تكوين تفويض نقطة الوصول في شبكة لاسلكية موحدة

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل WLC أن يخول الـ منفذ نقطة (ap) يؤسس على الـ MAC عنوان من الـ APs.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بكيفية تكوين محرك خدمات تعريف Cisco (ISE)
- معرفة تكوين نقاط الوصول من Cisco و Cisco WLCs
- معرفة حلول الأمان اللاسلكية الموحدة من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جمارب WLCs يتلا ليغشت ماظن ليغشتلا AireOS 8.8.111.0طاقن لوصولا نم ةجوملا 1: لا رادصإلاب يهتني AireOS معد نكلو نيموعدم 1600/2600/3600) 3500 و 1700/2700/3700 لازي 8.5.x(طاقن لوصولا نم ةجوملا 2: 1800/2800/3800/4800 و 1540 و 1560 ISE رادصإلا 2.3.0.298

مت إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تخويل نقطة الوصول في الوضع Lightweight

أثناء عملية تسجيل نقطة الوصول، تتم مصادقة نقاط الوصول (AP) و WLCs بشكل متبادل باستخدام شهادات X.509. يتم نسخ شهادات X.509 في ذاكرة فلاش محمية على كل من AP و WLC في المصنع من قبل Cisco.

على نقاط الوصول، تسمى الشهادات التي يتم تثبيتها في المصنع شهادات مثبتة على التصنيع (MIC). تحتوي جميع نقاط الوصول من Cisco التي تم تصنيعها بعد 18 يوليو 2005 على ميكروفونات.

بالإضافة إلى هذه المصادقة المتبادلة التي تحدث أثناء عملية التسجيل، يمكن أن تقيد وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs) أيضا نقاط الوصول التي تسجل معها استنادا إلى عنوان MAC لنقطة الوصول.

ال يعد عدم وجود كلمة مرور قوية مع إستخدام عنوان MAC لنقطة الوصول مشكلة لأن وحدة التحكم تستخدم ميكروفون لمصادقة نقطة الوصول قبل تخويل نقطة الوصول من خلال خادم RADIUS. يوفر إستخدام الميكروفون مصادقة قوية.

يمكن تنفيذ تفويض نقطة الوصول بطريقتين:

- إستخدام قائمة التخويل الداخلي على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)
- إستخدام قاعدة بيانات عناوين MAC على خادم AAA

تختلف سلوكيات نقاط الوصول (AP) بناء على الشهادة المستخدمة:

- APs مع SSCs- يستخدم WLC قائمة التخويل الداخلي فقط ولا يرسل طلبا إلى خادم RADIUS لنقاط الوصول هذه
- APs مع MICs—WLC يستطيع استعمال إما قائمة التخويل الداخلي يشكل على ال WLC أو استعمال RADIUS لدان أن يخول ال APs

يناقش هذا المستند تفويض نقطة الوصول باستخدام كل من قائمة التخويل الداخلي وخادم AAA.

التكوين

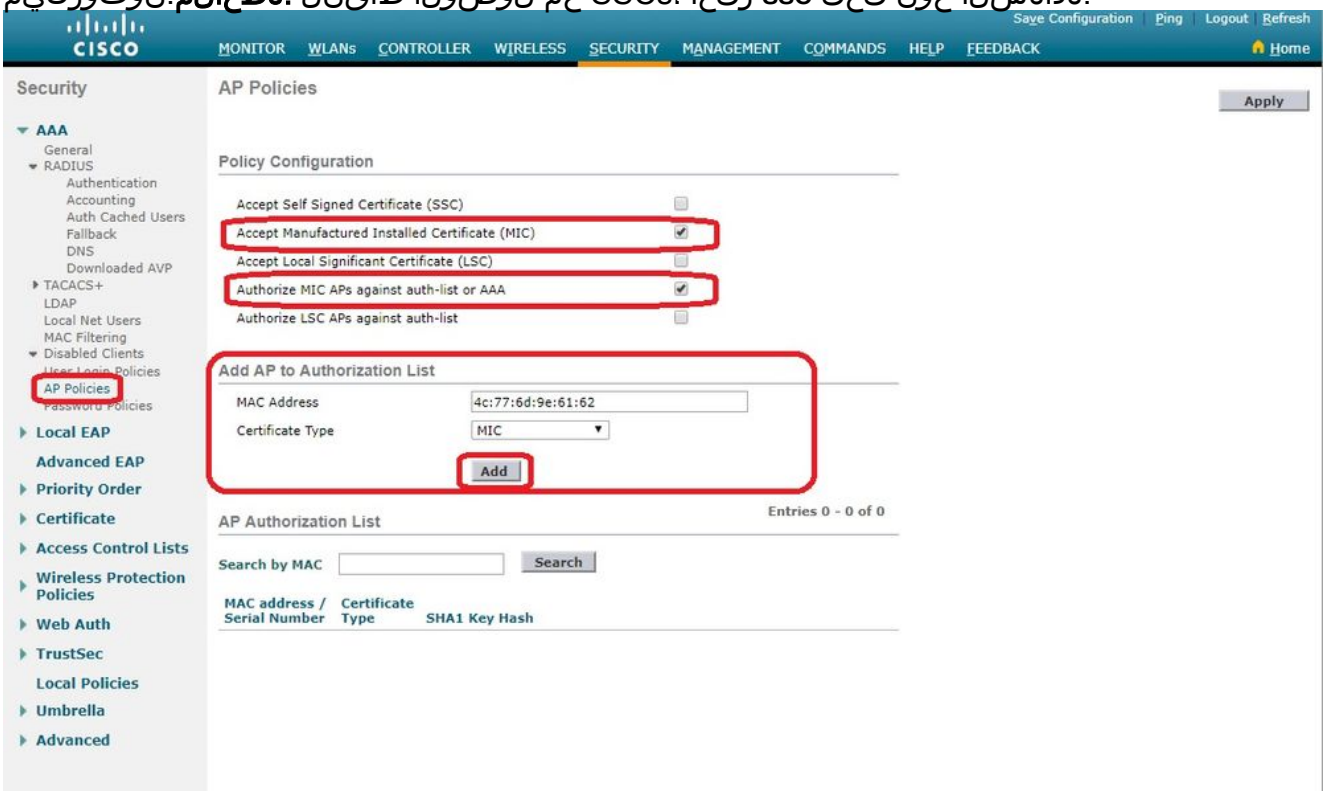
التكوين باستخدام قائمة التخويل الداخلية على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، أستخدم قائمة تخويل نقطة الوصول لتقييد نقاط الوصول استنادا إلى عنوان MAC الخاص بها. قائمة تخويل نقاط الوصول متوفرة تحت **Security > AP Policies** في واجهة المستخدم الرسومية (GUI) الخاصة بلجنة الاتصال اللاسلكية (WLC).

يوضح هذا المثال كيفية إضافة نقطة الوصول باستخدام عنوان MAC **4c:77:6d:9e:61:62**.

1. من واجهة المستخدم الرسومية (GUI) لوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **Security > AP Policies** لظهور صفحة سياسات نقطة الوصول (AP).
2. انقر فوق **Add** زر في الجانب الأيمن من الشاشة.

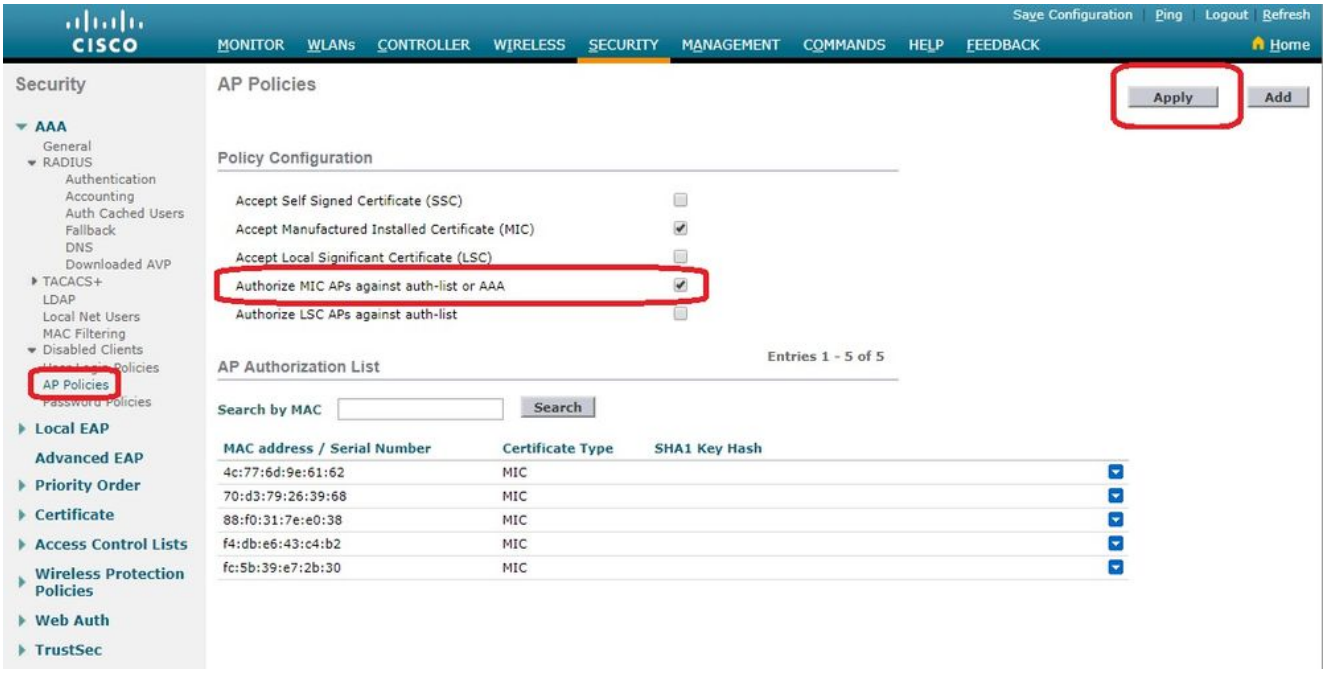
3. تحت **Add AP to Authorization List**، أدخل **AP MAC** العنوان (ليس عنوان MAC لراديو AP). ثم أختر نوع الشهادة وانقر **Add**.في هذا المثال، تتم إضافة نقطة وصول مزودة بشهادة ميكروفون.**ملاحظة:** لنقاط الوصول مع SSCs، أختر **ssc** تحت نوع الشهادة.



تتم إضافة نقطة الوصول إلى قائمة تخويل نقطة الوصول ويتم إدراجها ضمن **AP Authorization List**.

4. ضمن "تكوين النهج"، حدد المربع ل **Authorize MIC APs against auth-list or AAA**.عند تحديد هذه المعلمة، يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من قائمة

التخويل المحلية أولا. إذا لم يكن AP MAC موجودا، فإنه يتحقق من خادم RADIUS.



التحقق من الصحة

in order to دقق ات هذ ا تشكيل، أنت تحتاج أن يربط ال ap مع {upper}mac address **4c:77:6d:9e:61:62** إلى الشبكة والشاشة. أستخدم **debug capwap events/errors enable** و **debug aaa all enable** أوامر لتنفيذ هذا الإجراء.

يبدي هذا إنتاج ال debugs عندما ال ap {upper}mac address غير موجود في ال ap تخويل قائمة:

ملاحظة: تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة.

```
(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
```

يبدي اذه إنتاج ال debugs عندما ال{upper}mac address يكون أضفت إلى ال ap تخويل قائمة:

ملاحظة: تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة.

```
(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
```

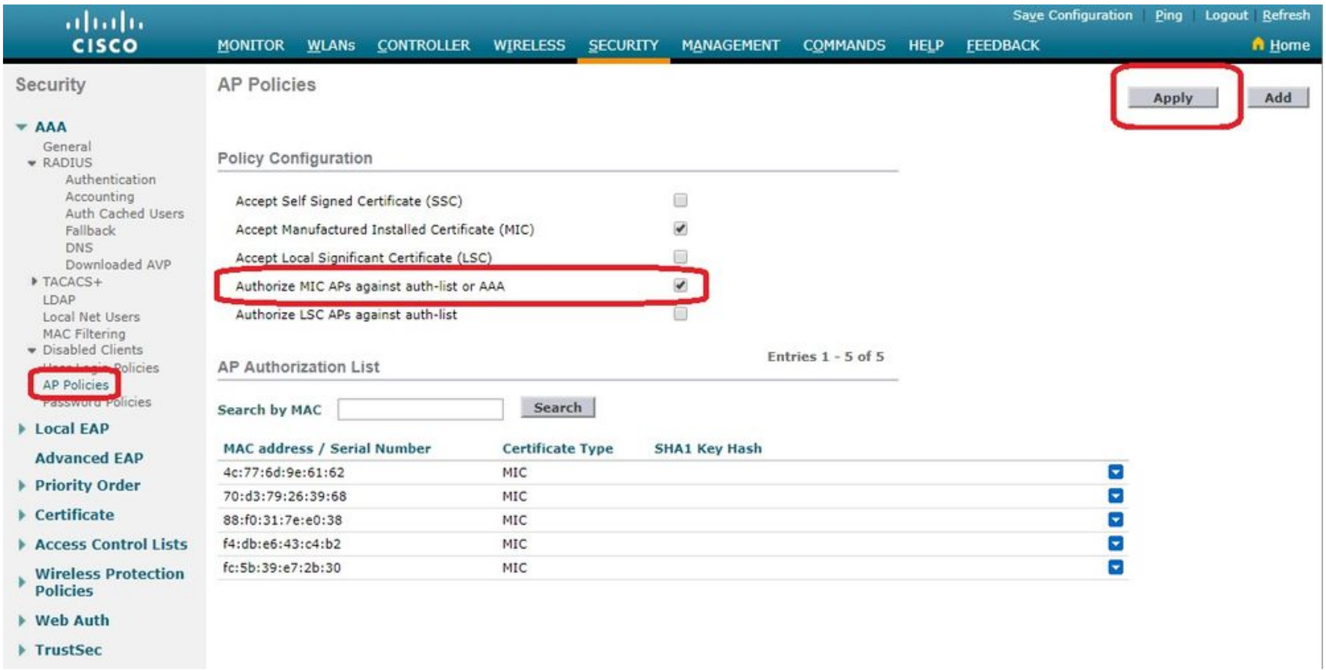
تفويض نقطة الوصول مقابل خادم AAA

أنت يستطيع أيضا شكلت WLCs أن يستعمل RADIUS لدان أن يخول APs يستعمل MICs. يستخدم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عنوان MAC لنقطة الوصول كاسم المستخدم وكلمة المرور عند إرسال المعلومات إلى خادم RADIUS. على سبيل

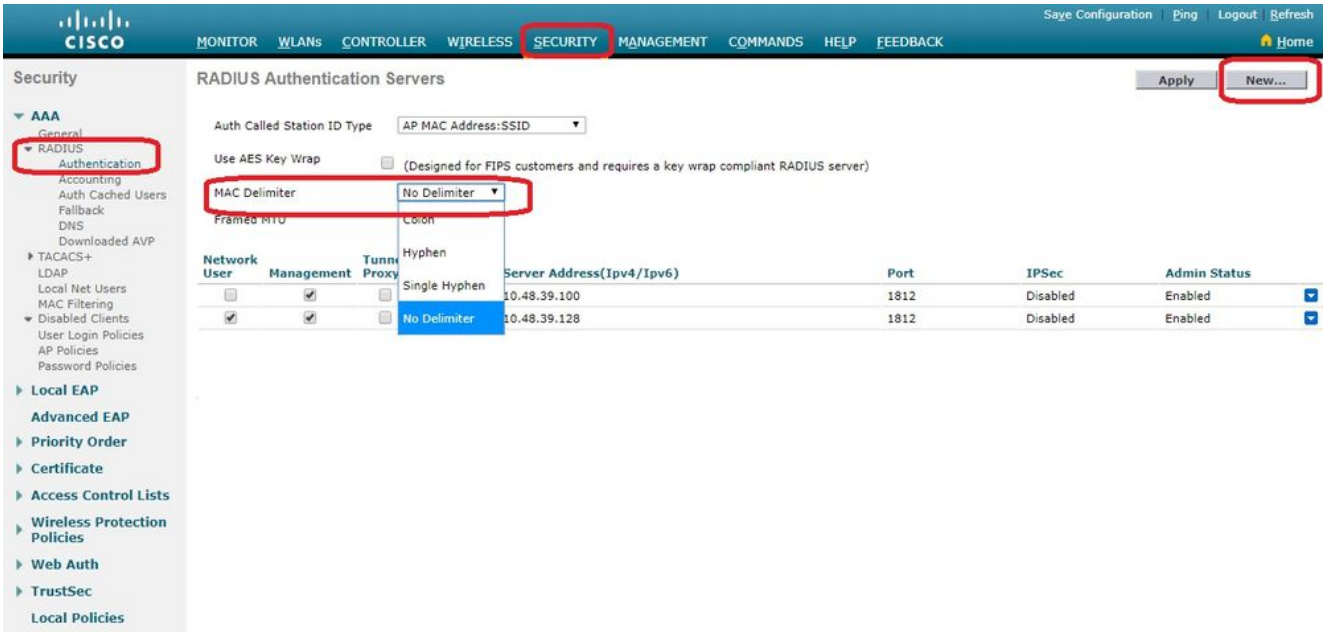
المثال، إذا كان عنوان MAC لنقطة الوصول هو **4c:77:6d:9e:61:62**، كل من ال username وكلمة يستعمل ب الجهاز تحكم أن يخول ال ap أن ماك عنوان يستعمل ال يعين.

يبدي هذا مثال كيف أن يشكل WLCs أن يخول APs يستعمل ال cisco ISE.

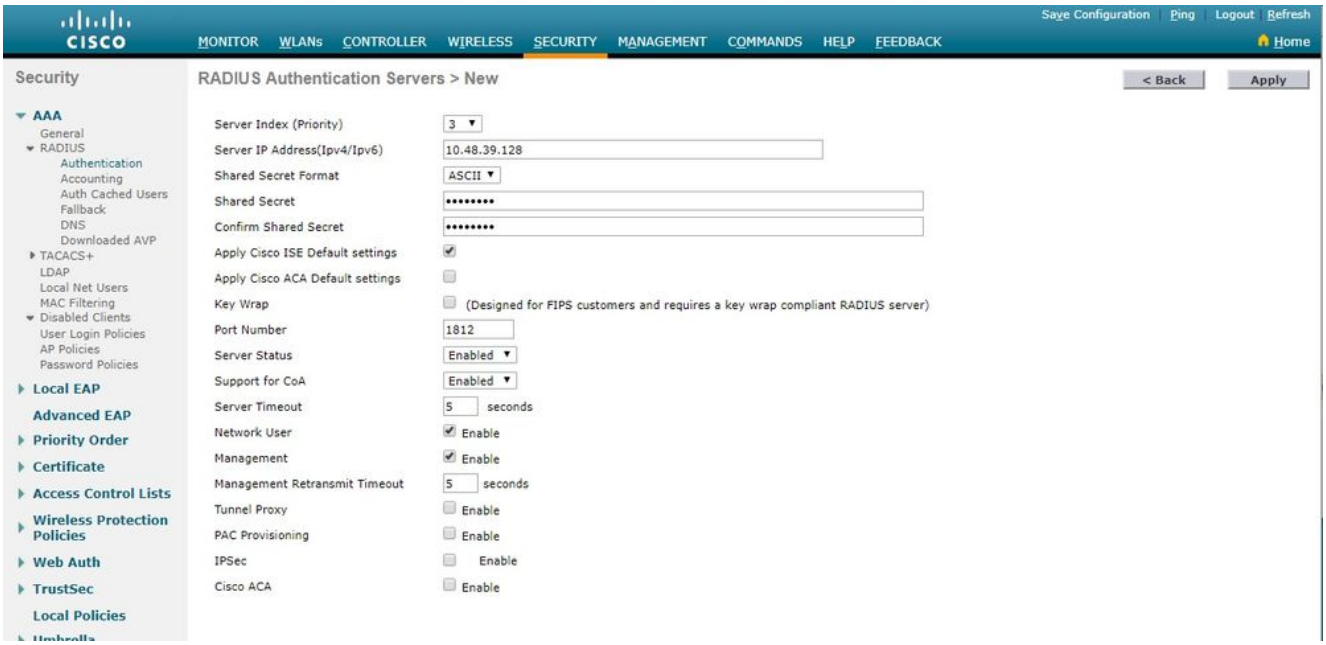
1. من واجهة المستخدم الرسومية (GUI) لوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **Security > AP Policies**. سوف تظهر صفحة سياسات نقطة الوصول.
2. ضمن "تكوين النهج"، حدد المربع ل **Authorize MIC APs against auth-list or AAA**.عندما تختار هذه المعلمة، يتحقق WLC أولا من قائمة التخويل المحلية. إذا لم يكن AP MAC موجودا، فإنه يتحقق من خادم RADIUS.



3. انتقل إلى **Security > RADIUS Authentication** من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم لعرض **RADIUS Authentication Servers** صفحة. في هذه الصفحة يمكنك تعريف **محدد MAC**. يحصل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) على عنوان MAC لنقطة الوصول ويرسلها إلى خادم Radius باستخدام المحدد المحدد هنا. هذا مهم حتى أن اسم المستخدم يطابق ما تم تكوينه في خادم Radius. في هذا المثال **No Delimiter** مستخدم so that username يكون **4c776d9e6162**.



4. ثم انقر **New** لتحديد خادم RADIUS.



5. تحديد معلمات خادم RADIUS على **RADIUS Authentication Servers > New** صفحة. هذه المعلمات تتضمن نصف القطر **Server IP Address**، **Shared Secret**، **Port Number**،و **Server Status**. عند الانتهاء، انقر فوق **Apply**. يستخدم هذا المثال Cisco ISE كخادم RADIUS مع عنوان IP 10.48.39.128.

قم بتكوين Cisco ISE لتخويل APs

in order to مكنت ال cisco ISE أن يخول APs، أنت تحتاج أن يتم هذا steps:

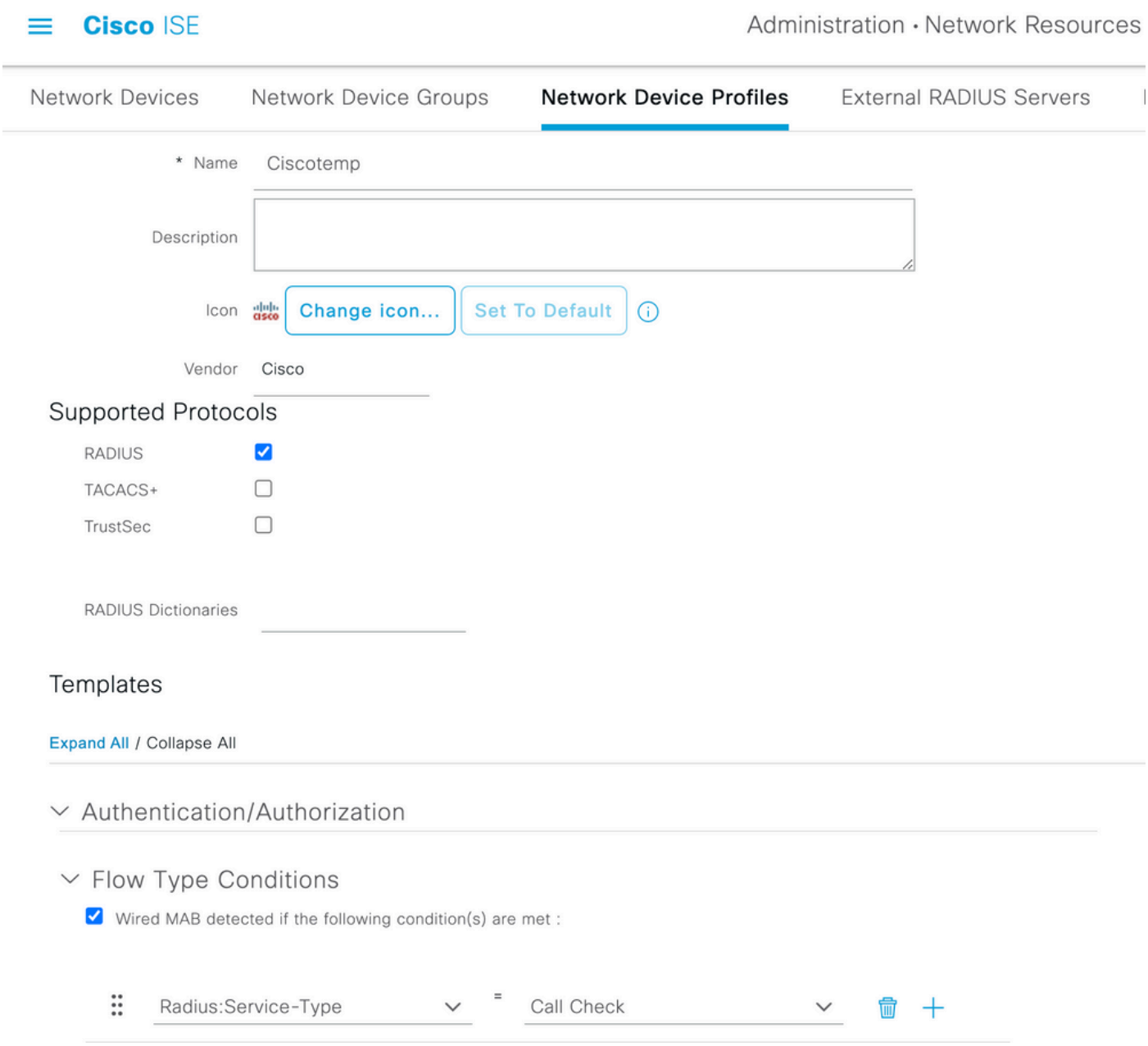
1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على Cisco ISE.
2. إضافة عناوين MAC لنقطة الوصول إلى قاعدة البيانات على Cisco ISE.

مهم، أنت يستطيع كنت أضفت ال ap {upper}mac address كنقاط نهاية (أفضل طريقة) أو كمستعمل (كلمة السر الخاصة بهم هي عنوان MAC أيضا) غير أن هذا يتطلب أنت أن يقلل الكلمة أمن سياسة متطلب.

نظرا لحقيقة أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ال يرسل سمة NAS-Port-Type التي تعد مطلبا على ISE لمطابقة سير عمل مصادقة عنوان MAC (MAB)، يلزمك تغيير هذا الإجراء.

تكوين ملف تعريف جهاز جديد حيث ال يتطلب MAB سمة نوع منفذ NAS

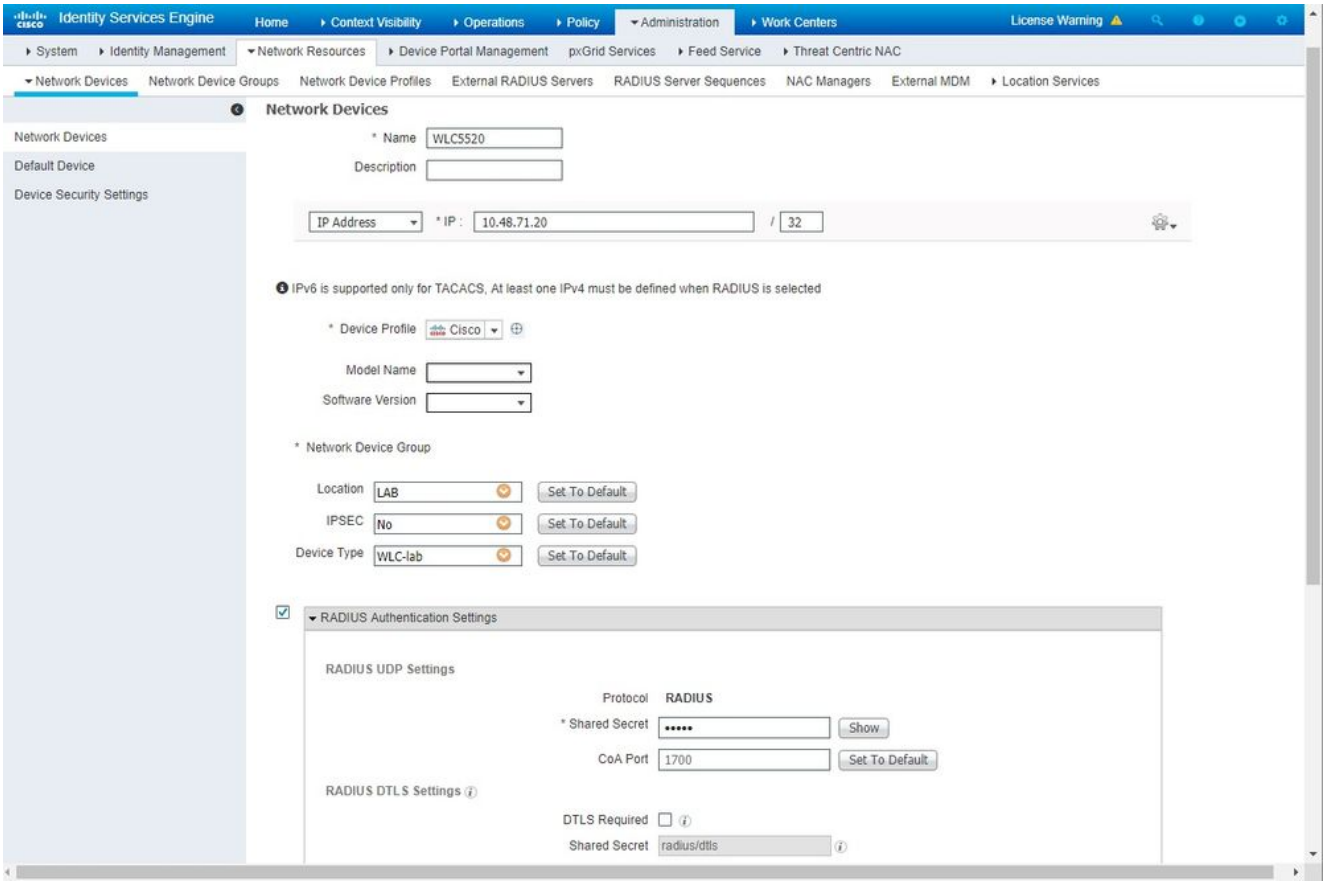
انتقل إلى **Administration > Network device profile** وإنشاء ملف تعريف جهاز جديد. قم بتمكين RADIUS وضبط تدفق MAB السلكي لطلب نوع الخدمة=Call-check كما هو موضح في الصورة. يمكنك نسخ إعدادات أخرى من ملف تعريف Cisco الكلاسيكي ولكن الفكرة هي أال تتطلب سمة 'nas-port-type' لسير عمل MAB سلكي.



تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على Cisco ISE

1. الانتقال إلى **Administration > Network Resources > Network Devices > Add**. تظهر صفحة جهاز الشبكة الجديدة.
2. في هذه الصفحة، قم بتعريف عنصر التحكم في الشبكة المحلية اللاسلكية

(WLC) **Name**,واجهة الإدارة **IP Address** و **Radius Authentications Settings** مثل **Shared Secret**. إذا كنت تخطط عند إدخال عناوين AP MAC كنقاط نهاية، فتأكد من إستخدام ملف تعريف الجهاز المخصص الذي تم تكوينه سابقا بدلا من ملف تعريف Cisco الافتراضي!



3. طقطقة **Submit**.

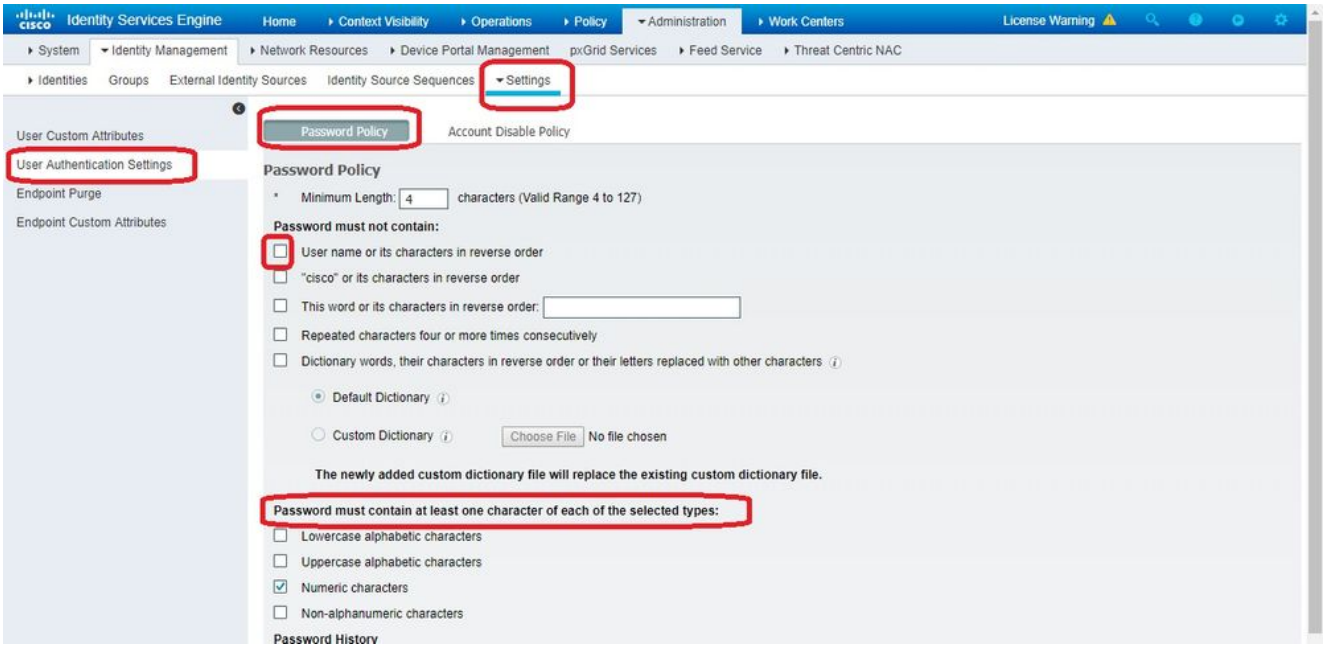
إضافة عنوان AP MAC إلى قاعدة بيانات نقطة النهاية على Cisco ISE

انتقل إلى **Administration > Identity Management > Identities** وإضافة عناوين MAC إلى قاعدة بيانات نقطة النهاية.

أضفت ال ap {upper}mac address إلى المستعمل قاعدة معطيات على ال cisco ISE (إختياري)

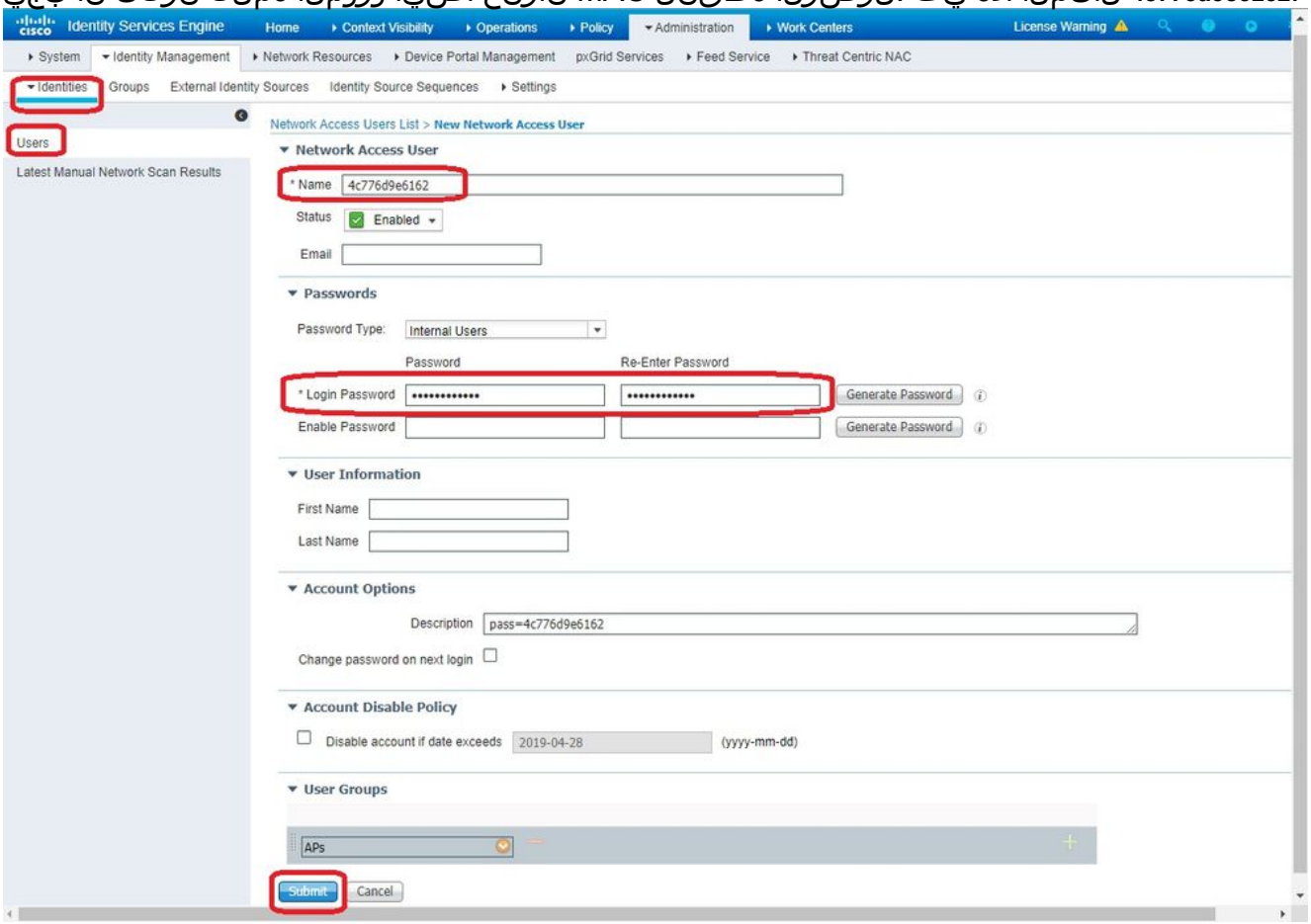
إن ال يريد أنت أن يعدل ال MAB السلكي واخترت أن يضع ال ap {upper}mac address كمستخدم، أنت يضطر أن يخفض الكلمة سياسة متطلب.

1. انتقل إلى **Administration > Identity Management**. هنا نحن بحاجة إلى التأكد من أن نهج كلمة المرور يسمح باستخدام اسم المستخدم كلمة مرور ويجب أن يسمح النهج أيضا باستخدام أحرف عنوان MAC لتبييض الحاجة إلى أنواع مختلفة من الأحرف. انتقل إلى **Settings > User Authentication Settings > Password Policy**:



2. ثم انتقل إلى **Identities > Users** وانقر فوق **Add**. عندما تظهر صفحة إعداد المستخدم، قم بتعريف اسم المستخدم وكلمة المرور لنقطة الوصول هذه كما هو موضح.

تلميح: أستخدم **Description** يكون الحقل لإدخال كلمة المرور بحيث يسهل لاحقا معرفة ما تم تعريفه ككلمة مرور.
يجب أن تكون كلمة المرور أيضا عنوان MAC لنقطة الوصول. في هذا المثال **4c776d9e6162**.

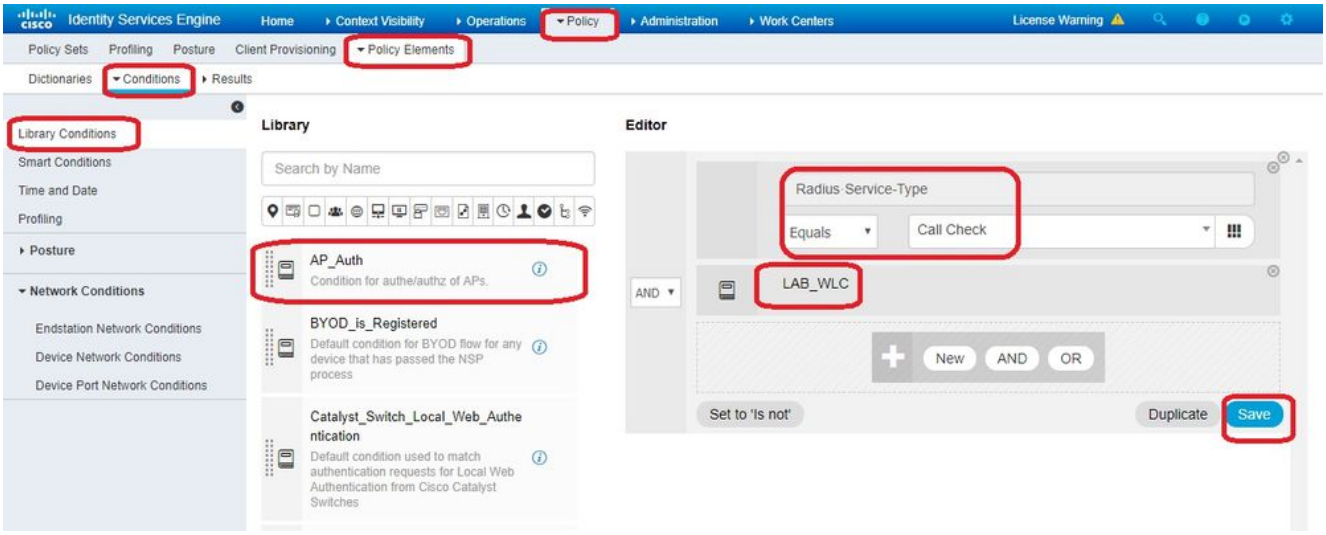


3. طقطقة **Submit**.

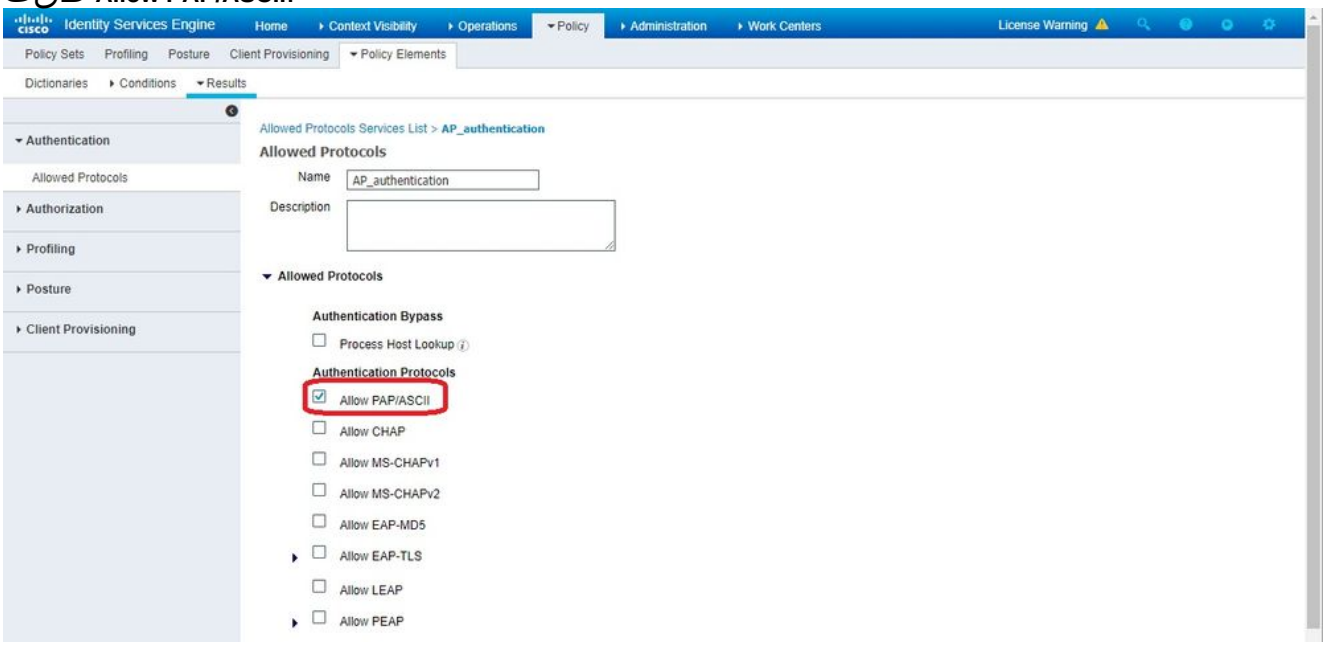
تحديد مجموعة نهج

1. تحتاج إلى تعريف **Policy Set** لمطابقة طلب المصادقة الوارد من عنصر التحكم في

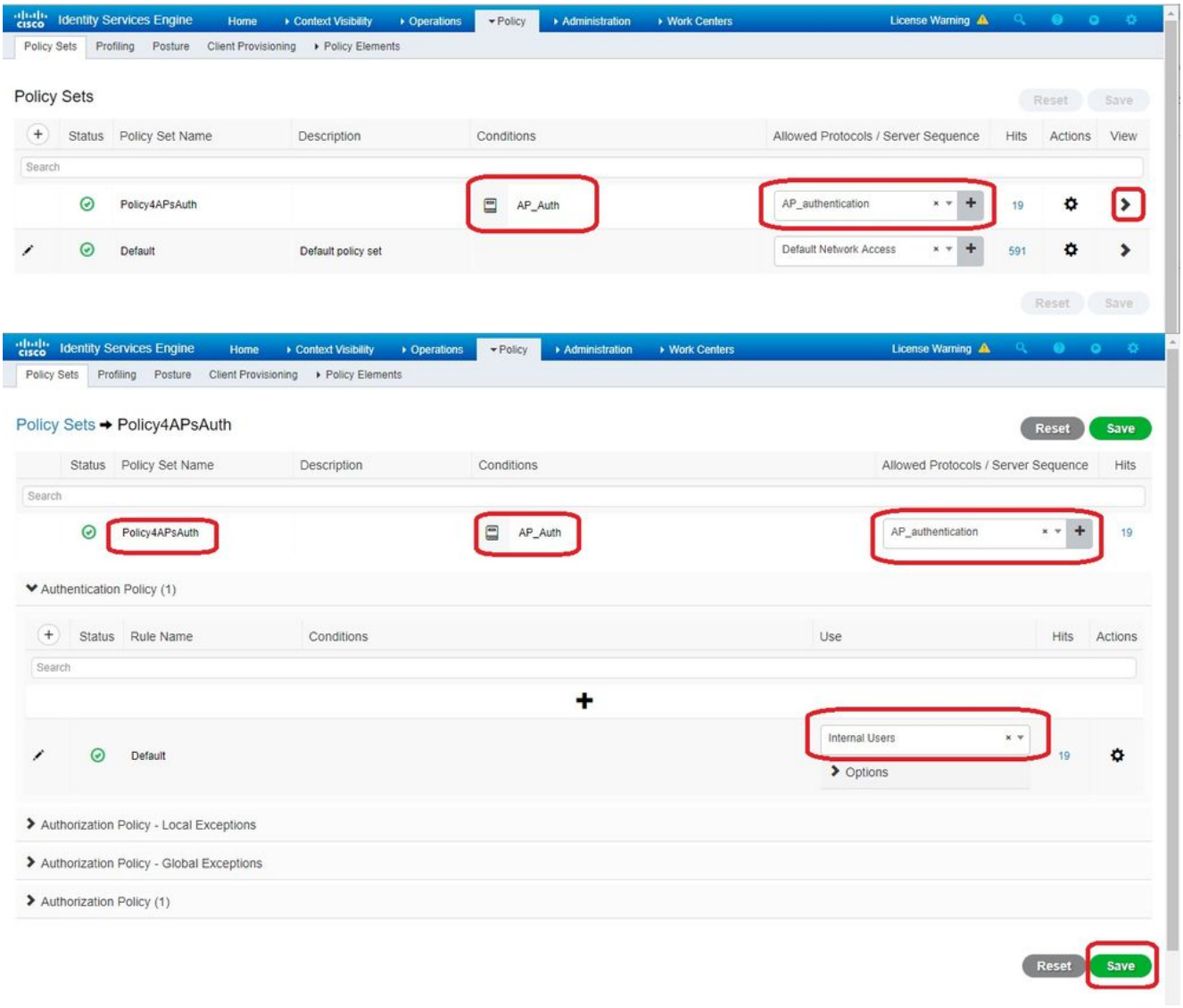
الشبكة المحلية اللاسلكية (WLC). أو الوقوم بإنشاء شرط بالانتقال إلى **Policy > Policy Elements > Conditions**، وإنشاء شرط جديد لمطابقة موقع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، في هذا المثال، 'LAB_WLC' و **Radius:Service-Type Equals Call Check** والذي يستخدم لمصادقة Mac. هنا يسمى الشرط 'AP_AUTH'.



2. طقطقة **Save**.
3. ثم قم بإنشاء جديد **Allowed Protocols Service** للحصول على مصادقة AP. تأكد من إختيارك فقط **Allow PAP/ASCII**:



4. أختر الخدمة التي تم إنشاؤها مسبقا في **Allowed Protocols/Server Sequence**.
تحت **Authentication Policy > Use > Internal Users** لذلك فإن ISE يبحث ال DB داخلي ل وتوسيع **View** ال username/كلمة من ال ap.



5. طقطقة **Save**.

التحقق من الصحة

in order to دقق ت اذه تشكيل، يجتاج أنت أن يربط ال ap مع {upper}mac address 4c:77:6d:9e:61:62 إلى الشبكة والشاشة.
أستخدم **debug capwap events/errors enable** و **debug aaa all enable** أمر in order to أنجزت اذه.

كما هو موضح من تصحيح الأخطاء، ال WLC مررت على ال ap {upper}mac address إلى ال RADIUS نادل 10.48.39.128، والخادم نجح في مصادقة ال AP. ثم يتم تسجيل نقطة الوصول مع وحدة التحكم.

ملاحظة: تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة.

```
*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
```

استكشاف الأخطاء وإصلاحها

أستخدم هذه الأوامر لاستكشاف أخطاء التكوين وإصلاحها:

- debug capwap events enable—تكوين تصحيح أخطاء أحداث LWAPP
- debug capwap packet enable—تكوين تصحيح أخطاء تتبع حزم LWAPP
- debug capwap errors enable—تكوين تصحيح أخطاء حزمة LWAPP
- debug aaa all enable—تكوين تصحيح أخطاء جميع رسائل AAA

في الحالة، تسجل تقارير ISE في Radius Live اسم المستخدم "غير صالح" في الوقت الذي يكون فيه ديك نقاط وصول مخولة مقابل ISE، وهذا يعني أنه تم التحقق من المصادقة مقابل قاعدة بيانات نقطة النهاية أو أنت لم تقم بتعديل ملف تعريف MAB السلكي كما تم تعريفه في ملف تعريف MAB السلكي/اللاسلكي، والذي يتطلب بشكل افتراضي سمة ون من نفذ NAS التي ال يتم إرسالها بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).