

Configurar a autorização de ponto de acesso em uma rede sem fio unificada

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Autorização de AP leve](#)

[Configurar](#)

[Configuração usando a lista de autorização interna no WLC](#)

[Verificar](#)

[Autorização AP em relação a um servidor AAA](#)

[Configurar o Cisco ISE para autorizar APs](#)

[Configure um novo perfil de dispositivo em que MAB não exija o atributo do tipo de porta NAS](#)

[Configurar a WLC como um cliente AAA no Cisco ISE](#)

[Adicione o endereço MAC do AP ao banco de dados de endpoint no Cisco ISE](#)

[Adicione o endereço MAC do AP ao banco de dados do usuário no Cisco ISE \(opcional\)](#)

[Definir um conjunto de políticas](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar a WLC para autorizar o Ponto de Acesso (AP) com base no endereço MAC dos APs.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de como configurar um Cisco Identity Services Engine (ISE)
- Conhecimento da configuração de APs Cisco e WLCs Cisco
- Conhecimento das soluções Cisco Unified Wireless Security

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLCs executando o software AireOS 8.8.11.0APs Wave1: 1700/2700/3700 e 3500

(1600/2600/3600 ainda são suportados, mas o suporte ao AireOS termina na versão 8.5.x) APs Wave2: 1800/2800/3800/4800, 1540 e 1560 versão do 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Autorização de AP leve

Durante o processo de registro do AP, os APs e as WLCs se autenticam mutuamente com o uso de certificados X.509. Os certificados X.509 são gravados em flash protegido no AP e na WLC na fábrica pela Cisco.

No AP, os certificados instalados na fábrica são chamados de certificados instalados na fábrica (MIC). Todos os APs da Cisco fabricados após 18 de julho de 2005 possuem MICs.

Além dessa autenticação mútua que ocorre durante o processo de registro, as WLCs também podem restringir os APs que se registram com eles com base no endereço MAC do AP.

A falta de uma senha forte com o uso do endereço MAC do AP não é um problema porque o controlador usa o MIC para autenticar o AP antes de autorizar o AP através do servidor RADIUS. O uso do MIC fornece autenticação forte.

A autorização do AP pode ser executada de duas maneiras:

- Usando a lista de autorização interna no WLC
- Usando o banco de dados de endereços MAC em um servidor AAA

Os comportamentos dos APs diferem com base no certificado usado:

- APs com SSCs—A WLC usa apenas a lista de autorização interna e não encaminha uma solicitação a um servidor RADIUS para esses APs
- APs com MICs—A WLC pode usar a lista de autorização interna configurada na WLC ou usar um servidor RADIUS para autorizar os APs

Este documento discute a autorização do AP com o uso da lista de autorização interna e do servidor AAA.

Configurar

Configuração usando a lista de autorização interna no WLC

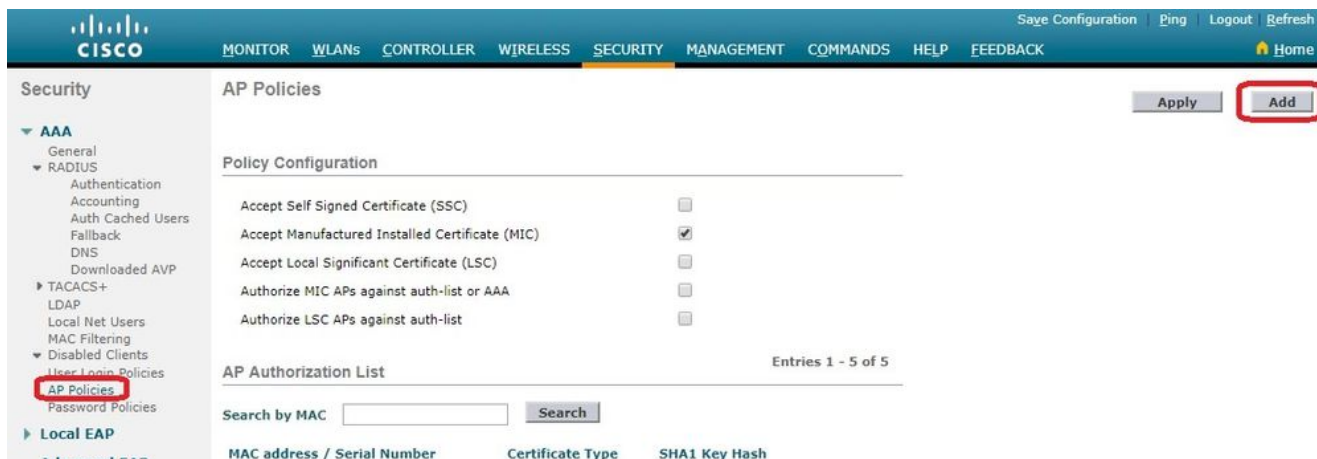
Na WLC, use a lista de autorização de APs para restringir os APs com base em seus endereços MAC. A lista de autorização de AP está disponível em **Security > AP Policies** na GUI da WLC.

Este exemplo mostra como adicionar o AP com endereço MAC `4c:77:6d:9e:61:62`.

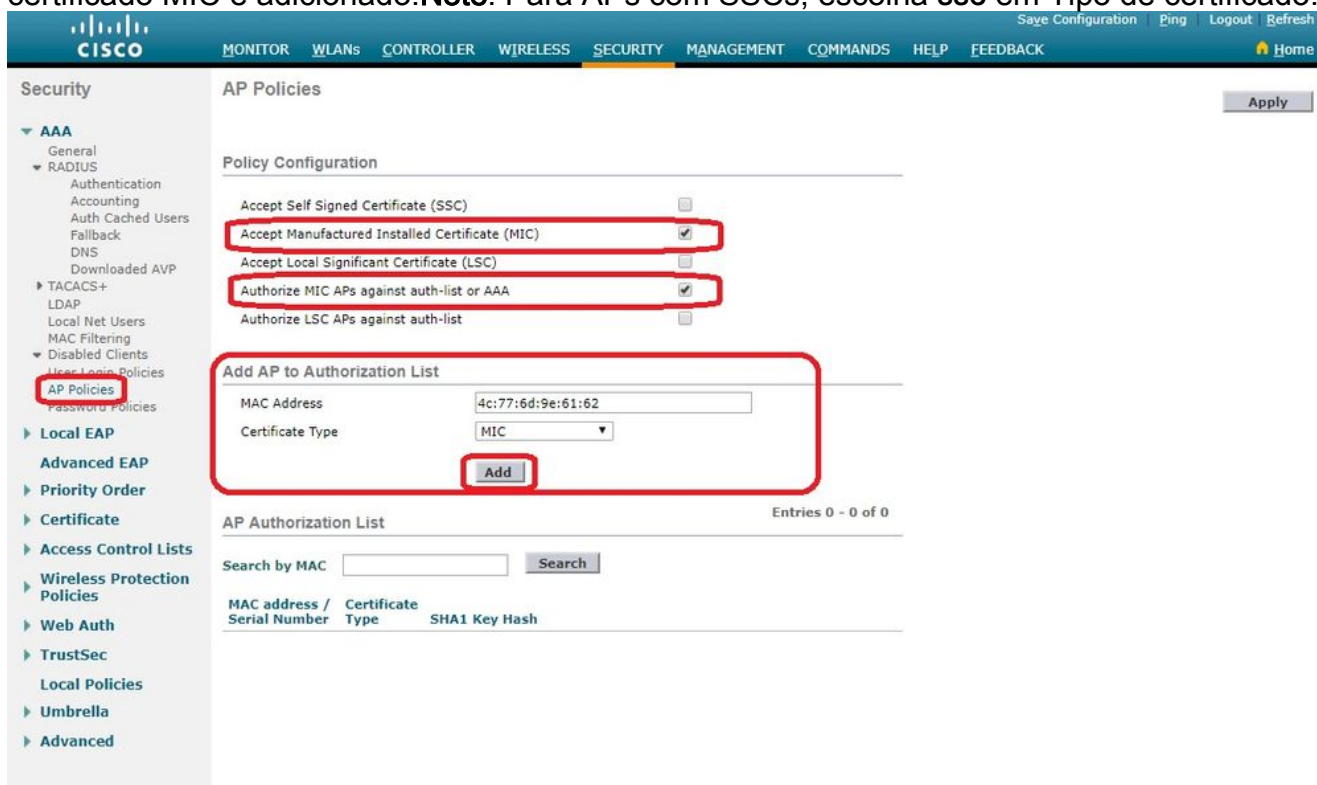
1. Na GUI da controladora do WLC, clique em **Security > AP Policies** e a página Políticas de AP é

exibida.

2. Clique no botão **Add** no lado direito da tela.



3. Sob **Add AP to Authorization List**, digite o AP MAC (não o endereço MAC do rádio do AP). Em seguida, escolha o tipo de certificado e clique em **Add**. Neste exemplo, um AP com um certificado MIC é adicionado. **Note:** Para APs com SSCs, escolha **ssc** em Tipo de certificado.



O AP é adicionado à lista de autorização de AP e está listado em AP Authorization List.

4. Em Configuração de política, marque a caixa para **Authorize MIC APs against auth-list or AAA**. Quando esse parâmetro é selecionado, a WLC verifica primeiro a lista de autorização local. Se o MAC do AP não estiver presente, ele verifica o servidor RADIUS.

The screenshot shows the Cisco Security configuration interface. The left sidebar has 'AP Policies' selected. The main content area shows the 'AP Policies' configuration. Under 'Policy Configuration', the checkbox for 'Authorize MIC APs against auth-list or AAA' is checked. Below this, the 'AP Authorization List' table contains the following 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	

Verificar

Para verificar essa configuração, você precisa conectar o AP com o endereço MAC **4c:77:6d:9e:61:62** à rede e ao monitor. Use o `debug capwap events/errors enable` e `debug aaa all enable` para executar essa tarefa.

Esta saída mostra as depurações quando o endereço MAC do AP não está presente na lista de autorização do AP:

Note: Algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

```
(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 saída mostra as depurações quando o endereço MAC do LAP é adicionado à lista de autorização do AP:

Note: Algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

```

(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
```

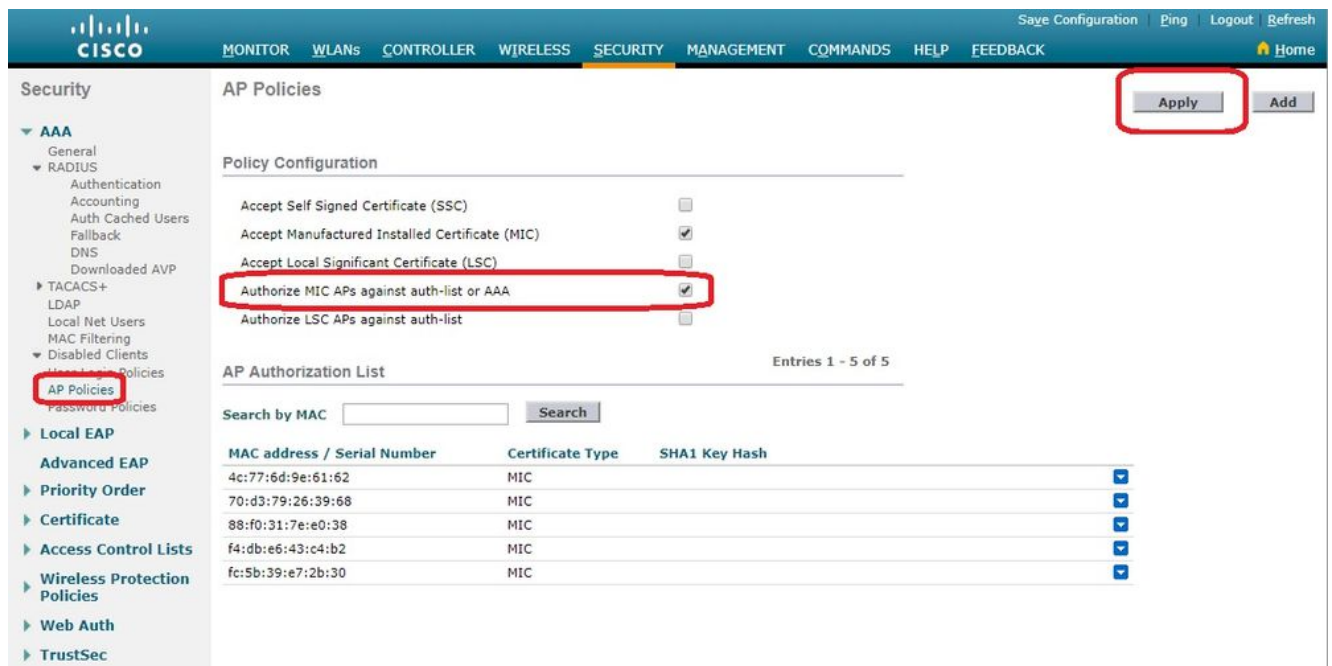
Autorização AP em relação a um servidor AAA

Você também pode configurar WLCs para usar servidores RADIUS para autorizar APs usando

MICs. A WLC usa um endereço MAC do AP como nome de usuário e senha ao enviar as informações para um servidor RADIUS. Por exemplo, se o endereço MAC do AP for 4c:77:6d:9e:61:62, o nome de usuário e a senha usados pelo controlador para autorizar o AP são aqueles endereços mac que usam o delimitador definido.

Este exemplo mostra como configurar as WLCs para autorizar APs usando o Cisco ISE.

1. Na GUI da controladora do WLC, clique em **Security > AP Policies**. A página Políticas de AP é exibida.
2. Em Configuração de política, marque a caixa para **Authorize MIC APs against auth-list or AAA**. Quando você escolhe esse parâmetro, a WLC verifica primeiro a lista de autorização local. Se o MAC do AP não estiver presente, ele verifica o servidor RADIUS.

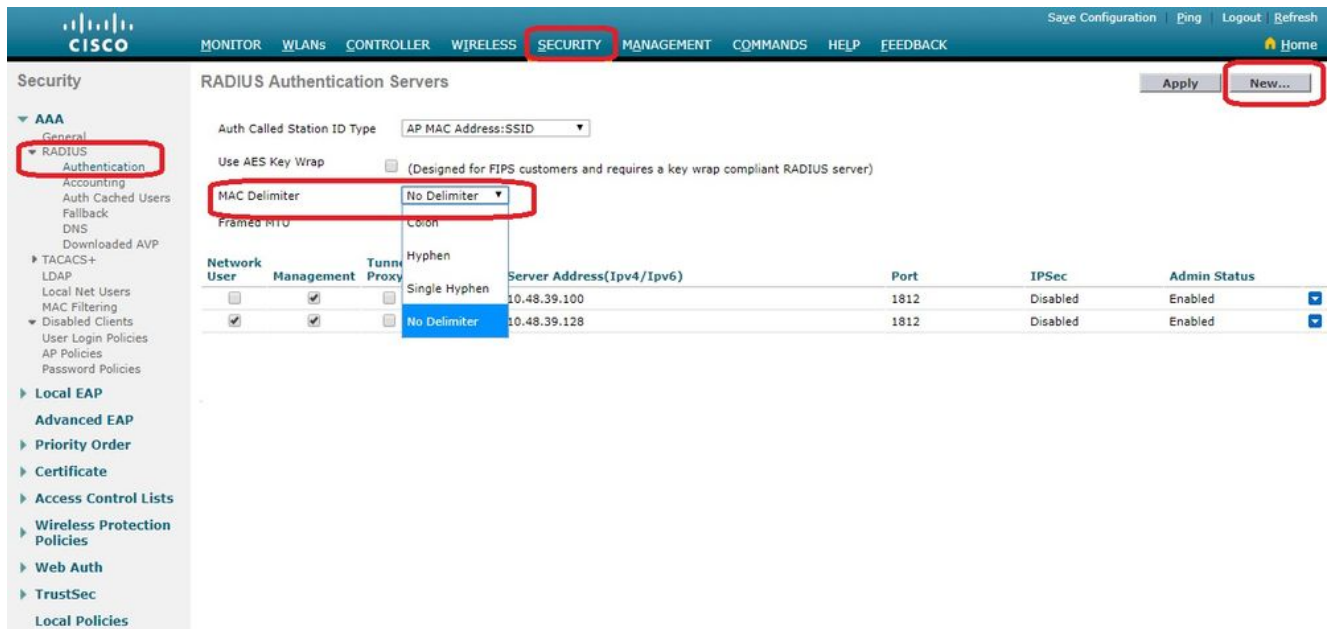


The screenshot shows the Cisco WLC GUI with the following configuration details:

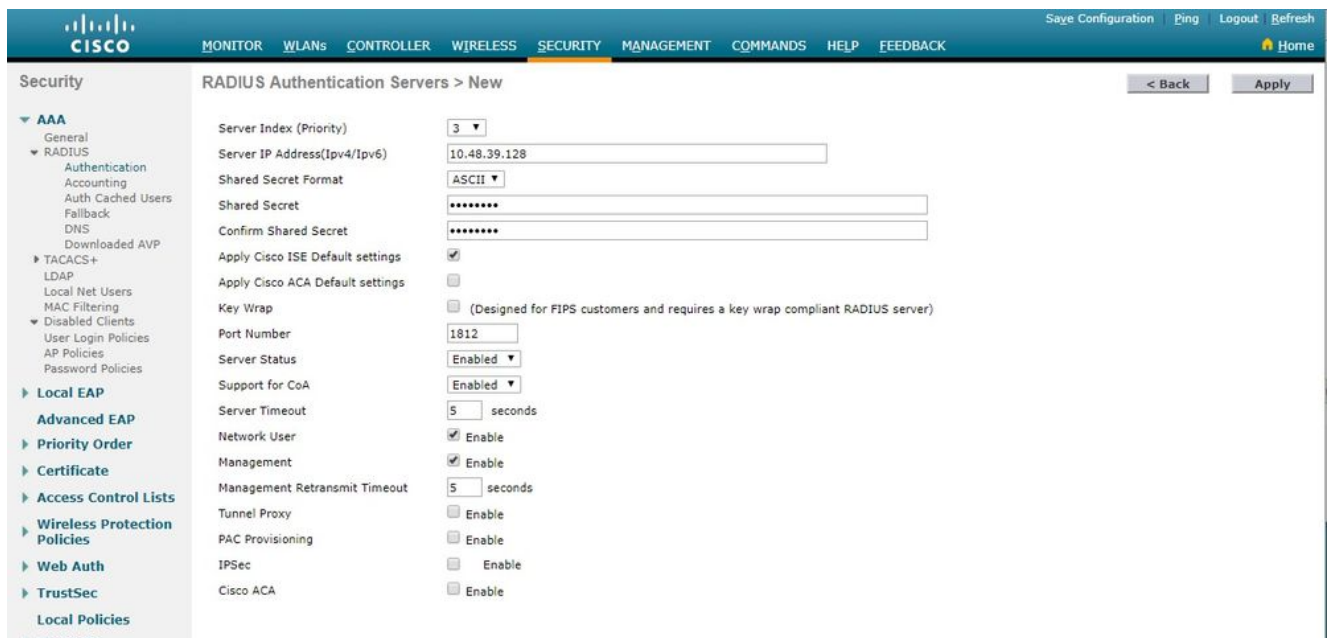
- Policy Configuration:**
 - Accept Self Signed Certificate (SSC)
 - Accept Manufactured Installed Certificate (MIC)
 - Accept Local Significant Certificate (LSC)
 - Authorize MIC APs against auth-list or AAA** (highlighted with a red box)
 - Authorize LSC APs against auth-list
- AP Authorization List:** Entries 1 - 5 of 5

MAC address / Serial Number	Certificate Type	SHA1 Key Hash
4c:77:6d:9e:61:62	MIC	
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. Navegue até **Security > RADIUS Authentication** na GUI do controlador para exibir a **RADIUS Authentication Servers**. Nesta página você pode definir o **Delimitador MAC**. A WLC obtém o endereço MAC do AP e o envia ao servidor Radius usando o delimitador definido aqui. Isso é importante para que o nome de usuário corresponda ao que está configurado no servidor Radius. Neste exemplo, o **No Delimiter** é usado para que o nome de usuário seja 4c776d9e6162.



4. Em seguida, clique em **New** para definir um servidor RADIUS.



5. Defina os parâmetros do servidor RADIUS no **RADIUS Authentication Servers > New**. Esses parâmetros incluem o **RADIUS Server IP Address**, **Shared Secret**, **Port Number**, e **Server Status**. Ao concluir, clique em **Apply**. Este exemplo usa o Cisco ISE como o servidor RADIUS com o endereço IP 10.48.39.128.

Configurar o Cisco ISE para autorizar APs

Para permitir que o Cisco ISE autorize APs, você precisa concluir estas etapas:

1. Configure a WLC como um cliente AAA no Cisco ISE.
2. Adicione os endereços MAC do AP ao banco de dados no Cisco ISE.

No entanto, você pode adicionar o endereço MAC do AP como endpoints (a melhor maneira) ou como usuários (cujas senhas também são o endereço MAC), mas isso exige que você reduza os requisitos das políticas de segurança de senha.

Devido ao fato de que a WLC não envia o atributo NAS-Port-Type, que é um requisito no ISE para corresponder ao fluxo de trabalho de autenticação de endereço Mac (MAB), você precisa ajustar isso.

Configure um novo perfil de dispositivo em que MAB não exija o atributo do tipo de porta NAS

Navegue até **Administration > Network device profile** e criar um novo perfil de dispositivo. Ative o RADIUS e defina o fluxo do MAB com fio para exigir service-type=Call-check, conforme ilustrado na imagem. Você pode copiar outras configurações do perfil clássico da Cisco, mas a ideia é não exigir o atributo 'Nas-port-type' para um fluxo de trabalho de MAB com fio.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 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 is for configuring a 'Network Device Profile' named 'Ciscotemp'. The 'Name' field is filled with 'Ciscotemp'. There is a large empty text box for the 'Description'. Below the description, there are two buttons: 'Change icon...' and 'Set To Default'. The 'Vendor' is set to 'Cisco'. Under the 'Supported Protocols' section, 'RADIUS' is checked, while 'TACACS+' and 'TrustSec' are unchecked. There is a section for 'RADIUS Dictionaries' which is currently empty. Below this, there is a 'Templates' section with a link to 'Expand All / Collapse All'. Underneath, there are two expandable sections: 'Authentication/Authorization' and 'Flow Type Conditions'. The 'Flow Type Conditions' section is expanded, showing a checked checkbox and the text 'Wired MAB detected if the following condition(s) are met :'. Below this, there is a list of conditions: '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.

Configurar a WLC como um cliente AAA no Cisco ISE

1. Ir para **Administration > Network Resources > Network Devices > Add**. A página Novo dispositivo de rede é exibida.
2. Nesta página, defina o WLC **Name**, Interface de

gerenciamento IP Address e Radius Authentications Settings curtir Shared Secret. Se você planeja inserir os endereços MAC do AP como pontos de extremidade, certifique-se de usar o perfil de dispositivo personalizado configurado anteriormente em vez do perfil padrão Cisco!

The screenshot shows the Cisco ISE Administration console for configuring a Network Device. The device name is WLC5520, and the IP address is 10.48.71.20/32. The device profile is set to Cisco. The RADIUS Authentication Settings are expanded, showing RADIUS UDP Settings with Protocol RADIUS, Shared Secret (masked), and CoA Port 1700. RADIUS DTLS Settings are also visible with DTLS Required unchecked and Shared Secret radius/dtls.

3. Clique em **Submit**.

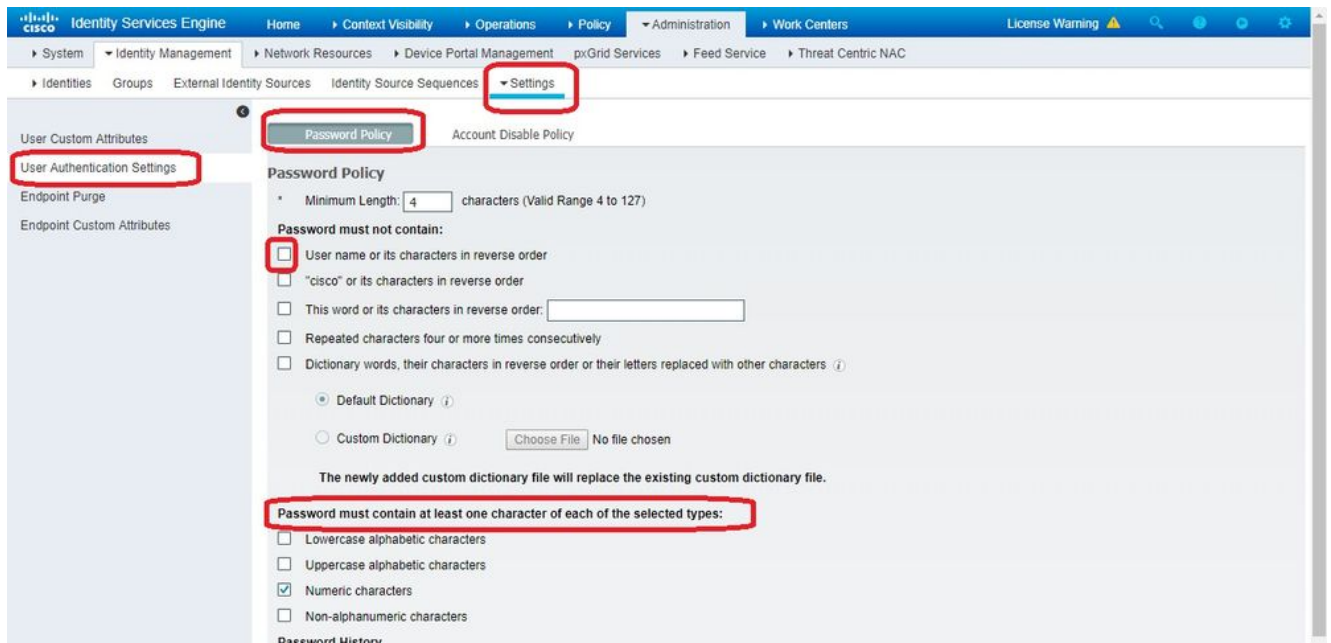
Adicione o endereço MAC do AP ao banco de dados de endpoint no Cisco ISE

Navegue até **Administration > Identity Management > Identities** e adicione os endereços MAC ao banco de dados do endpoint.

Adicione o endereço MAC do AP ao banco de dados do usuário no Cisco ISE (opcional)

Se você não quiser modificar o perfil MAB com fio e optar por colocar o endereço MAC do AP como um usuário, você terá que reduzir os requisitos da política de senha.

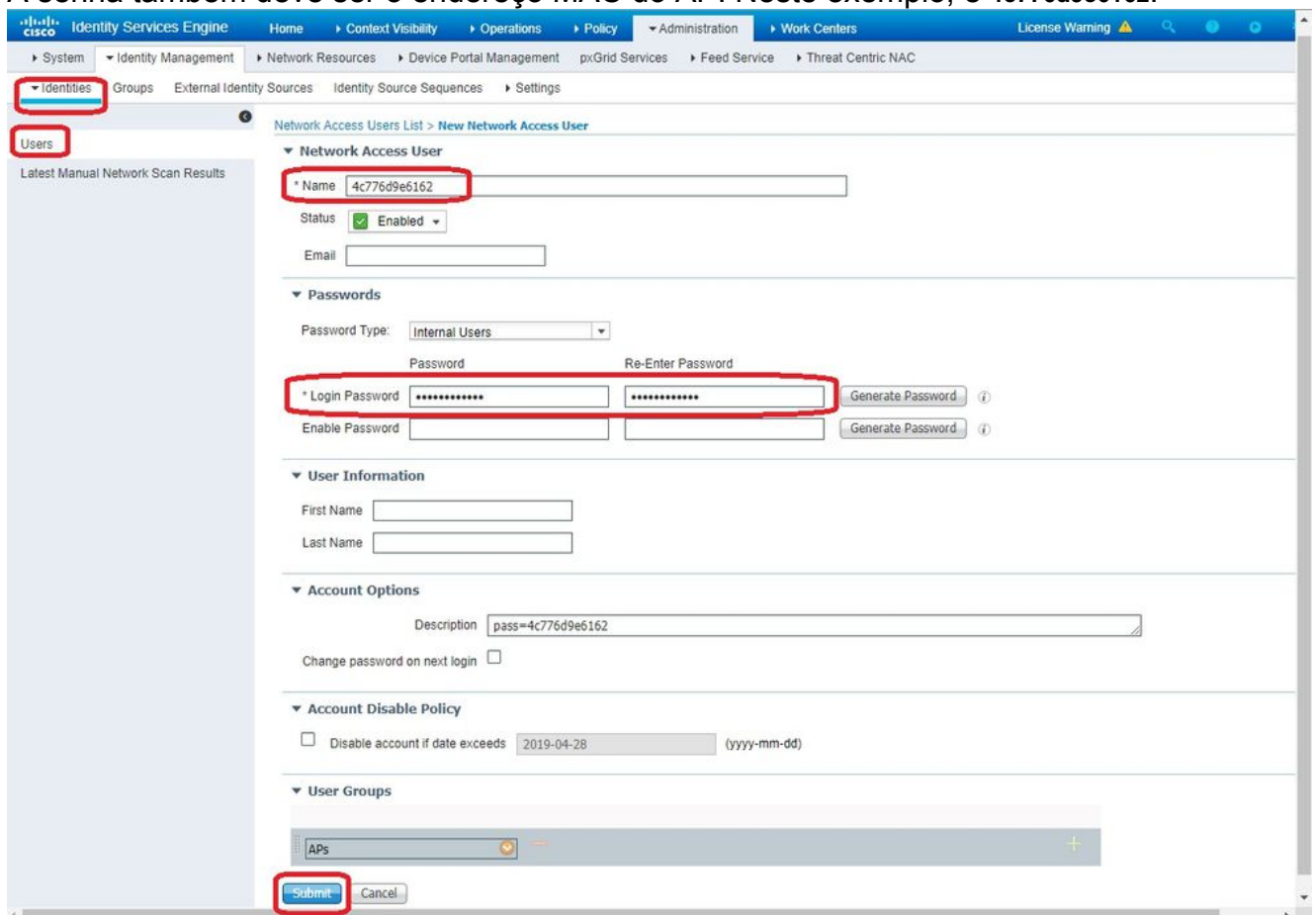
1. Navegue até **Administration > Identity Management**. Aqui precisamos ter certeza de que a política de senha permite o uso do nome de usuário como senha e a política também deve permitir o uso dos caracteres do endereço mac sem a necessidade de tipos diferentes de caracteres. Navegue até **Settings > User Authentication Settings > Password Policy**:



2. Em seguida, navegue até **Identities > Users** e clique em **Add**. Quando a página **User Setup** for exibida, defina o nome de usuário e a senha para esse AP como mostrado.

Tip: Use o **Description** para digitar a senha para depois ser fácil saber o que foi definido como senha.

A senha também deve ser o endereço MAC do AP. Neste exemplo, é **4c776d9e6162**.

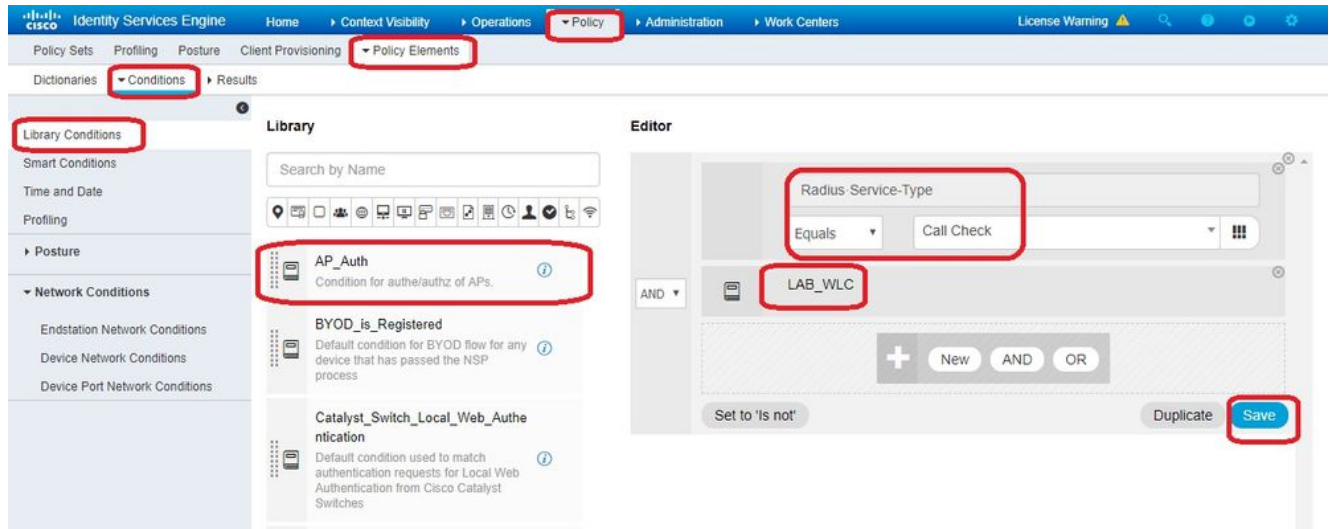


3. Clique em **Submit**.

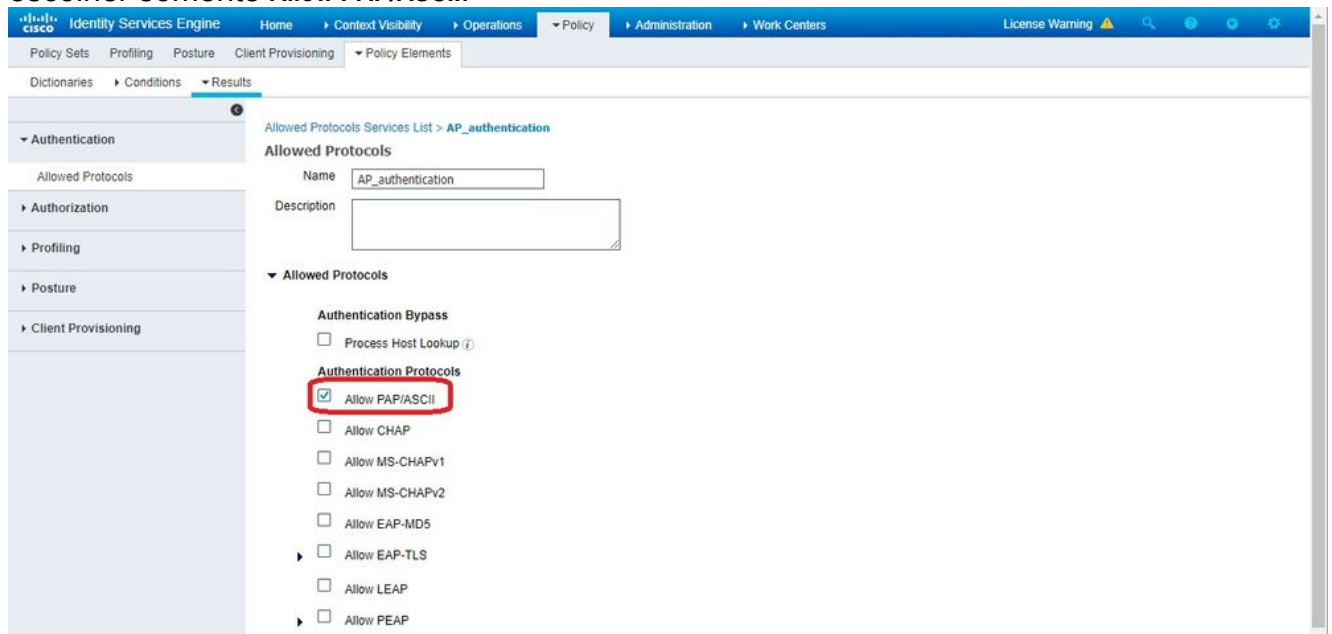
Definir um conjunto de políticas

1. Você precisa definir um **Policy Set** para corresponder à solicitação de autenticação

proveniente da WLC. Primeiro você constrói uma Condição navegando até **Policy > Policy Elements > Condition** criando uma nova condição para corresponder ao local da WLC, neste exemplo, "LAB_WLC" e **Radius:Service-Type Equals Call Check** que é usado para autenticação Mac. Aqui, a condição é chamada de 'AP_Auth'.



2. Clique em **Save**.
3. Em seguida, crie um novo **Allowed Protocols Service** para a autenticação do AP. Certifique-se de escolher somente **Allow PAP/ASCII**:



4. Escolha o Serviço criado anteriormente no **Allowed Protocols/Server Sequence**. Expanda a **View** e sob **Authentication Policy > Use > Internal Users** para que o ISE procure o nome de usuário/senha do AP no BD interno.

The image shows two screenshots of the Cisco Identity Services Engine (ISE) configuration interface. The top screenshot displays the 'Policy Sets' overview, where the 'Policy4APsAuth' policy set is selected. The 'Conditions' column shows 'AP_Auth' and the 'Allowed Protocols / Server Sequence' column shows 'AP_authentication'. The bottom screenshot shows the detailed configuration for 'Policy4APsAuth', where the 'Internal Users' protocol is selected under the 'Authentication Policy' section. The 'Save' button is highlighted in both screenshots.

5. Clique em **Save**.

Verificar

Para verificar essa configuração, você precisa conectar o AP com o endereço MAC 4c:77:6d:9e:61:62 à rede e ao monitor. Use o `debug capwap events/errors enable` e `debug aaa all enable` para executar isso.

Como visto nas depurações, a WLC passou o endereço MAC do AP para o servidor RADIUS 10.48.39.128 e o servidor autenticou com êxito o AP. O AP então se registra com a controladora.

Note: Algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

```
*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

Use estes comandos para solucionar problemas na configuração:

- debug capwap events enable—Configura a depuração de eventos LWAPP
- debug capwap packet enable—Configura a depuração do rastreamento de Pacote LWAPP
- debug capwap errors enable—Configura a depuração de erros do pacote LWAPP
- debug aaa all enable—Configura a depuração de todas as mensagens AAA

Nesse caso, o ISE relata no registro em tempo real do RADIUS o nome de usuário 'INVÁLIDO' no momento em que os APs estão sendo autorizados no ISE, isso significa que a autenticação está sendo verificada no banco de dados de endpoint e que você não modificou o perfil MAB com fio, conforme explicado neste documento. O ISE considera uma autenticação de endereço MAC inválida se ela não corresponder ao perfil MAB com fio/sem fio, que por padrão exige o atributo do tipo de porta NAS que não é enviado pela WLC.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.