

Configuratie van Centrale Webverificatie met Anchor op Catalyst 9800

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureer een Catalyst 9800 die aan een andere Catalyst 9800 is verankerd](#)

[Netwerkdigram](#)

[AAA instellen op beide 9800s](#)

[De WLAN's op de WLC's configureren](#)

[Maak het beleidsprofiel en de beleidstag op de externe WLC](#)

[Het beleidsprofiel op de ankerplaats WLC maken](#)

[Richt ACL op beide 9800s opnieuw](#)

[ISE configureren](#)

[Configuratie van een Catalyst 9800 verankerd aan een AireOS WLC](#)

[Catalyst 9800 buitenlandse configuratie](#)

[AAA configureren op het anker AireOS WLC](#)

[WLAN-configuratie op de AireOS-WLC](#)

[ACL omleiden via het AireOS WLC](#)

[ISE configureren](#)

[Verschillen in configuratie wanneer AireOS WLC het buitenland is en Catalyst 9800 het anker is](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Catalyst 9800 informatie over probleemoplossing](#)

[Clientgegevens](#)

[Ingesloten pakketvastlegging](#)

[RadioActive Traces](#)

[Informatie over AireOS-probleemoplossing](#)

[Clientgegevens](#)

[Debugs van het CLI](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u een Central Web Verificatie (CWA) kunt configureren en oplossen op Catalyst 9800, waarbij u naar een andere Wireless LAN Controller (WLC) wijst als een mobiliteitshandelaar, met inbegrip van bestemming met AireOS of een andere 9800 WLC.

Voorwaarden

Vereisten

Het wordt aanbevolen dat u een basisbegrip hebt van de 9800 WLC, AireOS WLC en Cisco ISE. Aangenomen wordt dat voordat u de CWA ankerconfiguratie start u de mobiliteitstunnel tussen de twee WLC's reeds hebt opgetild. Dit valt buiten de reikwijdte van dit configuratievoorbeeld. Als u hier hulp bij nodig hebt, raadpleeg dan het document "[Mobility Tunnel bouwen op Catalyst 9800 controllers](#)"

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

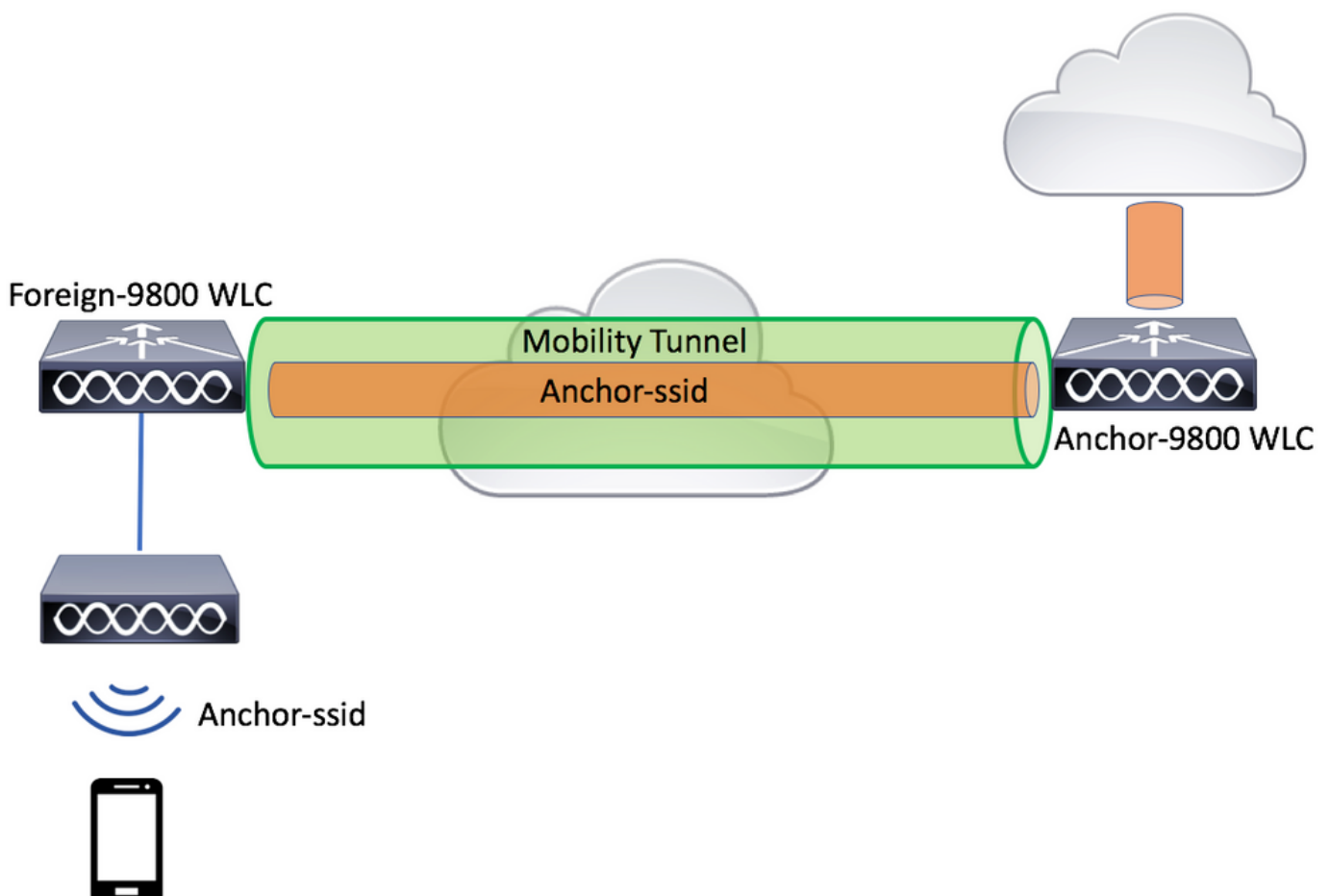
9800 17.2.1

5520 8.5.164 IRCM-beeld

ISE 2.4

Configureer een Catalyst 9800 die aan een andere Catalyst 9800 is verankerd

Netwerkdigram



AAA instellen op beide 9800s

Op zowel het anker als het buitenland moet u eerst de RADIUS-server toevoegen en ervoor zorgen dat CoA is ingeschakeld. Dit kan in het menu gedaan worden **Configuratie>Beveiliging>AAA>servers/groepen>servers>Klik op de knop Toevoegen**

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Security > AAA**. The **Servers / Groups** tab is selected, and the **+ Add** button is highlighted. The **RADIUS** server type is chosen, and the **Servers** sub-tab is active. A modal window titled **Create AAA Radius Server** is open, displaying the following configuration fields:

Name*	CLUS-Server
Server Address*	X.X.X.X
PAC Key	<input type="checkbox"/>
Key Type	Clear Text
Key*	*****
Confirm Key*	*****
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

At the bottom of the dialog, there are **Cancel** and **Apply to Device** buttons.

U moet nu een servergroep maken en de server die u zojuist hebt ingesteld, in die groep plaatsen. Dit gebeurt hier **Configuratie>Beveiliging>AAA>servers/groepen>servergroepen>+Add**.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS Servers Server Groups

TACACS+

LDAP

Create AAA Radius Server Group

Name* CLUS-Server-Group

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers Assigned Servers

CLUS-Server

Cancel Apply to Device

Maak nu een lijst van de **machtigingsmethode** (een lijst van de authenticatiemethode is niet vereist voor CWA) waar het type netwerk is en het groepstype groep. Voeg de servergroep uit de vorige actie toe aan deze methodelijst.

Dit configureren gebeurt hier **Configuration>Security>AAA>servers/AAA-methodelijst>Verificatie>+Add**

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization + Add × Delete

Accounting

Name	Type	Group Type
------	------	------------

Quick Setup: AAA Authorization

Method List Name* CLUS-AuthZ-Meth-List

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- ISE1

Assigned Server Groups

- CLUS-Server-Group

Cancel Apply to Device

(Optioneel) Maak een boekhoudingsmethodelijst met dezelfde servergroep als de machtigingsmethodelijst. U kunt de boekhoudlijst hier maken **Configuration>Security>AAA>servers/AAA-methodelijst>Accounting>+Add**

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top indicates the path: Configuration > Security > AAA. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'AAA Method List' and includes tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. Under the 'AAA Method List' tab, there are sections for 'Authentication', 'Authorization', and 'Accounting'. The 'Accounting' section is highlighted, and a '+ Add' button is visible. A modal dialog box titled 'Quick Setup: AAA Accounting' is open, showing the following configuration details:

- Method List Name*: CLUS-Acct-Meth-List
- Type*: identity
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

Buttons for 'Cancel' and 'Apply to Device' are located at the bottom of the dialog box.

De WLAN's op de WLC's configureren

Maak en vorm de WLAN's op beide WLC's. De WLAN's moeten op beide netwerken worden afgestemd. Het beveiligingstype moet bestaan uit het filteren van de mac en de lijst van de autorisatiemethode van de vorige stap moet worden toegepast. Deze configuratie wordt uitgevoerd onder **Configuration>Tags en profielen>WLAN's>+Add**

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

Status	Name	ID
--------	------	----

Add WLAN

General Security Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID

WLAN ID*

Status

Cancel Apply to Device

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

Status	Name	ID
--------	------	----

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Lobby Admin Access

MAC Filtering Fast Transition

OWE Transition Mode Over the DS

Authorization List* Reassociation Timeout

Cancel Apply to Device

Maak het beleidsprofiel en de beleidstag op de externe WLC

Ga naar het externe WLC web UI.

U maakt het beleidsprofiel als volgt naar **Configuratie>Tabellen en profielen>Beleid>+Add**

Bij verankering moet je centrale switching gebruiken.

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Tags & Profiles > Policy**. The **+ Add** button is highlighted. The **Add Policy Profile** dialog is open, showing the **General** tab. A warning message states: "Configuring in enabled state will result in loss of connectivity for clients associated with this profile." The **Name*** field is "CLUS-Policy-Profile" and the **Description** is "Policy Profile for CLUS". The **Status** is set to **ENABLED**. The **WLAN Switching Policy** section has **Central Switching**, **Central Authentication**, **Central DHCP**, and **Central Association** all set to **ENABLED**. The **CTS Policy** section has **Inline Tagging** and **SGACL Enforcement** set to **DISABLED**, and the **Default SGT** is "2-65519". The **Flex NAT/PAT** is set to **DISABLED**. The **Apply to Device** button is visible at the bottom right.

In het tabblad "Geavanceerd" zijn AAA-Override en RADIUS NAC verplicht voor CWA. Hier kunt u ook de boekhoudmethodelijst toepassen indien u ervoor kiest er een te maken.

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

NAC Type RADIUS

Policy Name default-aaa-policy

Accounting List CLUS-Acct-Meth-

Fabric Profile Search or Select

mDNS Service Policy Search or Select

Hotspot Server Search or Select

User Private Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map Not Configured Clear

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

In het tabblad "Mobility" **NIET** controleren u het selectieteken "uitvoeranker", maar voegt u eerder het anker WLC toe aan de ankerlijst. Zorg ervoor dat u op "Toepassen op apparaat" klikt. Ter herinnering, dit veronderstelt dat u al een mobiliteitstunnelinstelling hebt tussen de twee controllers

Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility **DISABLED**

Adding Mobility Anchors will cause the enabled VLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)

Anchor IP No anchors available

Selected (1)

Anchor IP	Anchor Priority
192.168.160.18	Primary (1)

Cancel Apply to Device

Om de AP's dit beleidsprofiel te kunnen gebruiken, zult u een beleidslaag moeten creëren en het

op de AP's moeten toepassen die u wilt gebruiken.

U kunt de beleidstag als volgt definiëren op **Configuration>Tags en profielen>Tags?Policy>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation at the top reads "Configuration > Tags & Profiles > Tags". The "Policy" tab is selected, and the "+ Add" button is highlighted. The "Add Policy Tag" dialog box is open, showing the following fields and actions:

- Name***: CLUS-Policy-Tag
- Description**: Policy Tag for CLUS
- WLAN-POLICY Maps: 0** (expanded)
- + Add** and **× Delete** buttons
- WLAN Profile** dropdown: CLUS-WLAN-Name
- Policy Profile** dropdown: CLUS-Policy-Profile
- Map WLAN and Policy** section with a table:

WLAN Profile*	Policy Profile*
CLUS-WLAN-Name	CLUS-Policy-Profile

Below the table, there are **×** and **✓** buttons. At the bottom of the dialog, there is a **Cancel** button and an **Apply to Device** button.

Als u dit wilt toevoegen aan meerdere AP's tegelijk, gaat u naar **Configuration>Wireless Setup>Geavanceerd>Nu starten**. Klik op de kogelbalken naast "Tabeljauze" en voeg de tag toe aan de door u gekozen AP's.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Wireless Setup > Advanced

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

<input type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	
<input checked="" type="checkbox"/>	Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local	E
<input checked="" type="checkbox"/>	Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local	E
<input checked="" type="checkbox"/>	AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local	D

1 10 items per page

Tag APs

Tags

Policy: CLUS-Policy-Tag

Site: Search or Select

RF: Search or Select

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Apply to Device

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

Tag APs

Done

Het beleidsprofiel op de ankerplaats WLC maken

Ga naar het ankerweb UI. Voeg het beleidsprofiel op het anker 9800 toe onder **Configuration>Taps en profielen>Taps>Policy>+Add**. Zorg ervoor dat dit overeenkomt met het beleidsprofiel dat op het buitenland is gemaakt, behalve het tabblad mobiliteit en de boekhoudlijst.

Hier voegt u geen anker toe maar u controleert wel het selectieteken "Exporteren Anchor". Voeg hier de boekhoudlijst niet toe. Ter herinnering, dit veronderstelt dat u al een mobiliteitstunnelinstelling hebt tussen de twee controllers

Opmerking: Er is geen reden om dit profiel aan een WLAN in een beleidstag te koppelen. Dit zal problemen opleveren als je dat doet. Als u dezelfde WLAN's voor AP's op deze WLC wilt gebruiken, maakt u er een ander beleidsprofiel voor.

← Cisco 17.2.1 Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add × Delete

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced


Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
 192.168.160.16 →	Anchors not assigned	

Cancel Apply to Device

Richt ACL op beide 9800s opnieuw

Daarna moet u ACL opnieuw richten op beide 9800s. De items op het buitenland doen er niet toe omdat het de ankerfunctie WLC is die ACL op het verkeer toepast. De enige vereiste is dat het er is en dat het een ingang heeft. De inzendingen op het anker moeten de toegang tot ISE op poort 8443 "ontzeggen" en "alles toestaan". Deze ACL wordt alleen toegepast op verkeer dat "binnen" van de client komt zodat regels voor retourverkeer niet nodig zijn. DHCP en DNS gaan zonder ingangen in de ACL door.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Welcome admin
Last login None

Configuration > Security > ACL

+ Add - Delete Associate Interfaces

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type

Protocol

Log DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		192.168.160.99		tcp	None	eq 8443	None	Disabled
<input type="checkbox"/> 100	permit	any		any		ip	None	None	None	Disabled

10 items per page 1 - 2 of 2 items

Cancel Apply to Device

ISE configureren

De laatste stap is ISE voor CWA te configureren. Er zijn een heleboel opties voor dit onderwerp, maar dit voorbeeld zal aan de basis blijven houden en het standaard zelf geregistreeerde gastartaal gebruiken.

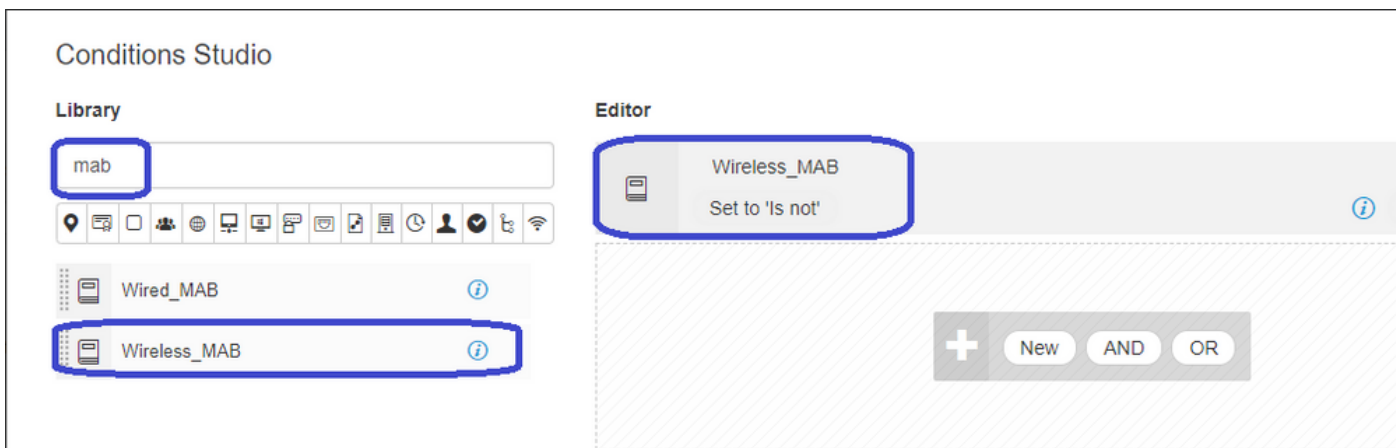
Op ISE, moet u een vergunningprofiel, een beleid creëren met een authenticatiebeleid en een vergunningenbeleid dat het vergunningprofiel gebruikt, 9800 (buitenlands) aan ISE als netwerkapparaat toevoegen, en een gebruikersnaam en wachtwoord om aan het netwerk in te loggen.

Als u het autorisatieprofiel wilt maken, gaat u naar **Beleidselementen>Vergunning>Resultaten>Vergunningsprofielen** en klikt u op **Toevoegen**. Zorg ervoor dat het geretourneerde toegangstype "access_accepteren" is en stel vervolgens de AVP's (attribuut-value paren) in die u wilt terugsturen. Voor CWA is het nasturen van ACL en het opnieuw richten van URL verplicht maar u kunt ook dingen zoals VLAN ID en sessietijd terugsturen. Het is belangrijk dat de ACL-naam overeenkomt met de naam van de herleiding ACL op zowel het buitenland als de anker naam 9800.

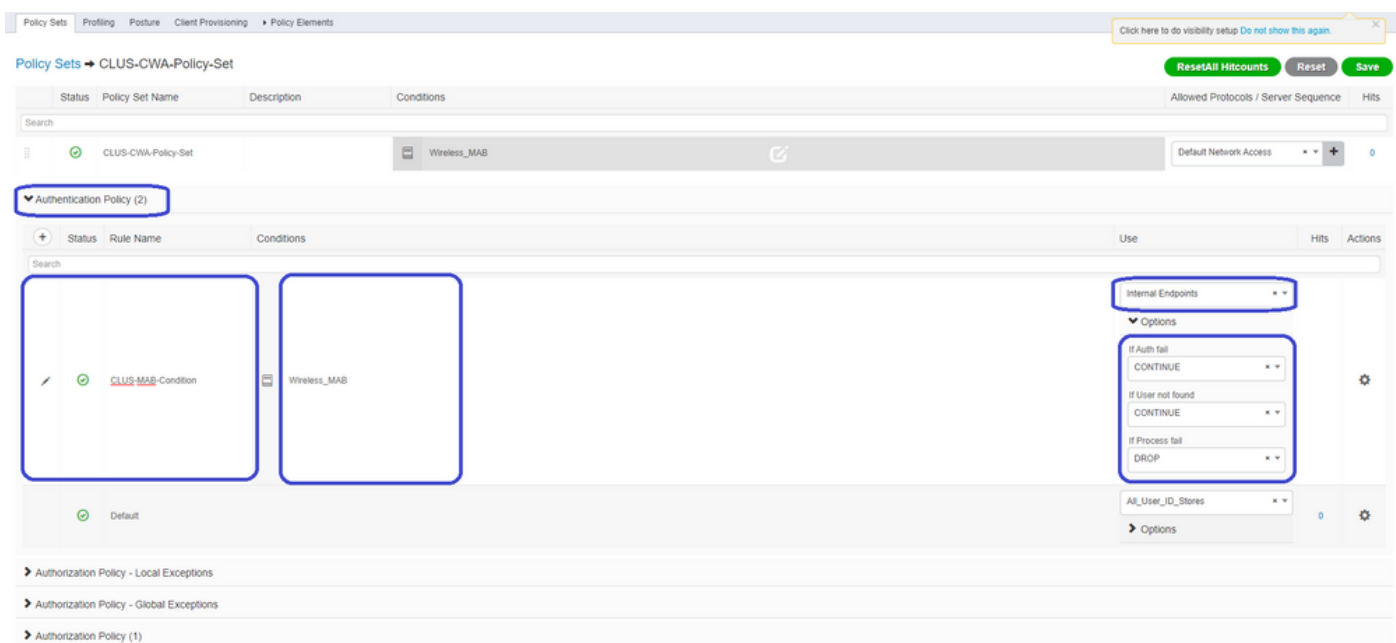
U moet dan een manier configureren om het autorisatieprofiel toe te passen dat u net hebt gemaakt voor de klanten die CWA doorlopen. Om dit te bereiken, is één manier om een beleidsset te creëren die authenticatie omzeilt bij het gebruik van MAB en het autorisatieprofiel toepast bij het gebruik van SSID's die in de opgeroepen stationID zijn verzonden. Nogmaals, er zijn een heleboel manieren om dit te bereiken, dus als je iets specifiekers of zekerder nodig hebt, dan is dit gewoon de eenvoudigste manier om het te doen.

Om de beleidsset te maken, gaat u naar **Beleidsformaten** en klikt u op de +-toets aan de linkerkant van het scherm. Geef de nieuwe beleidsset een naam en zorg ervoor dat deze is ingesteld op "standaard netwerktoegang" of een toegestane protocollijst waarmee "Proceshost Lookup" voor MAB(om de toegestane protocollijst te controleren gaat naar **Beleidsformaten>Resultaten>Verificatie>Toegestane protocollen**). Druk op dat + teken in het midden van de nieuwe beleidsset die u hebt gecreëerd.

Voor dit beleid wordt elke keer dat MAB in ISE wordt gebruikt, dit beleid doorgevoerd. Later kunt u autorisatiebeleid maken dat overeenkomt met de genoemde stationID zodat verschillende resultaten kunnen worden toegepast, afhankelijk van de WLAN's die worden gebruikt. Dit proces is zeer aanpasbaar met een hoop dingen waar je op kunt passen.



Voer in het beleidskader het beleid in. Het authenticatiebeleid kan opnieuw overeenkomen op MAB maar u moet de ID winkel wijzigen om 'interne eindpunten' te gebruiken en de opties wijzigen om auth fail en user not found te blijven.



Zodra het authenticatiebeleid is ingesteld, moet je twee regels opstellen in het autorisatiebeleid. Dit beleid leest als een ACL, zodat de volgorde aan de top en de pre-auth regel aan de onderkant moet zijn. De post-auth-regel zal gelijk zijn aan gebruikers die al door de gastenstroom zijn gegaan. Dat wil zeggen dat als zij al hebben getekend, zij die regel zullen treffen en daar ophouden. Als ze niet in hebben getekend, blijven ze de lijst volgen en op de pre-auth regel klikken om de herleiding te krijgen. Het is een goed idee om de regels van het autorisatiebeleid aan te passen aan het genoemde station ID eindigen met de SSID zodat het alleen raakt voor WLAN's die zo zijn geconfigureerd.

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)
 Authorization Policy - Local Exceptions
 Authorization Policy - Global Exceptions
 Authorization Policy (4)

Status	Rule Name	Conditions	Results	Security Groups
✓	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	Select from list
✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	Select from list
✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	Select from list
✓	Default		DenyAccess	Select from list

Nu de beleidsset is geconfigureerd, moet u ISE over de 9800 (buitenlandse) vertellen om ISE als authenticator te kunnen vertrouwen. Dit kan worden gedaan bij **Admin>Netwerkbronnen>Netwerkapparaat>+**. U moet het naam geven, het IP-adres instellen (of in dit geval het gehele admin-subnetwerk), RADIUS inschakelen en het gedeelde geheim instellen. Het gedeelde geheim op ISE moet overeenkomen met het gedeelde geheim over de 9800, anders zal dit proces mislukken. Nadat de configuratie is toegevoegd, drukt u op de knop Insturen om deze op te slaan.

Identity Services Engine Administration

System Identity Management **Network Resources** Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > JAysNet

Network Devices

Default Device
Device Security Settings

* Name **CLUS_Net-Device**
Description

IP Address * IP: **192.168.160.0** / **24**

* Device Profile Cisco
Model Name
Software Version

* Network Device Group
Location All Locations Set To Default
IPSEC No Set To Default
Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings
Protocol RADIUS
Shared Secret ********* Show
Use Second Shared Secret Show
CoA Port 1700 Set To Default

RADIUS DTLS Settings

Tot slot moet u de gebruikersnaam en het wachtwoord toevoegen dat de client naar de

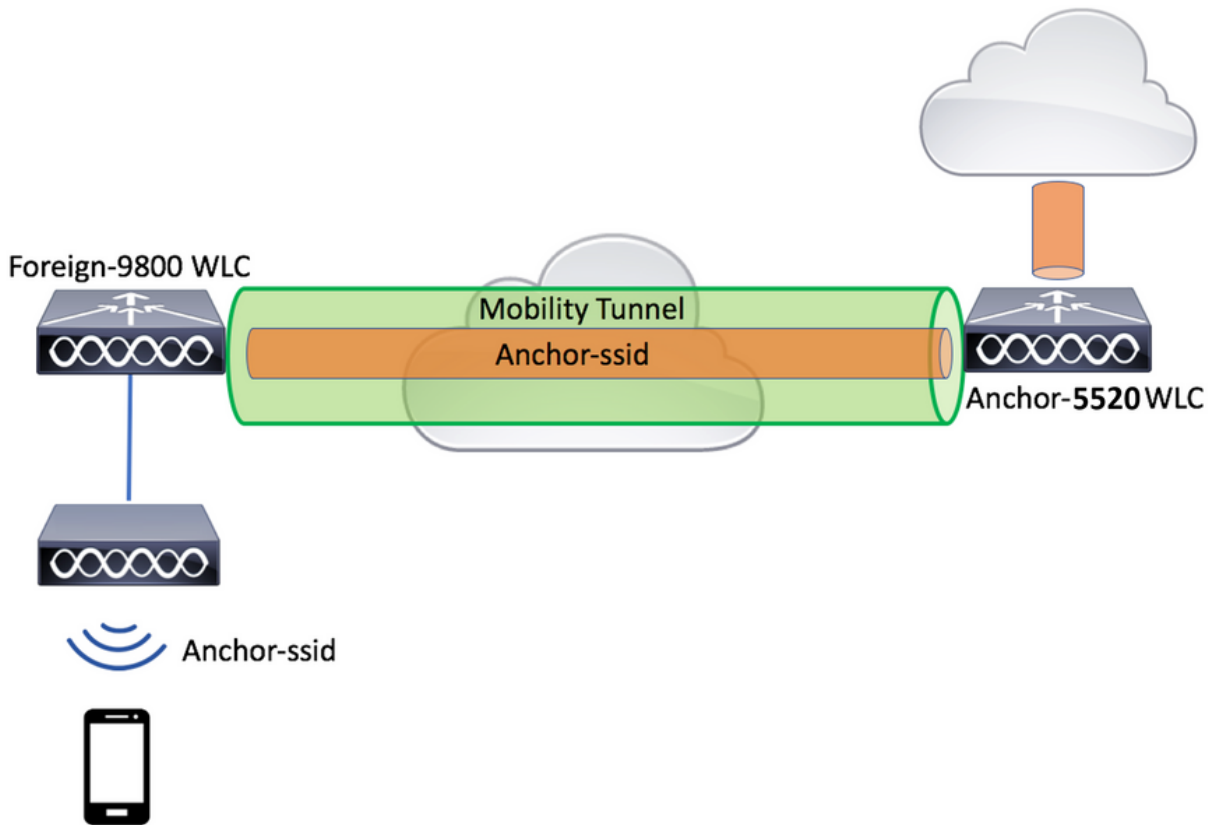
inlogpagina gaat invoeren om te kunnen bevestigen dat ze toegang hebben tot het netwerk. Dit gebeurt onder **Admin>identiteitsbeheer>Identity>Gebruikers>+Add** en zorg ervoor dat u na het toevoegen van de bestanden op **inzenden**. Zoals alles met ISE, is dit aanpasbaar en moet niet een lokaal opgeslagen gebruiker zijn maar opnieuw, is het de makkelijkste configuratie.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes: Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. Under Administration, the path is: System > Identity Management > Network Access Users List > New Network Access User. The left sidebar shows 'Users' and 'Latest Manual Network Scan Results'. The main form is titled 'New Network Access User' and contains the following sections:

- Network Access User:** * Name: CLUS-User; Status: Enabled; Email: (empty).
- Passwords:** Password Type: Internal Users; * Login Password: (masked); Re-Enter Password: (masked); Enable Password: (empty).
- User Information:** First Name: (empty); Last Name: (empty).
- Account Options:** Description: (empty); Change password on next login: (unchecked).
- Account Disable Policy:** Disable account if date exceeds: 2020-07-17 (yyyy-mm-dd).
- User Groups:** Select an item (dropdown menu).

At the bottom, there are 'Submit' and 'Cancel' buttons.

Configuratie van een Catalyst 9800 verankerd aan een AireOS WLC



Catalyst 9800 buitenlandse configuratie

Volg dezelfde stappen als eerder besproken en overslaat u het gedeelte "*Het beleidsprofiel maken op het ankergedeelte WLC*".

AAA configureren op het anker AireOS WLC

Voeg de server toe aan de WLC door naar **Security>AAA>RADIUS>Verificatie>New**. Voeg het server IP adres, gedeeld geheim en ondersteuning voor CoA toe.

The top screenshot shows the 'RADIUS Authentication Servers' configuration page in the Cisco Catalyst 9800 GUI. The 'Auth Called Station ID Type' is set to 'AP MAC Address:SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen' and the 'Framed MTU' is 1300. A table below shows columns for Network, User, Management, Tunnel, Proxy, Server Index, Server Address, Port, IPsec, and Admin Status.

The bottom screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The 'Server Index' is set to 1. The 'Server IP Address' is 192.168.160.99. The 'Shared Secret Format' is 'ASCII' and the 'Shared Secret' is masked with asterisks. The 'Confirm Shared Secret' is also masked. The 'Apply Cisco ISE Default settings' checkbox is checked. The 'Key Wrap' checkbox is unchecked. The 'Port Number' is 1812. The 'Server Status' is 'Enabled'. The 'Support for CoA' is 'Enabled'. The 'Server Timeout' is 5 seconds. The 'Network User' and 'Management' checkboxes are checked. The 'Management Retransmit Timeout' is 5 seconds. The 'Tunnel Proxy', 'PAC Provisioning', and 'IPsec' checkboxes are unchecked.

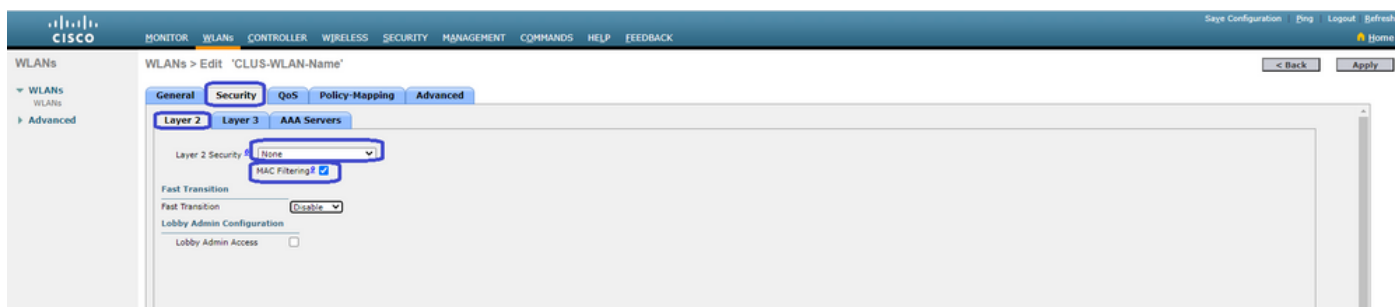
WLAN-configuratie op de AireOS-WLC

Ga naar **WLAN's>Nieuw>Ga naar WLAN's** om een WLAN te maken.

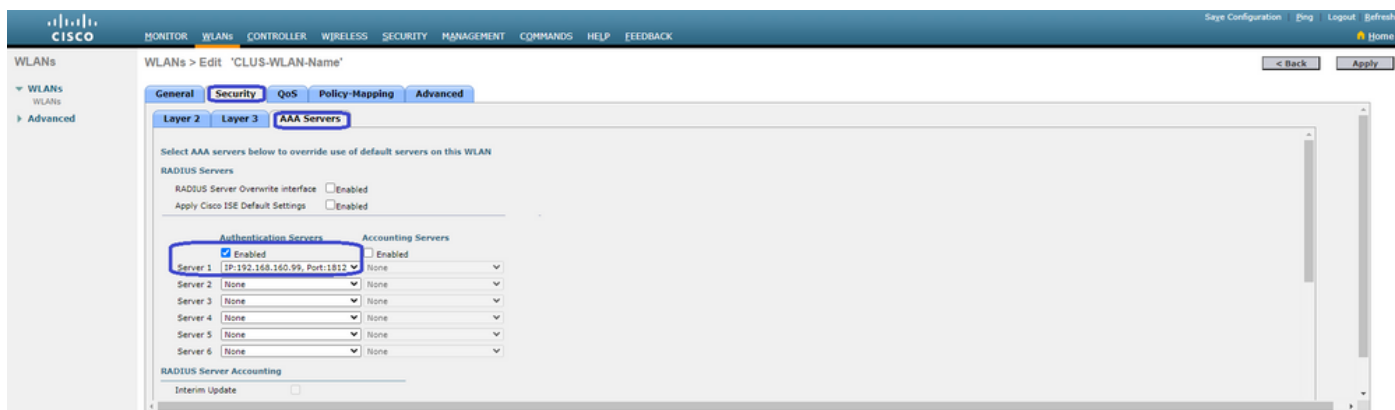
Configuratie van de naam van het profiel, WLAN ID, en SSID en druk vervolgens op "Toepassen".



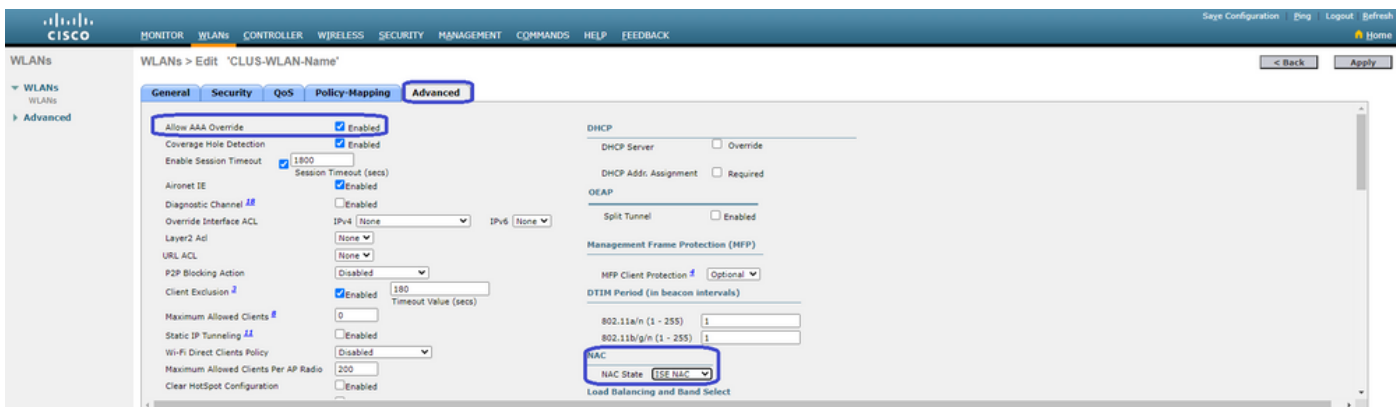
Dit zou u naar de WLAN-configuratie moeten brengen. Op het tabblad "Algemeen" kunt u de interface toevoegen die u wilt dat de clients worden gebruikt als u geen ISE gaat configureren om deze in een AVP te verzenden. Ga daarna naar het **tabblad Security>Layer 2** en stem het bestand "Layer 2 security" aan dat u op de 9800 hebt gebruikt en schakelt "MAC Filtering" in.



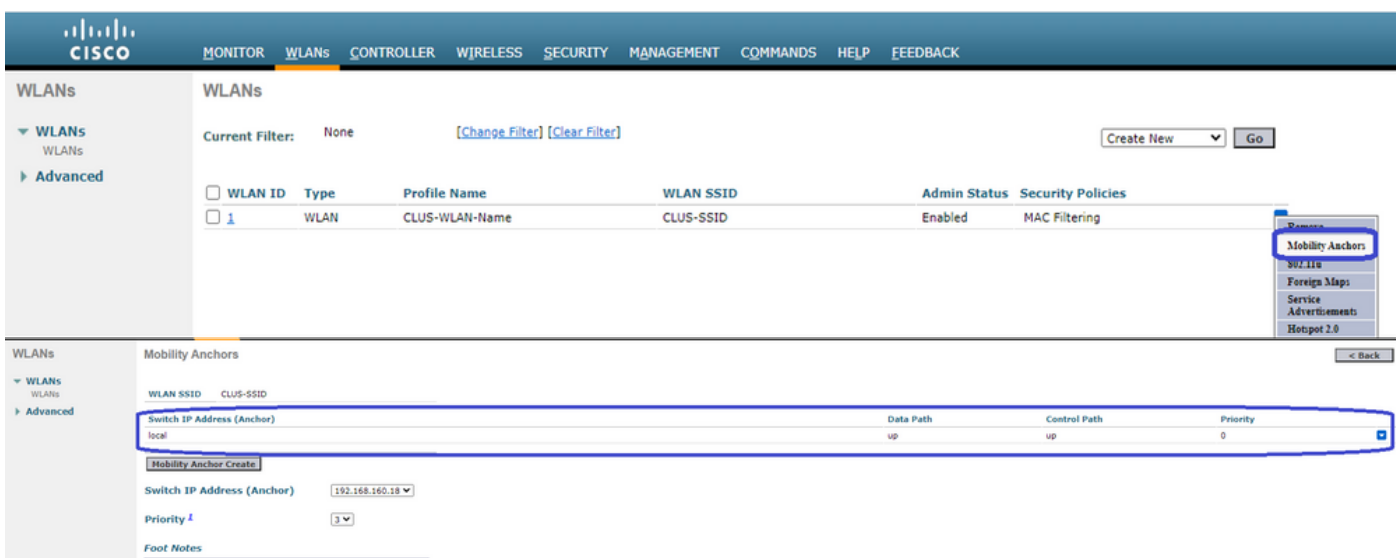
Ga nu naar het tabblad **Security>AAA-servers** en stel de ISE-server in als de "Verificatieservers". **Stel** niets in voor de "Accounting Server". Schakel het vakje "Inschakelen" uit voor het accounting.



Terwijl u nog in de WLAN-configuratie zit, gaat u naar het tabblad "Geavanceerd" en schakelt u "AAA-override toestaan" in en wijzigt u de "NAC-staat" in "ISE NAC"

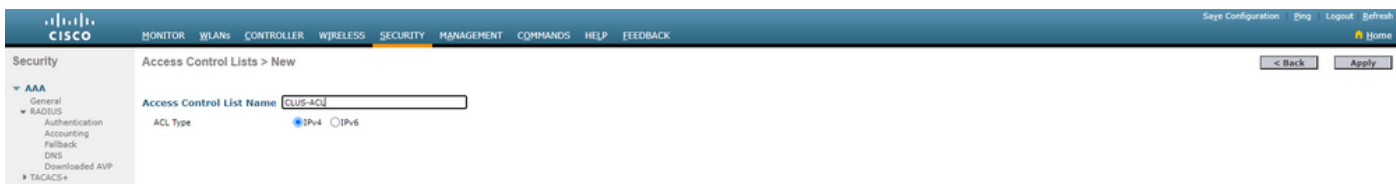


Het laatste is het verankeren ervan in zichzelf. Ga voor dit geval terug naar **WLAN's** pagina en klik op het blauwe vakje rechts van de WLAN>Mobiliteitsanaloge modem. Stel "Switch IP Address (Anchor)" in op Local en druk op de knop "Mobility Anchor Create". Het zou dan moeten verschijnen met prioriteit 0 verankerd lokaal.



ACL omleiden via het AireOS WLC

Dit is de laatste configuratie nodig op de AireOS WLC. Om ACL-richting te maken gaat u naar **Security>Toegangscontrolelijsten>Toegangscontrolelijsten>Nieuw**. Voer de ACL-naam in (deze moet overeenkomen met wat in de AVP's wordt verzonden) en druk op "Toepassen".



Klik nu op de naam van ACL die u zojuist hebt gemaakt. Klik op de knop "Nieuwe regel toevoegen". In tegenstelling tot de 9800 controller op AireOS WLC, vormt u een vergunningsverklaring voor verkeer dat ISE kan bereiken zonder herleiding. DHCP en DNS zijn standaard toegestaan.

Security

Access Control Lists > Edit

General

Access List Name: CLUS-ACL

Deny Counters: 5

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	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

ISE configureren

De laatste stap is ISE voor CWA te configureren. Er zijn een heleboel opties voor dit onderwerp, maar dit voorbeeld zal aan de basis blijven houden en het standaard zelf geregistreerde gastartaal gebruiken.

Op ISE, moet u een vergunningprofiel, een beleid creëren met een authenticatiebeleid en een vergunningenbeleid dat het vergunningprofiel gebruikt, 9800 (buitenlands) aan ISE als netwerkapparaat toevoegen, en een gebruikersnaam en wachtwoord om aan het netwerk in te loggen.

Ga naar **Beleidselementen > Vergunningsprofiel > Resultaten maken > Vergunningsprofielen > Auditing profielen > +Add**. Zorg ervoor dat het geretourneerde toegangstype "access_accepteren" is en stel vervolgens de AVP's (attribuut-value paren) in die u wilt terugsturen. Voor CWA is het nasturen van ACL en het opnieuw richten van URL verplicht maar u kunt ook dingen zoals VLAN ID en sessietijd terugsturen. Het is belangrijk dat de ACL-naam overeenkomt met de naam van de herleiding ACL op zowel het buitenland als de anker naam WLC.

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionary > Conditions > Results

Authorization Profiles > test

Authorization Profile

* Name: CLUS-AuthZ-Profile-ISE

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Voice Domain Permission

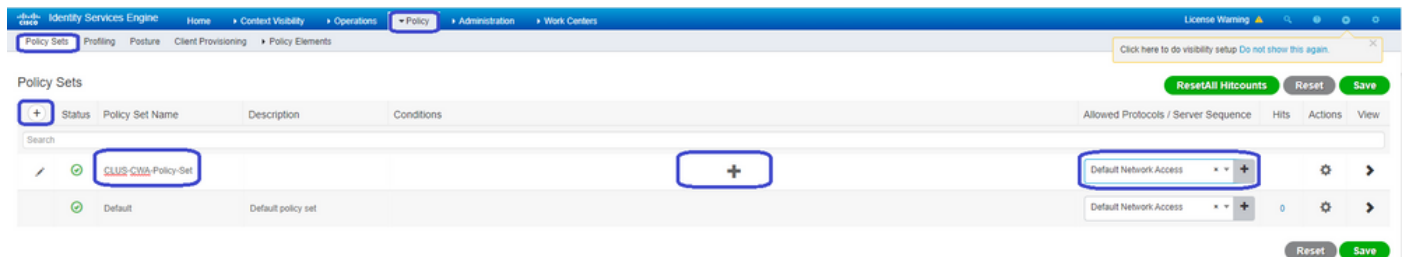
Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth: ACL: CLUS-ACL Value: Self-Registered Guest Portal

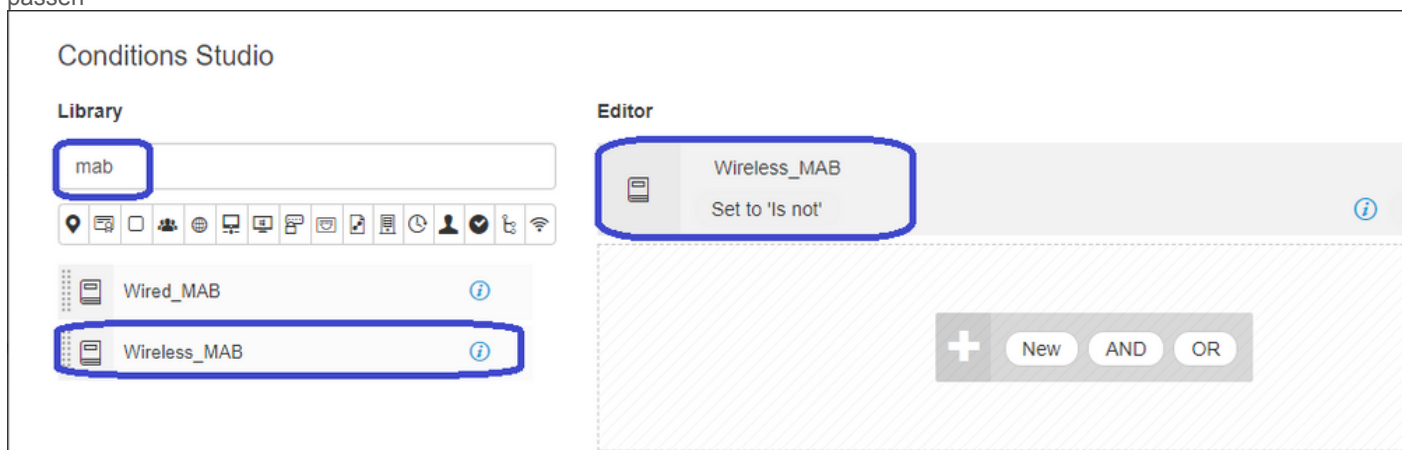
U moet dan een manier configureren om het autorisatieprofiel toe te passen dat u net hebt gemaakt voor de klanten die CWA

doorlopen. Om dit te bereiken, is één manier om een beleidsset te creëren die authenticatie omzeilt bij het gebruik van MAB en het autorisatieprofiel toepast bij het gebruik van SSID's die in de opgeroepen stationID zijn verzonden. Nogmaals, er zijn een heleboel manieren om dit te bereiken, dus als je iets specifiekers of zekerder nodig hebt, dan is dit gewoon de eenvoudigste manier om het te doen.

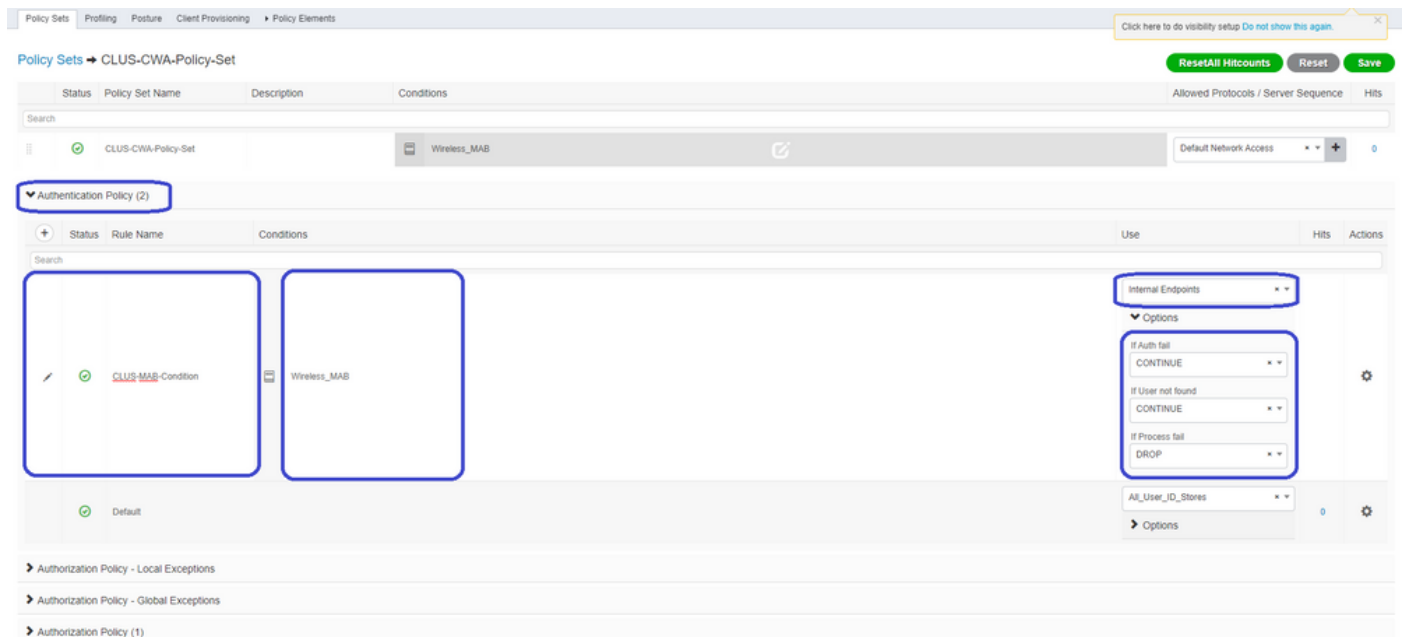
Om de beleidsset te maken, **gaat u naar Policy>Instellingen>**en klikt u op de +>toets aan de linkerkant van het scherm. Geef de nieuwe beleidsset een naam en zorg ervoor dat deze is ingesteld op "standaard netwerktoegang" of een toegestane protocollijst waarmee "Proceshost Lookup" voor MAB(om de toegestane protocollijst te controleren gaat naar Beleidselementen>Resultaten>Verificatie>Toegestane protocollen). Druk op dat + teken in het midden van de nieuwe beleidsset die u hebt gecreëerd.



Voor dit beleid wordt elke keer dat MAB in ISE wordt gebruikt, dit beleid doorgevoerd. Later kunt u autorisatiebeleid maken dat overeenkomt met de genoemde stationID zodat verschillende resultaten kunnen worden toegepast, afhankelijk van de WLAN's die worden gebruikt. Dit proces is zeer aanpasbaar met een hoop dingen waar je op kunt passen



Voer in het beleidskader het beleid in. Het authenticatiebeleid kan opnieuw overeenkomen op MAB maar u moet de ID winkel wijzigen om 'interne eindpunten' te gebruiken en de opties wijzigen om auth fail en user not found te blijven.



Zodra het authenticatiebeleid is ingesteld, moet je twee regels opstellen in het autorisatiebeleid. Dit beleid leest als een ACL, zodat de volgorde aan de top en de pre-auth regel aan de onderkant moet zijn. De post-auth-regel zal gelijk zijn aan gebruikers die al door de gastenstroom zijn gegaan. Dat wil zeggen dat als zij al hebben getekend, zij die regel zullen treffen en daar ophouden. Als ze niet in hebben getekend, blijven ze de lijst volgen en op de pre-auth regel klikken om de herleiding te krijgen. Het is een goed idee om de regels van het autorisatiebeleid aan te passen aan het genoemde station ID eindigen met de SSID zodat het alleen raakt voor WLAN's die zo zijn geconfigureerd.

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
🟢	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (4)

Status	Rule Name	Conditions	Results	Security Groups
🟢	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	Select from list
🟢	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	Select from list
🟢	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	Select from list
🟢	Default		DenyAccess	Select from list

Nu de beleidsset is geconfigureerd, moet u ISE over de 9800 (buitenlandse) vertellen om ISE als authenticator te kunnen vertrouwen. Dit kan worden gedaan op **Admin>Netwerkbronnen>Netwerkapparaat>+**. U moet het naam geven, het IP-adres instellen (of in dit geval het gehele admin-subnetwerk), RADIUS inschakelen en het gedeelde geheim instellen. Het gedeelde geheim op ISE moet overeenkomen met het gedeelde geheim over de 9800, anders zal dit proces mislukken. Nadat de configuratie is toegevoegd, drukt u op de knop Insturen om deze op te slaan.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the path is: Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC. The left sidebar shows: Network Devices, Default Device, and Device Security Settings. The main configuration area is titled "Network Devices List > JaysNet" and "Network Devices".

Configuration fields include:

- Name: CLUS_Net-Device
- Description: (empty)
- IP Address: 192.168.160.0
- Subnet: 24
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations
- IPSEC: No
- Device Type: All Device Types

The "RADIUS Authentication Settings" section is expanded, showing:

- RADIUS UDP Settings
 - Protocol: RADIUS
 - Shared Secret: (masked)
 - Use Second Shared Secret: (unchecked)
 - CoA Port: 1700
- RADIUS DTLS Settings: (info icon)

Tot slot moet u de gebruikersnaam en het wachtwoord toevoegen dat de client naar de inlogpagina gaat invoeren om te kunnen bevestigen dat ze toegang hebben tot het netwerk. Dit gebeurt onder **Admin>identiteitsbeheer>Identity>Gebruikers>+Adden** zorg ervoor dat u op Insturen klikt nadat u deze hebt toegevoegd. Zoals alles met ISE, is dit aanpasbaar en moet niet een lokaal opgeslagen gebruiker zijn maar opnieuw, is het de makkelijkste configuratie.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The main content area is titled 'Network Access Users List > New Network Access User'.

The configuration form is divided into several sections:

- Network Access User:**
 - * Name: CLUS-User
 - Status: Enabled
 - Email: [Empty field]
- Passwords:**
 - Password Type: Internal Users
 - * Login Password: [Masked]
 - Re-Enter Password: [Masked]
 - Enable Password: [Empty field]
- User Information:**
 - First Name: [Empty field]
 - Last Name: [Empty field]
- Account Options:**
 - Description: [Empty field]
 - Change password on next login:
- Account Disable Policy:**
 - Disable account if date exceeds: 2020-07-17 (yyyy-mm-dd)
- User Groups:**
 - Select an item: [Dropdown menu]

At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

Verschillen in configuratie wanneer AireOS WLC het buitenland is en Catalyst 9800 het anker is

Als u wilt dat AireOs WLC de buitenlandse controller is is de configuratie hetzelfde als met slechts twee verschillen.

1. AAA-accounting wordt nooit op het anker uitgevoerd zodat de 9800 geen boekhoudkundige methodelijst zou hebben en de AireOS WLC zou accounting mogelijk hebben gemaakt en naar ISE wijst.
2. Het AireOS zou zich aan de 9800 moeten koppelen in plaats van aan zichzelf. In het beleidsprofiel zou de 9800 geen geselecteerd anker hebben, maar het vakje "Exporteren Anchor" laten aangevinkt.
3. Het is belangrijk op te merken dat wanneer AireOS WLCs de client naar de 9800 exporteren er geen concept van beleidsprofielen is, het alleen de WLAN Profile Name verstuurt. Daarom zal de 9800 de WLAN-profielnaam toepassen die van AireOS wordt verzonden op zowel de WLAN-profielnaam als de beleidsprofielnaam. Dit gezegd hebbende, wanneer het anker worden van een AireOS-WLC naar een 9800 WLC, moet de WLAN-profielnaam op zowel WLC als de Policy Profile Name op de 9800 alle overeenkomen.

Verifiëren

Om de configuratie van de **9800** WLC te controleren voert u de opdrachten uit

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- Beleidsprofiel

```
Show wireless profile policy detailed <profile name>
```

- Beleidslijn

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- Controleer of de mobiliteit bij het anker is

```
Show wireless mobility summary
```

Om de configuratie van AireOS WLC te controleren voert u de opdrachten uit

- AAA

```
Show radius summary
```

Opmerking: RFC3576 is de CoA-configuratie

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- Controleer of mobiliteit in het buitenland is

```
Show mobility summary
```

Problemen oplossen

Problemen oplossen ziet er anders uit, afhankelijk van het punt in het proces dat de client stopt. Bijvoorbeeld, als de WLC nooit een reactie van ISE op MAB krijgt, zou de cliënt vast komen te zitten in de "Policy Manager State: Associatie" en wordt niet geëxporteerd naar de ankerplaats. In

deze situatie zou u alleen problemen oplossen op het buitenland en u zou een RA spoor en een pakketvastlegging voor verkeer tussen de WLC en ISE kunnen verzamelen. Een ander voorbeeld zou zijn dat MAB succesvol is overgegaan maar de cliënt ontvangt geen herleiding. In dat geval moet u ervoor zorgen dat het buitenland de herleiding in de AVP's heeft ontvangen en deze op de cliënt heeft toegepast. U moet ook het anker controleren om te verzekeren de client is met de juiste ACL. Dit bereik van probleemoplossing valt buiten het ontwerp van dit technische document (controleer de referenties voor een generieke client-probleemoplossing-richtlijnen).

Zie Cisco Live voor meer hulp bij het oplossen van problemen met CWA op de 9800 WLC!
presentatie DGTL-TSCENT-404

Catalyst 9800 informatie over probleemoplossing

Clientgegevens

```
show wireless client mac-address
```

Hier kunt u de "Policy Manager State", "Session Manager>Auth Methode", "Mobility Rol" bekijken.

U kunt deze informatie ook vinden in de GUI onder Controle>Clients

Ingesloten pakketvastlegging

Vanaf de CLI start de opdracht *#monitor Capture <Capture name>* en daarna komen de opties beschikbaar.

Ga vanuit de GUI naar probleemoplossing>Packet Capture>+Add

RadioActive Traces

Van de CLI

```
debug wireless mac/ip
```

Gebruik het bestandsindeling van de opdracht om het te stoppen. Dit wordt ingelogd op een bestand in een flitser met de naam "ra_trace", het MAC- of IP-adres van de client en de datum en tijd.

Ga vanuit de GUI naar probleemoplossing>Radioactief spoor>+Add. Voeg het mac- of ip-adres van de klant toe, klik op van toepassing en klik vervolgens op Start. Nadat u het proces een paar keer hebt doorlopen, stop het spoor, genereer het logbestand en download het op uw apparaat.

Informatie over AireOS-probleemoplossing

Clientgegevens

Van de CLI *toon clientgegevens <client mac>*

Vanuit de GUI-monitor>Clients

Debugs van het CLI

Debug client

Debug mobility handoff

Debug mobility config

Referenties

[Mobiliteitstunnel met 9800 controllers](#)

[Draadloze debugging en logcollectie op 9800](#)