

Catalyst 9800 WLC iPSK met ISE-encryptie configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Begrijp wat iPSK is en welke scenario's het past](#)

[Configureren 9800 WLC](#)

[ISE-configuratie](#)

[Problemen oplossen](#)

[Probleemoplossing voor de 9800 WLC](#)

[Probleemoplossing ISE](#)

Inleiding

Dit document beschrijft de configuratie van een iPSK beveiligde WLAN op een Cisco 9800 draadloze LAN-controller met Cisco ISE als RADIUS-server.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat u al bekend bent met de basisconfiguratie van een WLAN op 9800 en dat u de configuratie aan uw implementatie kunt aanpassen.

Gebruikte componenten

- Cisco Catalyst 9800-CL WLC met 17.6.3
- Cisco ISE-licentiekaart 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.

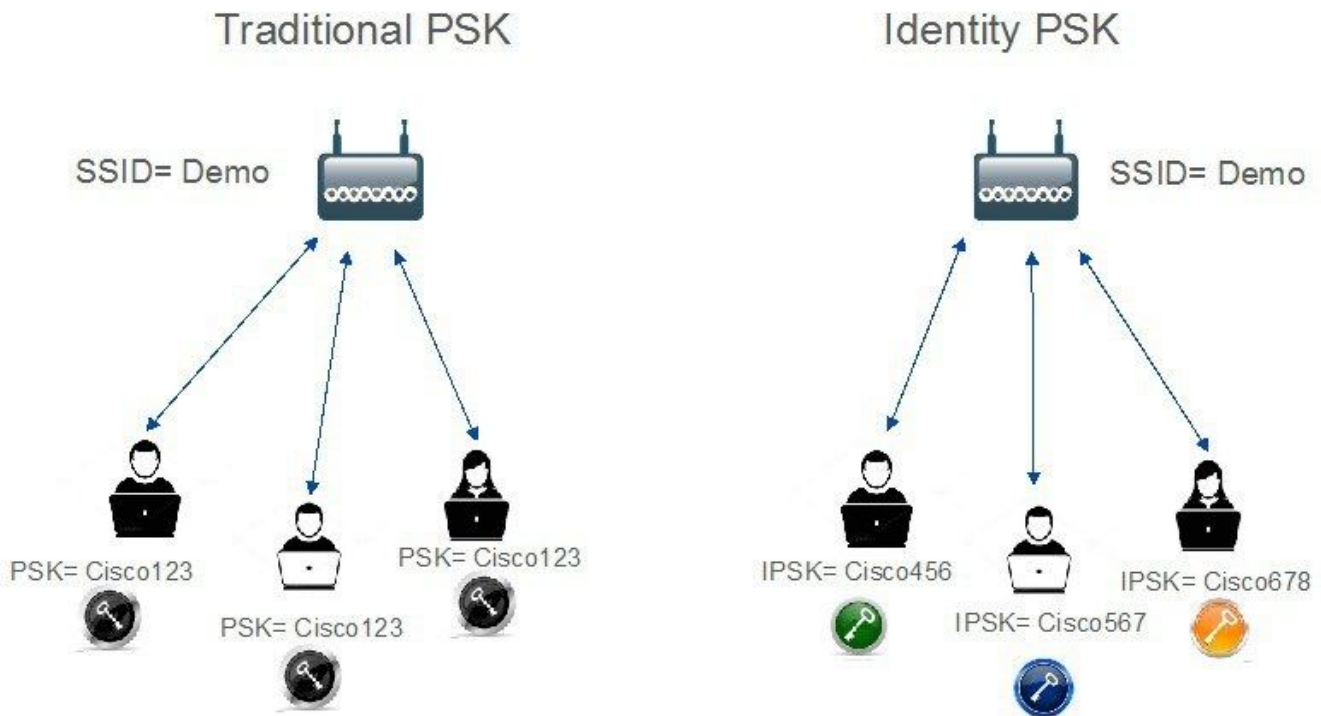
Begrijp wat iPSK is en welke scenario's het past

Traditionele vooraf gedeelde sleutel (PSK) beveiligde netwerken gebruiken hetzelfde wachtwoord voor alle verbonden clients. Dit kan ertoe leiden dat de sleutel wordt gedeeld met onbevoegde gebruikers waardoor een inbreuk op de beveiliging en onbevoegde toegang tot het netwerk ontstaat. De meest voorkomende beperking van deze inbreuk is de verandering van de PSK zelf, een verandering die van invloed is op alle gebruikers, aangezien veel eindapparaten moeten

worden bijgewerkt met de nieuwe sleutel om weer toegang te krijgen tot het netwerk.

Met Identity PSK (iPSK) worden unieke vooraf gedeelde sleutels gecreëerd voor individuen of een groep gebruikers op dezelfde SSID met behulp van een RADIUS-server. Dit type installatie is zeer nuttig in netwerken waar end-client-apparaten geen dot1x-verificatie ondersteunen, maar een veiligere en korrelige verificatieregeling nodig is. Vanuit een clientperspectief ziet dit WLAN er hetzelfde uit als het traditionele PSK-netwerk. Wanneer een van de PSK's gecompromitteerd is, hoeft alleen de betrokken persoon of groep zijn PSK bijgewerkt te krijgen. De rest van de apparaten die zijn aangesloten op het WLAN is ongewijzigd.

Traditional Vs Identity PSK



Configureren 9800 WLC

Onder **Configuration > Security > AAA > Servers/Group > Servers** voeg de ISE toe als RADIUS-server:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Address	Auth Port	Acct Port
<input type="checkbox"/> ISE_IPSK	10.48.39.126	1812	1813

10 items per page 1 - 1 of 1 items

Maak onder **Configuratie > Beveiliging > AAA > Servers/groepen > Servergroepen** een RADIUS-servergroep en voeg de eerder gemaakte ISE-server eraan toe:

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Server 1	Server 2	Server 3
<input type="checkbox"/> ISE_IPSK_Group	ISE_IPSK	N/A	N/A

1 - 1 of 1 items

Voer in het tabblad **AAA-methodelijst** een **autorisatielijst in** met het type "netwerk" en het groepstype "groep" dat naar de eerder gemaakte RADIUS-servergroep verwijst:

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Authz_List_IPSK	network	group	ISE_IPSK_Group	N/A	N/A	N/A

1 - 1 of 1 items

Accounting instellen is optioneel, maar kan door het type te configureren naar "identiteit" en het naar dezelfde RADIUS-servergroep te verwijzen:

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Acc_List_IPSK	identity	ISE_IPSK_Group	N/A	N/A	N/A

1 - 1 of 1 items

Dit kan ook via de opdrachtregel worden uitgevoerd met:

```
radius server
```

Voer onder **Configuration > Tags en profielen > WLAN's** een nieuw WLAN in. Onder Layer 2-configuratie:

- Schakel MAC-filtering in en stel de autorisatielijst in op de eerder gemaakte versie
- Schakel **PSK in** onder **Auth Key Management**
- Het vooraf gedeelde sleutelveld kan met elke waarde worden gevuld. Dit wordt alleen gedaan om te voldoen aan de eisen van het ontwerp van de webinterface. Geen gebruiker kan

verifiëren met deze toets. In dit geval is de voorgedeelde sleutel ingesteld op "12345678".

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Authorization List* Authz_List... ▼ ⓘ

Protected Management Frame

PMF Disabled ▼

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 Easy-PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

PSK Format ASCII ▼

PSK Type Unencrypted ▼

Pre-Shared Key*|

Lobby Admin Access

Fast Transition Adaptive Enabled▼

Over the DS

Reassociation Timeout 20

MPSK Configuration

MPSK

Gebruikerssegregatie kan worden bereikt onder het tabblad **Geavanceerd**. Door deze optie in te stellen op Allow Private Group kunnen gebruikers die dezelfde PSK gebruiken, met elkaar communiceren, terwijl gebruikers die een andere PSK gebruiken, worden geblokkeerd:

General	Security	Advanced	Add To Policy Tags
Coverage Hole Detection	<input checked="" type="checkbox"/>		Universal Admin <input type="checkbox"/>
Aironet IE	<input type="checkbox"/>		OKC <input checked="" type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>		Load Balance <input type="checkbox"/>
P2P Blocking Action	<input type="checkbox"/>	Allow Private Group ▼	Band Select <input type="checkbox"/>
Multicast Buffer	<input type="checkbox"/>	<input type="checkbox"/>	IP Source Guard <input type="checkbox"/>

Voer onder **Configuratie > Tags en profielen > Beleid** een nieuw beleidsprofiel in. In het tabblad **Toegangsbeleid** stelt u het VLAN of de VLAN-groep in die dit WLAN gebruikt:

Add Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
WLAN Local Profiling				
Global State of Device Classification	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="checkbox"/>			
VLAN				
VLAN/VLAN Group	<input type="checkbox"/>			
Multicast VLAN	<input type="checkbox"/>			

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Schakel in het tabblad **Geavanceerd** de optie AAA-negeren in en voeg een accounting lijst toe indien deze eerder is gemaakt:

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this 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)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List ⓘ ✕

Fabric Profile

Link-Local Bridging

mDNS Service Policy

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Zorg er onder **Configuratie > Tags & profielen > Tags > Beleid** voor dat het WLAN is toegewezen aan het profiel dat u hebt gemaakt:

Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

✕ Delete

Policy Tag Name

default-policy-tag

1 10 Items per page

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Description

WLAN-POLICY Maps: 1

+ Add

✕ Delete

WLAN Profile

Policy Profile

WLAN_iPSK Policy_Profile_iPSK

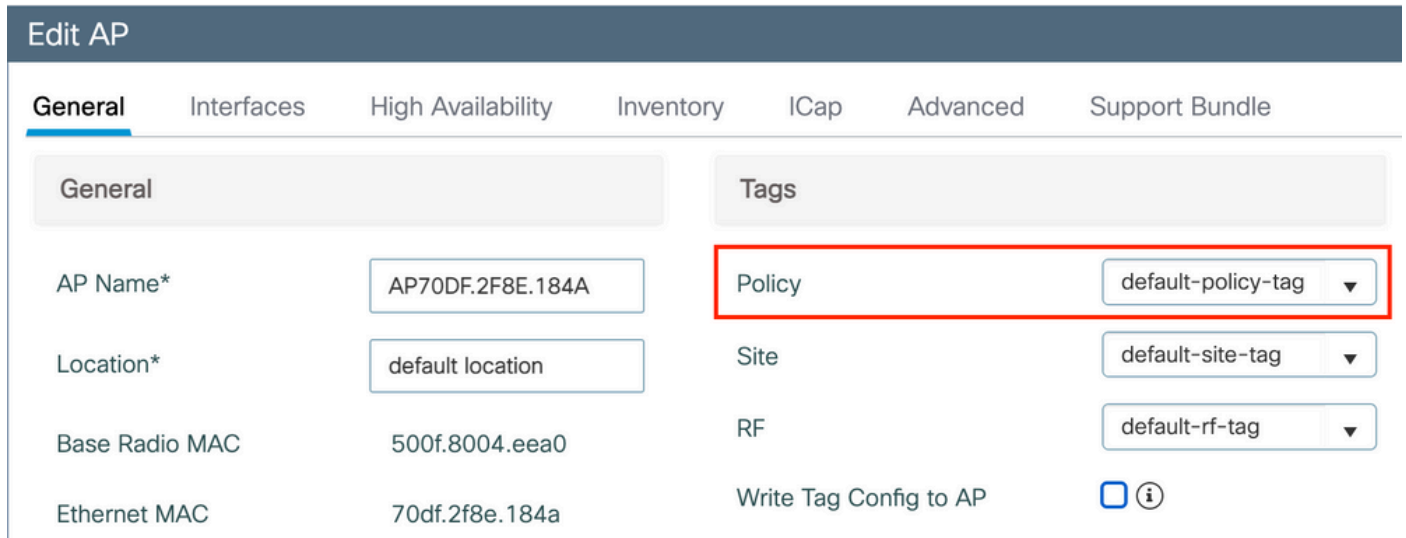
1 10 Items per page

1 - 1 of 1 items

Dit kan ook via de opdrachtregel worden uitgevoerd met:

wlan

Zorg er onder **Configuration > Wireless > Access points** voor dat deze tag is toegepast op de access points waarop het WLAN moet worden uitgezonden:



The screenshot shows the 'Edit AP' configuration page. The 'General' tab is selected. The 'Tags' section is highlighted with a red box. The 'Policy' dropdown menu is set to 'default-policy-tag'. Other fields include 'AP Name*' (AP70DF.2F8E.184A), 'Location*' (default location), 'Base Radio MAC' (500f.8004.eea0), 'Ethernet MAC' (70df.2f8e.184a), 'Site' (default-site-tag), 'RF' (default-rf-tag), and 'Write Tag Config to AP' (checkbox).

Field	Value
AP Name*	AP70DF.2F8E.184A
Location*	default location
Base Radio MAC	500f.8004.eea0
Ethernet MAC	70df.2f8e.184a
Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag
Write Tag Config to AP	<input type="checkbox"/> ⓘ

ISE-configuratie

Deze configuratiehandleiding bevat een scenario waarin de PSK van het apparaat wordt bepaald op basis van het MAC-adres van de client. Onder **Beheer > Netwerkbronnen > Netwerkapparaten**, voeg een nieuw apparaat toe, specificeer het IP-adres, schakel de RADIUS-verificatie-instellingen in en specificeer een RADIUS gedeeld geheim:

Cisco ISE Administration - Network Resources

Network Devices

Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | More

Network Devices List > New Network Device

Network Devices

* Name: 9800-WLC

Description: _____

IP Address: * IP: 10.48.38.86 / 32

* Device Profile: Cisco

Model Name: _____

Software Version: _____

* Network Device Group: _____

Location: All Locations [Set To Default]

IPSEC: Is IPSEC Device [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: [Show]

Voeg onder **Context Visibility > Endpoints > Verificatie** de MAC-adressen toe van alle apparaten (clients) die verbinding maken met het iPSK-netwerk:

Cisco ISE Context Visibility - Endpoints

Authentication | BYOD | Compliance | Compromised Endpoints | Endpoint Classification | Guest | Vulnerable Endpoints | Hardware

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

AUTHENTIFICATIONS

NETWORK DE

Rows/Page: 1 / 1 Total Rows

ANC | Change Authorization | Clear Threats & Vulnerabilities | Export | Import | MDM Actions | Release Rejected | Revoke Certificate

MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Re...	Authentication ...	Authorization P..
08:BE:AC:27:85:7E	*		08beac278...		Location...	Unknown	-	MAB	Basic_Authenticate.

Onder **Beheer > Identiteitsbeheer > Groepen > Endpoint Identity Groups**, maak een of meer groepen en wijs gebruikers aan hen toe. Elke groep kan later worden geconfigureerd om een andere PSK te gebruiken om verbinding te maken met het netwerk.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is "Administration > Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area is titled "Endpoint Identity Groups" and shows a table with two entries:

Name	Description
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iDevice	Identity Group for Profile: Apple-iDevice

Buttons for "Edit", "+ Add", and "Delete" are visible. The "Add" button is highlighted with a red box.

The screenshot shows the "New Endpoint Group" form. The breadcrumb navigation is "Administration > Identity Management > Endpoint Identity Group List > New Endpoint Group". The form title is "Endpoint Identity Group". The "Name" field contains "Identity_Group_IPSK" and is highlighted with a red box. There are fields for "Description" and "Parent Group". "Submit" and "Cancel" buttons are at the bottom.

Zodra de groep is gemaakt, kunt u nu gebruikers aan hen toewijzen. Selecteer de groep die u hebt gemaakt en klik op "Bewerken":

The screenshot shows the "Endpoint Identity Groups" list. The breadcrumb navigation is "Administration > Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area shows a table with three entries:

Name	Description
<input type="checkbox"/> Epson-Device	Identity Group for Profile: Epson-Device
<input type="checkbox"/> GuestEndpoints	Guest Endpoints Identity Group
<input checked="" type="checkbox"/> Identity_Group_IPSK	
<input type="checkbox"/> Iuniner-Device	Identity Group for Profile: Iuniner-Device

The "Identity_Group_IPSK" row is highlighted in blue. The "Edit" button is highlighted with a red box.

Voeg in de groepsconfiguratie het MAC-adres toe van de client(s) die u aan deze groep wilt toewijzen door op de knop "Toevoegen" te klikken:

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb path is "Endpoint Identity Group List > Identity_Group_IPSK". The main form is titled "Endpoint Identity Group" and contains the following fields:

- * Name: Identity_Group_IPSK
- Description: (empty text box)
- Parent Group: (empty dropdown)

Below the form are "Save" and "Reset" buttons. Underneath, there is a section for "Identity Group Endpoints" with "Selected 0 Total 1" and a refresh icon. There are "+ Add" and "Remove" buttons. A table below shows the endpoint configuration:

MAC Address	Static Group Assignment	Endpoint Profile
<input type="checkbox"/> 08:BE:AC:27:85:7E	true	Unknown

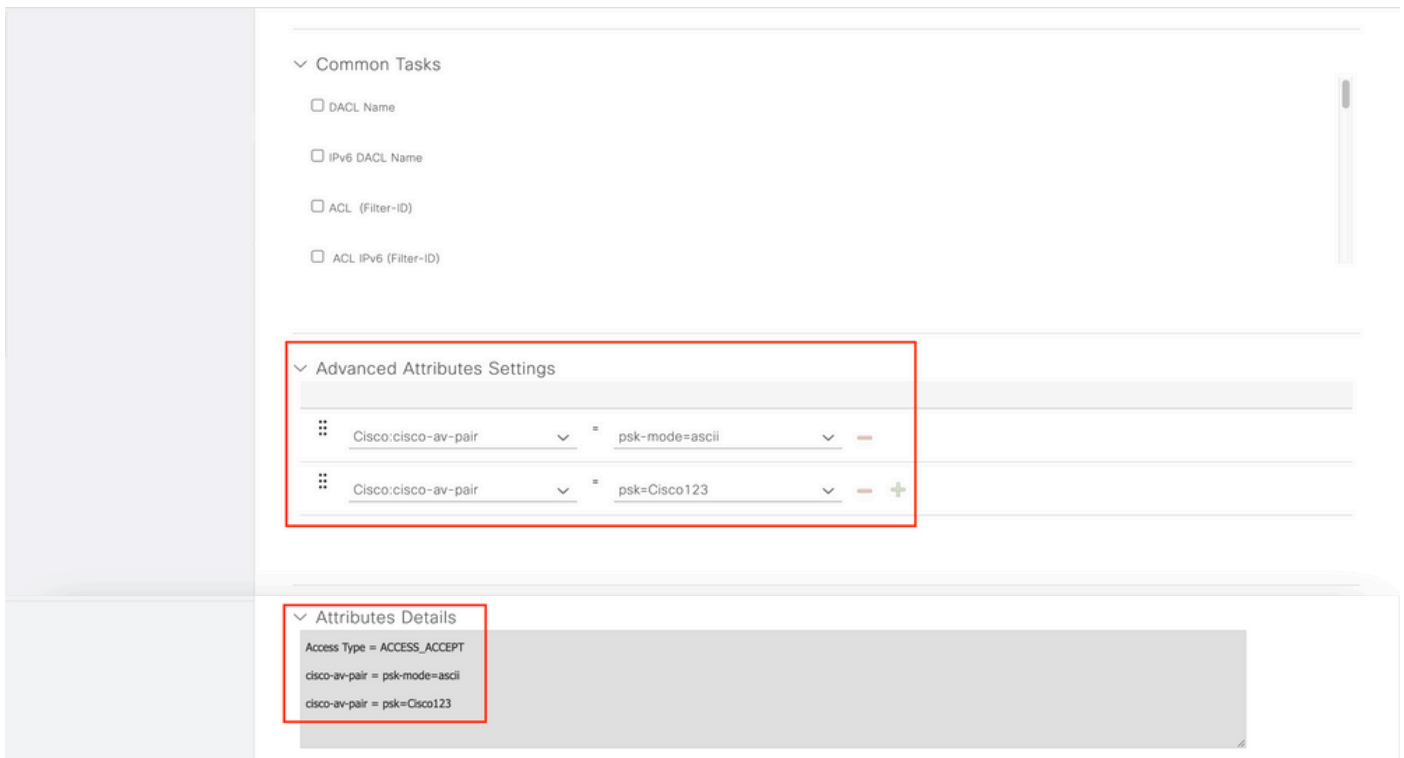
Voer onder **Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen** een nieuw profiel voor autorisatie in. Eigenschappen instellen op:

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

Voor elke gebruikersgroep die een andere PSK moet gebruiken, creëer een extra resultaat met een ander spk av-paar. Aanvullende parameters zoals ACL en VLAN-overschrijving kunnen hier ook worden geconfigureerd.

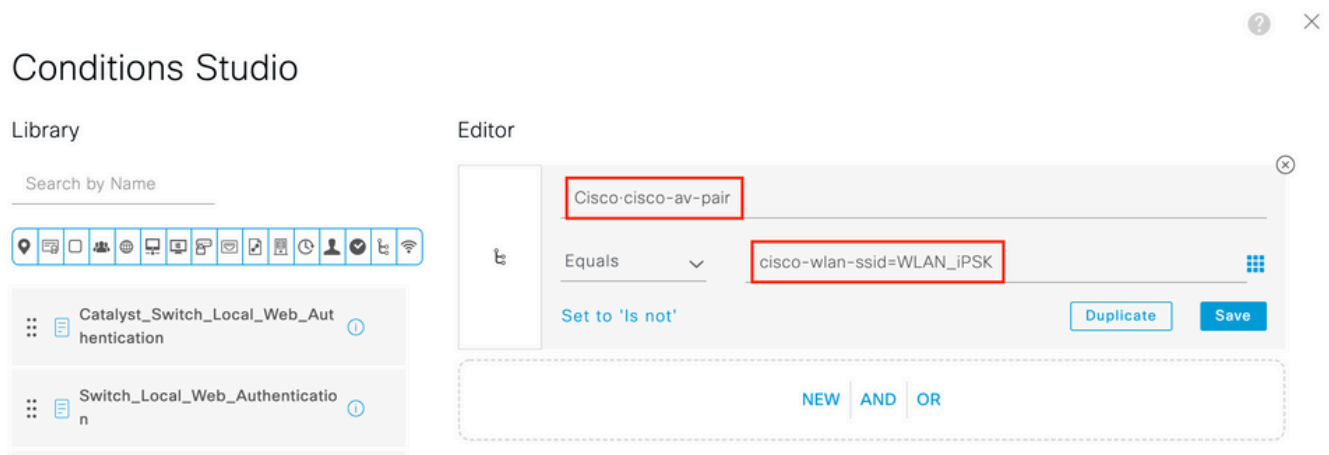
The screenshot shows the Cisco ISE Administration interface for Policy Elements. The breadcrumb path is "Policy > Policy Elements". The main form is titled "Authorization Profile" and contains the following fields:

- * Name: Authz_Profile_IPSK
- Description: (empty text box)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement: ⓘ
- Agentless Posture: ⓘ
- Passive Identity Tracking: ⓘ

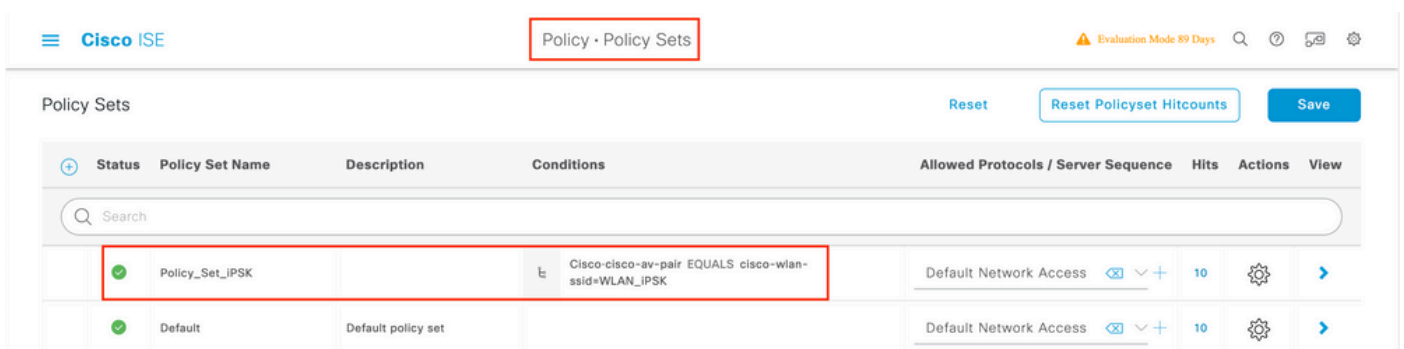


Voer onder **Beleid > Beleidssets** een nieuwe in. Om ervoor te zorgen dat de client voldoet aan de beleidsset, wordt deze voorwaarde gebruikt:

Cisco:cisco-av-pair **EQUALS** cisco-wlan-ssid=WLAN_iPSK // "WLAN_iPSK" is WLAN name



Er kunnen aanvullende voorwaarden worden toegevoegd om de afstemming van beleid veiliger te maken.




Ga naar de nieuwe configuratie van de iPSK Policy Set door op de blauwe pijl rechts van de

Policy Set-lijn te klikken:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy_Set_IPSK		Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_IPSK	Default Network Access	77	 	

Zorg ervoor dat het verificatiebeleid is ingesteld op "Interne endpoints":

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Policy_Set-IPSK		Radius-Called-Station-ID ENDS_WITH WLAN_IPSK	Default Network Access	0
Authentication Policy (1)					
Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints	0	

Voer onder **Autorisatiebeleid** een nieuwe regel in voor elk van de gebruikersgroepen. Als voorwaarde, gebruik:

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK //
```

"Identity_Group_iPSK" is name of the created endpoint group

met als **resultaat** het **autorisatieprofiel** dat eerder is gemaakt. Zorg ervoor dat de **standaard** regel onderaan blijft en wijst naar **DenyAccess**.

The screenshot shows the Cisco ISE Policy Sets configuration page. At the top, there is a search bar and navigation tabs for 'Internal Endpoints' and 'Options'. Below this, there are sections for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (1)'. The main table displays a list of rules. The rule 'Authz_Rule_Group1' is highlighted with a red box. Its details are as follows:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK x	Select from list	0	+
+	Default		DenyAccess x	Select from list	0	+

Als elke gebruiker een ander wachtwoord krijgt, kunnen in plaats van het maken van Endpoint groepen en regels die overeenkomen met die endpointgroep, een regel met deze voorwaarde worden gemaakt:

Radius-Calling-Station-ID **EQUALS** <client_mac_addr>

Opmerking: MAC-adresscheidingsteken kan worden geconfigureerd op de WLC onder **AAA >AAA Advanced > Global Config > Advanced Settings**. In dit voorbeeld is het teken "-" gebruikt.

The screenshot shows the Cisco ISE Policy Sets configuration page, similar to the first one. The 'Authorization Policy (1)' section is expanded. The main table displays a list of rules. The rule 'Authz_Rule_Single' is highlighted with a red box. Its details are as follows:

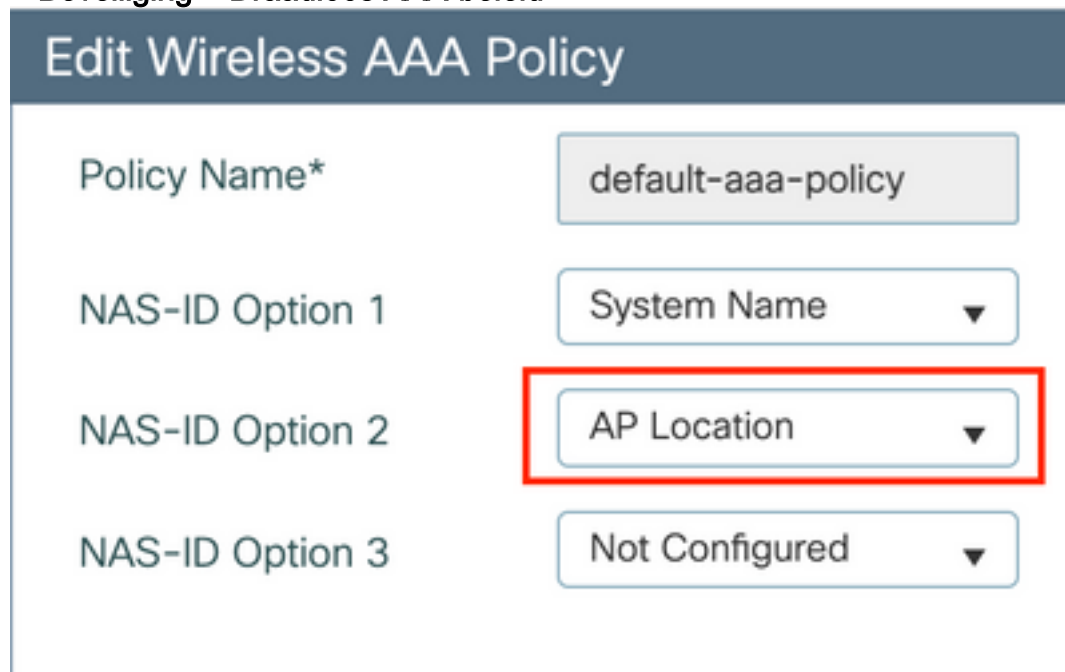
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	Authz_Rule_Single	Radius-Calling-Station-ID EQUALS 08-BE-AC-27-85-7E	Authz_Profile_IPSK x	Select from list	0	+
+	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK x	Select from list	0	+
+	Default		DenyAccess x	Select from list	0	+

Regels betreffende het autorisatiebeleid staan toe dat er veel andere parameters worden gebruikt om het wachtwoord in te voeren dat de gebruiker gebruikt. De meest gebruikte regels zijn:

1. Overeenkomend op basis van de gebruikerslocatie

In dit scenario, moet WLC AP informatie van de Plaats naar ISE verzenden. Hiermee kunnen

gebruikers op één locatie één wachtwoord gebruiken, terwijl gebruikers op een andere locatie een ander wachtwoord gebruiken. Dit kan worden geconfigureerd onder **Configuratie > Beveiliging > Draadloos AAA-beleid**:



The screenshot shows the 'Edit Wireless AAA Policy' configuration interface. It features a dark blue header with the title 'Edit Wireless AAA Policy'. Below the header, there are four configuration rows, each with a label on the left and a corresponding input field on the right:

- Policy Name***: A text input field containing 'default-aaa-policy'.
- NAS-ID Option 1**: A dropdown menu currently showing 'System Name'.
- NAS-ID Option 2**: A dropdown menu currently showing 'AP Location', which is highlighted with a red rectangular box.
- NAS-ID Option 3**: A dropdown menu currently showing 'Not Configured'.

2. Overeenkomsten op basis van apparaatprofilering

In dit scenario, moet WLC aan profielapparaten globaal worden gevormd. Hiermee kan een beheerder een ander wachtwoord instellen voor laptop- en telefoonapparaten. Globale apparaatclassificatie kan worden ingeschakeld onder **Configuration > Wireless > Wireless Global**. Raadpleeg voor de configuratie van apparaatprofilering op ISE de [ISE-ontwerpgids voor profielen](#).

Naast het retourneren van de coderingsleutel, omdat deze autorisatie gebeurt tijdens de 802.11-associatiefase, is het volledig mogelijk om andere AAA-kenmerken van ISE terug te geven, zoals ACL of VLAN-id.

Problemen oplossen

Probleemoplossing voor de 9800 WLC

Op de WLC moet het verzamelen van radioactieve sporen meer dan genoeg zijn om de meeste problemen te identificeren. Dit kan worden gedaan in de WLC web interface onder **Problemen oplossen > Radioactive Trace**. Voeg het MAC-adres van de client toe, druk op **Start** en probeer het probleem te reproduceren. Klik op **Generate** om het bestand te maken en te downloaden:

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file	
<input type="checkbox"/>	74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt	▶ Generate

◀ 1 ▶ 20 items per page 1 - 1 of 1 items

Belangrijk: iPhones op IOS 14 en Android 10 smartphones gebruiken gerandomiseerde mac-adressen wanneer ze aan het netwerk worden gekoppeld. Deze functionaliteit kan de iPSK configuratie volledig breken. Zorg dat deze optie uitgeschakeld is!

Als Radioactive Traces niet genoeg zijn om het probleem te identificeren, kunnen pakketopnamen direct op de WLC worden verzameld. Onder **Problemen oplossen > Packet Capture**, voegt u een opnamepunt toe. Standaard gebruikt WLC draadloze beheerinterface voor alle RADIUS AAA-communicatie. Vergroot de buffergrootte tot 100 MB als WLC veel clients heeft:

Edit Packet Capture

Capture Name*

iPSK

Filter*

any

Monitor Control Plane

Buffer Size (MB)*

100

Limit by*

Duration

3600

secs == 1.00 hour

Available (4)

Search



- GigabitEthernet1 →
- GigabitEthernet2 →
- GigabitEthernet3 →
- Vlan1 →

Selected (1)

- Vlan39 ←

In het onderstaande beeld wordt een pakketvastlegging weergegeven van een succesvolle verificatie- en boekhoudpoging. Gebruik dit Wireshark filter om alle relevante pakketten voor deze client uit te filteren:

ip.addr==

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

Probleemoplossing ISE

De belangrijkste techniek voor probleemoplossing op Cisco ISE is de pagina **Live Logs**, die u kunt vinden onder **Operations > RADIUS > Live Logs**. Ze kunnen worden gefilterd door het MAC-adres van de client in het veld Endpoint ID te zetten. Het openen van een volledig ISE-rapport geeft meer details over de reden van het falen. Zorg ervoor dat de client het juiste ISE-beleid aanraakt:

Operations - RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 1

Refresh Never Show Latest 20 records Within Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentic...	Authoriz...	Authorization Pro...	IP Address
Aug 19, 2022 08:04:20.5...	●		1	08:BE:AC:27:8...	08:BE:AC:27:85:7E	Unknown	Policy_Set...	Policy_Set...	Authz_Profile_IPSK	fe80::e864:b6
Aug 19, 2022 08:04:13.3...	✓			08:BE:AC:27:8...	08:BE:AC:27:85:7E	Unknown	Policy_Set...	Policy_Set...	Authz_Profile_IPSK	

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.