

# De autorisatie voor access points configureren in een Unified Wireless Network

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Lichtgewicht AP-autorisatie](#)

[Configureren](#)

[Configuratie met behulp van de interne autorisatielijst op de WLC](#)

[Verifiëren](#)

[AP-autorisatie tegen een AAA-server](#)

[Configuratie van Cisco ISE voor autorisatie van AP's](#)

[Een nieuw apparaatprofiel configureren waar MAB geen NAS-poorttype kenmerk vereist](#)

[De WLC configureren als een AAA-client op Cisco ISE-lijnkaart](#)

[Voeg het AP MAC-adres toe aan de Endpoint Database op Cisco ISE](#)

[Voeg het AP MAC-adres toe aan de gebruikersdatabase op Cisco ISE \(optioneel\)](#)

[Een beleidsset definiëren](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft hoe u WLC moet configureren om het access point (AP) te autoriseren op basis van het MAC-adres van de AP's.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de configuratie van een Cisco Identity Services Engine (ISE)
- Kennis van de configuratie van Cisco AP's en Cisco WLC's
- Kennis van Cisco Unified Wireless Security oplossingen

### Gebruikte componenten

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

- WLC's met AireOS 8.8.11.0-softwareWave1 APs: 1700/2700/3700 en 3500 (1600/2600/3600)

wordt nog steeds ondersteund, maar AireOS-ondersteuning eindigt op versie 8.5.x)Wave2 access points: 1800/2800/3800/4800, 1540 en 1560 ISE-versie 2.3.0.298

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.

## Lichtgewicht AP-autorisatie

Tijdens het AP registratieproces, authenticeren APs en WLCs wederzijds met het gebruik van X.509- certificaten. De X.509-certificaten worden in de fabriek op zowel de AP als WLC in beschermde flitser gebrand door Cisco.

Op het toegangspunt worden in de fabriek geïnstalleerde certificaten Manufacturing-Install Certificates (MIC) genoemd. Alle Cisco AP's die na 18 juli 2005 zijn geproduceerd, hebben MIC's.

Naast deze wederzijdse verificatie die tijdens het registratieproces plaatsvindt, kunnen de WLC's ook de AP's beperken die zich met hen registreren op basis van het MAC-adres van de AP.

Het ontbreken van een sterk wachtwoord met het gebruik van het MAC-adres van het toegangspunt is geen probleem, omdat de controller MIC gebruikt om het toegangspunt te verifiëren voordat het via de RADIUS-server is geautoriseerd. Het gebruik van MIC zorgt voor sterke authenticatie.

AP-autorisatie kan op twee manieren worden uitgevoerd:

- De interne autorisatielijst in de WLC gebruiken
- De MAC-adresdatabase op een AAA-server gebruiken

De gedragingen van de toegangspunten verschillen op basis van het gebruikte certificaat:

- APs met SSCs—De WLC gebruikt alleen de interne autorisatielijst en stuurt geen verzoek naar een RADIUS-server voor deze APs
- APs met MICs—WLC kan of de Interne die Autorisatielijst gebruiken op WLC wordt gevormd of een server van RADIUS gebruiken om APs te machtigen

In dit document wordt de AP-autorisatie besproken met behulp van zowel de interne autorisatielijst als de AAA-server.

## Configureren

### Configuratie met behulp van de interne autorisatielijst op de WLC

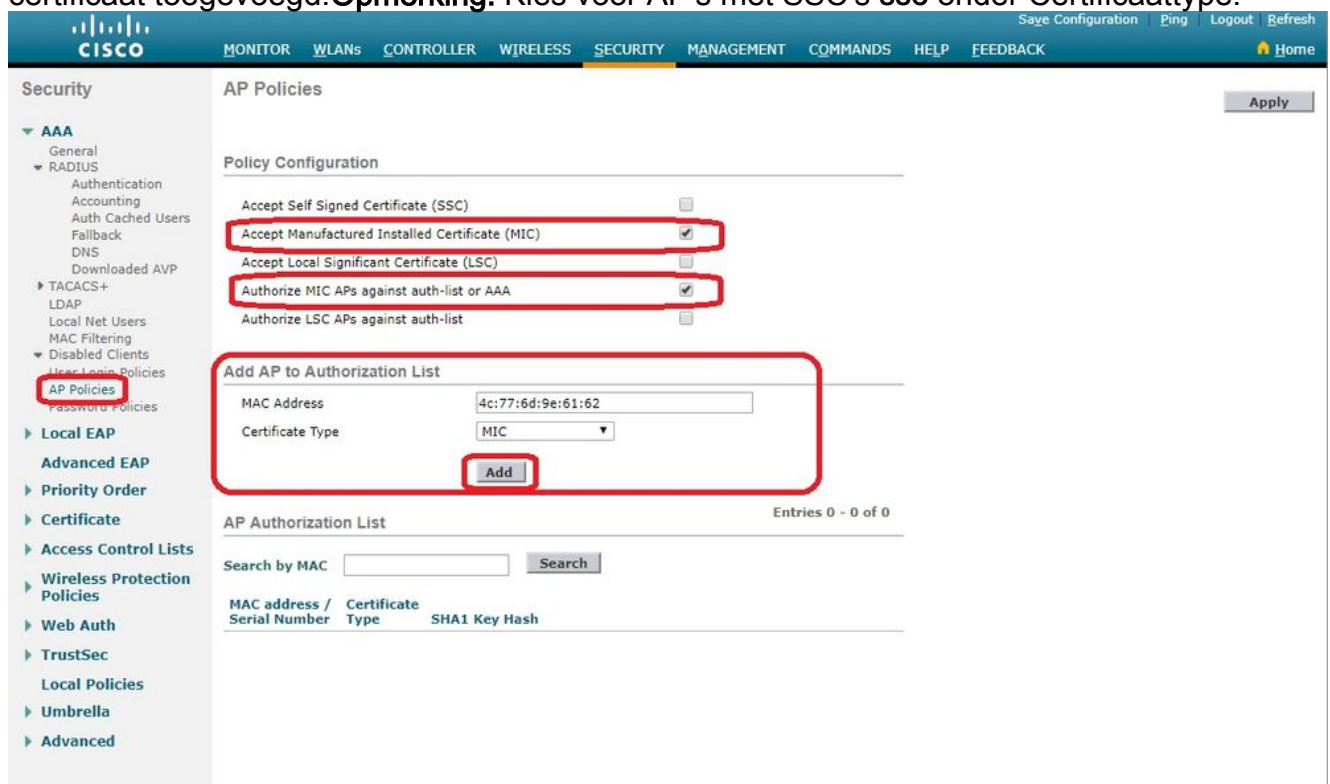
Voor WLC, gebruik de AP vergunningslijst om APs te beperken die op hun adres van MAC worden gebaseerd. De autorisatielijst van het toegangspunt is beschikbaar onder **Security > AP Policies** in de WLC GUI.

Dit voorbeeld toont hoe de AP met het adres van MAC moet worden toegevoegd 4c:77:6d:9e:61:62.

1. Klik vanuit de WLC-controller GUI op **Security > AP Policies** en de pagina AP-beleid verschijnt.
2. Klik op de **Add** aan de rechterkant van het scherm.



3. Onder **Add AP to Authorization List**, de **AP MAC** adres (niet het adres van het AP-radiostation). Kies vervolgens het certificaattype en klik op **Add**. In dit voorbeeld wordt een AP met een MIC certificaat toegevoegd. **Opmerking:** Kies voor AP's met SSC's **ssc** onder Certificaattype.



Het toegangspunt wordt toegevoegd aan de autorisatielijst van het toegangspunt en wordt vermeld onder **AP Authorization List**.

4. Controleer onder **Beleidsconfiguratie** het vakje voor **Authorize MIC APs against auth-list or AAA**. Wanneer deze parameter is geselecteerd, controleert de WLC eerst de lokale autorisatielijst. Als de AP-MAC niet aanwezig is, controleert deze de RADIUS-server.

The screenshot shows the Cisco Security configuration interface. The left sidebar has 'AP Policies' selected. The main area shows 'AP Policies' configuration. Under 'Policy Configuration', the checkbox for 'Authorize MIC APs against auth-list or AAA' is checked. Below this is the 'AP Authorization List' table with 5 entries. The first entry has MAC address 4c:77:6d:9e:61:62 and Certificate Type MIC. The 'Apply' button at the top right is highlighted.

## Verifiëren

Om deze configuratie te verifiëren, moet u AP verbinden met het adres van MAC **4c:77:6d:9e:61:62** naar het netwerk en de monitor. Gebruik de **debug capwap events/errors enable** en **debug aaa all enable** opdrachten om dit uit te voeren.

Deze output laat de debugs zien wanneer het AP MAC-adres niet in de AP-autorisatielijst staat:

**Opmerking:** Enkele lijnen in de output zijn verplaatst naar de tweede lijn toe te schrijven aan ruimtebeperkingen.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5256, already allocated index 277
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved)
```

```
*spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
```

```
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.
```

```
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state
```

```
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
```

**70:69:5a:51:4e:c0**

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed!

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256

\*aaaQueueReader: Feb 27 10:15:25.593: **Unable to find requested user entry for 4c776d9e6162**

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9

\*aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 40000001

\*aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638

\*aaaQueueReader: Feb 27 10:15:25.593: Callback.....0xd6cef02166

\*aaaQueueReader: Feb 27 10:15:25.593: protocolType.....0x40000001

\*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00

\*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs:

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.....4c776d9e6162 (12 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[02] Called-Station-Id.....70-69-5a-51-4e-c0 (17 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[03] Calling-Station-Id.....4c-77-6d-9e-61-62 (17 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[07] User-Password.....[...]

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator.....DATA (16 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0

\*aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770

\*aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0)

\*aaaQueueReader: Feb 27 10:15:25.593: resultCode.....-7

\*aaaQueueReader: Feb 27 10:15:25.593: protocolUsed.....0xffffffff

\*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00

\*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs:

```

*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls Connection.
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session 0xd6f0724fd8 for AP (192.168.79.151/5256). Notify(true)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys: lrad:192.168.79.151(5256) mwar:10.48.71.20(5246)

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted successfully for AP 192.168.79.151

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver (10.48.71.20/5246) client (192.168.79.151/5256)
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for 192.168.79.151:5256

```

Deze output toont de debugs wanneer het adres van MAC van het LAP aan de AP vergunningslijst wordt toegevoegd:

**Opmerking:** Enkele lijnen in de output zijn verplaatst naar de tweede lijn toe te schrijven aan ruimtebeperkingen.

```

(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 274

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from temporary database.
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP

```

```

:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is
not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
70:69:5a:51:4e:c0
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed!

*aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA
Authentication : 0
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile
70:69:5a:51:4e:c0
*aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408

*aaaQueueReader: Feb 27 09:50:25.394: structureSize.....194
*aaaQueueReader: Feb 27 09:50:25.394: resultCode.....0
*aaaQueueReader: Feb 27 09:50:25.394:
proxyState.....70:69:5A:51:4E:C0-00:00
*aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs:
*aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-
Type.....0x00000065 (101) (4 bytes)
*aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-
Identifier.....0x00000000 (0) (4 bytes)
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB
on WLAN ID :0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap_ac_platform.c:2095 - Operation State
0 ==> 4
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from
capwap_ac_platform.c 2136
*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP
70:69:5a:51:4e:c0 slot 0

```

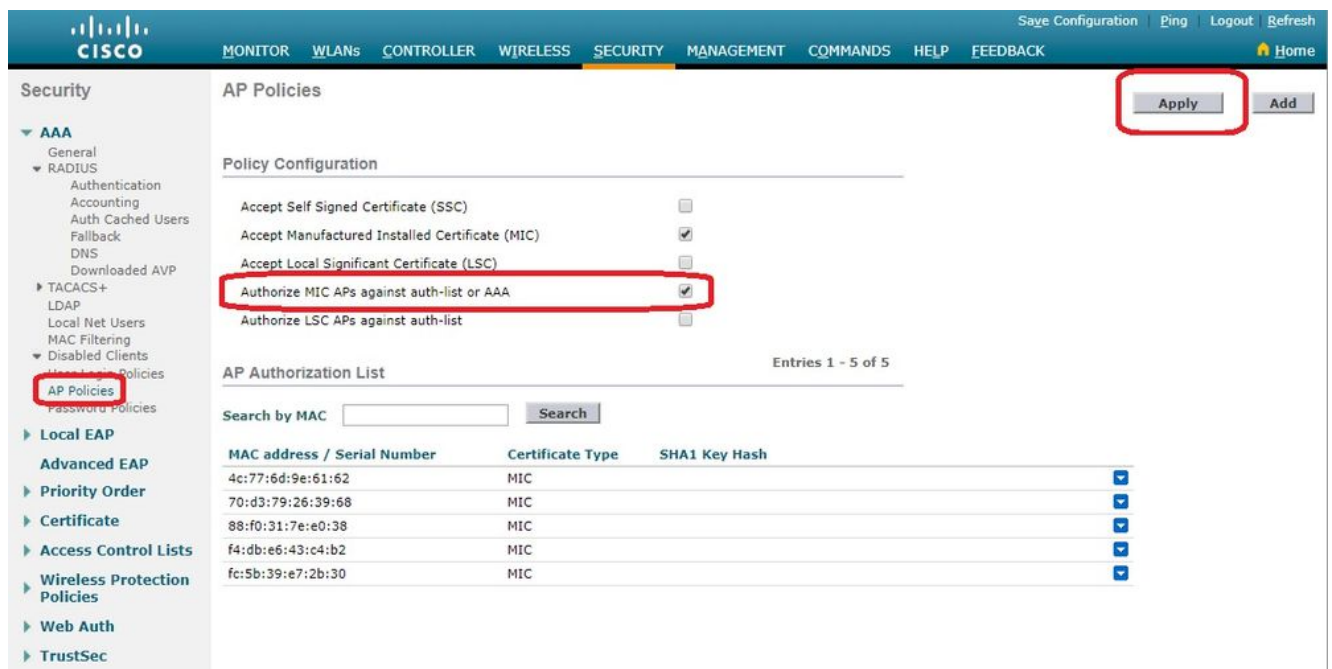
## AP-autorisatie tegen een AAA-server

U kunt WLC's ook configureren om RADIUS-servers te gebruiken om AP's te autoriseren met behulp van MIC's. De WLC gebruikt een AP MAC-adres als gebruikersnaam en wachtwoord bij

het verzenden van de informatie naar een RADIUS-server. Bijvoorbeeld als het MAC-adres van het toegangspunt **4c:77:6d:9e:61:62**. Zowel de gebruikersnaam als het wachtwoord dat door de controller wordt gebruikt voor de autorisatie van het toegangspunt, zijn dat mac-adres met behulp van de gedefinieerde scheidingsteken.

Dit voorbeeld toont hoe de WLC's moeten worden geconfigureerd om AP's te autoriseren met Cisco ISE.

1. Klik vanuit de WLC-controller GUI op **Security > AP Policies**. De pagina AP-beleid verschijnt.
2. Controleer onder Beleidsconfiguratie het vakje voor **Authorize MIC APs against auth-list or AAA**. Wanneer u deze parameter kiest, controleert WLC eerst de lokale autorisatielijst. Als de AP-MAC niet aanwezig is, controleert deze de RADIUS-server.

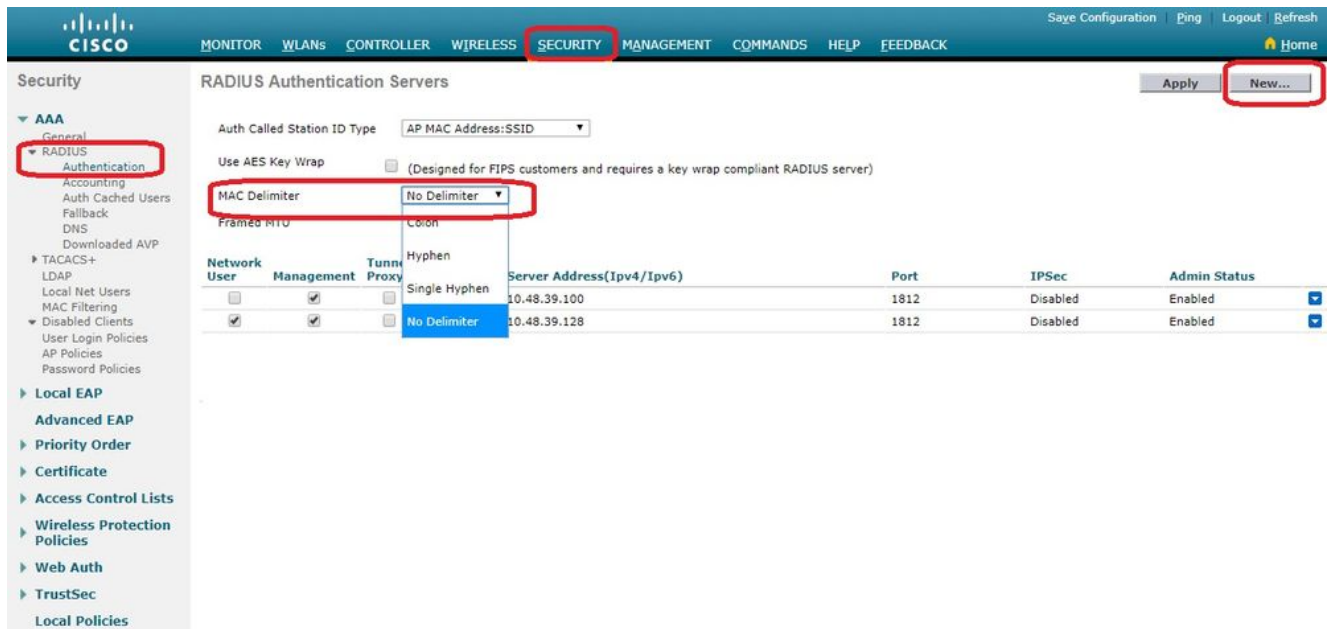


The screenshot shows the Cisco WLC GUI with the 'Security' tab selected. The left sidebar has 'AP Policies' highlighted. The main content area shows the 'AP Policies' configuration page. The 'Policy Configuration' section has several checkboxes, with 'Authorize MIC APs against auth-list or AAA' checked and highlighted by a red box. The 'AP Authorization List' section shows a table with 5 entries:

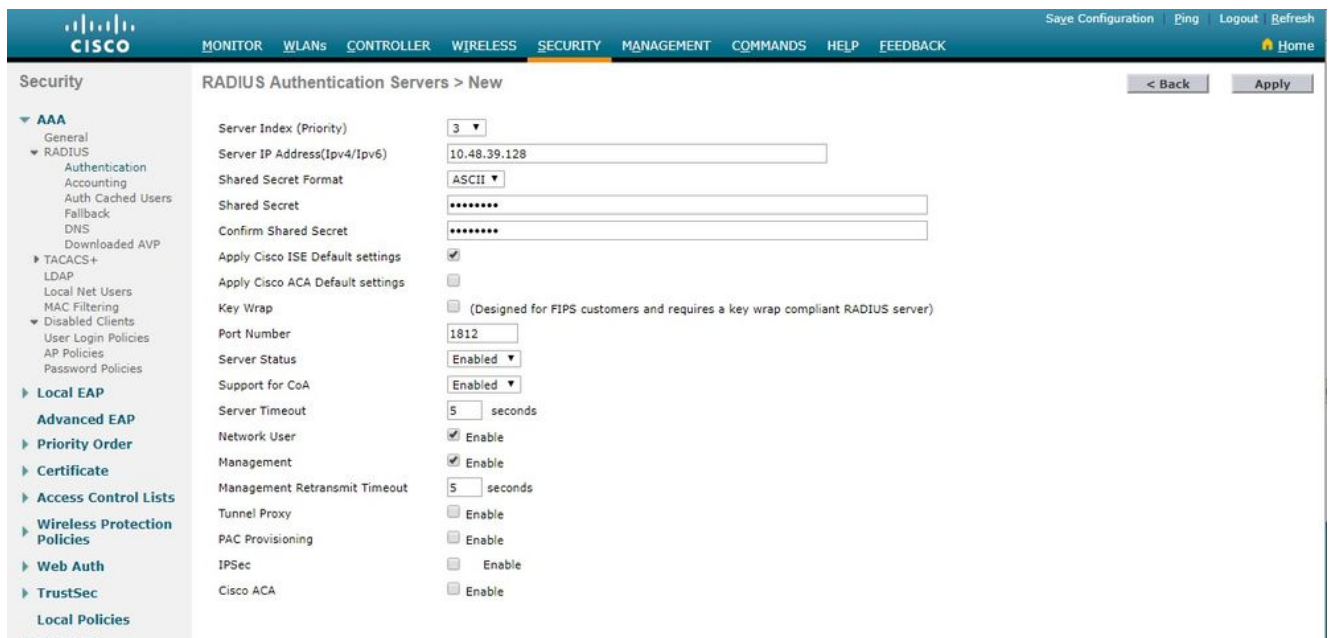
MAC address / Serial Number	Certificate Type	SHA1 Key Hash
4c:77:6d:9e:61:62	MIC	
70:d3:79:26:39:68	MIC	
88:f0:31:7e:e0:38	MIC	
f4:db:e6:43:c4:b2	MIC	
fc:5b:39:e7:2b:30	MIC	

3. Navigeer naar **Security > RADIUS Authentication** van de controller GUI om de **RADIUS Authentication Servers** pagina. Op deze pagina kunt u de **MAC-scheidingsteken** definiëren. De WLC krijgt het AP Mac-adres en stuurt het naar de Radius Server met behulp van de hier gedefinieerde scheidingsteken. Dit is belangrijk zodat de gebruikersnaam overeenkomt met wat is geconfigureerd in de Radius-server. In dit voorbeeld **No Delimiter** wordt gebruikt zodat de gebruikersnaam **4c776d9e6162**.





4. Klik vervolgens op **New** om een RADIUS-server te definiëren.



5. Definieer de RADIUS-serverparameters op de RADIUS Authentication Servers > New pagina. Deze parameters omvatten de RADIUS Server IP Address, Shared Secret, Port Number, en Server Status. Als u klaar bent, klikt u op **Apply**. In dit voorbeeld wordt Cisco ISE gebruikt als de RADIUS-server met IP-adres 10.48.39.128.

## Configuratie van Cisco ISE voor autorisatie van AP's

U dient de volgende stappen te voltooien om Cisco ISE in staat te stellen access points te autoriseren:

1. Configureer de WLC als een AAA-client op Cisco ISE.
2. Voeg de AP MAC-adressen toe aan de database op Cisco ISE.

U kunt het AP MAC-adres echter toevoegen als eindpunten (de beste manier) of als gebruikers (wier wachtwoorden ook het MAC-adres zijn), maar dit vereist dat u de vereisten voor wachtwoordbeveiligingsbeleid verlaagt.

Vanwege het feit dat de WLC niet de NAS-Port-Type attribuut verstuurt, wat een vereiste is voor ISE om de Mac-adresverificatie (MAB) te matchen, moet u dit bijstellen.

## Een nieuw apparaatprofiel configureren waar MAB geen NAS-poorttype kenmerk vereist

Navigeer naar **Administration > Network device profile** en maakt u een nieuw apparaatprofiel. Schakel RADIUS in en stel de bekabelde MAB-stroom in om service-type=Call-controle te vereisen zoals in de afbeelding wordt weergegeven. U kunt andere instellingen kopiëren van het klassieke Cisco-profiel, maar het idee is om geen 'Nas-port-type' attribuut te vereisen voor een bekabeld MAB-workflow.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is "Administration > Network Resources". The main menu includes "Network Devices", "Network Device Groups", "Network Device Profiles" (which is selected), and "External RADIUS Servers".

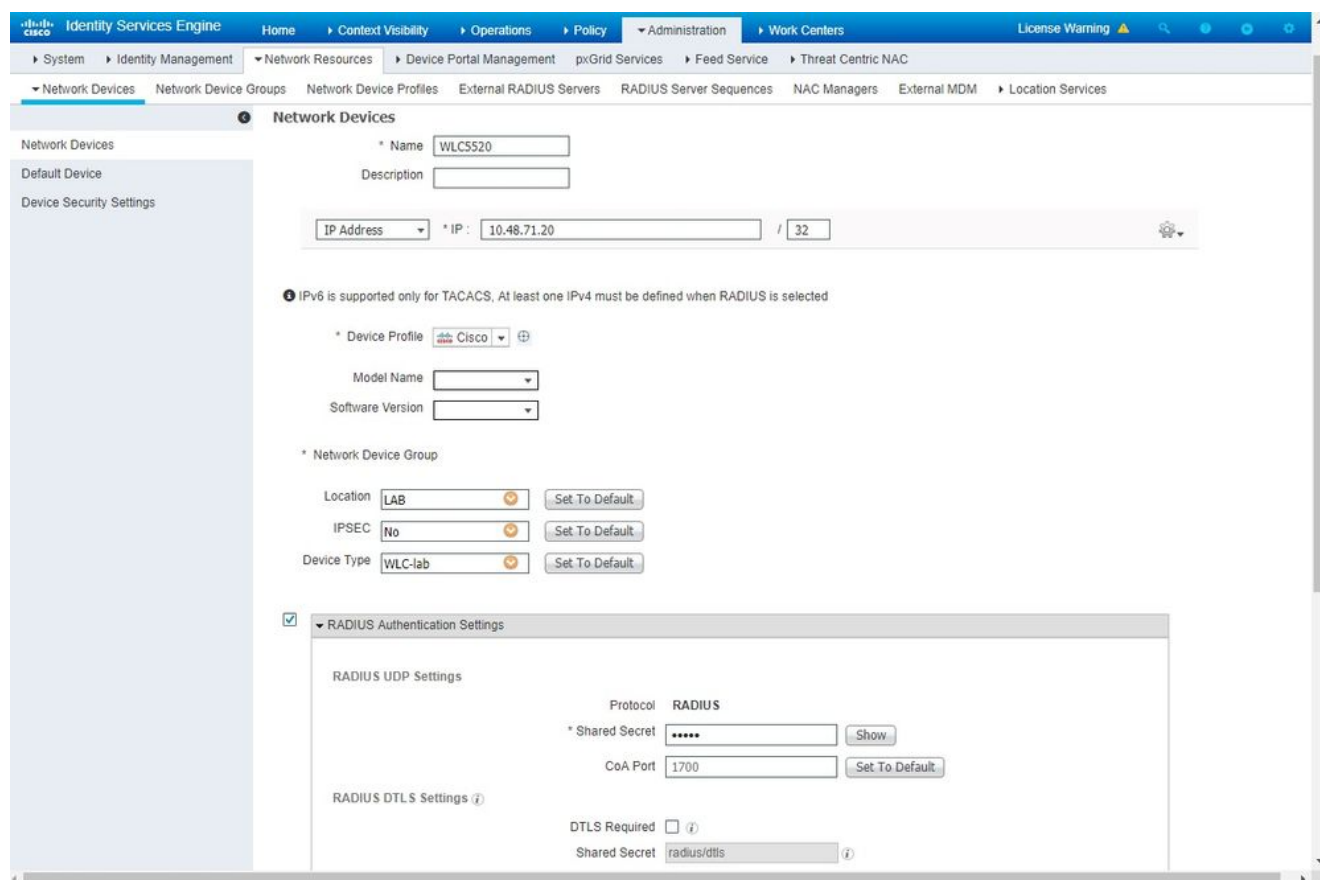
The configuration form for the "Ciscotemp" profile includes the following fields and options:

- Name:** Ciscotemp
- Description:** A large empty text area.
- Icon:** A Cisco logo icon with buttons for "Change icon..." and "Set To Default".
- Vendor:** Cisco
- Supported Protocols:**
  - RADIUS:
  - TACACS+:
  - TrustSec:
- RADIUS Dictionaries:** An empty dropdown menu.
- Templates:** A section with "Expand All / Collapse All" and a dropdown menu.
- Authentication/Authorization:** A dropdown menu.
- Flow Type Conditions:**
  - Wired MAB detected if the following condition(s) are met :
  - Condition list:
    - Radius:Service-Type = Call Check

## De WLC configureren als een AAA-client op Cisco ISE-lijnklaar

1. Ga naar veld **Administration > Network Resources > Network Devices > Add**. De pagina Nieuw netwerkapparaat verschijnt.
2. Definieer op deze pagina de WLC **Name**,

beheerinterface IP Address en Radius Authentications Settings gelijkaardig Shared Secret. Als u de MAC-adressen van het toegangspunt als eindpunten wilt invoeren, moet u ervoor zorgen dat u het aangepaste apparaatprofiel gebruikt dat eerder is geconfigureerd dan het standaard Cisco-profiel!



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The sub-menu is Network Resources > Network Devices. The page title is 'Network Devices'. The configuration form includes the following fields and options:

- Name: WLC5520
- Description: (empty)
- IP Address: 10.48.71.20 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: LAB (Set To Default)
- Location: LAB (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: WLC-lab (Set To Default)
- RADIUS Authentication Settings (checked):
  - RADIUS UDP Settings:
    - Protocol: RADIUS
    - Shared Secret: (masked) (Show)
    - CoA Port: 1700 (Set To Default)
  - RADIUS DTLS Settings (i):
    - DTLS Required:  (i)
    - Shared Secret: radius/dtls (i)

3. Klik **Submit**.

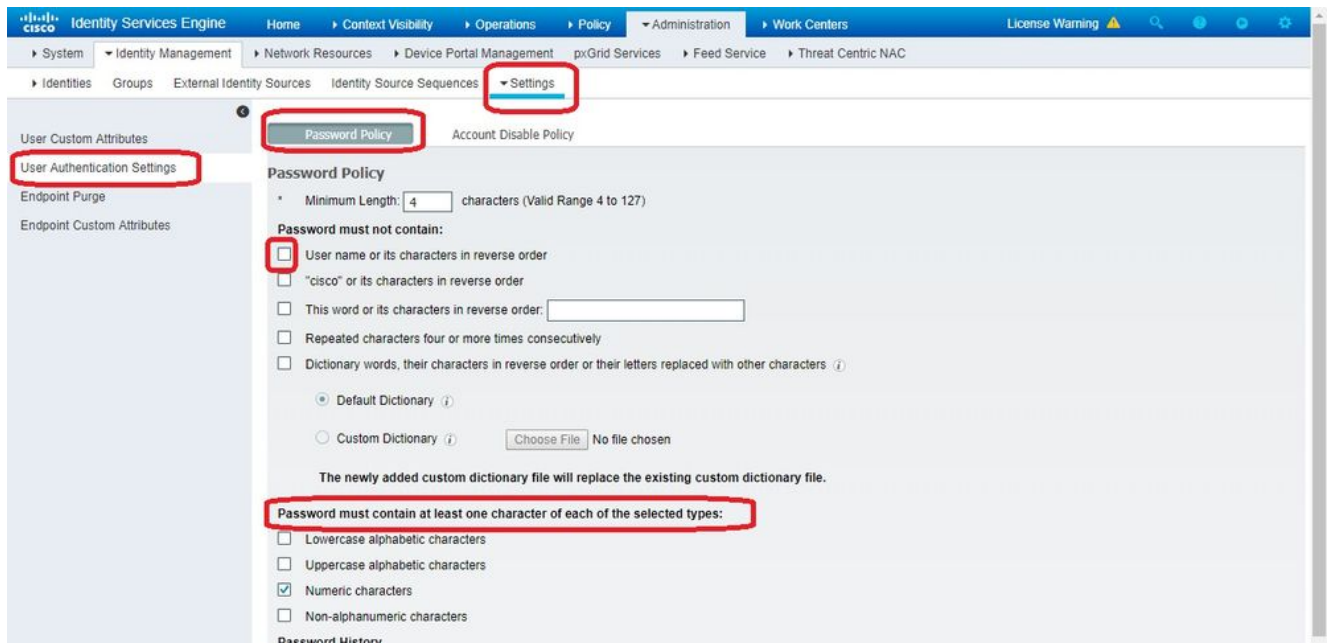
## Voeg het AP MAC-adres toe aan de Endpoint Database op Cisco ISE

Navigeer naar **Administration > Identity Management > Identities** en voeg de MAC-adressen toe aan de endpointdatabase.

## Voeg het AP MAC-adres toe aan de gebruikersdatabase op Cisco ISE (optioneel)

Als u het bekabelde MAB-profiel niet wilt wijzigen en ervoor kiest om het MAC-adres van het toegangspunt als gebruiker in te stellen, moet u de vereisten voor het wachtwoordbeleid verlagen.

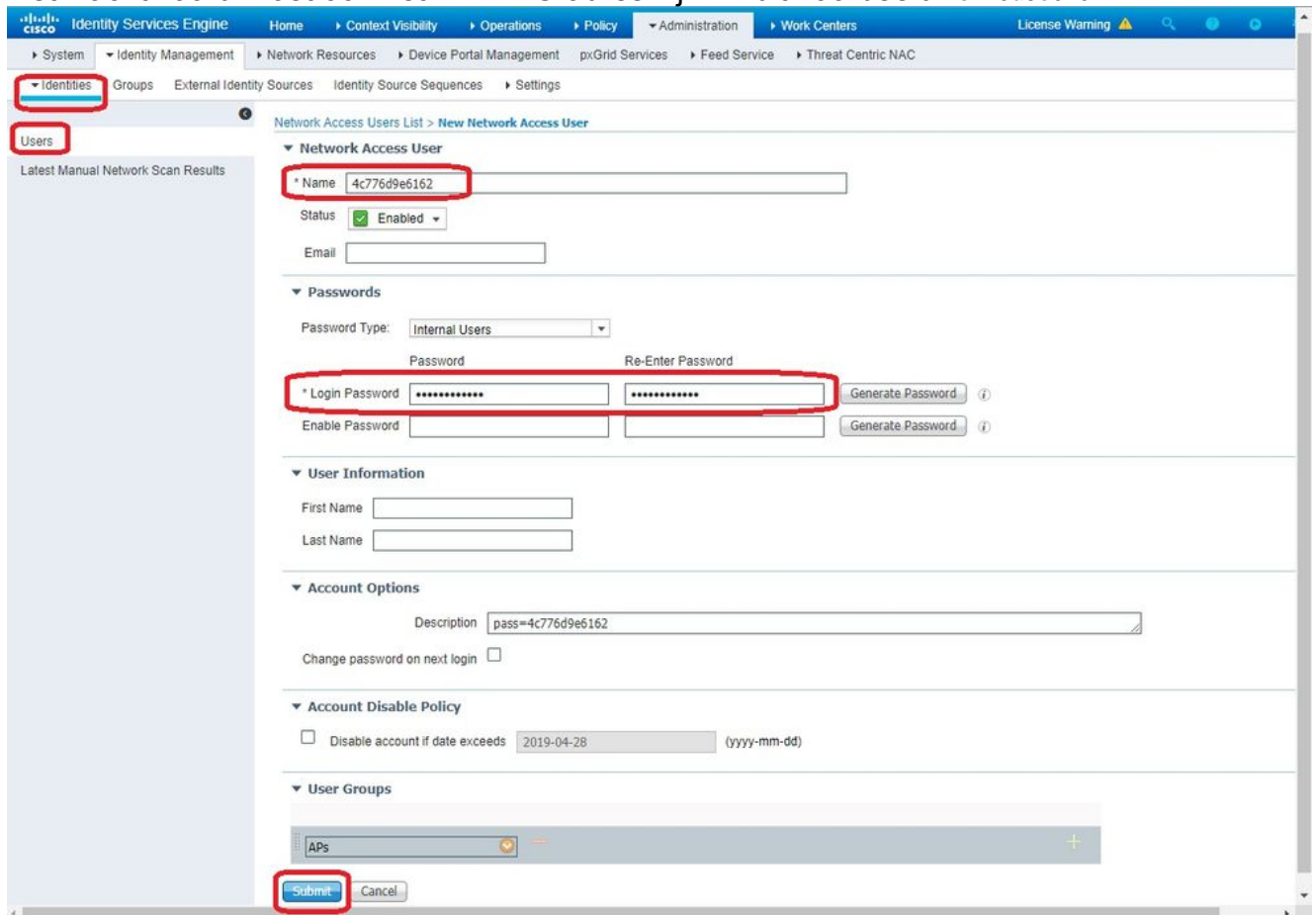
1. Navigeer naar **Administration > Identity Management**. Hier moeten we ervoor zorgen dat het wachtwoordbeleid het gebruik van de gebruikersnaam als wachtwoord toestaat en het beleid moet ook het gebruik van de mac-adrestekens toestaan zonder de noodzaak van verschillende soorten tekens. Navigeer naar **Settings > User Authentication Settings > Password Policy**:



2. Navigeer vervolgens naar **Identities > Users** en klik op **Add**. Wanneer de pagina Gebruikersinstelling verschijnt, definieert u de gebruikersnaam en het wachtwoord voor dit toegangspunt zoals aangegeven op de afbeelding.

**Tip:** Gebruik de **Description** veld om het wachtwoord in te voeren zodat u later eenvoudig kunt weten wat als wachtwoord is gedefinieerd.

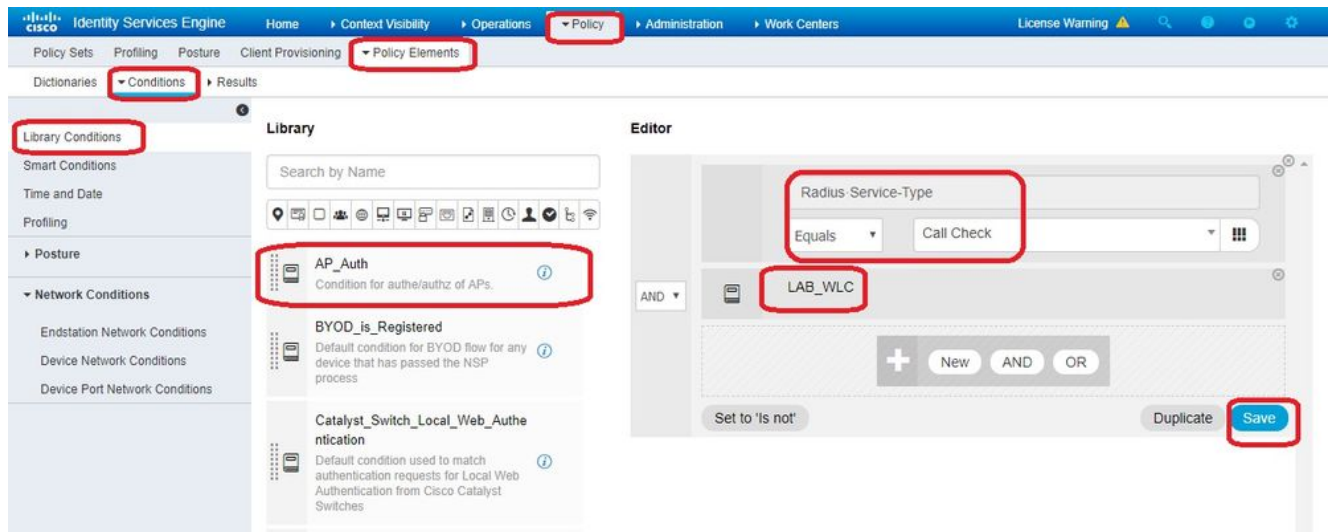
Het wachtwoord moet ook het AP MAC-adres zijn. In dit voorbeeld **4c776d9e6162**.



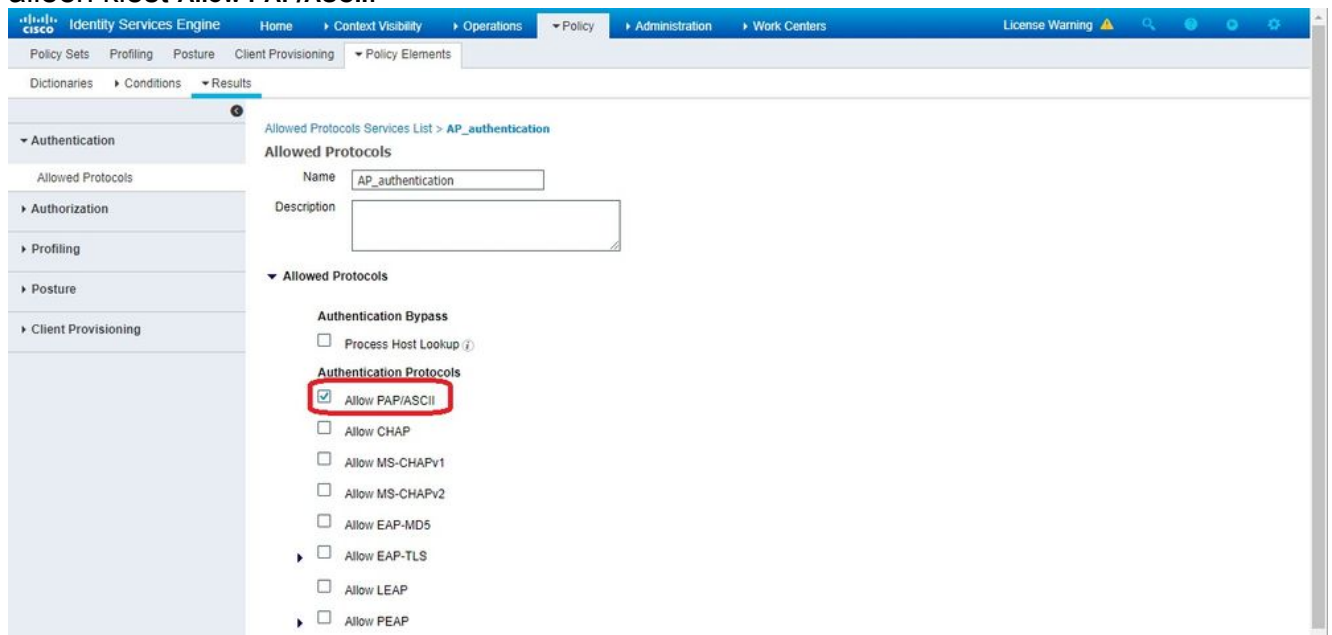
3. Klik **Submit**.

Een beleidsset definiëren

1. U moet een **Policy Set** om het authenticatieverzoek aan te passen dat uit WLC komt. Eerst bouwt u een **Conditie** door te navigeren naar **Policy > Policy Elements > Conditions**, en het creëren van een nieuwe voorwaarde om de plaats WLC aan te passen, in dit voorbeeld, "LAB\_WLC" en **Radius:Service-Type Equals Call Check** die gebruikt wordt voor Mac-authenticatie. Hier wordt de voorwaarde 'AP\_Auth' genoemd.



2. Klik **Save**.
3. Maak vervolgens een nieuwe **Allowed Protocols Service** voor de AP-verificatie. Zorg ervoor dat u **alleen** kiest **Allow PAP/ASCII**:



4. Kies de eerder gemaakte service in de **Allowed Protocols/Server Sequence**. Breid de view en onder **Authentication Policy > Use > Internal Users** zodat ISE in de interne DB zoekt naar de gebruikersnaam/het wachtwoord van het toegangspunt.

The image displays two screenshots of the Cisco Identity Services Engine (ISE) configuration interface. The top screenshot shows the 'Policy Sets' overview table. The bottom screenshot shows the detailed configuration for the 'Policy4APsAuth' policy set.

**Top Screenshot: Policy Sets Overview**

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy4APsAuth		AP_Auth	AP_authentication	19	⚙️	➔
✓	Default	Default policy set		Default Network Access	591	⚙️	➔

**Bottom Screenshot: Policy4APsAuth Configuration**

**Authentication Policy (1)**

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	19	⚙️

Buttons: **Reset** (grey), **Save** (green)

5. Klik **Save**.

## Verifiëren

Om deze configuratie te verifiëren, moet u het toegangspunt verbinden met het MAC-adres 4c:77:6d:9e:61:62 met het netwerk en de monitor. Gebruik de `debug capwap events/errors enable` en `debug aaa all enable` opdrachten om dit uit te voeren.

Zoals gezien van debugs, gaf WLC het AP adres van MAC aan de server van de RADIUS 10.48.39.128 over, en de server heeft met succes AP voor authenticatie verklaard. Het toegangspunt registreert vervolgens bij de controller.

**Opmerking:** Enkele lijnen in de output zijn verplaatst naar de tweede lijn toe te schrijven aan ruimtebeperkingen.

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248
```

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already allocated index 437
```

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request
```

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP
```

192.168.79.151:5248, already allocated index 437

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved)

\*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from temporary database.

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap\_wtp\_event\_response, state Capwap\_no\_state

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap\_wtp\_event\_response is not allowed to send in state Capwap\_no\_state for AP 192.168.79.151

\*spamApTask4: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0**

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed!

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248

\*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248

\*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9**

\*aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001

\*aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8

\*aaaQueueReader: Feb 27 14:58:07.566: Callback.....0xd6cef02166

\*aaaQueueReader: Feb 27 14:58:07.566: protocolType.....0x40000001

\*aaaQueueReader: Feb 27 14:58:07.566: proxyState.....70:69:5A:51:4E:C0-00:00

\*aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs:

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id.....70:69:5a:51:4e:c0 (17 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator.....DATA (16 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate: **RADIUS server is ready 10.48.39.128 port 1812 index 1 active 1**

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into qid:0 of server at index:1

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 **Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812** from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00

\*aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6d .....'......Zm

\*aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61

\*aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a 62..70:69:5a:51:

\*aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d:

\*aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 00 01 04 06 9e:61:62.....

\*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a\*8

\*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a ZW"[A..a.l.....

\*aaaQueueReader: Feb 27 14:58:07.566: 00000080: 15 f9 ..

\*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.**

\*radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp\_len=28, vId=9)

\*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 \*\*\* Counted VSA 150994944 AVP of length 28, code 1 atrlen 22)

\*radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp\_len=28, vId=9)

\*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22

\*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk

\*radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown

\*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes

\*radiusTransportThread: Feb 27 14:58:07.588: **70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128** (qid:0) with port:1812, pktId:185

\*radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1)

\*radiusTransportThread: Feb 27 14:58:07.588: structureSize.....432

\*radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....0x00000001

\*radiusTransportThread: Feb 27 14:58:07.588: proxyState.....70:69:5A:51:4E:C0-00:00

\*radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs:

\*radiusTransportThread: Feb 27 14:58:07.588: **AVP[01] User-Name.....4c776d9e6162** (12 bytes)

\*radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3dr cFsHuYpChs (65 bytes)

\*radiusTransportThread: Feb 27 14:58:07.588: AVP[03] Class.....DATA (83 bytes)



```
*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-
Authenticator.....DATA (16 bytes)

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join
```

## Problemen oplossen

Gebruik deze opdrachten om problemen met uw configuratie op te lossen:

- debug capwap events enable—Bevat debug van LWAPP-gebeurtenissen
- debug capwap packet enable—Bevestigt debug van LWAPP Packet trace
- debug capwap errors enable—Configureert debug van LWAP-pakketfouten
- debug aaa all enable—Hiermee wordt de debug van alle AAA-berichten geconfigureerd

In het geval dat ISE rapporten in de RADIUS live logs de gebruikersnaam 'INGELDIG' op het moment dat u APs worden geautoriseerd tegen ISE, betekent het dat de verificatie wordt geverifieerd met de endpointdatabase en u hebt niet gewijzigd het bekabelde MAB profiel zoals uitgelegd in dit document. ISE beschouwt een MAC-adresverificatie als ongeldig als het niet overeenkomt met het profiel Wired/Wireless MAB, waarvoor standaard het kenmerk NAS-poorttype vereist is dat niet door de WLC wordt verzonden.

## 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.