Standaardiseer bekabelde 802.1X AP-verificatie met IBNS 2.0- en interfacesjablonen

Inhoud

Inleiding

Dit document beschrijft de 802.1X-configuratie met behulp van IBNS 2.0-interfacesjablonen.

probleemstelling

Het gebruik van IEEE 802.1X voor poortbeveiliging is een gebruikelijke best practice. Naast het verbeteren van de netwerkbeveiliging, vereenvoudigt het ook de implementatie van switch door een gestandaardiseerde toegangspoortconfiguratie in het hele netwerk mogelijk te maken.

In deze handleiding wordt beschreven hoe één gestandaardiseerde switchpoortconfiguratie kan

worden gebruikt voor zowel eindapparaten als Cisco Access Points (AP's). Hoewel elke switchpoort aanvankelijk als een standaard toegangspoort werkt en IEEE 802.1X-verificatie uitvoert, kan een geverifieerd toegangspunt afhankelijk van het implementatiescenario een andere operationele modus vereisen.

Met name AP's die in de lokale switchmodus van FlexConnect werken, moeten op een trunkpoort werken omdat clientverkeer van meerdere SSID's lokaal wordt overbrugd. Als gevolg hiervan moet de switch-interface na een geslaagde verificatie dynamisch overschakelen van een toegangspoort naar een trunkpoort.

Toegangspoorten die infrastructuurapparaten verbinden in plaats van eenvoudige eindapparaten vereisen vaak interfaceconfiguraties die verschillen van het standaardgedrag van de toegangspoort.

Daarom moet de switch-interfaceconfiguratie tijdens het verificatieproces dynamisch worden gewijzigd. In de loop der jaren zijn verschillende benaderingen gebruikt om dit gedrag te bereiken, waaronder Auto SmartPorts en Embedded Event Manager (EEM) -applets. De aanbevolen oplossing is tegenwoordig IBNS 2.0 [1] in combinatie met interfacesjablonen, die een schaalbare en consistente methode bieden voor het dynamisch wijzigen van de interfaceconfiguratie na succesvolle verificatie.

nadering

Voor een goed functionerende setup moeten er verschillende componenten goed geconfigureerd zijn, namelijk

- Radius Server (Identity Service Engine)
- Switch
- Toegangspunt / draadloze LAN-controller

Aangezien er bestaande documentatie bestaat (zie referenties aan het einde), richten we ons in dit document op een bepaald scenario en verwijzen we bestaande documentatie als ondersteunend materiaal.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Draadloze LAN-controller (WLC) en lichte toegangspunten (LAP)
- 802.1x op Cisco-switches en ISE
- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-In User Service (RADIUS)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

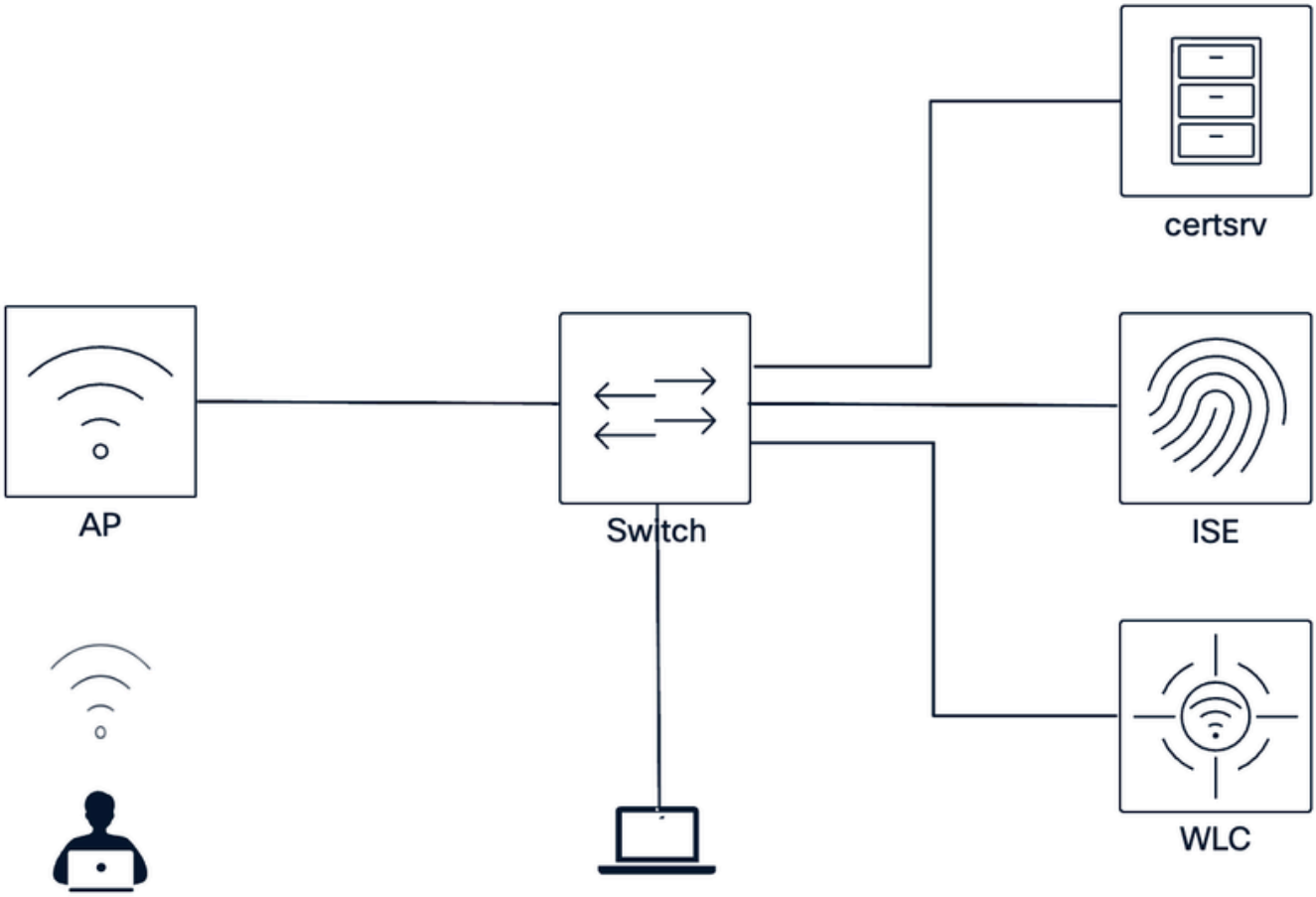
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C9800-40 WLC - IOS XE 26.1.1
- ISE versie 3.5 Patch 1
- AP CW917x, CW916x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie is ook gedocumenteerd in netascode.cisco.com datamodellen voor switching en ISE om de setup eenvoudig te repliceren.

Configuratie

Netwerkdiagram



Voorbeeldinstelling

Voor ons doel richten we ons op één scenario en bieden we configuratiesnippets en stapsgewijze begeleiding. Omdat er onderweg verschillende variaties zijn, wijzen we ze aan en verwijzen we naar bestaande documentatie voor dit doel.

Scenario in deze gids:

- AP-bekabelde Dot1X met EAP-FAST-verificatie
- Dot1X-referenties geleverd via C9800 WLC
- AP in lokale switchmodus voor Flex Connect

In dit ontwerp maakt de switchport in eerste instantie gebruik van een gemeenschappelijke 802.1X-configuratie in gesloten modus met MAB-fallback. Tijdens de eerste onboarding heeft de AP mogelijk nog geen 802.1X-referenties, dus ISE kan de AP autoriseren via MAB met beperkte toegang die voldoende is om het WLC of Catalyst Center te bereiken. Nadat referenties of certificaten zijn verstrekt, voert het toegangspunt bekabelde 802.1X-verificatie uit. ISE retourneert

vervolgens een autorisatieresultaat dat van toepassing is op de AP_FLEX_TRUNK-interfacesjabloon en converteert de poort naar de vereiste FlexConnect-trunkconfiguratie.

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		

Tabel 1: Aanvullende variaties en opties in een overzicht

AP-configuratie

Als u bekabelde Dot1x-verificatie in combinatie met uw toegangspunt wilt gebruiken, moet u eerst referenties en/of certificaten uitrollen, afhankelijk van de geselecteerde verificatiemethode.

Cisco Catalyst AP Dot1x-aanvrager ondersteunt in het algemeen EAP-FAST, EAP-PEAP of EAP-TLS. Daarnaast kan MAB ook een optie zijn, vooral omdat AP's eerst de referenties of certificaten moeten verzamelen om EAP-typeverificatie uit te kunnen voeren.

- MAB:
  - Geen installatie aan AP-zijde vereist
  - Voor het beheren van hardware-MAC-adressen is tooling vereist
  - Kan gemakkelijk worden gespookt
  - Maakt een gemeenschappelijke poortconfiguratie mogelijk

- EAP-FAST:
  - Op gebruikersnaam/wachtwoord gebaseerd
  - Eenvoudig uit te rollen
  - Vereist anonieme in-band PAC-provisioning ingeschakeld op ISE

- EAP-PEAP:
  - Op gebruikersnaam/wachtwoord gebaseerd

    - Vereist certificaten voor servervalidatie
    - Verlenging van certificaten moet dienovereenkomstig worden gepland

- EAP-TLS:
    - Op certificaat gebaseerd
    - Verlenging van certificaten moet dienovereenkomstig worden gepland

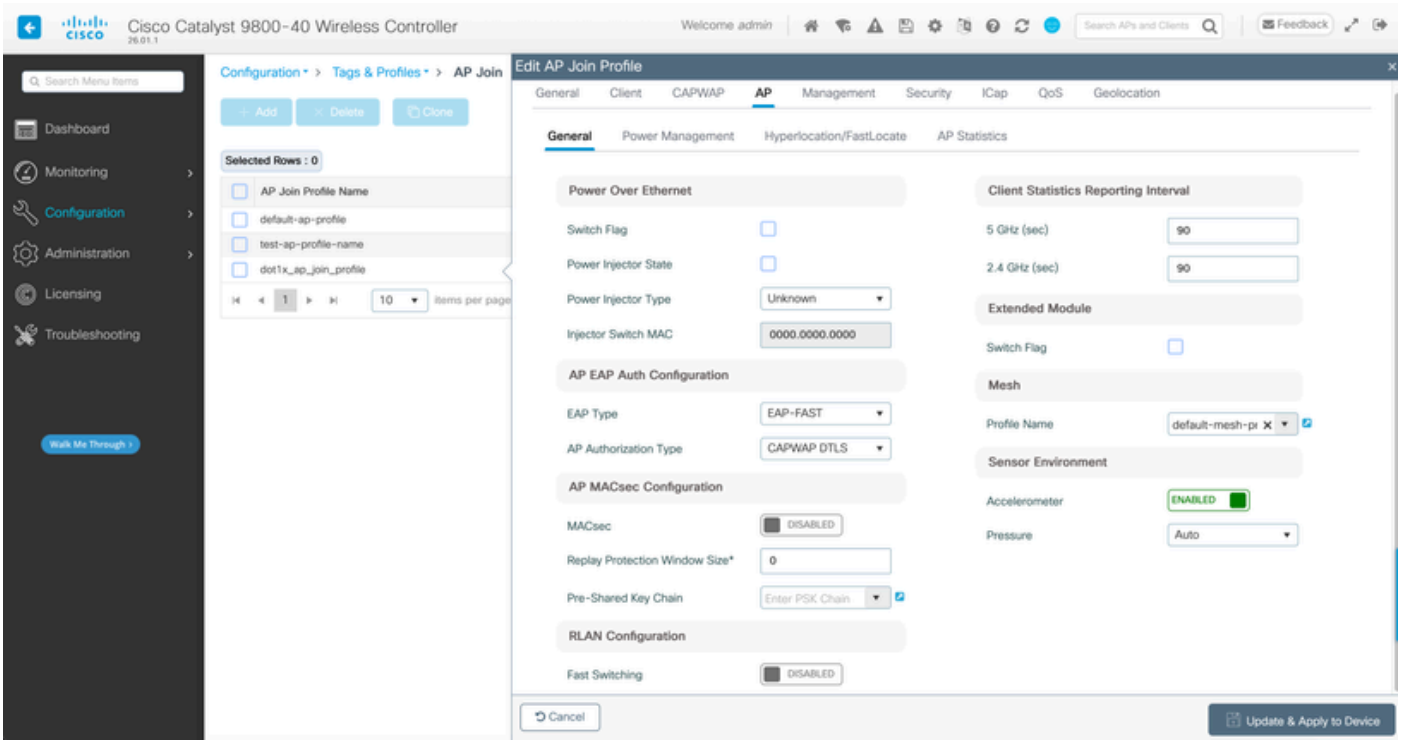
Voor het configureren van de bedrade AP Dot1X-supplicant zijn er twee benaderingen hiervoor, hetzij via de Wireless LAN Controller of Catalyst Center, die hier worden beschreven. Voordat u op deze details ingaat, moet het type verificatie dat u gaat gebruiken vooraf worden geselecteerd.

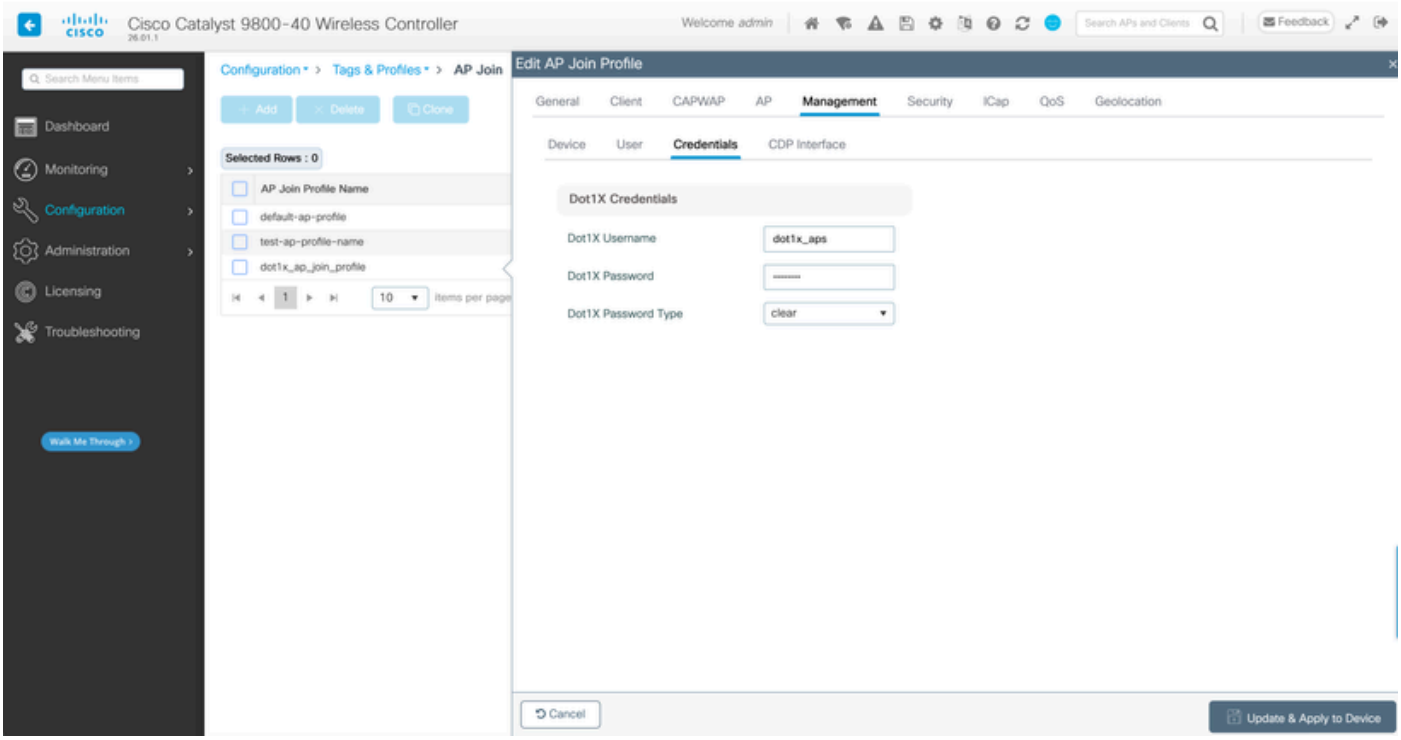
Dot1X via Cisco 9800 Wireless LAN-controller bekabeld installeren

Als u een certificaatgebaseerde verificatie (EAP-PEAP of EAP-TLS [1]) hebt geselecteerd, moet u als volgende stap beslissen over de aanpak voor de manier waarop u van plan bent lokaal significante AP-certificaten (LSC) uit te geven, hetzij via SCEP [2] of EST [3].

Wanneer u EAP-FAST gebruikt, zoals in ons scenario, volstaat het om een AP-join-profiel te genereren, waarbij u de Dot1X-gebruiker en het wachtwoord invoert, dat Join-profiel aan een Site-Tag bindt en aan de AP's toewijst.

GUI-configuratie





CLI-configuratie

```
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>
```

Dot1X via Catalyst Center Plug and Play instellen

Om PnP [4] te laten werken, moet het Catalyst Center worden geïntegreerd met ISE. Dit is gedeeltelijk vereist vanwege de certificaten die vereist zijn om servervalidatie vanaf de AP-zijde te kunnen uitvoeren voor EAP-verificatie met ISE. Voor het certificaat aan de apparaatzijde krijgen toegangspunten een certificaat dat is uitgegeven door Catalyst Center CA en dat standaard is ingebouwd of is geconfigureerd door een SubCA / SCEP van de betreffende CA.

Het installatieproces via PnP maakt het mogelijk om certificaten en/of referenties te leveren voordat het apparaat zich aansluit bij de WLC's.

Switchconfiguratie

Naast dat de authenticatie een beveiligingsmechanisme is, is het ook een manier om

switchpoortconfiguraties te standaardiseren. Daarom beschrijven deze delen de elementen die nodig zijn om dit te bereiken. Dit is een voorbeeldconfiguratie en moet worden beoordeeld en aangepast aan uw installatie. In het algemeen maakt deze configuratie Dot1x en fallback MAB mogelijk met de juiste afhandeling van dode Radius-scenario's, herverificatie enzovoort.

Global Radius Attributen:

```
!
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>
!
```

Radius-servergroep:

```
!
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>
!
```

AAA-configuratie:

```
!
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>
```

```
!
```

IBNS2.0 Klasse-kaart en servicesjabloon:

```
!
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
!
```

Servicebeleid 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
!
```

Interfacesjablonen:

```
!
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
!
```

Interface-configuratie:

```
!
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
!
```

Globaal Verplicht:

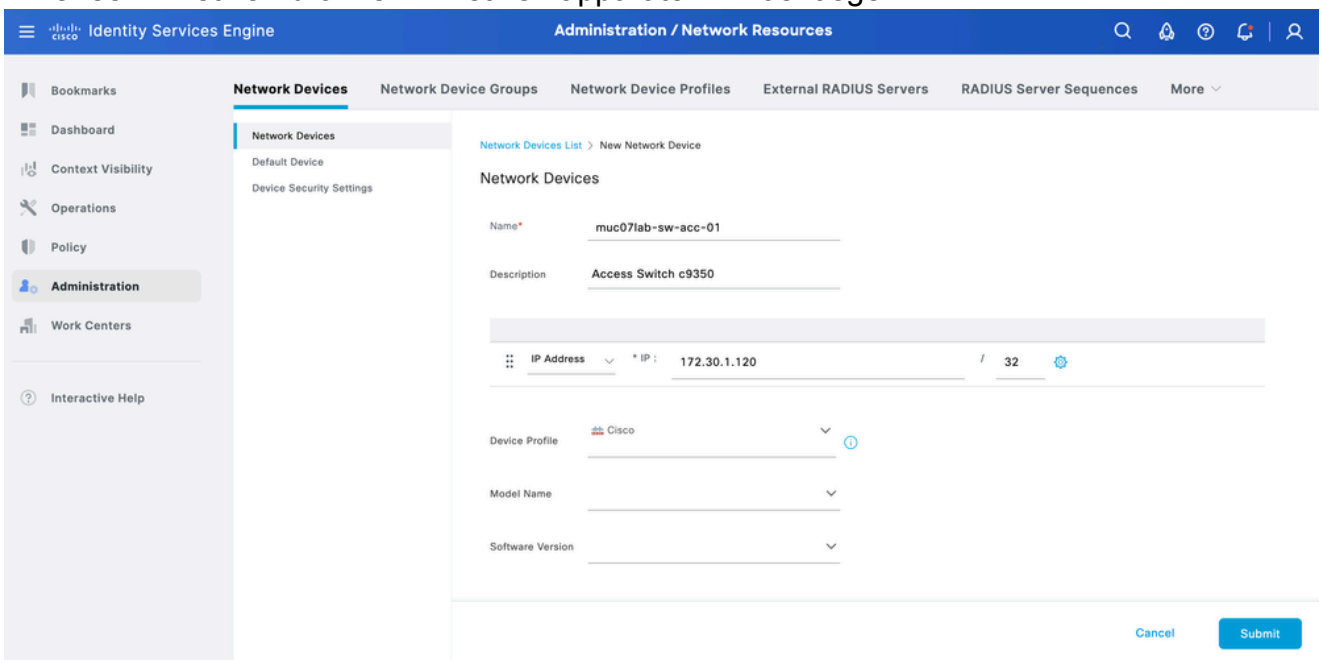
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

Opmerking: wanneer u een CW9178 gebruikt, worden er twee MAC-adressen weergegeven tijdens de verificatie. Om te voorkomen dat de switchpoort de status foutloos invoert, moet de poort in eerste instantie worden geconfigureerd voor multi-auth in hostmodus. Na succesvolle 802.1X-verificatie wordt aanbevolen om de poortconfiguratie dynamisch te wijzigen in hostmodus met meerdere hosts.

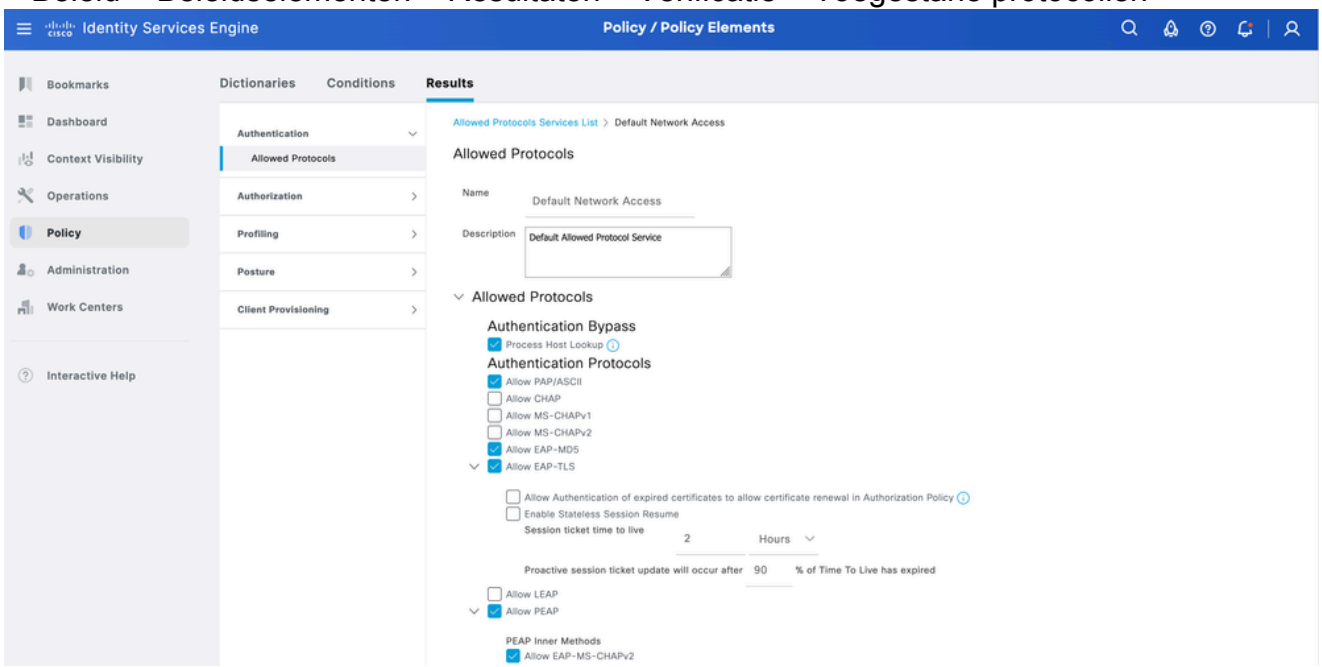
Configuratie van Identity Services-engine

Ten slotte moet ook de RADIUS-server worden geconfigureerd om verificatie mogelijk te maken. Voor bekabelde Dot1x is er een uitgebreide gids [5] dus we richten ons in dit geval alleen op de relevante onderdelen.

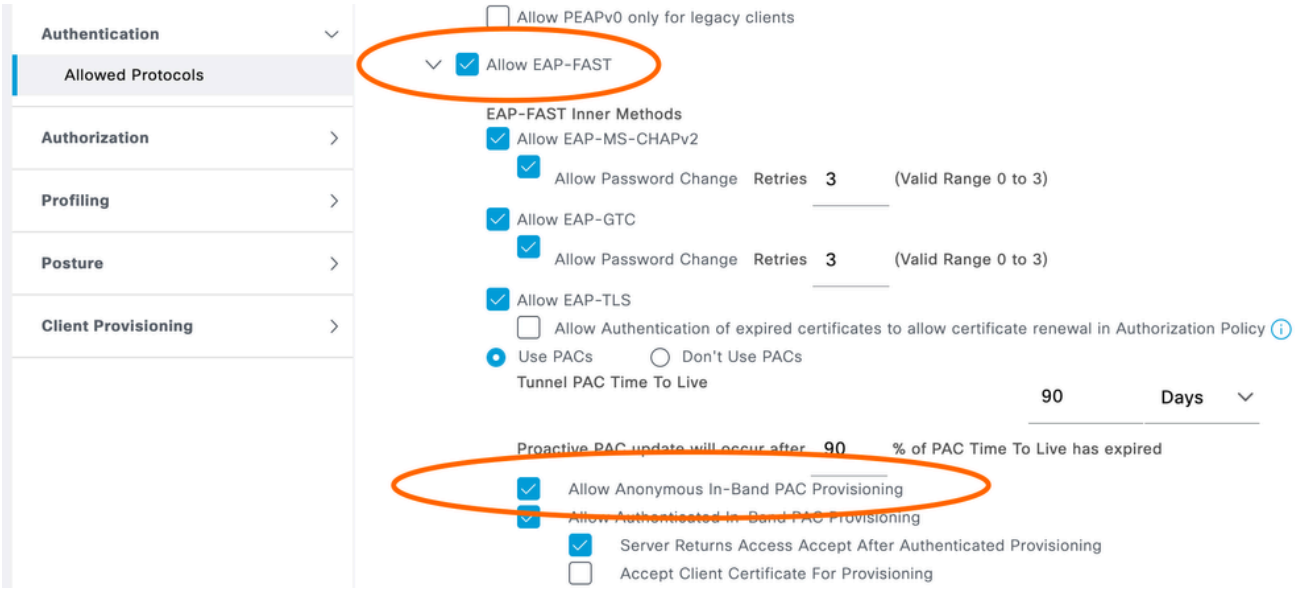
1. De switch als netwerktoegangsapparaat toevoegen:
   > Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen



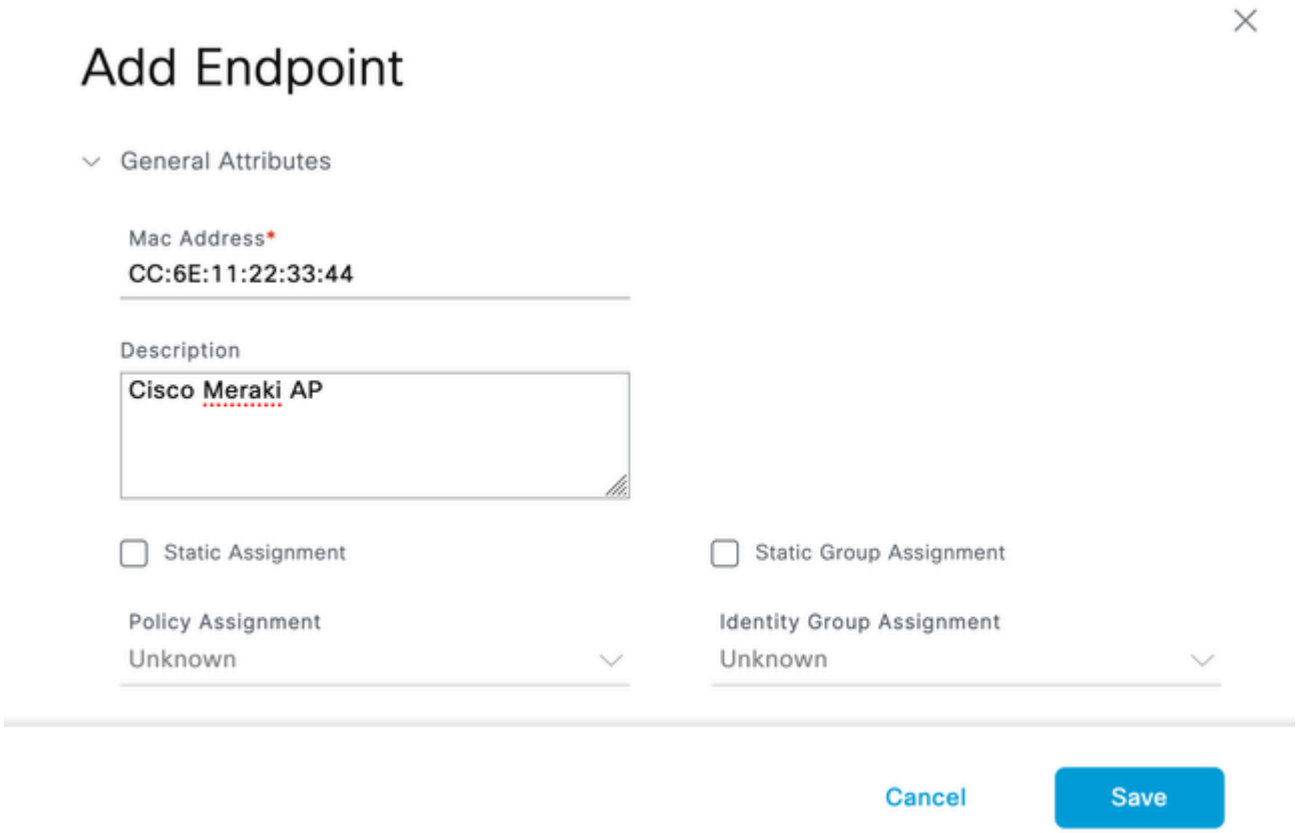
2. Schakel het EAP-protocol in dat u gebruikt:
   > Beleid > Beleidselementen > Resultaten > Verificatie > Toegestane protocollen



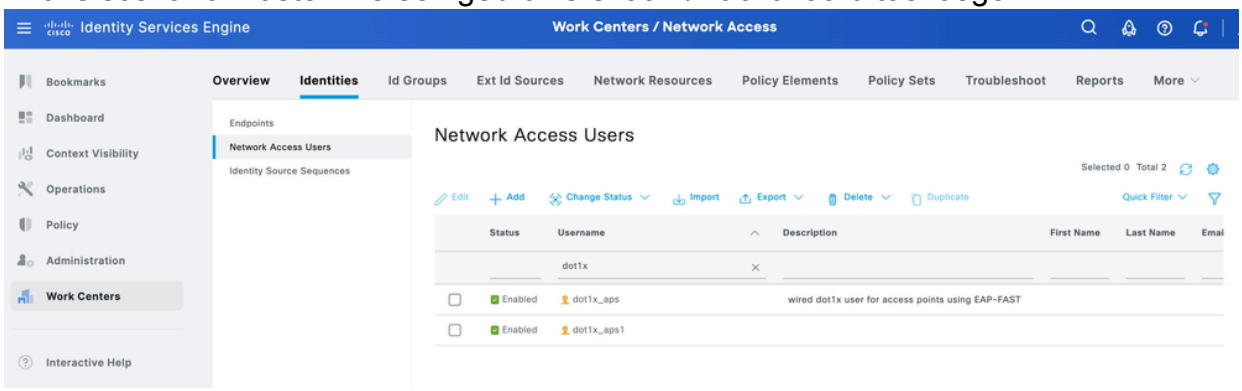
3. Houd er voor ons scenario, aangezien we EAP-FAST gebruiken, rekening mee dat "Anonieme In-band PAC Provisioning" moet worden ingeschakeld:



4. Identiteiten toevoegen
   > Werkcentra > Netwerktoegang > Identiteiten
   a. Voor een succesvolle werking bestaat het proces meestal uit twee stappen. In eerste instantie heeft het toegangspunt geen referenties en kan het daarom niet reageren op EAP-verificatie. Als gevolg hiervan moet de switch-poort eerst het toegangspunt verifiëren met behulp van MAB. Dit kan gebaseerd zijn op een algemeen autorisatiebeleid, een locatiegebaseerd beleid of apparaatprofilering. Ongeacht het gebruikte beleid, moet de eerste MAB-verificatie slagen om het toegangspunt in staat te stellen zijn referenties te verkrijgen, hetzij van de WLC via CAPWAP of van Cisco Catalyst Center via Plug and Play (PnP).

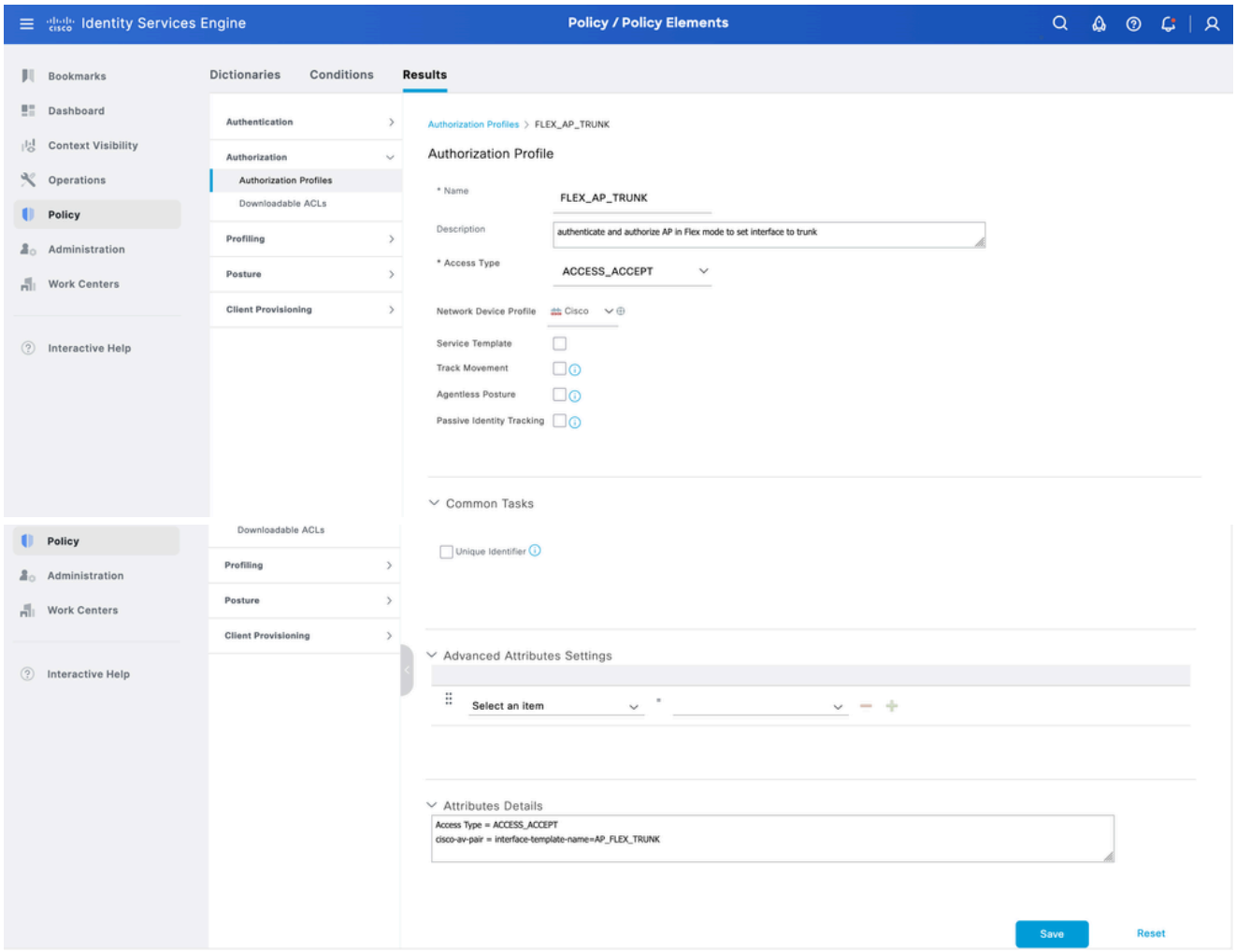


b. Nadat het toegangspunt de referenties/het certificaat heeft verzameld, reageert de AP-bedrade Dot1X-aanvrager op EAPoL en is Dot1X de daaropvolgende methode voor verificatie waarmee het toegangspunt volledige toegang krijgt.
In ons scenario moeten we een gebruikersnaam/wachtwoord toevoegen:



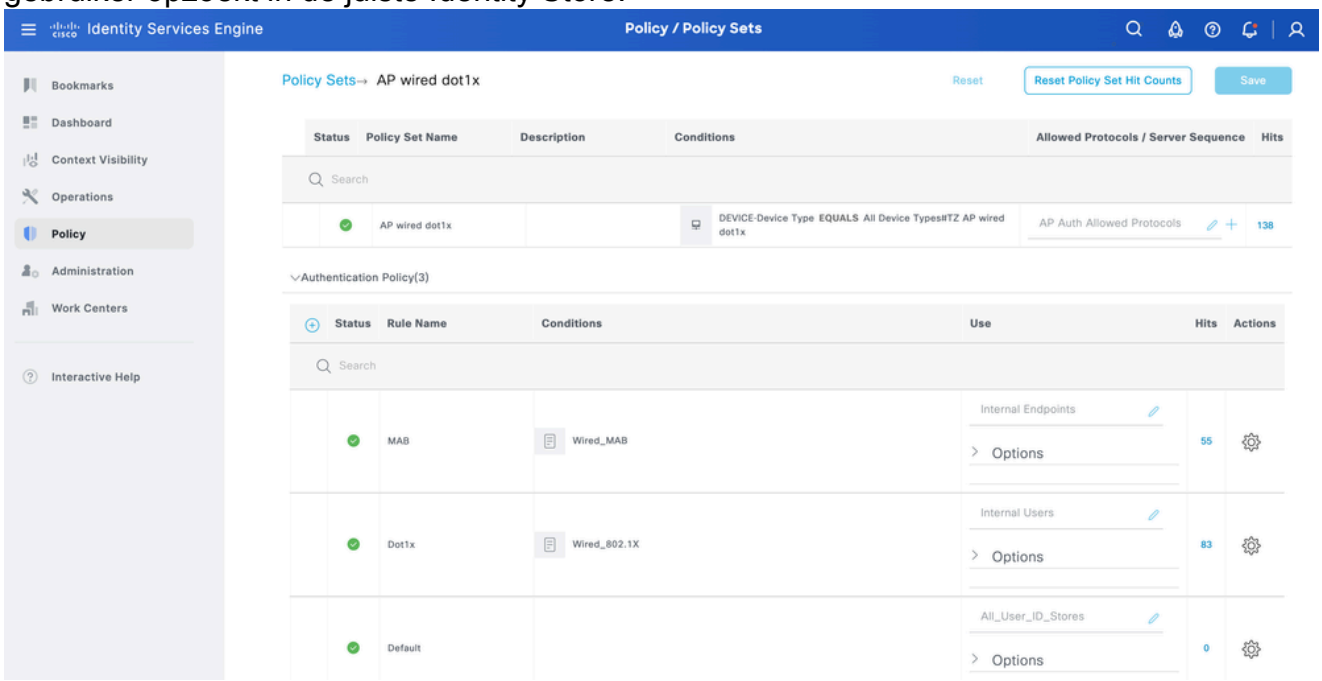
5. Autorisatieprofiel maken
Het autorisatieprofiel reageert met het vereiste av-paar. In ons geval, omdat we de switchport dynamisch wijzigen, moet de interface-sjabloon worden geconfigureerd:
> Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen

Naam: FLEX_AP_TRUNK
Toegangstype: ACCESS_ACCEPT
Interfacesjabloon: AP_FLEX_TRUNK



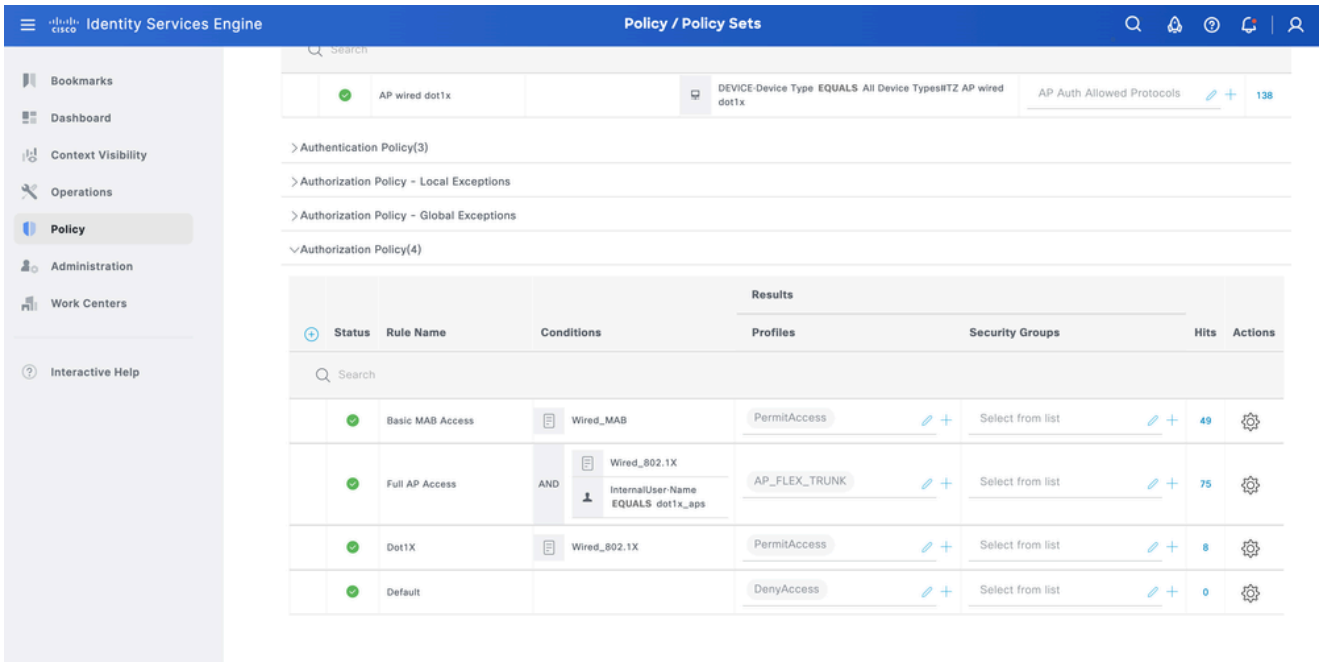
6. Autorisatiebeleid maken

   Maak een verificatiebeleid dat zowel MAB als bekabelde Dot1X toestaat en het eindpunt/de gebruiker opzoekt in de juiste Identity Store.



   Plaats een beperkt toegangsautorisatieresultaat, afhankelijk van uw behoeften voor MAB, en

een volledig toegangspunt inclusief het waarnaar wordt verwezen interface-sjabloon av-paar voor Dot1x:



Verifiëren

Als deze configuratie is geïnstalleerd, sluit u het toegangspunt aan op de switch. Als voorwaarde wordt verwacht dat de standaard netwerkinstellingen, in ons geval een DHCP-pool in het Access VLAN met optie 43 die naar de WLC en CAPWAP-communicatie wijst, mogelijk zijn voor het toegangspunt naar de WLC.

AP-opdrachten

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

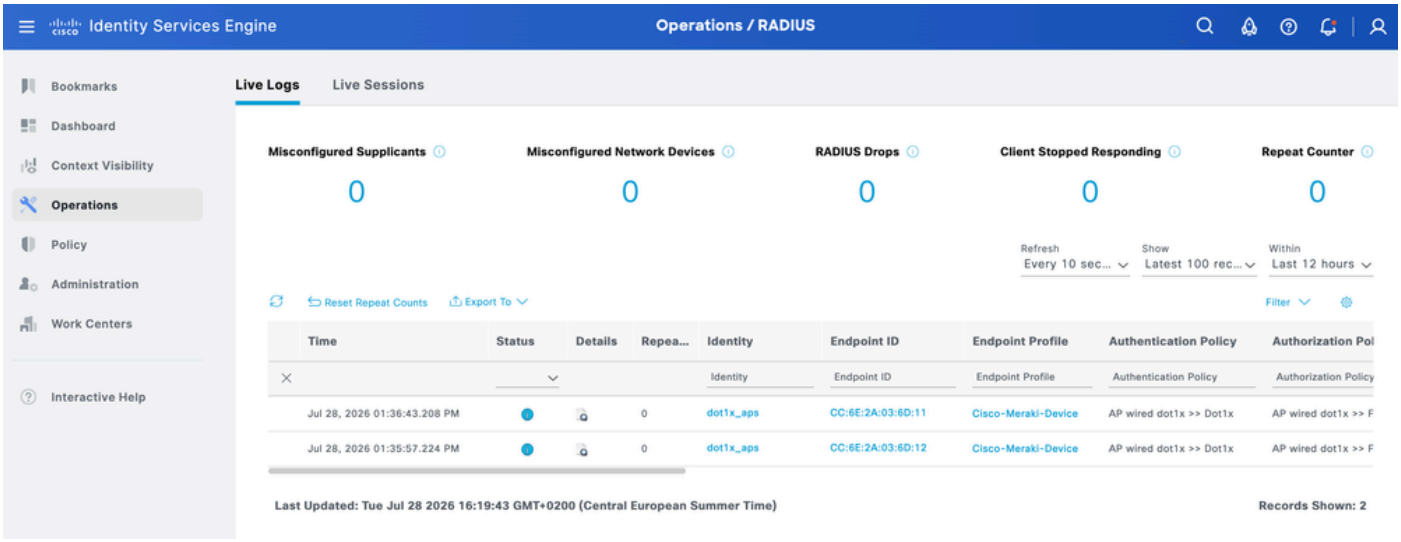
Switch-opdrachten

```
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



Lijst van acroniemen

acroniem	expansie
AAA	Verificatie, autorisatie en accounting
AP	access point
AuthC	verificatie
AuthZ	Authorization
CA	certificeringsinstantie
CISP	Client Information Signaling Protocol
Dot1x	IEEE 802.1X
EAP	Extensible Authentication Protocol
EST	Inschrijving via Veilig transport
SNEL	Flexibele verificatie via beveiligde tunneling
IBNS	Identiteitsgebaseerde netwerkservices
ISE	Identity Services-engine
MAB	MAC-verificatiebypass
NAD	netwerktoegangsapparaat

PEAP	Protected Extensible Authentication Protocol
SCEP	Simple Certificate Enrollment Protocol
TLS	beveiliging van transportlaag
WLC	Draadloze LAN-controller

Referenties

[1] 802.1X configureren op AP's voor PEAP of EAP-TLS met LSC

[2] SCEP configureren voor lokaal significante certificaatprovisioning op 9800 WLC

[3] Cisco Wireless EST On-Prem Deployment Guide

[4] Secure AP onboarding - Een introductie tot verbeterde netwerkbeveiliging

[5] ISE Secure Wired Access Prescriptive Deployment Guide

[6] Config Guide-sectie voor LSC

[7] 802.1X-leverancier configureren voor toegangspunten met 9800-controller

[8] een Flexconnect AP-switchport beveiligen met Dot1x

[9] Cisco Catalyst 9800-reeks Configuratiegids voor draadloze controllers, Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Center User Guide, versie 3.2.x - Beheerinstellingen configureren voor een AP-profiel voor Cisco IOS XE-apparaten

[12] IBNS 2.0 en interfacesjablonen gebruiken voor een standaardconfiguratie van de switchport

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.