Catalyst 9800ワイヤレスコントローラAP認証リストの設定

内容

はじめに

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラアクセスポイント(AP)認証ポリシーを設定する方法について説明します。

背景説明

アクセスポイント(AP)を認可するには、9800 Wireless LAN Controller(WLC)を使用するローカルデータベース、または外部Remote Authentication Dial-In User Service(RADIUS)サーバに対して、APのイーサネットMACアドレスを認可する必要があります。

この機能により、許可されたアクセスポイント(AP)だけがCatalyst 9800ワイヤレスLANコントローラに接続できるようになります。このドキュメントでは、コントローラに加入するためにMACフィルタエントリを必要とするが、一般的なAP認証フローをトレースしないメッシュ（1500シリーズ）APの場合については説明しません（参考資料を参照）。

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。

- 9800 WLC
- ワイヤレスコントローラへのコマンドラインインターフェイス(CLI)アクセス

使用するコンポーネント

9800 WLC v16.12

AP 1810W

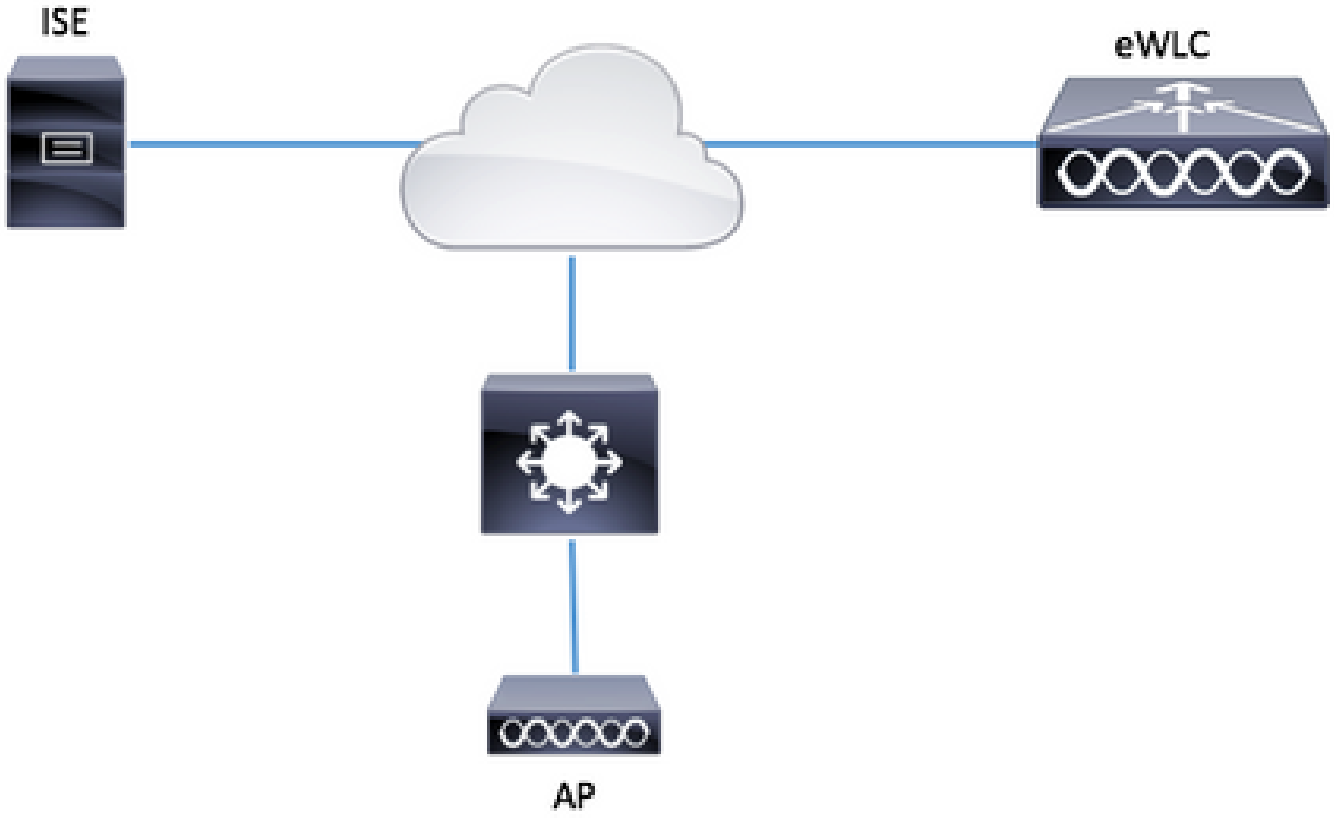
AP 1700

Identity Service Engine(ISE)v2.2

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、クリアな（デフォルト）設定で作業を開始しています。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。

設定

ネットワーク図



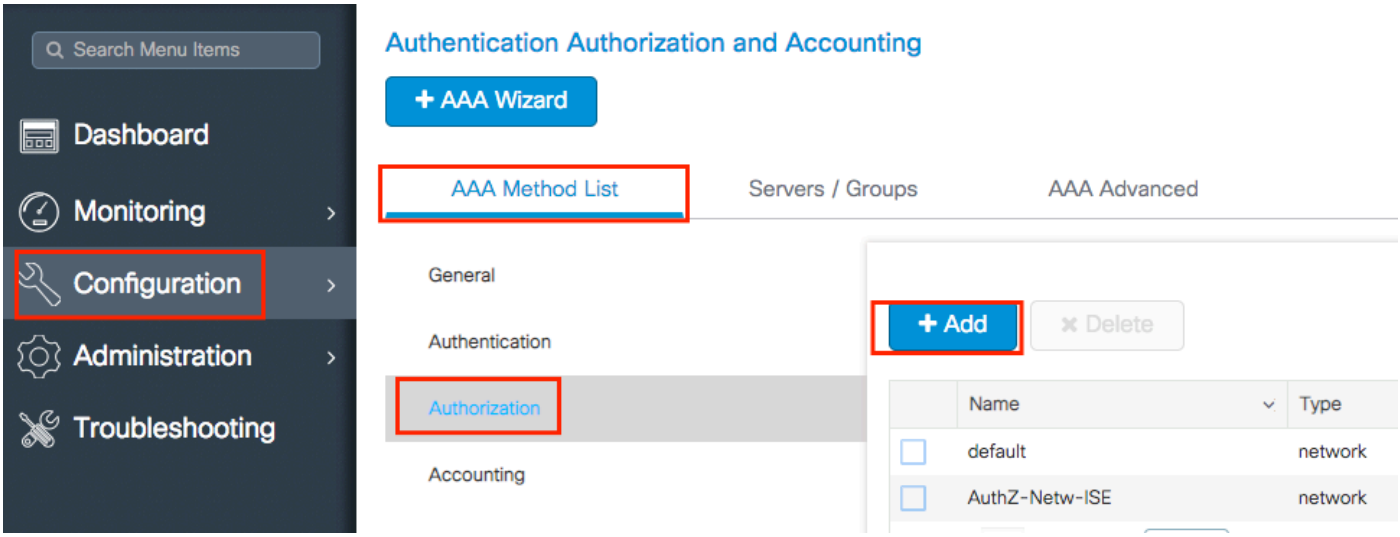
コンフィギュレーション

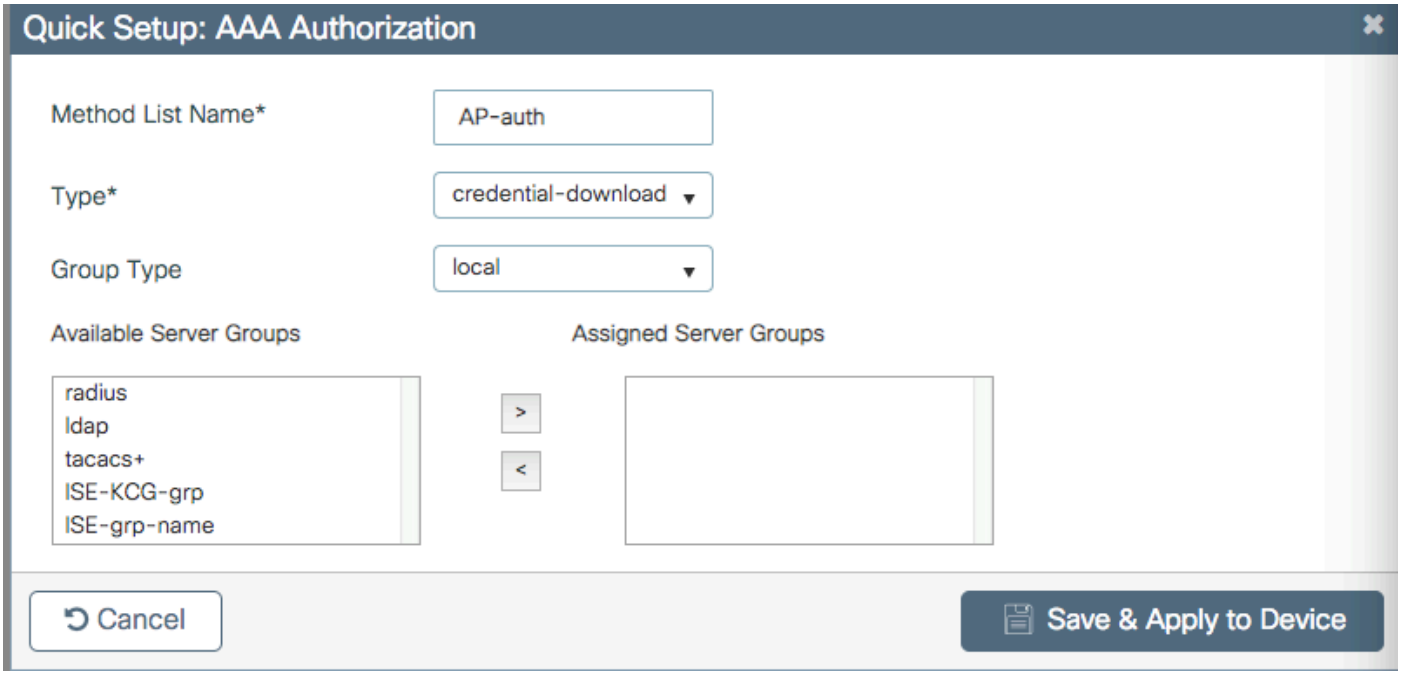
MAC AP認証リスト – ローカル

許可されたAPのMACアドレスは、9800 WLCにローカルに保存されます。

ステップ 1：ローカル認証のクレデンシャルダウンロード方式リストを作成します。

Configuration > Security > AAA > AAA Method List > Authorization > + Addの順に移動します。



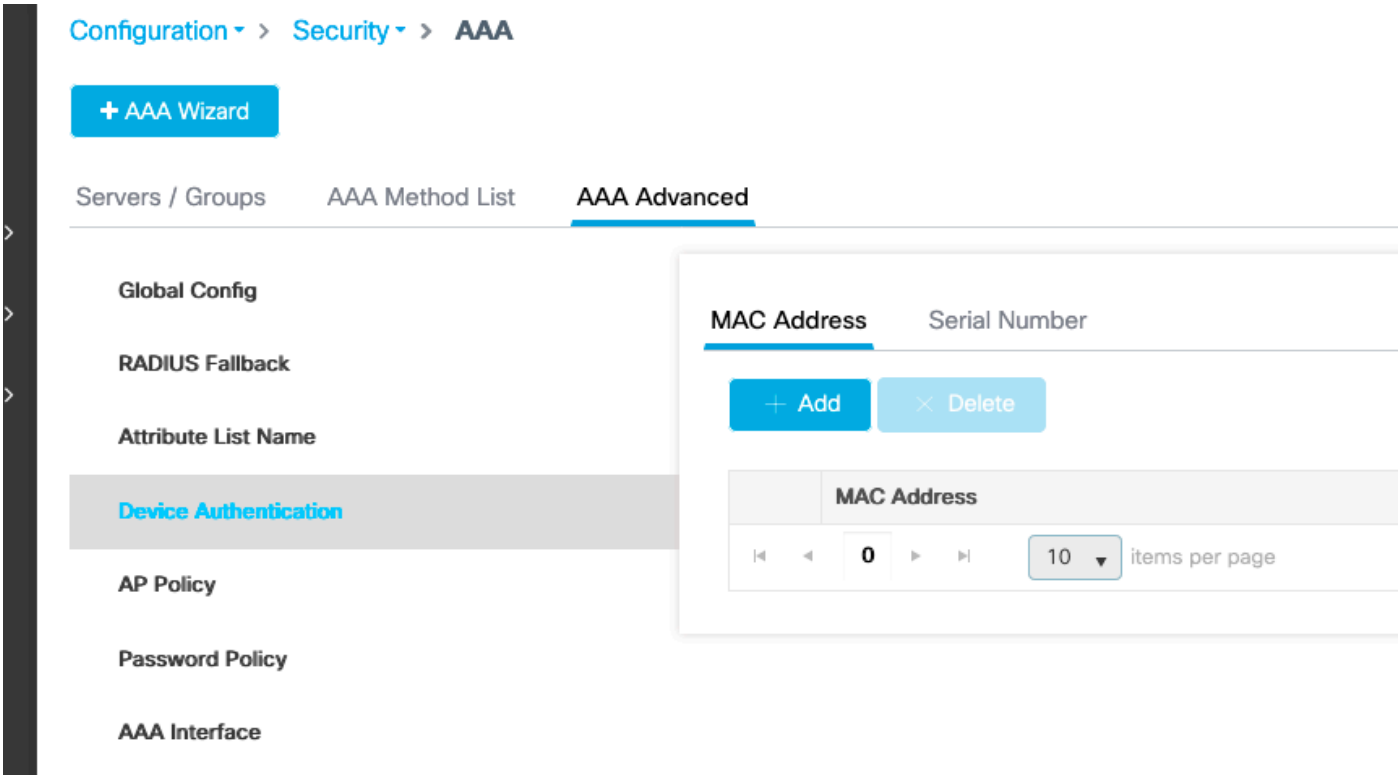


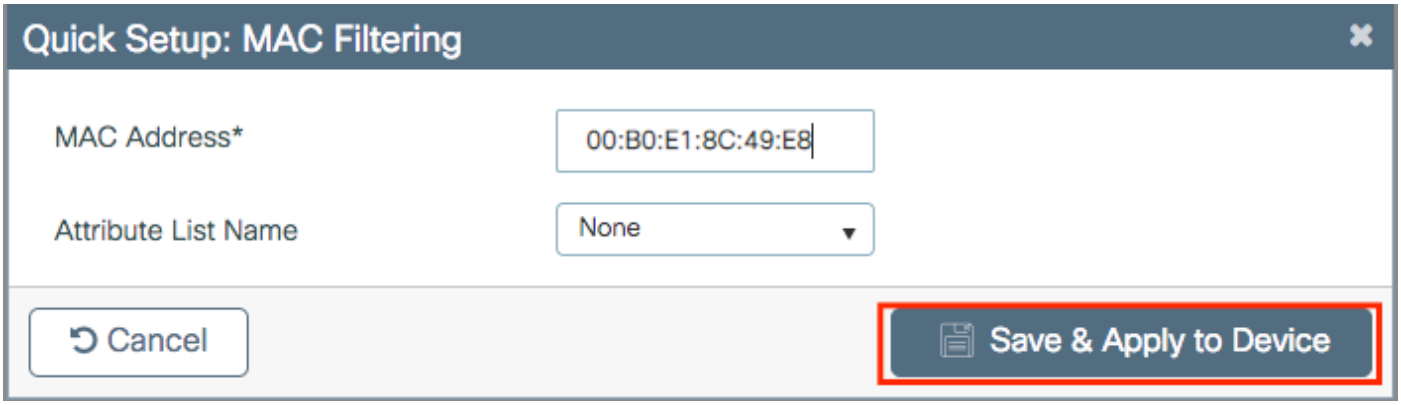
ステップ 2：APのMAC認証を有効にします。

移動先 Configuration > Security > AAA > AAA Advanced > AP Policyの順に選択します。
Authorize APs against MACを有効にし、ステップ1で作成したAuthorization Method Listを選択します。

ステップ 3：APのイーサネットMACアドレスを追加します。

移動先 Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add





注:APイーサネットMACアドレスは、 バージョン16.12のWeb UI(xx:xx:xx:xx:xx:xx（または）xxxx.xxxx.xxxx（または）xx-xx-xx-xx-xx-xx(xx)で入力した場合は、次のいずれかの形式になります。バージョン17.3では、区切り文字なしでxxxxxxxxxxxxの形式にする必要があります。CLI形式は、どのバージョンでも常にxxxxxxxxxxxxです（16.12では、Web UIは構成内の区切り文字を削除します）。Cisco Bug ID CSCvv43870では、それ以降のリリースでCLIまたはWeb UIの任意の形式を使用できます。

CLI：

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP認証リスト：外部RADIUSサーバ

9800 WLCの設定

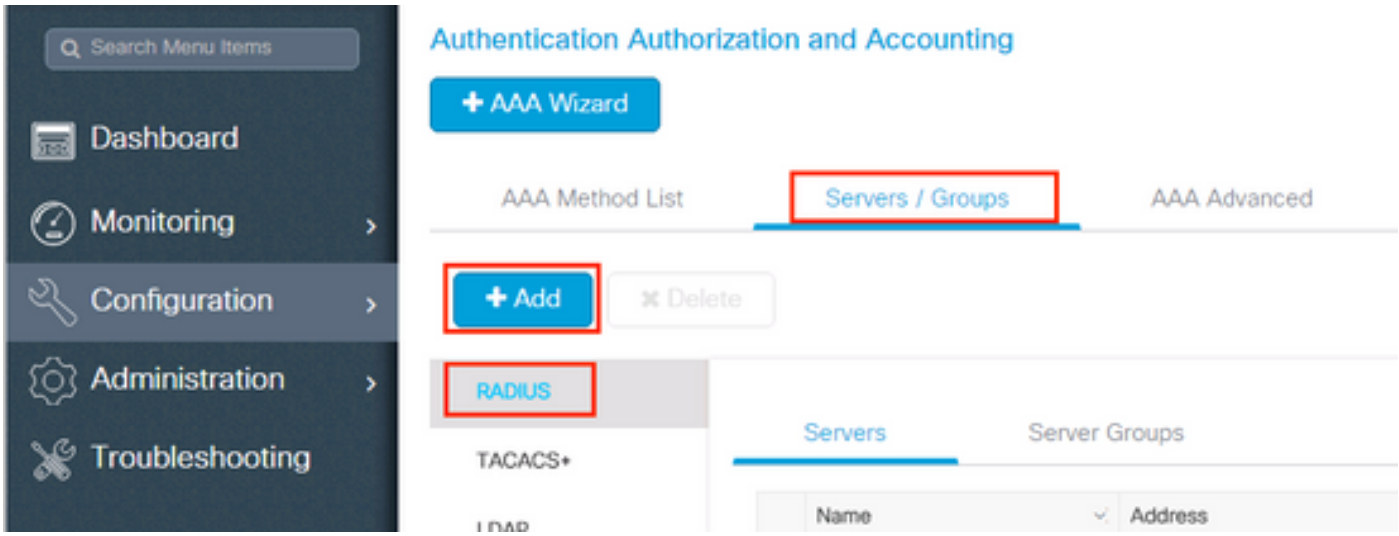
許可されたAPのMACアドレスは、外部RADIUSサーバ（この例ではISE）に保存されます。

ISEでは、APのMACアドレスをユーザ名/パスワードまたはエンドポイントとして登録できます。手順に沿って、いずれかの方法を選択して使用する方法が指示されます。

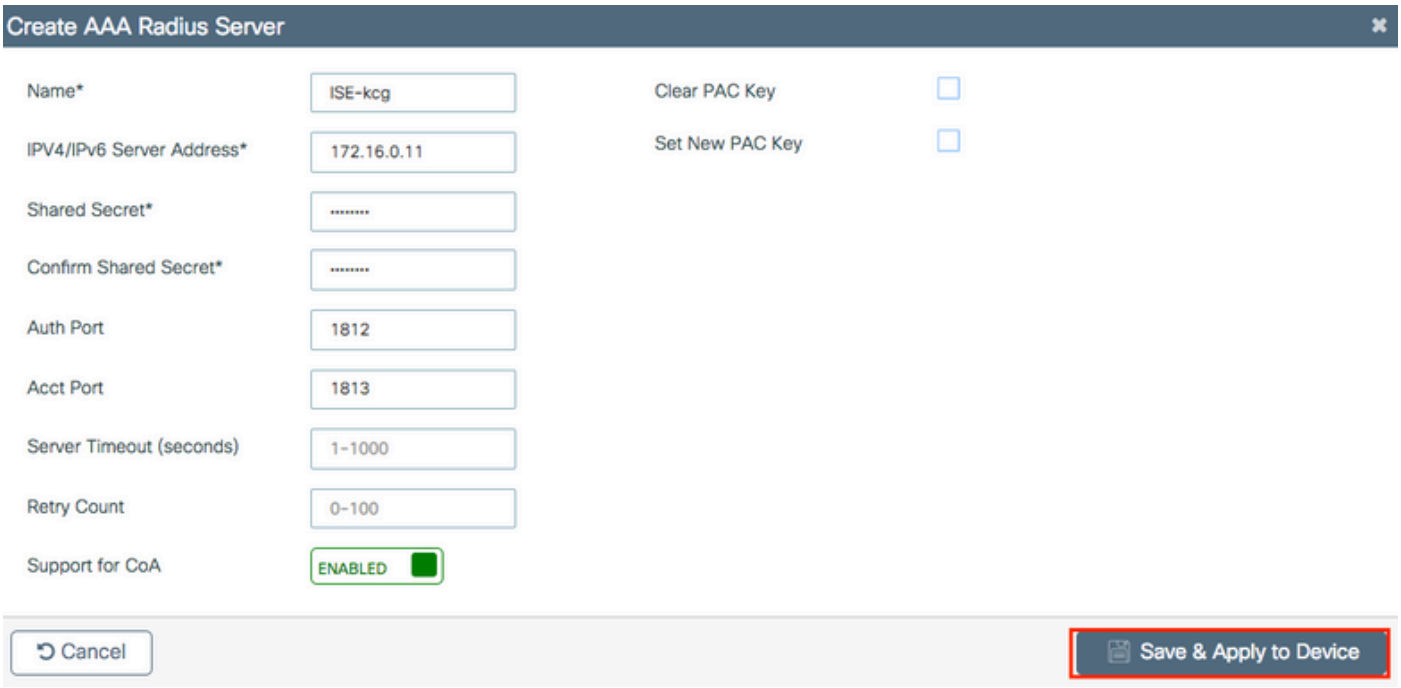
GUI：

ステップ 1：RADIUSサーバの宣言

Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Addの順に移動し、RADIUSサーバの情報を入力します。



将来的に中央 Web 認証（または CoA を必要とするあらゆる種類のセキュリティ）を使用する予定がある場合は、CoA のサポートが有効になっていることを確認します。

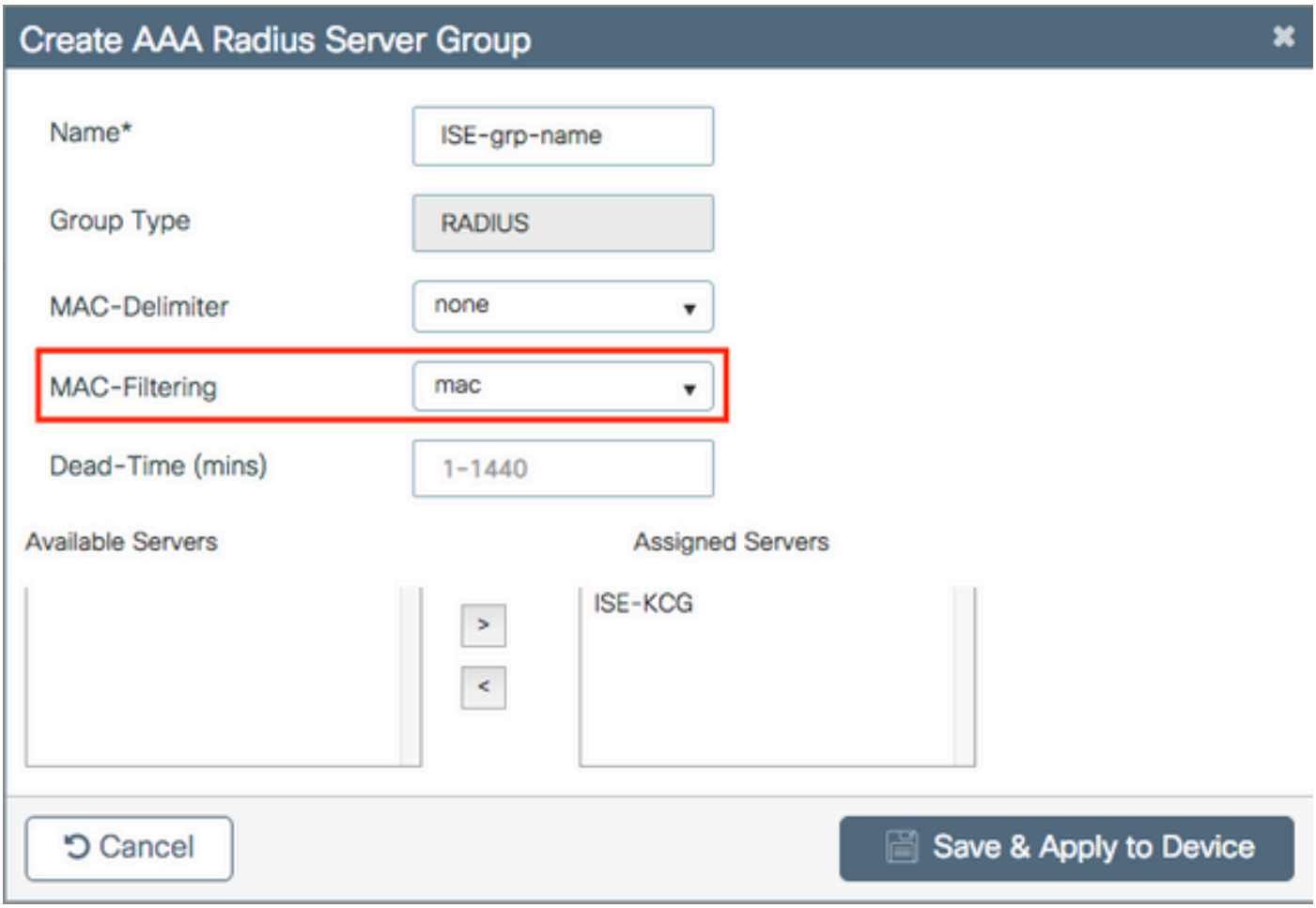


ステップ 2：RADIUSグループへのRADIUSサーバの追加

Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Addの順に移動します。

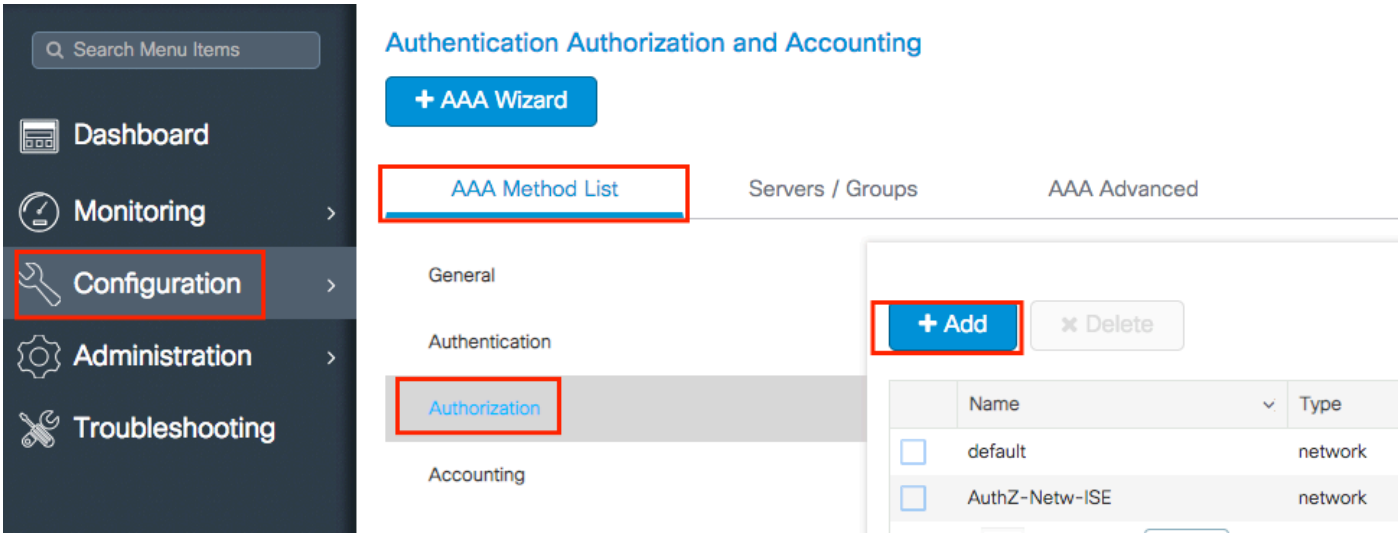
ISEでAPのMACアドレスをユーザ名として認証するには、MACフィルタリングはnoneのままにします。

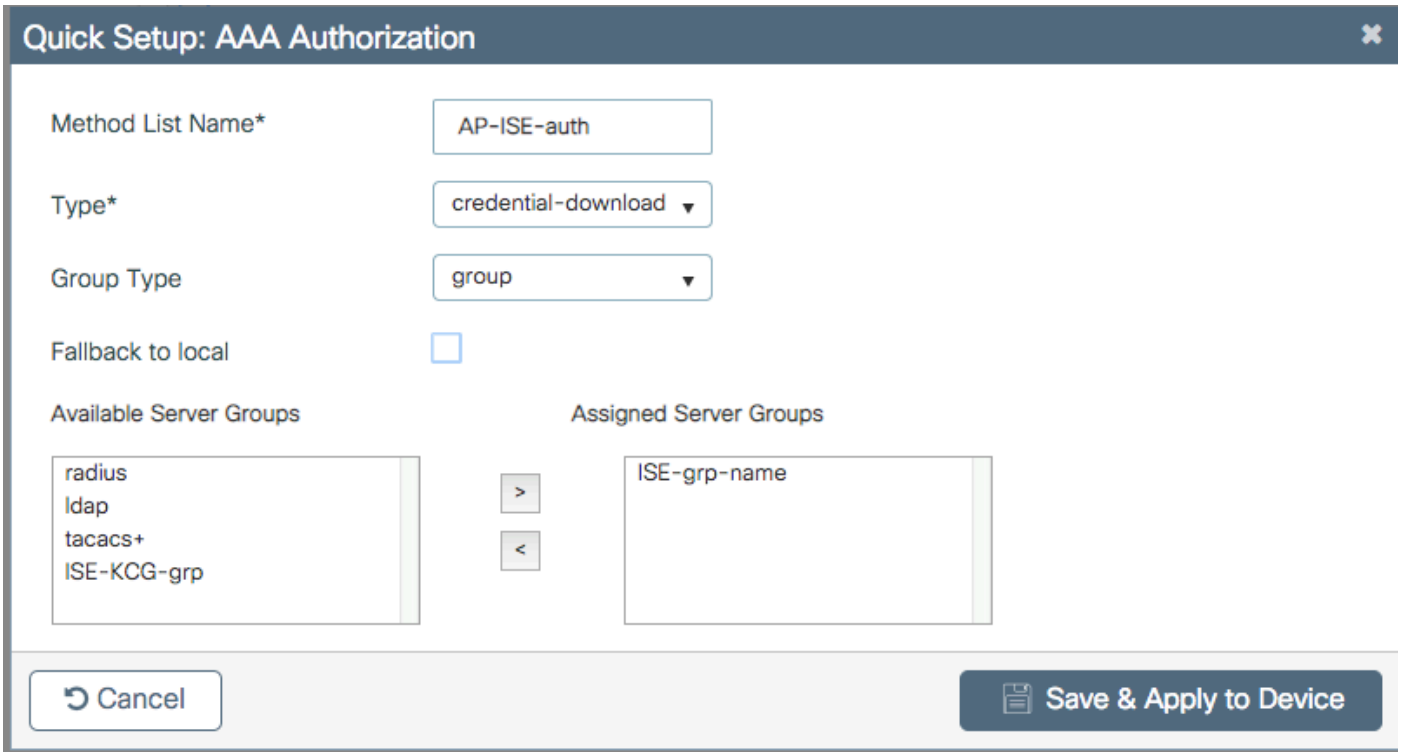
エンドポイントがMACフィルタリングをMACに変更するときに、ISEにAPのMACアドレスを認証させるには、



ステップ 3：許可クレデンシャルダウンロード方式リストを作成します。

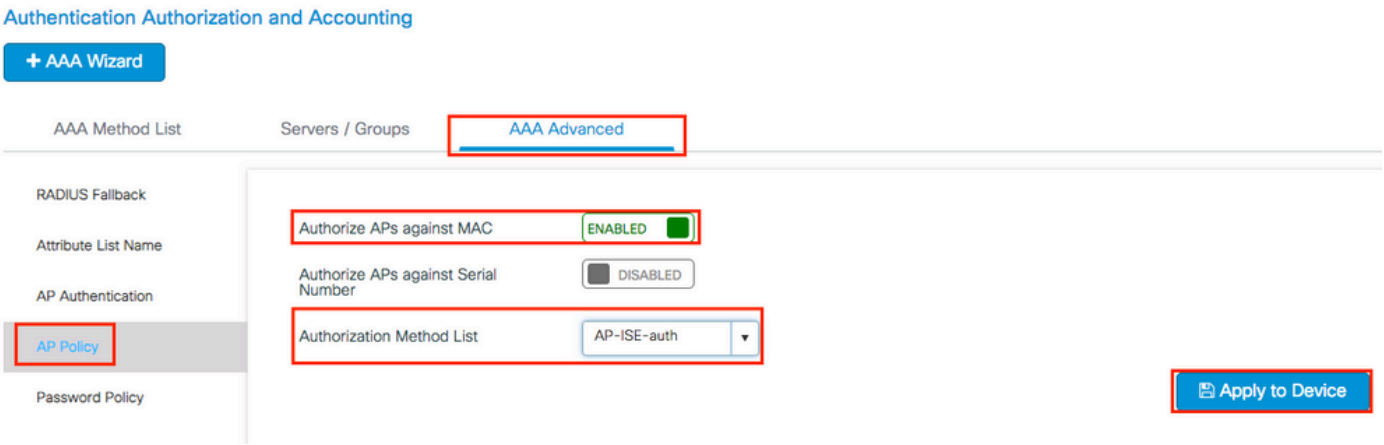
Configuration > Security > AAA > AAA Method List > Authorization > + Addの順に移動します。





ステップ 4：APのMAC認証を有効にします。

移動先 Configuration > Security > AAA > AAA Advanced > AP Policyの順に選択します。
Authorize APs against MACを有効にし、ステップ3で作成したAuthorization Method Listを選択します。



CLI：

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
```

```
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISEの設定

ステップ 1：9800 WLCをISEに追加するには、次の手順を実行します。

ISEでの9800 WLCの宣言

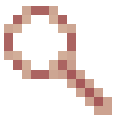
認証に基づいて、必要な手順でAPのMACアドレスを設定することを選択します。

MACアドレスをエンドポイントとして認証するためのUSEの設定

MACアドレスをユーザ名/パスワードとして認証するようにISEを設定する

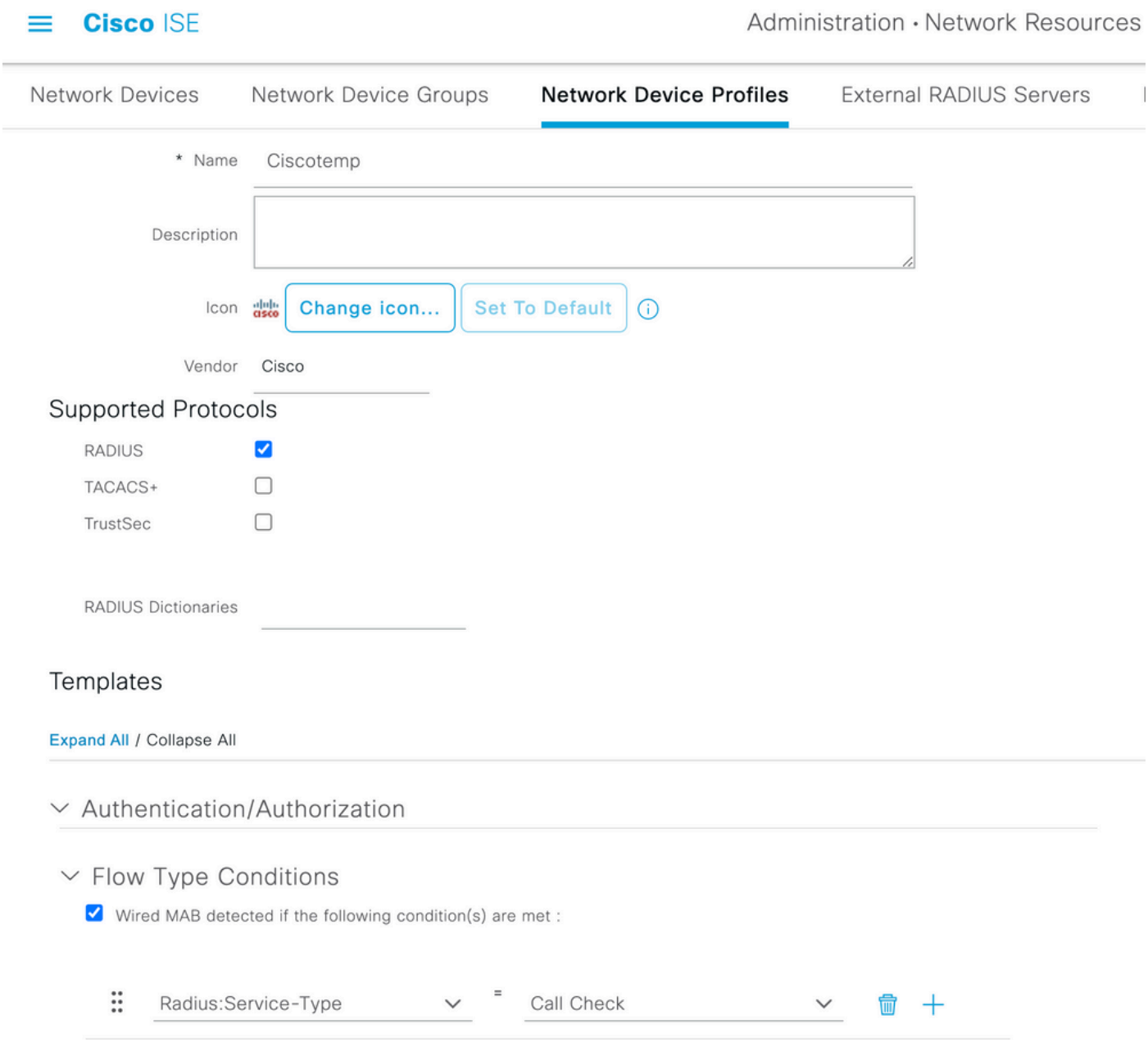
MACアドレスをエンドポイントとして認証するようにISEを設定する

手順2:（オプション）アクセスポイントのIDグループを作成する



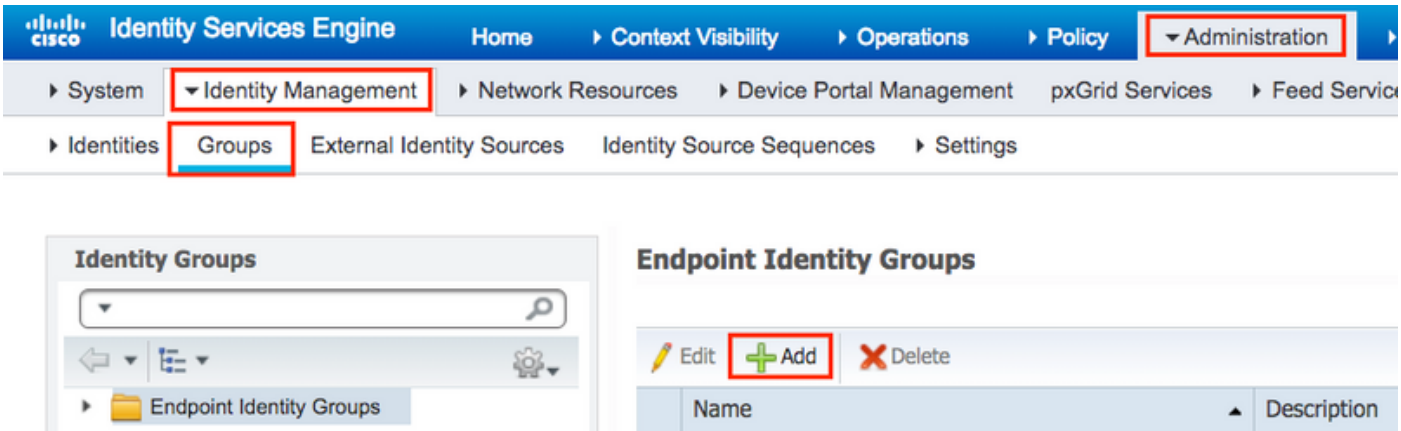
9800はAP認証とともにNAS-port-Type属性を送信しないため、Cisco Bug IDCSCvy74904)、ISEはAP認証をMABワークフローとして認識しないため、ISEでNAS-PORT-type属性を必要としないようにMABワークフローを変更しない限り、APのMACアドレスがエンドポイントリストに配置されている場合は、APを認証できません。

Administrator > Network device profileの順に移動し、新しいデバイスプロファイルを作成します。RADIUSを有効にし、有線MABのservice-type=call-checkを追加します。残りはシスコの元のプロファイルからコピーできます。この概念は、有線MABに「nas-port-type」条件を設定しないことです。

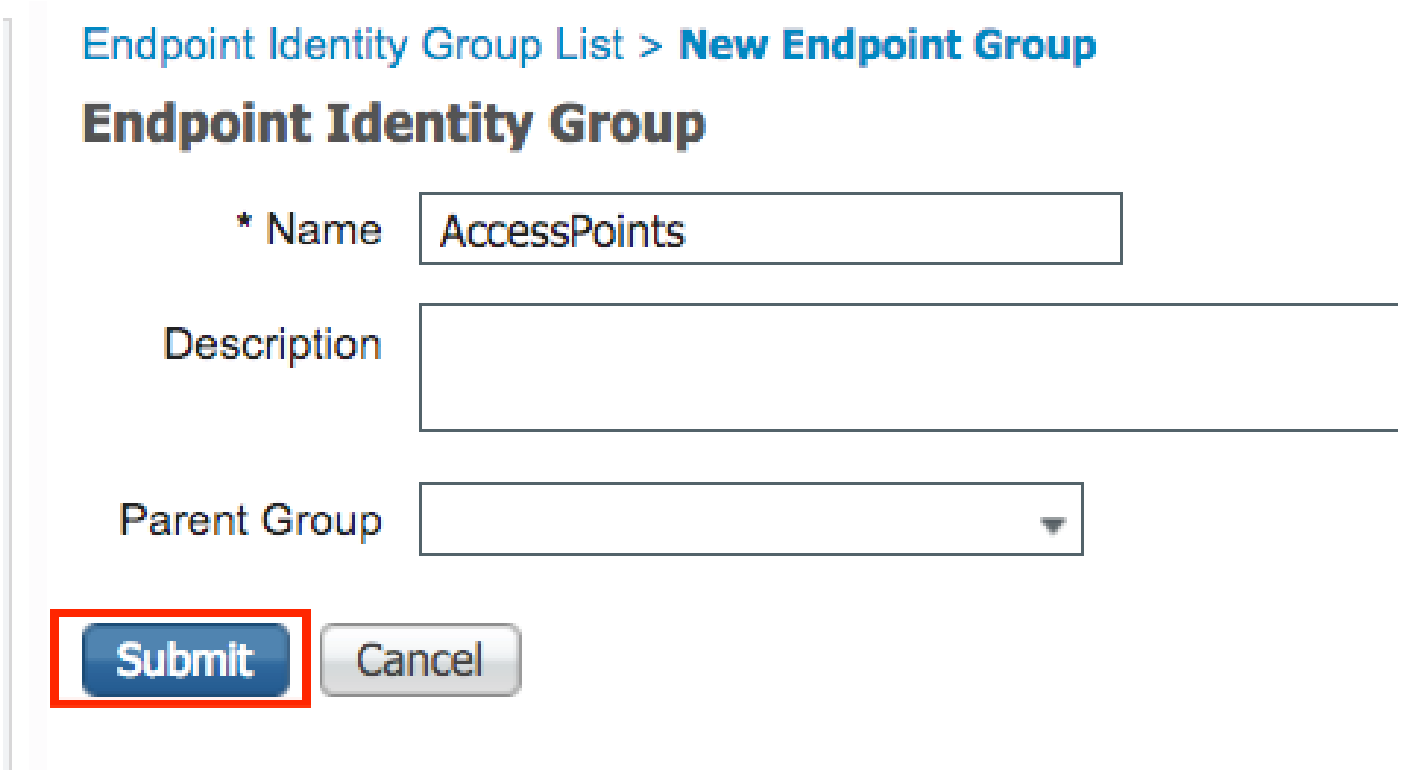


9800のネットワークデバイスエントリに戻り、プロファイルを新しく作成したデバイスプロファイルに設定します。

Administration > Identity Management > Groups > Endpoint Identity Groups > + Addの順に移動します。

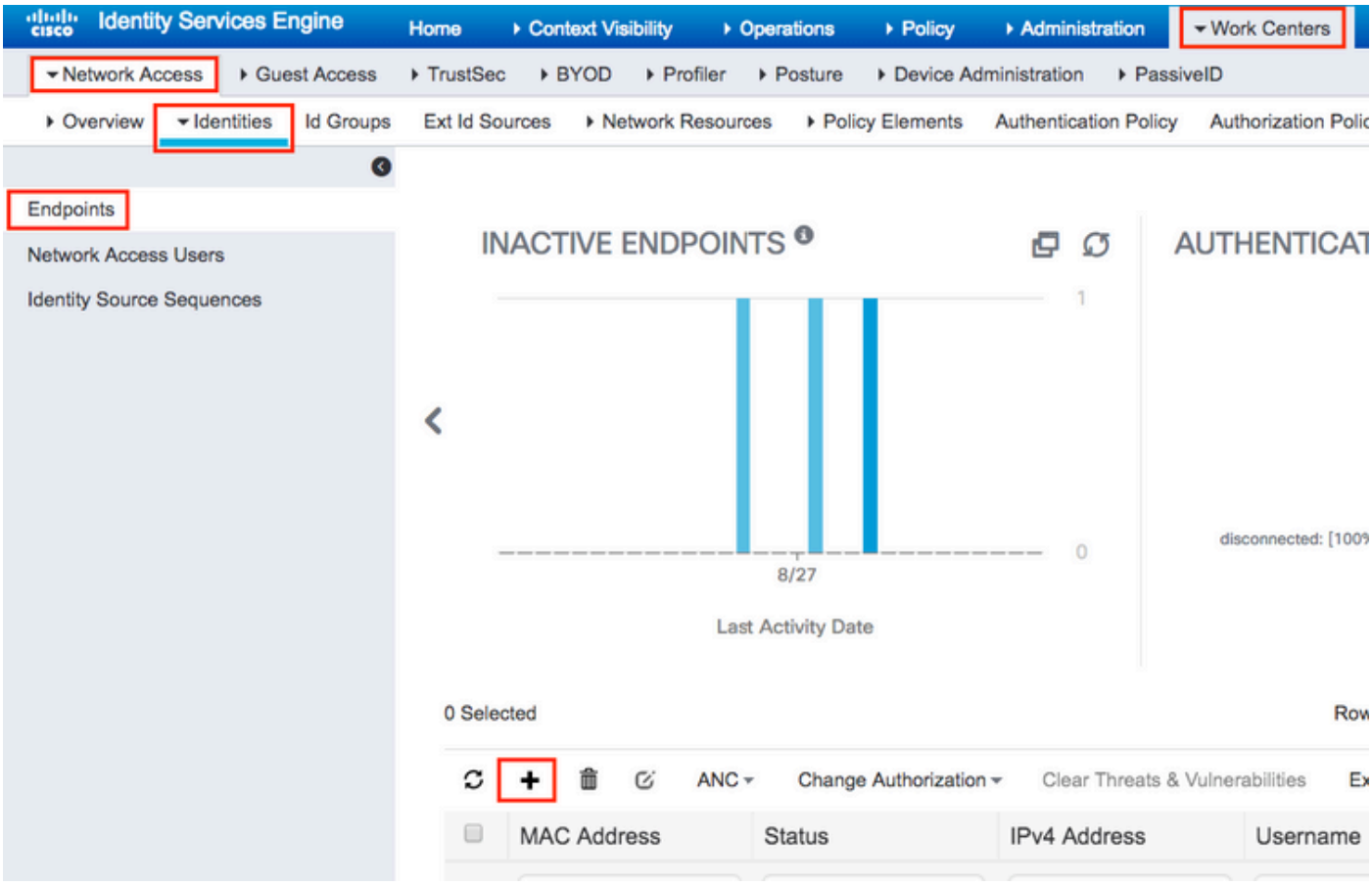


名前を選択して、Submitをクリックします。

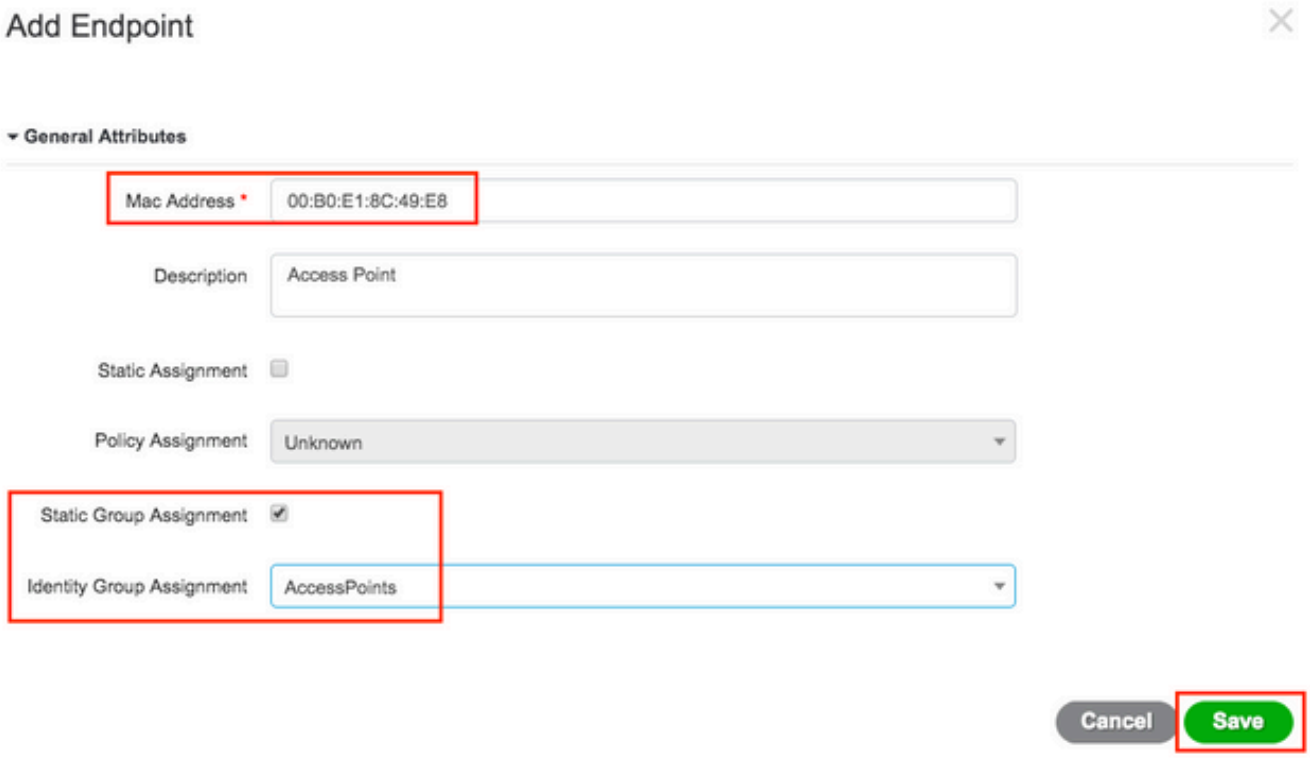


ステップ 3：APのイーサネットMACアドレスをエンドポイントIDグループに追加します。

Work Centers > Network Access > Identities > Endpoints > +の順に移動します

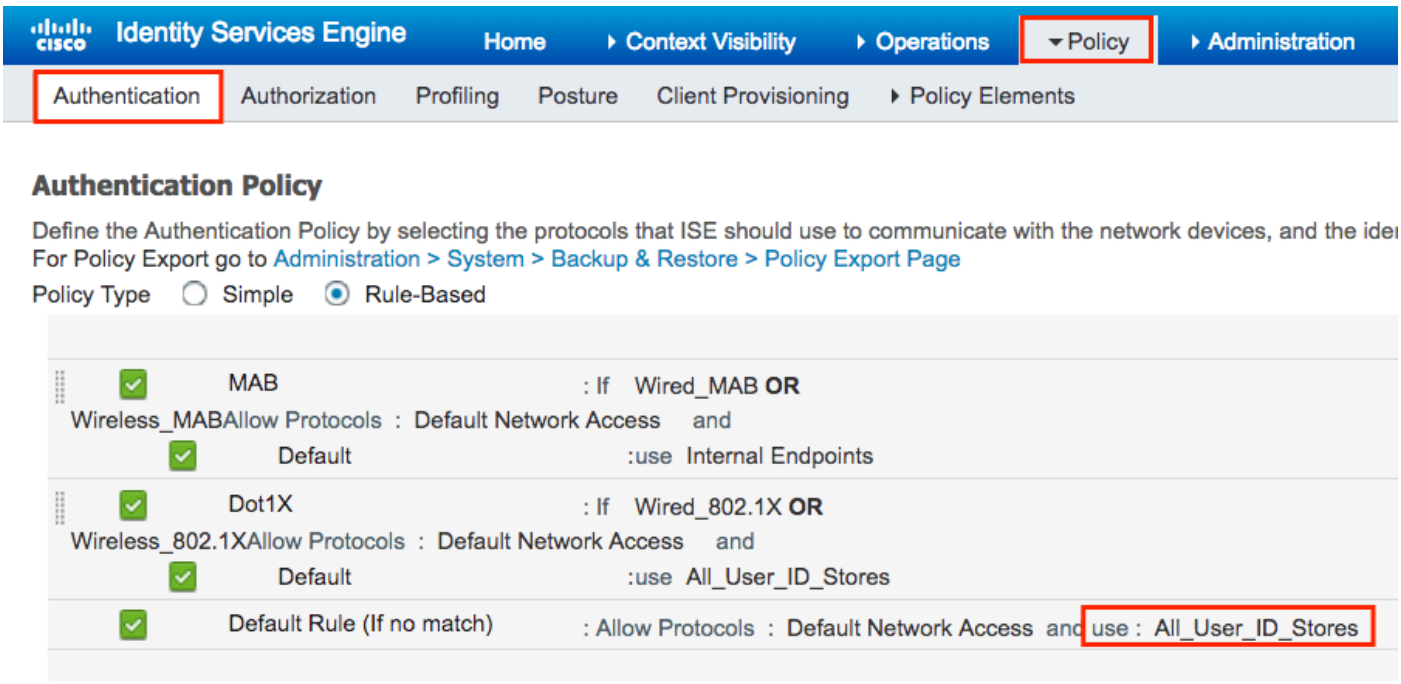


必要な情報を入力します。

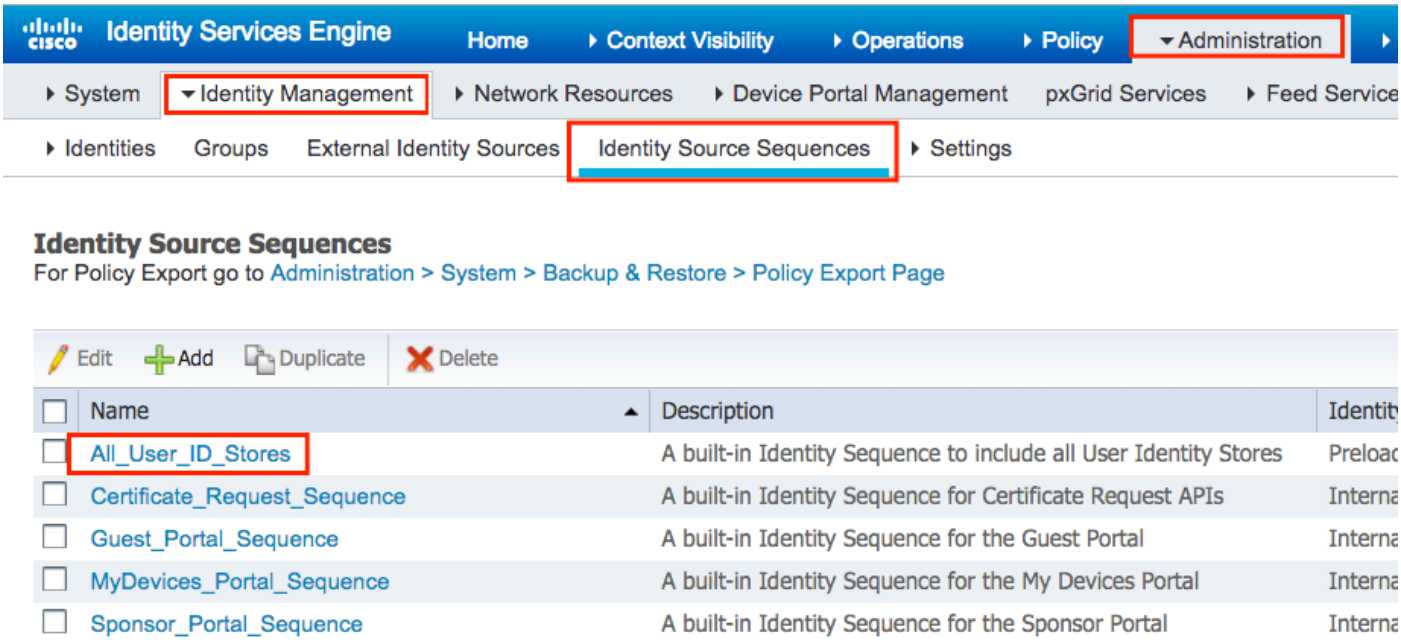


ステップ 4：デフォルトの認証ルールで使用されているIDストアに内部エンドポイントが含まれていることを確認します。

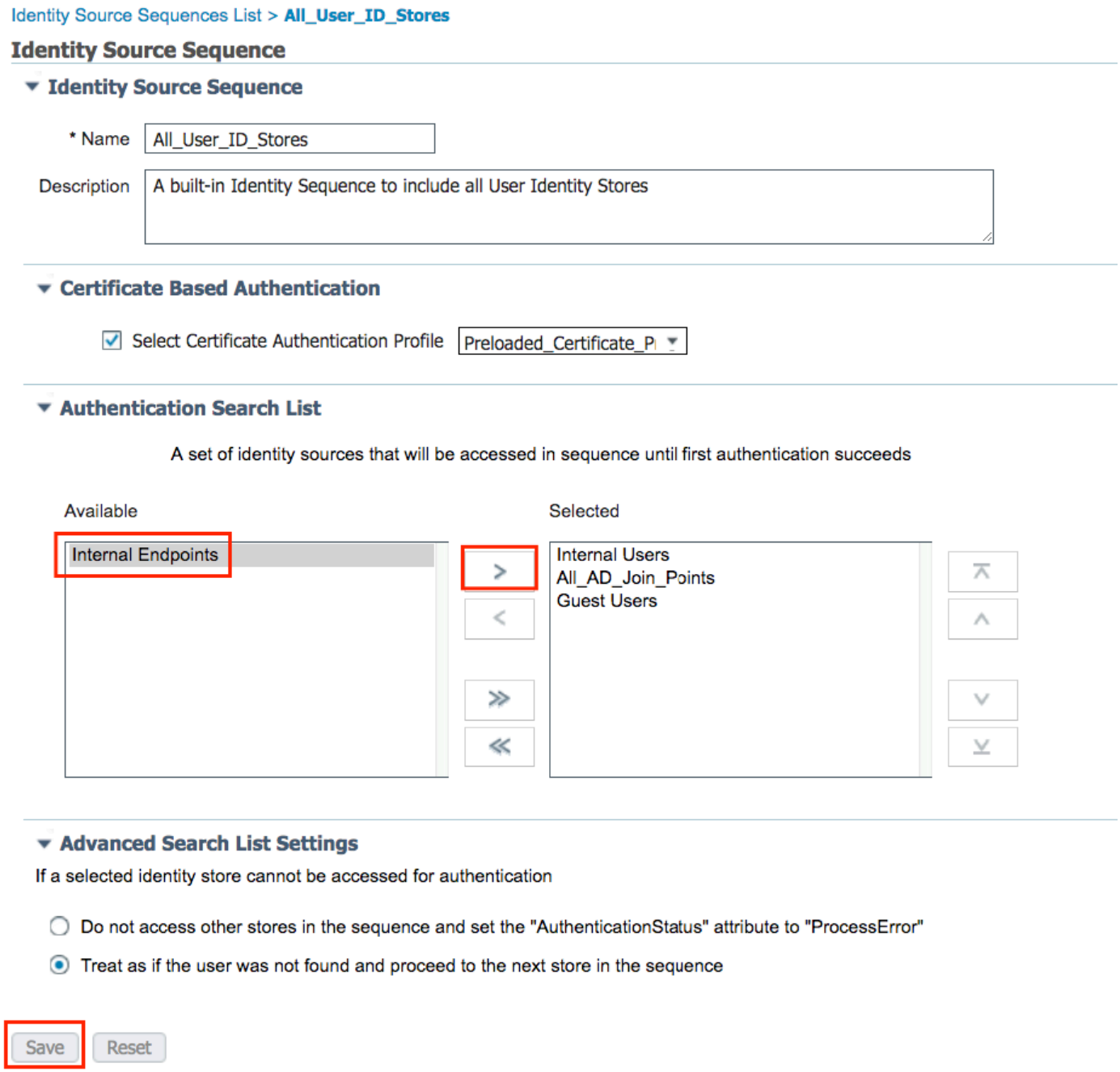
A. Policy > Authenticationの順に移動し、IDストアをメモします。



B. Administration > Identity Management > Identity Source Sequences > Identity Nameの順に移動します。



C.内部エンドポイントが内部エンドポイントに属していることを確認します。属していない場合は追加します。



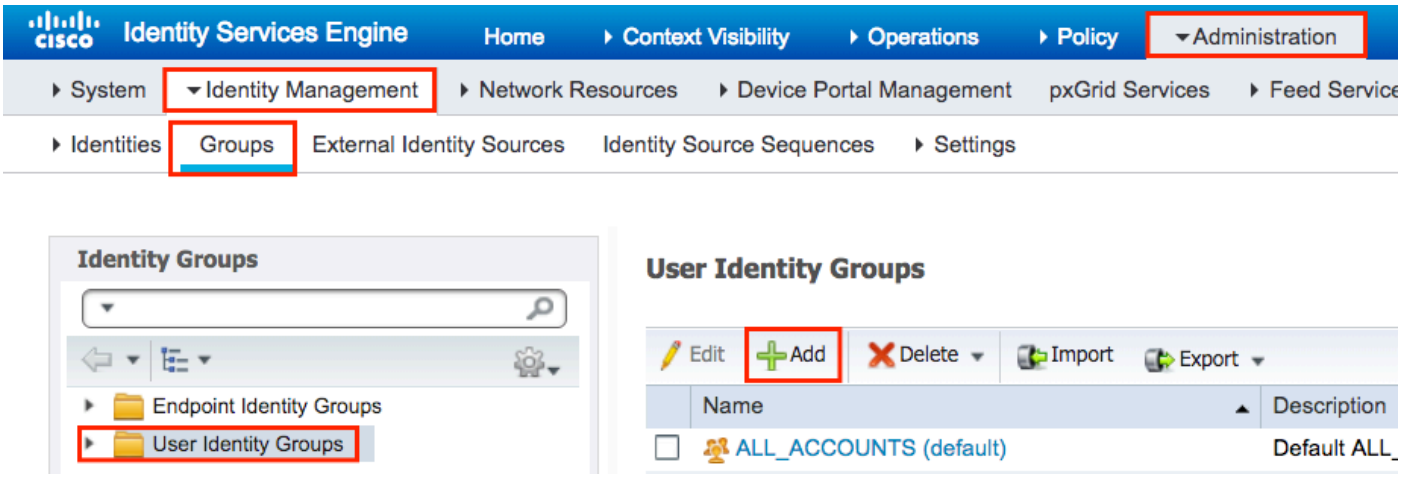
MACアドレスをユーザ名/パスワードとして認証するようにISEを設定する

この方法では、ユーザ名と同じパスワードを許可するために低いパスワードポリシーが必要になるため、この方法はお勧めしません。

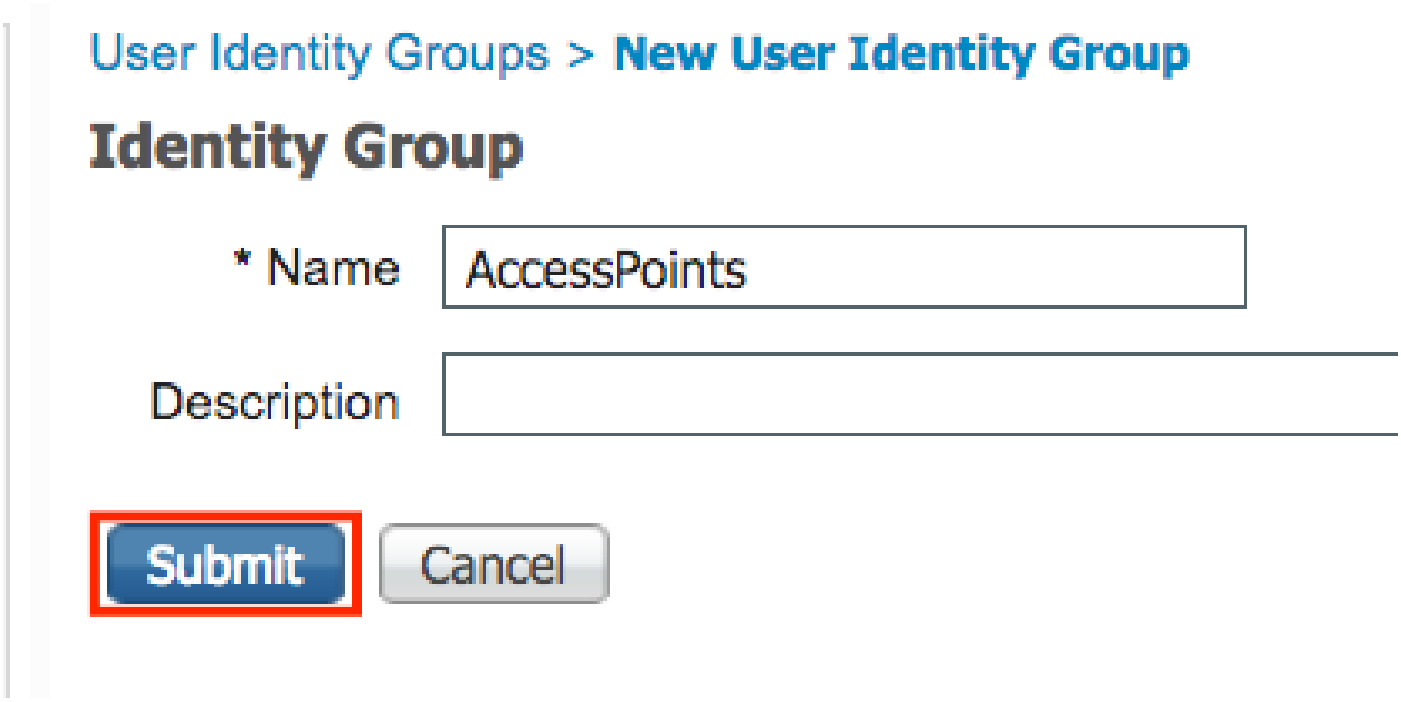
ただし、ネットワークデバイスプロファイルを変更できない場合は、回避策として使用できます

手順2:（オプション）アクセスポイントのIDグループを作成する

Administration > Identity Management > Groups > User Identity Groups > + Addの順に移動します。

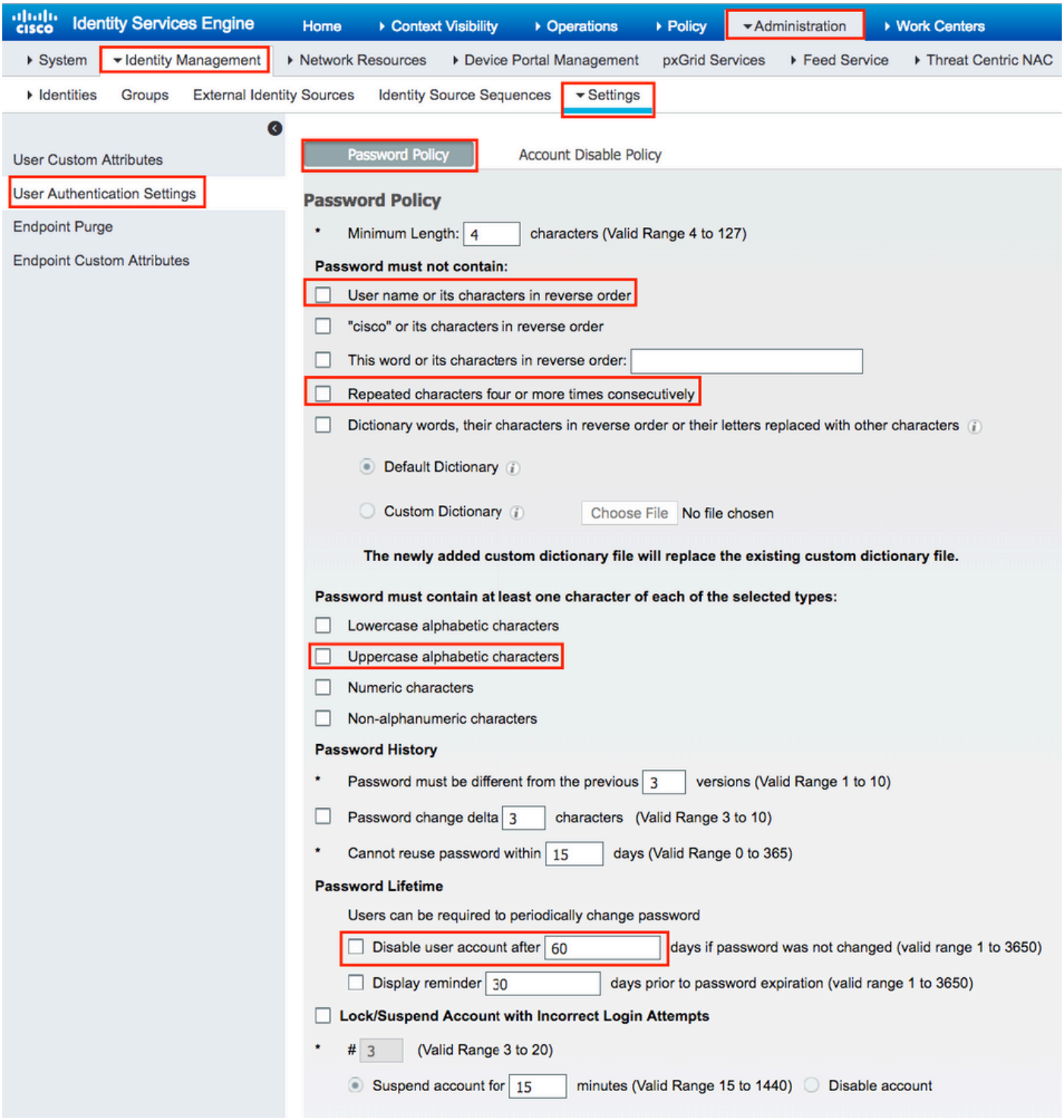


名前を選択して、Submitをクリックします。



ステップ 3：現在のパスワードポリシーでMACアドレスをユーザ名とパスワードとして追加できることを確認します。

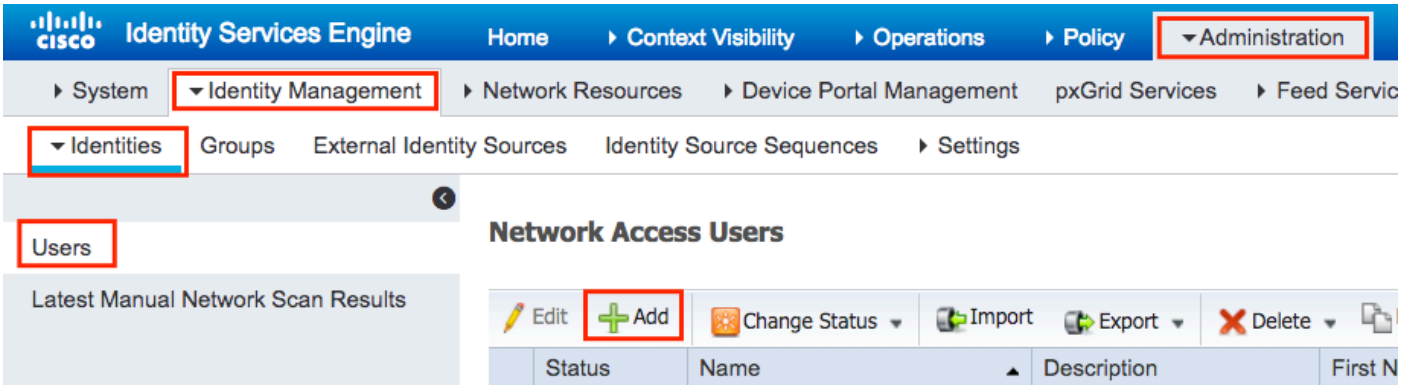
Administration > Identity Management > Settings > User Authentication Settings > Password Policyの順に移動し、少なくとも次のオプションが無効になっていることを確認します。



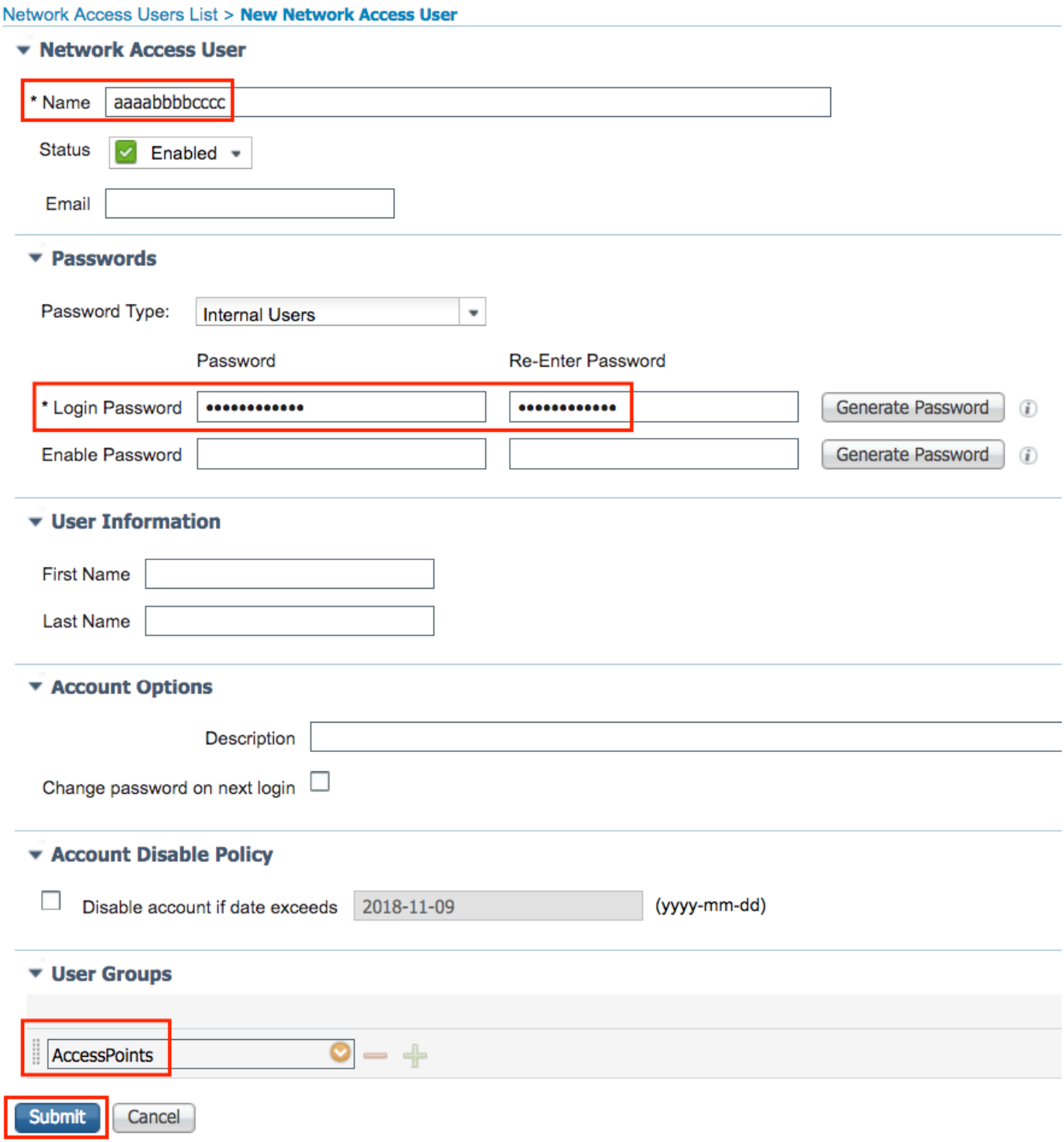
注:パスワードが変更されなかった場合は、Disable user account after XX daysオプションを無効にすることもできます。これはMACアドレスであるため、パスワードは変更されません。

ステップ 4：APのイーサネットMACアドレスを追加します。

Administration > Identity Management > Identities > Users > + Addの順に移動します。



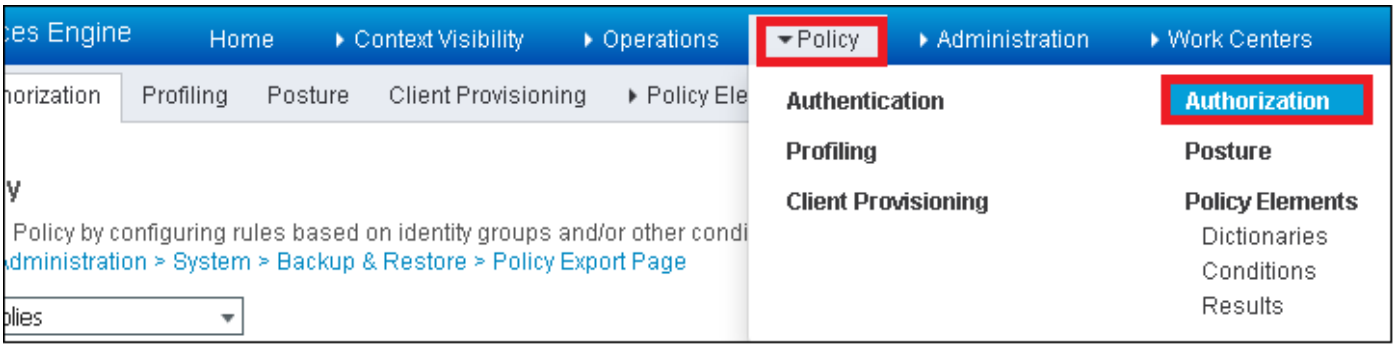
必要な情報を入力します。



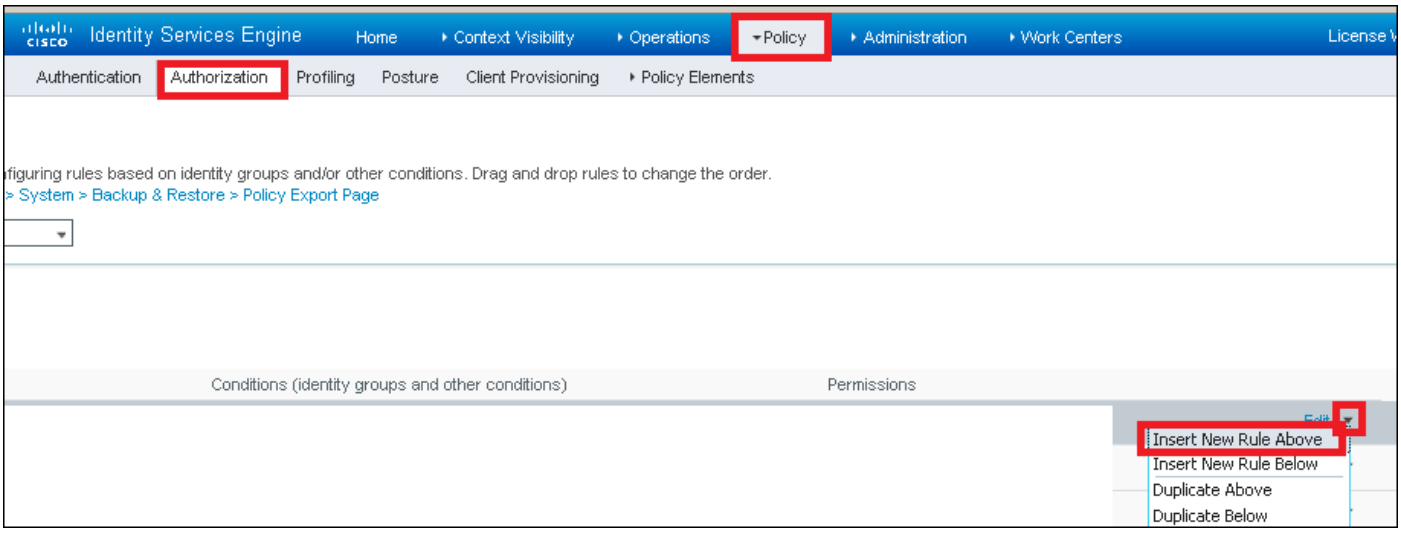
注:NameおよびLogin Passwordフィールドは、APのイーサネットMACアドレスで、すべて小文字で区切り文字を使用しない必要があります。

APを認証する認可ポリシー

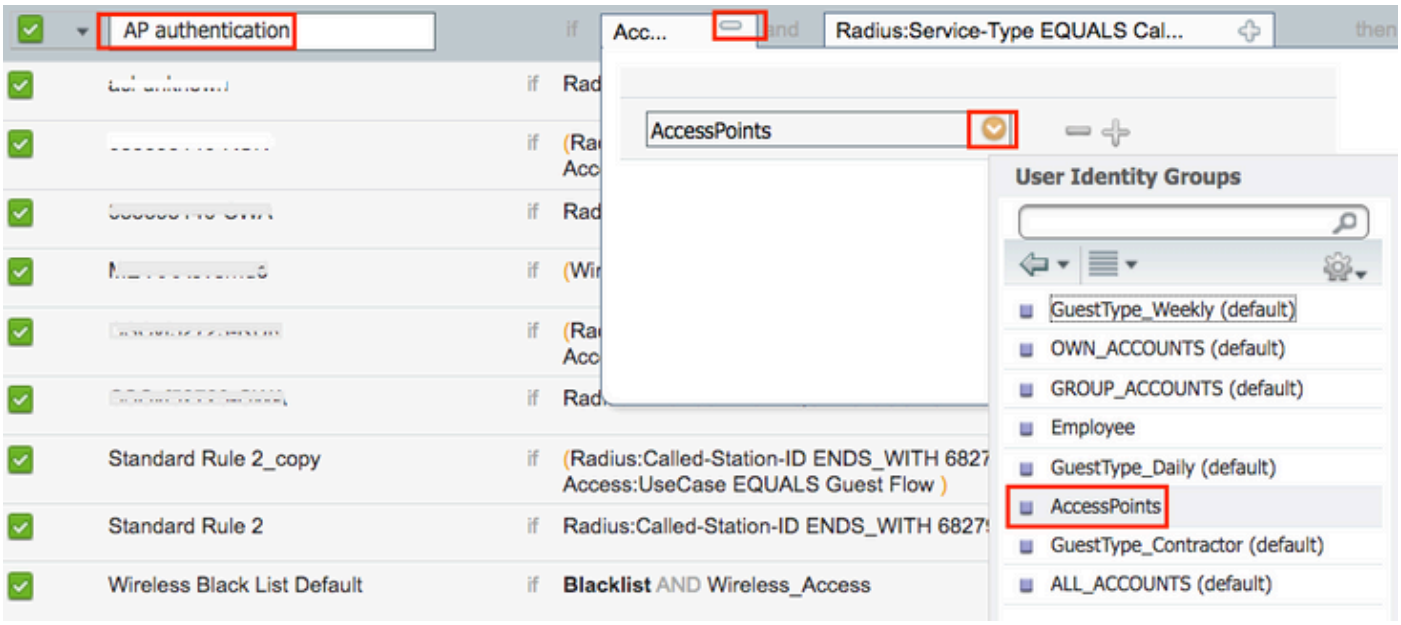
図に示すように、Policy > Authorizationの順に移動します。



図に示すように、新しいルールを挿入します。

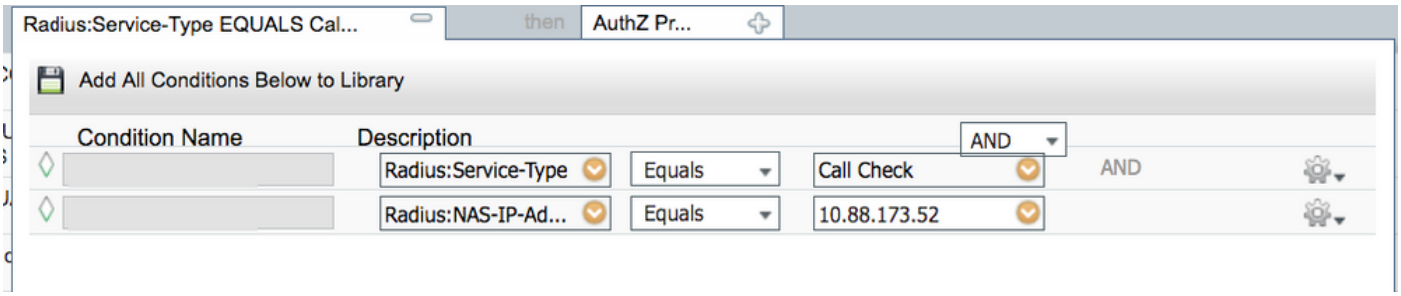


まず、ルールの名前と、アクセスポイント(AccessPoint)が保存されているIDグループ(AccessPoints)を選択します。 MACアドレスをユーザ名パスワードとして認証する場合はUser Identity Groupsを選択し、APのMACアドレスをエンドポイントとして認証する場合はEndpoint Identity Groupsを選択します。

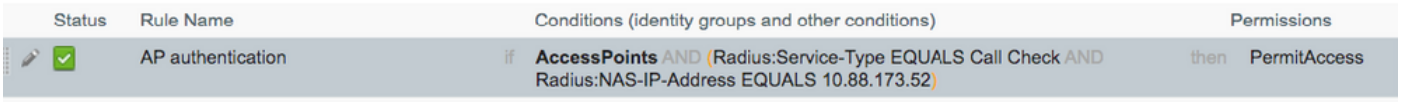


その後、認可プロセスを実行する他の条件を選択して、このルールに該当するようにします。この例では、認可プロセスがサービスタイプのコールチェックを使用し、認証要求がIPアドレス

10.88.173.52から送信される場合、このルールに該当します。



最後に、そのルールに一致するクライアントに割り当てられている認可プロファイルを選択し、Doneeをクリックして、図に示すように保存します。



注:コントローラにすでに参加しているAPの関連付けは失われません。ただし、許可リストが有効になった後でコントローラとの通信が失われ、再度参加しようとすると、認証プロセスが実行されます。それらのMACアドレスがローカルまたはRADIUSサーバにリストされていない場合は、コントローラに再度参加できません。

確認

9800 WLCでap認証リストが有効になっているかどうかを確認する

<#root>

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

RADIUS設定を確認します。

<#root>

```
#
```

```
show run aaa
```

トラブルシュート

WLC 9800には、常時接続のトレース機能があります。これにより、すべてのAP加入に関連するエラー、警告、通知レベルのメッセージが常にログに記録され、インシデントまたは障害状態が発生した後にログを表示できます。

注：生成されるログの量は、数時間から数日までさまざまです。

9800 WLCがデフォルトで収集したトレースを表示するには、次の手順でSSH/Telnet経由で9800 WLCに接続します（セッションをテキストファイルにログに記録していることを確認してください）。

ステップ 1：問題が発生した時点までのログを追跡できるように、コントローラの現在時刻を確認します。

```
# show clock
```

ステップ 2：システム設定に従って、コントローラバッファまたは外部syslogからsyslogを収集します。これにより、システムの正常性とエラー（発生している場合）をすぐに確認できます。

```
# show logging
```

ステップ 3：デバッグ条件が有効になっているかどうかを確認します。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Trace Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

注：条件が一覧表示されている場合は、有効な条件（MACアドレス、IPアドレスなど）に遭遇するすべてのプロセスについて、トレースがデバッグレベルでログに記録されていることを意味します。これにより、ログの量が増加します。したがって、デバッグが必要ないときは、すべての条件をクリアすることをお勧めします。

ステップ 4：テスト対象のMACアドレスがステップ3の条件としてリストされていないとすると

、特定の無線MACアドレスのalways-on notice levelトレースを収集します。

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

セッションで内容を表示するか、ファイルを外部 TFTP サーバーにコピーできます。

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件付きデバッグとラジオアクティブトレース

常時接続トレースで、調査中の問題のトリガーを判別するのに十分な情報が得られない場合は、条件付きデバッグを有効にしてRadio Active(RA)トレースをキャプチャできます。これにより、指定された条件（この場合はクライアントMACアドレス）と対話するすべてのプロセスにデバッグレベルのトレースが提供されます。

ステップ 5：デバッグ条件が有効になっていないことを確認します。

```
# clear platform condition all
```

手順 6：監視するワイヤレスクライアントのMACアドレスのデバッグ条件を有効にします。

このコマンドは、指定されたMACアドレスの監視を30分間（1800秒）開始します。必要に応じて、この時間を最大 2085978494 秒まで増やすことができます。

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

注:複数のクライアントを同時にモニタするには、MACアドレスごとにdebug wireless mac <aaaa.bbbb.cccc>コマンドを実行します。

注:すべてが後で表示できるように内部でバッファされるため、ターミナルセッションのクライアントアクティビティの出力は表示されません。

手順 7：監視する問題または動作を再現します。

ステップ 8：デフォルトまたは設定されたモニタ時間がアップする前に問題が再現した場合は、デバッグを停止します。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

モニター時間が経過するか、debug wireless が停止すると、9800 WLC では次の名前のローカルファイルが生成されます。

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

ステップ 9： MAC アドレスアクティビティのファイルを収集します。　ra trace.log を外部サーバーにコピーするか、出力を画面に直接表示できます。

RAトレースファイルの名前を確認します

```
# dir bootflash: | inc ra_trace
```

ファイルを外部サーバーにコピーします。

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

内容を表示します。

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

ステップ 10：根本原因がまだ明らかでない場合は、デバッグレベルの口グのより詳細なビューである内部口グを収集します。クライアントを再度デバッグする必要はありません。すでに収集され、内部に保存されているデバッグ口グをさらに詳しく調べるだけです。

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

注：このコマンド出力は、すべてのプロセスのすべての口グレベルのトレースを返し、非常に大量です。これらのトレースを解析する場合は、Cisco TAC にお問い合わせください。

---

ra-internal-FILENAME.txt を外部サーバーにコピーするか、出力を画面に直接表示できます。

ファイルを外部サーバーにコピーします。

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

内容を表示します。

```
# more bootflash:ra-internal-<FILENAME>.txt
```

ステップ 11デバッグ条件を削除します。

```
# clear platform condition all
```

注：トラブルシューティングセッションの後は、必ずデバッグ条件を削除してください。

参考資料

メッシュAPの9800 WLCへの加入

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。