

Configuración de la autorización del punto de acceso en una red inalámbrica unificada

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Autorización de punto de acceso ligero](#)

[Configurar](#)

[Configuración mediante la lista de autorización interna en el WLC](#)

[Verificación](#)

[Autorización de AP contra un Servidor AAA](#)

[Configuración de Cisco ISE para autorizar puntos de acceso](#)

[Configure un nuevo perfil de dispositivo donde MAB no requiera el atributo NAS-Port-Type](#)

[Configure el WLC como un cliente AAA en Cisco ISE](#)

[Agregue la dirección MAC del punto de acceso a la base de datos de terminales en Cisco ISE](#)

[Agregar la dirección MAC del punto de acceso a la base de datos de usuarios en Cisco ISE \(opcional\)](#)

[Definir un conjunto de políticas](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar el WLC para autorizar el punto de acceso (AP) basado en la dirección MAC de los AP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos sobre cómo configurar Cisco Identity Services Engine (ISE)
- Conocimiento de la configuración de Cisco AP y Cisco WLC
- Conocimiento de las soluciones Cisco Unified Wireless Security

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLCs que ejecutan AireOS 8.8.111.0 SoftwareAP Wave1: 1700/2700/3700 y 3500 (1600/2600/3600 siguen siendo compatibles, pero la compatibilidad con AireOS finaliza en la versión 8.5.x)AP Wave2: 1800/2800/3800/4800, 1540 y 1560 versión de ISE 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Autorización de punto de acceso ligero

Durante el proceso de registro de AP, los AP y WLC se autentican mutuamente con el uso de certificados X.509. Cisco graba los certificados X.509 en el flash protegido en el AP y el WLC en la fábrica.

En el AP, los certificados instalados de fábrica se llaman certificados instalados de fabricación (MIC). Todos los AP de Cisco fabricados después del 18 de julio de 2005, tienen MIC.

Además de esta autenticación mutua que ocurre durante el proceso de registro, los WLC también pueden restringir los AP que se registran con ellos basándose en la dirección MAC del AP.

La falta de una contraseña segura con el uso de la dirección MAC del AP no es un problema porque el controlador utiliza MIC para autenticar el AP antes de autorizar el AP a través del servidor RADIUS. El uso de MIC proporciona una autenticación sólida.

La autorización de AP se puede realizar de dos maneras:

- Uso de la lista de autorización interna en el WLC
- Uso de la base de datos de direcciones MAC en un servidor AAA

Los comportamientos de los AP difieren según el certificado utilizado:

- AP con SSC: el WLC utiliza solamente la lista de autorización interna y no reenvía una solicitud a un servidor RADIUS para estos AP
- AP con MIC—WLC puede utilizar la lista de autorización interna configurada en el WLC o utilizar un servidor RADIUS para autorizar los AP

Este documento describe la autorización de AP con el uso de la lista de autorización interna y el servidor AAA.

Configurar

Configuración mediante la lista de autorización interna en el WLC

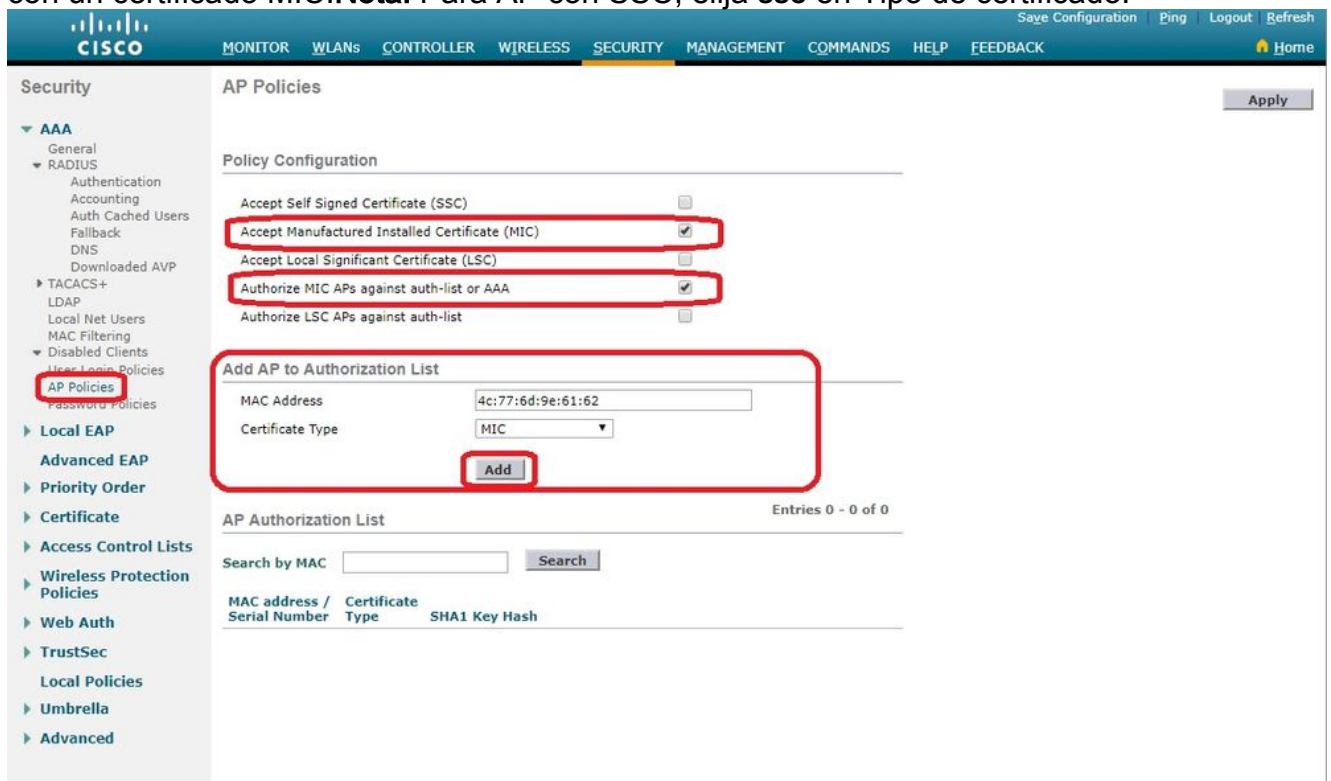
En el WLC, utilice la lista de autorización de AP para restringir los AP basados en su dirección MAC. La lista de autorizaciones de AP está disponible en **Security > AP Policies** en la GUI del WLC.

Este ejemplo muestra cómo agregar el AP con la dirección MAC **4c:77:6d:9e:61:62**.

1. Desde la GUI del controlador del WLC, haga clic **Security > AP Policies** y aparecerá la página Políticas de punto de acceso.
2. Haga clic en el **Add** situado en el lado derecho de la pantalla.



3. Bajo **Add AP to Authorization List**, escriba el **AP MAC** (no la dirección MAC de radio AP). A continuación, elija el tipo de certificado y haga clic en **Add**. En este ejemplo, se agrega un AP con un certificado MIC. **Nota:** Para AP con SSC, elija **ssc** en Tipo de certificado.



- El AP se agrega a la lista de autorización del AP y se enumera debajo **AP Authorization List**.
4. En Configuración de directivas, active la casilla de verificación **Authorize MIC APs against auth-list or AAA**. Cuando se selecciona este parámetro, el WLC verifica primero la lista de autorización local. Si el MAC AP no está presente, verifica el servidor RADIUS.

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:

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	

Verificación

Para verificar esta configuración, necesita conectar el AP con la dirección MAC **4c:77:6d:9e:61:62** a la red y al monitor. Use el comando `debug capwap events/errors enable` y `debug aaa all enable` comandos para realizar esta operación.

Este resultado muestra las depuraciones cuando la dirección MAC del AP no está presente en la lista de autorización del AP:

Nota: Algunas de las líneas del resultado se han movido a la segunda línea debido a restricciones de espacio.

```
(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

```

Esta salida muestra los debugs cuando la dirección MAC del LAP se agrega a la lista de autorización AP:

Nota: Algunas de las líneas del resultado se han movido a la segunda línea debido a restricciones de espacio.

```

(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

```

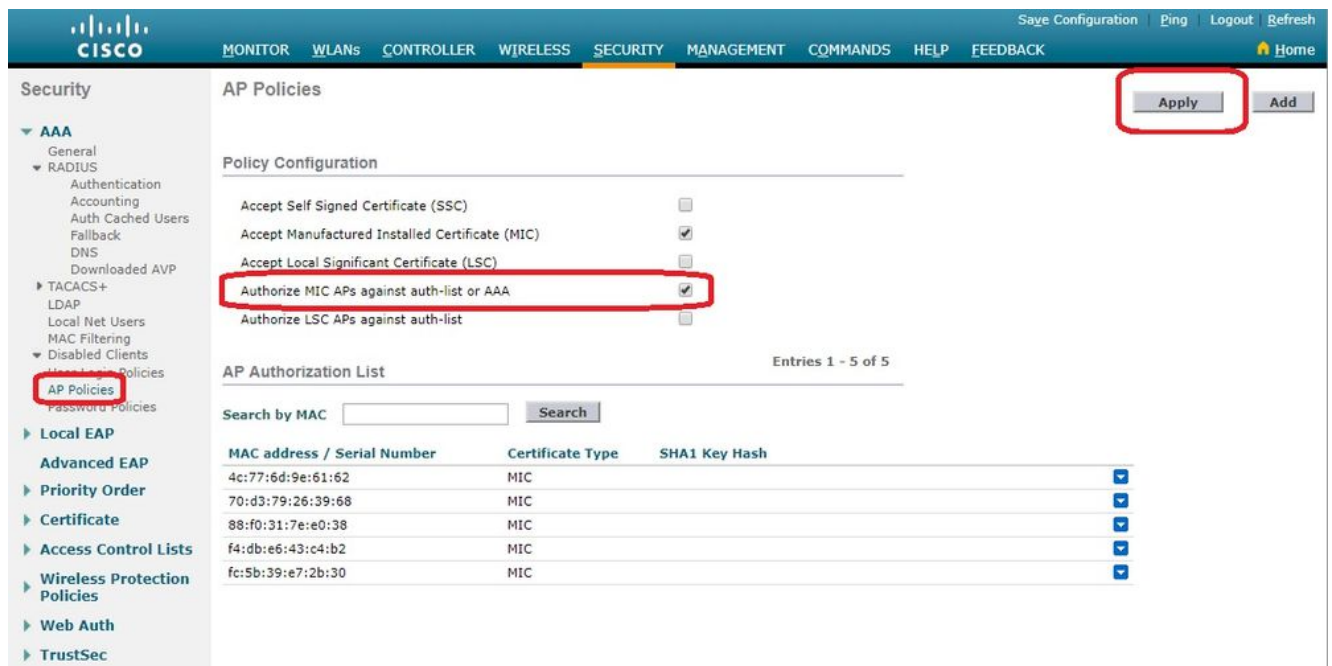
Autorización de AP contra un Servidor AAA

También puede configurar los WLC para utilizar los servidores RADIUS para autorizar los AP que

utilizan los MIC. El WLC utiliza una dirección MAC del AP como nombre de usuario y contraseña cuando envía la información a un servidor RADIUS. Por ejemplo, si la dirección MAC del AP es 4c:77:6d:9e:61:62, tanto el nombre de usuario como la contraseña utilizados por el controlador para autorizar el AP son esa dirección mac usando el delimitador definido.

Este ejemplo muestra cómo configurar los WLC para autorizar los AP usando Cisco ISE.

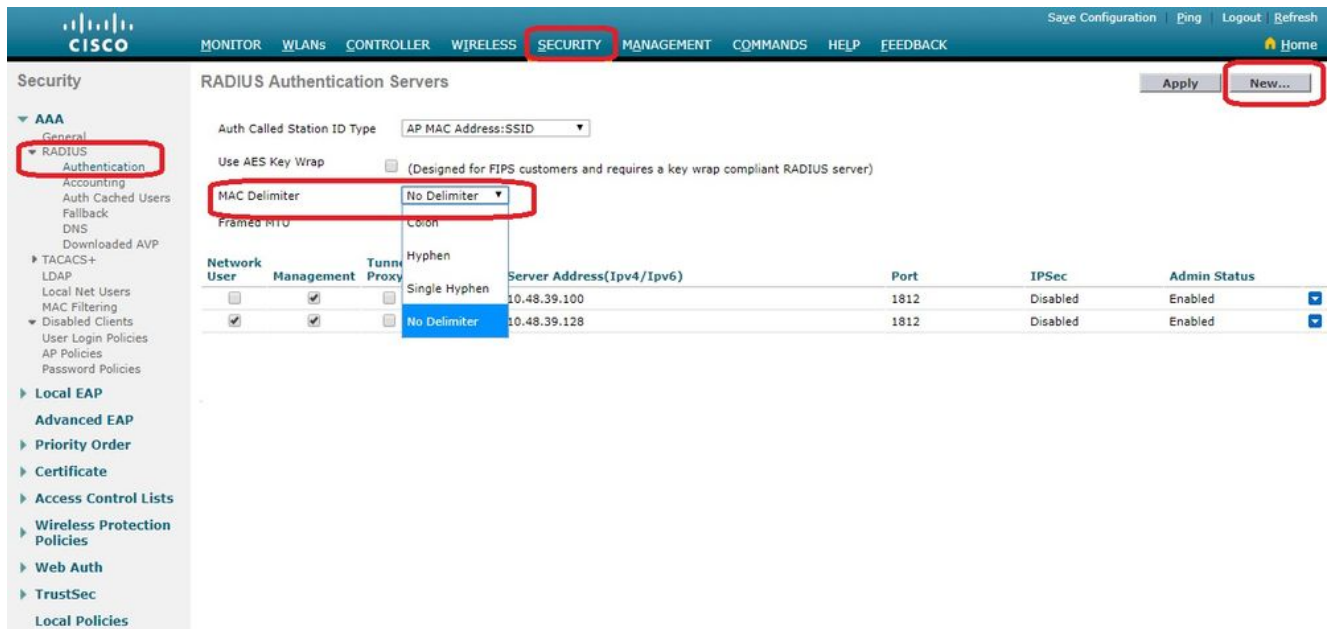
1. Desde la GUI del controlador del WLC, haga clic **Security > AP Policies**. Aparecerá la página Políticas de AP.
2. En Configuración de directivas, active la casilla de verificación **Authorize MIC APs against auth-list or AAA**. Cuando elige este parámetro, el WLC verifica primero la lista de autorización local. Si el MAC AP no está presente, verifica el servidor RADIUS.



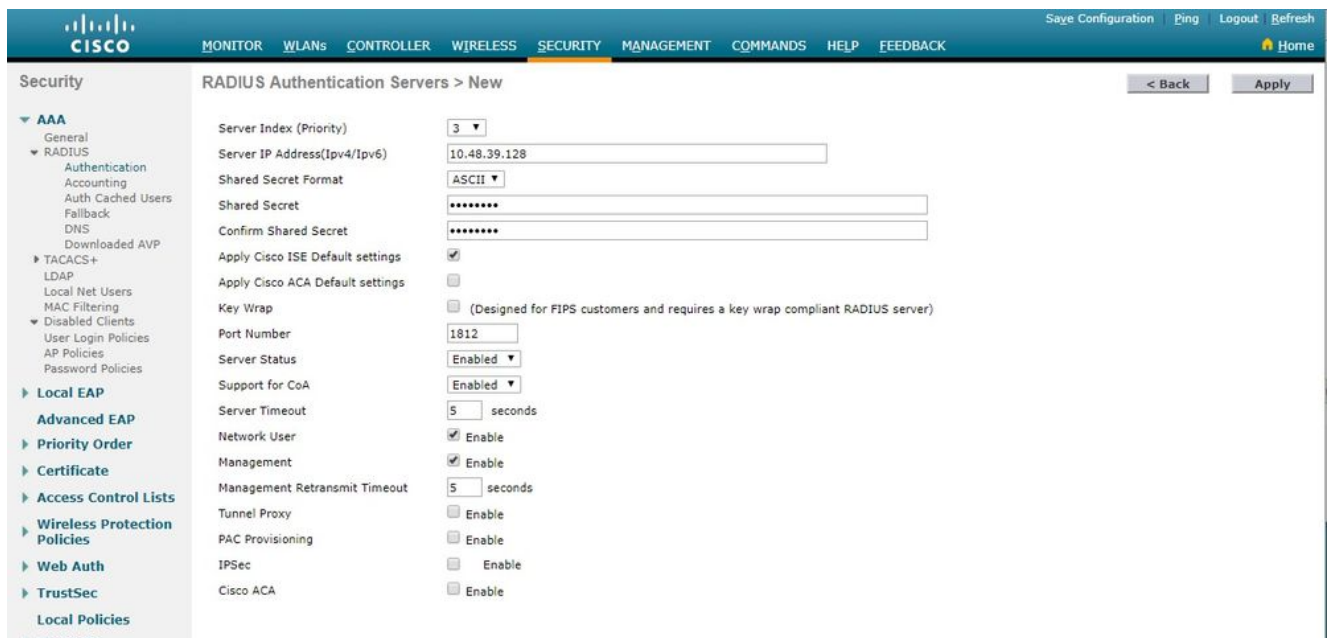
The screenshot shows the Cisco WLC GUI for AP Policies configuration. The left sidebar has 'AP Policies' highlighted. The main area shows the 'Policy Configuration' section with several checkboxes. The checkbox for 'Authorize MIC APs against auth-list or AAA' is checked and highlighted with a red box. 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	

3. Vaya a **Security > RADIUS Authentication** desde la GUI del controlador para mostrar el **RADIUS Authentication Servers** página. En esta página puede definir el **delimitador MAC**. El WLC obtiene la dirección MAC del AP y la envía al servidor Radius usando el delimitador definido aquí. esto es importante para que el nombre de usuario coincida con lo que está configurado en el servidor Radius. En este ejemplo, **No Delimiter** se utiliza para que el nombre de usuario sea 4c776d9e6162.



4. A continuación, haga clic en New para definir un servidor RADIUS.



5. Defina los parámetros del servidor RADIUS en el RADIUS Authentication Servers > New página. Estos parámetros incluyen el RADIUS Server IP Address, Shared Secret, Port Number, y Server Status. Cuando haya terminado, haga clic en Apply. En este ejemplo se utiliza Cisco ISE como servidor RADIUS con la dirección IP 10.48.39.128.

Configuración de Cisco ISE para autorizar puntos de acceso

Para habilitar Cisco ISE para autorizar AP, debe completar estos pasos:

1. Configure el WLC como un cliente AAA en Cisco ISE.
2. Agregue las direcciones MAC de AP a la base de datos en Cisco ISE.

Sin embargo, podría estar agregando la dirección MAC del AP como terminales (la mejor manera) o como usuarios (cuyas contraseñas son también la dirección MAC), pero esto requiere que reduzca los requisitos de las políticas de seguridad de contraseñas.

Debido al hecho de que el WLC no envía el atributo NAS-Port-Type, que es un requisito en ISE para coincidir con el flujo de trabajo de autenticación de dirección MAC (MAB), debe ajustar esto.

Configure un nuevo perfil de dispositivo donde MAB no requiera el atributo NAS-Port-Type

Vaya a **Administration > Network device profile** y crear un nuevo perfil de dispositivo. Habilite RADIUS y establezca el flujo de MAB cableado para requerir service-type=Call-check como se ilustra en la imagen. Puede copiar otras configuraciones del perfil clásico de Cisco, pero la idea es no requerir el atributo 'Nas-port-type' para un flujo de trabajo de MAB cableado.

The screenshot shows the Cisco ISE Administration interface. At the top, there is a navigation bar with the Cisco ISE logo and the path 'Administration > Network Resources'. Below this, there are tabs for 'Network Devices', 'Network Device Groups', 'Network Device Profiles' (which is selected), and 'External RADIUS Servers'. The main content area shows the configuration for a profile named 'Ciscotemp'. The 'Name' field is 'Ciscotemp'. The 'Description' field is empty. The 'Icon' field has a Cisco logo and two buttons: 'Change icon...' and 'Set To Default'. The 'Vendor' field is 'Cisco'. Under 'Supported Protocols', 'RADIUS' is checked, while 'TACACS+' and 'TrustSec' are unchecked. Below this is a section for 'RADIUS Dictionaries'. The 'Templates' section is expanded, showing 'Authentication/Authorization' and 'Flow Type Conditions'. Under 'Flow Type Conditions', there is a checked checkbox for 'Wired MAB detected if the following condition(s) are met :'. Below this, there is a configuration rule: 'Radius:Service-Type' followed by a dropdown arrow, an equals sign, 'Call Check' followed by a dropdown arrow, a trash icon, and a plus icon.

Configure el WLC como un cliente AAA en Cisco ISE

1. Vaya a **Administration > Network Resources > Network Devices > Add**. Aparecerá la página Nuevo dispositivo de red.
2. En esta página, defina el WLC Name, Interfaz de gestión IP Address y Radius Authentications Settings como Shared Secret. Si planea ingresar las

direcciones MAC del AP como puntos finales, asegúrese de utilizar el perfil de dispositivo personalizado configurado anteriormente en lugar del perfil predeterminado de Cisco.

The screenshot shows 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 the navigation menu with options like System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, 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 shows the configuration for a device named "WLC5520". The configuration includes fields for Name, Description, IP Address (10.48.71.20/32), Device Profile (Cisco), Model Name, Software Version, Location (LAB), IPSEC (No), and Device Type (WLC-lab). The RADIUS Authentication Settings are also visible, including the Shared Secret and CoA Port (1700).

3. Haga clic **Submit**.

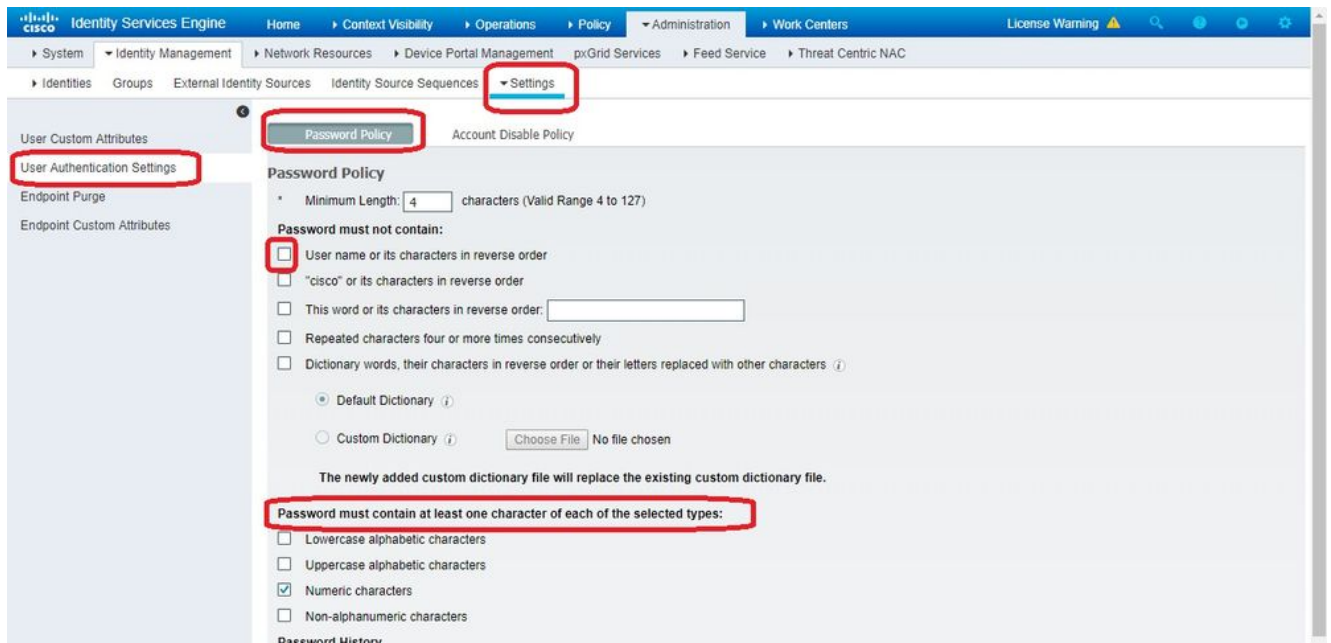
Agregue la dirección MAC del punto de acceso a la base de datos de terminales en Cisco ISE

Vaya a **Administration > Identity Management > Identities** y agregue las direcciones MAC a la base de datos de terminales.

Agregar la dirección MAC del punto de acceso a la base de datos de usuarios en Cisco ISE (opcional)

Si no desea modificar el perfil de MAB cableado y elige poner la dirección MAC del AP como usuario, debe reducir los requisitos de la política de contraseñas.

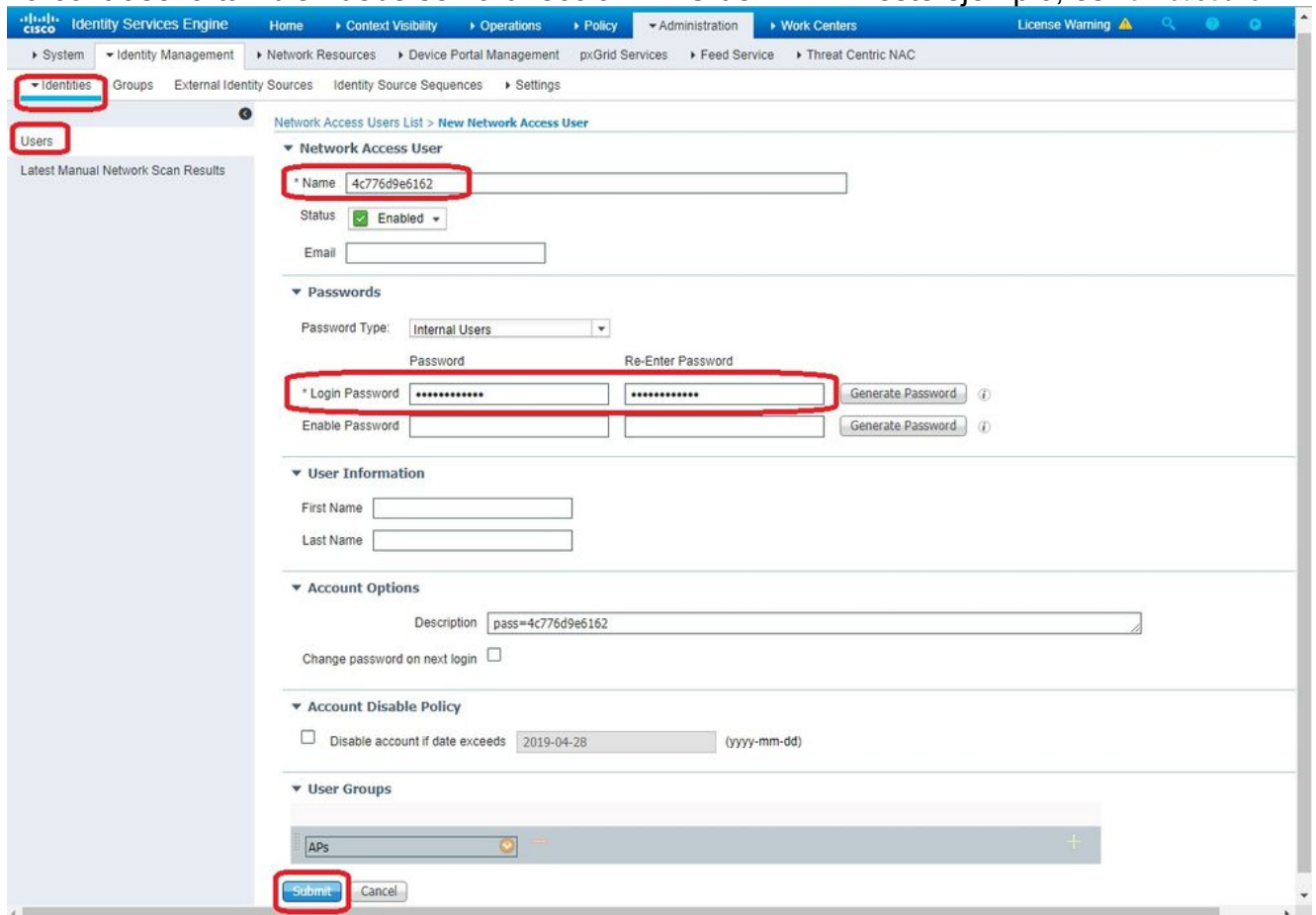
1. Vaya a **Administration > Identity Management**. Aquí tenemos que asegurarnos de que la política de contraseñas permite el uso del nombre de usuario como contraseña y la política también debe permitir el uso de los caracteres de dirección mac sin la necesidad de diferentes tipos de caracteres. Vaya a **Settings > User Authentication Settings > Password Policy**:



2. A continuación, vaya a **Identities > Users** y haga clic en **Add**. Cuando aparezca la página **User Setup** (Configuración de usuario), defina el nombre de usuario y la contraseña para este AP como se muestra.

Consejo: Use el comando **Description** para introducir la contraseña y poder saber fácilmente qué se ha definido como contraseña.

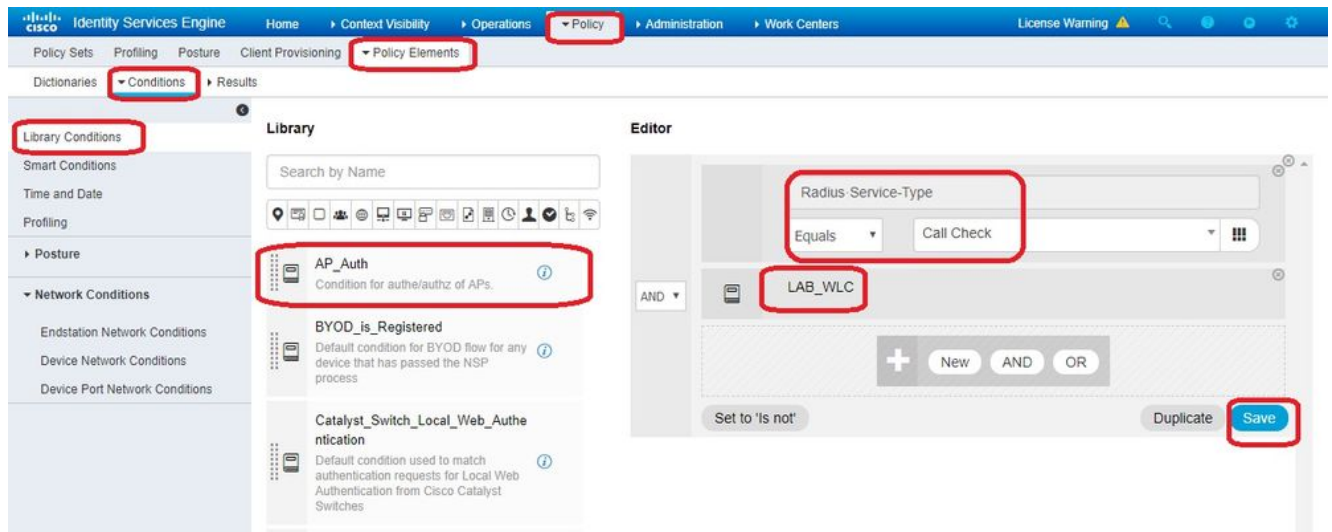
La contraseña también debe ser la dirección MAC del AP. En este ejemplo, es **4c776d9e6162**.



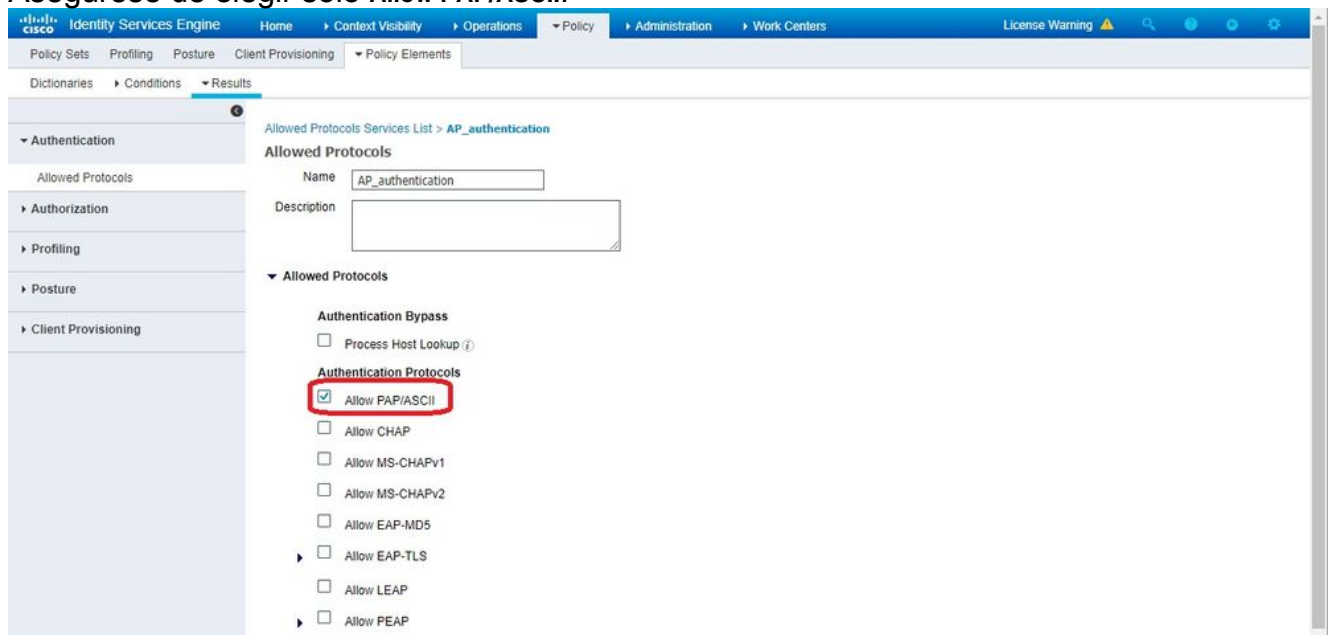
3. Haga clic **Submit**.

Definir un conjunto de políticas

1. Es necesario definir un **Policy Set** para hacer coincidir la solicitud de autenticación proveniente del WLC. En primer lugar, cree una condición desplazándose a **Policy > Policy Elements > Conditions** y creando una nueva condición para que coincida con la ubicación del WLC, en este ejemplo, 'LAB_WLC' y **Radius:Service-Type Equals Call Check** que se utiliza para la autenticación de Mac. Aquí la condición se denomina 'AP_Auth'.



2. Haga clic **Save**.
3. A continuación, cree una nueva **Allowed Protocols Service** para la autenticación de AP. Asegúrese de elegir sólo **Allow PAP/ASCII**:



4. Elija el servicio creado anteriormente en el **Allowed Protocols/Server Sequence**. Expanda el **View** y en **Authentication Policy > Use > Internal Users** para que ISE busque en la base de datos interna el nombre de usuario/contraseña del punto de acceso.

The image displays two screenshots of the Cisco Identity Services Engine (ISE) web interface, specifically the Policy Sets configuration page.

Top Screenshot: Policy Sets Overview

- Navigation: Home > Context Visibility > Operations > Policy > Administration > Work Centers
- Sub-navigation: Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements
- Buttons: Reset, Save
- Table Headers: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, View
- Table Content:

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

- Navigation: Home > Context Visibility > Operations > Policy > Administration > Work Centers
- Sub-navigation: Policy Sets > Policy4APsAuth
- Buttons: Reset, Save
- Table Headers: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits
- Table Content:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Policy4APsAuth		AP_Auth	AP_authentication	19
- Section: Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Users	19	⚙️
- Buttons: Reset, Save

5. Haga clic **Save**.

Verificación

Para verificar esta configuración, necesita conectar el AP con la dirección MAC 4c:77:6d:9e:61:62 a la red y al monitor. Use el comando `debug capwap events/errors enable` y `debug aaa all enable` para realizar esta acción.

Como se ve desde los debugs, el WLC pasó la dirección MAC del AP al servidor RADIUS 10.48.39.128, y el servidor autenticó con éxito el AP. Luego, el AP se registra con el controlador.

Nota: Algunas de las líneas del resultado se han movido a la segunda línea debido a restricciones de espacio.

```
*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, 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 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 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: 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

Utilice estos comandos para resolver problemas de configuración:

- debug capwap events enable: configura la depuración de los eventos LWAPP
- debug capwap packet enable: configura la depuración del seguimiento del paquete LWAPP
- debug capwap errors enable—Configura el debug de los errores del paquete LWAPP
- debug aaa all enable: configura la depuración de todos los mensajes AAA

En este caso, ISE informa en los registros en directo de RADIUS que el nombre de usuario no es VÁLIDO en el momento en que se están autorizando los AP en ISE, significa que la autenticación se está verificando en la base de datos de terminales y que no ha modificado el perfil de MAB cableado como se explica en este documento. ISE considera que una autenticación de dirección MAC no es válida si no coincide con el perfil MAB por cable/inalámbrico, que de forma predeterminada requiere el atributo NAS-port-type que no envía el WLC.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).