

Configureren Verifiëren en Probleemoplossing Web Auth op Mac Filter falen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Webparameters configureren](#)

[Beleidsprofiel configureren](#)

[WLAN-profiel configureren](#)

[AAA-instellingen configureren:](#)

[ISE-configuratie:](#)

[Verifiëren](#)

[Controllerconfiguratie](#)

[Beleidsstatus van client voor controller](#)

[Problemen oplossen](#)

[Radioactief spoor verzamelen](#)

[Ingesloten pakketvastlegging:](#)

[Verwant artikel](#)

Inleiding

Dit document beschrijft hoe u lokale webautorisatie kunt configureren, probleemoplossing kunt uitvoeren en controleren op de functie "Mac Filter Failure" met ISE voor externe verificatie.

Voorwaarden

Configureer ISE voor MAC-verificatie

Geldige gebruikersreferenties ingesteld op ISE/Active Directory

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

Basisbegrip om door controller Web UI te navigeren

Policy, WLAN-profiel en Policy Tags configuratie

Servicebeleidsconfiguratie op ISE

Gebruikte componenten

9800 WLC versie 17.12.2

C9120 AXI access point

9300 switch

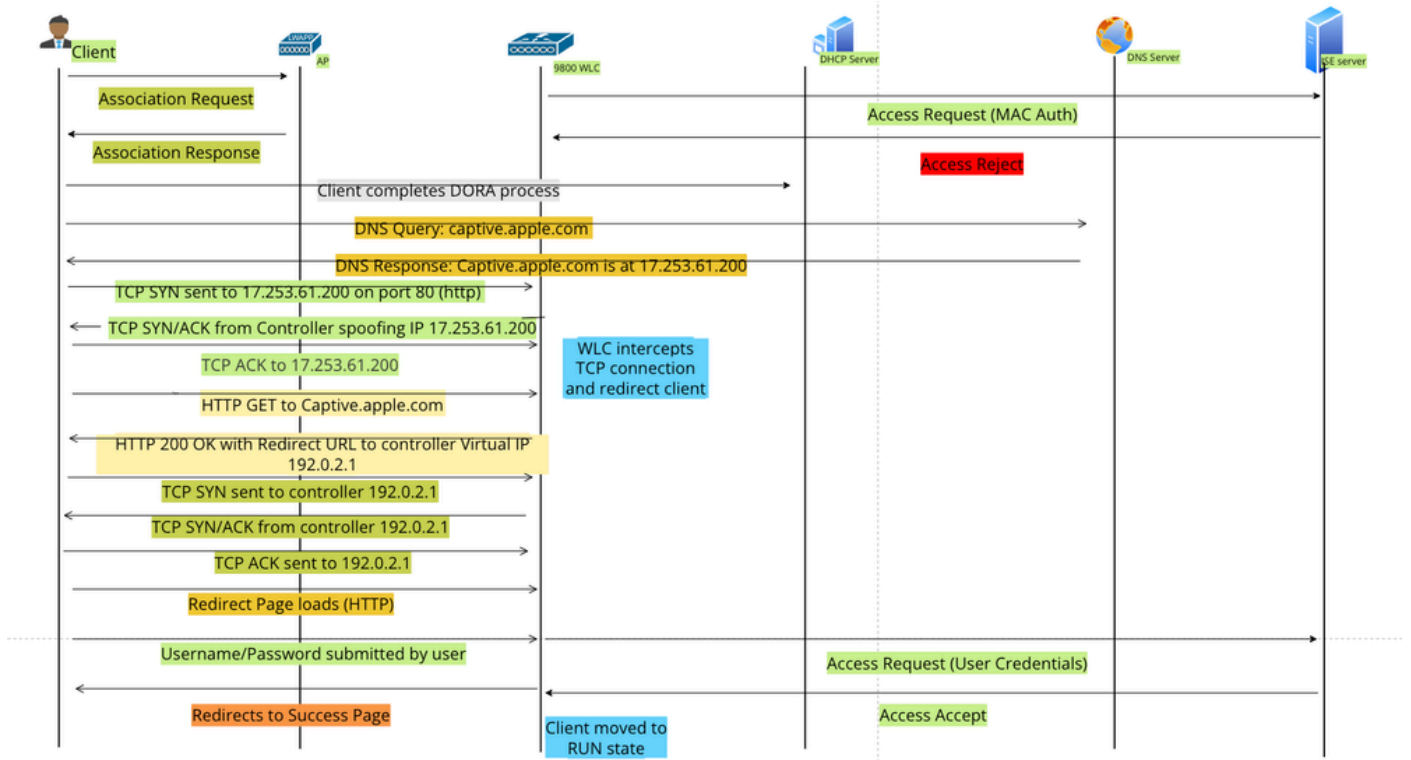
ISE-versie 3.1.0.518

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.

Achtergrondinformatie

De functie Web Auth "On Mac Failure Filter" fungeert als een terugvalmechanisme in WLAN-omgevingen die zowel MAC-verificatie als webverificatie gebruiken.

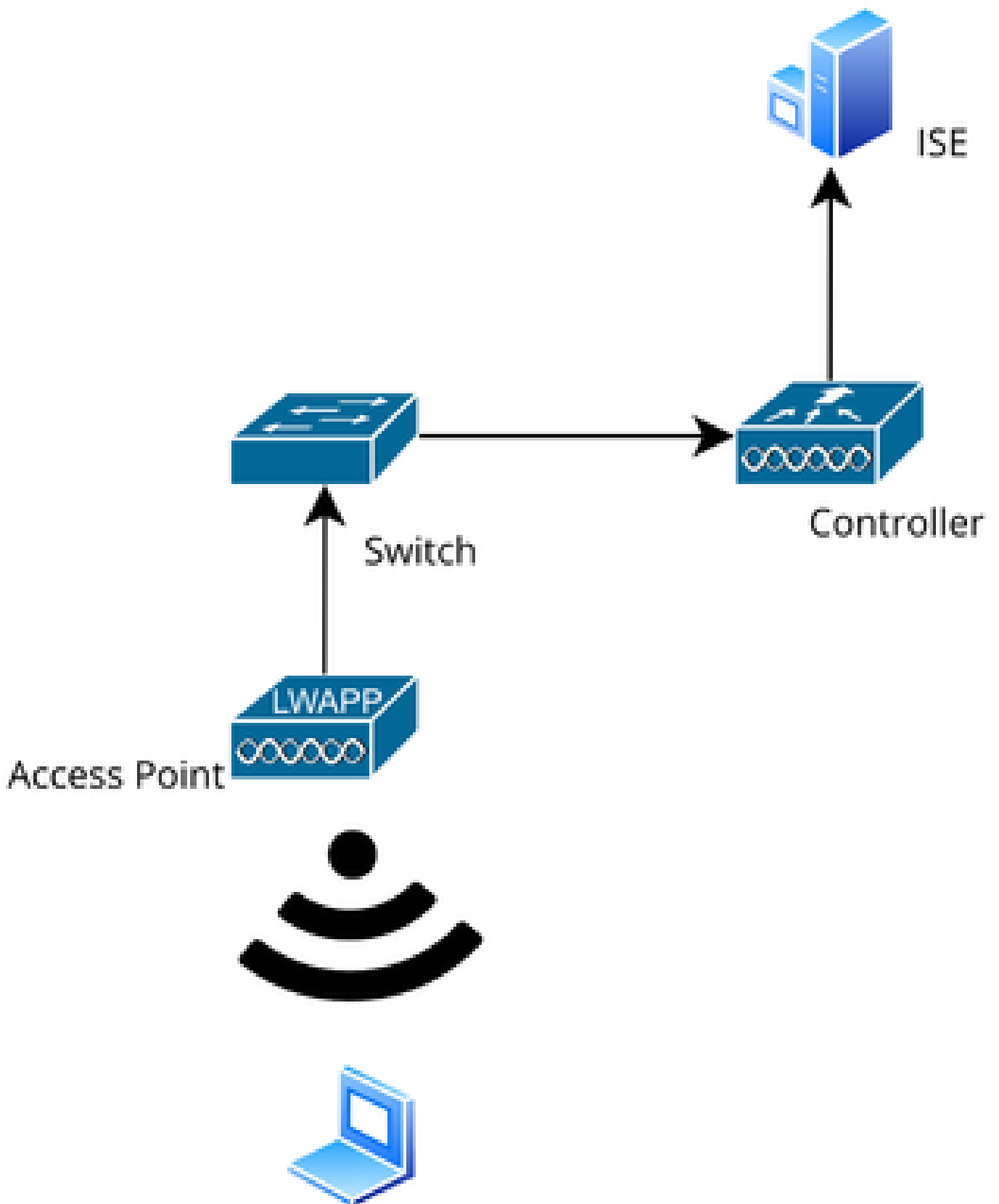
- **Fallback Mechanism:** Wanneer een client probeert verbinding te maken met een WLAN met MAC Filter tegen een externe RADIUS-server (ISE) of lokale server en niet kan worden geverifieerd, wordt met deze optie automatisch een Layer 3 Web Verification gestart.
- **Succesvolle verificatie:** Als een client met succes wordt geverifieerd via het MAC-filter, wordt webverificatie omzeild, zodat de client rechtstreeks verbinding kan maken met het WLAN.
- **Disassociaties voorkomen:** deze functie helpt disassociaties te voorkomen die anders kunnen optreden door fouten in de MAC-filterverificatie.



Web Auth Flow

Configurieren

Netzwerkdiagramm



Netwerktopologie

Configuraties

Webparameters configureren

Navigeer naar Configuration > Security > Web Auth en selecteer de Global parameter map

Controleer de virtuele IP- en Trustpoint-configuratie op de Global Parameter Map. Alle aangepaste webautorisatieparameterprofielen erven de virtuele IP- en Trustpointconfiguratie van de Global Parameter Map.

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
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"/>		
Sleeping Client Status	<input type="checkbox"/>		

Banner Configuration

Profiel van Global Web Auth Parameter

Stap 1: Selecteer "Add" om een aangepaste web authenticatie parameterkaart te maken. Voer een profielnaam in en kies Type als "Webauth".

Configuration > Security > Web Auth

+ Add Delete

Parameter Map Name

global

Create Web Auth Parameter

Parameter-map Name*	Web-Filter
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth

Close Apply to Device

Als uw clients ook een IPv6-adres krijgen, moet u ook een virtueel IPv6-adres toevoegen op de parameterkaart. Gebruik een IP in het documentatiebereik 2001:db8::/32

Als uw clients een IPv6-adres hebben gekregen, is er een goede kans dat ze proberen om de HTTP web auth omleiding in V6 en niet V4 te krijgen, daarom moet de Virtuele IPv6 ook worden ingesteld.

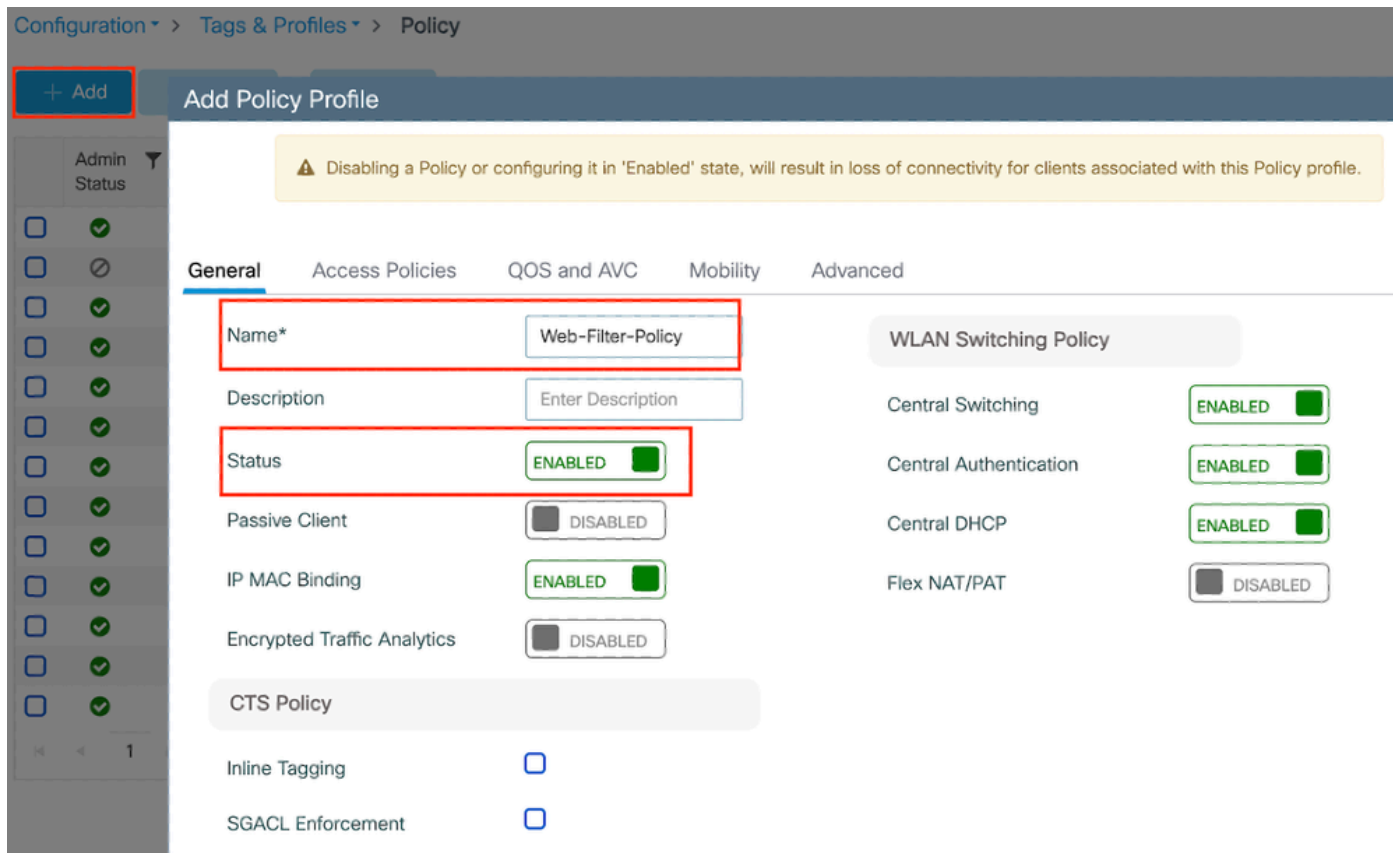
CLI-configuratie:

```
parameter-map type webauth Web-Filter  
type webauth
```

Beleidsprofiel configureren

Stap 1: Een beleidsprofiel maken

Ga naar Configuration > Tags en profielen > Policy. Selecteer "Toevoegen". Specificeer op het tabblad Algemeen een naam voor het profiel en schakel de statusschakelaar in.



Beleidsprofiel

Stap 2:

Kies op het tabblad Toegangsbeleid de client-VLAN in de vervolgkeuzelijst VLAN-sectie.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select ⓘ

VLAN

VLAN/VLAN Group VLAN2074 ⓘ

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select ⓘ

IPv6 ACL Search or Select ⓘ

URL Filters ⓘ

Pre Auth Search or Select ⓘ

Post Auth Search or Select ⓘ

Tabblad Toegangsbeleid

CLI-configuratie:

```
wireless profile policy Web-Filter-Policy
vlan VLAN2074
no shutdown
```

WLAN-profiel configureren

Stap 1: Navigeer naar Configuration > Tags en profielen > WLAN's. Selecteer "Add" om een nieuw profiel te maken. Definieer een profielnaam en een SSID-naam en schakel het statusveld in.

+ Add × Delete Clone Enable WLAN Disable WLAN

Add WLAN

General Security Advanced

Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz

Status **ENABLED** ⓘ

- ✖ WPA3 Enabled
- ✔ Dot11ax Enabled

5 GHz

Status **ENABLED**

2.4 GHz

Status **ENABLED**

802.11b/g Policy 802.11b/g ▼

WLAN-profiel

Stap 2: Schakel onder het tabblad Beveiliging het selectievakje "Mac Filtering" in en configureer de RADIUS-server in de Autorisatielijst (ISE of lokale server). Deze setup maakt gebruik van ISE voor zowel Mac-verificatie als webverificatie.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Authorization List*

network

OWE Transition Mode

Lobby Admin Access

Fast Transition

Status

Disabled

Over the DS

Reassociation Timeout *

20

WLAN Layer 2-beveiliging

Stap 3: Navigeer naar Security > Layer 3. Schakel Webbeleid in en koppel het aan het profiel voor de Webverificatieparameter. Schakel het aanvinkvakje "On Mac Filter Failure" in en kies de RADIUS-server in de vervolgkeuzelijst Verificatielijst.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map

Web-Filter

Authentication List

ISE-List

<< Hide

On MAC Filter Failure

Splash Web Redirect

DISABLED

Preauthentication ACL

For Local Login Method List to work, please make sure

WLAN Layer 3-beveiligingstabblad

CLI-configuratie

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
mac-filtering network
radio policy dot11 24ghz
radio policy dot11 5ghz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list ISE-List
security web-auth on-macfilter-failure
security web-auth parameter-map Web-Filter
no shutdown
```

Stap 4: Beleidstags configureren, WLAN-profiel maken en beleidsprofieltoewijzing maken

Navigeren naar Configuratie > Tags & profielen > Tags > Beleid. Klik op "Toevoegen" om een naam voor de beleidstag te definiëren. Selecteer onder WLAN-beleidskaarten de optie "Add" om het eerder gemaakte WLAN- en beleidsprofiel in kaart te brengen.

The screenshot shows the 'Policy' configuration page with tabs for Policy, Site, RF, and AP. The '+ Add' button is highlighted with a red box. Below it is the 'Add Policy Tag' modal window. The 'Name*' field contains 'default-policy-tag' and the 'Description' field contains 'Enter Description'. Under 'WLAN-POLICY Maps: 0', there are '+ Add' and 'x Delete' buttons. A table with columns 'WLAN Profile' and 'Policy Profile' is shown with '0' items and a 'No items to display' message. The 'Map WLAN and Policy' section is highlighted with a red box, featuring 'WLAN Profile*' and 'Policy Profile*' fields with search/select buttons and confirmation buttons.

Beleids TAG-kaart

CLI-configuratie:

```
wireless tag policy default-policy-tag
description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

Stap 5: Navigeer naar Configuration > Wireless > Access point. Selecteer het toegangspunt dat verantwoordelijk is voor het uitzenden van deze SSID. Wijs in het menu AP bewerken de gemaakte beleidstag toe.

The screenshot shows the 'Edit AP' configuration page in the Meraki dashboard. The left sidebar shows a list of access points, with 'AP2-AIR-AP3802I-D-K9-2' selected. The main content area is divided into several tabs: General, Interfaces, High Availability, Inventory, Geolocation, ICap, Advanced, and Support Bundle. The 'General' tab is active, showing various configuration fields. The 'Tags' section is highlighted with a red box, showing a dropdown menu for 'Policy' set to 'default-policy-tag'. Other tags shown include 'default-site-tag' and 'default-rf-tag'. The 'Version' section shows the primary software version as 17.12.2.35.

Toewijzingsbeleid TAG aan AP

AAA-instellingen configureren:

Stap 1: Een RADIUS-server maken:

Blader naar Configuratie > Beveiliging > AAA. Klik op de optie "Toevoegen" onder de sectie Server/groep. Voer op de pagina "AAA-radiusserver 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](#)

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 de optie "Toevoegen" onder het gedeelte Servergroepen om een servergroep te definiëren. Schakel de servers in die opgenomen moeten worden in dezelfde groepsconfiguratie.

Het is niet vereist om de broninterface in te stellen. Standaard gebruikt de 9800 zijn routingstabel om de interface te bepalen die moet worden gebruikt om de RADIUS-server te bereiken en gebruikt doorgaans de standaardgateway.

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 Group

Name* ⓘ Name is required

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance DISABLED

Source Interface VLAN ID

Available Servers Assigned Servers

Servergroep

CLI-configuratie

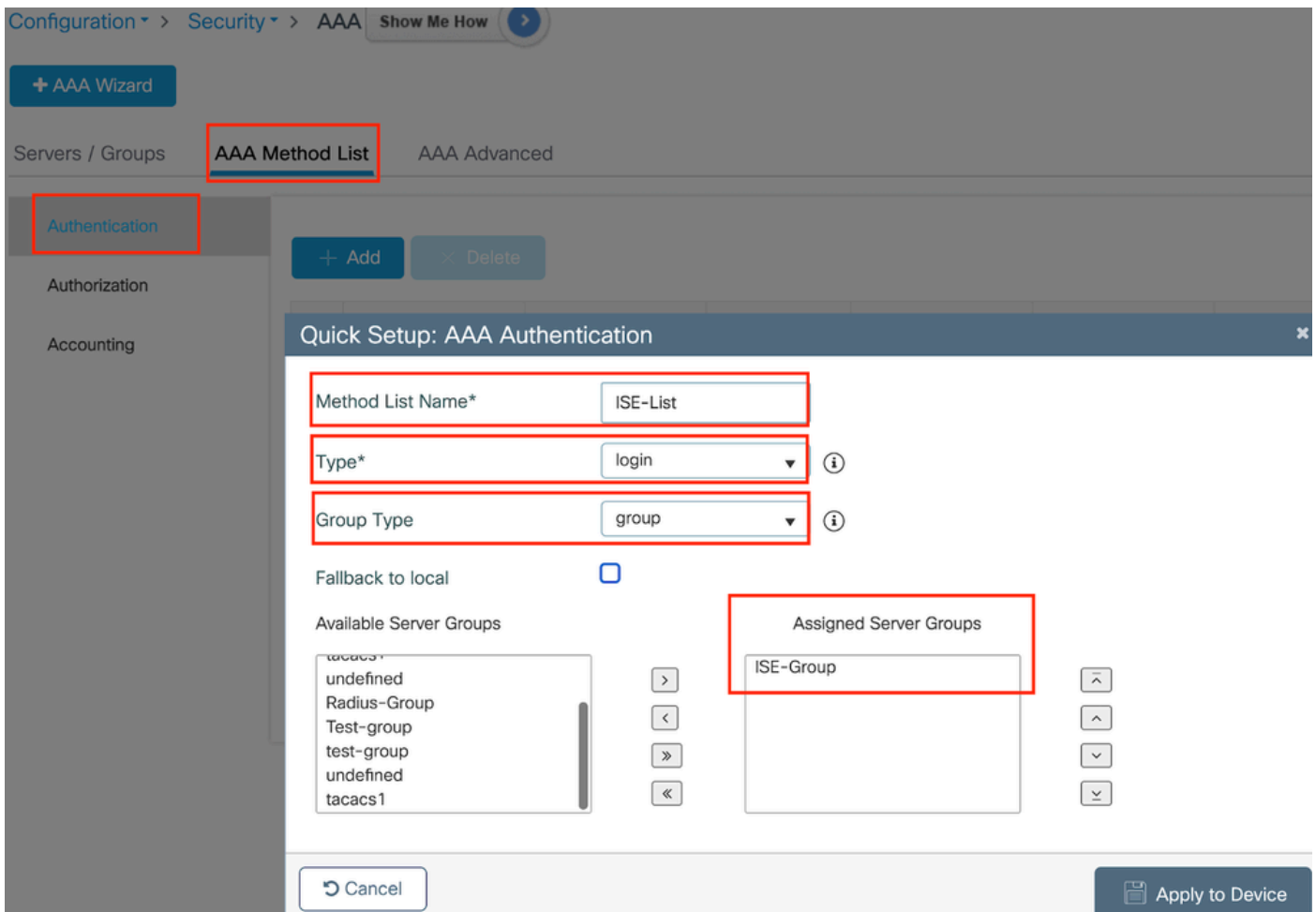
```

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 AAA-methodelijst. Klik onder Verificatie op Toevoegen. Definieer een methodelijst naam met Type als "login" en Groepstype als "Groep". Wijs de ingestelde verificatieservergroep toe in het gedeelte Toegewezen servergroep.



Lijst met verificatiemethoden

CLI-configuratie

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

Navigeer naar het gedeelte Autorisatiemethode en klik op "Toevoegen". Definieer een methodelijst naam en stel het type in op "netwerk" met Groepstype als "Groep". Schakel de geconfigureerde RADIUS-server in op het gedeelte Toegewezen servergroepen.

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add × Delete

Quick Setup: AAA Authorization

Method List Name* network

Type* network i

Group Type group i

Fallback to local

Authenticated

Available Server Groups

tacacs1
undefined
Radius-Group
Test-group
test-group
undefined
tacacs1

Assigned Server Groups

ISE-Group

Lijst van autorisatiemethoden

CLI-configuratie

```
aaa authorization network network group ISE-Group
```

ISE-configuratie:

WLC als netwerkapparaat toevoegen aan ISE

Stap 1: Navigeer naar Beheer > Netwerkapparaten en klik op Toevoegen. Voer het IP-adres van de controller, de hostnaam en het gedeelde geheim in onder de Radius-verificatie-instellingen

Network Devices

Name

Description

 IP Address * IP : / 32 

Netwerkapparaat toevoegen

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Show

Gedeeld geheim

Stap 2: Gebruikersvermelding maken

Selecteer onder Identiteitsbeheer > Identiteiten de optie Toevoegen.

De gebruikersnaam en het wachtwoord configureren die de client moet gebruiken voor webverificatie

✓ Network Access User

* Username

Status Enabled

Email

✓ Passwords

Password Type:

* Login Password

Gebruikersreferenties toevoegen

Stap 3: Navigeer naar Beheer > Identity Management > Groepen > Geregistreerde apparaten en klik op Add.

Voer het adres in van de apparaatnaam om een naam op de server te definiëren.

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

Identity Groups

- Endpoint Identity Groups
 - Blocked List
 - GuestEndpoints
 - Profiled
 - RegisteredDevices**
 - Unknown
- User Identity Groups

Endpoint Identity Group List > RegisteredDevices

Endpoint Identity Group

* Name: **RegisteredDevices**

Description: Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints

+ Add Remove

MAC Address Static Group Assignment Endpoint Profile

Save

Netwerkadres van apparaat toevoegen

Stap 4: Servicebeleid maken

Navigeer naar Beleidssets > Beleidssets en selecteer "+"-teken om een nieuwe beleidsset te maken

Deze beleidsset is bedoeld voor gebruikerswebverificatie, waarbij een gebruikersnaam en wachtwoord voor de client wordt aangemaakt in Identity Management

Policy Sets → User-Webauth Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users		Options

Servicebeleid voor webverificatie

Op dezelfde manier een MAB-servicebeleid maken en interne endpoints toewijzen onder

authenticatiebeleid.

Policy Sets -> Test-MAB Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Test-MAB		Normalised Radius-RadiusFlowType EQUALS WirelessMAB	Default Network Access ⌵ +	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Endpoints ⌵ > Options	0	

MAB-verificatie-servicebeleid

Verifiëren

Controllerconfiguratie

```
<#root>
```

```
show wireless tag policy detailed
```

```
default-policy-tag
```

```
Policy Tag Name : default-policy-tag
```

```
Description      : default policy-tag
```

```
Number of WLAN-POLICY maps: 1
```

```
WLAN Profile Name      Policy Name
```

```
-----  
Mac_Filtering_Wlan
```

```
Web-Filter-Policy
```

```
<#root>
```

```
show wireless profile policy detailed
```

```
Web-Filter-Policy
```

```
Policy Profile Name      :
```

```
Web-Filter-Policy
```

Description :
Status :
ENABLED
VLAN :
2074
Multicast VLAN : 0

<#root>

show wlan name

Mac_Filtering_Wlan

WLAN Profile Name :

Mac_Filtering_Wlan

=====
Identifier : 9
Description :
Network Name (SSID) :

Mac_Filtering_Wlan

Status :

Enabled

Broadcast SSID :

Enabled

Mac Filter Authorization list name :

network

Webauth On-mac-filter Failure :

Enabled

Webauth Authentication List Name :

ISE-List

Webauth Authorization List Name : Disabled

Webauth Parameter Map :

Web-Filter

<#root>

show parameter-map type webauth name Web-Filter

Parameter Map Name :

Web-Filter

Type :

webauth

Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window :

Enabled

Webauth success-window :

Enabled

Consent Email : Disabled
Activation Mode : Replace
Sleeping-Client : Disabled
Webauth login-auth-bypass:

<#root>

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 server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:

Enabled

HTTP secure server port:

443

show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping



WLAN Profile Name	Policy Name	VLAN	Flex
Mac_Filtering_Wlan	Web-Filter-Policy	2074	ENAB

Beleidsstatus van client voor controller

Navigeer naar het gedeelte Dashboard > Clients om de status van verbonden clients te bevestigen.

De client is momenteel in status voor webautorisatie in behandeling

[Clients](#)
[Sleeping Clients](#)
[Excluded Clients](#)

[Delete](#)



Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

1 - 1 of 1 clients

Clientgegevens

```
show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type	ID	State	Protocol	Method
6c7e.67e3.6db9	AP2-AIR-AP3802I-D-K9-2	WLAN	9	Webauth Pending	11ac	Web

```
<#root>
```

```
show wireless client mac-address 6c7e.67e3.6db9 detail
```

```
Client MAC Address :
```

```
6c7e.67e3.6db9
```

```
Client MAC Type : Universally Administered Address
```

```
Client DUID: NA
```

```
Client IPv4 Address :
```

```
10.76.6.150
```

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
```

```
Client Username :
```

```
6c7e67e36db9
```

```
AP MAC Address : 1880.902b.05e0
```

```
AP Name: AP2-AIR-AP3802I-D-K9-2
```

```
AP slot : 1
```

```
Client State : Associated
```

```
Policy Profile :
```

Web-Filter-Policy

Flex Profile : N/A
Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List

Method : Web Auth
Webauth State :

Get Redirect

Webauth Method :

Webauth

Na succesvolle webverificatie overgangen naar RUN voor client policy manager

<#root>

show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A

Problemen oplossen

De functionaliteit van de Web Auth on MAC Failure-functie is afhankelijk van de controller-mogelijkheid om webverificatie te activeren bij MAB-fout. Ons primaire doel is om RA-sporen efficiënt te verzamelen van de controller voor probleemoplossing en analyse.

Radioactief spoor verzamelen

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

Stappen om radioactieve tracersing 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 controller bootflash.

```
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 addr
```

Toont het debug-logbestand:

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

RA-overtrekken inschakelen in GUI,

Stap 1: Ga naar Problemen oplossen > Radioactief spoor. Selecteer de optie om een nieuw item toe te voegen en voer vervolgens het MAC-adres van de client in het toegewezen tabblad MAC/IP-adres toevoegen.

The screenshot shows the 'Radioactive Trace' interface. At the top, it says 'Troubleshooting > Radioactive Trace'. Below that, a status bar indicates 'Conditional Debug Global State: Started'. There are four buttons: '+ Add' (highlighted with a red box), '× Delete', '✓ Start', and '■ Stop'. To the right, there is a 'Wireless Deb' logo and 'Last Run'. A modal dialog box titled 'Add MAC/IP Address' is open. It has a label 'MAC/IP Address*' (highlighted with a red box) and a large text input area with the placeholder text 'Enter a MAC/IP Address every newline'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Apply to Device' (highlighted with a red box).

Radioactief spoor

Ingesloten pakketvastlegging:

Ga naar Problemen oplossen > Packet Capture. Voer de opnamenaam in en specificeer het MAC-adres van de client als de binnenste filter voor MAC. Stel de buffergrootte in op 100 en kies de uplink-interface om inkomende en uitgaande pakketten te bewaken.

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane

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.

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	<input type="button" value="Start"/>

Opname 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)

Pakketopname exporteren naar externe TFTP-server

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

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	Start Export

Export Capture - TestPCap

Export to* desktop

Cancel Export

Packet-opname voor export

Voorbeeldscenario tijdens succesvolle MAC-verificatie, een client-apparaat verbindt met het netwerk, zijn MAC-adres wordt gevalideerd door de RADIUS-server door middel van geconfigureerd beleid, en na verificatie wordt toegang verleend door het netwerk-toegangsapparaat, waardoor netwerkconnectiviteit mogelijk wordt.

Zodra client associates, controller een Access-request naar ISE-server verstuurt,

Gebruikersnaam is het hoofdadres van de client, aangezien dit MAB-verificatie is

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
```

ISE verzendt access-Accept omdat we een geldige gebruikersvermelding hebben

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

Status clientbeleid getransformeerd naar Mac Auth voltooid

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29 Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

De client is in IP-leerstatus na succesvolle MAB-verificatie

```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d29
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

De staat van de de beleidsmanager van de cliënt die wordt bijgewerkt om te LOPEN, wordt de WebVerificatie overgeslagen voor de cliënt die MAB authenticatie voltooit

2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD

Verificatie met ingesloten pakketvastlegging

radius						
Time	Source	Destination	Length	Protocol	Info	
02:42:52.710961	10.76.6.156	10.197.224.122		RADIUS	Access-Request id=0	
02:42:52.778951	10.197.224.122	10.76.6.156		RADIUS	Access-Accept id=0	

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x0 (0)
Length: 422
Authenticator: 19c6635633a7e6b6f30070b02a7f753c
[\[The response to this request is in frame 54\]](#)
Attribute Value Pairs
> AVP: t=User-Name(1) l=14 val=6c7e67b72d29
> AVP: t=User-Password(2) l=18 val=Encrypted
> AVP: t=Service-Type(6) l=6 val=Call-Check(10)
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
> AVP: t=Framed-MTU(12) l=6 val=1485

Radius-pakket

Voorbeeld waar MAC-verificatiefout voor een clientapparaat

Mac-verificatie gestart voor een client na succesvolle associatie

2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Success
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cl
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]

ISE zou access-reject sturen omdat dit apparaat niet aanwezig is in ISE

2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000

Webex-autorisatie gestart voor clientapparaat als MAB is mislukt

2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cl

Zodra de client een HTTP GET aanvraag initieert, wordt de URL omgeleid naar het clientapparaat, aangezien de bijbehorende TCP sessie wordt gespoofd door de controller.

2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6

De client start een HTTP Get naar de redirect URL en zodra de pagina wordt geladen worden de inlogreferenties ingediend.

De controller stuurt een toegangs aanvraag naar ISE

Dit is een webverificatie omdat een geldige gebruikersnaam wordt waargenomen in een access-acceptatiepakket

2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco

Access-Accept ontvangen van ISE

2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato

Web verificatie is geslaagd en client status transmissie naar RUN status

2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db

Verificatie via EPC

De client voltooit de TCP-handdruk met het virtuele IP-adres van de controller en de client laadt de portaalpagina omleiden. Zodra de gebruiker gebruikersnaam en wachtwoord indient, kunnen we een radius access-request van het controller beheer IP-adres waarnemen.

Na succesvolle verificatie wordt de client-TCP-sessie gesloten en op de controller worden de clientovergangen naar de toestand RUN uitgevoerd.

15649	08:52:51.122979	10.76.6.150	192.0.2.1	TCP	58832 → 443 [SYN, ECE, CWI] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650	08:52:51.123986	192.0.2.1	10.76.6.150	TCP	443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=4022788871
15651	08:52:51.125985	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652	08:52:51.126992	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
15653	08:52:51.126992	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654	08:52:51.126992	192.0.2.1	10.76.6.150	85,1,64	TLSv1.2 Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655	08:52:51.129982	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656	08:52:51.129982	10.76.6.150	192.0.2.1	1,64	TLSv1.2 Change Cipher Spec, Encrypted Handshake Message
15657	08:52:51.130989	10.76.6.150	192.0.2.1	640	TLSv1.2 Application Data
15658	08:52:51.130989	10.76.6.150	192.0.2.1	160	TLSv1.2 Application Data
15659	08:52:51.130989	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3
15665	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment t
15667	08:52:51.191976	192.0.2.1	10.76.6.150	2496	TLSv1.2 Application Data
15668	08:52:51.192983	192.0.2.1	10.76.6.150	48	TLSv1.2 Encrypted Alert
15673	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15676	08:52:51.197987	10.76.6.150	192.0.2.1	48	TLSv1.2 Encrypted Alert
15677	08:52:51.197987	10.76.6.150	192.0.2.1	TCP	58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0

TCP-stroom met RADIUS-pakket

15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3

```

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x3 (3)
  Length: 457
  Authenticator: fd400f7e3567dc5a63cfefaef379eeaa
  [The response to this request is in frame 15663]
  Attribute Value Pairs
    AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
    AVP: t=User-Name(1) l=10 val=testuser
    AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
    AVP: t=Message-Authenticator(80) l=16 val=501b124c30216cfd5973086d99f3a185
  > AVP: t=Service-Type(6) l=6 val=Dialogout-Framed-User(5)
  > AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
  > AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
  > AVP: t=User-Password(2) l=18 val=Encrypted
  
```

Radius-pakket verzonden naar ISE met gebruikersreferenties

De client-side wireshark Capture om het clientverkeer te valideren wordt omgeleid naar de portal pagina en valideert de TCP handshake om het virtuele IP-adres/webserver te controleren

Time	Source	Destination	Length	Protocol	Info
105	08:51:34.203945	10.76.6.150	10.76.6.145	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
108	08:51:34.206602	10.76.6.145	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)
234	08:51:39.028084	10.76.6.150	7.7.7.7	HTTP	GET / HTTP/1.1
236	08:51:39.031420	7.7.7.7	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)

Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
 Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
 Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
 Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637

Hypertext Transfer Protocol

Line-based text data: text/html (9 lines)

```
<HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
<HEAD>\n
<TITLE> Web Authentication Redirect</TITLE>\n
<META http-equiv="Cache-control" content="no-cache">\n
<META http-equiv="Pragma" content="no-cache">\n
<META http-equiv="Expires" content="-1">\n
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
</HEAD>\n
</HTML>
```

Opname aan cliëntzijde om de omleiding te valideren

De client maakt TCP-handdruk naar het virtuele IP-adres van de controller

Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1	TCP	58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PERM
117	08:51:34.211190	192.0.2.1	10.76.6.150	TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr=0
118	08:51:34.211275	10.76.6.150	192.0.2.1	TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLsv1.2 Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150	TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLsv1.2 Server Hello, Certificate
126	08:51:34.220835	192.0.2.1	10.76.6.150	783	TLsv1.2 Server Key Exchange, Server Hello Done

TCP-handdruk tussen cliënt en webserver

Sessie wordt afgesloten na succesvolle web authenticatie,

144	08:51:34.235915	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLsv1.2 Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1	TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLsv1.2 Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150	TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

TCP-sessie afgesloten nadat cliënt webverificatie heeft voltooid

Verwant artikel

[Inzicht in draadloze debuggen en logbestanden op Catalyst 9800 draadloze LAN-controllers](#)

[Web gebaseerde verificatie op basis van 9800](#)

[Lokale webverificatie op 9800 configureren](#)

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.