

# 在Catalyst 9800 WLC和ISE上配置狀態

## 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](#)

#### [策略ACL配置](#)

#### [ISE上的AAA配置和狀態設定](#)

### [範例](#)

### [驗證](#)

### [疑難排解](#)

#### [核對表](#)

### [收集調試](#)

### [參考資料](#)

---

## 簡介

本檔案介紹如何透過圖形使用者介面(GUI)在Catalyst 9800 WLC和ISE上設定狀態WLAN。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 9800 WLC一般組態
- ISE策略和配置檔案配置

### 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 Cupertino v17.9.5
- 身分識別服務引擎(ISE)v3.2
- 筆記型電腦Windows 10企業版

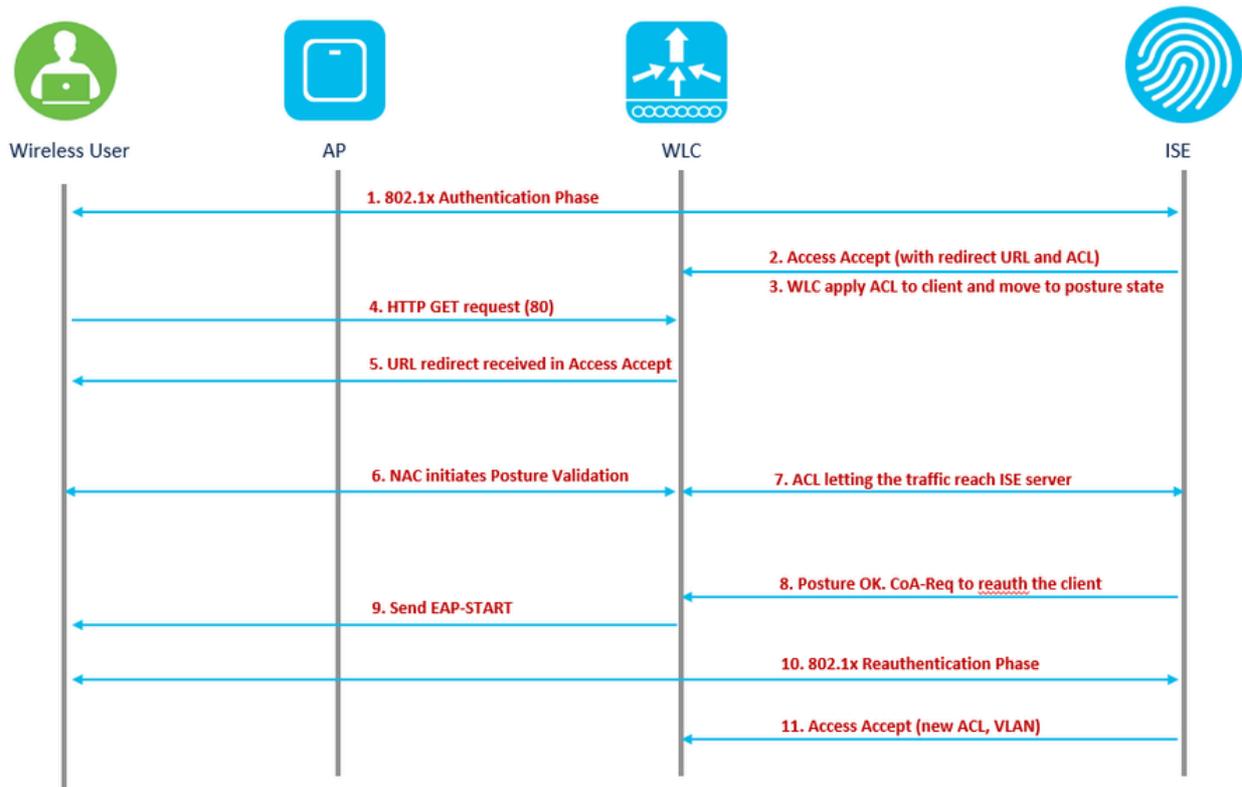
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

無線LAN控制器RADIUS NAC和CoA功能流

- 1.客戶端使用dot1x身份驗證進行身份驗證。
2. RADIUS Access Accept傳送連線埠80的重新導向URL和預先驗證ACL，包括允許IP位址和連線埠，或隔離VLAN。
- 3.客戶端被重定向到access accept中提供的URL，並進入新狀態，直到狀態驗證完成。處於此狀態的客戶端與ISE伺服器對話並根據ISE NAC伺服器上配置的策略驗證自身。
- 4.客戶端上的NAC代理啟動狀態驗證 ( 到埠80的流量 )：代理向埠80傳送HTTP發現請求，控制器將埠重定向到訪問接受中提供的URL。ISE知道客戶端嘗試聯絡並直接響應客戶端。這樣，客戶端可以瞭解ISE伺服器IP，從現在開始，客戶端將直接與ISE伺服器對話。
5. WLC允許此流量，因為ACL設定為允許此流量。在發生VLAN覆寫的情況下，流量會橋接以便到達ISE伺服器。
- 6.一旦ISE客戶端完成評估，將向WLC傳送帶有reauth服務的RADIUS CoA-Req。這將啟動客戶端的重新身份驗證 ( 通過傳送EAP-START )。重新身份驗證成功後，ISE會傳送訪問接受並帶有一個新的ACL ( 如果有 ) 和沒有URL重定向或訪問VLAN。
- 7.根據RFC 3576,WLC支援CoA-Req和Disconnect-Req。根據RFC 5176,WLC需要支援重新驗證服務的CoA-Req。
- 8.在WLC上使用的是預配置的ACL，而不是可下載的ACL。ISE伺服器只傳送ACL名稱，該名稱已在控制器中配置。
- 9.此設計適用於VLAN和ACL案例。在發生VLAN覆寫的情況下，我們只需將連線埠80重新導向，並允許 ( 橋接 ) 隔離VLAN上的其餘流量。對於ACL，會套用在access accept中接收的預先驗證ACL。

下圖直觀地顯示了此功能流程：



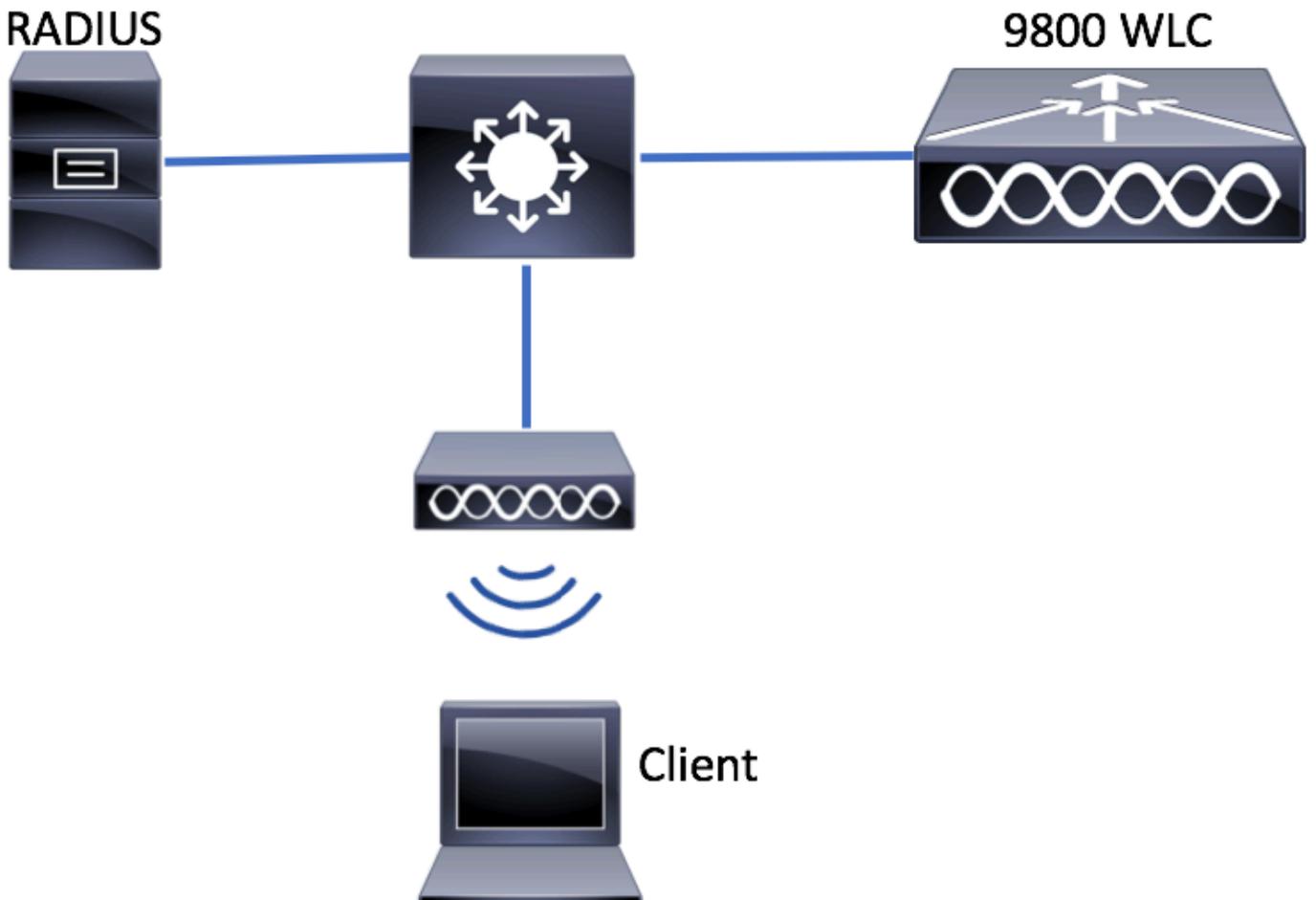
#### 功能工作流

對於此使用案例，僅用於企業使用者的SSID將啟用安全狀態。此SSID上不存在其他使用案例，例如BYOD、訪客或任何其他使用案例。

當無線客戶端首次連線到終端安全評估SSID時，它必須在ISE的重定向門戶下載並安裝終端安全評估模組，最後根據終端安全評估檢查結果（合規/不合規）應用相關ACL。

## 設定

### 網路圖表



網路圖表

## 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，如圖所示。確保為狀態NAC啟用對CoA的支援。

The screenshot shows the Cisco ISE configuration interface. The breadcrumb navigation path is Configuration > Security > AAA. Under AAA, the 'Servers / Groups' tab is selected. The 'RADIUS' sub-tab is also selected. The 'Servers' list is empty, and the '+ Add' button is visible. The interface also shows a search bar and a sidebar with navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting.

### Create AAA Radius Server

Name*	posture-radius	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	10.124.57.141	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	•••••
Key Type	Clear Text ▼	Confirm CoA Server Key	•••••
Key* ⓘ	•••••	Automate Tester	<input type="checkbox"/>
Confirm Key*	•••••		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

步驟2.建立身份驗證方法清單。導覽至Configuration > Security > AAA > AAA Method List > Authentication > + Add，如下圖所示：

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is selected, and the 'Authentication' sub-tab is active. A '+ Add' button is highlighted in a red box. Below it, a table lists the authentication methods:

Name	Type	Group Type
default	login	local

The table has a page indicator showing 1 of 10 items.

## Quick Setup: AAA Authentication



Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

### Available Server Groups

ldap  
tacacs+



### Assigned Server Groups

radius



Cancel

Apply to Device

9800建立身份驗證清單詳細資訊

步驟3. (可選) 建立會計方法清單，如下圖所示：

Configuration > Security > AAA [Show Me How](#)

+ AAA Wizard

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

Authentication

Authorization

**Accounting**

+ Add × Delete

Name	Type
0	10

9800新增帳戶清單

## Quick Setup: AAA Accounting



Method List Name\*

POSTUREacct

Type\*

identity



Available Server Groups

Assigned Server Groups

ldap  
tacacs+



radius



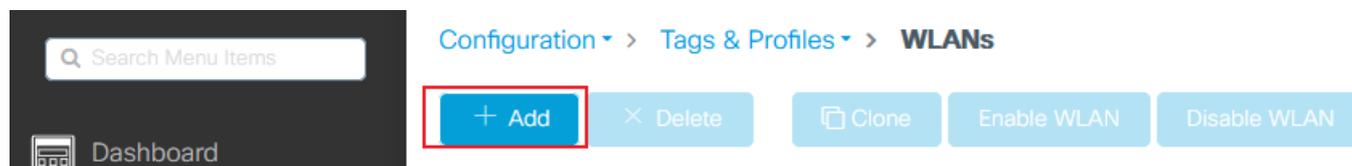
Cancel

Apply to Device

9800建立帳戶清單詳細資訊

## WLAN配置

步驟1. 建立WLAN。導覽至Configuration > Tags & Profiles > WLANs > + Add，然後根據需要配置網路：



9800 WLAN新增

步驟2. 輸入WLAN一般資訊。

## Add WLAN



### General

### Security

### Advanced

Profile Name\*

SSID\*

WLAN ID\*

Status  ENABLED

Broadcast SSID  ENABLED

### Radio Policy ⓘ

[Show slot configuration](#)

#### 6 GHz

Status  ENABLED ⓘ

- ✘ WPA2 Disabled
- ✘ WPA3 Enabled
- ✔ Dot11ax Enabled

#### 5 GHz

Status  ENABLED

#### 2.4 GHz

Status  ENABLED

802.11b/g Policy

Cancel

Apply to Device

9800建立WLAN一般資訊

步驟3.定位至安全標籤並選擇所需的安全方法。在這種情況下，請選擇「802.1x」，並且需要AAA身份驗證清單(在AAA配置部分中的步驟2中建立):

## Add WLAN



General **Security** Advanced

**Layer2** Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

### WPA Parameters

WPA Policy  WPA2 Policy   
GTK Randomize  OSEN Policy

### WPA2 Encryption

AES(CCMP128)  CCMP256   
GCMP128  GCMP256

### Protected Management Frame

PMF

### Fast Transition

Status

Over the DS

Reassociation Timeout \*

### Auth Key Mgmt

802.1x  PSK   
Easy-PSK  CCKM   
FT + 802.1x  FT + PSK   
802.1x-SHA256  PSK-SHA256

Cancel

Apply to Device

9800建立WLAN安全L2

## Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 **AAA**

Authentication List

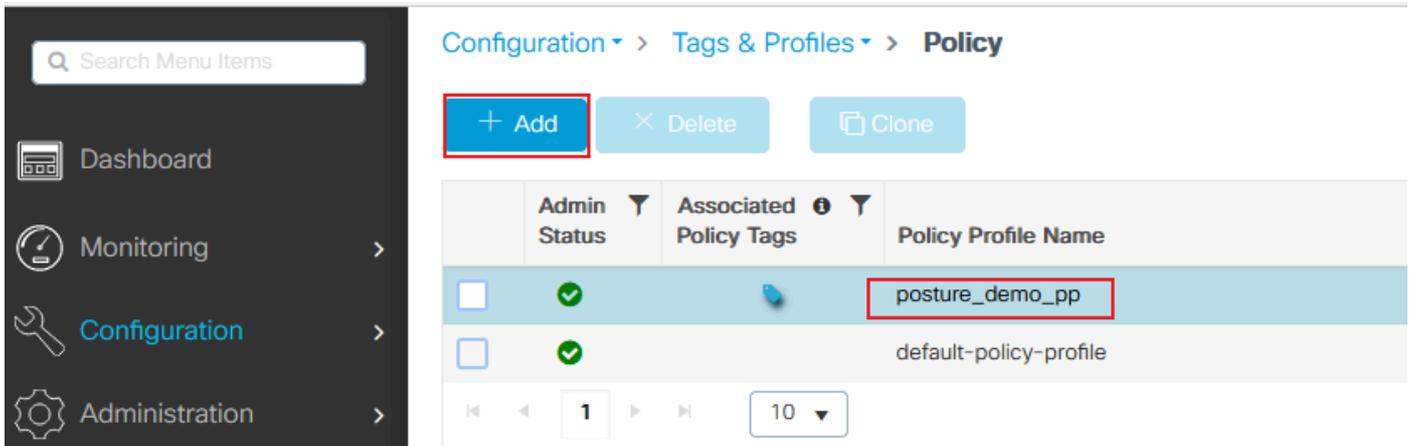
Local EAP Authentication

9800建立WLAN安全AAA

原則設定檔組態

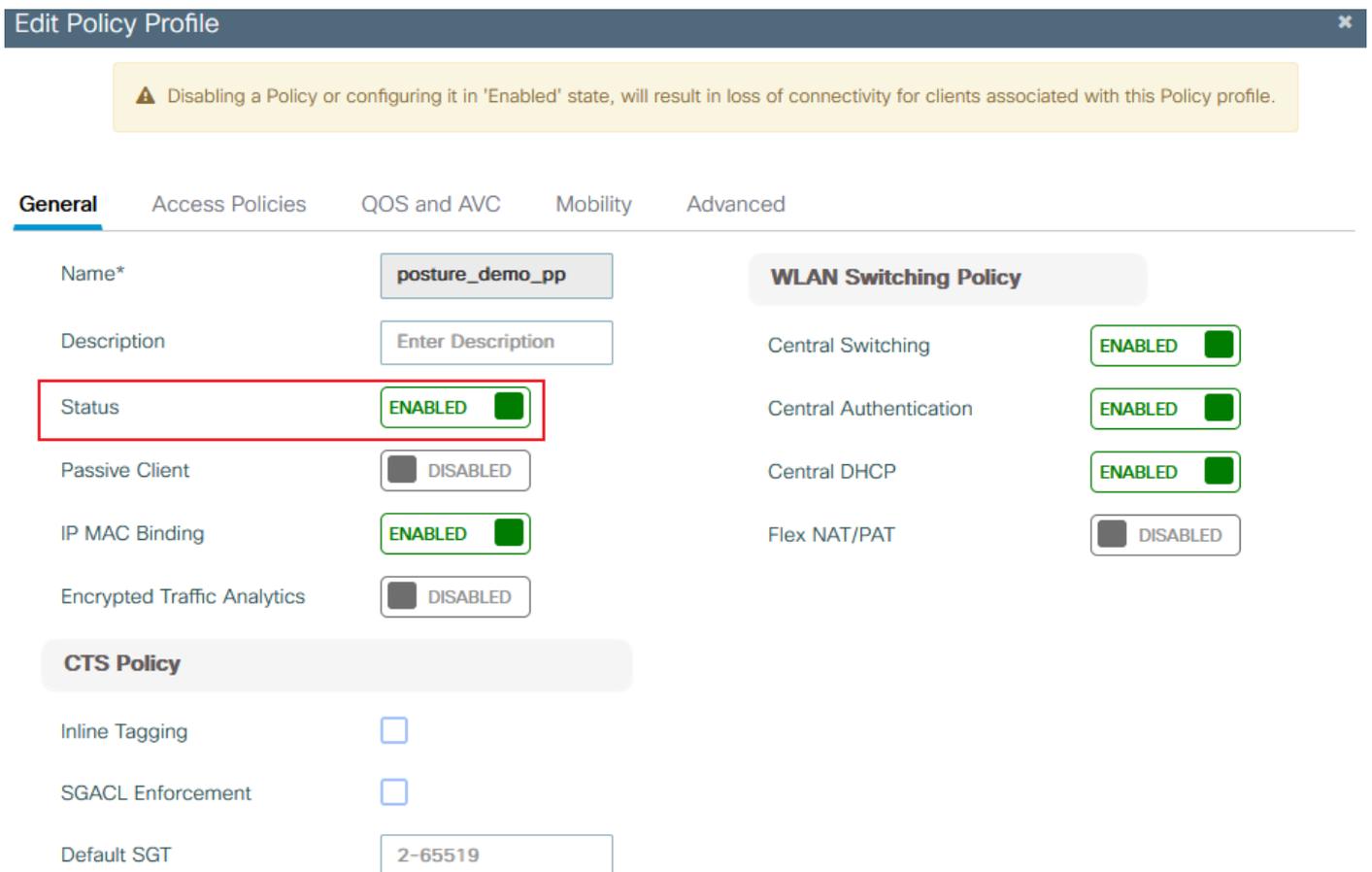
在策略配置檔案中，您可以決定分配客戶端到哪個VLAN，以及其他設定(如訪問控制清單(ACL)、服務品質(QoS)、移動錨點、計時器等)。您可使用預設原則設定檔，或可建立新的設定檔。

步驟1.建立新的策略配置檔案。導覽至Configuration > Tags & Profiles > Policy，然後建立一個新的：



9800新增策略配置檔案

確認設定檔已啟用。



9800建立策略配置檔案常規

步驟2.選擇VLAN。導覽至Access Policies索引標籤，並從下拉選單中選擇VLAN名稱或手動輸入

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  ⓘ

### VLAN

VLAN/VLAN Group  ⓘ

Multicast VLAN

### WLAN ACL

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

### URL Filters ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

9800建立策略配置檔案VLAN

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 )。您也可以指定會計方法：

⚠ 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

Policy Name  ✕ ⓘ

Accounting List  ✕ ⓘ

### WGB Parameters

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

Cancel

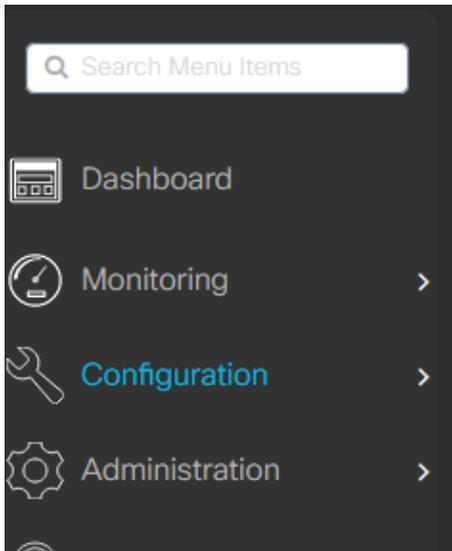
Update & Apply to Device

9800建立策略配置檔案高級版

## 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。

導覽至 Configuration > Tags & Profiles > Tags > Policy，然後根據需要新增一個，如下圖所示：



**Policy** Site RF AP

**+ Add** **× Delete** **Clone**

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

1 10

9800策略標籤新增

將您的WLAN簡檔連結到所需的策略簡檔：

**Edit Policy Tag**

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name\*

Description

▼ **WLAN-POLICY Maps: 1**

**+ Add** **× Delete**

WLAN Profile	Policy Profile
<input type="checkbox"/> posture_demo	posture_demo_pp

1 10 1 - 1 of 1 items

9800策略標籤詳細資訊

## 原則標籤指派

指派原則標籤至需要的 AP。導航到 Configuration > Wireless > Access Points > AP Name > General Tags，進行所需的分配，然後點選 Update & Apply to Device。

Edit AP ✕

---

General
Interfaces
High Availability
Inventory
ICap
Advanced
Support Bundle

**General**

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

**Tags**

**⚠** Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy

Site

RF

9800策略標籤分配

## 重新導向 ACL 組態

導覽至Configuration > Security > ACL > + Add以建立一個新的ACL。

狀態門戶重定向使用的ACL要求與CWA ( 中央Web身份驗證 ) 相同。

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，而是雙向ACL，定義哪些流量會進入CPU ( 在允許的情況下 ) 進行進一步處理 ( 例如重新導向 ) 以及哪些流量會停留在資料平面上 ( 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10.124.57.141 ) ：

**Edit ACL** ✕

ACL Name\*  ACL Type

---

**Rules**

Sequence\*  Action

Source Type

Destination Type

Protocol

Log  DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.124.57.141		ip	None	None	None	Disa
<input type="checkbox"/> 20	deny	10.124.57.141		any		ip	None	None	None	Disa
<input type="checkbox"/> 30	deny	any		any		udp	None	eq domain	None	Disa
<input type="checkbox"/> 40	deny	any		any		udp	eq domain	None	None	Disa
<input type="checkbox"/> 50	permit	any		any		tcp	None	eq www	None	Disa

9800重新導向ACL詳細資訊

## 策略ACL配置

在這種情況下，您需要在9800 WLC上為ISE定義單獨的ACL，以便根據未來檢查結果授權合規和非合規方案。

[Configuration](#) > [Security](#) > **ACL**

	ACL Name	ACL Type
<input type="checkbox"/>	POSTURE_COMPLIANT_ACL	IPv4 Extended
<input type="checkbox"/>	POSTURE_NON-COMPLIANT_ACL	IPv4 Extended
<input type="checkbox"/>	POSTURE_REDIRECT_ACL	IPv4 Extended

◀ 1 ▶ 10 ▼

9800 ACL一般資訊

對於相容情況，在此案例中只需使用permit all。作為另一種常見配置，您還可以讓ISE不授權合規結果中的任何ACL，這相當於permit all on 9800端：

**Edit ACL** ✕

ACL Name\*  ACL Type

**Rules**

Sequence\*  Action

Source Type

Destination Type

Protocol

Log  DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	permit	any		any		ip	None	None	None	Disable

1 - 1 of 1 items

### 9800 ACL — 合規

對於不合規情況，客戶端僅允許訪問特定網路，通常訪問補救伺服器（在此例中為ISE本身）：

**Edit ACL** ✕

ACL Name\*  ACL Type

**Rules**

Sequence\*  Action

Source Type

Destination Type

Protocol

Log  DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	permit	10.124.57.141		any		ip	None	None	None	Disa
<input type="checkbox"/> 20	permit	any		10.124.57.141		ip	None	None	None	Disa
<input type="checkbox"/> 30	permit	any		any		udp	None	eq domain	None	Disa
<input type="checkbox"/> 40	permit	any		any		udp	eq domain	None	None	Disa
<input type="checkbox"/> 50	deny	any		any		ip	None	None	None	Disa

1 - 5 of 5 items

### 9800 ACL — 不符合要求

## ISE上的AAA配置和狀態設定

安全狀態要求：在本示例中，確定符合性的要求是檢測用於測試Windows PC的案頭上是否存在特

定測試檔案。

步驟1.在ISE上將WLC 9800新增為NAD。導覽至Administration > Network Resources > Network Devices > Add:

The screenshot shows the Cisco ISE Administration interface for adding a new Network Device. The breadcrumb path is Administration > Network Resources > Network Devices > Add. The form fields are as follows:

- Name: WLC9800
- Description: (empty)
- IP Address: 10.124.60.41 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: All Device Types (Set To Default)

新增網路裝置01

The screenshot shows the 'RADIUS Authentication Settings' form in the Cisco ISE Administration interface. The breadcrumb path is Administration > Network Resources > Network Devices > Add > RADIUS Authentication Settings. The form fields are as follows:

- RADIUS UDP Settings:**
  - Protocol: RADIUS
  - Shared Secret: (masked with dots)
  - Use Second Shared Secret: (unchecked)
  - Second Shared Secret: (empty)
  - CoA Port: 1700 (Set To Default)
- RADIUS DTLS Settings:**
  - DTLS Required: (unchecked)
  - Shared Secret: radius/dtls
  - CoA Port: 2083 (Set To Default)
  - Issuer CA of ISE Certificates for CoA: Select if required (optional)
  - DNS Name: (empty)

新增網路裝置02

步驟2.在思科軟體CCO網站上下載思科安全客戶端頭端部署包和合規性模組。

訪問和搜尋Cisco Secure Client:

Cisco Secure Client Headend Deployment Package (Windows)

06-Feb-2024

111.59 MB

[cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg](#)

[Advisories](#) 

安全使用者端5.1.2.42

ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later.

30-Jan-2023

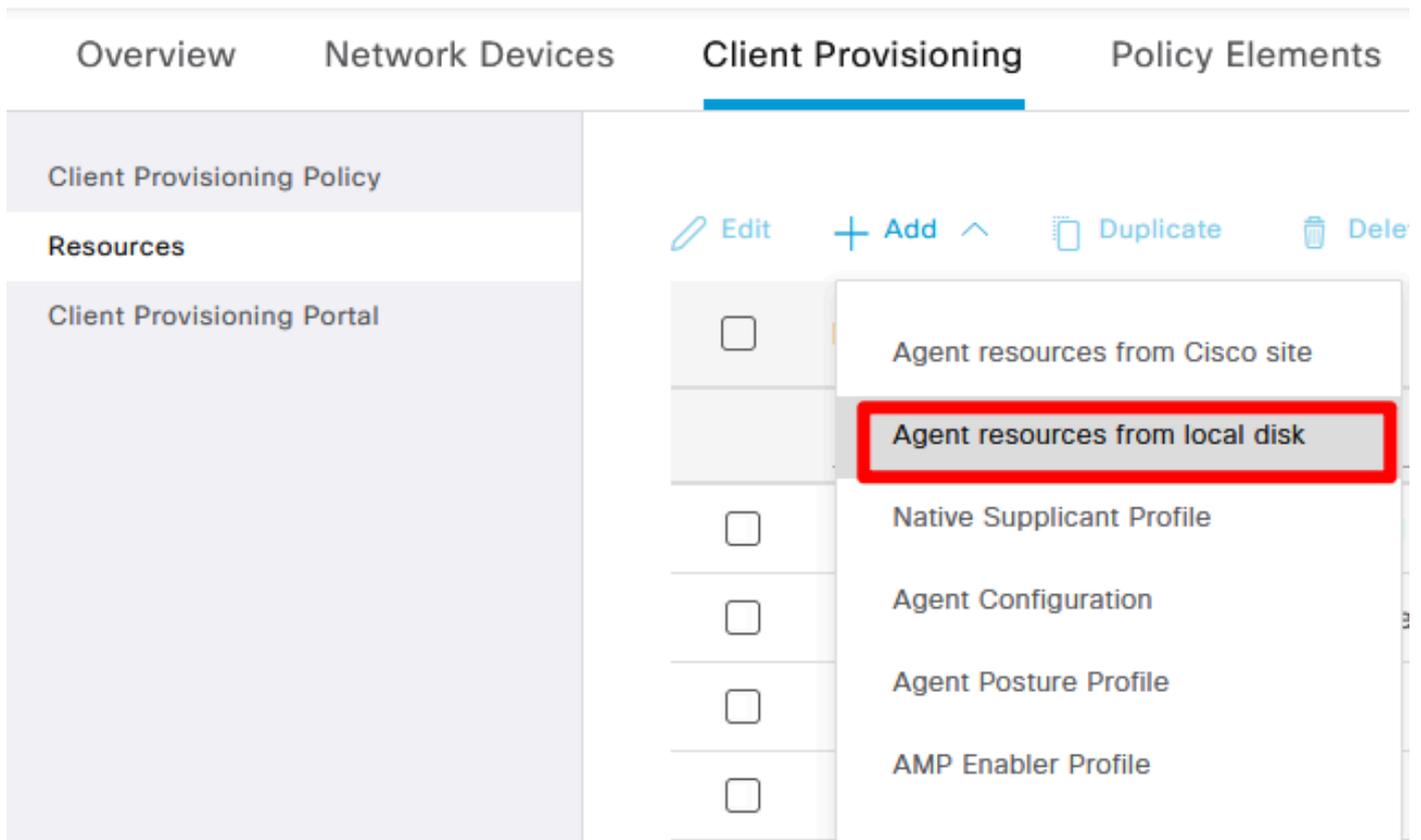
19.59 MB

[cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg](#)

[Advisories](#) 

ISE合規性模組4.3

步驟3.將思科安全客戶端頭端部署包和合規性模組包上傳到ISE客戶端調配。導航到工作中心>狀態>客戶端調配>資源。從下拉框中按一下新增，從本地磁碟中選擇Agent resources:



Overview Network Devices **Client Provisioning** Policy Elements

Client Provisioning Policy

Resources

Client Provisioning Portal

Edit Add Duplicate Delete

- Agent resources from Cisco site
- Agent resources from local disk
- Native Supplicant Profile
- Agent Configuration
- Agent Posture Profile
- AMP Enabler Profile

上傳安全客戶端

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy Resources Client Provisioning Portal

Selected 0 Total 13

Quick Filter

Name	Type	Version	Last Update	Description
CiscoTemporalAgentOSX 4.10.02051	CiscoTemporalAgentOSX	4.10.2051.0	2021/08/10 03:12:31	With CM: 4.3.1858.4353
CiscoSecureClientComplianceModuleWindows 4.3.3335.6146	CiscoSecureClientComplianceModuleWindows	4.3.3335.6146	2024/03/30 19:28:34	Cisco Secure Client Win...
Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/10/07 04:01:12	Pre-configured Native S...
CiscoAgentlessOSX 4.10.02051	CiscoAgentlessOSX	4.10.2051.0	2021/08/10 03:12:36	With CM: 4.3.1858.4353
bloomtest-Posture for Windows	AgentProfile	Not Applicable	2024/03/30 19:31:40	test windows PC for con...
AnyConnectDesktopWindows 4.10.7073.0	AnyConnectDesktopWindows	4.10.7073.0	2024/03/30 19:47:18	AnyConnect Secure Mob...
MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2021/08/10 03:12:27	Supplicant Provisioning ...
CiscoAgentlessWindows 4.10.02051	CiscoAgentlessWindows	4.10.2051.0	2021/08/10 03:12:33	With CM: 4.3.2227.6145
Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/10/07 04:01:12	Pre-configured Native S...
WLC9800-windows	AgentConfig	Not Applicable	2024/04/01 17:44:50	Test for WLC9800 Wirele...
WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/10 03:12:27	Supplicant Provisioning ...
CiscoTemporalAgentWindows 4.10.02051	CiscoTemporalAgentWindows	4.10.2051.0	2021/08/10 03:12:28	With CM: 4.3.2227.6145
CiscoSecureClientDesktopWindows 5.1.2.042	CiscoSecureClientDesktopWindows	5.1.2.42	2024/03/30 19:20:54	Cisco Secure Client for ...

成功上傳安全客戶端和合規性模組

步驟4. 建立代理狀態配置檔案導航到工作中心>狀態>客戶端調配>資源>新增>代理狀態配置檔案:

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy Resources Client Provisioning Portal

ISE Posture Agent Profile Settings > bloomtest-Posture for Windows

Agent Posture Profile

Name \*  
bloomtest-Posture for Windows

Description:  
test windows PC for connecting WLC9800

Agent Behavior

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent
Operate on non-802.1X wireless	No	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled	Agent can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Disabled	Display user notifications even when in Stealth mode.

代理狀態配置檔案

步驟5. 建立代理配置導航到工作中心>狀態>客戶端調配>資源>新增>代理配置:

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

\* Select Agent Package: CiscoSecureClientDesktopWindows 5.1

\* Configuration Name: WLC9800-windows

Description: Test for WLC9800 Wireless dot1x

Description Value Notes

\* Compliance Module CiscoSecureClientComplianceModuleW

Cisco Secure Client Module Selection

ISE Posture

VPN

Zero Trust Access

Network Access Manager

Secure Firewall Posture

Network Visibility

Umbrella

Start Before Logon

Dagnostic and Reporting Tool

Profile Selection

\* ISE Posture bloomtest-Posture for Windows

新增代理配置

步驟6.確認客戶端調配門戶，使用預設門戶進行測試。（請從CA伺服器生成CSR並應用SSL證書，並替換此門戶設定上的證書組標籤。否則，在測試過程中會出現證書不可信警告。）

導航至工作中心>狀態>客戶端調配>客戶端調配門戶：

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

## Client Provisioning Portals

You can edit and customize the default Client Provisioning portal and create additional ones

Create Edit Duplicate Delete

Client Provisioning Portal (default)

Default portal and user experience used to install the posture agents and verify compliance on user's devices

選擇客戶端調配門戶01

Client Provisioning Policy  
Resources  
Client Provisioning Portal

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:\* **8443**  
(8000 - 8999)

Bidirectional port:\* **8449**  
(8000 - 8999)

Allowed Interfaces:\*

For PSNs Using Physical Interfaces

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

- Bond 0  
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- Bond 1  
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- Bond 2  
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: \* **Test-CPP** ▼  
Configure certificates at:  
[Administration > System > Certificates > System Certificates](#)

Authentication method: \* **Certificate\_Request\_Sequence** ▼  
Configure authentication methods at:  
[Administration > Identity Management > Identity Source Sequences](#)

選擇客戶端調配門戶02

步驟7.建立客戶端調配策略。導航到Work Centers> Posture> Client Provisioning> Client Provisioning Policy > Edit>插入上述新策略。

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
WLC9800-Windows	If Any	and Windows All	and Condition(s)	then WLC9800-windows
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.10.02051 And MacOSXSPWizard 2.7.0.1 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

建立客戶端調配策略

步驟8.建立檔案條件。導航到工作中心>狀態>策略元素>條件>檔案>檔案條件>新增:

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

File Conditions List > WLC9800-Posture-demo

**File Condition**

Name \* WLC9800-Posture-demo

Description test for WLC9800

\* Operating System Windows All

Compliance Module Any version

\* File Type FileExistence

\* File Path USER\_DESKTOP WLC9800-Posture-Demo.txt

\* File Operator Exists

建立檔案條件

步驟9. 建立補救導航到工作中心>狀態>策略元素>補救>檔案>新增:

≡ Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

File Remediations List > WLC9800-Posture-Demo

**File Remediation**

\* Name WLC9800-Posture-Demo

Description your PC must have file named WLC9800-Posture-

Compliance Module Any version

Version 1.0

File Uploaded WLC9800-Posture-Demo.txt

建立檔案補救

步驟10. 建立需求。 導航至工作中心>狀態>策略元素>要求>插入新要求:

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions

Remediations

Application

Anti-Malware

Anti-Spyware

Anti-Virus

File

Firewall

Launch Program

Link

Patch Management

Script

USB

Windows Server Update Servi...

Windows Update

Requirements

Allowed Protocols

Authorization Profiles

Downloadable ACLs

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst then	Message Text Only <a href="#">Edit</a>
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win then	Select Remediations <a href="#">Edit</a>
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac then	Select Remediations <a href="#">Edit</a>
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check then	Select Remediations <a href="#">Edit</a>
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check then	Select Remediations <a href="#">Edit</a>
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win then	Default_Firewall_Remediation_Win <a href="#">Edit</a>
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac then	Default_Firewall_Remediation_Mac <a href="#">Edit</a>
WLC9800-Posture-Demo	for Windows All	using Any version	using Agent	met if WLC9800-Posture-demo then	WLC9800-Posture-Demo <a href="#">Edit</a>

Note:  
Remediation Action is filtered based on the operating system and stealth mode selection.  
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.  
Remediations Actions are not applicable for Agentless Posture type.

建立狀態要求

步驟11.建立狀態策略。導航到工作中心>狀態>插入新策略:

Work Centers - Posture

Overview Network Devices Client Provisioning **Posture Policy** Policy Sets Troubleshoot Reports Settings

Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions. WLC9800

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	WLC9800-Posture-Demo	if Any	and Windows All	and Any version	and Agent	and	then WLC9800-Posture-Demo <a href="#">Edit</a>

建立狀態策略

步驟12.建立三個授權配置檔案：狀態未知；安全評估狀態為「不符合」；安全評估狀態是符合的。導航到Policy> Policy Elements> Results> Authorization> Authorization Profiles> Add:

Dictionarys Conditions **Results**

Authentication

Allowed Protocols

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

### Standard Authorization Profiles

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

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	WLC9800	X	
<input type="checkbox"/>	WLC9800-Posture-Compliant	Cisco	
<input type="checkbox"/>	WLC9800-Posture-NonCompliant	Cisco	
<input type="checkbox"/>	WLC9800-Posure-Unknown	Cisco	

建立授權配置檔案01

[Dictionaries](#)
[Conditions](#)
[Results](#)

[Authentication](#)

- Allowed Protocols

[Authorization](#)

- Authorization Profiles
- Downloadable ACLs

[Profiling](#)

[Posture](#)

[Client Provisioning](#)

[Authorization Profiles](#) > WLC9800-Posture-Unknown

### Authorization Profile

\* Name WLC9800-Posture-Unknown

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

✓ Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ACL POSTURE\_REDIRECT\_ACL Value Client Provisioning Portal (def:)

Static IP/Host name/FQDN  
 Suppress Profiler CoA for endpoints in Logical Profile

建立授權配置檔案02

[Dictionaries](#)
[Conditions](#)
[Results](#)

[Authentication](#)

- Allowed Protocols

[Authorization](#)

- Authorization Profiles
- Downloadable ACLs

[Profiling](#)

[Posture](#)

[Client Provisioning](#)

[Authorization Profiles](#) > WLC9800-Posture-Compliant

### Authorization Profile

\* Name WLC9800-Posture-Compliant

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

✓ Common Tasks

Interface Template

Web Authentication (Local Web Auth)

Airespace ACL Name POSTURE\_COMPLIANT\_ACL

Airespace IPv6 ACL Name

建立授權配置檔案03

Dictionarys Conditions Results

**Authorization Profile**

\* Name: WLC9800-Posture-NonComp

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Agentless Posture:

Passive Identity Tracking:

Common Tasks

Interface Template

Web Authentication (Local Web Auth)

Airespace ACL Name: POSTURE\_NON-COMPLIANT\_

Airespace IPv6 ACL Name

Advanced Attributes Settings

步驟13.建立策略集。導覽至Policy> Policy

Policy Sets Reset

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	WLC9800-Posture-Demo		AND Network Access Device IP Address EQUALS 10.124.60.41 Normalised Radius-SSID CONTAINS posture_demo	Default Network Access	0		
	Default	Default policy set		Default Network Access	0		

Reset

建立策略集

Sets> Add Icon:

步驟14.建立身份驗證策略導航到Policy> Policy Sets>展開「WLC9800-Posture-Demo」> Authentication Policy> Add:

Cisco ISE Policy - Policy Sets

WLC9800-Posture-Demo AND Network Access Device IP Address EQUALS 10.124.60.41 Normalised Radius-SSID CONTAINS posture\_demo Default Network Access

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Wireless-dot1x	Wireless_802.1X	Internal Users	0	Options
●	Default		All_User_ID_Stores	0	Options

建立身份驗證策略

步驟15.建立授權策略導航到Policy> Policy Sets>展開「WLC9800-Posture-Demo」> Authorization Policy>新增:

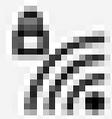
Authorization Policy (4)

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Posture-Compliant	Session PostureStatus EQUALS Compliant	WLC9800-Posture-Co...	Select from list	0
●	Posture-Noncompliant	Session PostureStatus EQUALS NonCompliant	WLC9800-Posture-No...	Select from list	0
●	Posture-Unknown	Session PostureStatus EQUALS Unknown	WLC9800-Posture-Unk...	Select from list	0
●	Default		DenyAccess	Select from list	0

建立授權策略

## 範例

1.使用正確的802.1X憑證連線的測試SSID posture\_demo。



posture\_demo  
Secured

Enter your user name and password

wlc9800-user

••••••••



OK

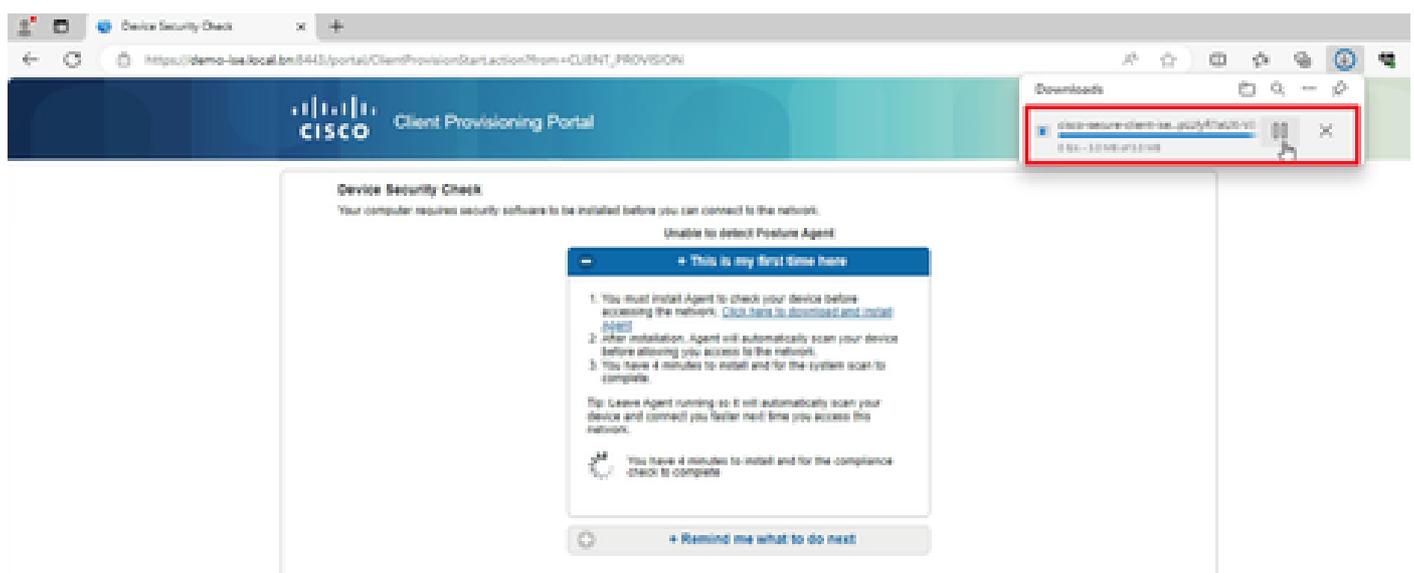
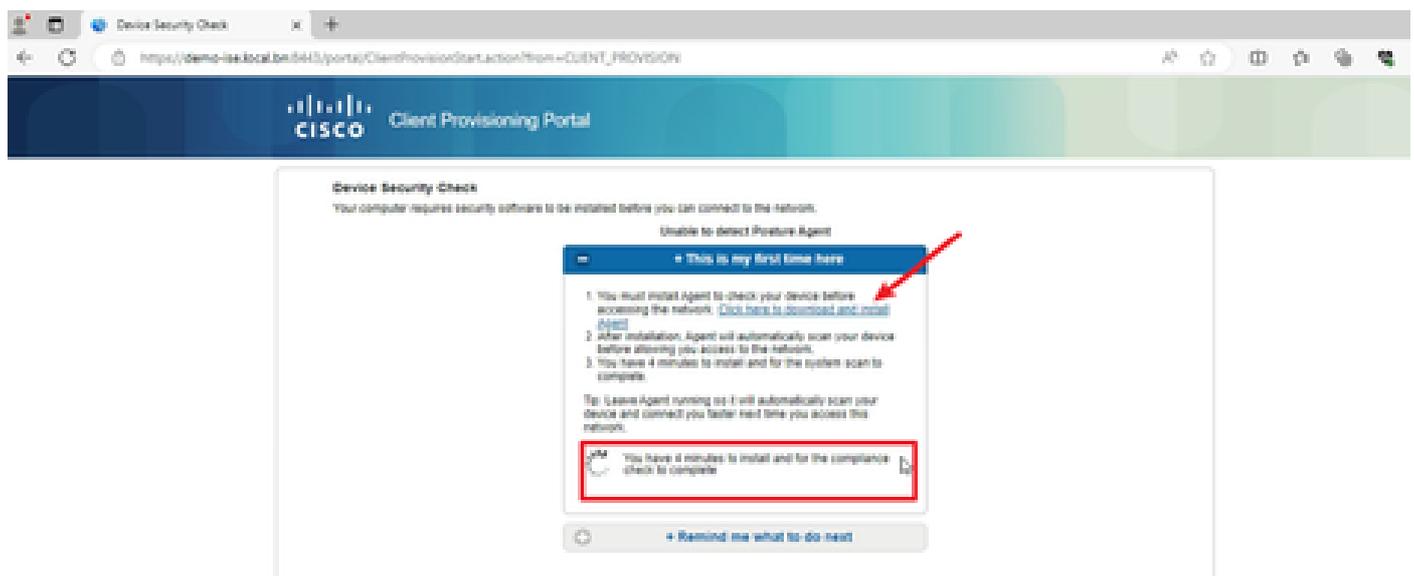
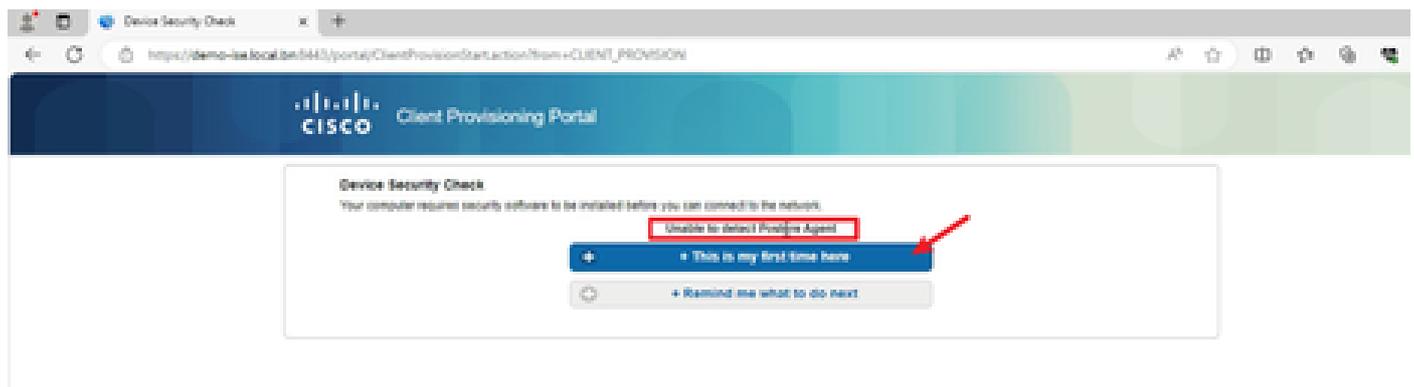
Cancel

## Network & Internet settings

Change settings, such as making a connection metered.

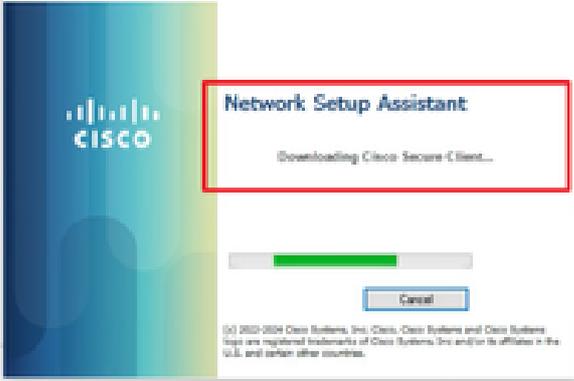


沒有安裝任何版本的終端安全評估代理，您可能看到「無法檢測終端安全評估代理」的結果，請按一下這是我第一次在此處按一下。您需要下載並安裝代理。



**Device Security Check**  
Your computer requires security software to be installed before you can connect to the network.

Network Setup Assistant



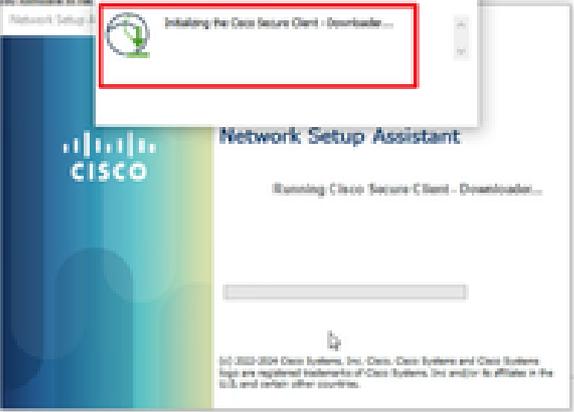
**Network Setup Assistant**  
Downloading Cisco Secure Client...

Cancel

© 2021-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.

**Device Security Check**  
Your computer requires security software to be installed before you can connect to the network.

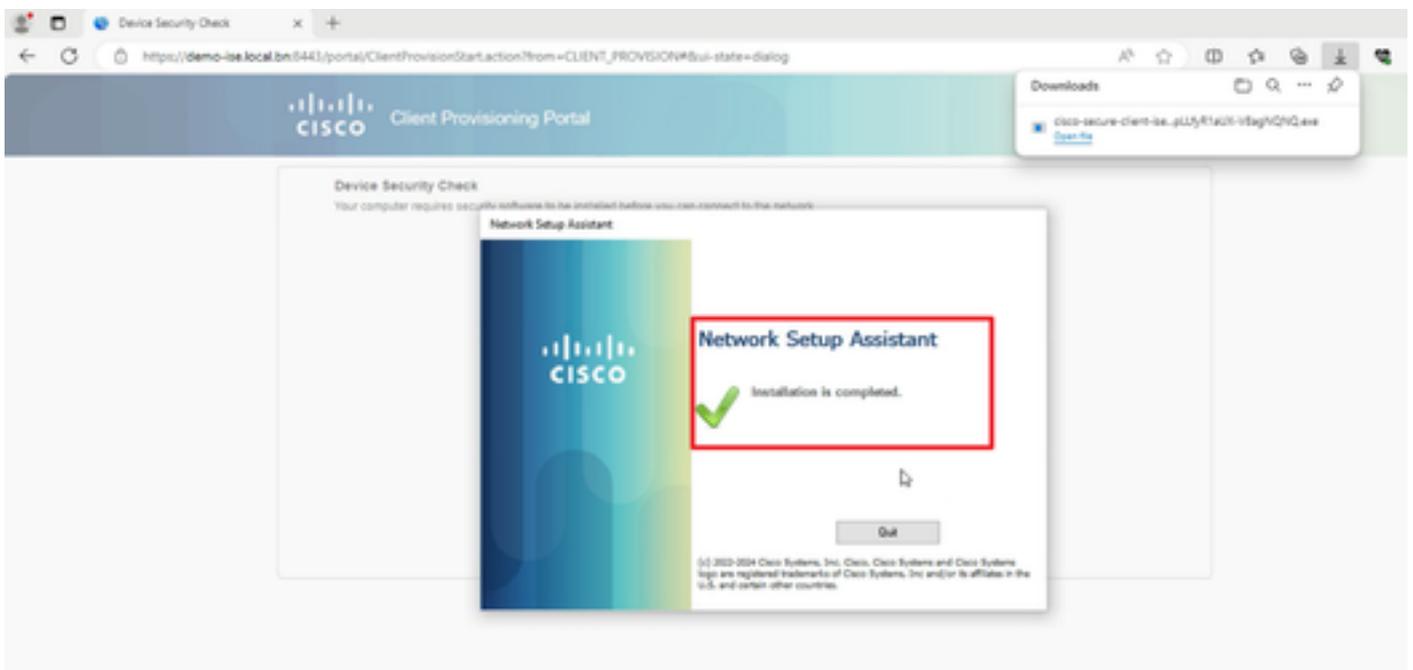
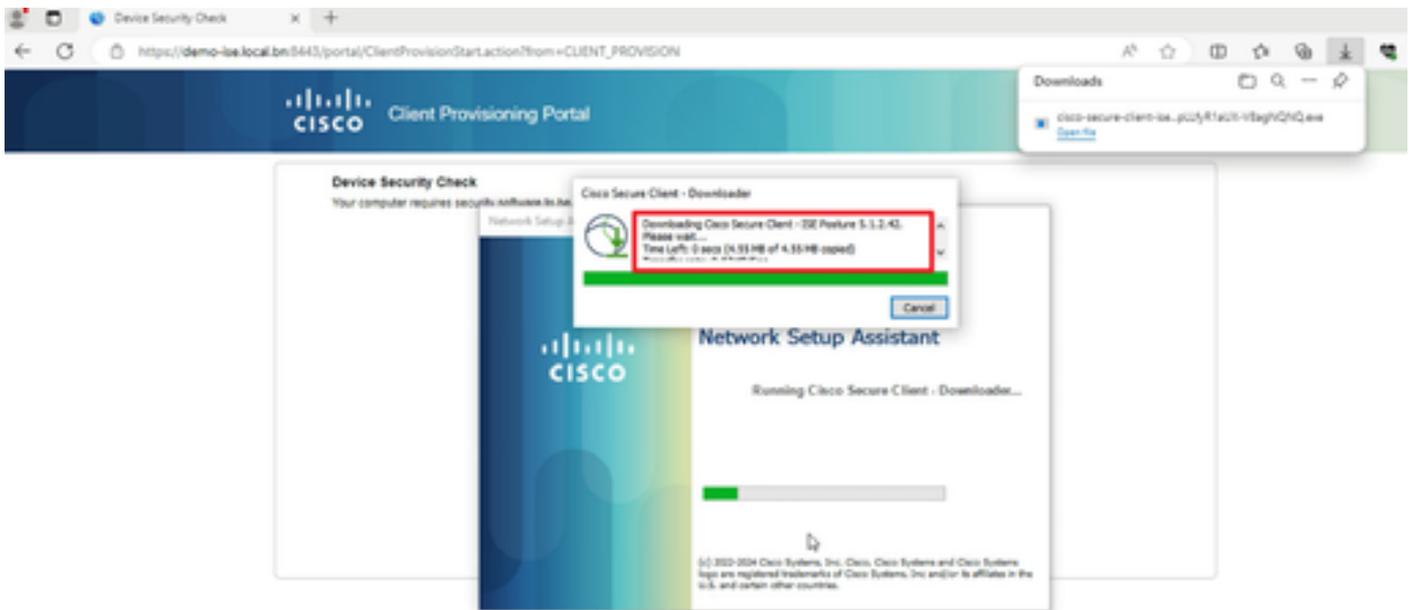
Network Setup Assistant



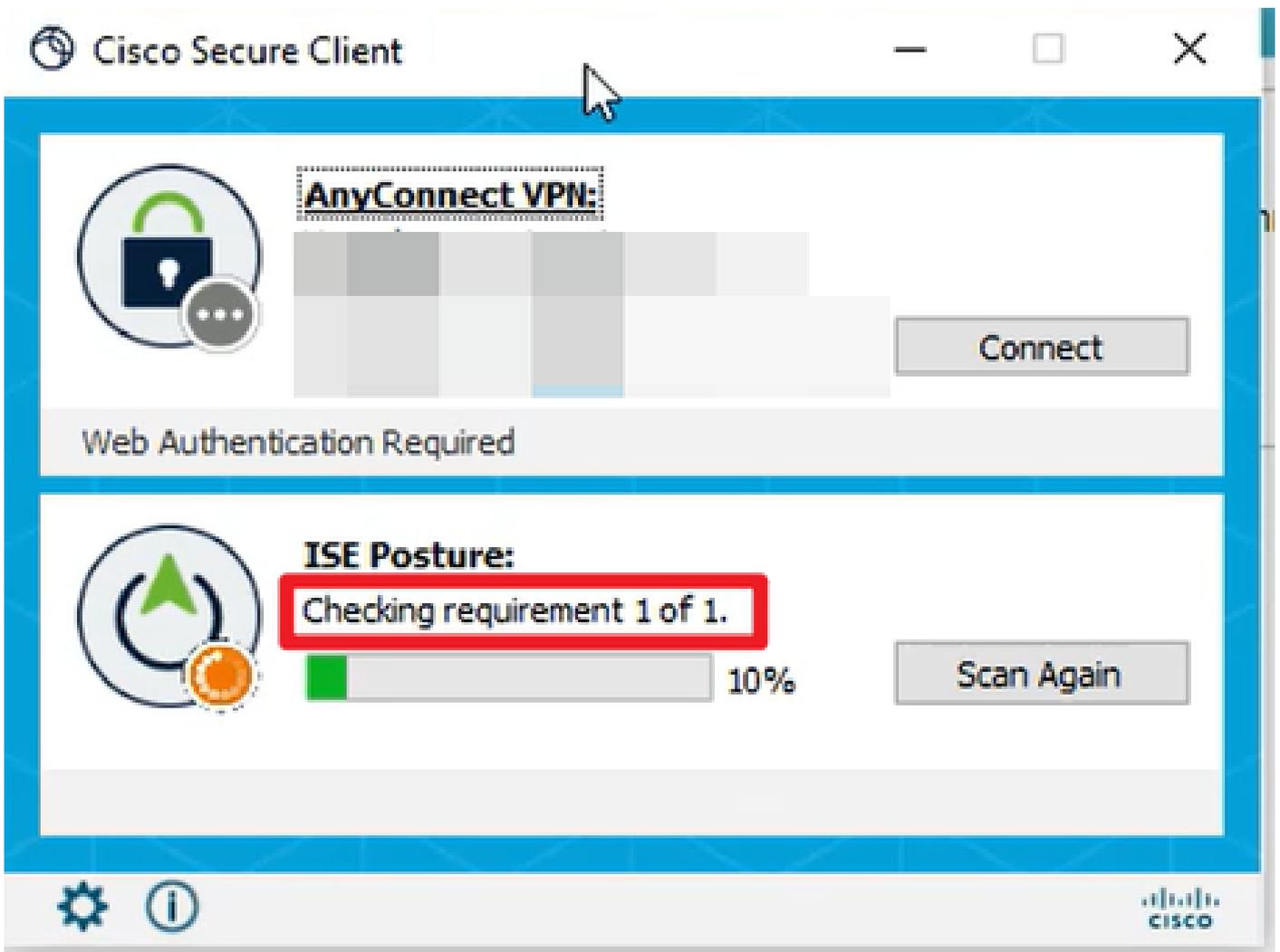
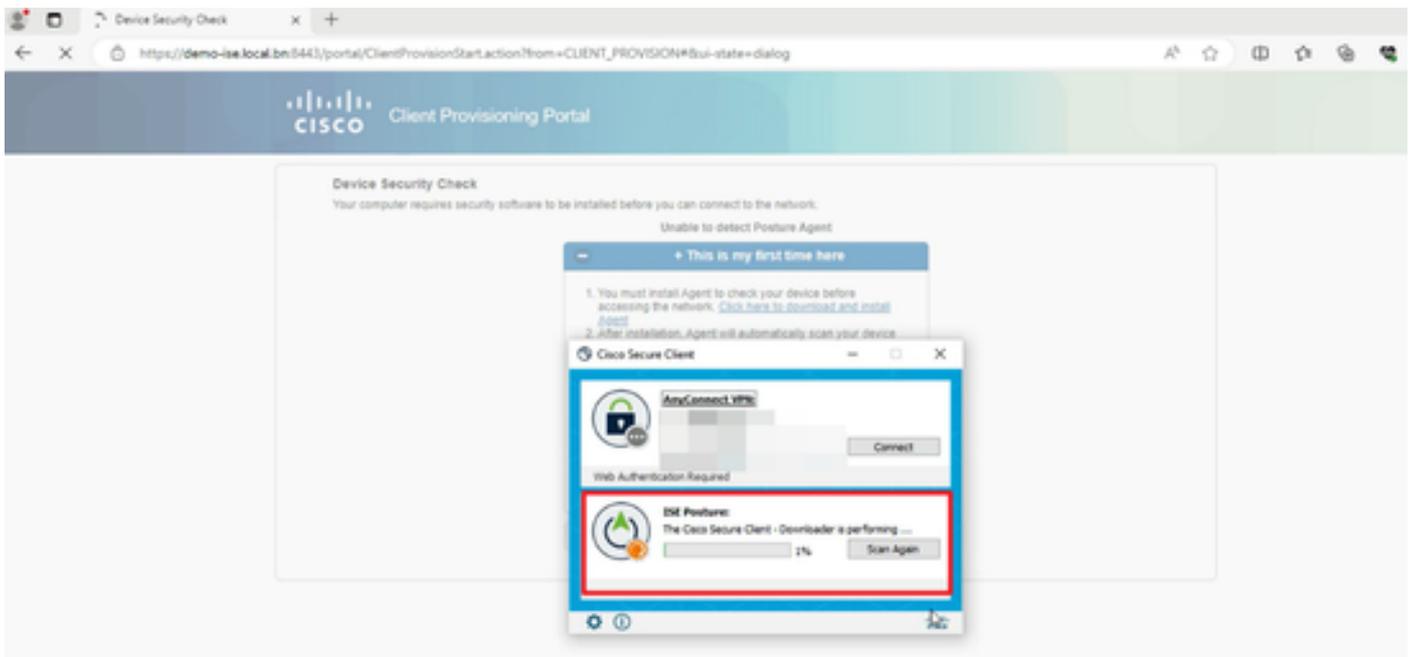
**Network Setup Assistant**  
Running Cisco Secure Client - Downloader...

Cancel

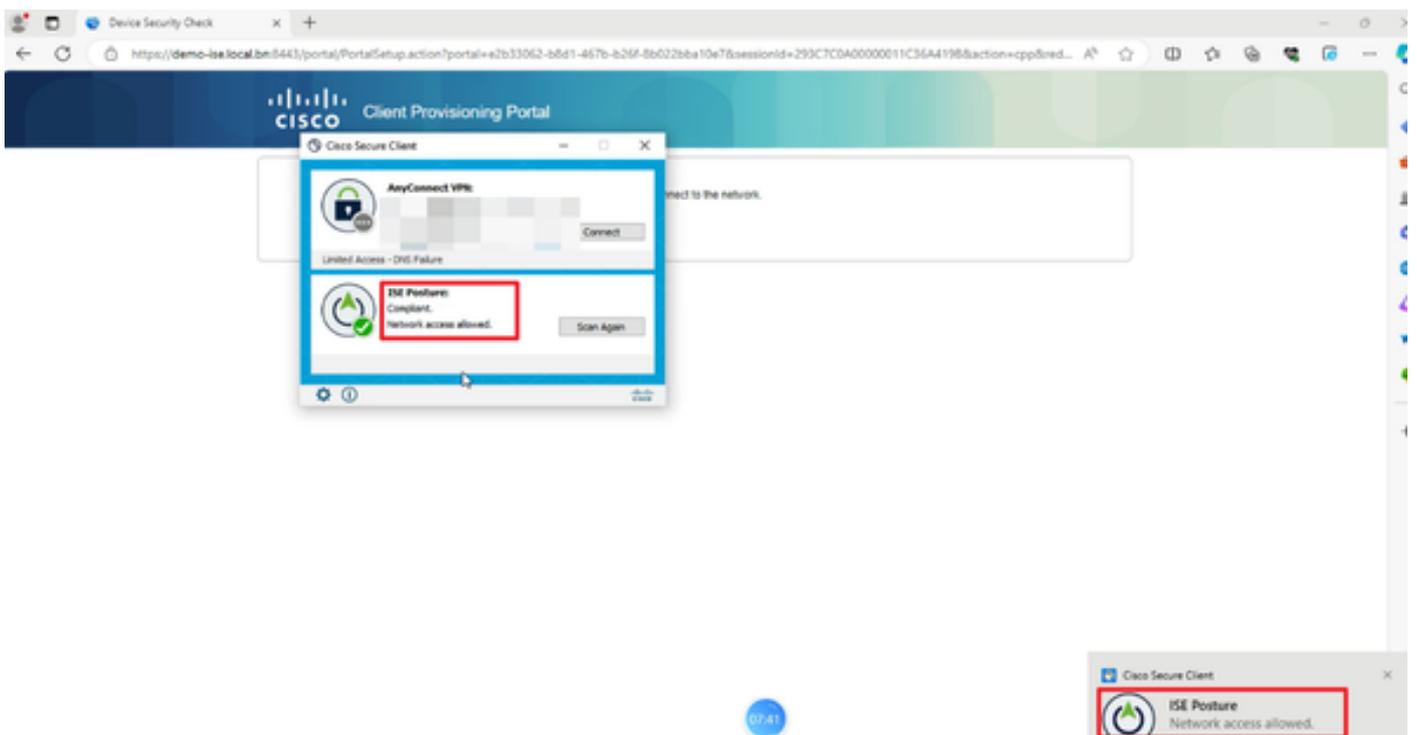
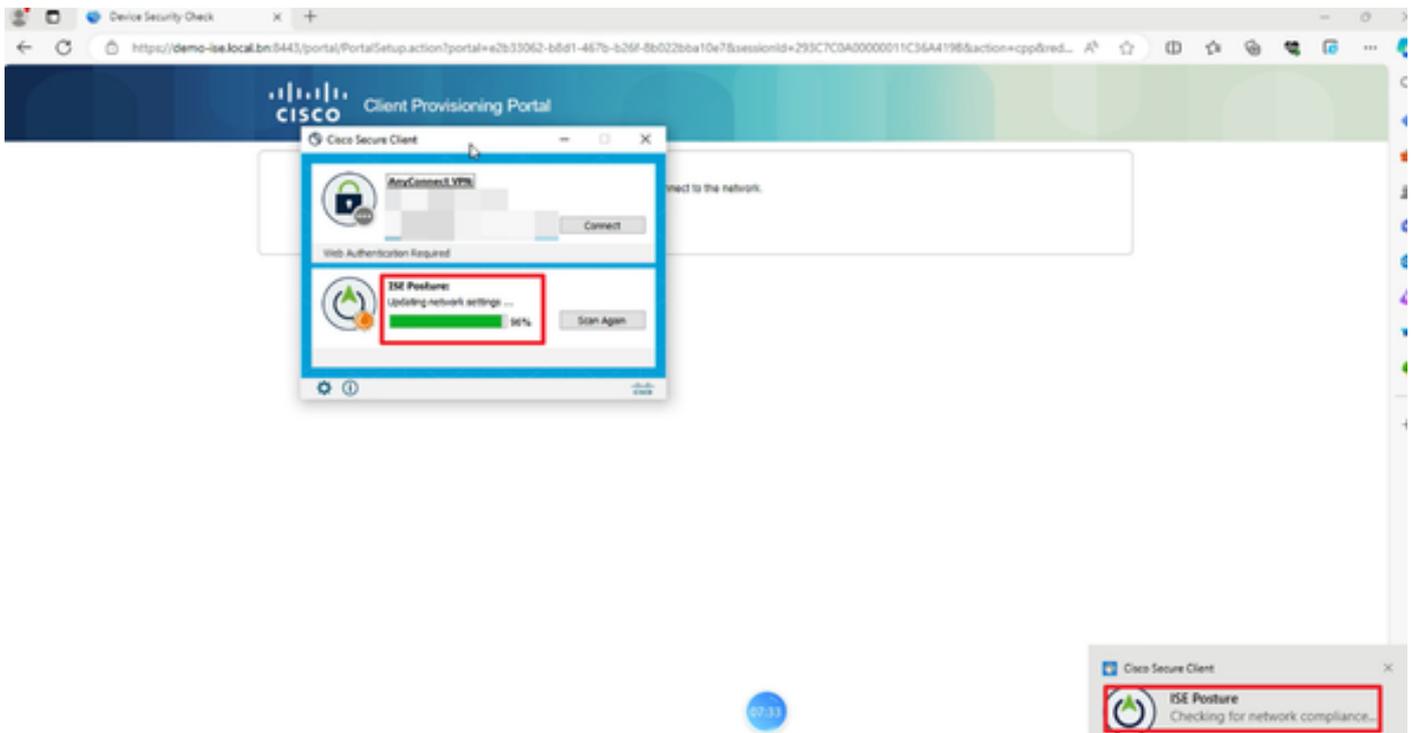
© 2021-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.



4. 安全評估代理運行並從ISE獲取安全評估要求。



5. 當檢查結果滿足終端安全評估要求時，PC向ISE傳送終端安全評估合規報告。ISE觸發CoA，因為此終端的終端安全評估狀態已更改。



## 驗證

在C9800 GUI上，驗證客戶端是否根據投訴/無投訴狀態結果獲得適當的ACL。

合規：

The screenshot shows the Cisco ISE Client configuration interface. The left pane displays a list of clients with columns for Client MAC Address, IPv4 Address, IPv6 Address, and AP Name. The right pane shows the configuration for a specific client, with the 'Security Information' tab selected. Under the 'Server Policies' section, the 'Filter-ID' is set to 'POSTURE\_COMPLIANT\_ACL', which is highlighted with a red box. Other tabs like 'General', 'QOS Statistics', and 'ATF Statistics' are also visible.

不符合：

This screenshot is similar to the one above, showing the Cisco ISE Client configuration interface. However, in the 'Server Policies' section, the 'Filter-ID' is set to 'POSTURE\_NON-COMPLIANT\_ACL', which is highlighted with a red box. This indicates a non-compliant configuration.

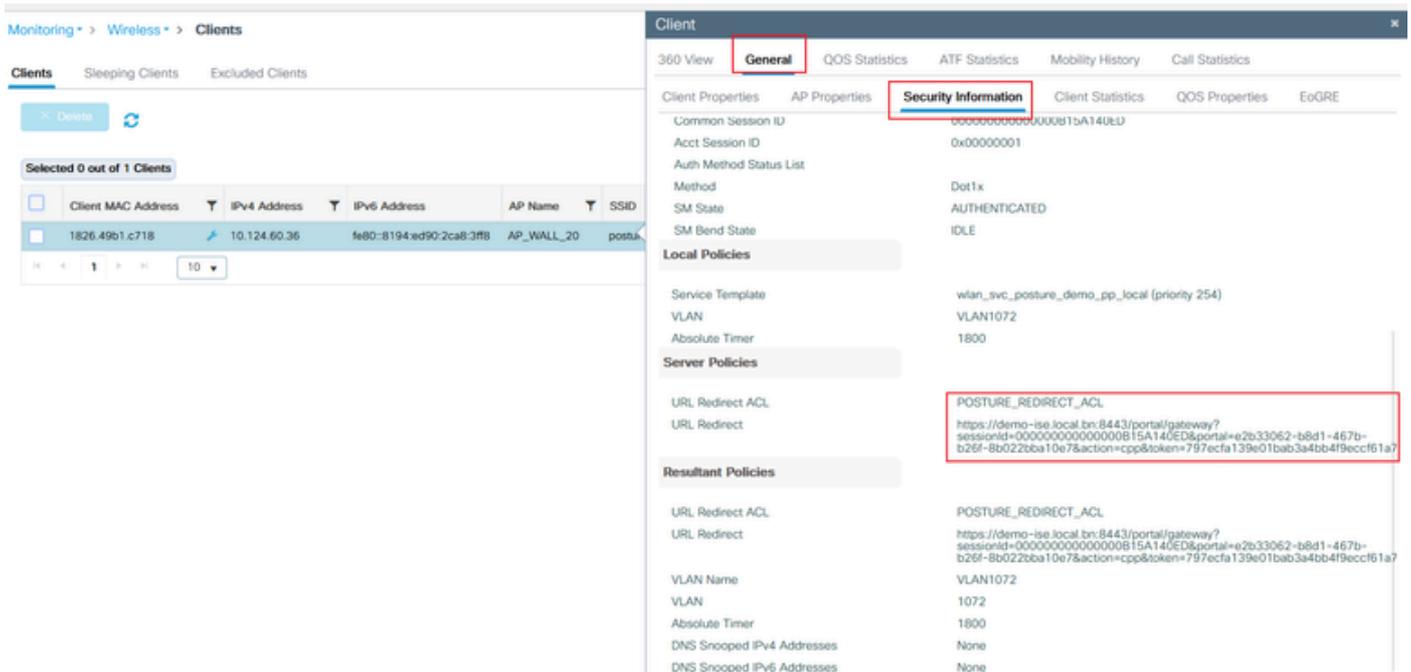
在ISE上，只需檢查Radius即時日誌，確認是否匹配正確的策略。

Timestamp	Status	Client	IP Address	Policy	Result
May 29, 2024 03:46:35.4...	Success	wlc9800-user	40.5B:D8:0F:45:65	WLC9800-Posture-Compliant	Compliant
May 29, 2024 03:46:34.8...	Success	wlc9800-user	40.5B:D8:0F:45:65	WLC9800-Posture-Compliant	Compliant
May 29, 2024 03:40:27.6...	Success	wlc9800-user	40.5B:D8:0F:45:65	WLC9800-Posture-Unknown	Pending

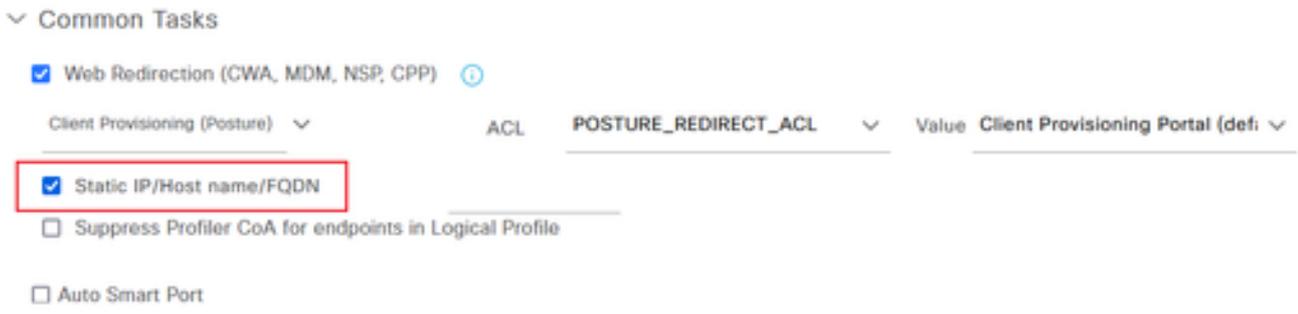
## 疑難排解

### 核對表

- 確保客戶端連線並獲得有效的IP地址。
- 確保WLC從ISE獲取正確的重定向URL和ACL。您可透過GUI檢查：



- 如果重新導向不是自動的，請開啟瀏覽器並嘗試隨機的IP地址。例如10.0.0.1。如果重新導向有效，則可能存在DNS解析問題。確認您擁有通過DHCP提供的有效DNS伺服器，並且該伺服器可以解析主機名。
- 如果瀏覽器已重定向到ISE門戶URL，但頁面無法載入，請檢查ISE域名是否未新增到DNS伺服器，因此客戶端無法解析門戶URL。若要快速解決此問題，請檢查Authorization Profile下的Static IP/Host name/FQDN，以在重定向URL中提供IP地址。但是，這可能是一個安全問題，因為它公開了ISE的IP地址。



## 收集調試

[在C9800上啟用調試](#)

[在ISE上啟用調試](#)

## 參考資料

- [在Catalyst 9800 WLC和ISE上配置CWA - Cisco](#)
- [帶身份服務引擎的無線BYOD](#)
- [部署ISE終端安全評估](#)
- [排除ISE會話管理和狀態故障](#)
- [將ISE終端安全評估重定向流量與ISE終端安全評估無重定向流量進行比較](#)

## 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）。