Configurer le point d'accès léger comme demandeur 802.1x

Introduction

Ce document décrit comment configurer un point d'accès léger (LAP) en tant que demandeur 802.1x afin de s'authentifier auprès du serveur Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur LAN sans fil (WLC) et LAP
- 802.1x sur les commutateurs Cisco
- ISE
- Protocole EAP (Extensible Authentication Protocol) - Authentification flexible via FAST (Secure Tunneling)

Composants utilisés

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

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE 2.0

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

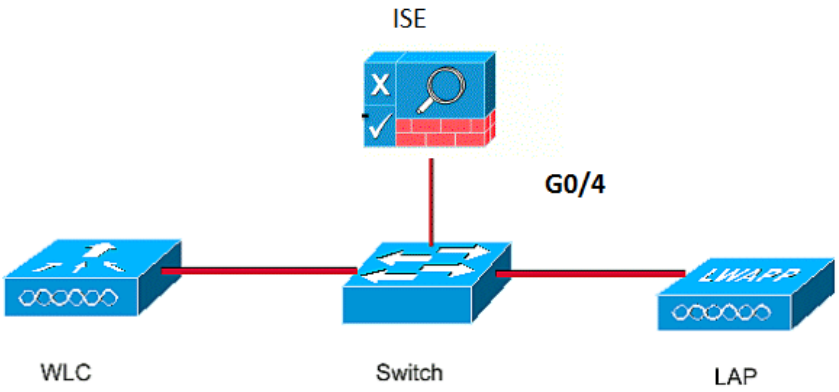
Dans cette configuration, le point d'accès (AP) agit en tant que demandeur 802.1x et est authentifié par le commutateur par rapport à l'ISE qui utilise EAP-FAST avec la mise en service anonyme des informations d'identification d'accès protégé (PAC). Une fois le port configuré pour l'authentification 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 soit avant qu'il ne rejoigne un WLC, soit après qu'il ait rejoint un WLC, auquel cas vous configurez 802.1x sur le commutateur après que le LAP ait rejoint le WLC.

Configurer

Dans cette section, vous trouverez les informations nécessaires à la configuration des fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

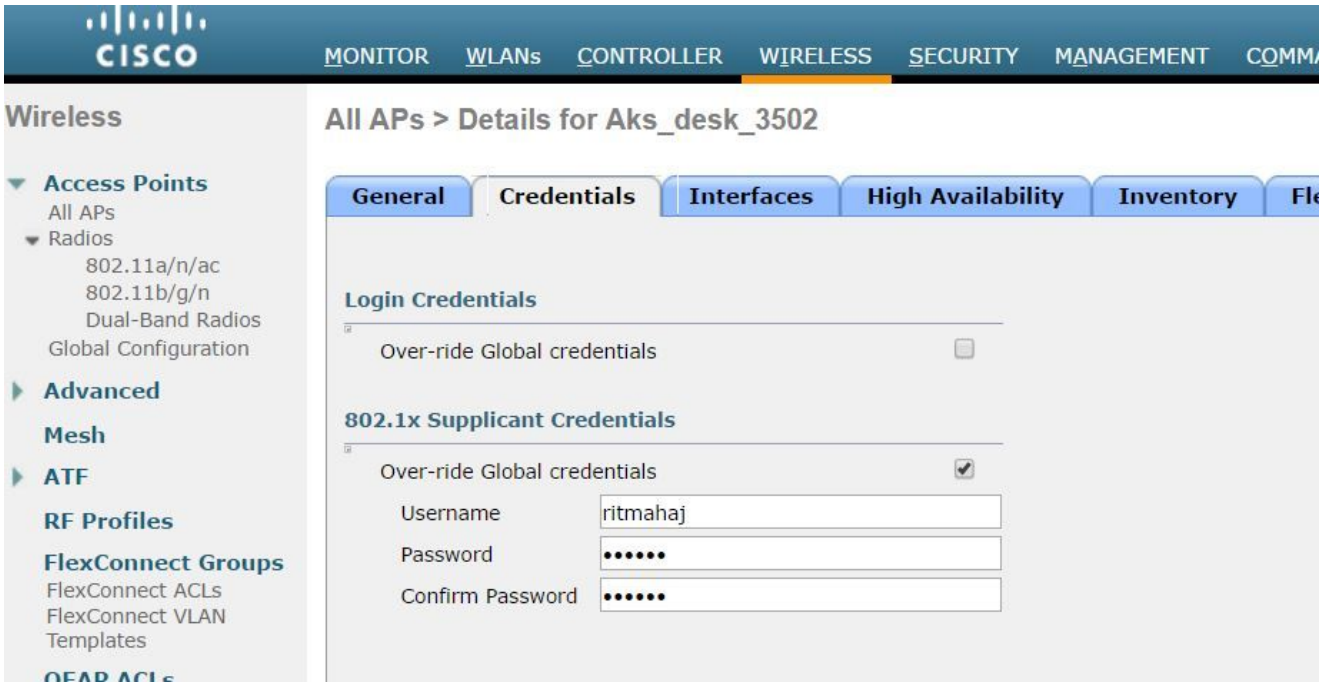
Ce document utilise ces adresses IP :

- L'adresse IP du commutateur est 10.48.39.141
- L'adresse IP du serveur ISE est 10.48.39.161
- L'adresse IP du WLC est 10.48.39.142

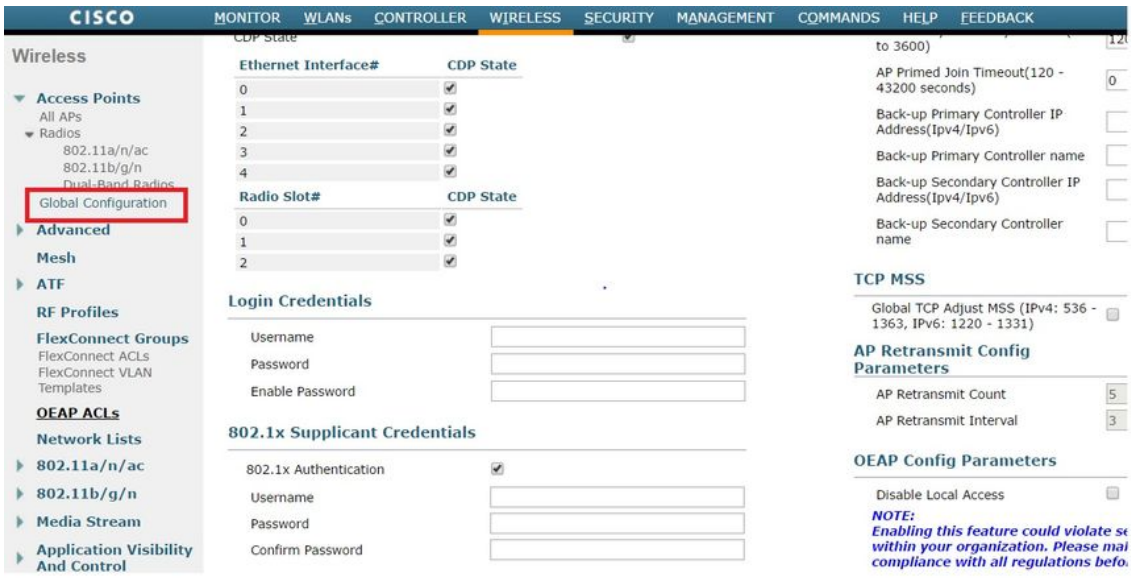
Configuration du LAP

Dans cette section, les informations vous sont présentées pour configurer le LAP en tant que demandeur 802.1x.

1. Si l'AP est déjà joint au WLC, allez dans l'onglet Wireless et cliquez sur l'AP, allez dans le champ Credentials et sous l'en-tête 802.1x Supplicant Credentials, cochez la case Override Global credentials afin de définir le nom d'utilisateur et le mot de passe 802.1x pour cet AP.



Vous pouvez également définir un nom d'utilisateur et un mot de passe communs pour tous les AP qui sont joints au WLC avec le menu de configuration globale.



2. Si l'AP n'a pas encore rejoint un WLC, vous devez vous connecter au LAP en mode console afin de définir les informations d'identification et d'utiliser ces commandes CLI :
<#root>

LAP#

debug capwap console cli

LAP#

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

Configuration du commutateur

1. Activez dot1x sur le commutateur globalement et ajoutez le serveur ISE au commutateur.
   <#root>

```
aaa new-model

!

aaa authentication dot1x default group radius

!

dot1x system-auth-control

!

radius server ISE

address ipv4 10.48.39.161 auth-port 1645 acct-port 1646

  key 7 123A0C0411045D5679
```

2. À présent, configurez le port du commutateur AP.
   <#root>

```
interface GigabitEthernet0/4

switchport access vlan 231

switchport mode access

authentication order dot1x

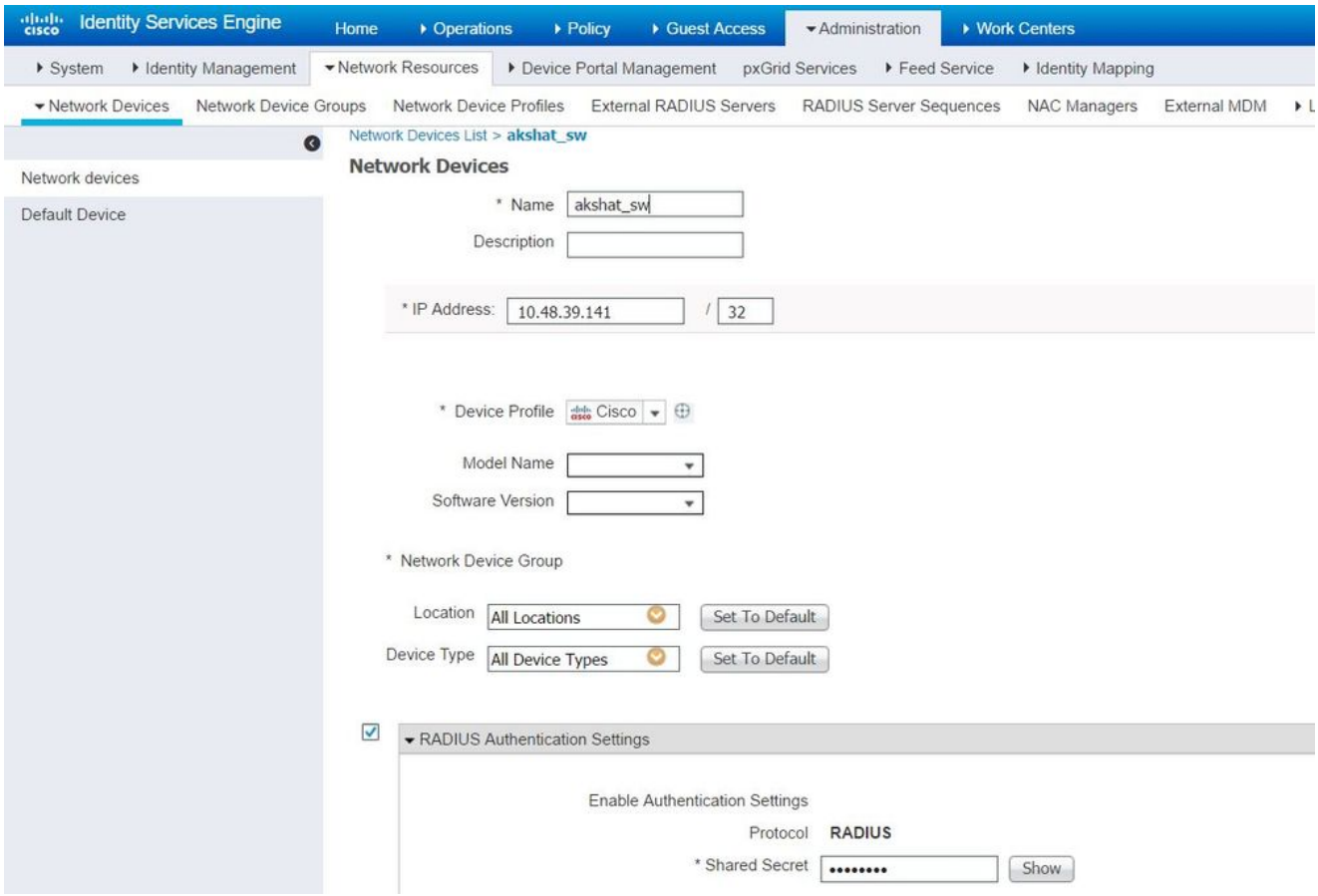
authentication port-control auto
```

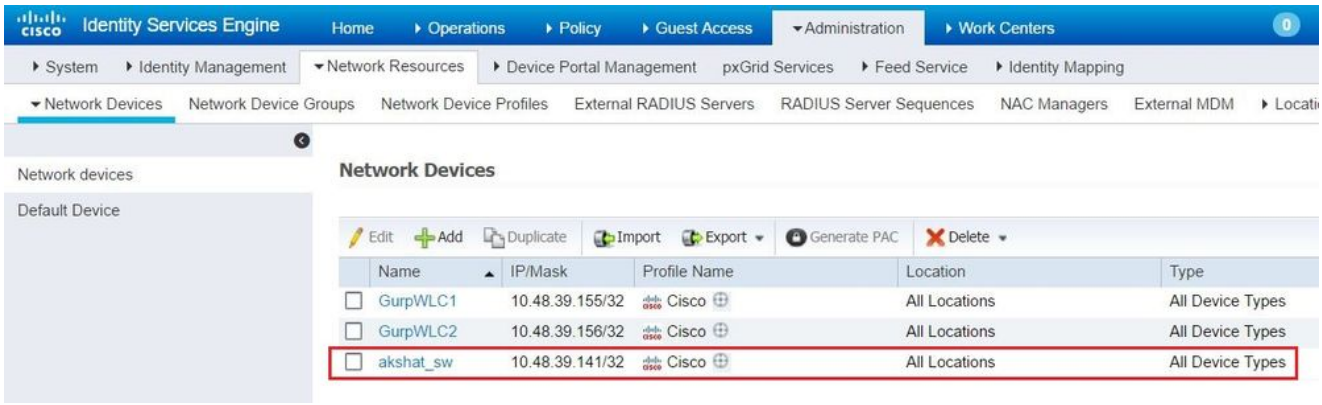
```
dot1x pae authenticator

spanning-tree portfast edge
```

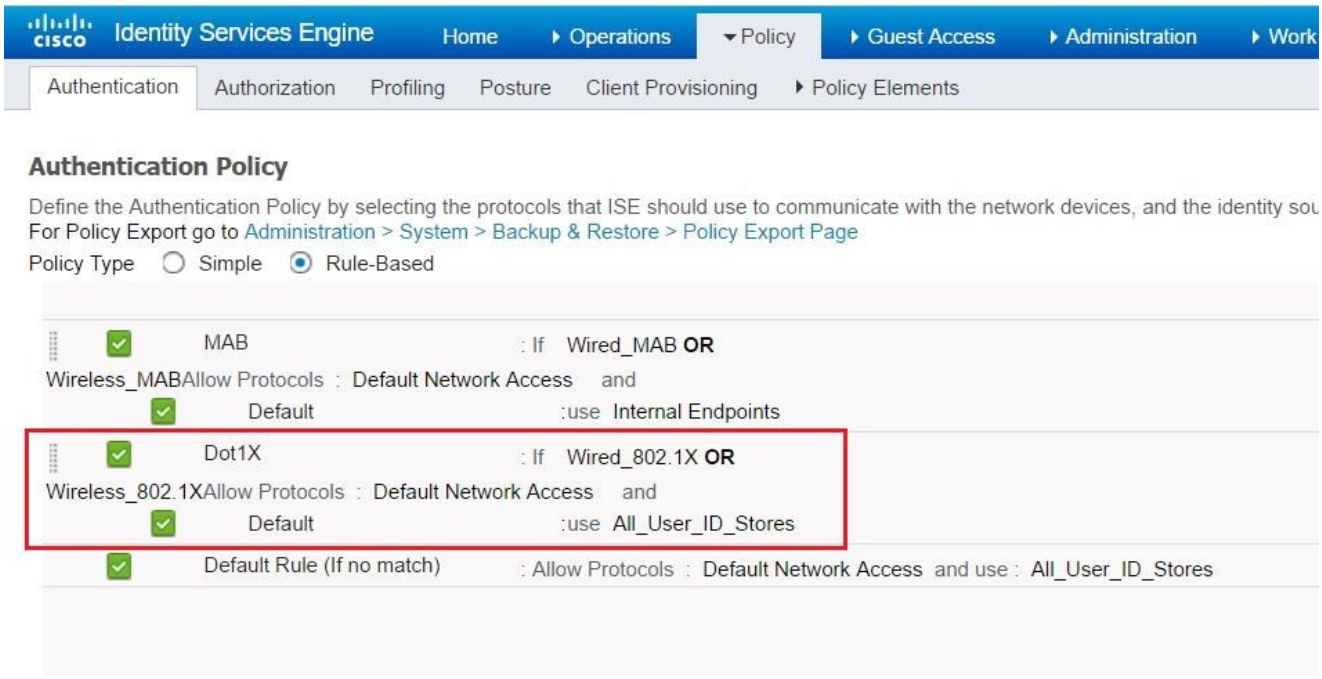
Configuration du serveur ISE

1. Ajoutez le commutateur en tant que client AAA (Authentication, Authorization, and Accounting) sur le serveur ISE.

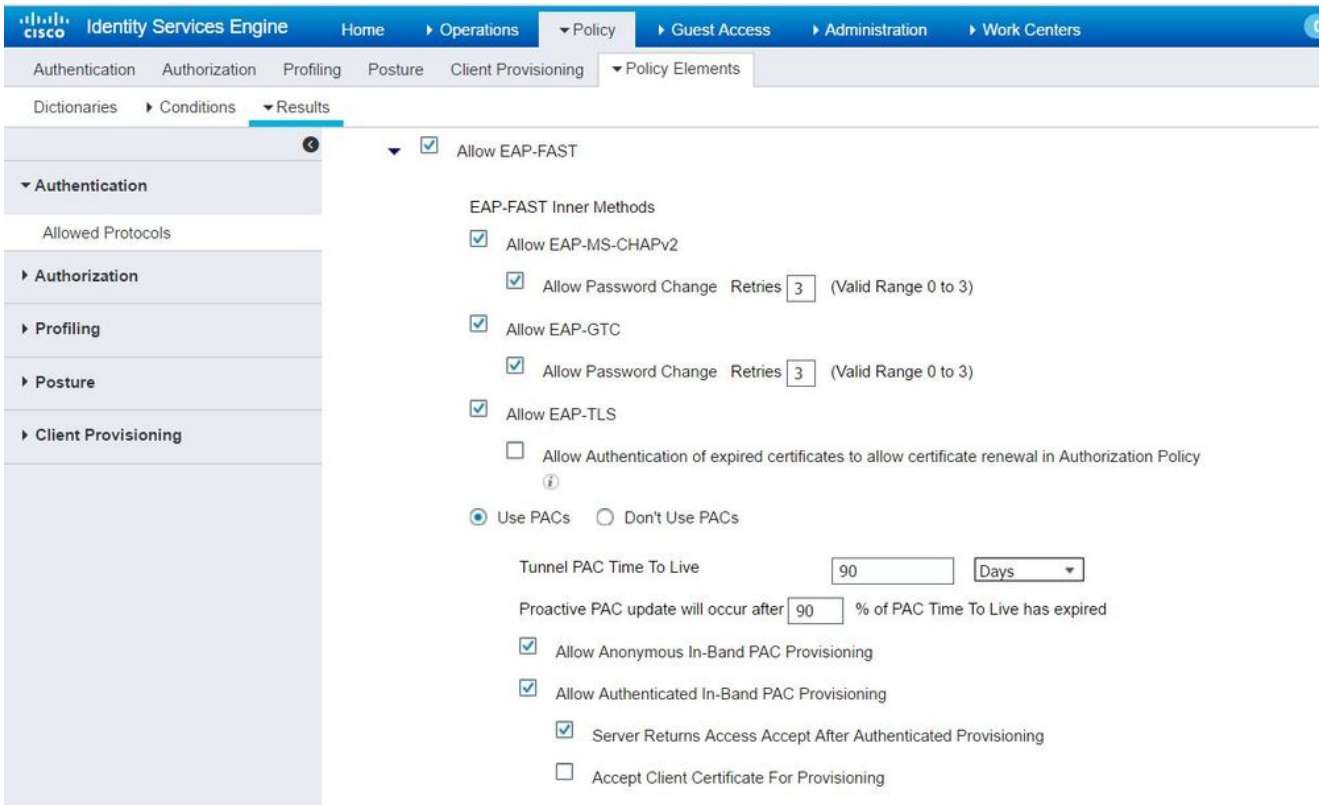




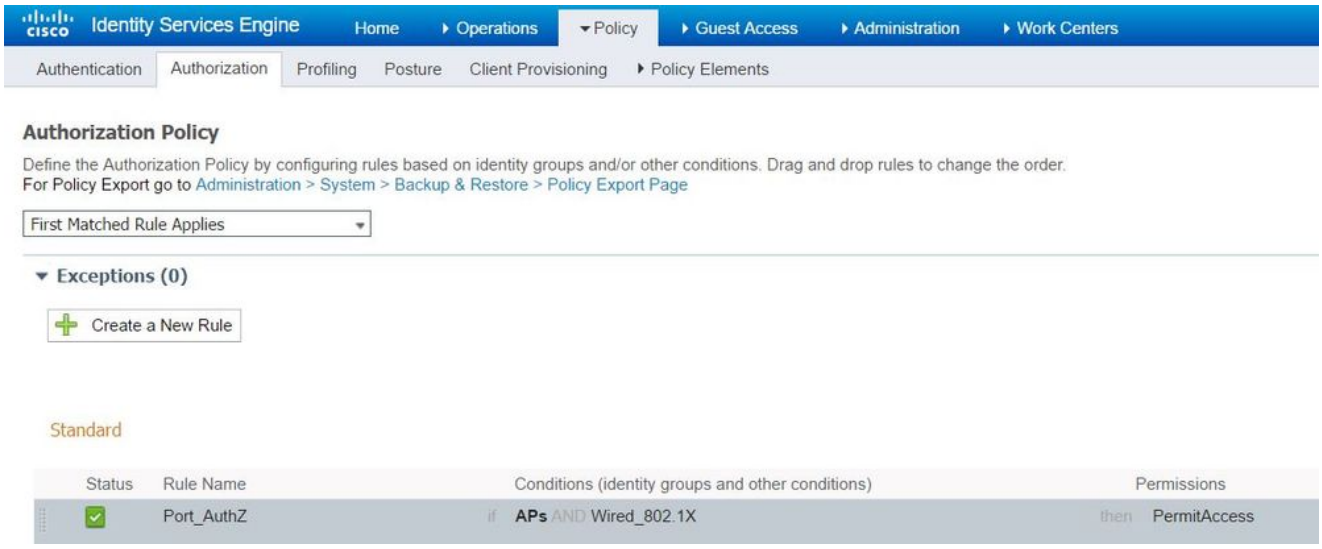
2. Sur ISE, configurez la stratégie d'authentification et la stratégie d'autorisation. Dans ce cas, la règle d'authentification par défaut, qui est le point.1x câblé, est utilisée, mais on peut la personnaliser selon les besoins.

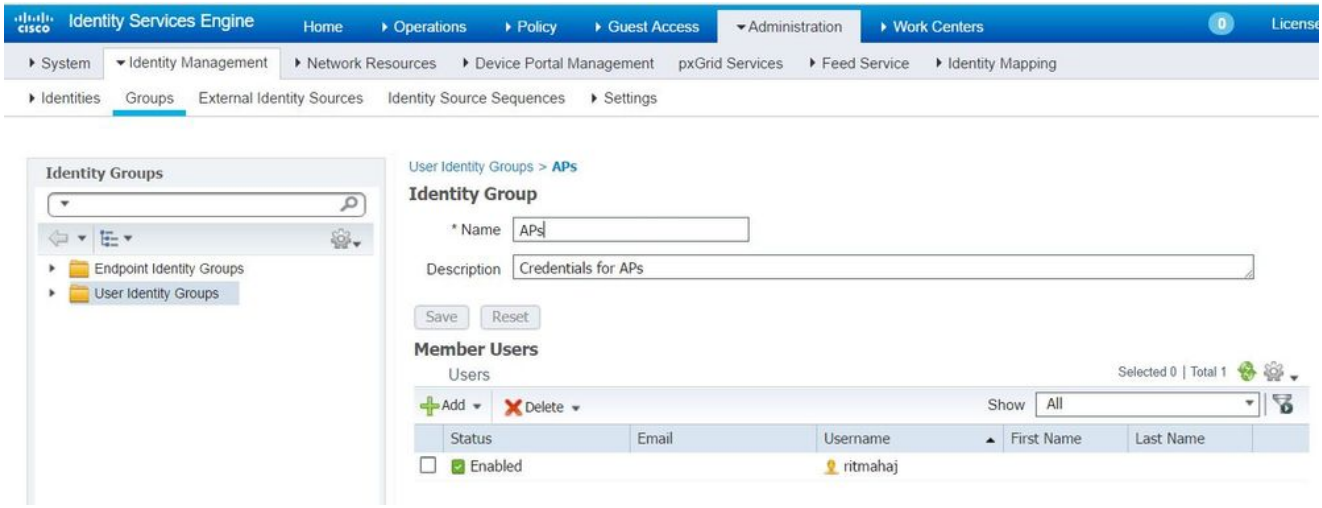


Assurez-vous que dans les protocoles autorisés par l'accès réseau par défaut, EAP-FAST est autorisé.



3. En ce qui concerne la stratégie d'autorisation (Port_AuthZ), dans ce cas, les informations d'identification d'AP ont été ajoutées à un groupe d'utilisateurs (AP). La condition utilisée était : « Si l'utilisateur appartient au groupe AP et fait le point1x filaire, alors poussez le profil d'autorisation par défaut autoriser l'accès. » Encore une fois, cela peut être personnalisé selon les besoins.





Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Une fois que la norme 802.1x est activée sur le port du commutateur, tout le trafic, à l'exception du trafic 802.1x, est bloqué par le port. Le LAP, qui s'il est déjà enregistré sur le WLC, est dissocié. Un autre trafic n'est autorisé à passer qu'après une authentification 802.1x réussie. L'enregistrement réussi du LAP sur le WLC après que le 802.1x est activé sur le commutateur indique que l'authentification LAP est réussie. Vous pouvez également utiliser ces méthodes afin de vérifier si le LAP est authentifié.

1. Sur le commutateur, entrez l'une des commandes show afin de vérifier si le port a été authentifié ou non.
   <#root>

   ```
   akshat_sw#

   show dot1x interface g0/4



   Dot1x Info for GigabitEthernet0/4
   ```

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


akshat_sw#
```

show dot1x interface g0/4 details

```
Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30

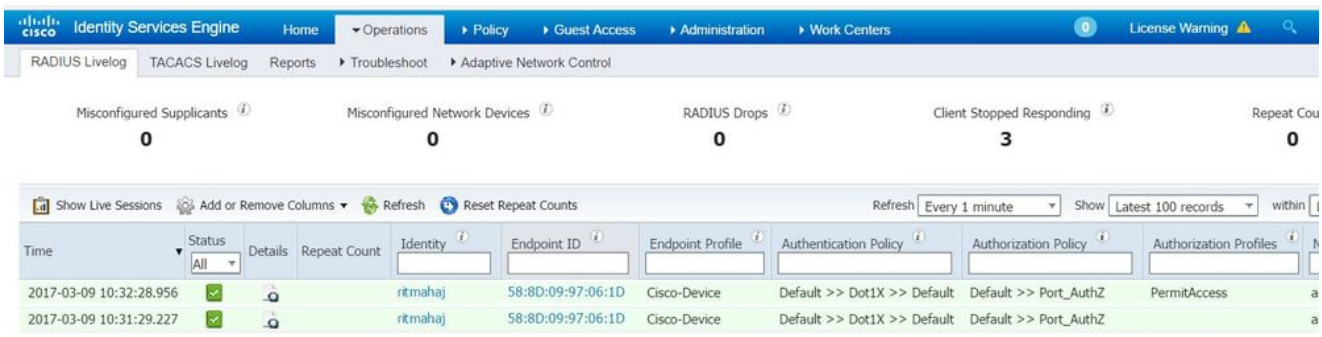

Dot1x Authenticator Client List
-------------------------------
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
 Auth SM State = AUTHENTICATED
 Auth BEND SM State = IDLE


akshat_sw#
```

show authentication sessions

```
Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

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



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 ACS.
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.

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.