

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](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[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](#)

[MAC AP認証リスト : 外部RADIUSサーバ](#)

[9800 WLCの設定](#)

[ISEの設定](#)

[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](#)

[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](#)

[APを認証する認可ポリシー](#)

[確認](#)

[トラブルシューティング](#)

[参考資料](#)

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

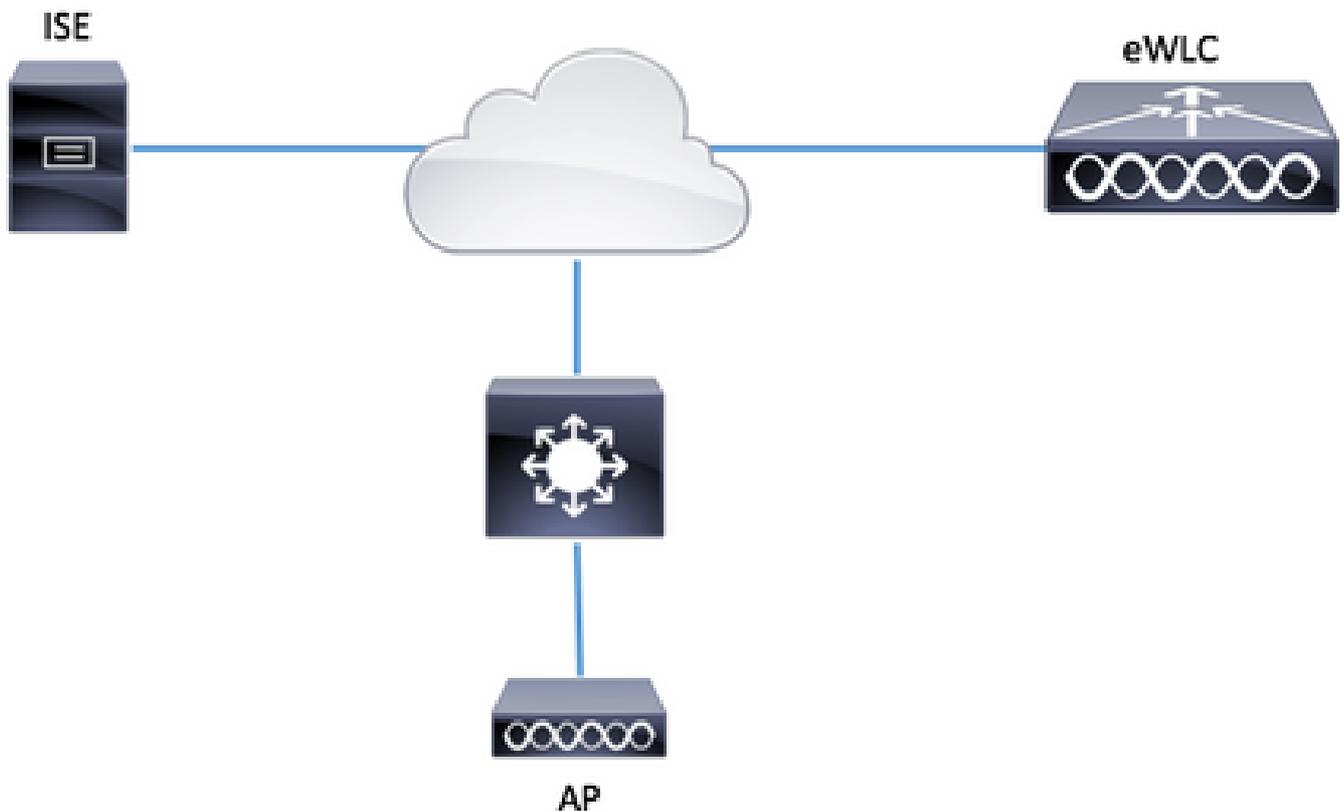
AP 1700

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。

The screenshot shows the Cisco configuration interface. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is titled "Authentication Authorization and Accounting" and contains a "+ AAA Wizard" button. Below this are three tabs: "AAA Method List" (highlighted with a red box), "Servers / Groups", and "AAA Advanced". Under the "AAA Method List" tab, there are sub-sections: "General", "Authentication", "Authorization" (highlighted with a red box), and "Accounting". To the right of the "Authorization" section is a "+ Add" button (highlighted with a red box) and a "x Delete" button. Below these buttons is a table with two columns: "Name" and "Type".

Name	Type
<input type="checkbox"/> default	network
<input type="checkbox"/> AuthZ-Netw-ISE	network

The screenshot shows the "Quick Setup: AAA Authorization" dialog box. It has a title bar with a close button (X). The form contains the following fields:

- Method List Name*: AP-auth
- Type*: credential-download
- Group Type: local

Below these fields are two sections: "Available Server Groups" and "Assigned Server Groups".

Available Server Groups: radius, ldap, tacacs+, ISE-KCG-grp, ISE-grp-name

Assigned Server Groups: (empty)

At the bottom, there are two buttons: "Cancel" and "Save & Apply to Device".

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。

+ AAA Wizard

AAA Method List Servers / Groups **AAA Advanced**

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC **ENABLED**

Authorize APs against Serial Number **DISABLED**

Authorization Method List

Apply to Device

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

Configuration > **Security** > **AAA**

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

AP Policy

Password Policy

AAA Interface

MAC Address Serial Number

+ Add **× Delete**

MAC Address

◀ ◁ 0 ▷ ▶ 10 items per page

Quick Setup: MAC Filtering ✕

MAC Address*

Attribute List Name

Cancel **Save & Apply to Device**

 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xxxxxxxxxxxxx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xxxxxxxxxxxxx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

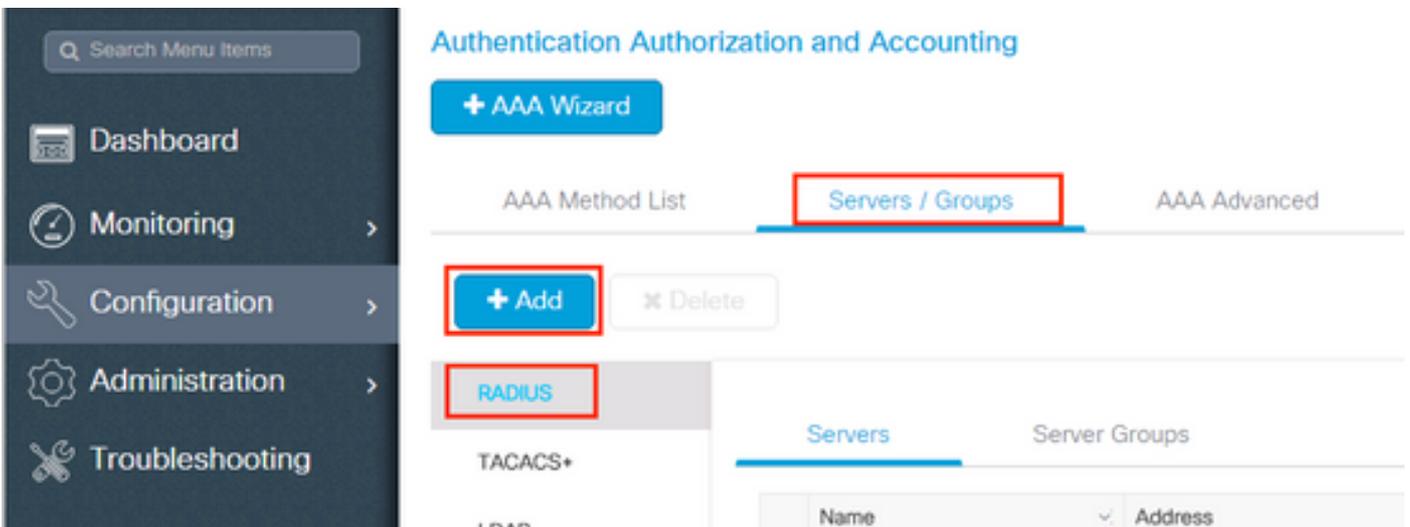
許可されたAPのMACアドレスは、外部RADIUSサーバ (この例ではISE) に保存されます。

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。



The screenshot displays the Cisco WLC GUI for 'Authentication Authorization and Accounting'. The left sidebar shows navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area shows the configuration path: AAA Method List, Servers / Groups (highlighted with a red box), and AAA Advanced. Below this, there are '+ Add' and 'Delete' buttons, with '+ Add' highlighted by a red box. Under the '+ Add' button, 'RADIUS' is selected and highlighted with a red box. The 'Servers' tab is active, showing a table with columns for Name and Address.

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。

Create AAA Radius Server ✕

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

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。

Create AAA Radius Server Group



Name*	<input type="text" value="ISE-grp-name"/>
Group Type	<input type="text" value="RADIUS"/>
MAC-Delimiter	<input type="text" value="none"/>
MAC-Filtering	<input type="text" value="none"/>
Dead-Time (mins)	<input type="text" value="1-1440"/>
Available Servers	<input type="text"/>
	<input type="button" value=">"/>
	<input type="button" value="<"/>
	Assigned Servers
	<input type="text" value="ISE-iccg"/>

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、

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers Assigned Servers

ISE-KCG

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。

Search Menu Items

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

Authentication Authorization and Accounting

[+ AAA Wizard](#)

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

[+ Add](#) [x Delete](#)

	Name	Type
<input type="checkbox"/>	default	network
<input type="checkbox"/>	AuthZ-Netw-ISE	network

Quick Setup: AAA Authorization ✕

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

radius
 ldap
 tacacs+
 ISE-KCG-grp

Assigned Server Groups

ISE-grp-name

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。

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List
Servers / Groups
AAA Advanced

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED

Authorize APs against Serial Number DISABLED

Authorization Method List

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ISEの設定](#)

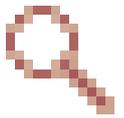
[MACアドレスをユーザ名/パスワードとして認証するようにISEを設定する](#)

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。



* Name

Description

Icon



[Change icon...](#)

[Set To Default](#)



Vendor

Supported Protocols

- RADIUS
- TACACS+
- TrustSec

RADIUS Dictionaries

Templates

[Expand All](#) / [Collapse All](#)

Authentication/Authorization

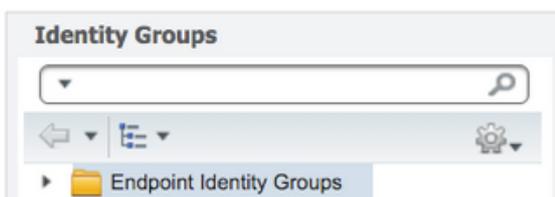
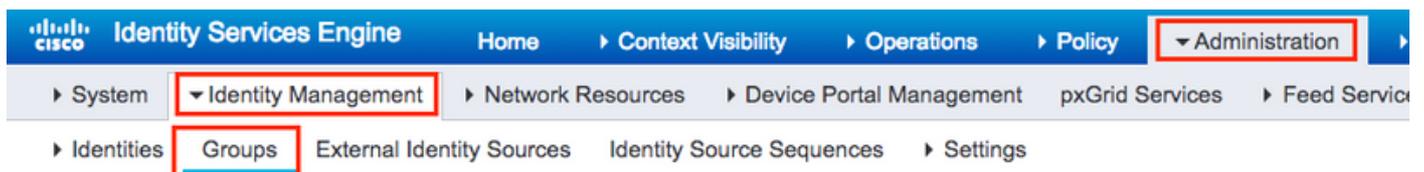
Flow Type Conditions

Wired MAB detected if the following condition(s) are met :

⋮ ⌵ = ⌵

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

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



Endpoint Identity Groups

Edit **Add** Delete

Name	Description
------	-------------

名前を選択して、Submitをクリックします。

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

Endpoint Identity Group

* Name

Description

Parent Group

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Identities > Endpoints. The 'Endpoints' section is active, showing a bar chart titled 'INACTIVE ENDPOINTS' with a value of 1. The x-axis is labeled 'Last Activity Date' and shows a date of 8/27. The y-axis ranges from 0 to 1. To the right, there is a section for 'AUTHENTICATED' endpoints, with a note 'disconnected: [1009]'. At the bottom, there is a table with columns for 'MAC Address', 'Status', 'IPv4 Address', and 'Username'. A red box highlights the '+' icon in the table's toolbar.

必要な情報を入力します。

Add Endpoint ✕

▼ General Attributes

Mac Address * 00:B0:E1:8C:49:E8

Description Access Point

Static Assignment

Policy Assignment Unknown

Static Group Assignment

Identity Group Assignment AccessPoints

Cancel

Save

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。

Identity Services Engine Home Context Visibility Operations Policy Administration

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identifier for Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MABAllow Protocols	: Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1XAllow Protocols	: Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

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

Identity Source Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Description	Identity
<input type="checkbox"/>	All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preload
<input type="checkbox"/>	Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Request APIs	Internal
<input type="checkbox"/>	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal
<input type="checkbox"/>	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal
<input type="checkbox"/>	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal

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。

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
<input type="text" value="Internal Endpoints"/>	<input type="button" value=">"/>	<input type="text" value="Internal Users"/> <input type="text" value="All_AD_Join_Points"/> <input type="text" value="Guest Users"/>
	<input type="button" value="<"/>	<input type="button" value="↑"/>
	<input type="button" value="⇒"/>	<input type="button" value="^"/>
	<input type="button" value="⇐"/>	<input type="button" value="v"/>
		<input type="button" value="⇩"/>

▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

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。

Identity Groups

User Identity Groups

Actions: Edit, Add, Delete, Import, Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_

名前を選択して、Submitをクリックします。

User Identity Groups > New User Identity Group

Identity Group

* Name

Description

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。

Identity Services Engine Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

User Custom Attributes

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Password Policy Account Disable Policy

Password Policy

* Minimum Length: 4 characters (Valid Range 4 to 127)

Password must not contain:

- User name or its characters in reverse order
- "cisco" or its characters in reverse order
- This word or its characters in reverse order:
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ?

Default Dictionary ?

Custom Dictionary ? No file chosen

The newly added custom dictionary file will replace the existing custom dictionary file.

Password must contain at least one character of each of the selected types:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- * Password must be different from the previous 3 versions (Valid Range 1 to 10)
- Password change delta 3 characters (Valid Range 3 to 10)
- * Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

Users can be required to periodically change password

- Disable user account after 60 days if password was not changed (valid range 1 to 3650)
- Display reminder 30 days prior to password expiration (valid range 1 to 3650)
- Lock/Suspend Account with Incorrect Login Attempts

- * # 3 (Valid Range 3 to 20)
- Suspend account for 15 minutes (Valid Range 15 to 1440) Disable account

 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。

CISCO Identity Services Engine Home > Context Visibility > Operations > Policy > Administration

> System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Services

> Identities Groups External Identity Sources Identity Source Sequences > Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit + Add Change Status Import Export Delete

Status	Name	Description	First N
--------	------	-------------	---------

必要な情報を入力します。

▼ Network Access User

* Name

Status Enabled ▼

Email

▼ Passwords

Password Type: ▼

Password

Re-Enter Password

* Login Password

ⓘ

Enable Password

ⓘ

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

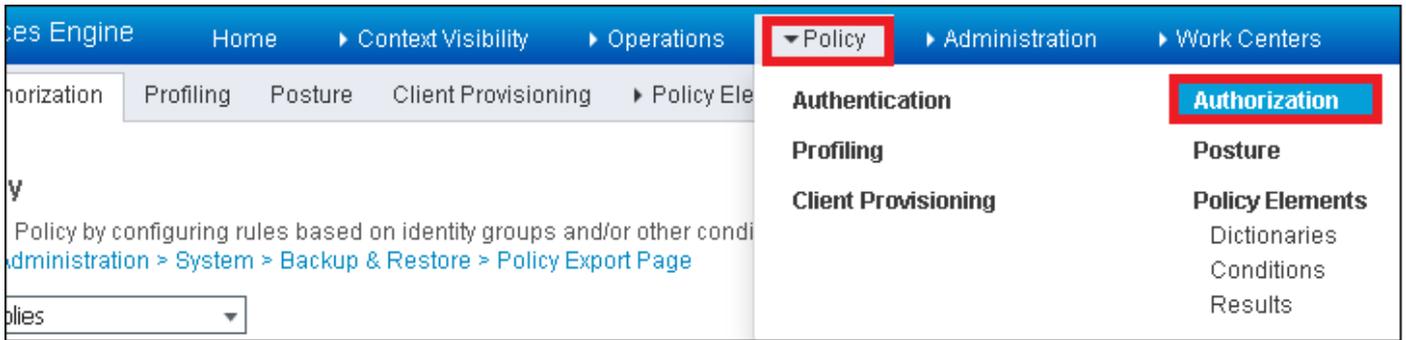
▼ User Groups

- +

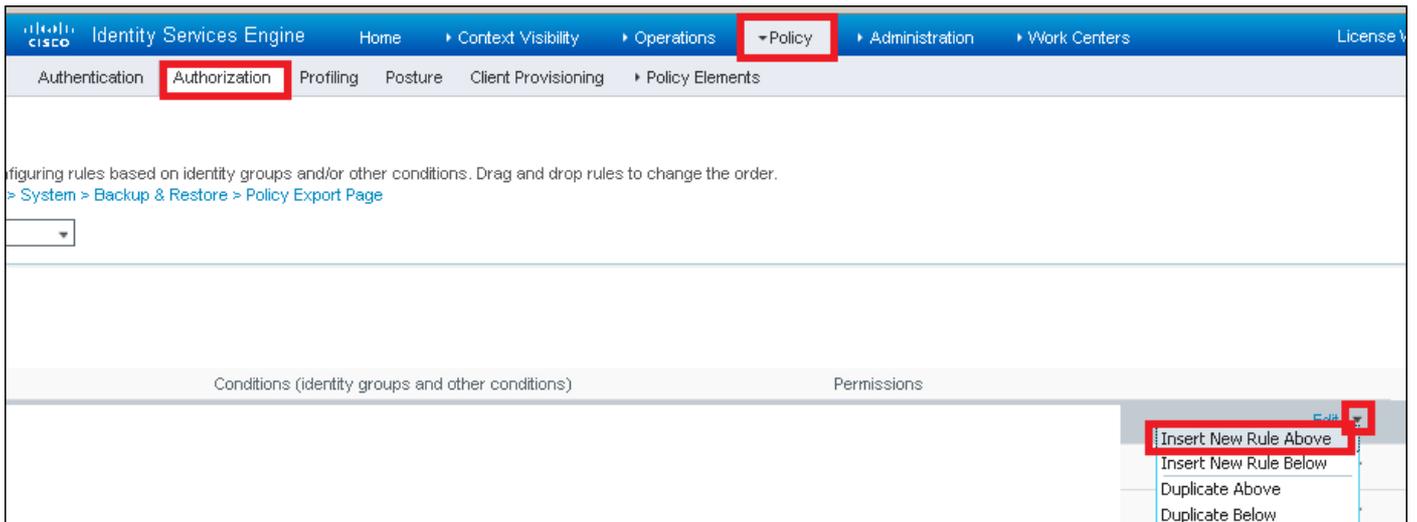
 注:NameおよびLogin Passwordフィールドは、APのイーサネットMACアドレスで、すべて小文字で区切り文字を使用しない必要があります。

APを認証する認可ポリシー

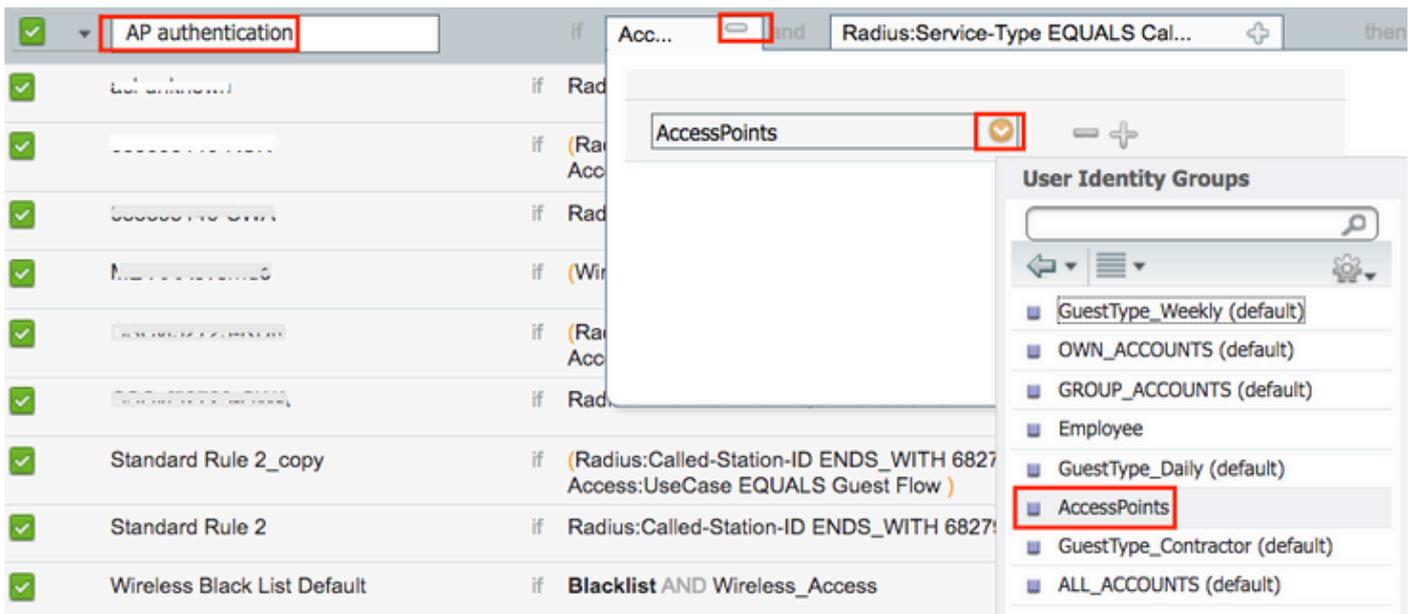
図に示すように、Policy > Authorizationの順に移動します。



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。

Condition Name	Description	Operator	Value	Logic
	Radius:Service-Type	Equals	Call Check	AND
	Radius:NAS-IP-Ad...	Equals	10.88.173.52	

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。

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	AP authentication	if AccessPoints AND (Radius:Service-Type EQUALS Call Check AND Radius:NAS-IP-Address EQUALS 10.88.173.52)	then PermitAccess

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、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、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、デバッグが不要なときは、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、デバッグレベルのログのより詳細なビューである内部ログを収集します。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ロ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。