Configurer un point d'accès léger en tant que demandeur 802.1x

Contenu

Introduction

Ce document décrit comment configurer un point d'accès léger (LAP) pendant qu'un suppliant de 802.1x afin d'authentifier contre le serveur du Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur Sans fil de réseau local (WLC) et RECOUVREMENT
- 802.1x sur des Commutateurs de Cisco
- ISE
- Protocole EAP (Extensible Authentication Protocol) - Flexible Authentication via Secure Tunneling (JEÛNEZ)

[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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

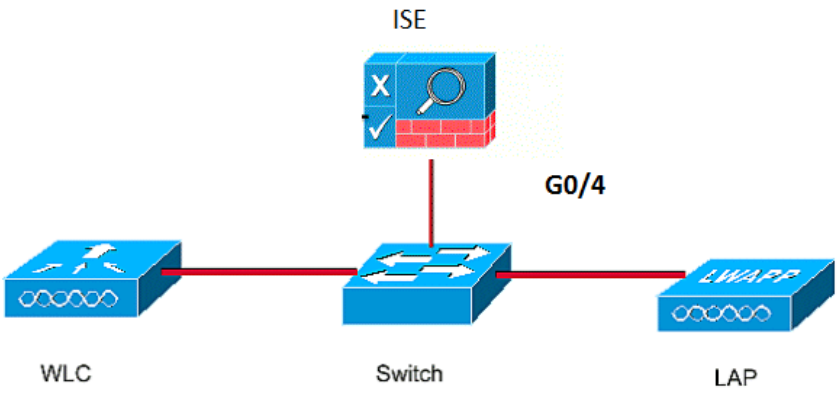
En cela installé le Point d'accès (AP) agit en tant que suppliant de 802.1x et est authentifié par le commutateur contre l'ISE qui utilise l'EAP-FAST avec le ravitaillement anonyme des qualifications de Protected Access (PAC). Une fois le port est configuré pour l'authentification de 802.1x, le commutateur ne permet pas à n'importe quel trafic autre que le trafic de 802.1x pour traverser le port jusqu'à ce que le périphérique connecté au port authentifie avec succès. AP peut être authentifié ou avant qu'il joigne un WLC ou après qu'il a joint un WLC, dans ce cas vous configurent le 802.1x sur le commutateur après que le RECOUVREMENT joigne le WLC.

Configurez

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

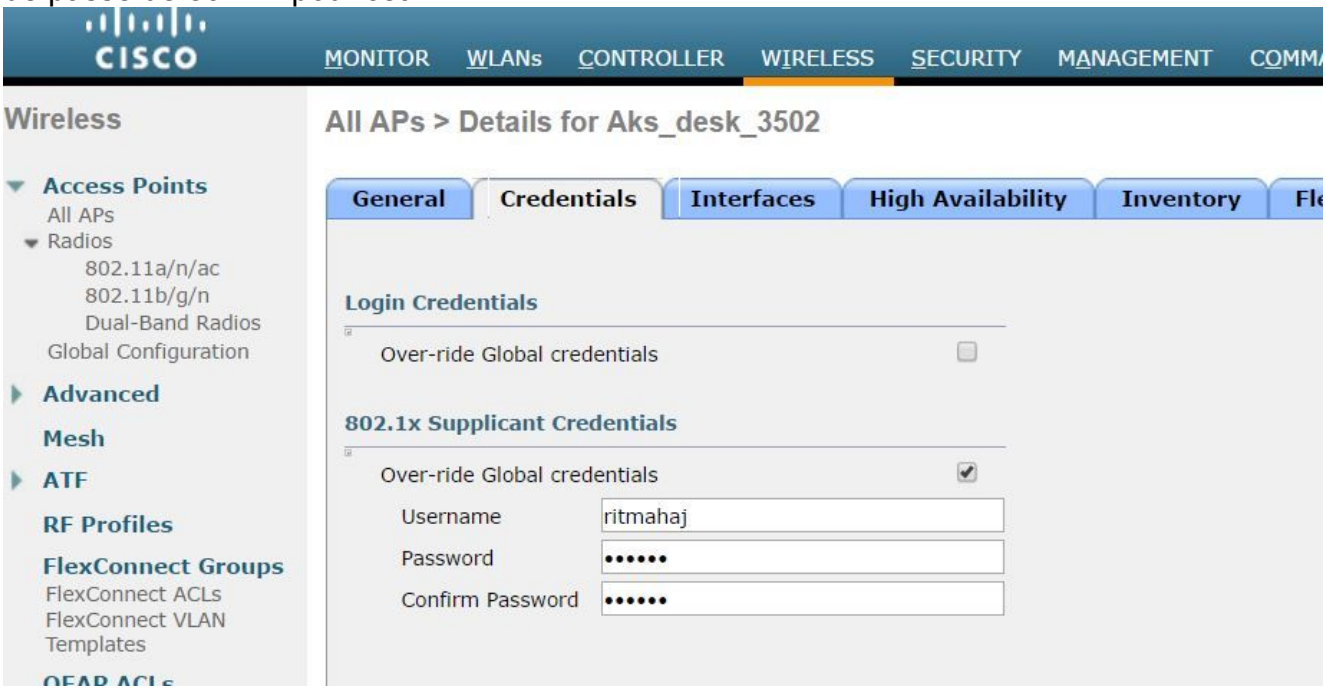
Ce document utilise ces adresses IP :

- 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

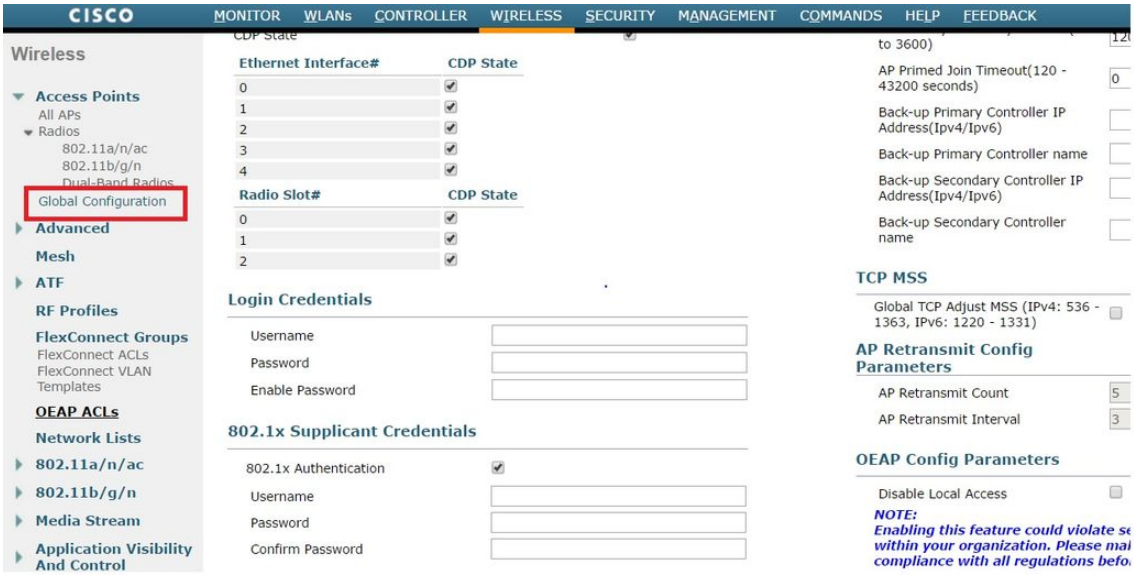
Configurez le RECOUVREMENT

Dans cette section, vous êtes présenté avec les informations pour configurer le RECOUVREMENT en tant que suppliant de 802.1x.

1. Si AP est déjà joint au WLC, allez l'onglet sans fil et cliquez sur en fonction AP, allez les qualifications mettent en place et sous les qualifications de suppliant de 802.1x se dirigeant, cochent la case **globale de qualifications de priorité** afin de placer le nom d'utilisateur et mot de passe de 802.1x pour cet AP.



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



2. Si AP n'a pas joint un WLC encore, vous devez consoler dans le RECOUVREMENT afin de placer les qualifications et utiliser ces commandes CLI :

```
LAP#debug capwap console cli
LAP#capwap ap dot1x username <username> password <password>
```

Configurez le commutateur

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

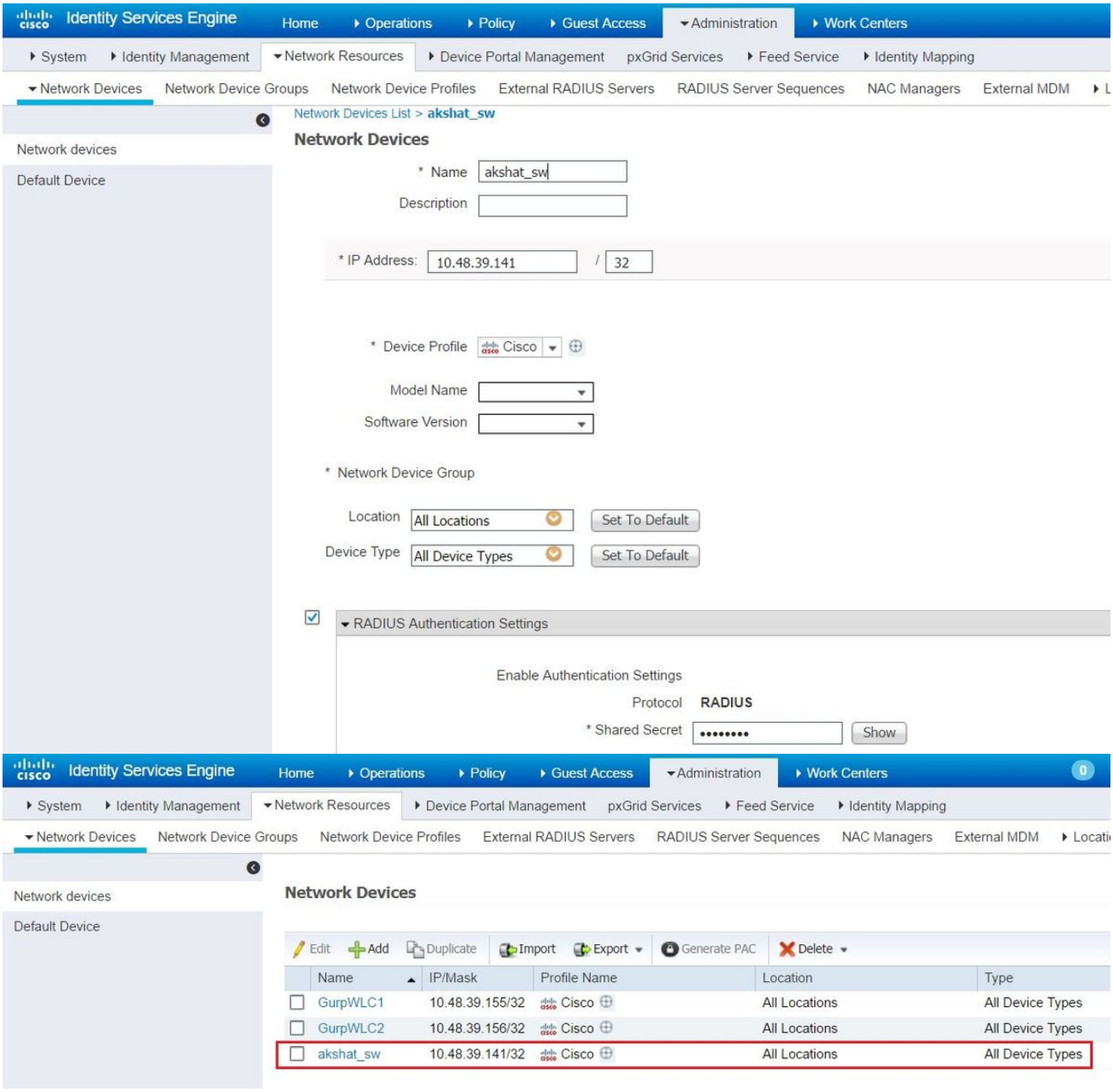
```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
  key 7 123A0C0411045D5679
```

2. Maintenant, configurez le port de commutateur AP.

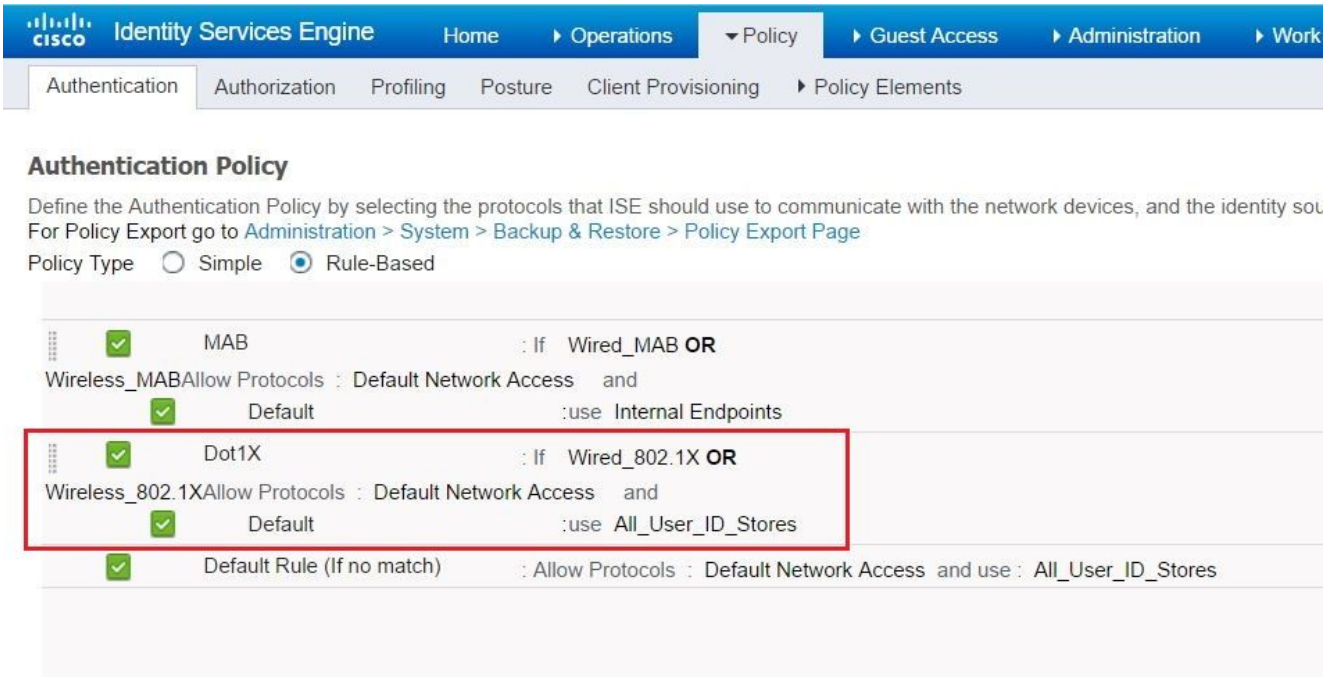
```
interface GigabitEthernet0/4


switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configurez le serveur ISE

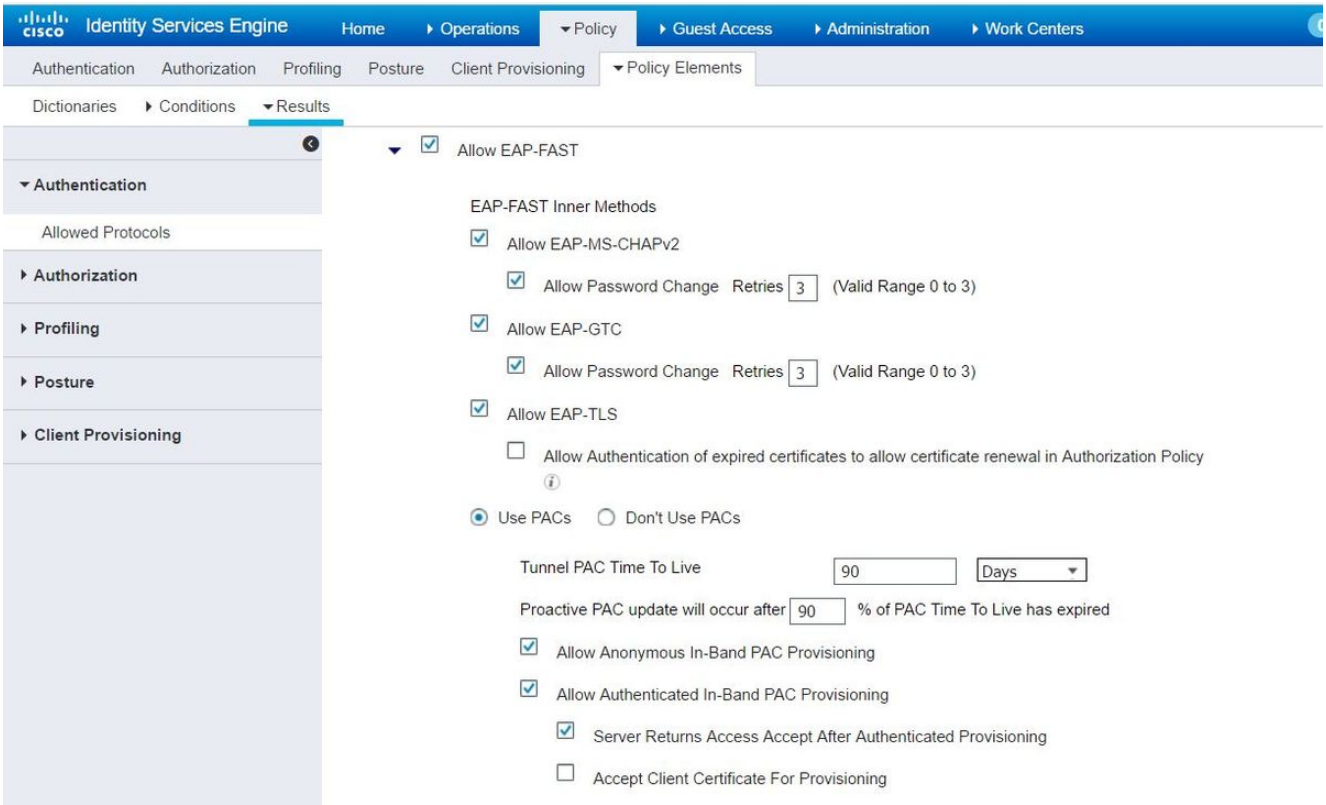
1. Ajoutez le commutateur en tant que client d'Authentification, autorisation et comptabilité (AAA) sur le serveur ISE.



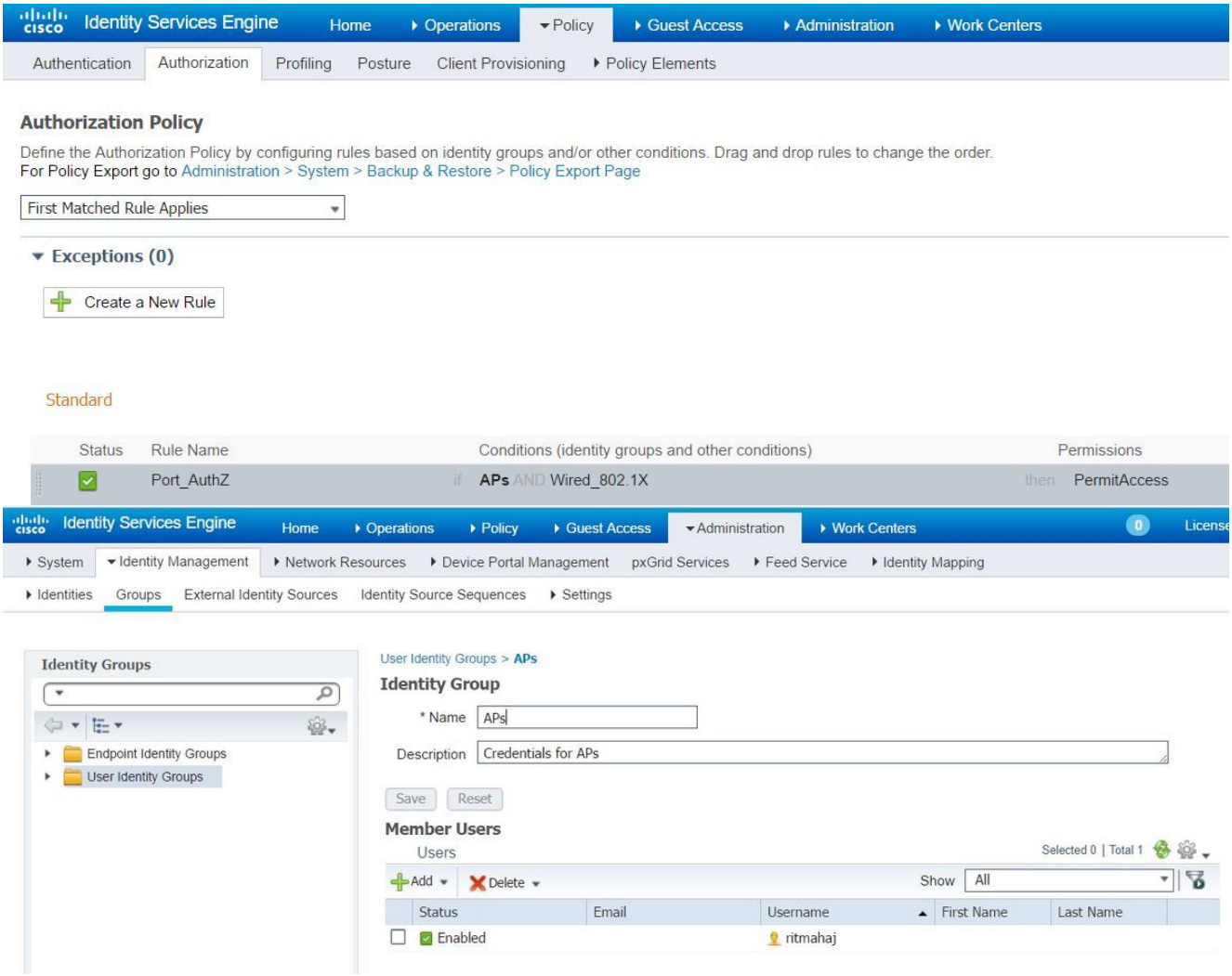
2. Sur ISE, configurez la stratégie de stratégie d'authentification et d'autorisation. Dans ce cas, la règle d'authentification par défaut qui est dot.1x de câble est utilisée, mais un peut le personnaliser selon la condition requise.



Assurez cela dans les protocoles permis qu'on permet l'accès au réseau par défaut, EAP-FAST.



3. Quant à la stratégie d'autorisation (Port_AuthZ), dans ce cas des qualifications AP ont été ajoutées à un groupe d'utilisateurs (aps). La condition utilisée était « si l'utilisateur appartient au groupe AP et faire le dot1x de câble, alors pousse l'accès par défaut d'autorisation de profil d'autorisation. » De nouveau, ceci peut être personnalisé selon la condition requise.



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

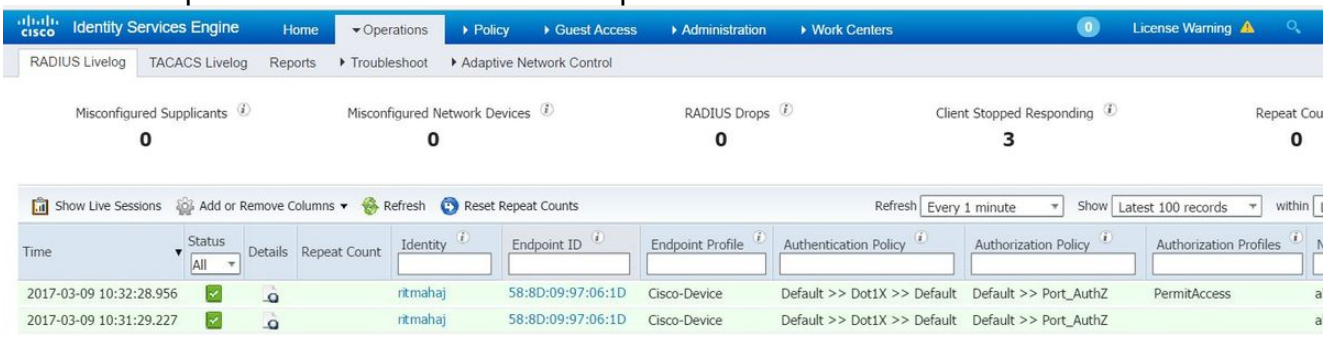
Une fois que le 802.1x est activé sur le port de commutateur, tout le trafic excepté le trafic de 802.1x est bloqué par le port. Le RECOUVREMENT, qui si déjà enregistré au WLC, obtient dissocié. Seulement après qu'une authentification réussie de 802.1x est l'autre trafic permis pour traverser. L'enregistrement réussi du RECOUVREMENT au WLC après que le 802.1x soit activé sur le commutateur indique que l'authentification de RECOUVREMENT est réussie. Vous pouvez également employer ces méthodes afin de vérifier si le RECOUVREMENT authentifiait.

1. Sur le commutateur, sélectionnez une des **commandes show** afin de vérifier si le port a été authentifié ou pas.

```
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 les **exécutions > le rayon Livelogs** et voyez que l'authentification est réussie et le profil correct d'autorisation est poussé.



Dépannez

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

1. Sélectionnez la **commande ping** afin de vérifier si le serveur ISE est accessible du commutateur.
2. Assurez-vous que le commutateur est configuré en tant que client d'AAA sur le serveur ISE.
3. Assurez-vous que le secret partagé est identique entre le commutateur et le serveur ACS.
4. Vérifiez si l'EAP-FAST est activé sur le serveur ISE.
5. Vérifiez si les qualifications de 802.1x sont configurées pour le RECOUVREMENT et sont mêmes sur le serveur ISE. **Note**: Le nom d'utilisateur et mot de passe distinguent les majuscules et minuscules.
6. Si l'authentification échoue, sélectionnez ces commandes sur le commutateur : **debug dot1x** et **debug authentication**.