

Catalyst 9800 WLCおよびISEでの中央Web認証(CWA)の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[9800 WLC での AAA 設定](#)

[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](#)

[リダイレクト ACL 設定](#)

[HTTPまたはHTTPSのリダイレクトを有効にする](#)

[ISE 設定](#)

[9800 WLC の ISE への追加](#)

[ISE での新しいユーザの作成](#)

[認証プロファイルの作成](#)

[認証ルール \(Authentication Rule \) の設定](#)

[許可ルール \(Authorization Rule \) の設定](#)

[FlexConnect ローカル スイッチング アクセス ポイントのみ](#)

[証明書](#)

[確認](#)

[トラブルシューティング](#)

[Checklist](#)

[RADIUSのサービスポートサポート](#)

[デバッグの収集](#)

[例](#)

はじめに

このドキュメントでは、Catalyst 9800 WLCおよびISEでCWAワイヤレスLAN(WLAN)を設定する方法について説明します。

前提条件

要件

9800ワイヤレスLANコントローラ(WLC)の設定に関する知識があることが推奨されます。

使用するコンポーネント

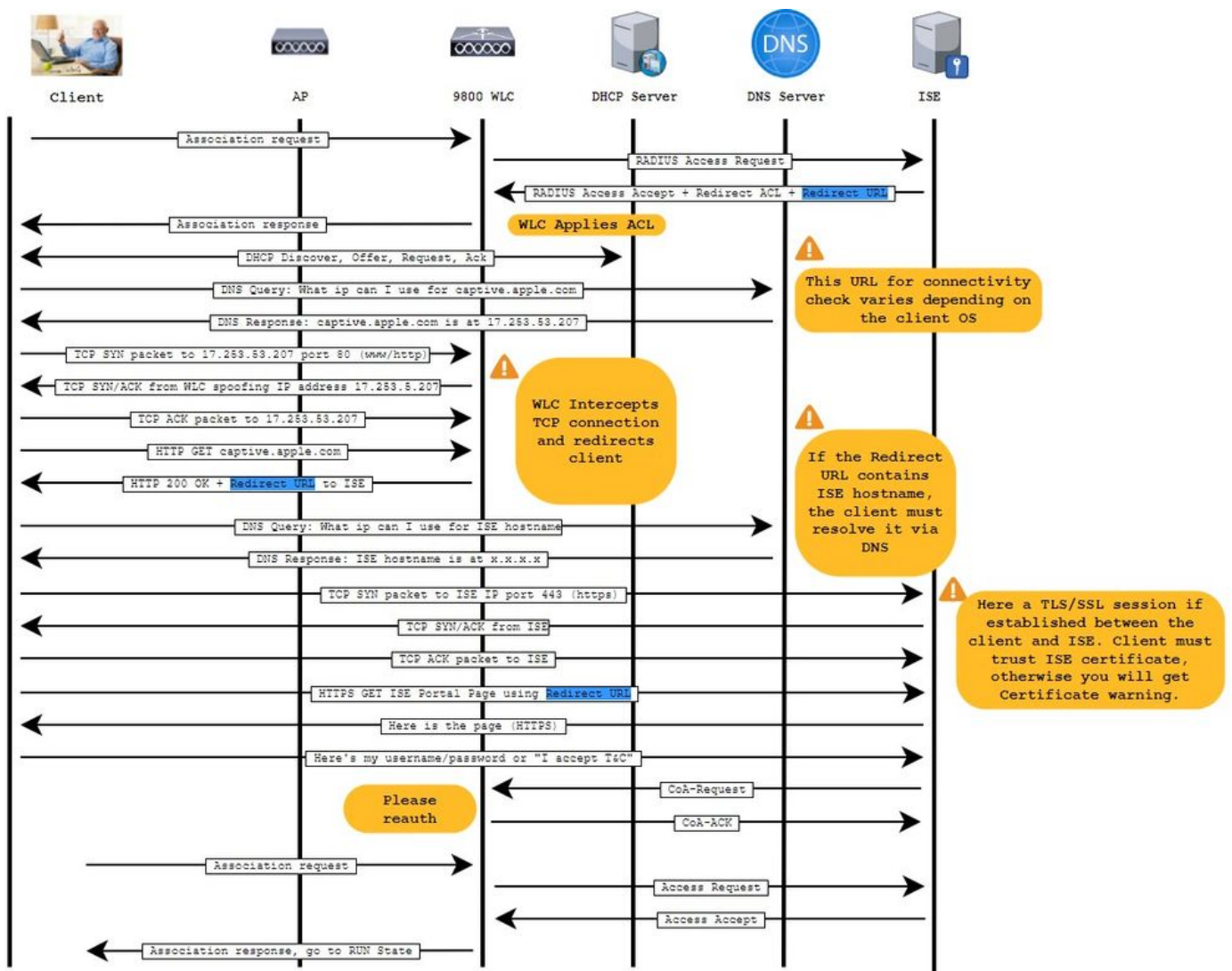
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9800 WLC Cisco IOS® XEジブラルタルv17.6.x
- Identity Service Engine(ISE)v3.0

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。

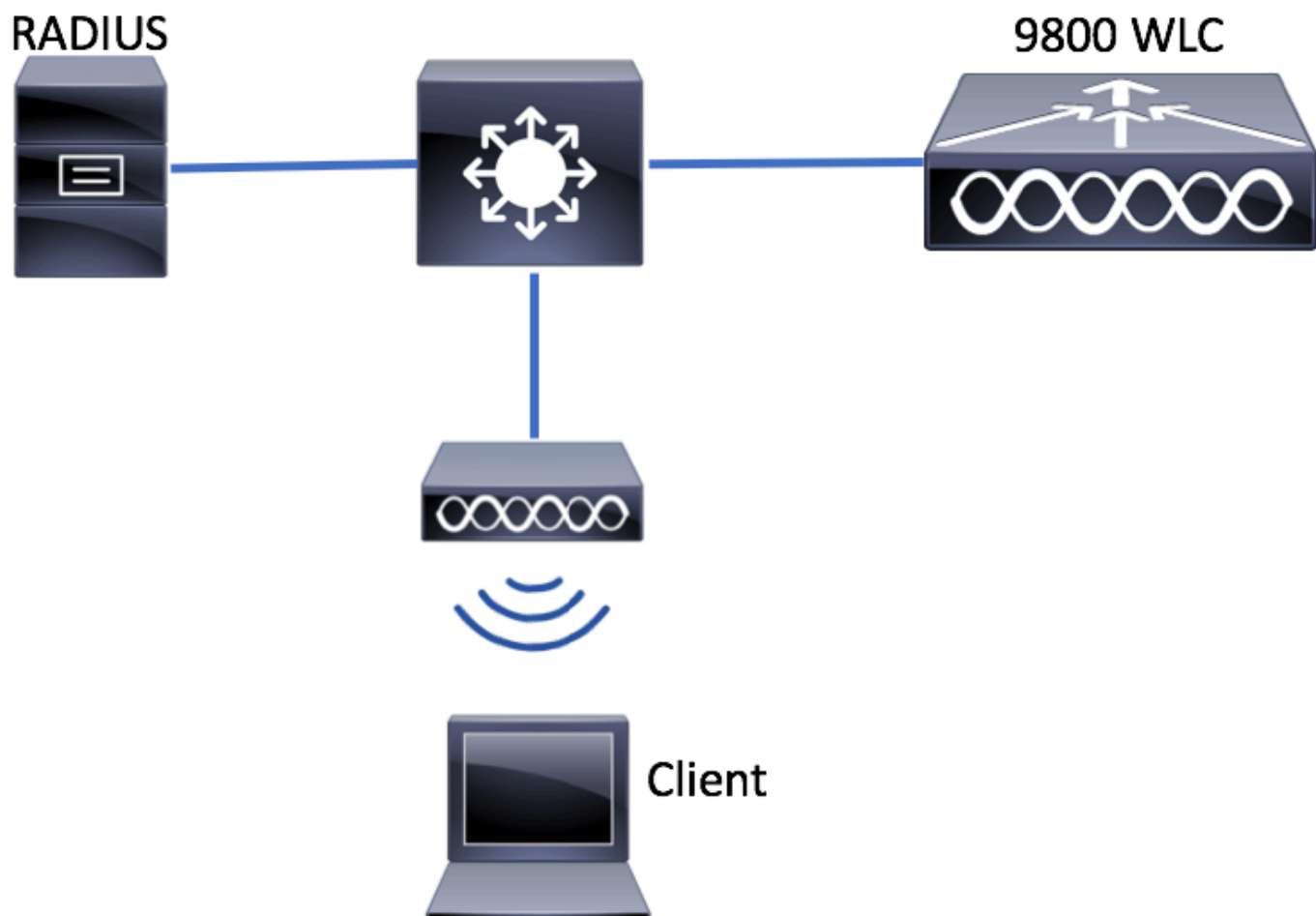
背景説明

CWAプロセスを次に示します。ここでは、例としてAppleデバイスのCWAプロセスを示します。



設定

ネットワーク図



9800 WLC での AAA 設定

ステップ 1 : ISEサーバを9800 WLC設定に追加します。

図に示すように、 Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add に移動し、RADIUSサーバ情報を入力します。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Address
0 items per page	

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* ISE-server

Server Address* [Redacted]

PAC Key

Key Type Clear Text

Key* [Redacted]

Confirm Key* [Redacted]

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

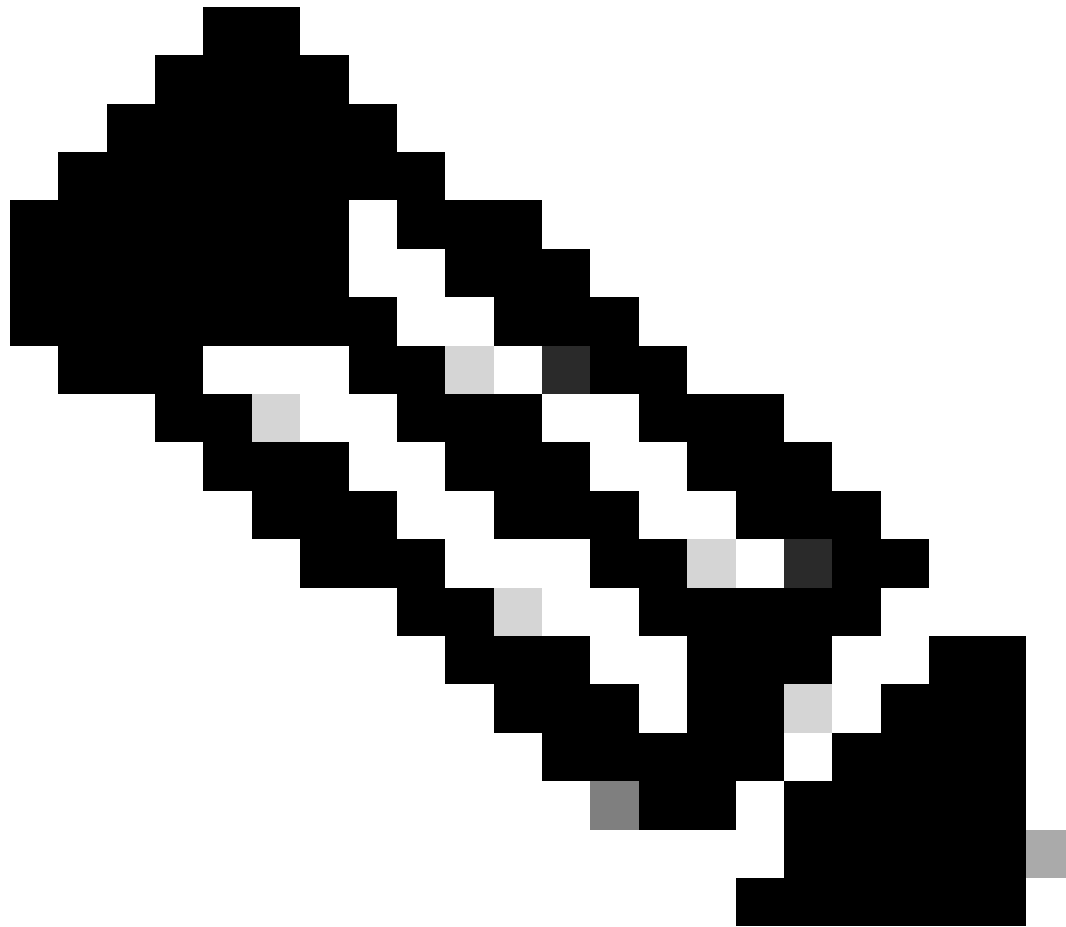
CoA Server Key Type Clear Text

CoA Server Key [Redacted]

Confirm CoA Server Key [Redacted]

Automate Tester

Cancel Apply to Device



注：バージョン17.4.X以降では、RADIUSサーバを設定する際にCoAサーバキーも設定するようにしてください。共有秘密と同じキーを使用します（ISEのデフォルトでは同じです）。RADIUSサーバで設定されている場合は、共有秘密キーとは異なるキーをCoAにオプションで設定することを目的としています。Cisco IOS XE 17.3では、Web UIは単にCoAキーと同じ共有秘密を使用していました。

ステップ 2：許可方式リストを作成します。

図に示すように、Configuration > Security > AAA > AAA Method List > Authorization > + Add に移動します。

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

+ Add x Delete

Name	Type	Group Type	Group
<input type="checkbox"/> default	network	local	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Fallback to local

Authenticated

Available Server Groups

ldap
tacacs+

Assigned Server Groups

radius

ステップ3: (オプション) 図に示すように、アカウント方式リストを作成します。

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups

Assigned Server Groups

注：Cisco Bug ID [CSCvh03827](#)が原因で、（Cisco IOS XE CLI設定から）RADIUSサーバのロードバランシングを行う場合は、CWAは機能しません。外部ロードバランサの使用は問題ありません。ただし、calling-station-id RADIUS属性を使用して、ロードバランサがクライアントごとに動作することを確認してください。UDP送信元ポートに依存するメカニズムは、9800からのRADIUS要求のバランシングではサポートされていません。

ステップ4: (オプション) AAAポリシーを定義して、SSID名をCalled-station-id属性として送信できます。これは、後でプロセスでこの条件をISEで使用する場合に便利です。

Configuration > Security > Wireless AAA Policyに移動し、デフォルトのAAAポリシーを編集するか、新しいポリシーを作成します。

Configuration > Security > Wireless AAA Policy

+ Add × Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

1 10 items per page

Dashboard
Monitoring
Configuration
Administration
Troubleshooting

オプション1としてSSIDを選択できます。SSIDのみを選択した場合でも、着信側ステーションIDはSSID名にAP MACアドレスを付加することに注意してください。

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

Option 1

SSID

Option 2

Not Configured

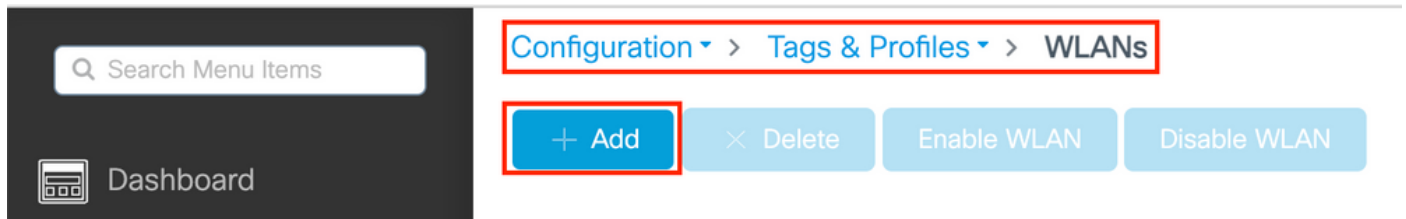
Option 3

Not Configured

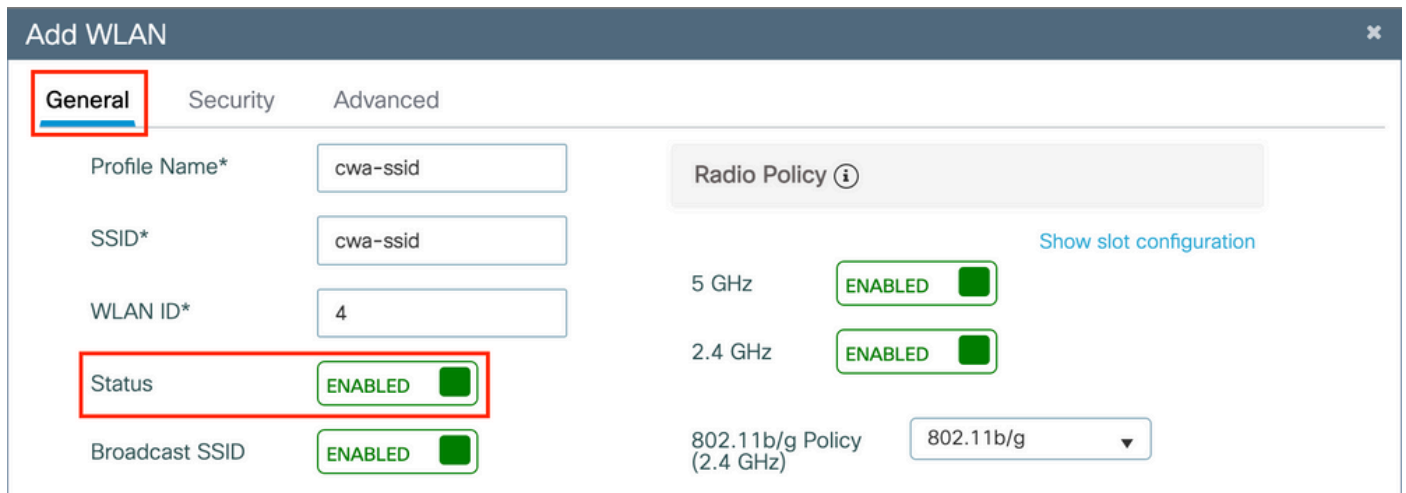
WLAN 設定

ステップ 1 : WLANを作成します。

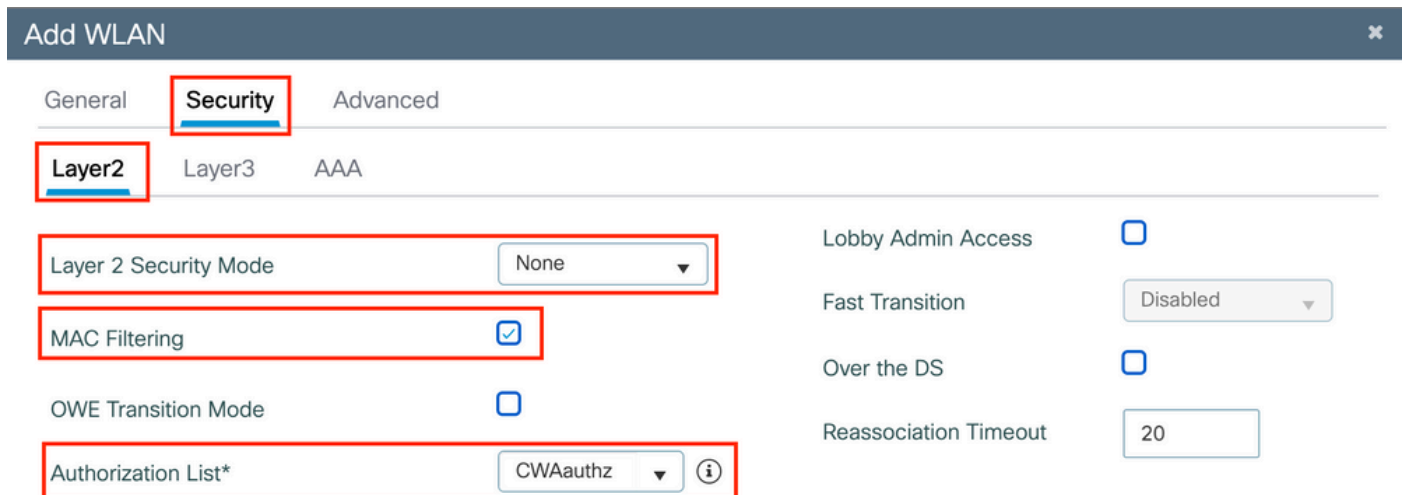
必要に応じてネットワークに移動 Configuration > Tags & Profiles > WLANs > + Add し、設定します。



ステップ 2 : WLANの一般情報を入力します。



ステップ 3 : Security タブに移動し、必要なセキュリティ方式を選択します。この場合、「MACフィルタリング」と(AAA Configuration セクションのステップ2で作成した)AAA許可リストだけが必要です。



CLI :

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
```

```
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

ポリシープロファイルの設定

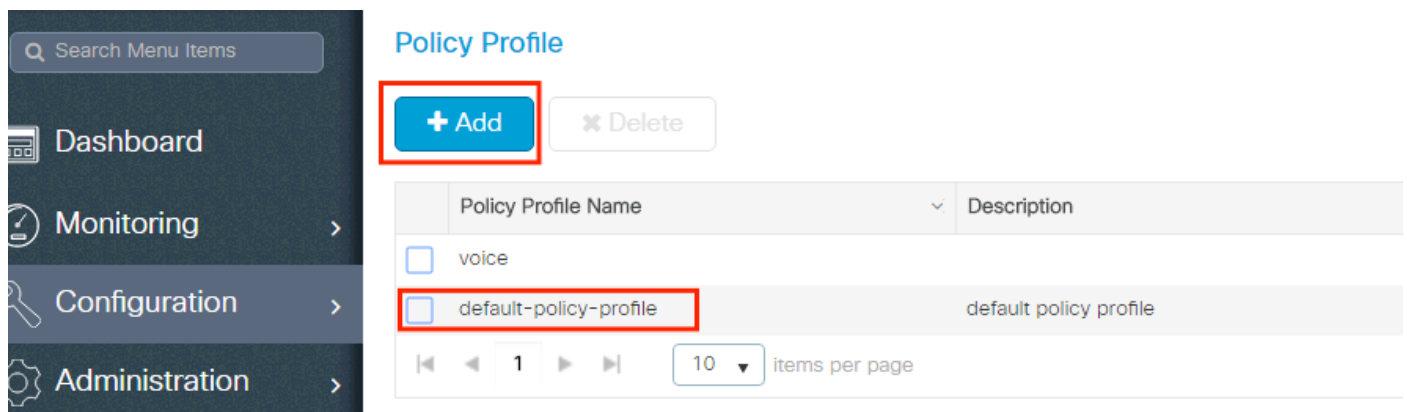
ポリシープロファイル内で、特にアクセスコントロールリスト(ACL)、Quality of Service(QoS)、モビリティアンカー、タイマーなどの設定に対して、VLANを割り当てるクライアントを決定できます。

デフォルトのポリシープロファイルを使用することも、新規に作成することもできます。

GUI :

ステップ 1 : 新しいPolicy Profileを作成します。

に移動 Configuration > Tags & Profiles > Policy し、を設定するか、新しいdefault-policy-profile を作成します。



The screenshot shows the 'Policy Profile' configuration page. On the left is a sidebar with 'Configuration' selected. The main area has a title 'Policy Profile' and two buttons: '+ Add' (highlighted with a red box) and 'Delete'. Below is a table with two columns: 'Policy Profile Name' and 'Description'. The table contains two entries: 'voice' and 'default-policy-profile' (highlighted with a red box). At the bottom, there is a pagination control showing '1' items per page and a dropdown for '10 items per page'.

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

プロファイルを有効にします。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

ステップ 2 : VLANを選択します。

Access Policies タブに移動し、ドロップダウンからVLAN名を選択するか、VLAN-IDを手動で入力します。ポリシープロファイルで ACL を設定しないでください。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

ステップ 3 : ISEオーバーライド (AAAオーバーライドを許可) および認可変更(CoA) (NAC状態) を受け入れるようにポリシープロファイルを設定します。必要に応じて、アカウントリング方法も指定できます。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="CWAacct"/> ⓘ ✕

WGB Parameters

Broadcast Tagging	<input type="checkbox"/>
WGB VLAN	<input type="checkbox"/>

Policy Proxy Settings

ARP Proxy	<input type="checkbox"/> DISABLED
IPv6 Proxy	<input type="text" value="None"/>

Fabric Profile

Link-Local Bridging

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

EoGRE Tunnel Profiles


Tunnel Profile

CLI :

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

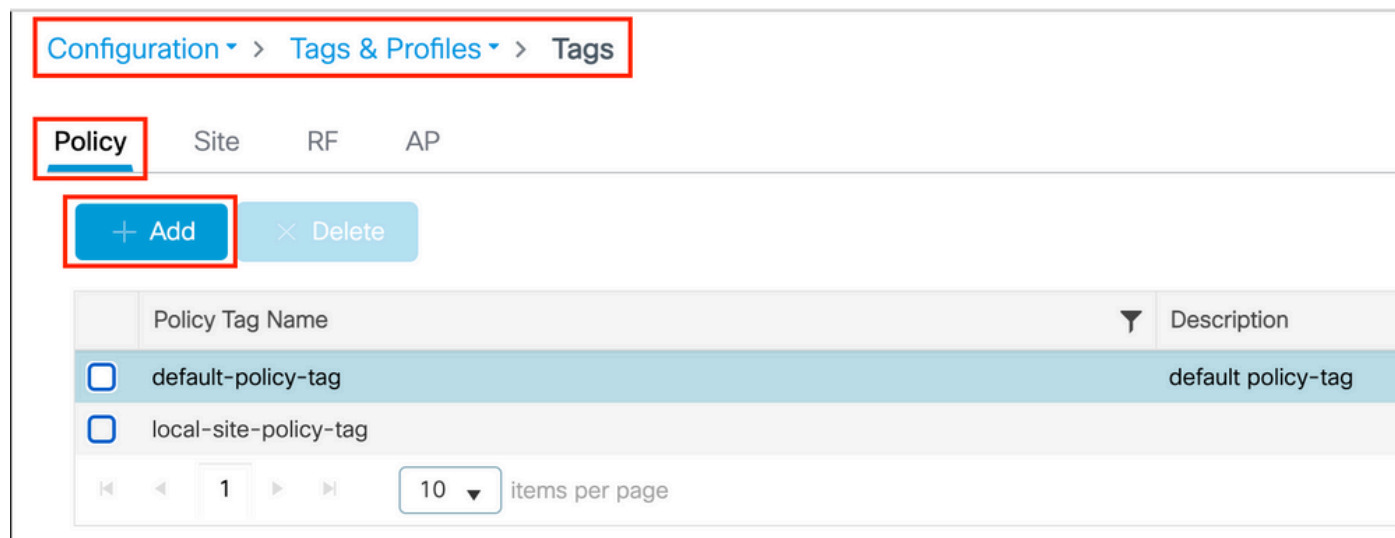
ポリシータグの設定

ポリシータグで、SSID をポリシープロファイルにリンクします。新しいポリシータグを作成するか、default-policy タグを使用します。

 注：default-policyタグは、1 ~ 16のWLAN IDを持つSSIDをdefault-policyプロファイルに自動的にマッピングします。変更や削除はできません。ID 17以降のWLANがある場合、default-policyタグは使用できません。

GUI :

図に示すように、必要に応じてConfiguration > Tags & Profiles > Tags > Policy に移動し、新しいプロファイルを追加します。



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

	Policy Tag Name	Description
<input type="checkbox"/>	default-policy-tag	default policy-tag
<input type="checkbox"/>	local-site-policy-tag	

1 10 items per page

WLAN プロファイルを目的のポリシープロファイルにリンクします。

Add Policy Tag

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

> RLAN-POLICY Maps: 0

CLI :

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

ポリシータグの割り当て

必要な AP にポリシータグを割り当てます。


GUI :

タグを1つのAPに割り当てるには、Configuration > Wireless > Access Points > AP Name > General Tagsに移動し、必要な割り当てを行い、Update & Apply to Deviceをクリックします。

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/> ENABLED	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/> ⓘ
Operation Status Registered	

 注：APのポリシータグを変更すると、9800 WLCとの関連付けが失われ、約1分以内に加入し直されることに注意してください。

同じポリシータグを複数のAPに割り当てるには、Configuration > Wireless > Wireless Setup > Advanced > Start Nowに移動します。

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply



Tag APs



Start Now →

Done

Configuration > Wireless Setup > Advanced

Show Me How

+ Tag APs

Number of APs: 2
Selected Number of APs: 2

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	Serial Number	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag
<input checked="" type="checkbox"/>	[Redacted]	AIR-AP1815I-E-K9	[Redacted]	[Redacted]	Flex	Disabled	Registered	local-site-policy-tag	flex-site-tag	defa rf-ta
<input checked="" type="checkbox"/>	[Redacted]	AIR-AP1815I-E-K9	[Redacted]	[Redacted]	Local	Enabled	Registered	default-policy-tag	default-site-tag	defa rf-ta

1 10 items per page 1 - 2 of 2 items

ホイッシュタグを選択し、図に示すようにSave & Apply to Deviceをクリックします。

Tag APs

Tags

Policy

Site

RF

Changing AP Tag(s) will cause associated AP(s) to rejoin and disrupt connected client(s)

CLI :

```
# config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end
```

リダイレクト ACL 設定

ステップ 1 : 新しいACLを作成するには、Configuration > Security > ACL > + Add に移動します。

ACLの名前を選択し、図に示すように、そのタイプをIPv4 Extended 作成し、すべてのルールをシーケンスとして追加します。

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type Host Name* ! This field is mandatory

Protocol

Log DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
0										


10 items per page No items to display

ISE PSN ノードへのトラフィックと DNS を拒否し、他はすべて許可する必要があります。このリダイレクトACLは、セキュリティACLではなく、追加の処理 (リダイレクションなど) のために (許可された) CPUに送られるトラフィックと (拒否された) データプレーンに留まるトラフィックを定義し、リダイレクションを回避するバントACLです。

ACLは次のようになります (この例では、10.48.39.28をISE IPアドレスに置き換えます)。


Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

1 items per page 10 items per page 1 - 5 of 5 items

 注 : リダイレクションACLの場合、denyのアクションを拒否リダイレクション (拒否トラフィックではない) と考え、permitのアクションを許可リダイレクションと考えます。WLCは、リダイレクト可能なトラフィック (デフォルトではポート80および443) のみを調べます。

CLI :

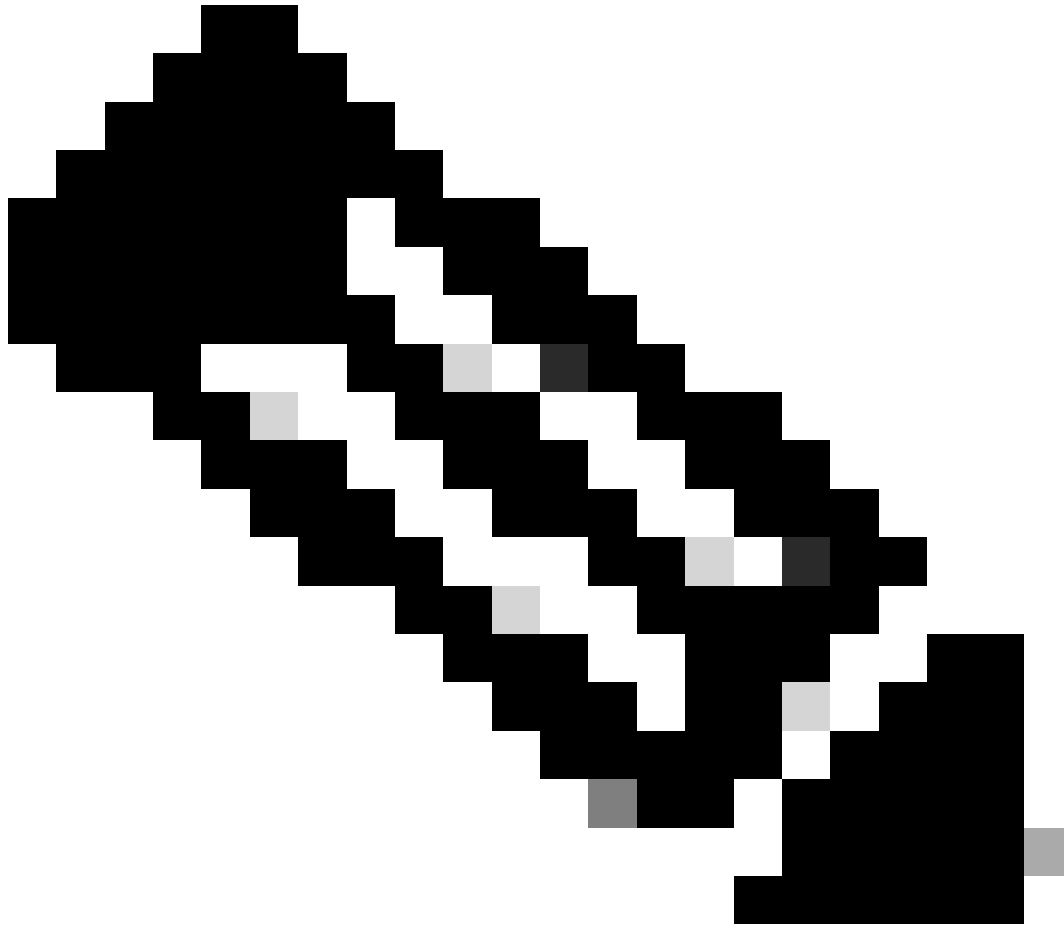
```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```

 注：ポート80に焦点を当てた許可の代わりにpermit ip any anyを使用してACLを終了すると、WLCはHTTPSもリダイレクトします。これは、それ自体の証明書を提供する必要があり、常に証明書違反を作成するため、望ましくない場合があります。これは、CWAの場合にWLC上の証明書は必要ないという前述の文の例外です。HTTPS代行受信を有効にしている場合には証明書は必要ですが、いずれにしても有効とは見なされません。

ISEサーバに対してゲストポート8443のみを拒否するように操作することで、ACLを改善できます。

HTTPまたはHTTPSのリダイレクトを有効にする

Web管理ポータルの設定はWeb認証ポータルに関連付けられており、リダイレクトするにはポート80でリッスンする必要があります。したがって、リダイレクションが正しく動作するには、HTTPを有効にする必要があります。この機能は、グローバルに有効にする(ip http serverコマンドを使用)か、Web認証モジュールに対してのみHTTPを有効にする(パラメータマップにwebauth-http-enableコマンドを使用する)から選択できます。



注:HTTPトラフィックのリダイレクションは、FlexConnectローカルスイッチングの場合でも、CAPWAP内で発生します。WLCがインターセプション作業を行うため、APはCAPWAPトンネル内でHTTP(S)パケットを送信し、WLCからCAPWAPに戻るリダイレクションを受信します

HTTPS URLにアクセスしようとするときにリダイレクトされるようにする場合は、パラメータマップでコマンドintercept-https-enableを追加しますが、これは最適な設定ではなく、WLCのCPUに影響を与え、証明書エラーを生成することに注意してください。

<#root>

parameter-map type webauth global

type webauth

intercept-https-enable

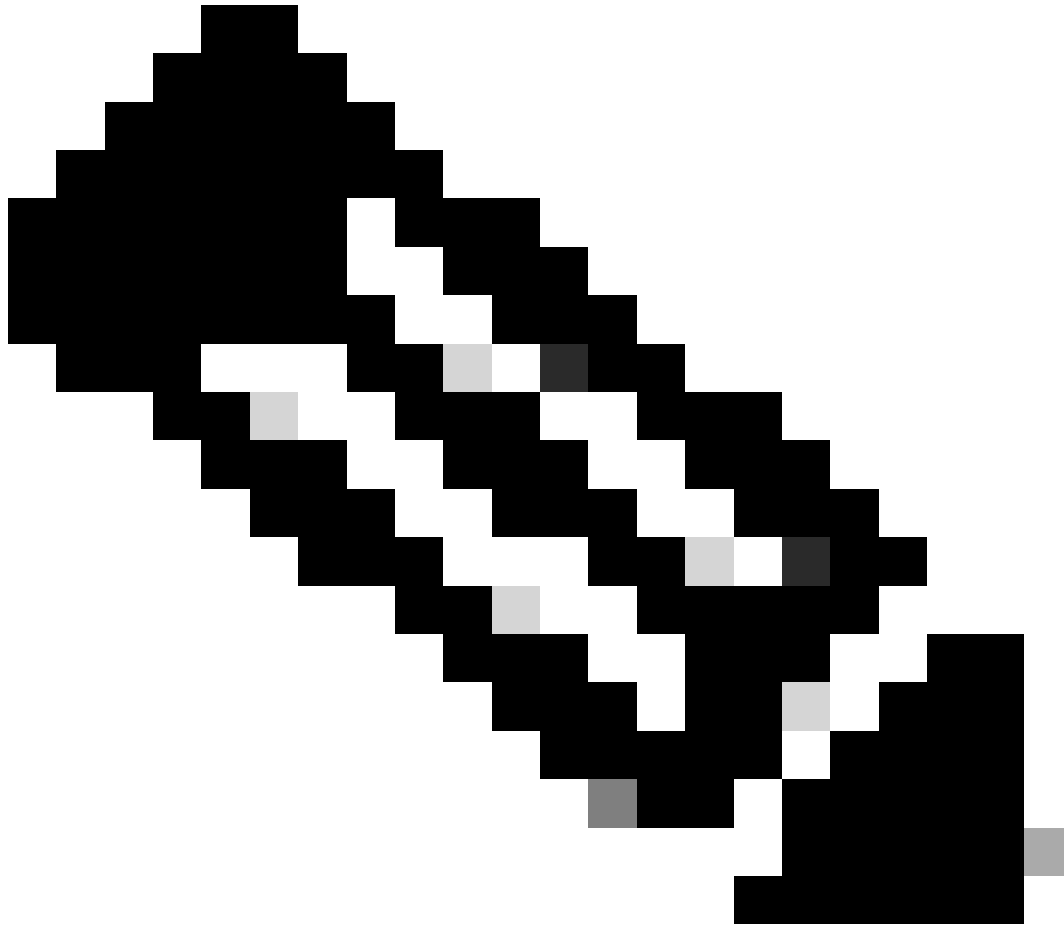
trustpoint xxxxx

また、パラメータマップ(Configuration > Security > Web Auth)でオプション「Web Auth intercept HTTPS」をチェックしてGUIから実行することもできます。

The screenshot shows the configuration interface for Web Auth. On the left is a navigation menu with options: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth' and contains a table of parameter maps. The 'global' map is selected. Below the table is a pagination control showing '1' items per page. On the right, the 'Edit Web Auth Parameter' panel is open, displaying various settings: Maximum HTTP connections (100), Init-State Timeout(secs) (120), Type (webauth), Virtual IPv4 Address, Trustpoint (--- Select ---), Virtual IPv6 Address (X::X::X::X), Web Auth intercept HTTPS (checked), and Captive Bypass Portal (unchecked). The 'Web Auth intercept HTTPS' checkbox is highlighted with a red box.

Parameter Map Name
<input type="checkbox"/> global

Edit Web Auth Parameter	
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Virtual IPv4 Address	
Trustpoint	--- Select ---
Virtual IPv6 Address	X::X::X::X
Web Auth intercept HTTPS	<input checked="" type="checkbox"/>
Captive Bypass Portal	<input type="checkbox"/>

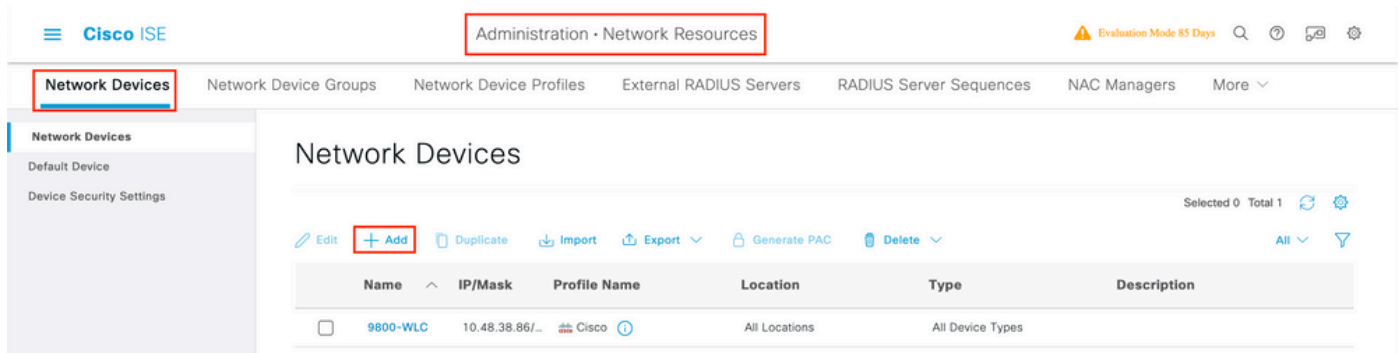


注：デフォルトでは、HTTPSリダイレクションが必要な場合、ブラウザはHTTP Webサイトを使用してリダイレクションプロセスを開始します。Web認証インターセプトHTTPSをチェックする必要があります。ただし、この設定はCPU使用率を増加させるため、推奨されません。

ISE 設定

9800 WLC の ISE への追加

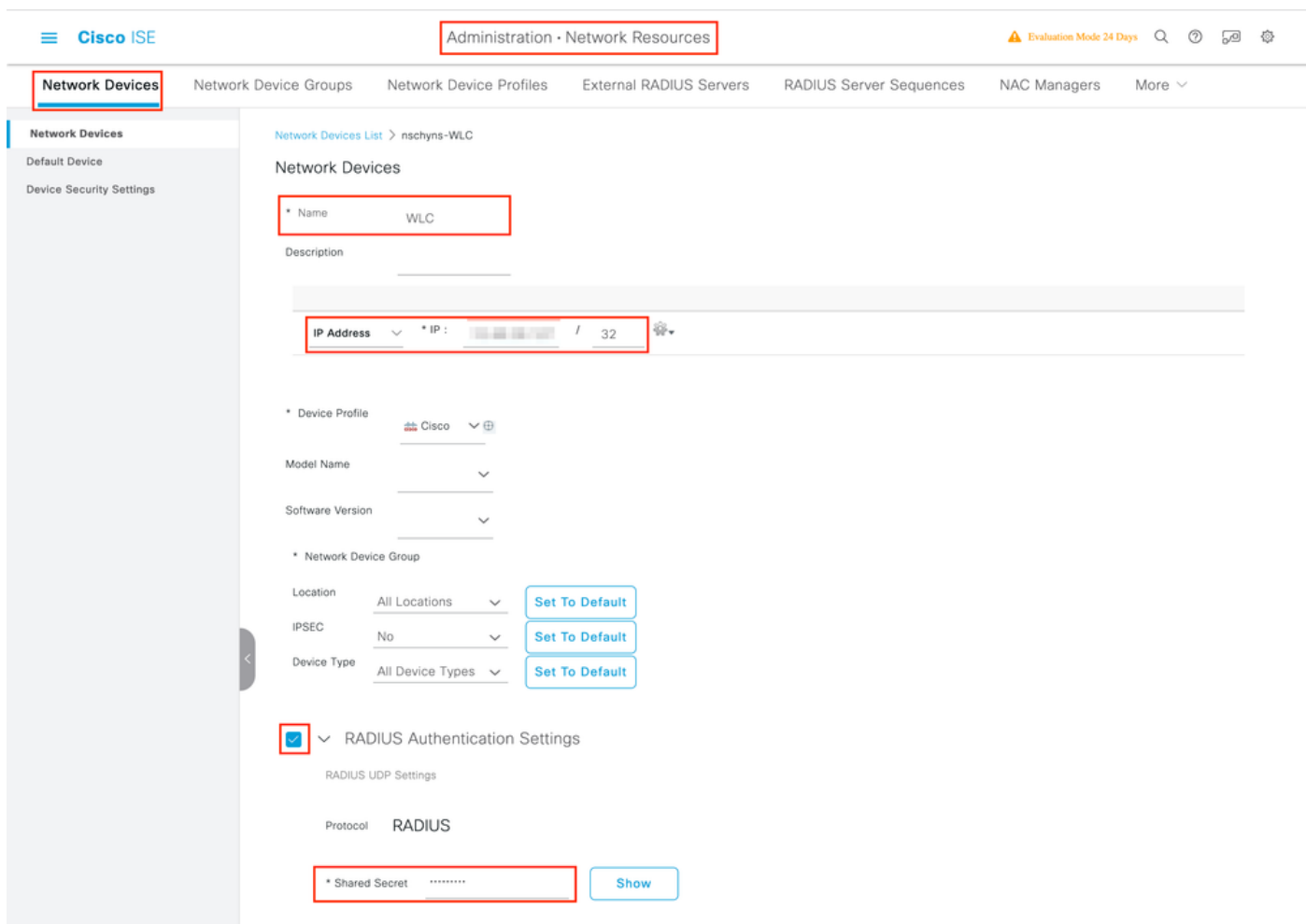
ステップ 1： ISEコンソールを開き、図に示すようにAdministration > Network Resources > Network Devices > Add、移動します。



ステップ 2 : ネットワークデバイスを設定します。

必要に応じて、モデル名、ソフトウェアバージョン、および説明を指定し、デバイスタイプ、ロケーション、またはWLCに基づいてネットワークデバイスグループを割り当てることができます。

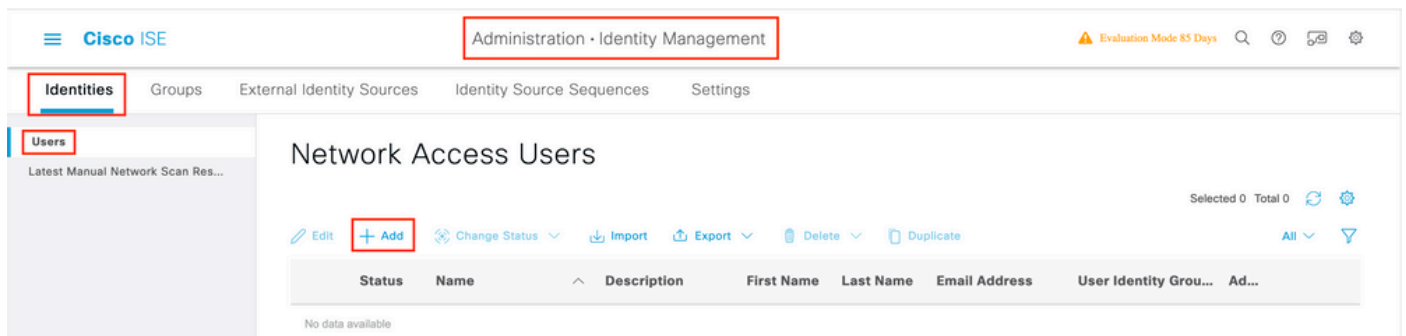
このIPアドレスは、認証要求を送信するWLCインターフェイスに対応しています。デフォルトでは、次の図に示すように管理インターフェイスになります。



ネットワークデバイスグループの詳細については、ISE管理ガイドの「章：ネットワークデバイスの管理：[ISE - ネットワークデバイスグループ](#)」を参照してください。

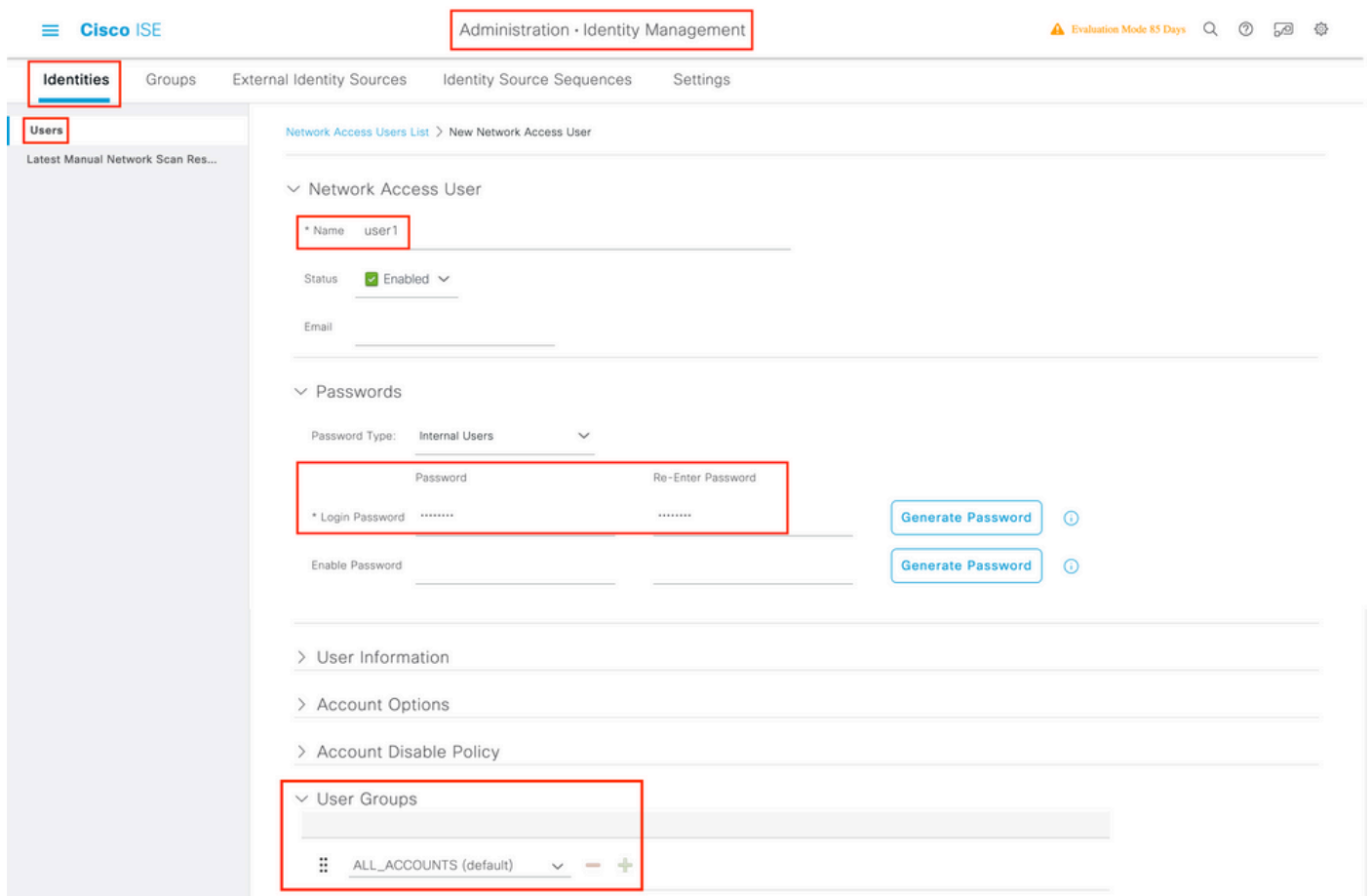
ISE での新しいユーザの作成

ステップ 1 : 図に示すように、Administration > Identity Management > Identities > Users > Add に移動します。



ステップ 2 : 情報を入力します。

この例では、このユーザはALL_ACCOUNTSというグループに属していますが、図に示すように必要に応じて調整できます。

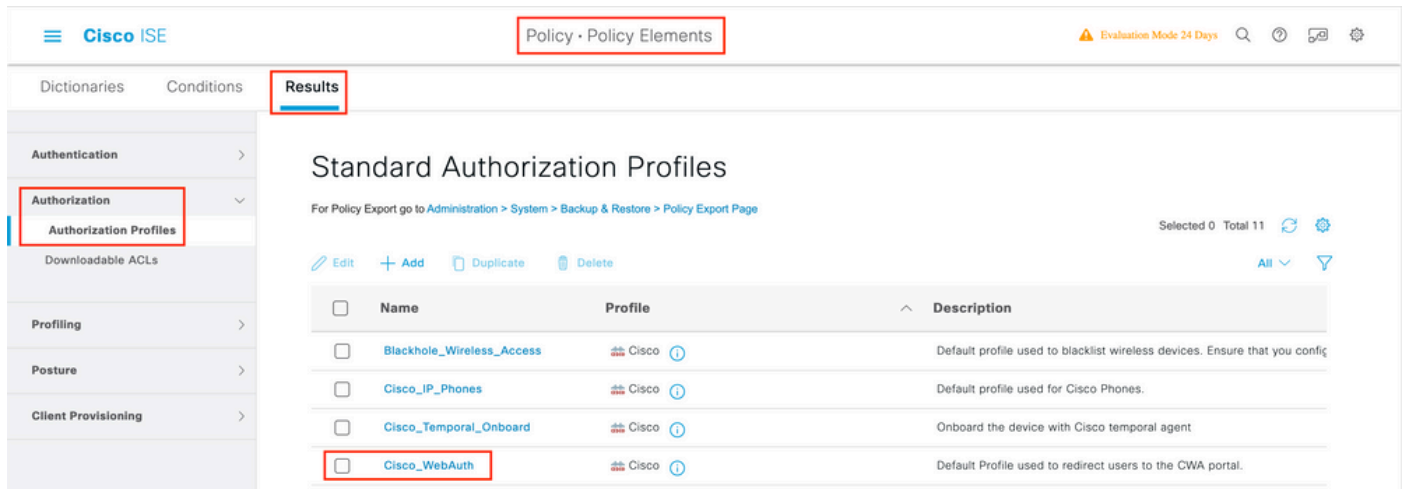


認証プロファイルの作成

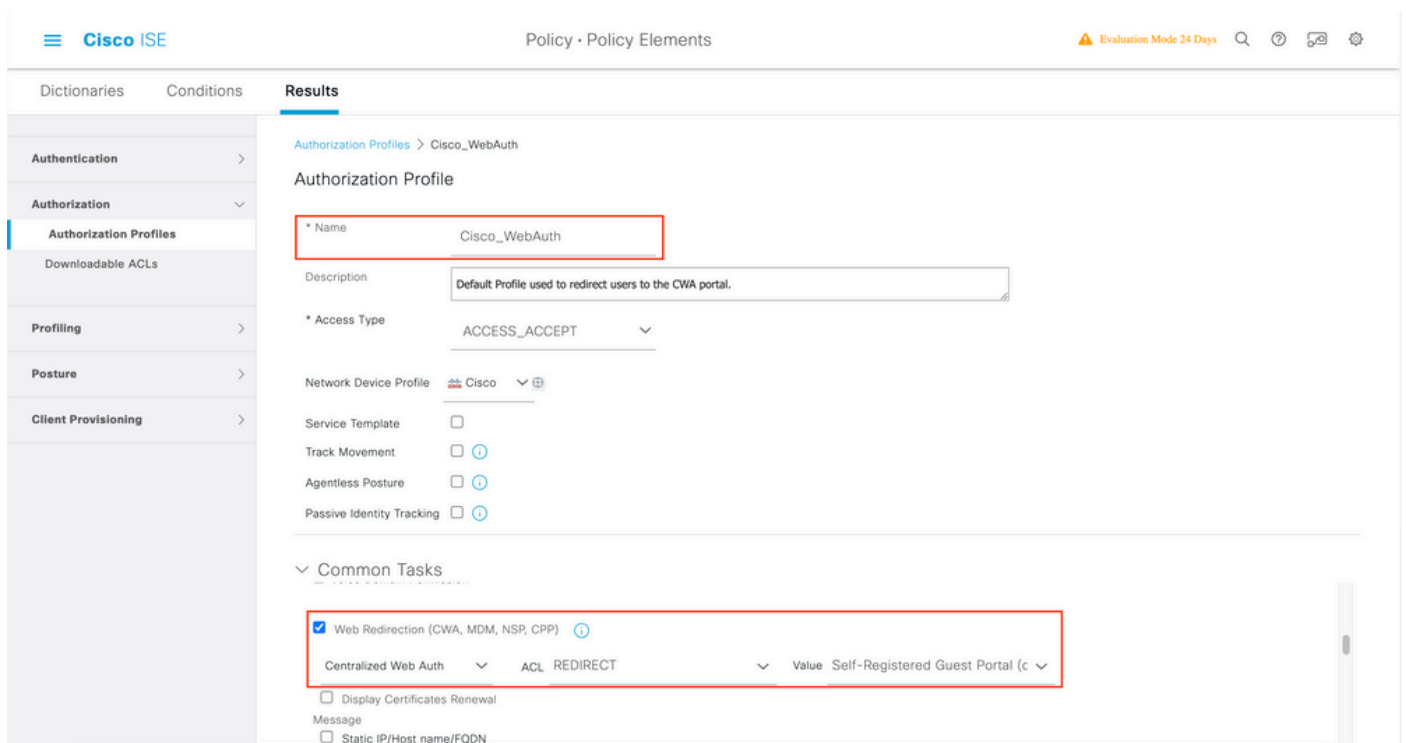
ポリシープロファイルは、パラメータ (MACアドレス、クレデンシャル、使用されるWLANなど) に基づいてクライアントに割り当てられる結果です。仮想ローカルエリアネットワーク(VLAN)、アクセスコントロールリスト(ACL)、Uniform Resource Locator(URL)リダイレクトなどの特定の設定を割り当てることができます。

ISE の最近のバージョンでは、Cisco_Webauth 許可の結果がすでに存在することに注意してください。WLC で設定したものと一致させるには、ここで編集して、リダイレクト ACL 名を変更します。

ステップ 1 : Policy > Policy Elements > Results > Authorization > Authorization Profilesに移動します。独自の結果を作成したり、デフォルトの結果を編集したりするには、addをクリックしますCisco_Webauth。



ステップ 2 : リダイレクト情報を入力します。ACL名が9800 WLCで設定されたものと同じであることを確認します。



認証ルール (Authentication Rule) の設定

ステップ 1 : ポリシーセットは、認証ルールと許可ルールの集合を定義します。ポリシーを作成するには、Policy > Policy Setsに移動し、リストの最初のポリシーセットのギアをクリックしてInsert new row 選択するか、右側の青い矢印をクリックしてデフォルトのポリシーセットを選択します。

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Default	Default policy set		Default Network Access	70	⚙️	➔

ステップ 2 : Authentication policyを展開します。MABのルール (有線またはワイヤレスMABでの一致) に対してOptionsを展開し、「If User not found」が表示される場合はCONTINUEオプションを選択します。

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options If Auth fail REJECT If User not found CONTINUE If Process fail DROP	0	⚙️

ステップ 3 : 変更を保存するには、Save をクリックします。

許可ルール (Authorization Rule) の設定

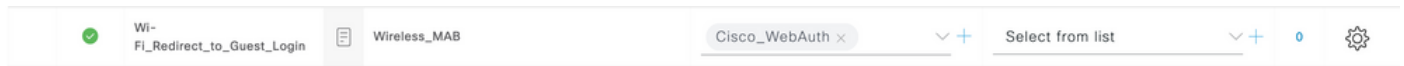
許可ルールは、クライアントに適用される許可 (認証プロファイル) の結果を決定するためのものです。

ステップ 1 : 同じポリシーセットページで、Authentication Policyを閉じて、図に示すようAuthorziation Policy に展開します。

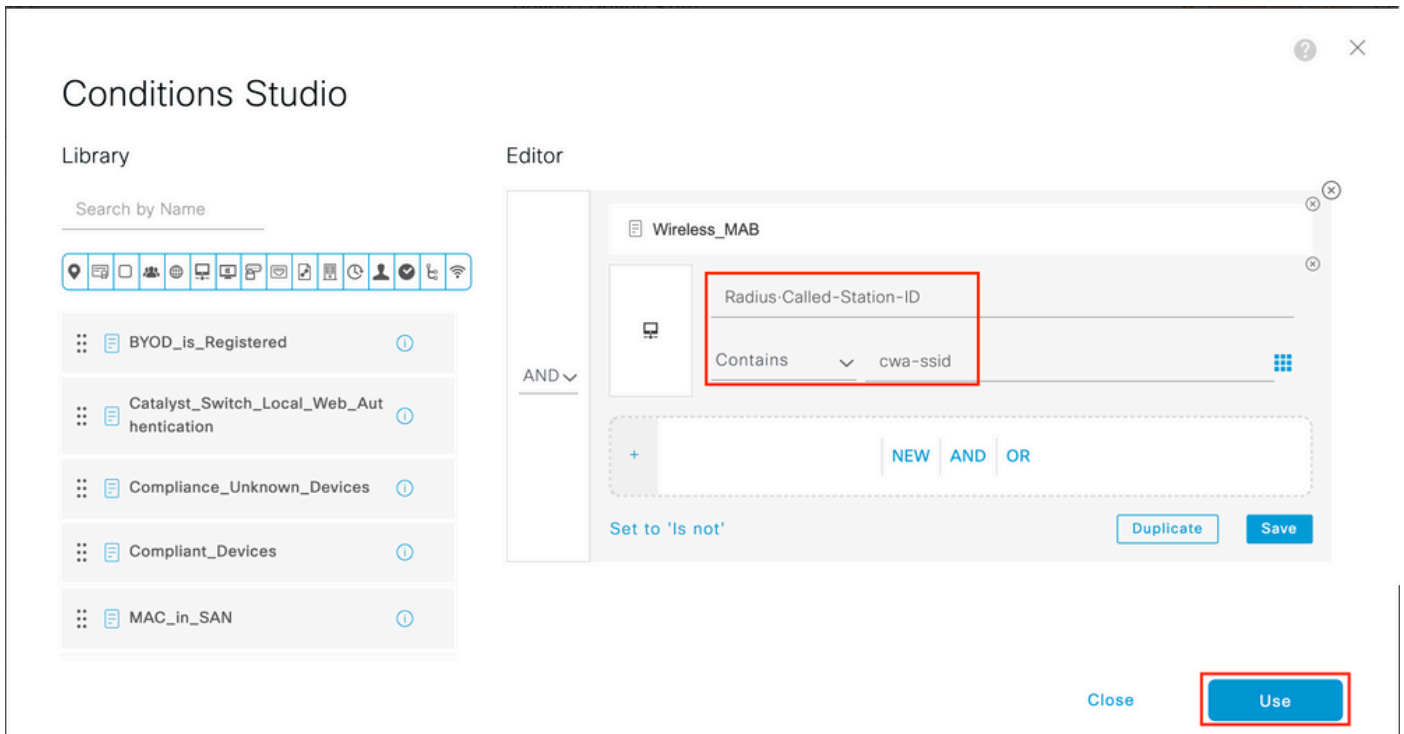
Policy Sets -> Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	70
<ul style="list-style-type: none"> > Authentication Policy (3) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions ▼ Authorization Policy (13) 					

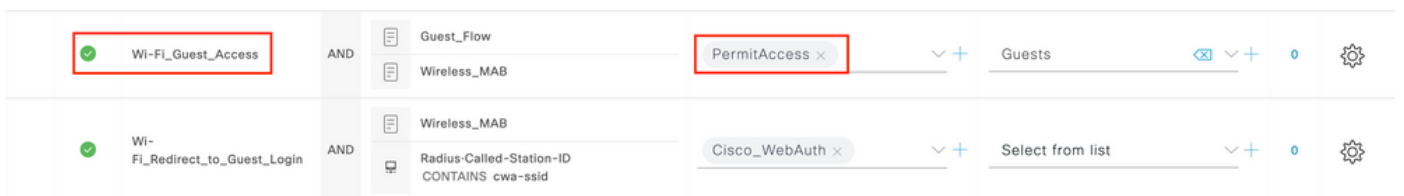
ステップ 2 : 最近のISEバージョンでは、Wifi_Redirect_to_Guest_Loginというルールが事前に作成されており、ほとんどの場合は二一ズに一致します。左側の灰色の記号をenableに変えます。



ステップ 3 : このルールはWireless_MABのみに一致し、CWAリダイレクト属性を返します。必要に応じて、少しツイストを追加し、特定のSSIDのみに一致させることができます。条件を選択して (現時点ではWireless_MAB)、Conditions Studioを表示します。右側に条件を追加し、Called-Station-ID属性を持つRadiusディクショナリを選択します。SSID名と一致するようにします。図に示すように、画面の下部に「Use」を入力して検証します。



ステップ 4 : Guest Flow ユーザがポータルで認証された後、ネットワークアクセスの詳細を返すため、条件に一致する2つ目のルール(高い優先度で定義)が必要です。最新のISEバージョンでは、デフォルトで事前に作成されているWifi Guest Accessルールを使用できます。後は左側のマークを緑色にして、ルールを有効にするだけです。デフォルトのPermitAccessを返すか、より厳密なアクセスリスト制限を設定できます。



ステップ 5 : ルールを保存します。

ルールの下部にあるSave をクリックします。

FlexConnect ローカル スイッチング アクセス ポイントのみ


FlexConnect ローカル スイッチング アクセス ポイントと WLAN がある場合はどうなりますか？前のセクションの手順が使用できません。ただし、事前にリダイレクトACLをAPにプッシュするには、追加の手順が必要です。

Configuration > Tags & Profiles > Flexに移動し、Flexプロファイルを選択します。次に、Policy ACLタブに移動します。

図に示Add するようにクリックします。

The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A red box highlights the '+ Add' button. Below the button are three dropdown menus: 'ACL Name', 'Central Web Auth', and 'URL Filter'. Below these is a table with 0 items per page and 'No items to display'.

リダイレクトACL名を選択し、中央Web認証を有効にします。このチェックボックスは、AP自体のACLを自動的に反転します（「deny」文はCisco IOS XEのWLCで「このIPにリダイレクトしない」を意味するためです）。ただし、APでは、「deny」文はその逆を意味します。したがって、このチェックボックスをオンにすると、APへのプッシュ時にすべての許可が自動的に入れ替わり、拒否されます。これは、AP CLIからshow ip access listを使用して確認できます。

 注：Flexconnectローカルスイッチングのシナリオでは、ACLで特にreturn文を指定する必要があります（これはローカルモードでは必ずしも必要ではありません）。そのため、すべてのACLルールでトラフィックの双方向（ISEとの間など）がカバーされていることを確認してください。

Saveを押してからUpdate and apply to the deviceを押すことを忘れないでください。

The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A modal dialog is open for adding a new ACL rule. The 'ACL Name*' field is set to 'REDIRECT', and the 'Central Web Auth' checkbox is checked. The 'Save' button is highlighted.

証明書

クライアントがWeb認証証明書を信頼するようにするためには、提示される証明書は（クライアントが信頼する必要がある

) ISE証明書だけであるため、WLCに証明書をインストールする必要はありません。

確認

以下のコマンドを使用して、現在の設定を確認できます。

<#root>

```
# 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 | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

この例に対応するWLCの設定の関連部分を次に示します。

<#root>

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE>
mac-filtering CWAauthz
no security fit adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

トラブルシューティング

Checklist

- クライアントが接続し、有効なIPアドレスを取得することを確認します。
- リダイレクトが自動でない場合は、ブラウザを開いてランダムなIPアドレスを試してください。たとえば、10.0.0.1 などは。リダイレクトが動作する場合は、DNS解決に問題がある可能性があります。DHCP経由で提供された有効なDNSサーバがあり、ホスト名を解決できることを確認します。

- HTTP上でリダイレクションが機能するようにコマンドip http serverが設定されていることを確認します。Web管理ポータルの設定はWeb認証ポータルの設定に関連付けられており、リダイレクトするにはポート80にリストされている必要があります。この機能は、グローバルに有効にする(ip http serverコマンドを使用)か、Web認証モジュールに対してのみHTTPを有効にする(パラメータマップにwebauth-http-enableコマンドを使用する)から選択できます。
- HTTPS URLにアクセスしようとするときにリダイレクトされず、それが必要な場合は、パラメータマップにintercept-https-enableコマンドがあることを確認します。

<#root>

```
parameter-map type webauth global
type webauth
```

```
intercept-https-enable
```

```
trustpoint xxxxxx
```

また、パラメータマップで「Web Auth intercept HTTPS」オプションにチェックマークが付いていることも、GUIを介して確認できます。

The screenshot shows the Cisco Catalyst GUI configuration page for 'Web Auth'. The breadcrumb navigation is 'Configuration > Security > Web Auth'. The main content area is titled 'Edit Web Auth Parameter' and contains several configuration fields:

- Maximum HTTP connections: 100
- Init-State Timeout(secs): 120
- Type: webauth
- Virtual IPv4 Address: (empty)
- Trustpoint: --- Select ---
- Virtual IPv6 Address: x::x::x
- Web Auth intercept HTTPS: (highlighted with a red box)
- Captive Bypass Portal:

On the left side, there is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The 'Configuration' menu item is currently selected.

RADIUSのサービスポートサポート

Cisco Catalyst 9800シリーズワイヤレスコントローラには、GigabitEthernet 0ポートと呼ばれるサービスポートがあります。バージョン17.6.1以降では、RADIUS (CoAを含む)がこのポートでサポートされています。

RADIUSのサービスポートを使用する場合は、次の設定が必要です。

<#root>

```
aaa server radius dynamic-author
client 10.48.39.28

vrf Mgmt-intf

  server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

  ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
  server name nicoISE

  ip vrf forwarding Mgmt-intf

  ip radius source-interface GigabitEthernet0
```

デバッグの収集

WLC 9800 では、ALWAYS-ON トレース機能を利用できます。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継続的にログに記録され、発生後にインシデントまたは障害状態のログを表示できます。



注：ログ内で数時間から数日を遡ることができますが、生成されるログの量によって異なります。

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、次の手順を実行します（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：WLCの現在の時刻を確認して、問題が発生した時刻までログを追跡できるようにします。

```
<#root>
```

```
# show clock
```

ステップ 2：システム設定に従って、WLC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（存在する場合）をすばやく確認できます。



```
<#root>
```

```
# 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。

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

 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わない場合は、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ものとして、特定のMACアドレスの Always-On Notice Level(AToS)トレースを収集します。

```
<#root>
```

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

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。

```
<#root>
```

```
# 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、無線アクティブ(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、次の手順に進みます。

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。

```
<#root>
```


```
# 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。

```
<#root>
```

```
# 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ているため、ターミナルセッションでクライアントアクティビティの出力は表示されません。

ステップ 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経過する前に問題が再現した場合は、デバッグを停止します。

```
<#root>
```

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

モニタ時間が経過するか、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_aaaabbbccccc_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を外部サーバにコピーするか、出力を画面に直接表示します。

RA トレースファイルの名前を確認します。

```
<#root>
```

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

ファイルを外部サーバーにコピーします。

```
<#root>
```

```
# copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

内容を表示します。


```
<#root>
```

```
# 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で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。

```
<#root>
```

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

 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に依頼します。

ra-internal-FILENAME.txtを外部サーバにコピーするか、出力を画面に直接表示します。

ファイルを外部サーバーにコピーします。

```
<#root>
```

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

内容を表示します。

```
<#root>
```

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

ステップ 11デバッグ条件を削除します。

```
<#root>
```

```
# 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。

例

認証結果が予想と異なる場合は、ISEOperations > Live logsのページに移動し、認証結果の詳細を取得することが重要です。

障害の理由（障害がある場合）とISEが受信したすべてのRadius属性が表示されます。

次の例では、許可ルールが一致しなかったため、ISEは認証を拒否しました。これは、認可がSSID名に完全に一致する間、APのMACアドレスに追加されたSSID名として送信されたCalled-station-ID属性が表示されるためです。このルールは、「equal」ではなく「contains」に変更されると修正されます。

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-Type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```


Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add - Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt Download

10 Items per page 1 - 1 of 1 items

Generate

この場合、問題は、ACL名を作成したときに入力ミスをし、ISEから返されたACL名と一致しなかったか、またはWLCがISEから要求されるようなACLがないと苦情を言ったことにあります。

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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。