Unified Wireless Networkでのアクセスポイント許可の設定

内容

概要

このドキュメントでは、アクセスポイント(AP)のMACアドレスに基づいてAPを認可するようにWLCを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine(ISE)の設定方法に関する基本的な知識
- Cisco APおよびCisco WLCの設定に関する知識
- Cisco Unified Wireless Security ソリューションについての知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AireOS 8.8.111.0ソフトウェアが稼働するWLCWave1 AP:1700/2700/3700および

3500（1600/2600/3600は引き続きサポートされますが、AireOSのサポートはバージョン8.5.xで終了します）Wave2 AP:1800/2800/3800/4800、1540、および1560 ISEバージョン2.3.0.298

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Lightweight AP認可

APの登録プロセス中、APとWLCはX.509証明書を使用して相互に認証します。X.509証明書は、シスコによって工場でAPとWLCの両方の保護されたフラッシュに書き込まれます。

APでは、工場出荷時にインストールされた証明書は、製造元でインストールされた証明書(MIC)と呼ばれます。 2005年7月18日以降に製造されたすべてのCisco APにはMICがあります。

登録プロセス中に発生するこの相互認証に加えて、WLCはAPのMACアドレスに基づいて、登録するAPを制限することもできます。

APのMACアドレスを使用する強力なパスワードがないと、コントローラはRADIUSサーバ経由でAPを認可する前に、MICを使用してAPを認証するため、問題にはなりません。MICを使用すると、強力な認証が提供されます。

AP認可は、次の2つの方法で実行できます。

- WLCでの内部認証リストの使用
- AAAサーバでのMACアドレスデータベースの使用

APの動作は、使用される証明書によって異なります。

- SSCを使用するAP:WLCは内部認証リストのみを使用し、これらのAPの要求をRADIUSサーバに転送しません
- MICを使用するAP:WLCでは、WLCに設定された内部認証リストを使用するか、RADIUSサーバを使用してAPを認証できます

このドキュメントでは、内部認証リストとAAAサーバの両方を使用したAP認証について説明します。

設定

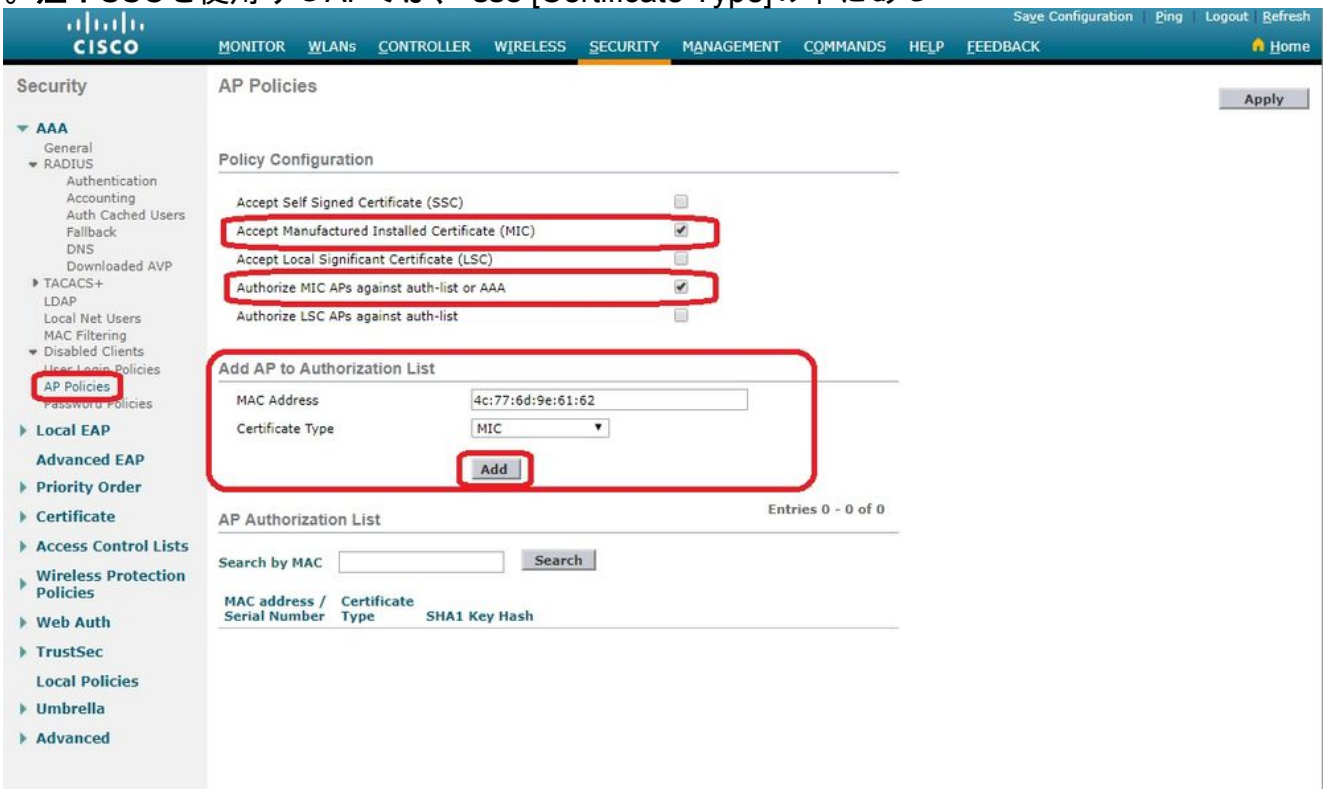
WLCの内部認証リストを使用した設定

WLCで、AP許可リストを使用して、MACアドレスに基づいてAPを制限します。AP認証リストは、 **Security > AP Policies** WLCのGUIで設定します。

次の例は、MACアドレスを持つAPを追加する方法を示しています **4c:77:6d:9e:61:62.**

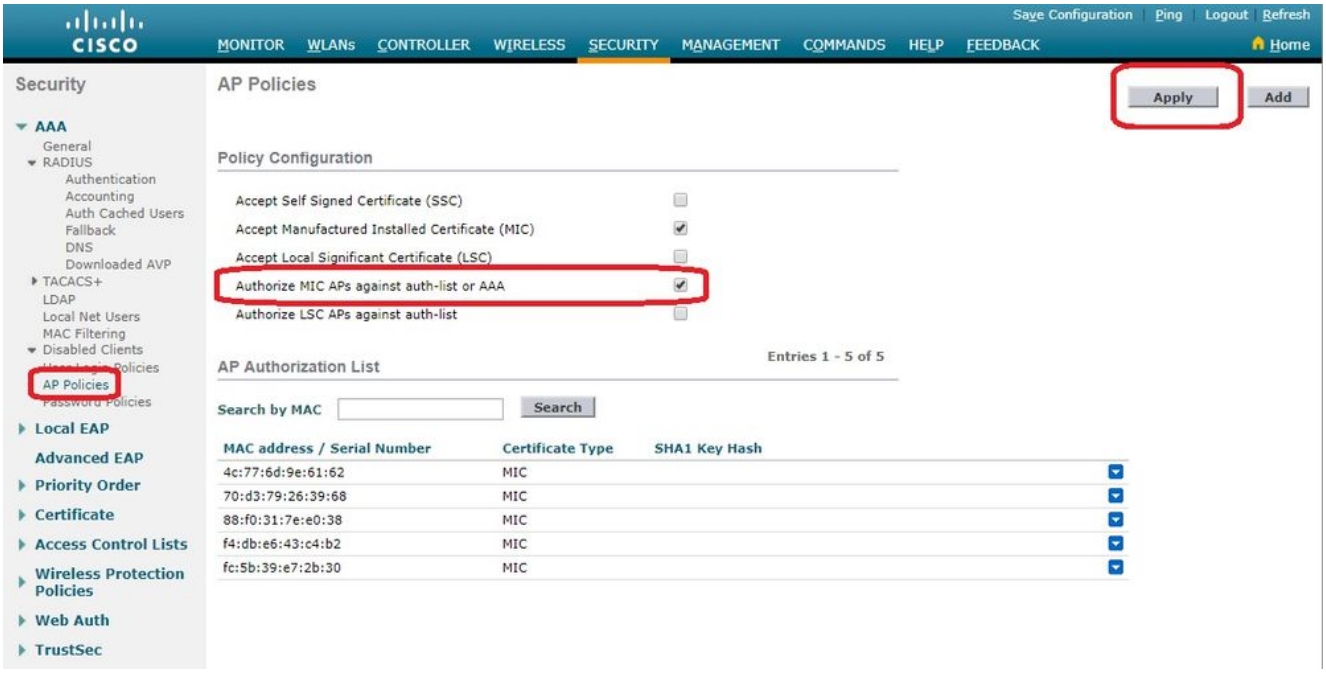
1. WLCコントローラのGUIで、 **Security > AP Policies** [AP Policies]ページが表示されます。
2. ポリシーの横の [レポート（Report）] **Add** ボタンをクリックします。

3. 通常の **Add AP to Authorization List**を入力し、 **AP MAC** アドレス（AP無線MACアドレスではない）。 次に、証明書タイプを選択し、 **Add.**この例では、MIC証明書を持つAPが追加されます。**注：**SSCを使用するAPでは、 **ssc** [Certificate Type]の下にある



APがAP認証リストに追加され、 **AP Authorization List.**

4. [Policy Configuration]で、次のチェックボックスをオンにします。
Authorize MIC APs against auth-list or AAA.このパラメータを選択すると、WLCは最初にローカル認証リストをチェックします。AP MACが存在しない場合は、RADIUSサーバをチェックします。



確認

この設定を確認するには、APをMACアドレスで接続する必要があります **4c:77:6d:9e:61:62** ネットワークとモニタに接続します **debug capwap events/errors enable** と **debug aaa all enable** コマンドを使用します。

次の出力は、APのMACアドレスがAP許可リストにない場合のデバッグを示しています。

> **注**：出力で、スペースの制約上 2 行に分割されている行があります。

```
(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**

次の出力は、LAP MACアドレスがAP認証リストに追加されたときのデバッグを示しています。

注：出力で、スペースの制約上 2 行に分割されている行があります。

(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

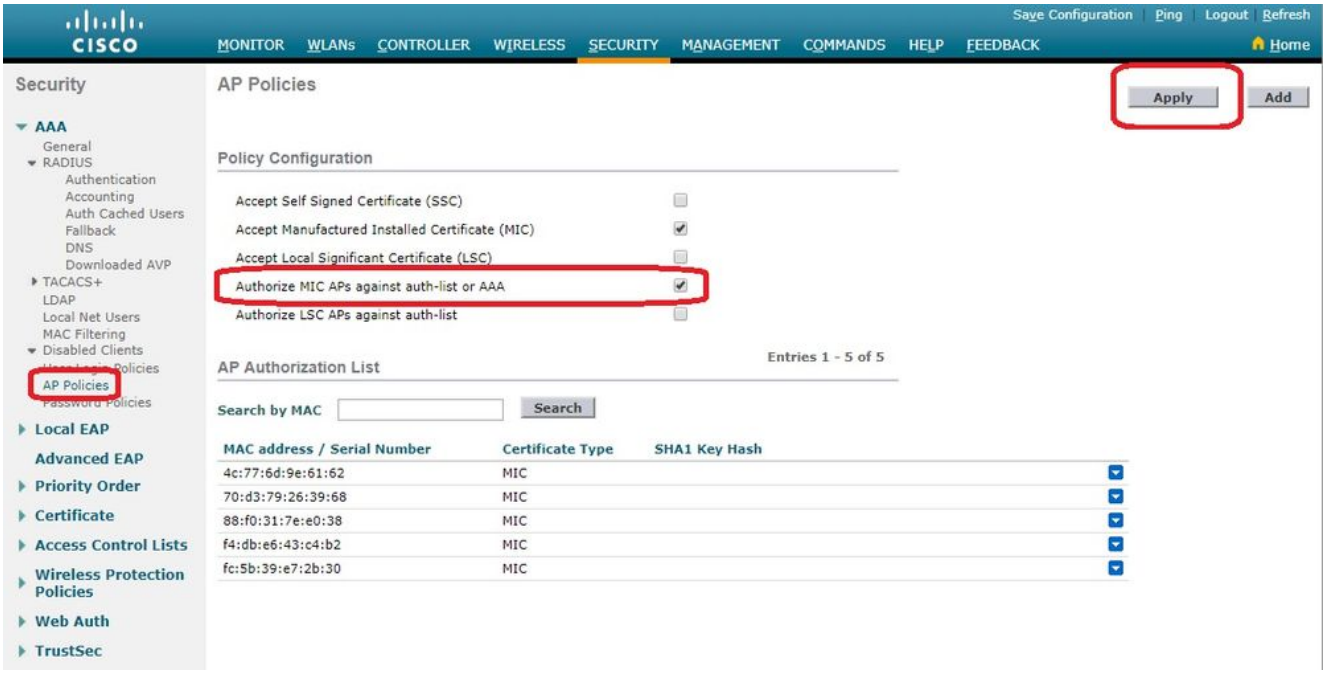
```
not allowed to send in state Capwap_no_state for AP 192.168.79.151

*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
```

AAAサーバに対するAP認証

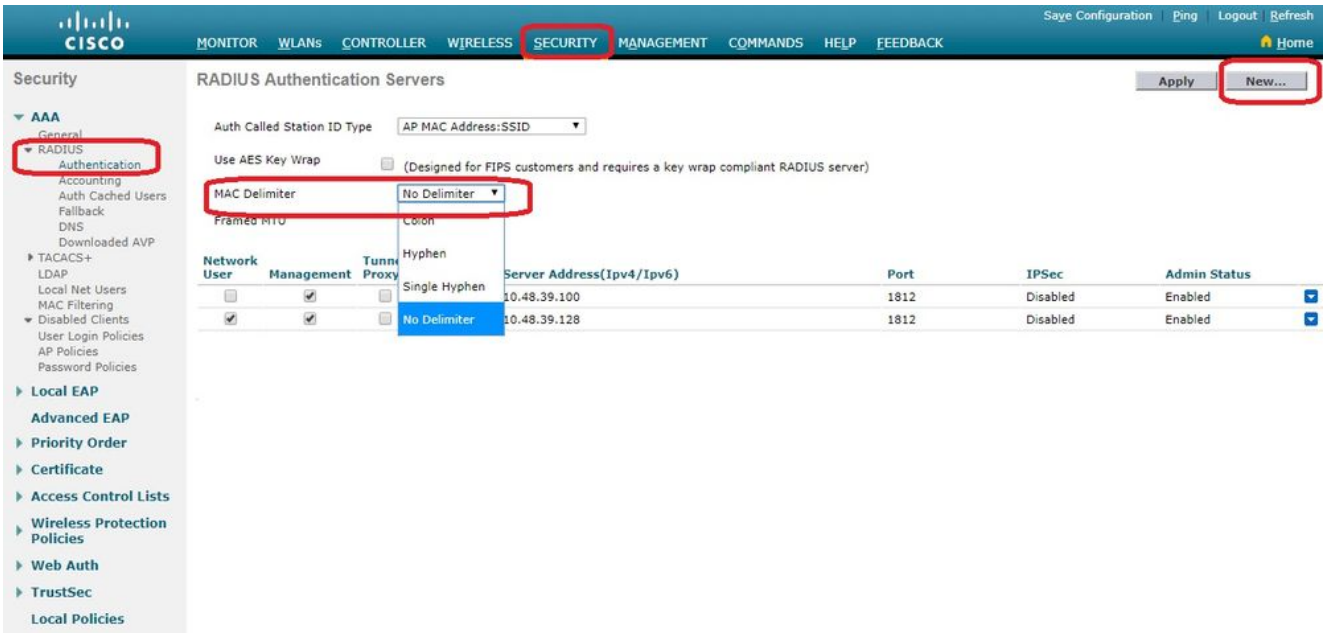
RADIUSサーバを使用してMICを使用してAPを認可するようにWLCを設定することもできます。WLCは、RADIUSサーバに情報を送信するときに、ユーザ名とパスワードの両方としてAP MACアドレスを使用します。たとえば、APのMACアドレスが **4c:77:6d:9e:61:62**に設定されている場合、コントローラがAPを認可するために使用するユーザ名とパスワードの両方が、定義されたデリメータを使用するMACアドレスになります。

この例では、Cisco ISEを使用してAPを認可するようにWLCを設定する方法を示します。

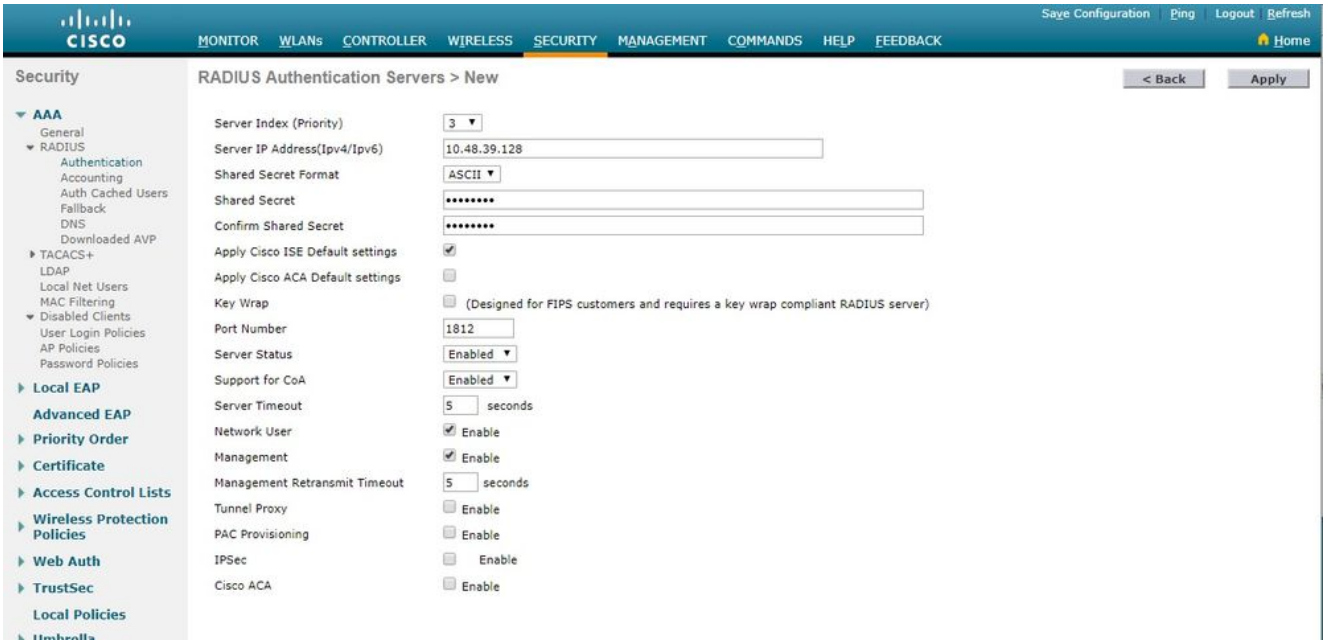
1. WLCコントローラのGUIで、 **Security > AP Policies**.[AP Policies]ページが表示されます。
2. [Policy Configuration]で、次のチェックボックスをオンにします。
   Authorize MIC APs against auth-list or AAA.このパラメータを選択すると、WLCは最初にローカル認証リストをチェックします。AP MACが存在しない場合は、RADIUSサーバをチェックします。



3. 移動先 **Security > RADIUS Authentication** コントローラのGUIから、 **RADIUS Authentication Servers** ページを使用します。このページでは、**MACデリミタ**を定義できます。WLCはAPのMACアドレスを取得し、ここで定義されたデリミタを使用してRADIUSサーバに送信します。これは、ユーザ名がRadiusサーバに設定されているものと一致するように重要です。この例では、**No Delimiter** ユーザ名が **4c776d9e6162**.



4. 次に、 **New** RADIUSサーバを定義します。



5. RADIUSサーバのパラメータを **RADIUS Authentication Servers > New** ページを使用します。これらのパラメータには、RADIUS **Server IP Address**、 **Shared Secret**、 **Port Number**,と **Server Status**.完了したら、 **Apply**.この例では、Cisco ISEをIPアドレス10.48.39.128のRADIUSサーバとして使用しています。

APを認可するためのCisco ISEの設定

Cisco ISEでAPを認可できるようにするには、次の手順を実行する必要があります。

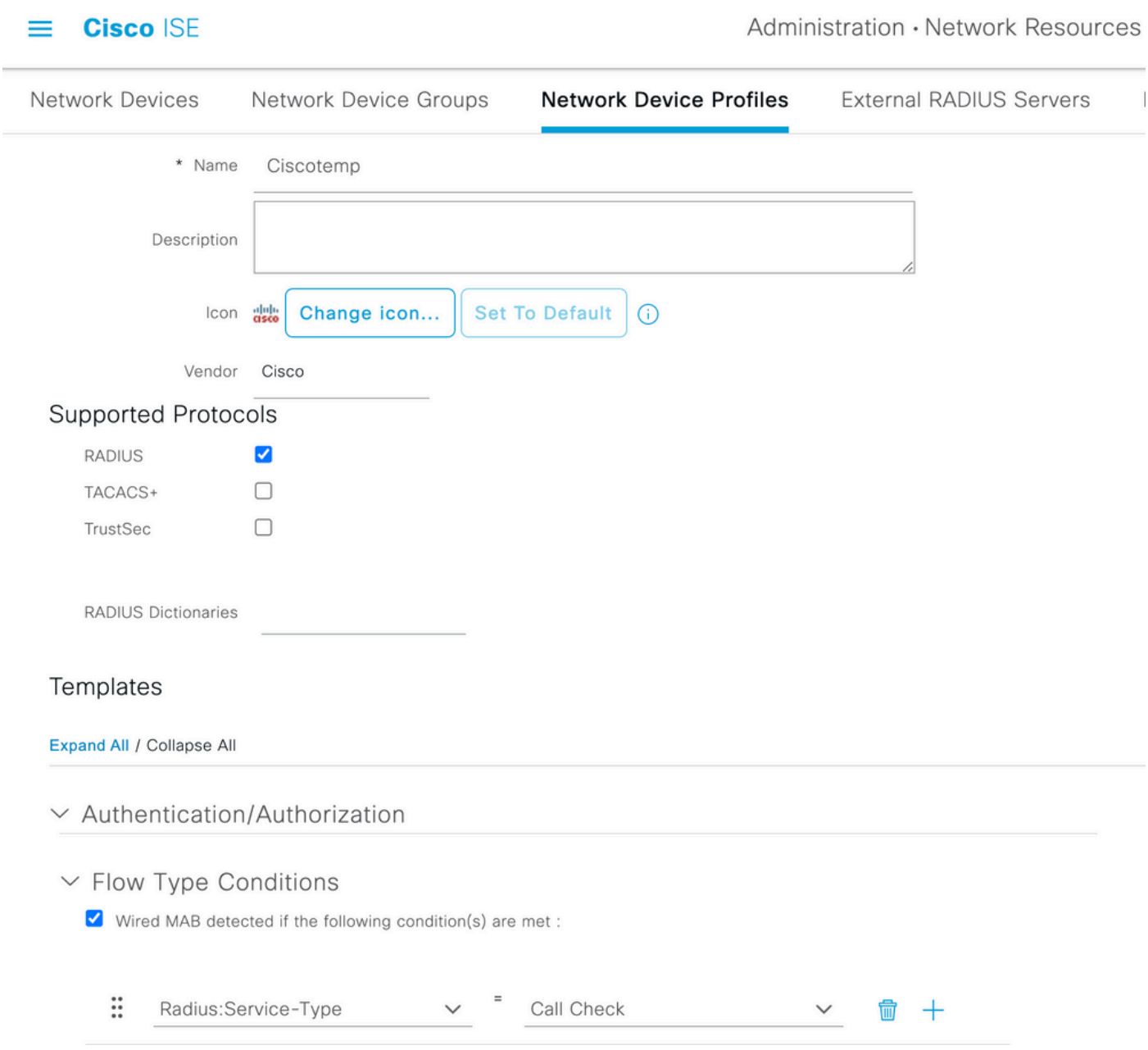
1. Cisco ISEでAAAクライアントとしてWLCを設定します。
2. Cisco ISEのデータベースにAPのMACアドレスを追加します。

ただし、APのMACアドレスをエンドポイント（最適な方法）またはユーザ（パスワードもMACアドレス）として追加することもできますが、その場合はパスワードのセキュリティポリシー要件を低くする必要があります。

WLCはNAS-Port-Type属性(MACアドレス認証(MAB)ワークフローに一致するISEの要件)を送信しないため、これを調整する必要があります。

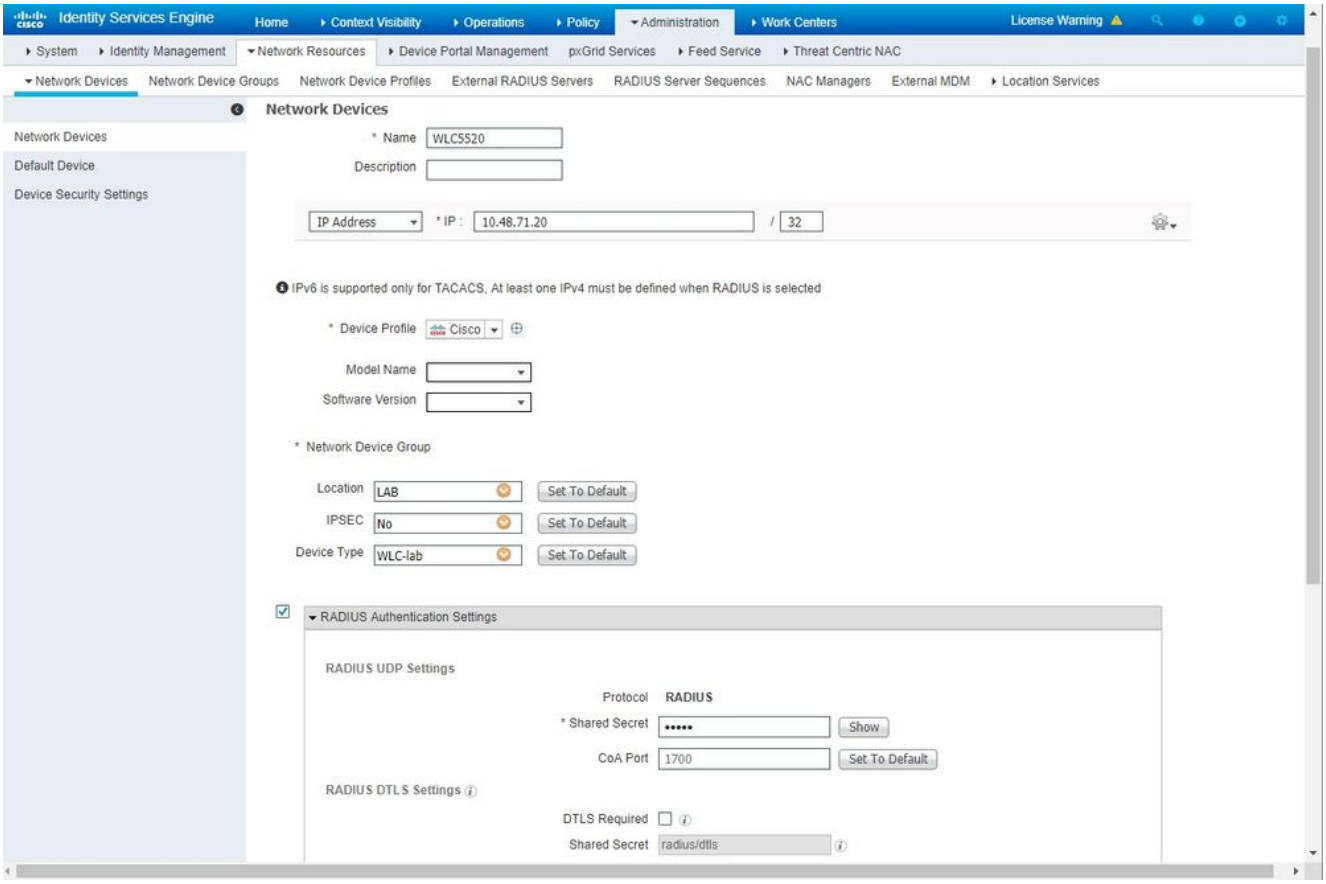
MABがNASポートタイプ属性を必要としない新しいデバイスプロファイルの設定

移動先 **Administration > Network device profile** 新しいデバイスプロファイルを作成します。図に示すように、RADIUSを有効にし、有線MABフローをrequire service-type=Call-checkに設定します。従来のCiscoプロファイルから他の設定をコピーできますが、その概念は、有線MABワークフローに「Nas-port-type」属性を必要としないことです。



Cisco ISEでAAAクライアントとしてWLCを設定する

1. 次に **Administration > Network Resources > Network Devices > Add.**[New Network Device]ページが表示されます。
2. このページで、WLCを定義します **Name,**管理インターフェイス **IP Address** と **Radius Authentications Settings** ~に似た **Shared Secret.**APのMACアドレスをエンドポイントとして入力する予定の場合は、デフォルトのCisco APではなく、以前に設定したカスタムデバイスプロファイルを使用してください。



3. クリック **Submit.**

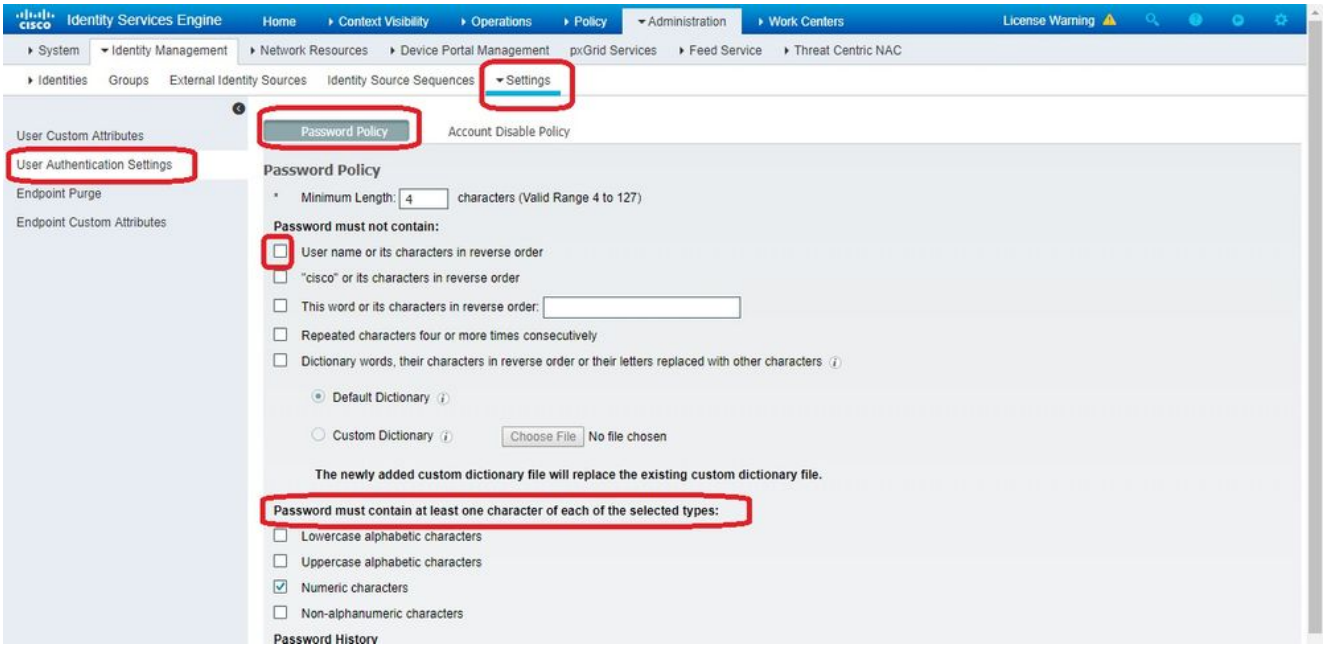
Cisco ISEのエンドポイントデータベースへのAP MACアドレスの追加

移動先 **Administration > Identity Management > Identities** MACアドレスをエンドポイントデータベースに追加します。

Cisco ISEのユーザデータベースへのAP MACアドレスの追加（オプション）

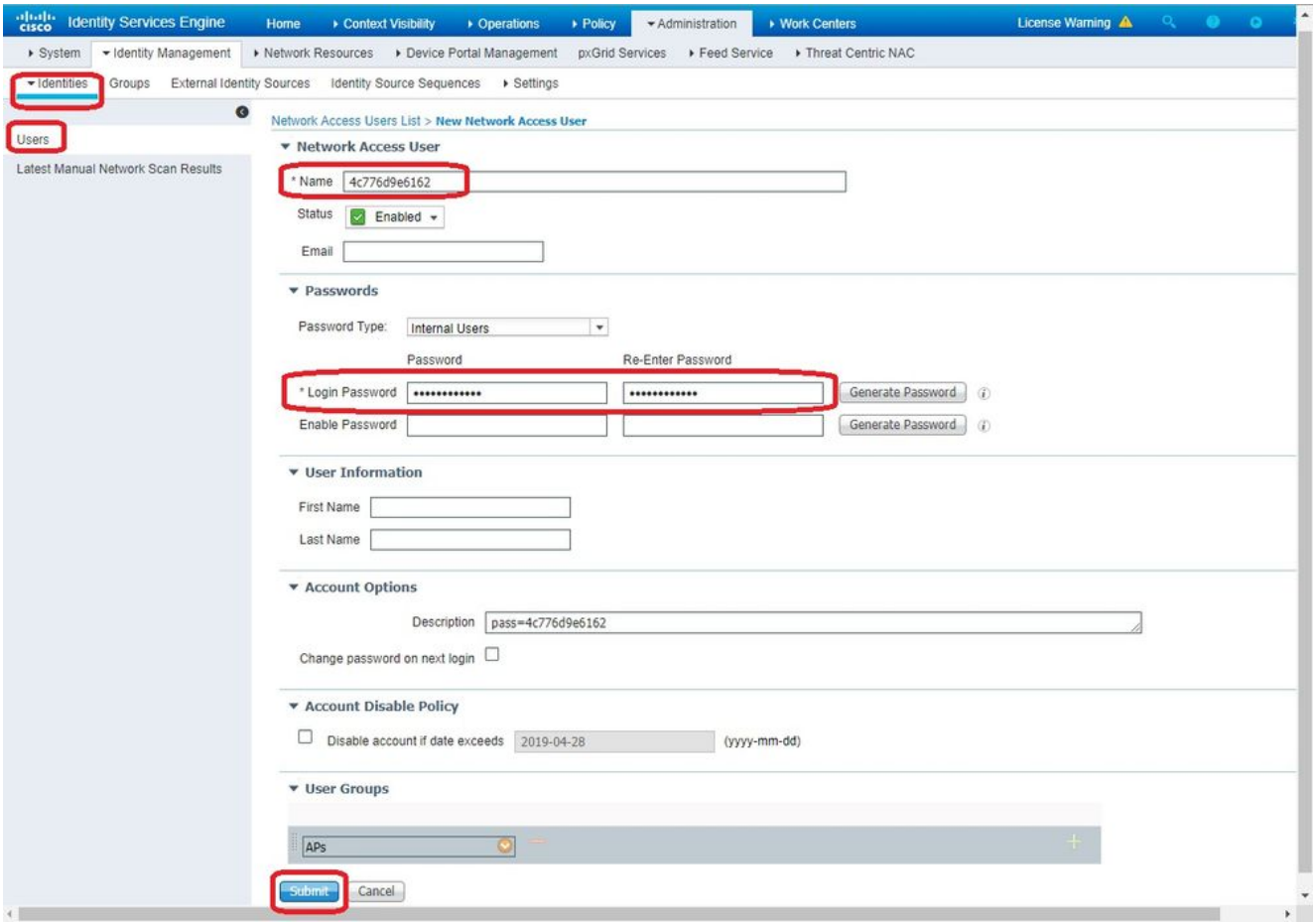
有線MABプロファイルを変更せずに、APのMACアドレスをユーザとして設定する場合は、パスワードポリシーの要件を低くする必要があります。

1. 移動先 **Administration > Identity Management.** ここでは、パスワードポリシーがユーザ名をパスワードとして使用することを許可し、ポリシーがMACアドレス文字の使用を許可し、文字の種類を変更する必要がないことを確認する必要があります。移動先
   Settings > User Authentication Settings > Password Policy:



2. 次に、 **Identities > Users** をクリックし、 **Add**.User Setupページが表示されたら、次に示すように、このAPのユーザ名とパスワードを定義します。

ヒント： **Description** パスワードとして定義された内容を後で簡単に確認できるように、パスワードを入力するためのフィールド。
パスワードは、APのMACアドレスである必要もあります。この例では、 **4c776d9e6162**.

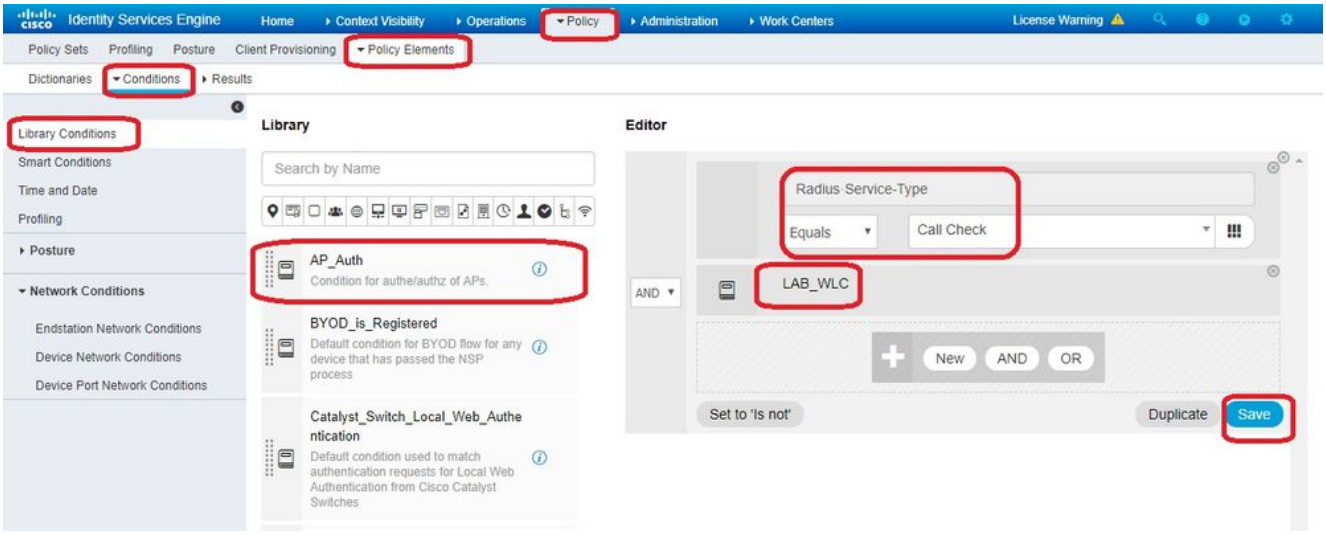


3. クリック **Submit**.

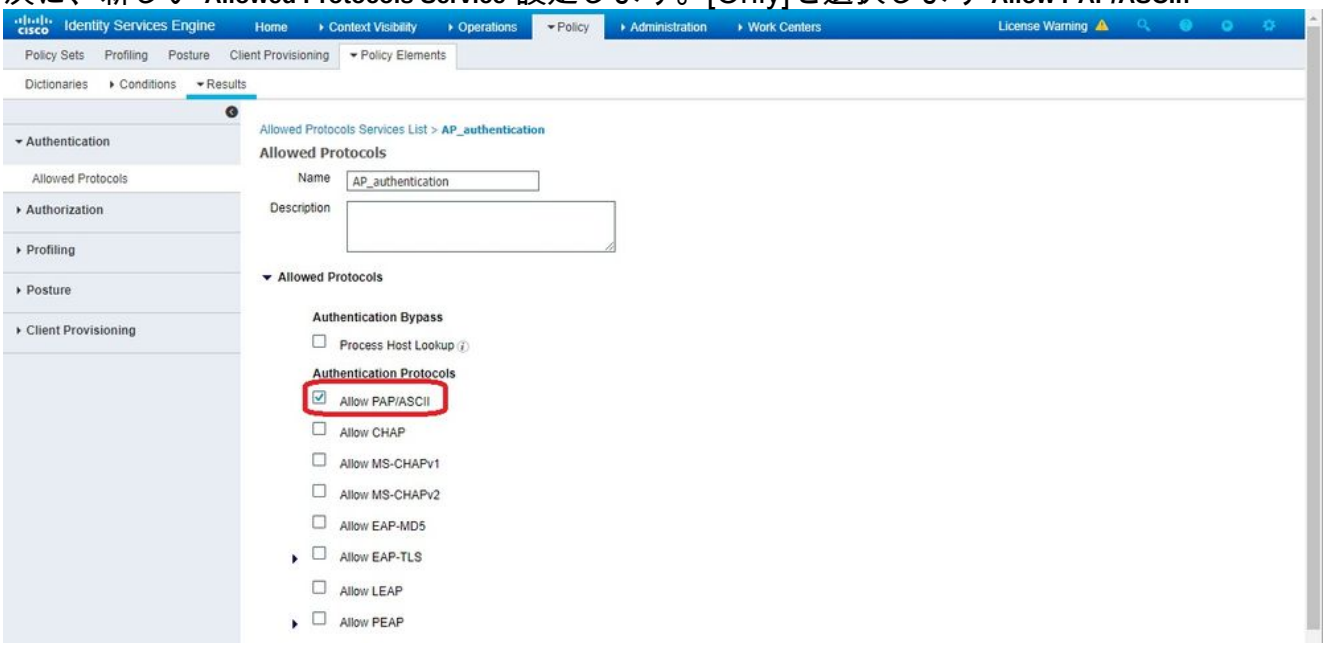
ポリシーセットの定義

1. この場合は、 **Policy Set** WLCからの認証要求と一致させます。最初に、に移動して条件を作

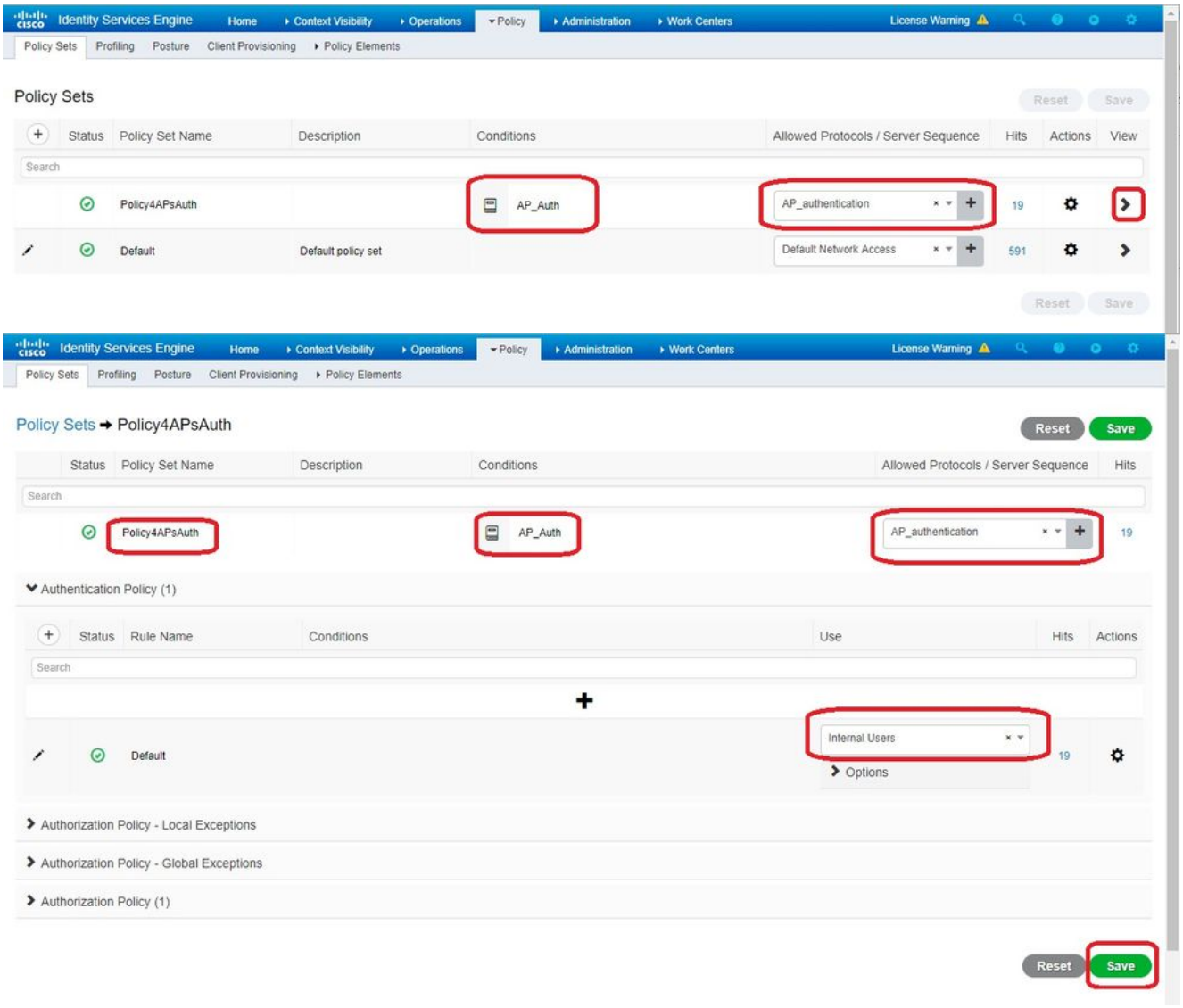
成します。 **Policy > Policy Elements > Conditions**、WLCの場所に一致する新しい条件の作成(この例では「LAB_WLC」および **Radius:Service-Type Equals Call Check** これはMac認証に使用されます。この条件の名前は「AP_Auth」です。



2. クリック **Save**.
3. 次に、新しい **Allowed Protocols Service** 設定します。[Only]を選択します **Allow PAP/ASCII**:



4. 以前に作成したサービスを **Allowed Protocols/Server Sequence**.[Expand the **View** 以下 **Authentication Policy > Use > Internal Users** これにより、ISEは内部DBでAPのユーザ名/パスワードを検索します。



5. クリック **Save**.

確認

この設定を確認するには、MACアドレス4c:77:6d:9e:61:62のAPをネットワークに接続してモニタする必要があります。 **debug capwap events/errors enable** と **debug aaa all enable** コマンドを発行します。

デバッグからわかるように、WLCはAPのMACアドレスをRADIUSサーバ10.48.39.128に渡し、サーバはAPを正常に認証しました。その後、APはコントローラに登録されます。

注：出力で、スペースの制約上 2 行に分割されている行があります。

```
*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
```

トラブルシュート

設定のトラブルシューティングを行うために、次のコマンドを使用できます。

- debug capwap events enable—LWAPPイベントのデバッグを設定します。
- debug capwap packet enable—LWAPPパケットトレースのデバッグを設定します。
- debug capwap errors enable—LWAPPパケットエラーのデバッグを設定します。
- debug aaa all enable – すべてのAAAメッセージのデバッグを設定します。

ISEに対してAPを認証させている際に、RADIUSライブログにユーザ名「INVALID」が記録される場合、これは、認証がエンドポイントデータベースに対して検証されており、このドキュメントで説明するように有線MABプロファイルを変更していないことを意味します。ISEは、有線/無線MABプロファイルと一致しない場合、MACアドレス認証を無効と見なします。デフォルトでは、WLCによって送信されないNASポートタイプ属性が必要です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。