

Configuratie van verificatie en probleemoplossing voor bekabelde gasten in draadloze LAN-controller

Inhoud

Inleiding

Dit document beschrijft hoe u bekabelde gasttoegang in 9800 en IRCM met externe webverificatie kunt configureren, verifiëren en oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

9800 WLC

AireOS WLC

Mobiliteitstunnel

ISE

Er wordt aangenomen dat een mobiliteitstunnel tussen de twee WLC's tot stand is gebracht voordat de bekabelde gasttoegang wordt geconfigureerd.

Dit aspect valt buiten het bereik van dit configuratievoorbeeld. Raadpleeg voor uitgebreide instructies het bijgevoegde document [Configuration Mobility Topologies op 9800](#)

Gebruikte componenten

9800 WLC versie 17.12.1

5520 WLC versie 8.10.185.0

ISE-versie 3.1.0.518

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.

Configuratie van bekabelde gast op Catalyst 9800 verankerd aan een andere Catalyst 9800

Netwerkdigram



Netwerktopologie

Configuratie op Foreign 9800 WLC

Web Parameter map configureren

Stap 1: Navigeer naar Configuration > Security > Web Auth, selecteer Global, controleer het virtuele IP-adres van de controller en Trustpoint mapping en zorg ervoor dat het type is ingesteld op webauth.

Parameter Map Name

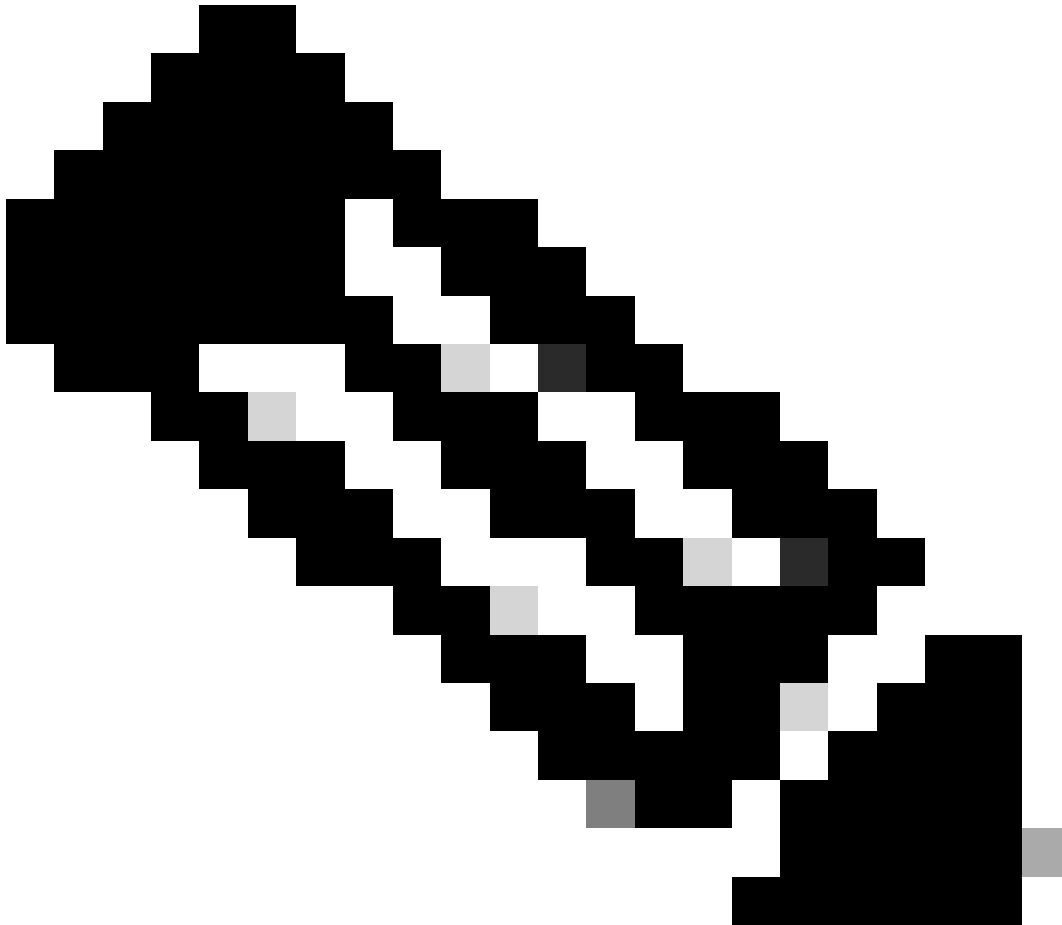
- global
- Web-Filter

1 10

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Globale parameterkaart



Opmerking: Web Auth intercept HTTP is een optionele instelling. Als HTTPS-omleiding vereist is, moet de optie Web Auth Intercept HTTPS zijn ingeschakeld. Deze configuratie wordt echter niet aanbevolen omdat deze het CPU-gebruik verhoogt.

Stap 2: Onder het tabblad Advanced moet u de externe URL van de webpagina configureren voor omleiding naar de client. Stel "Redirect URL for login" en "Redirect On-Failure" in; "Redirect On-Success" is optioneel. Na configuratie wordt een voorvertoning van de doorverwijzing van de URL weergegeven in het webautorisatieprofiel.

General **Advanced**

 Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Tabblad Geavanceerd

CLI-configuratie

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

Opmerking: in dit scenario wordt de globale parameterkaart gebruikt. Zoals per vereiste een aangepaste web parameter map te configureren door Add en te selecteren, stel de omleiding URL onder het tabblad Advanced in. De instellingen voor Trustpoint en Virtual IP worden overgenomen van het globale profiel.

AAA-instellingen:

Stap 1: Een RADIUS-server maken:

Navigeer naar Configuratie > Beveiliging > AAA, klik op "Add" onder de sectie Server/Group en voer op de pagina "AAA Radius Server maken" de servernaam, IP-adres en gedeeld geheim in.

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Add' button is highlighted in red. The 'Name*' and 'Server Address*' fields are also highlighted in red. The 'Key Type' dropdown is set to 'Clear Text'. The 'Auth Port' is 1812, 'Acct Port' is 1813, 'Server Timeout (seconds)' is 1-1000, and 'Retry Count' is 0-100. The 'Support for CoA' is enabled. The 'CoA Server Key Type' is 'Clear Text'. The 'CoA Server Key' and 'Confirm CoA Server Key' fields are empty. The 'Automate Tester' checkbox is unchecked. The 'Cancel' and 'Apply to Device' buttons are at the bottom.

Radius-serverconfiguratie

CLI-configuratie

```
radius server ISE-Auth  
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
```

key *****
server name ISE-Auth

Stap 2: Een RADIUS-servergroep maken:

Selecteer "Add" onder de sectie Servergroepen om een servergroep te definiëren en de servers in te schakelen die moeten worden opgenomen in de groepsconfiguratie.

The screenshot shows the 'Create AAA Radius Server Group' configuration window. The 'Name*' field is highlighted with a red box and contains the text 'ISE-Group'. To its right is a warning icon and the text 'Name is required'. Below this, the 'Group Type' is set to 'RADIUS', 'MAC-Delimiter' is 'none', 'MAC-Filtering' is 'none', 'Dead-Time (mins)' is '5', and 'Load Balance' is 'DISABLED'. The 'Source Interface VLAN ID' field is also highlighted with a red box and contains the value '2074'. At the bottom, the 'Assigned Servers' list contains the server 'ISE-Auth', which is also highlighted with a red box. The 'Available Servers' list is currently empty.

Radius-servergroep

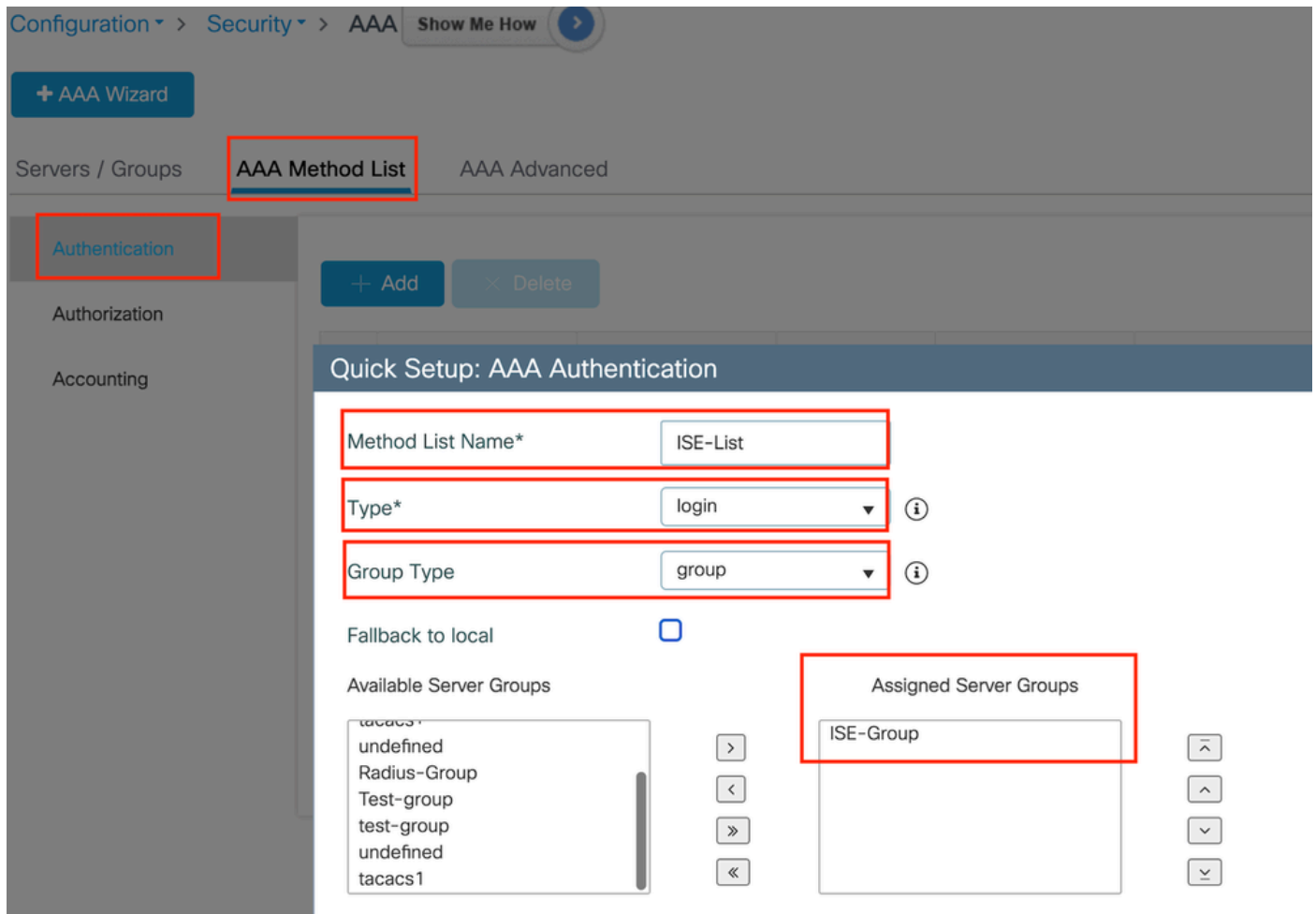
CLI-configuratie

```
aaa group server radius ISE-Group
```

```
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5
```

Stap 3: AAA-methodelijst configureren:

Navigeer naar het tabblad Lijst AAA-methode, selecteer Toevoegen onder Verificatie, definieer een naam voor de methodelijst met Type als "login" en Groepstype als "Groep" en geef de geconfigureerde verificatieservergroep in kaart onder de sectie Toegewezen servergroep.



Lijst met verificatiemethoden

CLI-configuratie

```
aaa authentication login ISE-List group ISE-Group
```

Beleidsprofiel configureren

Stap 1: Navigeer naar Configuratie > Tags & profielen > Beleid, geef uw nieuwe profiel een naam op het tabblad Algemeen en schakel het in via de statusschakelaar.

+ Add

× Delete

Clone

Add 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*

GuestLANPolicy

Description

Enter Description

Status

ENABLED

Passive Client

 DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

 DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

 DISABLED

Beleidsprofiel

Stap 2: Onder het tabblad Toegangsbeleid, wijs een willekeurig VLAN toe als VLAN-toewijzing is voltooid op de ankercontroller. In dit voorbeeld wordt VLAN 1 geconfigureerd

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 ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

Tabblad Toegangsbeleid

Stap 3: Onder het tabblad Mobiliteit schakelen u de ankercontroller om naar Primair (1) en configureert u naar keuze secundaire en tertiaire mobiliteitstunnels voor redundantievereisten

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 (3)	Selected (1)
Anchor IP	Anchor IP Anchor Priority
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.106.40.11 → </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.75 → </div> <div style="border: 1px solid #ccc; padding: 5px;">  10.76.118.74 → </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.70 <input type="text" value="Primary (1)"/> ← </div>

Mobiliteitskaart

CLI-configuratie

```
wireless profile policy GuestLANPolicy
mobility anchor 10.76.118.70 priority 1
no shutdown
```

Gast LAN-profiel configureren

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN, selecteer Add, configureer een unieke profielnaam, schakel bekabeld VLAN in, voer de VLAN-id in voor bekabelde gastgebruikers en schakel de profielstatus in op Enabled.

General	Security
Profile Name*	Client Association Limit
Guest LAN ID*	Wired VLAN Status
mDNS Mode	Wired VLAN ID*
Status	

Profile Name*

Client Association Limit

Guest LAN ID*

Wired VLAN Status ENABLE

mDNS Mode

Wired VLAN ID*

Status ENABLE

LAN-profiel voor gasten

Stap 2: Onder het tabblad Beveiliging, Web Auth inschakelen, de Web Auth parameterkaart toewijzen en de Radius-server selecteren uit de vervolgkeuzelijst Verificatie.

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



Tabblad Beveiliging gastnetwerk

CLI-configuratie

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

KAART VAN HET GASTLAN

Navigeer naar Configuratie > Draadloos > Gastnetwerk.

Selecteer onder de sectie Guest LAN MAP Configuration Add and map the Policy profile and Guest LAN profile

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map: GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page 0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

KAART VAN HET GASTLAN

CLI-configuratie

```
wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy
```

Configuratie op Anker 9800 WLC

Web Parameter map configureren

Stap 1: Navigeer naar Configuration > Security > Web Auth, selecteer Global, controleer het virtuele IP-adres van de controller en Trustpoint mapping en zorg ervoor dat het type is ingesteld op webauth.

Configuration > Security > Web Auth

+ Add × Delete

Parameter Map Name

- global
- Web-Filter

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Stap 2: Onder het tabblad Advanced moet u de externe URL van de webpagina configureren voor omleiding naar de client. Stel "Redirect URL for login" en "Redirect On-Failure" in; "Redirect On-Success" is optioneel.

Na configuratie wordt een voorvertoning van de doorverwijzing van de URL weergegeven in het webautorisatieprofiel.

General **Advanced**

i Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Tabblad Geavanceerd

CLI-configuratie

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable.
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

AAA-instellingen:

Stap 1: Een RADIUS-server maken:

Navigeer naar Configuratie > Beveiliging > AAA, klik op Add onder de sectie Server/Group en voer op de pagina "AAA Radius Server maken" de servernaam, het IP-adres en het gedeelde geheim in.

Configuration > Security > AAA [Show Me How](#)

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS **Servers** Server Groups

Create AAA Radius Server

Name*	<input type="text"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	<input type="text"/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="text"/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		

Cancel Apply to Device

Radius-serverconfiguratie

CLI-configuratie

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

Stap 2: Een RADIUS-servergroep maken:

Selecteer Add onder de sectie Servergroepen om een servergroep te definiëren en de servers om te schakelen die moeten worden opgenomen in de groepsconfiguratie.

Name* ISE-Group

Group Type RADIUS

MAC-Delimiter none ▼

MAC-Filtering none ▼

Dead-Time (mins) 5

Load Balance DISABLED

Source Interface VLAN ID 2081 ▼

Available Servers

Assigned Servers



ISE-Auth

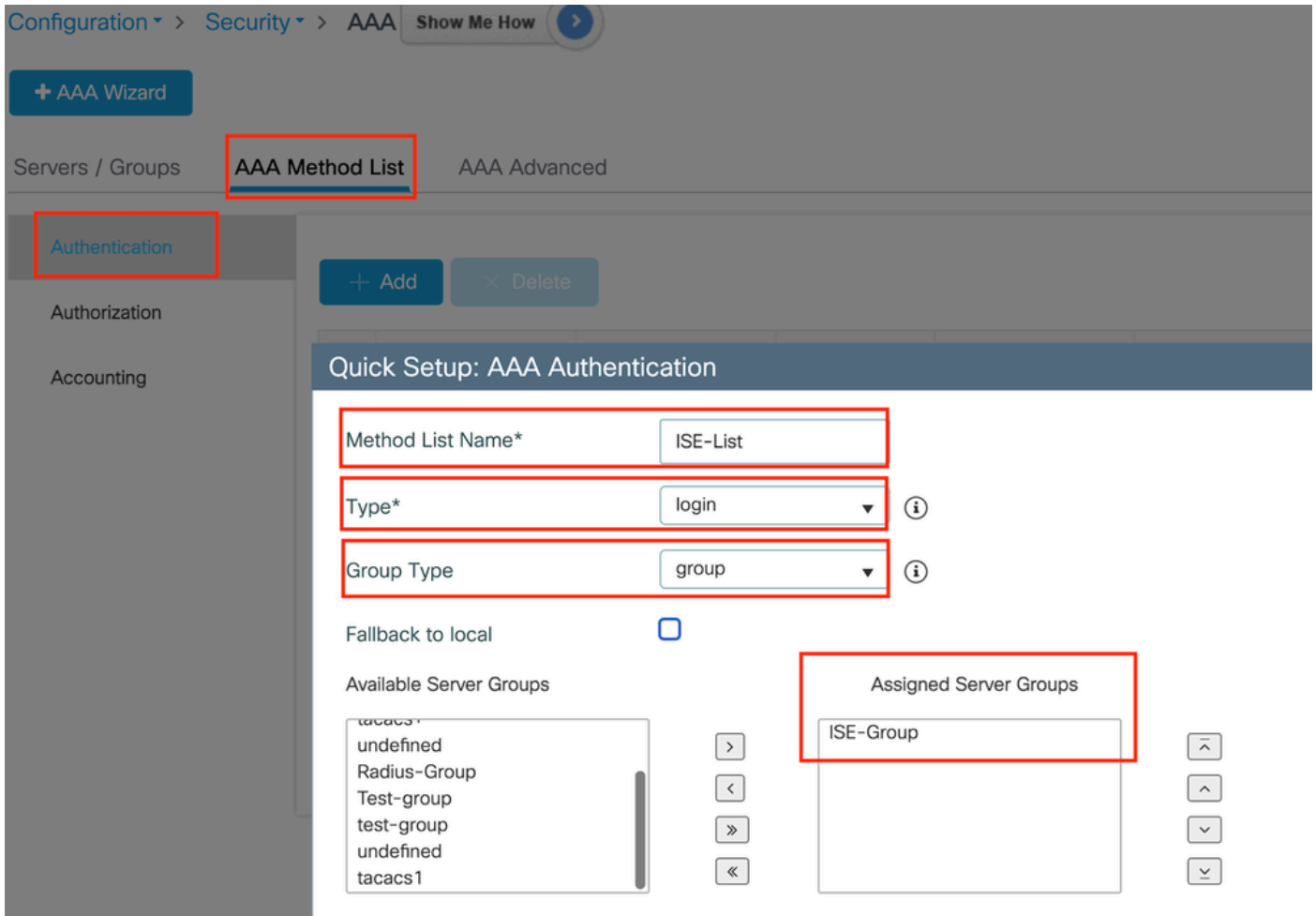
Vak Ankerstraat

CLI-configuratie

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2081
deadtime 5
```

Stap 3: AAA-methodelijst configureren:

Navigeer naar het tabblad AAA-methodelijst, selecteer Add onder Verificatie, definieer een methodelijstnaam met Type als "login" en Groepstype als "Groep" en geef de geconfigureerde verificatieservergroep in kaart onder het vak Toegewezen servergroep.



Lijst met verificatiemethoden

CLI-configuratie

```
aaa authentication login ISE-List group ISE-Group
```

Beleidsprofiel configureren

Stap 1: Navigeer naar Configuration > Tag & Profiles > Policy, configureer het beleidsprofiel met dezelfde naam als op de buitenlandse controller en schakel het profiel in.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*	GuestLANPolicy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
IP MAC Binding	ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy

Central Switching	ENABLED <input checked="" type="checkbox"/>
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	ENABLED <input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/> DISABLED

Ankerbeleidsprofiel

Stap 2: Onder het Toegangsbeleid brengt u het bekabelde client-VLAN in kaart vanuit de vervolgkeuzelijst

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

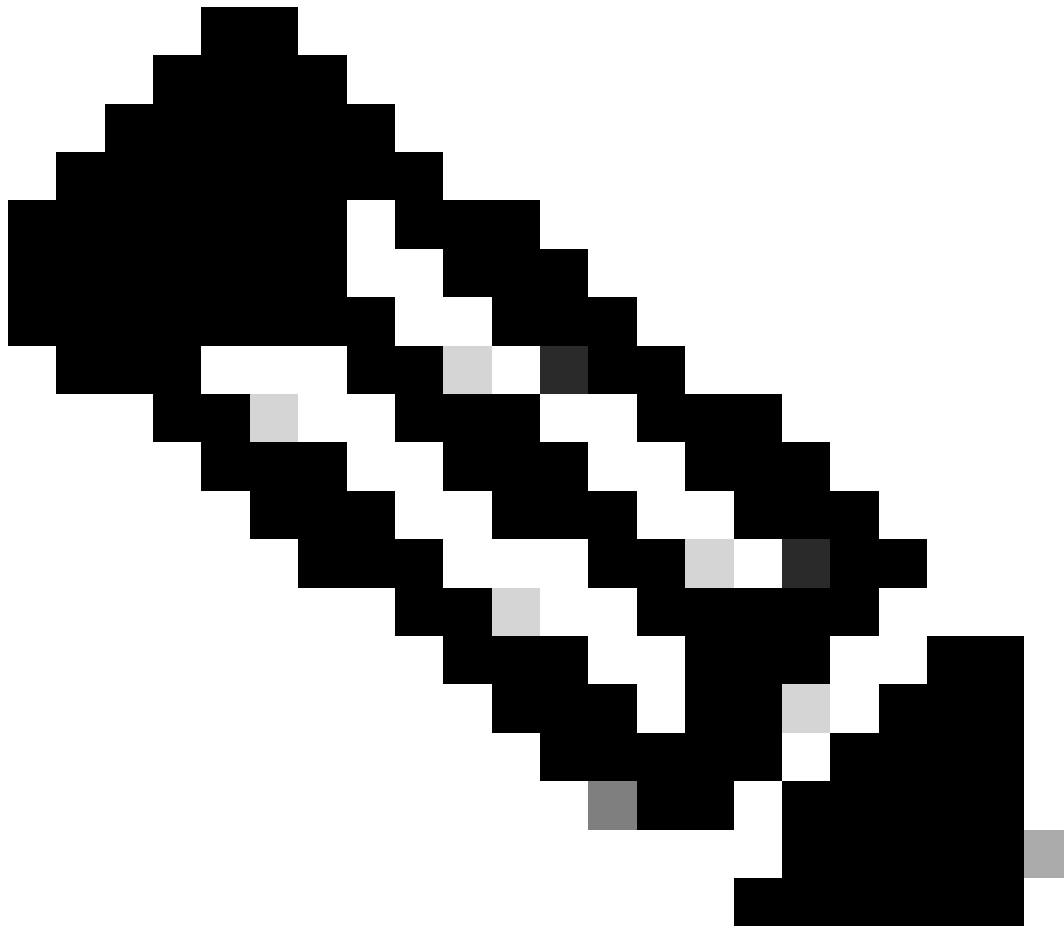


VLAN

VLAN/VLAN Group

VLAN2024





Opmerking: de configuratie van het beleidsprofiel moet overeenkomen op de controllers voor het buitenland en het anker, behalve op het VLAN.

Stap 3: Onder het tabblad Mobiliteit vinkt u het aankruisvakje Exportanker aan.

Mobility Anchors

Export Anchor



Static IP Mobility



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 (2)

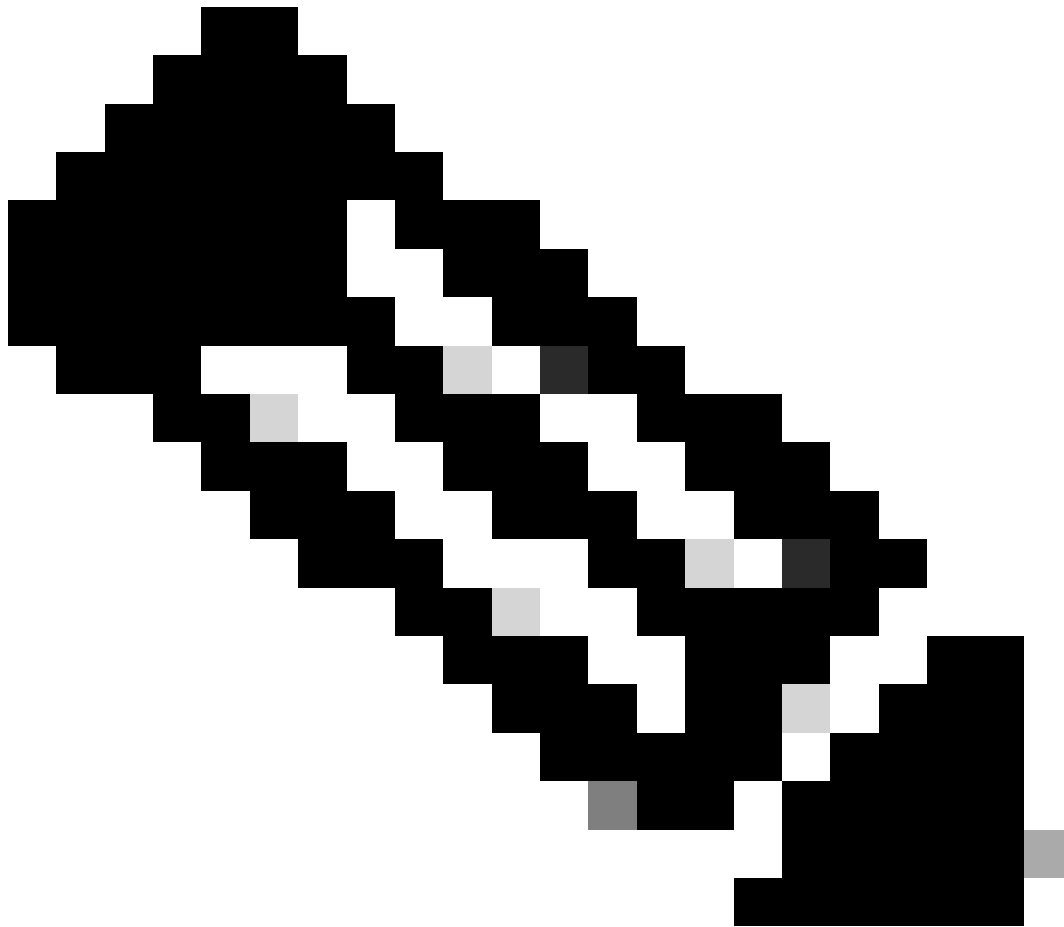
Selected (0)

Anchor IP

Anchor IP

Anchor IP

Anker exporteren



Opmerking: met deze configuratie wordt de 9800 draadloze LAN-controller (WLC) aangewezen als het anker WLC voor elk WLAN dat aan het opgegeven beleidsprofiel is gekoppeld. Wanneer een buitenlandse 9800 WLC clients omleidt naar het anker WLC, biedt het details over het WLAN en het beleidsprofiel dat aan de client is toegewezen. Dit stelt de anker WLC in staat om het juiste lokale beleidsprofiel toe te passen op basis van de ontvangen informatie.

CLI-configuratie

```
wireless profile policy GuestLANPolicy
mobility anchor
vlan VLAN2024
no shutdown
```

Gast LAN-profiel configureren

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN en selecteer vervolgens Add om het Guest LAN-profiel te maken en te configureren. Zorg ervoor dat de profielnaam overeenkomt met die van de buitenlandse controller. Merk op dat bekabeld VLAN moet worden uitgeschakeld op de ankercontroller.

Configuration > Wireless > Guest LAN

> Guest LAN Configuration

+ Add × Delete

Add Guest LAN Profile

General Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

LAN-profiel voor gasten

Stap 2: In de beveiligingsinstellingen, Web Auth inschakelen en vervolgens configureren van de Web Auth parameter map en de Verificatielijst.

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

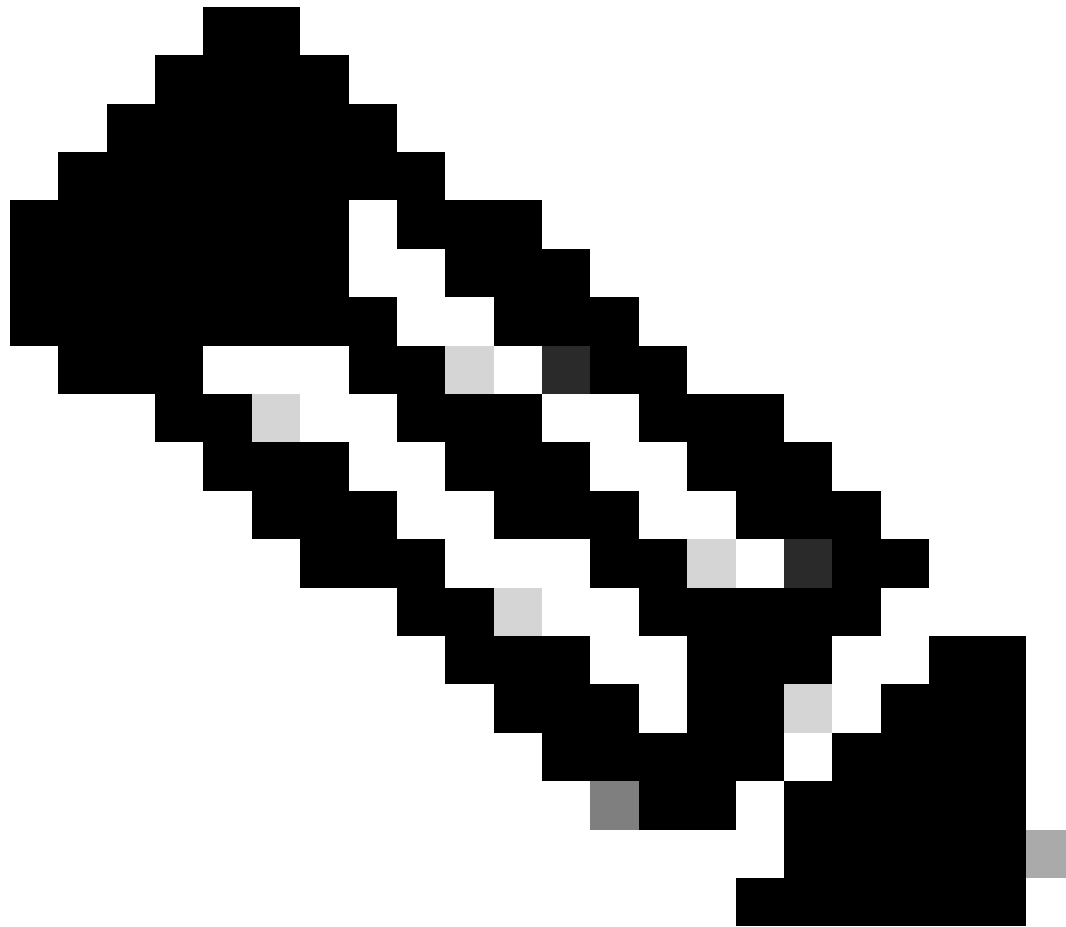
global



Authentication List

ISE-List





Opmerking: de profielconfiguratie van het gastnetwerk moet identiek zijn tussen de controllers voor het buitenland en voor het anker, behalve voor de status van het bekabelde VLAN

CLI-configuratie

```
guest-lan profile-name Guest-Profile 1  
security web-auth authentication-list ISE-List  
security web-auth parameter-map global
```

KAART VAN HET GASTLAN

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN. In de sectie van de configuratie van de Kaart van de Gast LAN, selecteer Add en breng het Profiel van het Beleid aan het LAN van de Gast in kaart profiel.

> Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page 0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

KAART VAN HET GASTLAN

wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy

Configuratie van bekabelde gast op Catalyst 9800 verankerd aan AireOS 5520 controller



Netwerktopologie

Configuratie op Foreign 9800 WLC

Web Parameter map configureren

Stap 1: Navigeer naar Configuration > Security > Web Auth en selecteer Global. Controleer dat het virtuele IP-adres van de controller en het Trustpoint correct in kaart worden gebracht op het profiel, waarbij het type is ingesteld op webauth.

General	Advanced		
Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3... ▼
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth ▼	Virtual IPv6 Address	x::x::x::x
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Web Parameter map

Stap 2: Onder het tabblad Advanced specificeert u de externe URL van de webpagina waarnaar clients moeten worden omgeleid. Configureer de Redirect URL voor aanmelding en wijs de fout opnieuw toe. De instelling Redirect On-Success is een optionele configuratie.

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

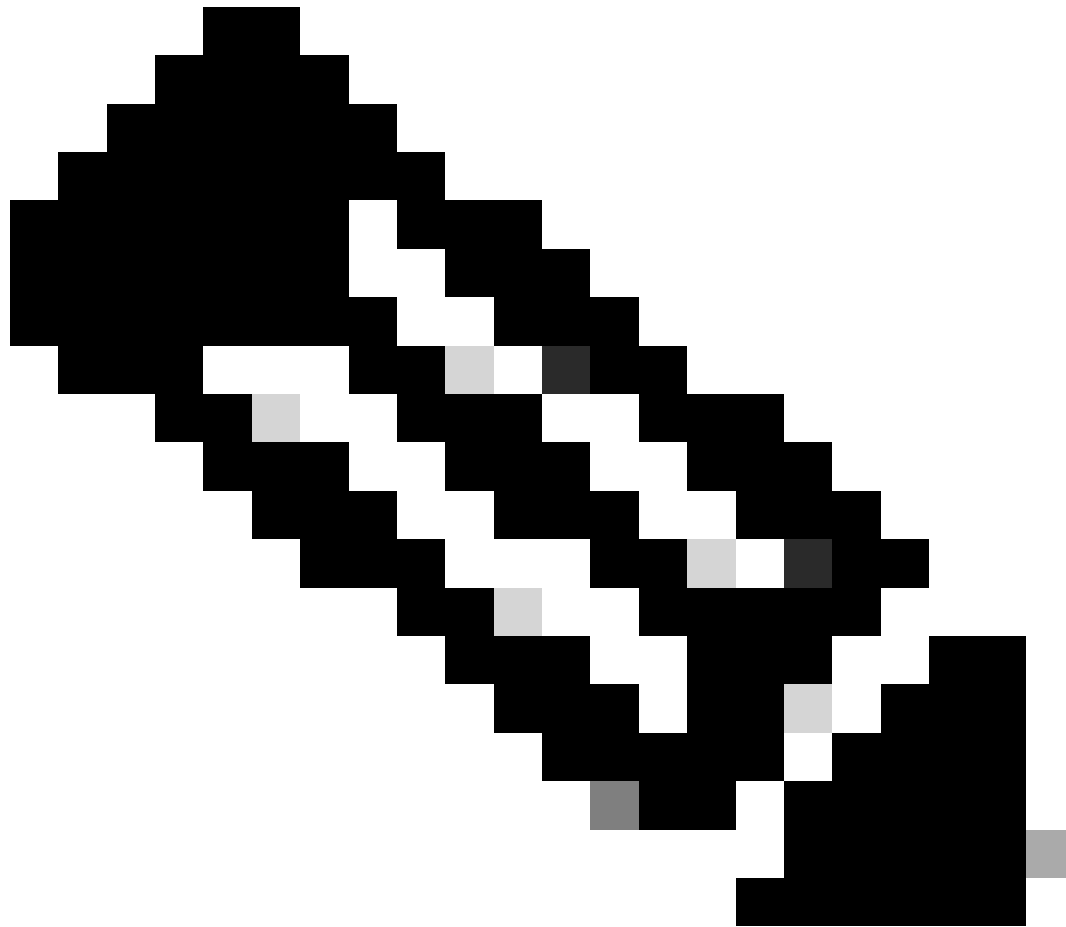
Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X::X"/>

Tabblad Geavanceerd

CLI-configuratie

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Opmerking: Raadpleeg voor AAA-configuratie de configuratiegegevens in het gedeelte "" voor de Foreign 9800 WLC.

Beleidsprofiel configureren

Stap 1: Navigeer naar Configuration > Tags & profielen > Policy. Selecteer Toevoegen en voer op het tabblad Algemeen een naam voor het profiel in en schakel de statusschakelaar in.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Beleidsprofiel

Stap 2: Wijs in het tabblad Toegangsbeleid een willekeurig VLAN toe.

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

1



Multicast VLAN

Enter Multicast VLAN

Toegangsbeleid

Stap 3: Op het tabblad Mobiliteit kunt u de ankercontroller schakelen en de prioriteit instellen op Primair (1)

Mobility Anchors

Export Anchor



Static IP Mobility



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)


Anchor IP

 10.76.6.156	→
---	---

Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) ▼
--	---------------

Tabblad Mobilitet

Opmerking: het beleidsprofiel van de 9800 Foreign WLC moet overeenkomen met het gastLAN-profiel van de 5520 Anker WLC behalve de VLAN-configuratie

CLI-configuratie

```
wireless profile policy Guest
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor 10.76.118.74 priority 1
no shutdown
```

Gast LAN-profiel configureren

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN en selecteer Add. Configureer een

unieke profielnaam en schakel bekabeld VLAN in. Specificeer de VLAN-id die is toegewezen aan bekabelde gastgebruikers. Schakel tot slot de profielstatus in op Ingeschakeld.

General

Security

Profile Name*	Guest	Client Association Limit	2000
Guest LAN ID*	2	Wired VLAN Status	ENABLE <input checked="" type="checkbox"/>
mDNS Mode	Bridging	Wired VLAN ID*	11
Status	ENABLE <input checked="" type="checkbox"/>		

Gast LAN-beleid

Stap 2: Onder het tabblad Security, Web Auth inschakelen, de Web Auth parameter map toewijzen en de RADIUS-server selecteren uit de vervolgkeuzelijst Verificatie.

General

Security

Layer3

Web Auth

ENABLE

Web Auth Parameter Map

global

Authentication List

ISE-List

Tabblad Beveiliging

Opmerking: de naam van het gastLAN-profiel moet dezelfde zijn voor de 9800 Foreign en 5520 Anker-controller

CLI-configuratie

```
guest-lan profile-name Guest 2 wired-vlan 11
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

KAART VAN HET GASTLAN

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN. In de sectie van de configuratie van de Kaart van het Gast LAN, selecteer Add en breng het Beleidsprofiel aan het LAN van de Gast in kaart profiel.

➤ Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page 0 - 0 of 0 items

Profile Name: Guest

Policy Name: Guest

Save Cancel

KAART VAN HET GASTLAN

CLI-configuratie

```
wireless guest-lan map GuestMap
guest-lan Guest policy Guest
```

Configuratie op anker 5520 WLC

Webverificatie configureren

Stap 1: Navigeer naar Security > Web Auth > Web Login Page. Stel het type webverificatie in op Extern (omleiden naar externe server) en configureer de externe URL voor webautorisatie. De Redirect URL na aanmelding is optioneel en kan worden geconfigureerd als clients moeten worden omgeleid naar een speciale pagina na succesvolle verificatie.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Save Configuration Ping Logout Refresh

User: admin(ReadWrite) Home

Security

Web Login Page

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: http://10.127.196.171/webauth/logout.html

Login Success Page Type: None

External Webauth URL: http://10.127.196.171/webauth/login.html

QrCode Scanning Bypass Timer: 0

QrCode Scanning Bypass Count: 0

Preview... Apply

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Auth Cached Users
 - Fallback
 - DNS
 - Downloaded AVP
- TACACS+
- LDAP
 - Local Net Users
 - MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
 - Web Login Page
 - Certificate

Instellingen webautorisatie

AAA-instellingen:

Stap 1: Straal server configureren

Navigeer naar Security > Radius > Verificatie > Nieuw.



Radius-server

Stap 2: Het configureren van de RADIUS-server IP en gedeeld geheim op de controller. Schakel de serverstatus in op Ingeschakeld en controleer het selectievakje Netwerkgebruiker.

RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Serverconfiguratie

Toegangscontrolelijst configureren

Stap 1: Navigeer naar Security > Access Control List en selecteer Nieuw. Maak een pre-verificatie

ACL die verkeer naar DNS en de externe webserver toelaat.

The screenshot shows the Cisco ISE Security configuration page for 'Access Control Lists > Edit'. The 'SECURITY' tab is highlighted in the top navigation bar. The left sidebar shows the 'Access Control Lists' menu item highlighted. The main content area displays the 'General' configuration for the 'Pre-Auth_ACL' list, showing 'Deny Counters' set to 0. Below this is a table of access list entries:

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Toeganglijst om verkeer naar webserver toe te laten

Gast LAN-profiel configureren

Stap 1: Navigeer naar WLAN's > selecteer Nieuw maken.

Selecteer Type als Guest LAN en configureer dezelfde naam als het beleidsprofiel van de 9800 Foreign controller.

The screenshot shows the Cisco ISE WLANs configuration page. The 'WLANs' tab is highlighted in the top navigation bar. The 'Create New' button is highlighted with a red box. Below the navigation bar, there is a 'Current Filter: None' section with links for '[Change Filter]' and '[Clear Filter]'. Below that, there is a table with columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. The 'Create New' button is highlighted with a red box.

Gastnetwerk maken

The screenshot shows the Cisco ISE WLANs configuration page for creating a new WLAN. The 'WLANs > New' page is displayed. The 'Type' dropdown menu is set to 'Guest LAN' and is highlighted with a red box. The 'Profile Name' field is set to 'Guest' and the 'ID' field is set to '2'. The 'Apply' button is highlighted with a red box.

LAN-profiel voor gasten

Stap 2: Stel de Ingress en uitgaande interfaces in kaart op het Guest LAN profiel.

De Ingress-interface is in dit geval geen omdat de ingangsiinterface de EoIP-tunnel is van de

Foreign controller.

De uitgaande interface is VLAN waar de bekabelde client fysiek verbinding maakt.

The screenshot shows the configuration page for a Guest profile. The 'Security' tab is selected. The 'Profile Name' is 'Guest', the 'Type' is 'Guest LAN', and the 'Status' is 'Enabled'. The 'Ingress Interface' is 'None' and the 'Egress Interface' is 'wired-vlan-11'. The 'NAS-ID' is 'none'. The 'Web-Auth' section is expanded, showing a note: '(Modifications done under security tab will appear after applying the changes.)'

LAN-profiel voor gasten

Stap 3: Selecteer onder het tabblad Beveiliging Layer 3-beveiliging als webverificatie en wijs de pre-verificatie ACL toe.

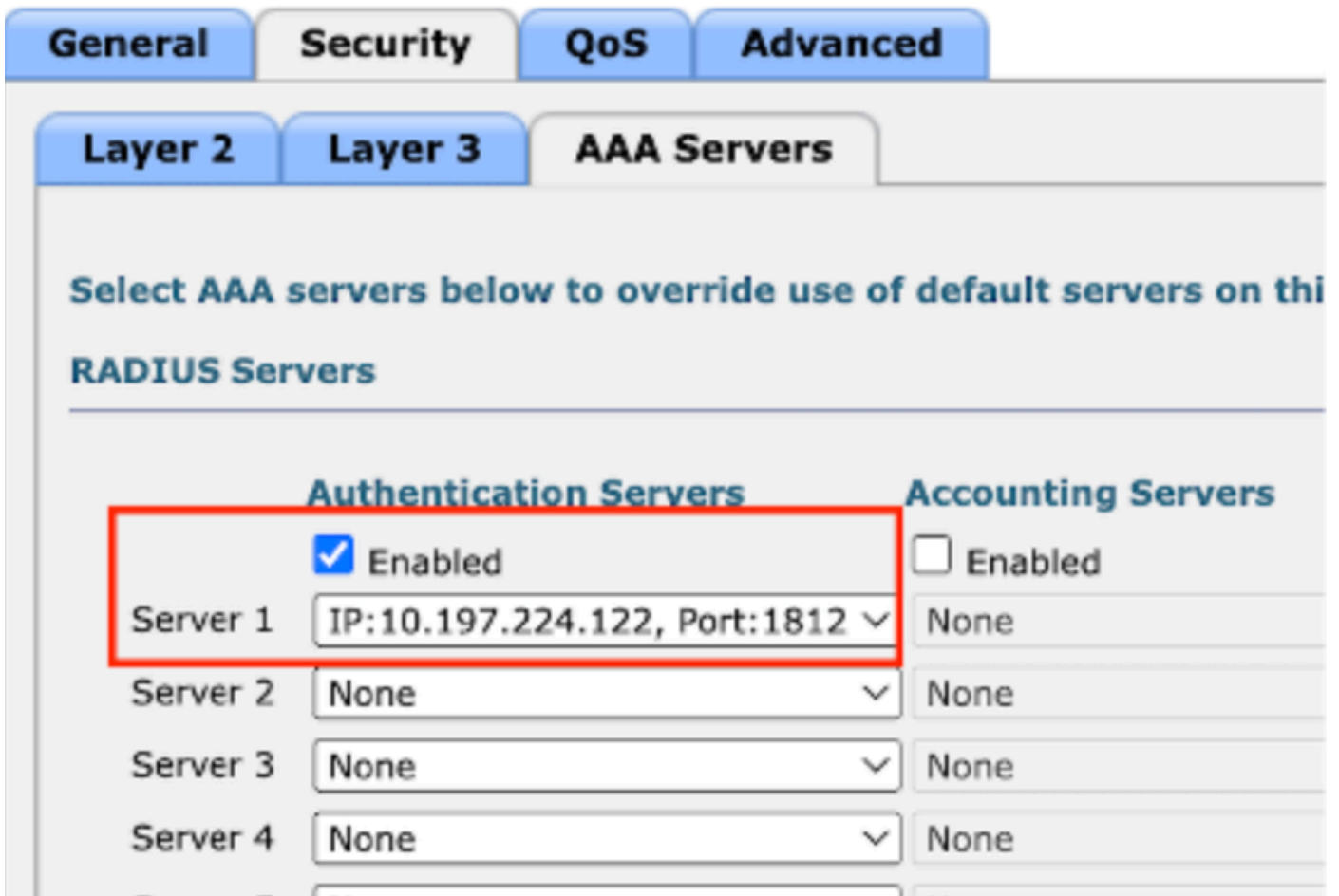
WLANS > Edit 'Guest'

The screenshot shows the configuration page for a Guest profile in the 'Security > Layer 3 > AAA Servers' tab. The 'Layer 3 Security' section is expanded, showing 'Preauthentication ACL' set to 'Pre-Auth_ACL' for IPv4 and 'None' for IPv6. The 'Web Authentication' dropdown is set to 'Web Authentication'. The 'Override Global Config' checkbox is unchecked.

Tabblad Beveiliging gastnetwerk

Stap 4: Navigeer naar Security > AAA-server.

Selecteer de uitrollijst en wijs de radiusserver toe aan het profiel voor het gastnetwerk.



Radiusserver toewijzen aan het LAN-profiel

Stap 5: Navigeer naar WLAN. Beweeg het uitrolpictogram van het gastLAN-profiel en selecteer Mobility Anchors.



Stap 6: Selecteer Mobility Anchor Create om de controller te configureren als exportanker voor dit gastLAN-profiel.



Mobiliteitsanker maken

Wired Guest configureren op AireOS 5520 verankerd aan Catalyst 9800



Netwerktopologie

Configuratie op Foreign 5520 WLC

Configuratie van controllerinterface

Stap 1: Navigeer naar Controller > Interfaces > Nieuw. Configureer een interfacenaam, VLAN-id en schakel gastLAN in.

De bekabelde gast vereist twee dynamische interfaces.

Maak eerst een Layer 2 dynamische interface en wijs deze aan als gastLAN. Deze interface fungeert als de toegangsinterface voor Guest LAN, waar bekabelde clients fysiek verbinding maken.

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANA'. The left sidebar lists various configuration categories, with 'Interfaces' highlighted in red. The main content area is titled 'Interfaces > Edit' and is divided into several sections:

- General Information:** Interface Name is 'wired-guest' (highlighted in red), and MAC Address is 'a0:e0:af:32:d9:ba'.
- Configuration:** 'Guest Lan' is checked (highlighted in red), and NAS-ID is 'none'.
- Physical Information:** Port Number is '1', Backup Port is '0', and Active Port is '1'.
- Interface Address:** VLAN Identifier is '2020' (highlighted in red), DHCP Proxy Mode is 'Global', and 'Enable DHCP Option 82' is unchecked.

Ingress-interface

Stap 2: Navigeer naar Controller > Interfaces > Nieuw. Configureer een interfacenaam, VLAN-id.

De tweede dynamische interface moet een Layer 3-interface op de controller zijn, de bekabelde clients ontvangen IP-adres van dit VLAN-subnetnummer. Deze interface fungeert als de uitgangsinterface voor het LAN-profiel van de gast.

Controller

Interfaces > Edit

General Information

Interface Name	vlan2024
MAC Address	a0:e0:af:32:d9:ba

Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Uitgaande interface

Switch-poortconfiguratie

Gebruikers van bekabelde gasten verbinden met Access Layer switch; deze aangewezen poorten moeten worden geconfigureerd met VLAN waarin Guest LAN is ingeschakeld op de controller

Poortconfiguratie voor switch op toegangslaag

interface Gigabit Ethernet <x/x>

Beschrijving Wired Guest Access

switchport access VLAN 2020

toegang tot switchport-modus

doel

Configuratie van externe controller-uplinkpoort

interface TienGigabit Ethernet<x/x>

beschrijving Trunkpoort naar de Foreign WLC

switchport mode-trunk

switchport trunk native VLAN 2081

switchport trunk toegestaan VLAN 2081.2020

doel

Configuratie van uplinkpoorten voor ankercontrollers

interface TienGigabit Ethernet<x/x>

beschrijving Trunkpoort naar het anker WLC

switchport mode-trunk

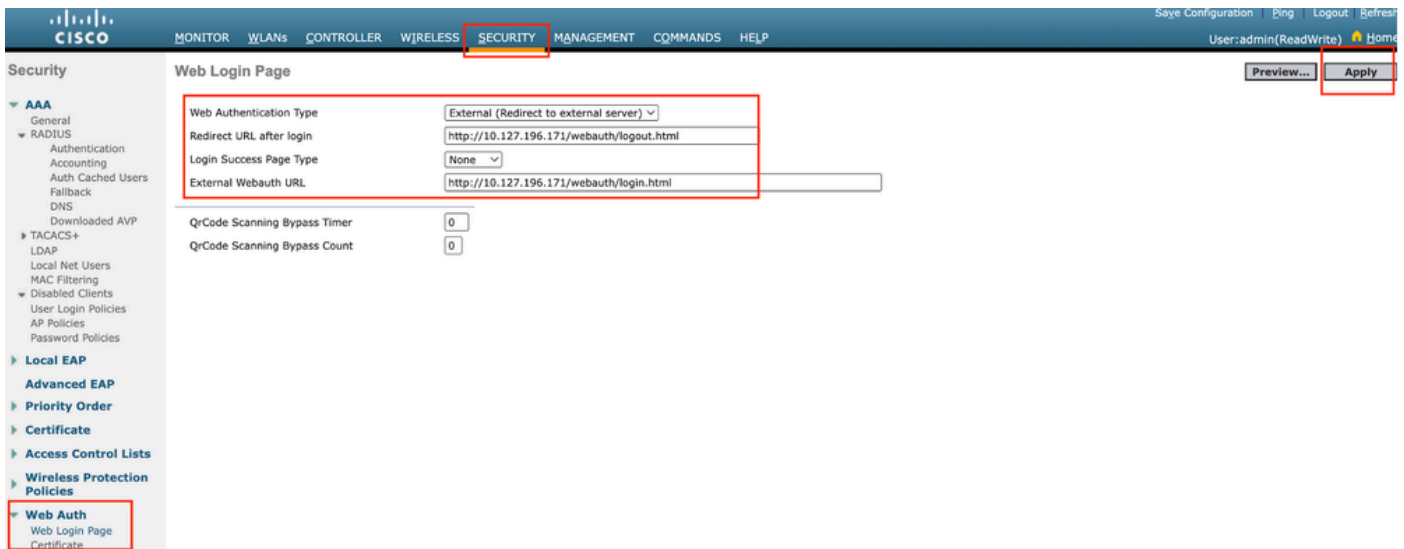
switchport trunk native VLAN 2081

switchport trunk toegestaan VLAN 2081.2024

doel

Webverificatie configureren

Stap 1: Navigeer naar Security > Web Auth > Web Login Page. Stel het type webverificatie in op Extern (omleiden naar externe server) en configureer de externe URL voor webautorisatie. De Redirect URL na aanmelding is optioneel en kan worden geconfigureerd als clients moeten worden omgeleid naar een speciale pagina na succesvolle verificatie.



Instellingen webautorisatie

AAA-instellingen:

Stap 1: Straal server configureren

Navigeer naar Security > Radius > Verificatie > Nieuw.



Radius-server

Stap 2: Het configureren van de RADIUS-server IP en gedeeld geheim op de controller. Schakel de serverstatus in op Ingeschakeld en controleer het selectievakje Netwerkgebruiker.

RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Serverconfiguratie

Toegangscontrolelijst configureren

Stap 1: Navigeer naar Security > Access Control List en selecteer Nieuw. Maak een pre-verificatie

ACL die verkeer naar DNS en de externe webserver toelaat.

The screenshot shows the Cisco ISE Security configuration page for 'Access Control Lists > Edit'. The 'SECURITY' tab is highlighted in the top navigation bar. The left sidebar shows the 'Access Control Lists' menu item highlighted. The main content area is titled 'General' and shows the 'Access List Name' as 'Pre-Auth_ACL' and 'Deny Counters' as '0'. Below this is a table with 11 columns: Seq, Action, Source IP/Mask, Destination IP/Mask, Protocol, Source Port, Dest Port, DSCP, Direction, Number of Hits, and a checkbox. The table contains six rows of permit rules for various protocols and destinations.

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0	<input checked="" type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0	<input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0	<input checked="" type="checkbox"/>
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0	<input checked="" type="checkbox"/>
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0	<input checked="" type="checkbox"/>
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0	<input checked="" type="checkbox"/>

Toeganglijst om verkeer naar webserver toe te laten

Gast LAN-profiel configureren

Stap 1: Navigeer naar WLAN > Nieuw maken > Ga.

The screenshot shows the Cisco ISE WLAN configuration page. The 'WLANs' tab is highlighted in the top navigation bar. The left sidebar shows the 'WLANs' menu item highlighted. The main content area shows the 'Current Filter' as 'None' with links for '[Change Filter]' and '[Clear Filter]'. A 'Create New' button with a dropdown arrow and a 'Go' button are highlighted with a red box. Below this is a table header with columns: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies.

LAN-profiel voor gasten

Selecteer Type als gastnetwerk en configureer een profielnaam. De zelfde naam moet op het beleidsprofiel en het LAN van de Gast profiel van het Ankercontrolemechanisme worden gevormd 9800.

WLANs > New

Type

Guest LAN

Profile Name

Guest-Profile

ID

3

LAN-profiel voor gasten

Stap 2: Onder het tabblad Algemeen, Kaart de Ingress en Uitgang interface op het Gast LAN profiel.

Ingress interface is het VLAN waarmee de bekabelde clients fysiek verbinding maken.

Uitgaande interface is het VLAN-subnetnummer dat door de clients wordt aangevraagd voor IP-adres.

General	Security	QoS	Advanced
Profile Name	Guest-Profile		
Type	Guest LAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	Web-Auth (Modifications done under security tab will appear after applying th		
Ingress Interface	wired-guest		
Egress Interface	vlan2024		
NAS-ID	none		

LAN-profiel voor gasten

Stap 3: Navigeer naar Security > Layer 3.

Selecteer Layer 3 Security als webverificatie en wijs de pre-verificatie ACL toe.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security

Preauthentication ACL IPv4 Pre-Auth_ACL IPv6 None

Override Global Config²⁰ Enable

Web Authentication

Layer 3-beveiligingstabblad

Stap 4:

Stel onder het tabblad AAA-servers de Radius-server in kaart en schakel het selectievakje Ingeschakeld in.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on the

RADIUS Servers

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.197.224.122, Port:1812	<input type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None
Server 4	None	None

Toewijzing van radiusservers aan het profiel van het Gastnetwerk

Stap 5: Navigeer naar WLAN-pagina en zweef over het dropdown-pictogram van het gastLAN-profiel en selecteer Mobility Ankers.

<input type="checkbox"/> 30	WLAN	guest-1665	guest-1665	Disabled	[WPA + WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>
<input type="checkbox"/> 1	Guest LAN	Guest-Profile	---	Enabled	Web-Auth	<input type="checkbox"/>
<input type="checkbox"/> 2	Guest LAN	Guest	---	Disabled	Web-Auth	<input type="checkbox"/>

Mobiliteitsankers

Stap 6: Breng het mobiliteitsanker van de drop-down lijst aan het LAN van de Gast Profiel in kaart.

Mobility Anchors

WLAN SSID Guest-Profile

Switch IP Address (Anchor)

local

10.106.39.41

10.76.6.156

10.76.118.70

Switch IP Address (Anchor)

Data Path

Foot Notes

Mobiliteitsanker toewijzen aan Gast LAN

Configuratie op Anker 9800 WLC

Web Parameter map configureren

Stap 1: Navigeer naar Configuration > Security > Web Auth en selecteer Global. Controleer dat het virtuele IP-adres van de controller en het Trustpoint correct in kaart worden gebracht op het profiel, waarbij het type is ingesteld op webauth.

General

Advanced

Parameter-map Name Maximum HTTP connections Init-State Timeout(secs) Type Captive Bypass Portal Disable Success Window Disable Logout Window Disable Cisco Logo Sleeping Client Status Sleeping Client Timeout (minutes) Virtual IPv4 Address Trustpoint Virtual IPv4 Hostname Virtual IPv6 Address Web Auth intercept HTTPs Enable HTTP server for Web Auth Disable HTTP secure server for Web Auth **Banner Configuration**Banner Title Banner Type None Banner Text Read From File

Web Parameter map

Stap 2: Onder het tabblad Advanced specificeert u de externe URL van de webpagina waarnaar clients moeten worden omgeleid. Configureer de Redirect URL voor aanmelding en wijs de fout opnieuw toe. De instelling Redirect On-Success is een optionele configuratie.

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

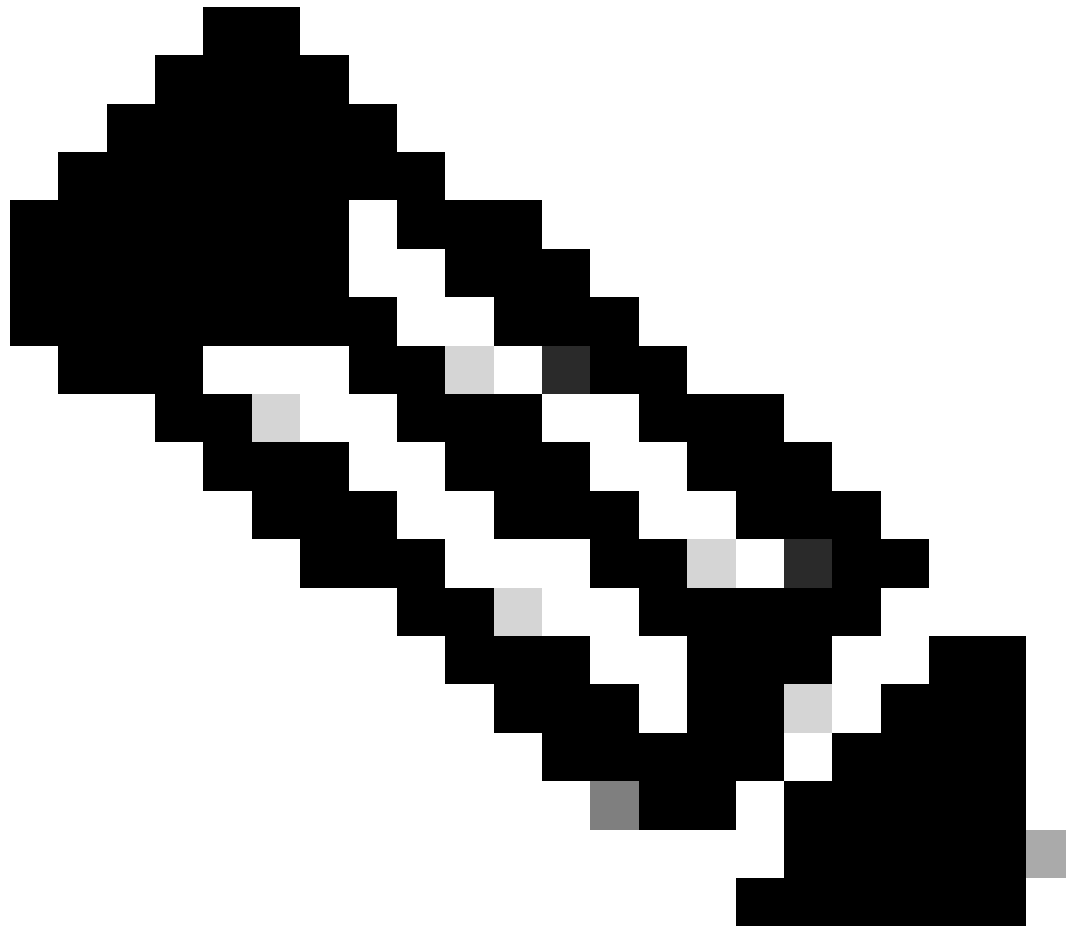
Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X"/>

Tabblad Geavanceerd

CLI-configuratie

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Opmerking: Raadpleeg voor AAA-configuratie de configuratiegegevens in de sectie "Configure Wired Guest on Catalyst 9800 verankerd aan een andere Catalyst 9800" voor de Foreign 9800 WLC.

Beleidsprofiel configureren

Stap 1: Navigeer naar Configuratie > Tags en profielen > Beleid. Configureer het beleidsprofiel met dezelfde naam die wordt gebruikt voor het gastLAN-profiel van de buitenlandse controller.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

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

Beleidsprofiel

Stap 2: Onder het tabblad Toegangsbeleid brengt u het bekabelde client-VLAN in kaart vanuit de vervolgkeuzelijst

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

VLAN2024



Multicast VLAN

Enter Multicast VLAN

Toegangsbeleid

Stap 3: Onder het tabblad Mobiliteit vinkt u het aankruisvakje Exportanker aan.

Mobility Anchors

Export Anchor



Static IP Mobility



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

Tabblad Mobiliteit

CLI-configuratie

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

Gast LAN-profiel configureren

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN en selecteer Add om het Guest LAN-profiel te configureren en de status van bekabeld VLAN uit te schakelen.

De naam van het LAN van de gast op Anchor moet het zelfde zijn als het LAN van de Gast profiel op Buitenlandse WLC.

General

Security

Profile Name*

Guest-Profile

Client Association Limit

2000

Guest LAN ID*

1

Wired VLAN Status



DISABLE

mDNS Mode

Bridging ▼

Status

ENABLE



LAN-profiel voor gasten

Stap 2: Onder het tabblad Security, Web Auth inschakelen. Selecteer de Webautorisatieparameterkaart en de Verificatielijst in de vervolgkeuzelijst

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global ▼

Authentication List

ISE-List ▼

Tabblad LAN-beveiliging

CLI-configuratie

```
guest-lan profile-name Guest-Profile 1
```

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

KAART VAN HET GASTLAN

Stap 1: Navigeer naar Configuration > Wireless > Guest LAN. In de sectie van de configuratie van de Kaart van het Gast LAN, selecteer Add en breng het Beleidsprofiel aan het LAN van de Gast in kaart profiel.

> Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map: GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page 0 - 0 of 0 items

Profile Name: Guest-Profile

Policy Name: Guest-Profile

✓ Save ↺ Cancel

KAART VAN HET GASTLAN

Verifiëren

Configuratie van controller valideren

#show guest-lan samenvatting

GLAN	GLAN Profile Name	Status
1	Guest-Profile	UP
2	Guest	UP

#show guest-lan ID 1

<#root>

```
Guest-LAN Profile Name      : Guest
=====
Guest-LAN ID                : 2
Wired-Vlan                  :
```

```

Status :
Enabled
Number of Active Clients : 0
Max Associated Clients : 2000
Security
  WebAuth :
Enabled
  Webauth Parameter Map : global
  Webauth Authentication List :
ISE-List
  Webauth Authorization List : Not configured
mDNS Gateway Status : Bridge

```

#show parameter-map type webauth global

```

<#root>
Parameter Map Name : global
Type :
webauth
  Redirect:
  For Login :
http://10.127.196.171/webauth/login.html
  On Success :
http://10.127.196.171/webauth/logout.html
  On Failure :
http://10.127.196.171/webauth/failed.html
  Portal ipv4 :
10.127.196.171
  Virtual-ipv4 :
192.0.2.1

```

#show parameter-map type webauth naam <profielnaam> (Als aangepaste web parameter profiel wordt gebruikt)

#show Wireless guest-lan-map samenvatting

GLAN Profile Name	Policy Name
Guest	Guest

#show overzicht draadloze mobiliteit

IP	Public Ip	MAC Address
10.76.118.70	10.76.118.70	f4bd.9e59.314b

#show ip http server status

HTTP server status: Enabled
HTTP server port: 80
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local

HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server trustpoint: TP-self-signed-3010594951

>Gastenoverzicht weergeven

Number of Guest LANs..... 1

GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

>Gastenoverzicht weergeven 2

Guest LAN Identifier..... 2
Profile Name..... Guest
Status..... Enabled
Interface..... wired-vlan-11
Radius Servers
 Authentication..... 10.197.224.122 1812 *
 Web Based Authentication..... Enabled
 Web Authentication Timeout..... 300
 IPv4 ACL..... Pre-Auth_ACL
 Mobility Anchor List
GLAN ID IP Address Status

2 10.76.118.74 Up

>Aangepast web weergeven

```
Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode..... None
Web Authentication Type..... External
Logout-popup..... Enabled
External Web Authentication URL..... http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer..... 0
QR Code Scanning Bypass Count..... 0
```

>toon custom-web guest-lan 2

```
Guest LAN Status..... Enabled
Web Security Policy..... Web Based Authentication
WebAuth Type..... External
Global Status..... Enabled
```

Beleidsstatus client valideren

in het buitenland,

Samenvatting van draadloze client #show

De staat van de de beleidsmanager van de cliënt op de Buitenlandse controller wordt IN WERKING GESTELD nadat de cliënt met succes associeert.

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	N/A			

GLAN 1

Run

802.3

Web Auth

Export Foreign

>toon clientdetail a0ce.c8c3.a9b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username N/A
Client Webauth Username N/A
Client State..... Associated
User Authenticated by None
Client User Group.....
Client NAC OOB State..... Access
guest-lan..... 1
Wireless LAN Profile Name..... Guest-Profile
Mobility State.....

Export Foreign

Mobility Anchor IP Address.....
10.76.118.70

Security Policy Completed.....

Yes

Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
EAP Type..... Unknown
Interface.....

wired-guest-egress

VLAN..... 2024
Quarantine VLAN..... 0

Op Anchor,

De overdracht van de clientstatus moet op de ankercontroller worden bewaakt.

De staat van de Clientbeleidsmanager is in behandeling voor Web Auth.

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	10.76.6.156			

GLAN 1

Webauth Pending

802.3

Web Auth

Export Anchor

Zodra de client is geverifieerd, verandert de status van de beleidsmanager in de status RUN.

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

#show draadloze client mac-adres a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :

10.105.211.69

Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
GLAN Id: 1
GLAN Name: Guest-Profile

Mobility:

Foreign IP Address :

10.76.118.74

Point of Attachment : 0xA0000003
Point of Presence : 0
Move Count : 1
Mobility Role :

Export Anchor

Mobility Roam Type :

L3 Requested

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:

Point of Attachment : mobility_a0000003
IIF ID : 0xA0000003
Authorized : FALSE
Session timeout : 28800
Common Session ID: 4a764c0a0000008ea0285466

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State :

Login

Webauth Method :

Webauth

Server Policies:

Resultant Policies:

URL Redirect ACL :

WA-v4-int-10.127.196.171

Preauth ACL :

WA-sec-10.127.196.171

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

De client beweegt zich om de status uit te voeren na succesvolle webverificatie.

toon draadloze client mac-adres a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5

Client MAC Type : Universally Administered Address

Client DUID: NA

Client IPv4 Address :

10.105.211.69

Client Username :

testuser

Client State : Associated

Policy Profile : Guest-Profile

Flex Profile : N/A

Guest Lan:

GLAN Id: 1

GLAN Name: Guest-Profile

Wireless LAN Network Name (SSID) : N/A

BSSID : N/A

Connected For : 81 seconds

Protocol : 802.3

Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 81 seconds

VLAN : VLAN2024

Last Tried Aaa Server Details:

Server IP :

10.197.224.122

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Resultant Policies:

URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

>toon clientdetail a0:ce:c8:c3:a9:b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username N/A
Client Webauth Username N/A
Client State..... Associated
Wireless LAN Profile Name..... Guest
WLAN Profile check for roaming..... Disabled
Hotspot (802.11u)..... Not Supported
Connected For 90 secs
IP Address..... 10.105.211.75
Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

Export Anchor

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No

Policy Manager State.....

WEBAUTH_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth_ACLPre-auth

IPv4 ACL Applied Status..... Yes
Pre-auth IPv4 ACL Applied Status.....

Yes

Na de Versies van de Verificatieclient om de status uit te voeren.

<#root>

show client detail a0:ce:c8:c3:a9:b5
Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username

testuser

Client Webauth Username

testuser

Client State.....

Associated

User Authenticated by

RADIUS Server

Client User Group..... testuser
Client NAC OOB State..... Access
Connected For 37 secs
IP Address.....

10.105.211.75

Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

Export Anchor

Mobility Foreign IP Address..... 10.76.118.70
Security Policy Completed..... Yes
Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
Pre-auth IPv4 ACL Applied Status..... Yes
EAP Type..... Unknown
Interface.....

wired-vlan-11

VLAN.....

11

Quarantine VLAN..... 0

Problemen oplossen

debug van AireOS-controller

Clientdebug inschakelen

```
>debug client <H.H>
```

Om te verifiëren of debugging is ingeschakeld

```
>debuggen tonen
```

debug uitschakelen

debug, uitschakelen

9800 radioactief spoor

Activeer Radio Active Tracing om client debug sporen te genereren voor het opgegeven MAC-adres in de CLI.

Stappen om radioactieve tracering in te schakelen:

Zorg ervoor dat alle voorwaardelijke debugs uitgeschakeld zijn.

```
clear platform condition all
```

debug voor opgegeven MAC-adres inschakelen.

```
debug wireless mac <H.H.H> monitor-time <Time is seconds>
```

Na het reproduceren van het probleem, blokkeer het debuggen om de RA-sporenverzameling te stoppen.

```
no debug wireless mac <H.H.H>
```

Zodra het RA-spoor is gestopt, wordt het debug-bestand gegenereerd in de bootflash van de controller.

```
show bootflash: | include ra_trace
2728      179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

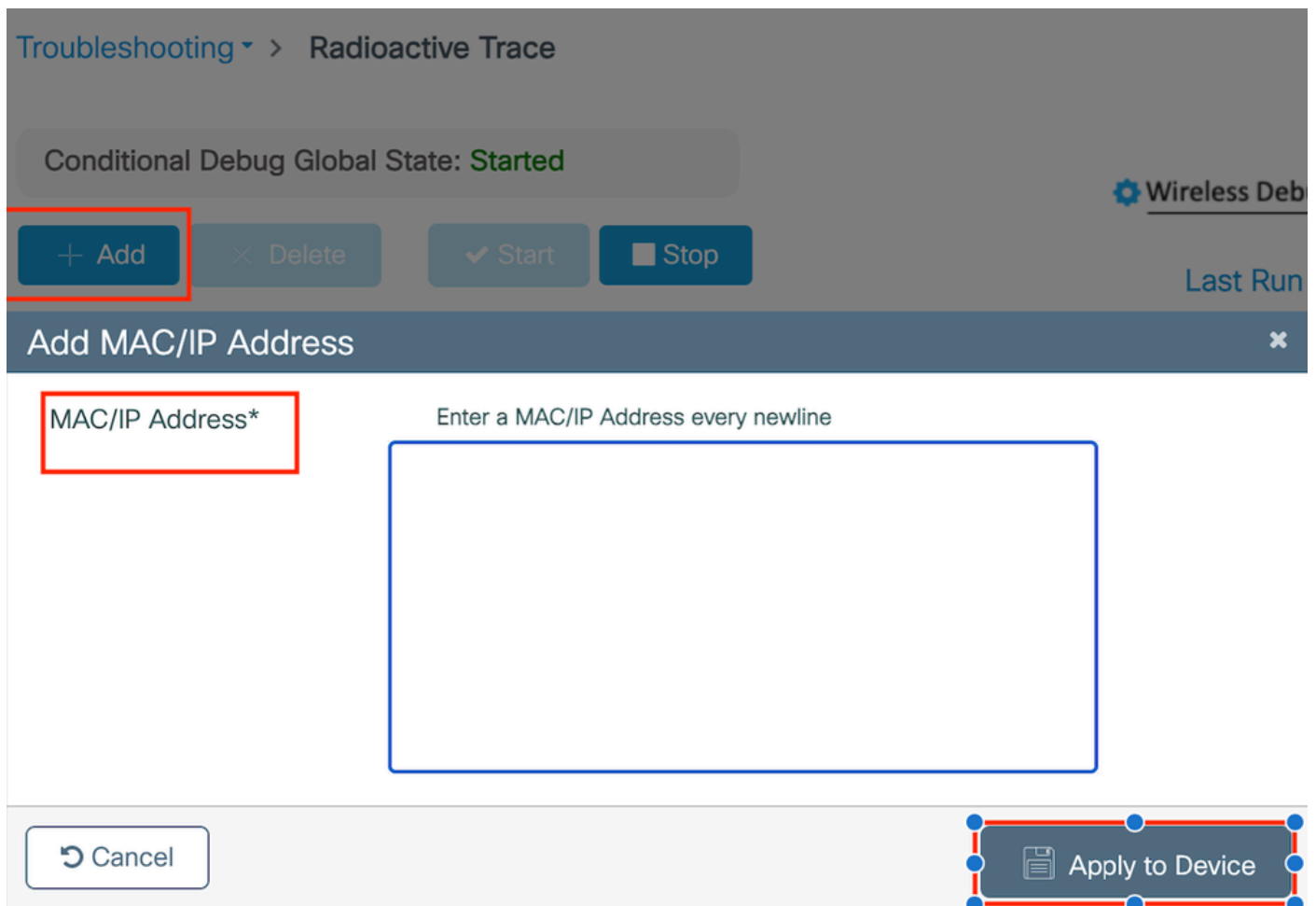
Kopieert het bestand naar een externe server.

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

Toont het debug-logbestand:

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

RA-overtrekken inschakelen in GUI,



RA-overtrekken inschakelen op WebUI

Ingesloten pakketvastlegging

Ga naar Problemen oplossen > Packet Capture. Voer de opnamenaam in en specificeer het MAC-adres van de client als de binnenste filter-MAC. Stel de buffergrootte in op 100 en kies de uplink-

interface om inkomende en uitgaande pakketten te bewaken.

Troubleshooting > Packet Capture

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane *i*





Inner Filter Protocol DHCP

Inner Filter MAC


Buffer Size (MB)* 100

Limit by* Duration 3600 secs == 1.00 hour

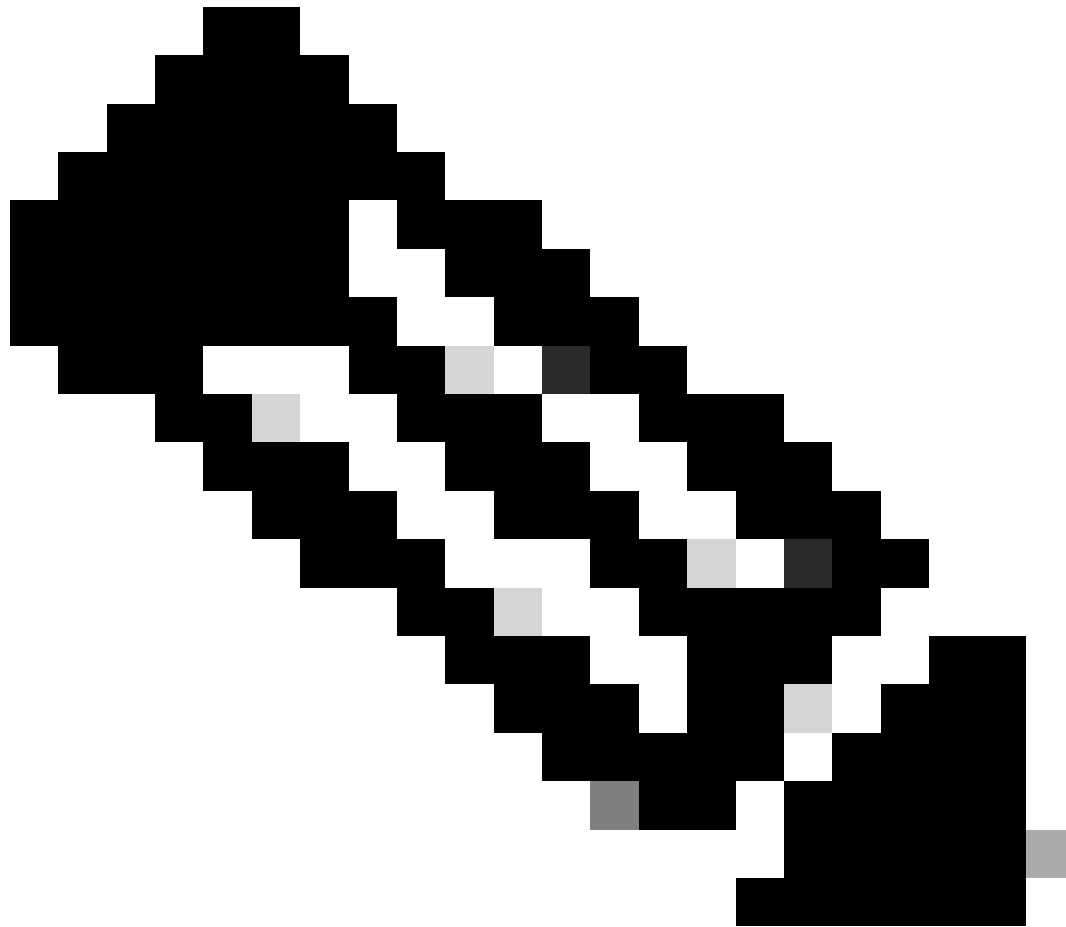
Available (12) Search

 Tw0/0/1	→
 Tw0/0/2	→
 Tw0/0/3	→
 Te0/1/0	→

Selected (1)

 Tw0/0/0	←
---	---

Ingesloten pakketvastlegging



Opmerking: Selecteer de optie "Monitorbesturing verkeer" om verkeer te bekijken dat naar de systeem CPU wordt omgeleid en in het gegevensvlak wordt opnieuw gespoten.

Navigeer naar Problemen oplossen > Packet Capture en selecteer Start om pakketten op te nemen.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start

Packet Capture starten

CLI-configuratie

```
monitor capture TestPCap inner mac <H.H.H>  
monitor capture TestPCap buffer size 100  
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
```

```
monitor capture TestPCap start
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Exporteer pakketopname naar externe TFTP-server.

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```

Navigeer naar Problemen oplossen > Packet Capture en selecteer Exporteren om het opnamebestand op de lokale machine te downloaden.

The screenshot shows a table of capture configurations. The first row is for 'TestPCap' on interface 'TwoGigabitEthernet0/0/0'. The 'Action' column has a green 'Start' button and a blue 'Export' button. The 'Export' button is highlighted with a red box. Below the table, an 'Export Capture - TestPCap' dialog box is open. It has a dropdown menu for 'Export to*' set to 'desktop'. At the bottom of the dialog, there are 'Cancel' and 'Export' buttons. The 'Export' button is also highlighted with a red box.

EPC downloaden

Werklogfragmenten

AireOS Foreign Controller-client-debuglogboek

Bedrad pakket ontvangen van bekabelde client

```
*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobi
```

Buitenlandse controller gebouw export ankerverzoek

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3
```

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM
```

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0
```

De buitenlandse controleur stuurt het ankerverzoek van de Uitvoer naar de ankercontrolemechanisme.

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70
```

Anchor controller stuurt bevestiging voor het Anchor-verzoek om client

```
*Dot1x_NW_MsgTask_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c
```

Mobiliteitsrol voor de klanten op de buitenlandse controller wordt bijgewerkt om te exporteren.

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) mobility role update requ  
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70
```

Client omgezet in de staat van de LOOPPAS.

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mobilit
```

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:
```

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800 radioactief spoor van buitenlandse controller

De client is aangesloten bij de controller.

2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Mobiliteitsdetectie is in volle gang na associatie.

2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Wanneer de mobiliteitsdetectie is verwerkt, wordt het clientroamtype bijgewerkt op de gevraagde L3.

2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM

2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t

De buitenlandse controller stuurt de export ankeraanvraag naar Anchor WLC.

2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo

2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For

De reactie van het Anker van de uitvoer wordt ontvangen van het Ankercontrolemechanisme en VLAN wordt toegepast van het gebruikersprofiel.

2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An

2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr

2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:

Zodra het Exporteren Anker verzoek wordt verwerkt, wordt de rol van de cliëntmobiliteit bijgewerkt aan Exporteren Buitenlandse.

2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce

2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili

2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20

2024/07/15 04:10:32.107592251 {wncd_x_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili

De overgangen van de cliënt in IP leren staat.

2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5

Na IP leren, de cliëntbewegingen om staat op Buitenlandse WLC in WERKING te STELLEN.

2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

AireOS ankercontroller client deubg log

Export Anchor-verzoek ontvangen van de buitenlandse controller.

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileNa

Lokale overbruggingsVLAN wordt toegepast op de client.

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol

De rol van de mobiliteit wordt bijgewerkt om Anker en cliëntstaat transistioned Geassocieerde uit te voeren.

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74

Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5

add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1

*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5

Sent message to add a0:ce:c8:c3:a9:b5 on mer

*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi

De mobiliteit is voltooid, de clientstatus is gekoppeld en de mobiliteitsrol is Exportaanker.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

Het IP-adres van de client wordt geleerd op de controller en de status die via DHCP wordt overgedragen, vereist voor de vereiste webautorisatie.

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

Webauth URL wordt samengesteld door het toevoegen van de externe omleiden url en controller virtuele ip-adres.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

Toegevoegd client mac adres en WLAN aan de URL.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http://
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

Laatste URL na het parchen van HTTP GET voor host 10.105.211.1

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

Redirect URL wordt verzonden naar de client in het 200 OK response-pakket.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

De client maakt een TCP-verbinding met redirect URL-host. Zodra de clients de inloggebruikersnaam en het wachtwoord op de portal indienen, wordt door de controller een radiusverzoek naar de radiusserver verzonden

Zodra de controller een Access-Accept ontvangt, sloot de client de TCP-sessie en wordt verplaatst naar RUN-status.

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe

*aaaQueueReader: May 28 10:46:59:077: AVP[01] User-Name.....testuser
*aaaQueueReader: May 28 10:46:59:077: AVP[03] Calling-Station-Id.....a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077: AVP[04] Nas-Port.....0x000000
*aaaQueueReader: May 28 10:46:59:077: AVP[05] Nas-Ip-Address.....0x0a4c76
*aaaQueueReader: May 28 10:46:59:077: AVP[06] NAS-Identifier.....POD1586-

*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv

*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c

*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800 radioactieve tracering van ankercontroller

Mobility kondigt bericht aan voor de klant van de Foreign controller.

```
2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re
```

Exporteer ankeraanvraag ontvangen van de buitenlandse controller wanneer de klant samenwerkt waarvoor Exporteren ankerrespons wordt verzonden door de Anchor controller die kan worden geverifieerd op het Foreign controller RA-spoor.

```
2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5
```

De client wordt verplaatst naar de associërende staat en de mobiliteitsrol wordt getransformeerd naar de Exporthandelaar.

```
2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

IP leren is voltooid, client-IP geleerd via ARP .

```
2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
```

De staat van het clientbeleid is in behandeling.

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli
```

De TCP-handdruk wordt gespoofd door de controller. Wanneer de client een HTTP GET verstuurt, wordt er een 200 OK response frame verzonden dat de redirect URL bevat.

De client moet een TCP-handdruk instellen met de doorverwijzing van de URL en de pagina laden.

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
```

Wanneer de client de inlogreferenties op de webpagina van het webportaal indient, wordt een pakket met toegangsaanvragen naar de radiusserver verzonden voor verificatie.

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair
```

Access-Accept wordt ontvangen van de radius server, webauth is succesvol.

```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
```

De verificatie is geslaagd en de status van het clientbeleid staat op RUN.

```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

Ingesloten pakketopnameanalyse

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)

> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)

> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156

> User Datagram Protocol, Src Port: 16667, Dst Port: 16667

> Control And Provisioning of Wireless Access Points - Data

> Ethernet II, Src: Cisco_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink_c3:a9:b5 (a0:ce:c8:c3:a9:b5)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095

> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69

> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Location: http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n

Content-Type: text/html\r\n

Content-Length: 527\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.000000000 seconds]

[Request in frame: 804]

[Request URI: http://10.105.211.1/auth/discovery?architecture=9]

File Data: 527 bytes

De client wordt omgeleid naar de portal-pagina

Sessie wordt gesloten na ontvangst van de doorverwijzing-URL.

804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
805	15:10:24.826953	10.105.211.1	10.105.211.69		TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)
807	15:10:24.826953	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
812	15:10:24.835955	10.105.211.69	10.105.211.1		TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
813	15:10:24.836947	10.105.211.1	10.105.211.69		TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
814	15:10:24.836947	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

TCP-sessie is gesloten na ontvangst van de doorverwijzing URL

De client initieert TCP 3 manier handshake naar de redirect URL host en verstuurt een HTTP GET aanvraag.

Nadat de pagina is geladen, worden de aanmeldingsgegevens op de portal verzonden, stuurt de controller een toegangs aanvraag naar de radiusserver om de client te verifiëren.

Na succesvolle verificatie wordt de TCP-sessie naar de webserver gesloten en wordt op de controller de status van de client policy manager omgezet naar RUN.

Verwant artikel

[WLAN-ankermobiliteit op Catalyst 9800 configureren](#)

[Configuratie-voorbeeld van bekabelde gasttoegang met AireOS-controllers](#)

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.