

Configureren van Catalyst 9800 draadloze controllers - AP-autorisatielijst

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[MAC AP-autorisatielijst - Lokaal](#)

[MAC AP-autorisatielijst - externe RADIUS-server](#)

[9800 WLC-configuratie](#)

[ISE-configuratie](#)

[Configureer ISE om MAC-adres als endpoints te verifiëren](#)

[Configureer ISE om MAC-adres als gebruikersnaam/wachtwoord te verifiëren](#)

[Vergunningsbeleid voor het verifiëren van AP's](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u het verificatiebeleid voor Catalyst 9800 draadloze LAN-controllers voor access point (AP) kunt configureren.

Achtergrondinformatie

Voor de autorisatie van een access point (AP) moet het Ethernet MAC-adres van het toegangspunt worden geautoriseerd ten opzichte van een lokale database met 9800 draadloze LAN-controller of ten opzichte van een externe Remote Verification Dial-In User Service (RADIUS)-server.

Deze functie zorgt ervoor dat alleen geautoriseerde access points (AP's) zich kunnen aansluiten bij een Catalyst 9800 draadloze LAN-controller. Dit document heeft geen betrekking op AP's van de maaswijdte (1500-serie) waarvoor een mac-filtervermelding nodig is om de controller te verbinden, maar die niet de typische AP-autorisatiestroom volgen (zie referenties).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 9800 WLC
- CLI-toegang (Command Line Interface) tot de draadloze controllers

Gebruikte componenten

980 WLC v16.12

AP 1810W

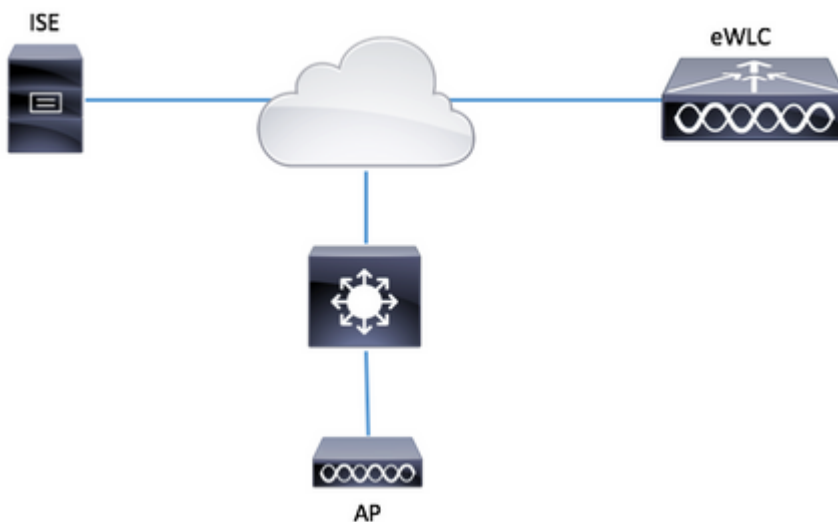
AP 1700

Identity Service Engine (ISE) v2.2

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



Configuraties

MAC AP-autorisatielijst - Lokaal

Het MAC-adres van de geautoriseerde AP's wordt lokaal opgeslagen in de 9800 WLC.

Stap 1. Maak een lokale autorisatie credential-download methodelijst.

Navigeren naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie > + Toevoegen**

Q Search Menu Items

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

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List

Servers / Groups

AA

General

Authentication

Authorization

Accounting

+ Add

Name

default

AuthZ-Netw

Quick Setup: AAA Authorization

Method List Name*

AP-auth

Type*

credential-download

Group Type

local

Available Server Groups

Assigned Server Groups

radius
ldap
tacacs+
ISE-KCG-grp
ISE-grp-name

>

<

Cancel

Save & Apply to Dev

Stap 2. Schakel AP MAC-autorisatie in.

Naar navigeren **Configuratie** > **Beveiliging** > **AAA** > **AAA Advanced** > **AP-beleid**. Schakel **AP's tegen MAC in** en selecteer de **Autorisatiemethode** die in Stap 1 gecreëerd is.

+ AAA Wizard

AAA Method List Servers / Groups **AAA Advanced**

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED

Authorize APs against Serial Number DISABLED

Authorization Method List AP-auth

Stap 3. Voeg het AP ethernetmac-adres toe.

Naar navigeren **Configuratie > Beveiliging > AAA > AAA Geavanceerd > Apparaatverificatie > MAC-adres > + Toevoegen**

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

AP Policy

Password Policy

AAA Interface

MAC Address Serial Number

+ Add × Delete

MAC Address

0 10 items per

Quick Setup: MAC Filtering ✕

MAC Address*	<input type="text" value="00:B0:E1:8C:49:E8"/>
Attribute List Name	<input type="text" value="None"/>

Opmerking: AP ethernetmac-adres moet in een van deze formaten wanneer deze in de web UI worden ingevoerd (xx:xx:xx:xx:xx:xx (of) xxxx.xxxx.xxxx (of) xx-xx-xx-xx-xx-xx) in versie 16.12. In versie 17.3 moeten ze in formaat xxxxxxxxx zijn zonder scheidingstekens. Het CLI-formaat is altijd xxxxxxxxx in elke versie (in 16.12 verwijderd de web-UI de scheidingstekens in het configuratiebestand). Cisco bug-id [CSCv43870](#) maakt het gebruik van elk formaat in CLI of web UI in latere releases mogelijk.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP-autorisatielijst - externe RADIUS-server

9800 WLC-configuratie

Het MAC-adres van de geautoriseerde AP's wordt opgeslagen op een externe RADIUS-server, in dit voorbeeld ISE.

Op ISE kunt u het MAC-adres van de AP's registreren als gebruikersnaam/wachtwoord of als Endpoints. Tijdens de stappen wordt u uitgelegd hoe u de ene of de andere manier moet selecteren.

GUI:

Stap 1. RADIUS-server declareren

Navigeren naar **Configuratie > Beveiliging > AAA > servers / groepen > RADIUS > servers > +** De RADIUS-serverinformatie **toevoegen** en invoeren.

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List **Servers / Groups** AAA Advanced

+ Add x Delete

RADIUS

TACACS+

Server Groups

Servers

Name Address

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 die CoA vereist).

Create AAA Radius Server

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

Cancel

Save & Apply to Dev

Stap 2. De RADIUS-server aan een RADIUS-groep toevoegen

Navigeren naar **Configuratie > Beveiliging > AAA > servers / groepen > RADIUS > Servergroepen > + Toevoegen**

Om ISE-verificatie van het AP MAC-adres als gebruikersnamen te hebben, laat MAC-filtering als geen.

Create AAA Radius Server Group

Name* ISE-grp-name

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers

Assigned Servers ISE-kcg

Cancel Save & Apply to Device

Als u ISE-verificatie van het AP MAC-adres als eindpunten wilt hebben, wijzigt u MAC-filtering in Mac.

Create AAA Radius Server Group

Name* ISE-grp-name

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering mac

Dead-Time (mins) 1-1440

Available Servers

Assigned Servers ISE-KCG

Cancel Save & Apply to Device

Stap 3. Maak een autorisatie credential-download methodelijst.

Navigeren naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie > + Toevoegen**

Q Search Menu Items

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

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List

Servers / Groups

AA

General

Authentication

Authorization

Accounting

+ Add

Name

default

AuthZ-Netw

Quick Setup: AAA Authorization

Method List Name*

AP-ISE-auth

Type*

credential-download ▼

Group Type

group ▼

Fallback to local

Available Server Groups

Assigned Server Groups

radius
ldap
tacacs+
ISE-KCG-grp



ISE-grp-name

Cancel

Save & Apply to Dev

Stap 4. Schakel AP MAC-autorisatie in.

Naar navigeren **Configuratie** > **Beveiliging** > **AAA** > **AAA Advanced** > **AP-beleid**. Schakel AP's tegen **MAC in** en selecteer de **lijst met autorisatiemethoden die** in stap 3 is gemaakt.

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups **AAA Advanced**

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED

Authorize APs against Serial Number DISABLED

Authorization Method List

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 authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISE-configuratie

Stap 1. De 9800 WLC toevoegen aan ISE:

[Verklaar 9800 WLC op ISE](#)

Kies om te configureren op basis van verificatie van het MAC-adres van AP's met de vereiste stappen:

[Gebruik configureren om MAC-adres als eindpunten te verifiëren](#)

[Configureer ISE om MAC-adres als gebruikersnaam/wachtwoord te verifiëren](#)

Configureer ISE om MAC-adres als endpoints te verifiëren

Stap 2. (optioneel) Maak een identiteitsgroep voor access points

Omdat de 9800 het kenmerk NAS-poorttype niet met AP-autorisatie verstuurt Cisco bug [IDCSCvy74904](#)) herkent ISE een AP-autorisatie niet als een MAB-workflow en daarom is het niet mogelijk om een AP te authenticeren als het MAC-adres van de AP in de eindpuntlijst wordt geplaatst, tenzij u de MAB-workflows wijzigt om het NAS-POORT-type attribuut op ISE niet te vereisen.

Navigeer naar **Beheerder > Apparaatprofiel netwerk** en maak een nieuw apparaatprofiel. Schakel RADIUS in en voeg service-type=call-check toe voor bekabelde MAB. U kunt de rest van het oorspronkelijke profiel van Cisco kopiëren. Het idee is dat u voor de bekabelde MAB geen conditie "nas-port-type" hebt.

* Name Ciscotemp

Description

Icon



Change icon...

Set To Default



Vendor Cisco

Supported Protocols

- RADIUS
- TACACS+
- TrustSec

RADIUS Dictionaries

Templates

[Expand All](#) / [Collapse All](#)

Authentication/Authorization

Flow Type Conditions

Wired MAB detected if the following condition(s) are met :



Radius:Service-Type



=

Call Check



Ga terug naar uw netwerkkapparaat voor de 9800 en stel het profiel in op het nieuwe apparaatprofiel.

Ga naar **Beheer > Identiteitsbeheer > Groepen > Endpoint Identity Groups > + Add.**

Identity Groups

Search:

Navigation:

Endpoint Identity Groups

Endpoint Identity Groups

Edit Add Delete

Name	De
------	----

Kies een naam en klik op **Indienen**.

Endpoint Identity Group List > **New Endpoint Group**

Endpoint Identity Group

* Name

Description

Parent Group

Stap 3. Voeg het AP ethernetmac-adres toe aan de bijbehorende endpointgroep.

Navigeren naar **werkcentra > Netwerktogang > Identiteiten > Endpoints > +**

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > Id Groups > Ext Id Sources > Network Resources > Policy Elements > Authentication Policy > Authorization Policy

Endpoints

Network Access Users

Identity Source Sequences

INACTIVE ENDPOINTS ¹

0 Selected

Refresh + Delete Edit ANC Change Authorization Clear Threats & Vulnerabilities

MAC Address	Status	IPv4 Address	Username
-------------	--------	--------------	----------

Voer de gewenste informatie in.

Add Endpoint



General Attributes

Mac Address * 00:B0:E1:8C:49:E8

Description Access Point

Static Assignment

Policy Assignment Unknown

Static Group Assignment

Identity Group Assignment AccessPoints

Cancel

Save

Stap 4. Controleer of het identiteitsarchief dat op uw standaardverificatieregel wordt gebruikt, de interne

endpoints bevat.

A. Navigeer naar **Beleid** > **Verificatie** en neem kennis van het identiteitsarchief.

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MAB	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : A

B. Ga naar **Beheer** > **Identity Management** > **Identity Source Sequences** > **Identity Name**.

Identity Source Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	All_User_ID_Stores	A built-in Identity Sequence to include all User
<input type="checkbox"/>	Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Requ
<input type="checkbox"/>	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Porta
<input type="checkbox"/>	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices
<input type="checkbox"/>	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Po

C. Zorg ervoor dat de interne endpoints er deel van uitmaken, en voeg deze toe als dat niet het geval is.

[Identity Source Sequences List](#) > [All_User_ID_Stores](#)

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

<input type="text" value="Internal Endpoints"/>

Selected

<input type="text" value="Internal Users"/> <input type="text" value="All_AD_Join_Points"/> <input type="text" value="Guest Users"/>
--

<input type="text" value=">"/>
<input type="text" value="<"/>
<input type="text" value=">>"/>
<input type="text" value="<<"/>

▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

<input type="button" value="Save"/>	<input type="button" value="Reset"/>
-------------------------------------	--------------------------------------

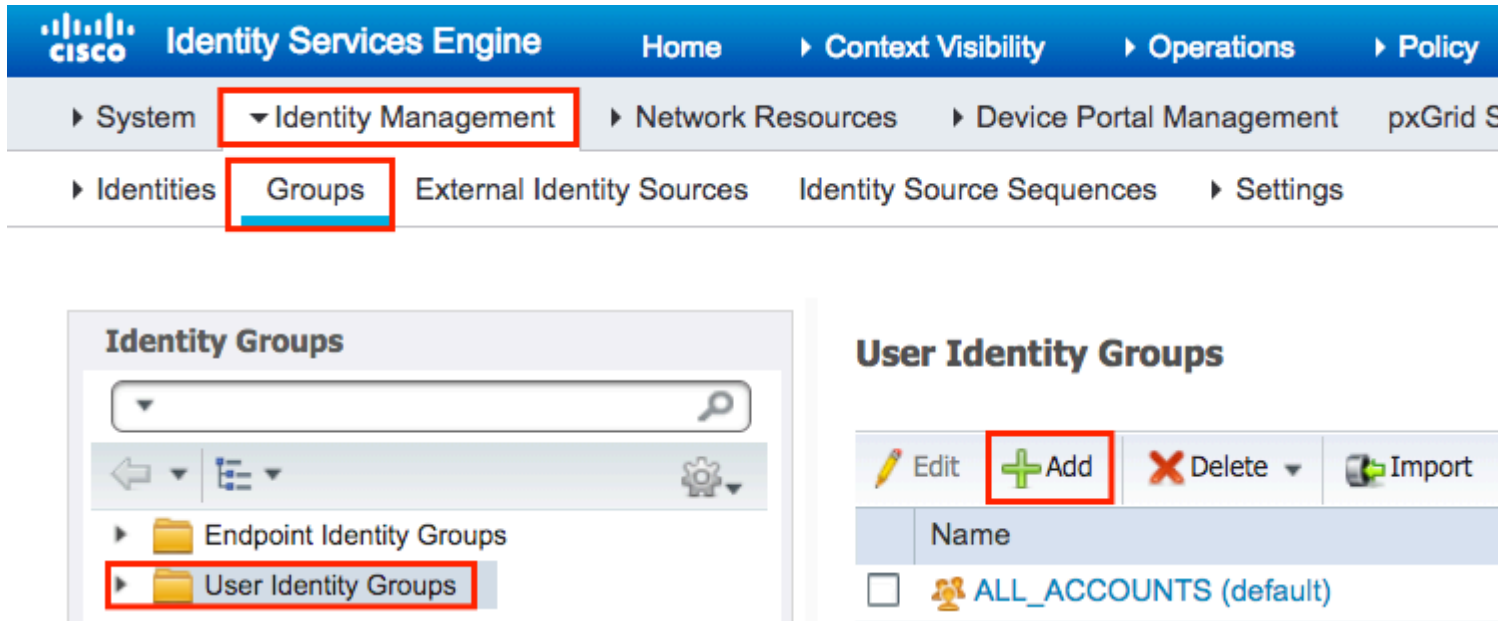
Configureer ISE om MAC-adres als gebruikersnaam/wachtwoord te verifiëren

Deze methode wordt niet geadviseerd aangezien het lager wachtwoordbeleid vereist om het zelfde wachtwoord toe te staan zoals de gebruikersbenaming.

Het kan echter wel een tijdelijke oplossing zijn voor het geval u uw netwerkkapparaatprofiel niet kunt wijzigen

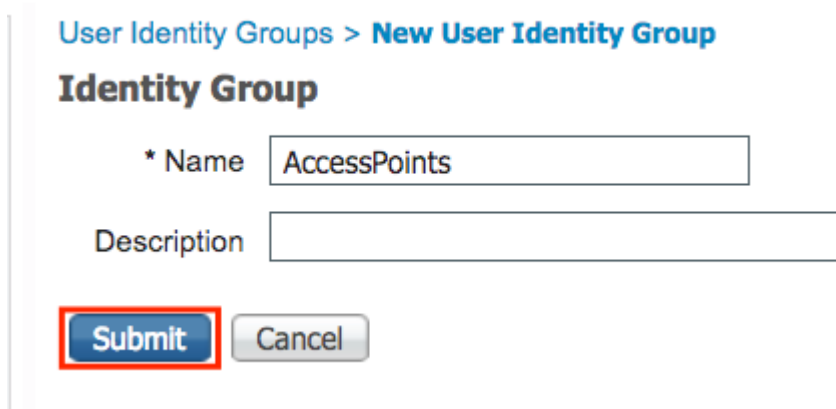
Stap 2. (optioneel) Maak een identiteitsgroep voor access points

Ga naar **Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > + Toevoegen**.



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation menu at the top includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. Below this, 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid S' are visible. The 'Identity Management' menu is expanded, showing 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' menu item is highlighted with a red box. Below the navigation, the 'Identity Groups' panel is shown, with a search bar and a list of groups: 'Endpoint Identity Groups' and 'User Identity Groups'. The 'User Identity Groups' folder is highlighted with a red box. To the right, the 'User Identity Groups' panel is shown, with a table of groups. The 'Add' button is highlighted with a red box.

Kies een naam en klik op **Indienen**.



The screenshot shows the 'New User Identity Group' form in the Cisco ISE web interface. The form has a title 'User Identity Groups > New User Identity Group' and a sub-title 'Identity Group'. There are two input fields: '* Name' with the value 'AccessPoints' and 'Description'. Below the fields are two buttons: 'Submit' and 'Cancel'. The 'Submit' button is highlighted with a red box.

Stap 3. Controleer dat je huidige wachtwoordbeleid je in staat stelt om een mac-adres toe te voegen als gebruikersnaam en wachtwoord.

Ga naar **Beheer > Identity Management > Instellingen > Gebruikersverificatie-instellingen > Wachtwoordbeleid** en controleer of ten minste deze opties zijn uitgeschakeld:

Cisco Identity Services Engine Home > Context Visibility > Operations > Policy > Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed

Identities Groups External Identity Sources Identity Source Sequences Settings

User Custom Attributes

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Password Policy

Account Disable Policy

Password Policy

- Minimum Length: characters (Valid Range 4 to 127)

Password must not contain:

- User name or its characters in reverse order
- "cisco" or its characters in reverse order
- This word or its characters in reverse order:
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced w

Default Dictionary ⓘ

Custom Dictionary ⓘ No file chosen

The newly added custom dictionary file will replace the existing cust

Password must contain at least one character of each of the selected types

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- Password must be different from the previous versions (Valid Range
- Password change delta characters (Valid Range 3 to 10)
- Cannot reuse password within days (Valid Range 0 to 365)

Password Lifetime

Users can be required to periodically change password

- Disable user account after days if password was not
- Display reminder days prior to password expiration (
- Lock/Suspend Account with Incorrect Login Attempts

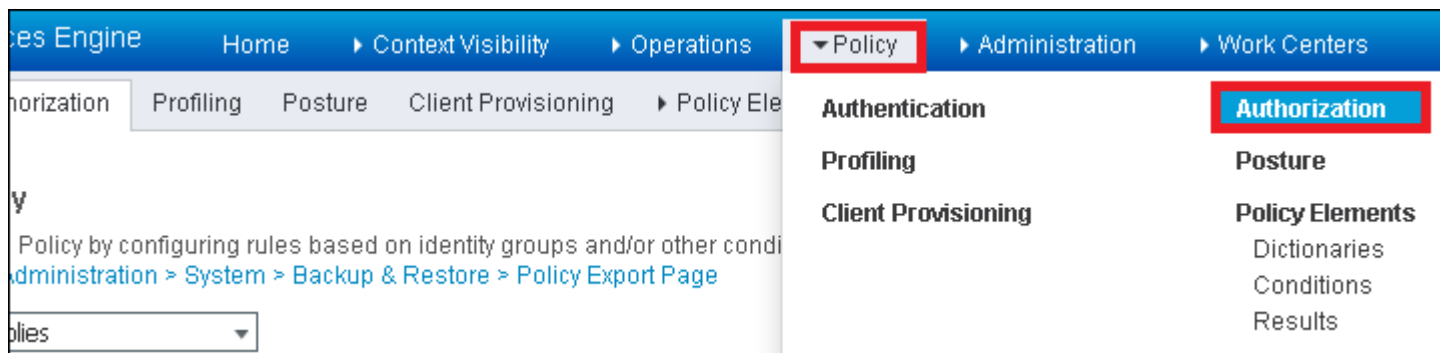
- # (Valid Range 3 to 20)
- Suspend account for minutes (Valid Range 15 to 1440) D

Opmerking: u kunt ook de optie **Gebruikersaccount uitschakelen na XX dagen** uitschakelen als het wachtwoord niet is

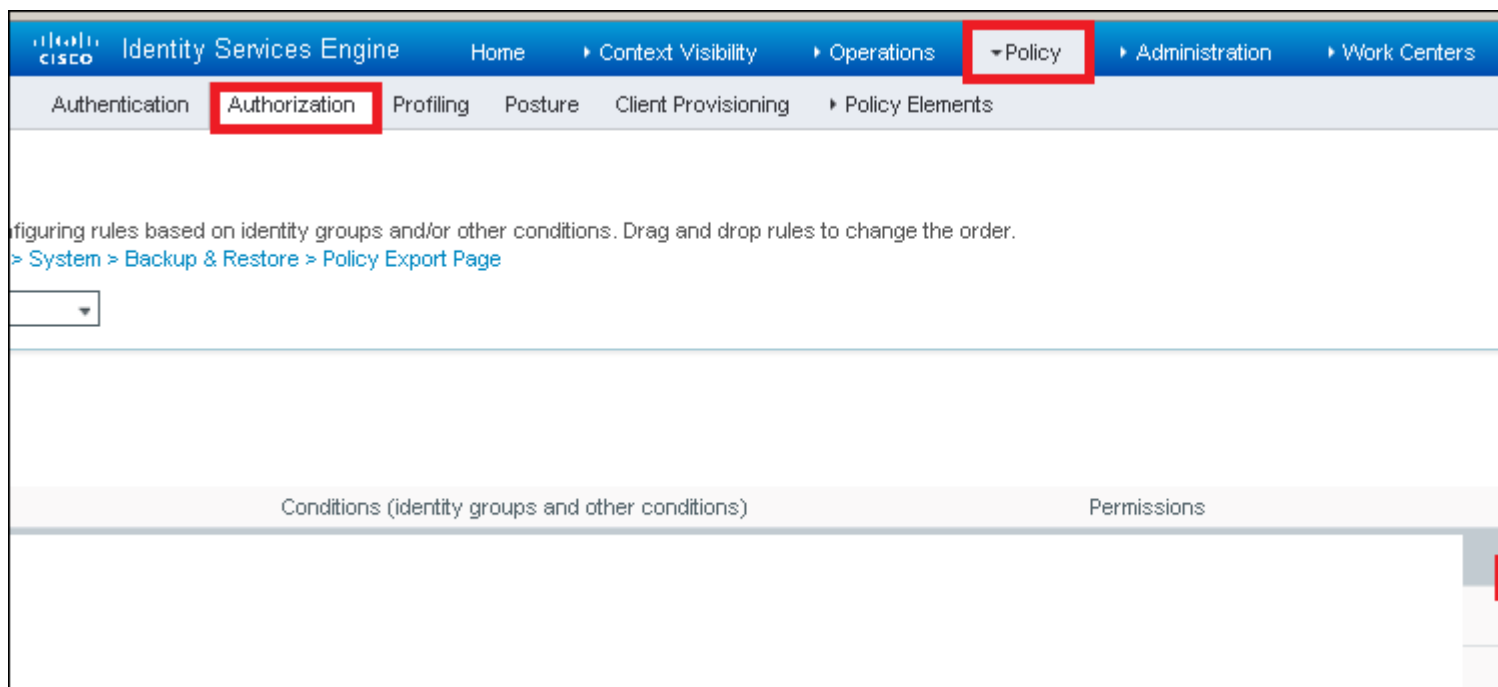
Wachtwoord Veld moet het Ethernet MAC-adres van het AP zijn, alle kleine letters en geen scheidingstekens.

Vergunningsbeleid voor het verifiëren van AP's

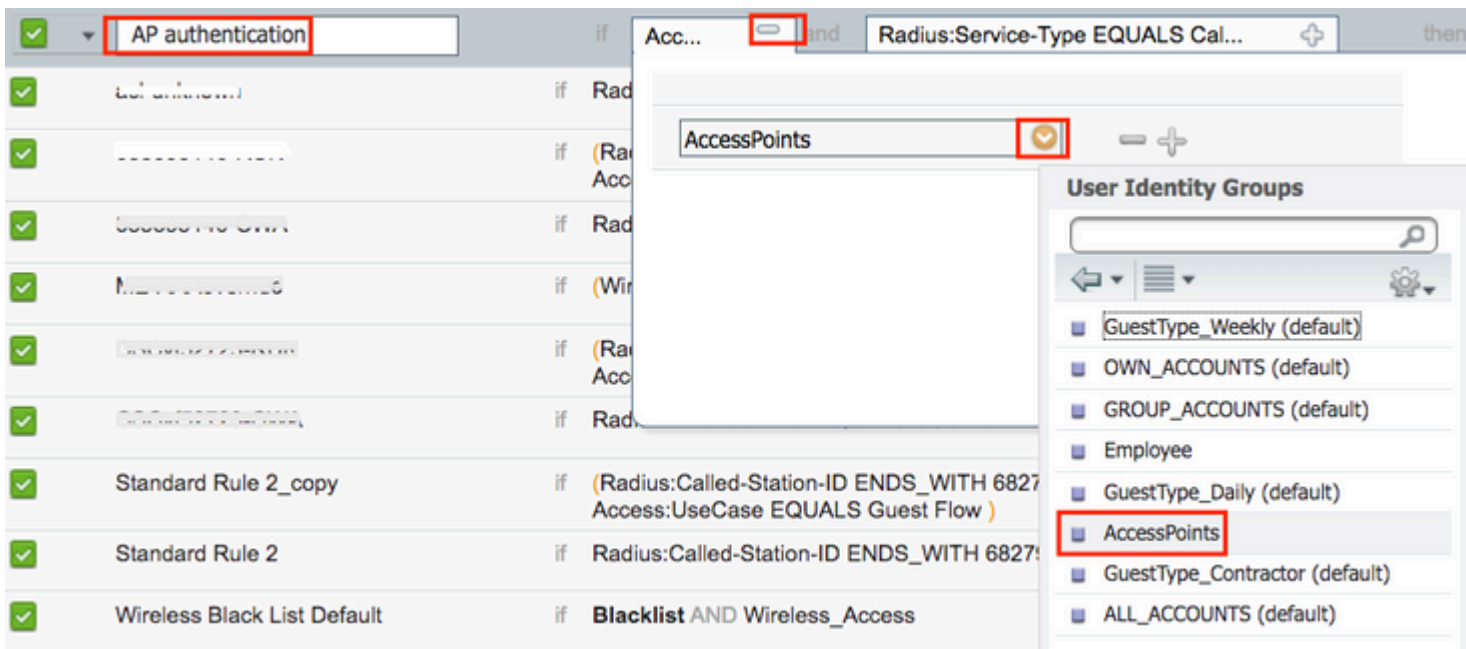
Navigeer naar **Beleid > Autorisatie** zoals in de afbeelding.



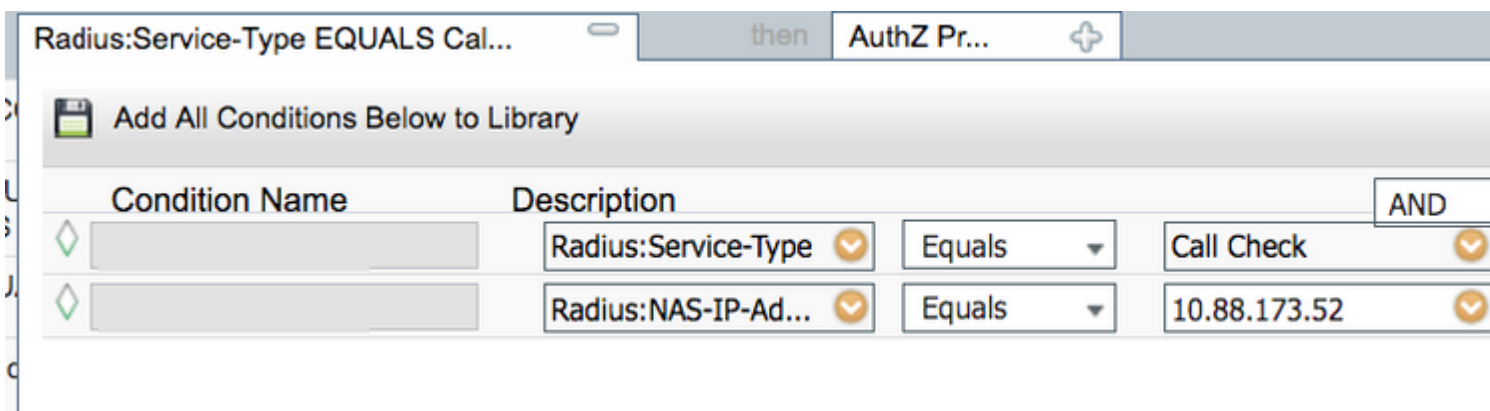
Plaats een nieuwe regel zoals in de afbeelding.



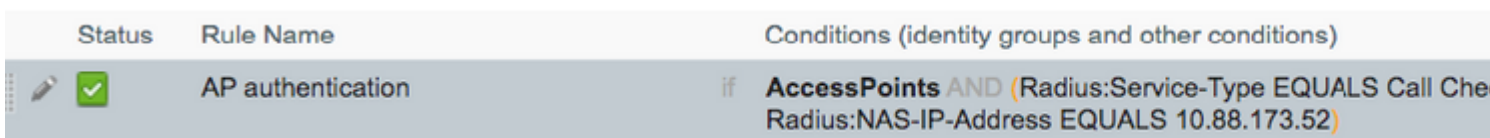
Selecteer eerst een naam voor de regel en de groep Identity waarin het access point is opgeslagen (Access points). Selecteer **Gebruikersidentiteitsgroepen** als u hebt besloten het MAC-adres te verifiëren als een gebruikersnaam, wachtwoord of **Endpoint Identity Groups** als u ervoor kiest het AP MAC-adres als eindpunten te authenticeren.



Selecteer vervolgens andere voorwaarden die ervoor zorgen dat het autorisatieproces onder deze regel valt. In dit voorbeeld raakt het autorisatieproces deze regel als het servicetype Call Check gebruikt en het verificatieverzoek komt van het IP-adres 10.8.173.52.



Selecteer tot slot het autorisatieprofiel dat is toegewezen aan de clients die op die regel zijn ingesteld. Klik vervolgens op Doneren en sla het op zoals in de afbeelding.



Opmerking: AP's die al zijn aangesloten bij de controller verliezen hun associatie niet. Als echter, nadat de autorisatielijst is ingeschakeld, ze de communicatie met de controller verliezen en proberen terug te keren, gaan ze door het verificatieproces. Als hun mac-adressen niet lokaal of in de RADIUS-server staan vermeld, kunnen ze niet teruggaan naar de controller.

Verifiëren

Controleer of de 9800 WLC ap-verificatielijst heeft ingeschakeld

```
<#root>
```

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled  
Authorize APs against Serial Num : Enabled  
Authorization Method List : <auth-list-name>
```

Controleer de radiusconfiguratie:

```
<#root>
```

```
#
```

```
show run aaa
```

Problemen oplossen

WLC 9800 biedt ALTIJD-ON traceermogelijkheden. Dit zorgt ervoor dat alle AP toetreden gerelateerde fouten, waarschuwing en meldingen niveau berichten constant worden geregistreerd en u kunt logbestanden bekijken voor een incident of fout situatie nadat het is voorgekomen.

Opmerking: het volume van de gegenereerde logbestanden varieert van enkele uren tot enkele dagen.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC via deze stappen (zorg ervoor dat u de sessie aan een tekstbestand registreert).

Stap 1. Controleer de huidige controllertijd zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem zich voordeed.

```
# show clock
```

Stap 2. Verzamel syslogs van de controllerbuffer of externe syslog zoals die door de systeemconfiguratie wordt gedictieerd. Dit geeft een snelle weergave van de eventuele gezondheids- en fouten in het systeem.

```
# show logging
```

Stap 3. Controleer of de debug-voorwaarden zijn ingeschakeld.

```
# show debugging  
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

IOSXE Packet Trace Configs:

Packet Infra debugs:

Ip Address	Port
-----	-----

Opmerking: als u een van de vermelde voorwaarden ziet, betekent dit dat de sporen zijn aangemeld om het debug-niveau te bereiken voor alle processen die de ingeschakelde voorwaarden ervaren (mac-adres, ip-adres, etc.). Dit zou het volume van de boomstammen doen toenemen. Daarom wordt aanbevolen alle voorwaarden te wissen wanneer niet actief debuggen

Stap 4. Stel dat het geteste mac-adres niet als een voorwaarde in Stap 3 is vermeld, verzamel de altijd-op-meldniveau sporen voor het specifieke radio mac-adres.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Voorwaardelijke debugging en radio actieve tracering

Als de altijd-on sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-spoor opnemen, dat debug level traces biedt voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval).

Stap 5. Zorg ervoor dat de debug-voorwaarden niet zijn ingeschakeld.

```
# clear platform condition all
```

Stap 6. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdracht wordt het opgegeven MAC-adres 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Opmerking: als u meer dan één client tegelijk wilt bewaken, voert u de opdracht debug wireless mac <aaaa.bbbb.ccc> per mac-adres uit.

Opmerking: U ziet de output van de client activiteit op de terminal sessie niet, omdat alles intern wordt gebufferd om later bekeken te worden.

Stap 7. Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 8. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Zodra de monitor-tijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam:

```
ra_trace_MAC_aabbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 9. Verzamel het bestand van de mac-adresactiviteit. U kunt het spoor .log naar een externe server kopiëren of de uitvoer direct op het scherm weergeven.

Controleer de naam van het RA traces bestand

```
# dir bootflash: | inc ra_trace
```

Kopieert het bestand naar een externe server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Geef de inhoud weer:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 10. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer breedspakige mening van debug niveaulogboeken zijn. U hoeft niet opnieuw te debuggen de client als we alleen een verdere gedetailleerde kijk op debug logs die al zijn verzameld en intern opgeslagen.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra
```

Opmerking: deze opdrachtoutput geeft sporen voor alle registratieniveaus voor alle processen en is vrij omvangrijk. Neem contact op met Cisco TAC om te helpen bij het doorlopen van deze sporen.

U kunt de Ra-internal-FILENAME.txt kopiëren naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Kopieert het bestand naar een externe server:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Geef de inhoud weer:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Stap 11. Verwijder de debug-voorwaarden.

```
# clear platform condition all
```

Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossing sessie.

Referenties

[Koppel de AP's aan de 9800 WLC](#)

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.