

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

Introduction

Ce document décrit comment configurer un LAP (Lightweight Access Point) comme demandeur 802.1x afin de s'authentifier sur le serveur ISE (Identity Services Engine).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur de réseau local sans fil (WLC) et LAP
- 802.1x sur les commutateurs Cisco
- ISE
- EAP (Extensible Authentication Protocol) - Authentification flexible via la tunnellation sécurisée (FAST)

Components Used

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

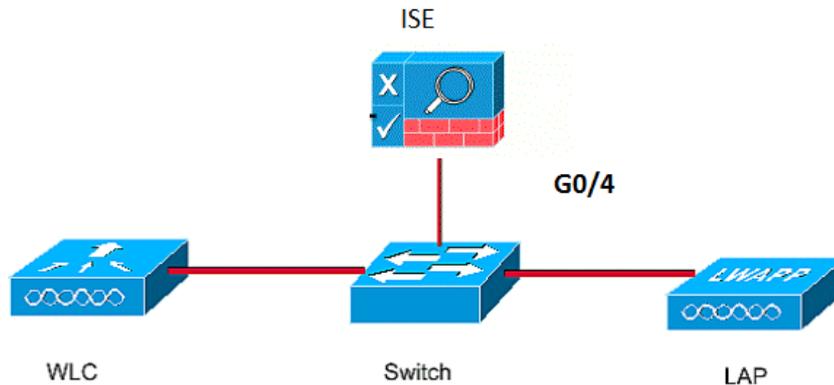
Dans cette configuration, le point d'accès (AP) agit en tant que demandeur 802.1x et est authentifié par le commutateur par rapport à l'ISE qui utilise EAP-FAST avec le provisionnement anonyme des informations d'identification et de connexion protégées (PAC). Une fois le port configuré pour l'authentification 802.1x, le commutateur n'autorise aucun trafic autre que le trafic 802.1x à traverser le port jusqu'à ce que le périphérique connecté au port s'authentifie correctement. Un point d'accès peut être authentifié avant de rejoindre un WLC ou après avoir rejoint un WLC, auquel cas vous configurez 802.1x sur le commutateur après que le LAP se connecte au WLC.

Configuration

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 les adresses IP suivantes :

- 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

Configurer le LAP

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

1. Si le point d'accès est déjà joint au WLC, accédez à l'onglet Wireless et cliquez sur le point d'accès, accédez au champ Credential et sous le titre 802.1x Supplicant Credential, cochez la case **Over-ride Global dential** afin de définir le nom d'utilisateur et le mot de passe 802.1x pour ce point d'accès.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMAN'. The left sidebar shows the 'Wireless' menu with options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', 'FlexConnect Groups', and 'OEAP ACLs'. 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 the 'Login Credentials' section with an 'Over-ride Global credentials' checkbox (unchecked) and the '802.1x Supplicant Credentials' section with an 'Over-ride Global credentials' checkbox (checked). Below this, there are input fields for 'Username' (containing 'ritmahaj'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots).

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 Configuration globale.

The screenshot shows the 'Global Configuration' page in the Cisco WLC interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Wireless' menu with 'Global Configuration' highlighted in a red box. The main content area is titled 'Global Configuration' and has tabs for 'Ethernet Interface#', 'Radio Slot#', 'Login Credentials', and '802.1x Supplicant Credentials'. The 'Login Credentials' section has input fields for 'Username', 'Password', and 'Enable Password'. The '802.1x Supplicant Credentials' section has a checked '802.1x Authentication' checkbox and input fields for 'Username', 'Password', and 'Confirm Password'. On the right side, there are various system parameters like 'AP Primed Join Timeout', 'Back-up Primary Controller IP Address', 'TCP MSS', 'AP Retransmit Config Parameters', and 'OEAP Config Parameters'.

2. Si le point d'accès n'a pas encore rejoint un WLC, vous devez vous connecter au LAP pour définir les informations d'identification et utiliser ces commandes CLI :

```
LAP#debug capwap console cli
LAP#capwap ap dot1x username
```

Configuration du commutateur

1. Activez dot1x globalement sur le commutateur 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 du 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
```

Configuration du serveur ISE

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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a Network Device. The page is titled "Network Devices" and shows the configuration for a device named "akshat_sw".

The configuration fields are as follows:

- Name: akshat_sw
- Description: (empty)
- IP Address: 10.48.39.141 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings: (checked)
- Enable Authentication Settings: (checked)
- Protocol: RADIUS
- Shared Secret: (masked with dots) (Show)

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

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

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 d'authentification et la stratégie d'autorisation. Dans ce cas, la règle d'authentification par défaut, qui est filaire dot.1x, est utilisée, mais on peut la personnaliser selon les besoins.

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-vous que dans les protocoles autorisés que Default Network Access, EAP-FAST est autorisé.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

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 Days

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. 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 point d'accès du groupe et fait un point1x câblé, alors appuyez sur l'accès d'autorisation par défaut du profil d'autorisation. » Encore une fois, il est possible de personnaliser cette option en fonction des besoins.

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

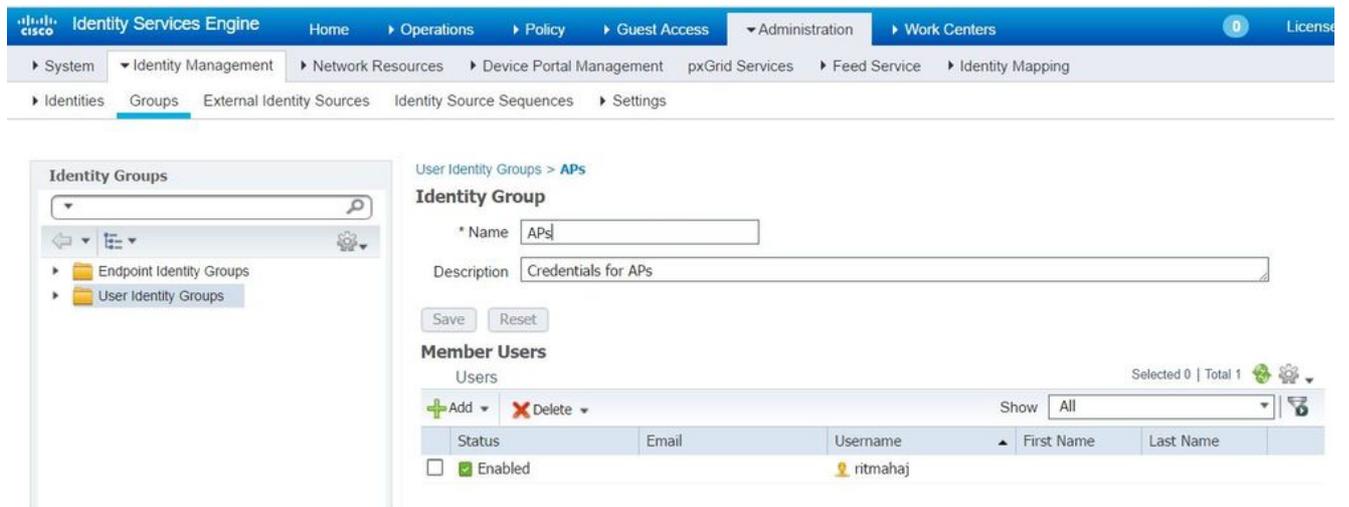
First Matched Rule Applies

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



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Une fois 802.1x activé sur le port de commutateur, tout le trafic, à l'exception du trafic 802.1x, est bloqué par le port. Le LAP, qui s'il est déjà inscrit au WLC, est dissocié. Ce n'est qu'après une authentification 802.1x réussie que d'autres trafics sont autorisés à passer. L'enregistrement réussi du LAP sur le WLC après l'activation de la norme 802.1x sur le commutateur indique que l'authentification du LAP a réussi. Vous pouvez également utiliser ces méthodes afin de vérifier si le LAP s'est authentifié.

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

```
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.

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

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 à partir du 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. **Note:** 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**.