

Configureer 802.1X-applicatie voor access points met 9800 controller

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[De LAP configureren als een 802.1x-supPLICANT](#)

[Als het toegangspunt al is aangesloten op de WLC:](#)

[Als het toegangspunt nog geen lid is van een WLC:](#)

[De Switch configureren](#)

[De ISE-server configureren](#)

[Verifiëren](#)

[Controleer het verificatietype](#)

[Controleer 802.1x op de Switch-poort](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u een Cisco Access Point (AP) kunt configureren als een 802.1x-aanvrager die moet worden geautoriseerd op een switchpoort tegen een RADIUS-server.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Draadloze LAN-controller (WLC) en LAP (lichtgewicht access point).
- 802.1x op Cisco-switches en ISE-lijnkaart
- Uitbreidbaar verificatieprotocol (EAP)
- Remote Verificatie-inbelgebruikersservice (RADIUS)

Gebruikte componenten

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

- WS-C3560CX, Cisco IOS® XE, 15.2(3r)E2

- C980-CL-K9, Cisco IOS® XE, 17.6.1
- ISE-lijnkaart 3,0
- LUCHTKAP3702
- AIR-AP3802 router

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.

Achtergrondinformatie

In deze configuratie fungeert het toegangspunt als de 802.1x-aanvrager en wordt het door de switch geverifieerd aan de hand van de ISE-methode EAP-FAST.

Zodra de poort is geconfigureerd voor 802.1X-verificatie, staat de switch geen ander verkeer dan 802.1X-verkeer toe om door de poort te gaan totdat het apparaat dat is aangesloten op de poort met succes wordt geverifieerd.

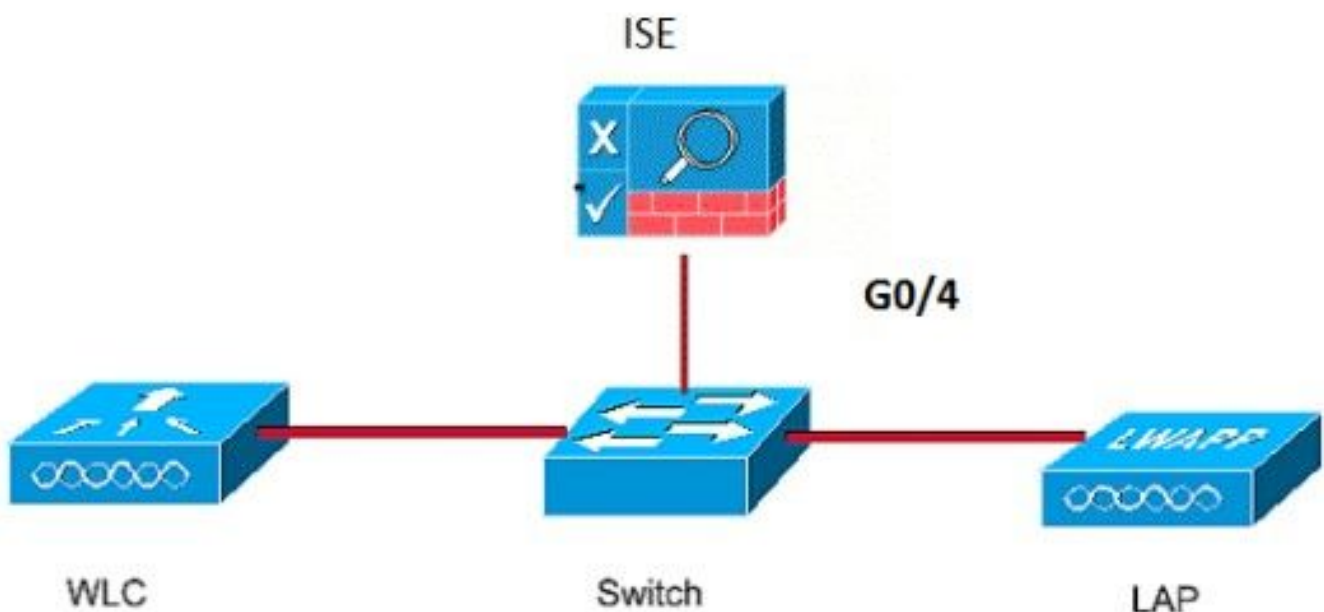
Een AP kan worden geverifieerd of voordat het zich aansluit bij een WLC of nadat het zich heeft aangesloten bij een WLC, in welk geval u 802.1X configureert op de switch nadat de LAP zich aansluit bij de WLC.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:

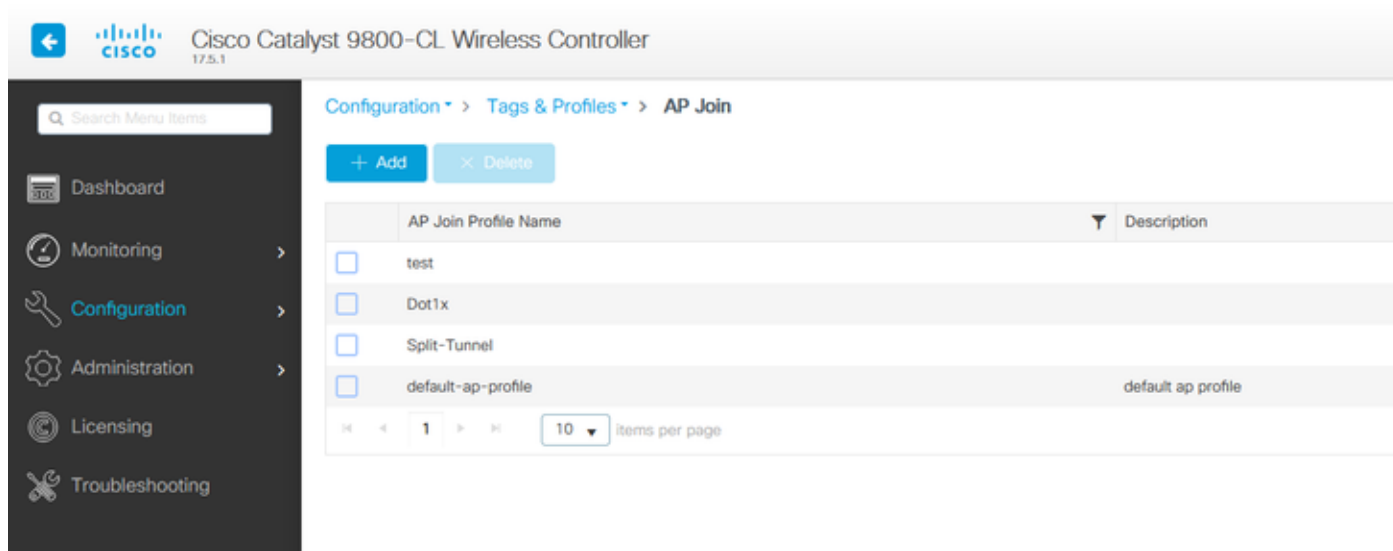


De LAP configureren als een 802.1x-supplicant

Als het toegangspunt al is aangesloten op de WLC:

Configureer het 802.1x-verificatietype en het LSC-verificatietype (Local Significant Certificate):

Stap 1. Navigeer naar Configuratie > **Tags en profielen** > **AP Join** > Op de **AP Join Profile** pagina, klik op **Add** om een nieuw Join Profile toe te voegen of een AP Join Profile te bewerken wanneer u op de naam ervan klikt.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > AP Join. There are '+ Add' and 'X Delete' buttons. A table lists AP Join Profiles:

| | AP Join Profile Name | Description |
|--------------------------|----------------------|--------------------|
| <input type="checkbox"/> | test | |
| <input type="checkbox"/> | Dot1x | |
| <input type="checkbox"/> | Split-Tunnel | |
| <input type="checkbox"/> | default-ap-profile | default ap profile |

At the bottom of the table, there is a pagination control showing '1' items per page and a dropdown menu set to '10' items per page.

Stap 2. Ga op de pagina Profiel samenvoegen met AP, van **AP > General**, naar het gedeelte **AP EAP Auth Configuration**. Selecteer in de vervolgkeuzelijst **EAP-type** het EAP-type als EAP-FAST, EAP-TLS of EAP-PEAP om het verificatietype dot1x te configureren.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

AP EAP Auth Configuration

EAP Type

AP Authorization Type

- EAP-FAST
- EAP-TLS
- EAP-PEAP

Extended Module

Enable

Mesh

Profile Name [Clear](#)

Stap 3. Kies in de vervolgkeuzelijst **Type autorisatie** het type als CAPWAP DTLS + of CAPWAP DTLS > Klik op **Bijwerken en toepassen op apparaat**.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

AP EAP Auth Configuration

EAP Type

AP Authorization Type

- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

Extended Module

Enable

Mesh

Profile Name [Clear](#)

De gebruikersnaam en het wachtwoord voor 802.1x configureren:

Stap 1. Van **Beheer > Credentials > Gebruikersnaam en wachtwoordgegevens voor Dot1x invoeren** > Kies het juiste 802.1x-wachtwoordtype > Klik op **Bijwerken en toepassen op apparaat**

Edit AP Join Profile ✕

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

Dot1x Credentials

| | |
|---------------------|---|
| Dot1x Username | <input type="text" value="Dot1x"/> |
| Dot1x Password | <input type="password" value="••••••••"/> |
| Dot1x Password Type | <input type="text" value="clear"/> |

Als het toegangspunt nog geen lid is van een WLC:

U moet in de LAP console om de referenties in te stellen en deze CLI-opdrachten te gebruiken:
(voor Cheetah OS en Cisco IOS® APs)

CLI:

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

De Dot1x-referenties op het toegangspunt wissen (indien nodig)

Voor Cisco IOS® APs, na dat herladen AP:

CLI:

```
LAP# clear capwap ap dot1x
```

Na het herladen van de AP van Cisco COS:

CLI:

```
LAP# capwap ap dot1x disable
```

De Switch configureren

Schakel dot1x op de switch wereldwijd in en voeg de ISE-server aan de switch toe.

CLI:

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

Configureer de AP switch poort.

CLI:

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

Als AP in **Flex Connect-modus** is, **lokale switching**, dan moet een extra configuratie gemaakt worden op de switch-interface om meerdere MAC-adressen op de poort toe te staan, aangezien het client-verkeer op AP-niveau wordt vrijgegeven:

```
authentication host-mode multi-host
```

Opmerking: betekent dat de lezer er notitie van neemt. De opmerkingen bevatten nuttige suggesties of verwijzingen naar materiaal dat niet in het document is opgenomen.

Opmerking: Multi-host mode-authenticeert het eerste MAC-adres en staat vervolgens een onbeperkt aantal andere MAC-adressen toe. Schakel de hostmodus in op de switch-poorten als het aangesloten AP is geconfigureerd met de lokale switchingmodus. Het laat het verkeer van de klant de switch haven overgaan. Als u een beveiligd verkeerspad wilt, dient u dot1x op het WLAN in te schakelen om de clientgegevens te beschermen

De ISE-server configureren

Stap 1. Voeg de switch toe als netwerkapparaat op de ISE-server. Navigeren naar **Beheer > Netwerkbronnen > Netwerkapparaten** > Klik op **Add** > Voer de naam van het apparaat in, IP-adres in, geef RADIUS-verificatie-instellingen op, specificeer de gedeelde geheime waarde, de Cacao-poort (of laat deze als standaard) > **Submit**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - Network Resources'. The left sidebar has 'Network Devices' highlighted. The main content area is titled 'Network Devices List > New Network Device'. The form includes the following fields and options:

- Name:** MySwitch
- Description:** (empty)
- IP Address:** 10.48.39.100 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:** (empty)
- Location:** All Locations (with 'Set To Default' button)
- IPSEC:** Is IPSEC Device (with 'Set To Default' button)
- Device Type:** All Device Types (with 'Set To Default' button)
- RADIUS Authentication Settings:** (checked, with 'Set To Default' button)
- RADIUS UDP Settings:**
 - Protocol:** RADIUS
 - Shared Secret:** (masked, with 'Show' button)
 - Use Second Shared Secret:** (checkbox, unchecked, with 'Show' button)
 - CoA Port:** 1700 (with 'Set To Default' button)
- RADIUS DTLS Settings:**
 - DTLS Required:** (checkbox, unchecked, with 'Show' button)
 - Shared Secret:** radius/dtls (with 'Show' button)

Stap 2. Voeg de referenties van het toegangspunt toe aan ISE. Navigeer naar **Beheer > Identity Management > Identiteiten > Gebruikers** en klik op de knop **Add** om een gebruiker toe te voegen. U moet hier de referenties invoeren die u hebt ingesteld op uw AP Join Profile op uw WLC. Merk op dat de gebruiker hier in de standaardgroep wordt gezet maar dit kan worden aangepast volgens uw vereisten.

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

Network Access User

* Name dot1x

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

* Login Password Generate Password

Enable Password Generate Password

User Information

Account Options

Account Disable Policy

User Groups

ALL_ACCOUNTS (default)

Stap 3. Configureer op ISE het **verificatiebeleid** en het **autorisatiebeleid**. Ga naar **Beleid > Beleidssets** en selecteer de beleidsset die u wilt configureren en de blauwe pijl rechts. In dit geval wordt de standaardbeleidsset gebruikt, maar men kan deze aanpassen aan de eisen.

Cisco ISE Policy - Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|-------------------------------------|-----------------|--------------------|------------|-------------------------------------|------|---------|------|
| <input checked="" type="checkbox"/> | Default | Default policy set | | Default Network Access | 6 | | |

Reset Save

Configureer vervolgens het **verificatiebeleid** en het **autorisatiebeleid**. De hier getoonde beleidsregels zijn de standaardbeleidsregels die op de ISE-server zijn gemaakt, maar kunnen worden aangepast en aangepast aan uw wensen. In dit voorbeeld kan de configuratie vertaald worden in: "Als 802.1X-bekabeld wordt gebruikt en de gebruiker bekend is op de ISE-server, dan verlenen we toegang tot de gebruikers waarvoor de verificatie succesvol was". Het toegangspunt wordt vervolgens geautoriseerd via de ISE-server.

Authentication Policy (3)

| Status | Rule Name | Conditions | Use | Hits | Actions |
|--------|-----------|---------------------------------------|---------------------------------|------|---------|
| ● | MAB | OR Wired_MAB Wireless_MAB | Internal Endpoints > Options | 0 | ⚙️ |
| ● | Dot1X | OR Wired_802.1X Wireless_802.1X | All_User_ID_Stores > Options | 6 | ⚙️ |
| ● | Default | | All_User_ID_Stores > Options | 0 | ⚙️ |

Authorization Policy (12)

| Status | Rule Name | Conditions | Profiles | Security Groups | Hits | Actions |
|--------|----------------------------|--------------------------------------|----------------|------------------|------|---------|
| ● | Basic_Authenticated_Access | Network_Access_Authentication_Passed | PermitAccess x | Select from list | 6 | ⚙️ |
| ● | Default | | DenyAccess x | Select from list | 0 | ⚙️ |

Stap 4. Zorg ervoor dat in de toegestane protocollen die standaard netwerktoegang, EAP-FAST is toegestaan. Ga naar **Beleid > Beleidselementen > Verificatie > Resultaten > Toegestane protocollen > Standaard netwerktoegang > EAP-TLS toestaan > Opslaan.**

Cisco ISE Policy - Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

- Authentication Bypass
 - Process Host Lookup
- Authentication Protocols
 - Allow PAP/ASCII
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - Allow EAP-MD5
 - Allow EAP-TLS

Expand Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Controleer het verificatietype

De opdracht show toont de verificatieinformatie van een AP-profiel:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

Voorbeeld:

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE   : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

Controleer 802.1x op de Switch-poort

Het showbevel toont de authenticatiestatus van 802.1x op de switch poort:

CLI:

```
Switch# show dot1x all
```

Voorbeeld uitvoer:

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout          = 0
SuppTimeout            = 30
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
```

Controleer of de poort al dan niet is geverifieerd

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

Voorbeeld uitvoer:

```
Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout          = 0
SuppTimeout            = 30
ReAuthMax              = 2
MaxReq                 = 2
```

TxPeriod = 30

Dot1x Authenticator Client List

```
-----  
EAP Method = FAST  
Supplicant = f4db.e67e.dd16  
Session ID = 0A30279E00000BB7411A6BC4  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE
```

ED

Auth BEND SM State = IDLE

Van CLI:

Switch#show authentication sessions

Voorbeeld uitvoer:

```
Interface MAC Address Method Domain Status Fg Session ID  
Gi0/8 f4db.e67e.dd16 dot1x DATA Auth 0A30279E00000BB7411A6BC4
```

Kies in ISE Operations > Radius Livelogs en bevestig dat de verificatie succesvol is en dat het juiste autorisatieprofiel is ingedrukt.

| Time | Status | Details | Repea... | Identity | Endpoint ID | Endpoint... | Authentication ... | Authorization Policy | Authorization Pr... | IP Address | Network De... | Device P |
|----------------------------|---------|---------|----------|----------|--------------------|--------------|--------------------|---------------------------------------|---------------------|------------|---------------|-----------|
| Nov 28, 2022 08:39:49.7... | Success | | | dot1x | A4:53:0E:37:A1:... | Cisco-Dev... | Default >> Dot1X | Default >> Basic_Authenticated_Access | | | nschyns-SW... | FastEther |
| Nov 28, 2022 08:33:34.4... | Success | | | dot1x | A4:53:0E:37:A1:... | Cisco-Dev... | Default >> Dot1X | Default >> Basic_Authenticated_Access | PermitAccess | | nschyns-SW... | FastEther |

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

1. Voer de opdracht **ping** in om te controleren of de ISE-server via de switch bereikbaar is.
2. Zorg ervoor dat de switch als AAA-client is geconfigureerd op de ISE-server.
3. Zorg ervoor dat het gedeelde geheim hetzelfde is tussen de switch en de ISE-server.
4. Controleer of EAP-FAST is ingeschakeld op de ISE-server.
5. Controleer of de 802.1x-referenties voor de LAP zijn geconfigureerd en op de ISE-server hetzelfde zijn.

Opmerking: de gebruikersnaam en het wachtwoord zijn hoofdlettergevoelig.

6. Als de verificatie mislukt, voert u deze opdrachten in op de switch: **debug dot1x** en **debug verificatie**.

Merk op dat op Cisco IOS gebaseerde access points (802.11ac wave 1) TLS versie 1.1 en 1.2 niet ondersteunen. Dit kan een probleem opleveren als uw ISE- of RADIUS-server zodanig is geconfigureerd dat TLS 1.2 alleen binnen 802.1X-verificatie mogelijk is.

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.