

# Configuration du demandeur 802.1X pour les points d'accès avec le contrôleur 9800

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer le LAP en tant que demandeur 802.1x](#)

[Si L'AP Est Déjà Joint Au WLC :](#)

[Si L'AP N'A Pas Encore Rejoint Un WLC :](#)

[Configuration du commutateur](#)

[Configuration du serveur ISE](#)

[Vérifier](#)

[Vérification du type d'authentification](#)

[Vérification de la norme 802.1x sur le port de commutateur](#)

[Dépannage](#)

[Références](#)

---

## Introduction

Ce document décrit comment configurer un point d'accès (AP) Cisco en tant que demandeur 802.1x pour être autorisé sur un port de commutateur par rapport à un serveur RADIUS.

## Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur LAN sans fil (WLC) et LAP (Lightweight Access Point).
- 802.1x sur les commutateurs Cisco et ISE
- Protocole EAP (Extensible Authentication Protocol)
- Remote Authentication Dial-In User Service (RADIUS)

## Composants utilisés

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

- WS-C3560CX, Cisco IOS® XE, 15.2(3r)E2
- C9800-CL-K9, Cisco IOS® XE, 17.6.5
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

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

Dans cette configuration, le point d'accès agit comme demandeur 802.1x et est authentifié par le commutateur par rapport à l'ISE avec la méthode EAP EAP-FAST.

Une fois le port configuré pour l'authentification 802.1X, le commutateur n'autorise aucun trafic autre que le trafic 802.1X à traverser le port tant que le périphérique connecté au port ne s'authentifie pas correctement.

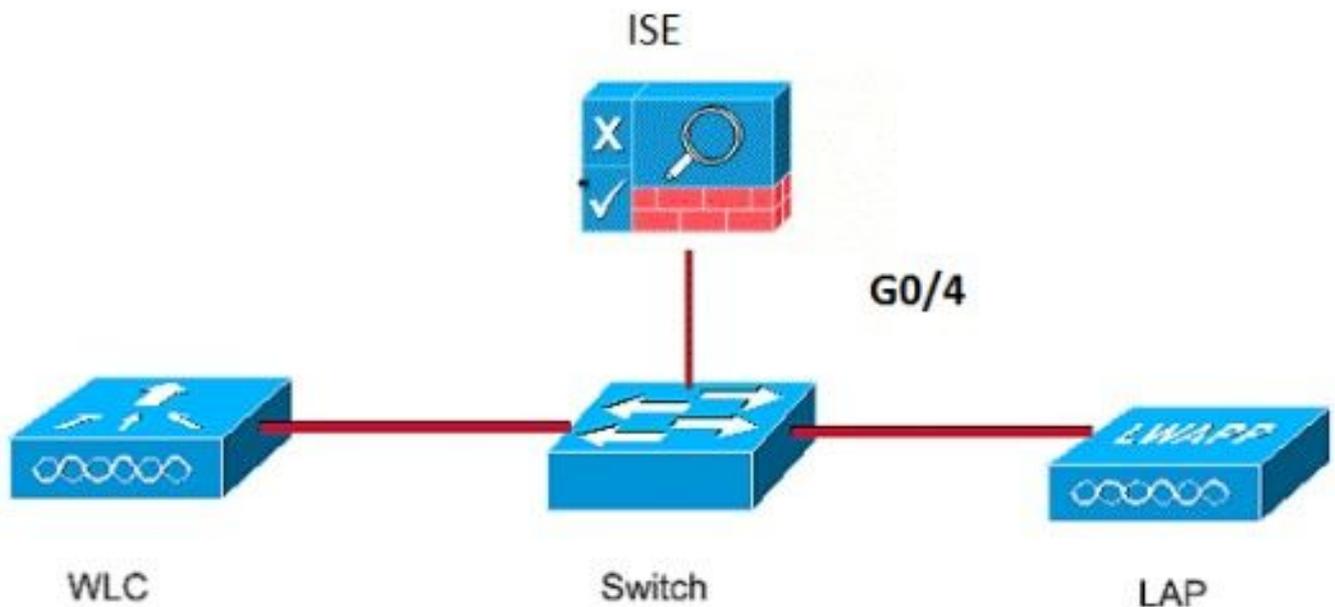
Un point d'accès peut être authentifié avant de rejoindre un WLC ou après qu'il ait rejoint un WLC, auquel cas, configurez 802.1X sur le commutateur après que le LAP ait rejoint le WLC.

## Configurer

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

### Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurer le LAP en tant que demandeur 802.1x

Si L'AP Est Déjà Joint Au WLC :

Configurez le type d'authentification 802.1x et le type d'authentification LSC (Locally Significant Certificate) AP :

Étape 1. Naviguez jusqu'à Configuration > Tags & Profiles > AP Join > Sur la page AP Join Profile, cliquez sur Add pour ajouter un nouveau profil de jointure ou modifier un profil de jointure AP lorsque vous cliquez sur son nom.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > AP Join. There are '+ Add' and 'x Delete' buttons. A table lists AP Join Profile Names and their descriptions:

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing '1' items per page.

Étape 2. Sur la page AP Join Profile, dans AP > General, naviguez jusqu'à la section AP EAP Auth Configuration. Dans la liste déroulante EAP Type, choisissez le type EAP comme EAP-FAST, EAP-TLS ou EAP-PEAP pour configurer le type d'authentification dot1x. EAP-FAST est le

seul type d'authentification qui utilise uniquement des noms d'utilisateur et des mots de passe et qui est le plus facile à configurer. PEAP et EAP-TLS nécessitent que vous mettiez en service des certificats sur les points d'accès via le workflow LSC (voir la section des références).

**Edit AP Join Profile**

General Client CAPWAP **AP** Management Security ICap QoS

**General** Hyperlocation Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type Unknown

Injector Switch MAC 00:00:00:00:00:00

**AP EAP Auth Configuration**

EAP Type EAP-FAST

AP Authorization Type EAP-FAST

EAP-TLS

EAP-PEAP

**Client Statistics Reporting Interval**

5 GHz (sec) 90

2.4 GHz (sec) 90

**Extended Module**

Enable

**Mesh**

Profile Name mesh-profile [Clear](#)

Cancel Update & Apply to Device

Étape 3. Dans la liste déroulante AP Authorization Type, choisissez le type comme CAPWAP DTLS + ou CAPWAP DTLS > Cliquez sur Update & Apply to Device.

**Edit AP Join Profile** ✕

General Client CAPWAP **AP** Management Security ICap QoS

**General** Hyperlocation Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

**AP EAP Auth Configuration**

EAP Type

AP Authorization Type 

- CAPWAP DTLS
- CAPWAP DTLS + DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

**Client Statistics Reporting Interval**

5 GHz (sec)

2.4 GHz (sec)

**Extended Module**

Enable

**Mesh**

Profile Name  [Clear](#)

Configurez le nom d'utilisateur et le mot de passe 802.1x :

Étape 1. Dans Management > Credentials > Enter Dot1x username and password details > Choisissez le type de mot de passe 802.1x approprié > Cliquez sur Update & Apply to Device

Edit AP Join Profile ✕

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

**Dot1x Credentials**

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

Si L'AP N'A Pas Encore Rejoint Un WLC :

Accédez au LAP par la console afin de définir les informations d'identification et d'utiliser ces commandes CLI : (pour Cheetah OS et Cisco IOS® AP)

CLI :

```
<#root>
```

```
LAP#
```

```
debug capwap console cli
```

```
LAP#
```

```
capwap ap dot1x username <username> password <password>
```

Pour Effacer Les Identifiants Dot1x Sur Le Point D'Accès (Si Nécessaire)

Pour les AP Cisco IOS®, après cela rechargez l'AP :

CLI :

```
<#root>
```

```
LAP#
```

```
clear capwap ap dot1x
```

Pour les points d'accès Cisco COS, après cela rechargez le point d'accès :

CLI :

```
<#root>
```

```
LAP#
```

```
capwap ap dot1x disable
```

## Configuration du commutateur

Activez dot1x sur le commutateur globalement et ajoutez le serveur ISE au commutateur.

CLI :

```
<#root>
```

```
Enable
```

```
Configure terminal
```

```
aaa new-model
```

```
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
```

```
dot1x system-auth-control
```

```
Radius-server host <ISE IP address> auth-port <port> acct-port <port>  
key 7 <server key>
```

Configurez le port du commutateur AP.

CLI :

```
<#root>
```

```
configure terminal
```

```
interface GigabitEthernet</>  
switchport access vlan <>  
switchport mode access  
authentication order dot1x  
authentication port-control auto  
dot1x pae authenticator  
spanning-tree portfast edge
```

```
end
```

Si le point d'accès est en mode Flex Connect, commutation locale, alors une configuration supplémentaire doit être faite sur l'interface du commutateur pour permettre plusieurs adresses MAC sur le port, puisque le trafic client est libéré au niveau du point d'accès :

```
<#root>
```

```
authentication host-mode multi-host
```

Note : Signifie que le lecteur prend note. Les notes contiennent des suggestions utiles ou des références à des éléments non traités dans le document.

---

 Remarque : le mode multi-hôte authentifie la première adresse MAC, puis autorise un nombre illimité d'autres adresses MAC. Activez le mode hôte sur les ports du commutateur si le point d'accès connecté a été configuré avec le mode de commutation local. Il permet au trafic du client de passer par le port de commutation. Si vous voulez un chemin de trafic sécurisé, activez dot1x sur le WLAN pour protéger les données du client

---

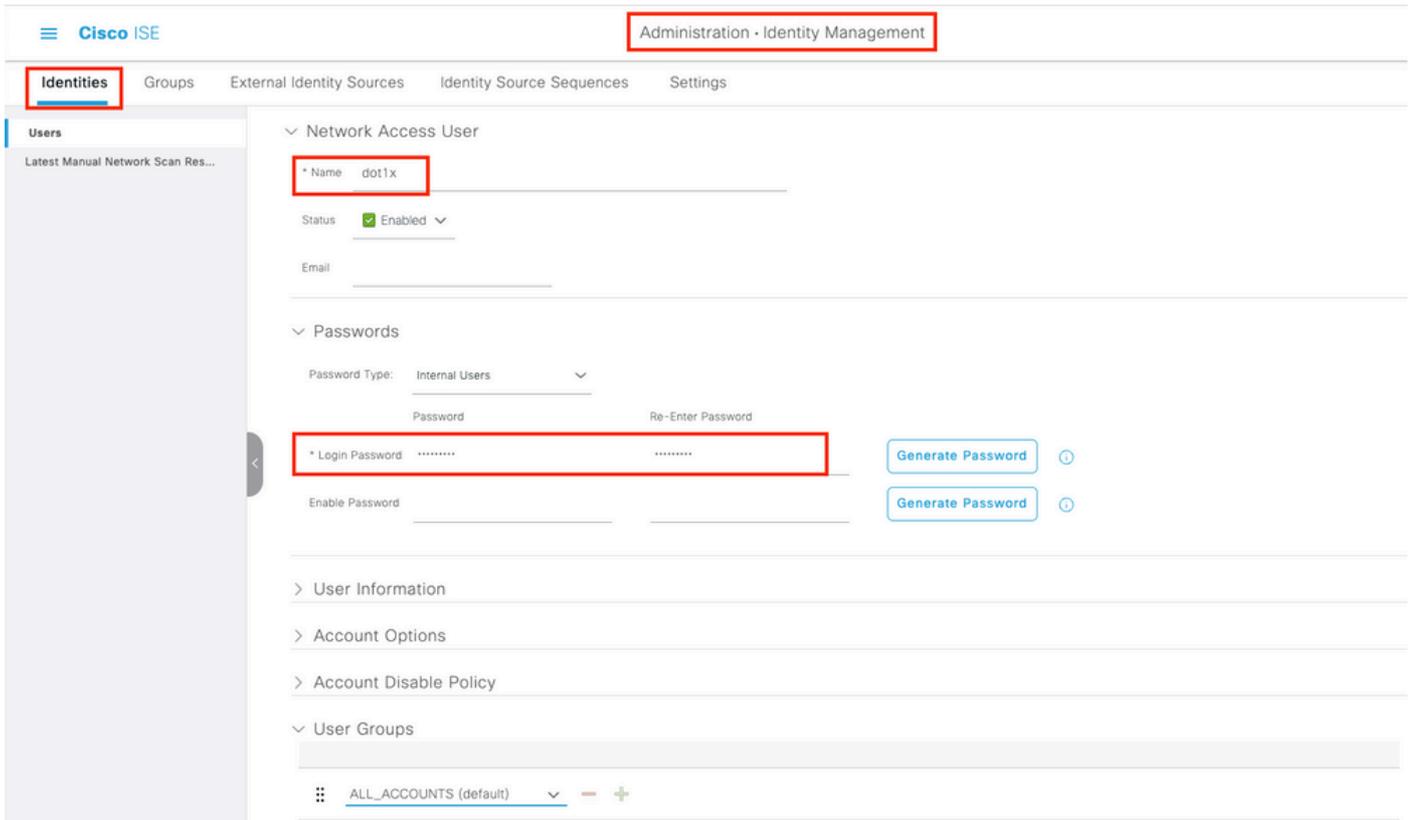
## Configuration du serveur ISE

Étape 1. Ajoutez le commutateur comme périphérique réseau sur le serveur ISE. Accédez à Administration > Network Resources > Network Devices > Cliquez sur Add > Enter Device name, IP address, activez RADIUS Authentication Settings, Specify Shared Secret Value, COA port (ou laissez-le par défaut) > Submit.

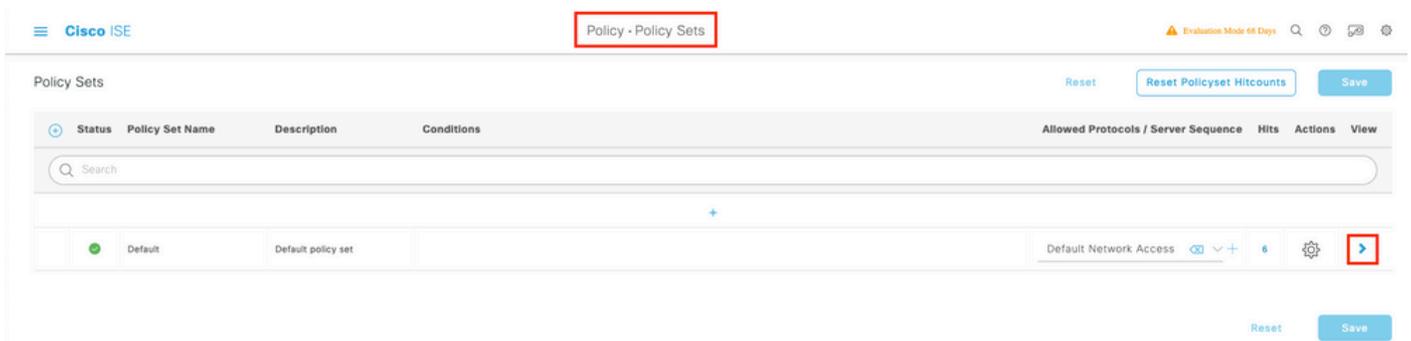
The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration - Network Resources'. The main navigation menu on the left has 'Network Devices' highlighted. The breadcrumb trail is 'Network Devices List > New Network Device'. The configuration page is titled 'Network Devices' and contains the following fields:

- Name: MySwitch
- Description: (empty)
- IP Address: 10.48.39.100 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: All Locations (with 'Set To Default' button)
- IPSEC: Is IPSEC Device (with 'Set To Default' button)
- Device Type: All Device Types (with 'Set To Default' button)
- RADIUS Authentication Settings** (highlighted with a red box):
  - Protocol: RADIUS
  - Shared Secret: (masked) (with 'Show' button)
  - Use Second Shared Secret: (checkbox) (with 'Show' button)
  - CoA Port: 1700 (with 'Set To Default' button)
  - RADIUS DTLS Settings: (link)
  - DTLS Required: (checkbox)
  - Shared Secret: radius/dtls (with 'Show' button)

Étape 2. Ajoutez les informations d'identification AP à ISE. Accédez à Administration > Identity Management > Identities > Users et cliquez sur le bouton Add pour ajouter un utilisateur. Entrez les informations d'identification que vous avez configurées sur votre profil de connexion AP sur votre WLC. Notez que l'utilisateur est placé dans le groupe par défaut ici, mais cela peut être ajusté selon vos besoins.



Étape 3. Sur ISE, configurez la stratégie d'authentification et la stratégie d'autorisation. Accédez à Policy > Policy Sets et sélectionnez le jeu de stratégie à configurer et la flèche bleue sur la droite. Dans ce cas, le jeu de stratégies par défaut est utilisé, mais il est possible de le personnaliser selon les besoins.



Configurez ensuite la stratégie d'authentification et la stratégie d'autorisation. Les politiques indiquées ici sont les politiques par défaut créées sur le serveur ISE, mais elles peuvent être adaptées et personnalisées selon vos besoins.

Dans cet exemple, la configuration peut être traduite en : "Si le 802.1X câblé est utilisé et que l'utilisateur est connu sur le serveur ISE, alors nous autorisons l'accès aux utilisateurs pour lesquels l'authentification a réussi". Le point d'accès est alors autorisé sur le serveur ISE.

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	⚙️
●	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy (12)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x Select from list			6	⚙️
●	Default		DenyAccess x Select from list			0	⚙️

Étape 4. Assurez-vous que dans les protocoles autorisés par l'accès réseau par défaut, EAP-FAST est autorisé. Accédez à Policy > Policy Elements > Authentication > Results > Allowed Protocols > Default Network Access > Enable EAP-TLS > Save.

Cisco ISE Policy · Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

- Process Host Lookup

Authentication Protocols

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1
- Allow MS-CHAPv2
- Allow EAP-MD5
- Allow EAP-TLS

Expand Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after: 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

## Vérifier

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

## Vérification du type d'authentification

La commande show affiche les informations d'authentification d'un profil AP :

CLI :

```
9800WLC#show ap profile name <profile-name> detailed
```

Exemple :

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE   : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

## Vérification de la norme 802.1x sur le port de commutateur

La commande show affiche l'état d'authentification 802.1x sur le port du commutateur :

CLI :

```
Switch# show dot1x all
```

Exemple de résultat :

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout          = 0
SuppTimeout            = 30
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
```

Vérifiez si le port a été authentifié ou non

CLI :

```
Switch#show dot1x interface <AP switch port number> details
```

Exemple de résultat :

```
Dot1x Info for GigabitEthernet0/8
```

```
-----  
PAE = AUTHENTICATOR  
QuietPeriod = 60  
ServerTimeout = 0  
SuppTimeout = 30  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30
```

```
Dot1x Authenticator Client List
```

```
-----  
EAP Method = FAST  
Supplicant = f4db.e67e.dd16  
Session ID = 0A30279E00000BB7411A6BC4  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE  
ED  
Auth BEND SM State = IDLE
```

À partir de CLI :

```
Switch#show authentication sessions
```

Exemple de résultat :

Interface	MAC Address	Method	Domain	Status	Fg	Session ID
Gi0/8	f4db.e67e.dd16	dot1x	DATA	Auth		0A30279E00000BB7411A6BC4

Dans ISE, choisissez Operations > Radius Livelogs et vérifiez que l'authentification est réussie et que le profil d'autorisation correct est activé.

Cisco ISE Operations - RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 1 Client Stopped Responding 0 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...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	✓	🔍		dot1x	A4-53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	Authorization Profiles	IP Address	Network Devi...	FastEther...
Nov 28, 2022 08:33:34.4...	✓	🔍		dot1x	A4-53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess		nschym-SW-...	FastEther...

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. Entrez la commande ping afin de vérifier si le serveur ISE est accessible depuis le commutateur.
2. Assurez-vous que le commutateur est configuré en tant que client AAA sur le serveur ISE.
3. Assurez-vous que le secret partagé est le même entre le commutateur et le serveur ISE.
4. Vérifiez si EAP-FAST est activé sur le serveur ISE.
5. Vérifiez si les informations d'identification 802.1x sont configurées pour le LAP et sont identiques sur le serveur ISE.

Remarque : le nom d'utilisateur et le mot de passe sont sensibles à la casse.

6. Si l'authentification échoue, entrez ces commandes sur le commutateur : debug dot1x et debug authentication.

Notez que les points d'accès basés sur Cisco IOS (802.11ac phase 1) ne prennent pas en charge TLS versions 1.1 et 1.2. Cela peut entraîner un problème si votre serveur ISE ou RADIUS est configuré pour autoriser uniquement l'authentification TLS 1.2 à l'intérieur de 802.1X.

## Références

[Configuration de 802.1X sur les points d'accès avec PEAP et EAP-TLS](#)

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.