

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurez le RECOUVREMENT](#)

[Configurez le commutateur](#)

[Configurez le serveur ISE](#)

[Vérifiez](#)

[Dépannez](#)

## 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

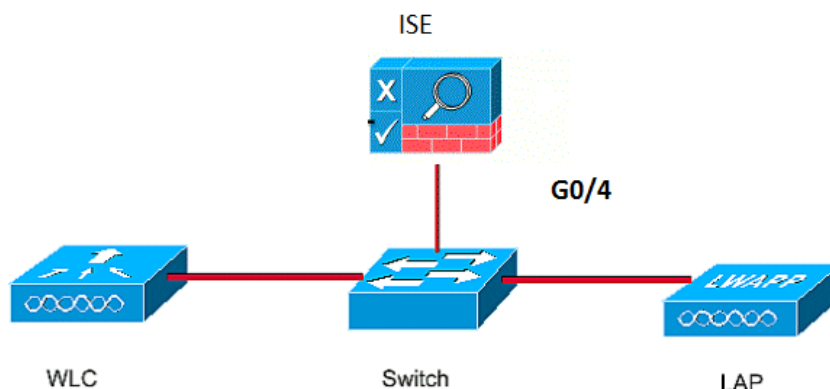
En cela installé le Point d'accès (AP) agit en tant que suppliant de 802.1x et est authentifié par le commutateur contre l'ISE qui utilise l'EAP-FAST avec le ravitaillement anonyme des qualifications de Protected Access (PAC). Une fois le port est configuré pour l'authentification de 802.1x, le commutateur 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, cochant la case **globale de qualifications de priorité** afin de placer le nom d'utilisateur et mot de passe de 802.1x pour cet AP.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMM'. The left sidebar shows the 'Wireless' menu with options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'All APs > Details for Aks\_desk\_3502' and has tabs for 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', and 'Flex'. The 'Credentials' tab is active, showing 'Login Credentials' and '802.1x Supplicant Credentials' sections. In the '802.1x Supplicant Credentials' section, the 'Over-ride Global credentials' checkbox is checked. Below this, there are three input fields: 'Username' with the value 'ritmahaj', 'Password' with masked characters '.....', and 'Confirm Password' with masked characters '.....'.

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.

The screenshot shows the Cisco Wireless configuration interface. The 'Global Configuration' link under 'Dual-Band Radios' is highlighted with a red box. The page displays various configuration sections:

- Ethernet Interface# CDP State:** A table with 5 rows (0-4) and a checked CDP State column.
- Radio Slot# CDP State:** A table with 3 rows (0-2) and a checked CDP State column.
- Login Credentials:** Fields for Username, Password, and Enable Password.
- 802.1x Supplicant Credentials:** A checked checkbox for 802.1x Authentication, and fields for Username, Password, and Confirm Password.
- TCP MSS:** A checkbox for Global TCP Adjust MSS (IPV4: 536 - 1363, IPV6: 1220 - 1331).
- AP Retransmit Config Parameters:** Fields for AP Retransmit Count (5) and AP Retransmit Interval (3).
- OEAP Config Parameters:** A checkbox for Disable Local Access.

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.

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices List > akshat\_sw

Network devices

Default Device

**Network Devices**

\* Name: akshat\_sw

Description: [ ]

\* IP Address: 10.48.39.141 / 32

\* Device Profile: Cisco

Model Name: [ ]

Software Version: [ ]

\* Network Device Group

Location: All Locations [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

\* Shared Secret: [ ] [Show]

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network devices

Default Device

**Network Devices**

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> GurpWLC1	10.48.39.155/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> GurpWLC2	10.48.39.156/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> akshat_sw	10.48.39.141/32	Cisco	All Locations	All Device Types

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.

**Identity Services Engine** Home Operations Policy Guest Access Administration Work

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

### Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type  Simple  Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MAB	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

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

**Identity Services Engine** Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Allow EAP-FAST

EAP-FAST Inner Methods

- Allow EAP-MS-CHAPv2
  - Allow Password Change Retries  (Valid Range 0 to 3)
- Allow EAP-GTC
  - Allow Password Change Retries  (Valid Range 0 to 3)
- Allow EAP-TLS
  - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Use PACs  Don't Use PACs
  - Tunnel PAC Time To Live
  - Proactive PAC update will occur after  % of PAC Time To Live has expired
  - Allow Anonymous In-Band PAC Provisioning
  - Allow Authenticated In-Band PAC Provisioning
    - Server Returns Access Accept After Authenticated Provisioning
    - Accept Client Certificate For Provisioning

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.

**Identity Services Engine** Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

### Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.  
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

Create a New Rule

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > APs

### Identity Group

Name: APs

Description: Credentials for APs

Save Reset

### Member Users

Users Selected 0 | Total 1

+ Add - Delete Show All

Status	Email	Username	First Name	Last Name
<input checked="" type="checkbox"/> Enabled		ritmahaj		

## Vérfiez

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.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-03-09 10:32:28.956	✓			ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess
2017-03-09 10:31:29.227	✓			ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	

## 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**.