

Configuratie van Dynamische VLAN-toewijzing met ISE en Catalyst 9800 draadloze LAN-controller

Inhoud

[Inleiding](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Dynamische VLAN-toewijzing met RADIUS-server](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratiestappen](#)

[Cisco ISE-configuratie](#)

[Stap 1. Configureer de Catalyst WLC als een AAA-client op de Cisco ISE-server](#)

[Stap 2. Configureer interne gebruikers op Cisco ISE](#)

[Stap 3. Het configureren van de RADIUS \(IETF\) eigenschappen die gebruikt worden voor dynamische VLAN-toewijzing](#)

[De Switch voor meerdere VLAN's configureren](#)

[Catalyst 9800 WLC-configuratie](#)

[Stap 1. Configureer de WLC met de details van de verificatieserver](#)

[Stap 2. Configureer de VLAN's](#)

[Stap 3. Configureer de WLAN's \(SSID's\)](#)

[Stap 4. Het beleidsprofiel configureren](#)

[Stap 5. De beleidsmarkering configureren](#)

[Stap 6. De beleidslaag aan een AP toewijzen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het concept van dynamische VLAN-toewijzing en hoe u de Catalyst 9800 draadloze LAN-controller (WLC) en Cisco Identity Services Engine (ISE) kunt configureren om Wireless LAN (WLAN) aan te wijzen om dit voor de draadloze client te realiseren.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- basiskennis hebben van de WLC en lichtgewicht access points (LAP's).
- beschikken over functionele kennis van de AAA-server zoals ISE.

- Zorg voor een grondige kennis van draadloze netwerken en draadloze beveiligingsproblemen.
- beschikken over functionele kennis over dynamische VLAN-toewijzing.
- basiskennis hebben van Control and Provisioning voor draadloos access point (CAPWAP).

Gebruikte componenten

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

- Cisco Catalyst 9800 WLC (Catalyst 9800-CL) met firmware release 16.12.4a
- Cisco 2800 Series LAP in lokale modus.
- Inheemse Windows 10 smeekbede.
- Cisco Identity Services Engine (ISE) die versie 2.7 uitvoert.
- Cisco 3850 Series switch met firmware release 16.9.6

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

Dynamische VLAN-toewijzing met RADIUS-server

In de meeste Wireless Local Area Network (WLAN) systemen heeft elk WLAN een statisch beleid dat van toepassing is op alle klanten die bij een Service Set-id (SSID) zijn gekoppeld. Hoewel krachtig, heeft deze methode beperkingen omdat het van cliënten om met verschillende SSIDs te associëren vereist om verschillend QoS en veiligheidsbeleid te erven.

De Cisco WLAN-oplossing ondersteunt echter identiteitsnetwerken. Dit staat het netwerk toe om één enkele SSID te adverteren en staat specifieke gebruikers toe om verschillend QoS of veiligheidsbeleid te erven gebaseerd op het gebruikersgeheugen.

Dynamische VLAN-toewijzing is één dergelijke functie die een draadloze gebruiker in een specifiek VLAN plaatst op basis van de referenties die door de gebruiker worden geleverd. De taak om gebruikers aan een specifiek VLAN toe te wijzen wordt behandeld door een RADIUS-verificatieserver, zoals Cisco ISE. Dit kan bijvoorbeeld gebruikt worden om de draadloze host op hetzelfde VLAN te laten blijven terwijl het binnen een campus-netwerk beweegt.

Daarom, wanneer een client probeert te associëren met een LAP die geregistreerd is met een controller, geeft WLC de referenties van de gebruiker voor validering door aan de RADIUS-server. Zodra de authenticatie succesvol is, passeert de RADIUS-server bepaalde eigenschappen van Internet Engineering Task Force (IETF) aan de gebruiker. Deze RADIUS-eigenschappen bepalen de VLAN-ID die aan de draadloze client moet worden toegewezen. SSID van de client maakt niet uit omdat de gebruiker altijd is toegewezen aan deze vooraf bepaalde VLAN-id.

De RADIUS-gebruikerseigenschappen die gebruikt worden voor de VLAN-ID-toewijzing zijn:

- IETF 64 (Tunnel type) - stel dit in op VLAN.
- IETF 65 (Tunnel Gemiddeld Type) — Stel dit in op 802.
- IETF 81 (Tunnel Private Group ID) - stel deze optie in op VLAN-id.

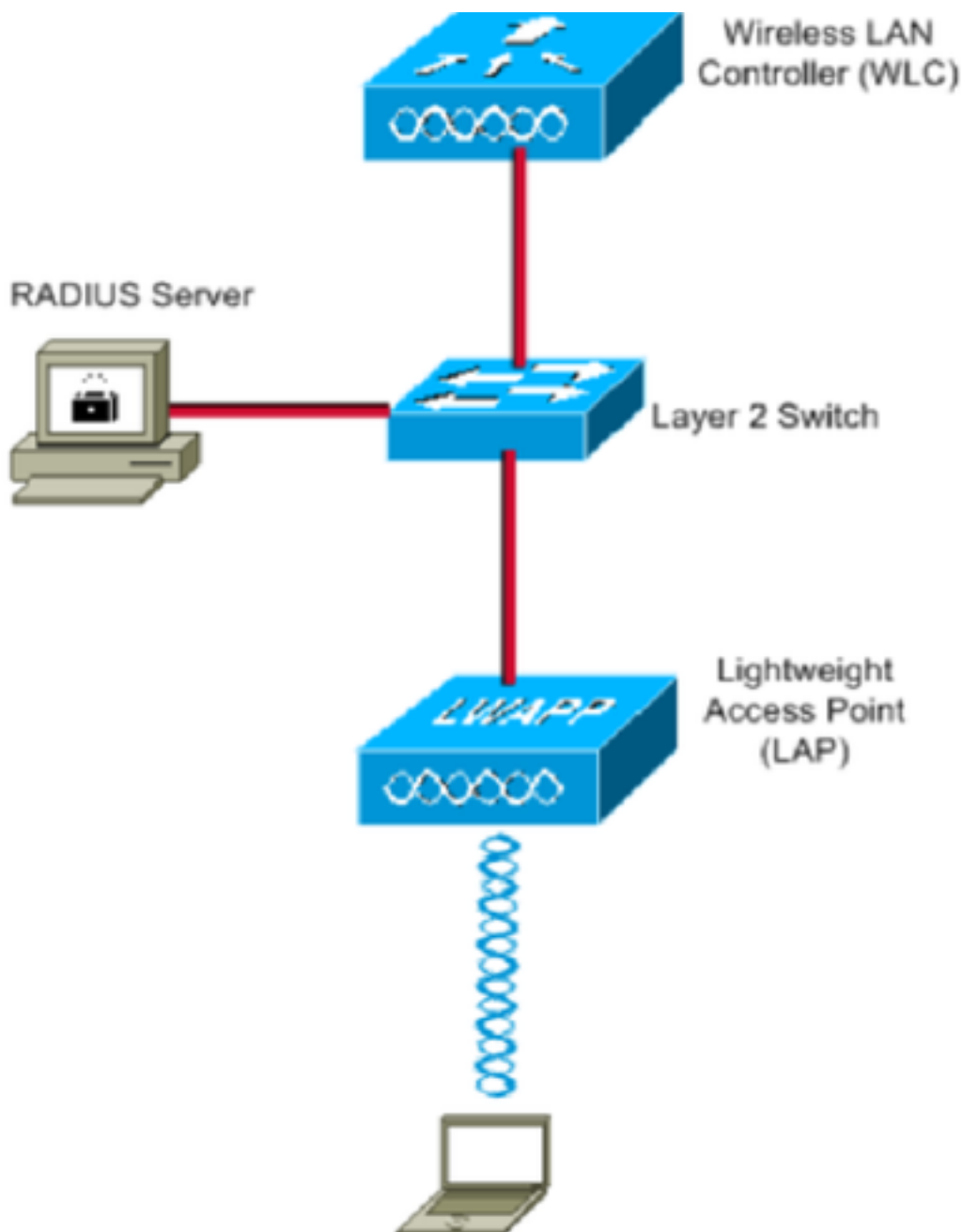
De VLAN-ID is 12 bits en neemt een waarde tussen 1 en 4094, inclusief. Omdat de Tunnel-Private-Group-ID van type string is, zoals gedefinieerd in [RFC2868](#) voor gebruik met IEEE 802.1X, wordt de integerwaarde van VLAN ID gecodeerd als een string. Wanneer deze tunnelkenmerken worden verstuurd, moeten ze in het veld Markering worden ingevoerd.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Dit zijn de configuratiegegevens van de in dit schema gebruikte onderdelen:

- Het IP-adres van Cisco ISE (RADIUS) server is 10.10.1.24.
- Het Management Interface-adres van de WLC is 10.10.1.17.
- De interne DHCP-server op de controller wordt gebruikt om het IP-adres aan draadloze klanten toe te wijzen.
- In dit document wordt 802.1x met PEAP als veiligheidsmechanisme gebruikt.
- VLAN102 wordt gebruikt door deze configuratie. De gebruikersnaam jonathga-102 is ingesteld om in VLAN102 te worden geplaatst door de RADIUS-server.

Configuratiestappen

Deze configuratie is in drie categorieën verdeeld:

- Cisco ISE-configuratie.
- Configureer de Switch voor meerdere VLAN's.
- Catalyst 9800 WLC configuratie.

Cisco ISE-configuratie

Voor deze configuratie zijn de volgende stappen vereist:

- Configureer de Catalyst WLC als een AAA-client op de Cisco ISE-server.
- Configureer interne gebruikers op Cisco ISE.
- Configureer de RADIUS (IETF)-kenmerken die worden gebruikt voor dynamische VLAN-toewijzing op Cisco ISE.

Stap 1. Configureer de Catalyst WLC als een AAA-client op de Cisco ISE-server

Deze procedure legt uit hoe de WLC als een AAA-client op de ISE-server moet worden toegevoegd zodat de WLC de gebruikersreferenties aan ISE kan doorgeven.

Voer de volgende stappen uit:

1. Vink vanuit de ISE GUI naar **Administration > Network Resources > Network Devices** en selecteer **Add**.
2. Voltooi de configuratie met het WLC beheer-IP-adres en het RADIUS-gedeelde geheim tussen WLC en ISE zoals in de afbeelding:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MD

Network Devices

Default Device

Device Security Settings

Network Devices List > **New Network Device**

Network Devices

* Name

Description

IP Address * IP: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

* Shared Secret

Use Second Shared Secret

CoA Port

Stap 2. Configureer interne gebruikers op Cisco ISE

Deze procedure legt uit hoe de gebruikers aan de interne gebruikersdatabase van Cisco ISE moeten worden toegevoegd.

Voer de volgende stappen uit:

1. Vink vanuit de ISE GUI naar **Administration > Identity Management > Identities** en selecteer **Add**.
2. Voltooi de configuratie met de gebruikersnaam, het wachtwoord en de gebruikersgroep zoals in de afbeelding wordt weergegeven:

The screenshot shows the 'New Network Access User' configuration page in the Cisco ISE GUI. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The page title is 'Network Access Users List > New Network Access User'. The configuration fields are as follows:

- Network Access User:**
 - * Name: jonathga-102
 - Status: Enabled
 - Email: (empty)
- Passwords:**
 - Password Type: Internal Users
 - * Login Password: (masked) Re-Enter Password: (masked) [Generate Password]
 - Enable Password: (masked) (masked) [Generate Password]
- User Information:**
 - First Name: (empty)
 - Last Name: (empty)
- Account Options:**
 - Description: (empty)
 - Change password on next login:
- Account Disable Policy:**
 - Disable account if date exceeds 2021-05-18 (yyyy-mm-dd)
- User Groups:**
 - VLAN102

Buttons: Submit, Cancel

Stap 3. Het configureren van de RADIUS (IETF) eigenschappen die gebruikt worden voor dynamische VLAN-toewijzing

Deze procedure legt uit hoe een autorisatieprofiel en een authenticatiebeleid voor draadloze gebruikers kunnen worden gecreëerd.

Voer de volgende stappen uit:

1. Vink vanuit de ISE GUI naar **Policy > Policy Elements > Results > Authorization > Authorization profiles** en selecteer **Add** om een nieuw profiel te maken.
2. Voltooi de configuratie van het autorisatieprofiel met VLAN-informatie voor de betreffende groep. Deze afbeelding toont **jonathga-VLAN-102** instellingen voor groepsconfiguratie.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > jonathga-VLAN-102

Authorization Profile

* Name

Description

Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN Tag ID **1** ID/Name

Advanced Attributes Settings

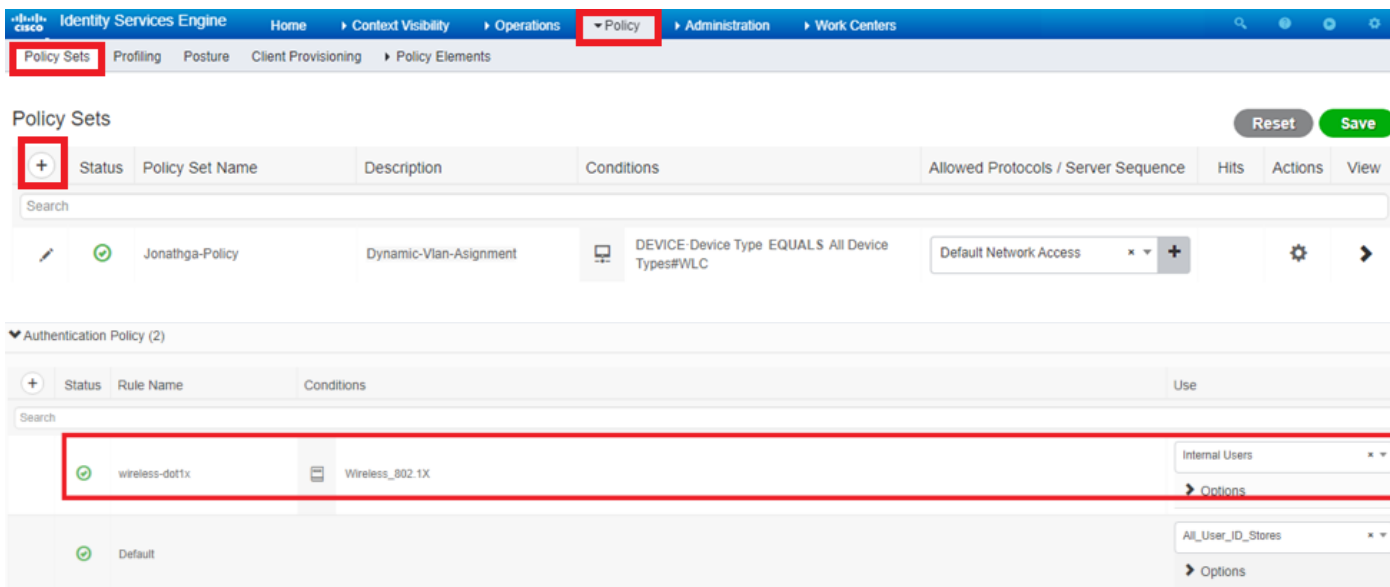
Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:102
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

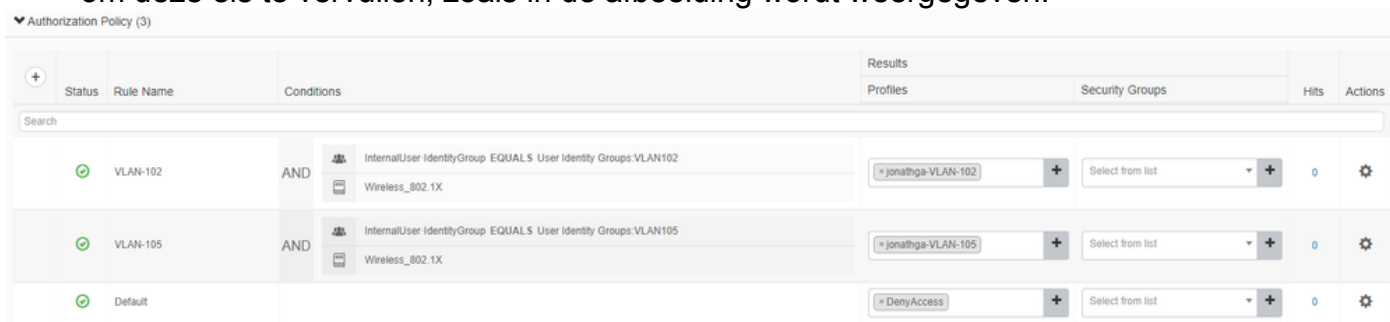
Nadat de autorisatieprofielen zijn ingesteld, moet een verificatiebeleid voor draadloze gebruikers worden gecreëerd. U kunt een nieuw apparaat gebruiken custom beleid voeren of de Default Beleidsreeks. In dit voorbeeld wordt een aangepaste profiel gemaakt.

3. Navigeren in om Policy > Policy Sets en selecteer Add om een nieuw beleid te creëren zoals in de afbeelding wordt getoond :



U moet nu een autorisatiebeleid voor gebruikers ontwikkelen om een respectievelijke autorisatieprofiel toe te kennen gebaseerd op groepslidmaatschap.

5. De afbeelding openen **Authorization policy** Hierin selecteert u een gedeelte en maakt u beleid om deze eis te vervullen, zoals in de afbeelding wordt weergegeven:



De Switch voor meerdere VLAN's configureren

Om meerdere VLAN's door de switch toe te staan, moet u deze opdrachten uitvoeren om de switch poort te configureren die op de controller is aangesloten:

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

Opmerking: Standaard staan de meeste switches alle VLAN's toe die op die switch via de boomstamport zijn gemaakt. Als een bekabeld netwerk op de switch is aangesloten, kan deze configuratie worden toegepast op de switch die op het bekabelde netwerk aangesloten is. Dit maakt de communicatie tussen dezelfde VLAN's in het bekabelde en draadloze netwerk mogelijk.

Catalyst 9800 WLC-configuratie

Voor deze configuratie zijn de volgende stappen vereist:

- Configureer de WLC met de details van de verificatieserver.
- Configureer de VLAN's.
- Configureer de WLAN's (SSID's).
- Configureren van beleidsprofiel.
- Configuratie van de tag Beleid.
- De beleidskabel aan een AP toewijzen.

Stap 1. Configureer de WLC met de details van de verificatieserver

Het is nodig om de WLC te configureren zodat het kan communiceren met de RADIUS-server om de clients te authenticeren.

Voer de volgende stappen uit:

1. Ga vanuit de controller GUI naar **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** en voer de RADIUS-serverinformatie in zoals in de afbeelding:

The screenshot displays the Cisco WLC GUI interface for configuring AAA. On the left is a dark sidebar menu with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Authentication Authorization and Accounting'. It features a '+ AAA Wizard' button at the top. Below this are three tabs: 'AAA Method List', 'Servers / Groups' (highlighted with a red box), and 'AAA Advanced'. Under the 'Servers / Groups' tab, there are '+ Add' and 'Delete' buttons, with the '+ Add' button highlighted by a red box. Below the buttons is a list of AAA methods, including 'RADIUS' (highlighted with a red box) and 'TACACS+'. To the right of the 'RADIUS' method, there are two sub-tabs: 'Servers' (highlighted with a blue bar) and 'Server Groups'. Below these sub-tabs is a table with columns for 'Name' and 'Address'.

Create AAA Radius Server

Name*	Cisco-ISE	Support for CoA	ENABLED <input checked="" type="checkbox"/> ⓘ
Server Address*	10.10.1.24	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* ⓘ	Automate Tester	<input type="checkbox"/>
Confirm Key*		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

- Als u de RADIUS-server aan een RADIUS-groep wilt toevoegen, navigeer dan naar **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** zoals in de afbeelding:

Create AAA Radius Server Group



Name*

ISE-SERVER

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

DISABLED

Source Interface VLAN ID

none

Available Servers

Assigned Servers

server-2019

Cisco-ISE

Cancel

Apply to Device

3. Om een verificatiemethode te maken, navigeer dan naar **Configuration > Security > AAA > AAA Method List > Authentication > + Add** zoals in de afbeeldingen:

The screenshot shows the network configuration interface. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), and Administration. The main content area is titled "Authentication Authorization and Accounting". It features a blue "+ AAA Wizard" button, a blue "AAA Method List" button (highlighted with a red box), and a "Servers / Groups" section. Under "General", the "Authentication" tab is selected (highlighted with a red box). In the "Servers / Groups" table, a blue "+ Add" button is highlighted with a red box. Below the table, the "Authorization" section is partially visible.

Quick Setup: AAA Authentication

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- radgrp_SykesLab
- server2019
- tacacgrp_SykesLab

Assigned Server Groups

- ISE-SERVER

Stap 2. Configureer de VLAN's

Deze procedure legt uit hoe u VLAN's op Catalyst 9800 WLC kunt configureren. Zoals eerder in dit document wordt uitgelegd, moet de VLAN-ID die onder de eigenschap Tunnel-Private-Group ID van de RADIUS-server is gespecificeerd, ook in de WLC voorkomen.

In het voorbeeld wordt de gebruiker jonathga-102 gespecificeerd met de Tunnel-Private-Group ID of 102 (VLAN =102) op de RADIUS-server.

1. Navigeren in om Configuration > Layer2 > VLAN > VLAN > + Add zoals in de afbeelding:

The screenshot shows the Catalyst 9800 WLC configuration interface. On the left, a dark sidebar contains navigation options: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is titled 'VLAN' and features a tabbed interface with 'SVI' and 'VLAN' (highlighted with a red box) tabs. Below the tabs are '+ Add' and 'x Delete' buttons, with the '+ Add' button highlighted in red. A table lists existing VLANs:

VLAN ID	Name
1	default
100	VLAN100
210	VLAN210
2602	VLAN2602

2. Geef de benodigde informatie op zoals in de afbeelding:

Create VLAN ✕

Create a single VLAN

VLAN ID*

Name

State **ACTIVATED**

IGMP Snooping DISABLED

ARP Broadcast DISABLED

Port Members

Available (2)

- Gi1 ➔
- Gi2 ➔

Associated (0)

No Associated Members

Create a range of VLANs

VLAN Range* - (Ex:5-7)

Opmerking: Als u geen naam specificeert, wordt VLAN automatisch toegewezen aan de naam van VLAN XXXX, waar XXXX de VLAN-id is.

Herhaal stap 1 en 2 voor alle gewenste VLAN's, kunt u na deze stap 3 verder gaan.

- Controleer of de VLAN's in uw gegevensinterfaces zijn toegestaan. Als u een havenkanaal in gebruik hebt, navigeer om **Configuration > Interface > Logical > PortChannel name > General**. Als u deze als ingesteld ziet **Allowed VLAN = All** Je bent klaar met de configuratie. Indien u ziet **Allowed VLAN = VLANs IDs**, voeg de gewenste VLAN's toe en selecteer vervolgens **Update & Apply to Device**. Als u geen poortkanaal in gebruik hebt, navigeer dan naar **Configuration > Interface > Ethernet > Interface Name > General**. Als u deze als ingesteld ziet **Allowed VLAN = All** Je bent klaar met de configuratie. Indien u ziet **Allowed VLAN = VLANs IDs**, voeg de gewenste VLAN's toe en selecteer vervolgens **Update & Apply to Device**.

Deze beelden tonen de configuratie met betrekking tot de interfaceinstelling als u Alle of specifieke VLAN IDs gebruikt.

General

Advanced

Interface

GigabitEthernet3

Description

(1-200 Characters)

Admin Status

UP 

Port Fast

disable ▼

Enable Layer 3 Address

DISABLED

Switchport Mode

trunk ▼

Allowed Vlan


All Vlan IDs

Native Vlan

▼

General

Advanced

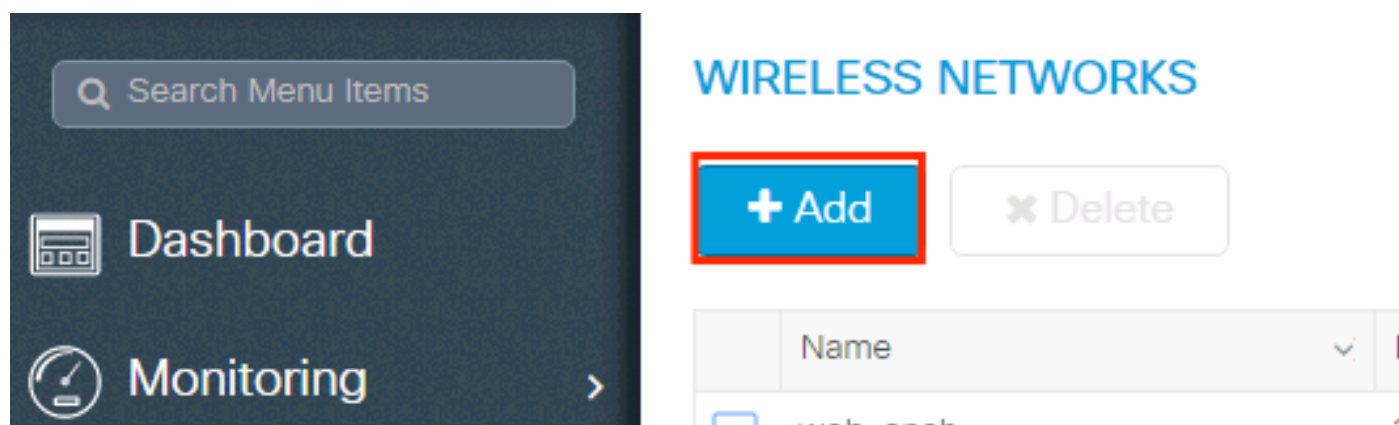
Interface	GigabitEthernet1	
Description	<input type="text"/>	(1-200 Characters)
Speed	1000	▼
Admin Status	UP 	
Enable Layer 3 Address	<input type="checkbox"/> DISABLED	
Switchport Mode	trunk ▼	
Allowed Vlan	<input type="radio"/> All <input checked="" type="radio"/> Vlan IDs	
Vlan IDs	551,102,105	(e.g. 1,2,4,6-10)
Native Vlan	551 ▼	

Stap 3. Configureer de WLAN's (SSID's)

Deze procedure legt uit hoe de WLAN's in de WLC moeten worden configureren.

Voer de volgende stappen uit:

1. Om de WLAN's te maken. Navigeren in om **Configuration > Wireless > WLANs > + Add** en stel het netwerk zo nodig in, zoals in de afbeelding wordt getoond:



2. Voer de WLAN-informatie in zoals in de afbeelding:

Add WLAN ✕

General Security Advanced

Profile Name*	Dinamyc-VLAN	Radio Policy	All ▼
SSID*	Dinamyc-VLAN	Broadcast SSID	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	6		
Status	ENABLED <input checked="" type="checkbox"/>		

Cancel

Apply to Device

3. Navigeren in om **Security** en selecteer de gewenste beveiligingsmethode. In dit geval was er WAP2 + 802.1x zoals in de afbeeldingen:

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	WPA + WPA2 ▼	Fast Transition	Adaptive Enab... ▼
MAC Filtering	<input type="checkbox"/>	Over the DS	<input checked="" type="checkbox"/>
Protected Management Frame		Reassociation Timeout	20
PMF	Disabled ▼		
WPA Parameters			
WPA Policy	<input type="checkbox"/>		

Cancel Save & Apply to Device

Add WLAN

PMF Disabled

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

VanSecurity > AAA tab, selecteer de verificatiemethode die op stap 3 is gemaakt **Configure the WLC with the Details of the Authentication Server** gedeelte zoals in de afbeelding weergegeven:

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISE-SERVER ⓘ

Local EAP Authentication

Cancel Apply to Device

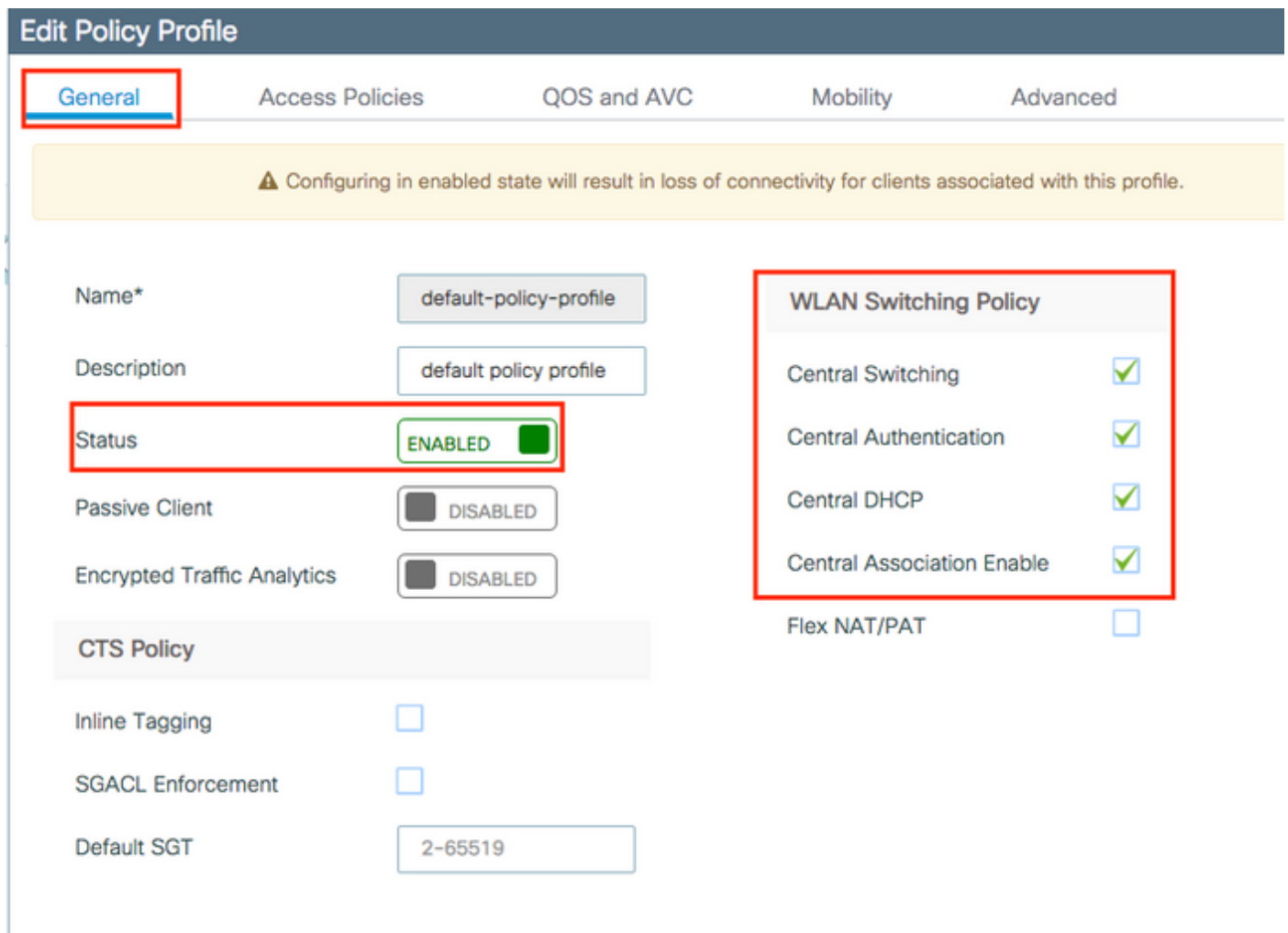
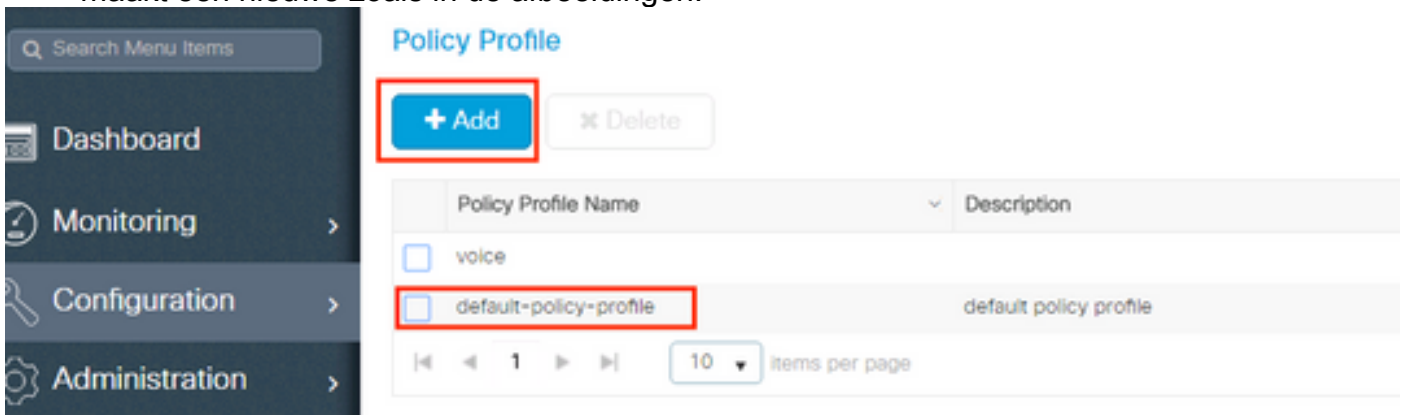
Stap 4. Het beleidsprofiel configureren

Deze procedure legt uit hoe u het beleidsprofiel in de WLC kunt configureren.

Voer de volgende stappen uit:

1. Navigeren in om **Configuration > Tags & Profiles > Policy Profile** en of pas uw default-policy-profile of

maakt een nieuwe zoals in de afbeeldingen:



2. Van de **Access Policies** tab toewijzen aan het VLAN waaraan de draadloze clients worden toegewezen wanneer ze standaard verbinding maken met dit WLAN zoals in de afbeelding:

Edit Policy Profile

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

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Opmerking: In het voorbeeld dat wordt gegeven, is het de taak van de RADIUS-server om een draadloze client aan een specifiek VLAN toe te wijzen bij succesvolle verificatie, zodat het VLAN dat op het beleidsprofiel is geconfigureerd een zwart gat VLAN kan zijn, de RADIUS-server voert deze afbeelding over en wijst de gebruiker die door dat WLAN komt toe aan het VLAN dat onder het veld Tunnel-Group-Private-ID in de RADIUS-server is gespecificeerd.

- Van de **Advance** tabblad, schakelt u het **Allow AAA Override** Schakel het vakje in om de WLC-configuratie te omzeilen wanneer de RADIUS-server de eigenschappen teruggeeft die nodig zijn om de client op het juiste VLAN te plaatsen zoals in de afbeelding:

Edit Policy Profile

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile Search or Select

Umbrella Parameter Map Not Configured

mDNS Service Policy default-mdns-service [Clear](#)

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

5 GHz Policy Search or Select

Cancel Update & Apply to Device

Stap 5. De beleidsmarkering configureren

Deze procedure legt uit hoe u de beleidstag in de WLC kunt configureren.

Voer de volgende stappen uit:

1. Navigeren in om **Configuration > Tags & Profiles > Tags > Policy** en voeg indien nodig een nieuwe toe zoals in de afbeelding:

Search Menu Items

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

Manage Tags

Policy Site RF AP

+ Add x Delete

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

10 items per page

2. Voeg een naam toe aan de Beleidslang en selecteer +Add, zoals in de afbeelding wordt getoond:

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

3. Koppel uw WLAN-profiel aan het gewenste beleidsprofiel zoals in de afbeeldingen:

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

Add Policy Tag



Name*

Dynamic-VLAN

Description

Enter Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> Dinamyc-VLAN	default-policy-profile

10 items per page 1 - 1 of 1 items

RLAN-POLICY Maps: 0

Cancel

Apply to Device

Stap 6. De beleidslaag aan een AP toewijzen

Deze procedure legt uit hoe u de beleidstag in de WLC kunt configureren.

Voer de volgende stappen uit:

1. Navigeren in om **Configuration > Wireless > Access Points > AP Name > General Tags** en verdeel de desbetreffende beleidslaag en selecteer vervolgens **Update & Apply to Device** zoals in de afbeelding:

Edit AP
✕

General
Interfaces
High Availability
Inventory
ICap
Advanced

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Tags

Policy

Site

Version

Primary Software Version

Predownloaded Status

Predownloaded Version

Next Retry Time

Boot Version

IOS Version

Mini IOS Version

IP Config

CAPWAP Preferred Mode

DHCP IPv4 Address

Static IP (IPv4/IPv6)

Time Statistics

Up Time

Controller Association Latency

↶ Cancel

Voorzichtig: Let erop dat als de beleidstag op een AP wordt gewijzigd, de associatie op de WLC wordt verminderd en dat deze opnieuw wordt toegevoegd.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Test-verbinding met Windows 10 en inheemse smeekbede, zodra u voor een gebruikersnaam en wachtwoord wordt gevraagd, voer de informatie van de gebruiker in die aan een VLAN op ISE in kaart is gebracht.

In het vorige voorbeeld, merk op dat jonathga-102 aan VLAN102 wordt toegewezen zoals gespecificeerd in de server van de RADIUS. Dit voorbeeld gebruikt deze gebruikersnaam om authenticatie te ontvangen en aan een VLAN toe te wijzen door de RADIUS-server:

Nadat de authenticatie is voltooid, moet u controleren dat uw client is toegewezen aan het juiste

VLAN zoals per verzonden RADIUS-eigenschappen. Voltooi de volgende stappen om deze taak te volbrengen:

1. Ga vanuit de controller GUI naar **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** en zoek naar het VLAN-veld zoals in de afbeelding:

The screenshot shows the Cisco controller GUI. On the left, the 'Clients' page displays a table with one client selected: MAC address b88a.6010.3c60, IPv4 address 10.10.102.121, and IPv6 address fe80::d8a2:dc93:3758:6. On the right, the 'Client' details page is open, with the 'Security Information' tab selected. Under 'Server Policies', the 'VLAN' field is set to 102. Under 'Resultant Policies', the 'VLAN' field is also set to 102.

Vanuit dit venster kunt u zien dat deze client is toegewezen aan VLAN102 zoals in de RADIUS-eigenschappen die op de RADIUS-server zijn ingesteld. Vanaf de CLI kunt u de `show wireless client summary detail` u kunt dezelfde informatie weergeven als in de afbeelding:

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address      SSID          AP Name      State  IP Address  Device-type  VLAN
BSSID           Auth Method  Created     Connected  Protocol Channel Width  SGI NSS Rate  CAP  Username
-----
[REDACTED] 10.3c60 Dinamyc-VLAN AIR-AP2802I-A-K9 Run 10.10.105.200 Intel-Device 105
[REDACTED] 44.4000 [802.1X] 05 06 11n(2.4) 1 20/20 Y/Y 1/1 24.0 E jonathga-105

Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address      SSID          AP Name      State  IP Address  Device-type  VLAN
BSSID           Auth Method  Created     Connected  Protocol Channel Width  SGI NSS Rate  CAP  Username
-----
[REDACTED] 10.3c60 Dinamyc-VLAN AIR-AP2802I-A-K9 Run 10.10.102.121 Intel-Device 102
[REDACTED] 44.4000 [802.1X] 54 55 11n(2.4) 1 20/20 Y/Y 1/1 m5 E jonathga-102
```

2. Het is mogelijk de **Radioactive traces** om te zorgen voor een succesvolle overdracht van de RADIUS-kenmerken aan de WLC. Volg daartoe de volgende stappen: Ga vanuit de controller GUI naar **Troubleshooting > Radioactive Trace > +Add**. Voer het Mac-adres van de draadloze client in. Selecteren **start**. Sluit de client aan op WLAN. Navigeren in om **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**.

Dit gedeelte van de sporenoutput zorgt voor een succesvolle overdracht van RADIUS-kenmerken:


```

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: authenticator e5 5e
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: User-Name
[11] 13 "jonathga-102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: State
[24] 40 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Class
[25] 54 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Type
[64] 6 VLAN [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Medium-Type
[65] 6 ALL_802 [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Message
[79] 6 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Message-
Authenticator[80] 18 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Private-
Group-Id[81] 6 "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Key-Name
[102] 67 *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Send-Key
[16] 52 *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Recv-Key
[17] 52 *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: username 0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: class 0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30 ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: tunnel-type 1 13 [vlan] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :
tunnel-medium-type 1 6 [ALL_802] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:tunnel-private-group-id 1 "102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: timeout 0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile

```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Gebruikershandleiding](#)