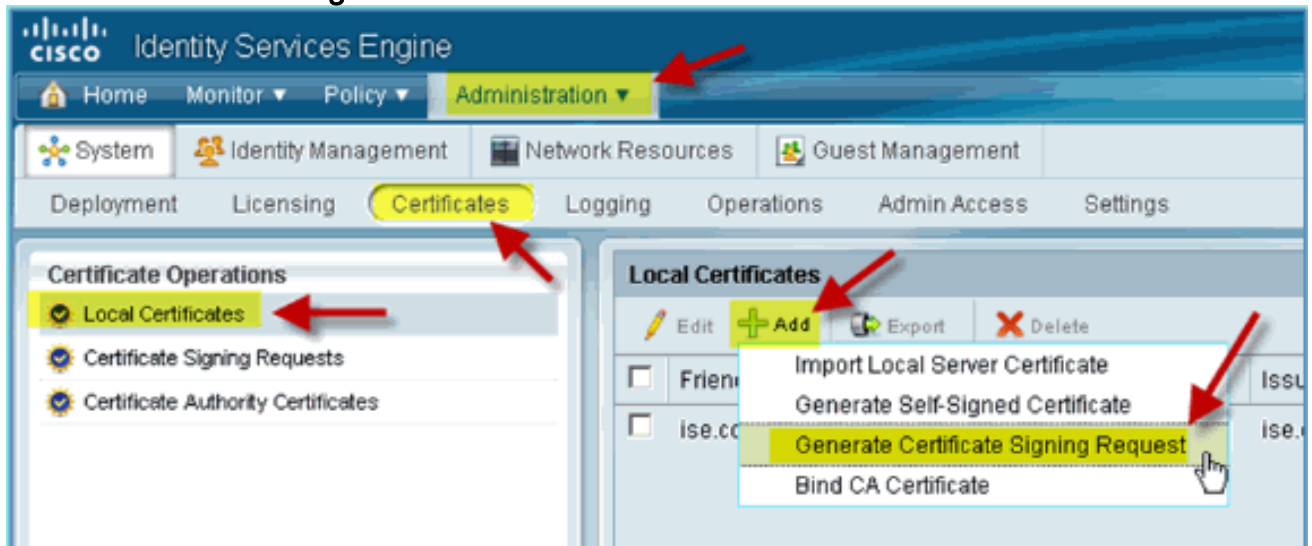


9. Bevestig dat de CA is toegevoegd als root-CA.



10. Ga vanuit een browser naar **Beheer > Systeem > Certificaten > Certificaten Autoriteit Certificaten**.

11. Klik op **Add** en **Genereer** vervolgens de **aanvraag voor certificaatondertekening**.



12. Geef deze waarden door: Certificaat Onderwerp: CN=ise.corp.rf-demo.com Sleutelengte: 2048

Local Certificates > Generate Certificate Signing Request

▼ **Generate Certificate Signing Request**

Certificate

* Certificate Subject

* Key Length

Digest to Sign With SHA1

13. ISE geeft aan dat de CSR beschikbaar is op de CSR-pagina. Klik op OK.



14. Selecteer de CSR op de ISE CSR-pagina en klik op **Exporteren**.
15. Het bestand op een willekeurige locatie opslaan (bijvoorbeeld downloads, enzovoort)
16. Bestand wordt opgeslagen als *.pem.

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Operations Admin Access Settings

Certificate Operations

- Local Certificates
- Certificate Signing Requests
- Certificate Authority Certificates

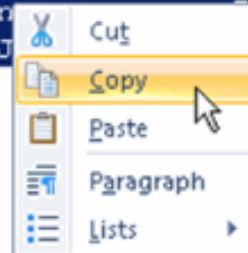
Certificate Signing Requests

Export Delete

<input checked="" type="checkbox"/>	Friendly Name	Certificate Subject	Key Length
<input checked="" type="checkbox"/>	ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048

17. Zoek het CSR-bestand en bewerk met Kladblok/Wordpad/TextEdit.
18. Kopieert de inhoud (selecteer alles > Kopiëren).

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyTCCAbECAQAwHzEdMBSGA1UEAxMUaXNlLmNvcnAucmYtZGVtby5jb20wggEi
MADGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXaeWDSqfiI64K59dyRLm8JAxan
WYTaAJ68/Ke206ws/K3BFAFJQhndQQ0hYVmGcJLVN03pXtRln/q/HBuglLIItIvbe
86FADPq3kUNb48UHcdR9b5rUs7B8T5E6banZia6eHSXjIzX4f0U7mVOrzALeAPDK
HXU+/y/gleyNL6P8zC4bvi/SZXhZp1OvTQpi+8lh14M5ROChhbPUnB3EGVaIVRiN
wYn8OjvejbtG//k0CItGARlG2IFbBbgUpkMVhDQqgixp3wrlm3hi9JXgffEI f4BO
sirLrhvMSuSNESnIVWYrRLz5Xt4dMct+bu08xaEYPqgoukYjxsA9gn0bRDMJAgMB
AAGgZTBjBqkqhkiG9w0BCQ4xVjBUMASGA1UdDwQEAwICrDAdBgNVHQ4EFgQU2jmj
715rSw0yVb/vlWAYkK/YBwkWewYDVR0lBAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4
QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBz4YPO9sN7WF2Htg+48300mw9q
gA/MMZsTioEPekcunm+ZFtlAXajB32uwHHi1lc9Rn93TgOWPFxKEX9E89fzSWDK
J4qsQM7KEYOpQt4bia07188Lm6BBTk9mRhiTBwSF3dx0tlzfgiHc72kjWvxsgg/c
k8a7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42riz7vK0g0nkWRHF52uiu3AkP
LPKQ72N2XYIXfu0jdgOaJjmsk6T9nLABVYQ6n...KDJTHchcwx6I1k/
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJ...W1ZuB6drHg9
-----END CERTIFICATE REQUEST-----
```



19. Open een browservenster op <https://<Pod-AD>/certsrv>.
20. Klik op **Certificaat aanvragen**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Welcome

Use this Web site to request a certificate for your Web browser to communicate with over the Web, sign and encrypt messages.

You can also use this Web site to download a certificate automatically for a pending request.

For more information about Active Directory Certificate Services, click the following link:

Select a task:

[Request a certificate](#)

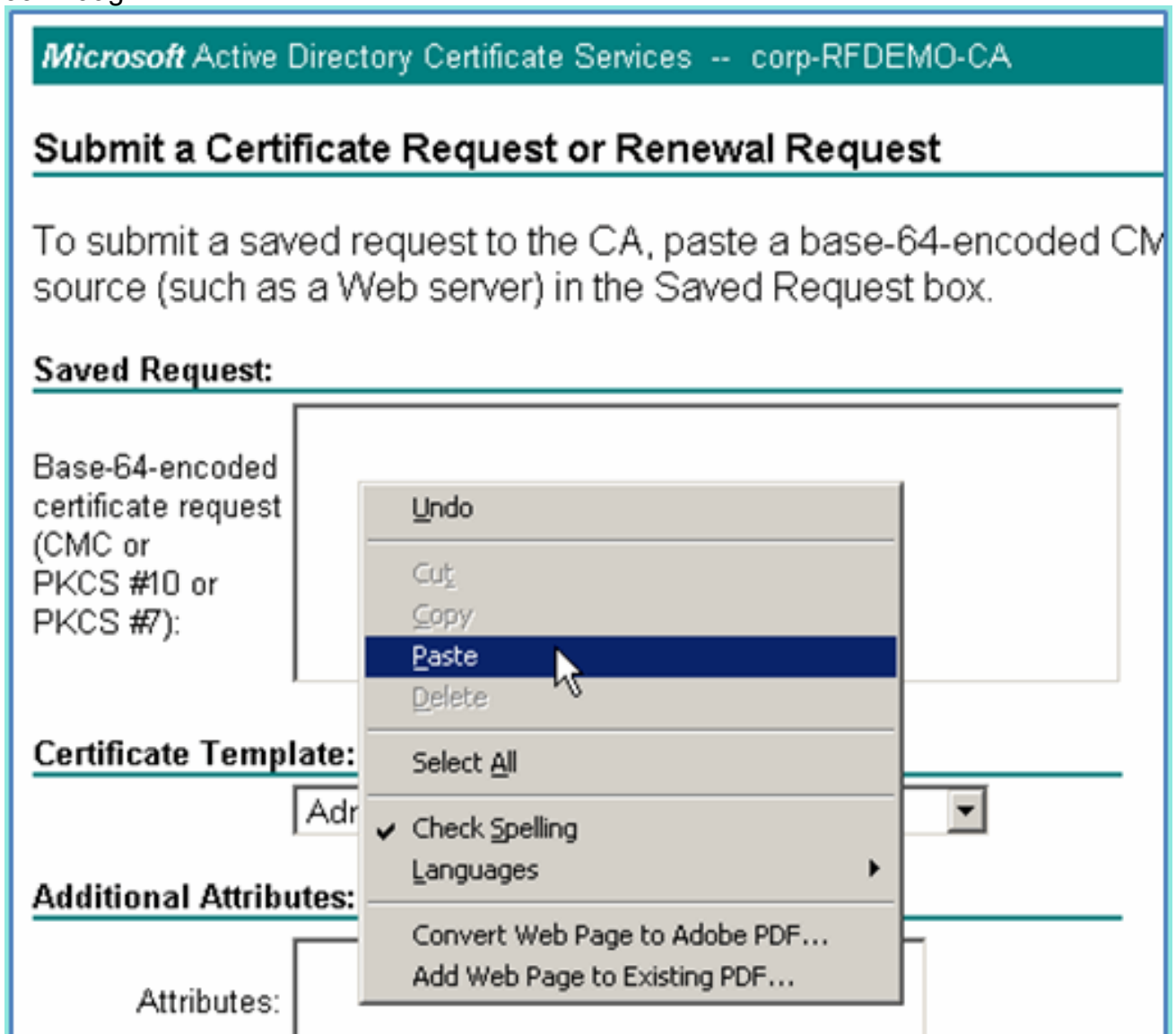
[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

21. Klik om een geavanceerde certificaataanvraag in te dienen.



22. Plakt de CSR-inhoud in het veld Opgeslagen aanvraag.



23. Selecteer **Webserver** als de certificaatsjabloon en klik vervolgens op **Indienen**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
gA/MMZsTioEPekcunnm+ZFt1AXajB32uwHH11c9
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF
kSa7LHYgkgLRYBnpul5RjQ7wWijArH8cK1OrVT42
LPKQ72N2XYIXfu0jdgogaJjmsk6T9nLABVYQ6nKQx
V5QYBOjTYHXIPG8/ned9z3MOiZd2sm4XNS2bJfO/
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

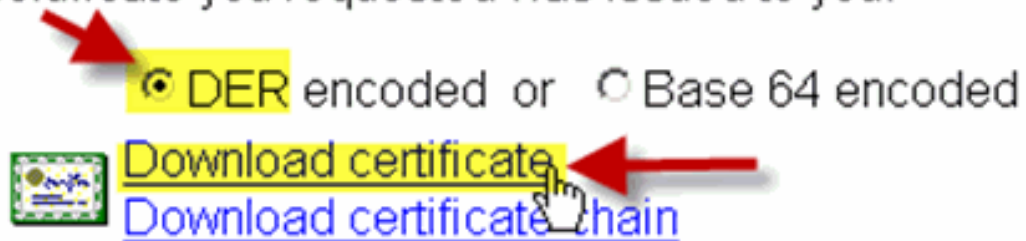
Attributes:

Submit >

24. Selecteer **DER encoded**, dan klik het certificaat van de **Download**.

Certificate Issued

The certificate you requested was issued to you.

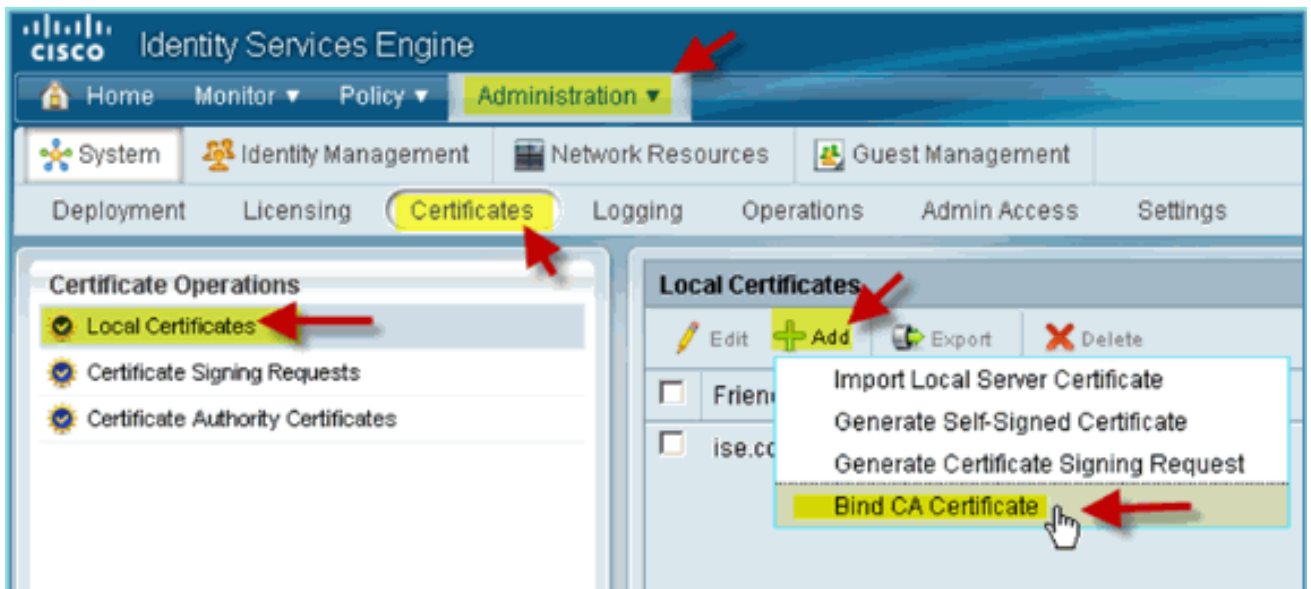


25. Het bestand op een bekende locatie opslaan (bijvoorbeeld downloads)

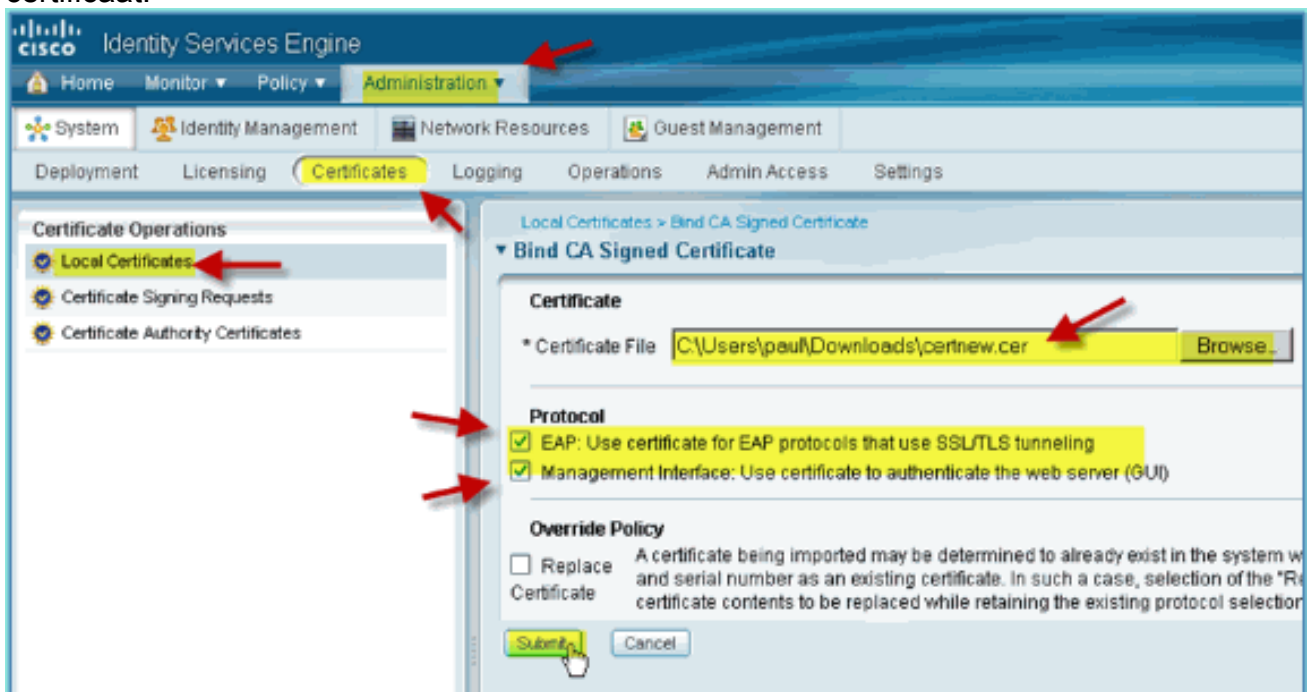
26. Ga naar **Beheer > Systeem > Certificaten > Certificaten van de Autoriteit Certificaten**.



27. Klik op **Add > Bind CA-**
certificaat.

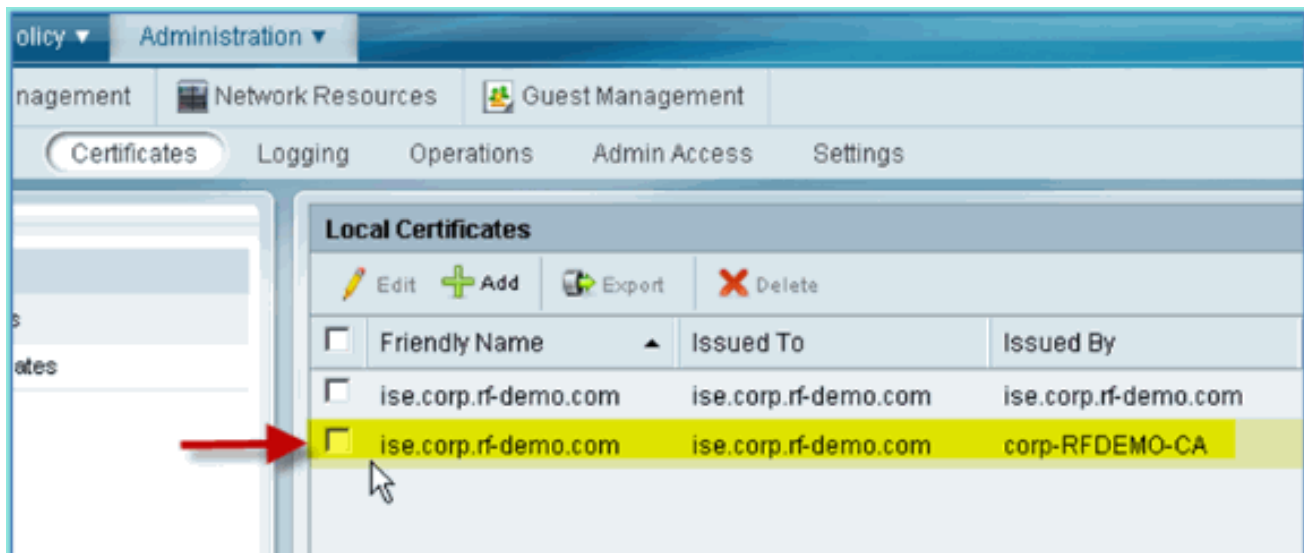


28. Blader naar het eerder gedownloadde CA-certificaat.



29. Selecteer zowel **Protocol EAP** als **Management Interface**, en klik vervolgens op **Indienen**.

30. Bevestig dat de CA is toegevoegd als root-CA.

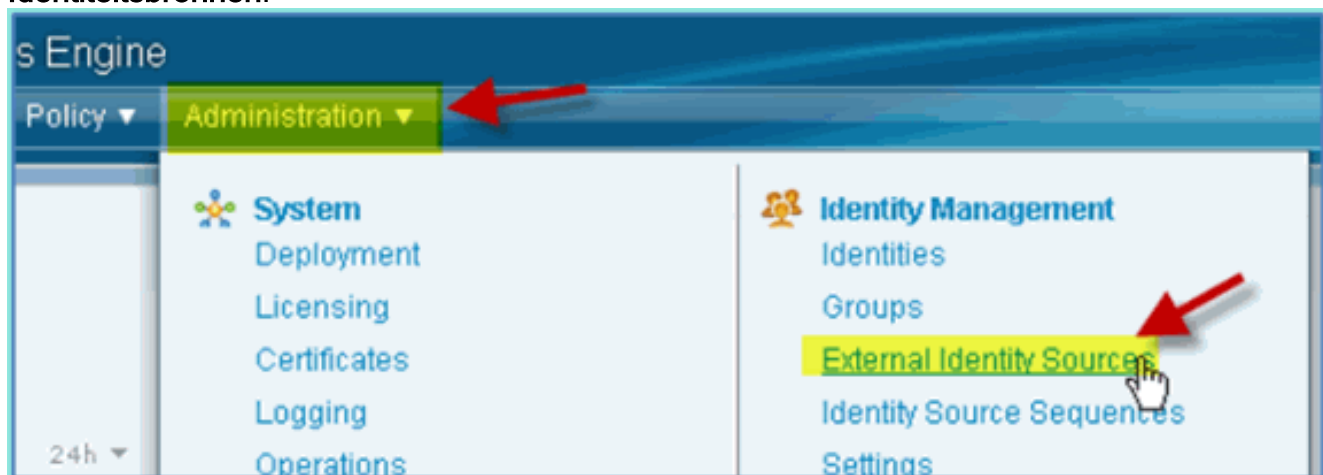


[Integratie van Windows 2008 Active Directory](#)

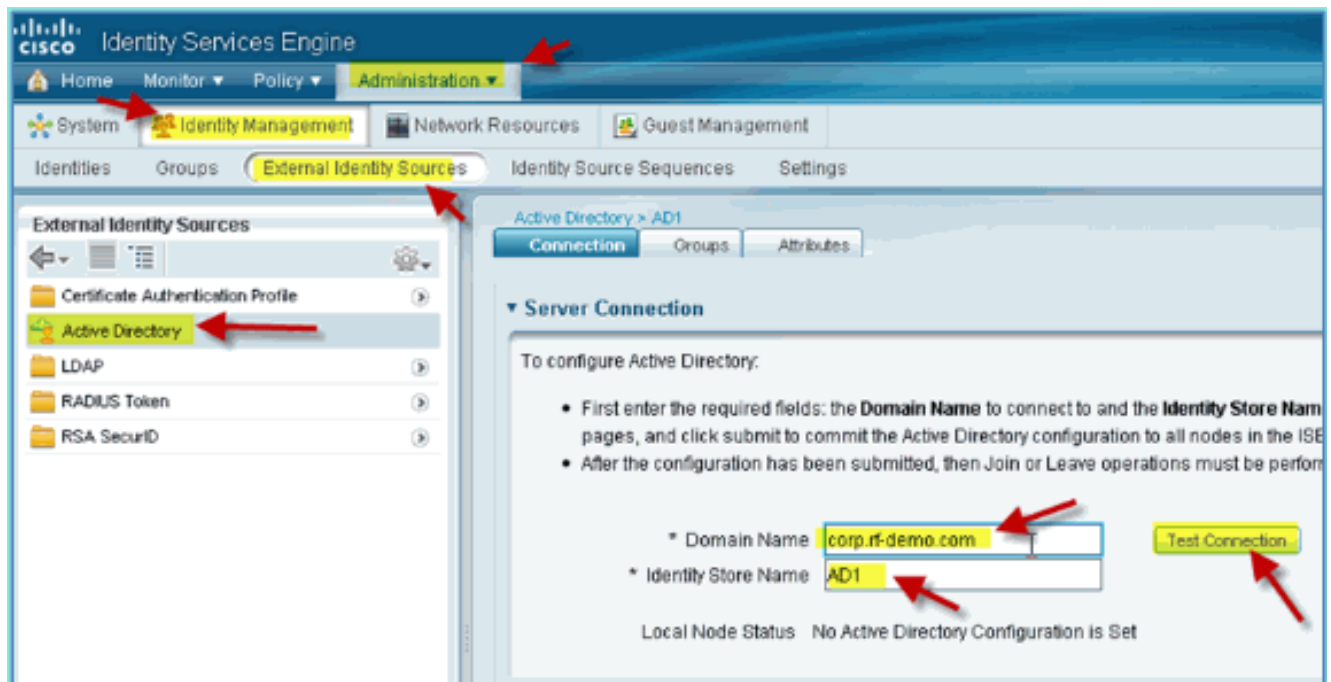
ISE kan direct communiceren met Active Directory (AD) voor gebruikers/machine-verificatie of voor het ophalen van autorisatiegegevens gebruikerskenmerken. Om met AD te kunnen communiceren, moet ISE worden "aangesloten" bij een AD-domein. In deze oefening sluit je je aan bij ISE in een AD-domein en bevestig je dat AD-communicatie correct werkt.

Voer de volgende stappen uit:

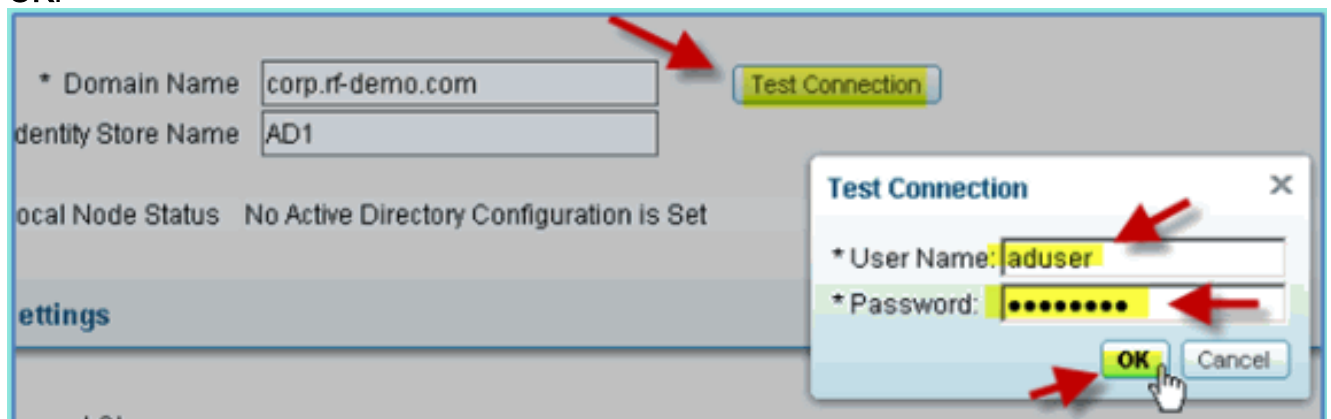
1. Om zich aan te sluiten bij ISE in het AD-domein, gaat ISE naar **Administratie > Identity Management > Externe Identiteitsbronnen**.



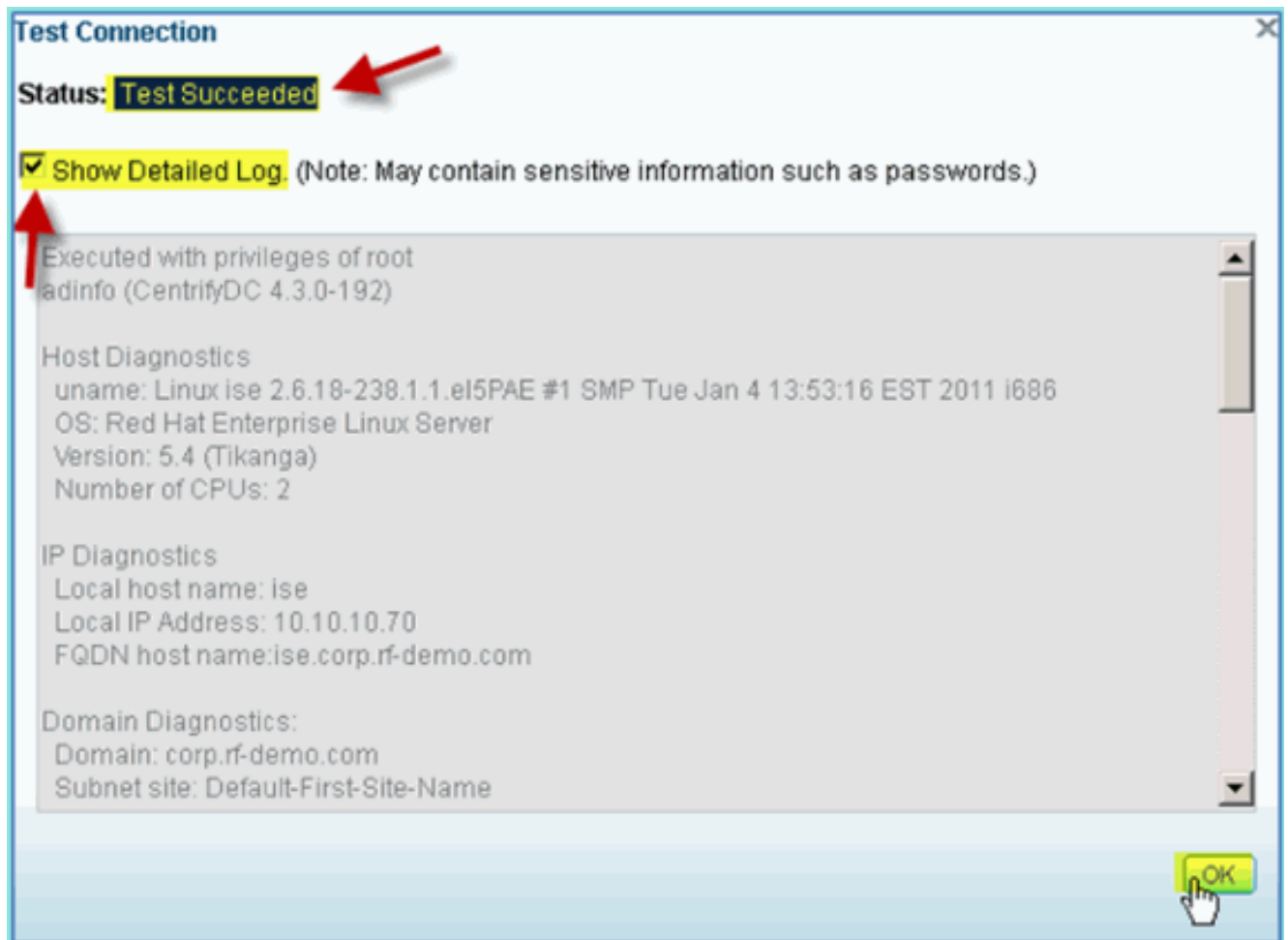
2. Selecteer in het linkerdeelvenster (Externe identiteitsbronnen) de optie **Active Directory**.
3. Selecteer aan de rechterkant het tabblad **Verbinding** en voer het volgende in: Domeinnaam: corp.rf-demo.com Identity Store Naam: AD1



4. Klik op **Verbinding testen**. Voer een AD-gebruikersnaam in (aduser/Cisco123) en klik vervolgens op **OK**.



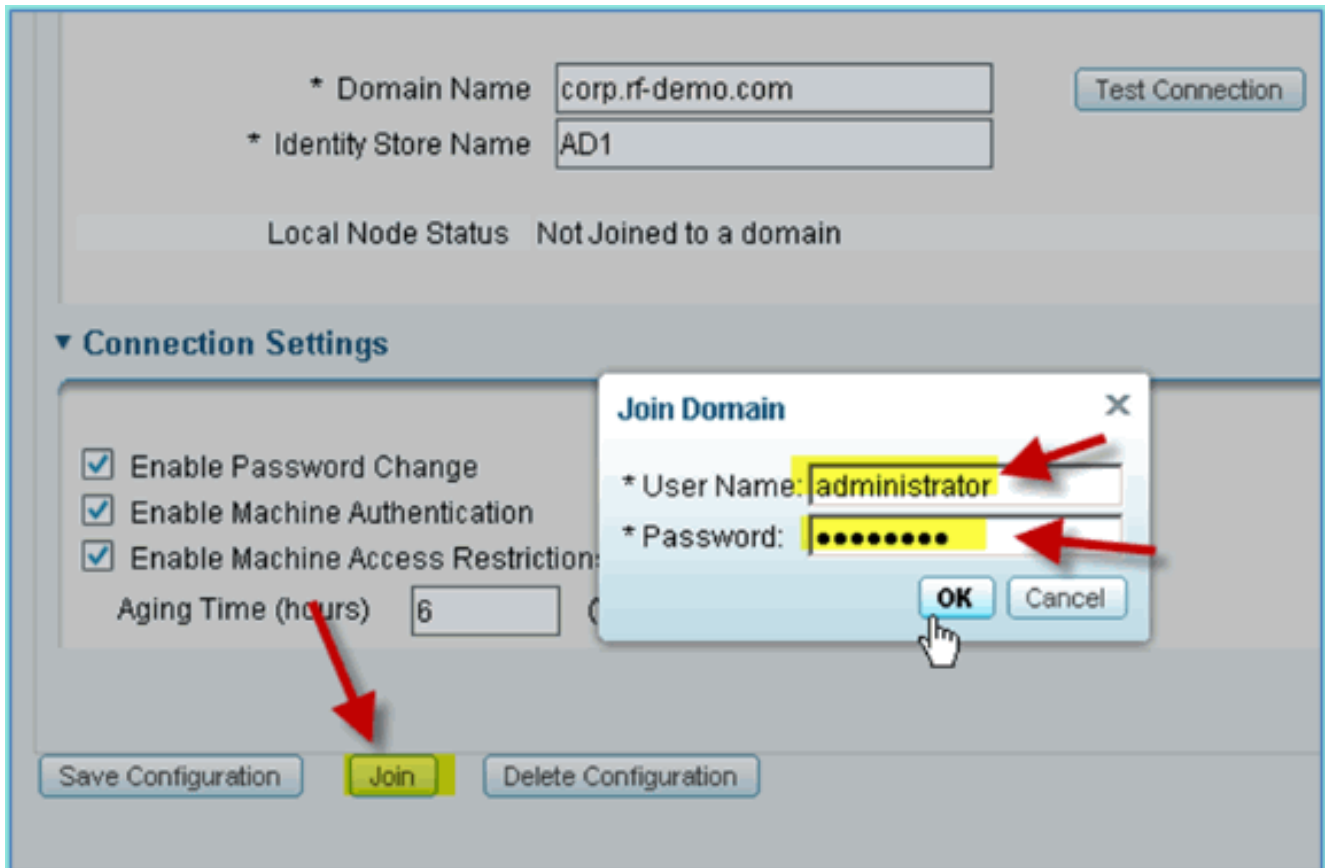
5. Bevestig dat de teststatus **Test Succeeded** laat zien.
6. Selecteer Gedetailleerd logbestand tonen en details bekijken die nuttig zijn voor het oplossen van problemen. Klik op **OK** om verder te gaan.



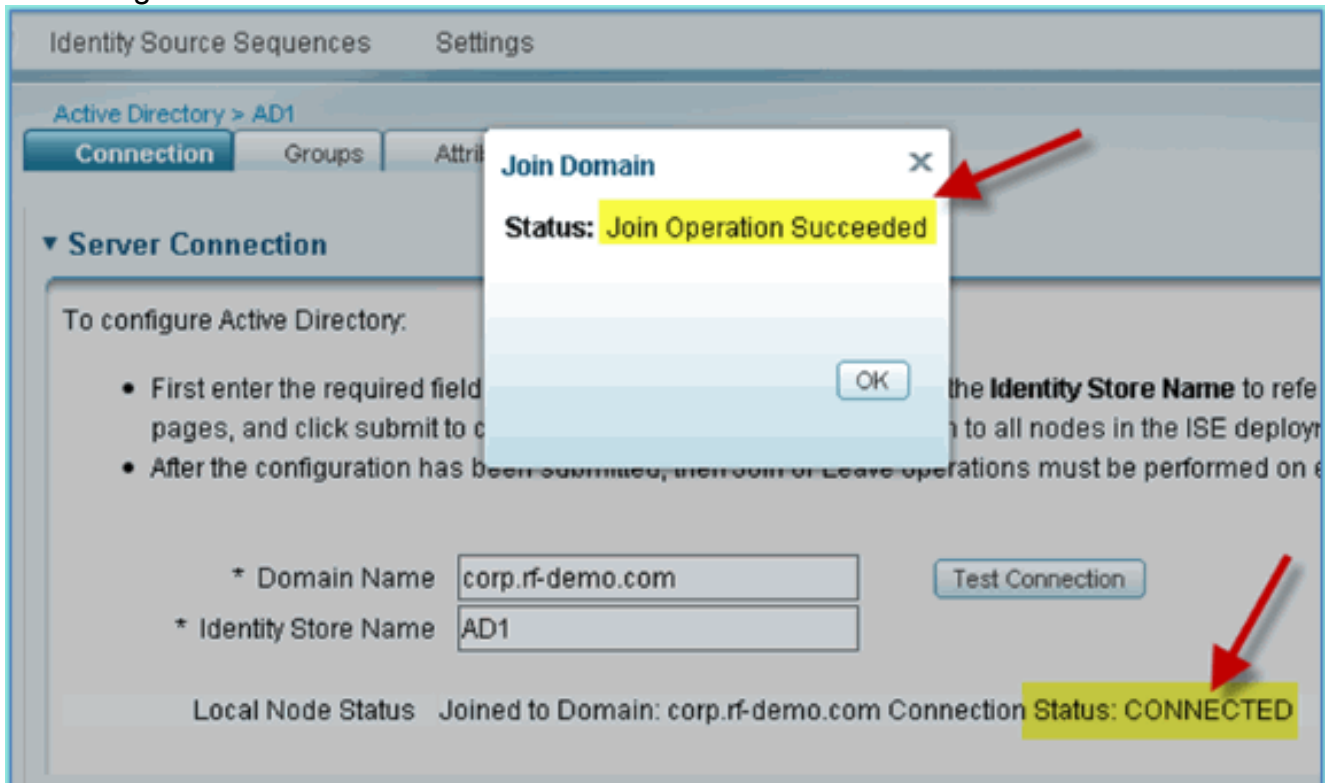
7. Klik op **Configuratie opslaan**.



8. Klik op **Samenvoegen**. Voer de AD-gebruiker in (beheerder/Cisco123) en klik vervolgens op **OK**.



9. Bevestig dat de Join Status van de Verrichting **Geslaagd** toont, dan klik **OK** om verder te gaan. De verbindingstatus van de server laat **CONNECTED** zien. Als deze status op elk moment verandert, helpt een testverbinding bij het oplossen van problemen met de AD-bewerkingen.



[Active Directory-groepen toevoegen](#)

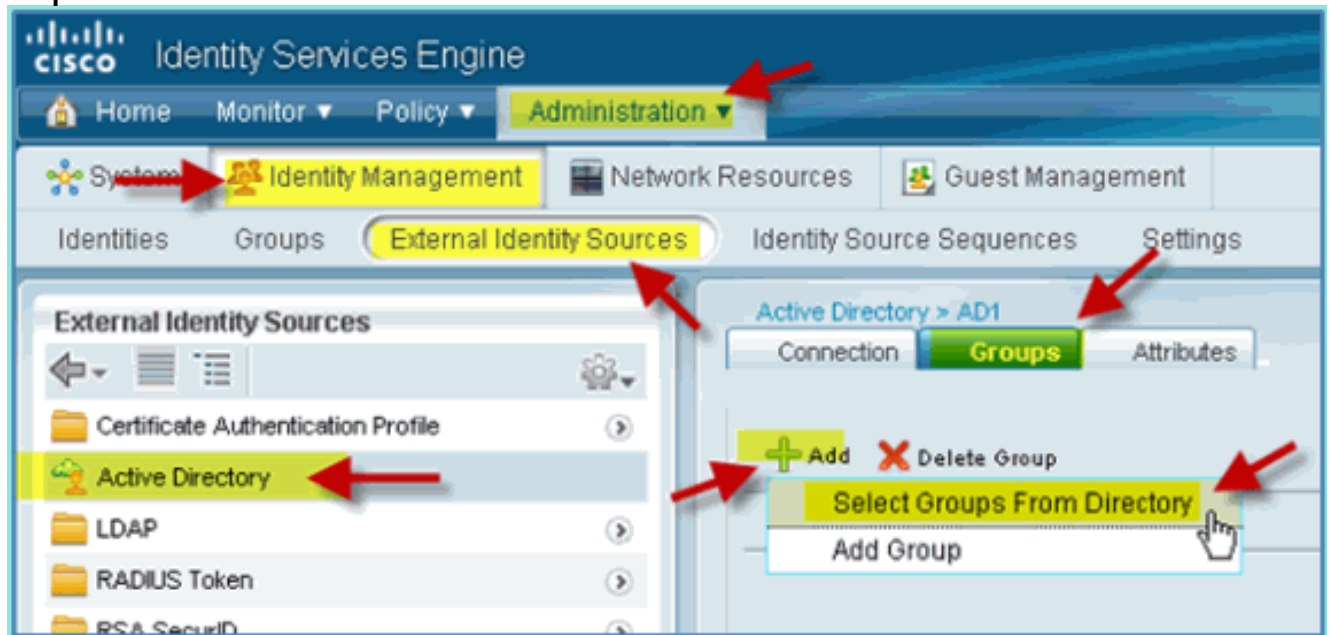
Wanneer AD-groepen worden toegevoegd, is een meer gedetailleerde controle over het ISE-

beleid toegestaan. Zo kunnen AD-groepen worden gedifferentieerd op basis van functionele rollen, zoals Werknemers- of Contractgroepen, zonder dat het gerelateerde bug wordt ervaren in eerdere ISE 1.0-oefeningen waarbij het beleid beperkt was tot gebruikers.

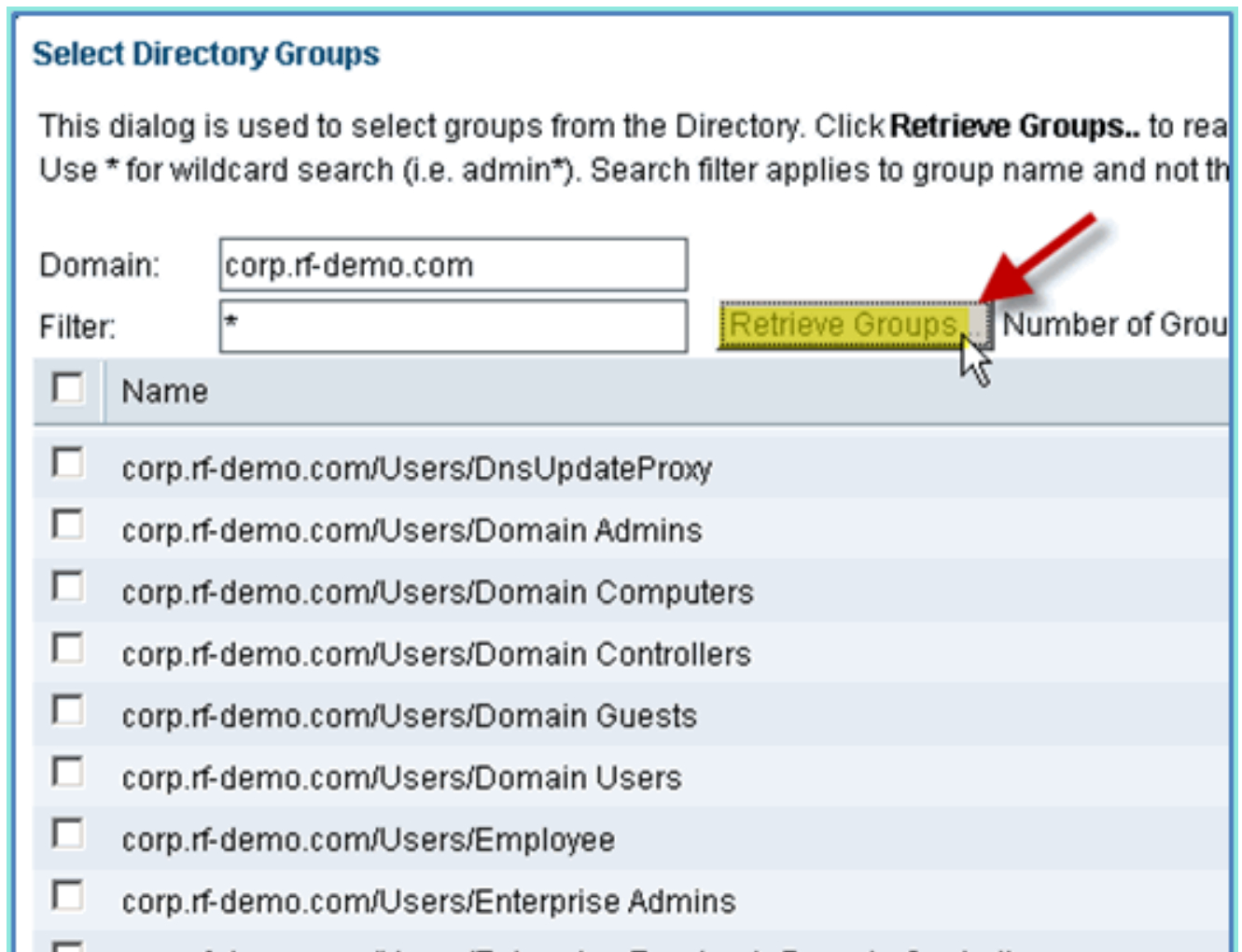
In dit laboratorium worden alleen de Domeingebruikers en/of de Werknemersgroep gebruikt.

Voer de volgende stappen uit:

1. Ga van ISE naar **Administratie > Identiteitsbeheer > Externe Identiteitsbronnen**.
2. Selecteer het tabblad **Active Directory > Groepen**.
3. Klik op **+Add** en selecteer vervolgens **Groepen uit map**.



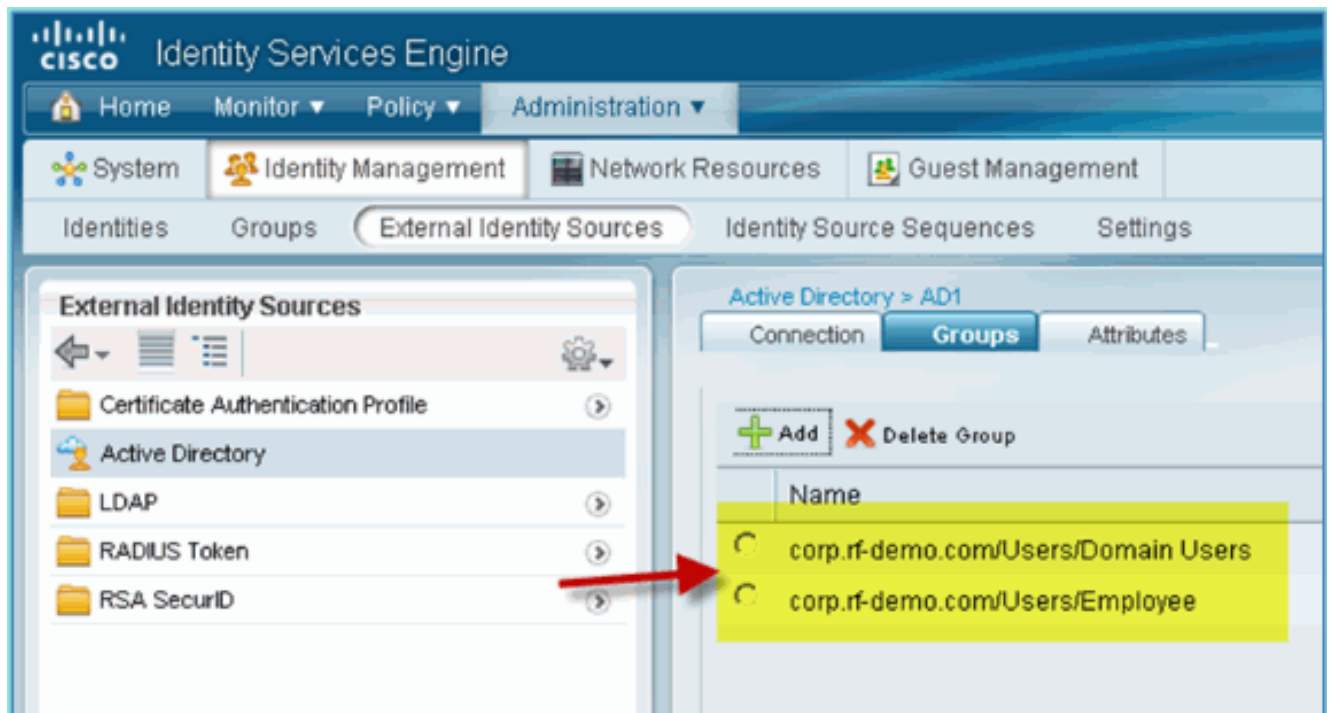
4. Accepteer in het vervolgvenster (Select Directory Groups) de defaults voor domain (corp-rf-demo.com) en Filter (*). Klik vervolgens op **Groepen ophalen**.



5. Selecteer de vakjes voor **domeingebruikers** en **werknemersgroepen**. Klik op **OK** als u klaar bent.



6. Bevestig dat de groepen aan de lijst zijn toegevoegd.

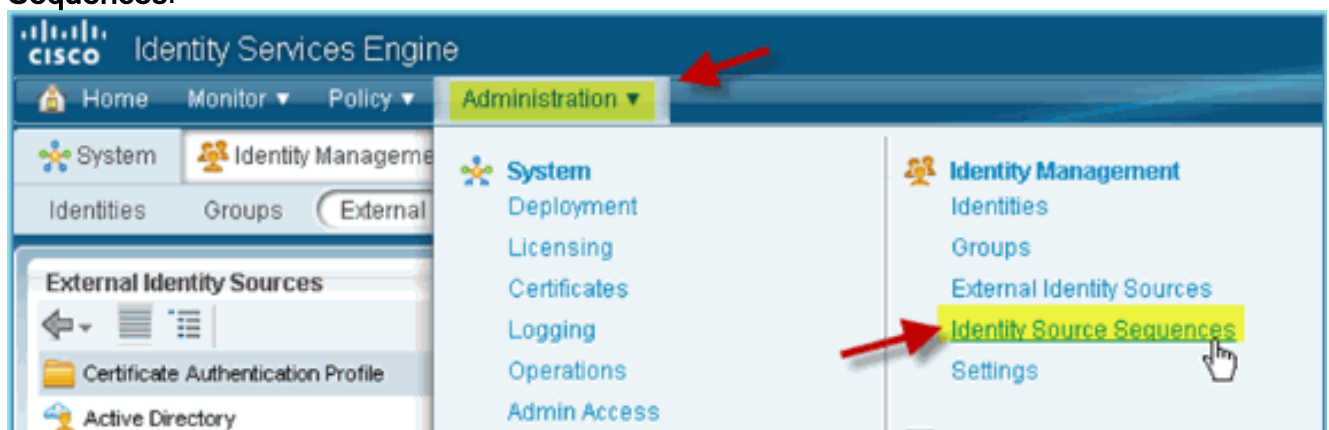


Identity Source Sequence toevoegen

Standaard is ISE ingesteld op Interne gebruikers voor het opslaan van authenticatie. Als AD wordt toegevoegd, kan een prioriteitsvolgorde van volgorde worden gemaakt om de AD te omvatten die ISE zal gebruiken om te controleren op authenticatie.

Voer de volgende stappen uit:

1. Ga van ISE naar **Administration > Identity Management > Identity Source Sequences**.



2. Klik op **+Add** om een nieuwe reeks toe te voegen.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Guest Management'. The 'Identity Source Sequences' page is active, showing a table of existing sequences. The 'Add' button is highlighted with a yellow box and a red arrow pointing to it.

Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

3. Voer de nieuwe naam in: **AD_Internal**. Voeg alle beschikbare bronnen toe aan het geselecteerde veld. Vervolgens kunt u de volgorde zo nodig wijzigen, zodat AD1 naar boven in de lijst wordt verplaatst. Klik op **Verzenden**.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > New Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
	AD1 Internal Users Internal Endpoints

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. Bevestig dat de volgorde aan de lijst is toegevoegd.

CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences

Edit Add Duplicates Delete Filter

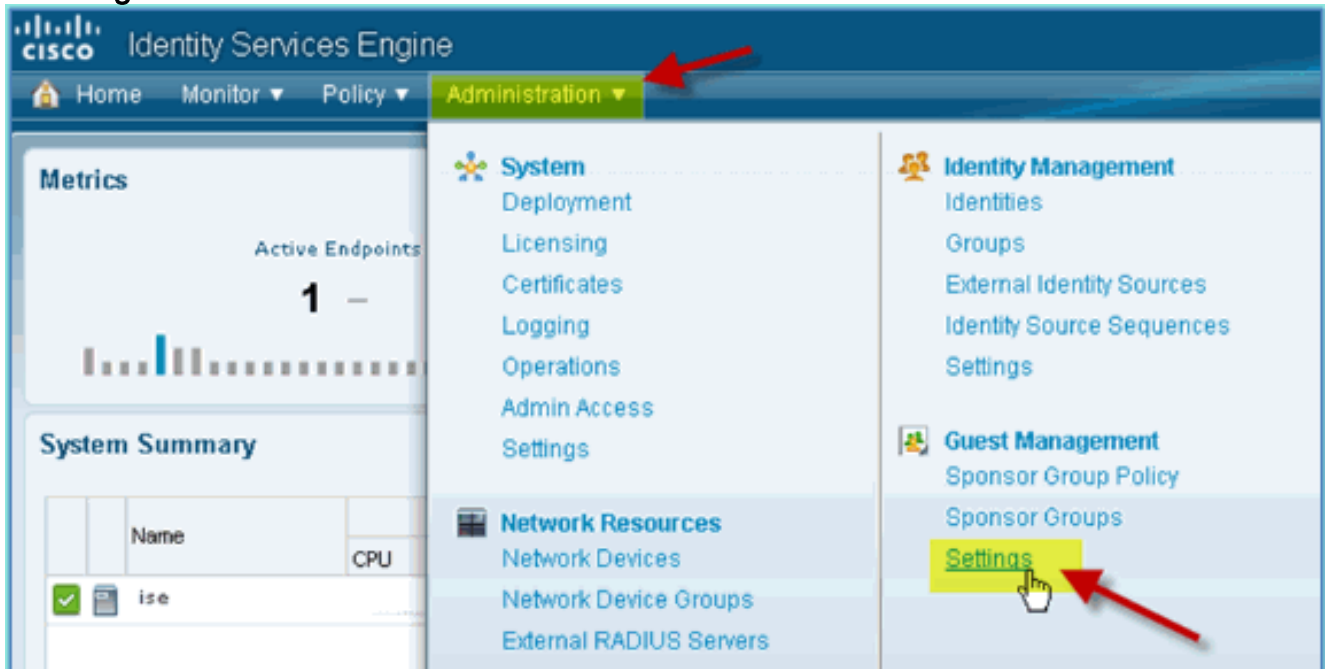
Name	Description	Identity Stores
AD_Internal		AD1, Internal Endpoints, Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

ISE draadloze gesponsorde gasttoegang met geïntegreerde AD

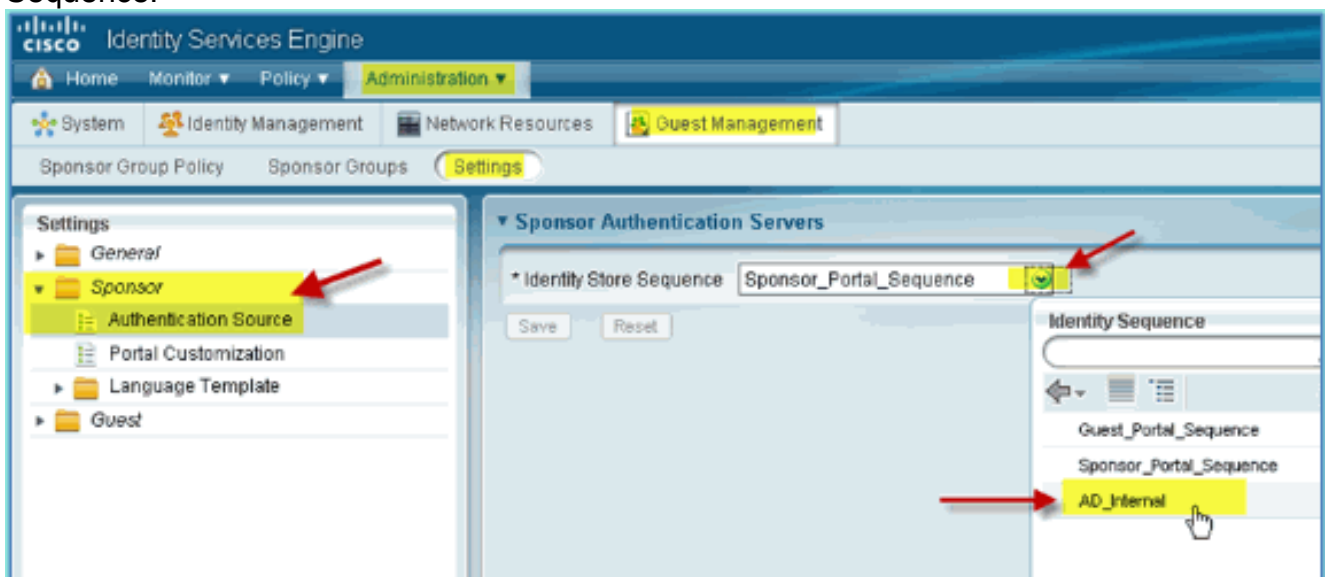
ISE kan zo worden geconfigureerd dat gasten kunnen worden gesponsord met beleid zodat AD-domeingebruikers gasttoegang kunnen sponsoren.

Voer de volgende stappen uit:

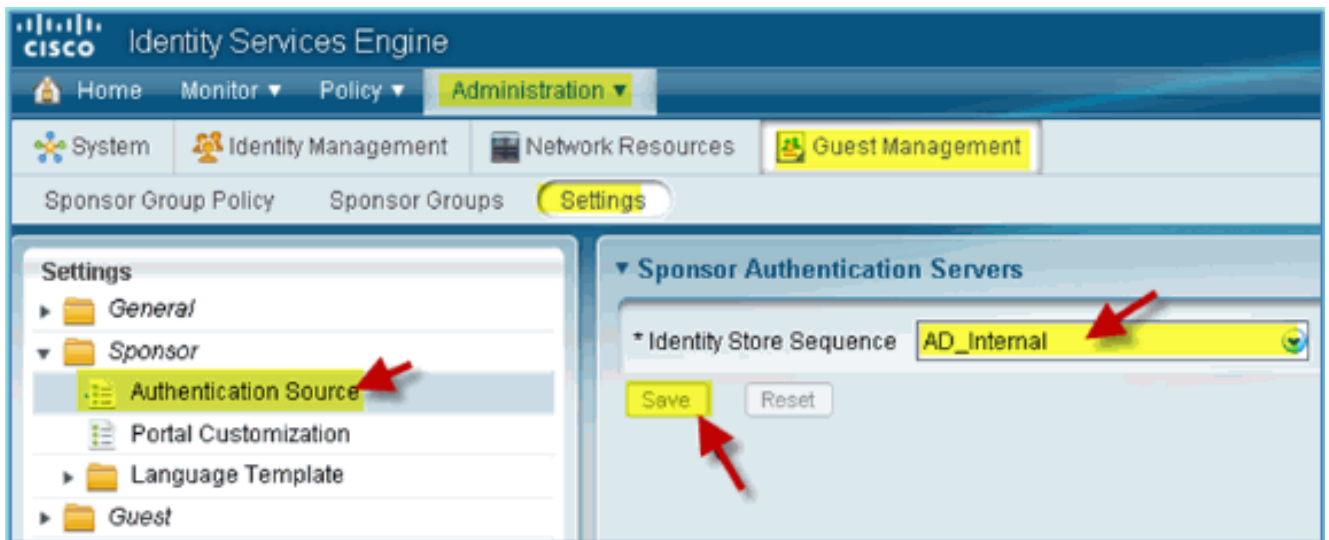
1. Ga van ISE naar **Administration > Guest Management > Instellingen**.



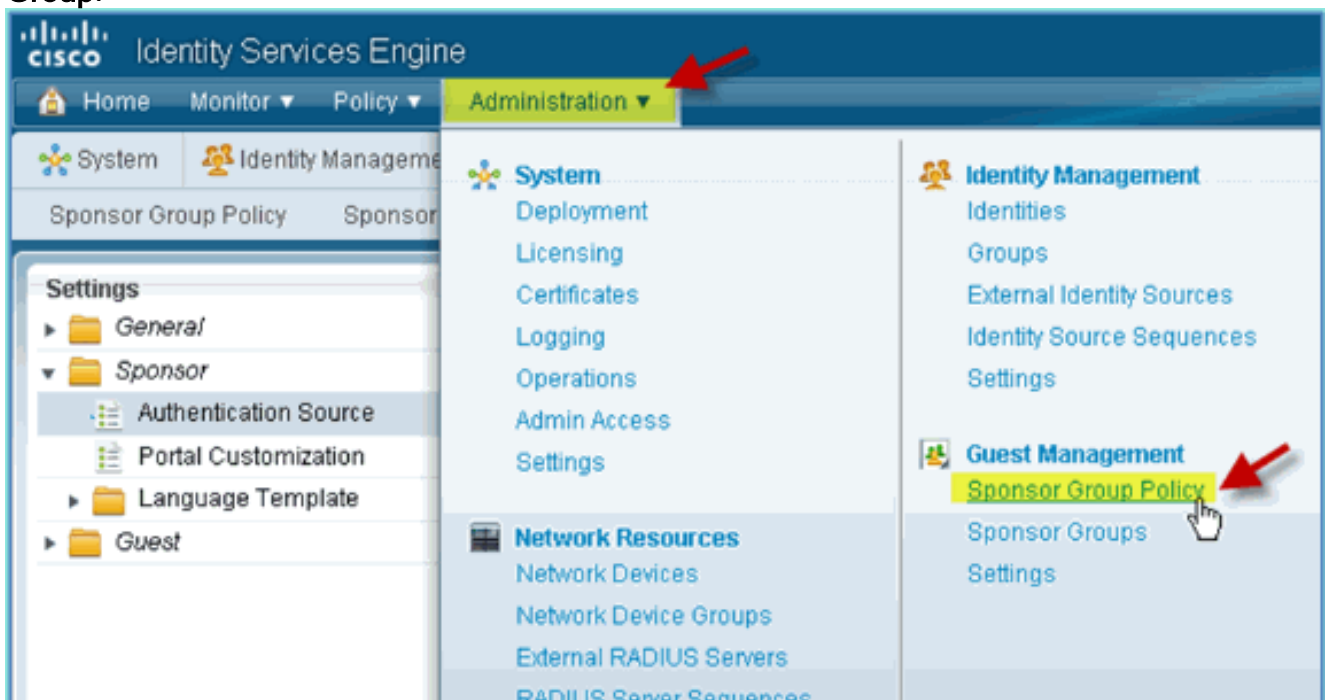
2. **Sponsor** uitvouwen en op **verificatiebron** klikken. Selecteer vervolgens **AD_Internal** als Identity Store Sequence.



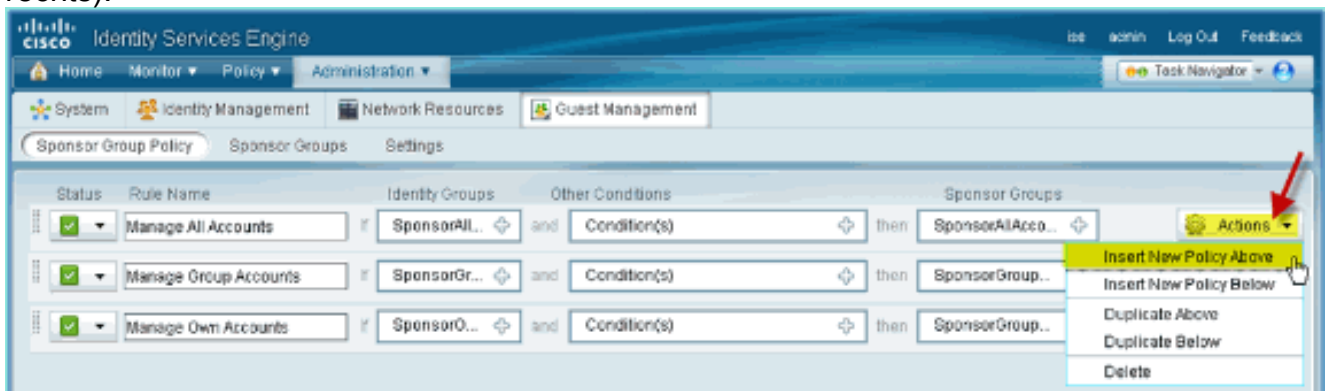
3. Bevestig **AD_Internal** als de Identity Store Sequence. Klik op **Save** (Opslaan).



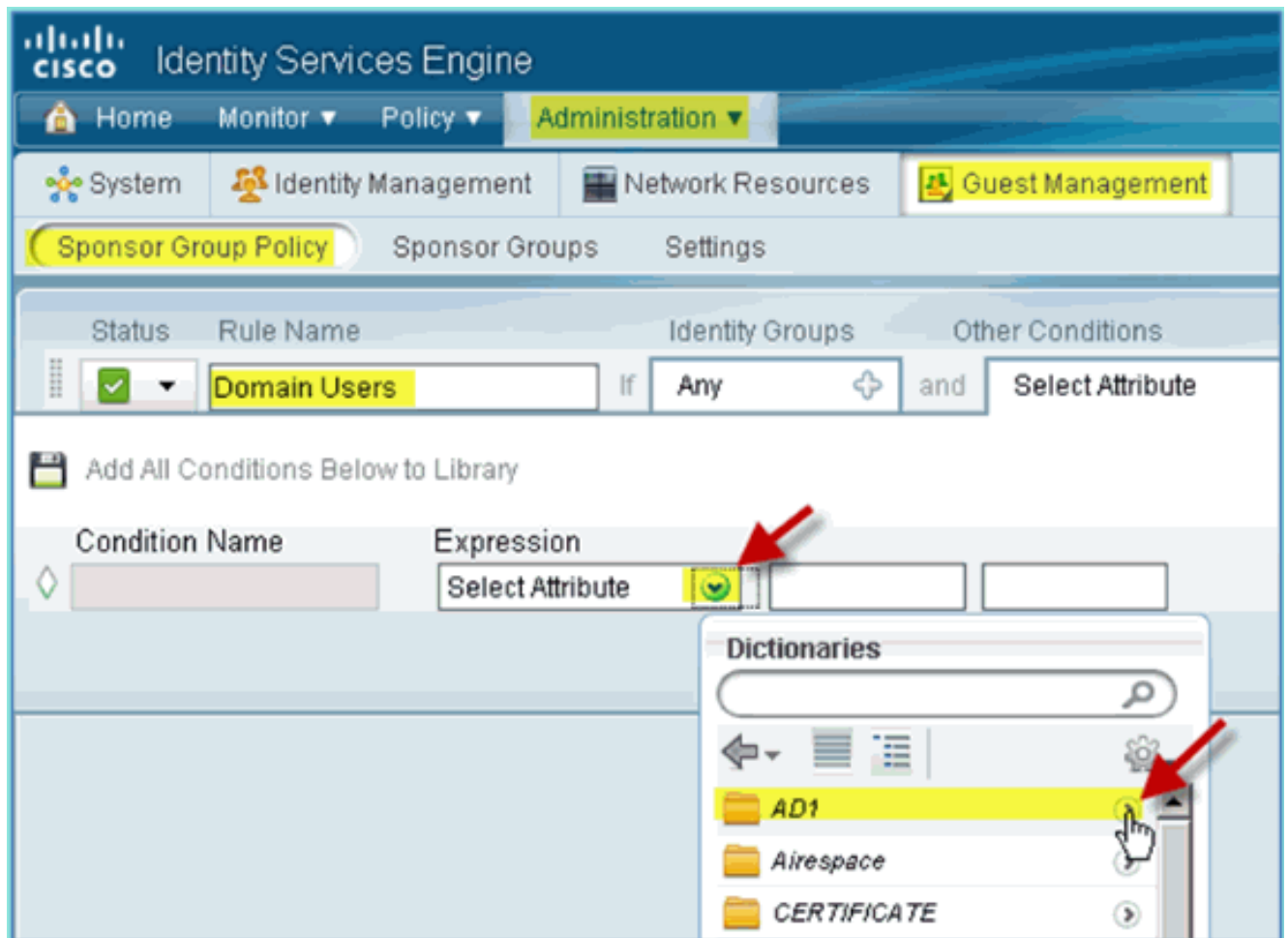
4. Ga naar **Beheer > Gastenbeheer > Beleid voor Sponsor Group**.



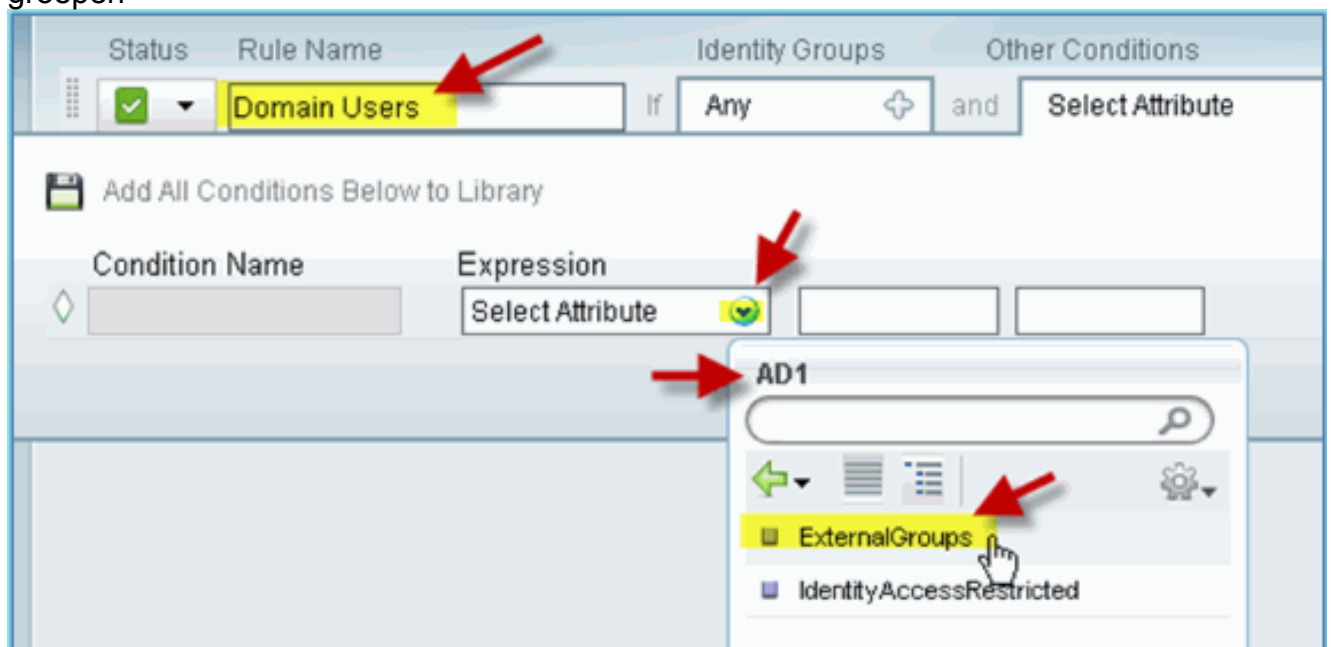
5. Voeg nieuw beleid toe boven de eerste regel (klik op het pictogram **Acties** rechts).



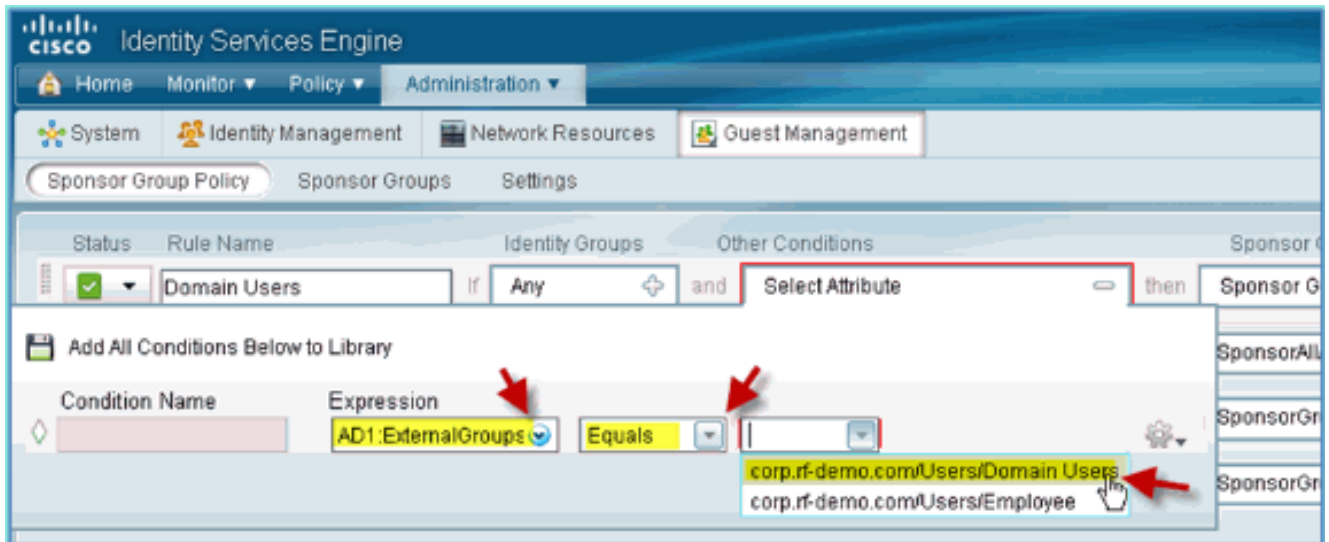
6. Voor het nieuwe beleid van de Groep van de Sponsor, creëer het volgende: Regel Naam: DomeingebruikersIdentiteitsgroepen: alleAndere voorwaarden: (Nieuw/Geavanceerd maken) > AD1



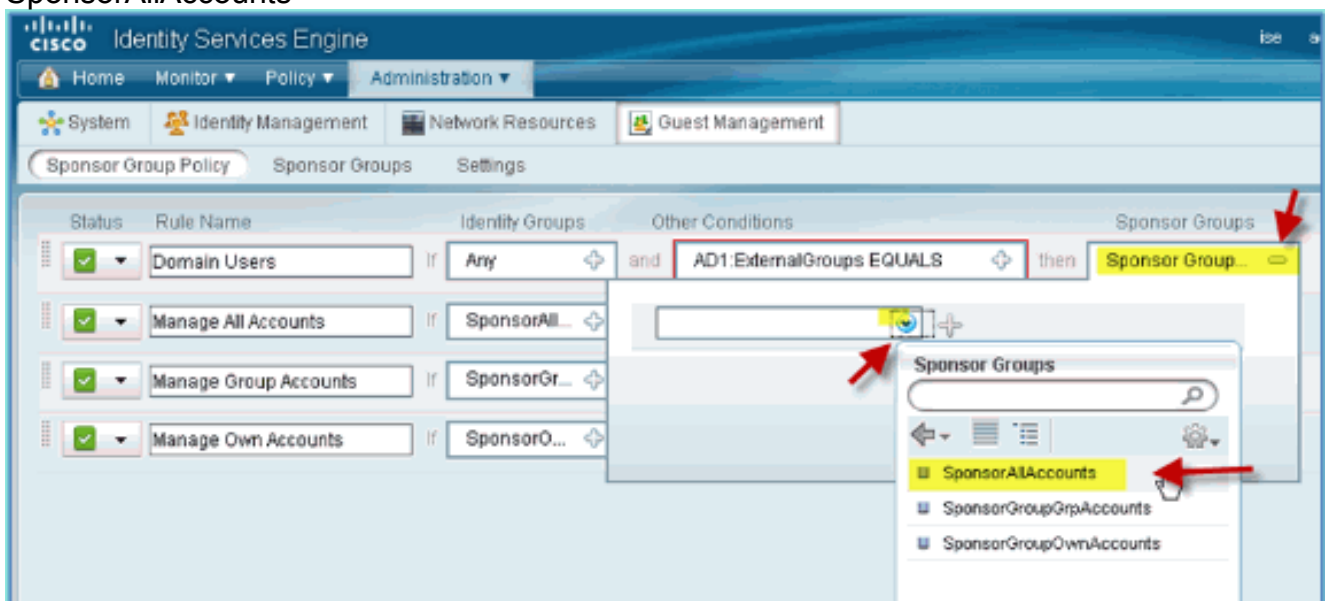
AD1: Externe groepen



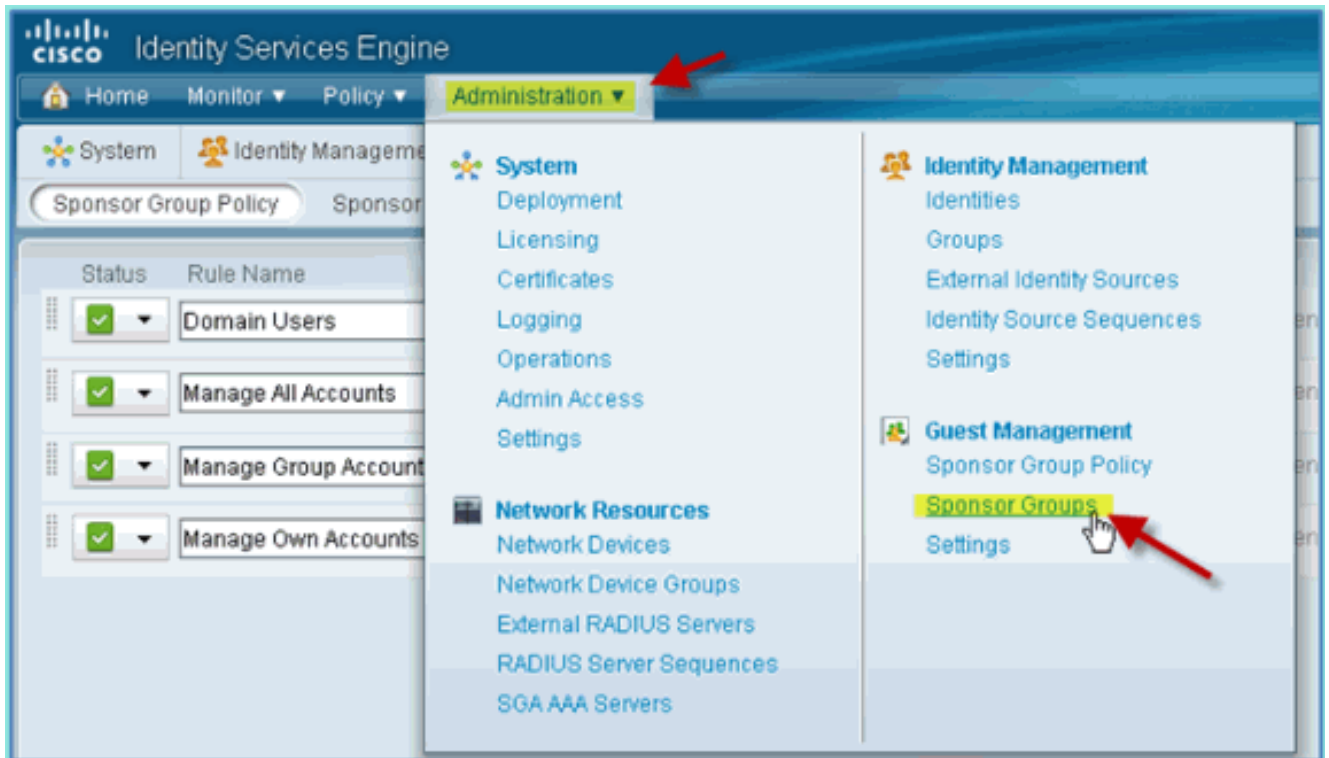
AD1 Externe Groepen > Gelijk > corp.rf-demo.com/Users/Domain Gebruikers



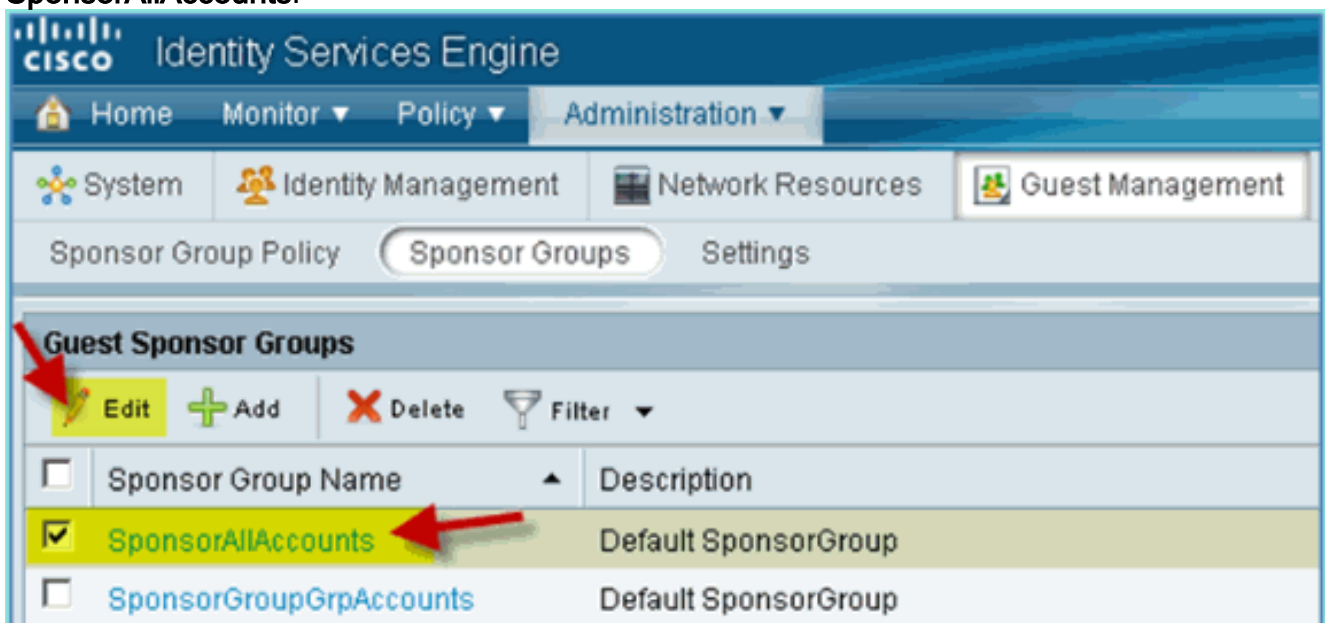
7. Stel in sponsorgroepen het volgende in: SponsorAllAccounts:
SponsorAllAccounts



8. Ga naar **Beheer > Gastenbeheer > Sponsor Groepen**.



9. Selecteer Bewerken > SponsorAllAccounts.



10. Selecteer Autorisatieniveaus en stel het volgende in: Wachtwoord voor gasten weergeven: Ja

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

General Authorization Levels Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Save Reset

[SPAN op de Switch configureren](#)

Configureer de SPAN - ISE-interface met mgt/sonde is L2 naast de WLC-beheerinterface. De switch kan aan SPAN en andere interfaces, zoals werknemer en gastinterface VLAN's worden geconfigureerd.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

[Referentie: Draadloze verificatie voor Apple MAC OS X](#)

Koppel aan de WLC via een geverifieerde SSID als een INTERNE gebruiker (of geïntegreerd, AD-

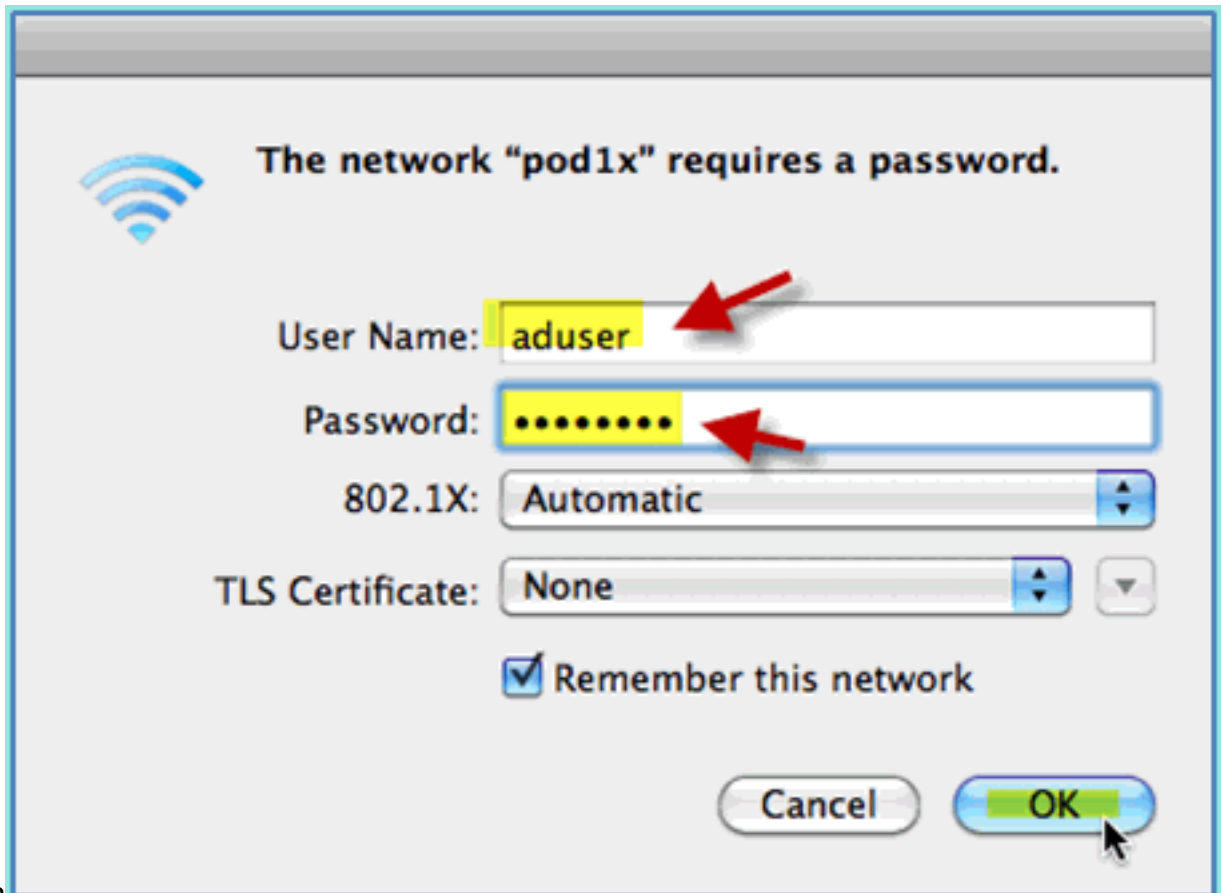
gebruiker) met behulp van een draadloze laptop van Apple Mac OS X. Sla over indien niet van toepassing.

1. Ga op een Mac naar de WLAN-instellingen. Schakel WIFI in en selecteer vervolgens de 802.1X-compatibele POD-SSID die in de vorige oefening is



gemaakt.

2. Geef de volgende informatie om verbinding te maken: Gebruikersnaam: aduser (bij gebruik van AD), werknemer (intern - werknemer), contractant (intern - contractant) Wachtwoord: XXXX802.1X: automatisch TLS-certificaat:

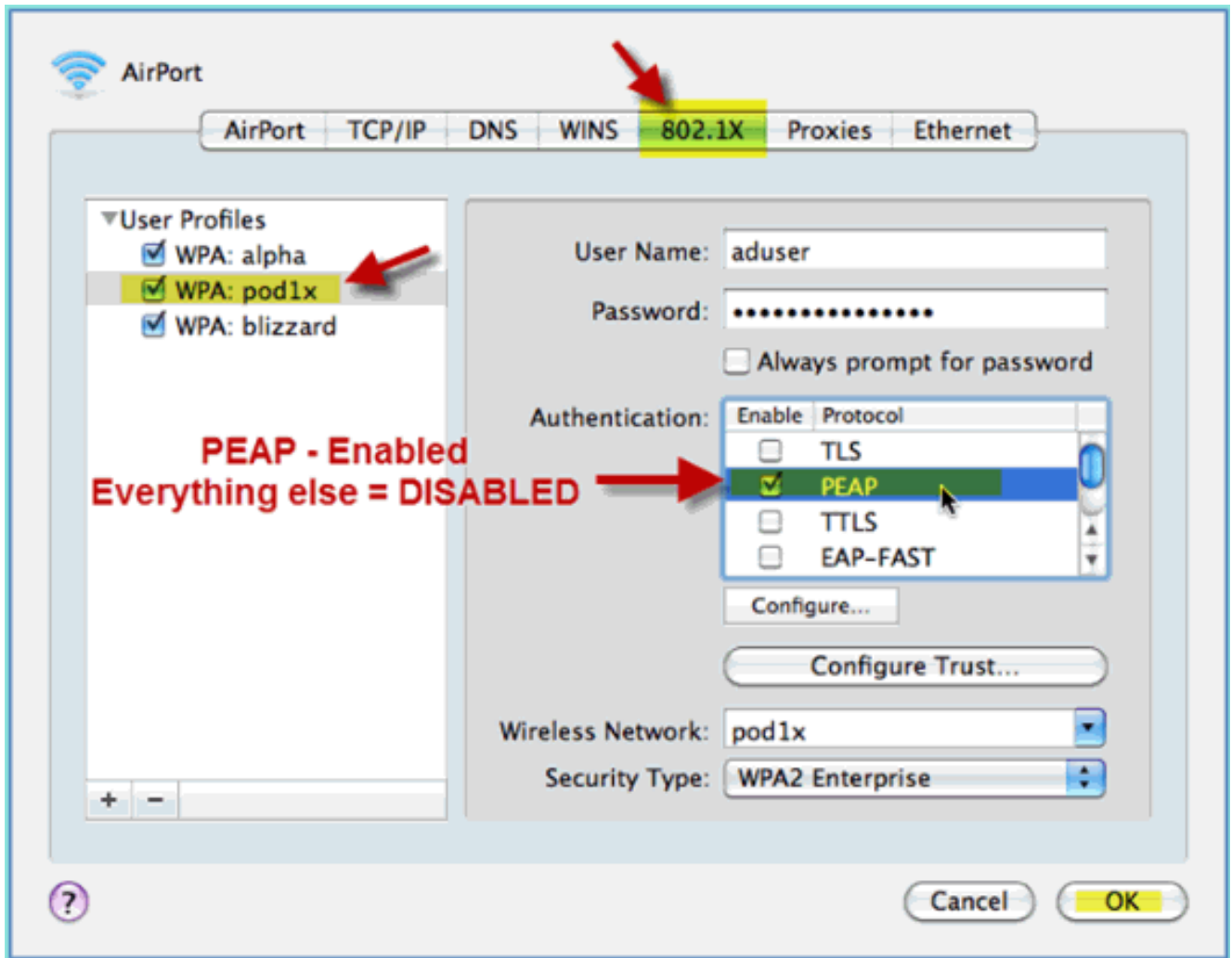


geen

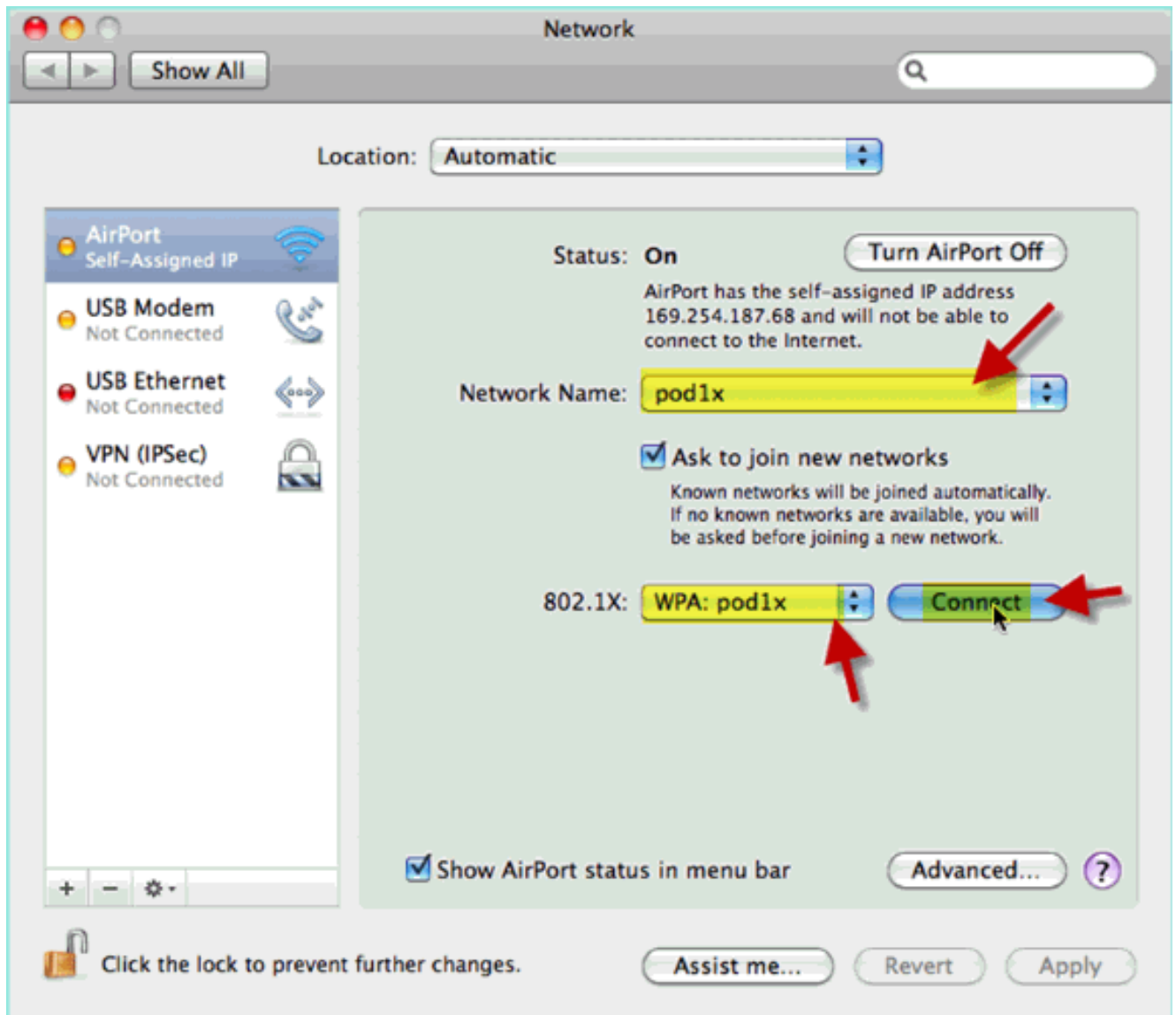
p dat moment maakt de laptop mogelijk geen verbinding. Bovendien kan ISE als volgt een mislukte gebeurtenis uitzenden:

```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of  
an unknown CA in the client certificates chain
```

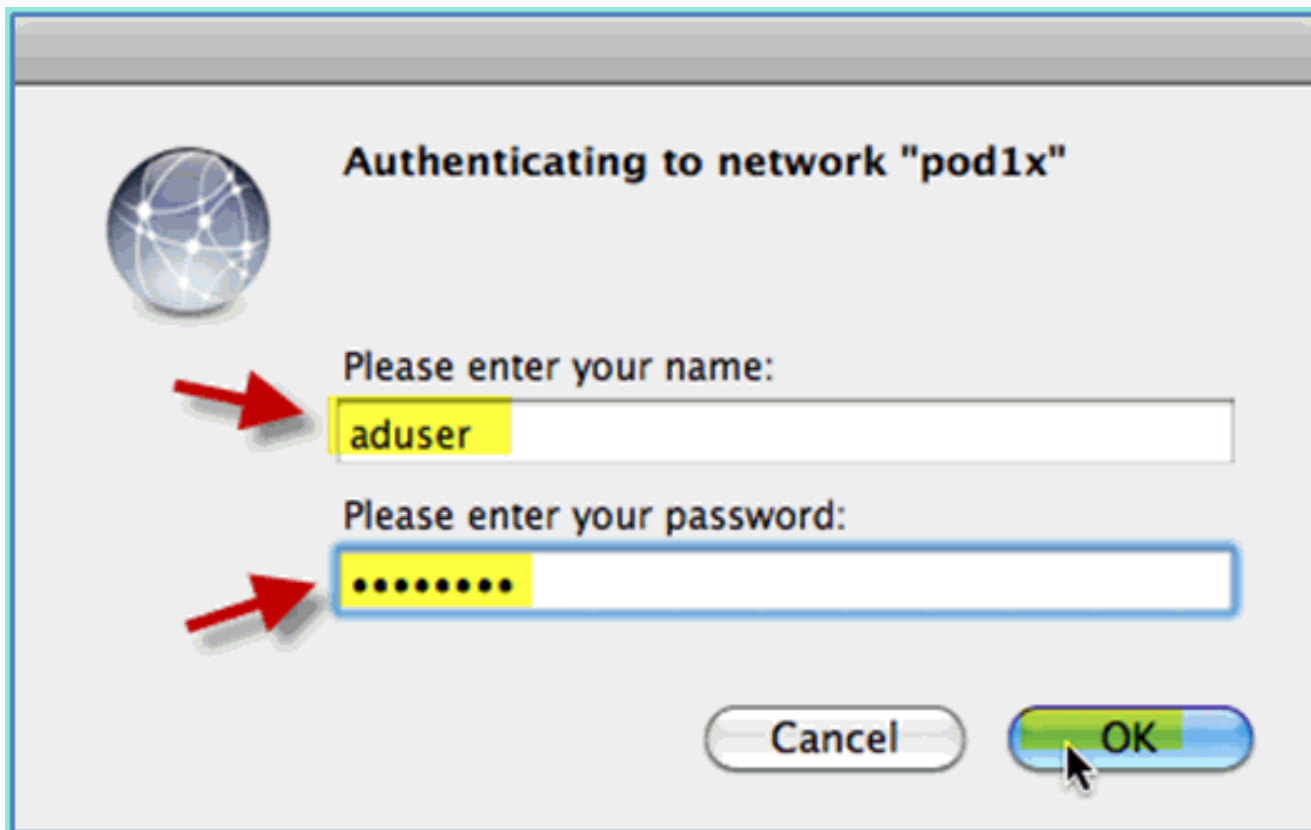
3. Ga naar de **Systeemvoorkeur > Netwerk > Luchthaven > 802.1X** instelling en stel de nieuwe POD SSID/WPA-profielverificatie in als:
TLS: Uitgeschakeld
PEAP: ingeschakeld
TTLS:
Uitgeschakeld
EAP-FAST:
uitgeschakeld



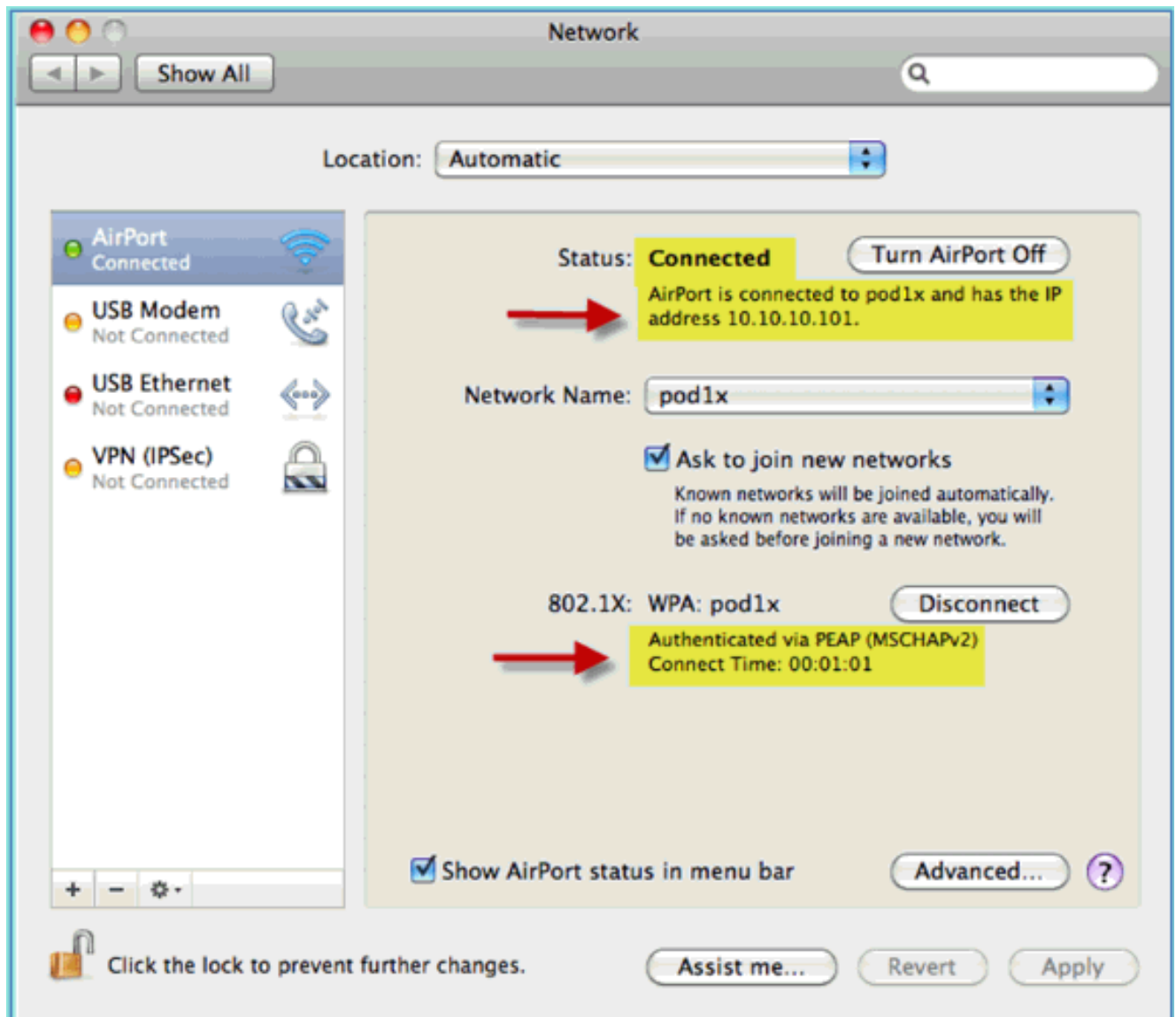
4. Klik op **OK** om door te gaan en toe te staan dat de instelling wordt opgeslagen.
5. Selecteer in het netwerkscherm het juiste SSID + 802.1X WPA-profiel en klik op **Verbinden**.



6. Het systeem kan vragen om een gebruikersnaam en wachtwoord. Voer de AD-gebruiker en het wachtwoord in (aduser/XXXX) en klik vervolgens op OK.



De client dient **Connected** via PEAP met een geldig IP-adres te tonen.

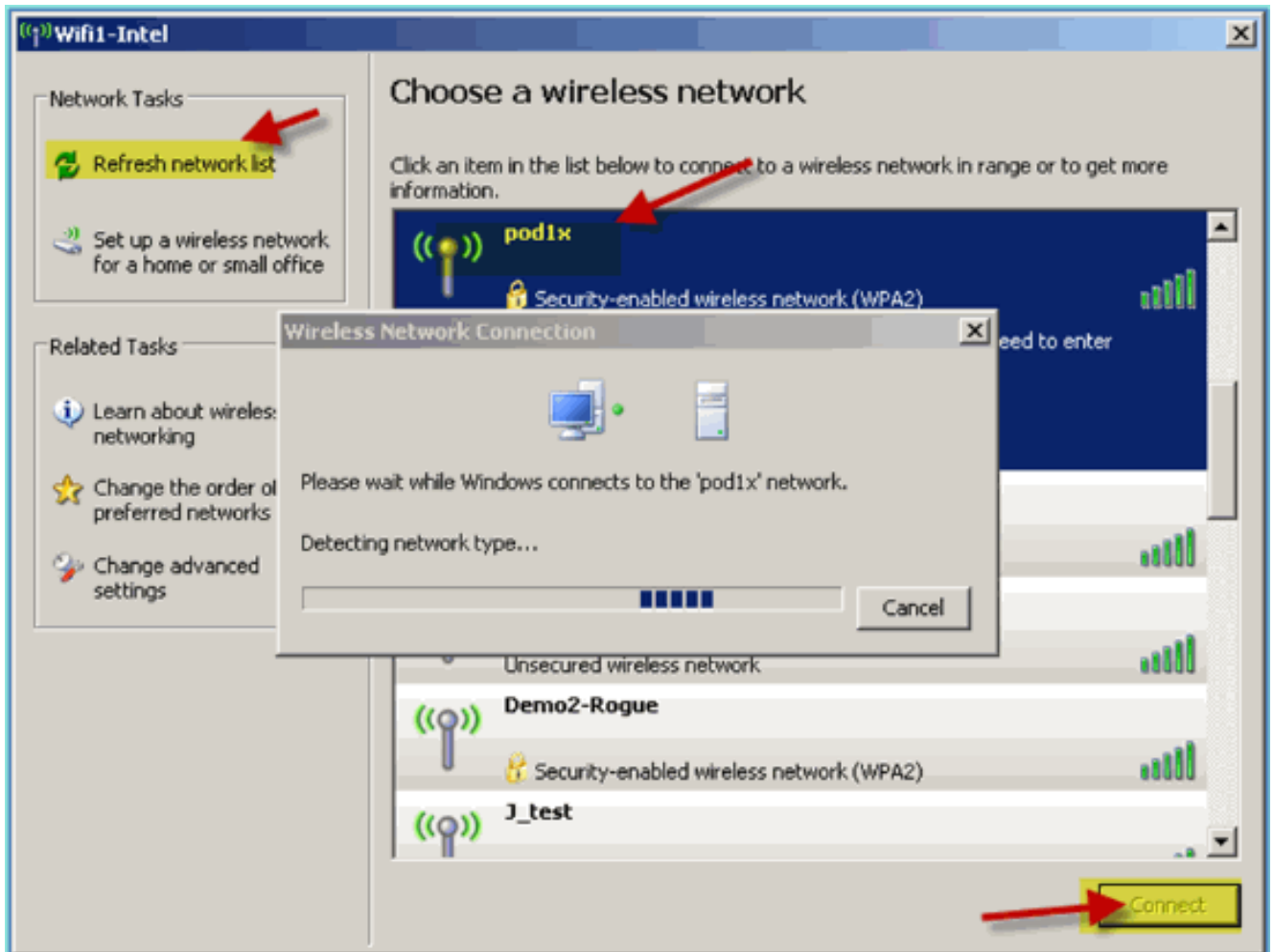


Referentie: Draadloze verificatie voor Microsoft Windows XP

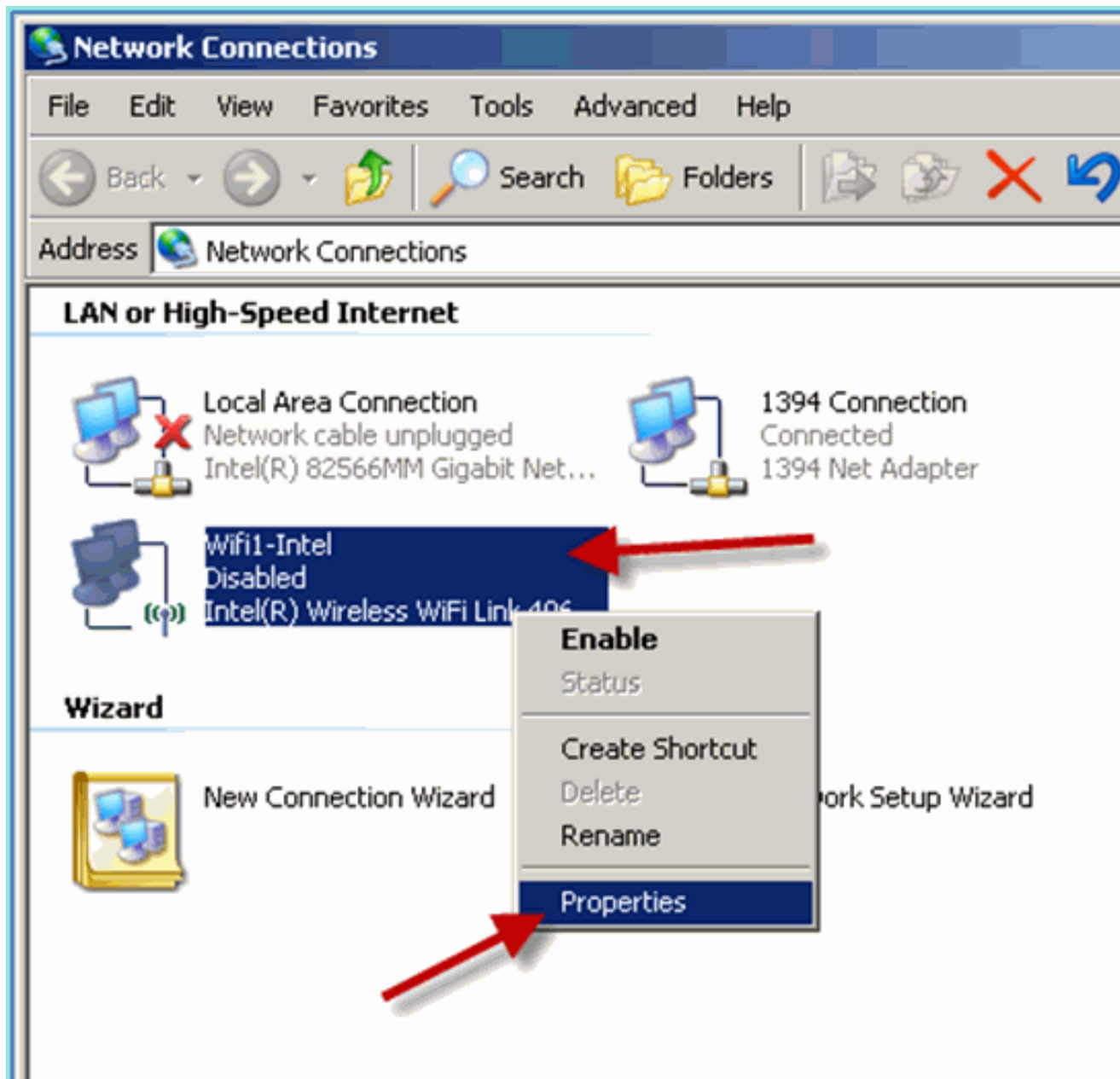
Koppel aan de WLC via een geverifieerde SSID als een INTERNE gebruiker (of geïntegreerd, AD-gebruiker) met behulp van een draadloze Windows XP-laptop. Sla over indien niet van toepassing.

Voer de volgende stappen uit:

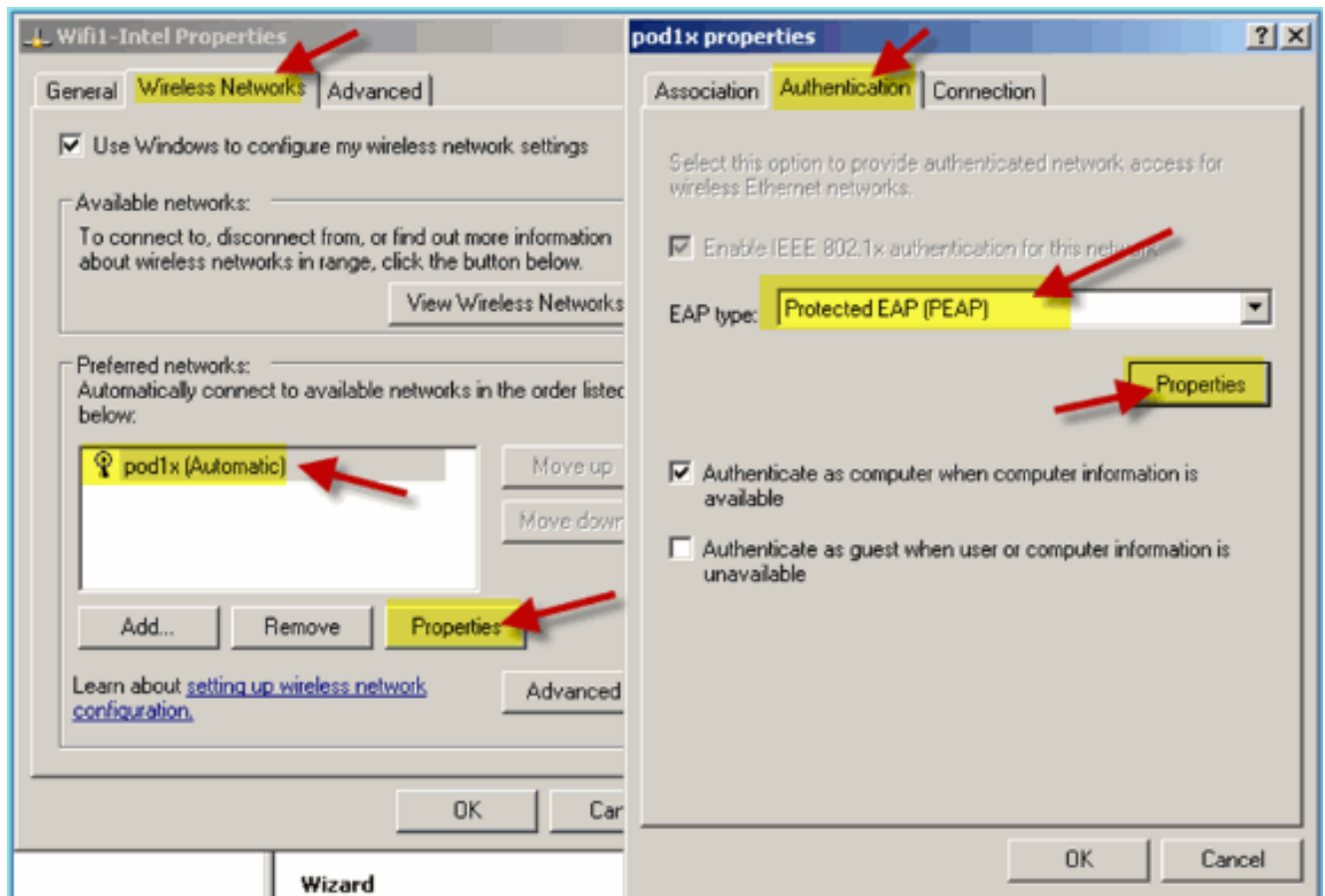
1. Ga op de laptop naar de WLAN-instellingen. Schakel WIFI in en maak verbinding met de 802.1X-compatibele POD-SSID die in de vorige oefening is gemaakt.



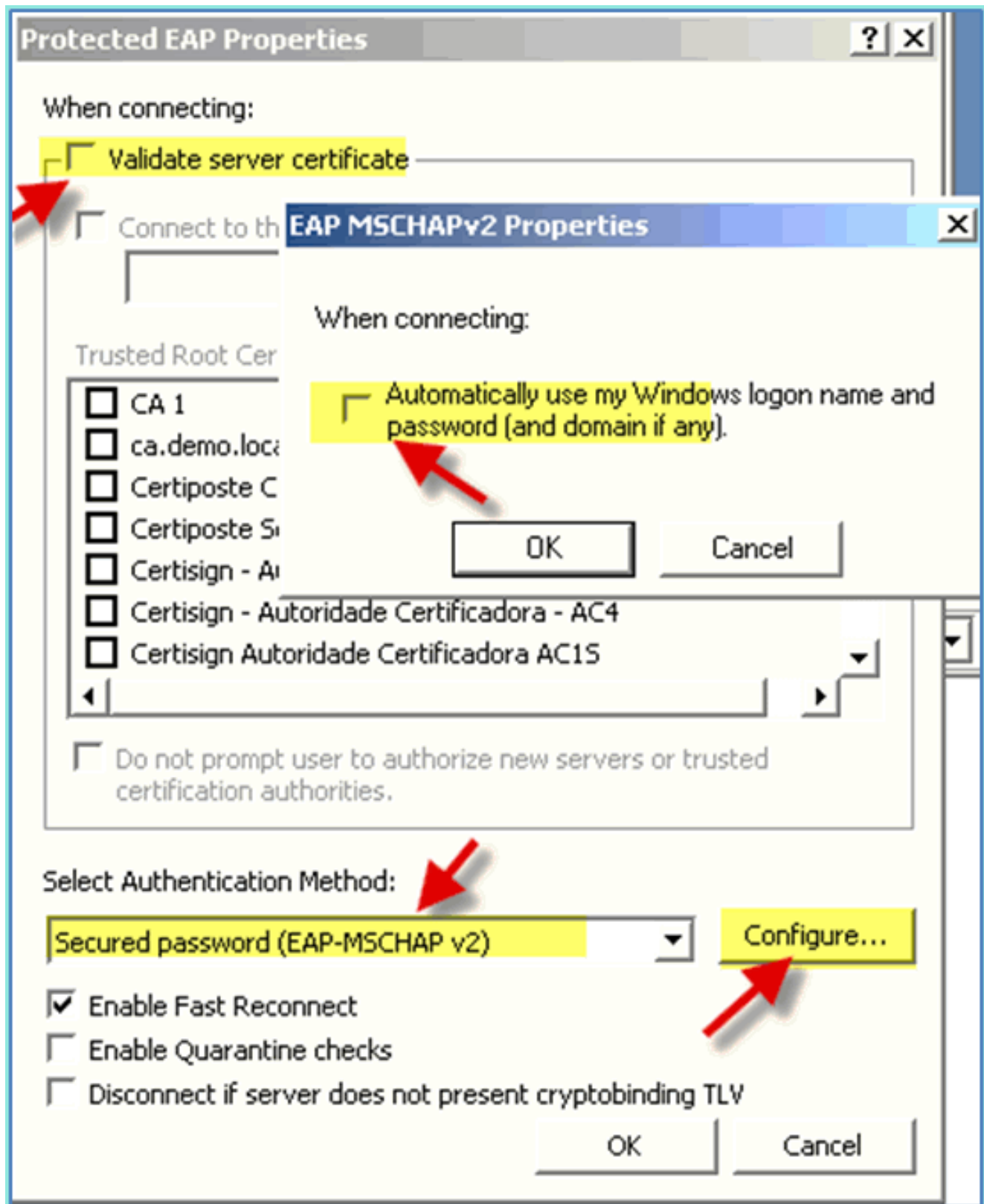
2. Toegang tot de netwerkeigenschappen van de WIFI-interface.



3. Ga naar het tabblad **Draadloze netwerken**. Selecteer de netwerkeigenschappen van de peul SSID > tabblad Verificatie > EAP-type = beschermde EAP (PEAP).



4. Klik op de EAP Properties.
5. Stel het volgende in: Servercertificaat valideren: uitgeschakeld Verificatiemethode: beveiligd wachtwoord (EAP-MSCHAP v2)

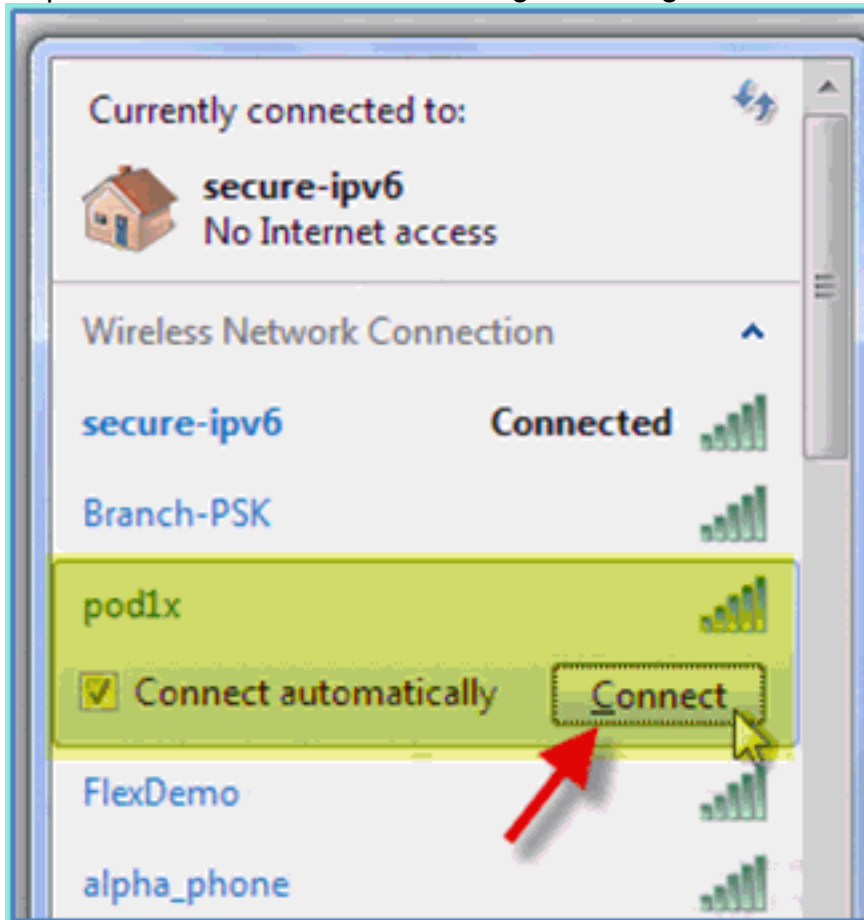


6. Klik op OK in alle vensters om deze configuratietask te voltooien.
7. Windows XP-client vraagt om gebruikersnaam en wachtwoord. In dit voorbeeld is het aduser/XXXX.
8. Bevestig netwerkconnectiviteit, IP-adressering (v4).

[Referentie: Draadloze verificatie voor Microsoft Windows 7](#)

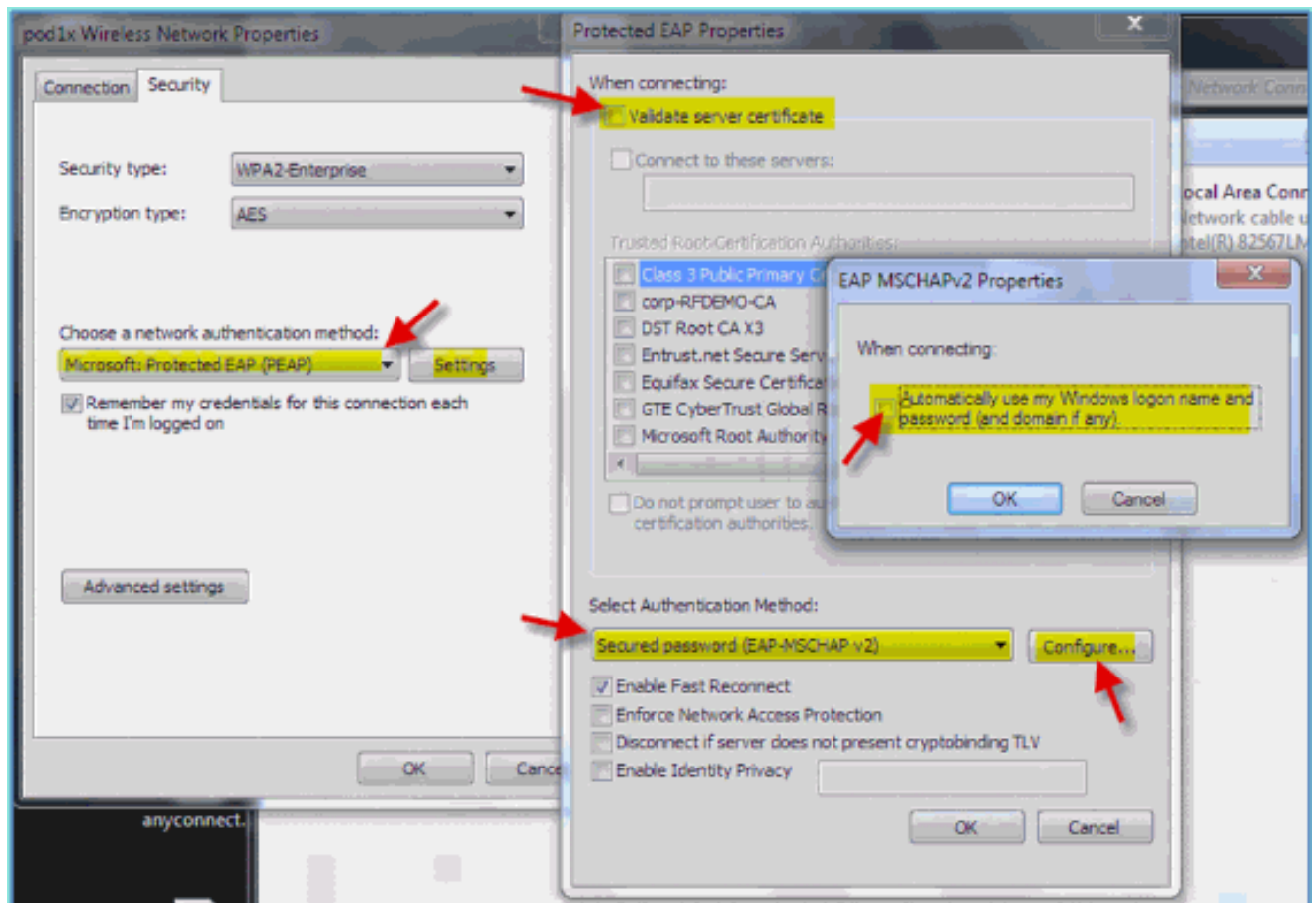
Koppel aan de WLC via een geverifieerde SSID als een INTERNE gebruiker (of geïntegreerd, AD-gebruiker) met behulp van een Windows 7 draadloze laptop.

1. Ga op de laptop naar de WLAN-instellingen. Schakel WIFI in en maak verbinding met de 802.1X-compatibele POD-SSID die in de vorige oefening is



gemaakt.

2. Ga naar de Wireless Manager en bewerk het nieuwe draadloze profiel van de POD.
3. Stel het volgende in:
Verificatiemethode: PEAP
Othoud mijn referenties...:
Uitgeschakeld
Servercertificaat valideren (geavanceerde instelling):
uitgeschakeld
Verificatiemethode (adv.-instelling): EAP-MSCHAP v2
Automatisch mijn
Windows-aanmelding gebruiken...:
Uitgeschakeld



[Gerelateerde informatie](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.