

Sécuriser un port de commutation Flexconnect AP avec Dot1x

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration de point d'accès:](#)

[Configuration du commutateur](#)

[Configuration ISE:](#)

[Vérifier](#)

[Dépannage](#)

[Références](#)

Introduction

Ce document décrit la configuration pour sécuriser les ports de commutation où les points d'accès FlexConnect s'authentifient avec Dot1x.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexConnect sur contrôleur LAN sans fil (WLC)
- 802.1x sur les commutateurs Cisco
- Topologie NEAT (Network Edge Authentication Topology)

Composants utilisés

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

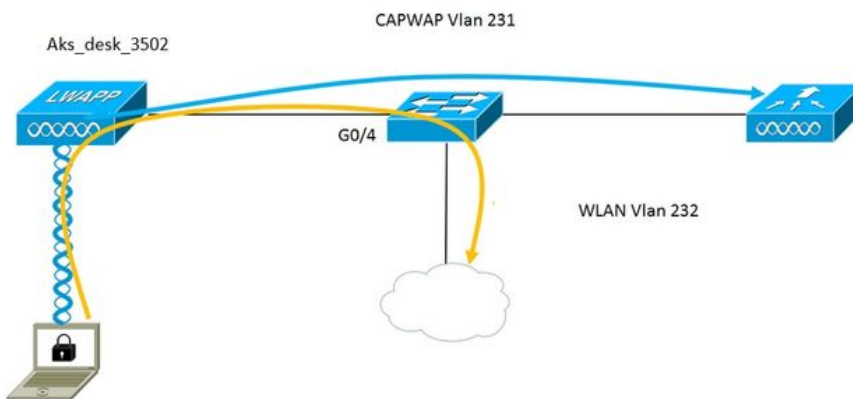
- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Identity Service Engine (ISE) 2.0
- Points d'accès basés sur IOS (séries x500, x600, x700).

Les points d'accès de phase 2 basés sur le système d'exploitation AP ne prennent pas en charge flexconnect trunk dot1x au moment de cette écriture.

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.

Configurer

Diagramme du réseau



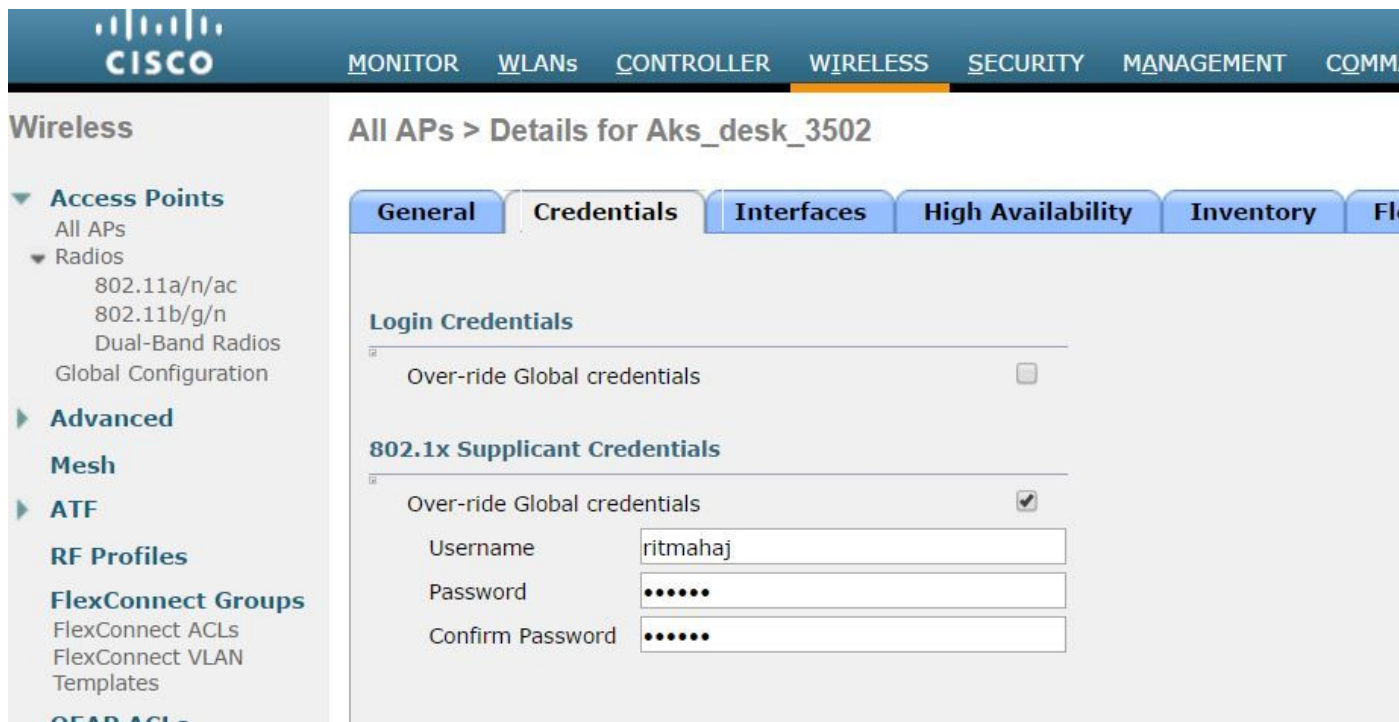
Dans cette configuration, le point d'accès agit en tant que demandeur 802.1x et est authentifié par le commutateur par rapport à ISE à l'aide d'EAP-FAST. Une fois le port configuré pour l'authentification 802.1x, le commutateur n'autorise aucun trafic autre que le trafic 802.1x à traverser le port tant que le périphérique connecté au port ne s'authentifie pas correctement.

Une fois que le point d'accès s'authentifie correctement auprès d'ISE, le commutateur reçoit l'attribut Cisco VSA « device-traffic-class=switch » et déplace automatiquement le port vers l'agrégation.

Cela signifie que si le point d'accès prend en charge le mode FlexConnect et a des SSID commutés localement configurés, il est capable d'envoyer du trafic étiqueté. Assurez-vous que la prise en charge du VLAN est activée sur le point d'accès et que le VLAN natif correct est configuré.

Configuration de point d'accès:

1. Si le point d'accès est déjà connecté au WLC, accédez à l'onglet Wireless et cliquez sur le point d'accès. Rendez-vous dans le champ Informations d'identification et sous l'en-tête Informations d'identification du demandeur 802.1x, cochez la case Remplacer les informations d'identification globales pour définir le nom d'utilisateur et le mot de passe 802.1x pour ce point d'accès.



The screenshot shows the Cisco 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'. In the '802.1x Supplicant Credentials' section, the 'Over-ride Global credentials' checkbox is checked. Below it, the 'Username' field contains 'ritmahaj', and the 'Password' and 'Confirm Password' fields are masked with dots.

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

The screenshot shows the Cisco Wireless configuration interface. The left sidebar contains a tree view with 'Global Configuration' highlighted. The main content area is divided into several sections:

- Ethernet Interface# CDP State:** A table with columns for Ethernet Interface# (0-4) and CDP State (checked).
- Radio Slot# CDP State:** A table with columns for Radio Slot# (0-2) and CDP State (checked).
- Login Credentials:** Fields for Username, Password, and Enable Password.
- 802.1x Supplicant Credentials:** A checkbox for 802.1x Authentication (checked) and fields for Username, Password, and Confirm Password.
- TCP MSS:** A section 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.

A note at the bottom states: **NOTE:** Enabling this feature could violate security within your organization. Please maintain compliance with all regulations before enabling.

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

```
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

```
aaa new-model
```

!

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

!

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

!

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

!

Serveur RADIUS ISE

```
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
```

```
clé 7 123A0C0411045D5679
```

2. Configurez maintenant le port de commutateur AP

```
interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
authentication host-mode multi-host
ordre d'authentification dot1x
authentication port-control auto
authentificateur de page dot1x
spanning-tree portfast edge
```

Configuration ISE:

1. Sur ISE, on peut simplement activer NEAT pour le profil d'autorisation AP afin de définir l'attribut correct, cependant, sur d'autres serveurs RADIUS, vous pouvez configurer manuellement.

[Authorization Profiles > AP_Flex_Trunk](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

▼ Common Tasks

NEAT

▼ Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = device-traffic-class=switch

2. Sur ISE, il faut également configurer la stratégie d'authentification et la stratégie d'autorisation. Dans ce cas, nous atteignons la règle d'authentification par défaut qui est filaire dot1x, mais on peut la personnaliser selon l'exigence.

En ce qui concerne la stratégie d'autorisation (Port_AuthZ), dans ce cas, nous avons ajouté les informations d'identification d'AP à un groupe d'utilisateurs (AP) et avons poussé le profil d'autorisation (AP_Flex_Trunk) en fonction de cela.

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)

Standard

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

Vérifier

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

1. Sur le commutateur, une fois peut utiliser la commande « debug authentication feature autocfg all » pour vérifier si le port est déplacé vers le port trunk ou non.

```
20 février 12:34:18.119: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changé d'état en up
20 février 12:34:19.122: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface
GigabitEthernet0/4, changé d'état en up
akshat_sw#
akshat_sw#
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle:
3372220456
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Type de
périphérique = commutateur
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] nouveau client
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] État interne de l'application de
macro AutoCfg : 1
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Type de périphérique : 2
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp has port_config
0x85777D8
20 février 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp port_config has
bpd guard_config 2
20 février 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Application de la commande
auto-cfg sur le port.
20 Février 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: 231 Vlan-Str: 231
20 février 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Application de la macro
dot1x_autocfg_supp
20 février 12:38:11.116: Application de la commande... 'no switchport access vlan 231' à Gi0/4
20 février 12:38:11.127: Application de la commande... 'no switchport nonegotiate' à Gi0/4
20 février 12:38:11.127: Application de la commande... 'switchport mode trunk' à Gi0/4
20 février 12:38:11.134: Application de la commande... 'switchport trunk native vlan 231' à Gi0/4
20 février 12:38:11.134: Application de la commande... 'spanning-tree portfast trunk' à Gi0/4
20 février 12:38:12.120: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface
GigabitEthernet0/4, changé d'état en down
20 février 12:38:15.139: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface
GigabitEthernet0/4, changé d'état en up
```

2. Le résultat de la commande « show run int g0/4 » indique que le port est devenu un port agrégé.

Configuration actuelle : 295 octets

```
!  
interface GigabitEthernet0/4  
switchport trunk allowed vlan 231,232,239  
switchport trunk native vlan 231  
switchport mode trunk  
authentication host-mode multi-host  
ordre d'authentification dot1x  
authentication port-control auto  
authentificateur de page dot1x  
spanning-tree port fast edge trunk  
tranche
```

3. Sur ISE, sous Operations>>Radius Livelogs on peut voir l'authentification réussie et le profil d'autorisation correct poussé.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-02-20 15:05:48.991				0 ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4. Si nous connectons un client après cela, son adresse MAC est apprise sur le port du commutateur AP dans le VLAN client 232.

```
akshat_sw#sh mac address-table int g0/4
```

Table d'adresses MAC

```
-----  
Ports De Type D'Adresse Mac Vlan
```

```
-----  
231 588d.0997.061d STATIQUE Gi0/4 - AP  
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Client
```

Sur le WLC, dans le détail du client, on peut voir que ce client appartient au VLAN 232 et que le SSID est commuté localement. En voici un extrait.

```
(Contrôleur Cisco) >show client detail c0:ee:fb:d7:88:24  
Adresse MAC du client..... c0:ee:fb:d7:88:24  
Nom d'utilisateur du client ..... S/O  
Adresse MAC du point d'accès..... b4:14:89:82:cb:90  
Nom AP..... Aks_desk_3502  
ID d'emplacement radio AP..... 1  
État du client..... Associé  
Groupe d'utilisateurs client.....  
État OOB NAC du client..... Accès
```

ID LAN sans fil..... 2
 Nom du réseau local sans fil (SSID)..... Port-Auth
 Nom du profil LAN sans fil..... Port-auth
 Hotspot (802.11u)..... Non pris en charge
 BSSID..... b4:14:89:82:cb:9f
 Connecté pendant 42 secondes
 Canal..... 44
 Adresse IP..... 192.168.232.90
 Adresse de passerelle..... Commutateurs 192.168.232.1
 Masque réseau..... 255.255.255.0
 ID d'association..... 1
 Algorithme d'authentification..... Système ouvert
 Code raison..... 1
 Code d'état..... 0

Commutation de données FlexConnect..... Municipal
 État DHCP FlexConnect..... Municipal
 Commutation centrale basée sur le VLAN FlexConnect..... Non
 Authentification FlexConnect..... Central
 Association FlexConnect Central..... Non
 FlexConnect VLAN NAME..... vlan 232
 Quarantaine VLAN..... 0
 Accès au VLAN..... 232
 Pontage local VLAN..... 232

Dépannage

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

- Si l'authentification échoue, utilisez les commandes `debug dot1x`, `debug authentication`.
- Si le port n'est pas déplacé vers l'agrégation, entrez la commande `debug authentication feature autocfg all`.
- Assurez-vous que le mode multi-hôte (authentification `host-mode multi-host`) est configuré. Multi-Host doit être activé afin d'autoriser les adresses MAC sans fil des clients.
- La commande « `aaa authorization network` » doit être configurée pour que le commutateur accepte et applique les attributs envoyés par ISE.

Les points d'accès Cisco IOS prennent uniquement en charge TLS 1.0. Cela peut poser un problème si votre serveur RADIUS est configuré pour autoriser uniquement les authentifications TLS 1.2 802.1X

Références

[Configurez le demandeur dot1x avec un point d'accès et un WLC 9800](#)

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.