

Configuration de l'attribution dynamique de VLAN avec ISE et le contrôleur de réseau local sans fil Catalyst 9800

Contenu

[Introduction](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Affectation de VLAN dynamique avec le serveur RADIUS](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration Steps](#)

[Configuration de Cisco ISE](#)

[Étape 1. Configurer le WLC Catalyst en tant que client AAA sur le serveur Cisco ISE](#)

[Étape 2. Configurer les utilisateurs internes sur Cisco ISE](#)

[Étape 3. Configurez les attributs RADIUS \(IETF\) utilisés pour l'attribution dynamique de VLAN](#)

[Configurer la commutation pour plusieurs VLAN](#)

[Configuration du WLC du Catalyst 9800](#)

[Étape 1. Configurer le WLC avec les détails du serveur d'authentification](#)

[Étape 2. Configurer les VLAN](#)

[Étape 3. Configurer les WLAN \(SSID\)](#)

[Étape 4. Configurer le profil de stratégie](#)

[Étape 5. Configurer la balise de stratégie](#)

[Étape 6. Attribuer le Balise de stratégie à un point d'accès](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit le concept d'affectation de VLAN dynamique et comment configurer le contrôleur de réseau local sans fil (WLC) Catalyst 9800 et Cisco Identity Service Engine (ISE) pour attribuer un LAN sans fil (WLAN) afin d'accomplir ceci pour les clients sans fil.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Avoir une connaissance de base du WLC et des points d'accès légers (LAP).
- Connaître le serveur AAA, par exemple ISE.
- posséder une connaissance approfondie des réseaux sans fil et des problèmes de sécurité

sans fil ;

- Avoir des connaissances fonctionnelles sur l'affectation dynamique de VLAN.
- Connaître de base le contrôle et la mise en service du point d'accès sans fil (CAPWAP).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC Cisco Catalyst 9800 (Catalyst 9800-CL) qui exécute la version 16.12.4a du micrologiciel.
- LAP de la gamme Cisco 2800 en mode local.
- Complicant Windows 10 natif.
- Cisco Identity Service Engine (ISE) qui exécute la version 2.7.
- Commutateur de la gamme Cisco 3850 qui exécute la version 16.9.6 du micrologiciel.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Affectation de VLAN dynamique avec le serveur RADIUS

Dans la plupart des systèmes de réseau local sans fil (WLAN), chaque WLAN a une politique statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier). Bien que puissante, cette méthode présente des limites car elle exige que les clients s'associent à différents SSID pour hériter de politiques de sécurité et de qualité de service différentes.

Cependant, la solution WLAN de Cisco prend en charge la mise en réseau d'identités. Cela permet au réseau d'annoncer un SSID unique et permet à des utilisateurs spécifiques d'hériter de politiques de sécurité ou de qualité de service différentes en fonction des informations d'identification de l'utilisateur.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. La tâche d'affectation d'utilisateurs à un VLAN spécifique est gérée par un serveur d'authentification RADIUS, tel que Cisco ISE. Elle peut être utilisée, par exemple, pour permettre à l'hôte sans fil de rester sur le même VLAN alors qu'il se déplace au sein d'un réseau de campus.

Par conséquent, lorsqu'un client tente de s'associer à un LAP enregistré auprès d'un contrôleur, le WLC transmet les informations d'identification de l'utilisateur au serveur RADIUS pour validation. Une fois que l'authentification est réussie, le serveur RADIUS passe certains attributs de l'Internet Engineering Task Force (IETF) à l'utilisateur. Ces attributs RADIUS déterminent l'ID de VLAN qui doit être attribué au client sans fil. Le SSID du client n'a pas d'importance car l'utilisateur est toujours affecté à cet ID de VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

- IETF 64 (Tunnel Type) — Définissez cette valeur sur VLAN.
- IETF 65 (Tunnel Medium Type) — Définissez cette valeur sur 802.
- IETF 81 (Tunnel Private Group ID) — Définissez cette valeur sur l'ID du VLAN

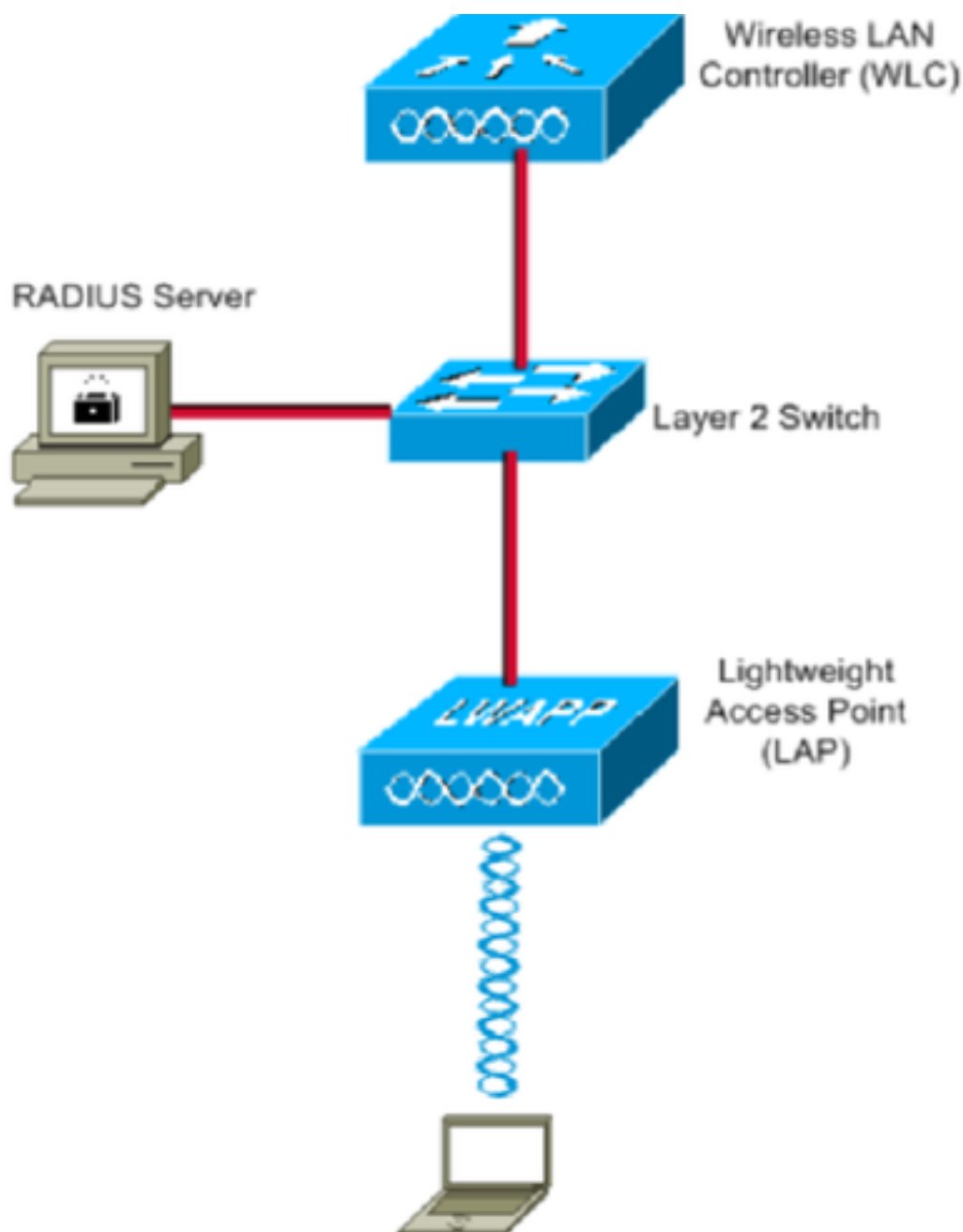
L'ID de VLAN est de 12 bits et prend une valeur comprise entre 1 et 4 094, inclus. Puisque Tunnel-Private-Group-ID est de type chaîne, comme défini dans [RFC2868 pour une utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée en tant que chaîne](#). Lorsque ces attributs de tunnel sont envoyés, il est nécessaire de les entrer dans le champ Balise.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur Cisco ISE (RADIUS) est 10.10.1.24.
- L'adresse de l'interface de gestion du WLC est 10.10.1.17.
- Le serveur DHCP interne sur le contrôleur est utilisé pour affecter l'adresse IP aux clients sans fil.
- Ce document utilise 802.1x avec PEAP comme mécanisme de sécurité.
- VLAN102 est utilisé dans toute cette configuration. Le nom d'utilisateur jonathga-102 est configuré pour être placé dans le VLAN102 par le serveur RADIUS.

Configuration Steps

Cette configuration est divisée en trois catégories :

- Configuration de Cisco ISE.
- Configurez le commutateur pour plusieurs VLAN.
- Configuration du WLC du Catalyst 9800.

Configuration de Cisco ISE

Cette configuration requiert les étapes suivantes :

- Configurez le WLC Catalyst en tant que client AAA sur le serveur Cisco ISE.
- Configurez les utilisateurs internes sur Cisco ISE.
- Configurez les attributs RADIUS (IETF) utilisés pour l'attribution dynamique de VLAN sur Cisco ISE.

Étape 1. Configurer le WLC Catalyst en tant que client AAA sur le serveur Cisco ISE

Cette procédure explique comment ajouter le WLC en tant que client AAA sur le serveur ISE afin que le WLC puisse transmettre les informations d'identification de l'utilisateur à ISE.

Procédez comme suit :

1. À partir de l'interface utilisateur graphique ISE, accédez à **Administration > Network Resources > Network Devices** et sélectionnez **Add**.
2. Complétez la configuration avec l'adresse IP de gestion du WLC et le secret partagé RADIUS entre le WLC et ISE, comme indiqué sur l'image :

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 /

* 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

Étape 2. Configurer les utilisateurs internes sur Cisco ISE

Cette procédure explique comment ajouter les utilisateurs dans la base de données utilisateur interne de Cisco ISE.

Procédez comme suit :

1. À partir de l'interface utilisateur graphique ISE, accédez à **Administration > Identity Management > Identities** et sélectionnez **Add**.
2. Complétez la configuration avec le nom d'utilisateur, le mot de passe et le groupe d'utilisateurs, comme illustré dans l'image :

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Network Access Users List > New Network Access User

Users

Latest Manual Network Scan Results

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="Generate Password"/> ⓘ

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

Étape 3. Configurez les attributs RADIUS (IETF) utilisés pour l'attribution dynamique de VLAN

Cette procédure explique comment créer un profil d'autorisation et une stratégie d'authentification pour les utilisateurs sans fil.

Procédez comme suit :

1. À partir de l'interface utilisateur graphique ISE, accédez à **Policy > Policy Elements > Results > Authorization > Authorization profiles** et sélectionnez **Add** pour créer un nouveau profil.
2. Complétez la configuration du profil d'autorisation avec les informations VLAN pour le groupe respectif. Cette image montre **jonathga-VLAN-102** paramètres de configuration du groupe.

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile named "jonathga-VLAN-102". The navigation path is: Policy > Policy Elements > Results. The left sidebar shows the "Authorization" section expanded, with "Authorization Profiles" selected. The main configuration area includes the following fields and options:

- Name:** jonathga-VLAN-102
- Description:** Dynamic-Vlan-Assignment
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**
- Passive Identity Tracking:**

The "Common Tasks" section includes the following options:

- DACL Name
- ACL (Filter-ID)
- Security Group
- VLAN (Tag ID 1, ID/Name 102)

The "Advanced Attributes Settings" section shows a dropdown menu for "Select an item" with a plus sign icon.

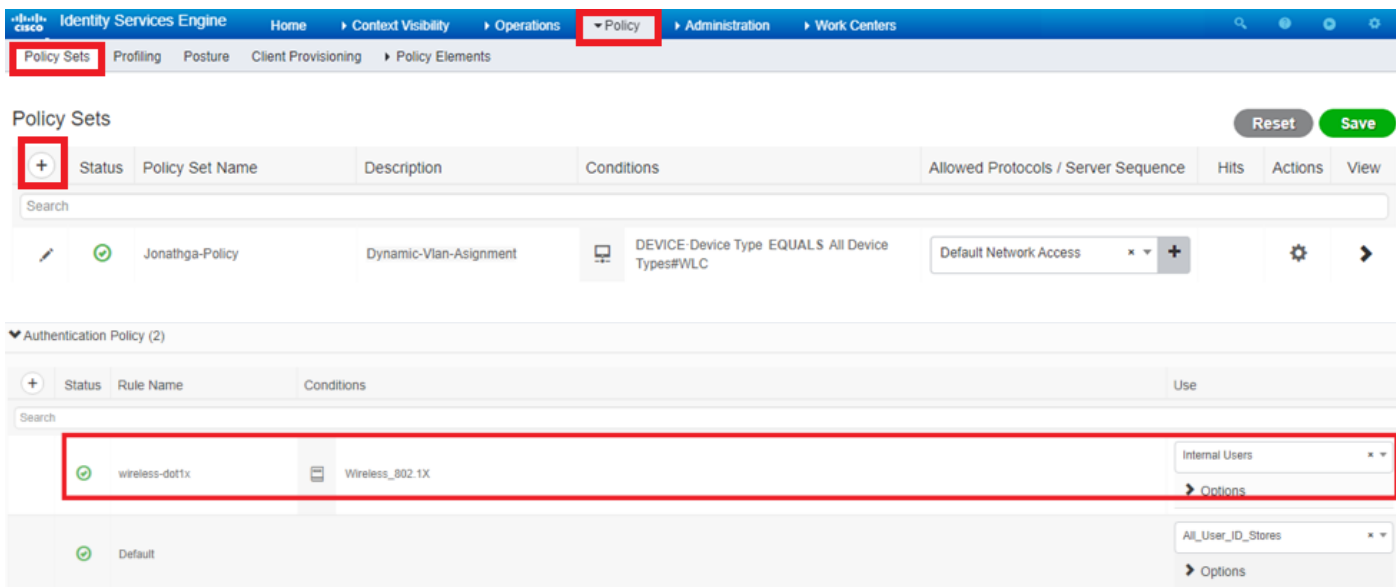
The "Attributes Details" section displays the following information:

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

The "Save" button is highlighted with a red box.

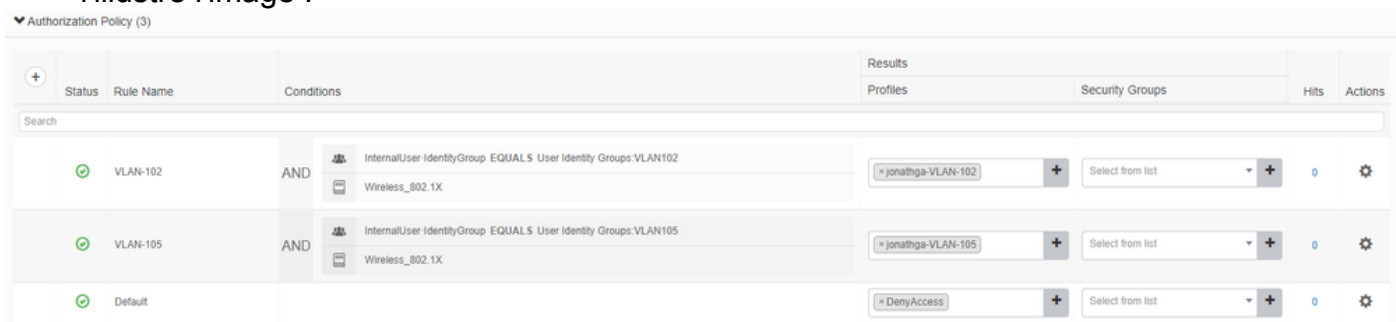
Une fois les profils d'autorisation configurés, une stratégie d'authentification pour les utilisateurs sans fil doit être créée. Vous pouvez utiliser une nouvelle custom ou modifiez le Default Jeu de stratégies. Dans cet exemple, un profil personnalisé est créé.

3. Accéder à **Policy > Policy Sets** et sélectionnez **Add** pour créer une nouvelle stratégie comme l'illustre l'image :



Vous devez maintenant créer des stratégies d'autorisation pour les utilisateurs afin d'attribuer un profil d'autorisation respectif basé sur l'appartenance au groupe.

5. Ouvrez le **Authorization policy** et créez des stratégies pour accomplir cette condition, comme l'illustre l'image :



Configurer la commutation pour plusieurs VLAN

Pour autoriser plusieurs VLAN via le commutateur, vous devez émettre ces commandes pour configurer le port de commutateur connecté au contrôleur :

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

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

Note: Par défaut, la plupart des commutateurs autorisent tous les VLAN créés sur ce commutateur à travers le port de jonction. Si un réseau câblé est connecté au commutateur, alors cette même configuration peut être appliquée au port de commutation qui se connecte au réseau câblé. Cela active la communication entre les mêmes VLAN dans le réseau câble et sans fil.

Configuration du WLC du Catalyst 9800

Cette configuration requiert les étapes suivantes :

- Configurez le WLC avec les détails du serveur d'authentification.
- Configurez les VLAN.
- Configurez les WLAN (SSID).
- Configurez le profil de stratégie.
- Configurez la balise Policy.
- Attribuez la balise Policy à un point d'accès.

Étape 1. Configurer le WLC avec les détails du serveur d'authentification

Il est nécessaire de configurer le WLC afin qu'il puisse communiquer avec le serveur RADIUS pour authentifier les clients.

Procédez comme suit :

1. À partir de l'interface graphique du contrôleur, accédez à **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** et saisissez les informations du serveur RADIUS comme indiqué dans l'image :

The screenshot displays the Cisco WLC GUI. On the left is a dark sidebar menu with options: Dashboard, Monitoring, Configuration (highlighted), Administration, and Troubleshooting. The main content area is titled 'Authentication Authorization and Accounting'. It features a '+ AAA Wizard' button and three tabs: 'AAA Method List', 'Servers / Groups' (highlighted with a red box), and 'AAA Advanced'. Below the tabs are '+ Add' and 'Delete' buttons, with the '+ Add' button highlighted by a red box. Underneath, there are two sub-tabs: 'RADIUS' (highlighted with a red box) and 'TACACS+'. The 'RADIUS' sub-tab is active, showing two sub-sections: 'Servers' (highlighted with a blue underline) and 'Server Groups'. The 'Servers' section contains a table with columns '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		

2. Pour ajouter le serveur RADIUS à un groupe RADIUS, accédez à **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** comme le montre l'image :

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. Pour créer une liste de méthodes d'authentification, accédez à **Configuration > Security > AAA > AAA Method List > Authentication > + Add** comme le montrent les images :

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). A blue "+ Add" button (highlighted with a red box) is visible next to a "x Del" button. Below the tabs, a table with a "Name" column 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

Étape 2. Configurer les VLAN

Cette procédure explique comment configurer des VLAN sur le WLC Catalyst 9800. Comme expliqué plus tôt dans ce document, l'ID de VLAN spécifié sous l'attribut Tunnel-Private-Group ID du serveur RADIUS doit également exister dans le WLC.

Dans l'exemple, l'utilisateur jonathga-102 est spécifié avec le Tunnel-Private-Group ID of 102 (VLAN =102) sur le serveur RADIUS.

1. Accéder à Configuration > Layer2 > VLAN > VLAN > + Add comme le montre l'image :

Search Menu Items

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

VLAN

SVI **VLAN** VLAN Group

	VLAN ID	Name
<input type="checkbox"/>	1	default
<input type="checkbox"/>	100	VLAN
<input type="checkbox"/>	210	VLAN
<input type="checkbox"/>	2602	VLAN

2. Saisissez les informations nécessaires comme indiqué sur l'image :

✕
Create VLAN

Create a single VLAN

VLAN ID*

Name ⓘ

State ACTIVATED

IGMP Snooping DISABLED

ARP Broadcast DISABLED

Port Members 🔍 Search

Available (2)

Gi1 ➔

Gi2 ➔

Associated (0)

No Associated Members

Create a range of VLANs

VLAN Range* - (Ex:5-7)

↶ Cancel

📄 Apply to Device

Note: Si vous ne spécifiez pas de nom, le VLAN reçoit automatiquement le nom VLANXXXX, où XXXX est l'ID VLAN.

Répétez les étapes 1 et 2 pour tous les VLAN nécessaires, une fois terminé, vous pouvez passer à l'étape 3.

3. Vérifiez que les VLAN sont autorisés dans vos interfaces de données. Si vous utilisez un canal de port, accédez à **Configuration > Interface > Logical > PortChannel name > General**. Si vous le voyez configuré comme **Allowed VLAN = All** la configuration est terminée. Si vous voyez **Allowed VLAN = VLANs IDs**, ajoutez les VLAN nécessaires et, après cela, sélectionnez **Update & Apply to Device**. Si aucun canal de port n'est utilisé, accédez à **Configuration > Interface > Ethernet > Interface Name > General**. Si vous le voyez configuré comme **Allowed VLAN = All** la configuration est terminée. Si vous voyez **Allowed VLAN = VLANs IDs**, ajoutez les VLAN nécessaires et, après cela, sélectionnez **Update & Apply to Device**.

Ces images montrent la configuration associée à la configuration de l'interface si vous utilisez Tous ou des ID de VLAN spécifiques.

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

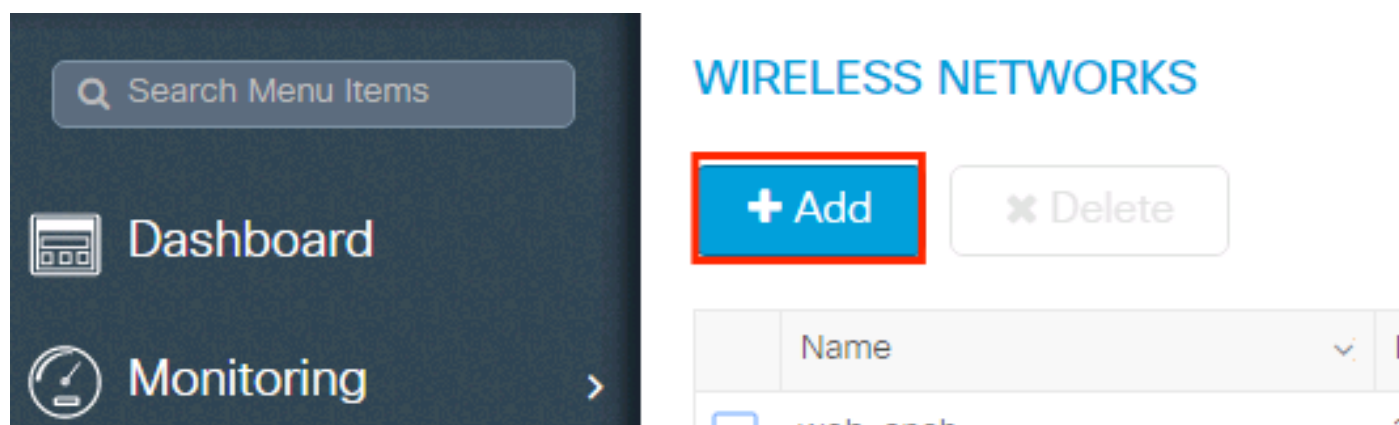
Interface	GigabitEthernet1	
Description	<input type="text"/>	(1-200 Characters)
Speed	1000	▼
Admin Status	UP 	
Enable Layer 3 Address	<input type="checkbox"/> DISABLED	
Switchport Mode	trunk ▼	
Allowed Vlan	<input type="radio"/> All <input checked="" type="radio"/> Vlan IDs	
Vlan IDs	551,102,105	(e.g.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

Étape 3. Configurer les WLAN (SSID)

Cette procédure explique comment configurer les WLAN dans le WLC.

Procédez comme suit :

1. Pour créer le WLAN. Accéder à **Configuration > Wireless > WLANs > + Add** et configurez le réseau en fonction des besoins, comme l'illustre l'image :



2. Entrez les informations WLAN comme indiqué sur l'image :

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. Accéder à **Security** et sélectionnez la méthode de sécurité requise. Dans ce cas, WPA2 + 802.1x, comme le montrent les images :

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

ExpéditeurSecurity > AAA , sélectionnez la méthode d'authentification créée à l'étape 3 dans **Configure the WLC with the Details of the Authentication Server** comme l'illustre l'image :

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISE-SERVER ⓘ

Local EAP Authentication

Cancel Apply to Device

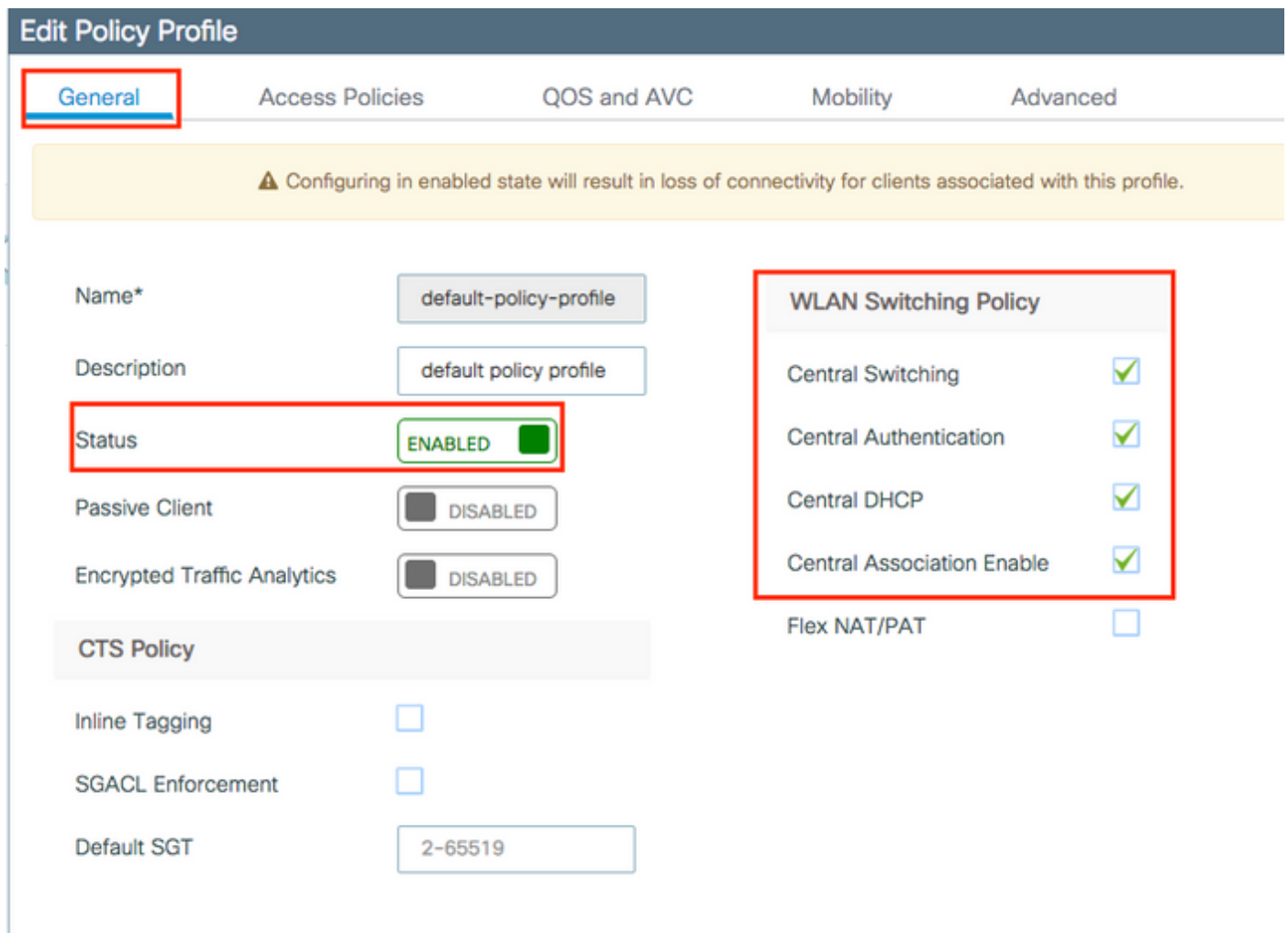
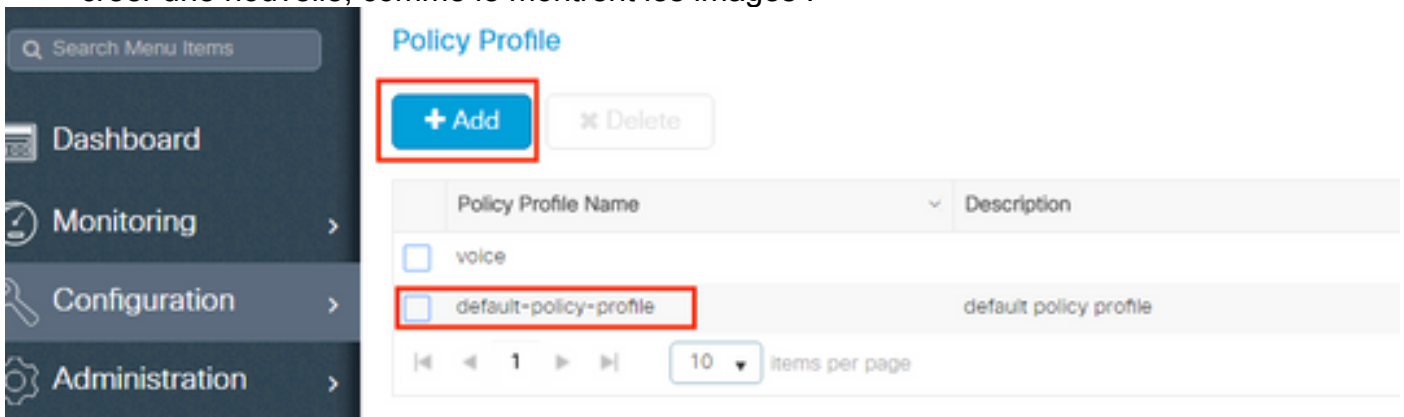
Étape 4. Configurer le profil de stratégie

Cette procédure explique comment configurer le profil de stratégie dans le WLC.

Procédez comme suit :

1. Accéder à **Configuration > Tags & Profiles > Policy Profile** et configurer votre **default-policy-profile** ou en

créer une nouvelle, comme le montrent les images :



2. A partir des versions **Access Policies** Attribuez par défaut le VLAN auquel les clients sans fil sont affectés lorsqu'ils se connectent à ce WLAN, comme illustré dans l'image :

The screenshot shows the 'Edit Policy Profile' interface with the 'Access Policies' tab selected. The interface is divided into several sections:

- WLAN Local Profiling:** Includes checkboxes for HTTP TLV Caching, RADIUS Profiling, and DHCP TLV Caching, all currently unchecked. It also has a 'Local Subscriber Policy Name' dropdown menu.
- VLAN:** This section is highlighted with a red box. It contains a 'VLAN/VLAN Group' dropdown menu with 'VLAN2602' selected, and a 'Multicast VLAN' input field with the placeholder text 'Enter Multicast VLAN'.
- WLAN ACL:** Includes 'IPv4 ACL' and 'IPv6 ACL' dropdown menus, both with 'Search or Select' options.
- URL Filters:** Includes 'Pre Auth' and 'Post Auth' dropdown menus, both with 'Search or Select' options.

Note: Dans l'exemple fourni, il incombe au serveur RADIUS d'affecter un client sans fil à un VLAN spécifique lors d'une authentification réussie. Par conséquent, le VLAN configuré sur le profil de stratégie peut être un VLAN à trou noir, le serveur RADIUS remplace ce mappage et affecte l'utilisateur qui passe par ce WLAN au VLAN spécifié sous le champ Tunnel-Group-Private-ID du serveur RADIUS.

3. A partir des versions *Advance* , activez la **Allow AAA Override** pour remplacer la configuration du WLC lorsque le serveur RADIUS retourne les attributs nécessaires pour placer le client sur le VLAN approprié, comme l'illustre l'image :

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

Étape 5. Configurer la balise de stratégie

Cette procédure explique comment configurer la balise Policy dans le WLC.

Procédez comme suit :

1. Accéder à Configuration > Tags & Profiles > Tags > Policy et en ajouter un nouveau si nécessaire, comme l'illustre l'image :

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. Ajoutez un nom à la balise de stratégie et sélectionnez +Add, comme le montre l'image :

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

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

3. Liez votre profil WLAN au profil de stratégie souhaité, comme illustré dans les images :

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*

Description

WLAN-POLICY Maps: 1

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

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

> RLAN-POLICY Maps: 0

Étape 6. Attribuer le Balise de stratégie à un point d'accès

Cette procédure explique comment configurer la balise Policy dans le WLC.

Procédez comme suit :

1. Accéder à **Configuration > Wireless > Access Points > AP Name > General Tags** et attribuez la balise de stratégie appropriée, puis sélectionnez **Update & Apply to Device** comme le montre l'image :

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

Update & Apply to Device

Attention : N'oubliez pas que lorsque la balise de stratégie sur un AP est modifiée, elle abandonne son association au WLC et se reconnecte.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Testez la connexion avec Windows 10 et le demandeur natif, une fois que vous êtes invité à entrer un nom d'utilisateur et un mot de passe, entrez les informations de l'utilisateur mappé à un VLAN sur ISE.

Dans l'exemple précédent, notez que jonathga-102 est attribué au VLAN102 comme spécifié dans le serveur RADIUS. Cet exemple utilise ce nom d'utilisateur pour recevoir l'authentification et être attribué à un VLAN par le serveur RADIUS :

Une fois l'authentification terminée, vous devez vérifier que votre client est affecté au VLAN

approprié conformément aux attributs RADIUS envoyés. Effectuez les étapes suivantes pour accomplir cette tâche :

1. À partir de l'interface graphique du contrôleur, accédez à **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** et recherchez le champ VLAN comme illustré dans l'image :

The screenshot shows the Cisco WLC 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... The right-hand pane shows the 'Client' configuration for this client. The 'General' tab is active, and the 'Security Information' sub-tab is selected. Under 'Server Policies', the 'VLAN' is configured to 102. Other fields like 'VLAN Name' are set to 'VLAN0102'.

Dans cette fenêtre, vous pouvez observer que ce client est affecté au VLAN102 conformément aux attributs RADIUS configurés sur le serveur RADIUS. À partir de l'interface de ligne de commande, vous pouvez utiliser le **show wireless client summary detail** pour afficher les mêmes informations que dans l'image

```
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. Il est possible d'activer **Radioactive traces** pour assurer le transfert réussi des attributs RADIUS vers le WLC. Pour ce faire, procédez comme suit : À partir de l'interface graphique du contrôleur, accédez à **Troubleshooting > Radioactive Trace > +Add**. Saisissez l'adresse MAC du client sans fil. Sélectionner **Start**. Connectez le client au WLAN. Accéder à **Stop > Generate > Choose 10**

minutes > Apply to Device > Select the trace file to download the log.

Cette partie de la sortie de trace assure une transmission réussie des attributs RADIUS :

```
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
[1] 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
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Guide de l'utilisateur final](#)