Standardiser l'authentification des points d'accès 802.1X avec IBNS 2.0 et les modèles d'interface

Table des matières

Introduction

Ce document décrit la configuration 802.1X à l'aide des modèles d'interface IBNS 2.0.

Énoncé du problème

L'utilisation de la norme IEEE 802.1X pour la sécurité des ports est une pratique recommandée courante. Outre l'amélioration de la sécurité du réseau, elle simplifie également les déploiements de commutateurs en permettant une configuration normalisée des ports d'accès sur l'ensemble du réseau.

Ce guide décrit comment une configuration de port de commutation unique et normalisée peut être utilisée à la fois pour les périphériques finaux et les points d'accès Cisco. Alors que chaque port de commutation fonctionne initialement comme un port d'accès standard et effectue l'authentification IEEE 802.1X, un point d'accès authentifié peut nécessiter un mode de fonctionnement différent selon son scénario de déploiement.

En particulier, les points d'accès fonctionnant en mode de commutation locale FlexConnect doivent fonctionner sur un port agrégé, car le trafic client provenant de plusieurs SSID est ponté localement. Par conséquent, l'interface du commutateur doit passer dynamiquement d'un port d'accès à un port agrégé après une authentification réussie.

Les ports d'accès connectant des périphériques d'infrastructure plutôt que de simples périphériques finaux nécessitent souvent des configurations d'interface qui diffèrent du comportement de port d'accès par défaut.

Par conséquent, la configuration de l’interface du commutateur doit être modifiée dynamiquement pendant le processus d’authentification. Au fil des ans, plusieurs approches ont été utilisées pour parvenir à ce comportement, notamment les applets Auto SmartPorts et Embedded Event Manager (EEM). Aujourd'hui, la solution recommandée est IBNS 2.0 [1] en association avec des modèles d'interface, qui fournit une méthode évolutive et cohérente pour modifier dynamiquement la configuration de l'interface après une authentification réussie.

Approche

Pour qu'une configuration fonctionne, différents composants doivent être configurés correctement, notamment

- Serveur Radius (Identity Service Engine)
- Commutateur
- Point d'accès / Contrôleur LAN sans fil

Comme il existe des documentations existantes (voir les références à la fin), nous nous concentrons sur un scénario particulier dans ce document et référençons la documentation existante comme matériel de support.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur LAN sans fil (WLC) et points d'accès légers (LAP)
- 802.1x sur les commutateurs Cisco et ISE
- Protocole EAP (Extensible Authentication Protocol)
- RADIUS (Remote Authentication Dial-In User Service)

Composants utilisés

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

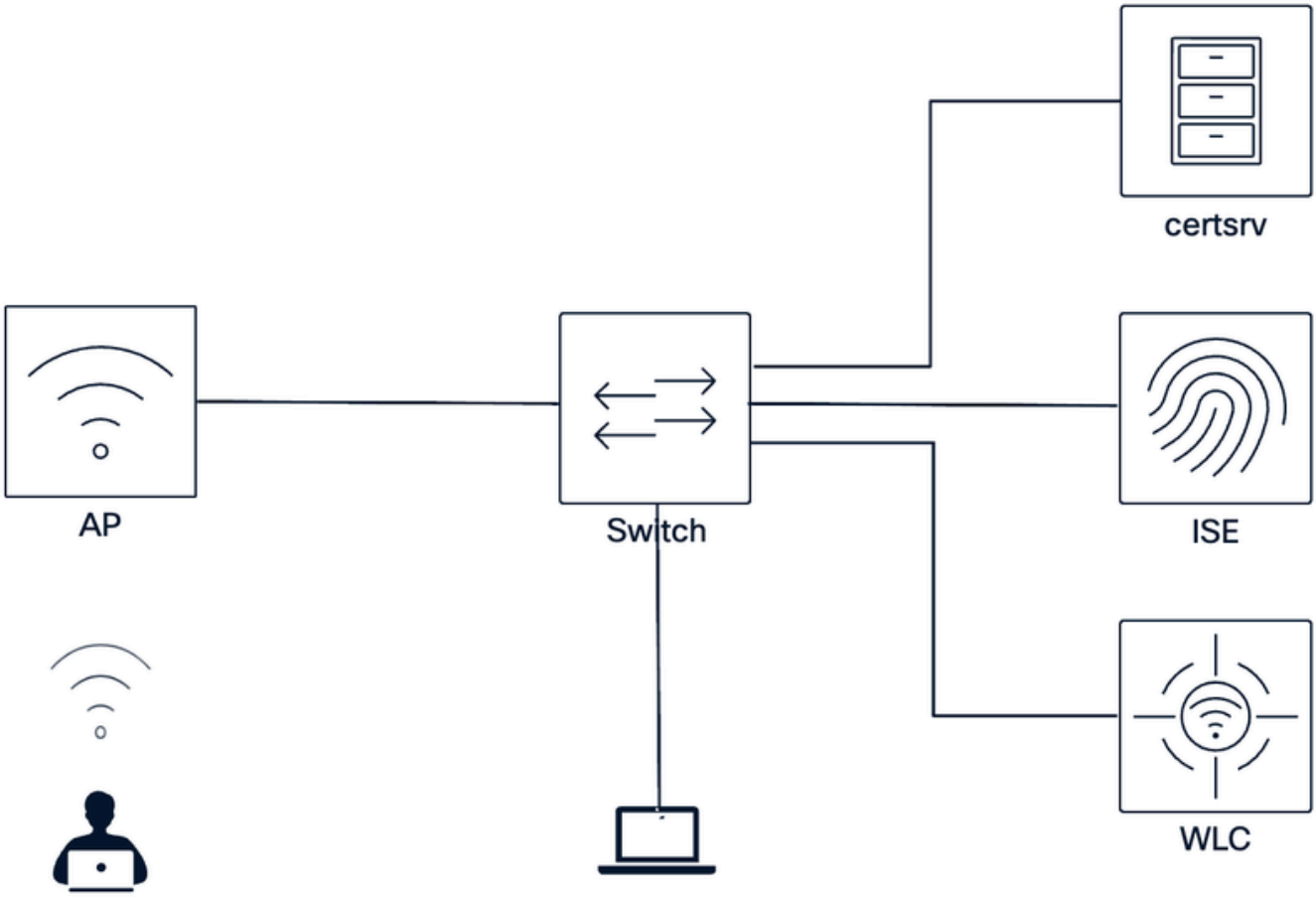
- Cisco C9350 - IOS XE 26.1.1a
- WLC Cisco C9800-40 - IOS XE 26.1.1
- ISE version 3.5 Patch 1
- AP CW917x, CW916x

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.

La configuration est également documentée dans netascode.cisco.com modèles de données pour la commutation et ISE afin de répliquer facilement la configuration.

Configuration

Diagramme du réseau



Exemple de configuration

Pour ce faire, nous nous concentrons sur un seul scénario et fournissons des extraits de configuration et des conseils pas à pas. Comme il existe différentes variantes, nous les signalons et référençons la documentation existante à cet effet.

Scénario traité dans ce guide :

- Point d'accès 1X câblé avec authentification EAP-FAST
- Identifiants Dot1X provisionnés via le WLC C9800
- Point d'accès en mode de commutation locale Flex Connect

Dans cette conception, le port de commutation utilise initialement une configuration 802.1X en mode fermé commune avec reprise MAB. Lors de la première intégration, le point d'accès n'a peut-être pas encore d'informations d'identification 802.1X, de sorte qu'ISE peut autoriser le point d'accès via MAB avec un accès limité suffisant pour atteindre le WLC ou Catalyst Center. Une fois les informations d'identification ou les certificats provisionnés, le point d'accès effectue

l'authentification 802.1X câblée. ISE renvoie ensuite un résultat d'autorisation qui s'applique au modèle d'interface AP_FLEX_TRUNK, convertissant le port en configuration d'agrégation FlexConnect requise.

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

Tableau 1 : Variantes et options supplémentaires dans une présentation

Configuration de point d’accès

Pour utiliser l'authentification Dot1x filaire en combinaison avec votre point d'accès, vous devez d'abord déployer les informations d'identification et/ou les certificats en fonction de la méthode d'authentification sélectionnée vers les points d'accès.

Le demandeur Cisco Catalyst AP Dot1x prend généralement en charge EAP-FAST, EAP-PEAP ou EAP-TLS. En outre, MAB pourrait également être une option, en particulier parce que les AP ont besoin de rassembler en premier lieu les informations d'identification ou les certificats pour pouvoir exécuter l'authentification de type EAP.

- MAB :
  - Aucune configuration côté point d'accès requise
  - La gestion des adresses MAC matérielles nécessite des outils
  - Peut être facilement usurpé
  - Permet une configuration de port commune

- EAP-FAST :
  - Basé sur le nom d'utilisateur/mot de passe
  - Facilité de déploiement
  - Nécessite l'approvisionnement PAC intrabande anonyme activé sur ISE

- EAP-PEAP :
  - Basé sur le nom d'utilisateur/mot de passe
  - Nécessite des certificats pour la validation du serveur
  - Le renouvellement du certificat doit être planifié en conséquence

- EAP-TLS :
  - Basé sur certificat
  - Le renouvellement du certificat doit être planifié en conséquence

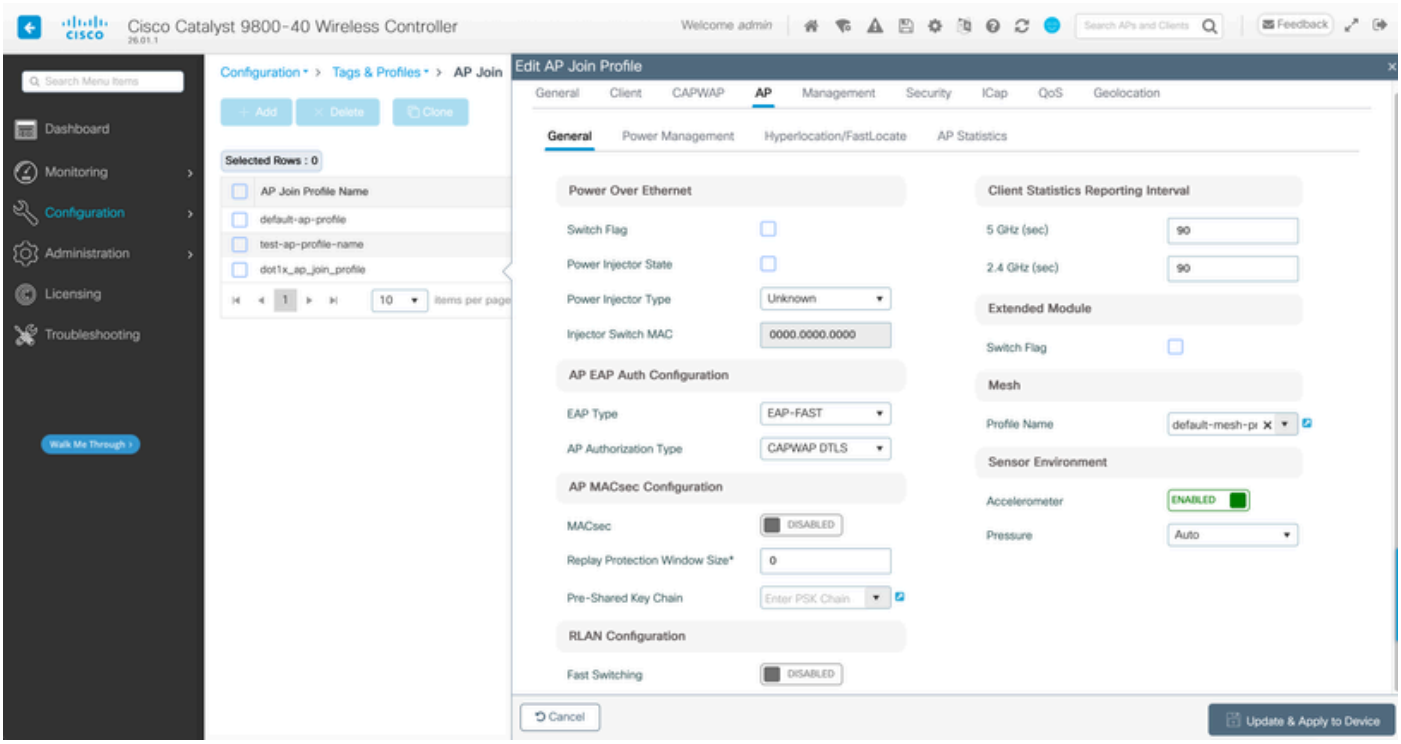
Pour configurer le demandeur point d'accès 1X câblé, il existe deux approches pour cela, soit par le biais du contrôleur LAN sans fil ou de Catalyst Center qui sont décrites ici. Avant d'entrer dans ces détails, vous devez sélectionner au préalable le type d'authentification que vous allez utiliser.

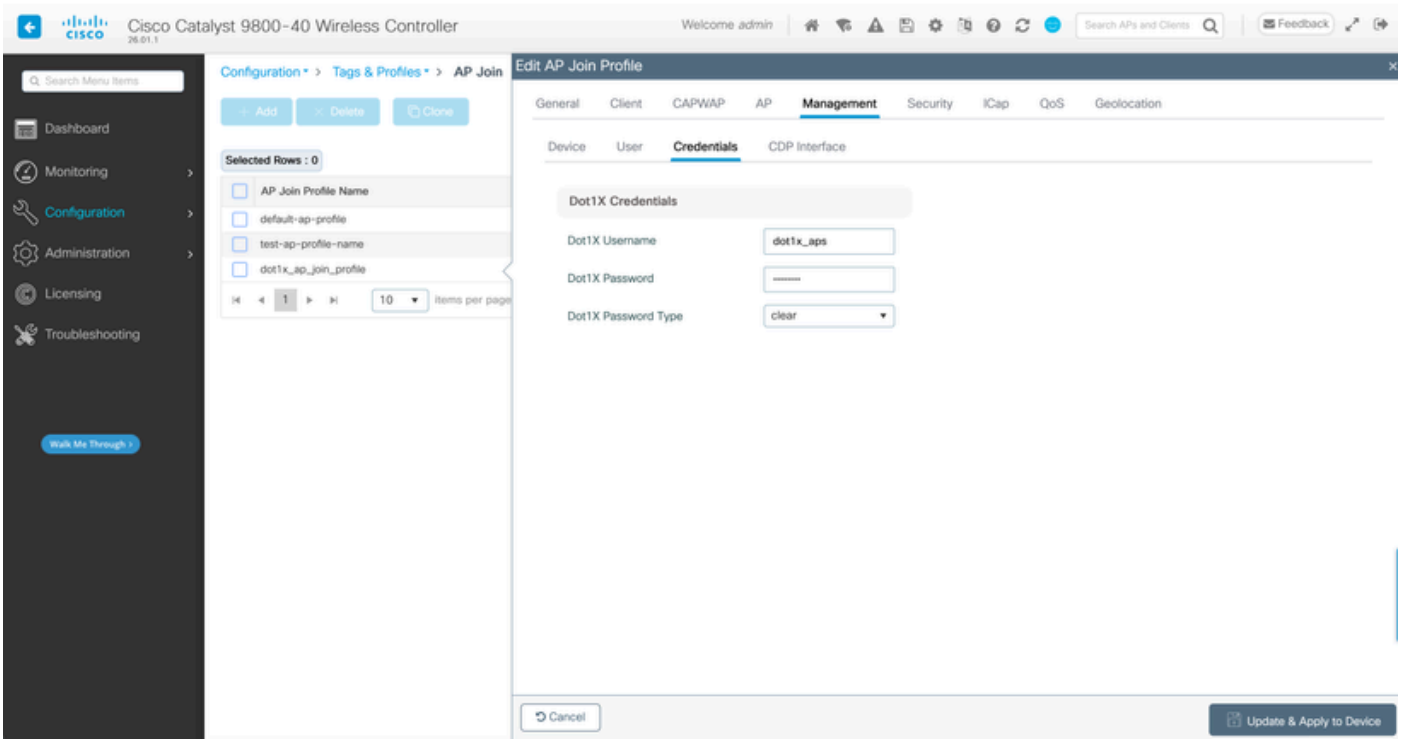
Configuration de Dot1X filaire via le contrôleur LAN sans fil Cisco 9800

Si vous avez sélectionné une authentification basée sur un certificat (EAP-PEAP ou EAP-TLS [1]), vous devez décider comme étape suivante de la façon dont vous prévoyez d'émettre des certificats d'AP significatifs localement (LSC), soit par l'intermédiaire de SCEP [2] ou EST [3].

Lors de l'utilisation d'EAP-FAST comme dans notre scénario, il suffit de générer un profil de jonction AP, où vous entrez l'utilisateur et le mot de passe Dot1X, liez ce profil de jonction à un Site-Tag et attribuez-le aux AP.

Configuration GUI





Configuration CLI

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

Configuration de Dot1X filaire via Catalyst Center Plug and Play

Pour que le PnP [4] fonctionne, Catalyst Center doit être intégré à ISE. Cela est partiellement requis en raison des certificats qui sont requis pour être en mesure d'effectuer la validation du serveur du côté AP pour l'authentification EAP avec ISE. Pour le certificat côté périphérique, les points d'accès obtiennent un certificat émis par l'autorité de certification Catalyst Center qui est soit par défaut son propre certificat intégré, soit s'il est configuré par une autorité de certification secondaire / SCEP de l'autorité de certification respective.

Le processus de configuration via PnP permet la mise en service de certificats et/ou d'informations d'identification avant que le périphérique ne rejoigne les WLC.

Configuration du commutateur

Outre le fait que l'authentification est un mécanisme de sécurité, c'est également un moyen de standardiser les configurations de port de commutation. Par conséquent, ces parties décrivent les éléments requis pour y parvenir. Il s'agit d'un exemple de configuration qui doit être révisé et adapté à votre configuration. En général, cette configuration permet Dot1x et MAB de secours avec une gestion appropriée des scénarios Radius morts, une réauthentification, etc.

Attributs de rayon global :

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Groupe de serveurs Radius :

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
```

```
!
!
aaa group server radius client-radius-group
 server name client-radius-server01
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Configuration AAA :

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

Carte de classe et modèle de service IBNS2.0 :

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
```

```
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

Politique de service IBNS 2.0 :

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
```

```
  10 authenticate using mab priority 20
 70 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
!
```

Modèles d'interface :

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

Configuration d'interface :

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Global Obligatoire :

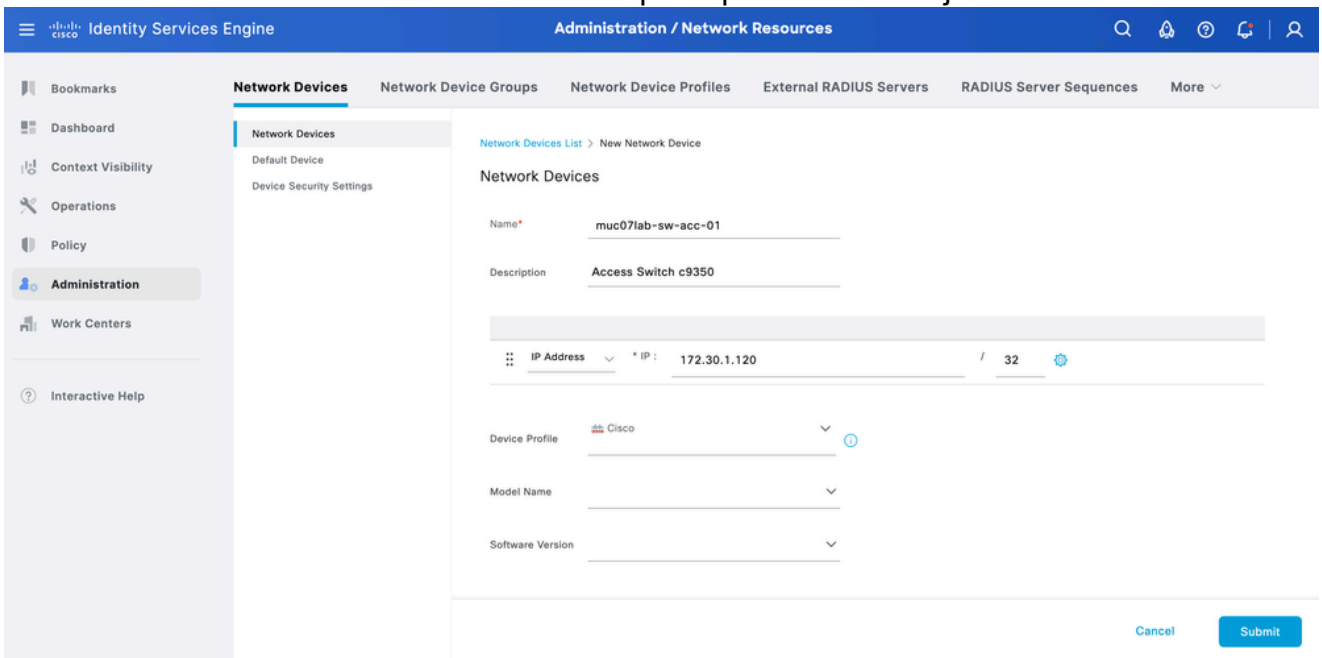
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

Remarque : Lors de l'utilisation d'un CW9178, le point d'accès présente deux adresses MAC pendant l'authentification. Pour empêcher le port de commutation de passer à l'état err-disabled, le port doit d'abord être configuré pour l'authentification multiple en mode hôte. Après une authentification 802.1X réussie, il est recommandé de modifier dynamiquement la configuration du port en mode hôte multi-hôte.

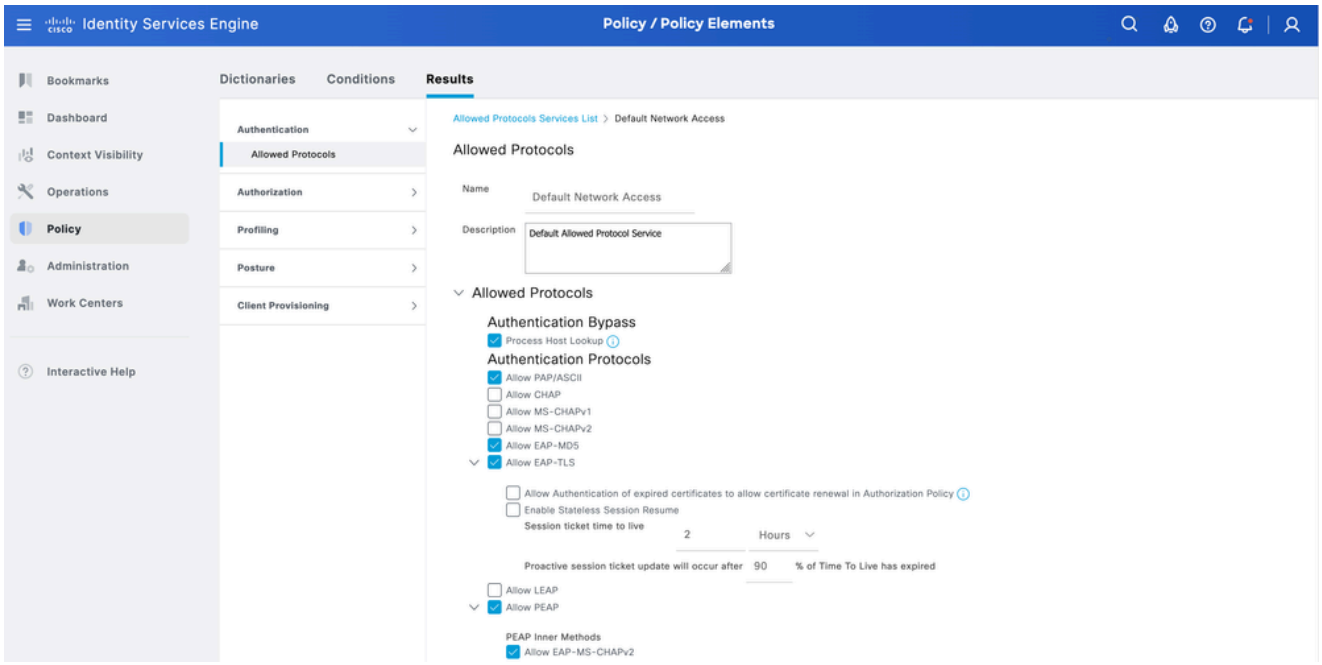
Configuration d'Identity Services Engine

Enfin, le serveur RADIUS doit également être configuré pour autoriser l'authentification. Pour les câbles Dot1x, il existe un de guide complet[5] de sorte que nous nous concentrons uniquement sur les parties pertinentes dans ce cas.

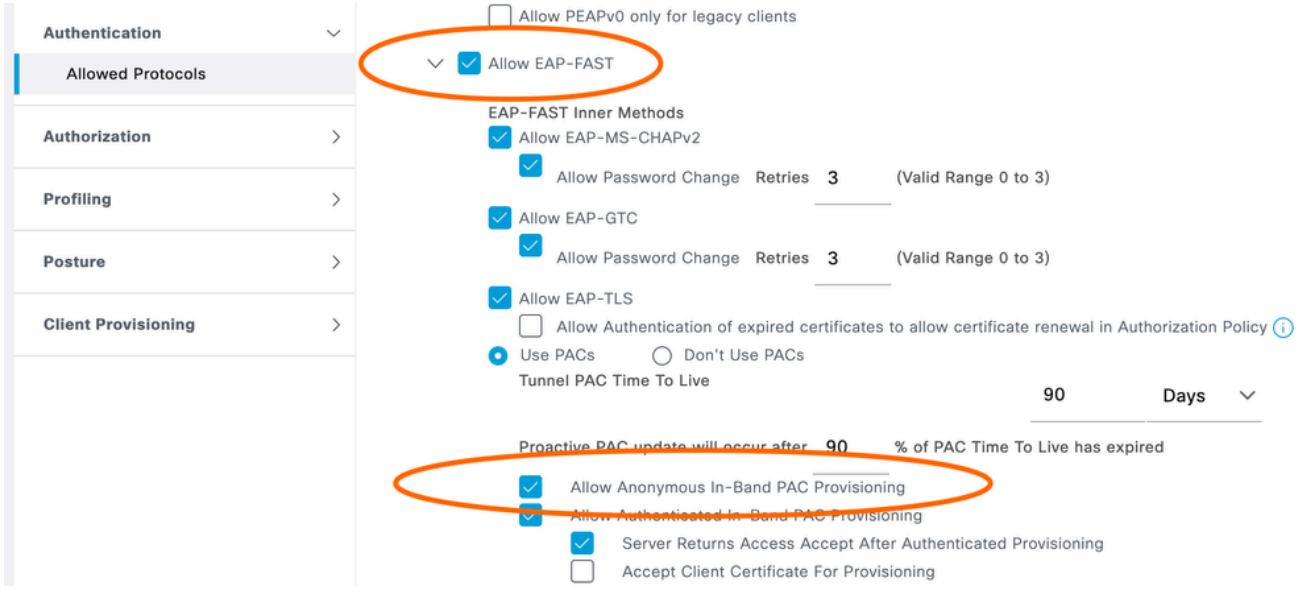
1. Ajoutez le commutateur en tant que périphérique d'accès réseau :
   > Administration > Ressources réseau > Périphériques réseau > Ajouter



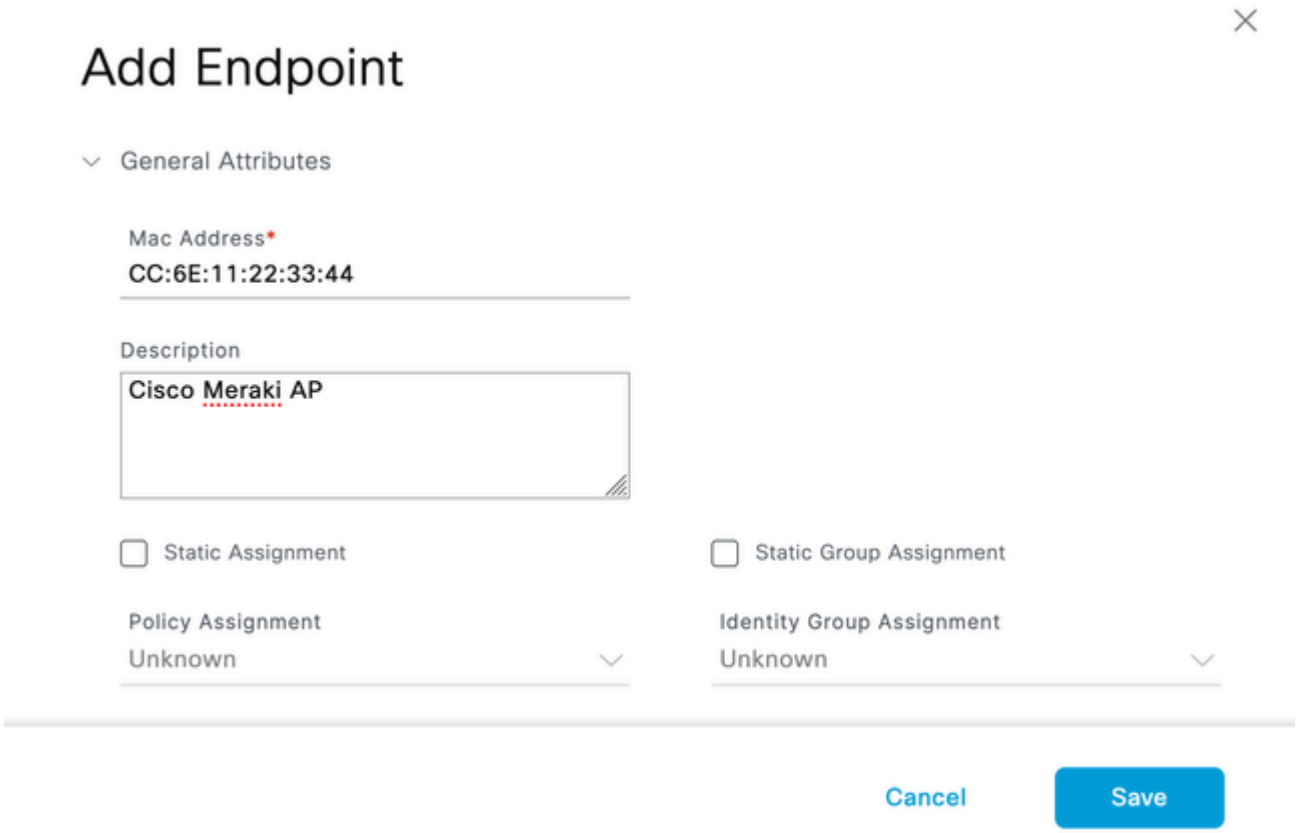
2. Activez le protocole EAP que vous utilisez :
   > Stratégie > Éléments de stratégie > Résultats > Authentification > Protocoles autorisés



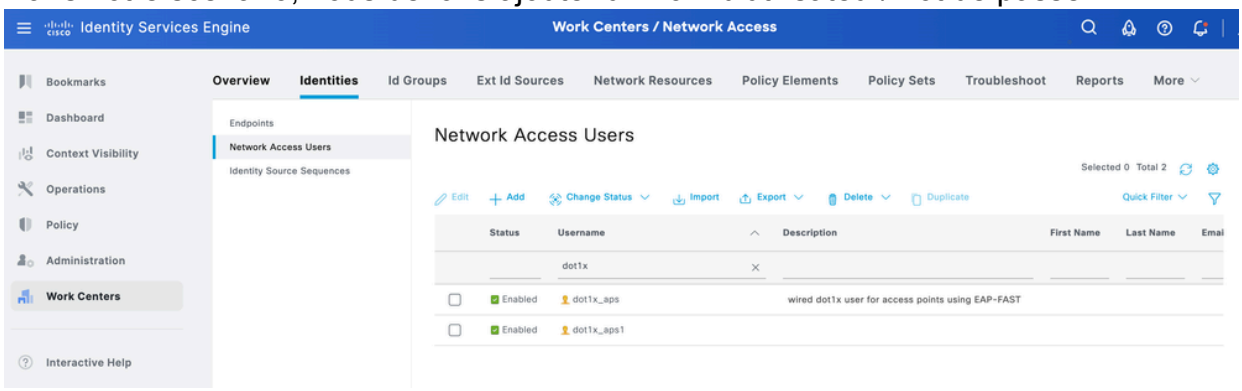
3. Pour notre scénario, comme nous utilisons EAP-FAST, gardez à l'esprit que le « provisionnement PAC intrabande anonyme » doit être activé :



4. Ajouter des identités
   > Centres de travail > Accès réseau > Identités
   a. Pour un fonctionnement réussi, le processus se compose généralement de deux étapes. Initialement, le point d'accès n'a pas d'informations d'identification et ne peut donc pas répondre à l'authentification EAP. Par conséquent, le port de commutateur doit d'abord authentifier le point d'accès à l'aide de MAB. Cela peut être basé sur une politique d'autorisation générique, une politique basée sur l'emplacement ou un profilage de périphérique. Quelle que soit la politique utilisée, l'authentification MAB initiale doit réussir pour permettre au point d'accès d'obtenir ses informations d'identification, soit du WLC via CAPWAP ou de Cisco Catalyst Center via Plug and Play (PnP).



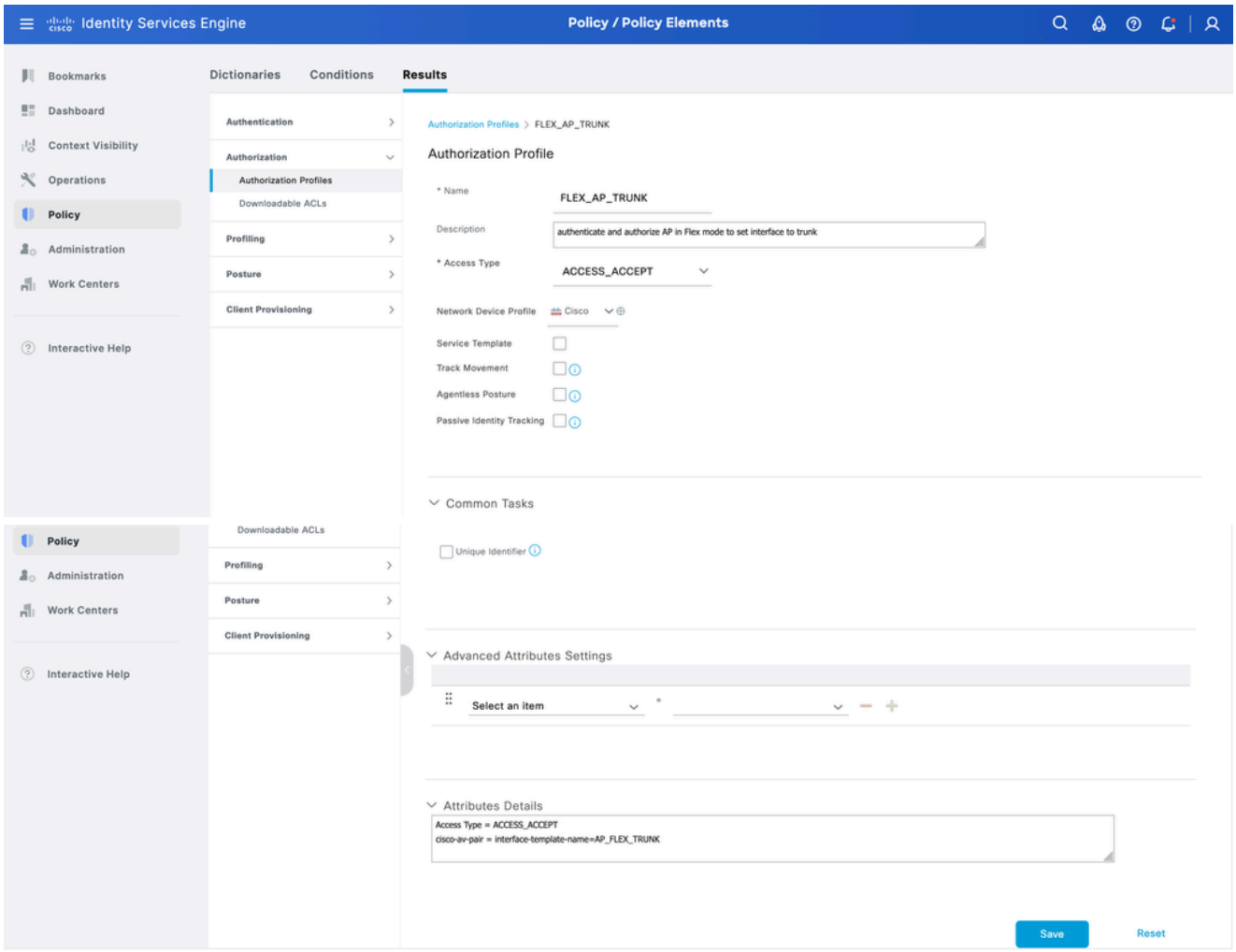
b. Une fois que le point d'accès a collecté les informations d'identification/certificat, le demandeur point d'accès 1X câblé répond à EAPoL et point d'accès 1X est la méthode suivante pour l'authentification permettant au point d'accès d'avoir un accès complet. Dans notre scénario, nous devons ajouter un nom d'utilisateur/mot de passe :



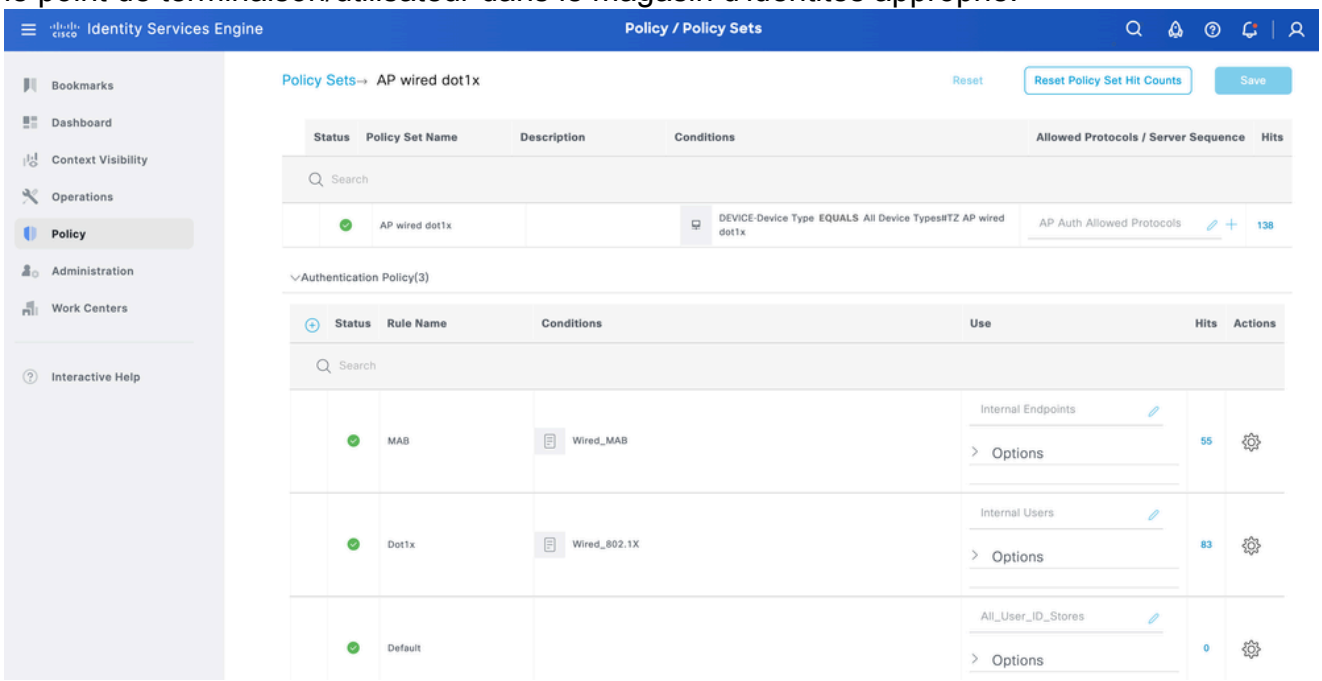
5. Créer un profil d'autorisation

Le profil d'autorisation répond avec la paire av requise. Dans notre cas, comme nous modifions dynamiquement le port de commutation, le modèle d'interface doit être configuré : > Règle > Éléments de règle > Résultats > Autorisation > Profils d'autorisation

Name : FLEX_AP_TRUNK
Type d'accès : ACCESS_ACCEPT
Modèle d'interface : AP_FLEX_TRUNK

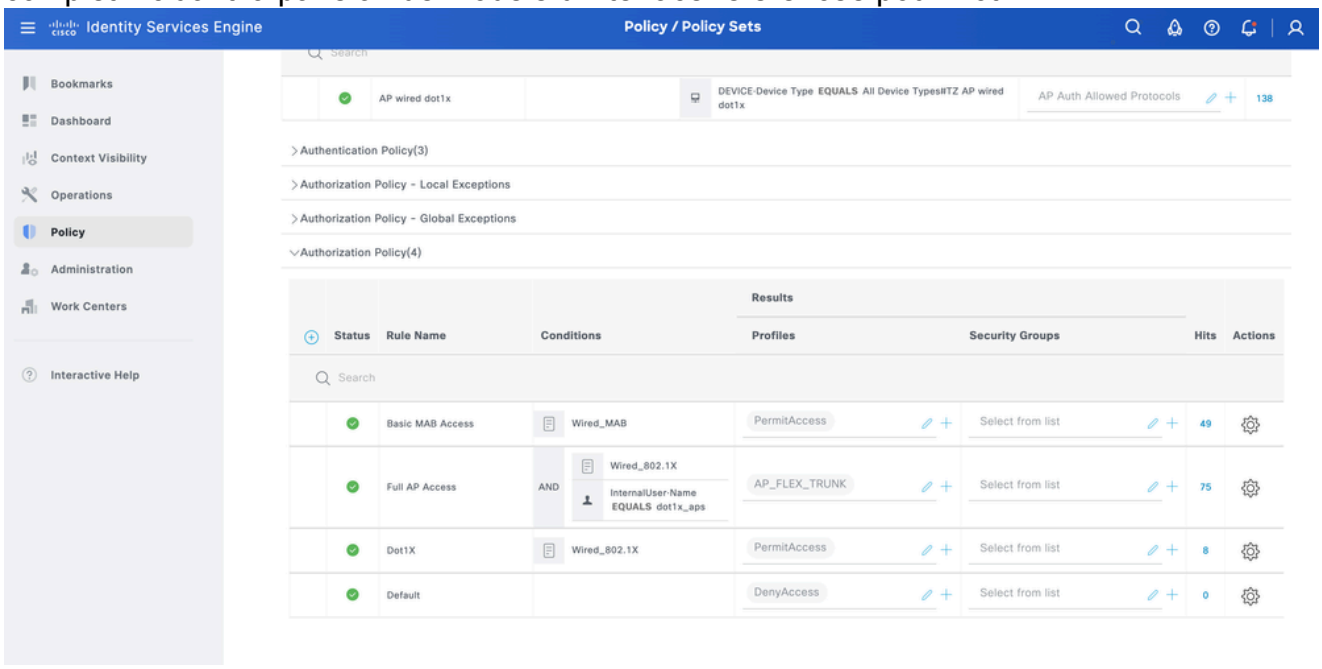


6. Créer une stratégie d'autorisation
   Créez une stratégie d'authentification qui autorise MAB ainsi que Dot1X filaire et recherche le point de terminaison/utilisateur dans le magasin d'identités approprié.



Placez un résultat d'autorisation d'accès limité, selon vos besoins pour MAB, et un accès AP

complet incluant la paire av de modèle d'interface référencée pour Dot1x :



Vérifier

Une fois cette configuration mise en place, connectez le point d'accès au commutateur. Comme condition préalable, il est prévu que les paramètres réseau par défaut, dans notre cas un pool DHCP dans le VLAN d'accès avec l'option 43 pointant vers le WLC et la communication CAPWAP est possible pour l'AP au WLC.

Commandes AP

```
show ap authentication status
show crypto
show crypto pki trustpool
```

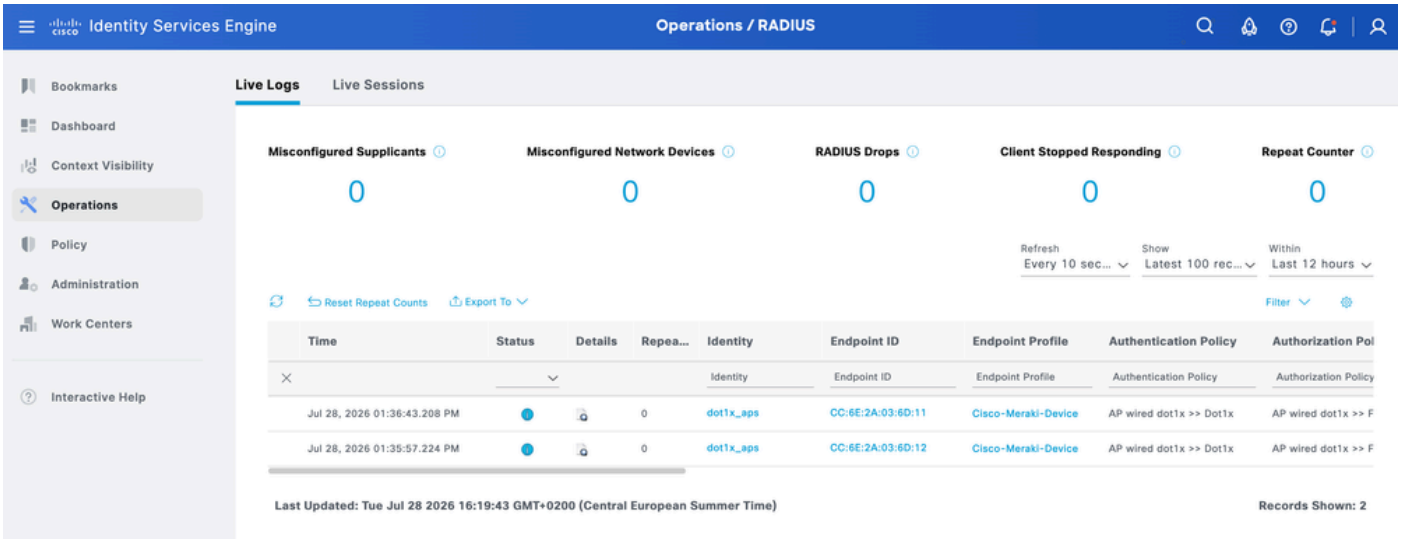
Commandes de commutateur

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
Interface MAC Address Method Domain Status Fg Session ID
```

```
---------------------------------------------------------------------------------------
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



Liste des acronymes

Acronyme	Extension
AAA	authentification, autorisation et administration (aaa)
POINT D'ACCÈS	point d'accès
AuthC	authentification
AuthZ	Autorisation
AC	autorité de certification
CISP	protocole de signalisation d'informations client
Point1x	IEEE 802.1X
PAE	Extensible Authentication Protocol
EST	Inscription sur transport sécurisé
FAST	Authentification flexible via une tunnellisation sécurisée
IBNS	Services réseau basés sur l'identité
ISE	Plateforme de services d’identité
MAB	Contournement d'authentification MAC

NAD	Périphérique d'accès réseau
PEAP	protocole d'authentification extensible protégée
SCEP	Protocole d'inscription de certificat simple
TLS	Sécurité de la couche transport
WLC	Contrôleur LAN sans fil

Références

[1] Configurez 802.1X sur les points d'accès pour PEAP ou EAP-TLS avec LSC

[2] Configurer SCEP pour le provisionnement de certificats significatifs localement sur le WLC 9800

[3] Guide de déploiement sur site de Cisco Wireless EST

[4] Intégration sécurisée des points d'accès - Introduction à la sécurité réseau améliorée

[5] Guide de déploiement normatif ISE Secure Wired Access

[6] Guide de configuration pour LSC

[7] Configurer le demandeur 802.1X pour les points d'accès avec le contrôleur 9800

[8] Sécuriser un port de commutation Flexconnect AP avec Dot1x

[9] Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800, Cisco IOS XE 17.18.x - 802.1x

[11] Guide de l'utilisateur de Cisco Catalyst Center, version 3.2.x - Configuration des paramètres de gestion d'un profil AP pour les périphériques Cisco IOS XE

[12] Utilisation d'IBNS 2.0 et de modèles d'interface pour une configuration de port de commutateur par défaut

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.