

Configureren van Central Web Verification (CWA) op Catalyst 9800 WLC en ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[AAA-configuratie op 9800 WLC](#)

[WLAN-configuratie](#)

[Configuratie van beleidsprofiel](#)

[Configuratie van beleidstag](#)

[Toewijzing van beleidstags](#)

[Configuratie ACL-omleiding](#)

[Omleiding voor HTTP of HTTPS inschakelen](#)

[ISE-configuratie](#)

[De 9800 WLC toevoegen aan ISE](#)

[Nieuwe gebruiker maken op ISE](#)

[Autorisatieprofiel maken](#)

[Verificatieregel configureren](#)

[Autorisatieregels configureren](#)

[Alleen FlexConnect lokale switching-access points](#)

[Certificaten](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Checklist](#)

[Ondersteuning van servicepoort voor RADIUS](#)

[Debugs verzamelen](#)

[Voorbeelden](#)

Inleiding

Dit document beschrijft hoe u een draadloos LAN van de CWA kunt configureren op een Catalyst 9800 WLC en ISE.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met de configuratie van 9800 draadloze LAN-controllers (WLC).

Gebruikte componenten

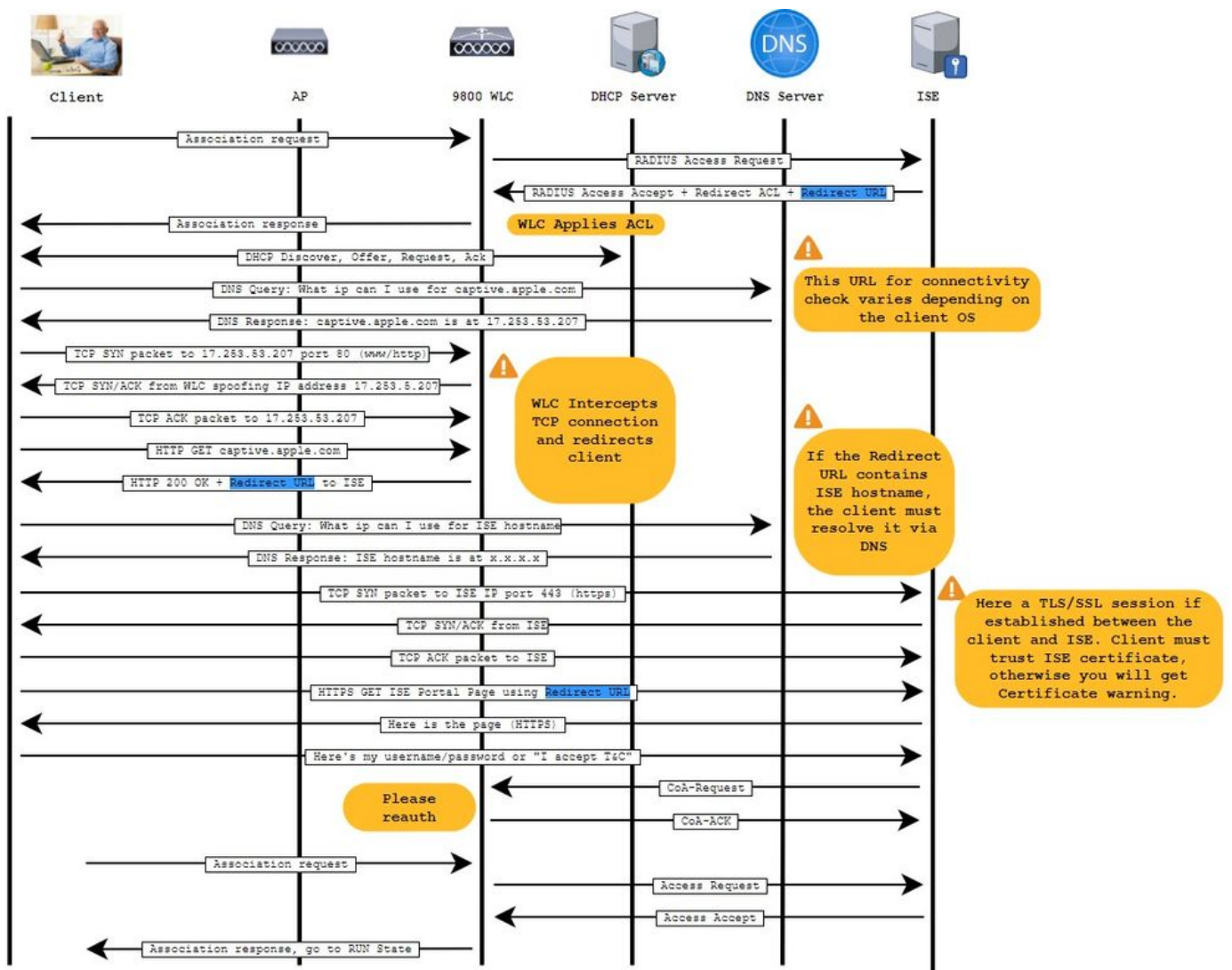
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 980 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

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

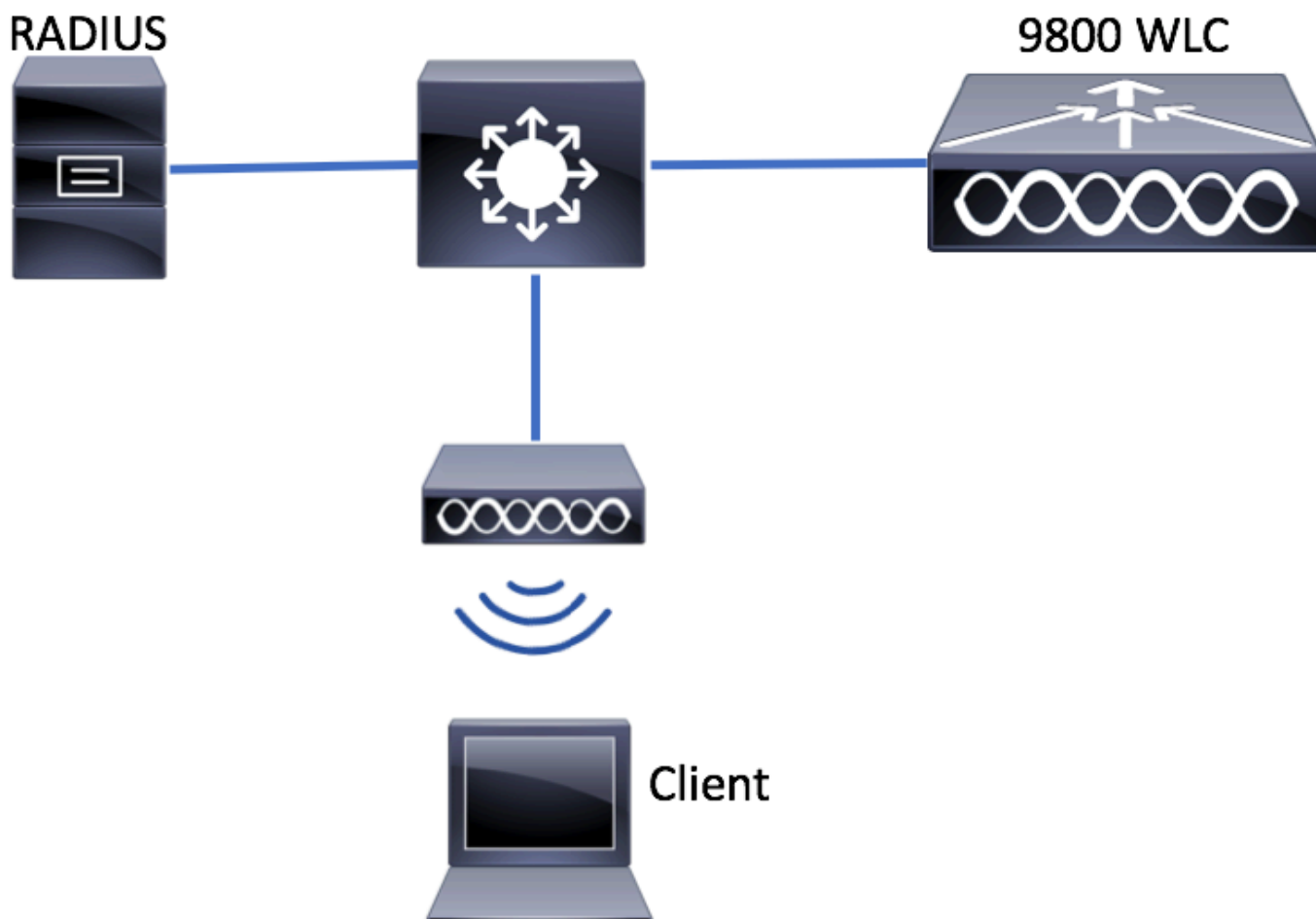
Achtergrondinformatie

Het CWA-proces wordt hier getoond waar u het CWA-proces van een Apple-apparaat als voorbeeld kunt zien:



Configureren

Netwerkdigram



AAA-configuratie op 9800 WLC

Stap 1. Voeg de ISE-server toe aan de 9800 WLC-configuratie.

Navigeer naar Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add en voer de RADIUS-serverinformatie in zoals in de afbeeldingen.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Address
0	

10 items per page

Zorg ervoor dat ondersteuning voor CoA is ingeschakeld als u van plan bent om in de toekomst gebruik te maken van Central Web Verification (of een ander soort beveiliging die CoA vereist).

Create AAA Radius Server

Name* ISE-server

Server Address* [Redacted]

PAC Key

Key Type Clear Text

Key* [Redacted]

Confirm Key* [Redacted]

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

CoA Server Key Type Clear Text

CoA Server Key [Redacted]

Confirm CoA Server Key [Redacted]

Automate Tester

Cancel Apply to Device



Opmerking: Zorg er bij versie 17.4.X en hoger voor dat u de CoA-servertoets ook configureert wanneer u de RADIUS-server configureert. Gebruik dezelfde sleutel als het gedeelde geheim (deze zijn standaard hetzelfde bij ISE). Het doel is om optioneel een andere sleutel voor CoA dan het gedeelde geheim te configureren als dat is wat uw RADIUS-server heeft geconfigureerd. In Cisco IOS XE 17.3 gebruikte de web-UI gewoon hetzelfde gedeelde geheim als de CoA-toets.

Stap 2. Maak een lijst met autorisatiemethoden.

Navigeren naar Configuration > Security > AAA > AAA Method List > Authorization > + Add zoals in de afbeelding.

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

+ Add **x Delete**

Name	Type	Group Type	Group
<input type="checkbox"/> default	network	local	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Fallback to local

Authenticated

Available Server Groups **Assigned Server Groups**

ldap
tacacs+

radius

Stap 3. (Optioneel) Maak een lijst met boekhoudmethoden zoals in de afbeelding.

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

+ AAA Wizard

AAA Method List

Servers / Groups

General

Authentication

Authorization

Accounting

+ Add

x Delete

Name

0

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups

Assigned Server Groups

ldap
tacacs+

radius

Cancel

Apply to Device

Opmerking: CWA werkt niet als u besluit de taakverdeling (vanaf de Cisco IOS XE CLI-configuratie) voor uw radiusservers in te stellen vanwege Cisco bug-id [CSCvh03827](#). Het gebruik van externe lastverdelers is prima. Zorg er echter voor dat de taakverdeler per client werkt met behulp van het RADIUS-kenmerk call-station-id. Het vertrouwen op UDP-bronpoort is geen ondersteund mechanisme voor het in evenwicht brengen van RADIUS-verzoeken van de 9800.

Stap 4. (Optioneel) U kunt het AAA-beleid definiëren om de SSID-naam te verzenden als een Calling-station-id attribuut, dat nuttig kan zijn als u later in het proces van deze voorwaarde op ISE wilt profiteren.

Navigeer naar Configuration > Security > Wireless AAA Policy en bewerk het standaard AAA-beleid of maak een nieuw beleid.

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪
⏩
1
⏪
⏩

10

items per page

U kunt kiezen SSID als optie 1. Vergeet niet dat zelfs wanneer u alleen SSID kiest, de aangeroepen station-id nog steeds het AP MAC-adres aan de SSID-naam toevoegt.

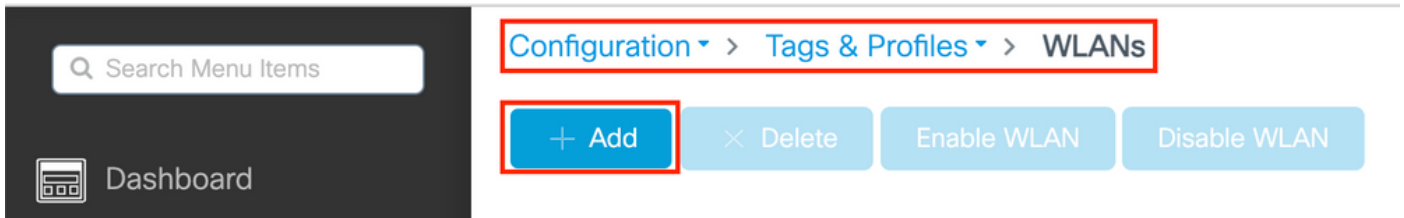
Edit Wireless AAA Policy

Policy Name*	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="default-aaa-policy"/>
Option 1	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="SSID"/>
Option 2	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="Not Configured"/>
Option 3	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="Not Configured"/>

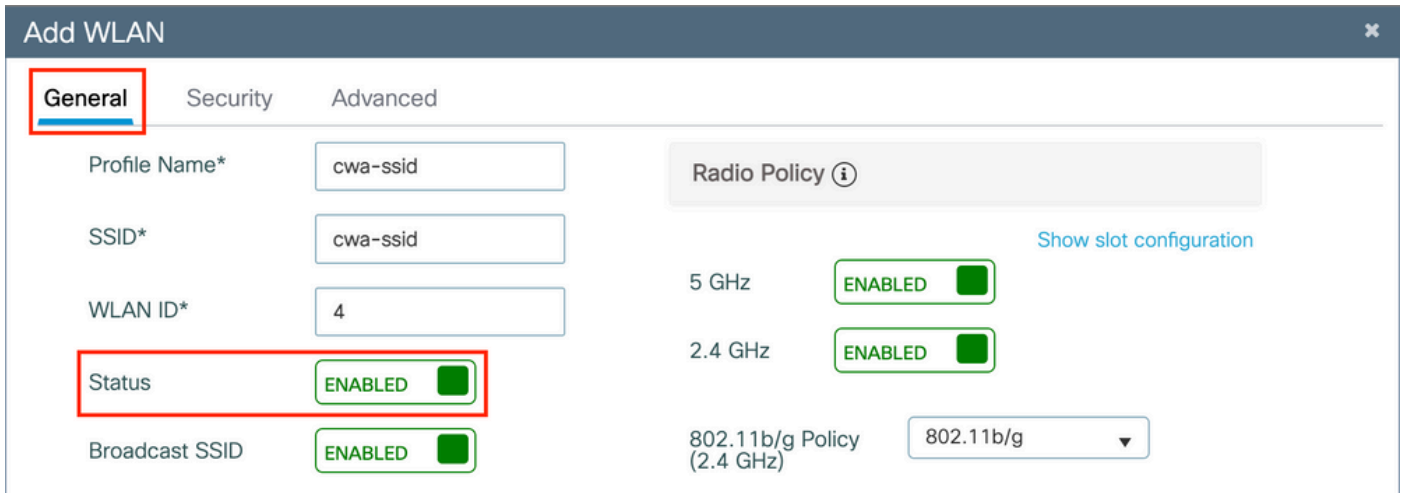
WLAN-configuratie

Stap 1. Maak het WLAN.

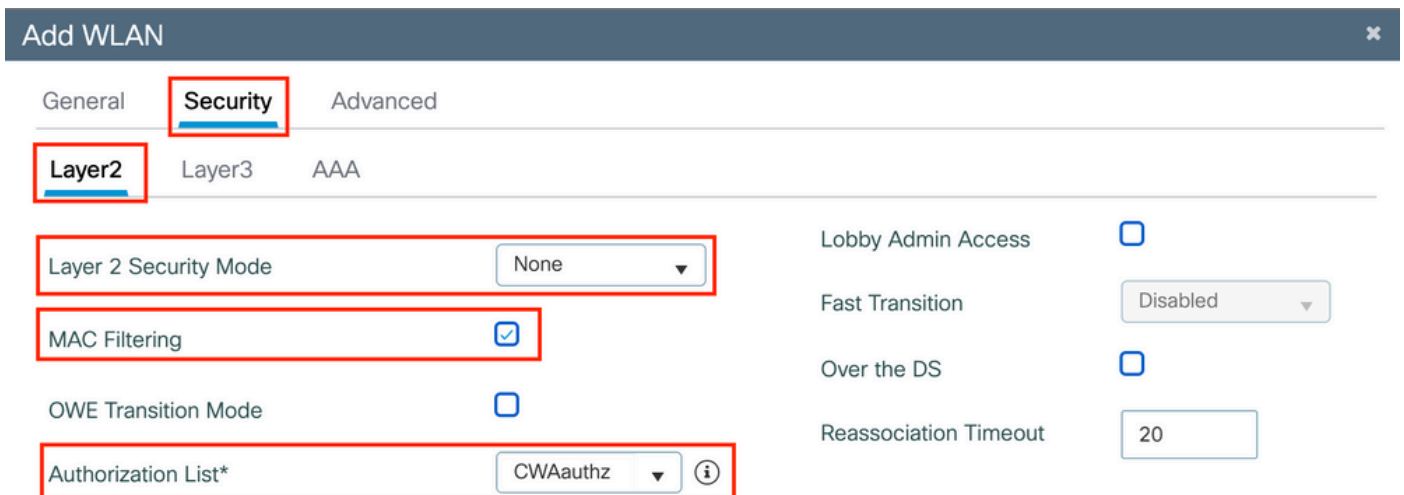
Navigeer naar Configuration > Tags & Profiles > WLANs > + Add en configureer het netwerk naar wens.



Stap 2. Voer de algemene informatie over WLAN in.



Stap 3. Navigeer naar het Security tabblad en kies de gewenste beveiligingsmethode. In dit geval zijn alleen 'MAC-filtering' en de AAA-autorisatielijst (die u in Stap 2. in de AAA Configuration sectie hebt aangemaakt) nodig.



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

(config-wlan)#no security wpa wpa2 ciphers aes

(config-wlan)#no security wpa akm dot1x

(config-wlan)#no shutdown

Configuratie van beleidsprofiel

Binnen een beleidsprofiel kunt u beslissen de clients toe te wijzen aan wie VLAN, onder andere instellingen (zoals ACL's (toegangscontrolelijst), Quality of Service (QoS), mobiliteitsanker, timers enzovoort).

U kunt uw standaardbeleidsprofiel gebruiken of u kunt een nieuw profiel maken.

GUI:

Stap 1. Maak een nieuwe Policy Profile.

Navigeer naar Configuration > Tags & Profiles > Policy en configureer uw default-policy-profile of maak een nieuwe.

Policy Profile

+ Add x Delete

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

1 10 items per page

Zorg ervoor dat het profiel is ingeschakeld.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Stap 2. Kies VLAN.

Navigeer naar het Access Policies tabblad en kies de VLAN-naam in de vervolgkeuzelijst of typ handmatig de VLAN-ID. Configureer geen ACL in het beleidsprofiel.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Stap 3. Configureer het beleidsprofiel om ISE-overschrijvingen te accepteren (AAA-overschrijding toestaan) en wijziging van autorisatie (CoA) (NAC-status). U kunt optioneel ook een boekhoudingsmethode specificeren.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List ⓘ ✕

WGB Parameters

Broadcast Tagging

WGB VLAN

Policy Proxy Settings

ARP Proxy DISABLED

IPv6 Proxy

Fabric Profile

Link-Local Bridging

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

EoGRE Tunnel Profiles


Tunnel Profile

CLI:

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

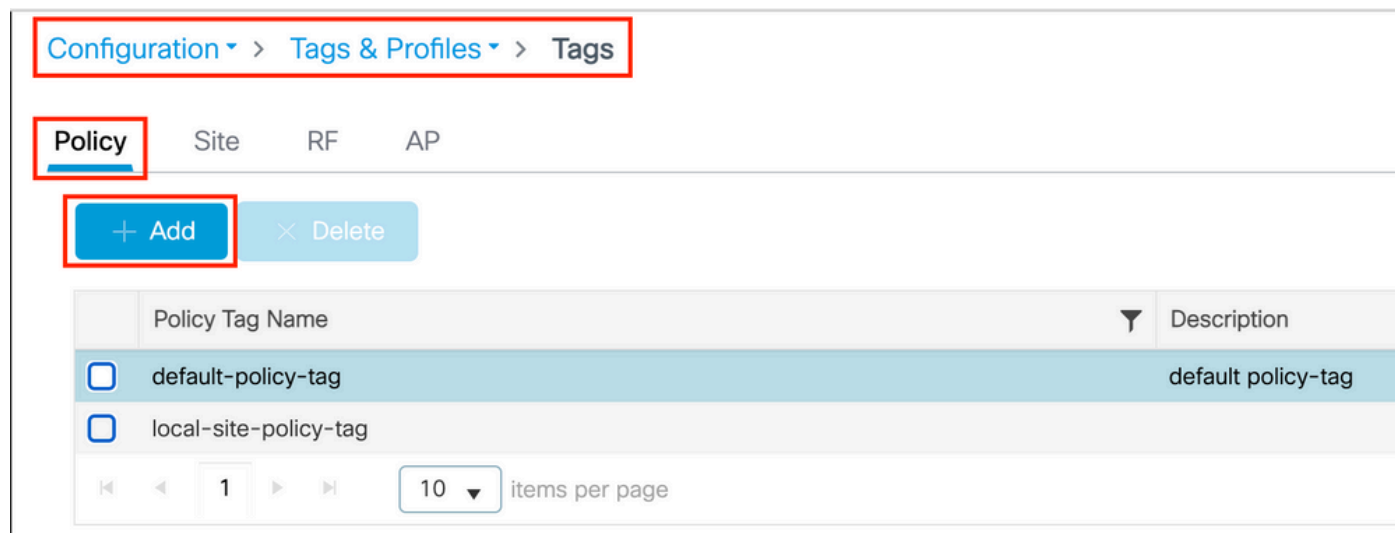
Configuratie van beleidstag

Binnen de Policy Tag is waar u uw SSID koppelt aan uw Policy Profile. U kunt een nieuwe Policy Tag maken of de standaard-policy tag gebruiken.

 **Opmerking:** De standaard-beleidstag brengt automatisch elke SSID met een WLAN-id tussen 1 en 16 in kaart aan het standaard-beleidsprofiel. Dit kan niet worden gewijzigd of verwijderd. Als u een WLAN met ID 17 of hoger hebt, kan de standaard-beleidstag niet worden gebruikt.

GUI:

Navigeer naar Configuration > Tags & Profiles > Tags > Policy en voeg indien nodig een nieuwe toe zoals in de afbeelding.



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

Policy Tag Name	Description
<input type="checkbox"/> default-policy-tag	default policy-tag
<input type="checkbox"/> local-site-policy-tag	

1 10 items per page

Koppel uw WLAN-profiel aan het gewenste beleidsprofiel.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

◀ ◁ 1 ▷ ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

CLI:

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

Toewijzing van beleidstags

Wijs de beleidstag toe aan de benodigde toegangspunten.


GUI:

Om de tag aan één AP toe te wijzen, navigeer je naar Configuration > Wireless > Access Points > AP Name > General Tags, maak je de benodigde toewijzing en klik je vervolgens op Update & Apply to Device.

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/> ENABLED	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/> ⓘ
Operation Status Registered	

 **Opmerking:** Houd er rekening mee dat nadat u de beleidstag op een AP hebt gewijzigd, deze de associatie met de 9800 WLC verliest en zich binnen ongeveer 1 minuut opnieuw aansluit.

Als u dezelfde beleidstag wilt toewijzen aan meerdere AP's, gaat u naar Configuration > Wireless > Wireless Setup > Advanced > Start Now.

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply



Tag APs



Start Now →

Done

Configuration > Wireless Setup > Advanced

Show Me How

+ Tag APs

Number of APs: 2
Selected Number of APs: 2

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	Serial Number	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag
<input checked="" type="checkbox"/>	[blurred]	AIR-AP1815I-E-K9	[blurred]	[blurred]	Flex	Disabled	Registered	local-site-policy-tag	flex-site-tag	defa rf-ta
<input checked="" type="checkbox"/>	[blurred]	AIR-AP1815I-E-K9	[blurred]	[blurred]	Local	Enabled	Registered	default-policy-tag	default-site-tag	defa rf-ta

1 10 items per page 1 - 2 of 2 items

Kies de gefloten tag en klik Save & Apply to Device zoals in de afbeelding.

Tag APs

Tags

Policy

Site

RF


Changing AP Tag(s) will cause associated AP(s) to rejoin and disrupt connected client(s)

CLI:

```
# config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end
```



```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```

 **Opmerking:** Als u de ACL beëindigt met een permit ip any any in plaats van een vergunning gericht op poort 80, richt de WLC ook HTTPS, wat vaak ongewenst is omdat het zijn eigen certificaat moet verstrekken en altijd een certificaatschending creëert. Dit is de uitzondering op de vorige verklaring die zegt dat u geen certificaat op de WLC nodig hebt in het geval van CWA: u hebt er een nodig als u HTTPS-interceptie ingeschakeld hebt, maar het wordt toch nooit als geldig beschouwd.

U kunt de ACL verbeteren door actie om alleen de gastpoort 8443 aan de ISE-server te ontkennen.

Omleiding voor HTTP of HTTPS inschakelen

De web admin portal configuratie is verbonden met de web authenticatie portal configuratie en het moet luisteren op poort 80 om te leiden. Daarom moet HTTP ingeschakeld zijn om de omleiding goed te laten werken. U kunt ervoor kiezen om het globaal in te schakelen (met behulp van de opdracht ip http server) of u kunt HTTP alleen inschakelen voor de web authenticatie module (met behulp van de opdracht webauth-http-enable onder de parameterkaart).



Opmerking: de omleiding van het HTTP-verkeer gebeurt binnen CAPWAP, zelfs in het geval van FlexConnect Local Switching. Aangezien de WLC de interceptiewerkzaamheden uitvoert, verstuurt de AP de HTTP(S)-pakketten binnen de CAPWAP-tunnel en ontvangt hij de omleiding van de WLC terug in CAPWAP

Als u wilt worden omgeleid wanneer u probeert om toegang te krijgen tot een HTTPS URL, voeg dan de opdracht toe `intercept-https-enable` onder de parameterkaart maar merk op dat dit geen optimale configuratie is, dat het een impact heeft op de WLC CPU en toch certificaatfouten genereert:

```
<#root>
```

```
parameter-map type webauth global
```

type webauth

intercept-https-enable

trustpoint xxxxx

U kunt dit ook doen via de GUI met de optie 'Web Auth intercept HTTPS' ingeschakeld in de Parameter Map (Configuration > Security > Web Auth).

The screenshot shows the GUI for configuring Web Auth parameters. On the left is a navigation menu with options: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth' and contains a table of parameter maps. The 'global' parameter map is selected. Below the table is a pagination control showing '1' items per page. On the right is the 'Edit Web Auth Parameter' form with the following fields:

Parameter Name	Value
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Virtual IPv4 Address	
Trustpoint	--- Select ---
Virtual IPv6 Address	XXXX:XX:XX:XX
Web Auth intercept HTTPS	<input type="checkbox"/>
Captive Bypass Portal	<input type="checkbox"/>

The 'Web Auth intercept HTTPS' checkbox is highlighted with a red box.

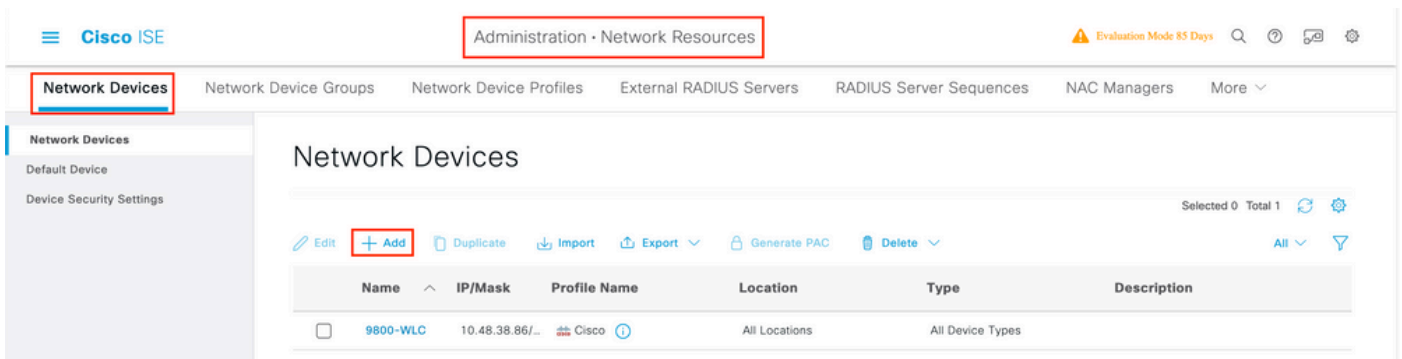


Opmerking: browsers gebruiken standaard een HTTP-website om het omleidingsproces te starten. Als er een HTTPS-omleiding nodig is, moet Web Auth Intercept HTTPS worden gecontroleerd. Deze configuratie wordt echter niet aanbevolen omdat deze het CPU-gebruik verhoogt.

ISE-configuratie

De 9800 WLC toevoegen aan ISE

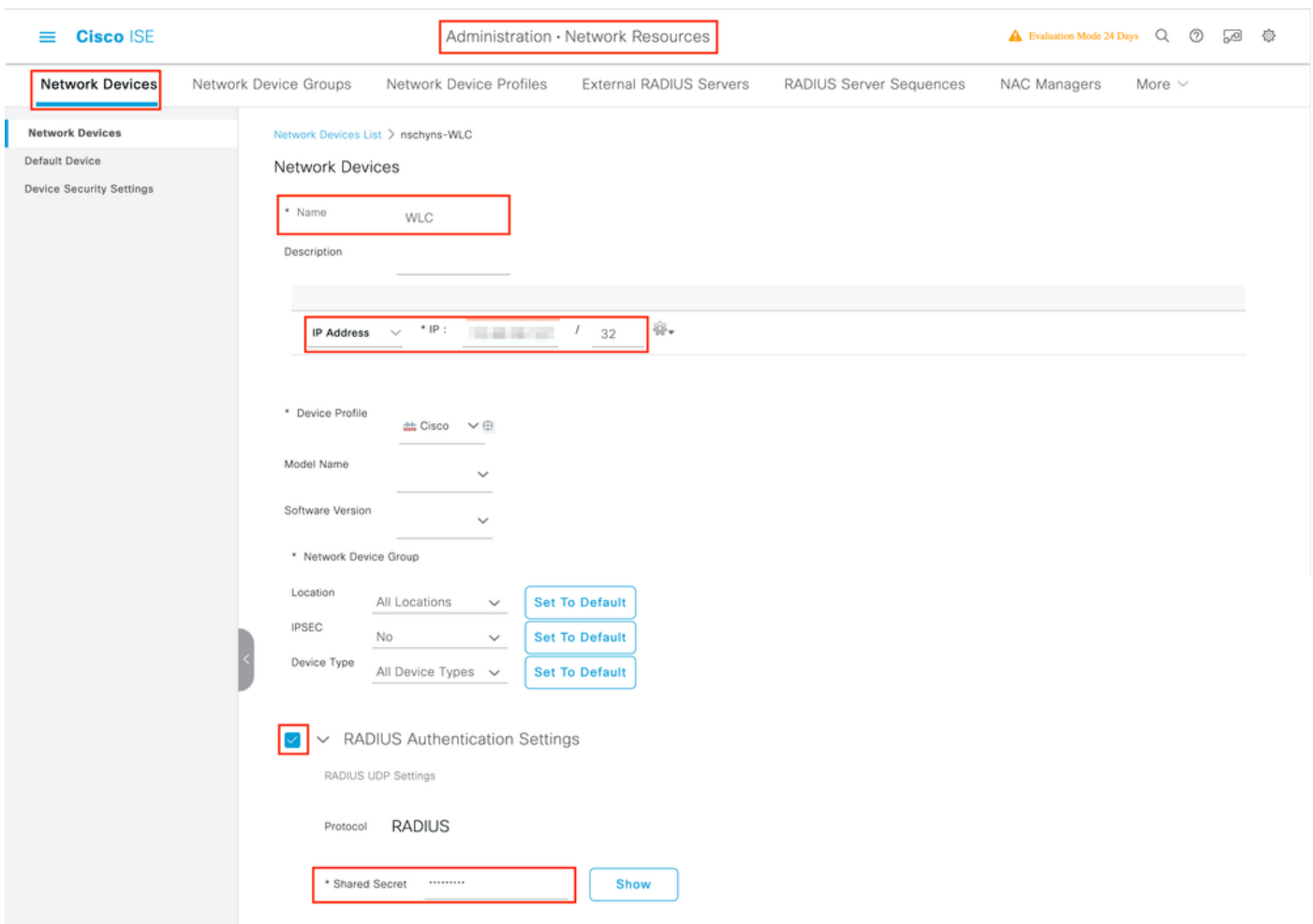
Stap 1. Open de ISE-console en navigeer naar `Administration > Network Resources > Network Devices > Add` zoals in de afbeelding.



Stap 2. Configureer het netwerkapparaat.

Optioneel kan het een opgegeven modelnaam, softwareversie en beschrijving zijn en netwerkapparaatgroepen toewijzen op basis van apparaattypen, locatie of WLC's.

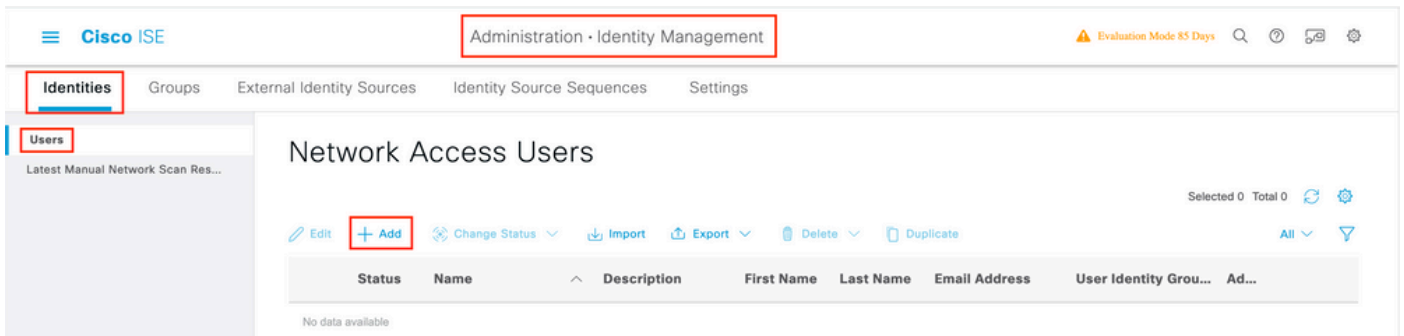
Het IP-adres komt hier overeen met de WLC-interface die de verificatieaanvragen verstuurt. Standaard is dit de beheerinterface zoals in het afbeelding:



Raadpleeg voor meer informatie over netwerkapparaatgroepen het hoofdstuk van de ISE-beheerhandleiding: Netwerkapparaten beheren: [ISE - Network Device Groepen](#).

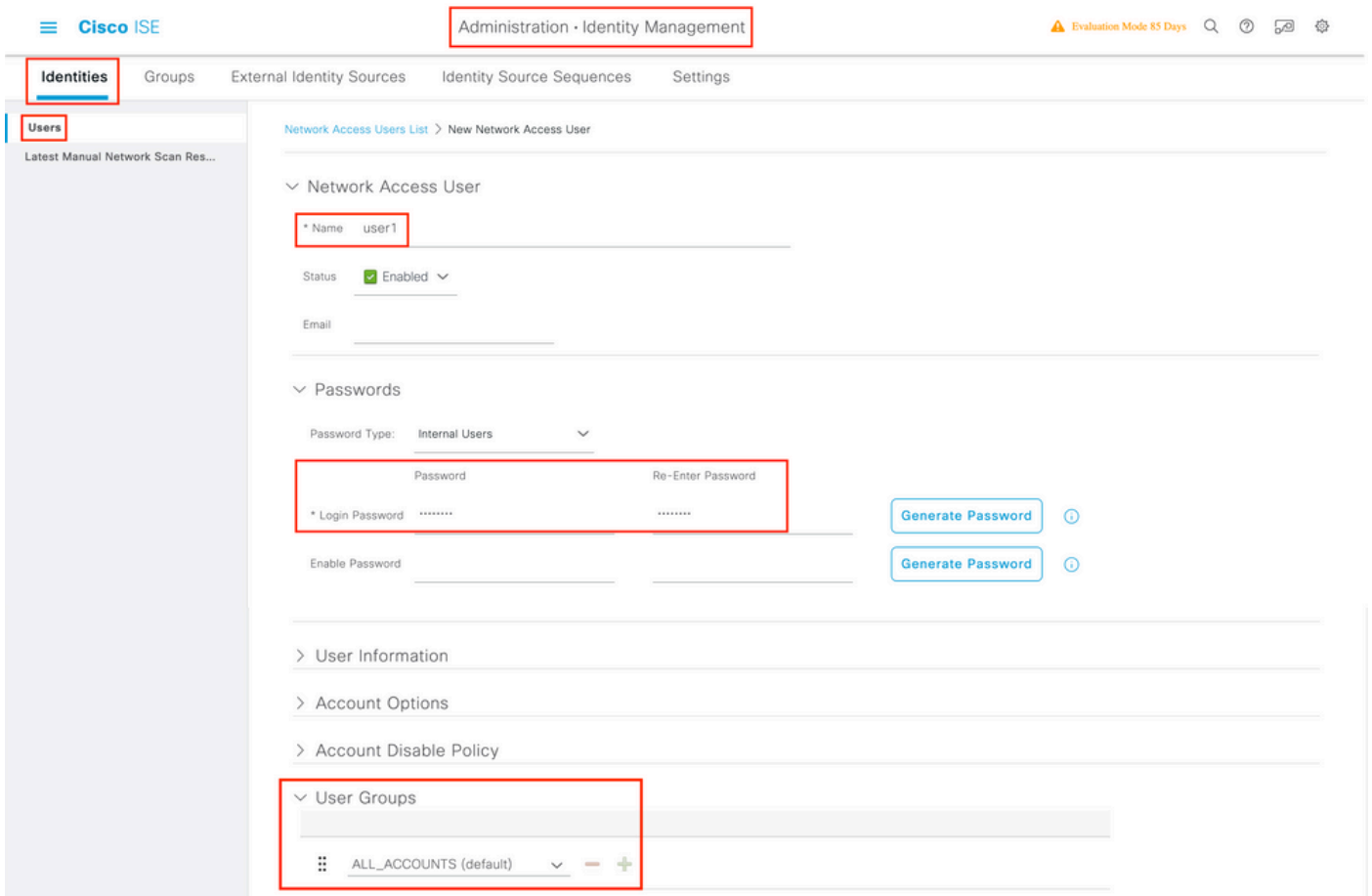
Nieuwe gebruiker maken op ISE

Stap 1. Navigeren naar Administration > Identity Management > Identities > Users > Add zoals in de afbeelding.



Stap 2. Voer de informatie in.

In dit voorbeeld, deze gebruiker behoort tot een groep genoemd ALL_ACCOUNTS maar het kan worden aangepast zoals nodig, zoals getoond in het beeld.



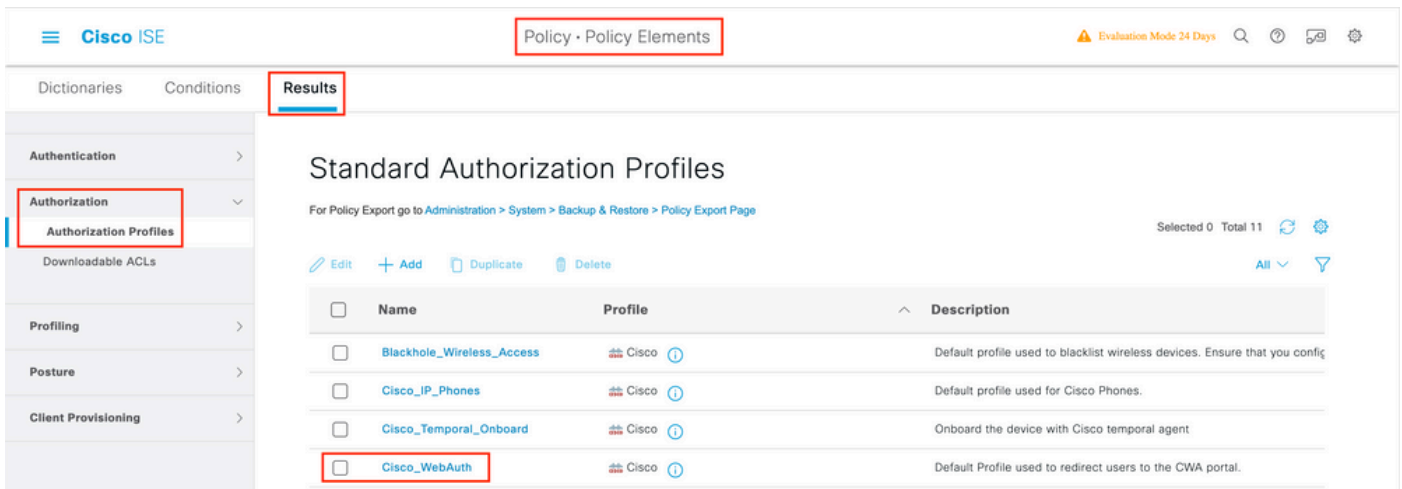
Autorisatieprofiel maken

Het beleidsprofiel is het resultaat dat aan een client is toegewezen op basis van de parameters (zoals mac-adres, referenties, gebruikt WLAN, enzovoort). Het kan specifieke instellingen toewijzen, zoals Virtual Local Area Network (VLAN), Access Control Lists (ACL's), Uniform Resource Locator (URL) omleidingen, enzovoort.

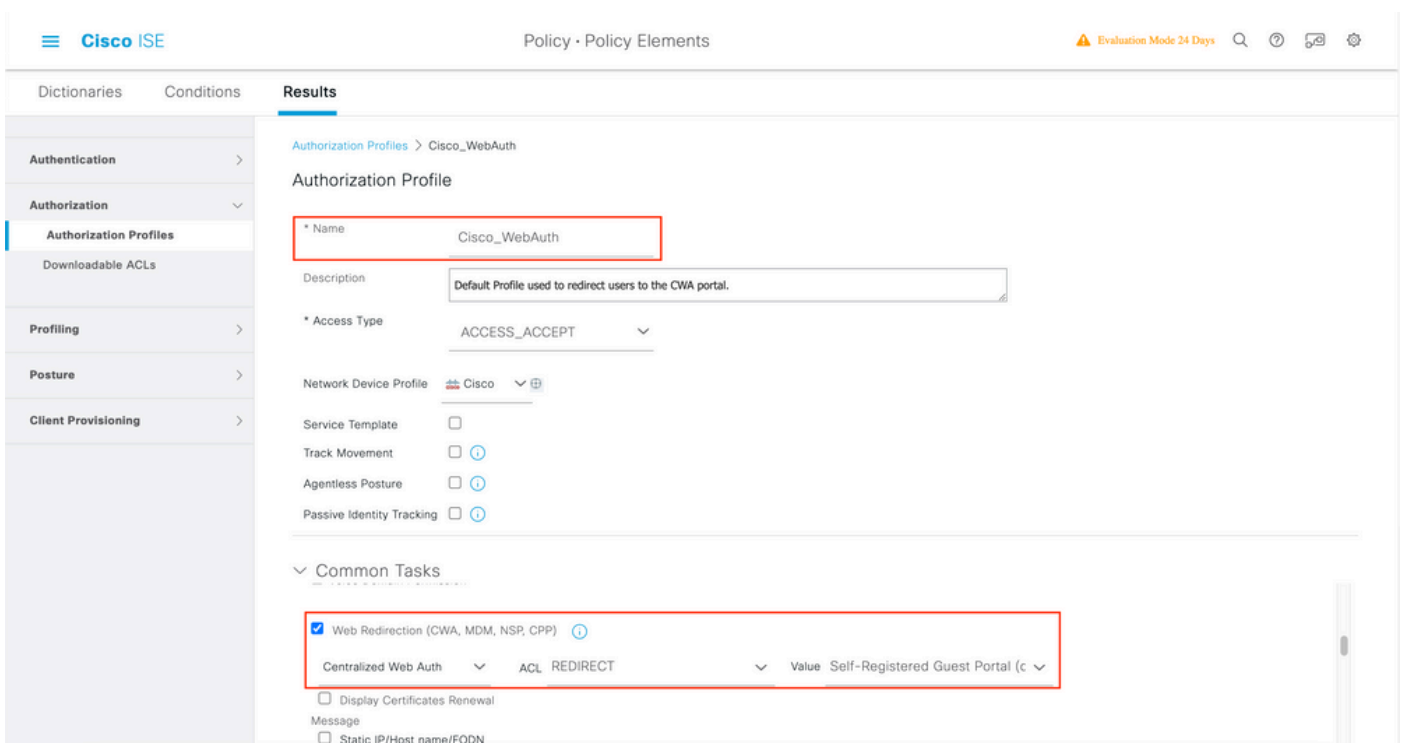
Let op dat in recente versies van ISE al een Cisco_Webauth-autorisatieresultaat bestaat. Hier, kunt u het bewerken om de omleiding ACL naam

te wijzigen om aan te passen wat u op de WLC hebt geconfigureerd.

Stap 1. Navigeer naar Policy > Policy Elements > Results > Authorization > Authorization Profiles. Klik add om uw eigen standaardresultaat te maken of te bewerken Cisco_Webauth.

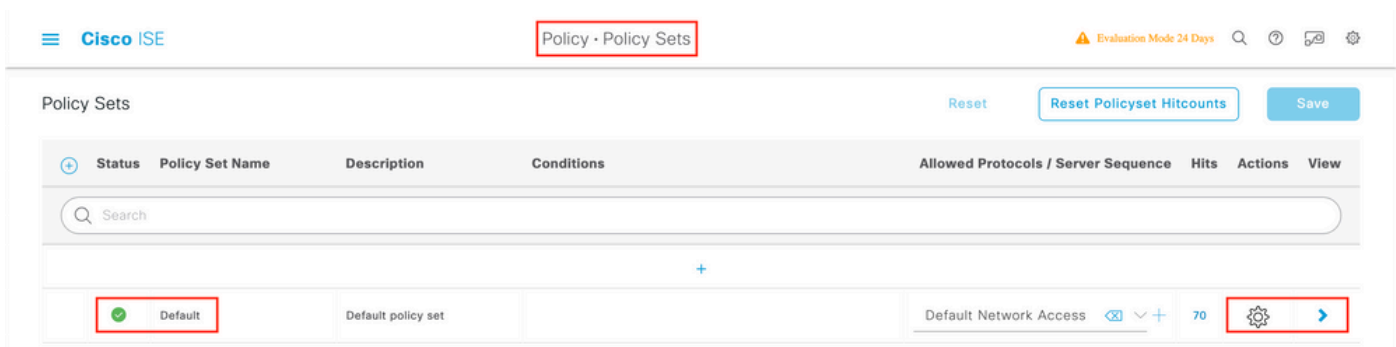


Stap 2. Voer de omleidingsinformatie in. Zorg ervoor dat de ACL-naam hetzelfde is als de naam die op de 9800 WLC is geconfigureerd.

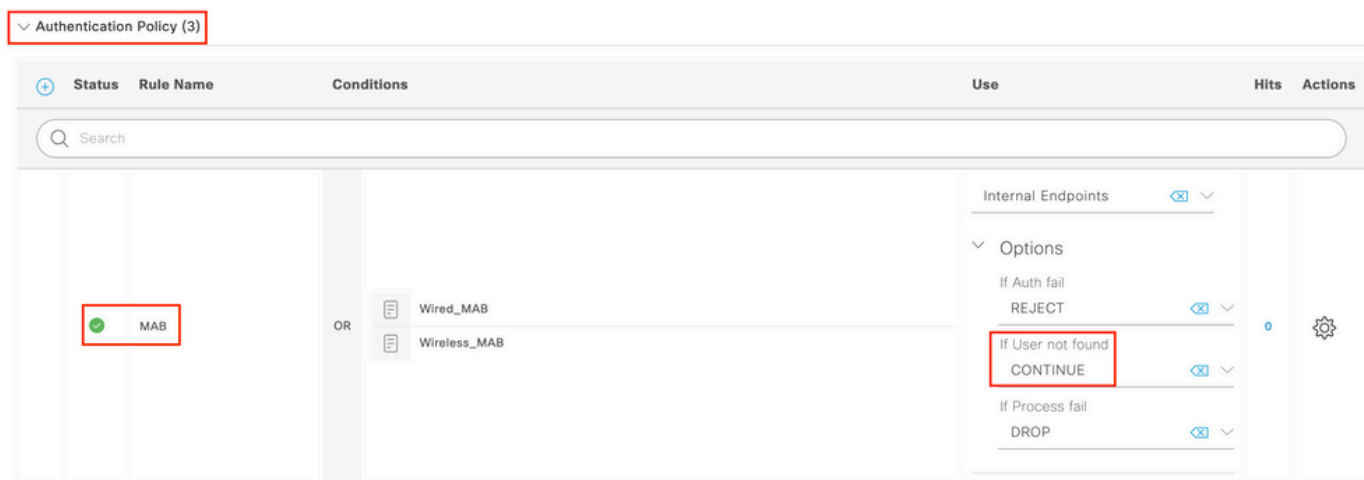


Verificatieregels configureren

Stap 1. Een beleidsset definieert een verzameling verificatie- en autorisatieregels. Om een te maken, navigeer naar Policy > Policy Sets, klik op het tandwiel van de eerste Policy Set in de lijst en Insert new row kies of klik op de blauwe pijl rechts om de standaard Policy Set te kiezen.



Stap 2. Breid het Authentication beleid uit. MAB Voor de regel (match op bekabeld of draadloos MAB), vouw Options uit en kies de optie voor CONTINUE het geval u 'Als Gebruiker niet gevonden' ziet.

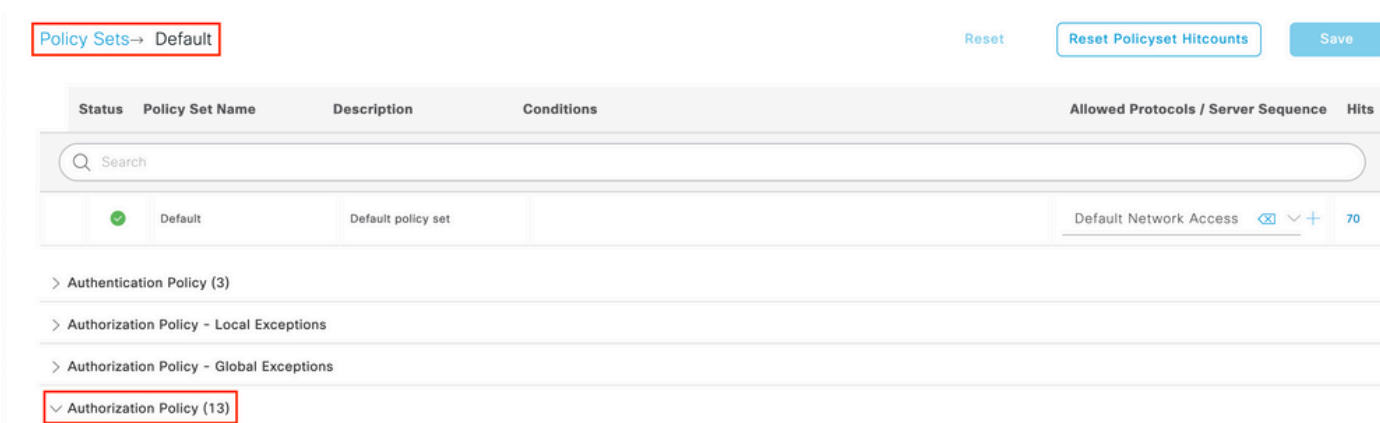


Stap 3. Klik Save om de wijzigingen op te slaan.

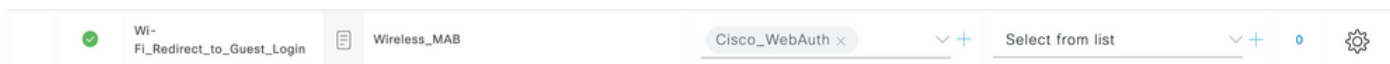
Autorisatieregels configureren

De autorisatieregel is de regel die bepaalt welke permissies (welk autorisatieprofiel) op de client worden toegepast.

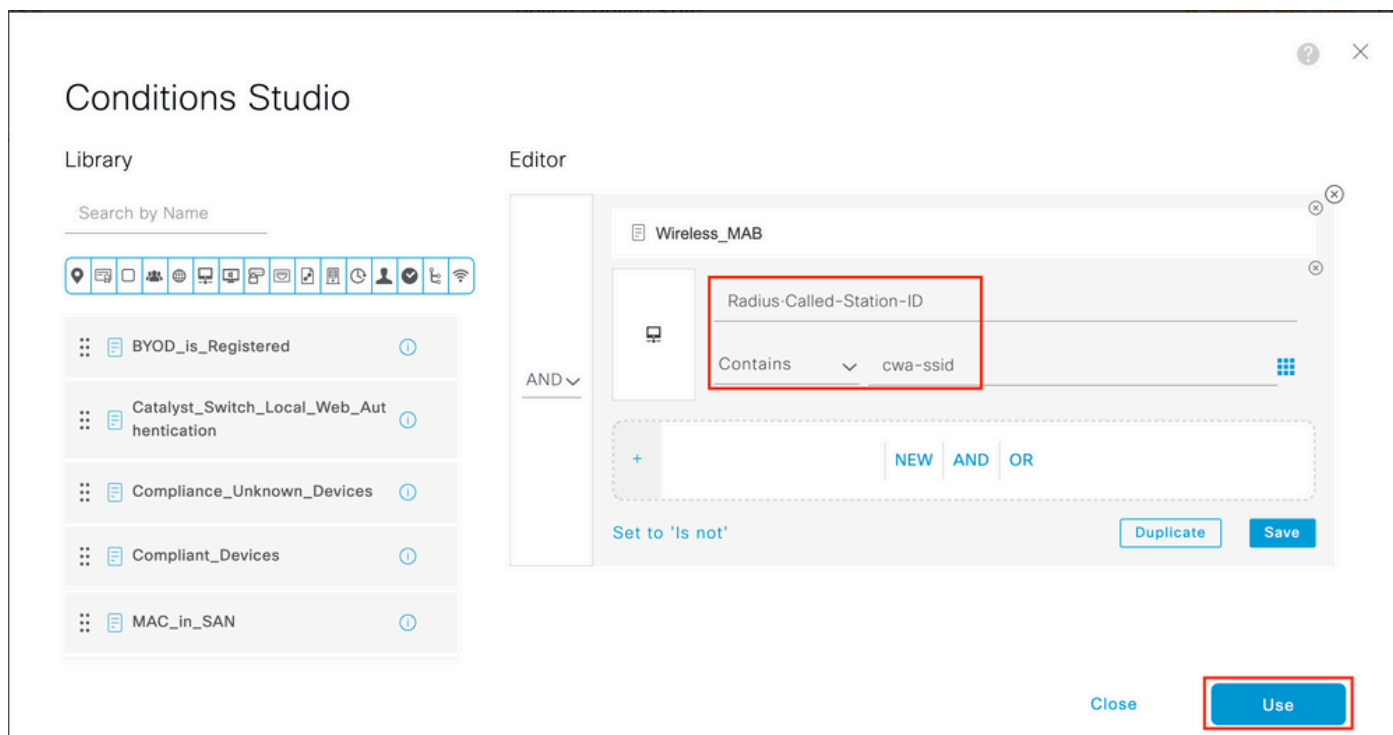
Stap 1. Sluit de pagina Authentication Policy op dezelfde beleidsset en vouw Authorziation Policy de pagina uit zoals in de afbeelding.



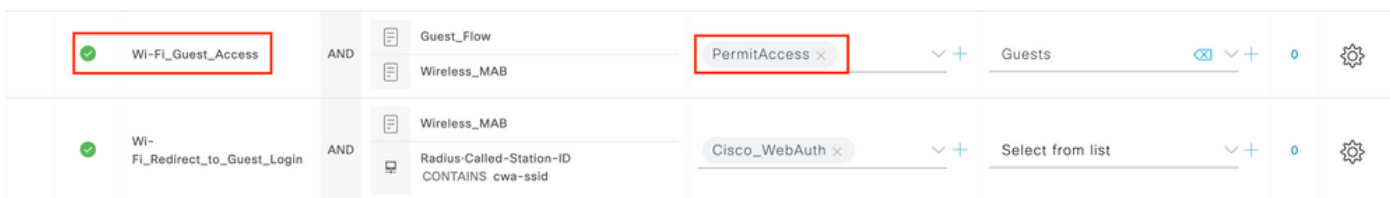
Stap 2. Recente ISE versies beginnen met een vooraf gemaakte regel genaamd Wifi_Redirect_to_Guest_Login die grotendeels aan onze behoeften voldoet. Draai het grijze teken links naar enable.



Stap 3. Die regel past alleen Wireless_MAB aan en geeft de CWA-omleidingskenmerken terug. Nu kunt u optioneel een kleine draai toevoegen en het alleen laten overeenkomen met de specifieke SSID. Kies de voorwaarde (Wireless_MAB vanaf nu) om de Conditioes Studio te laten verschijnen. Voeg aan de rechterkant een voorwaarde toe en kies het Radius woordenboek met het Called-Station-ID kenmerk. Zorg dat het overeenkomt met uw SSID naam. Valideren met de Use onderkant van het scherm zoals weergegeven in de afbeelding.



Stap 4. U hebt nu een tweede regel nodig, gedefinieerd met een hogere prioriteit, die overeenkomt met de Guest Flow voorwaarde om netwerktoegangsgegevens terug te sturen zodra de gebruiker op de portal is geverifieerd. U kunt de regel gebruiken Wifi Guest Access die standaard ook vooraf is gemaakt voor recente ISE-versies. Dan hoeft u de regel alleen maar in te schakelen met een groen teken aan de linkerkant. U kunt de standaard PermitAccess teruggeven of preciezere toegangslijstbeperkingen configureren.



Stap 5. Sla de regels op.

Klik Save onderaan de regels.

Alleen FlexConnect lokale switching-access points

Wat als u Flexconnect lokale switching access points en WLAN's hebt? De vorige secties zijn nog steeds geldig. U moet echter een extra stap zetten om de doorverwijzing van ACL naar de AP's van te voren in te drukken.

Navigeer naar Configuration > Tags & Profiles > Flex en kies uw Flex profiel. Navigeer vervolgens naar het Policy ACL tabblad.

Klik Add zoals in de afbeelding.

The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A red box highlights the '+ Add' button. Another red box highlights the 'Policy ACL' tab. Below the tabs, there are buttons for '+ Add' and '× Delete'. A table header shows 'ACL Name', 'Central Web Auth', and 'URL Filter'. Below the table, there are navigation arrows, a page number '0', a dropdown for '10 items per page', and the text 'No items to display'.

Kies uw omleiden ACL naam en laat centrale webverificatie toe. Dit selectievakje zal automatisch de ACL op de AP zelf omkeren (dit komt doordat een 'deny' statement betekent 'niet omleiden naar dit IP' op de WLC in Cisco IOS XE. Op het toegangspunt betekent de verklaring 'ontkennen' echter het tegenovergestelde. Dus, deze checkbox ruilt automatisch alle vergunningen en ontkent ze wanneer het de druk naar de AP. U kunt dit verifiëren met een show ip access list bericht van het AP (CLI).

Opmerking: in Flexconnect lokaal switchingscenario moet de ACL specifiek terugkeerverklaringen vermelden (wat niet per se vereist is in de lokale modus), zodat al uw ACL-regels betrekking hebben op beide manieren van verkeer (van en naar de ISE bijvoorbeeld).

Vergeet niet te slaan Save en dan Update and apply to the device.

The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A modal dialog is open for adding a new ACL rule. The 'ACL Name*' field is set to 'REDIRECT' and the 'Central Web Auth' checkbox is checked. The 'Save' button is highlighted.

Certificaten

Om de client vertrouwen te hebben in het web authenticatie certificaat, is het niet nodig om een certificaat te installeren op de WLC, aangezien het enige certificaat dat wordt gepresenteerd het ISE certificaat is (dat moet worden vertrouwd door de client).

Verifiëren

U kunt deze opdrachten gebruiken om de huidige configuratie te verifiëren.

```
<#root>
```

```
# show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Hier is het relevante deel van de configuratie van de WLC dat overeenkomt met dit voorbeeld:

```
<#root>
```

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE
mac-filtering CWAauthz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akmdot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

Problemen oplossen

Checklist

- Zorg ervoor dat de client verbinding maakt en een geldig IP-adres krijgt.
- Als de omleiding niet automatisch is, open een browser en probeer een willekeurig IP-adres. Bijvoorbeeld 10.0.0.1. Als de omleiding werkt, is het mogelijk dat u een DNS-resolutieprobleem hebt. Controleer dat u een geldige DNS-server via DHCP hebt en dat het hostnamen kan oplossen.
- Zorg ervoor dat u de opdracht `ip http server` hebt geconfigureerd voor omleiding op HTTP om te werken. De web admin portal configuratie is gekoppeld aan de web authenticatie portal configuratie en het moet worden vermeld op poort 80 om omleiden. U kunt

ervoor kiezen om het globaal in te schakelen (met behulp van de opdracht ip http server) of u kunt HTTP alleen inschakelen voor de web authenticatie module (met behulp van de opdracht webauth-http-enable onder de parameterkaart).

- Als u niet wordt doorgestuurd wanneer u probeert om toegang te krijgen tot een HTTPS URL en die is vereist, dan controleert u of u de opdracht hebt intercept-https-enable onder de parameterkaart:

```
<#root>
```

```
parameter-map type webauth global  
type webauth
```

```
intercept-https-enable
```

```
trustpoint xxxxx
```

U kunt ook via de GUI controleren of u de optie 'Web Auth intercept HTTPS' hebt ingeschakeld op de Parameter Map:

The screenshot displays the Cisco GUI configuration interface. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth'. Below this, there are '+ Add' and 'x Delete' buttons. A table lists 'Parameter Map Name' with one entry: 'global'. Below the table is a pagination control showing '1' items per page. On the right, the 'Edit Web Auth Parameter' panel is open, showing various settings: Maximum HTTP connections (100), Init-State Timeout(secs) (120), Type (webauth), Virtual IPv4 Address, Trustpoint (--- Select ---), Virtual IPv6 Address (xxxxxx), Web Auth intercept HTTPS (checked), and Captive Bypass Portal (unchecked). The 'Web Auth intercept HTTPS' checkbox is highlighted with a red rectangle.

Ondersteuning van servicepoort voor RADIUS

De Cisco Catalyst 9800 Series draadloze controller heeft een servicepoort die GigabitEthernet 0poort wordt genoemd. Vanaf versie 17.6.1 wordt RADIUS (inclusief CoA) ondersteund via deze poort.

Als u de servicepoort voor RADIUS wilt gebruiken, hebt u deze configuratie nodig:

```
<#root>
```

```
aaa server radius dynamic-author  
client 10.48.39.28
```

```
vrf Mgmt-intf
```

```
server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

ip address x.x.x.x x.x.x.x


!if using aaa group server:
aaa group server radius group-name
server name nicoISE

ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0
```

Debugs verzamelen

WLC 9800 biedt ALTIJD-ON traceermogelijkheden. Dit zorgt ervoor dat alle client-connectiviteit gerelateerde fouten, waarschuwingen en meldingen voortdurend worden vastgelegd en u kunt logbestanden bekijken voor een incident of storing nadat het is opgetreden.

 **Opmerking:** u kunt een paar uur terug naar meerdere dagen in de logbestanden, maar het hangt af van het volume van de gegenereerde logbestanden.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC en deze stappen uitvoeren (zorg ervoor dat u de sessie aan een tekstbestand registreert).

Stap 1. Controleer de WLC huidige tijd zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem gebeurde.

```
<#root>
# show clock
```


Stap 2. Verzamel syslogs van de buffer WLC of externe syslog zoals die door de systeemconfiguratie wordt gedicteerd. Dit geeft een snel overzicht van de gezondheid van het systeem en eventuele fouten.

```
<#root>
# show logging
```


Stap 3. Controleer of de debug-voorwaarden zijn ingeschakeld.

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

 **Opmerking:** als u een van de vermelde voorwaarden ziet, betekent dit dat de sporen zijn aangemeld om het debug-niveau te bereiken voor alle processen die de ingeschakelde voorwaarden ervaren (mac-adres, IP-adres, enzovoort). Dit verhoogt het volume van logboeken. Daarom wordt aanbevolen om alle voorwaarden te wissen wanneer u niet actief debug.

Stap 4. Met de aanname dat het te testen mac-adres niet als een voorwaarde in Stap 3 vermeld was., verzamel de altijd-op meldingen niveau sporen voor het specifieke mac-adres.

```
<#root>
```

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

```
<#root>
```

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

```
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Voorwaardelijke debugging en radio actieve tracersing

Als de altijd-op sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-spoor opnemen, dat debug-level sporen biedt voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Ga verder met deze stappen om voorwaardelijke debugging mogelijk te maken.

Stap 5. Zorg ervoor dat geen debug voorwaarden zijn ingeschakeld.

```
<#root>
```


```
# clear platform condition all
```


Stap 6. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdrachten wordt het opgegeven MAC-adres 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

```
<#root>
```

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 **Opmerking:** als u meer dan één client tegelijk wilt bewaken, voert u debug-opdracht voor draadloze mac<aaaa.bbbb.cccc> uit per mac-adres.

 **Opmerking:** u ziet de output van de client activiteit niet op de terminal sessie, omdat alles intern wordt gebufferd om later bekeken te worden.

Stap 7". Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 8. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

```
<#root>
```

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Zodra de monitortijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam:

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 9. Verzamel het bestand met de MAC-adresactiviteit. U kunt de video kopiëren ra trace .log naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Controleer de naam van het RA traces bestand.

<#root>

```
# dir bootflash: | inc ra_trace
```

Kopieert het bestand naar een externe server:

<#root>

```
# copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

Geef de inhoud weer:


<#root>

```
# more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 10. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer uitgebreide mening van debug-niveau logboeken zijn. U hoeft niet opnieuw te debuggen de client als we nemen alleen een verdere gedetailleerde kijk op debug logs die al zijn verzameld en intern opgeslagen.

<#root>

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

 **Opmerking:** deze opdrachtoutput geeft sporen voor alle logniveaus voor alle processen en is vrij omvangrijk. Neem Cisco TAC in om te helpen bij het doorlopen van deze sporen.

U kunt de video kopiëren ra-internal-FILENAME.txt naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Kopieert het bestand naar een externe server:

<#root>

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Geef de inhoud weer:

```
<#root>
```

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Stap 11. Verwijder de debug-voorwaarden.

```
<#root>
```

```
# clear platform condition all
```



Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossingssessie.

Voorbeelden

Als het verificatieresultaat niet is wat u verwacht, is het belangrijk om naar de ISE-pagina te navigeren Operations > Live logs en de details van het verificatieresultaat te krijgen.

U krijgt de reden voor de storing (als er een storing is) en alle Radius-kenmerken die ISE heeft ontvangen.

In het volgende voorbeeld weigerde ISE verificatie omdat er geen autorisatieregel overeenkwam. Dit komt doordat het kenmerk Call-Station-ID wordt verzonden als de naam van de SSID wordt toegevoegd aan het MAC-adres van het AP, terwijl de autorisatie exact overeenkomt met de naam van de SSID. Met de wijziging van die regel wordt het probleem opgelost in "bevat" in plaats van "gelijk".

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-1 type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Search Menu Items

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt Download

1 10 Items per page 1 - 1 of 1 items

Generate

In dit geval ligt het probleem bij het feit dat u een typo hebt gemaakt toen u de ACL-naam maakte en het komt niet overeen met de ACL-naam die door ISEs is geretourneerd of de WLC klaagt dat er geen dergelijke ACL is zoals de door ISE gevraagde ACL:

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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.