

# Configureer 802.1X-verificatie op Catalyst 9800 draadloze controller Series

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[WLC-configuratie](#)

[AAA-configuratie op 9800 WLC's](#)

[WLAN-profielconfiguratie](#)

[Configuratie van beleidsprofiel](#)

[Configuratie van beleidstag](#)

[Toewijzing van beleidstags](#)

[ISE-configuratie](#)

[De WLC op ISE verklaren](#)

[Nieuwe gebruiker maken op ISE](#)

[Autorisatieprofiel maken](#)

[Een beleidsset maken](#)

[Verificatiebeleid maken](#)

[Autorisatiebeleid maken](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Probleemoplossing op de WLC](#)

[Probleemoplossing op ISE](#)

## Inleiding

Dit document beschrijft hoe u een WLAN met 802.1X-beveiliging op een Cisco Catalyst 9800 Series draadloze controller kunt instellen.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 802.1X

## Gebruikte componenten

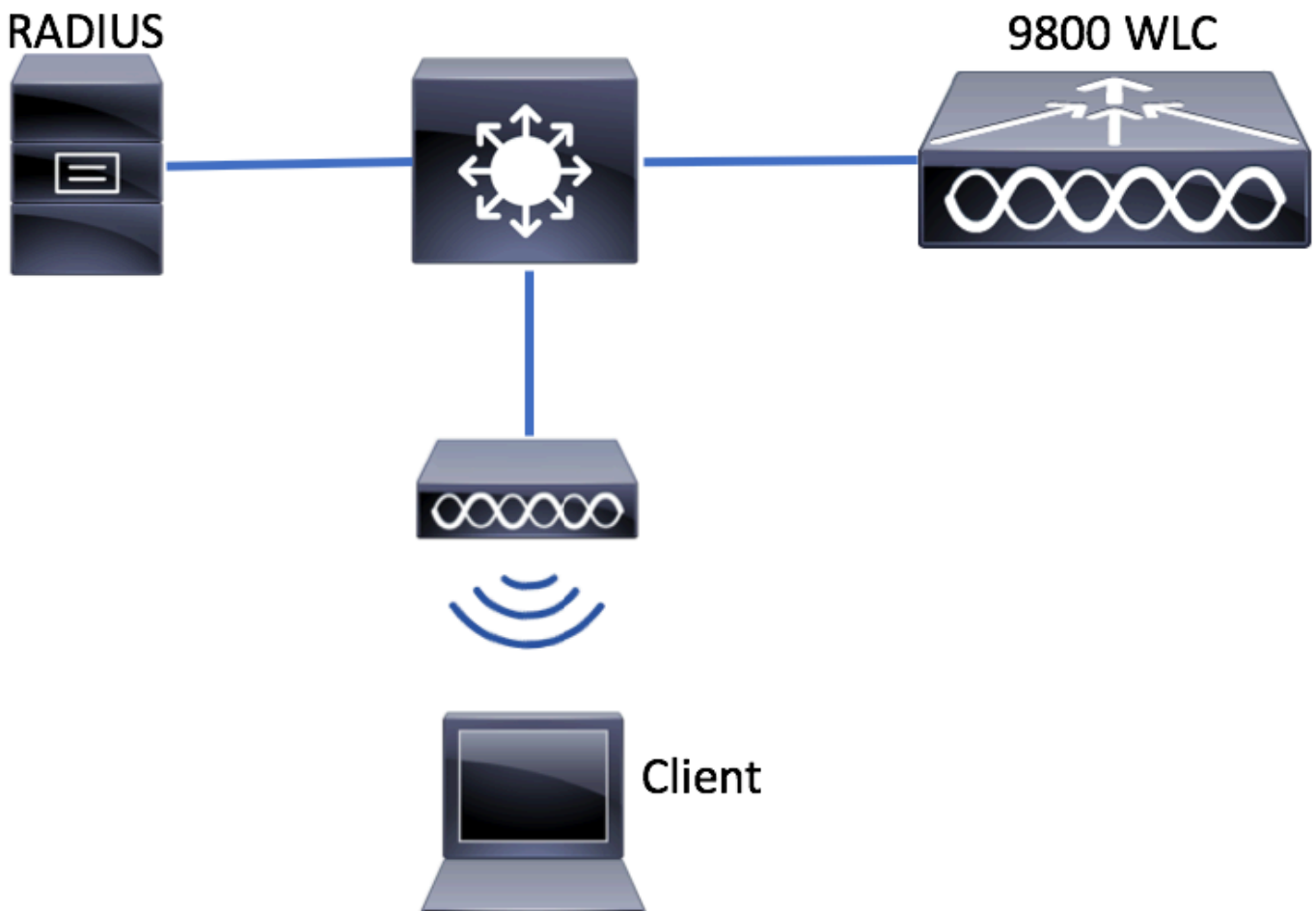
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9800 draadloze controller Series (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE-lijnkaart 3.0

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.

## Configureren

### Netwerkdigram



### WLC-configuratie

#### AAA-configuratie op 9800 WLC's

#### GUI:

Stap 1. RADIUS-server declareren. Naar navigeren **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** en voer de RADIUS-serverinformatie in.

Zorg ervoor dat **ondersteuning voor CoA** is ingeschakeld als u van plan bent om in de toekomst gebruik te maken van Central Web Verification (of een ander soort beveiliging waarvoor een wijziging van autorisatie [CoA] vereist is).

Create AAA Radius Server ✕

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

Stap 2. Voeg de RADIUS-server toe aan een RADIUS-groep. Naar navigeren **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Geef een naam aan uw groep en verplaats de server die u eerder hebt gemaakt in de lijst met **Assigned Servers**.

### Create AAA Radius Server Group

Name\*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Stap 3. Maak een lijst met verificatiemethoden. Naar navigeren Configuration > Security > AAA > AAA Method List > Authentication > + Add.

The screenshot shows the network configuration interface. On the left is a dark sidebar menu with a search bar and four main categories: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' category is highlighted with a red box. The main content area is titled 'Authentication Authorization and Accounting'. It features a blue '+ AAA Wizard' button, a blue 'AAA Method List' button (highlighted with a red box), and a 'Servers / Groups' section. Below this, there are two tabs: 'General' and 'Authentication' (highlighted with a red box). In the 'Authentication' tab, there is a blue '+ Add' button (highlighted with a red box) and a grey 'x Del' button. At the bottom, a table header with 'Name' is visible.

Voer de informatie in:

Quick Setup: AAA Authentication ✕

Method List Name\*

Type\*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

## CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

## Opmerking over de AAA-dode-serverdetectie

Nadat u uw RADIUS-server hebt geconfigureerd, kunt u controleren of deze wordt beschouwd als "LEVEND":

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC
(2) : current UP Platform State from WNCDC (3) : current UP Platform State from WNCDC (4) :
current UP ...
```

U kunt de **dead criteria**, alsmede de **deadtime** op uw WLC, vooral als u meerdere RADIUS-servers gebruikt.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

**Opmerking:** **dead criteria** is de criteria die worden gebruikt om een RADIUS-server als dood te markeren. Het bestaat uit: 1. Een time-out (in seconden) die de tijd vertegenwoordigt die

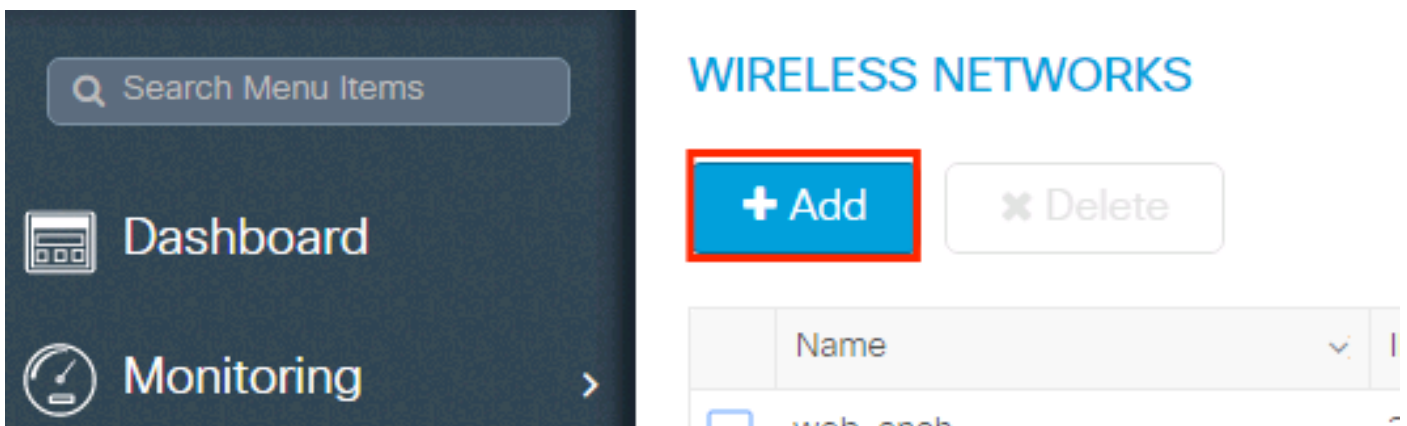
moet verstrijken vanaf het moment dat de controller voor het laatst een geldig pakket van de RADIUS-server heeft ontvangen tot het moment dat de server als dood is gemarkeerd. 2. Een teller, die het aantal opeenvolgende onderbrekingen vertegenwoordigt die op de controller moeten voorkomen voordat de RADIUS-server als dood wordt gemarkeerd.

**Opmerking:** *deadtime* geeft aan hoeveel tijd (in minuten) de server in dode status blijft nadat dode criteria het als dood markeren. Als de deadline is verlopen, markeert de controller de server als UP (ALIVE) en waarschuwt de geregistreerde clients over de statuswijziging. Als de server nog steeds onbereikbaar is nadat de status is gemarkeerd als UP en als aan de dode criteria is voldaan, dan wordt de server opnieuw gemarkeerd als dood voor het dode interval.

## WLAN-profielconfiguratie

### GUI:

Stap 1. Maak het WLAN. Navigeer naar **Configuratie > Draadloos > WLAN's > + Voeg het netwerk toe** en configureer het naar wens.



Stap 2. Voer de WLAN-informatie in

## Add WLAN ✕

General	Security	Advanced
Profile Name*	<input type="text" value="prof-name"/>	Radio Policy <input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID <input checked="" type="checkbox"/>
WLAN ID*	<input type="text" value="1"/>	
Status	<input checked="" type="checkbox"/>	

Stap 3. Naar het **Beveiliging** tabblad en selecteer de gewenste beveiligingsmethode. In dit geval **WPA2 + 802.1x**.

General	Security	Advanced
	<b>Layer2</b>	Layer3
	Layer 2 Security Mode <input type="text" value="WPA + WPA2"/>	AAA
	MAC Filtering <input type="checkbox"/>	Fast Transition <input type="text" value="Adaptive Enab..."/>
	<b>Protected Management Frame</b>	Over the DS <input checked="" type="checkbox"/>
	PMF <input type="text" value="Disabled"/>	Reassociation Timeout <input type="text" value="20"/>
	<b>WPA Parameters</b>	
	WPA Policy <input type="checkbox"/>	

**Add WLAN**

PMF Disabled

**WPA Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

Stap 4. Van de **Security > AAA** Selecteer op het tabblad de verificatiemethode die in Stap 3 is gemaakt vanuit AAA Configuration op de 9800 WLC-sectie.

**Add WLAN**

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List list-name

Local EAP Authentication

Cancel Save & Apply to Device

**CLI:**

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```



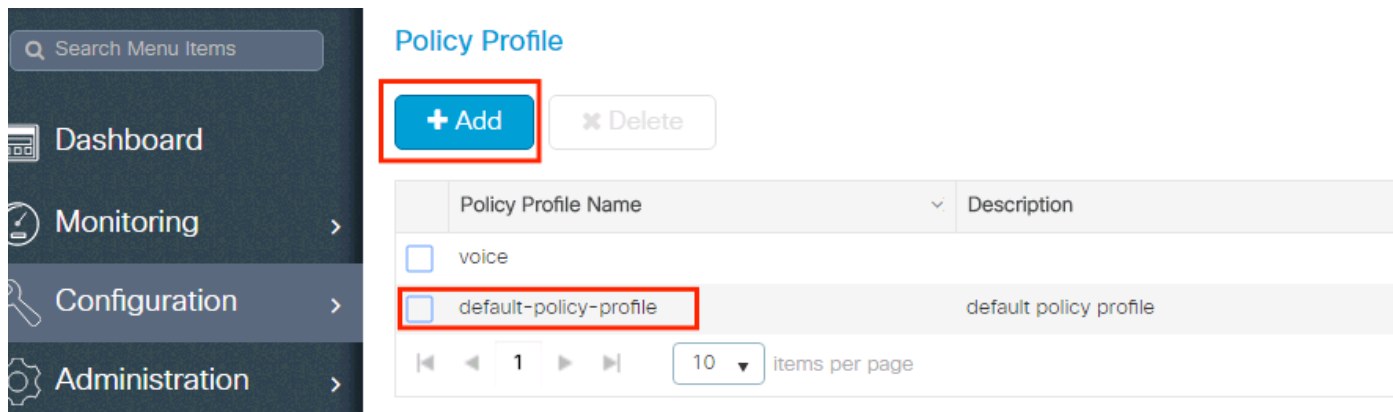
## Configuratie van beleidsprofiel

Binnen een beleidsprofiel kunt u beslissen aan welk VLAN de clients worden toegewezen, onder andere instellingen (zoals toegangscontrolelijst [ACL's], Quality of Service [QoS], mobiliteitsanker, timers enzovoort).

U kunt uw standaardbeleidsprofiel gebruiken of u kunt een nieuw profiel maken.

### GUI:

Navigeer naar **Configuration > Tags & profielen > Policy Profile** en configureer uw **standaard-policy-profiel** of maak een nieuw profiel.



Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

Zorg ervoor dat het profiel is ingeschakeld.

Als uw access point (AP) zich in de lokale modus bevindt, moet u er ook voor zorgen dat het beleidsprofiel **Central Switching** en **Central Verification** heeft ingeschakeld.

## Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name\*

Description

Status **ENABLED**

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

### WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

Selecteer het VLAN waar de clients moeten worden toegewezen in het tabblad **Toegangsbeleid**.

## Edit Policy Profile

General | **Access Policies** | QOS and AVC | Mobility | Advanced

### WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

### VLAN

VLAN/VLAN Group

Multicast VLAN

### WLAN ACL

IPv4 ACL

IPv6 ACL

### URL Filters

Pre Auth

Post Auth

Als u van plan bent om ISE-retourkenmerken te hebben in de Access-Accept like VLAN Assignment, dient u AAA-override in te schakelen in het **Advanced** tabblad:

Edit Policy Profile ✕

---

General
Access Policies
QOS and AVC
Mobility
Advanced

**WLAN Timeout**

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy  [Clear](#)

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

2.4 GHz Policy

5 GHz Policy

↶ Cancel

↶
Update & Apply to Device

**CLI:**

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

**Configuratie van beleidstag**

Policy Tag wordt gebruikt om de SSID te koppelen aan het beleidprofiel. U kunt een nieuwe Policy Tag maken of de standaard-policy tag gebruiken.

**Opmerking:** De standaard-policy-tag brengt automatisch elke SSID met een WLAN-id tussen 1 en 16 in kaart aan het standaard-beleid-profiel. Dit kan niet worden gewijzigd of verwijderd. Als u een WLAN met een ID 17 of hoger hebt, kan de standaard-beleidstag niet worden gebruikt.

**GUI:**

Naar navigeren **Configuratie > Tags & Profiles > Tags > Policy** en voeg indien nodig een nieuwe toe.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

### Manage Tags

Policy Site RF AP

**+ Add** **✕ Delete**

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

Koppel uw WLAN-profiel aan het gewenste beleidsprofiel.

### Add Policy Tag

Name\* PolicyTagName

Description Enter Description

**+ Add** **✕ Delete**

WLAN Profile	Policy Profile
No items to display	

0 10 items per page

Cancel Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<span>◀◀ 0 ▶▶</span> <span>10 items per page</span> <span style="float: right;">No items to display</span>	

Map WLAN and Policy

WLAN Profile\* 
Policy Profile\*

✕
✓

↻ Cancel
📄 Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile

◀◀ 1 ▶▶ 10 items per page 1 - 1 of 1 items

↻ Cancel
📄 Save & Apply to Device

**CLI:**

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

**Toewijzing van beleidstags**

Wijs de beleidstag toe aan de benodigde toegangspunten.

**GUI:**

Om de tag aan één AP toe te wijzen, navigeer naar **Configuration > Wireless > Access Points > AP Name > General Tags**, de relevante beleidstag toe te wijzen en vervolgens op **Update & Apply to Device**.

**Edit AP**

**General** | Interfaces | High Availability | Inventory | Advanced

<b>General</b>		<b>Version</b>	
AP Name*	AP3802-02-WS	Primary Software Version	10.0.200.50
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	00:42:68:c6:41:20	Predownloaded Version	N/A
Ethernet MAC	00:42:68:a0:d0:22	Next Retry Time	N/A
Admin Status	Enabled	Boot Version	1.0.0
AP Mode	Local	IOS Version	10.0.200.52
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled		
<b>Tags</b>		<b>IP Config</b>	
Policy	default-policy-tag	IP Address	172.16.0.207
Site	default-site-tag	Static IP	<input type="checkbox"/>
RF	default-rf-tag	<b>Time Statistics</b>	
		Up Time	9 days 1 hrs 17 mins 24 secs
		Controller Associated Time	0 days 3 hrs 26 mins 41 secs
		Controller Association Latency	8 days 21 hrs 50 mins 33 secs

**Cancel** | **Update & Apply to Device**

**Opmerking:** houd er rekening mee dat wanneer de beleidstag op een AP wordt gewijzigd, deze de associatie met de 9800 WLC laat vallen en een paar momenten later terugkomt.

Als u dezelfde beleidsmarkering aan meerdere toegangspunten wilt toewijzen, navigeer dan naar **Configuration > Wireless Setup > Advanced > Start Now > Apply**.



## 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.