

# Configure Catalyst 9800 Wireless Controller AP Authorization List

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Network Diagram](#)

[Configurations](#)

[MAC AP authorization List - Local](#)

[MAC AP Authorization List - External RADIUS Server](#)

[9800 WLC Config](#)

[ISE Config](#)

[Configure ISE to Authenticate MAC Address as Endpoints](#)

[Configure ISE to Authenticate MAC Address as Username/Password](#)

[Authorization Policy to Authenticate APs](#)

### [Verify](#)

### [Troubleshoot](#)

### [References](#)

---

## Introduction

This document describes how to configure Catalyst 9800 Wireless LAN Controller Access Point (AP) authentication policy.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC
- Command line Interface (CLI) access to the wireless controllers

### Components Used

Cisco recommends these hardware and software versions:

- 9800 WLC v17.3
- AP 1810W
- AP 1700
- Identity Service Engine (ISE) v2.2

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.

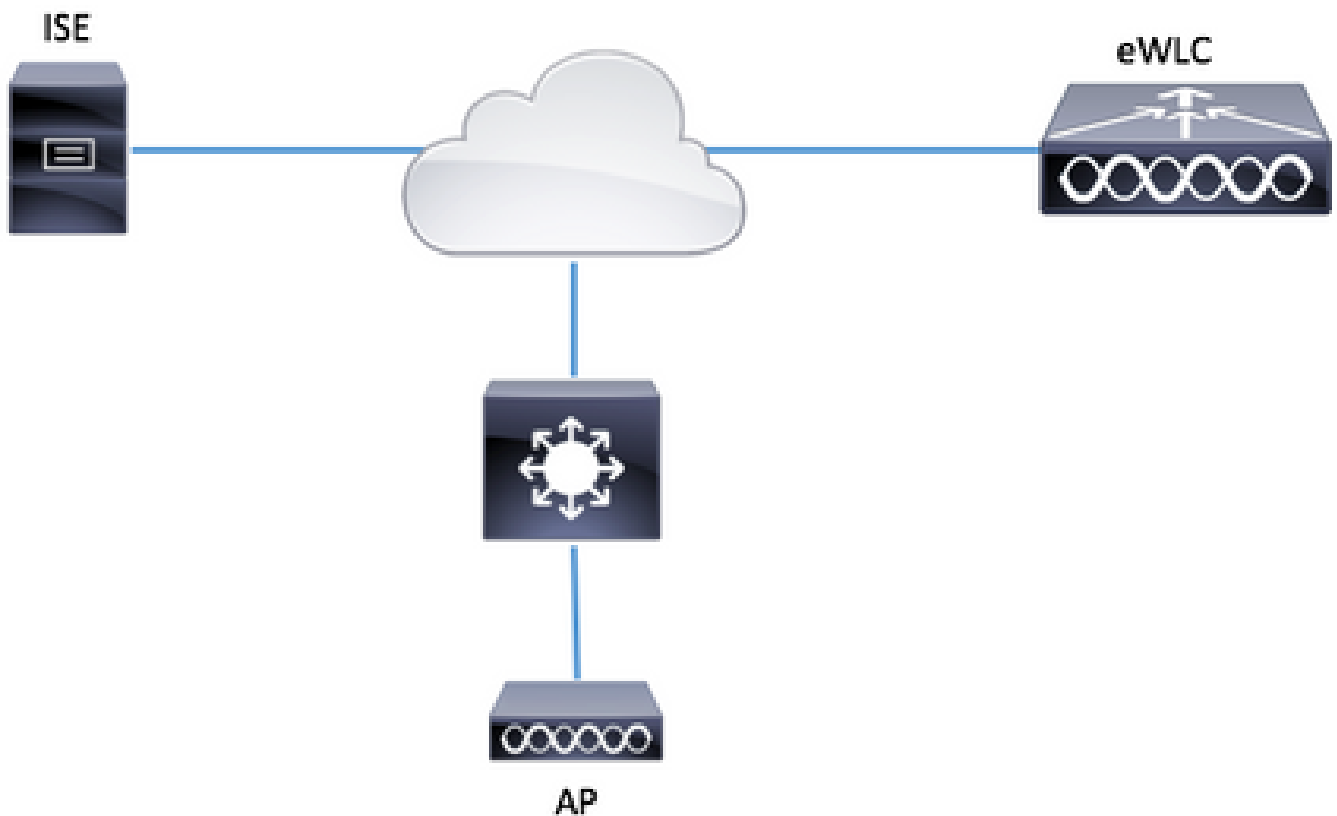
## Background Information

To authorize an Access Point (AP), Ethernet MAC address of the AP needs to be authorized against local database with 9800 Wireless LAN Controller or against an external Remote Authentication Dial-In User Service (RADIUS) server.

This feature ensures that only authorized Access Points (APs) are able to join a Catalyst 9800 Wireless LAN Controller. This document does not cover the case of mesh (1500 series) APs which require a MAC filter entry to join the controller but do not trace the typical AP authorization flow (see references).

## Configure

### Network Diagram



### Configurations

#### MAC AP authorization List - Local

The MAC address of the authorized APs are stored locally in the 9800 WLC.

Step 1. Create a local authorization credential-download method list.

Navigate to **Configuration > Security > AAA > AAA Method List > Authorization > + Add.**

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List   Servers / Groups   AAA Advanced

General

Authentication

Authorization

Accounting

+ Add   x Delete

	Name	Type
<input type="checkbox"/>	default	network
<input type="checkbox"/>	AuthZ-Netw-ISE	network

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 Device

Step 2. Enable AP MAC authorization.

Navigate to **Configuration > Security > AAA > AAA Advanced > AP Policy**. Enable **Authorize APs against MAC** and select the **Authorization Method List** created in Step 1.

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   AP-auth

Apply to Device

Step 3. Add the AP ethernet MAC Address.

Navigate to **Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add**.

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    x Delete

MAC Address

0    10 items per page

Quick Setup: MAC Filtering

MAC Address\*    00:B0:E1:8C:49:E8

Attribute List Name    None

Cancel    Save & Apply to Device

**Note:** AP ethernet MAC address must be in one of these formats when entered in the web UI (xx:xx:xx:xx:xx:xx (or) xxxx.xxxx.xxxx (or) xx-xx-xx-xx-xx-xx) in version 16.12. In version 17.3, they have to be in format xxxxxxxxxxxx without any separator. The CLI format is always xxxxxxxxxxxx in any version (in 16.12, the web UI removes the separators in the config). Cisco bug ID [CSCvv43870](#) allows the use of any format in CLI or web UI in later releases.

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 Authorization List - External RADIUS Server

### 9800 WLC Config

The MAC address of the authorized APs are stored on an external RADIUS server, in this example ISE.

On ISE, you can register the MAC address of the APs either as usernames/password or as Endpoints. Along the steps you are instructed how to select to use one way or the other.

GUI:

Step 1. Declare RADIUS server.

Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** and enter the RADIUS server information.

The screenshot shows the ISE GUI navigation path: **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add**. The 'Servers / Groups' tab is selected, and the 'RADIUS' sub-tab is active. The '+ Add' button is highlighted with a red box. Below the navigation, there are tabs for 'Servers' and 'Server Groups', with 'Servers' selected. A table with columns 'Name' and 'Address' is visible at the bottom.

Ensure **Support for CoA** is enabled if you plan to use Central Web Authentication (or any kind of security that requires CoA) in the future.

The screenshot shows the 'Create AAA Radius Server' form with the following fields and values:

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"/>		

At the bottom, there are two buttons: 'Cancel' and 'Save & Apply to Device' (highlighted with a red box).

Step 2. Add the RADIUS server to a RADIUS group.

Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.**

To have ISE authenticate the AP MAC address as usernames, leave MAC-Filtering as none.

The screenshot shows the 'Create AAA Radius Server Group' configuration window. The 'Name' field is highlighted with a red box and contains the text 'ISE-grp-name'. The 'Group Type' is set to 'RADIUS'. The 'MAC-Delimiter' is set to 'none'. The 'MAC-Filtering' is set to 'none'. The 'Dead-Time (mins)' is set to '1-1440'. The 'Assigned Servers' list is highlighted with a red box and contains the text 'ISE-ikcg'. The 'Save & Apply to Device' button is highlighted with a red box.

To have ISE authenticate the AP MAC address as Endpoints, change MAC-Filtering to MAC.

### Create AAA Radius Server Group

Name\*

Group Type

MAC-Delimiter

**MAC-Filtering**

Dead-Time (mins)

Available Servers Assigned Servers

ISE-KCG

Step 3. Create an authorization credential-download method list.

Navigate to **Configuration > Security > AAA > AAA Method List > Authorization > + Add.**

Search Menu Items

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

### Authentication Authorization and Accounting

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

General

Authentication

**Authorization**

Accounting

	Name		Type
<input type="checkbox"/>	default		network
<input type="checkbox"/>	AuthZ-Netw-ISE		network

**Quick Setup: AAA Authorization** ✕

Method List Name\*

Type\*

Group Type

Fallback to local

Available Server Groups

radius  
 ldap  
 tacacs+  
 ISE-KCG-grp

Assigned Server Groups

ISE-grp-name

Step 4. Enable AP MAC authorization.

Navigate to **Configuration > Security > AAA > AAA Advanced > AP Policy**. Enable **Authorize APs against MAC** and select the **Authorization Method List** created in Step 3.

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

Apply to Device

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 Config**

Step 1. To add 9800 WLC to ISE:

### [Declare 9800 WLC on ISE](#)

Choose to configure the AP's MAC address based on authentication with the required steps:

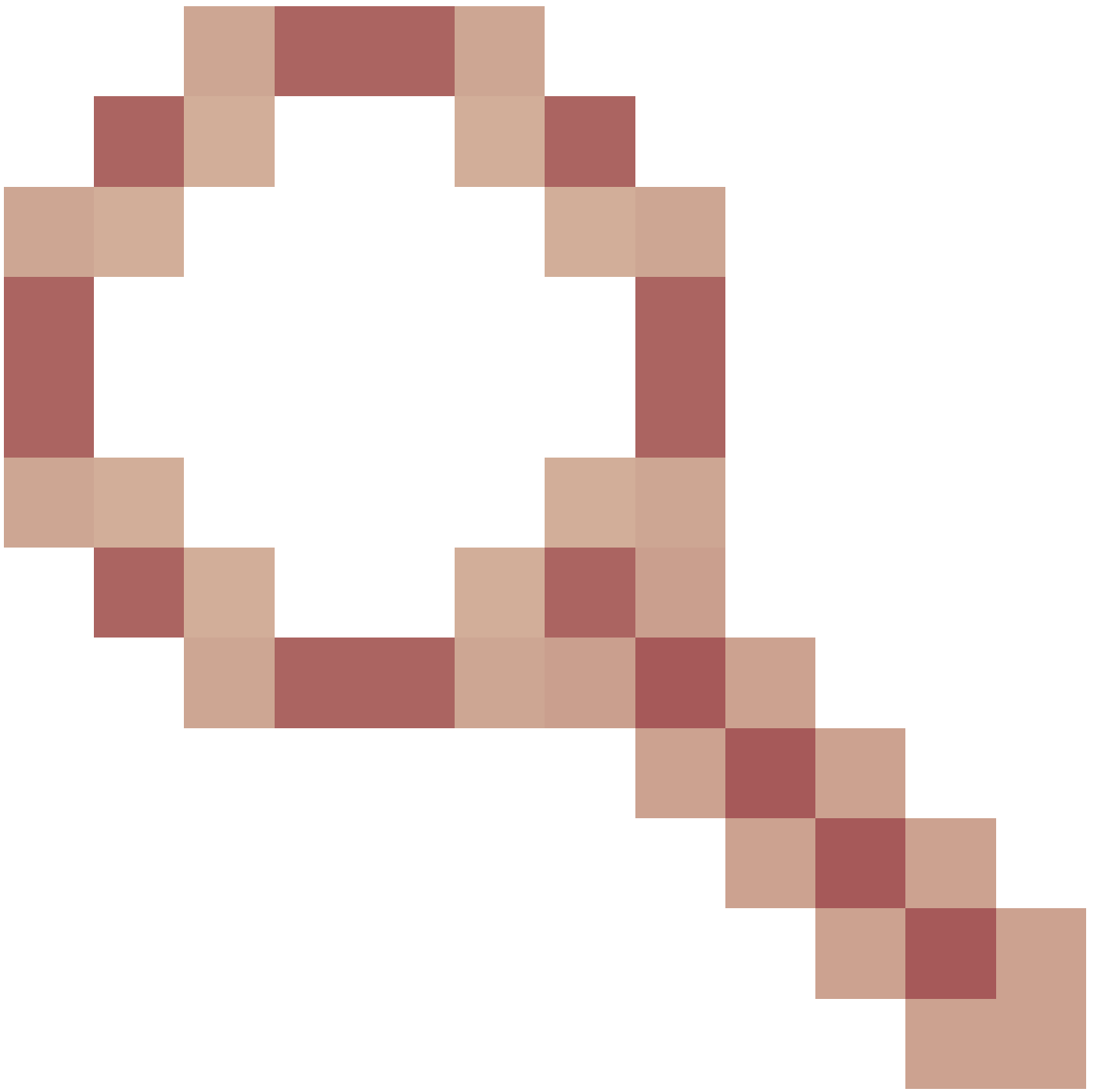
### [Configure USE to authenticate MAC address as endpoints](#)

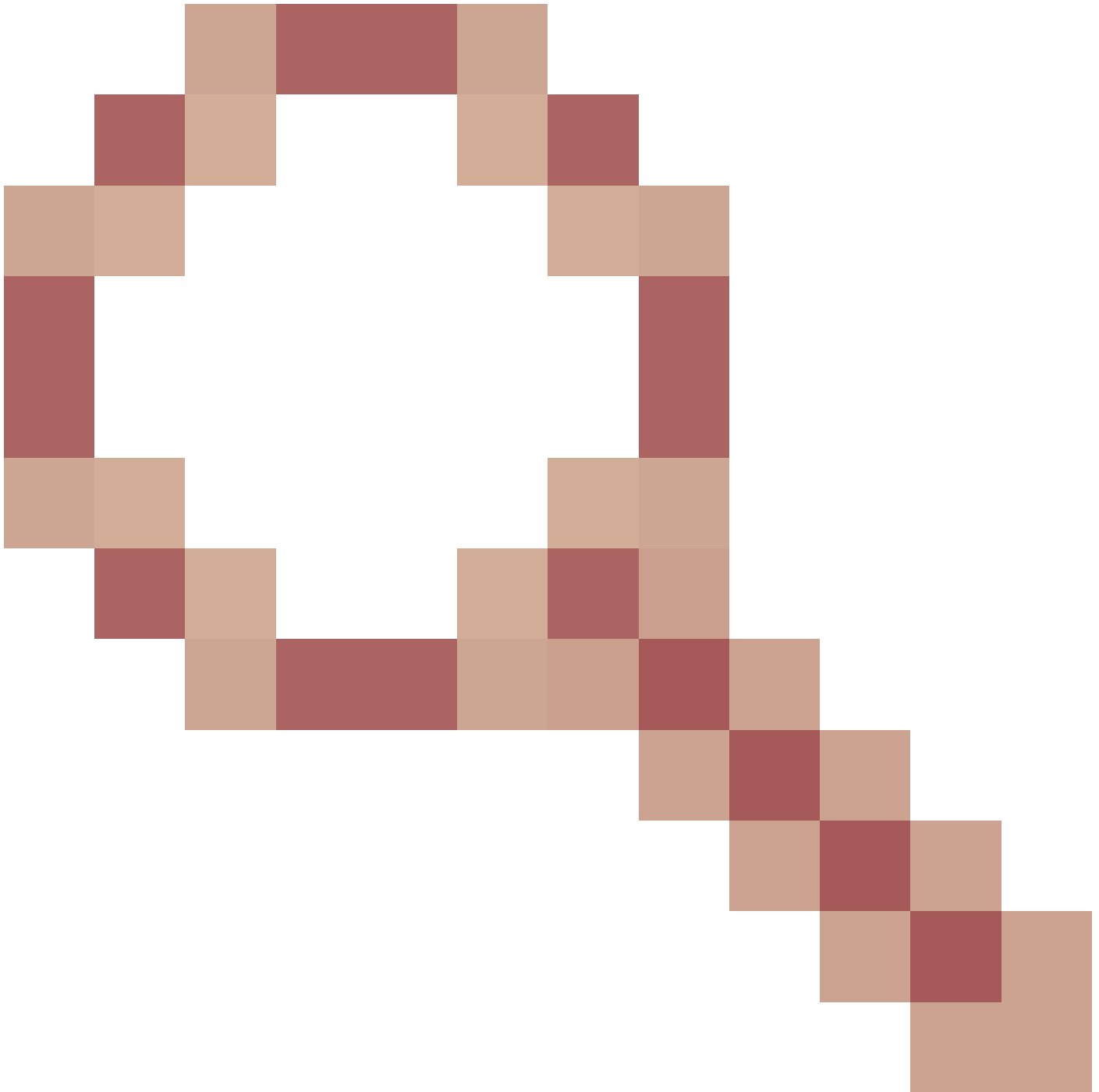
### [Configure ISE to authenticate MAC address as username/password](#)

## **Configure ISE to Authenticate MAC Address as Endpoints**

Step 2. (Optional) Create an identity group for Access Points.

Because the 9800 does not send the NAS-port-Type attribute with AP authorization (Cisco bug [ID CSCvy74904](#)).





ISE does not recognize an AP authorization as a MAB workflow. Therefore, it is not possible to authenticate an AP if the MAC address of the AP is placed in the endpoint list unless you modify the MAB workflows to not require the NAS-PORT-type attribute on ISE.

Navigate to **Administrator > Network device profile** and create a new device profile. Enable **RADIUS**, and add service-type=call-check for Wired MAB. You can copy the rest from the Cisco original profile. The idea is to have no nas-port-type condition for the Wired MAB.

\* Name  

Description

Icon



[Change icon...](#)

[Set To Default](#)



Vendor  

### Supported Protocols

- RADIUS
- TACACS+
- TrustSec

RADIUS Dictionaries

### Templates

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

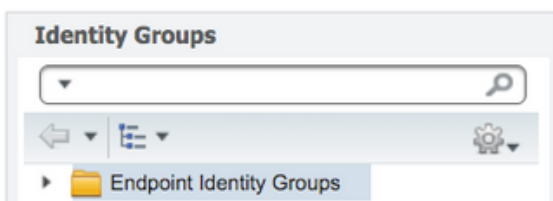
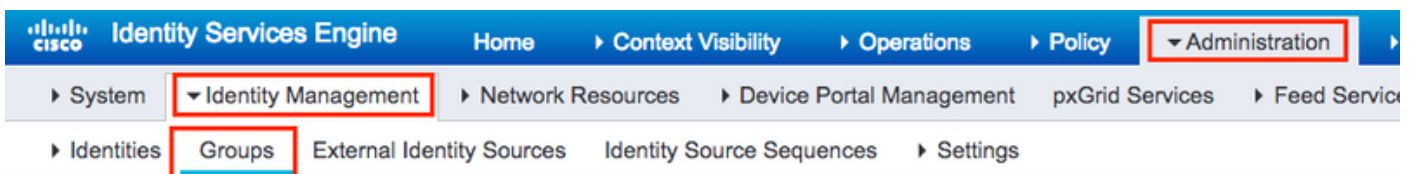
#### Authentication/Authorization

#### Flow Type Conditions

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

Go back to your network device entry for the 9800 and set its profile to the newly created device profile.

Navigate to **Administration > Identity Management > Groups > Endpoint Identity Groups > + Add**.



### Endpoint Identity Groups

Edit   **Add**   Delete

Name	Description
------	-------------

Choose a name and click **Submit**.

## Endpoint Identity Group List > New Endpoint Group

### Endpoint Identity Group

\* Name

AccessPoints

Description

Parent Group

Submit

Cancel

Step 3. Add the AP ethernet MAC address to its endpoint identity group.

Navigate to **Work Centers > Network Access > Identities > Endpoints > +**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Identities > Endpoints. The 'Endpoints' section is active, showing a bar chart titled 'INACTIVE ENDPOINTS' with 3 bars and a date of 8/27. The chart shows 1 active endpoint and 0 inactive endpoints. The 'AUTHENTICATED' section is partially visible on the right. The 'disconnected: [1009]' status is shown. The '0 Selected' status is shown at the bottom. The table below the chart has columns for MAC Address, Status, IPv4 Address, and Username. The '+' icon in the table header is highlighted with a red box.

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

Enter the needed information.

## Add Endpoint



### General Attributes

Mac Address \*

Description

Static Assignment

Policy Assignment

Static Group Assignment

Identity Group Assignment

Step 4. Verify the identity store used on your default authentication rule that contains the internal endpoints.

A. Navigate to **Policy > Authentication** and take note of the Identity store.

**Authentication Policy**

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity store used for authentication. 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 : All_User_ID_Stores

B. Navigate to **Administration > 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	Identity
<input type="checkbox"/>	All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preload
<input type="checkbox"/>	Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Request APIs	Internal
<input type="checkbox"/>	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal
<input type="checkbox"/>	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal
<input type="checkbox"/>	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal

C. Ensure Internal Endpoints belong to it. Otherwise, add them.

## 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		Selected
<input type="text" value="Internal Endpoints"/>	<input type="button" value="&gt;"/>	<input type="text" value="Internal Users"/>
	<input type="button" value="&lt;"/>	<input type="text" value="All_AD_Join_Points"/>
	<input type="button" value="&gt;&gt;"/>	<input type="text" value="Guest Users"/>
	<input type="button" value="&lt;&lt;"/>	

Navigation buttons on the right: ↑, ↓, ↕

### ▼ 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

## Configure ISE to Authenticate MAC Address as Username/Password

This method is not advised as it requires lower password policies to allow the same password as the username.

It can, however, be a workaround in case you cannot modify your Network device profile.

Step 2. (Optional) Create an identity group for Access Points.

Navigate to **Administration > Identity Management > Groups > User Identity Groups > + Add.**



The screenshot shows two panels. The left panel, titled "Identity Groups", has a search bar and a list of folders: "Endpoint Identity Groups" and "User Identity Groups" (which is highlighted with a red box). The right panel, titled "User Identity Groups", has a toolbar with "Edit", "Add" (highlighted with a red box), "Delete", "Import", and "Export" buttons. Below the toolbar is a table with columns "Name" and "Description". The table contains one entry: "ALL\_ACCOUNTS (default)" with a checkbox and the description "Default ALL\_".

Choose a name and click **Submit**.

## User Identity Groups > New User Identity Group

### Identity Group

\* Name

Description

Step 3. Verify that your current password policy allows you to add a MAC address as username and password.

Navigate to **Administration > Identity Management > Settings > User Authentication Settings > Password Policy** and ensure that at least these options are disabled:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

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

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Account Disable Policy

### 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**

- \* Password must be different from the previous 3 versions (Valid Range 1 to 10)
- Password change delta 3 characters (Valid Range 3 to 10)
- \* Cannot reuse password within 15 days (Valid Range 0 to 365)

**Password Lifetime**

Users can be required to periodically change password

- Disable user account after 60 days if password was not changed (valid range 1 to 3650)
- Display reminder 30 days prior to password expiration (valid range 1 to 3650)
- Lock/Suspend Account with Incorrect Login Attempts

- \* # 3 (Valid Range 3 to 20)
- Suspend account for 15 minutes (Valid Range 15 to 1440)  Disable account

 **Note:** You can also want to disable the option **Disable user account after XX days if password was not changed**. As this is a MAC address, the password never changes.

Step 4. Add the AP ethernet MAC address.

Navigate to **Administration > Identity Management > Identities > Users > + Add**.

**CISCO Identity Services Engine** Home > Context Visibility > Operations > Policy > Administration

> System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Services

> Identities Groups External Identity Sources Identity Source Sequences > Settings

Users

Latest Manual Network Scan Results

**Network Access Users**

Edit + Add Change Status Import Export Delete

Status	Name	Description	First N
--------	------	-------------	---------

Enter the needed information.

▼ **Network Access User**

\* Name

Status  Enabled ▼

Email

▼ **Passwords**

Password Type:

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ

▼ **User Information**

First Name

Last Name

▼ **Account Options**

Description


Change password on next login

▼ **Account Disable Policy**

Disable account if date exceeds  (yyyy-mm-dd)

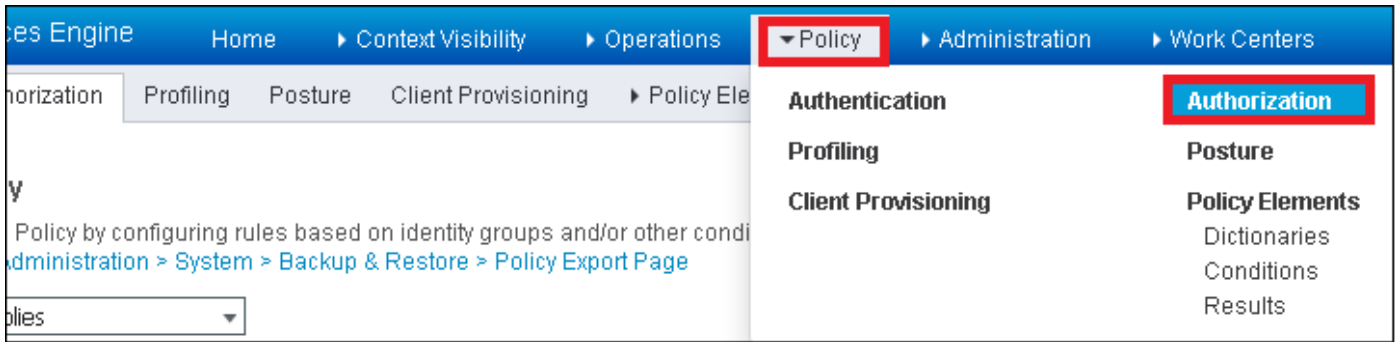
▼ **User Groups**

- +

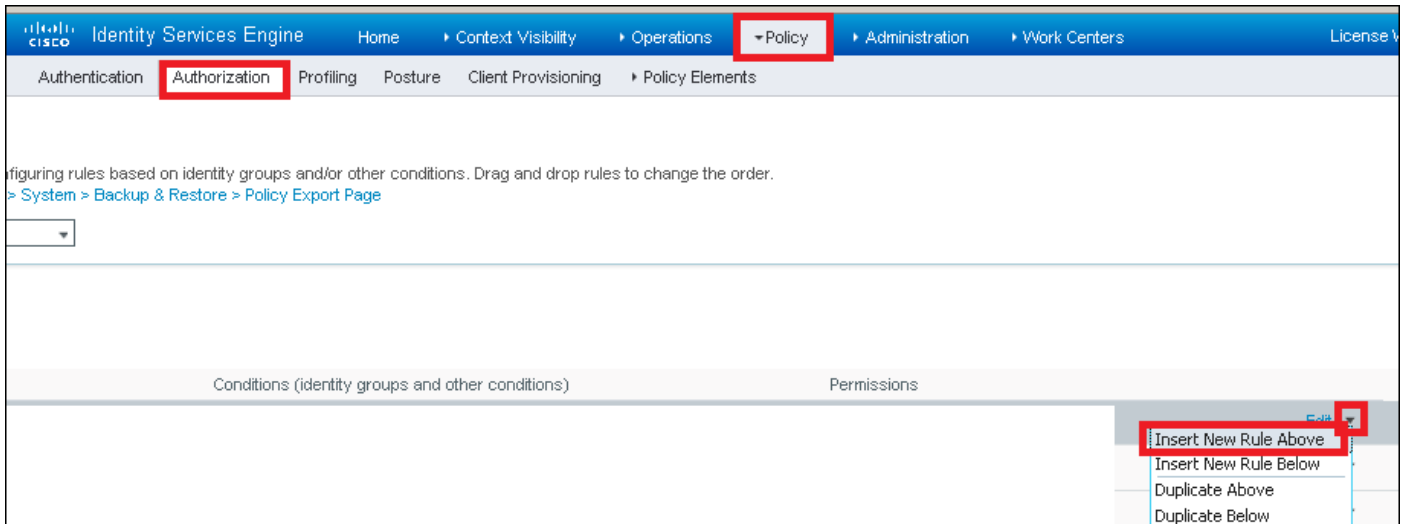
 **Note:** Name and Login Password fields must be the ethernet MAC address of the AP, all lower case and no separators.

**Authorization Policy to Authenticate APs**

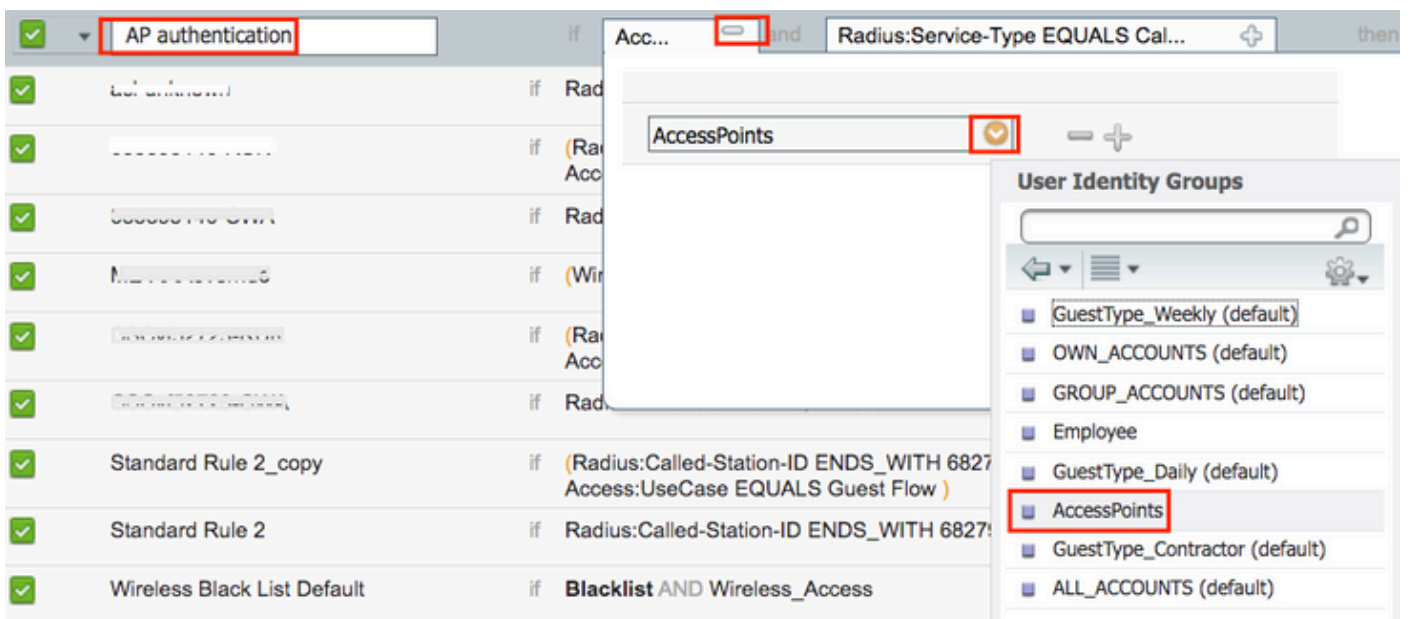
Navigate to **Policy > Authorization** as shown in the image.



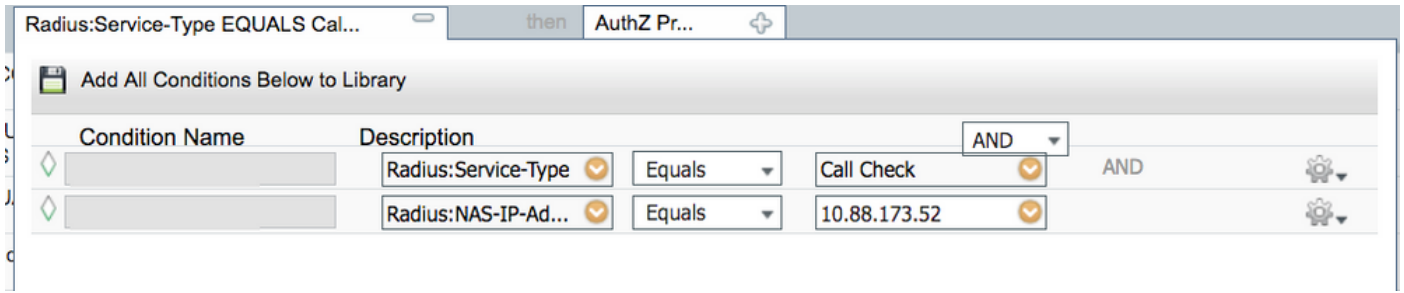
Insert a new rule as shown in the image.



First, select a name for the rule and the Identity group where the Access Point is stored (AccessPoints). Select **User Identity Groups** if you decided to authenticate the MAC address as username password or **Endpoint Identity Groups** if you choose to authenticate the AP MAC address as endpoints.



After that, select other conditions that cause the authorization process to fall under this rule. In this example, the authorization process hits this rule if it uses service-type Call Check and the authentication request comes from the IP address 10.88.173.52.



Finally, select the Authorization profile that is assigned to the clients that hit that rule, click **Done** and **save** it as shown in the image.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	AP authentication	if <b>AccessPoints</b> AND (Radius:Service-Type EQUALS Call Check AND Radius:NAS-IP-Address EQUALS 10.88.173.52)	then PermitAccess

**Note:** APs that already joined in the controller do not lose their association. If, however, after authorization list is enabled, they lose communication with the controller and attempt to rejoin, they go through the authentication process. If their MAC addresses are not listed locally or in the RADIUS server, they are not be able to rejoin the controller.

## Verify

Verify if 9800 WLC has enabled the AP authentication list.

```
<#root>
```

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

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

Verify radius configuration:

```
<#root>
```

```
#
```

```
show run aaa
```

## Troubleshoot

WLC 9800 provides ALWAYS-ON trace capabilities. This ensures all AP join-related errors, warning and notice level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

---

 **Note:** Volume of logs generated vary retroactively from a few hours to several days.

---

To view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC through these steps. (Ensure that you log the session to a text file).

Step 1. Check the controller current time so you can track the logs in the time back to when the issue happened.

```
# show clock
```

Step 2. Collect syslogs from the controller buffer or the external syslog as dictated by the system configuration. This provides a quick view into the system health and errors, if any.

```
# show logging
```

Step 3. Verify if any debug conditions are enabled.

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


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

```
IOSXE Packet Trace Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                                     Port
-----|-----
```

---

 **Note:** If you see any condition listed, it means the traces are logged up to debug level for all the processes that encounter the enabled conditions (MAC address, IP address etc). This would increase the volume of logs. Therefore, it is recommended to clear all conditions when not actively debugging.

---

Step 4. Assume the tested MAC address was not listed as a condition. in Step 3, collect the always-on notice level traces for the specific radio MAC address.

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

You can either display the content in the session or you can copy the file to an external 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>
```

## Conditional Debugging and Radio Active Tracing

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture the Radio Active (RA) trace, which provides debug level traces for all processes that interact with the specified condition (client mac address in this case).

Step 5. Ensure there are no debug conditions enabled.


```
# clear platform condition all
```

Step 6. Enable the debug condition for the wireless client MAC address that you want to monitor.

This command starts to monitor the provided MAC address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2085978494 seconds.

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

---

 **Note:** In order to monitor more than one client at a time, run debug wireless MAC <aaaa.bbbb.cccc> command per MAC address.

---

 **Note:** You do not see the output of the client activity in the terminal session, as everything is buffered internally to be viewed later.

---

Step 7. Reproduce the issue or behavior that you want to monitor.

Step 8. Stop the debugs if the issue is reproduced before the default or configured monitor time is up.

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

Once the monitor time has elapsed or the debug wireless has been stopped, the 9800 WLC generates a local file with the name:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```



Step 9. Collect the file of the MAC address activity. You can either copy the ra trace .log to an external server or display the output directly on the screen.

Check the name of the RA traces file:

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

Copy the file to an external server:

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

Display the content:

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

Step 10. If the root cause is still not obvious, collect the internal logs which are a more verbose view of debug level logs. You do not need to debug the client again as you only take a further detailed look at debug logs that have been already collected and internally stored.

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



**Note:** This command output returns traces for all logging levels for all processes and is quite voluminous. Please engage Cisco TAC to help parse through these traces.

---

You can either copy the ra-internal-FILENAME.txt to an external server or display the output directly on the screen.

Copy the file to an external server:

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


Display the content:

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

Step 11. Remove the debug conditions:

```
# clear platform condition all
```

---

 **Note:** Ensure that you always remove the debug conditions after a troubleshooting session.

---

## References

[Join mesh APs to 9800 WLC](#)