在统一无线网络中配置接入点授权

目录

简介

本文档介绍如何配置WLC以根据AP的MAC地址授权接入点(AP)。

先决条件

要求

Cisco 建议您了解以下主题：

- 有关如何配置思科身份服务引擎(ISE)的基本知识
- 了解Cisco AP和Cisco WLC的配置
- Cisco Unified无线安全解决方法知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行AireOS 8.8.111.0软件的WLCWave1 AP:1700/2700/3700和3500（仍然支持1600/2600/3600，但AireOS支持终止于版本8.5.x）Wave2 AP:1800/2800/3800/4800、1540和1560 ISE版本 2.3.0.298

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

轻量AP授权

在AP注册过程中，AP和WLC使用X.509证书相互进行身份验证。Cisco在工厂将X.509证书烧录到AP和WLC上的受保护闪存中。

在AP上，出厂安装的证书称为制造安装的证书(MIC)。 所有在2005年7月18日之后生产的思科AP都具有MIC。

除了在注册过程中发生的这种相互身份验证外，WLC还可以根据AP的MAC地址限制向其注册的AP。

使用AP MAC地址时缺少强密码不是问题，因为控制器在通过RADIUS服务器授权AP之前使用MIC对AP进行身份验证。使用MIC提供强大的身份验证。

AP授权可通过两种方式执行：

- 使用WLC上的内部授权列表
- 在AAA服务器上使用MAC地址数据库

AP的行为因使用的证书而异：

- 带SSC的AP - WLC仅使用内部授权列表，不会向这些AP的RADIUS服务器转发请求
- 带MIC的AP - WLC可以使用在WLC上配置的内部授权列表或使用RADIUS服务器授权AP

本文档讨论使用内部授权列表和AAA服务器的AP授权。

配置

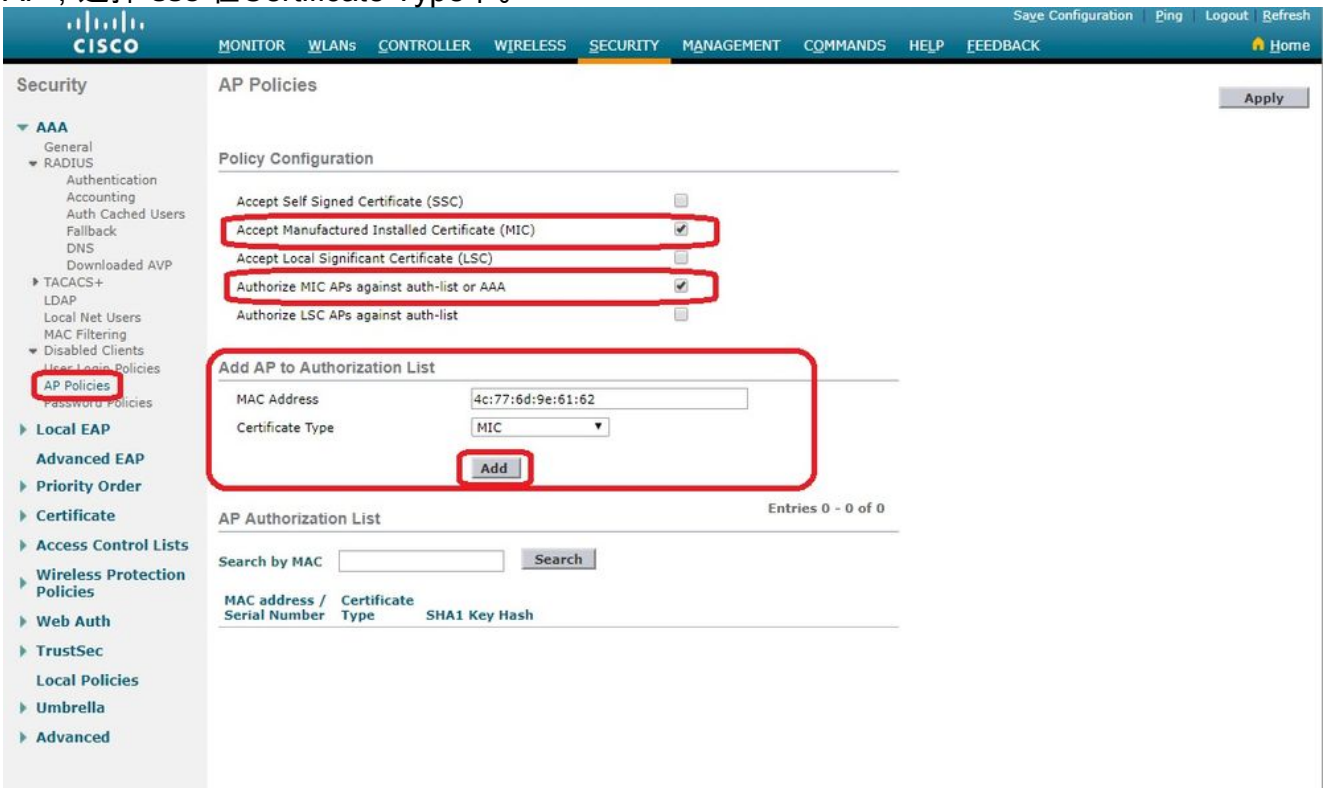
使用WLC上的内部授权列表进行配置

在WLC上，使用AP授权列表根据其MAC地址限制AP。AP授权列表位于 **Security > AP Policies** 在WLC GUI中。

此示例显示如何添加具有MAC地址的AP **4c:77:6d:9e:61:62**.

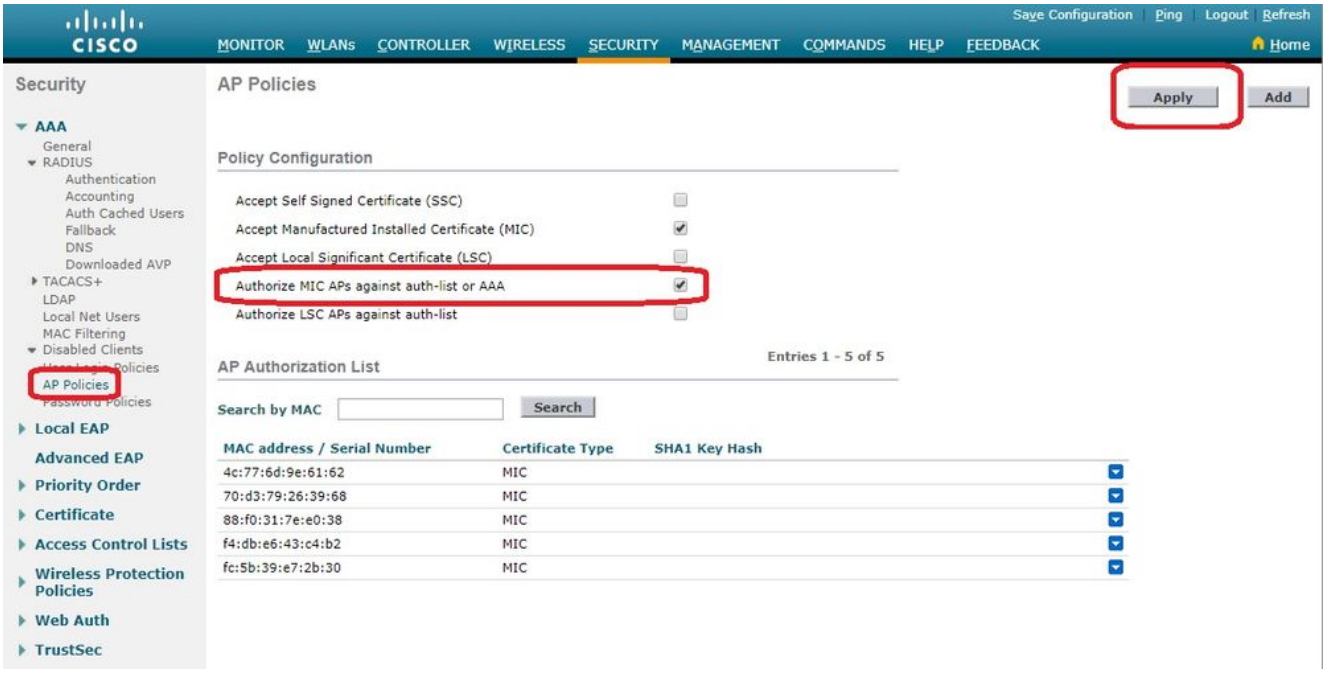
1. 在WLC控制器GUI中，单击 **Security > AP Policies** 系统将显示AP Policies页面。
2. 单击 **Add** 按钮。

3. 低于 **Add AP to Authorization List**，输入 **AP MAC** 地址（不是AP无线电mac地址）。 然后，选择证书类型并单击 **Add**.在本示例中，添加了一个具有MIC证书的AP。**注意**：对于具有SSC的AP，选择 ssc 在Certificate Type下。



AP将添加到AP授权列表，并列在 **AP Authorization List.**

4. 在Policy Configuration（策略配置）下，选中 **Authorize MIC APs against auth-list or AAA**.选择该参数时，WLC首先检查本地授权列表。如果AP MAC不存在，它会检查RADIUS服务器。



验证

要验证此配置，您需要使用MAC地址连接AP **4c:77:6d:9e:61:62** 连接到网络和监控器。请使用 **debug capwap events/errors enable** 和 **debug aaa all enable** 命令。

此输出显示当AP MAC地址不存在于AP授权列表时的调试：

注意：由于空间限制，输出中的某些行已移至第二行。

```
(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
```

此输出显示将LAP MAC地址添加到AP授权列表时的调试：

注意：由于空间限制，输出中的某些行已移至第二行。

```
(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
```

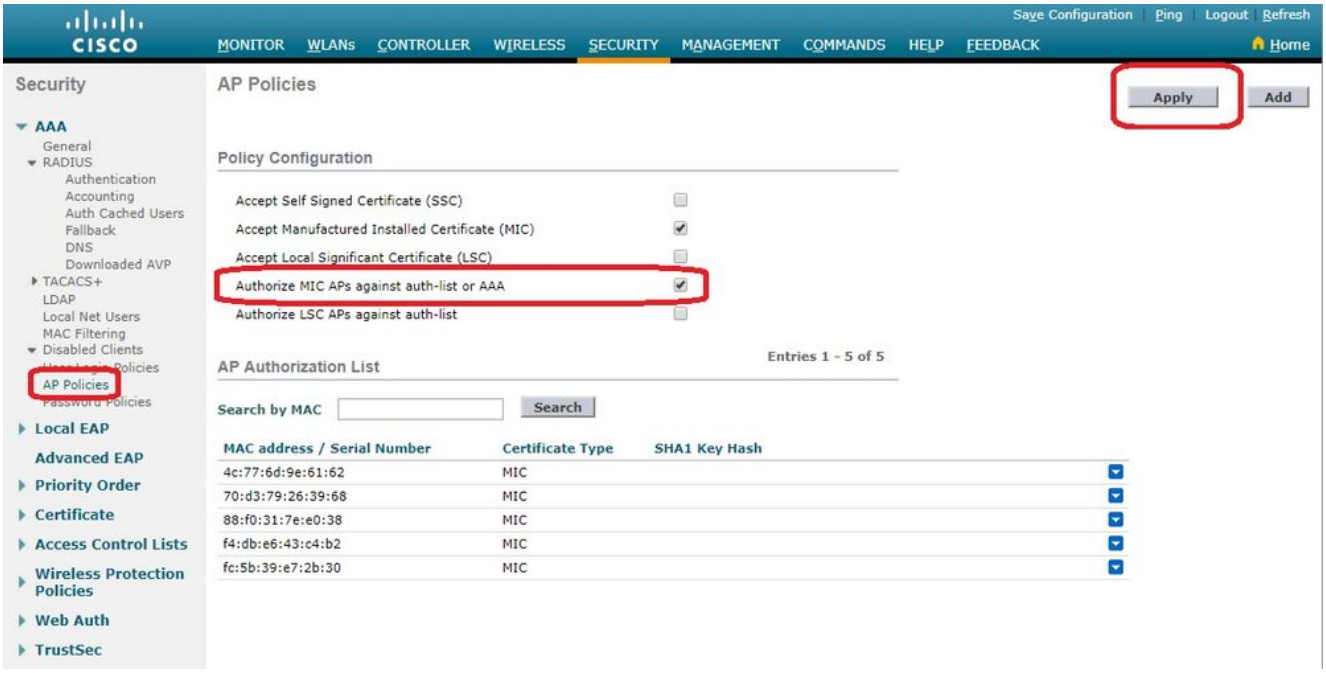
```
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
70:69:5a:51:4e:c0
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed!


*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: Ox36 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
```

针对AAA服务器的AP授权

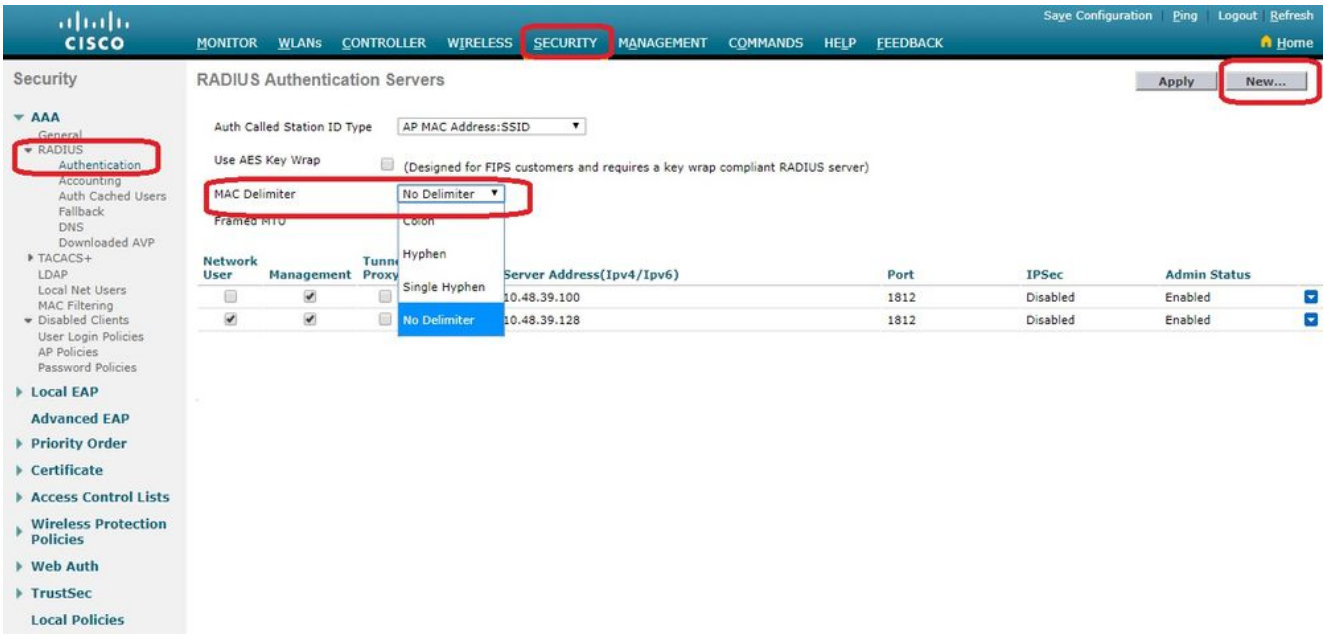
您还可以将WLC配置为使用RADIUS服务器授权使用MIC的AP。当向RADIUS服务器发送信息时，WLC使用AP MAC地址作为用户名和密码。例如，如果AP的MAC地址是 **4c:77:6d:9e:61:62**中，控制器用于授权AP的用户名和密码都是使用已定义的传递器的mac地址。

此示例显示如何配置WLC以使用Cisco ISE授权AP。

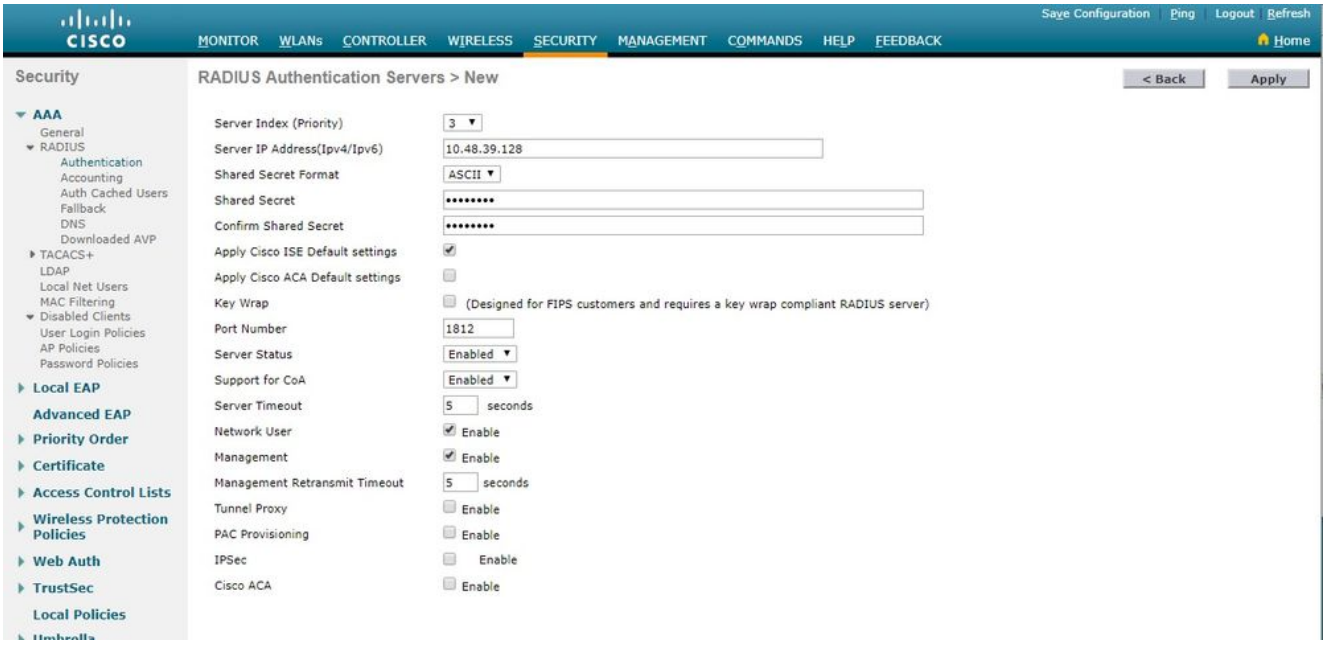
1. 在WLC控制器GUI中，单击 **Security > AP Policies**.系统将显示AP Policies页面。
2. 在Policy Configuration（策略配置）下，选中 **Authorize MIC APs against auth-list or AAA**.当您选择此参数时，WLC首先检查本地授权列表。如果AP MAC不存在，它会检查RADIUS服务器。



3. 导航至 **Security > RADIUS Authentication** 从控制器GUI显示 **RADIUS Authentication Servers** 页码.在此页中，可以定义**MAC分隔符**。WLC获取AP的Mac地址并使用此处定义的分隔符将其发送到Radius服务器。这一点非常重要，以便用户名与Radius服务器中的配置匹配。在本示例中，**No Delimiter** 用于使用户名 **4c776d9e6162**.



4. 然后，单击 **New** 以便定义RADIUS服务器。



5. 在上定义RADIUS服务器参数 **RADIUS Authentication Servers > New** 页码.这些参数包括RADIUS **Server IP Address**, **Shared Secret**, **Port Number**,和 **Server Status**.完成后，单击 **Apply**.此示例使用Cisco ISE作为IP地址为10.48.39.128的RADIUS服务器。

配置Cisco ISE授权AP

要启用Cisco ISE授权AP，您需要完成以下步骤：

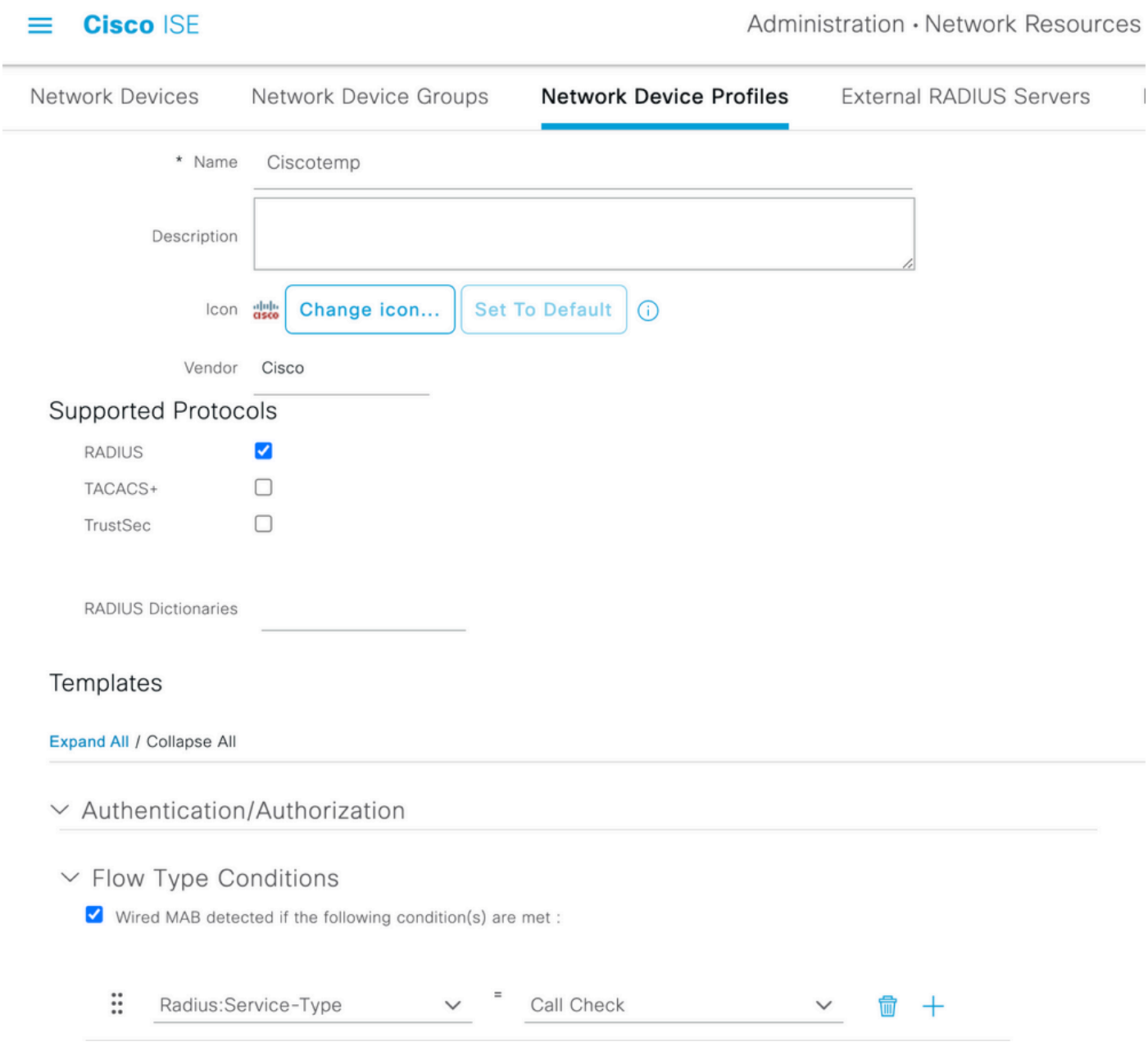
1. 将WLC配置为Cisco ISE上的AAA客户端。
2. 将AP MAC地址添加到Cisco ISE上的数据库。

但是，您可以将AP MAC地址添加为终端（最佳方式）或用户（其密码也是MAC地址），但这要求您降低密码安全策略要求。

由于WLC不发送NAS-Port-Type属性(ISE要求该属性匹配Mac地址身份验证(MAB)工作流程)，您需要调整此属性。

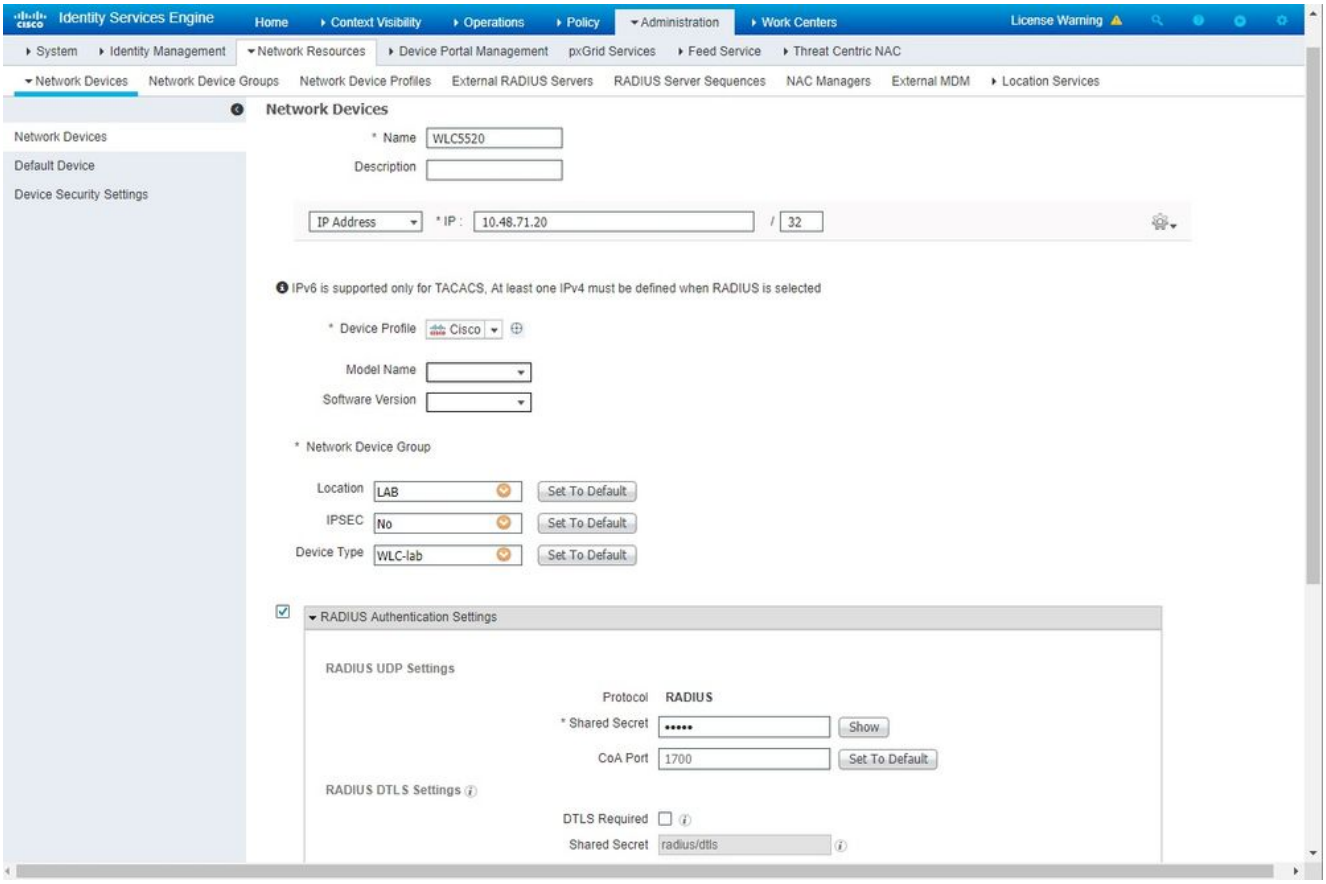
配置MAB不需要NAS端口类型属性的新设备配置文件

导航至 **Administration > Network device profile** 并创建新的设备配置文件。启用RADIUS并将有线MAB流设置为需要service-type=Call-check，如图所示。您可以从经典思科配置文件复制其他设置，但想法是不需要“Nas-port-type”属性来用于有线MAB工作流程。



将WLC配置为Cisco ISE上的AAA客户端

1. 转到 **Administration > Network Resources > Network Devices > Add**.系统将显示New Network Device页面。
2. 在此页面上，定义WLC **Name**,管理接口 **IP Address** 和 **Radius Authentications Settings** 喜欢 **Shared Secret**.如果您计划输入AP MAC地址作为终端，请确保使用之前配置的自定义设备配置文件而非默认思科配置文件！



3. 点击 **Submit**.

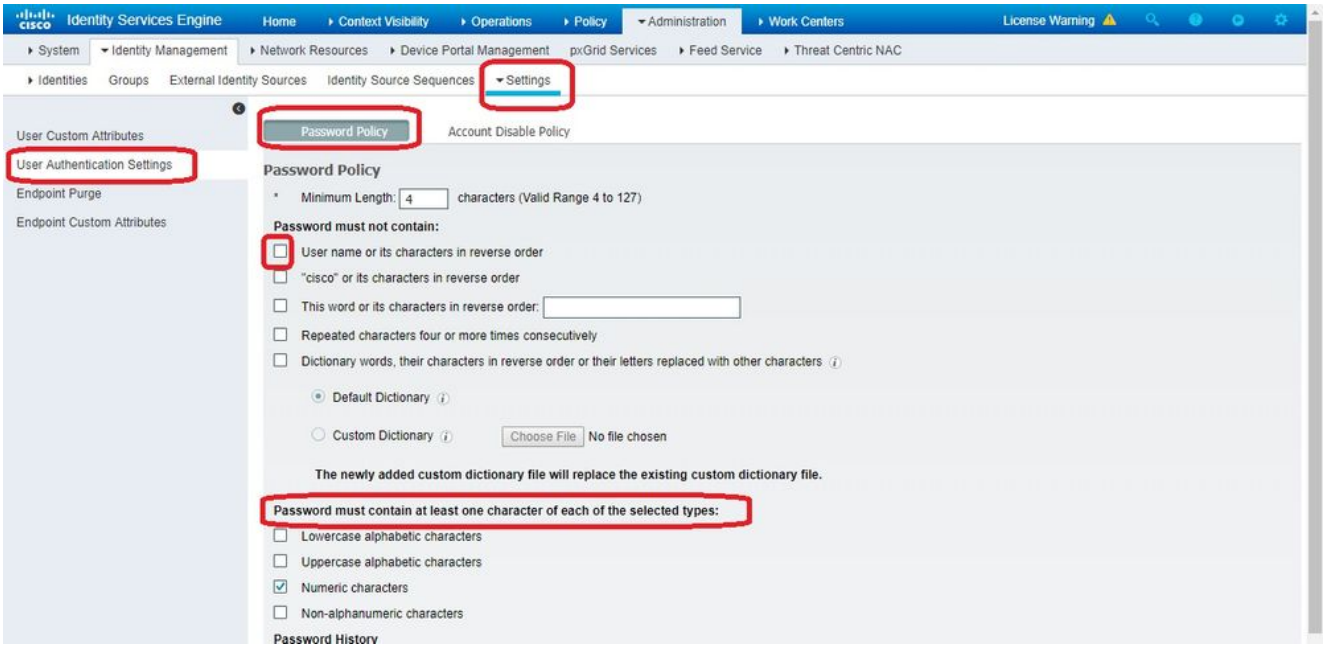
将AP MAC地址添加到思科ISE上的终端数据库

导航至 **Administration > Identity Management > Identities** 并将MAC地址添加到终端数据库。

将AP MAC地址添加到思科ISE上的用户数据库（可选）

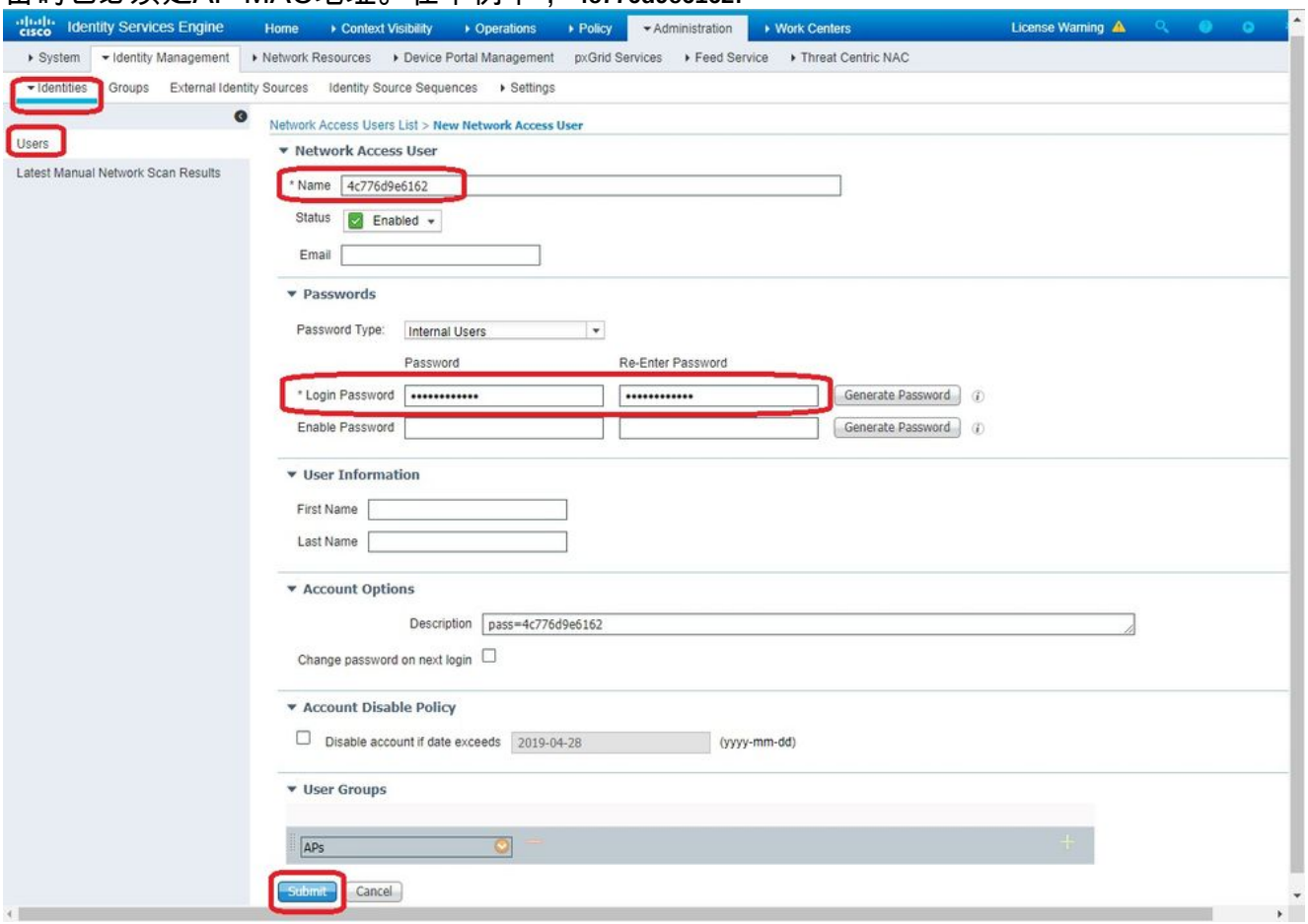
如果您不想修改有线MAB配置文件并选择将AP MAC地址作为用户放置，则必须降低密码策略要求。

1. 导航至 **Administration > Identity Management**.此处我们需要确保密码策略允许使用用户名作为密码，并且策略也必须允许使用mac地址字符，而不需要不同类型的字符。导航至 **Settings > User Authentication Settings > Password Policy**：



2. 然后导航至 **Identities > Users** 并点击 **Add**.显示User Setup页面时，请按照所示定义此AP的用户名和密码。

提示：请使用 **Description** 字段输入密码，以便稍后轻松了解密码的定义。
密码也必须是AP MAC地址。在本例中， **4c776d9e6162**.

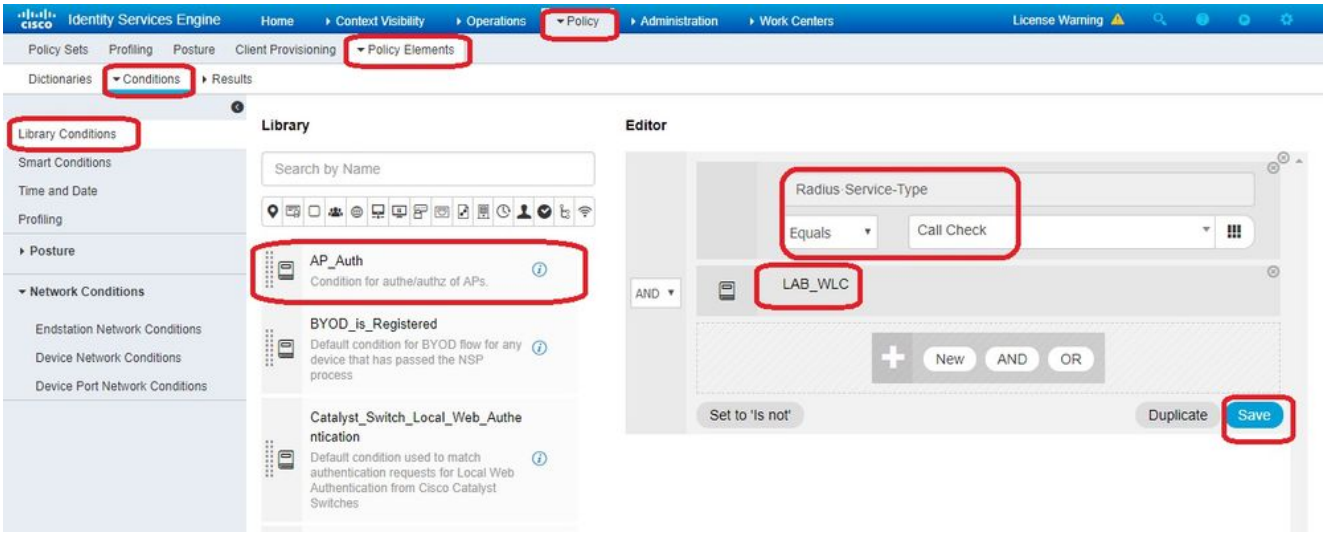


3. 点击 **Submit**.

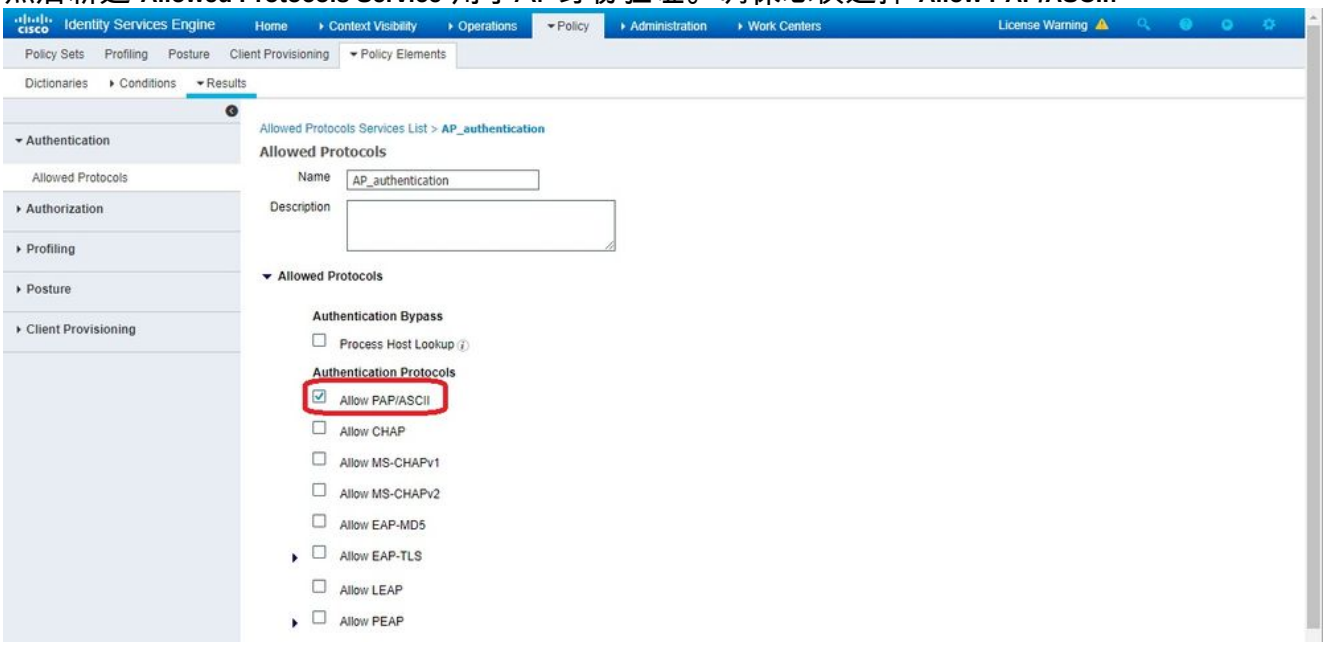
定义策略集

1. 您需要定义 **Policy Set** 匹配来自WLC的身份验证请求。首先，通过导航到 **Policy > Policy Elements > Conditions**，并创建一个与WLC位置匹配的新条件，在本例中

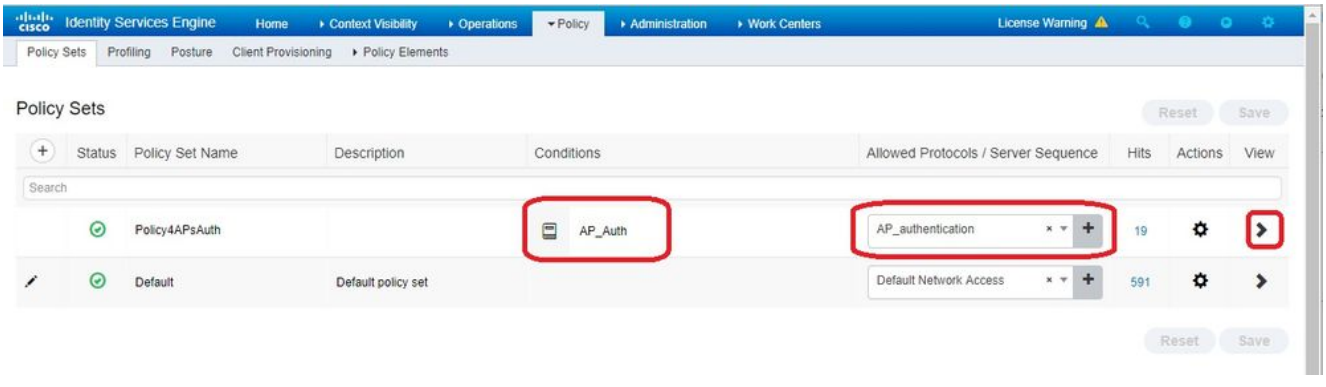
，“LAB_WLC”和 **Radius:Service-Type Equals Call Check** 用于Mac身份验证。此处的条件名为“AP_Auth”。

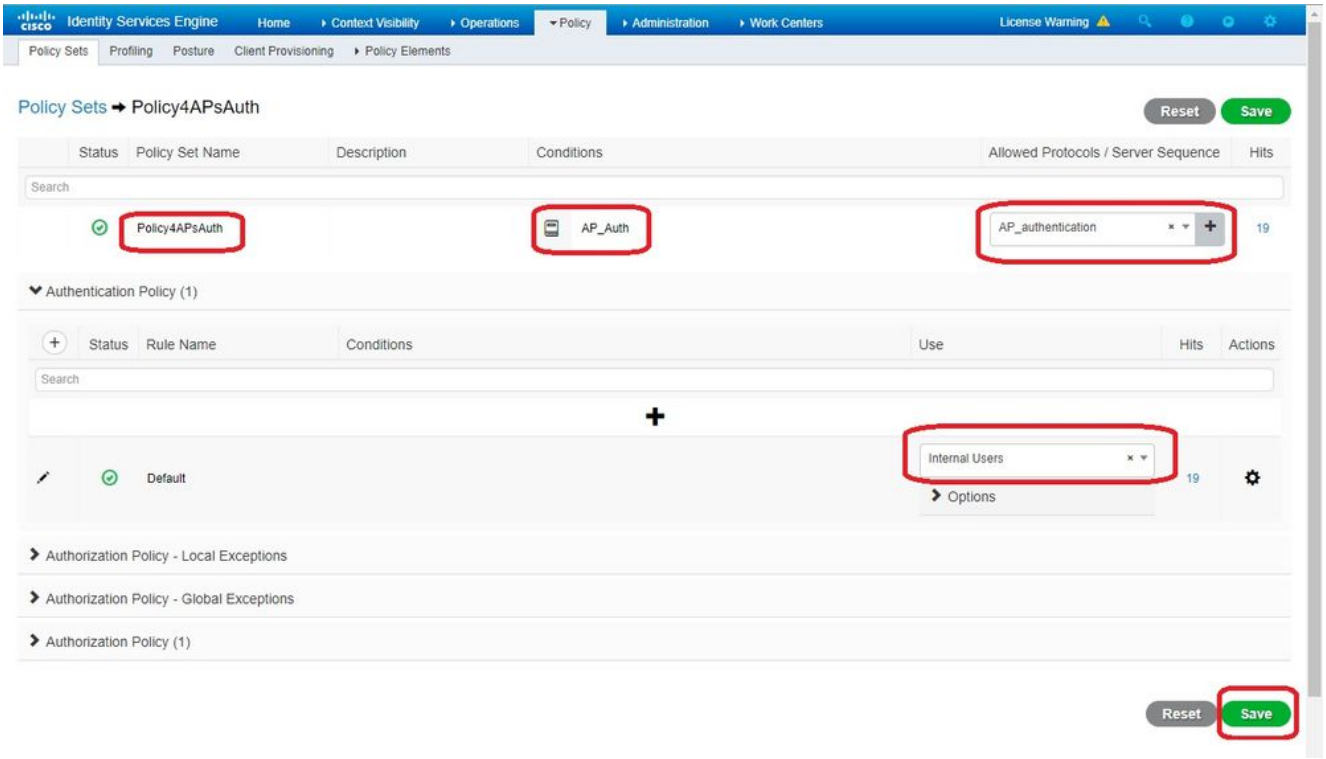


2. 点击 **Save**.
3. 然后新建 **Allowed Protocols Service** 用于AP身份验证。确保您仅选择 **Allow PAP/ASCII**:



4. 在 **Allowed Protocols/Server Sequence**.展开 **View** 和 **Authentication Policy > Use > Internal Users** 以便ISE在内部数据库中搜索AP的用户名/密码。





5. 点击 **Save**.

验证

要验证此配置，您需要将MAC地址为4c:77:6d:9e:61:62的AP连接到网络和监视器。请使用 **debug capwap events/errors enable** 和 **debug aaa all enable** 命令。

从调试中可以看到，WLC将AP MAC地址传递给RADIUS服务器10.48.39.128，并且服务器已成功对AP进行身份验证。然后，AP向控制器注册。

注意：由于空间限制，输出中的某些行已移至第二行。

```
*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 00 01 04 06
9e:61:62........
*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38
.0G...no..TF.a*8
*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a
ZW"[A..a.l......
*aaaQueueReader: Feb 27 14:58:07.566: 00000080: 15 f9 ..
*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.**
*radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9)
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 *** Counted VSA 150994944 AVP of length 28, code 1 atrlen 22)
*radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9)
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22

*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk
*radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes
*radiusTransportThread: Feb 27 14:58:07.588: **70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128** (qid:0) with port:1812, pktId:185
*radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Feb 27 14:58:07.588: structureSize.............................432

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

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

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

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

*radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.................................ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3drcFsHuYpChs (65 bytes)

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

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

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

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

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

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

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

故障排除

使用以下命令排除配置故障：

- debug capwap events enable — 配置LWAPP事件的调试
- debug capwap packet enable — 配置LWAPP数据包跟踪的调试
- debug capwap errors enable — 配置LWAPP数据包错误的调试
- debug aaa all enable — 配置所有AAA消息的调试

如果RADIUS实时中的ISE报告在您对ISE授权AP时用户名“INVALID”，这意味着身份验证正在根据终端数据库进行验证，并且您未修改有线MAB配置文件，如本文档所述。如果MAC地址身份验证与有线/无线MAB配置文件不匹配，ISE会认为该身份验证无效，默认情况下，WLC不会发送NAS端口类型属性。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。