

在Catalyst 9800 WLC和ISE上配置中央Web身份驗證(CWA)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[9800 WLC 的 AAA 組態](#)

[WLAN配置](#)

[原則設定檔組態](#)

[原則標籤組態](#)

[原則標籤指派](#)

[重新導向 ACL 組態](#)

[啟用HTTP或HTTPS重新導向](#)

[ISE 組態](#)

[將 9800 WLC 新增至 ISE](#)

[在 ISE 上建立新使用者](#)

[建立授權設定檔](#)

[設定驗證規則](#)

[設定授權規則](#)

[僅限 FlexConnect 本機交換存取點](#)

[憑證](#)

[驗證](#)

[疑難排解](#)

[檢查清單](#)

[RADIUS的服務連線埠支援](#)

[收集調試](#)

[範例](#)

簡介

本文檔介紹如何在Catalyst 9800 WLC和ISE上配置CWA無線LAN。

必要條件

需求

思科建議您瞭解9800無線LAN控制器(WLC)的組態。

採用元件

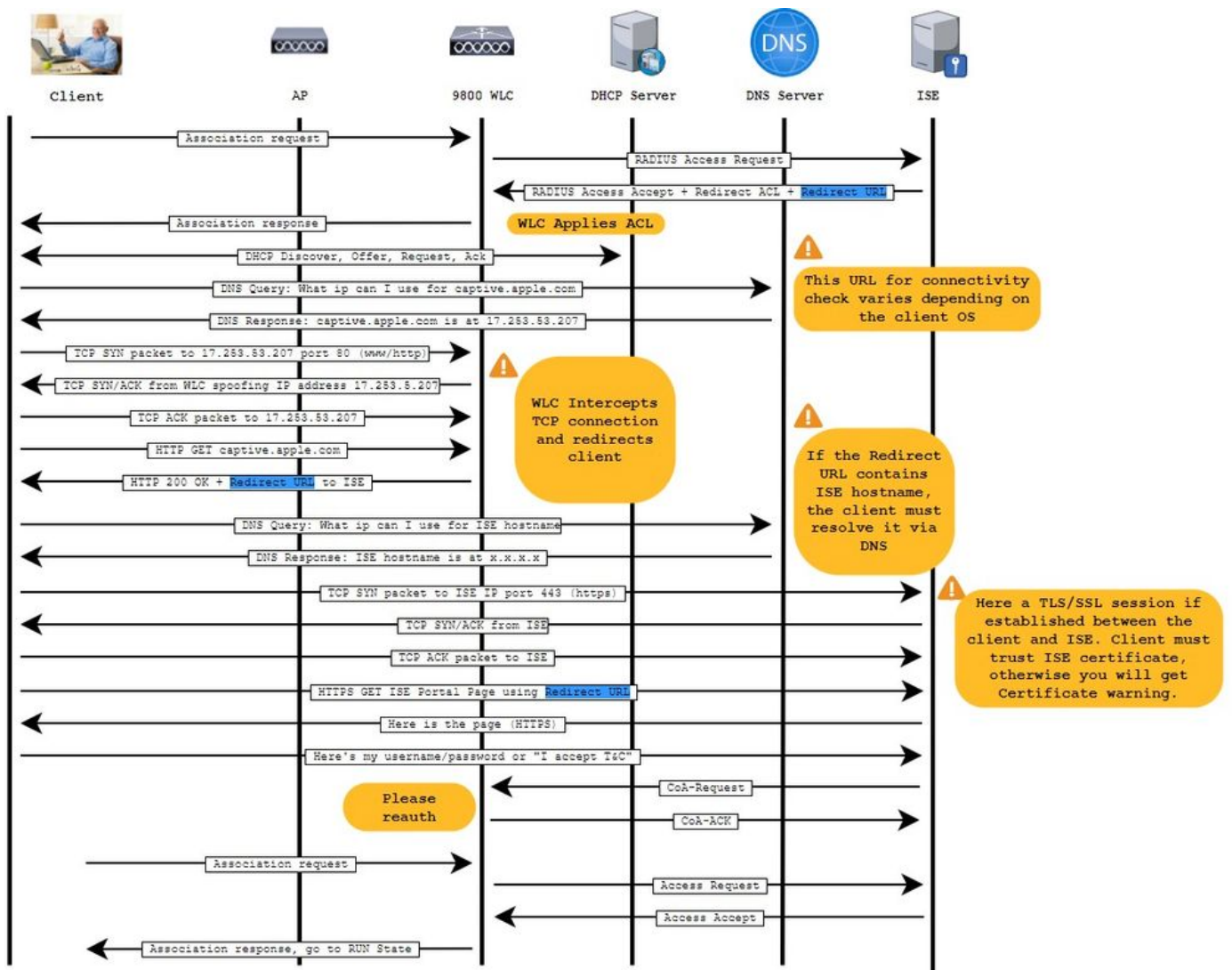
本文中的資訊係根據以下軟體和硬體版本：

- 9800 WLC Cisco IOS® XE直布羅陀版v17.6.x
- 身分辨識服務引擎(ISE) v3.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

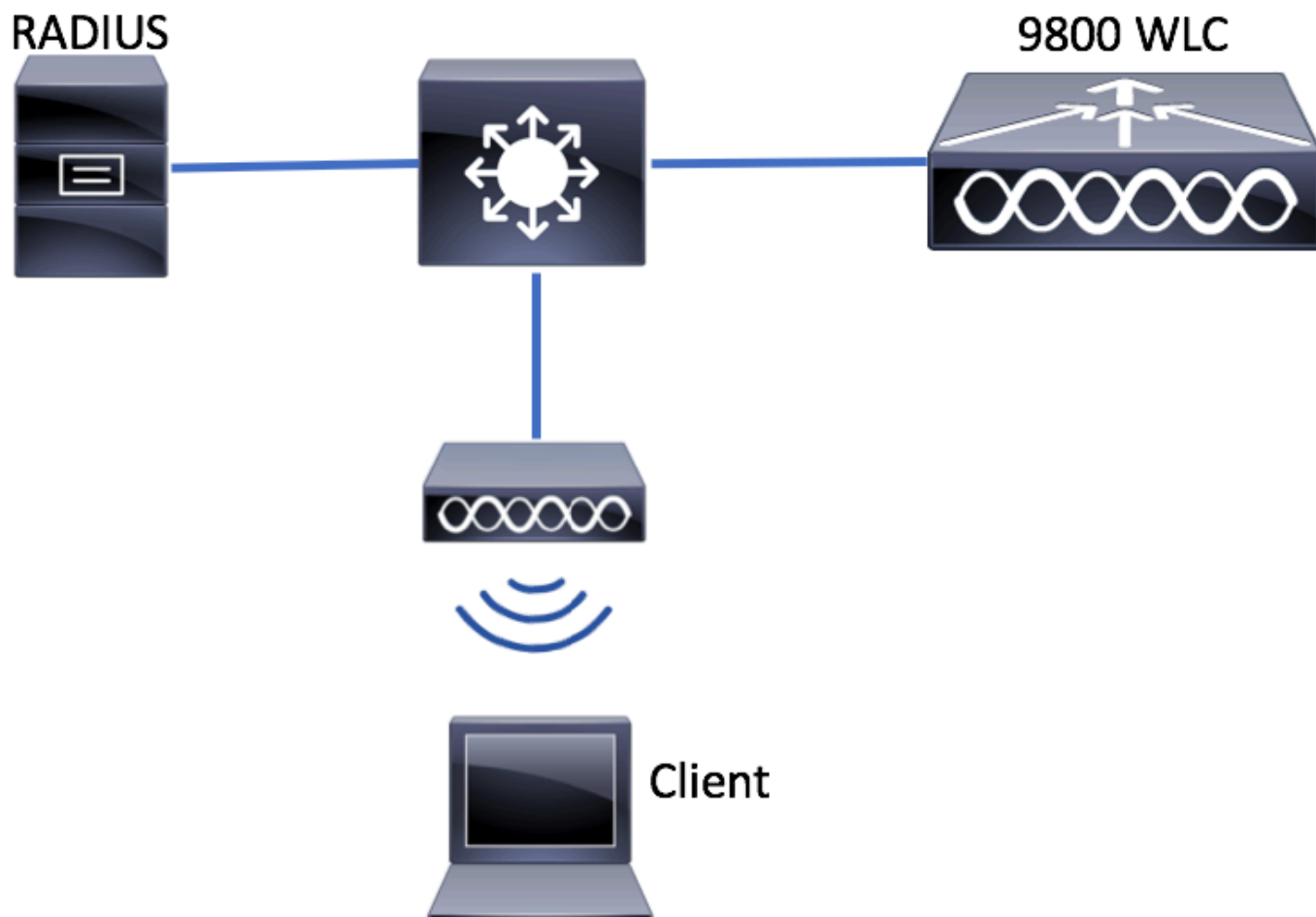
背景資訊

此處顯示了CWA進程，您可以在這裡看到Apple裝置的CWA進程作為示例：



設定

網路圖表



9800 WLC 的 AAA 組態

步驟 1. 將ISE伺服器增加到9800 WLC配置。

導覽至 [Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add](#) 並輸入RADIUS伺服器資訊，如下圖所示。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Address
0	

10 items per page

如果您未來計畫使用中央 Web 驗證 (或任何需要 CoA 的安全性類型) ，請確認「CoA 支援」已啟用。

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



注意：在版本17.4.X及更高版本中，請確保在配置RADIUS伺服器時也配置CoA伺服器金鑰。使用與共用金鑰相同的金鑰（在ISE上預設情況下相同）。目的是要選擇為CoA配置與共用金鑰不同的金鑰，如果共用金鑰是您的RADIUS伺服器配置的。在Cisco IOS XE 17.3中，Web UI僅使用與CoA金鑰相同的共用金鑰。

步驟 2. 建立授權方法清單。

導覽至 Configuration > Security > AAA > AAA Method List > Authorization > + Add ，如下圖所示。

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

^ v ^ v

步驟3. (可選) 建立會計方式清單, 如下圖所示。

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

+ AAA Wizard

AAA Method List

Servers / Groups

General

Authentication

Authorization

Accounting

+ Add

x Delete

Name

0

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups

Assigned Server Groups

ldap
tacacs+

radius

Cancel

Apply to Device

注意：如果由於思科漏洞ID [CSCvh03827](#)，您決定對您的RADIUS伺服器進行負載均衡（透過Cisco IOS XE CLI配置），則CWA不起作用。外部負載均衡器的使用是正常的。但是，透過使用calling-station-id RADIUS屬性，確保負載均衡器針對每個客戶端運行。依賴UDP源埠不是用於平衡來自9800的RADIUS請求的受支援機制。

第4步：（可選）您可以定義AAA策略將SSID名稱作為被叫站ID屬性傳送，如果您要在稍後的ISE中利用此條件，這會非常有用。

導航到Configuration > Security > Wireless AAA Policy，然後編輯預設AAA策略或建立新策略。

- ☰ Dashboard
- 🕒 Monitoring >
- 🔧 **Configuration** >
- ⚙️ Administration >
- 🔧 Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

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

⏪
⏩
1
⏪
⏩
10 items per page

您可以選擇SSID作為選項1。請注意，即使您僅選擇SSID，被叫站ID仍會將AP MAC地址附加到SSID名稱中。

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

Option 1

SSID ▼

Option 2

Not Configured ▼

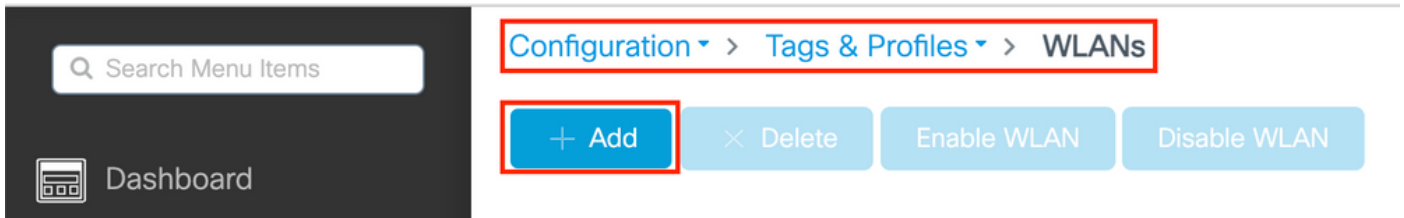
Option 3

Not Configured ▼

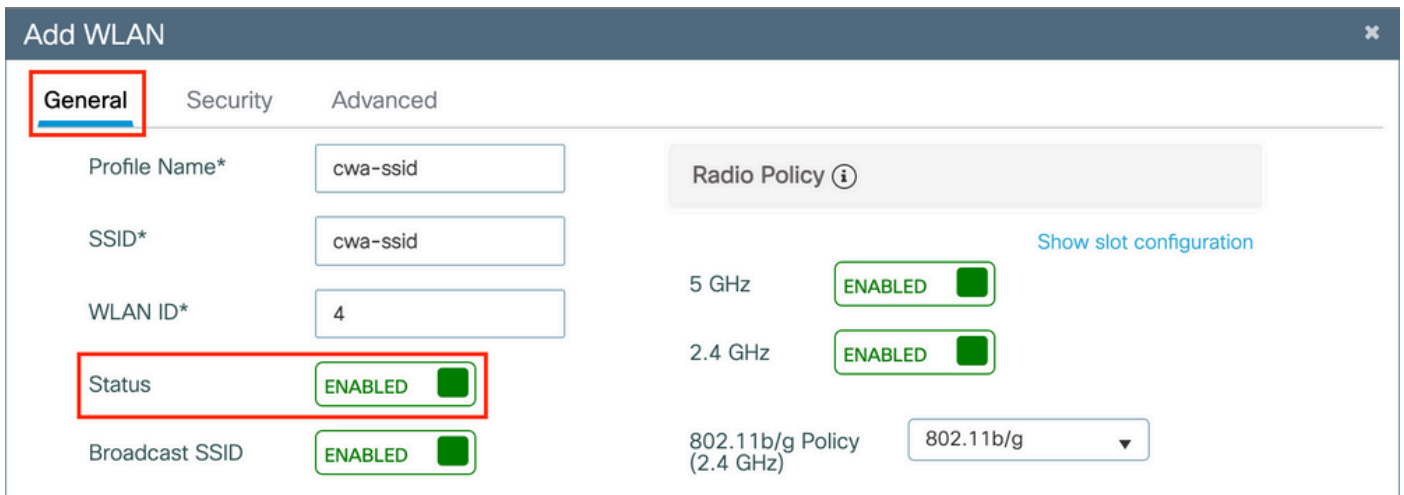
WLAN配置

步驟 1. 建立WLAN。

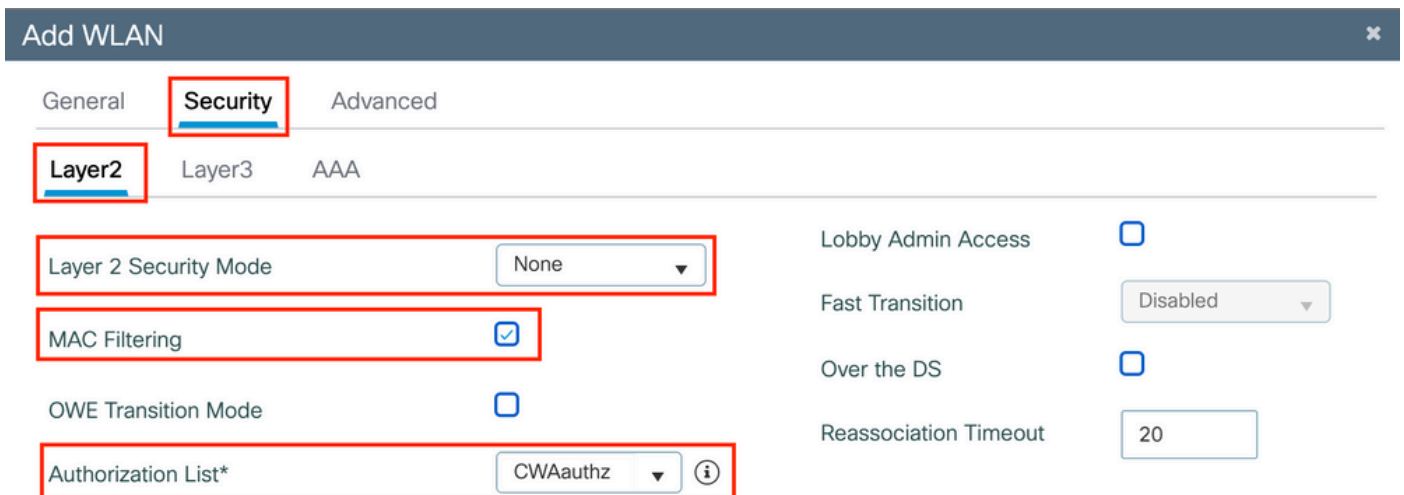
根據需要導航到Configuration > Tags & Profiles > WLANs > + Add 並配置網路。



步驟 2.輸入WLAN一般資訊。



步驟 3.導航到Security 頁籤並選擇所需的安全方法。在這種情況下，僅需要「MAC過濾」和AAA授權清單(在AAA Configuration 部分的步驟2中建立)。



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

原則設定檔組態

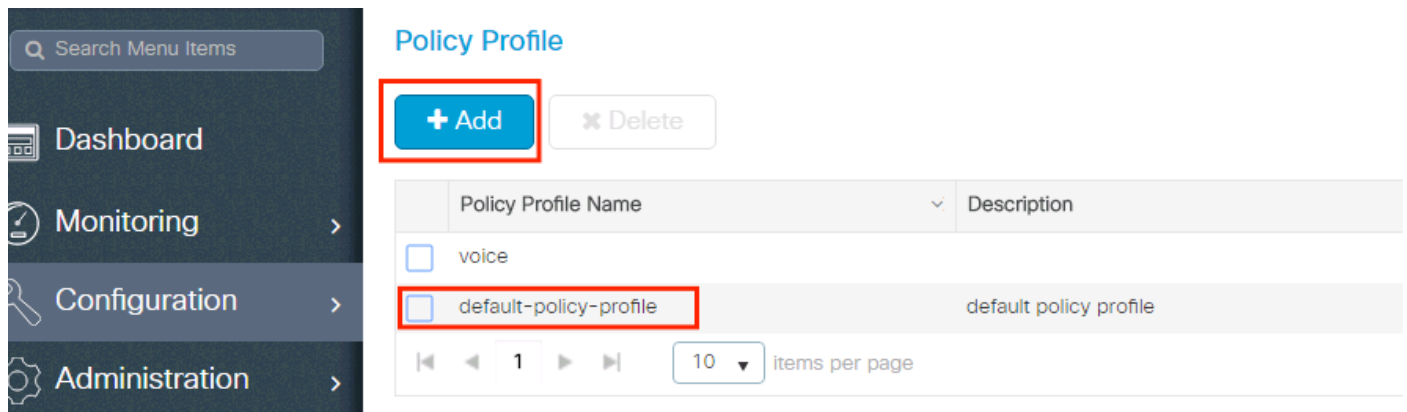
在策略配置檔案中，除了其他設定(如訪問控制清單(ACL)、服務品質(QoS)、移動錨點、計時器等)外，您可以決定為哪些VLAN分配客戶端。

您可使用預設原則設定檔，或可建立新的設定檔。

GUI：

步驟 1.新建Policy Profile。

導航到Configuration > Tags & Profiles > Policy 並配置default-policy-profile 或建立新配置。



Policy Profile

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

10 items per page

確認設定檔已啟用。

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

步驟 2.選擇VLAN。

導航到Access Policies 頁籤，從下拉選單中選擇VLAN名稱或手動鍵入VLAN-ID。請勿在原則設定檔中設定 ACL。

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 ▼

步驟 3. 配置策略配置檔案以接受ISE覆蓋 (允許AAA覆蓋) 和授權更改(CoA) (NAC狀態)。您亦可選擇性指定帳戶處理方法。

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)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List ⓘ ✕

WGB Parameters

Broadcast Tagging

WGB VLAN

Policy Proxy Settings

ARP Proxy DISABLED

IPv6 Proxy

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
```

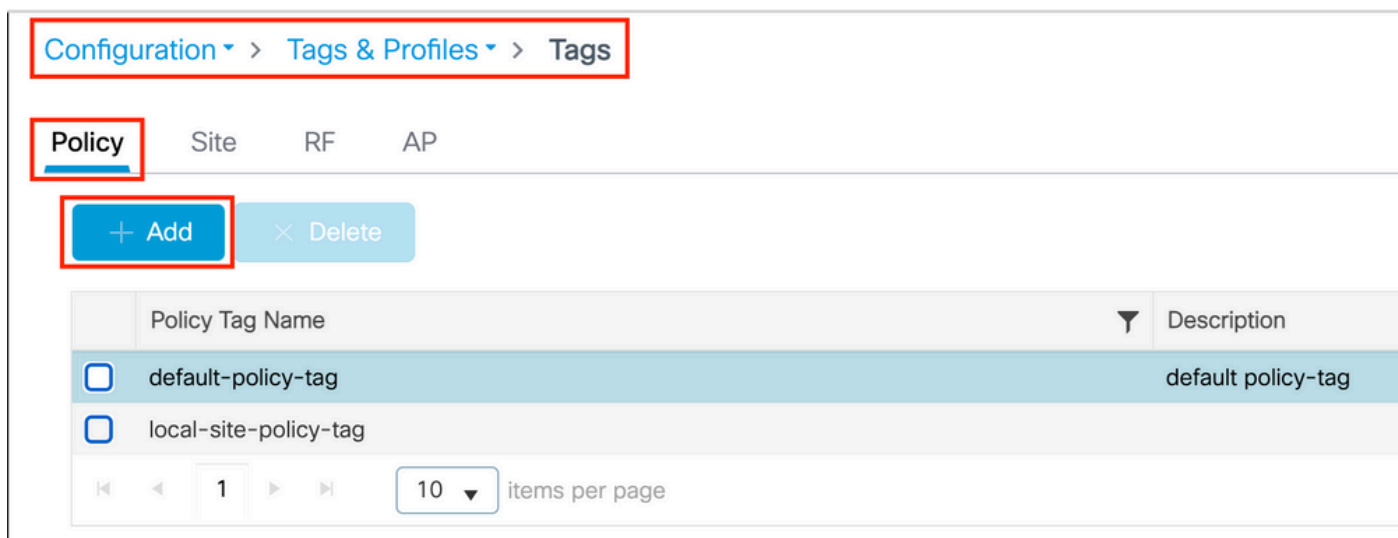
原則標籤組態

在原則標籤內，您可以將 SSID 與原則設定檔連結。您可以建立新的原則標籤，或使用 default-policy-tag。

 **注意：**預設策略標籤會自動將WLAN ID介於1和16之間的任何SSID對映到預設策略配置檔案。無法修改或刪除。如果您的WLAN的ID為17或更新版本，則無法使用預設策略標籤。

GUI：

如果需要，請導航到Configuration > Tags & Profiles > Tags > Policy 並增加一個新路徑，如圖所示。



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

將 WLAN 設定檔連結至想要的原則設定檔。

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 1**

+ Add
✕ Delete

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**

↶ Cancel
📄 Apply to Device

CLI :

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

原則標籤指派

指派原則標籤至需要的 AP。


GUI :

要將標籤分配給一個AP，請導航到Configuration > Wireless > Access Points > AP Name > General Tags，進行所需的分配，然後按一下 Update & Apply to Device。

Edit AP

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

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

 **注意：**請注意，變更AP上的原則標籤後，它會失去與9800 WLC的關聯，並在大約1分鐘內重新加入。

要為多個AP分配相同的策略標籤，請導航到Configuration > Wireless > Wireless Setup > Advanced > Start Now。

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply

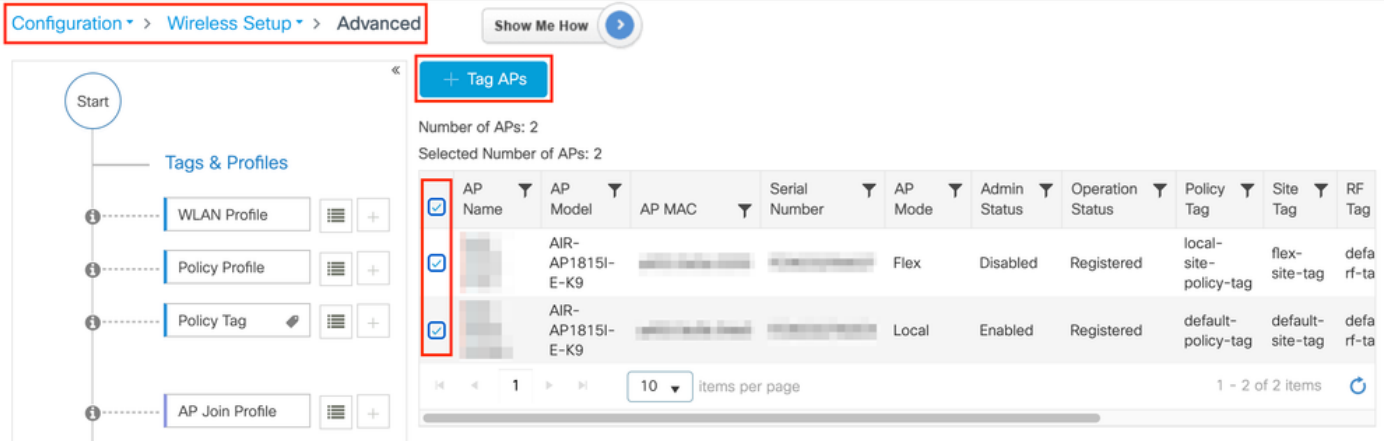


Tag APs

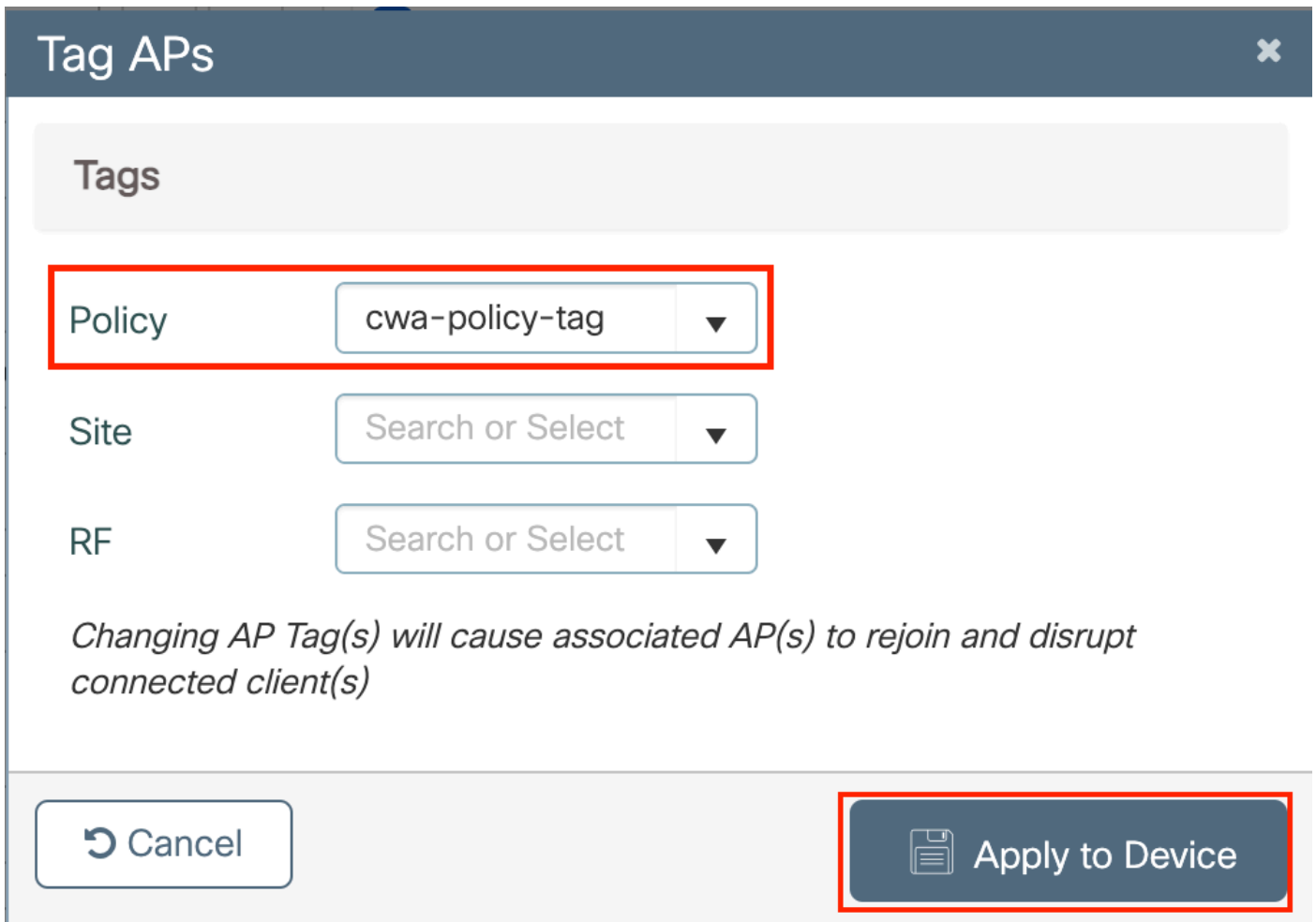


Done

Start Now →



選擇whished Tag並按一下Save & Apply to Device(如圖所示)。



CLI :

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

重新導向 ACL 組態

步驟 1. 導航到 Configuration > Security > ACL > + Add 以建立新的ACL。

為ACL選擇一個名稱，然後將其設定為IPv4 Extended 型別，並將每個規則增加為序列 (如圖所示)。

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

您需要拒絕流向 ISE PSN 節點的流量，並拒絕 DNS 和允許所有其他流量。此重新導向ACL不是安全ACL，而是傳送的ACL，會定義哪些流量會進入CPU (在允許的情況下) 以進行進一步處理 (例如重新導向)，以及哪些流量會保留在資料平面上 (在拒絕時)，並避免重新導向。

ACL必須如下所示 (在本例中用您的ISE IP地址替換10.48.39.28)：


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

 **注意：**對於重定向ACL，請將deny操作視為deny重定向 (非拒絕流量)，將permit操作視為permit重定向。WLC只會檢查可重新導向的流量 (預設為連線埠80和443)。

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
```

 **注意：** 如果使用 `permit ip any any` 結束 ACL 而不是使用側重於埠 80 的許可證，WLC 還會重定向 HTTPS，這通常是不受歡迎的，因為它必須提供自己的證書並始終建立證書衝突。這是之前宣告的一個例外，該宣告表示在發生 CWA 時在 WLC 上不需要證書：如果您啟用了 HTTPS 攔截，則您需要一個證書，但它無論如何都不會被認為是有效的。

您可以透過操作改進 ACL，僅拒絕訪客埠 8443 到達 ISE 伺服器。

啟用 HTTP 或 HTTPS 重新導向

Web 管理員門戶配置與 Web 身份驗證門戶配置繫結，它需要在埠 80 上偵聽才能進行重定向。因此，必須啟用 HTTP 才能讓重新導向正常運作。您可以選擇全域啟用 (使用 `ip http server` 命令)，或是僅為 Web 驗證模組啟用 HTTP (使用引數對應下的命令 `webauth-http-enable`)。



注意：重定向HTTP流量發生在CAPWAP內部，即使FlexConnect本地交換也是如此。由於是WLC執行偵聽工作，因此AP在CAPWAP隧道內傳送HTTP(S)資料包，並在CAPWAP中接收從WLC重新定向的重定向消息

如果您希望在嘗試訪問HTTPS URL時進行重定向，然後在引數對映下增加命令intercept-https-enable，但請注意，這不是最佳配置，它對WLC CPU有影響，無論如何都會生成證書錯誤：

<#root>

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

`intercept-https-enable`

`trustpoint xxxxx`

您還可以在GUI上執行此操作，並在引數對映中選中Web Auth intercept HTTPS(Configuration > Security > Web Auth)。

The screenshot displays the Cisco ISE GUI configuration interface. On the left is a dark sidebar with navigation options: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth'. It features a table with one entry, 'global', which is selected. Below the table is a pagination control showing '1' of 10 items per page. On the right, the 'Edit Web Auth Parameter' panel is open, showing various settings: Maximum HTTP connections (100), Init-State Timeout(secs) (120), Type (webauth), Virtual IPv4 Address (empty), Trustpoint (--- Select ---), Virtual IPv6 Address (xxxxxx::x), Web Auth intercept HTTPS (checked), and Captive Bypass Portal (unchecked). The 'Web Auth intercept HTTPS' checkbox is highlighted with a red rectangle.

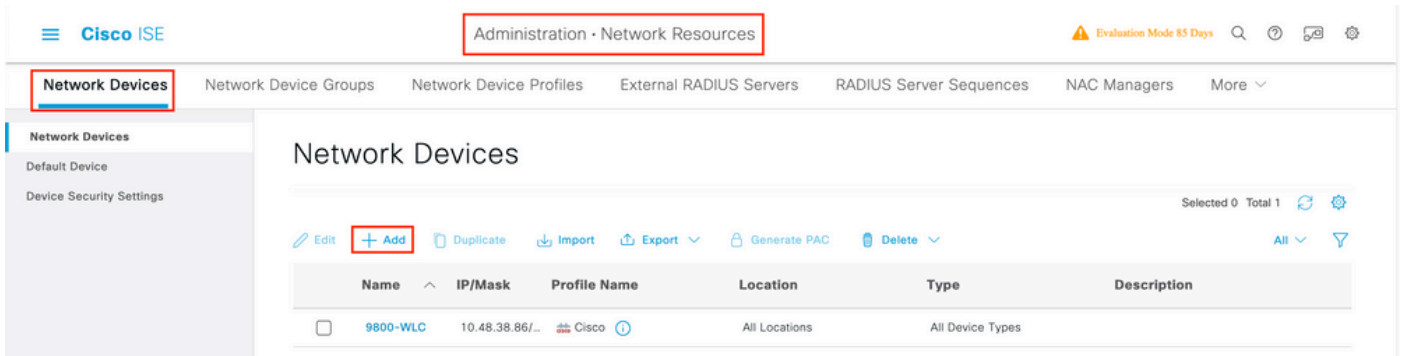


注意：預設情況下，瀏覽器使用HTTP網站啟動重定向進程，如果需要HTTPS重定向，則必須選中Web Auth intercept HTTPS；但是，由於此配置會增加CPU使用率，因此不建議使用此配置。

ISE 組態

將 9800 WLC 新增至 ISE

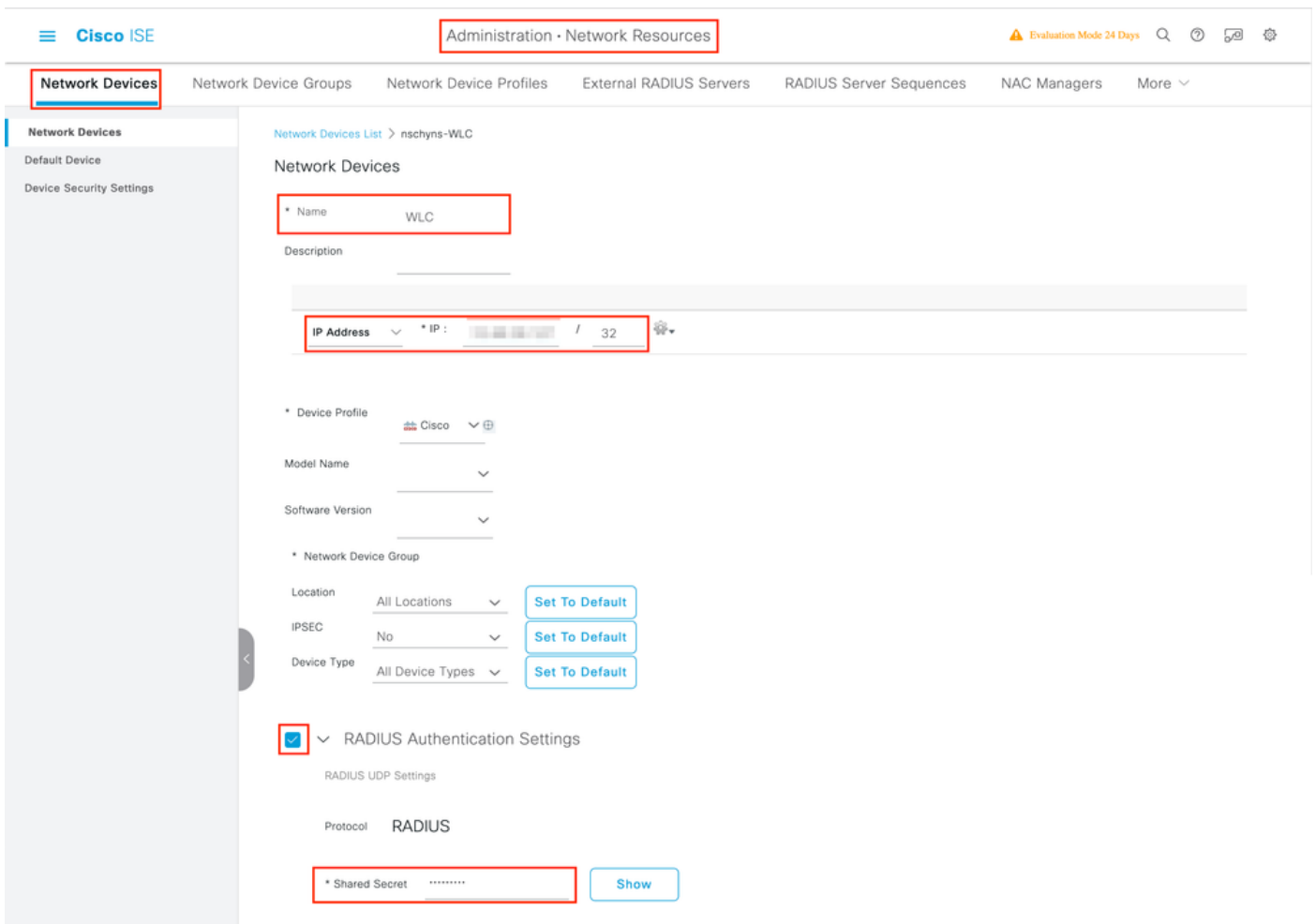
步驟 1. 打開ISE控制檯並導航到Administration > Network Resources > Network Devices > Add，如圖所示。



步驟 2. 配置網路裝置。

它可以是指定的型號名稱、軟體版本和說明，並根據裝置型別、位置或WLC分配網路裝置組。

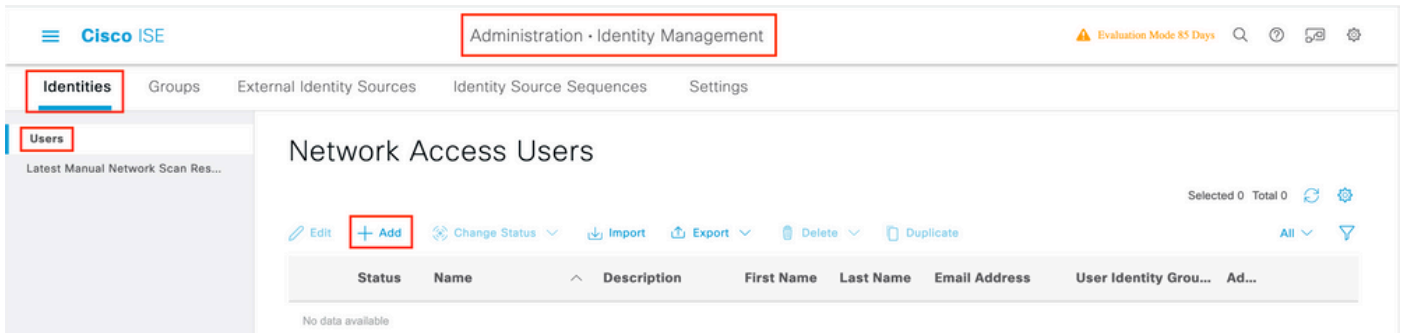
這裡的IP位址對應到傳送驗證要求的WLC介面。預設情況下，這是管理介面，如下圖所示：



有關網路裝置組的詳細資訊，請參閱ISE管理指南章節：管理網路裝置：[ISE-網路裝置組](#)。

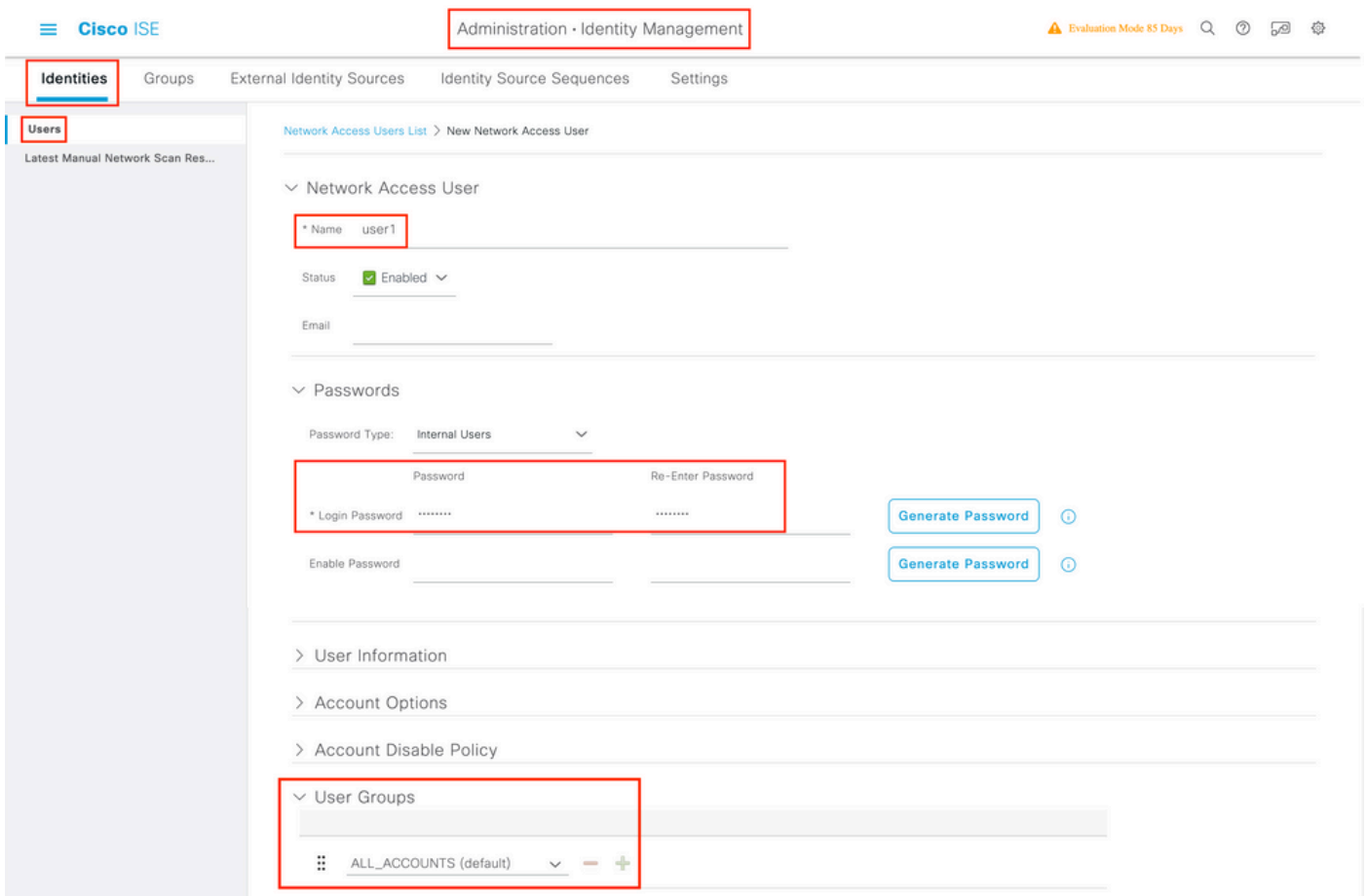
在 ISE 上建立新使用者

步驟 1. 導覽至Administration > Identity Management > Identities > Users > Add ，如下圖所示。



步驟 2. 輸入資訊。

在本示例中，此使用者屬於名為ALL_ACCOUNTS的組，但可以根據需要進行調整，如圖所示。



建立授權設定檔

策略配置檔案是根據客戶端引數 (如MAC地址、憑證、使用的WLAN等) 分配給客戶端的結果。它可以指定特定的設定，例如虛擬區域網路(VLAN)、存取控制清單(ACL)、統一資源定位器(URL)重新導向等等。

請注意，在最近的 ISE 版本中，Cisco_Webauth 授權結果已存在。此處，您可編輯該項目以修改重新導向 ACL 名稱，使其符合您在 WLC 上設定的名稱。

步驟 1. 導航到 Policy > Policy Elements > Results > Authorization > Authorization Profiles。點選add以建立您自己的結果或編輯 Cisco_Webauth預設結果。

Policy · Policy Elements

Authentication

Authorization

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 11

Edit + Add Duplicate Delete

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you config
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.

步驟 2. 輸入重新導向資訊。確保ACL名稱與9800 WLC上配置的ACL名稱相同。

Policy · Policy Elements

Authorization Profiles > Cisco_WebAuth

Authorization Profile

Name: Cisco_WebAuth

Description: Default Profile used to redirect users to the CWA portal.

Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Agentless Posture:

Passive Identity Tracking:

Common Tasks

- Web Redirection (CWA, MDM, NSP, CPP)
 - Centralized Web Auth: ACL REDIRECT
 - Value: Self-Registered Guest Portal (c)
- Display Certificates Renewal
- Message
- Static IP/Host name/FQDN

設定驗證規則

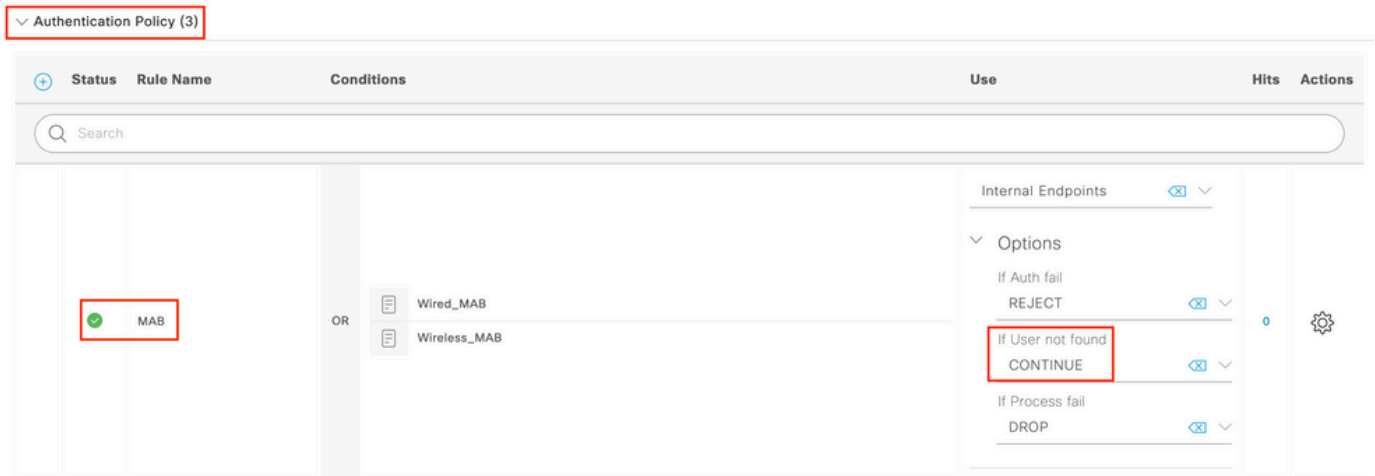
步驟 1. 策略集定義身份驗證和授權規則的集合。要建立策略集，請導航到Policy > Policy Sets，按一下清單中第一個策略集的齒輪，然後選Insert new row，或者按一下右側的藍色箭頭選擇預設策略集。

Policy · Policy Sets

Reset Reset Policyset Hitcounts Save

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

步驟 2.展開Authentication policy。對於MAB規則（有線或無線MAB上的匹配），展開Options，然後選擇CONTINUE選項，以免顯示「If User not found」。

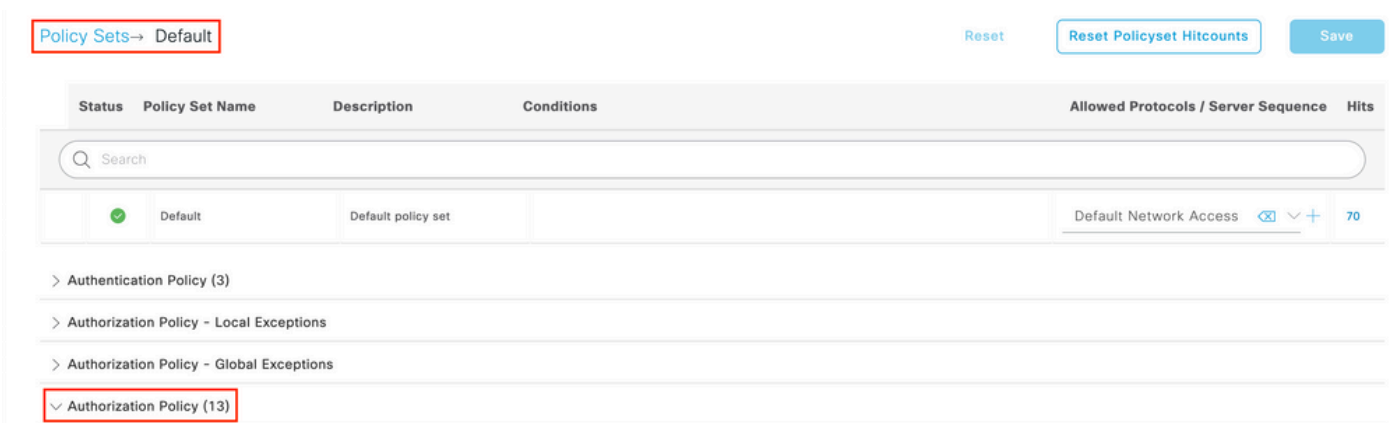


步驟 3.按一下Save 以儲存更改。

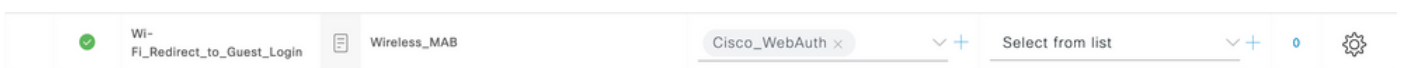
設定授權規則

授權規則為負責決定哪個權限（哪個授權設定檔）結果套用至用戶端的項目。

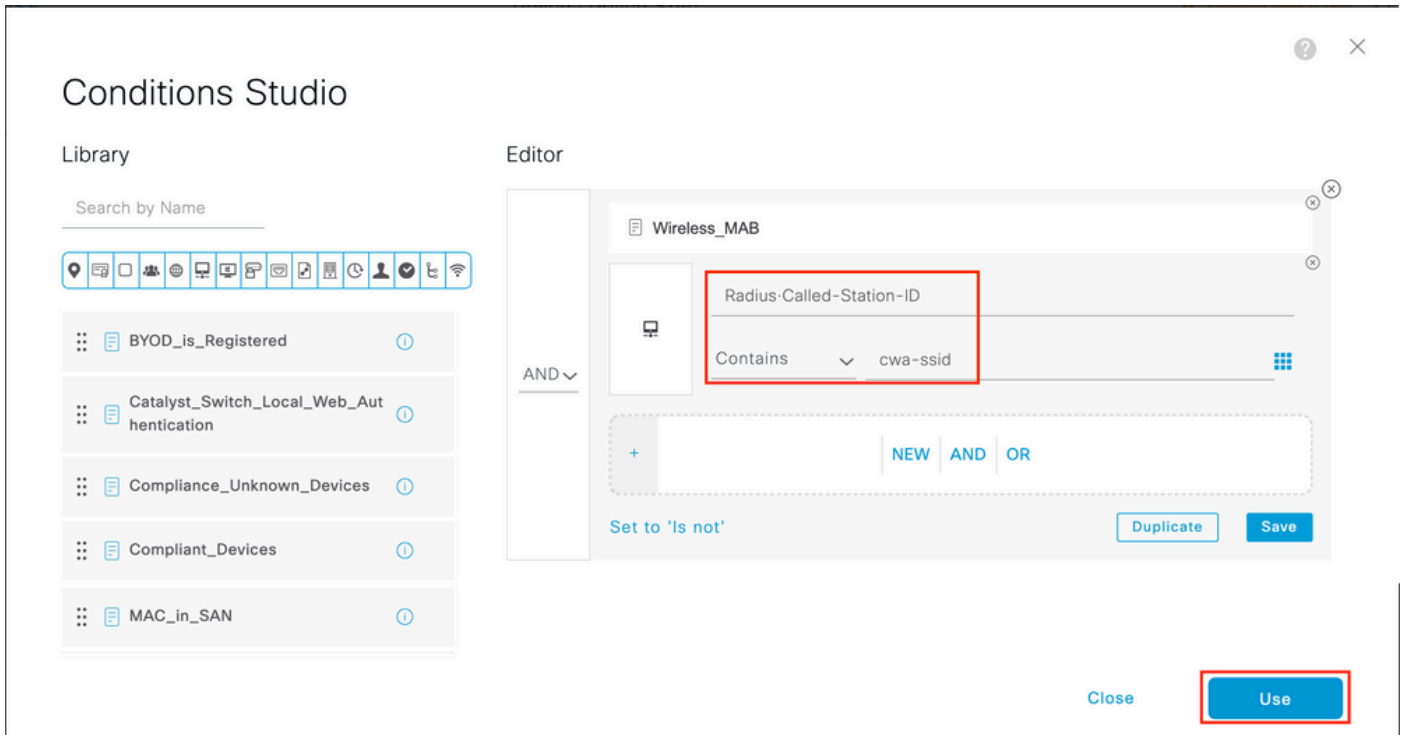
步驟 1.在同一策略集頁上，關閉Authentication Policy並展開Authorziation Policy，如圖所示。



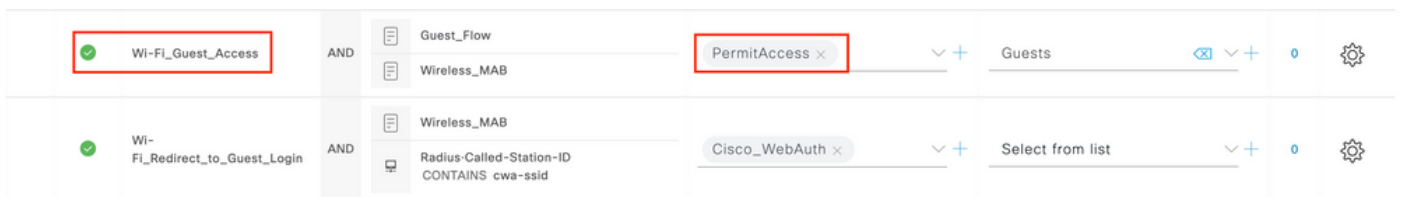
步驟 2.最近ISE版本以名為Wifi_Redirect_to_Guest_Login的預建立規則開始，它主要滿足我們的需求。將左邊的灰色符號轉為enable。



步驟 3.該規則僅匹配Wireless_MAB並返回CWA重定向屬性。現在，您可以選擇增加一些小扭曲，使其僅與特定SSID匹配。選擇條件（目前的Wireless_MAB）以顯示Conditions Studio。在右側增加條件，然後選擇帶有Called-Station-ID屬性的Radius詞典。使其符合您的SSID名稱。使用螢幕底部的Use進行驗證，如圖所示。



步驟 4.現在，您需要一條優先順序更高的規則，用於匹配Guest Flow條件，以便在使用者在門戶上進行身份驗證後返回網路訪問詳細資訊。您可以使用Wifi Guest Access規則，該規則在預設情況下也預先在最新的ISE版本上建立。接著，您僅須藉由左側顯示的綠色標示啟用規則。您可以返回預設PermitAccess或配置更精確的訪問清單限制。



步驟 5.儲存規則。

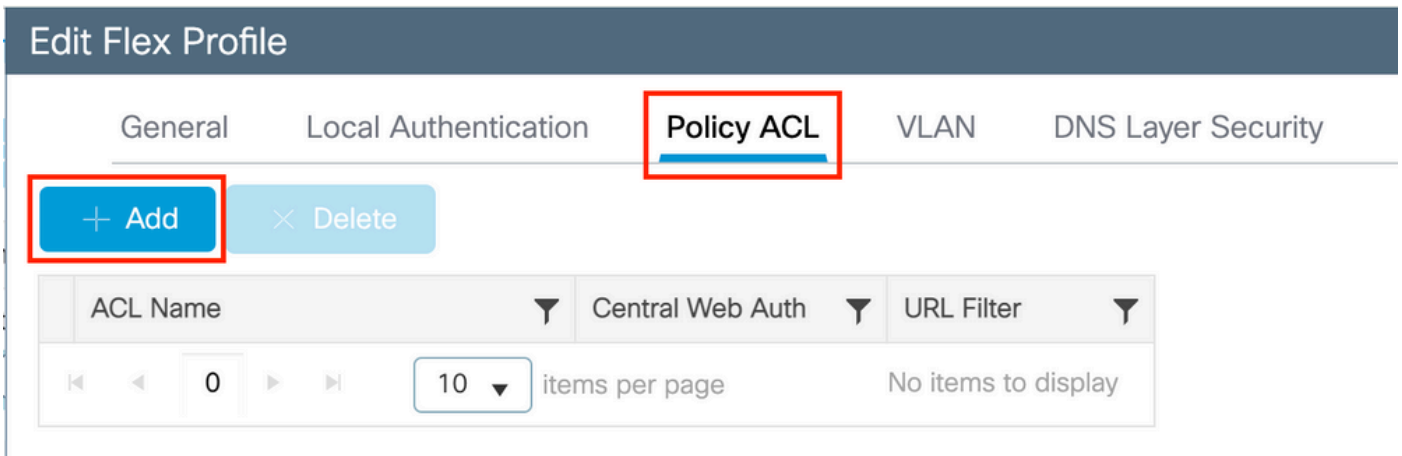
按一下規則底部的Save。

僅限 FlexConnect 本機交換存取點


假設您擁有 Flexconnect 本機交換存取點和 WLAN 會如何？先前的章節仍然有效。但是，您需要執行額外的步驟，以便提前將重定向ACL推送到AP。

導航到Configuration > Tags & Profiles > Flex，然後選擇您的Flex配置檔案。然後，導航至Policy ACL頁籤。

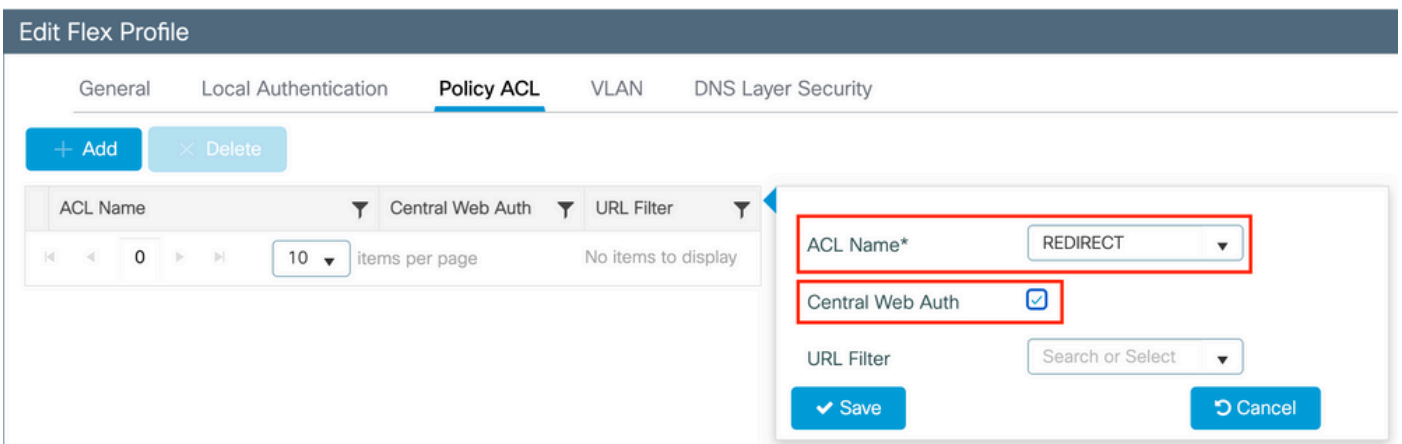
按一下Add（如圖所示）。



選擇您的重新導向ACL名稱並啟用中央Web驗證。此核取方塊會自動反轉AP本身的ACL (這是因為「deny」陳述式在Cisco IOS XE的WLC上表示「請勿重新導向到此IP」)。但是，在AP上，「deny」語句的含義相反。因此，此覈取方塊會在向AP推送許可證時自動交換所有許可證並拒絕它們。您可以透過AP CLI中的show ip access list命令進行驗證。

 **注意：**在Flexconnect本地交換方案中，ACL必須特別提及返回語句 (在本地模式下不一定需要)，因此請確保所有ACL規則都涵蓋兩種流量方式 (例如，來往於ISE)。

別忘了先按下Save鍵，然後按下Update and apply to the device鍵。



憑證

要使客戶端信任Web身份驗證證書，不需要在WLC上安裝任何證書，因為提供的唯一證書是ISE證書 (必須由客戶端信任)。

驗證

您可以使用以下命令確認目前的組態。

<#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>
```

以下為對應此範例的WLC組態相關部分：

<#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 ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akmdot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

疑難排解

檢查清單

- 確保客戶端連線並獲得有效的IP地址。
- 如果重新導向不是自動的，請開啟瀏覽器並嘗試隨機IP位址。例如10.0.0.1。如果重新導向有效，可能是因為您有DNS解析問題。確認您有透過DHCP提供的有效DNS伺服器，並且該伺服器可以解析主機名。
- 確保配置了ip http server命令，以便在HTTP上進行重定向（轉發）正常運行。Web管理員門戶配置與Web身份驗證門戶配置繫結，需要將其列在埠80上才能進行重定向。您可以選擇全域啟用(使用ip http server命令)，或是僅為Web驗證模組啟用HTTP(使用引數對應下的命令webauth-http-enable)。
- 如果在嘗試訪問HTTPS URL時沒有重定向此消息（這是必需的），請驗證引數對映下是否有命令intercept-https-enable：

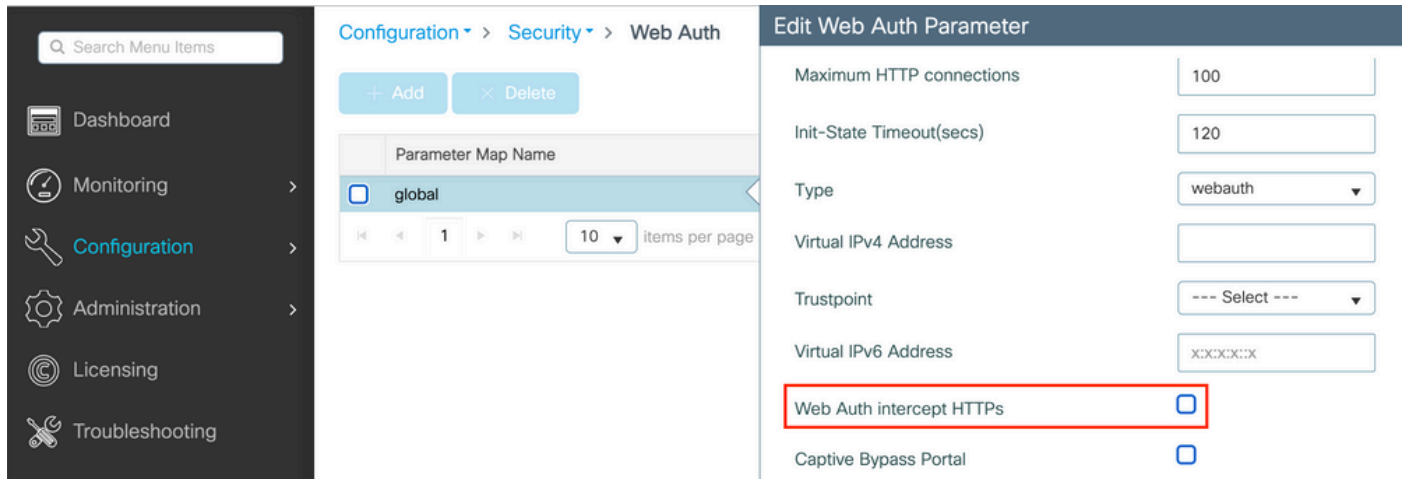
<#root>

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

intercept-https-enable

trustpoint xxxxx

您還可以透過GUI檢查是否選中「Parameter Map :



RADIUS的服務連線埠支援

Cisco Catalyst 9800系列無線控制器的服務埠稱為GigabitEthernet 0埠。自版本17.6.1起，透過此埠支援RADIUS (包括CoA)。

如果要使用RADIUS的服務埠，則需要此配置：

<#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
```

收集調試

WLC 9800 提供永不間斷的追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別的消息持續記錄，並且您可以在事件發生後檢視事件或故障條件的日誌。



註：您可以在日誌中返回幾小時到幾天，但取決於生成的日誌量。

為了檢視9800 WLC預設收集的跟蹤，您可以透過SSH/Telnet連線到9800 WLC並執行以下步驟（確保將會話記錄到文本檔案中）。

步驟 1. 檢查WLC目前時間，以便您可以追蹤問題發生時的記錄。

```
<#root>
```

```
# show clock
```

步驟 2. 根據系統配置的指示，從WLC緩衝區或外部系統日誌收集系統日誌。這樣可以快速檢視系統的運行狀況和錯誤（如果有）。

```
<#root>
```

```
# show logging
```

步驟 3. 驗證是否啟用了任何調試條件。

```
<#root>
```

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



注意：如果發現列出任何條件，則意味著所有遇到啟用條件（MAC地址、IP地址等）的進程的跟蹤將記錄到調試級別。這將增加日誌的量。因此，建議您在不主動調試時清除所有條件。

步驟 4. 假設步驟3中沒有將正在測試的mac地址列為條件，收集特定mac地址的always-on notice level跟蹤。


```
<#root>
```

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

您可顯示作業階段中的內容，或可將檔案複製到外部 TFTP 伺服器。

```
<#root>
```

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

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

條件式偵錯和無線電主動式追蹤

如果永遠線上的追蹤無法提供足夠資訊來判斷觸發調查中問題的原因，您可以啟用條件式偵錯並擷取「無線電作用中(RA)」追蹤，此追蹤會為與指定條件（此案例為使用者端mac位址）互動的所有處理作業提供偵錯層級追蹤。若要啟用條件式除錯，請繼續執行以下步驟。

步驟 5. 確保未啟用調試條件。

```
<#root>
```


```
# clear platform condition all
```


步驟 6. 為要監控的無線客戶端MAC地址啟用調試條件。

以下命令會開始監控提供的 MAC 位址 30 分鐘（1800 秒）。您可選擇將此時間增加至 2085978494 秒。

```
<#root>
```

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

 注意：要同時監控多個客戶端，請對每個mac地址運行debug wireless mac<aaaa.bbbb.cccc> 命令。

 注意：您不會在終端會話中看到客戶端活動的輸出，因為所有內容都在內部緩衝，以便以後檢視。

步驟7'。重現您要監控的問題或行為。

步驟 8.如果在預設或配置的監控時間之前重現問題，則停止調試。

```
<#root>
```

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

一旦經過監控時間或停止偵錯無線，9800 WLC會產生具有以下名稱的本機檔案：

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步驟9.收集MAC地址活動的檔案。您可以將ra trace .log複製到外部伺服器，或直接在螢幕上顯示輸出。

檢查 RA 追蹤檔案的名稱。

```
<#root>
```

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

將檔案複製到外部伺服器：

```
<#root>
```

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

顯示內容：

```
<#root>
```

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

步驟 10. 如果根本原因仍不明顯，請收集內部日誌，這些日誌是調試級別日誌的更詳細檢視。您不需要再次調試客戶端，因為我們只需進一步詳細檢視已收集並內部儲存的調試日誌。

```
<#root>
```

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



注意：此命令輸出返回所有進程的所有日誌級別的跟蹤，而且數量非常大。與Cisco TAC接洽，幫助分析這些跟蹤。

您可以將ra-internal-FILENAME.txt複製到外部伺服器，或直接在螢幕上顯示輸出。

將檔案複製到外部伺服器：

```
<#root>
```

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

顯示內容：

```
<#root>
```

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

步驟 11. 移除偵錯條件。

```
<#root>
```

```
# clear platform condition all
```



注意：請確保在排除會話故障後始終刪除調試條件。

範例

如果身份驗證結果不是您預期的結果，請務必導航到ISEOperations > Live logs頁面並獲取身份驗證結果的詳細資訊。

系統將顯示失敗原因（如果出現故障）和ISE接收的所有RADIUS屬性。

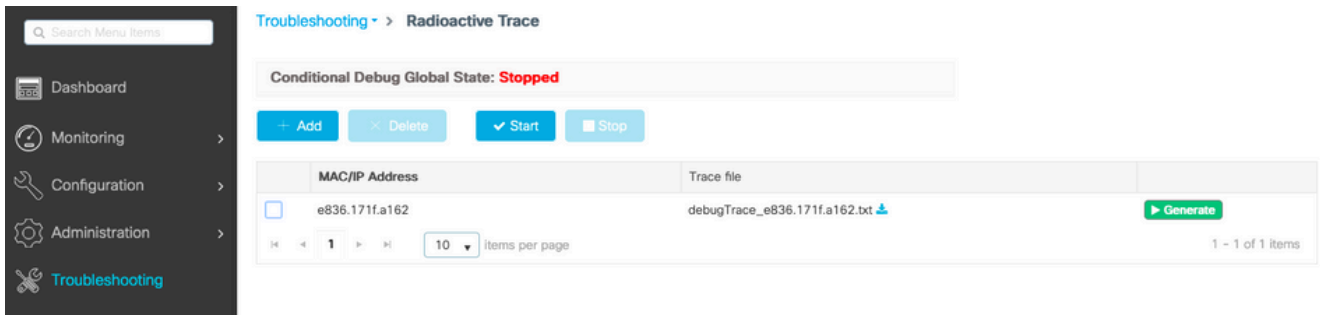
在下個範例中，由於無任何授權規則符合，因此ISE拒絕驗證。這是因為，您會看到被呼叫站ID屬性作為SSID名稱附加到AP MAC地址，而授權與SSID名稱完全匹配。該規則更改為「包含」而非「等於」，即可修復該規則。

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



在這種情況下，問題出在您建立ACL名稱時進行了拼寫，但該名稱與ISE返回的ACL名稱不匹配，或者WLC投訴沒有像ISE請求的ACL：

<#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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。