

# Configure Access Point Authorization in a Unified Wireless Network

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Lightweight AP Authorization](#)

### [Configure](#)

[Configuration using the Internal Authorization List on the WLC](#)

[Verify](#)

[AP Authorization Against an AAA Server](#)

[Configure the Cisco ISE to Authorize APs](#)

[Configure a New Device Profile Where MAB does not Require NAS-Port-Type Attribute](#)

[Configure the WLC as an AAA Client on the Cisco ISE](#)

[Add the AP MAC Address to the Endpoint Database on the Cisco ISE](#)

[Add the AP MAC Address to the User Database on the Cisco ISE \(Optional\)](#)

[Define a Policy Set](#)

[Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes how to configure WLC to authorize the Access Point (AP) based on the MAC address of the APs.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of how to configure a Cisco Identity Services Engine (ISE)
- Knowledge of the configuration of Cisco APs and Cisco WLCs
- Knowledge of Cisco Unified Wireless Security Solutions

### Components Used

The information in this document is based on these software and hardware versions:

- WLCs running AireOS 8.8.111.0 Software

- Wave1 APs: 1700/2700/3700 and 3500 (1600/2600/3600 are still supported but AireOS support ends on version 8.5.x)
- Wave2 APs: 1800/2800/3800/4800, 1540, and 1560
- ISE version 2.3.0.298

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Lightweight AP Authorization

During the AP registration process, the APs and WLCs mutually authenticate with the use of X.509 certificates. The X.509 certificates are burned into protected flash on both the AP and WLC at the factory by Cisco.

On the AP, factory-installed certificates are called manufacturing-installed certificates (MIC). All Cisco APs manufactured after July 18, 2005, have MICs.

In addition to this mutual authentication that occurs during the registration process, the WLCs can also restrict the APs that register with them based on the MAC address of the AP.

The lack of a strong password with the use of the AP MAC address is not an issue because the controller uses MIC to authenticate the AP before authorizing the AP through the RADIUS server. The use of MIC provides strong authentication.

AP authorization can be performed in two ways:

- Using the Internal Authorization list on the WLC
- Using the MAC address database on an AAA server

The behaviors of the APs differ based on the certificate used:

- APs with SSCs—The WLC only uses the Internal Authorization list and does not forward a request to a RADIUS server for these APs
- APs with MICs—WLC can use either the Internal Authorization list configured on the WLC or use a RADIUS server to authorize the APs

This document discusses AP authorization with the use of both the Internal Authorization list and the AAA server.

## Configure

### Configuration using the Internal Authorization List on the WLC

On the WLC, use the AP authorization list to restrict APs based on their MAC address. The AP authorization list is available under **Security > AP Policies** in the WLC GUI.


This example shows how to add the AP with MAC address 4c:77:6d:9e:61:62.

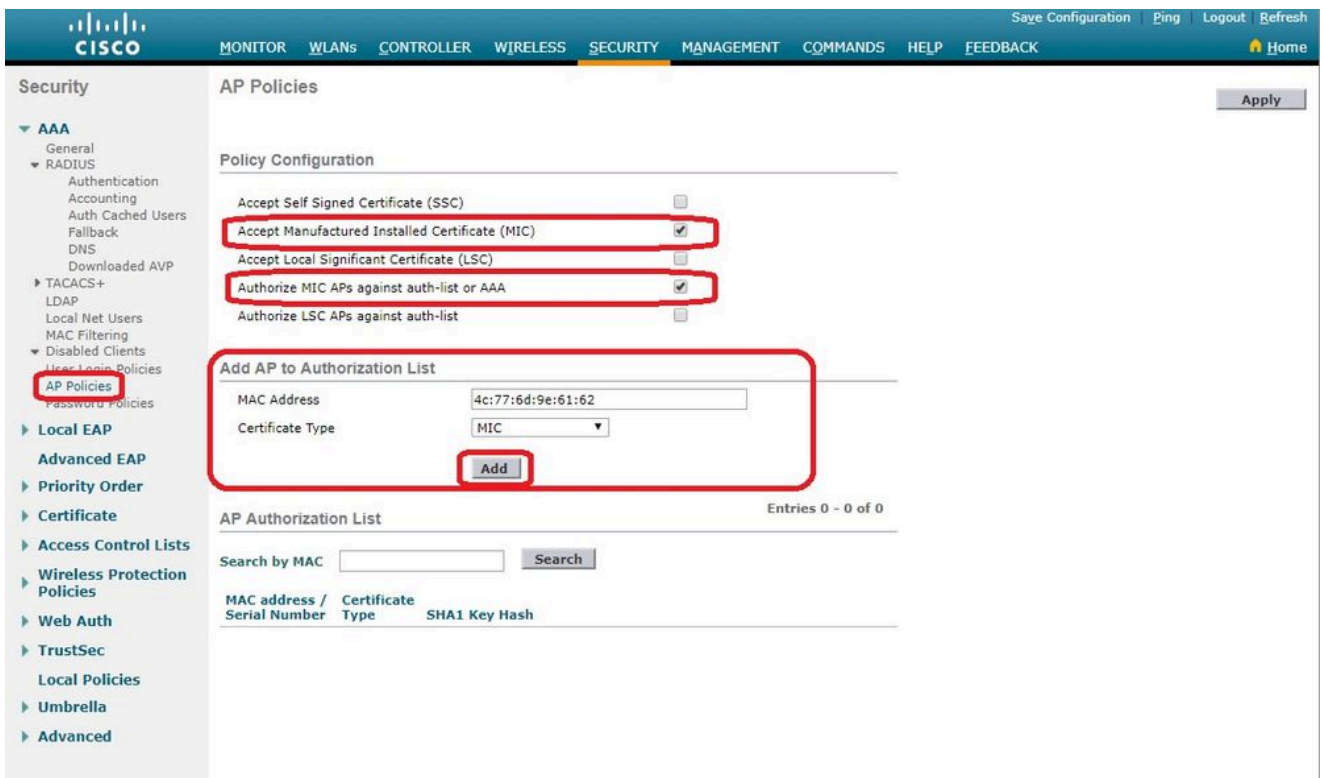
1. From the WLC controller GUI, click **Security > AP Policies** and the AP Policies page appears.
2. Click the **Add** button on the right hand side of the screen.



3. Under **Add AP to Authorization List**, enter the AP MAC address (not the AP Radio mac address). Then, choose the certificate type and click **Add**.

In this example, an AP with a MIC certificate is added.

 **Note:** For APs with SSCs, choose SSC under Certificate Type.



The AP is added to the AP authorization list and is listed under **AP Authorization List**.

4. Under Policy Configuration, check the box for **Authorize MIC APs against auth-list or AAA**.

When this parameter is selected, the WLC checks the local authorization list first. If the AP MAC is not present, it checks the RADIUS server.

The screenshot shows the Cisco WLC 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.

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	

## Verify

In order to verify this configuration, connect the AP with MAC address **4c:77:6d:9e:61:62** to the network and monitor. Use the **debug capwap events/errors enable** and **debug aaa all enable** commands to perform this.

This output shows the debugs when the AP MAC address is not present in the AP authorization list:

**Note:** Some of the lines in the output have been moved to the second line due to space constraints.

```
<#root>
```

```
(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
```

```
*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 te
```

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

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :19

\*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

\*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

\*aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 4000000

\*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:

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

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

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[02] Called-Station-Id.....70-69-5a-51

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

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-IP-Address.....0x0a304714

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier.....0x6e6f (282)

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

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

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

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

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

\*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:

\*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: 0x36 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 = 7

\*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 Co

\*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session 0xd6f0

\*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: trad:192.168.79.

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

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver (

\*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

This output show the debugs when the LAP MAC address is added to the AP authorization list:

---

 **Note:** Some of the lines in the output have been moved to the second line due to space constraints.

---

<#root>

(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

```

*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 tempora
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in ap gro

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allo

*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
*aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs:
*aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-Type.....0x00000065 (101)
*aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-Identifer.....0x00000000 (0) (
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB on WLAN
*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 ==>
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from capwap_ac_pla

*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP 70:69:5a:51:4e:c0 s

```

## AP Authorization Against an AAA Server

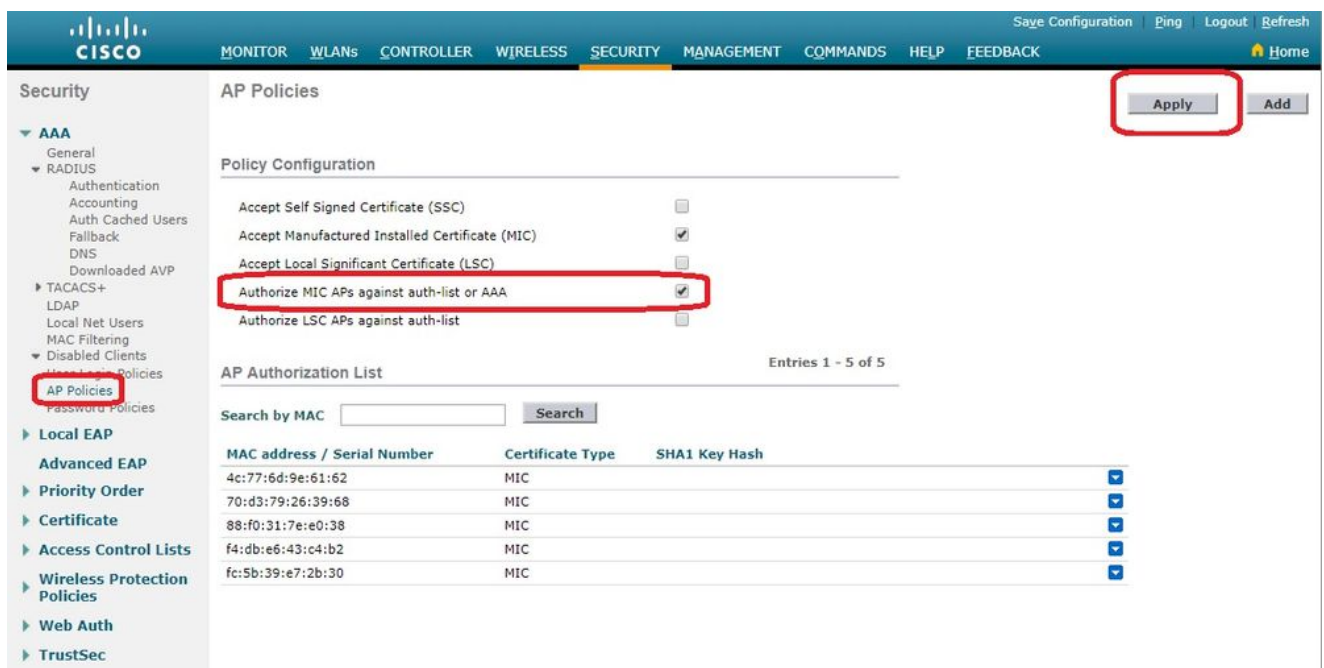
You can also configure WLCs to use RADIUS servers to authorize APs using MICs. The WLC uses a AP MAC address as both the username and password when sending the information to a RADIUS server.

For example, if the MAC address of the AP is **4c:77:6d:9e:61:62**, both the username and password used by the controller to authorize the AP are that mac address using the defined delimiter.

This example shows how to configure the WLCs to authorize APs using the Cisco ISE.

1. From the WLC controller GUI, click **Security > AP Policies**. The AP Policies page appears.
2. Under Policy Configuration, check the box for **Authorize MIC APs against auth-list or AAA**.

When you choose this parameter, the WLC checks the local authorization list first. If the AP MAC is not present, it checks the RADIUS server.



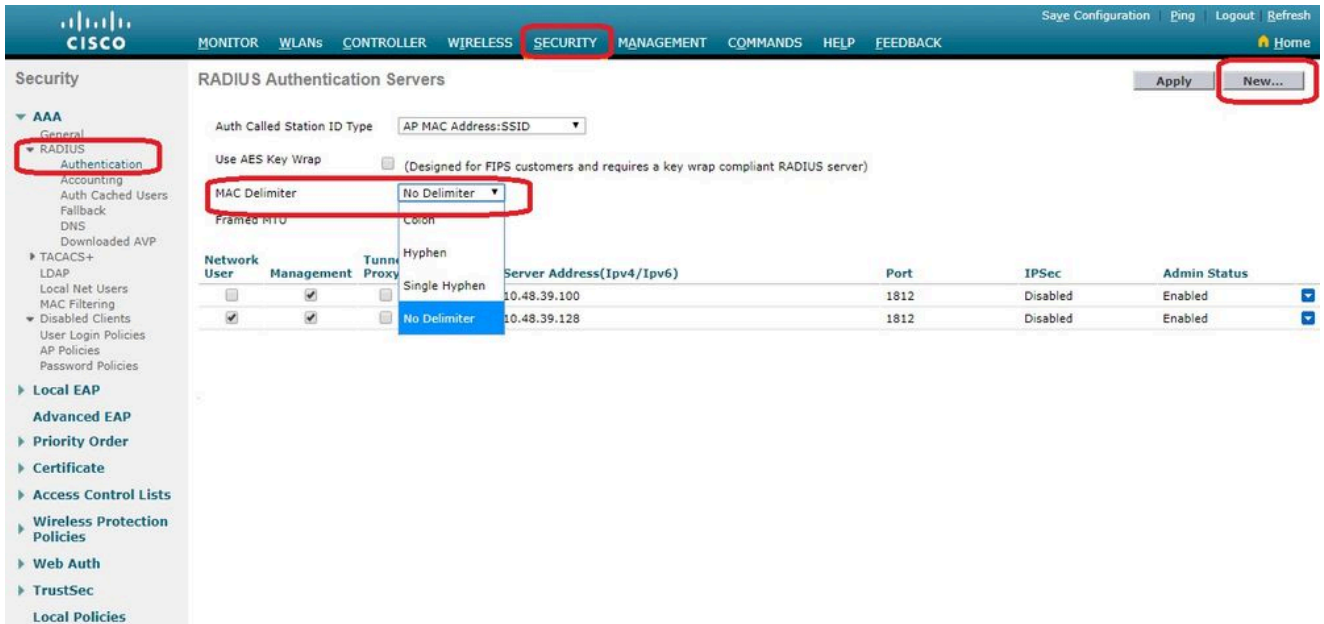
The screenshot shows the Cisco WLC GUI with the following details:

- Navigation: **Security > AP Policies**
- Policy Configuration:
  - Accept Self Signed Certificate (SSC):
  - Accept Manufactured Installed Certificate (MIC):
  - Accept Local Significant Certificate (LSC):
  - Authorize MIC APs against auth-list or AAA:**
  - Authorize LSC APs against auth-list:
- AP Authorization List (Entries 1 - 5 of 5):

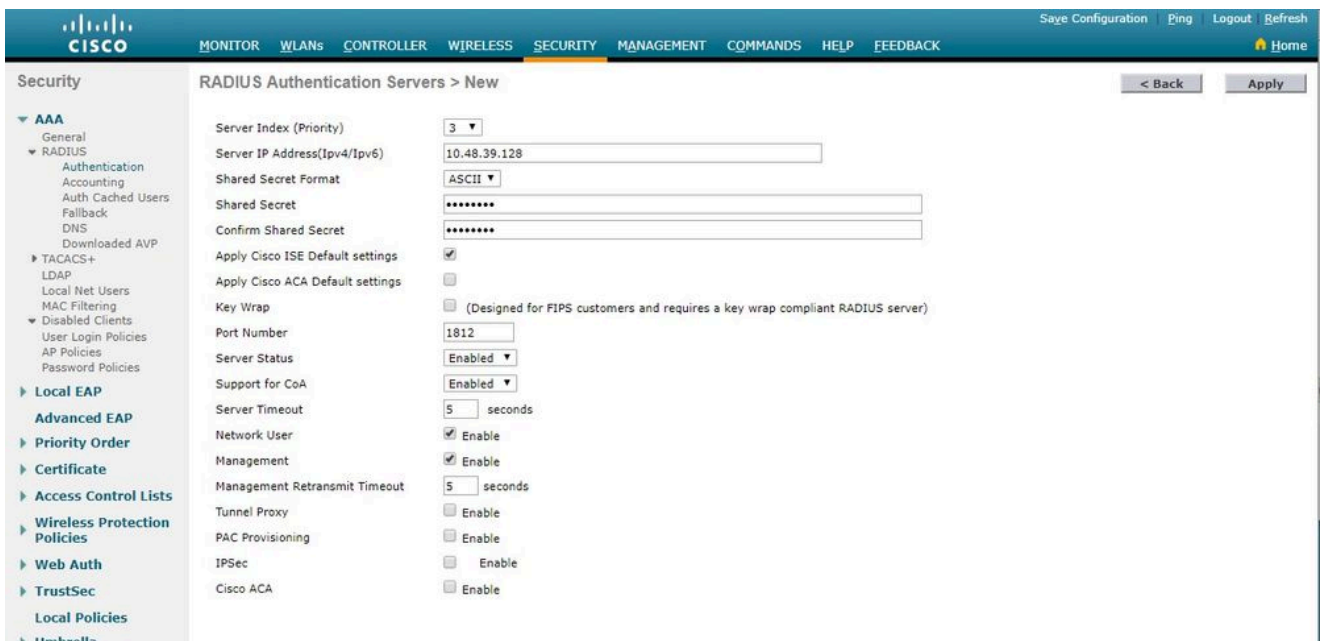
MAC address / Serial Number	Certificate Type	SHA1 Key Hash
4c:77:6d:9e:61:62	MIC	[Dropdown]
70:d3:79:26:39:68	MIC	[Dropdown]
88:f0:31:7e:e0:38	MIC	[Dropdown]
f4:db:e6:43:c4:b2	MIC	[Dropdown]
fc:5b:39:e7:2b:30	MIC	[Dropdown]

3. Navigate to **Security > RADIUS Authentication** from the controller GUI to display the **RADIUS Authentication Servers** page. In this page you can define the **MAC Delimiter**. The WLC gets the AP Mac address and sends it to the Radius Server using the delimiter defined here. It is important that the username matches what is configured in the Radius server. In this example the **No Delimiter** is used so that the username is **4c776d9e6162**.





4. Then, click **New** in order to define a RADIUS server.



5. Define the RADIUS server parameters on the **RADIUS Authentication Servers > New** page. These parameters include the RADIUS **Server IP Address**, **Shared Secret**, **Port Number**, and **Server Status**. When done, click **Apply**. This example uses the Cisco ISE as the RADIUS server with IP address 10.48.39.128.

## Configure the Cisco ISE to Authorize APs

In order to enable the Cisco ISE to authorize APs, you need to complete these steps:

1. Configure the WLC as an AAA Client on the Cisco ISE.
2. Add the AP MAC Addresses to the Database on the Cisco ISE.

However, you could be adding the AP MAC address as endpoints (the best way) or as users (whose

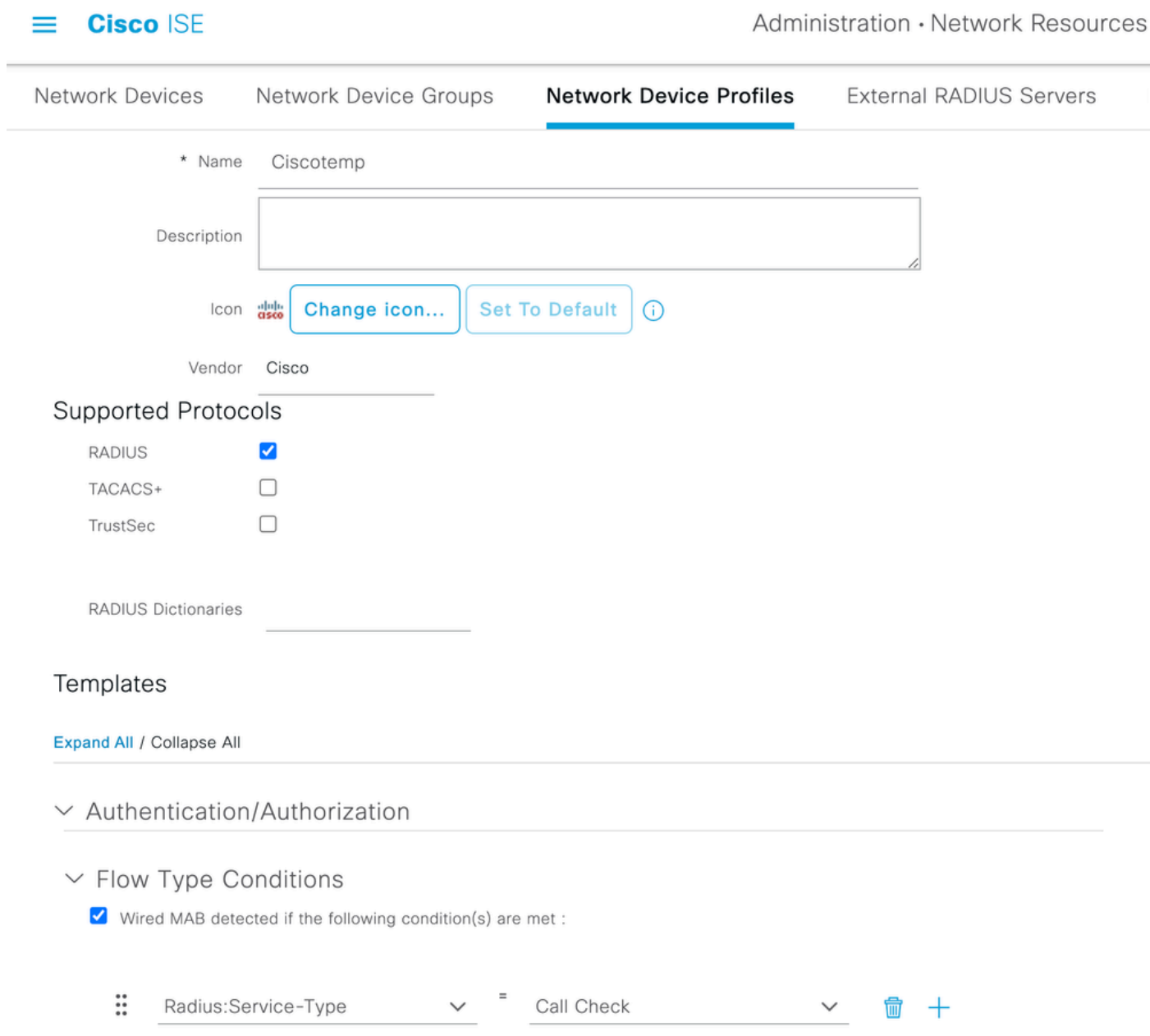
passwords are the MAC address as well) but this requires you to lower the password security policies requirements.

Due to the WLC not sending the NAS-Port-Type attribute which is a requirement on ISE to match the Mac address authentication (MAB) workflow, you must adjust this.

### Configure a New Device Profile Where MAB does not Require NAS-Port-Type Attribute

Navigate to **Administration > Network device profile** and create a new device profile. Enable RADIUS and set the Wired MAB flow to require service-type=Call-check as illustrated in the image.

You can copy other settings from the classic Cisco profile but the idea is to not require 'Nas-port-type' attribute for a Wired MAB workflow.

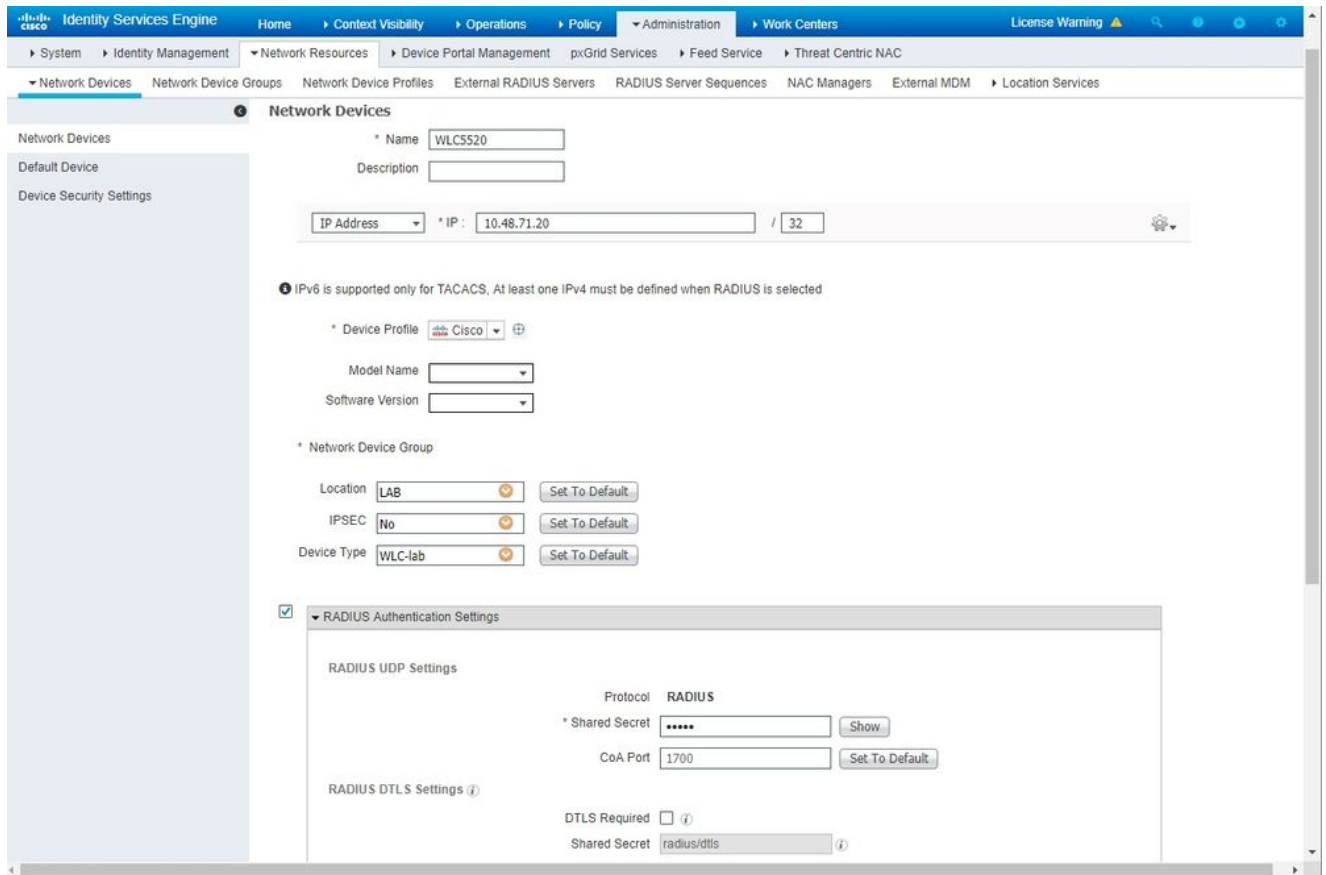


### Configure the WLC as an AAA Client on the Cisco ISE

1. Go to **Administration > Network Resources > Network Devices > Add**. The New Network Device page appears.

## 2. On this page, define the WLC Name, Management

Interface IP Address and Radius Authentications Settings like Shared Secret. If you plan to enter the AP MAC addresses as endpoints, verify that you use the custom device profile configured earlier rather than the default Cisco profile.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows Network Resources, Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The main content area is titled "Network Devices" and contains the following configuration fields:

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

## 3. Click Submit.

### Add the AP MAC Address to the Endpoint Database on the Cisco ISE

Navigate to **Administration > Identity Management > Identities** and add the MAC addresses to the endpoint database.

### Add the AP MAC Address to the User Database on the Cisco ISE (Optional)

If you do not want to modify the wired MAB profile and chose to put the AP MAC address as a user, lower the password policy requirements.

1. Navigate to **Administration > Identity Management**. Verify the password policy allows the usage of the username as password and the policy allows the usage of the mac address characters whitout the need for different types of characters. Navigate to **Settings > User Authentication Settings > Password Policy**:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

User Custom Attributes Password Policy Account Disable Policy

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Password Policy

Minimum Length: 4 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 with other characters [?](#)

Default Dictionary [?](#)

Custom Dictionary [?](#)  No file chosen

The newly added custom dictionary file will replace the existing custom dictionary file.

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

Lowercase alphabetic characters

Uppercase alphabetic characters

Numeric characters

Non-alphanumeric characters

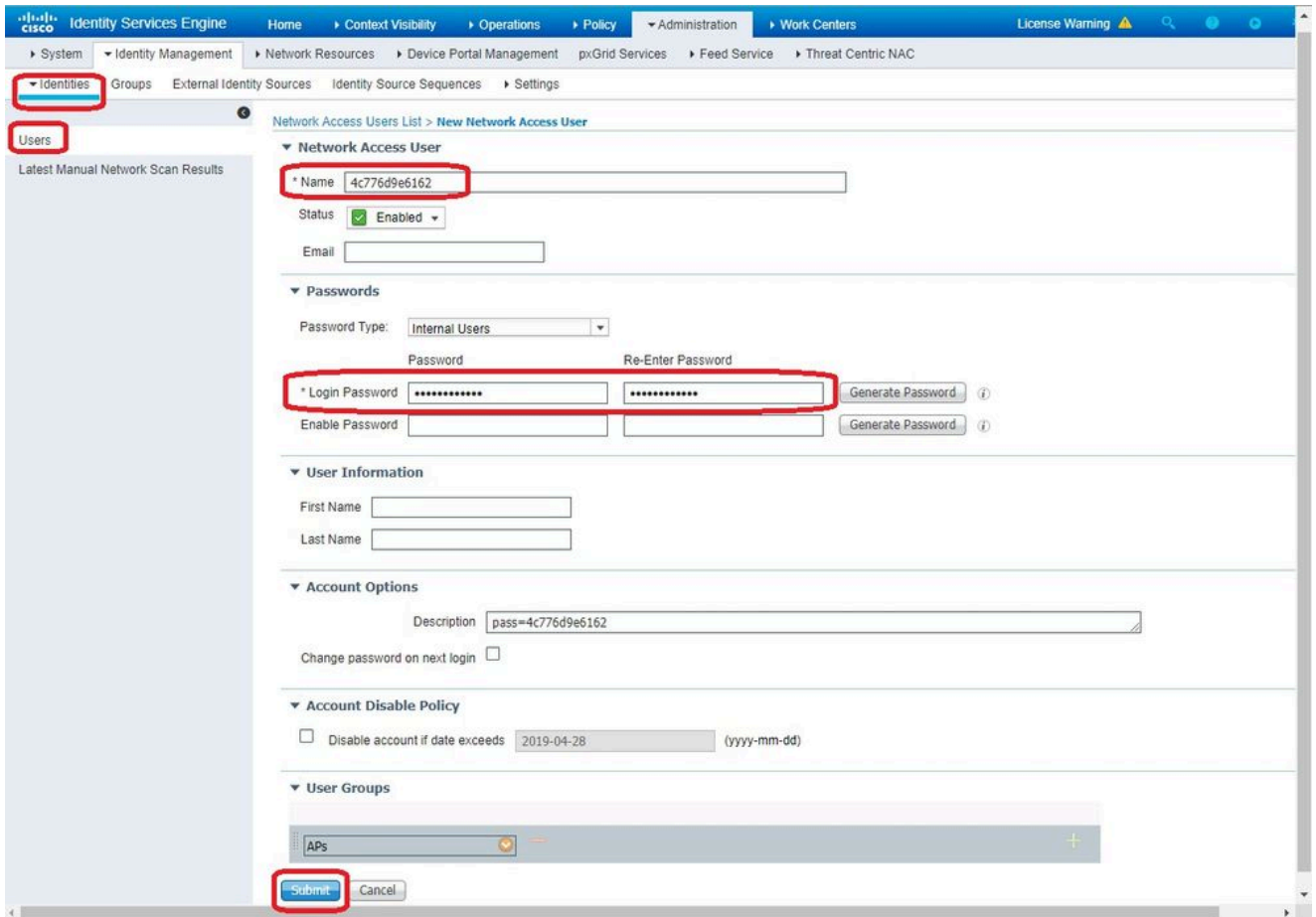
Password History

2. Navigate to **Identities > Users** and click **Add**. When the User Setup page appears, define the username and password for this AP as shown.



**Tip:** Use the **Description** field to enter the password to later be easy to know what was defined as password.

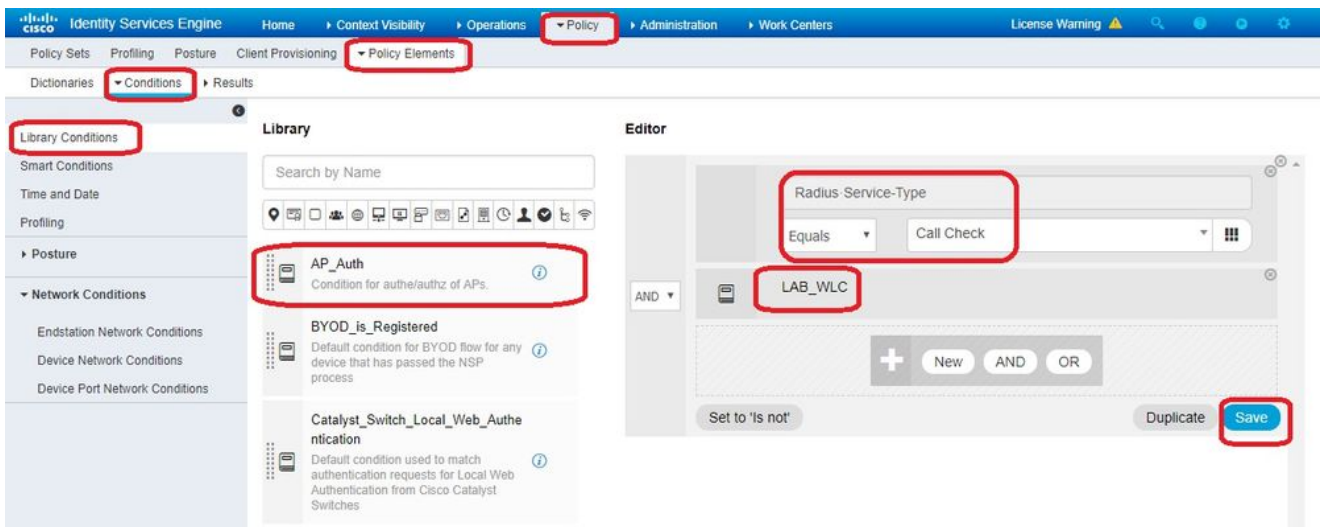
The password must also be the AP MAC address. In this example, it is **4c776d9e6162**.



3. Click **Submit**.

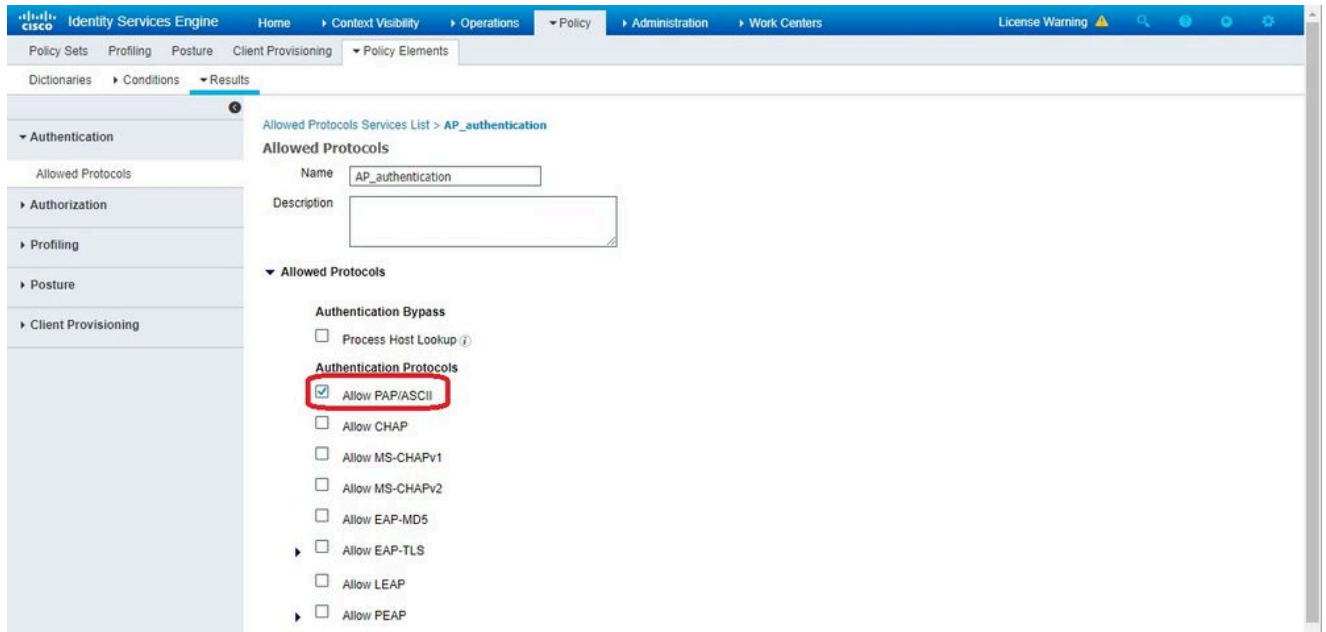
## Define a Policy Set

1. Define a **Policy Set** to match the authentication request coming from the WLC. First, build a **Condition** by navigating to **Policy > Policy Elements > Conditions**, and create a new condition to match the WLC location, in this example, 'LAB\_WLC' and **Radius:Service-Type Equals Call Check** which is used for Mac authentication. Here the condition is named 'AP\_Auth'.

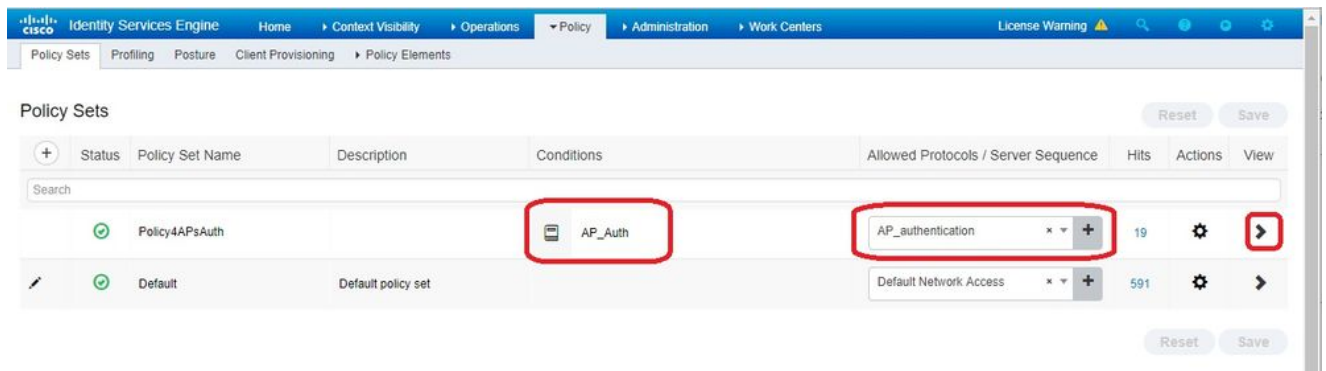


2. Click **Save**.

3. Then create a new **Allowed Protocols Service** for the AP authentication. Make sure you choose only **Allow PAP/ASCII**:



4. Choose the previously created Service in the **Allowed Protocols/Server Sequence**. Expand the **View** under **Authentication Policy > Use > Internal Users** so that ISE searches the internal DB for the username/password of the AP.



5. Click **Save**.

## Verify

In order to verify this configuration, connect the AP with MAC address 4c:77:6d:9e:61:62 to the network and monitor. Use the `debug capwap events/errors enable` and `debug aaa all enable` commands in order to perform this.

As seen from the debugs, the WLC passed on the AP MAC address to the RADIUS server 10.48.39.128, and the server has successfully authenticated the AP. The AP then registers with the controller.

**Note:** Some of the lines in the output have been moved to the second line due to space constraints.

```
<#root>
```

```
*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 alloced 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  
  
\*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 tempora  
\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap gro  
  
\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168  
  
\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap\_wtp\_event\_response is not allo  
  
\*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 :  
\*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:  
  
\*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  
\*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  
\*aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:6  
\*aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (C  
\*aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (1709  
\*aaaQueueReader: Feb 27 14:58:07.566: AVP[06] NAS-Identifier.....0x6e6f (28271) (C  
\*aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10)  
\*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 w  
\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the  
\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into qi  
\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812



\*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 .....
\*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....4
\*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:
\*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..
\*aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 01 04 06 9e:61:6
\*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .OG...n
\*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 0a ZW"[A..
\*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
\*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, vendorL
\*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b
\*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, c
\*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:51:4
\*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.....ReauthSes
\*radiusTransportThread: Feb 27 14:58:07.588: AVP[03] Class.....DATA (83
\*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-Authenticator.....DATA (16

\*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: 0x36 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



# Troubleshoot

Use these commands to troubleshoot your configuration:

- `debug capwap events enable`—Configures debug of LWAPP events
- `debug capwap packet enable`—Configures debug of LWAPP Packet trace
- `debug capwap errors enable`—Configures debug of LWAPP Packet errors
- `debug aaa all enable`—Configures debug of all AAA messages

If ISE reports in the RADIUS live logs the username 'INVALID' when APs being authorized against ISE, it means that authentication is being verified against the endpoint database and you have not modified the wired MAB profile as explained in this document.

ISE considers a MAC address authentication invalid if it does not match the Wired/Wireless MAB profile, which by default require the NAS-port-type attribute which is not sent by the WLC.