

Catalyst 9800 ワイヤレスコントローラでの MAC 認証 SSID の設定

内容

[はじめに](#)

[前提条件](#)

[Requirement](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[9800 WLCでのAAAの設定](#)

[外部サーバによるクライアントの認証](#)

[クライアントのローカル認証](#)

[WLAN 設定](#)

[ポリシープロファイルの設定](#)

[ポリシータグの設定](#)

[ポリシータグの割り当て](#)

[ローカル認証用のMACアドレスをWLCにローカルで登録する](#)

[ISEエンドポイントデータベースのMACアドレスの入力](#)

[認証ルールの作成](#)

[許可ルールの作成](#)

[確認](#)

[トラブルシューティング](#)

[条件付きデバッグとラジオアクティブトレース](#)

はじめに

このドキュメントでは、Cisco Catalyst 9800 WLCでMAC認証セキュリティを使用してワイヤレスローカルエリアネットワーク(WLAN)を設定する方法について説明します。

前提条件

Requirement

次の項目に関する知識があることが推奨されます。

- MAC Address
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- アイデンティティサービスエンジン(ISE)

使用するコンポーネント

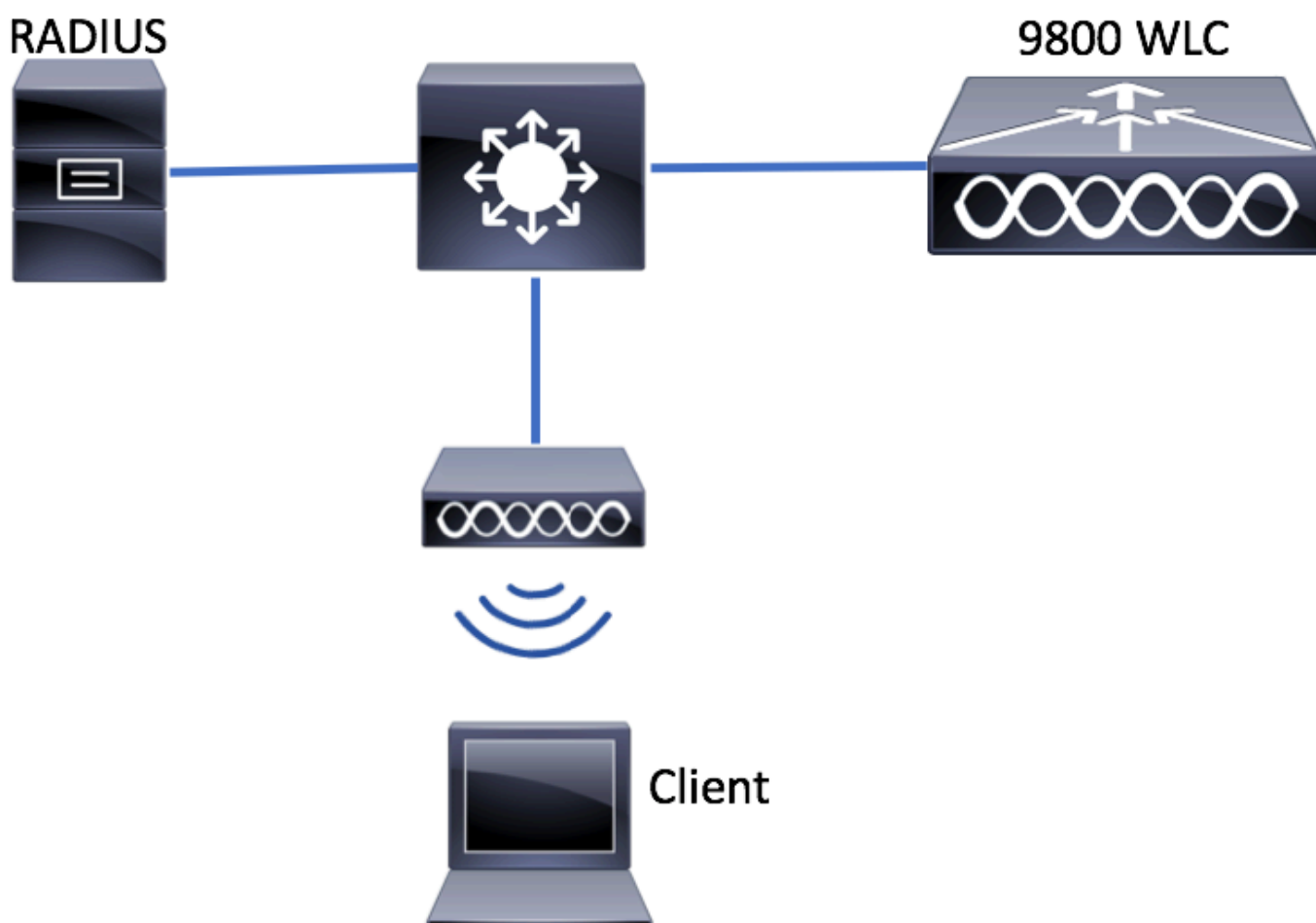
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS® XEジブラルタルv16.12
- 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



9800 WLC での AAA 設定

外部サーバによるクライアントの認証

GUI :

次のリンクから、「9800 WLCでのAAA設定」セクションのステップ1 ~ 3を読みます。

9800シリーズWLCでのAAAの設定

ステップ 4 : 認可ネットワーク方式を作成します。

に移動し Configuration > Security > AAA > AAA Method List > Authorization > + Add で作成します。

The screenshot shows the Cisco ISE configuration interface. On the left is a navigation menu with 'Configuration' highlighted. The main area is titled 'Authentication Authorization and Accounting'. Below the title is a '+ AAA Wizard' button. There are three tabs: 'AAA Method List' (highlighted with a red box), 'Servers / Groups', and 'AAA Advanced'. Under 'AAA Method List', there are sub-tabs for 'General', 'Authentication', and 'Authorization' (highlighted with a red box). A '+ Add' button (highlighted with a red box) and a 'Delete' button are visible. Below these is a table with columns 'Name' and 'Type'.

The screenshot shows the 'Quick Setup: AAA Authorization' dialog box. It has several input fields: 'Method List Name*' with the value 'AuthZ-method-name', 'Type*' with a dropdown set to 'network', and 'Group Type' with a dropdown set to 'group'. There is a 'Fallback to local' checkbox which is unchecked. Below are two lists: 'Available Server Groups' containing 'radius', 'ldap', and 'tacacs+', and 'Assigned Server Groups' containing 'ISE-KCG-grp'. At the bottom, there is a 'Cancel' button and a 'Save & Apply to Device' button (highlighted with a red box).

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 network <AuthZ-method-name> group <radius-grp-name>
```

クライアントのローカル認証

ローカル認証ネットワーク方式を作成します。

に移動し Configuration > Security > AAA > AAA Method List > Authorization > + Add で作成します。

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

+ Add x Delete

Name	Type
AuthZ-local	network

Quick Setup: AAA Authorization

Method List Name* AuthZ-local

Type* network

Group Type local

Available Server Groups Assigned Server Groups

radius
ldap
tacacs+
ISE-KCG-grp

Cancel Save & Apply to Device

CLI :

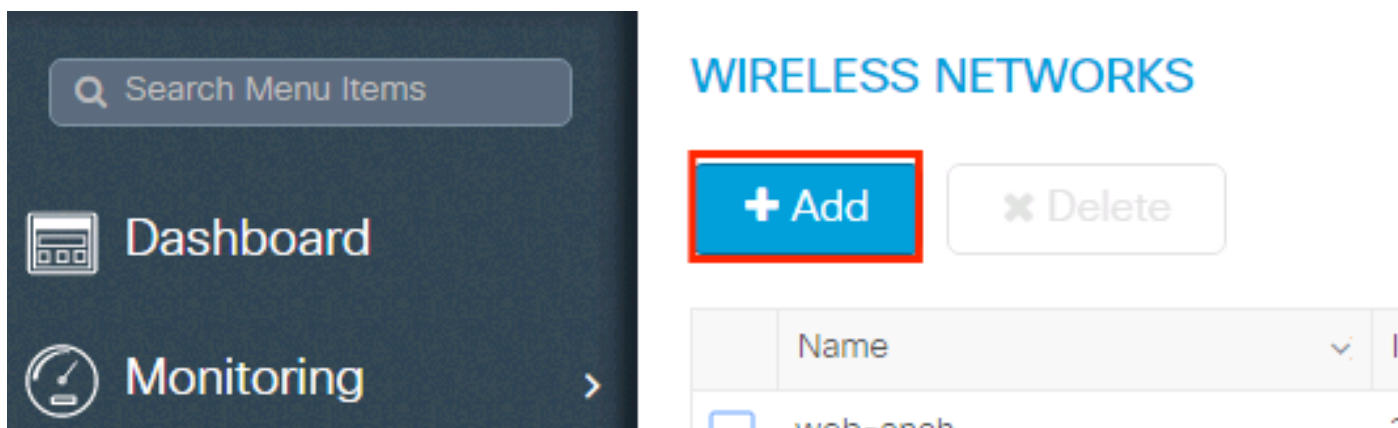
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

WLAN 設定

GUI :

ステップ 1 : WLANを作成します。

必要に応じ Configuration > Wireless > WLANs > + Add でネットワークに移動し、設定します。



ステップ 2 : WLAN情報を入力します。

Add WLAN ✕

General	Security	Advanced
Profile Name*	<input type="text" value="mac-auth"/>	Radio Policy <input type="text" value="All"/>
SSID	<input type="text" value="mac-auth"/>	Broadcast SSID <input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="3"/>	
Status	<input checked="" type="checkbox"/> ENABLED	

ステップ 3 : タ SecurityLayer 2 Security Mode プに移動し、無効および有効にMAC Filteringします。から Authorization List、 前の手順で作成した許可方式を選択します。次に、をクリックしSave & Apply to Deviceます。

Add WLAN ✕

General	Security	Advanced
	Layer2	Layer3
	Layer 2 Security Mode <input type="text" value="None"/>	Fast Transition <input type="text" value="Adaptive Enab..."/>
	MAC Filtering <input checked="" type="checkbox"/>	Over the DS <input checked="" type="checkbox"/>
	Authorization List* <input type="text" value="AuthZ-method-name"/>	Reassociation Timeout <input type="text" value="20"/>

CLI :

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

ポリシープロファイルの設定

SSIDごとのMACフィルタリングが正常に機能するようにaaa-override、ポリシープロファイルで有効にする必要があります。

[9800 WLCでのポリシープロファイルの設定](#)

ポリシータグの設定

[9800 WLCのポリシータグ](#)

ポリシータグの割り当て

[9800 WLCでのポリシータグの割り当て](#)

許可されたMACアドレスを登録します。

ローカル認証用のMACアドレスをWLCにローカルで登録する

に移動し Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add ます。


The screenshot displays the Cisco WLC configuration interface. On the left is a dark sidebar menu with options: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is titled 'Authentication Authorization and Accounting' and has a '+ AAA Wizard' button. Below this are tabs for 'AAA Method List', 'Servers / Groups', and 'AAA Advanced' (highlighted with a red box). Under 'AAA Advanced', there are sections for 'RADIUS Fallback', 'Attribute List Name', 'AP Authentication' (highlighted with a red box), 'AP Policy', and 'Password Policy'. The 'AP Authentication' section is expanded to show a table with columns 'MAC Address' and 'Serial Number'. A '+ Add' button (highlighted with a red box) and a 'x Delete' button are visible. The table contains two entries: 'aabbccddeeff' and 'e4b3187c3058'. At the bottom of the table, there is a pagination control showing '1' of 10 items per page.

MACアドレスを区切り文字なしで小文字で入力し、をクリックしSave & Apply to Device ます。

Quick Setup: MAC Filtering ✕

MAC Address*

Attribute List Name

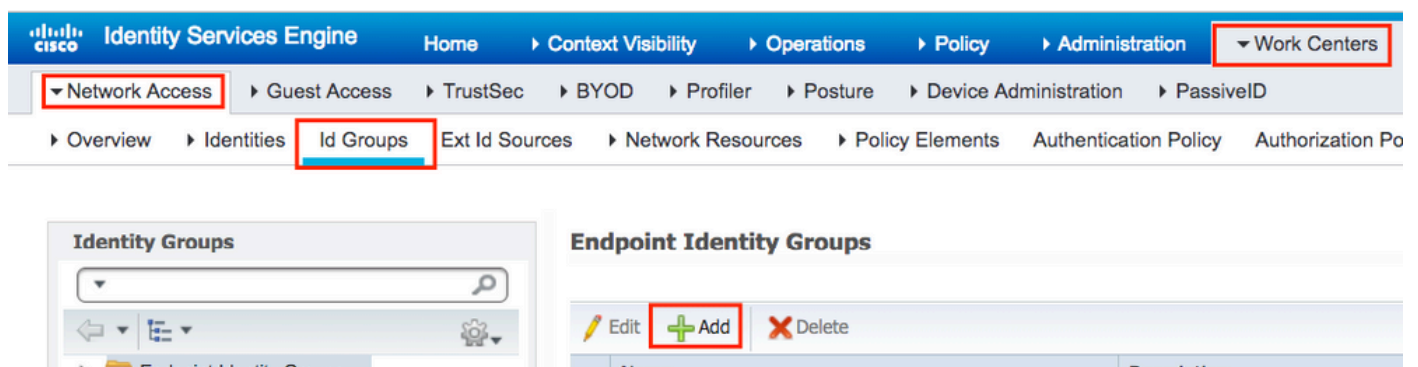
 注:17.3より前のバージョンでは、Web UIによって、図に示す「区切り文字なし」形式に入力したMAC形式が変更されていました。17.3以降のWeb UIでは、入力したデザインはすべて尊重されるため、区切り文字を入力しないことが重要です。機能強化のバグCisco Bug ID [CSCvv43870](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvv43870)では、MAC認証のためのいくつかの形式のサポートが追跡されています。

CLI :

```
# config t
# username <aabbccddeeff> mac
```

ISEエンドポイントデータベースのMACアドレスの入力

ステップ1: (オプション) 新しいエンドポイントグループを作成します。
に移動しWork Centers > Network Access > Id Groups > Endpoint Identity Groups > + Addます。



The screenshot shows the Cisco Identity Services Engine (ISE) Work Centers interface. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Work Centers, Network Access is selected, and Id Groups is highlighted. The Endpoint Identity Groups section is visible, showing an Add button with a green plus sign.

Identity Groups

Endpoint Identity Group List > **New Endpoint Group**

Endpoint Identity Group

* Name

Description

Parent Group

ステップ 2 : に移動し Work Centers > Network Access > Identities > Endpoints > +Add ます。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > **Work Centers**

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > **Identities** > Id Groups > Ext Id Sources > Network Resources > Policy Elements > Authentication Policy > Authorization Policy > Troubleshoot

Endpoints

Network Access Users
Identity Source Sequences

INACTIVE ENDPOINTS ⓘ

AUTHENTICATION STATUS ⓘ

No data available

Last Activity Date

Change Authorization Change Clear Threats & Vulnerabilities Export Import

Add Endpoint ✕

▼ General Attributes

Mac Address *

Description

Static Assignment

Policy Assignment

Static Group Assignment

Identity Group Assignment

ISE 設定

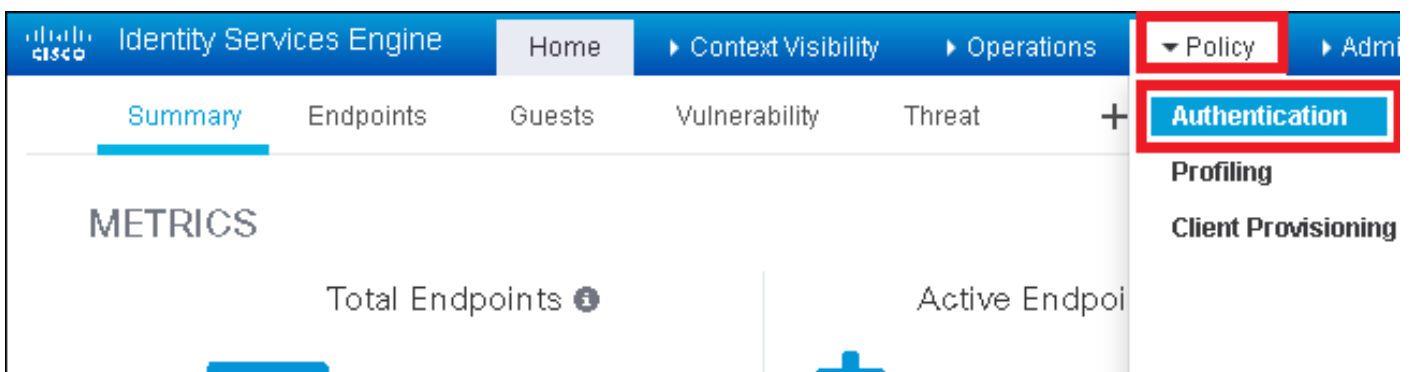
9800 WLC の ISE への追加.

このリンクの手順「[WLCからISEへの宣言](#)」をお読みください。

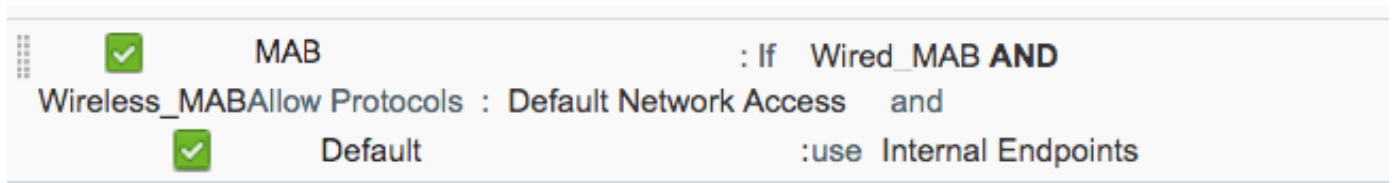
認証ルールの作成

認証ルールはユーザのクレデンシャルが正しいか検証 (ユーザ本当に本人かどうかの確認) し、それに使用する許可されている認証方法を制限するのに使用されます。

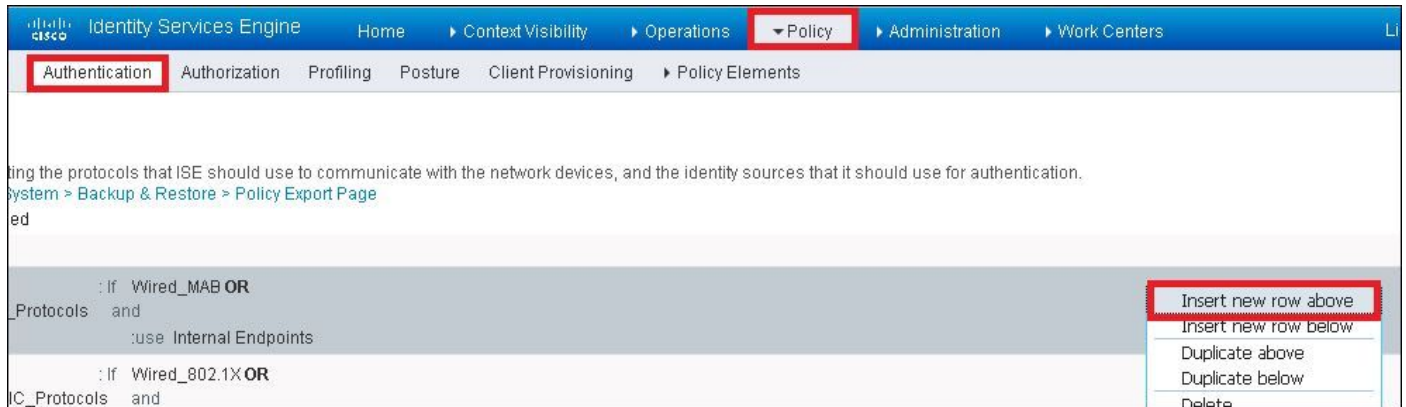
ステップ 1 : 図に示Policy > Authentication するように、に移動します。
デフォルトのMABルールがISEに存在することを確認します。



ステップ 2 : MABのデフォルトの認証ルールがすでに存在することを確認します。



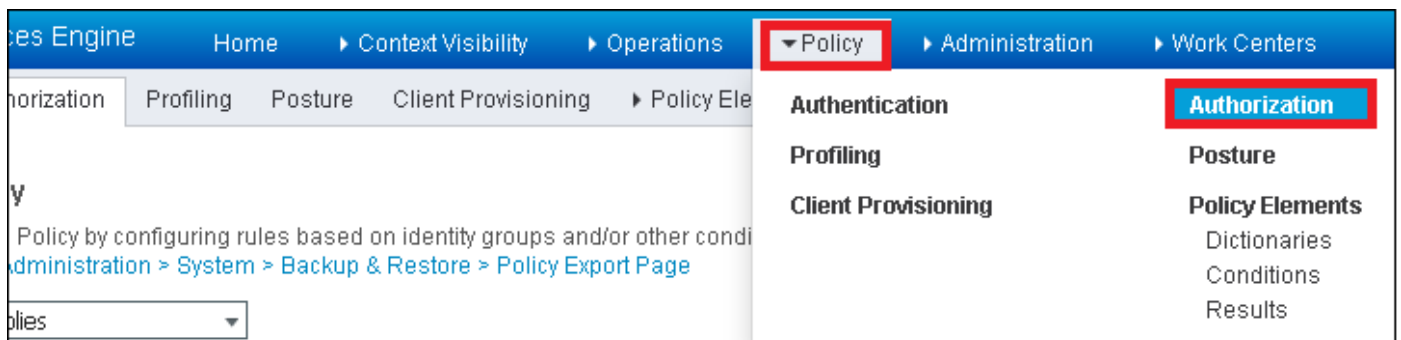
そうでない場合は、をクリックすると新しいファイルを追加でき Insert new row above ます。



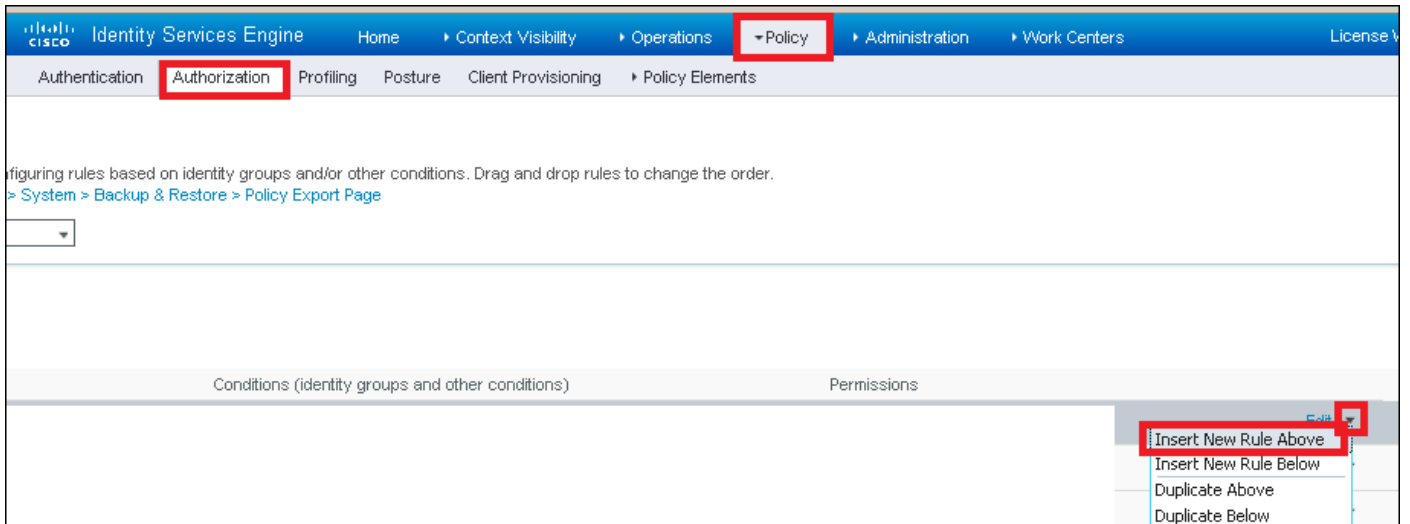
許可ルールの作成

許可ルールは、クライアントに適用される許可（認証プロファイル）の結果を決定するためのものです。

ステップ 1：図に示Policy > Authorization すように、に移動します。

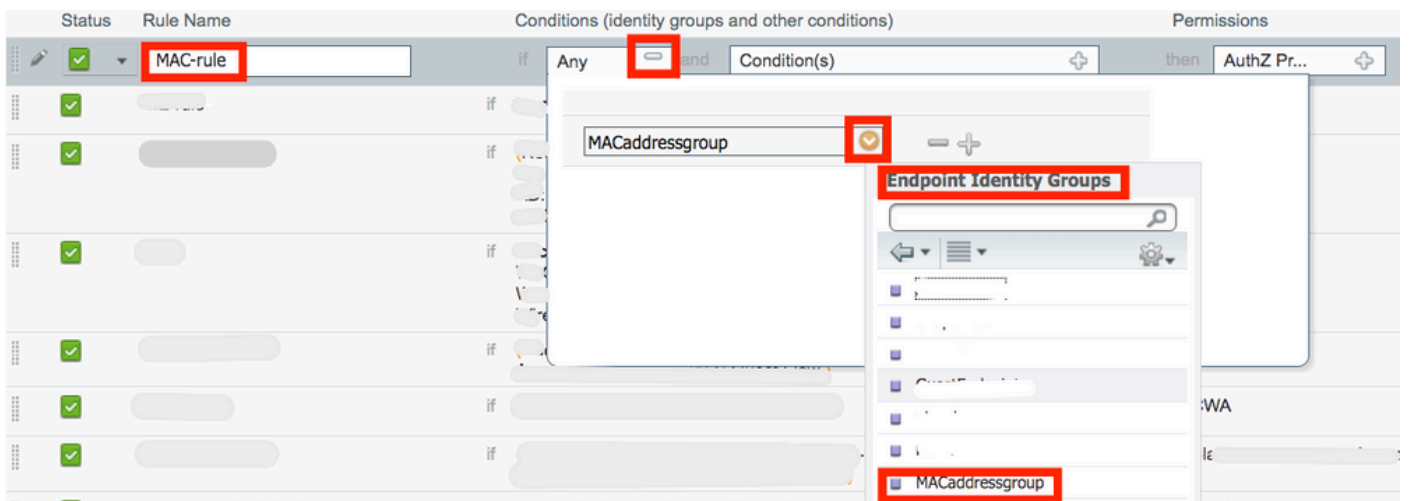


ステップ 2：図に示すように、新しいルールを挿入します。

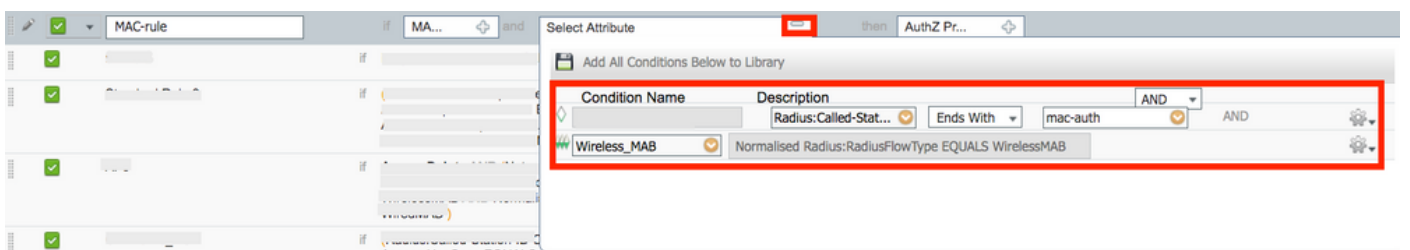


ステップ 3：値を入力します。

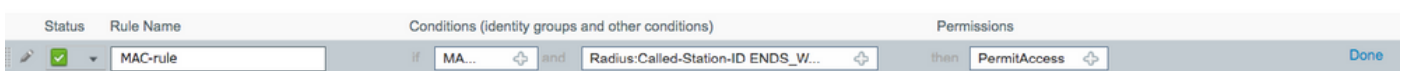
まず、図に示すように、ルールの名前とエンドポイントが保存されているIDグループ (MACaddressgroup) を選択します。



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分類します。この例では、図に示すように、認可プロセスでワイヤレスMABが使用され、着信側ステーションID (SSIDの名前) が mac-auth で終わる場合、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る PermitAccess 認可プロファイルを選択します。をクリックし Done で保存します。




確認

次のコマンドを使用して、現在の設定を確認できます。

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

トラブルシューティング

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、クライアント接続に関連するすべてのエラー、警告、および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によって異なりますが、数時間から数日に戻ることができます。

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

ステップ 1：コントローラの現在の時刻を確認して、ログをその時刻から問題が発生した時刻まで追跡できるようにします。

```
# 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、システムの状態とエラーを簡単に確認できます。

```
# 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 Tracing 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、アクティブにデバッグを行っていない場合は、すべての条件をクリアすることを推奨します。

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場合は、特定の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。条件付きデバッグを有効にするには、次の手順を参照してください。


ステップ 5：有効なデバッグ条件が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。

次のコマンドは、指定された MAC アドレスの 30 分間（1800 秒）のモニターを開始します。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ーするには、MACアドレスごとにdebug wireless mac コマンドを実行します。

 注:すべての内容は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ー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、ワイヤレスのデバッグが停止すると、9800 WLCは次の名前のローカ

ルファイルを生成します。 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。 を外部サーバra trace .log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、デバッグレベルのログのより詳細なビューである内部ログを収集します。すでに収集されて内部に保存されているデバッグログをさらに詳しく調べるだけなので、クライアントを再度デバッグする必要はありません。

```
# 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ログレベルのトレースを返し、非常に大量です。これらのトレースの解析をCisco TACに依頼してください。

を外部サーバにコピーするか ra-internal-FILENAME.txt、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。

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。