

使用外部身份驗證配置本地Web身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[Web驗證](#)

[身份驗證型別](#)

[用於身份驗證的資料庫](#)

[本地Web驗證](#)

[使用外部驗證的本地Web驗證](#)

[設定](#)

[網路圖表](#)

[在CLI上配置使用外部身份驗證的本地Web身份驗證](#)

[配置AAA伺服器 and 伺服器組](#)

[配置本地身份驗證和授權](#)

[配置引數對映](#)

[配置WLAN安全引數](#)

[建立無線策略配置檔案](#)

[建立策略標籤](#)

[為AP分配策略標籤](#)

[在WebUI上配置使用外部身份驗證的本地Web身份驗證](#)

[9800 WLC 的 AAA 組態](#)

[WebAuth組態](#)

[WLAN 組態](#)

[原則設定檔組態](#)

[原則標籤組態](#)

[原則標籤指派](#)

[ISE 組態](#)

[連線訪客客戶端](#)

[驗證](#)

[顯示WLAN摘要](#)

[顯示引數對映配置](#)

[顯示AAA資訊](#)

[疑難排解](#)

[常見問題](#)

[條件式偵錯和無線電主動追蹤以及嵌入式封包擷取](#)

[成功嘗試的示例](#)

[相關資訊](#)

簡介

本文說明如何在9800 WLC和ISE上使用外部身份驗證配置本地Web身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- 9800無線LAN控制器(WLC)組態
- 輕量型存取點(LAP)
- 如何設定和配置外部Web伺服器身份服務引擎(ISE)。
- 如何設定和配置DHCP和DNS伺服器。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800-40 WLC Cisco IOS® XE版本17.18.4a，帶APSP1和APSP2
- 身分識別服務引擎(ISE)，版本3.2.0.542
- Cisco®無線9172I系列Wi-Fi 7接入點，版本17.18.4.202

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。

Web驗證

Web驗證是第3層安全功能，允許訪客使用者存取網路。

此功能旨在提供對開放式SSID的簡單、安全的訪客訪問，無需配置使用者配置檔案，並且還可以與第2層安全方法配合使用。

Web驗證的目的在於允許不可信裝置（訪客）透過可設定安全機制的訪客WLAN以有限網路存取許可權，且網路的安全性不會受到損害。訪客使用者要訪問網路，需要成功進行身份驗證，即需要提供正確憑證或接受可接受使用策略(AUP)才能訪問網路。

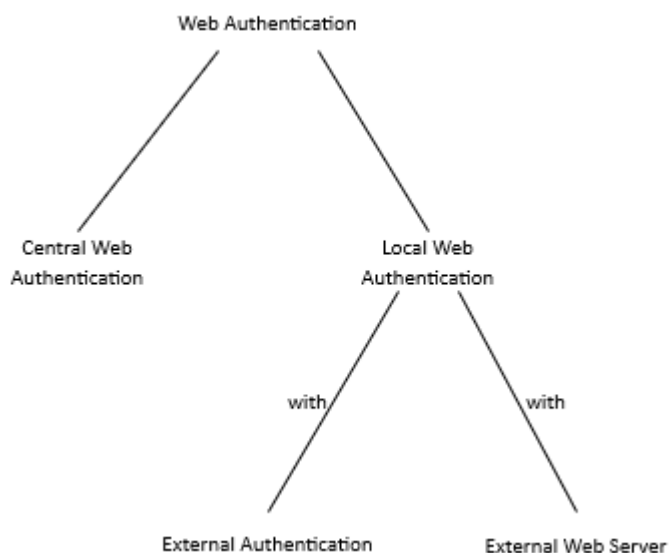
Web驗證對公司來說是一項優勢，因為它提高了使用者忠誠度，使公司遵守了訪客使用者必須接受的免責宣告，並允許公司與訪客進行接觸。

要部署Web驗證，必須考慮如何處理訪客入口和驗證。有兩種常見方法：

- 本地Web驗證(LWA):將訪客使用者直接從WLC重新導向到入口的方法。重新導向和預先WebAuth ACL是在WLC本機上設定的。
- 中央Web驗證(CWA):一種訪客使用者重新導向的方法，其中重新導向URL和重新導向ACL是集中設定在外部伺服器（例如ISE）上，並透過RADIUS傳送到WLC。在中央Web驗證中，重新導向URL和重新導向ACL是位於外部伺服器（例如RADIUS）上的中央位置。RADIUS伺服器是處理驗證的伺服器，它會將指令傳送到WLC。在CWA中，WLC不需要本地Web身份驗證證書，中央Web門戶只需要一個證書，並且需要中央身份驗證伺服器，例如ISE。要詳細閱讀CWA，請導覽至[在Catalyst 9800 WLC和ISE上設定中央Web驗證\(CWA\)](#)。

在本地Web驗證中，Web輸入網站可以位於WLC上或外部伺服器上。在使用外部驗證的LWA中，WLC上存在Web輸入網站。在帶有外部Web伺服器的LWA中，Web門戶位於外部伺服器（例如Cisco DNA Spaces）上。以下詳細介紹使用外部Web伺服器的LWA示例：[使用Catalyst 9800 WLC配置DNA空間捕獲門戶](#)。

不同Web驗證方法的示意圖：



不同Web驗證方法的圖表



附註：如果您在9800 WLC上部署使用Web驗證的Wi-Fi 7 AP，請確保您正在運行推薦的Cisco IOS XE版本，例如17.18.4a或更高版本。

身份驗證型別

對訪客使用者進行身份驗證有四種型別：

- Webauth:輸入使用者名稱和密碼。
- 同意 (USB傳輸)：接受AUP。
- Authbypass:根據訪客使用者裝置的MAC地址進行身份驗證。
- Web同意：使用者名稱/密碼和接受AUP的混合。

webauth	authbypass	consent	webconsent
Username: Password: OK	Client connects to the SSID and gets an IP address, then the 9800 WLC checks if the MAC address is allowed to enter the network, if yes, it is moved to RUN state, if it is not it is not allowed to join. (It won't fall back to web authentication)	banner1 ☒ Accept ☐ Don't Accept OK	banner login ☒ Accept ☐ Don't Accept Username: Password: OK

用於對訪客使用者進行身份驗證的四種身份驗證型別

用於身份驗證的資料庫

身份驗證的憑據可以儲存在LDAP伺服器上、本地儲存在WLC或RADIUS伺服器上。

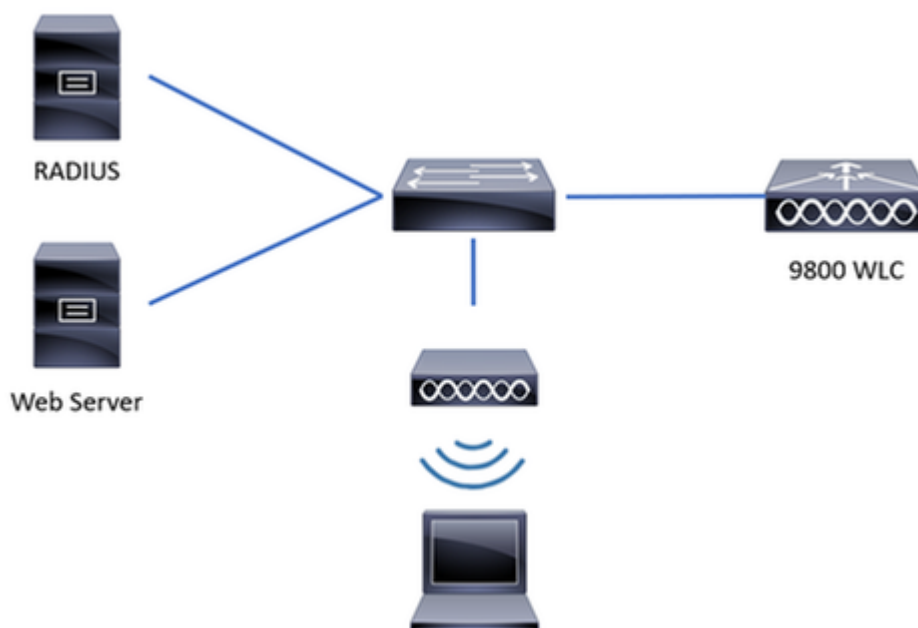
- 本地資料庫：憑證 (使用者名稱和密碼) 儲存在WLC本機。
- LDAP資料庫：憑據儲存在LDAP後端資料庫中。WLC向LDAP伺服器查詢資料庫中特定使用者的憑證。
- RADIUS資料庫：憑證儲存在RADIUS後端資料庫。WLC會向RADIUS伺服器查詢資料庫中特定使用者的認證。

本地Web驗證

在本地Web驗證中，訪客使用者會直接從WLC重新導向到Web輸入網站。

Web輸入網站可以位於WLC中或其他伺服器中。如此一來，本地化的特點為重新導向URL和匹配流量的ACL必須位於WLC上（不是Web輸入網站的位置）。在LWA中，當訪客使用者連線到訪客WLAN時，WLC會攔截來自訪客使用者的連線，並將其重新導向到要求訪客使用者進行驗證的Web輸入網站URL。訪客使用者輸入憑證（使用者名稱和密碼）時，WLC會擷取憑證。WLC會使用LDAP伺服器、RADIUS伺服器或本機資料庫（WLC本機上有資料庫）驗證訪客使用者的身分。對於RADIUS伺服器（外部伺服器，如ISE），它不僅可用於儲存憑證，還可用於提供裝置註冊和自我調配選項。如果是外部Web伺服器（例如Cisco DNA Spaces），則系統會顯示Web輸入網站。在LWA中，WLC上有一個憑證，Web入口上有一個憑證。

該圖表示LWA的通用拓撲：



LWA的通用拓撲

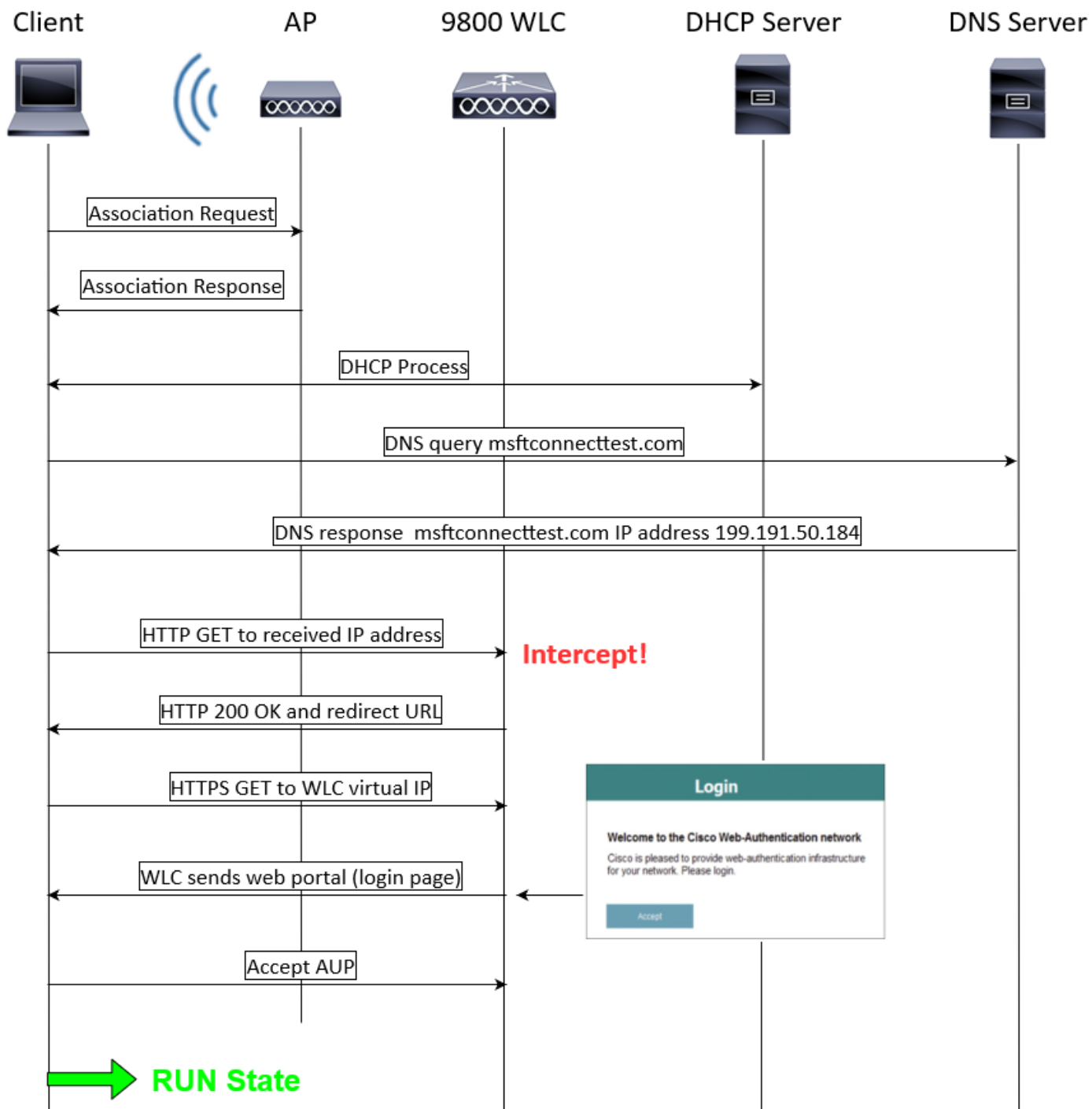
LWA網路拓撲中的裝置：

- 用戶端:向DHCP和DNS伺服器傳送請求，請求對訪客WLAN的訪問，並響應來自WLC的請求。
- 存取器:連線到交換機，廣播訪客WLAN，並為訪客使用者裝置提供無線連線。還允許在訪客使用者通過身份驗證（在輸入有效憑證之前）之前使用DHCP和DNS資料包。
- WLC:管理AP和客戶端。WLC託管重新導向URL和匹配流量的ACL。攔截來自訪客使用者的HTTP請求，將其重定向到訪客使用者必須進行身份驗證的Web門戶（登入頁面）。它捕獲憑證並對訪客使用者進行身份驗證，並向外部伺服器、LDAP伺服器或本地資料庫傳送訪問請求，以確認憑證是否有效。
- 身份驗證伺服器：使用存取接受/拒絕來回應來自WLC的存取要求。驗證伺服器會驗證來自訪客使用者的憑證，如果憑證有效或無效，便會通知WLC。如果憑證有效，則訪客使用者被授權訪問網路（身份驗證伺服器提供裝置註冊和自我調配的選項）。如果憑證無效，則拒絕訪

客使用者訪問網路。

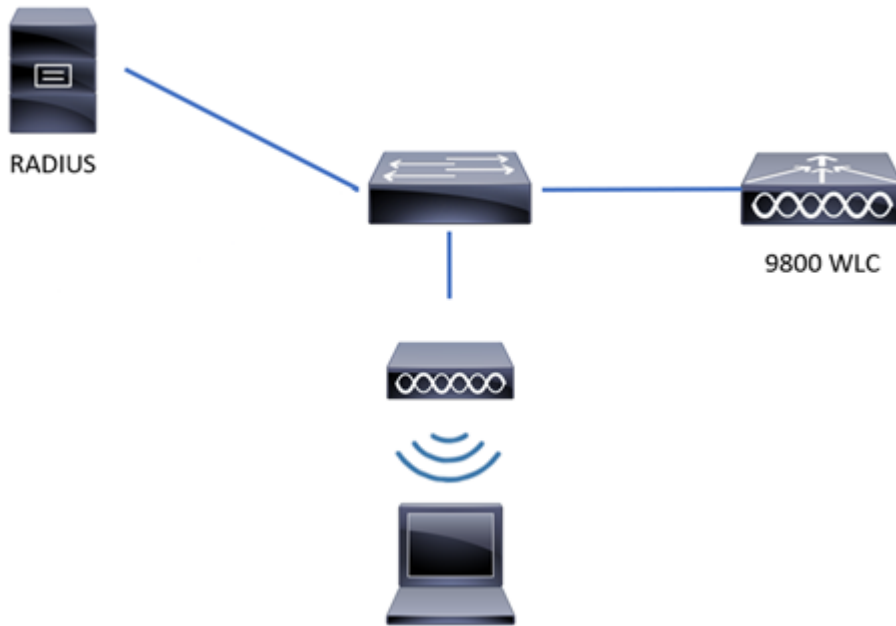
LWA流：

- 訪客使用者會與廣播訪客WLAN的AP建立關聯。
- 訪客使用者通過DHCP過程以獲取IP地址。
- 訪客使用者希望對強制網路門戶進行Internet連線檢查。如果是蘋果裝置，它會嘗試蘋果強制網路門戶；如果是Android裝置，它會嘗試Android強制網路門戶；如果是Windows裝置，它會嘗試Windows連線測試門戶。
- 訪客使用者傳送DNS查詢以請求強制網路門戶IP地址。DNS伺服器使用對應IP地址響應查詢。
- 訪客使用者向強制網路門戶的IP地址傳送HTTP GET消息。
- WLC會攔截該訊息，並使用HTTP 200 OK和重新導向URL回覆訪客使用者。
- 訪客使用者向WLC虛擬IP傳送HTTPS GET訊息，WLC會使用Web入口進行回應。
- 系統會要求訪客使用者在Web門戶中輸入身份驗證憑證。
- Web入口會使用提供的憑證將使用者重新導向回WLC（如果使用外部Web入口）。
- WLC透過本機資料庫驗證訪客使用者，或向RADIUS或LDAP伺服器傳送查詢，以確認憑證是否正確（如果驗證型別是webconsent或webauth）。
- 如果憑證正確，WLC會對訪客使用者進行驗證，使其進入RUN狀態。如果憑證錯誤，WLC會刪除訪客使用者。
- WLC將使用者端重新導向回在Web瀏覽器中輸入的原始URL。



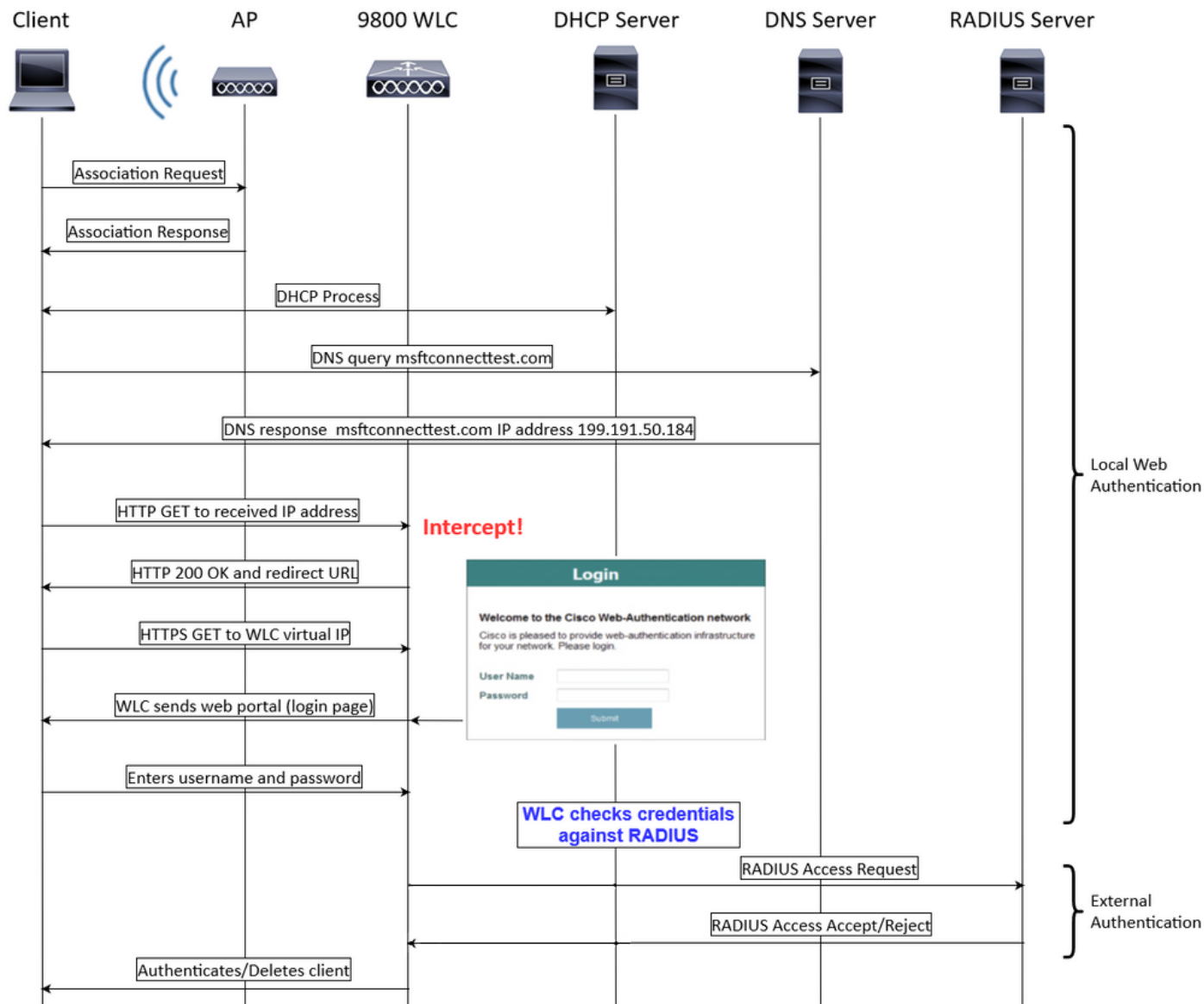
LWA流

使用外部驗證的本地Web驗證



LWA-EA的通用拓撲

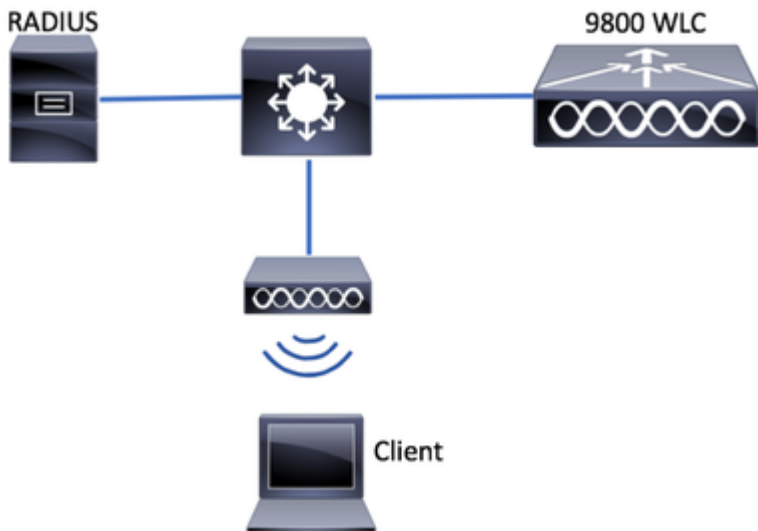
LWA-EA是LWA的一種方法，其中Web門戶和重定向URL位於WLC上，而憑證儲存在外部伺服器（例如ISE）上。WLC會擷取憑證並通過外部RADIUS伺服器驗證使用者端。訪客使用者輸入憑證時，WLC會針對RADIUS檢查憑證，然後傳送RADIUS存取要求，並從RADIUS伺服器接收RADIUS存取接受/拒絕。然後，如果憑證正確，則訪客使用者進入RUN狀態。如果憑證不正確，WLC會刪除訪客使用者。



LWA-EA流

設定

網路圖表



網路圖表



附註：此組態範例僅涵蓋中央交換/驗證。Flex本地交換配置對配置Web身份驗證的要求略有不同。

在CLI上配置使用外部身份驗證的本地Web身份驗證

配置AAA伺服器和伺服器組

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4

    auth-port 1812 acct-port 1813

9800WLC(config-radius-server)#key cisco

9800WLC(config-radius-server)#exit

9800WLC(config)#aaa group server radius RADIUSGROUP

9800WLC(config-sg-radius)#server name RADIUS

9800WLC(config-sg-radius)#end
```

配置本地身份驗證和授權

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#end
```

配置WLAN安全引數

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

建立無線策略配置檔案

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

建立策略標籤

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

為AP分配策略標籤

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap
```

>

```
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
```

```
9800WLC(config-ap-tag)#end
```

要在ISE端完成配置，請跳至ISE配置部分。

在WebUI上配置使用外部身份驗證的本地Web身份驗證

9800 WLC 的 AAA 組態

步驟1.將ISE伺服器新增到9800 WLC配置。

導覽至Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add，然後輸入RADIUS伺服器資訊，如下圖所示：

Create AAA Radius Server

General

RadSec

Show Me How >

Name*	RADIUS	Support for CoA ⓘ	ENABLED ☒
Server Address*	192.0.2.30	CoA Server Key Type	Clear Text ▼
PAC Key	☐	CoA Server Key ⓘ	
Key Type	Clear Text ▼	Confirm CoA Server Key	
Key* ⓘ		VRF	
Confirm Key*		Automate Tester	☐
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

Cancel

Apply to Device

9800 WLC 的 AAA 組態

步驟2.新增RADIUS伺服器組。

導覽至Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add，然後輸入RADIUS伺服器群組資訊：

Create AAA Radius Server Group ✕

Name*

RADIUSGROUP

Group Type

RADIUS

Show Me How >

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

☐ DISABLED

IPv4 Source Interface

Search or Select

▼

i

IPv4 VRF

Search or Select

▼

+

IPv6 Source Interface

Search or Select

▼

i

IPv6 VRF

Search or Select

▼

+

Available Servers

Assigned Servers

>

<

>>

<<

RADIUS

▲

▼

▲

▼

▼

Cancel

Apply to Device

新增RADIUS伺服器組

步驟3.建立身份驗證方法清單。

導覽至Configuration > Security > AAA > AAA Method List > Authentication > + Add:

Quick Setup: AAA Authentication

Method List Name*

LWA_AUTHENTICATION

Type*

login

Group Type

group

Fallback to local

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

建立身份驗證方法清單

步驟4.建立授權方法清單。

導覽至Configuration > Security > AAA > AAA Method List > Authorization > + Add:

Quick Setup: AAA Authorization

Method List Name*

LWA_AUTHORIZATION

Type*

network

Group Type

group

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

建立授權方法清單

WebAuth組態

建立或編輯引數對映。選擇型別webauth,虛擬IPv4位址必須是網路上未使用的位址，才能避免IP位址衝突，然後新增一個信任點。

導覽至Configuration > Security > Web Auth > + Add或選擇引數對映：

Configuration > Security > Web Auth

+ Add - Delete

Parameter Map Name

global

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name: global

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ File Name

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-94747...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::XX

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☐

Disable HTTP secure server for Web Auth: ☐

Cancel Update & Apply

WebAuth組態

WLAN 組態

步驟1.建立WLAN。

導覽至「組態」>「標籤和設定檔」>「WLAN」>「+ 新增」，並依需要設定網路。

Add WLAN

General Security Advanced

Profile Name*: LWA_EA

SSID*: LWA_EA

WLAN ID*: 1

Status: ENABLED

Broadcast SSID: ENABLED

Wi-Fi 6E Compatibility: 1/2 requirements met

Wi-Fi 7 Compatibility: 0/3 requirements met 0/3 bands enabled

Radio Policy ⓘ

Show slot configuration

6 GHz Status: ENABLED ⓘ

5 GHz Status: ENABLED

2.4 GHz Status: ENABLED

802.11b/g Policy: 802.11b/g

建立WLAN

步驟2.導覽至Security > Layer2，然後在Layer 2 Security Mode中選擇None。

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

☐ WPA + WPA2 ☐ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☒ None

MAC Filtering ☐

OWE Transition Mode ☐

Lobby Admin Access ☐

建立WLAN安全性

步驟3.導覽至Security > Layer3，然後在Web Policy上勾選此方塊，在Web Auth Parameter Map上選擇引數名稱，然後在Authentication List上選擇先前建立的驗證清單。

Add WLAN

General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy ☒ [Show Advanced Settings >>>](#)

Web Auth Parameter Map

Authentication List

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

建立WLAN驗證清單

WLAN顯示在WLAN list上：

Configuration > Tags & Profiles > WLANs

+ Add

× Delete

Clone

Enable WLAN

Disable WLAN

WLAN Wizard

Selected WLANs : 0

☐	Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
☐		LWA_EA	1	LWA_EA	[open],[Web Auth]	

1

10

1 - 1 of 1 items

已建立WLAN

原則設定檔組態

在策略配置檔案中，您可以選擇分配客戶端的VLAN以及其他設定。

您可使用預設原則設定檔，或可建立新的設定檔。

步驟 1. 建立新的原則設定檔。

導覽至Configuration > Tags & Profiles > Policy，然後配置您的預設策略配置檔案或建立新配置檔案。

確認設定檔已啟用。

Add 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*

POLICY_PROFILE

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

建立新的策略配置檔案

步驟 2. 選取 VLAN。

導覽至「存取原則」標籤，然後從下拉式清單選取 VLAN 名稱，或手動輸入 VLAN-ID。

The screenshot shows the 'Add Policy Profile' window with the 'Access Policies' tab selected. A warning message at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' The 'Access Policies' tab is highlighted with a red box. Below the tabs, there are sections for 'WLAN Local Profiling' (with checkboxes for RADIUS Profiling, HTTP TLV Caching, and DHCP TLV Caching), 'Global State of Device Classification' (set to Disabled), and 'Local Subscriber Policy Name' (a search field). The 'VLAN' section is highlighted with a red box and contains a 'VLAN/VLAN Group' dropdown menu showing 'VLAN1432' (also highlighted with a red box) and a 'Multicast VLAN' field. To the right, there are sections for 'WLAN ACL' (with IPv4 and IPv6 ACL search fields), 'URL Filters' (with Pre Auth and Post Auth search fields), and 'Advanced' settings. At the bottom, there is a 'Cancel' button and a highlighted 'Apply to Device' button (indicated by a red box).

選擇VLAN

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。

如有需要，請導覽至「組態」>「標籤和設定檔」>「標籤」>「原則」，然後新增標籤（如圖所示）。

選擇+ Add:

Add Policy Tag

Name*

POLICY_TAG

Description

Enter Description

WLAN-POLICY Maps : 0

+ Add

× Delete

WLAN Profile

Policy Profile

No records available.

10

items per page

0 - 0 of 0 items

原則標籤組態

將您的WLAN簡檔連結到所需的策略簡檔：

Add Policy Tag

+ Add

× Delete

WLAN Profile

Policy Profile

No records available.

10

items per page

0 - 0 of 0 items

Map WLAN and Policy

WLAN Profile*

LWA_EA

Policy Profile*

POLICY_PRO...

×

✓

> WLAN-POLICY Maps : 0

Cancel

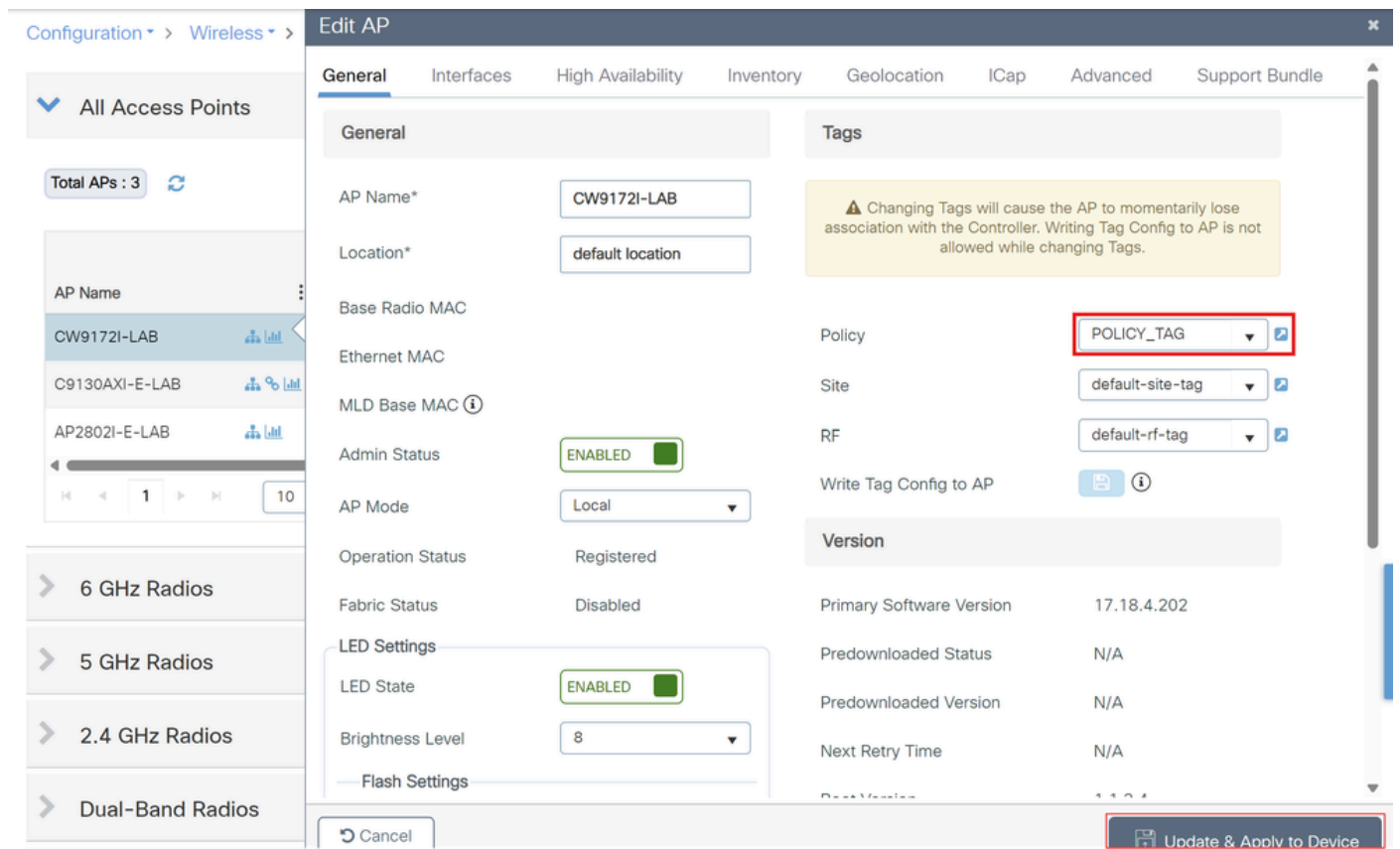
Apply to Device

原則標籤組態

原則標籤指派

指派原則標籤至需要的 AP。

若要指派標籤至一個 AP，請導覽至「組態」>「無線」>「存取點」>「AP 名稱」>「一般標籤」，然後按一下「更新並套用至裝置」。

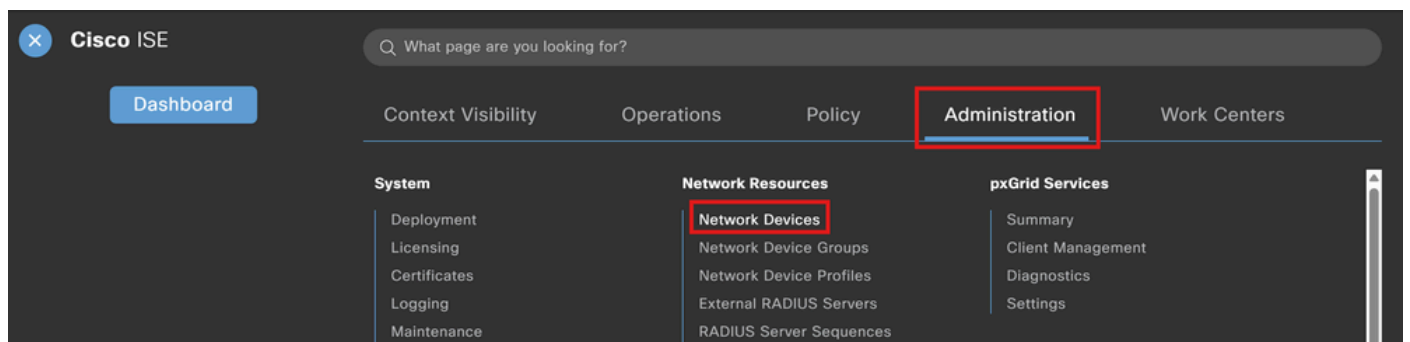


原則標籤指派

ISE 組態

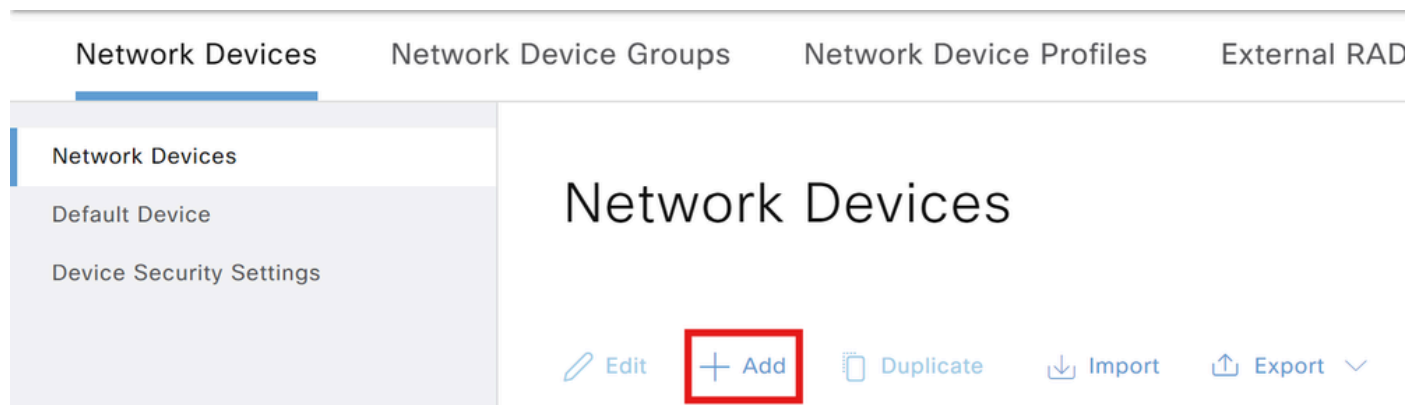
將 9800 WLC 新增至 ISE

步驟 1. 導覽至「管理」>「網路資源」>「網路裝置」（如圖所示）。



將 9800 WLC 新增至 ISE

步驟2.按一下+Add。



新增網路裝置

或者，也可以是指定的機型名稱、軟體版本、說明，並可根據裝置類型、位置或 WLC 指派網路裝置群組。

步驟3.輸入9800 WLC設定，如下圖所示。在WLC端輸入在伺服器建立時定義的RADIUS金鑰。然後按一下Submit。

Network Devices

Name

9800-WLC

Description



IP Address



* IP :

192.0.2.20



32



Device Profile



Cisco



Model Name



Software Version



Network Device Group

Location

All Locations



[Set To Default](#)

IPSEC

Is IPSEC Device



[Set To Default](#)

Device Type

All Device Types



[Set To Default](#)



✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

[Show](#)

9800 WLC設定

步驟4.導覽至Administration > Network Resources > Network Devices，即可看到網路裝置清單。

Network Devices

Selected 0 Total 6  

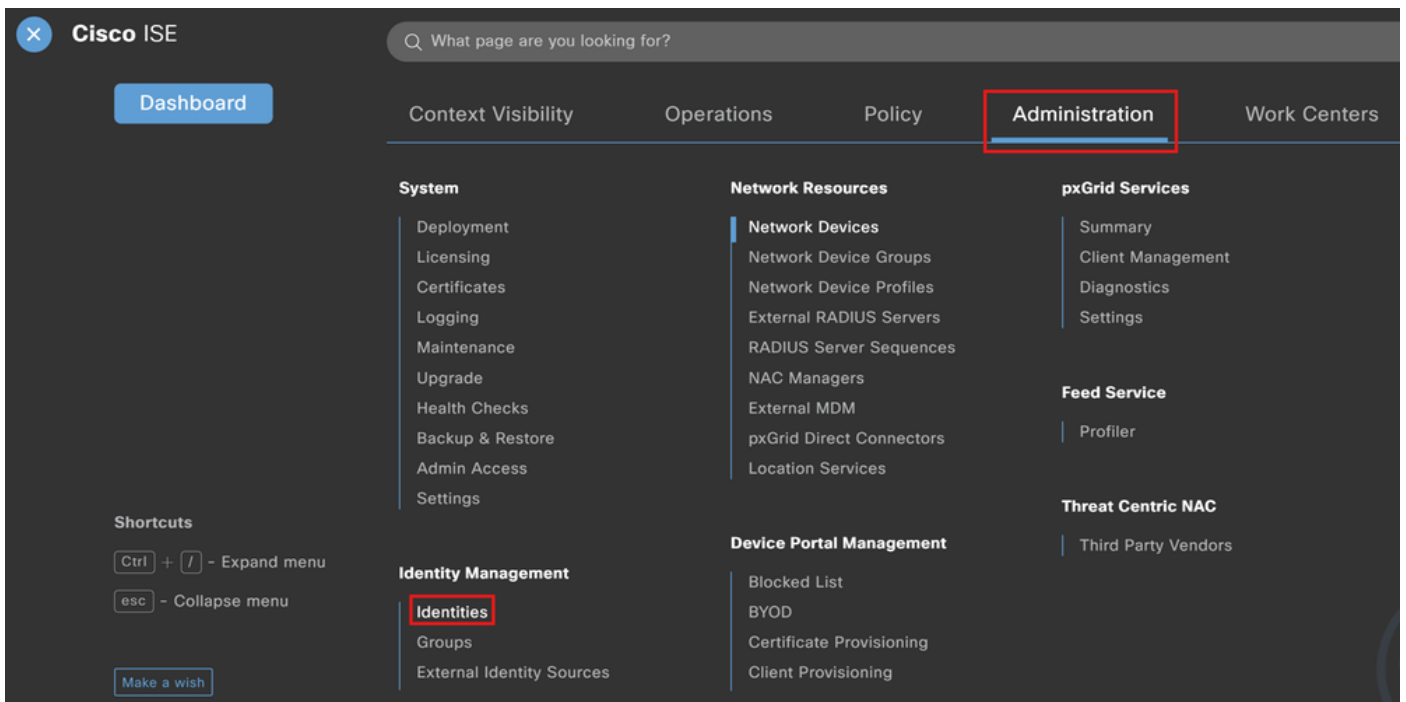
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

☐	Name	IP/Mask	Profile Name	Location	Type
☐	9800		 Cisco 	All Locations	All Device Types
☐	9800-2		 Cisco 	All Locations	All Device Types
☐	9800-40		 Cisco 	All Locations	All Device Types
☐	9800-WLC	192.0.2.20/32	 Cisco 	All Locations	All Device Types

網路裝置清單

在 ISE 上建立新使用者

步驟1.導航到管理>身份管理>身份：



The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. Below the navigation bar, the 'Administration' section is expanded, showing a sidebar with 'System', 'Network Resources', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Network Resources' section is further expanded, showing 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', 'pxGrid Direct Connectors', and 'Location Services'. The 'Identity Management' section is also expanded, showing 'Identities' (highlighted with a red box), 'Groups', and 'External Identity Sources'. The 'Identities' section is further expanded, showing 'Blocked List', 'BYOD', 'Certificate Provisioning', and 'Client Provisioning'.

ISE管理 — 身份

步驟2.導覽至Users，按一下+Add。

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#)

Status

Username ^

Description

First Name

Last Name

Em:

新增使用者

步驟3.輸入訪客使用者的使用者名稱和密碼，然後點選Submit。

[Network Access Users List](#) > [New Network Access User](#)

Network Access User

* Username

guest

Status

☒ Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

☒ With Expiration

Password will expire in 60 days

☐ Never Expires

Password

Re-Enter Password

* Login Password

[Generate Password](#)

i

Enable Password

[Generate Password](#)

i

在 ISE 上建立新使用者

步驟4.導航到管理>身份管理>身份>使用者，您可以看到使用者清單。

Network Access Users

Edit

+ Add

Change Status

Import

Export

Delete

Duplicate

Status

Username

Descripti...

First Name

Last Name

Email Address

User Identity Groups

Admin

Enabled

guest

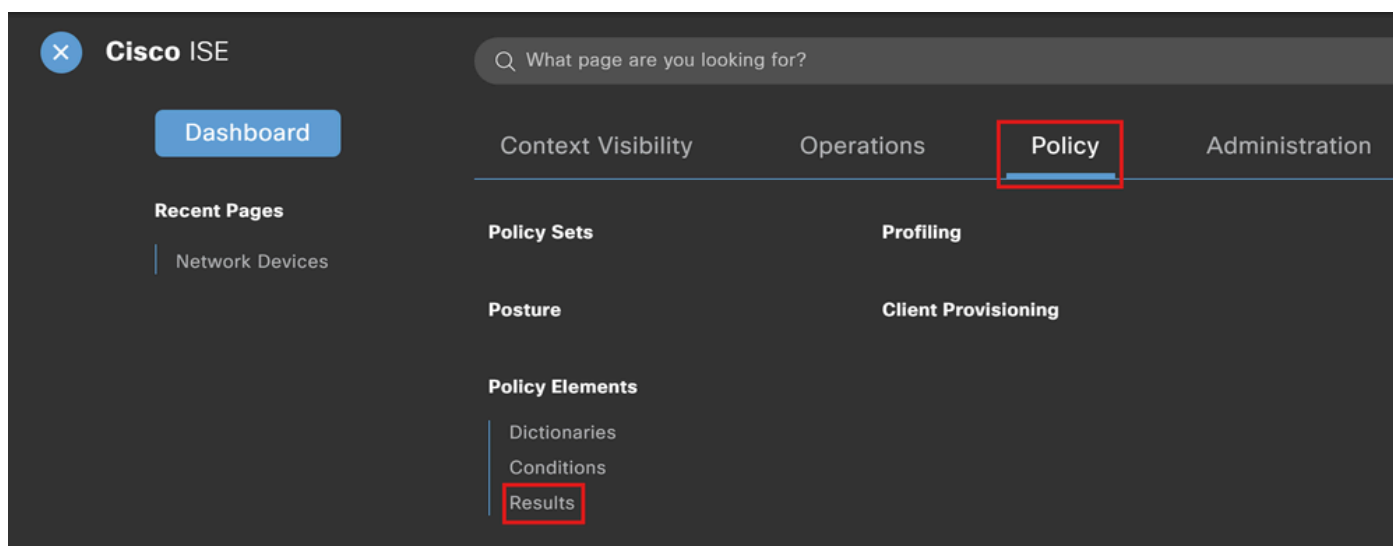
網路訪問使用者清單

建立授權設定檔

原則設定檔為根據其參數（如 MAC 位址、認證及使用的 WLAN 等）指派至用戶端的結果。其可指派虛擬區域網路 (VLAN)、存取控制清單 (ACL) 及統一資源定位器 (URL) 重新導向等特定設定。

以下步驟顯示如何建立需要的授權設定檔，以將用戶端重新導向至驗證入口網站。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. 導覽至Policy > Policy Elements > Results。



ISE策略 — 結果

步驟2.導航至Authorization > Authorization Profiles。按一下「+Add」以建立授權設定檔。

Dictionaries

Conditions

Results

Authentication >

Authorization ▾

Authorization Profiles

Downloadable ACLs

Standard Authorization Profiles

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

新增授權配置檔案

步驟3. 建立授權配置檔案LWA_EA_AUTHORIZATION。屬性詳細資訊必須為Access Type=ACCESS_ACCEPT。按一下「Submit」。

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name

LWA_EA_AUTHORIZATION

Description

* Access Type

ACCESS_ACCEPT ▾

Network Device Profile

 Cisco ▾ ⊕

Service Template

☐

Track Movement

☐

Agentless Posture

☐

Passive Identity Tracking

☐

建立授權設定檔

步驟4. 導航至Policy > Policy Elements > Results > Authorization > Authorization Profiles，您可以檢視授權配置檔案。

DictionarysConditionsResults

Authentication>

Authorization▼

Authorization ProfilesDownloadable ACLs

Profiling>

Posture>

Client Provisioning>

Standard Authorization Profiles

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

EditAddDuplicateDelete

☐	Name	Profile
☐	9800-admin-priv	Cisco ⓘ
☐	9800-helpdeskuser-priv	Cisco ⓘ
☐	AuthZ-Guest	Cisco ⓘ
☐	AuthZ_Guest-Redirect	Cisco ⓘ
☐	AuthZ_Mobile	Cisco ⓘ
☐	Block_Wireless_Access	Cisco ⓘ
☐	Cisco_IP_Phones	Cisco ⓘ
☐	Cisco_Temporal_Onboard	Cisco ⓘ
☐	Cisco_WebAuth	Cisco ⓘ
☐	LWA_EA_AUTHORIZATION	Cisco ⓘ

授權配置檔案清單

設定驗證規則

步驟 1. 導覽至「原則」>「原則集」。

Cisco ISE

Dashboard

Recent Pages

- Results
- Policy Sets
- Identities
- Network Devices

Q What page are you looking for?

Context VisibilityOperationsPolicyAdministration

Policy Sets

Posture

Policy Elements

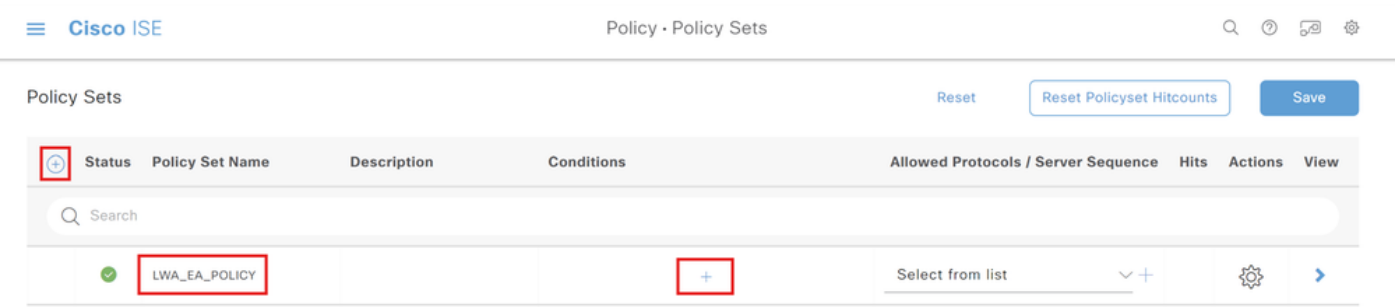
- Dictionarys
- Conditions
- Results

Profiling

Client Provisioning

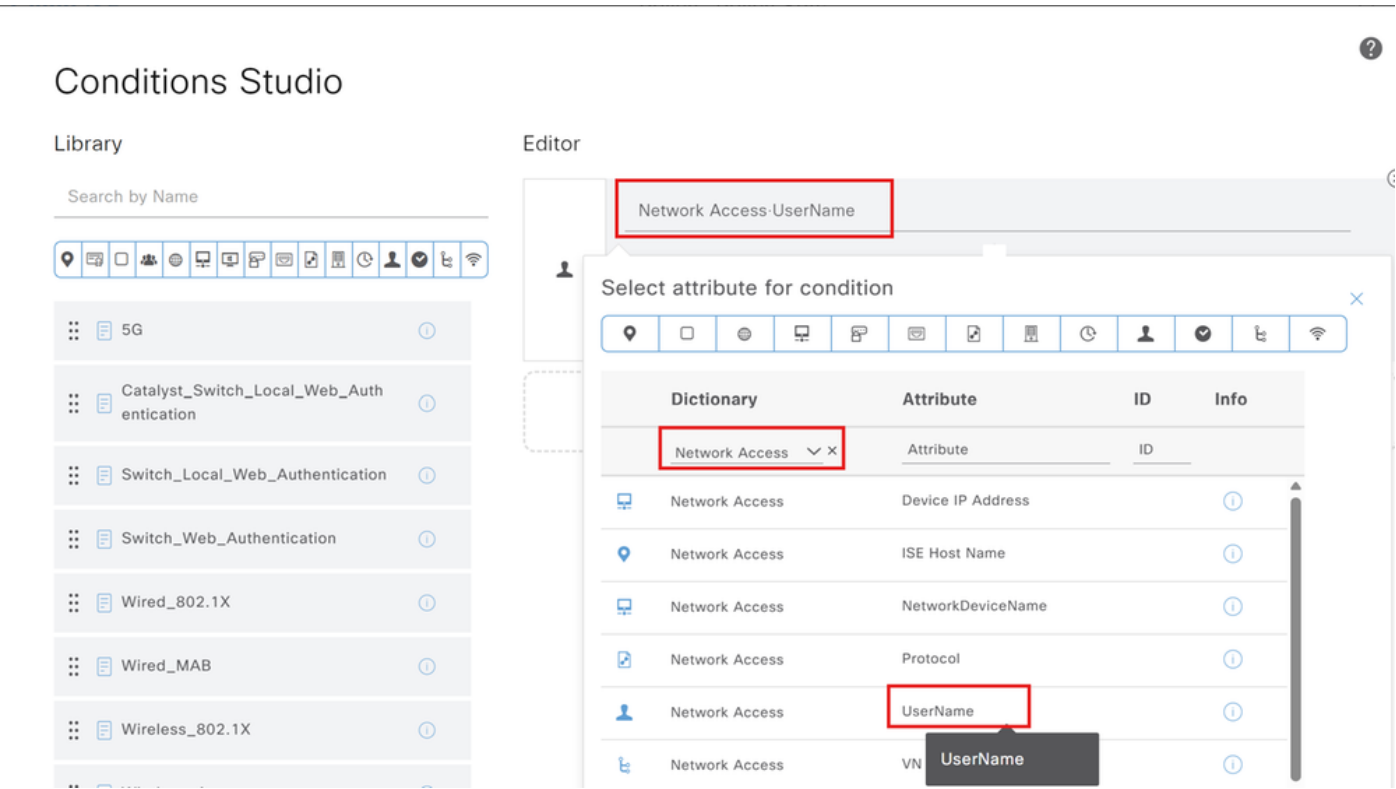
ISE策略 — 策略集

步驟2.選擇+號，鍵入策略集LWA_EA_POLICY的名稱。按一下Conditions列。



設定驗證規則

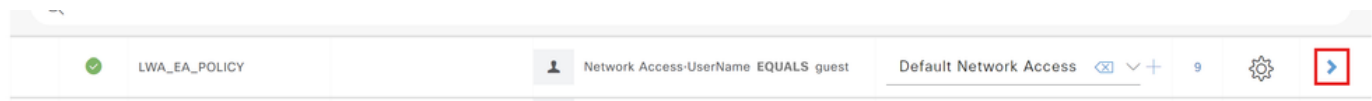
步驟3.在Dictionary上選擇Network Access。在Attribute上選擇Username。



撥號網路存取

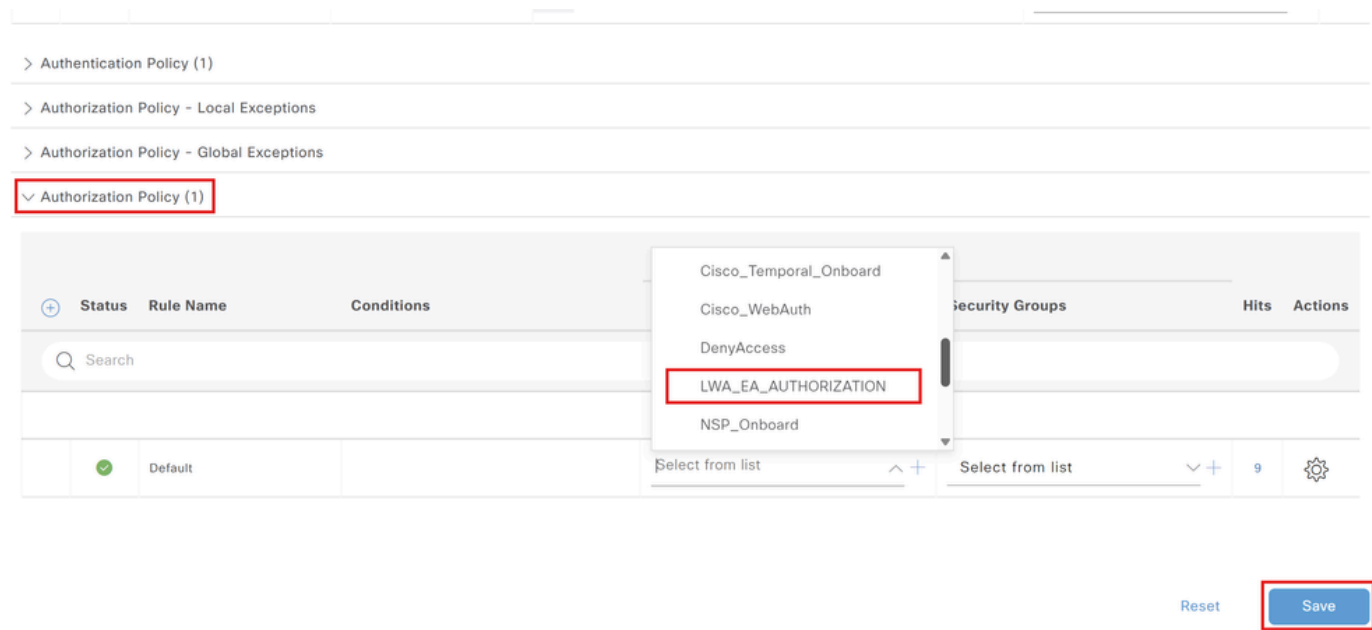
步驟4.設定Equals，然後在文本框中鍵入guest(在管理>身份管理>身份>使用者上定義的使用者名稱)。按一下儲存以儲存更改。

步驟 1. 導覽至「原則」>「原則集」。點選您建立的策略集上的箭頭圖示。



策略集箭頭

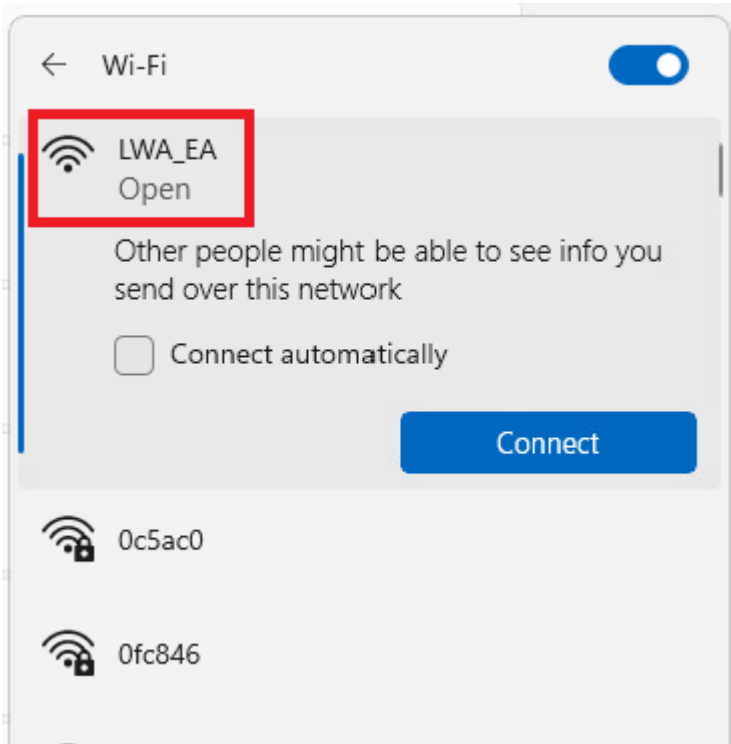
步驟2.在同一「Policy set」頁面上，展開Authorization Policy，如下圖所示。在Profiles列中，刪除DenyAccess並新增LWA_EA_AUTHORIZATION。按一下Save以儲存更改。



授權策略

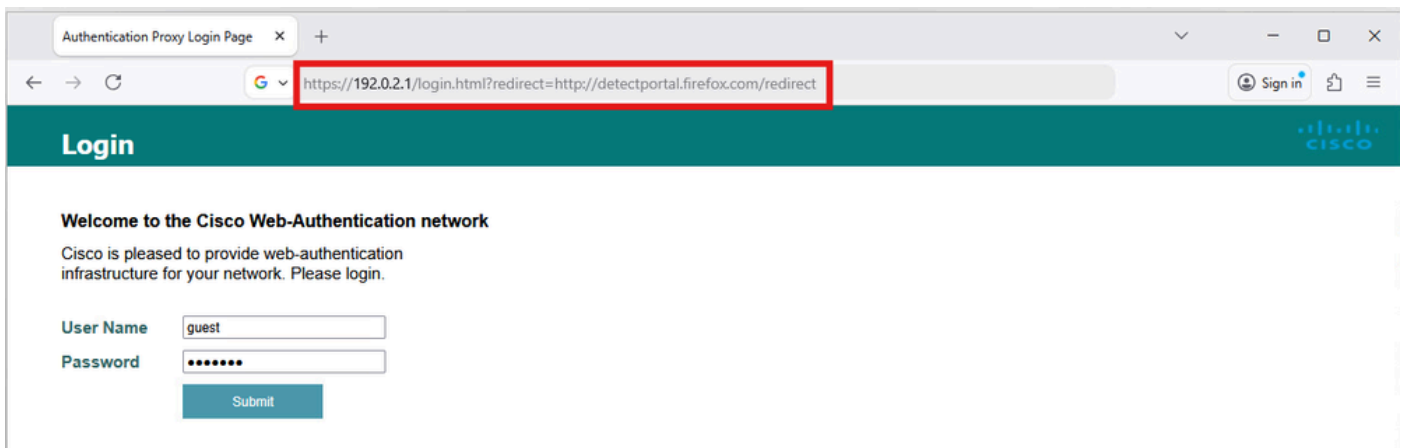
連線訪客客戶端

步驟1.在您的電腦/電話上導航到Wi-Fi網路，找到SSID LWA_EA，然後選擇Connect。



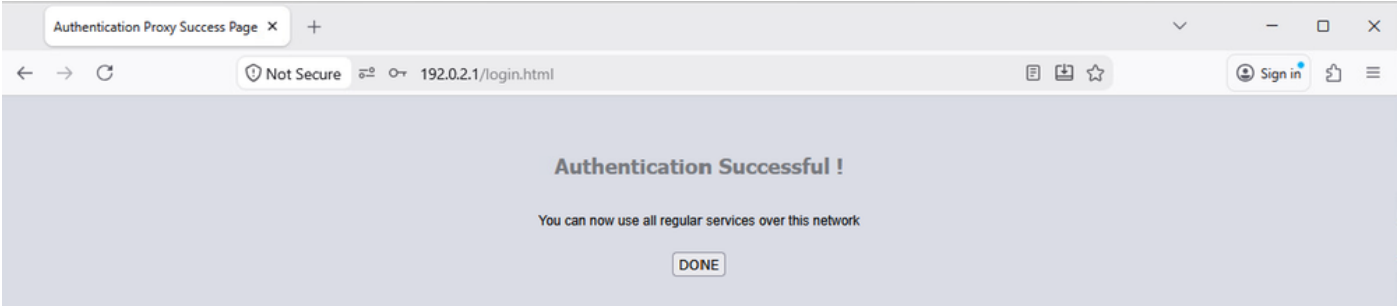
連線訪客客戶端

步驟2.彈出一個瀏覽器視窗，其中顯示登入頁面。重新導向URL位於URL框中，您必須輸入Username和Password才能訪問網路。然後選擇Submit。



包含重新導向URL的登入頁面

如果憑證正確，將顯示身份驗證成功頁面：



「身份驗證成功登入」頁

 附註：提供的URL由WLC提供。它包含WLC虛擬IP和Windows連線測試URL的重新導向。

步驟3.導覽至Operations > RADIUS > Live Logs。您可以看到經過身份驗證的客戶端裝置及其身份驗證和授權策略。

Cisco ISE

Operations · RADIUS

Live Logs

Live Sessions

Misconfigured Supplicants0

Misconfigured Network Devices0

RADIUS Drops0

Client Stopped Responding0

Repeat Counter2

Refresh: Never

Show: Latest 20 records

Within: Last 3 hours

Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Sep 18, 2026 10:00:26.1...			2	guest	08-BE-AC:...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...
Sep 18, 2026 09:54:58.3...				guest	08-BE-AC:...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...
Sep 18, 2026 09:41:04.9...				guest	08-BE-AC:...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...

Last Updated: Fri Sep 18 2026 11:00:54 GMT+0100 (Hora de verão da Europa Ocidental)

Records Shown: 3

Radius即時日誌

驗證

使用本節內容，確認您的組態是否正常運作。

Show WLAN Summary

<#root>

9800WLC#show wlan summary

Number of WLANs: 1
ID Profile Name SSID Status 2.4GHz/5GHz Security

1 LWA_EA LWA_EA UP [open],[Web Auth]

9800WLC#

show wlan name LWA_EA

WLAN Profile Name : LWA_EA

Identifier : 1

Description :

Network Name (SSID) : LWA_EA

Status : Enabled

Broadcast SSID : Enabled

Advertise-Apname : Disabled

Universal AP Admin : Disabled

(...)

Accounting list name :

802.1x authentication list name : Disabled

802.1x authorization list name : Disabled

Security

Web Based Authentication : Enabled

OWE Transition Mode : Disabled

Conditional Web Redirect : Disabled

Splash-Page Web Redirect : Disabled

Webauth On-mac-filter Failure : Disabled

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

(...)

Security-2.4GHz/5GHz

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OSEN : Disabled

PMF Support : Disabled

```
(...)  
Band Select : Disabled  
Load Balancing : Disabled  
(...)
```

Show Parameter Map Configuration

```
9800WLC#show running-config | section parameter-map type webauth global
```

```
parameter-map type webauth global  
type webauth  
virtual-ip ipv4 192.0.2.1  
trustpoint TP-self-signed-123456
```

Show AAA Information

```
<#root>
```

```
9800WLC#show aaa method-lists authentication
```

```
authen queue=AAA_ML_AUTHEN_LOGIN
```

```
name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP
```

```
authen queue=AAA_ML_AUTHEN_ENABLE  
authen queue=AAA_ML_AUTHEN_PPP  
authen queue=AAA_ML_AUTHEN_SGBP  
(...)
```

```
9800WLC#show aaa method-lists authorization
```

```
author queue=AAA_ML_AUTHOR_SHELL  
author queue=AAA_ML_AUTHOR_NET
```

```
name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP
```

```
author queue=AAA_ML_AUTHOR_CONN  
author queue=AAA_ML_AUTHOR_IPMOBILE  
author queue=AAA_ML_AUTHOR_RM  
(...)
```

```
9800WLC#show aaa servers
```

```
RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS
```

State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCN (0) : current UP
(...)

疑難排解

常見問題

以下是有關如何排除Web驗證問題的幾個指南，例如：

- 使用者無法進行驗證。
- 憑證問題。
- 重定向URL無效。
- 訪客使用者無法連線到訪客WLAN。
- 使用者未取得IP位址。
- 重定向到「Web身份驗證登入」頁失敗。
- 身份驗證成功後，訪客使用者無法訪問網際網路。

以下指南詳細描述故障排除步驟：

- [排除Web驗證的常見問題](#)
- [須排解的其他疑難情況](#)

條件式偵錯和無線電主動追蹤以及嵌入式封包擷取

您可以啟用條件調試和捕獲無線活動(RA)跟蹤，該跟蹤為與指定條件（本例中為客戶端MAC地址）互動的所有進程提供調試級別跟蹤。若要啟用條件調試，請使用指南「[條件調試](#)」和[RadioActive跟蹤中的步驟](#)。

您還可以收集嵌入式資料包捕獲(EPC)。EPC是一種封包擷取工具，允許檢視目的地為、來源和通過Catalyst 9800 WLC的封包，即LWA中的DHCP、DNS、HTTP GET封包。可以匯出這些捕獲以便使用Wireshark進行離線分析。有關如何執行此操作的詳細步驟，請參閱[嵌入式封包擷取](#)。

成功嘗試的示例

這是RA_traces的輸出，表示在與RADIUS伺服器的訪客SSID連線時，在關聯/身份驗證過程中成功嘗試識別每個階段。

802.11關聯/身份驗證：

[client-orch-sm] [17062]: (註) : MAC:08be.ac3f已收到關聯。BSSID cc70.edcf.552f , WLAN LWA_EA , 插槽1 AP 2ce3.8eb4,CW9172I-LAB

[client-orch-sm] [17062]: (調試) : MAC:08be.ac3f已收到Dot11關聯請求。處理已啟動 , SSID:LWA_EA , 策略配置檔案 : POLICY_PROFILE、AP名稱 : CW9172I-LAB , Ap Mac地址 : 2ce3.8eb4BSSID MAC0000.0000.0000wlan ID:1RSSI:-49,SNR:46

[client-orch-state] [17062]: (註) : MAC:08be.ac3f客戶端狀態轉換 : S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [17062]: (資訊) : MAC:08be.ac3f Dot11 ie驗證擴展/支援速率。針對支援的費率通過了驗證 radio_type 2

[dot11-validate] [17062]: (資訊) : MAC:08be.ac3f WiFi direct:Dot11驗證P2P IE。P2P IE不存在。

[dot11] [17062]: (調試) : MAC:08be.ac3f dot11傳送關聯響應。使用resp_status_code建立關聯響應 : 0

[dot11] [17062]: (調試) : MAC:08be.ac3f Dot11功能資訊byte1 1, byte2:11

[dot11-frame] [17062]: (資訊) : MAC:08be.ac3f WiFi direct:使用P2P IE跳過構建關聯響應 : Wifi直接策略已禁用

[dot11] [17062]: (資訊) : MAC:08be.ac3f dot11傳送關聯響應。正在傳送相關響應 , 響應長度為 : 130和 resp_status_code:0,DOT11_STATUS:DOT11_STATUS_SUCCESS

[dot11] [17062]: (註) : MAC:08be.ac3f關聯成功。AID 1 , 漫遊=假 , WGB=假 , 11r=假 , 11w=假快速漫遊=假

[dot11] [17062]: (資訊) : MAC:08be.ac3f DOT11狀態轉換 : S_DOT11_INIT -> S_DOT11_ASSOCIATED

[client-orch-sm] [17062]: (調試) : MAC:08be.ac3f Station Dot11關聯成功。

IP學習流程：

[client-orch-state] [17062]: (註) : MAC:08be.ac3f客戶端狀態轉換 : S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [17062]: (資訊) : MAC:08be.ac3f IP-learn狀態轉換 : S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

[client-auth] [17062]: (資訊) : MAC:08be.ac3f客戶端身份驗證介面狀態轉換 : S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

[client-iplearn] [17062]: (註) : MAC:08be.ac3f客戶端IP學習成功。方法 : DHCP IP:10.14.32.109

[client-iplearn] [17062]: (資訊) : MAC:08be.ac3f IP-learn狀態轉換 : S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

[client-orch-sm] [17062]: (調試) : MAC:08be.ac3f收到ip learn響應。方法 : IPLEARN_METHOD_DHCP

第3層身份驗證：

[client-orch-sm] [17062]: (調試) : MAC:08be.ac3f觸發的L3身份驗證。狀態= 0x0 , 成功

[client-orch-state] [17062]: (註) : MAC:08be.ac3f客戶端狀態轉換 : S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS

[client-auth] [17062]: (註) : MAC:08be.ac3f L3身份驗證已啟動。LWA

[client-auth] [17062]: (資訊) : MAC:08be.ac3f客戶端身份驗證介面狀態轉換 : S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]處於LOGIN狀態時獲取 rcvd

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET請求

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]解析GET , src [10.14.32.109] dst [10.107.221.82] url [<http://firefox.detect.portal/>]

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]讀取完成 : parse_request返回8

[webauth-io] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO狀態讀取 —>寫入

[webauth-io] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO狀態寫入 —

>讀取

[webauth-io] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO狀態新 — >讀取

[webauth-io] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218讀取事件，消息就緒

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]處於LOGIN狀態時的POST rcvd

第3層身份驗證成功，將客戶端移動到RUN狀態：

[auth-mgr] [17062]: (資訊) : [08be.ac3f:capwap_90000004]客戶端08be.ac3f的已接收使用者名稱訪客

[auth-mgr] [17062]: (資訊) : 已收到attr auth-domain(954)的[08be.ac3f:capwap_90000004] auth mgr attr add/change notification

[auth-mgr] [17062]: (資訊) : [08be.ac3f:capwap_90000004]方法webauth將狀態從「Running」更改為「Authc Success」

[auth-mgr] [17062]: (資訊) : [08be.ac3f:capwap_90000004]上下文狀態從「正在運行」更改為「授權成功」

[auth-mgr] [17062]: (資訊) : 已收到attr方法(757)的[08be.ac3f:capwap_90000004] auth mgr attr add/change notification

[auth-mgr] [17062]: (資訊) : [08be.ac3f:capwap_90000004]引發的事件AUTHZ_SUCCESS(11)

[auth-mgr] [17062]: (資訊) : [08be.ac3f:capwap_90000004]上下文狀態從「Authc Success」更改為「Authz Success」

[webauth-acl] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]通過SVM應用IPv4註銷ACL，名稱：IP-Adm-V4-LOGOUT-ACL，優先順序：51, IIF-ID:0

[webauth-sess] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]使用的引數對映：全球

[webauth-state] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]使用的引數對映：全球

[webauth-state] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]狀態AUTHC_SUCCESS -> AUTHZ

[webauth-page] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]正在發送Webauth成功頁面

[webauth-io] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO狀態身份驗證 — >寫入

[webauth-io] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO狀態寫入 — >END

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218刪除IO交換機和關閉套接字，id [99000029]

[client-auth] [17062]: (註) : MAC:08be.ac3f L3身份驗證成功。ACL:[]

[client-auth] [17062]: (資訊) : MAC:08be.ac3f客戶端身份驗證介面狀態轉換：S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

[webauth-httpd] [17062]: (資訊) : capwap_90000004[08be.ac3f][10.48.39.243]56538/219刪除IO時鐘並關閉套接字，id [D7000028]

[errmsg] [17062]: (資訊) : %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:R0/0:wncd:對於具有MAC的裝置，使用者名稱條目（訪客）與ssid(LWA_EA)聯合：08be.ac3f

[aaa-attr-inf] [17062]: (資訊) : [應用的屬性：bsn-vlan-interface-name 0 "VLAN0039"]

[aaa-attr-inf] [17062]: (資訊) : [應用的屬性：timeout 0 1800(0x708)]

[aaa-attr-inf] [17062]: (資訊) : [應用的屬性：url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]

[ewlc-qos-client] [17062]: (資訊) : MAC:08be.ac3f客戶端QoS運行狀態處理程式

[rog-proxy-capwap] [17062]: (調試) : 託管客戶端RUN狀態通知：08be.ac3f

[client-orch-state] [17062]: (註) : MAC:08be.ac3f客戶端狀態轉換：S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

相關資訊

- [思科技術支援與下載](#)

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）。