

Configuration de l'authentification 802.1X sur les contrôleurs sans fil Catalyst 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration WLC](#)

[Configuration AAA sur les WLC 9800](#)

[Configuration du profil WLAN](#)

[Configuration du profil des politiques](#)

[Configuration des balises des politiques](#)

[Attribution de balise de stratégie](#)

[Configuration ISE](#)

[Déclarer le WLCOnISE](#)

[Créer un nouvel utilisateur sur ISE](#)

[Créer un profil d'autorisation](#)

[Créer un ensemble de stratégies](#)

[Créer une stratégie d'authentification](#)

[Créer une stratégie d'autorisation](#)

[Vérifier](#)

[Dépannage](#)

[Dépannage sur le WLC](#)

[Dépannage sur ISE](#)

Introduction

Ce document décrit comment configurer un WLAN avec la sécurité 802.1X sur un contrôleur sans fil de la gamme Cisco Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 802.1X

Composants utilisés

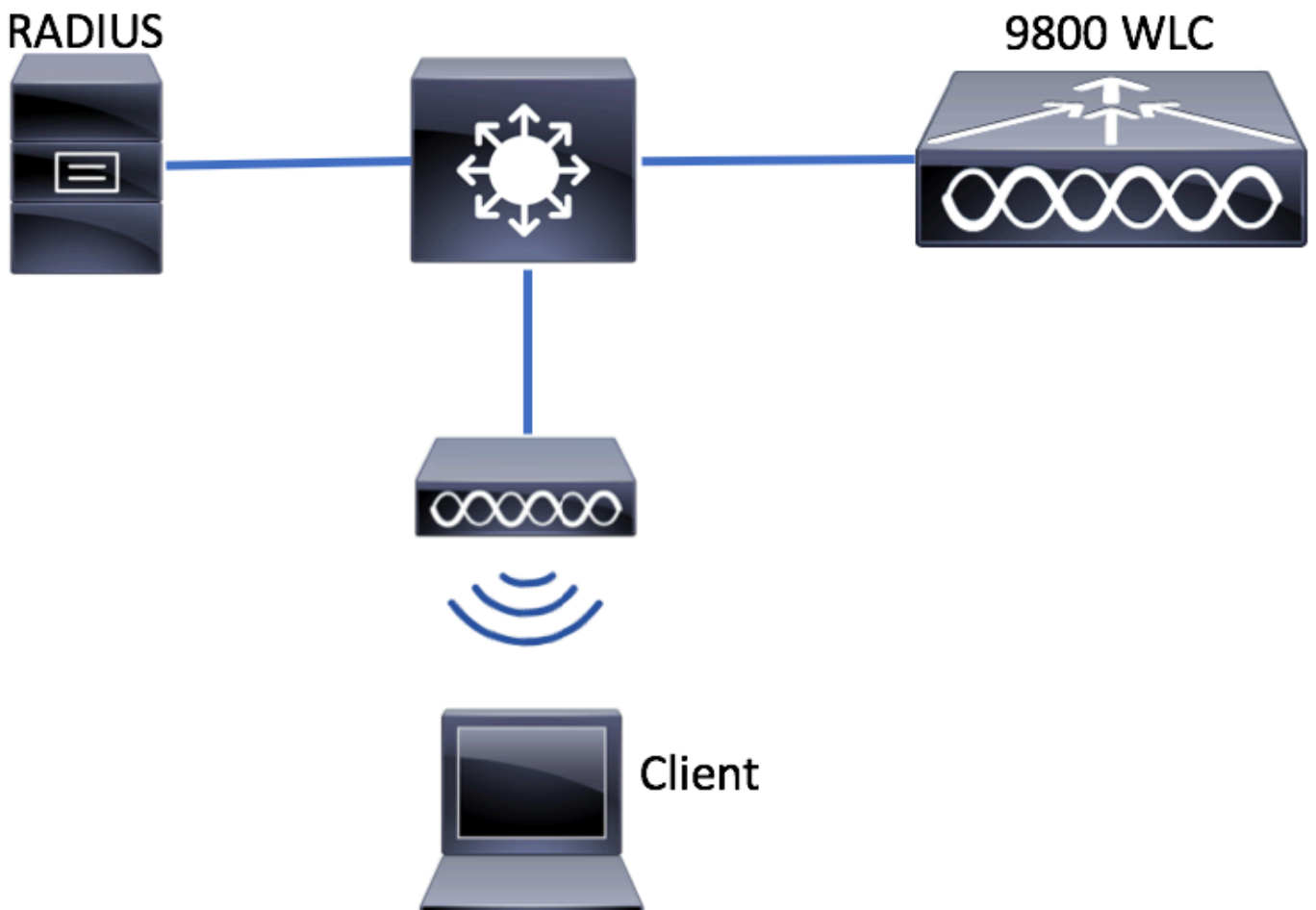
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme de contrôleurs sans fil Catalyst 9800 (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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.

Configurer

Diagramme du réseau

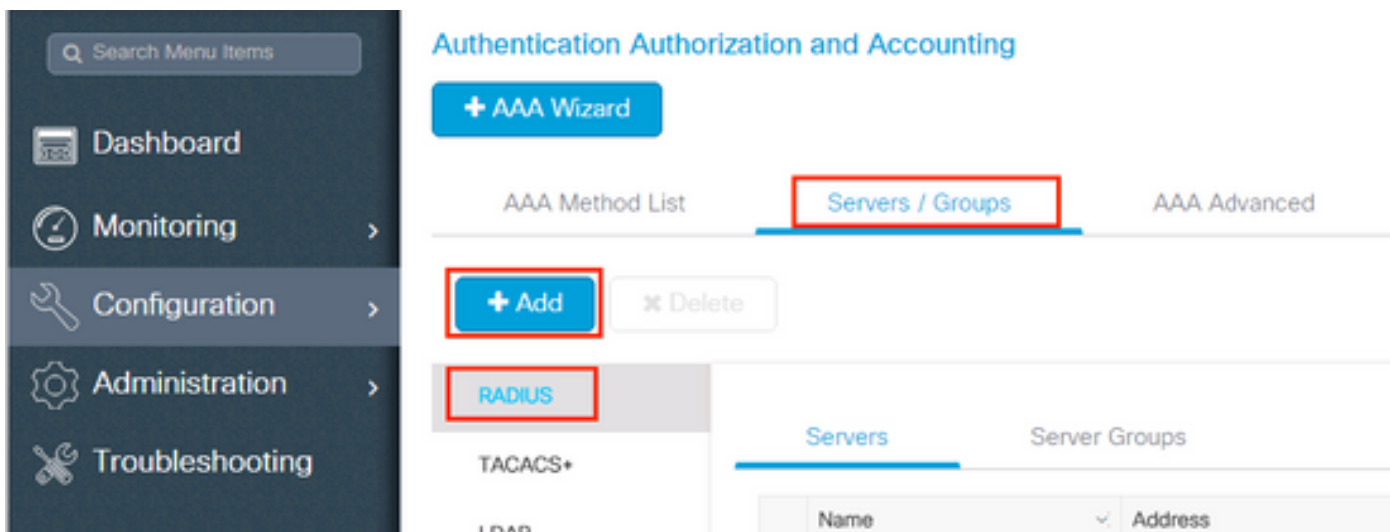


Configuration WLC

Configuration AAA sur les WLC 9800

IUG:

Étape 1. Déclarez le serveur RADIUS. Naviguez jusqu'au serveur RADIUS **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** et saisissez-le.



Assurez-vous que **la prise en charge de CoA** est activée si vous prévoyez d'utiliser l'authentification Web centrale (ou tout type de sécurité nécessitant un changement d'autorisation [CoA]) à l'avenir.

The screenshot shows the 'Create AAA Radius Server' form. It has a dark header bar with the title and a close button. The form contains several input fields and checkboxes. The fields are: Name* (ISE-kcg), IPV4/IPv6 Server Address* (172.16.0.11), Shared Secret* (masked with dots), Confirm Shared Secret* (masked with dots), Auth Port (1812), Acct Port (1813), Server Timeout (seconds) (1-1000), and Retry Count (0-100). There are two checkboxes: 'Clear PAC Key' and 'Set New PAC Key', both unchecked. At the bottom, there is a 'Support for CoA' section with a green 'ENABLED' button. At the very bottom, there are two buttons: 'Cancel' and 'Save & Apply to Device' (highlighted with a red box).

Étape 2. Ajoutez le serveur RADIUS à un groupe RADIUS. Accédez à **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Attribuer un nom à votre groupe et déplacez le serveur que vous avez créé précédemment dans la liste des **Assigned Servers**.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Étape 3. Créez une liste de méthodes d'authentification. Naviguez jusqu'à **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

Authentication Authorization and Accounting

Servers / Groups

General

Authorization

Name

Entrez l'information:

Quick Setup: AAA Authentication

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

CLI :

```
# config t # aaa new-model # radius server <radius-server-name> # address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813 # timeout 300 # retransmit 3
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```


Remarque sur la détection de serveur mort AAA


Après avoir configuré votre serveur RADIUS, vous pouvez vérifier s'il est considéré comme « ACTIF » :

```
#show aaa servers | s WNC D Platform State from WNC D (1) : current UP Platform State from WNC D (2) : current
```

Vous pouvez configurer le **dead criteria**, ainsi que le **deadtime** sur votre WLC, en particulier si vous utilisez plusieurs serveurs RADIUS.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

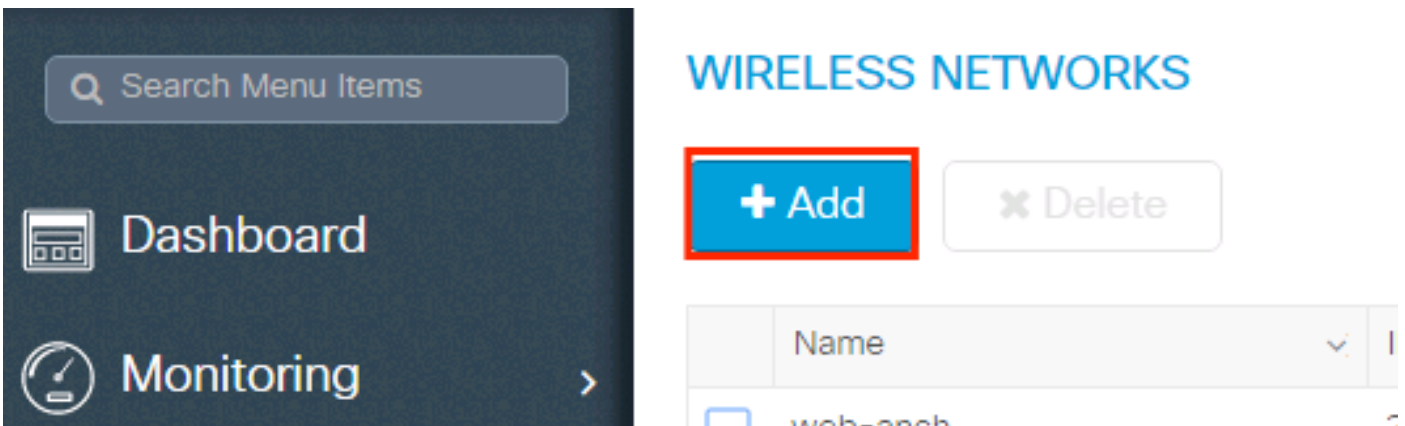
 **Remarque :** le **dead criteria** est le critère utilisé pour marquer un serveur RADIUS comme étant mort. Il se compose de : 1. Un délai d'attente (en secondes) qui représente le temps qui doit s'écouler entre le moment où le contrôleur a reçu pour la dernière fois un paquet valide du serveur RADIUS et le moment où le serveur est marqué comme étant mort. 2. Un compteur, qui représente le nombre de délais d'attente consécutifs qui doivent se produire sur le contrôleur avant que le serveur RADIUS ne soit marqué comme étant mort.

 **Remarque** : la **deadtime** spécifie la durée (en minutes) pendant laquelle le serveur reste à l'état Dead après que le critère Dead l'ait marqué comme étant Dead. Une fois le délai d'attente expiré, le contrôleur marque le serveur comme étant UP (ALIVE) et informe les clients enregistrés du changement d'état. Si le serveur est toujours inaccessible après que l'état a été marqué comme UP et si les critères Dead sont satisfaits, le serveur est marqué de nouveau comme Dead pour l'intervalle de temps d'arrêt.

Configuration du profil WLAN

IUG:

Étape 1. Créez le WLAN. Accédez à **Configuration > Wireless > WLANs > + Add** et configurez le réseau selon les besoins.



Étape 2. Entrez les informations sur le réseau WLAN

Add WLAN ✕

General	Security	Advanced
Profile Name*	<input type="text" value="prof-name"/>	Radio Policy <input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID <input checked="" type="checkbox"/>
WLAN ID*	<input type="text" value="1"/>	
Status	<input checked="" type="checkbox"/>	

Étape 3. Allez à l'onglet Security (sécurité) et sélectionnez la méthode de sécurité requise. Dans ce cas, **WPA2 + 802.1x**.

Add WLAN [Close]

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

Fast Transition Adaptive Enab... ▼

Over the DS

Reassociation Timeout 20

PMF Disabled ▼

WPA Parameters

WPA Policy

[Cancel] [Save & Apply to Device]

Add WLAN [Close]

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]

Étape 4. Dans l' **Security** > **AAA** onglet, sélectionnez la méthode d'authentification créée à l'étape 3 de la section Configuration AAA sur 9800 WLC.

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List list-name

Local EAP Authentication

Cancel Save & Apply to Device

CLI :

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # security dot1x authentication-list <dot1x-list-name> # no shutdown
```

Configuration du profil des politiques

Dans un profil de stratégie, vous pouvez décider à quel VLAN attribuer les clients, entre autres paramètres (comme la liste de contrôle d'accès [ACL], la qualité de service [QoS], l'ancrage de mobilité, les minuteurs, etc.).

Vous pouvez utiliser votre profil de stratégie par défaut ou en créer un nouveau.

IUG:

Accédez à **Configuration > Tags & Profiles > Policy Profile** et configurez votre **default-policy-profile** ou créez-en un nouveau.

Policy Profile

+ Add ✕ Delete

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

1 10 items per page

Assurez-vous que le profil est activé.

En outre, si votre point d'accès (AP) est en mode local, assurez-vous que le profil de stratégie a la **commutation centrale** et l'**authentification centrale** activées.

Edit Policy Profile

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

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	default-policy-profile
Description	default policy profile
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED

CTS Policy

Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy

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

Sélectionnez le VLAN auquel les clients doivent être affectés dans l'onglet **Access Policies**.

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

Search or Select



VLAN

VLAN/VLAN Group

VLAN2602



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



Si vous prévoyez d'avoir des attributs de retour ISE dans l'Access-Accept comme l'attribution de VLAN, veuillez activer le remplacement AAA dans l' **Advanced** onglet :

✕
Edit Policy Profile

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)	<input style="width: 90%;" type="text" value="1800"/>
Idle Timeout (sec)	<input style="width: 90%;" type="text" value="300"/>
Idle Threshold (bytes)	<input style="width: 90%;" type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input style="width: 90%;" type="text" value="60"/>

DHCP

IPv4 DHCP Required	<input checked="" type="checkbox"/>
DHCP Server IP Address	<input style="width: 90%;" type="text"/>

Show more >>>

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input style="width: 90%;" type="text" value="default-aaa-policy x"/>

Fabric Profile	<input type="checkbox"/> <input style="width: 90%;" type="text" value="Search or Select"/>
Umbrella Parameter Map	<input style="width: 90%;" type="text" value="Not Configured"/>
mDNS Service Policy	<input style="width: 90%;" type="text" value="default-mdns-service"/> Clear

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input style="width: 90%;" type="text" value="Search or Select"/>

Air Time Fairness Policies

2.4 GHz Policy	<input style="width: 90%;" type="text" value="Search or Select"/>
5 GHz Policy	<input style="width: 90%;" type="text" value="Search or Select"/>

↶ Cancel

↵
Update & Apply to Device

CLI:

```
# config # wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> # no shutdown
```

Configuration des balises des politiques

La balise de stratégie est utilisée pour lier le SSID au profil de stratégie. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

Remarque : la balise default-policy-tag mappe automatiquement tout SSID avec un ID WLAN compris entre 1 et 16 au profil default-policy-profile. Il ne peut pas être modifié ni supprimé. Si vous disposez d'un WLAN avec l'ID 17 ou supérieur, la balise default-policy-tag ne peut pas être utilisée.

IUG:

Naviguez jusqu'à **Configuration > Tags & Profiles > Tags > Policy** et ajoutez-en un nouveau si nécessaire.

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

1 10 items per page

Liez votre profil de réseau WLAN au profil de politiques souhaité.

Add Policy Tag

Name* PolicyTagName

Description Enter Description

+ Add x Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

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

Map WLAN and Policy

WLAN Profile*

Policy Profile*

✕
✓

↶ Cancel
📄 Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
◀ ◁ 1 ▷ ▶	10 items per page
1 - 1 of 1 items	

↶ Cancel
📄 Save & Apply to Device

CLI :

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

Attribution de balise de stratégie

Affectez la balise de politiques aux points d'accès nécessaires.


IUG:

Pour attribuer la balise à un point d'accès, naviguez jusqu'à **Configuration > Wireless > Access Points > AP Name > General Tags**, attribuer la balise de stratégie appropriée, puis cliquez sur **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration page with the following details:

- General Tab:** AP Name* (AP3802-02-WS), Location* (default location), Base Radio MAC (00:42:68:c6:41:20), Ethernet MAC (00:42:68:a0:d0:22), Admin Status (Enabled), AP Mode (Local), Operation Status (Registered), Fabric Status (Disabled).
- Version:** Primary Software Version (10.0.200.50), Predownloaded Status (N/A), Predownloaded Version (N/A), Next Retry Time (N/A), Boot Version (1.0.0), IOS Version (10.0.200.52), Mini IOS Version (0.0.0.0).
- IP Config:** IP Address (172.16.0.207), Static IP (unchecked).
- Time Statistics:** Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), Controller Association Latency (8 days 21 hrs 50 mins 33 secs).
- Tags:** Policy (default-policy-tag), Site (default-site-tag), RF (default-rf-tag).

Buttons: Cancel (left), Update & Apply to Device (right).

 **Remarque :** sachez que lorsque la balise de stratégie sur un AP est modifiée, elle abandonne son association au WLC 9800 et revient quelques instants plus tard.

Pour attribuer la même balise de stratégie à plusieurs points d'accès, accédez à **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply



Tag APs

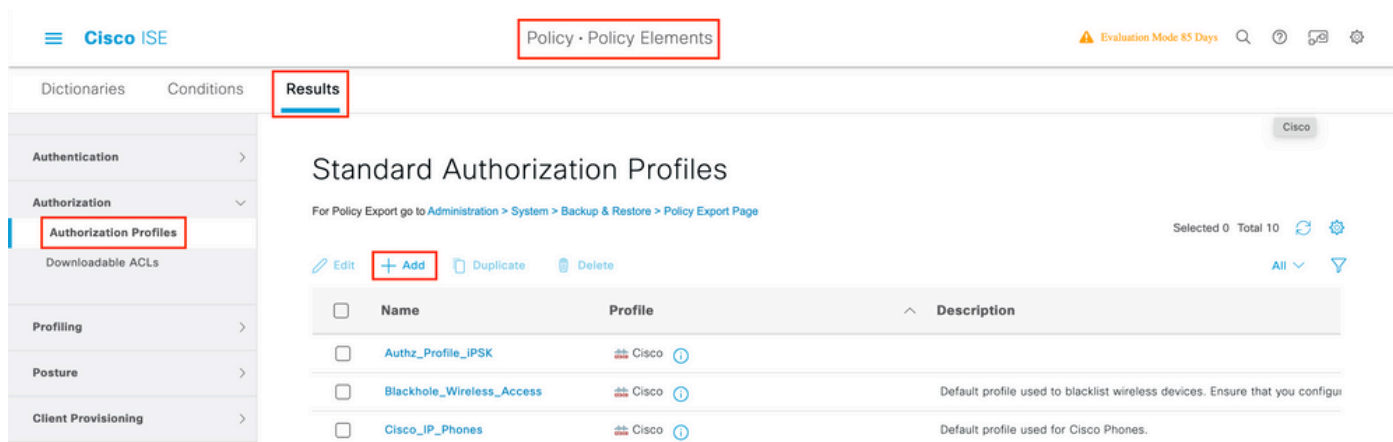


Start Now →

Done

se compose d'un ensemble d'attributs renvoyés lorsqu'une condition est satisfaite. Le profil d'autorisation détermine si le client a accès ou non au réseau, les listes de contrôle d'accès (ACL) push, le remplacement de VLAN ou tout autre paramètre. Le profil d'autorisation présenté dans cet exemple envoie un accord d'accès pour le client et attribue le client au VLAN 1416.

Étape 1. Accédez à **Policy > Policy Elements > Results > Authorization > Authorization Profiles** et cliquez sur le **Add** bouton.



Étape 2. Entrez les valeurs indiquées dans l'image. Ici, nous pouvons retourner des attributs AAA override comme VLAN par exemple. Le WLC 9800 accepte les attributs de tunnel 64, 65, 81 qui utilisent l'ID ou le nom de VLAN, et accepte également l'utilisation de l' **AirSpace-Interface-Name** attribut.

Cisco ISE Policy - Policy Elements Evaluation Mode 85 Days

Dictionarys Conditions Results

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > PermitAccessVlan1416

Authorization Profile

* Name PermitAccessVlan1416

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Security Group

VLAN Tag ID 1 Edit Tag ID/Name 1416

Voice Domain Permission

Advanced Attributes Settings

Select an item

Attributes Details

Access Type = ACCESS_ACCEPT

Tunnel-Private-Group-ID = 1:1416

Tunnel-Type = 1:13

Tunnel-Medium-Type = 1:6

Créer un ensemble de stratégies

Un ensemble de stratégies définit un ensemble de règles d'authentification et d'autorisation. Pour en créer un, accédez à **Policy > Policy Sets**, cliquez sur l'engrenage du premier jeu de stratégies de la liste et sélectionnez **Insert new row above** comme indiqué dans cette image :

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy_Set_IPSK		Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_IPSK	Default Network Access	77	⚙️	➔
✓	Default	Default policy set		Default Network Access			➔

Configurez un nom et créez une condition pour cet ensemble de stratégies. Dans cet exemple, la condition spécifie que nous faisons correspondre le trafic qui provient du WLC :

Radius:NAS-IP-Address EQUALS X.X.X.X // X.X.X.X is the WLC IP address

Assurez-vous que **Default Network Access** est sélectionné sous **Allowed Protocols / Server Sequence**.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy_Set_802.1X		Radius:NAS-IP-Address EQUALS 10.48.38.86	Default Network Access	3	⚙️	➔

Créer une stratégie d'authentification

Pour configurer les stratégies d'authentification et d'autorisation, vous devez entrer la configuration du jeu de stratégies. Cela peut être fait si vous cliquez sur la flèche bleue à droite de la **Policy Set** ligne :

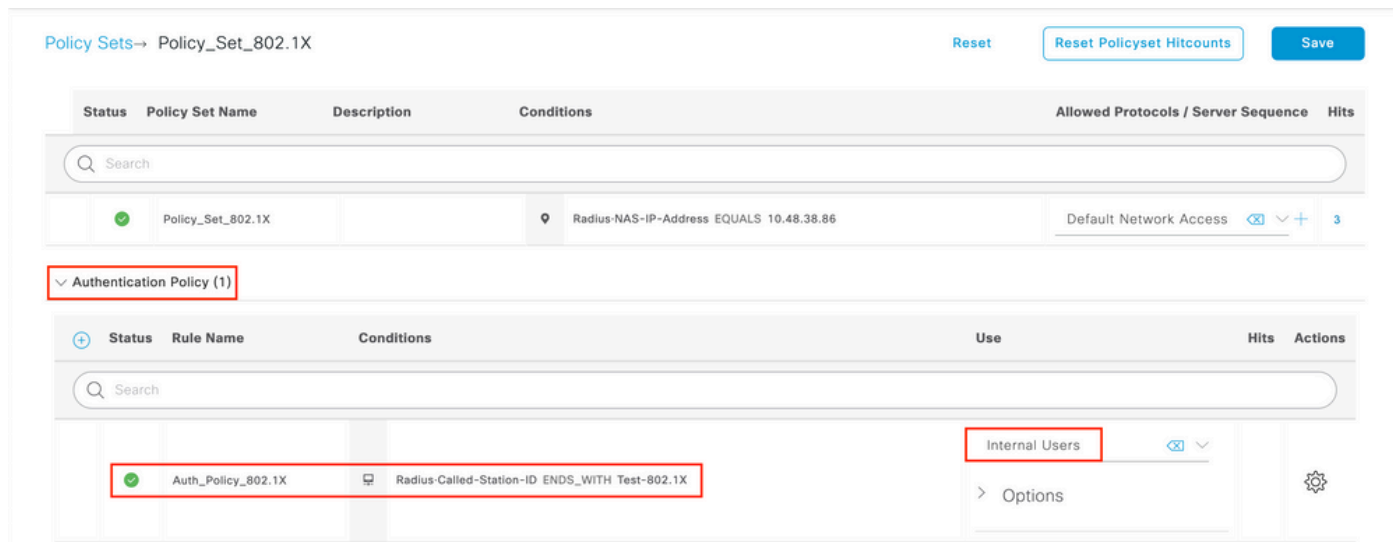
Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy_Set_802.1X		Radius:NAS-IP-Address EQUALS 10.48.38.86	Default Network Access	3	⚙️	➔

Les stratégies d'authentification sont utilisées pour vérifier si les informations d'identification des utilisateurs sont correctes (vérifier si l'utilisateur est réellement celui qu'il dit être). Sous **Authenticaton Policy**, create an Authentication Policy et configurez-la comme indiqué dans cette image. La condition de la stratégie utilisée dans cet exemple est la suivante :

RADIUS:Called-Station-ID ENDS_WITH <SSID> // <SSID> is the SSID of your WLAN

Choisissez également **Internal Users** sous l' **Use** onglet de cette stratégie d'authentification.

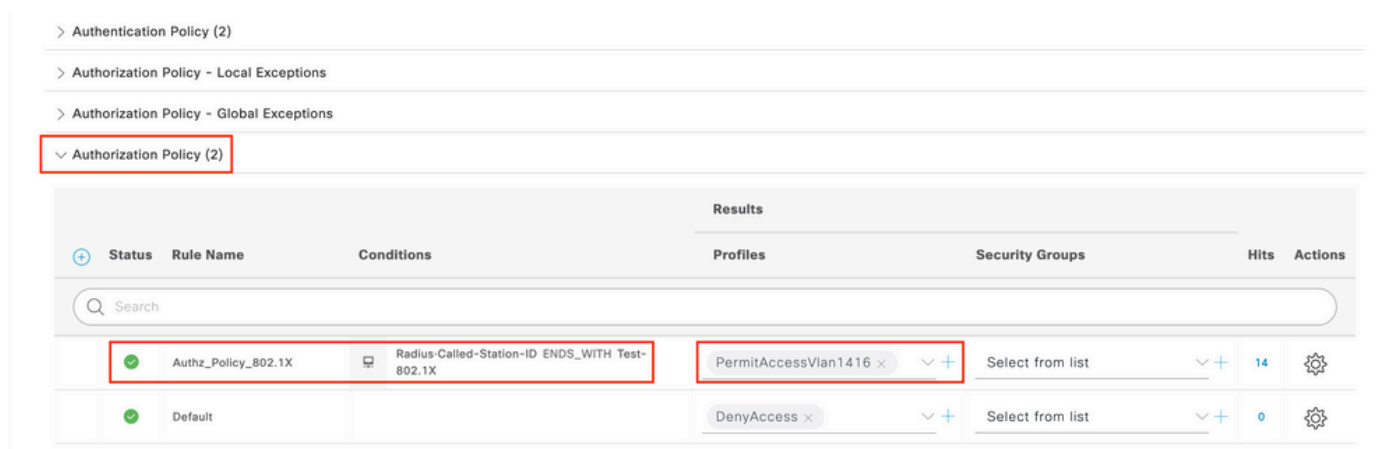


Créer une stratégie d'autorisation

Sur la même page, accédez à **Authorization Policy** et créez-en une nouvelle. La condition de cette stratégie d'autorisation est la suivante :

RADIUS:Called-Station-ID ENDS_WITH <SSID> // <SSID> is the SSID of your WLAN

Sous l' **Result > Profiles** onglet de cette stratégie, sélectionnez la **Authorization Profile** stratégie que vous avez créée précédemment. ISE envoie alors les attributs corrects au WLC si l'utilisateur est authentifié.



À ce stade, toute la configuration pour le WLC et ISE est terminée, vous pouvez maintenant essayer de vous connecter à un client.

Pour plus d'informations sur les stratégies d'autorisation de protocoles ISE, consultez le chapitre : Manage Authentication Policies du Cisco Identity Services Engine Administrator Guide [Manage Authentication Policies](#)

Pour plus d'informations sur les sources d'identité ISE, consultez le chapitre : Manage Users and External Identity Sources du guide Cisco Identity Services Engine Administrator Guide : [Identity Sources](#)

Vérifier

Vous pouvez utiliser ces commandes pour vérifier votre configuration actuelle :

```
# show run wlan // WLAN configuration # show run aaa // AAA configuration (server, server group, methods) # show aaa servers // Configured AAA servers
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name> // Detailed information on given policy profile
```

Dépannage



Remarque : l'utilisation d'équilibreurs de charge externes est correcte. Cependant, assurez-vous que votre équilibreur de charge fonctionne sur une base par client en utilisant l'attribut RADIUS call-station-id. L'utilisation du port source UDP n'est pas un mécanisme pris en charge pour équilibrer les requêtes RADIUS du 9800.

Dépannage sur le WLC

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que toutes les erreurs, avertissements et messages de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit.

Cela dépend du volume de journaux générés, mais généralement, vous pouvez revenir en arrière de quelques heures à plusieurs jours.

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter par SSH/Telnet au WLC 9800 et effectuer ces étapes : (Assurez-vous que vous conservez la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du WLC de sorte que vous puissiez suivre les journaux dans le temps de retour à quand le problème s'est produit.


```
# show clock
```

Étape 2. Collectez les syslog à partir de la mémoire tampon WLC ou du syslog externe, comme dicté par la configuration du système. Cela fournit un aperçu rapide de l'intégrité du système et des erreurs, le cas échéant.

```
# show logging
```

Étape 3. Vérifiez si les conditions de débogage sont activées.

```
# show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Ad
```

 **Remarque :** si une condition est répertoriée, cela signifie que les traces sont consignées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmente le volume des journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque vous ne procédez pas activement au débogage.

Étape 4. Supposons que l'adresse MAC testée n'était pas répertoriée comme condition à l'étape 3, collectez les traces de niveau de notification toujours actif pour l'adresse MAC spécifique :

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe:

```
# more bootflash:always-on-<FILENAME.txt>
```

or

```
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Débogage conditionnel et traçage Radio Active

Si les traces toujours actives ne vous donnent pas suffisamment d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui fournit des traces au niveau du débogage pour tous les processus qui interagissent avec la condition spécifiée (l'adresse MAC du client dans ce cas). Vous pouvez le faire via l'interface utilisateur graphique ou l'interface de ligne de commande.

CLI :

Pour activer le débogage conditionnel, procédez comme suit :

Étape 5. Assurez-vous qu'aucune condition de débogage n'est activée.

```
# clear platform condition all
```

Étape 6. Activez la condition de débogage pour l'adresse MAC du client sans fil que vous souhaitez surveiller.

Cette commande commence à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez éventuellement augmenter ce délai jusqu'à 2085978494 secondes.

```
# debug wireless mac <aaaa.bbbb.cccc> { monitor-time <seconds> }
```



Remarque : Afin de surveiller plusieurs clients à la fois, exécutez la <aaaa.bbbb.cccc>commande de débogage sans fil mac par adresse MAC.



Remarque : vous ne voyez pas le résultat de l'activité du client sur une session de terminal, car tout est mis en mémoire tampon en interne pour être visualisé ultérieurement.

Étape 7. Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 8. Arrêtez les débogages si le problème est reproduit avant l'expiration du temps de surveillance par défaut ou configuré.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Une fois que le temps de surveillance s'est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 9. Recueillir le fichier de l'activité de l'adresse MAC. Vous pouvez copier le fichier ra trace.log sur un serveur externe ou afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA:

```
# dir bootflash: | inc ra_trace
```

Copiez le fichier sur un serveur externe :


```
# copy bootflash:ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

Affichez-en le contenu :

```
# more bootflash:ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 10. Si la cause première n'est toujours pas évidente, collectez les journaux internes, qui sont une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client car nous examinons plus en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.


```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

 **Remarque** : cette sortie de commande retourne des traces pour tous les niveaux de log pour tous les processus et est assez volumineuse. Veuillez faire appel à Cisco TAC pour faciliter l'analyse de ces suivis.

Vous pouvez soit copier le fichier ra-internal-FILENAME.txt sur un serveur externe, soit afficher le résultat directement à l'écran.

Copiez le fichier sur un serveur externe :


```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Affichez-en le contenu :

```
# more bootflash:ra-internal-<FILENAME>.txt
```

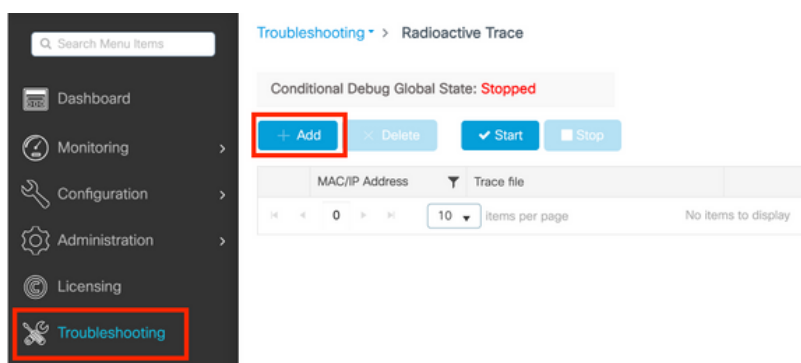
Étape 11. Supprimez les conditions de débogage.

```
# clear platform condition all
```

 **Remarque** : veillez à toujours supprimer les conditions de débogage après une session de dépannage.

IUG:

Étape 1. Accédez à **Troubleshooting > Radioactive Trace > + Add** et spécifiez l'adresse MAC/IP du ou des clients que vous souhaitez dépanner.



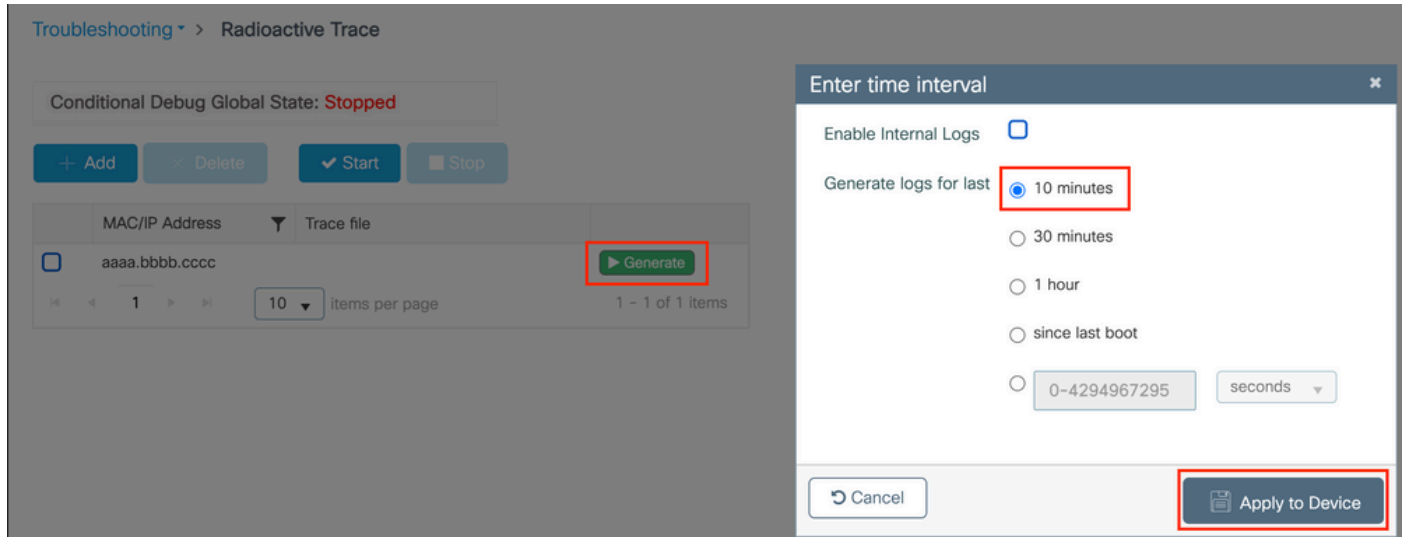
The screenshot shows the Cisco IUG interface for configuring Radioactive Trace. On the left, a navigation menu is visible with 'Troubleshooting' highlighted. The main content area shows the 'Radioactive Trace' configuration page. At the top, the 'Conditional Debug Global State' is 'Stopped'. Below this, there are four buttons: '+ Add', 'Delete', 'Start', and 'Stop'. The '+ Add' button is highlighted with a red box. Below the buttons is a table with columns for 'MAC/IP Address' and 'Trace file'. The table is currently empty, showing '0' items per page and 'No items to display'.

Étape 2. Cliquez sur **Démarrer**.

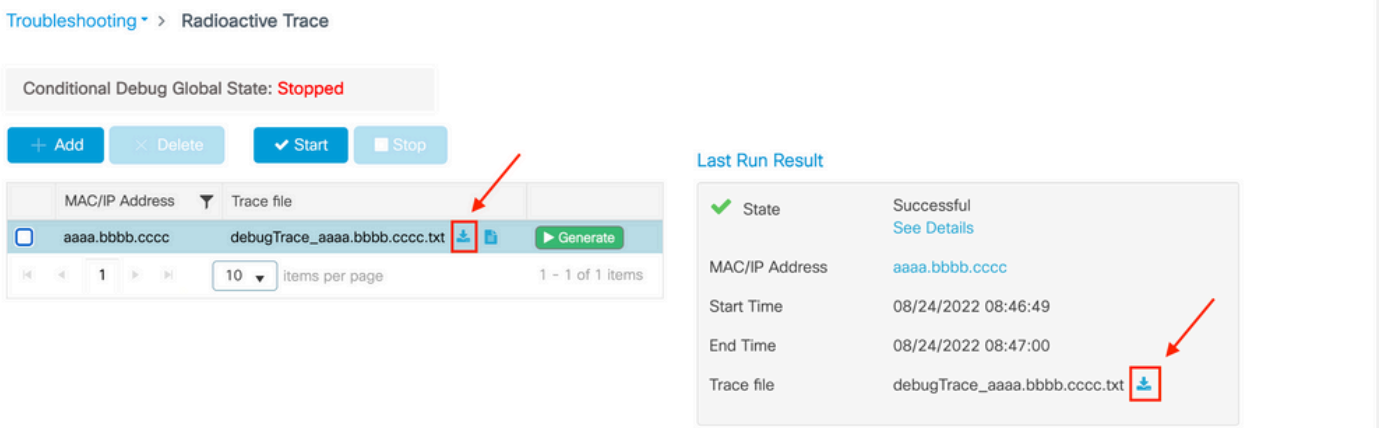
Étape 3. Reproduisez le problème.

Étape 4. Cliquez sur **Stop**.

Étape 5. Cliquez sur le **Generate** bouton, sélectionnez l'intervalle de temps pour lequel vous souhaitez obtenir les journaux, puis cliquez sur **Apply to Device**. In this example, the logs for the last 10 minutes are requested.



Étape 6. Téléchargez le logiciel Radioactive Trace sur votre ordinateur, cliquez sur le bouton de téléchargement et inspectez-le.



Dépannage sur ISE

Si vous rencontrez des problèmes avec l'authentification du client, vous pouvez vérifier les journaux sur le serveur ISE. Accédez à **Operations > RADIUS > Live Logs** et vous voyez la liste des demandes d'authentification, ainsi que le jeu de stratégies qui a été mis en correspondance, le résultat de chaque demande, etc. Vous pouvez obtenir plus de détails en cliquant sur la loupe sous l' **Details** onglet de chaque ligne, comme le montre l'image :

Live Logs

Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0



Client Stopped Responding 2

Repeat Counter 0

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Refresh | Reset Repeat Counts | Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Netwo
Aug 23, 2022 06:18:42.5...	●		0	user1	08:BE:AC:27:85:...	Unknown	Policy_Set...	Policy_Set...	PermitAcc...	10.14.16.112,...	
Aug 23, 2022 09:45:48.1...	●			user1	BC:D0:74:2B:6D:...						9800-W

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.