在Catalyst 9800 WLC和ISE上配置狀態

目錄

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。

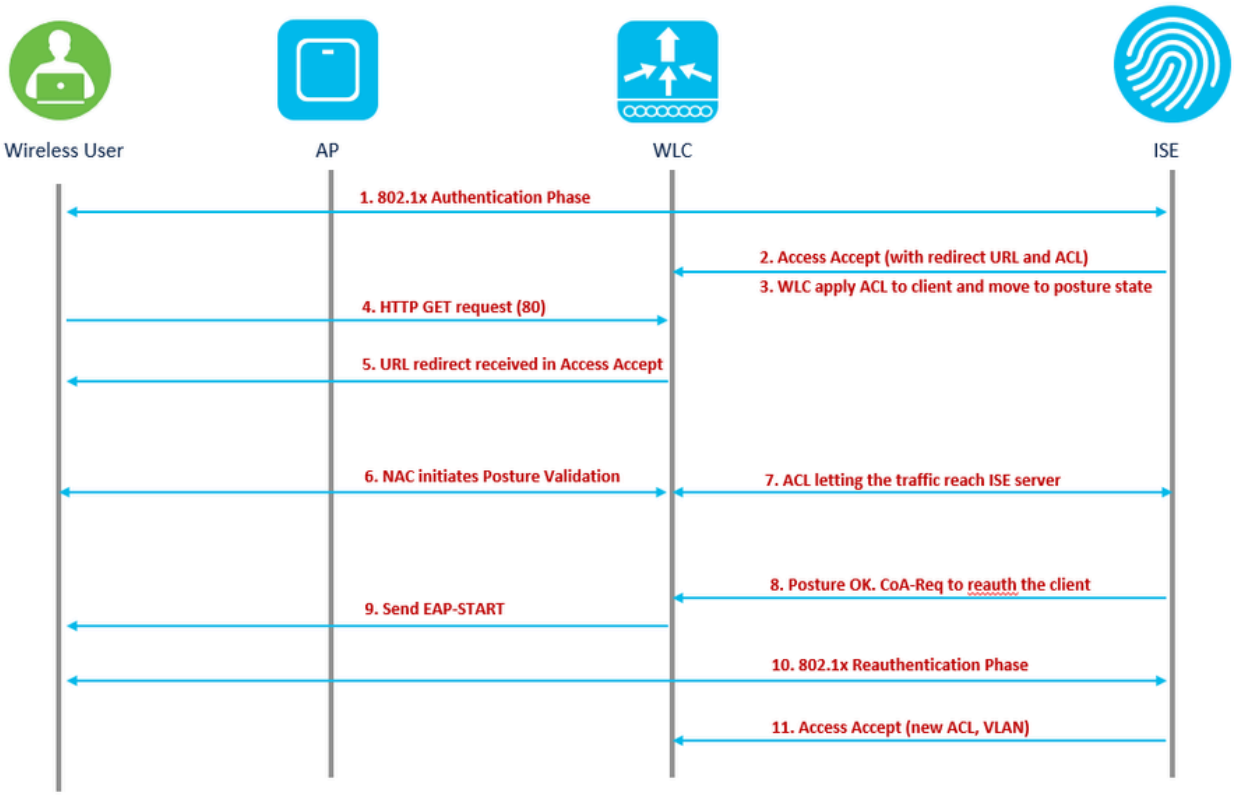
6.一旦ISE客戶端完成評估，將向WLC傳送帶有reauth服務的RADIUS CoA-Req。這將啟動客戶端的重新身份驗證（通過傳送EAP-START）。 重新身份驗證成功後，ISE會傳送訪問接受並帶有一個新的ACL（如果有）和沒有URL重定向或訪問VLAN。

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：



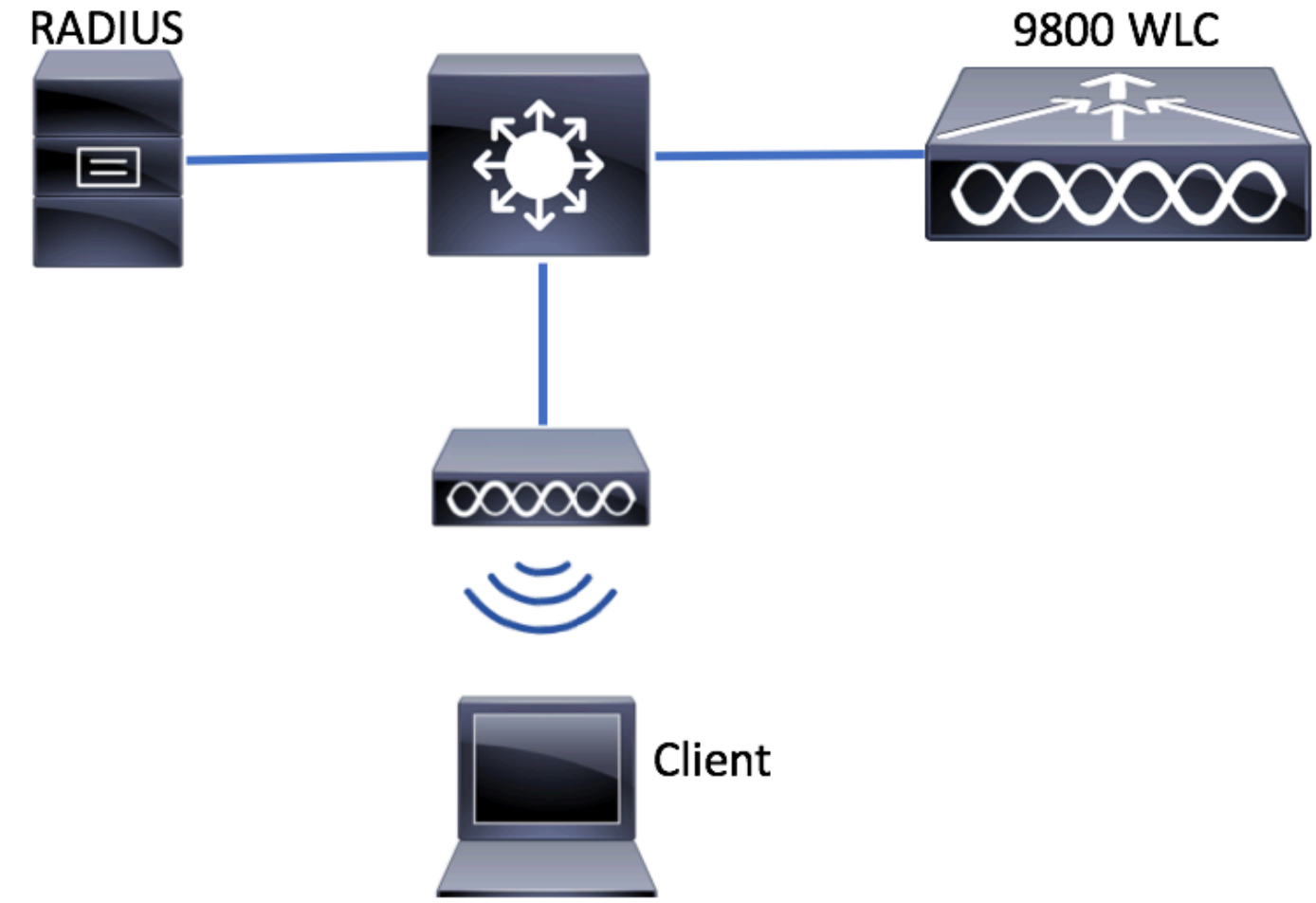
功能工作流

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

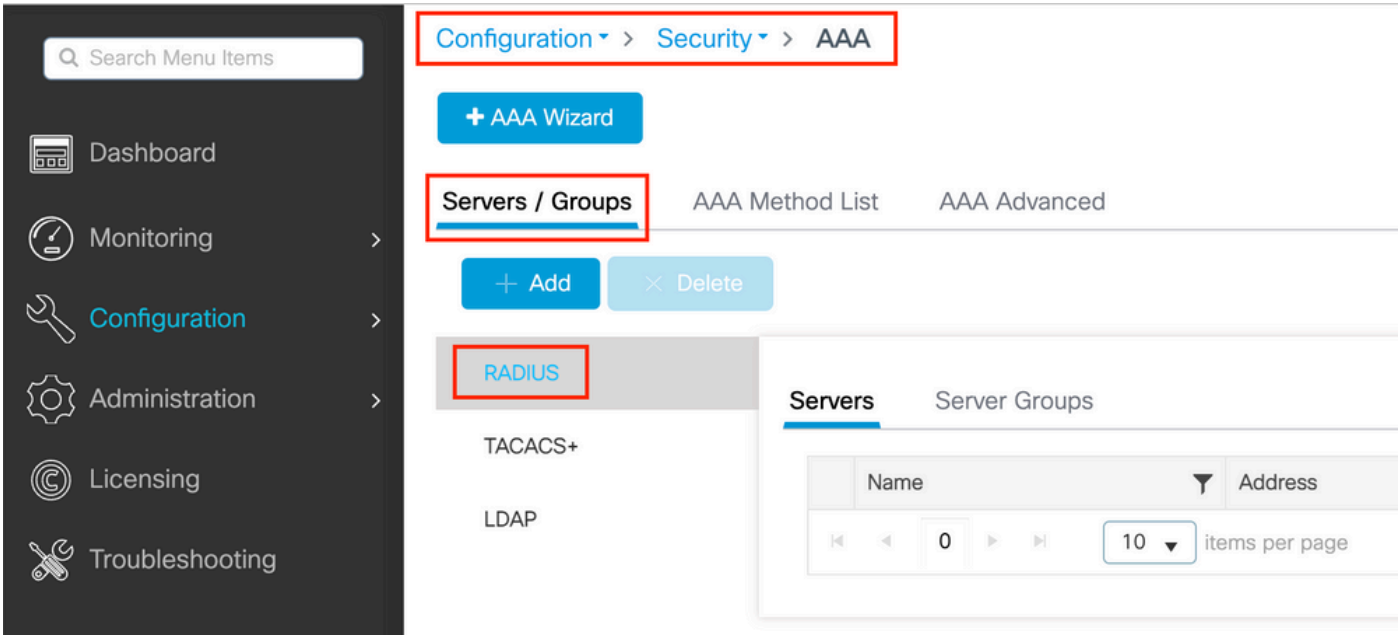
網路圖表



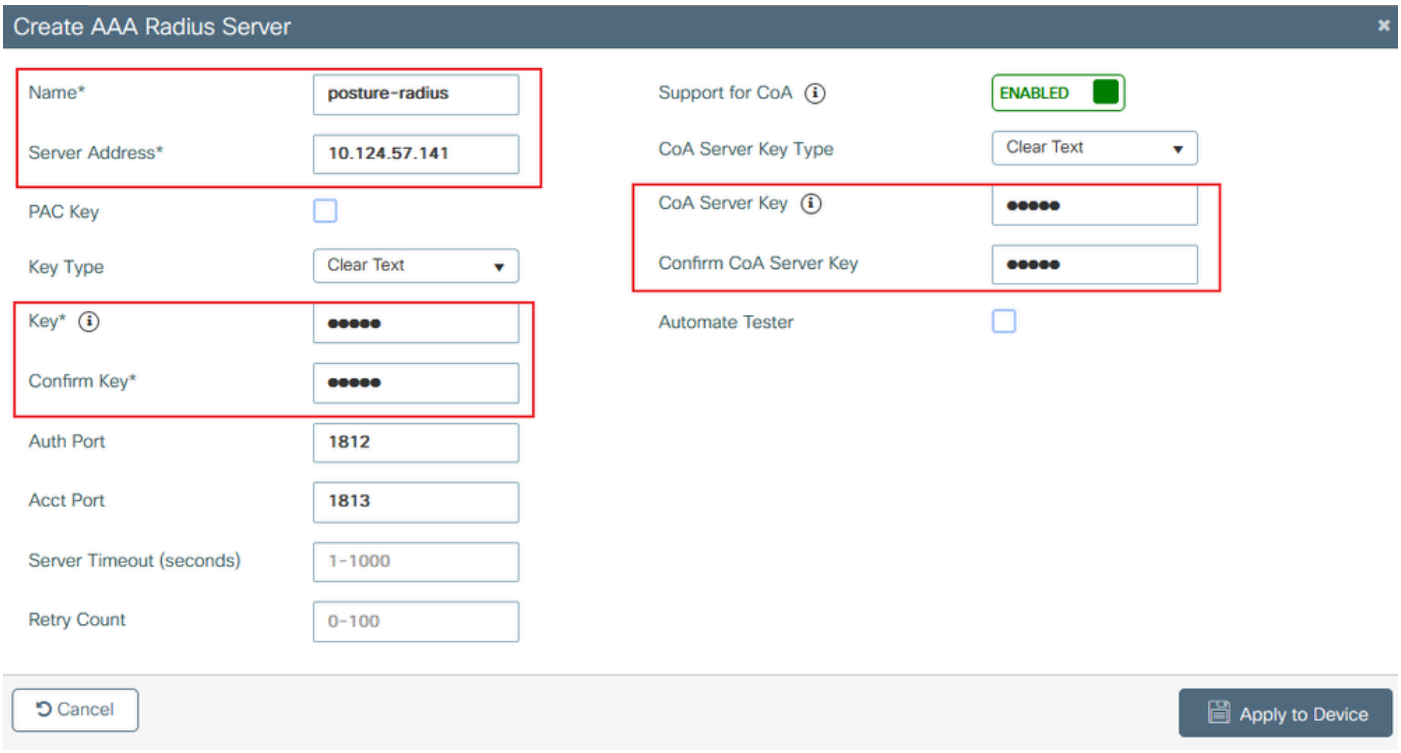
網路圖表

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。

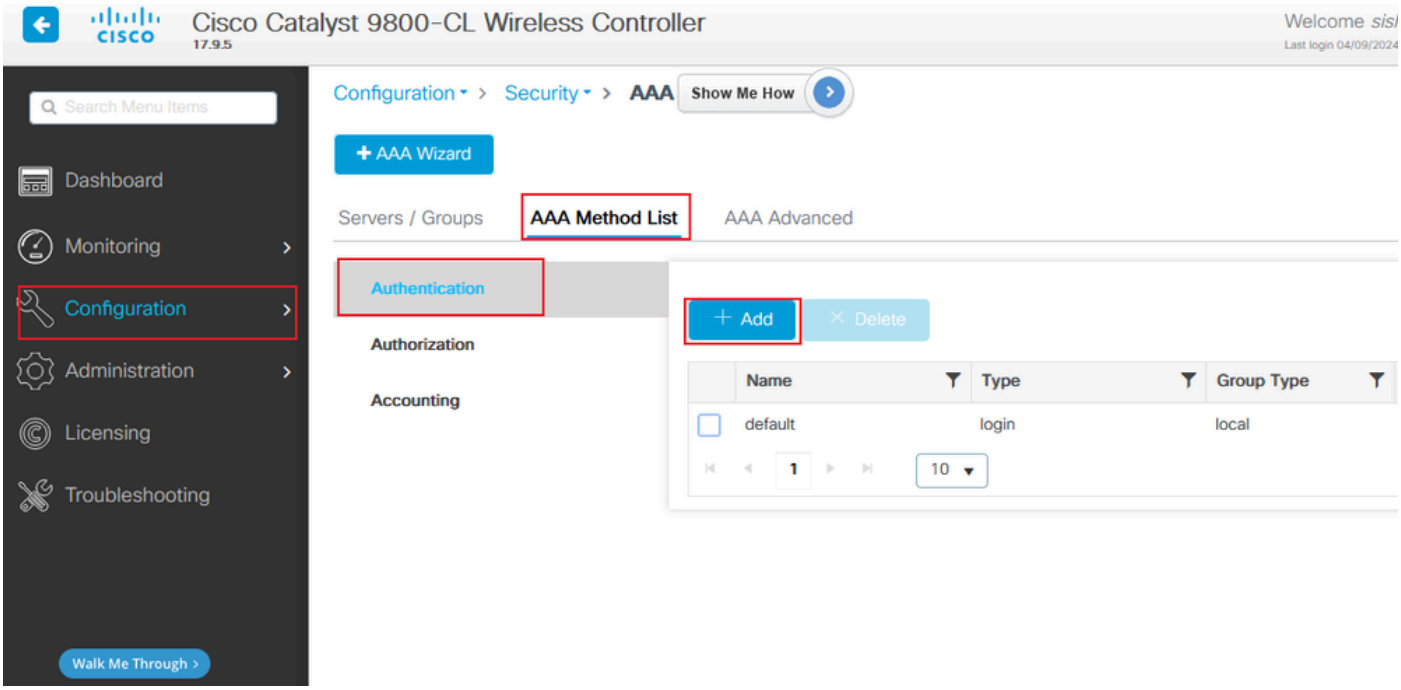


9800建立radius伺服器

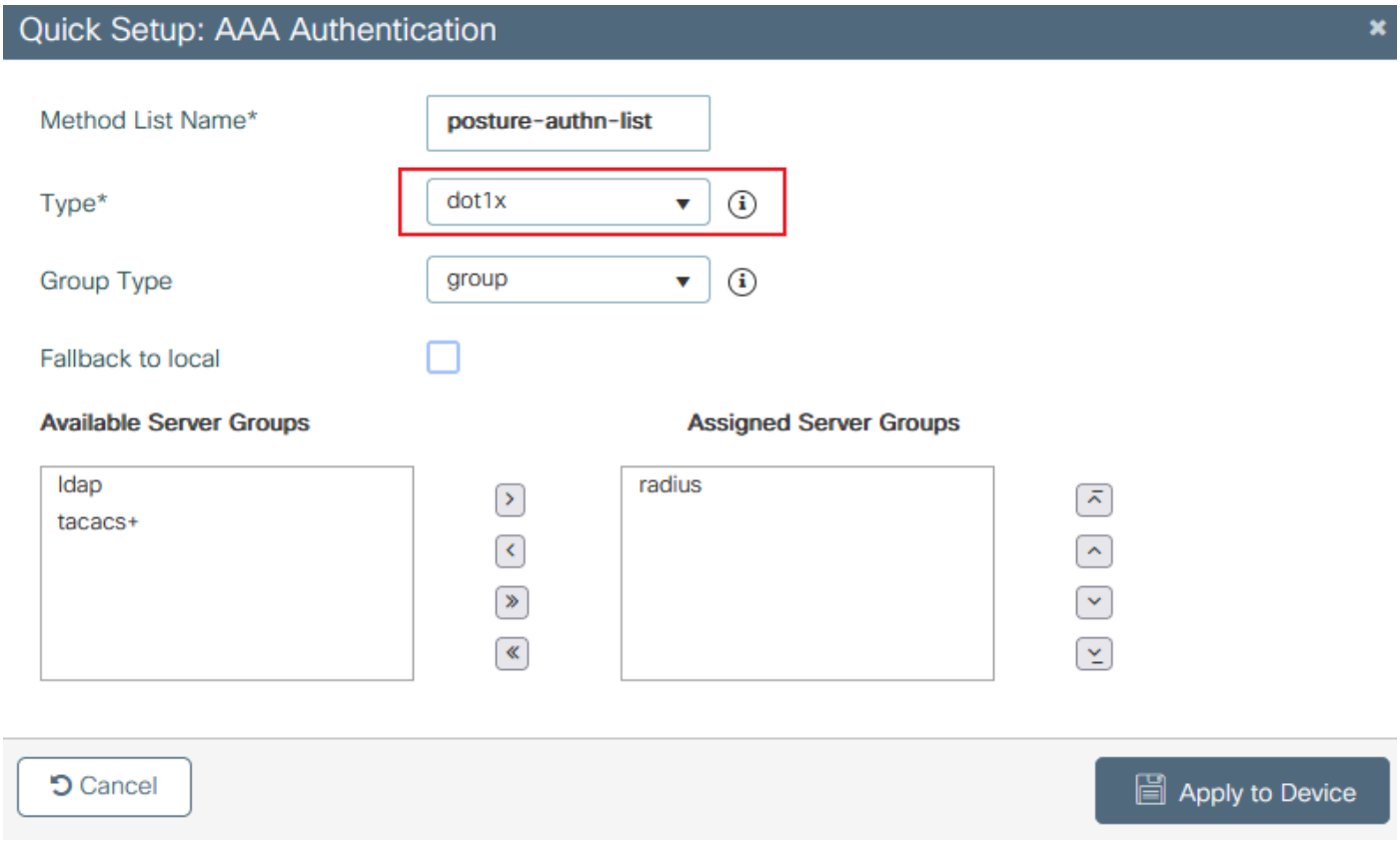


9800建立radius詳細資訊

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：

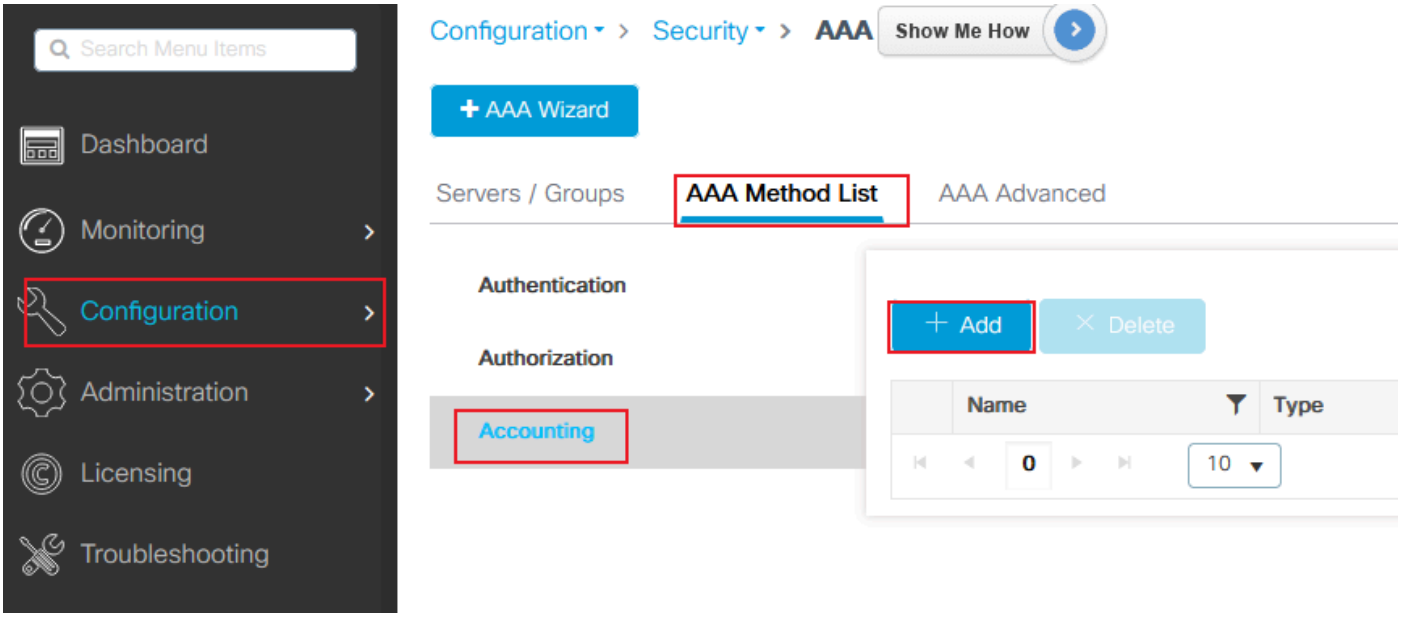


9800新增身份驗證清單

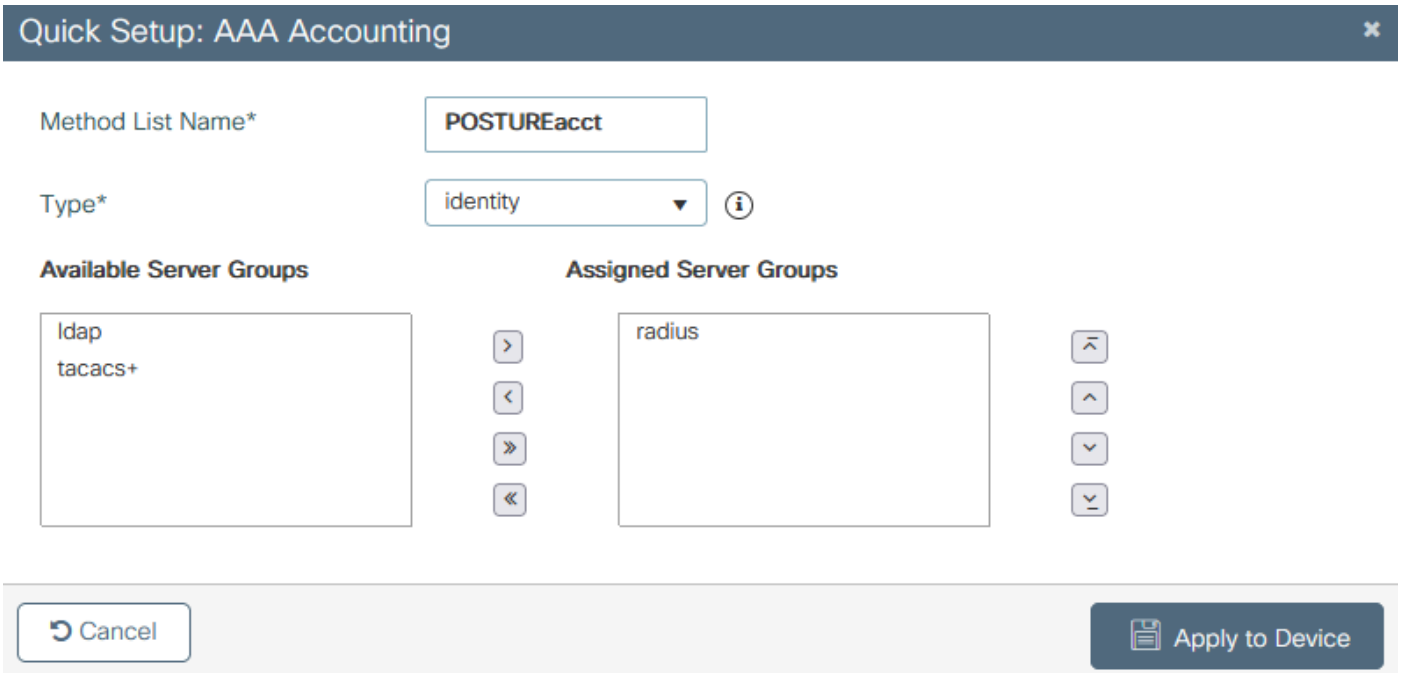


9800建立身份驗證清單詳細資訊

步驟3.（可選）建立會計方法清單，如下圖所示：



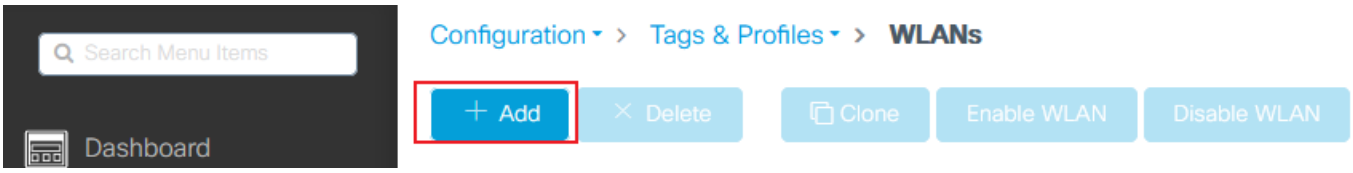
9800新增帳戶清單



9800建立帳戶清單詳細資訊

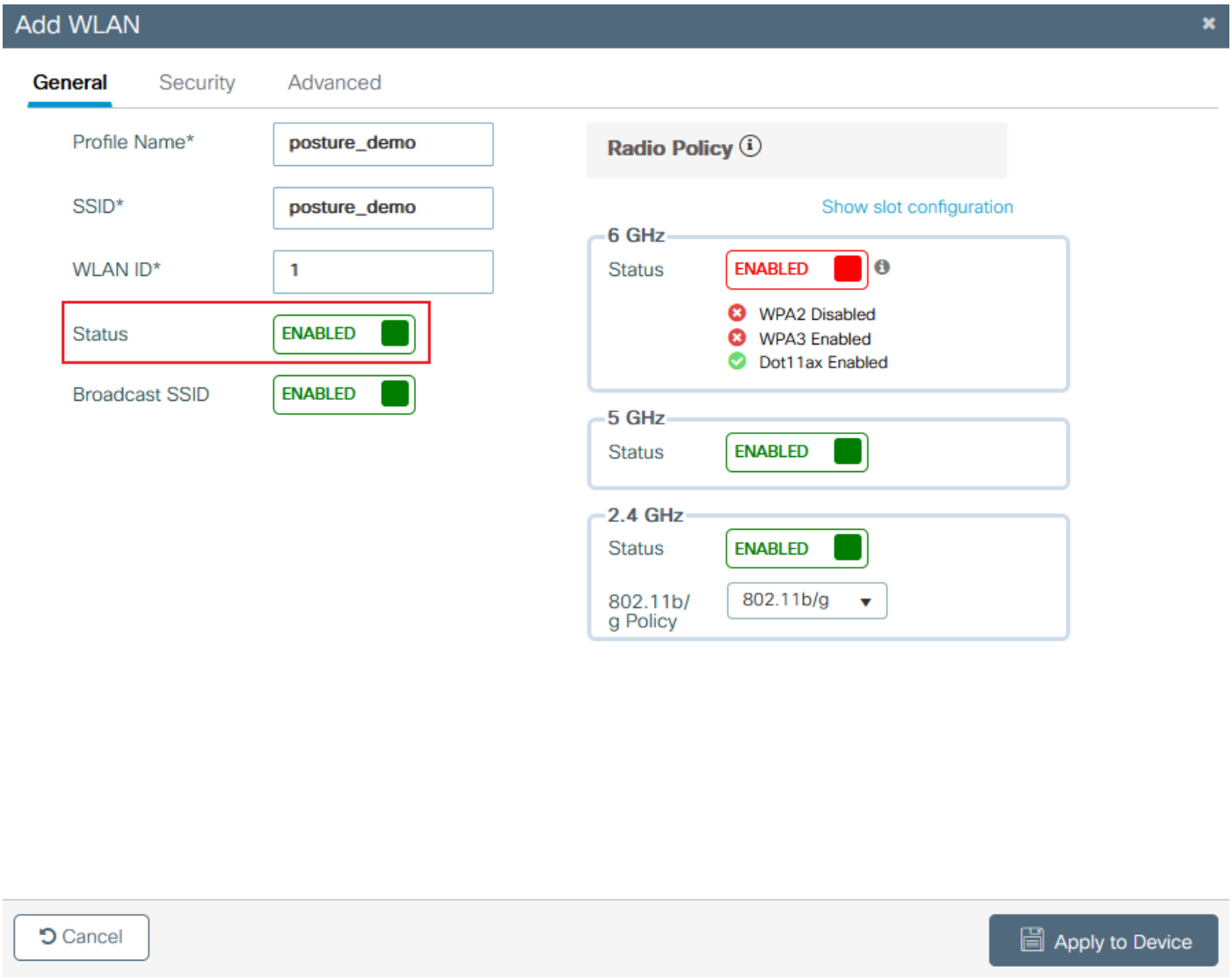
WLAN配置

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



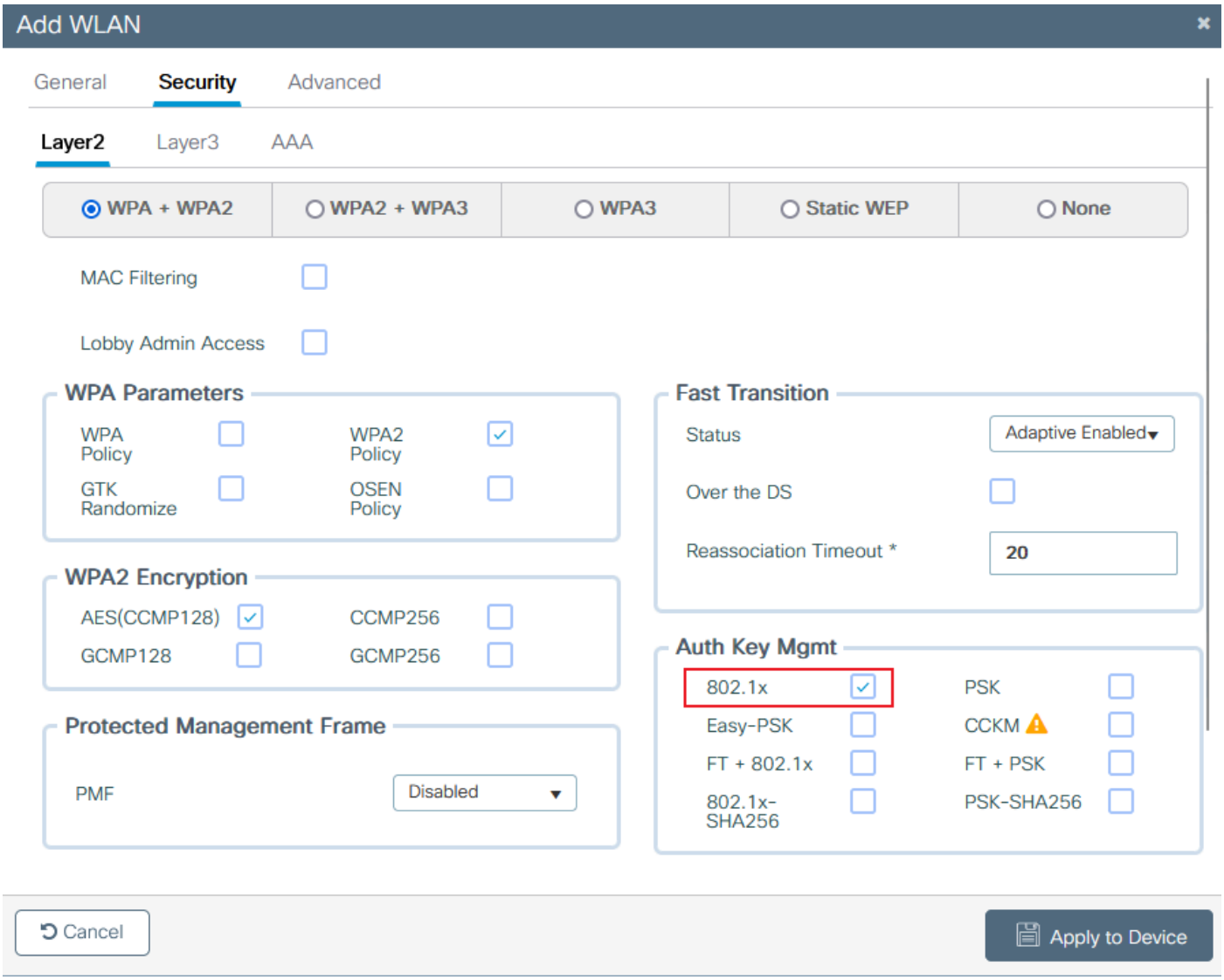
9800 WLAN新增

步驟2.輸入WLAN一般資訊。

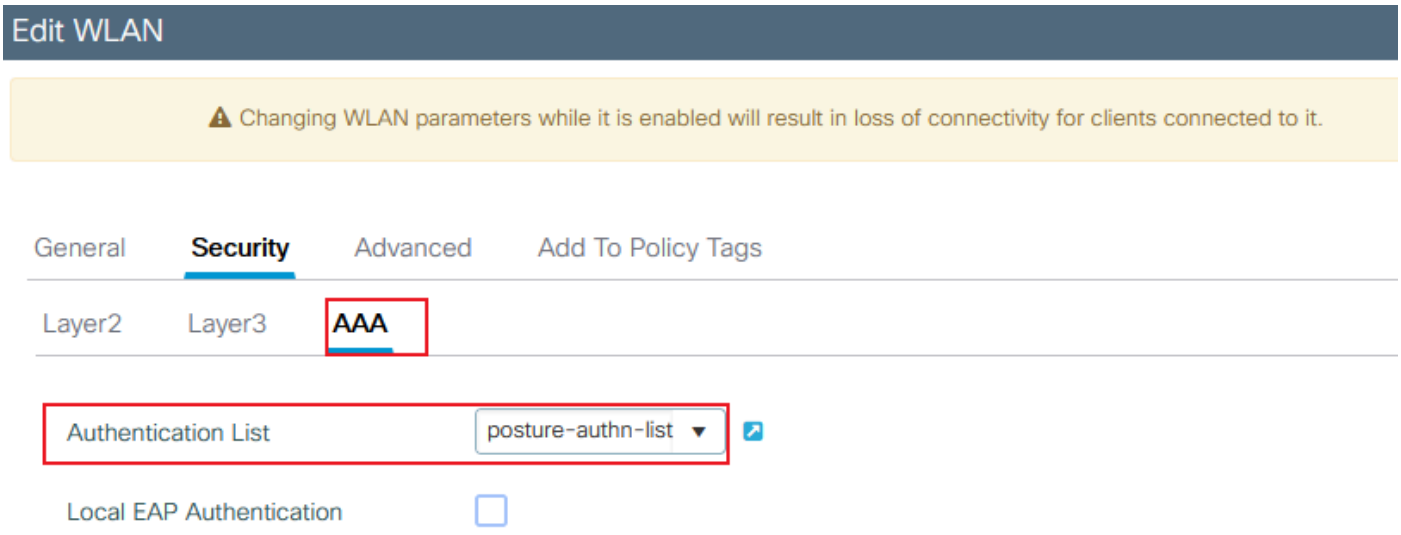


9800建立WLAN一般資訊

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):



9800建立WLAN安全L2

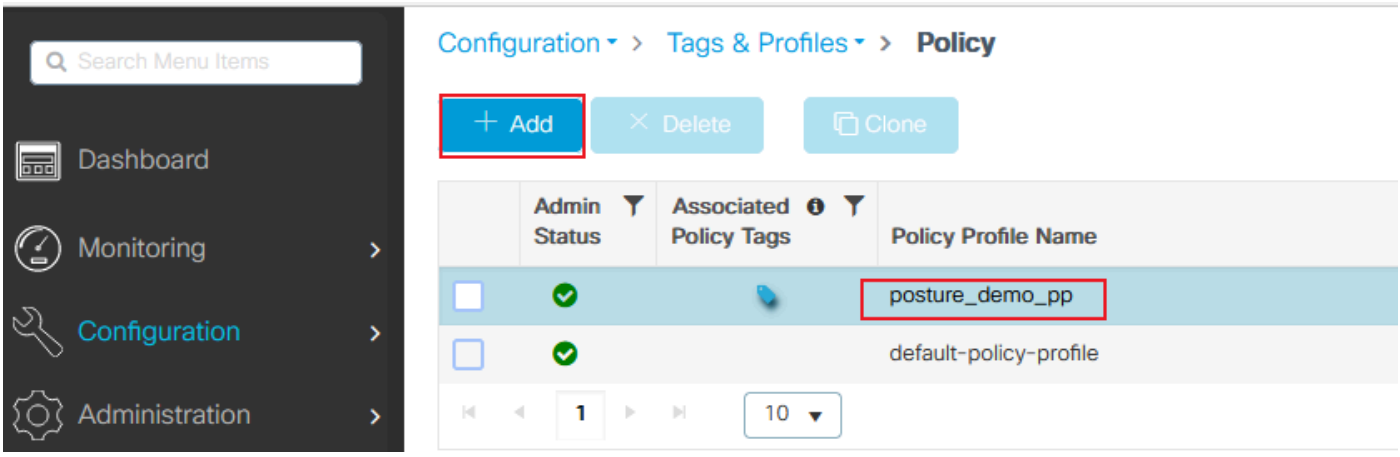


9800建立WLAN安全AAA

原則設定檔組態

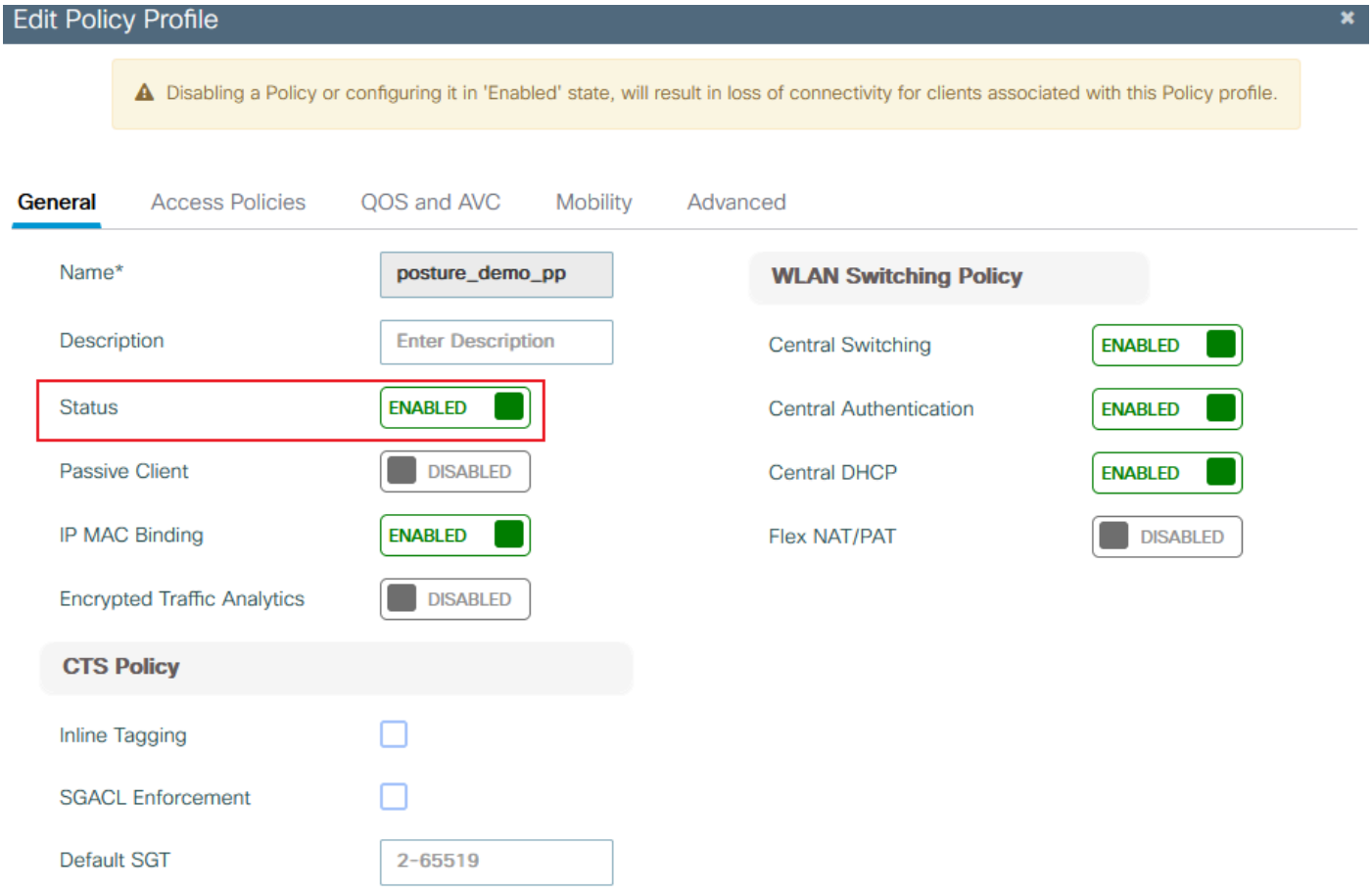
在策略配置檔案中，您可以決定分配客戶端到哪個VLAN，以及其他設定(如訪問控制清單(ACL)、服務品質(QoS)、移動錨點、計時器等)。 您可使用預設原則設定檔，或可建立新的設定檔。

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

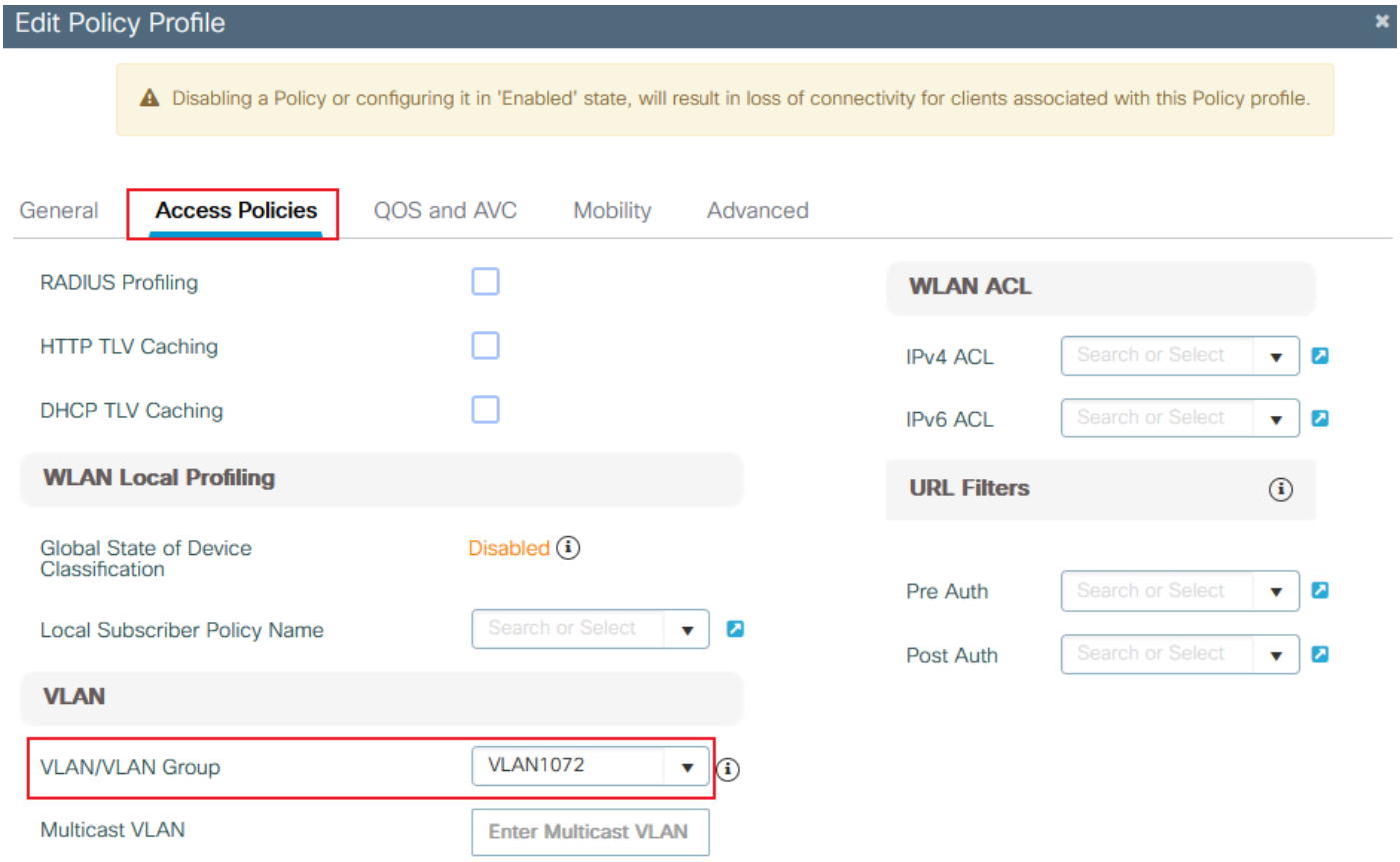
確認設定檔已啟用。



9800建立策略配置檔案常規

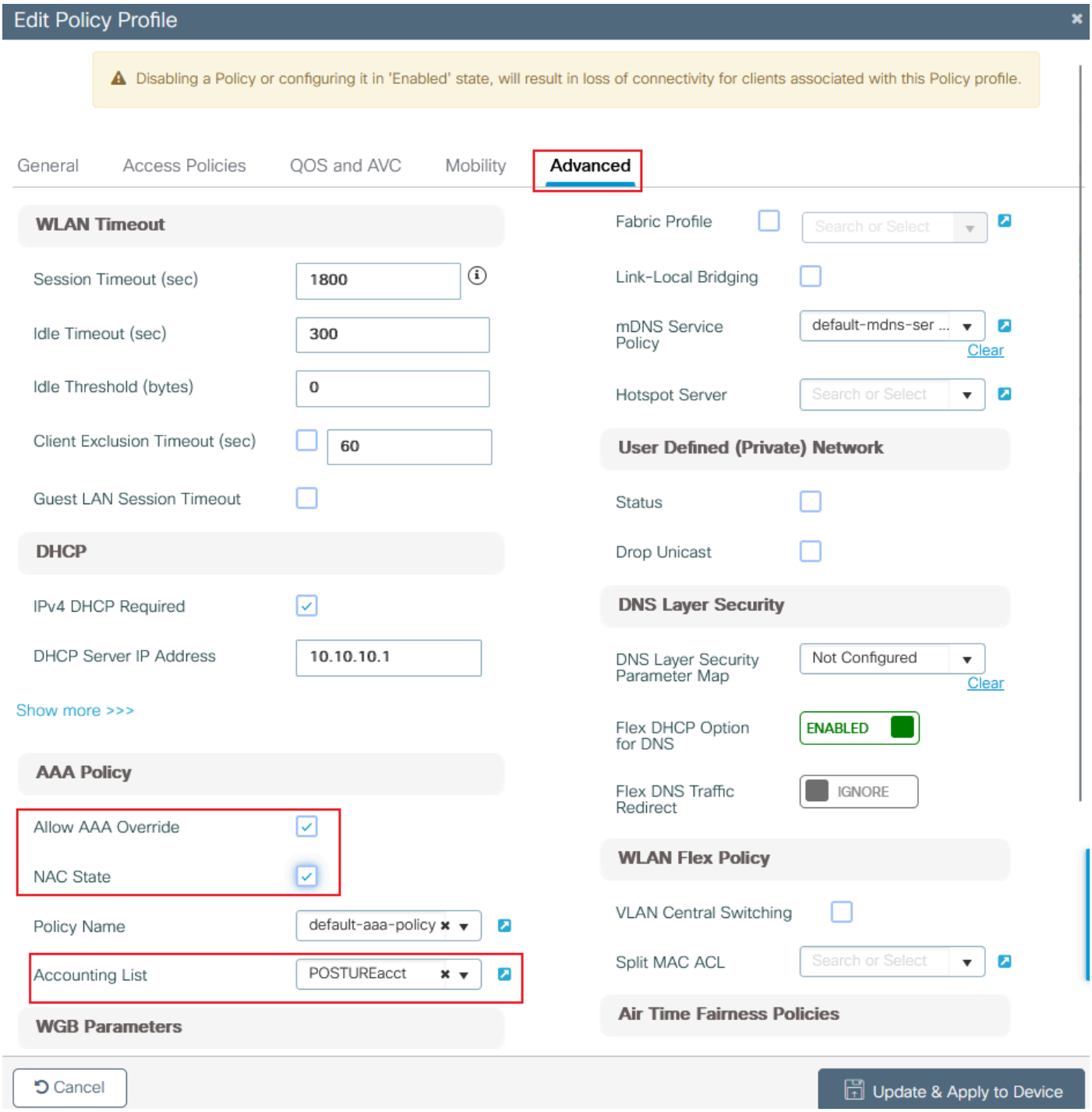
步驟2.選擇VLAN。導覽至Access Policies索引標籤，並從下拉選單中選擇VLAN名稱或手動輸入

VLAN-ID。請勿在原則設定檔中設定ACL:



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：

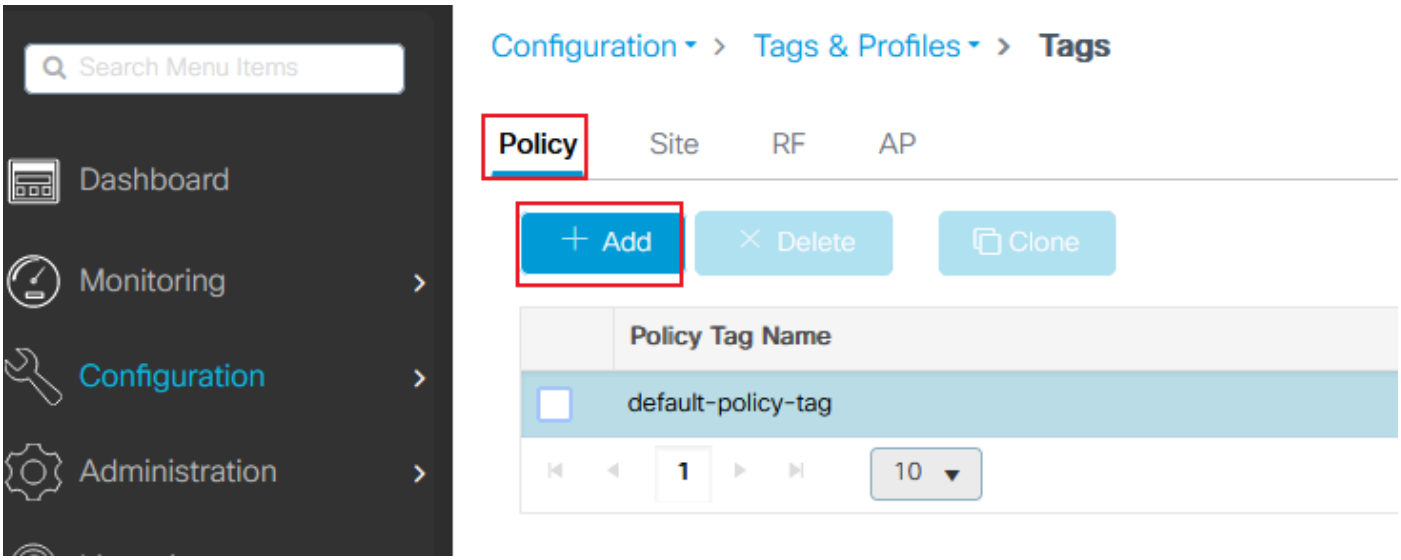


9800建立策略配置檔案高級版

原則標籤組態

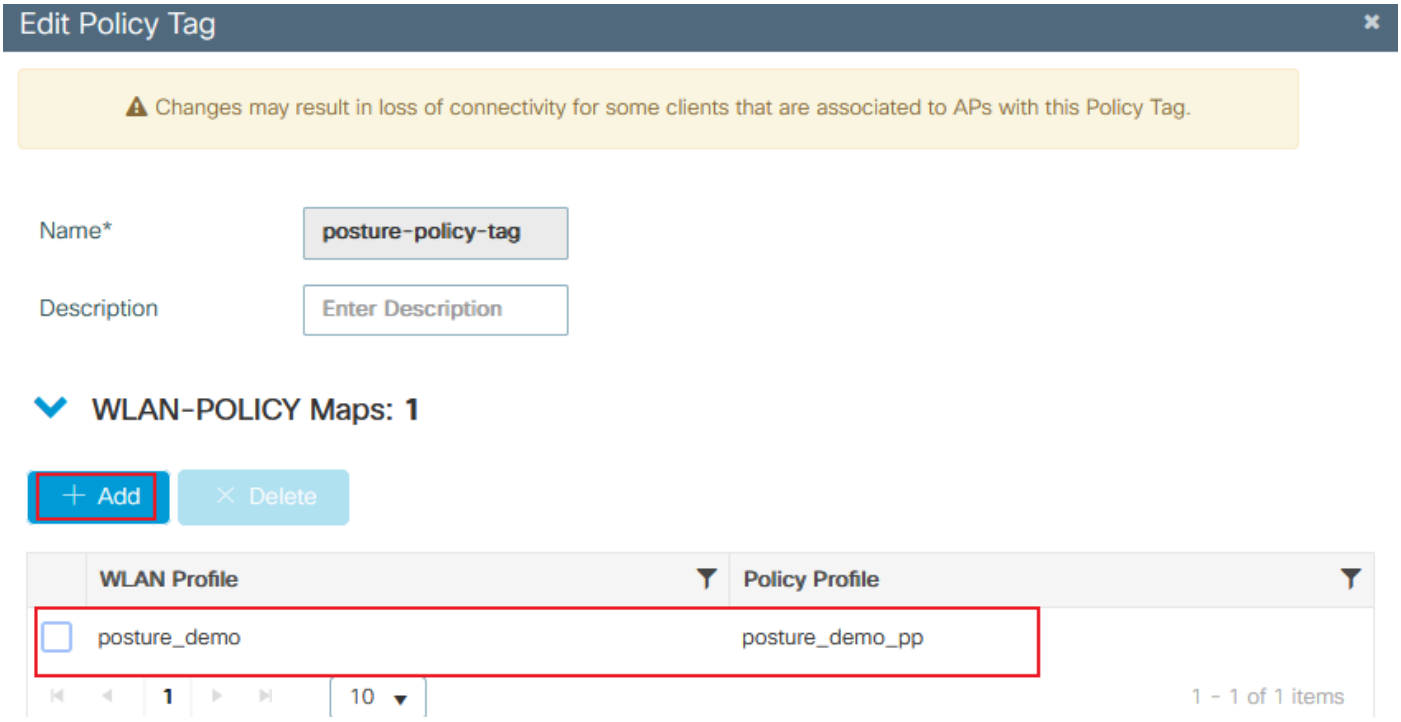
在原則標籤內，您可以將 SSID 與原則設定檔連結。您可以建立新的原則標籤，或使用 default-policy-tag。

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



9800策略標籤新增

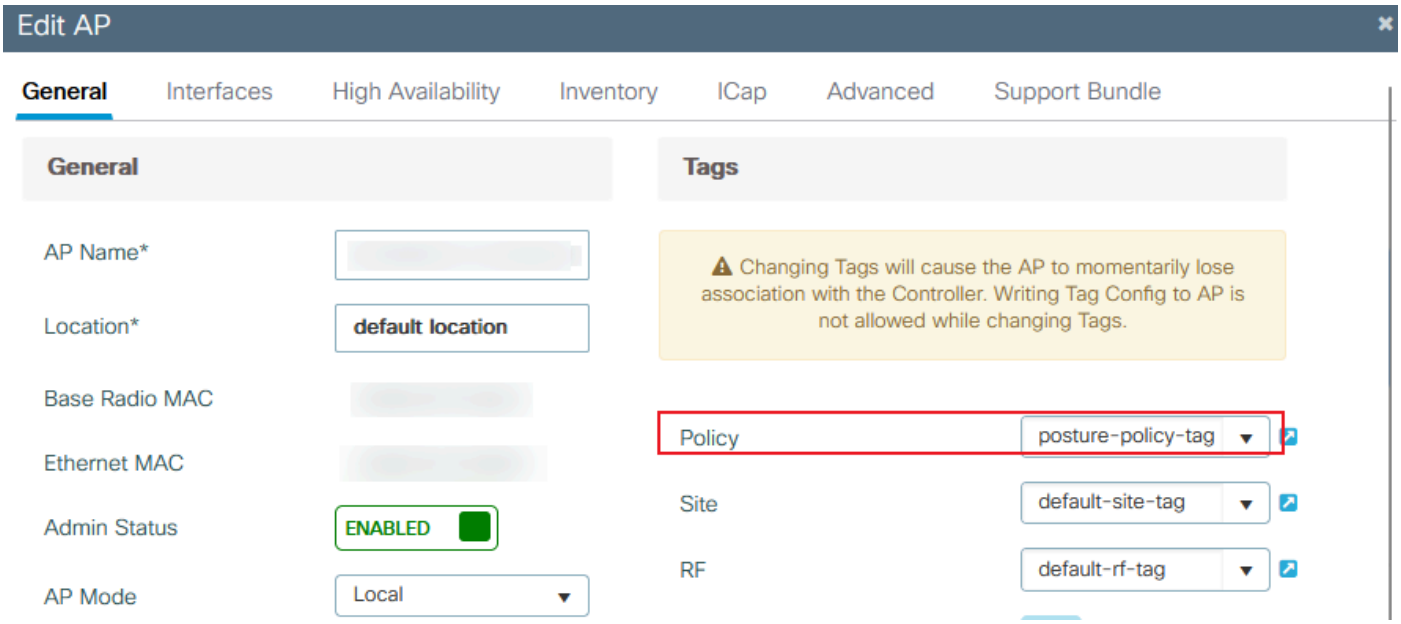
將您的WLAN簡檔連結到所需的策略簡檔：



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。



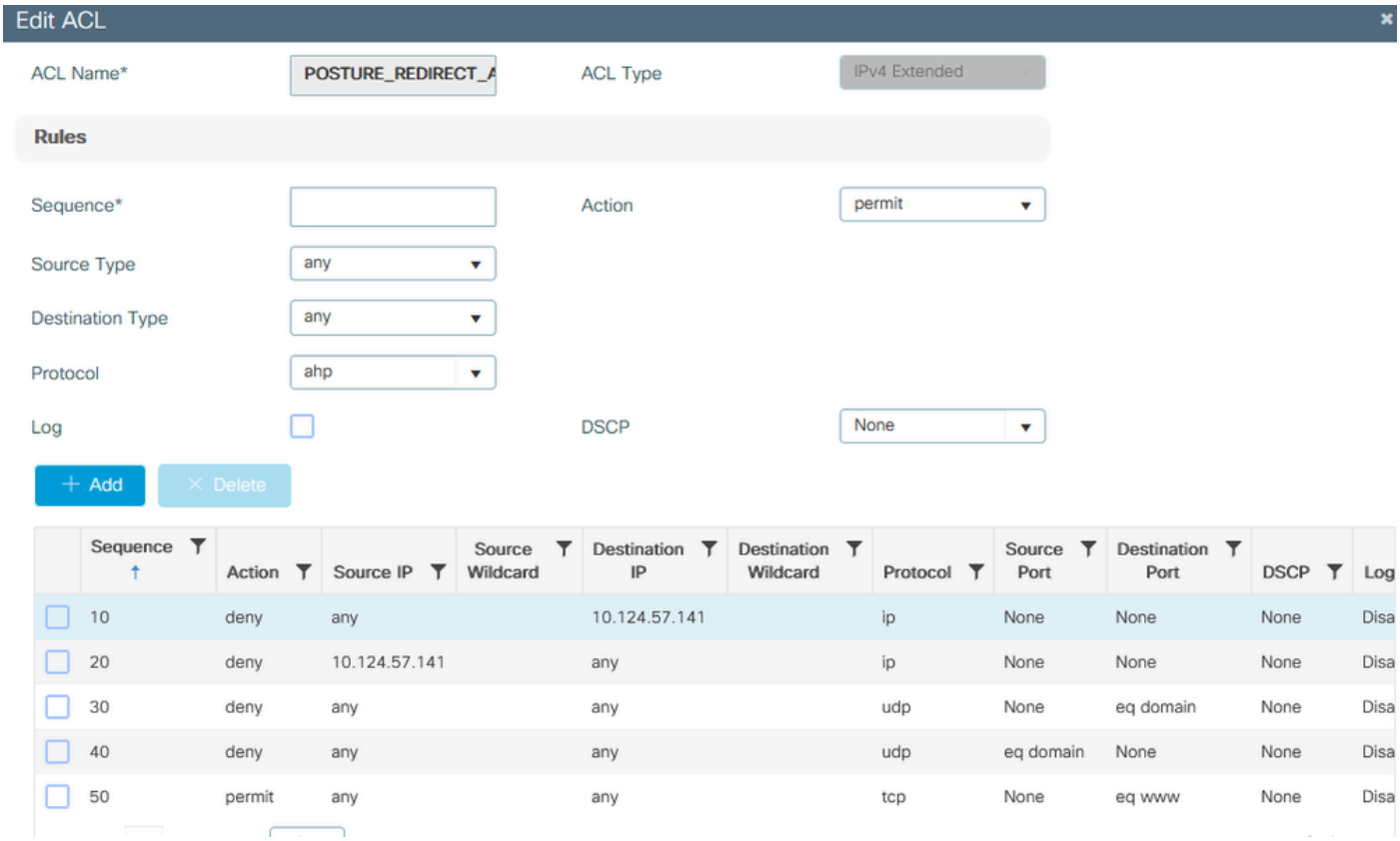
9800策略標籤分配

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。

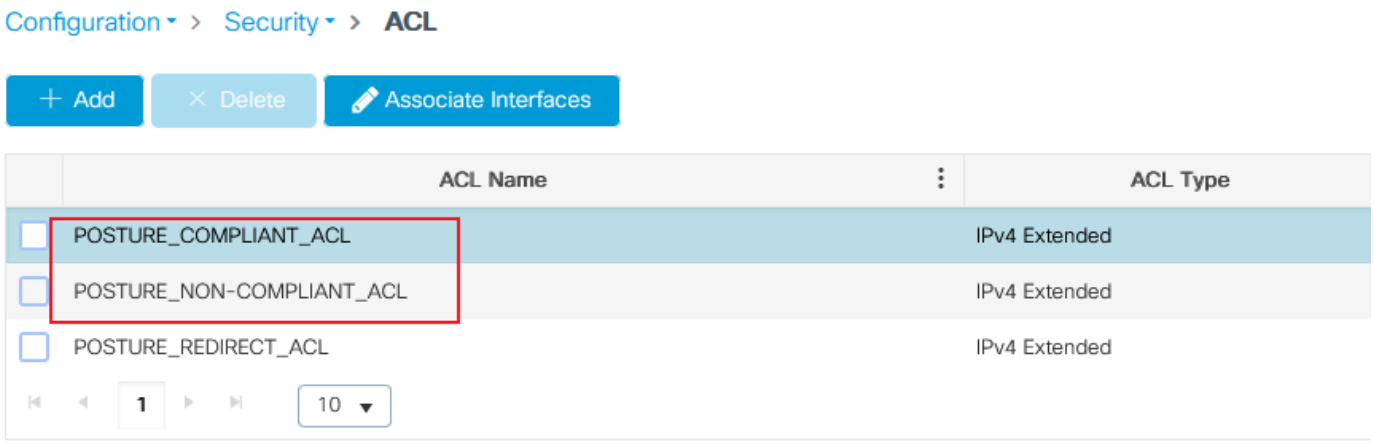
您需要拒絕流向 ISE PSN 節點的流量，並拒絕 DNS 和允許所有其他流量。此重新導向ACL不是安全ACL，而是雙向ACL，定義哪些流量會進入CPU（在允許的情況下）進行進一步處理（例如重新導向）以及哪些流量會停留在資料平面上（在拒絕時）並避免重新導向。ACL必須如下所示（在本例中用您的ISE IP地址替換10.124.57.141）：



9800重新導向ACL詳細資訊

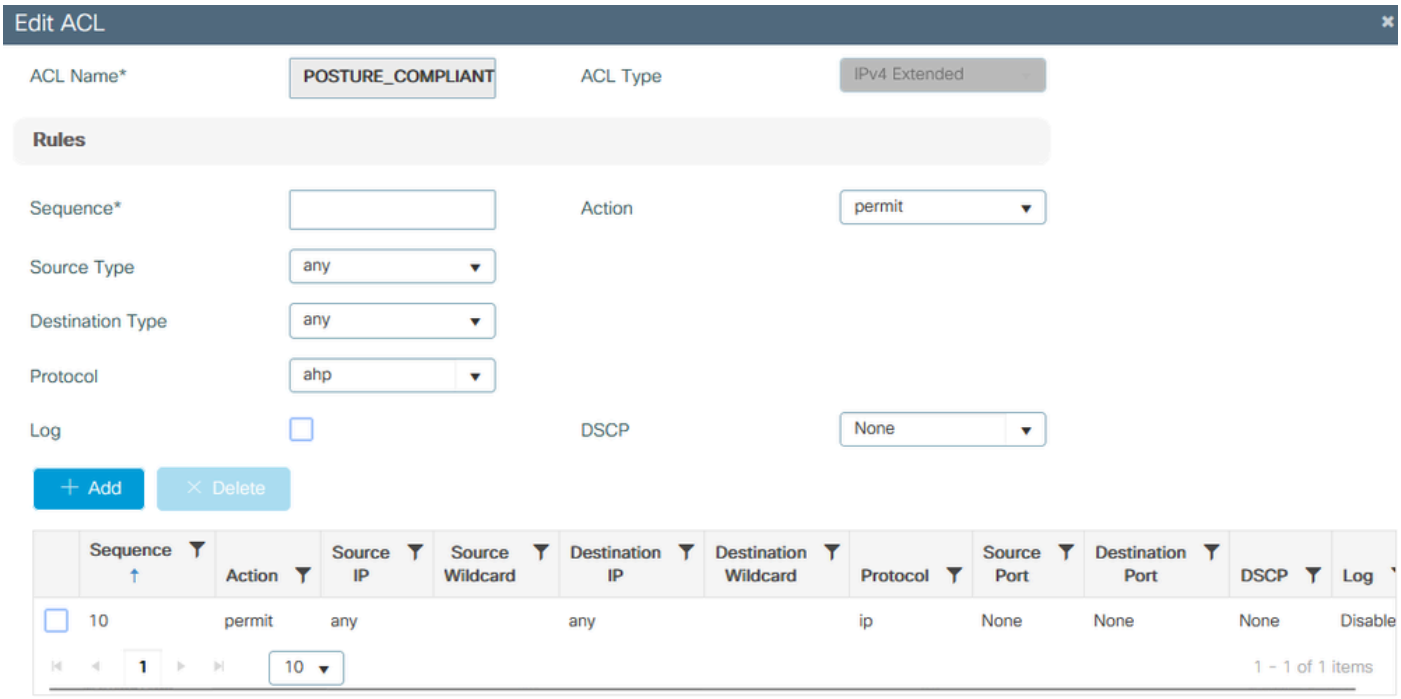
策略ACL配置

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。



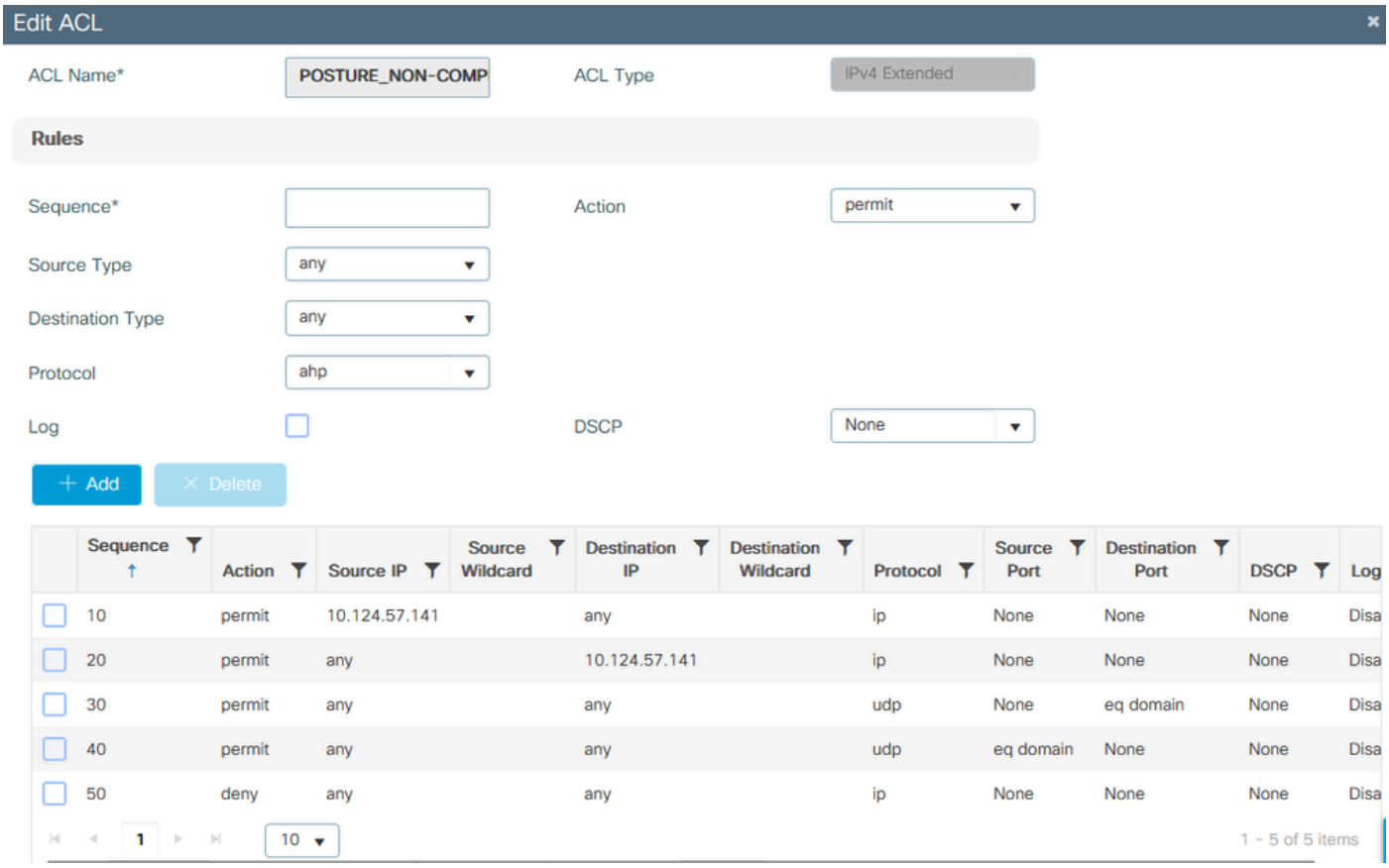
9800 ACL一般資訊

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：



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）：



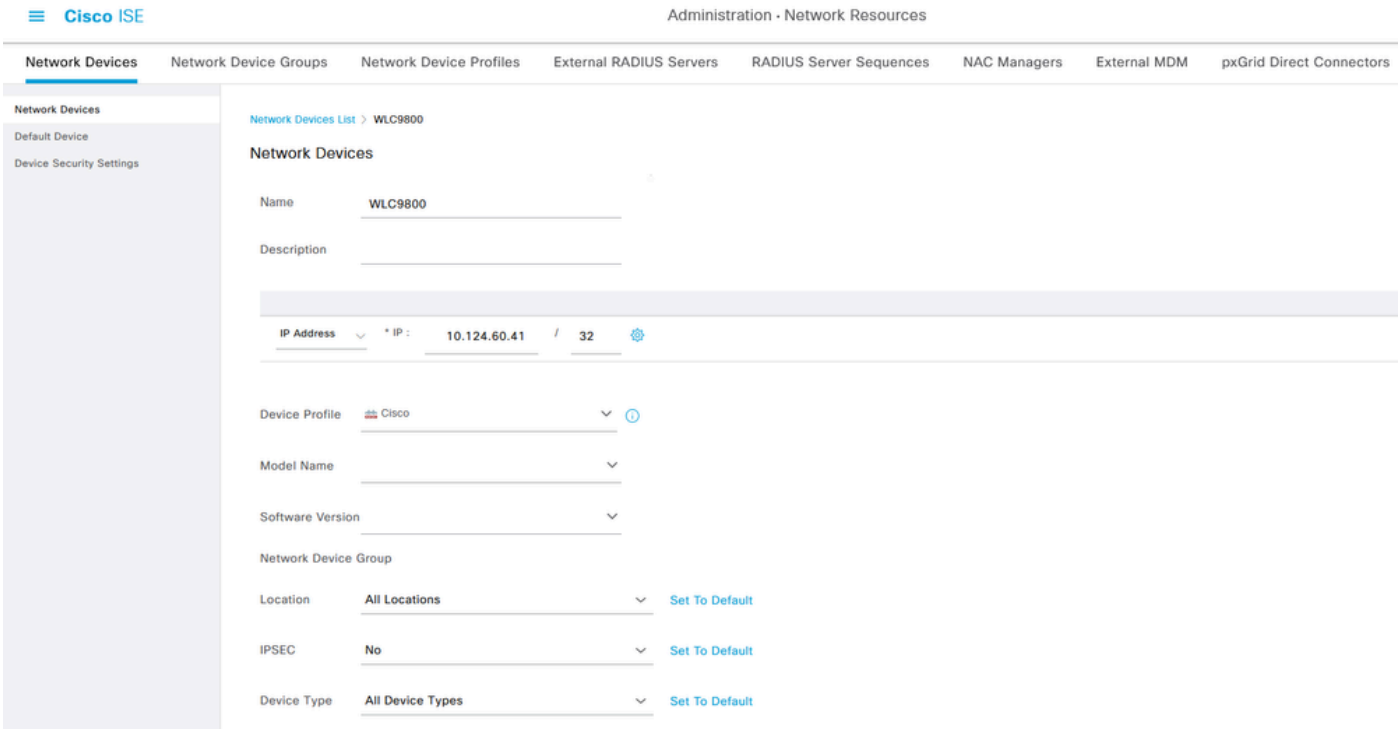
9800 ACL — 不符合要求

ISE上的AAA配置和狀態設定

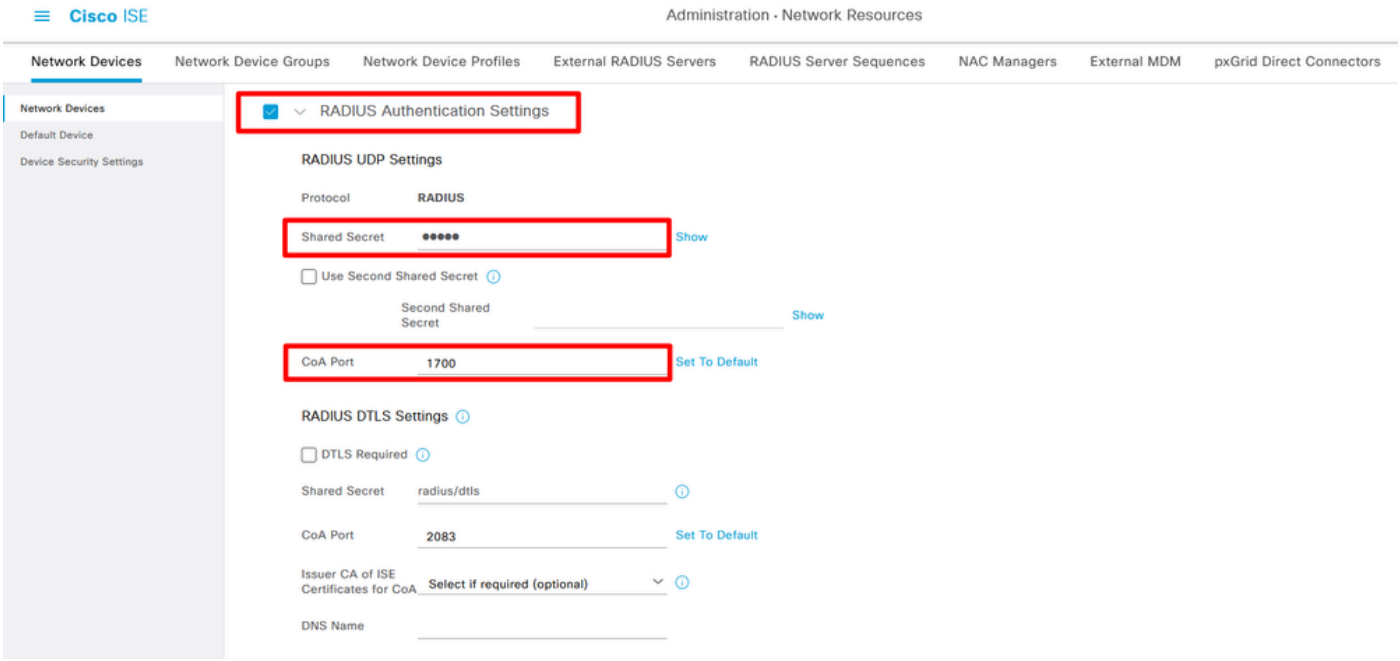
安全狀態要求：在本示例中，確定符合性的要求是檢測用於測試Windows PC的案頭上是否存在特

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:



新增網路裝置01



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:

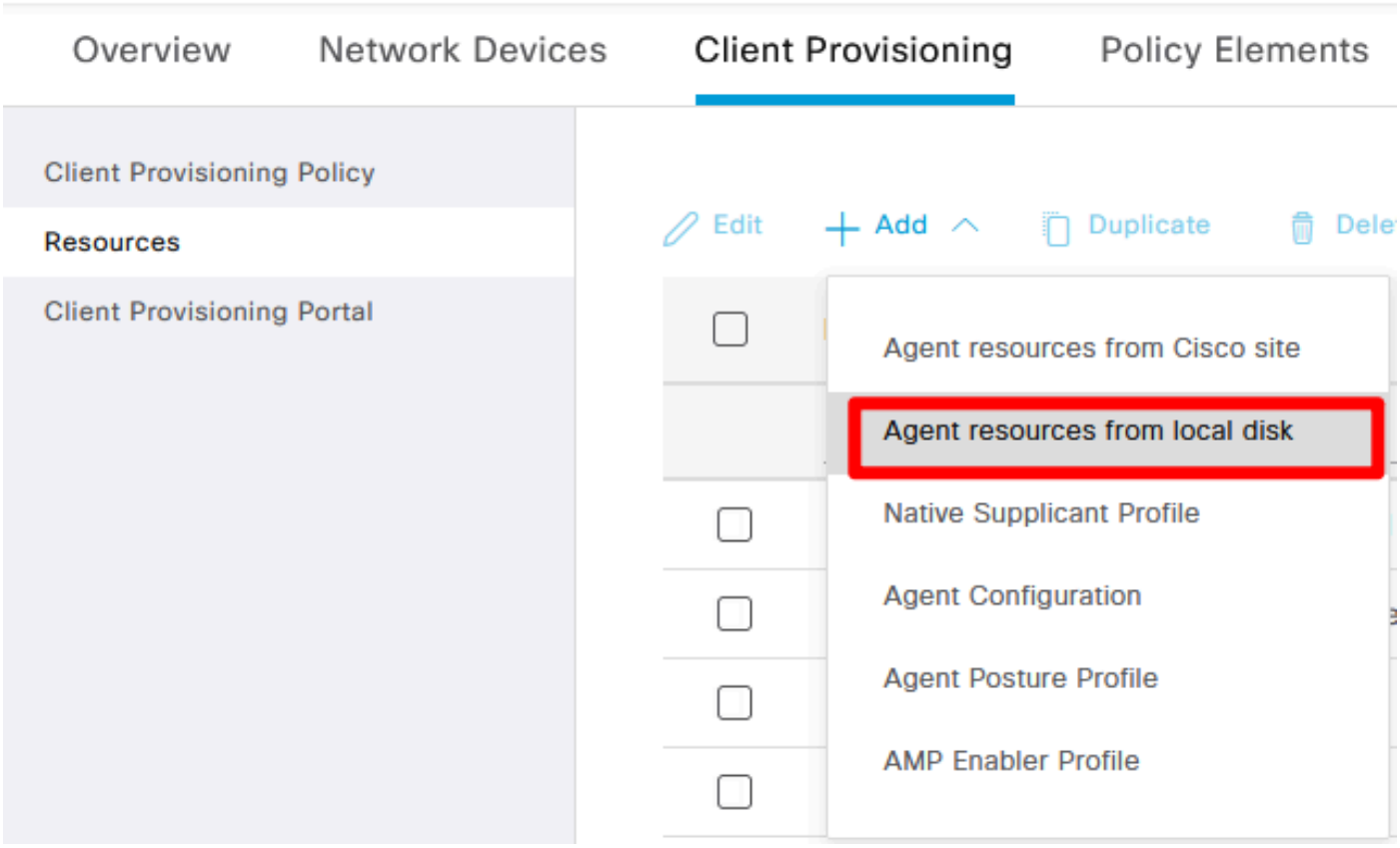
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB

安全使用者端5.1.2.42

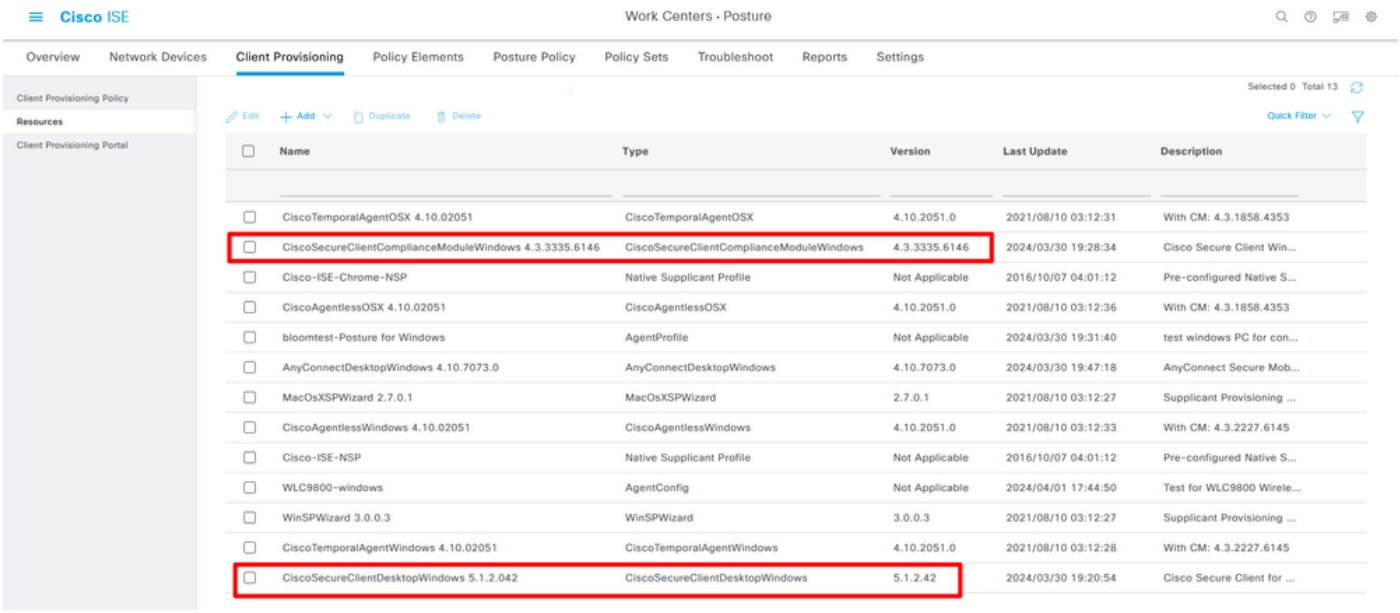
ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later. cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg Advisories	30-Jan-2023	19.59 MB

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:

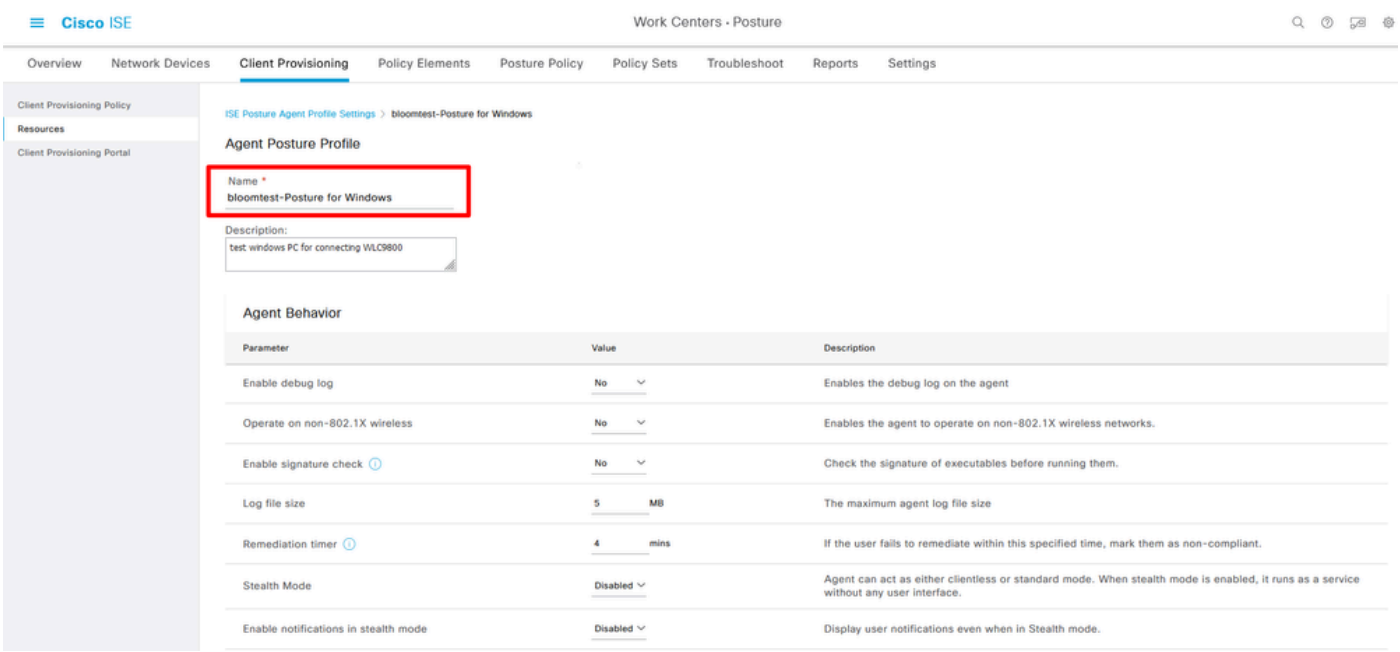


上傳安全客戶端



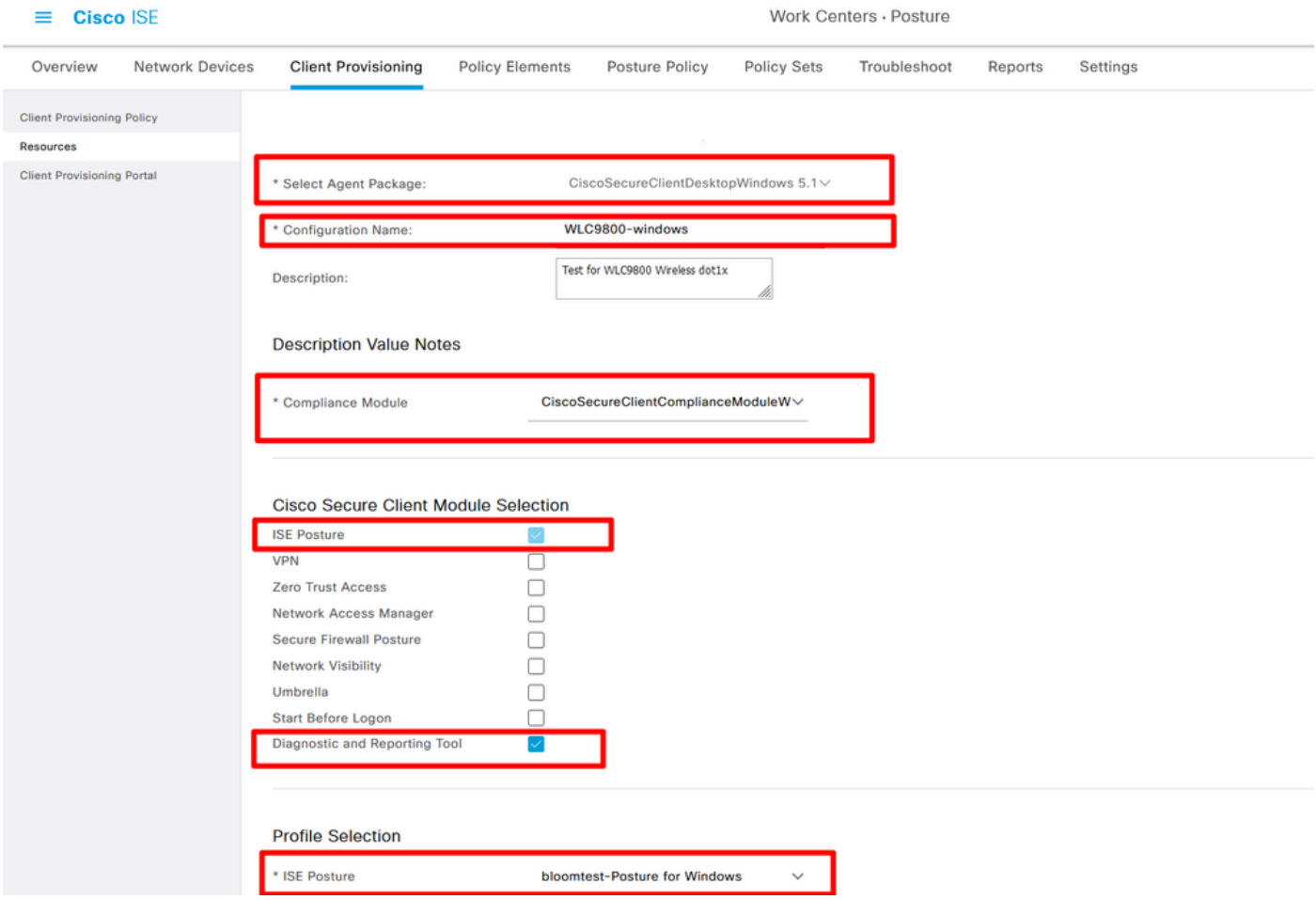
成功上傳安全客戶端和合規性模組

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:



代理狀態配置檔案

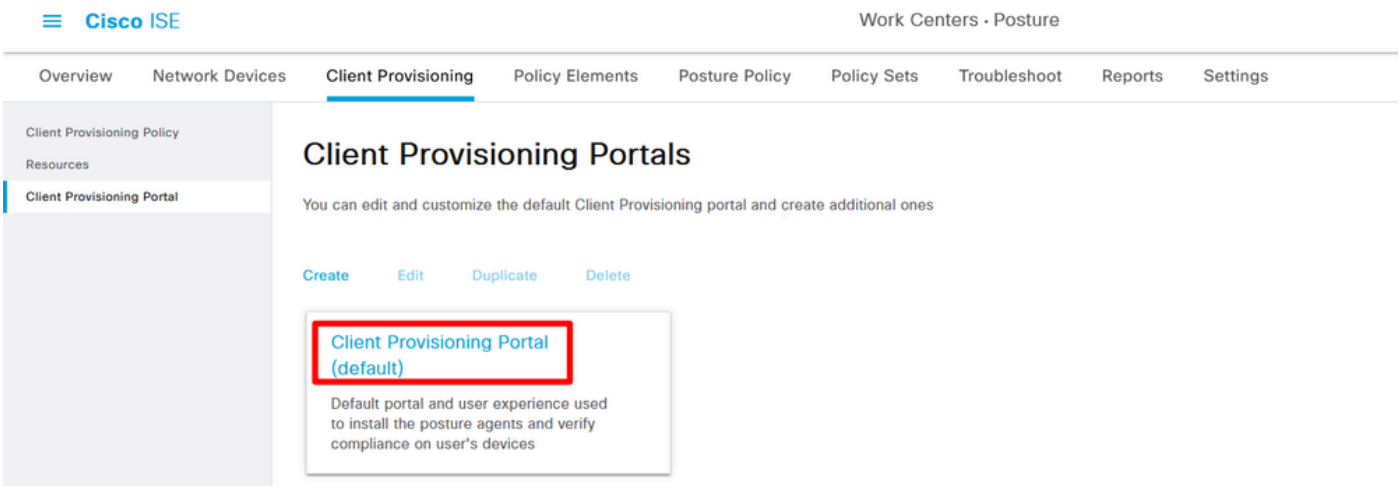
步驟5.建立代理配置導航到工作中心>狀態>客戶端調配>資源>新增>代理配置:



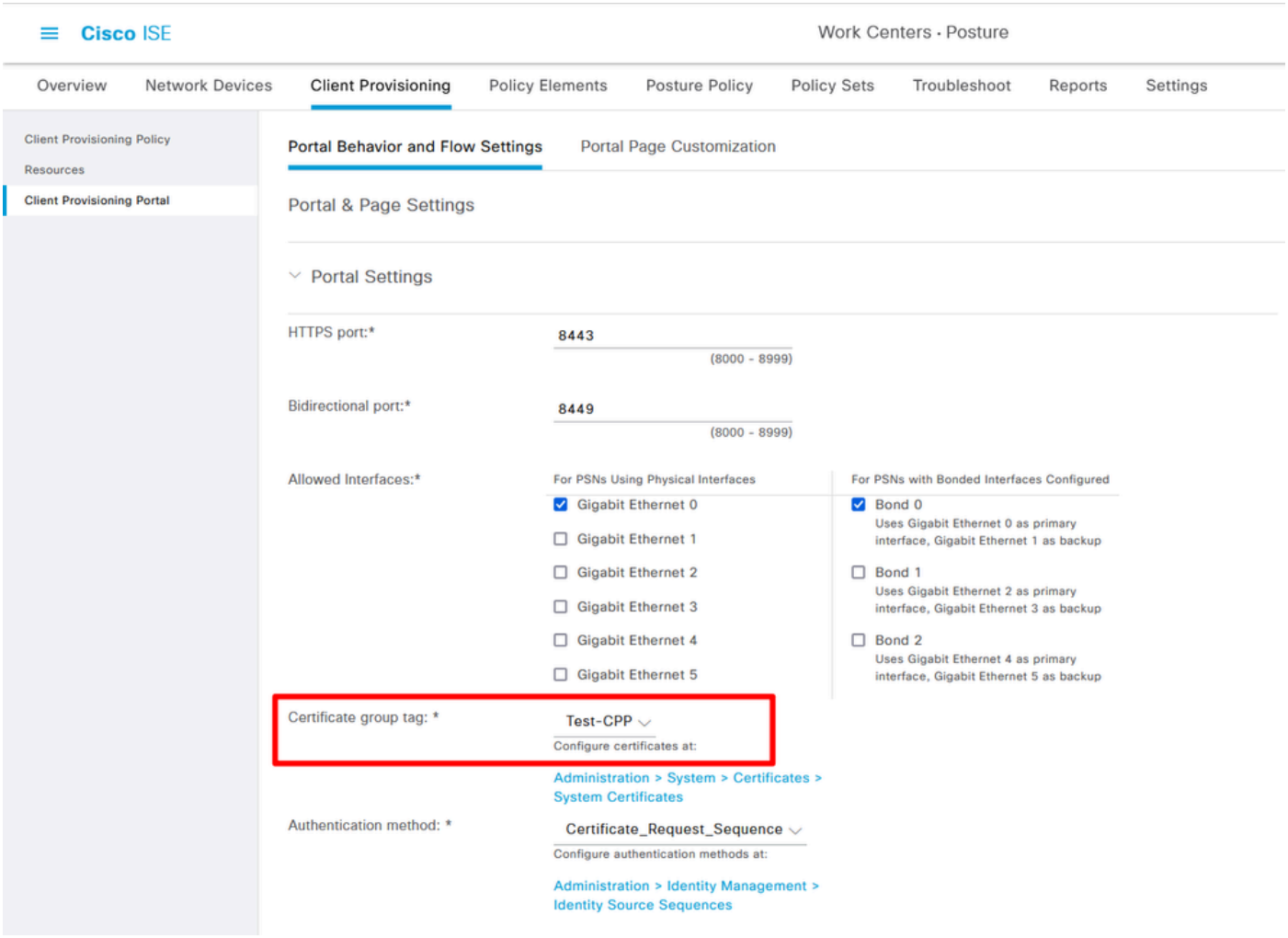
新增代理配置

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:

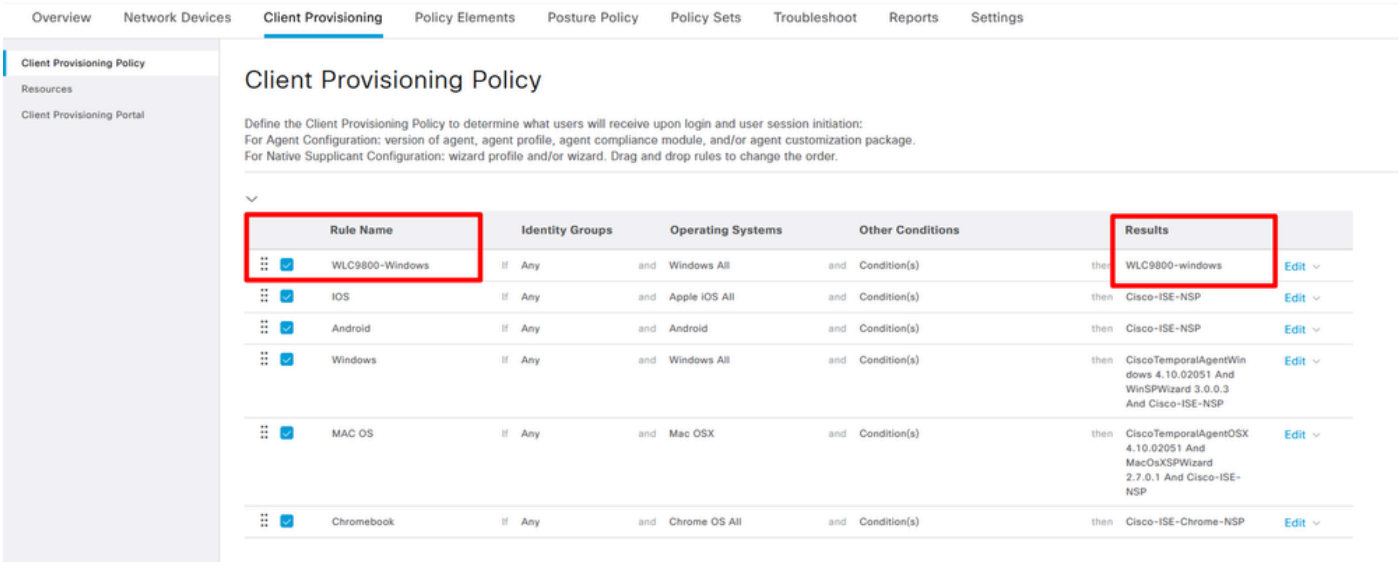


選擇客戶端調配門戶01



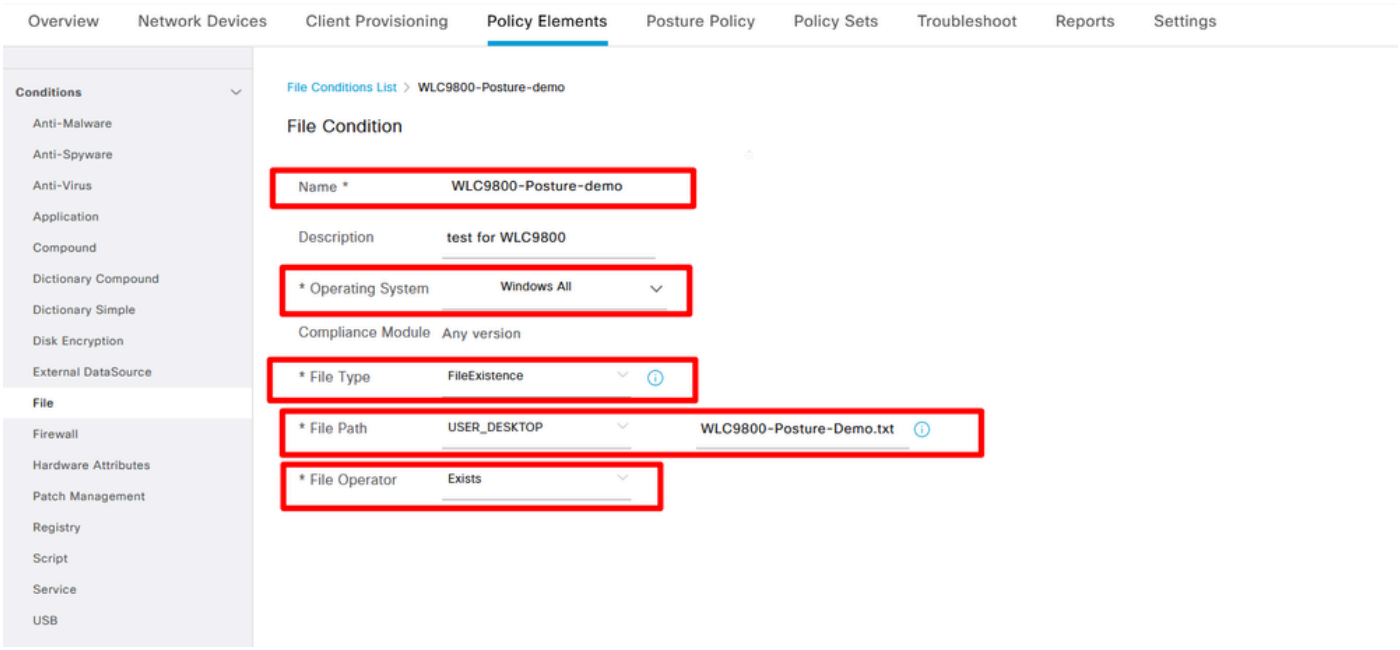
選擇客戶端調配門戶02

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。



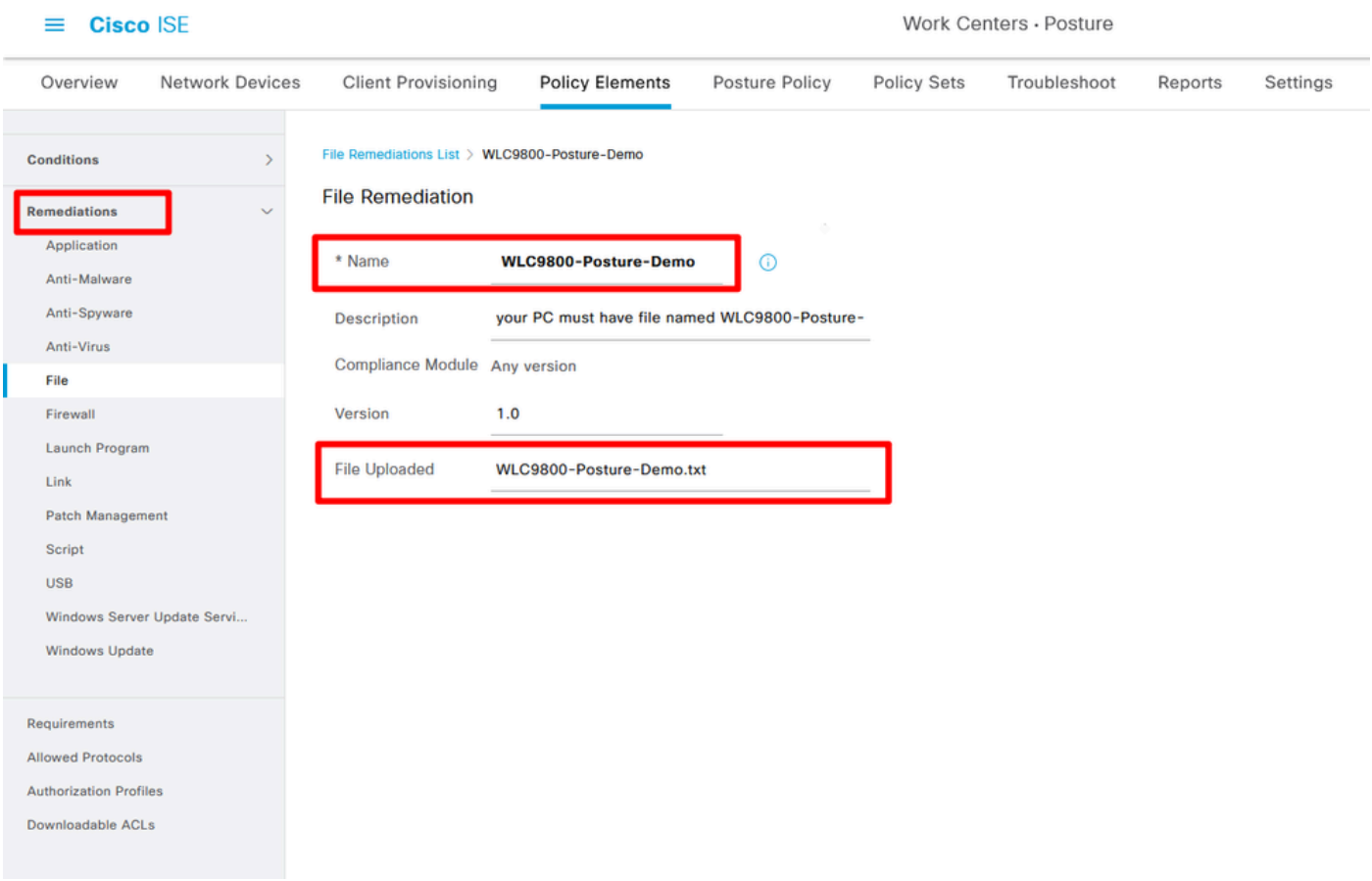
建立客戶端調配策略

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:



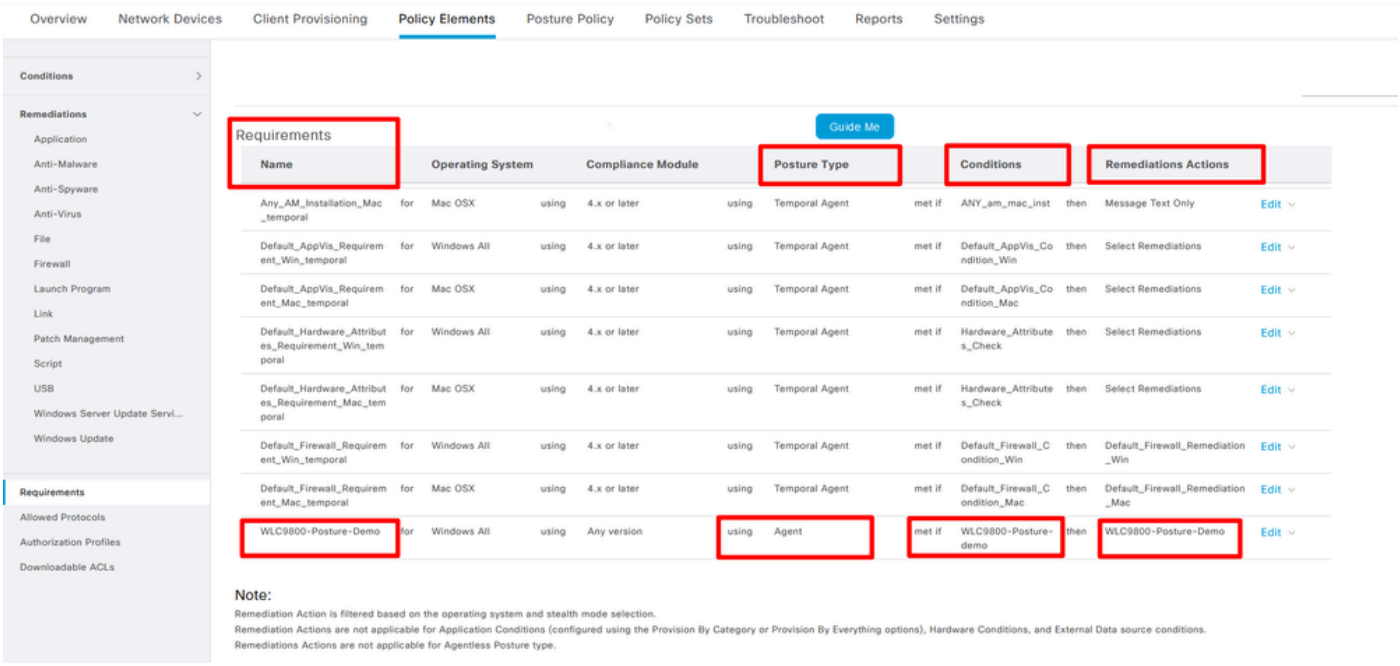
建立檔案條件

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:



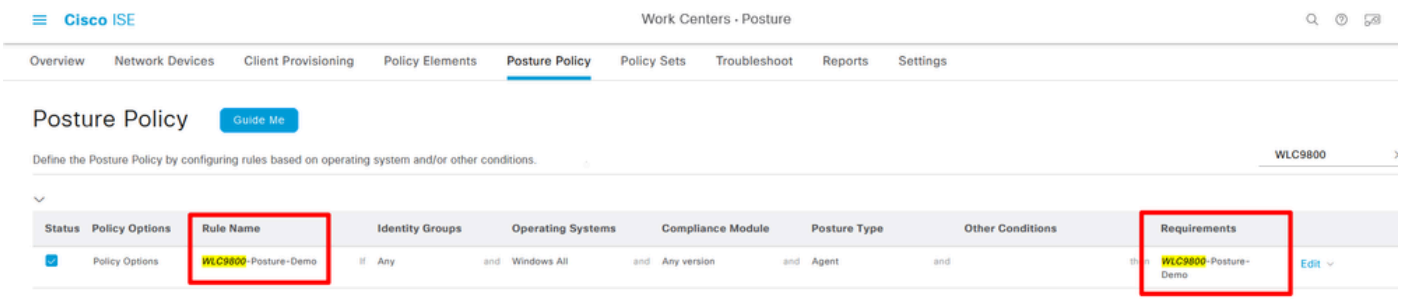
建立檔案補救

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:



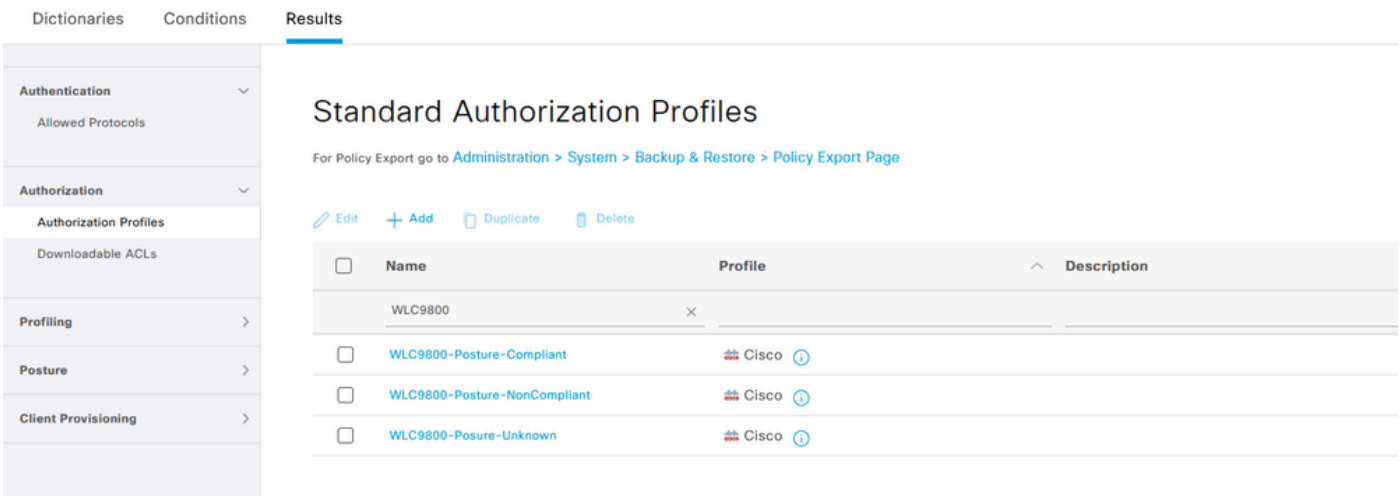
建立狀態要求

步驟11.建立狀態策略。導航到工作中心>狀態>插入新策略:

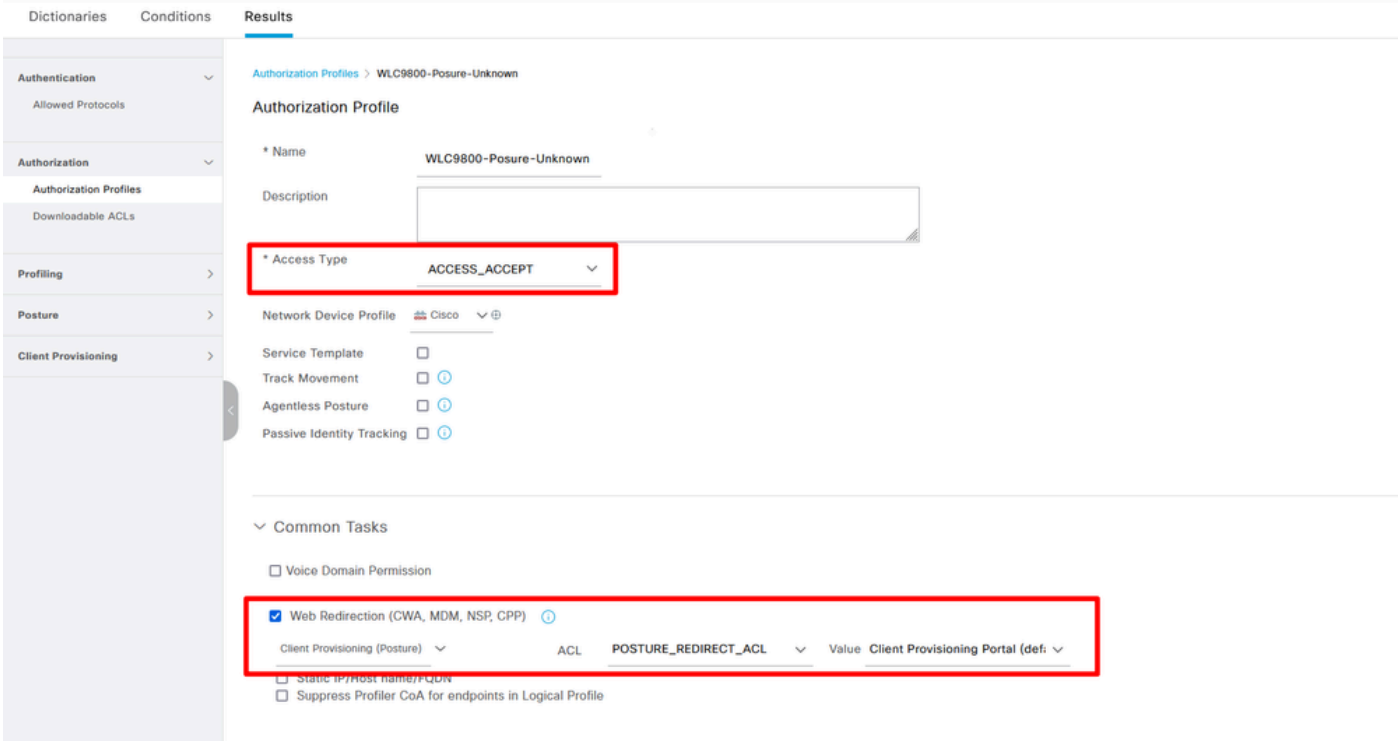


建立狀態策略

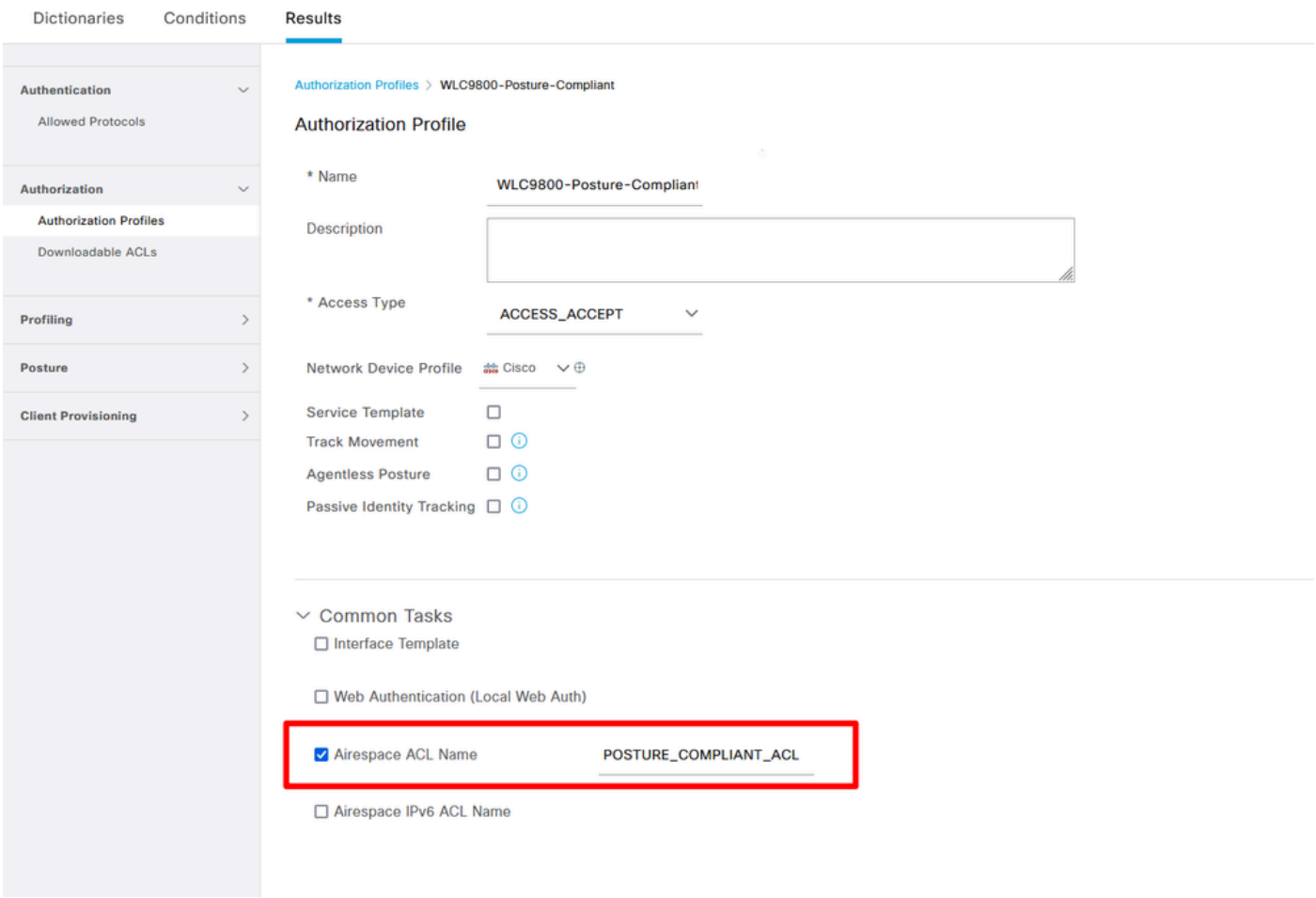
步驟12.建立三個授權配置檔案：狀態未知；安全評估狀態為「不符合」；安全評估狀態是符合的。導航到Policy> Policy Elements> Results> Authorization> Authorization Profiles> Add:



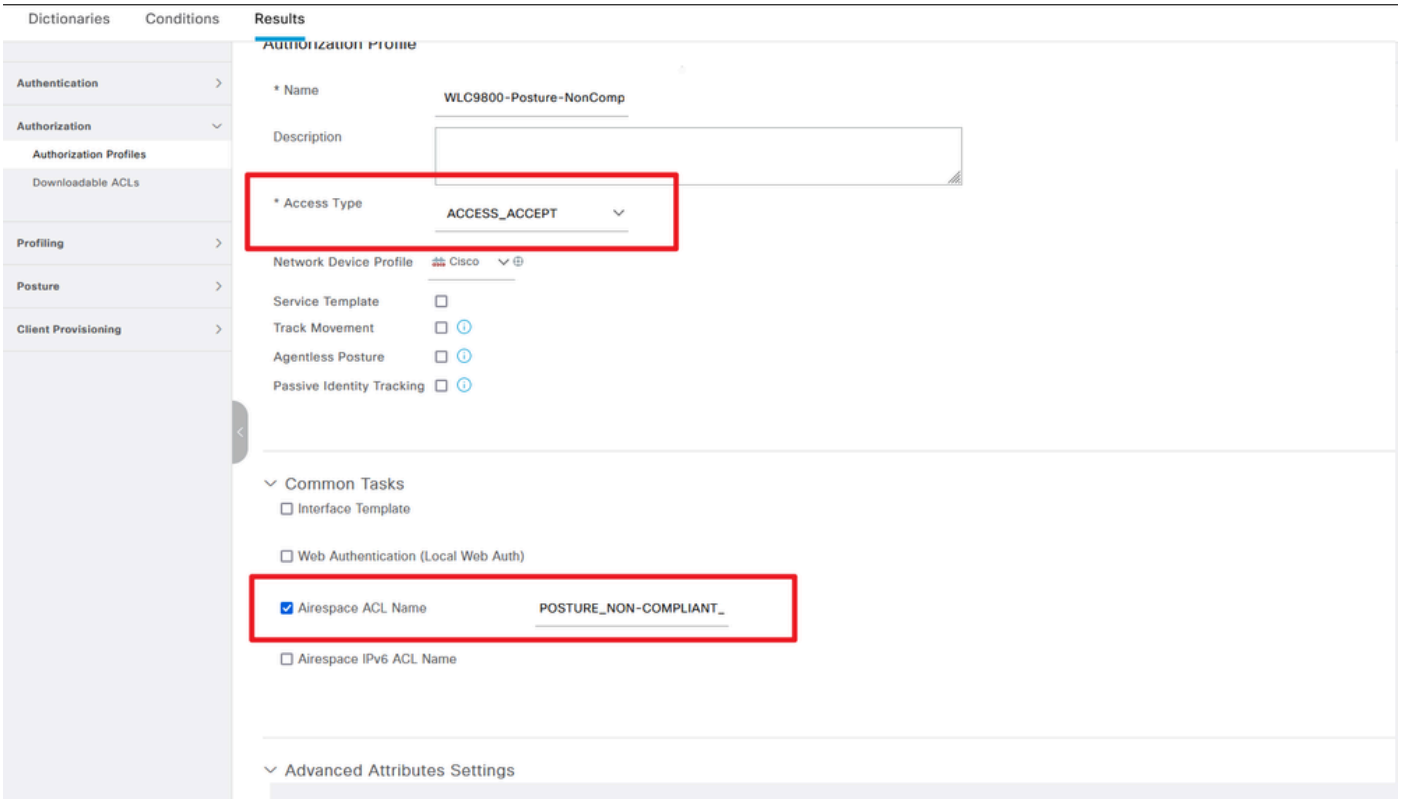
建立授權配置檔案01



建立授權配置檔案02



建立授權配置檔案03

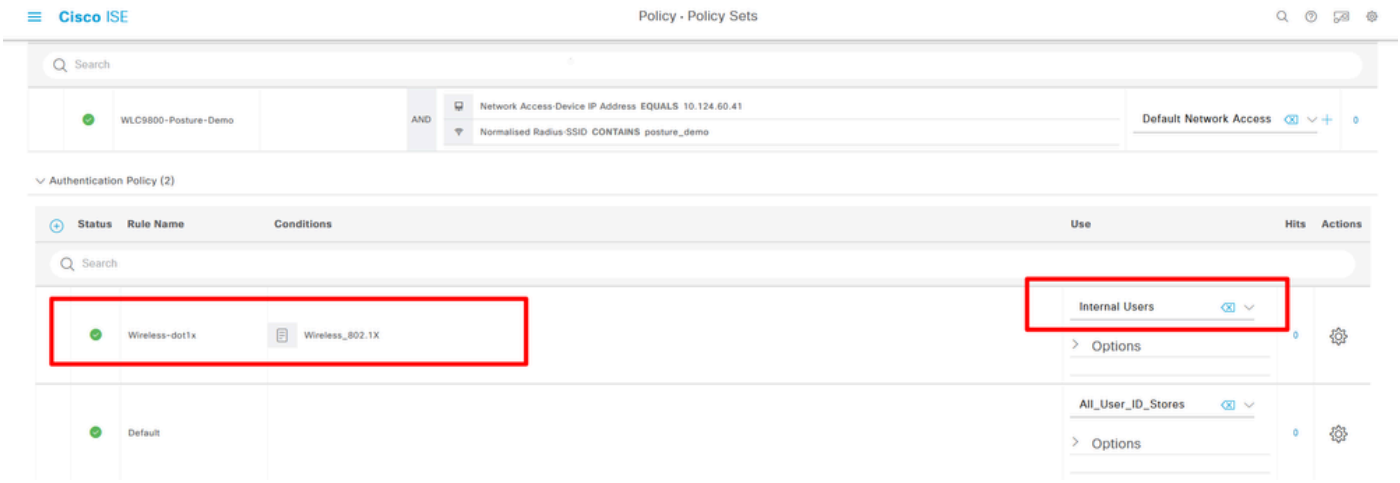


步驟13.建立策略集。導覽至Policy> Policy

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:



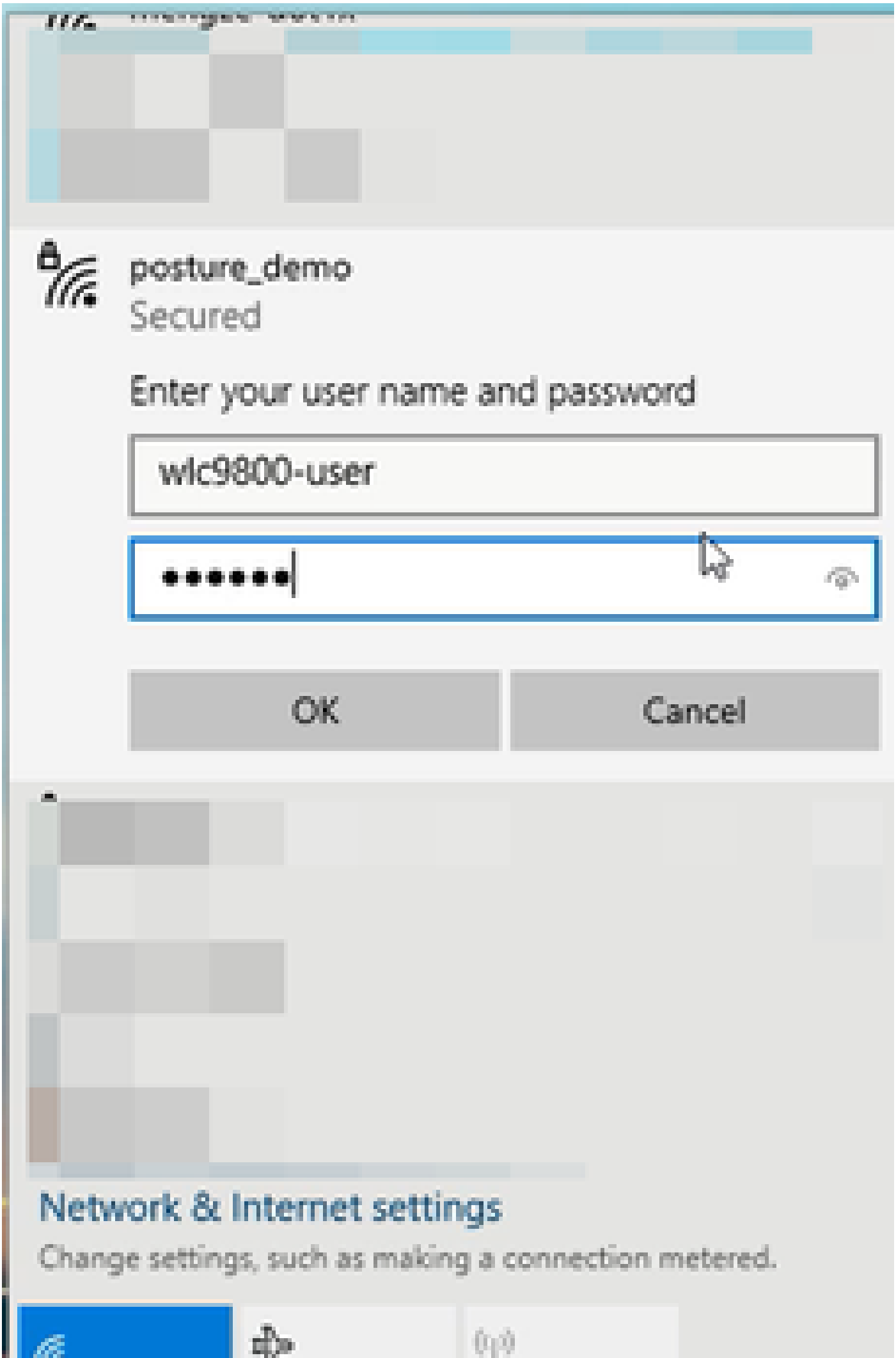
建立身份驗證策略

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

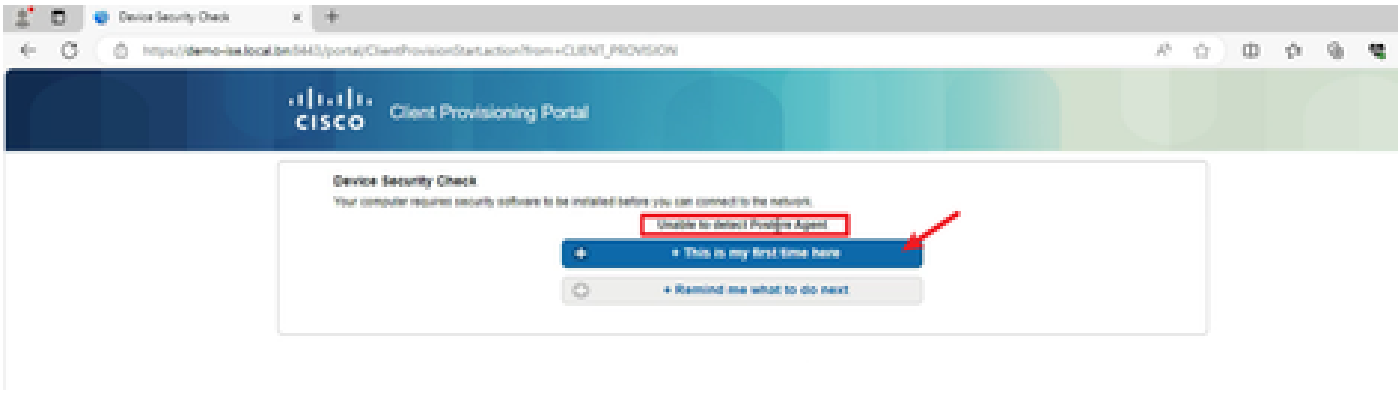
建立授權策略

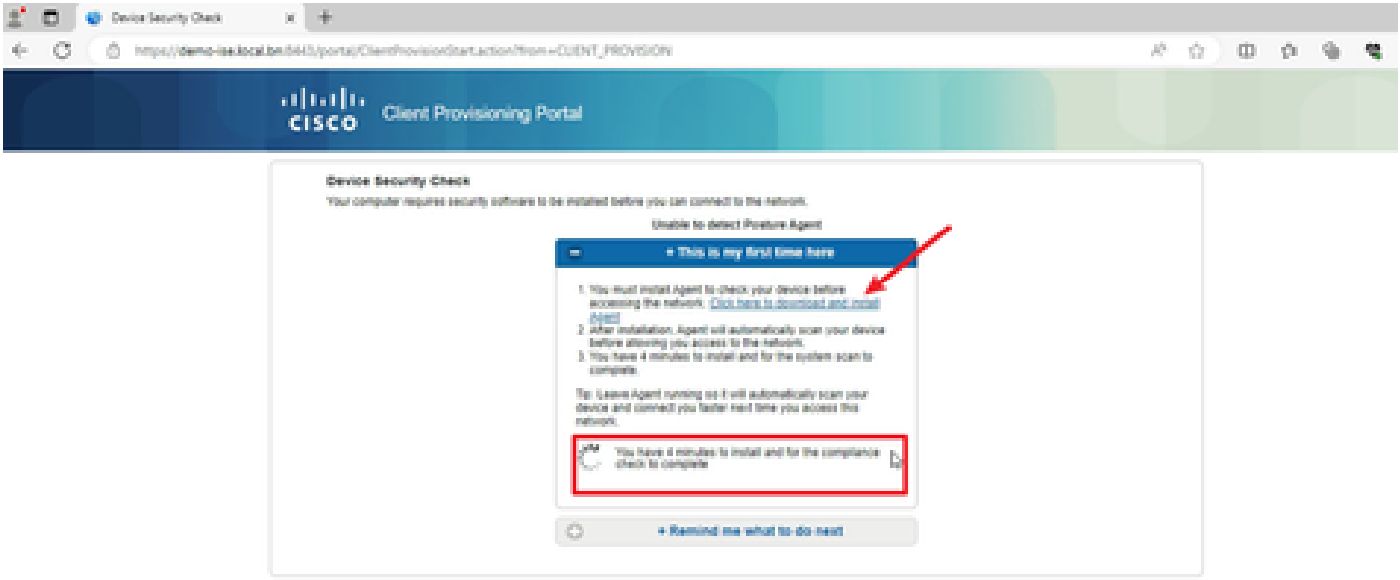
範例

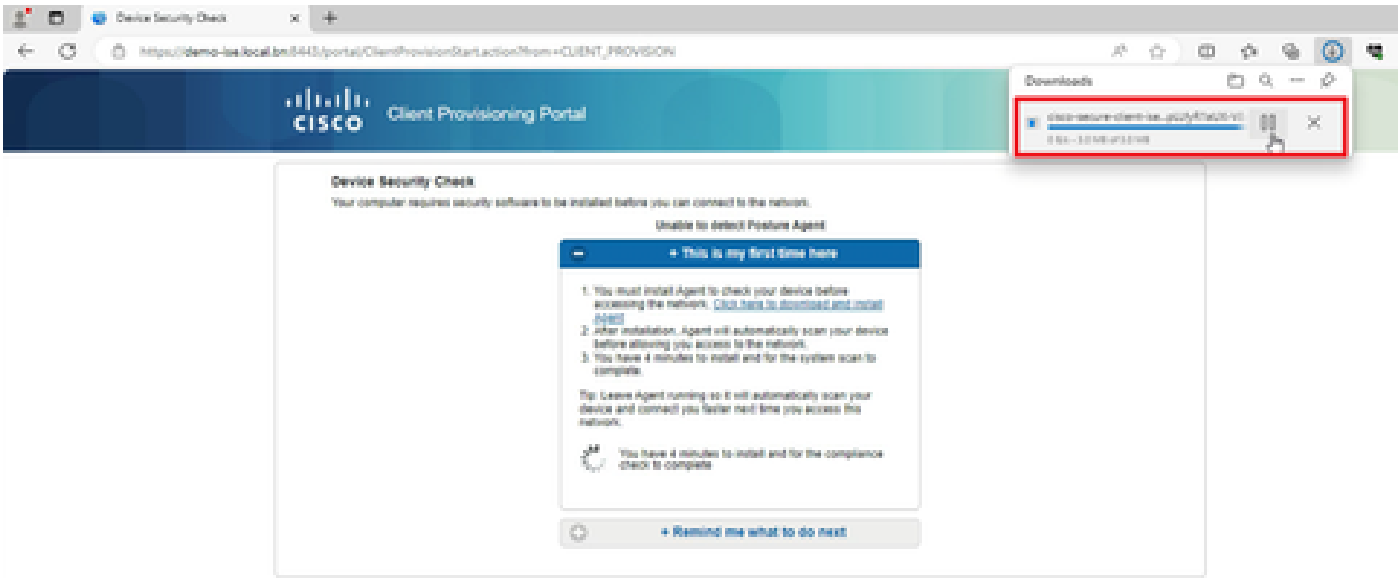
1.使用正確的802.1X憑證連線的測試SSID posture_demo。

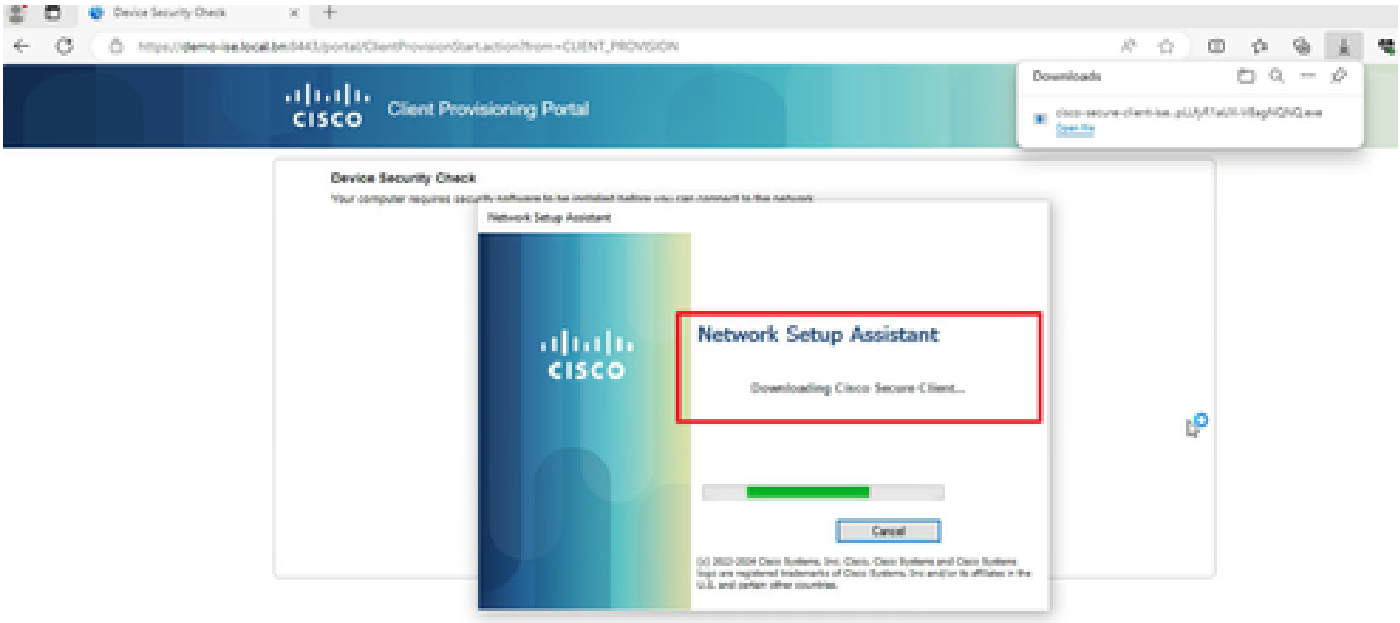

posture_demo
Secured
Enter your user name and password
wlc9800-user
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.

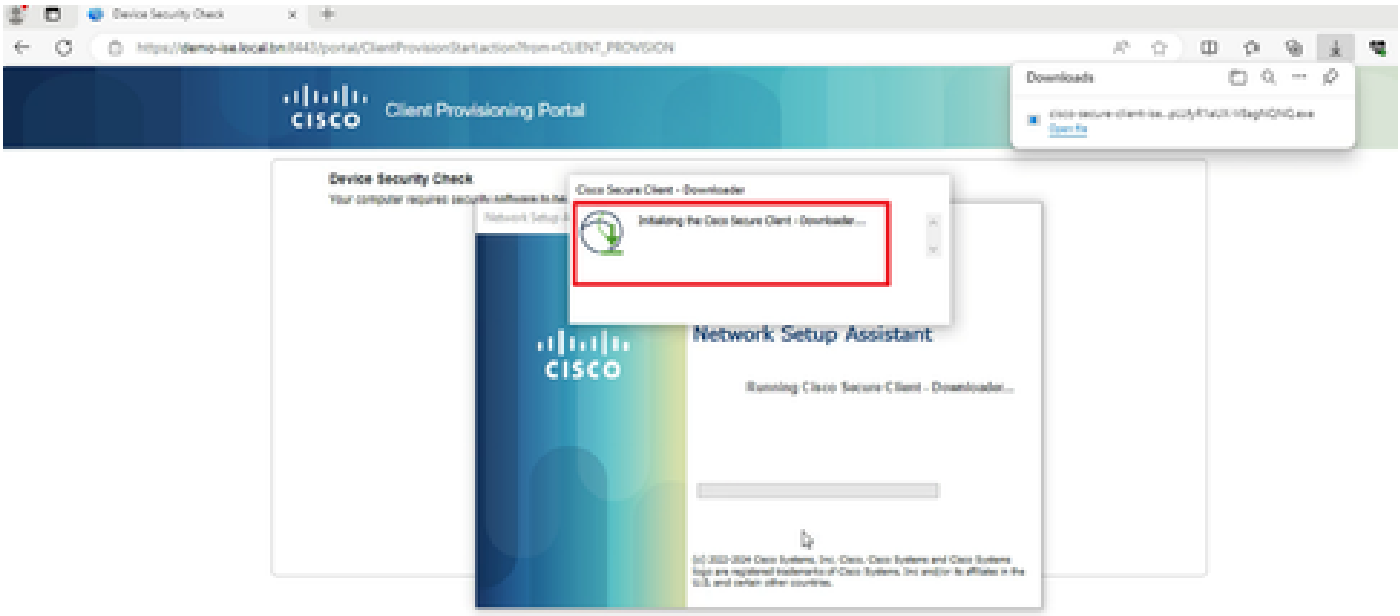
沒有安裝任何版本的終端安全評估代理，您可能會看到「無法檢測終端安全評估代理」的結果，請按一下這是我第一次在此處按一下。您需要下載並安裝代理。

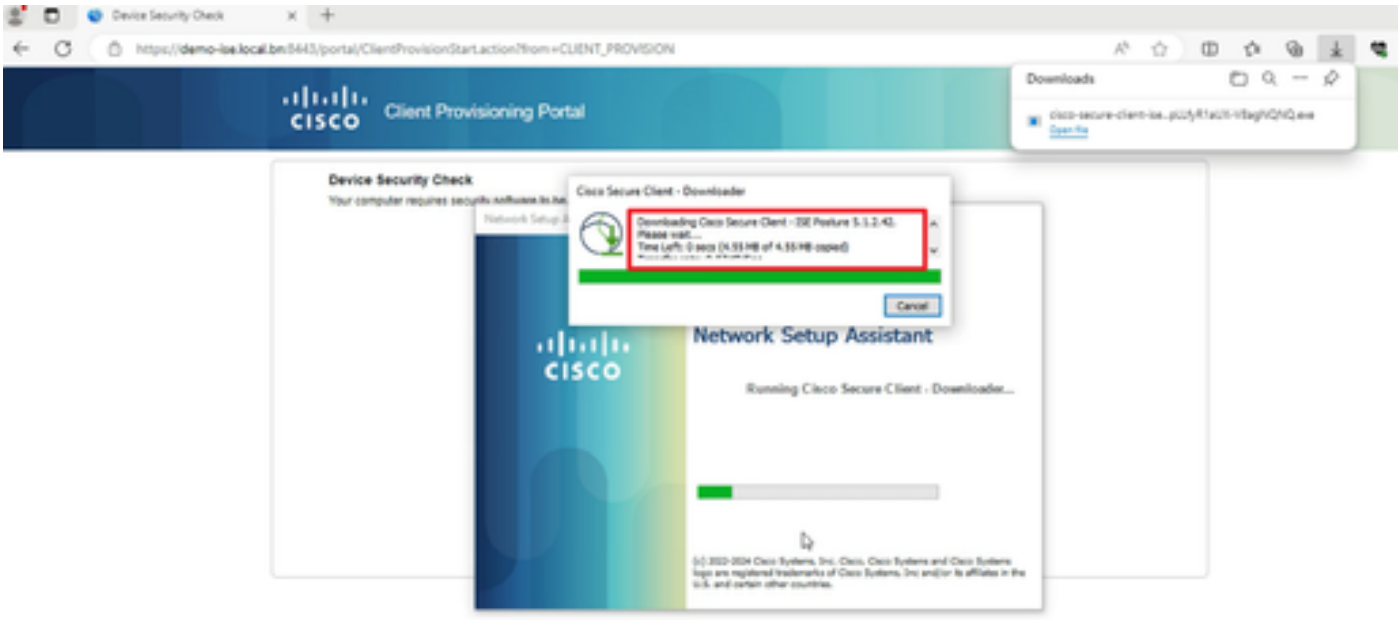


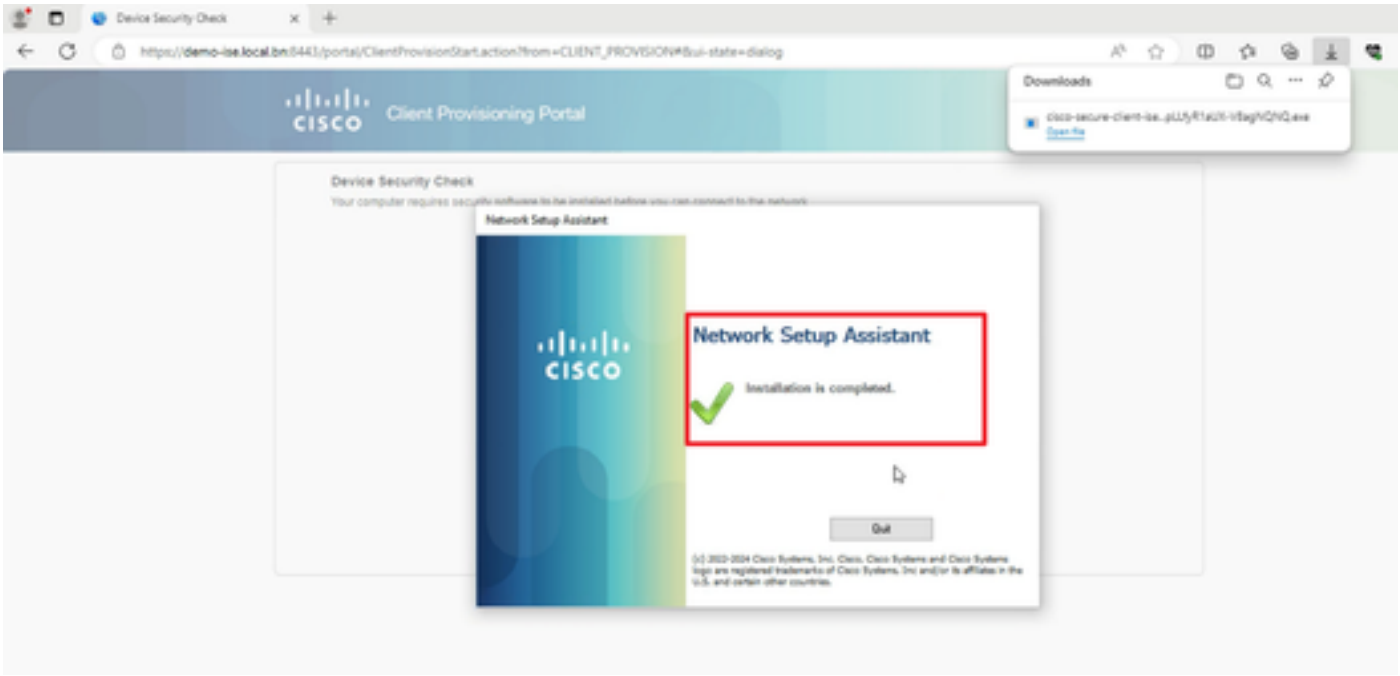




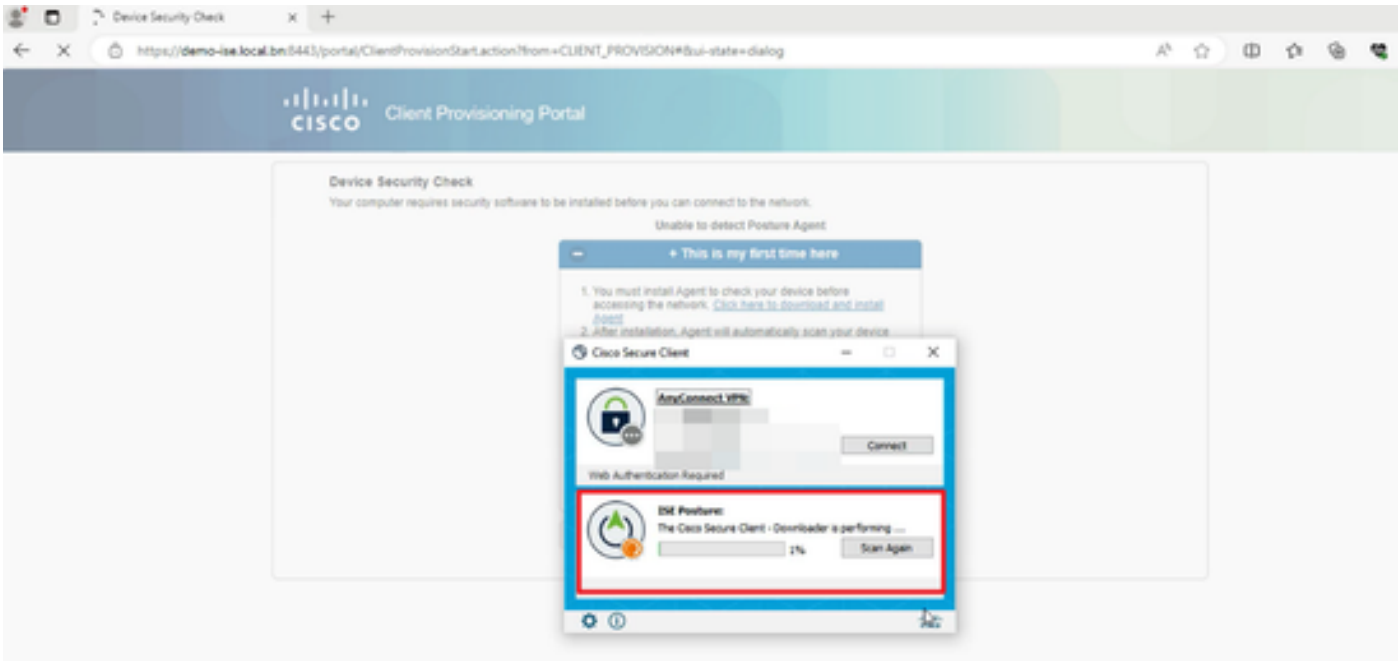

Client Provisioning Portal
Downloads
Device Security Check
Network Setup Assistant
Network Setup Assistant
Downloading Cisco Secure Client...
Cancel

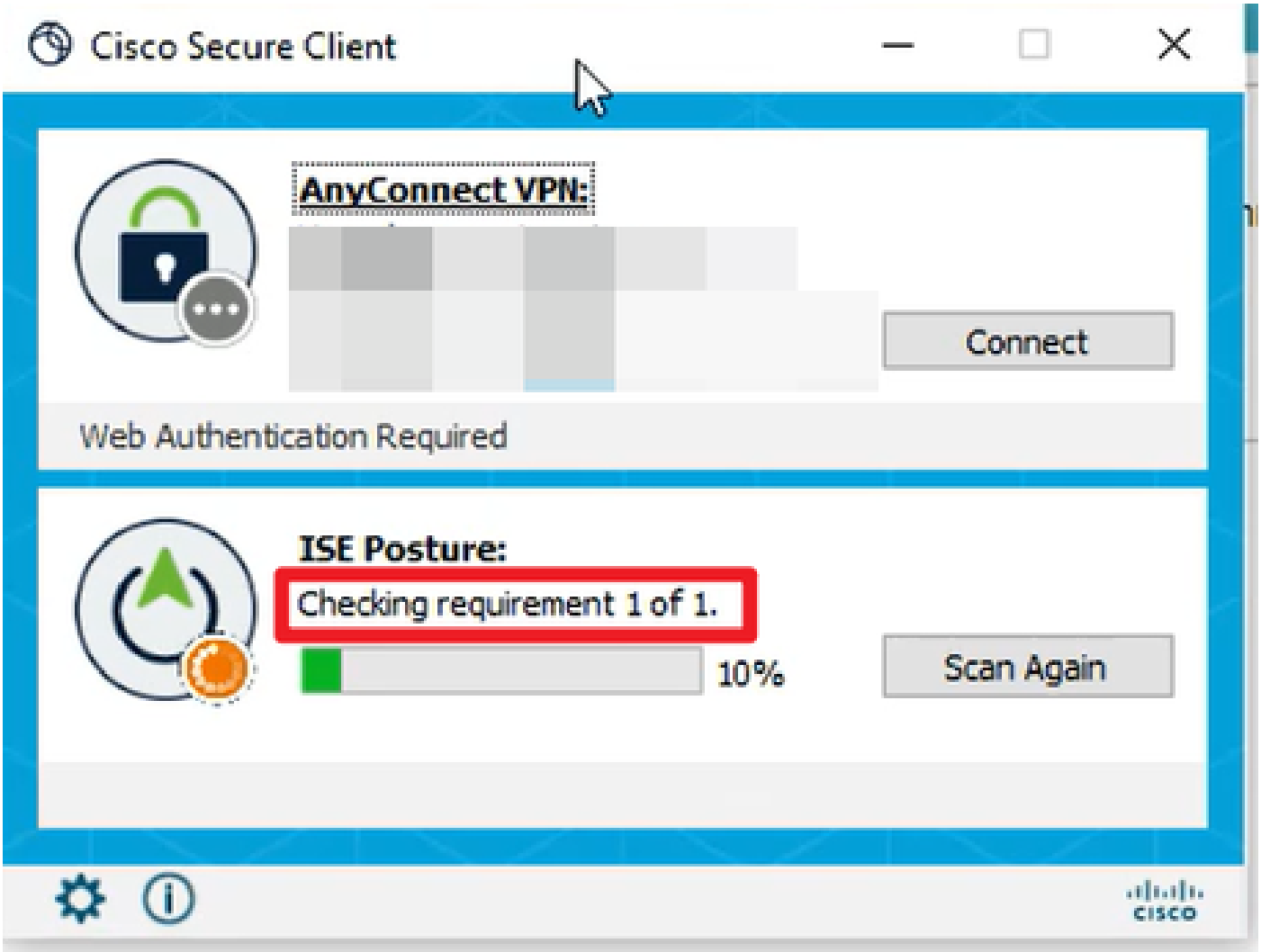

Client Provisioning Portal
Downloads
Device Security Check
Cisco Secure Client - Downloader
Initializing the Cisco Secure Client - Downloader...
Network Setup Assistant
Running Cisco Secure Client - Downloader...



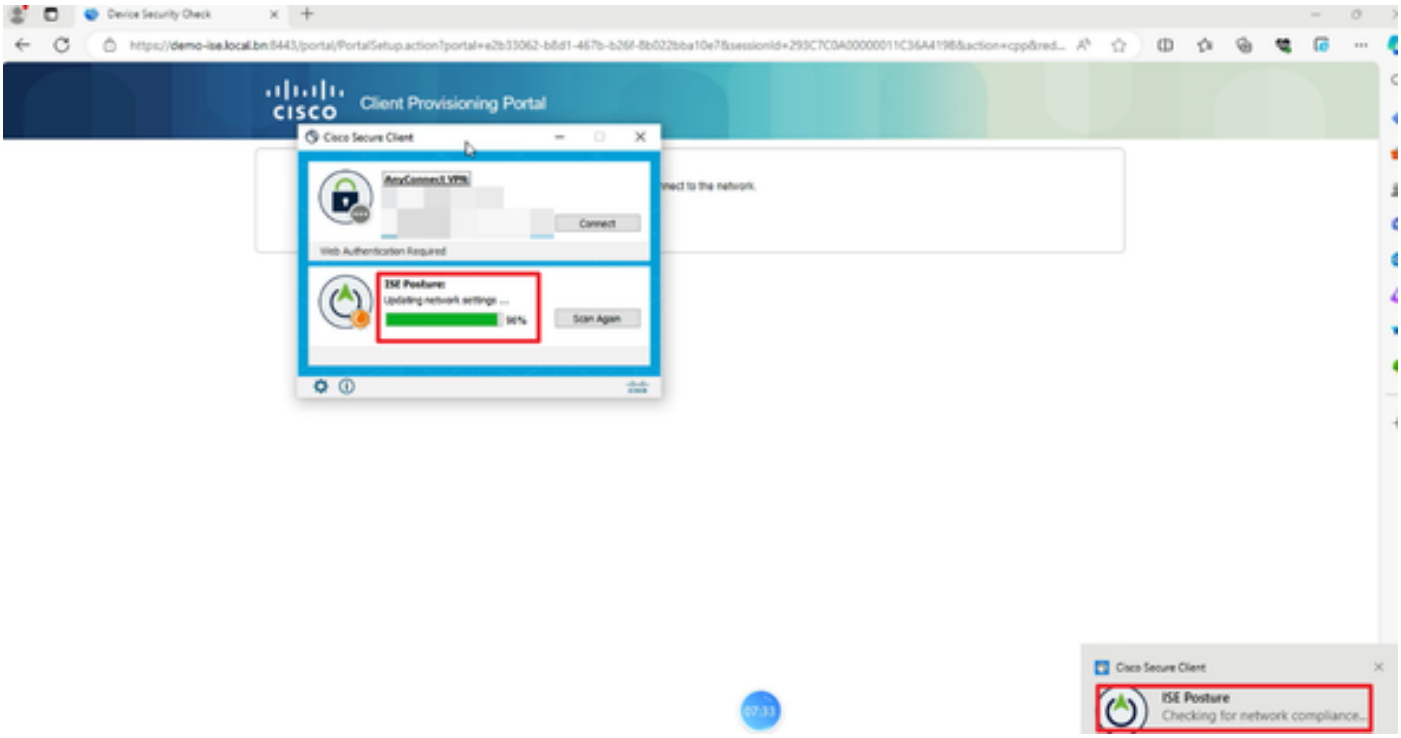


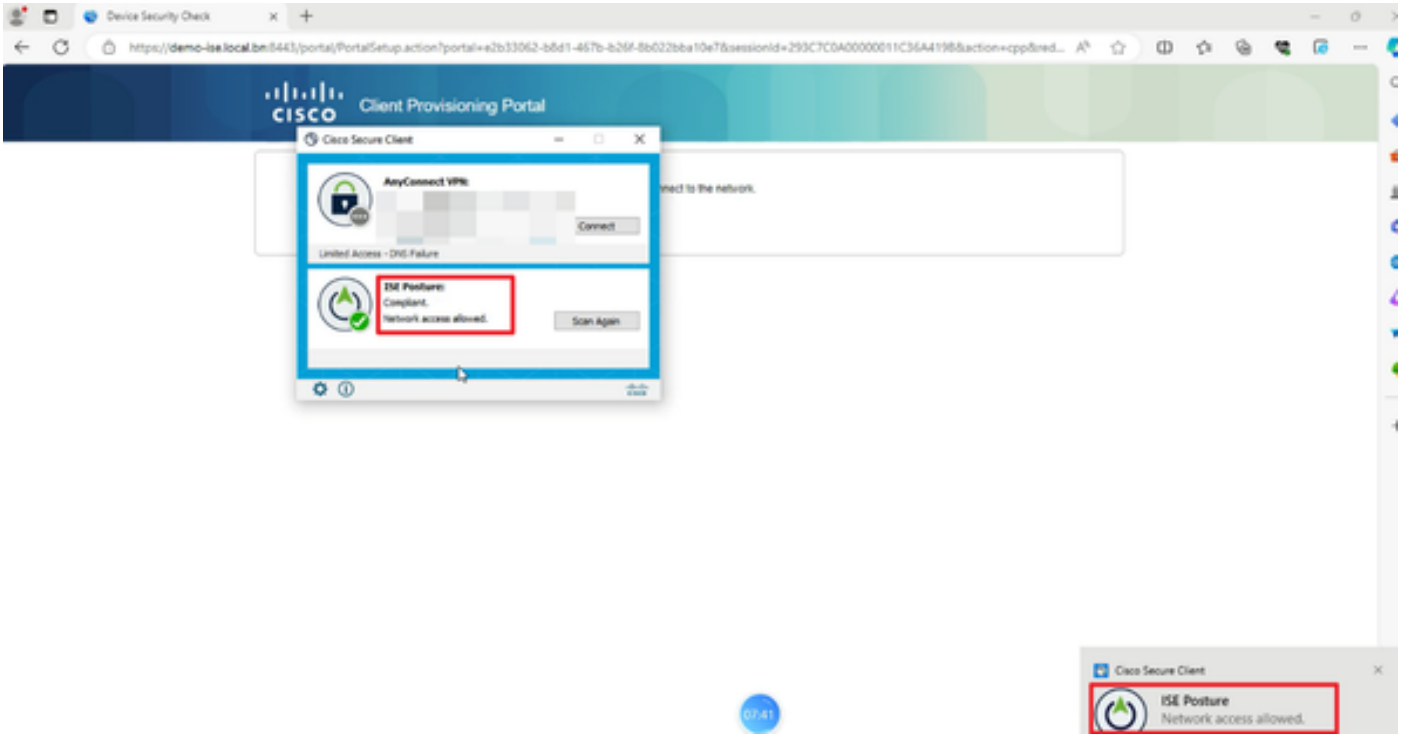
4.安全評估代理運行並從ISE獲取安全評估要求。





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。

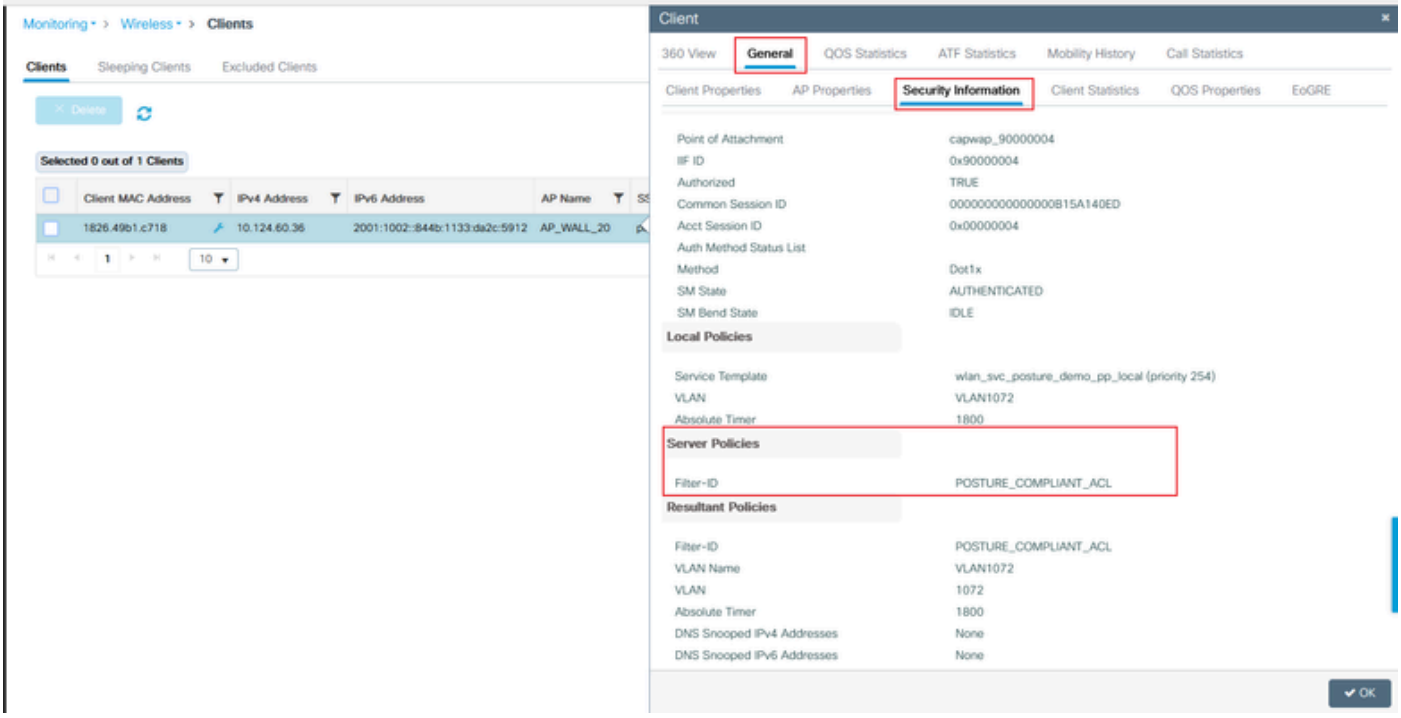




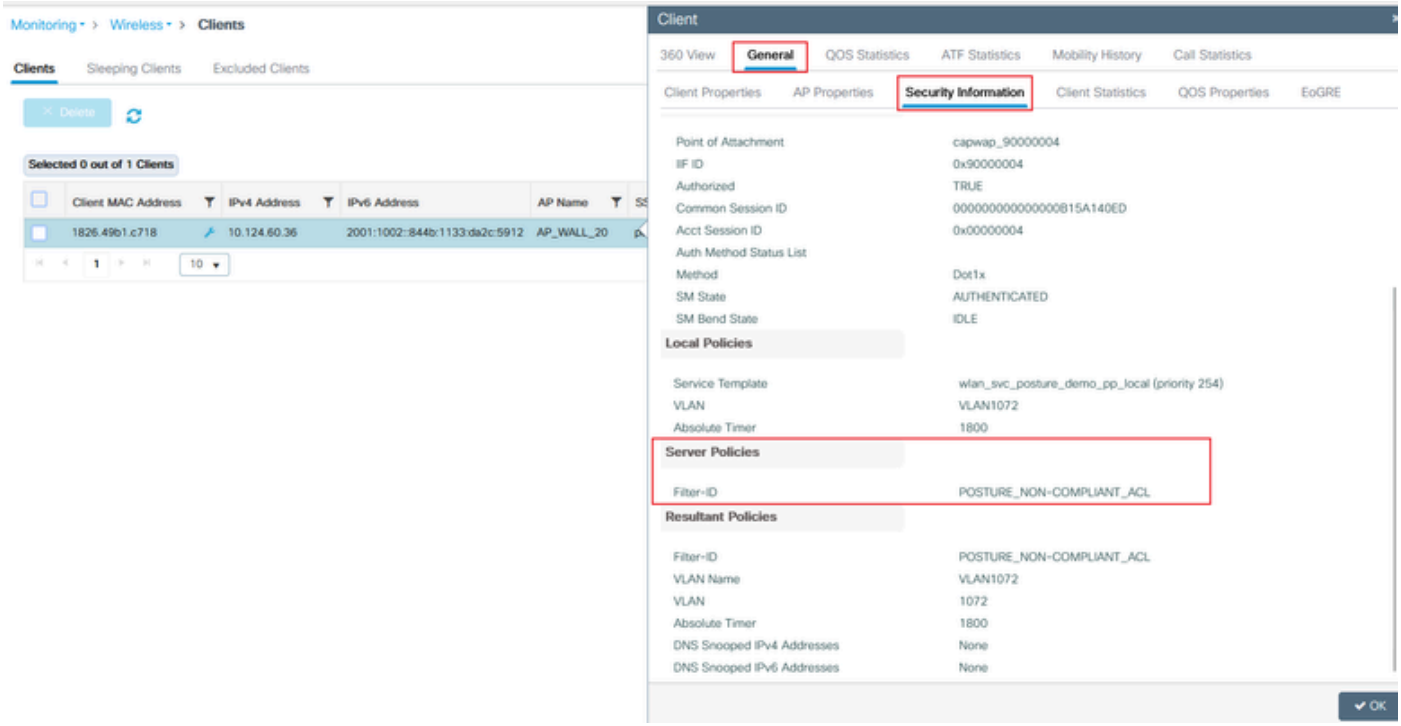
驗證

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。

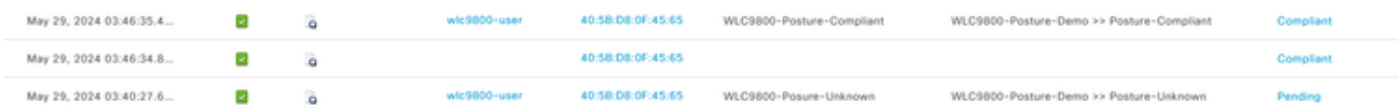
合規：



不符合：



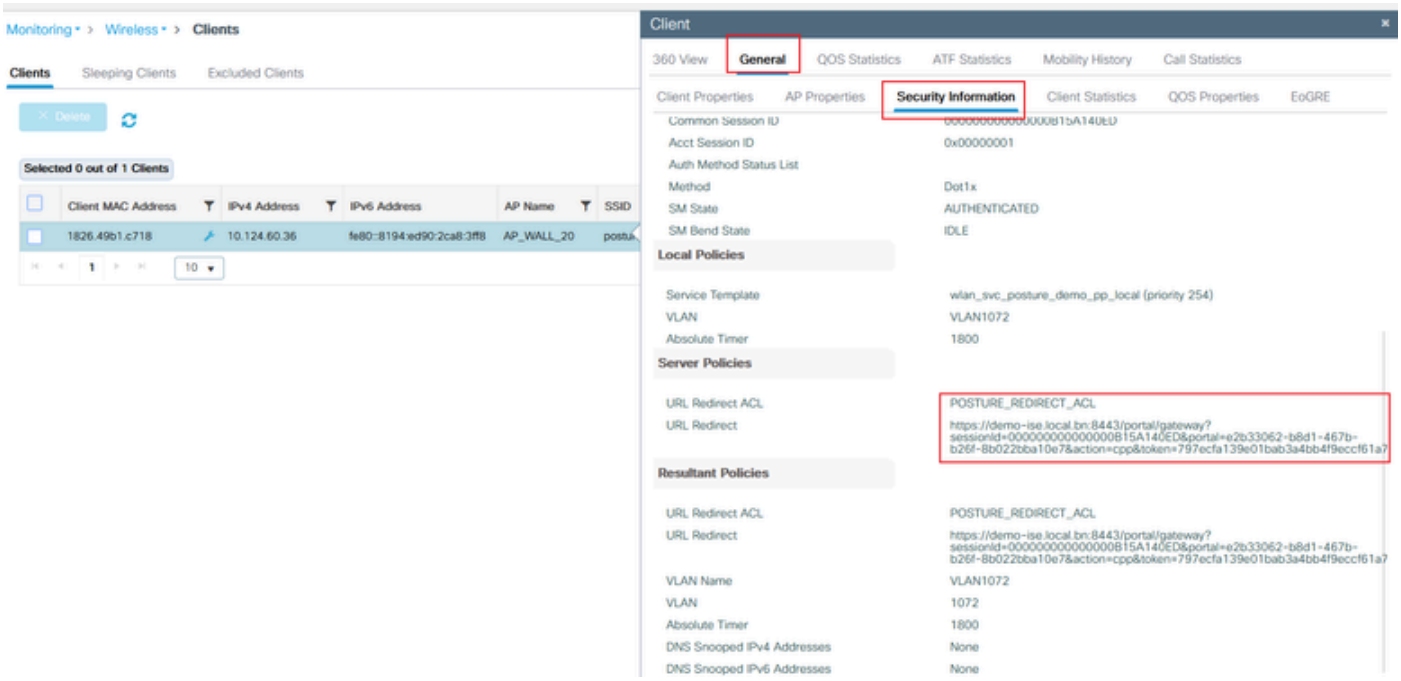
在ISE上，只需檢查Radius即時日誌，確認是否匹配正確的策略。



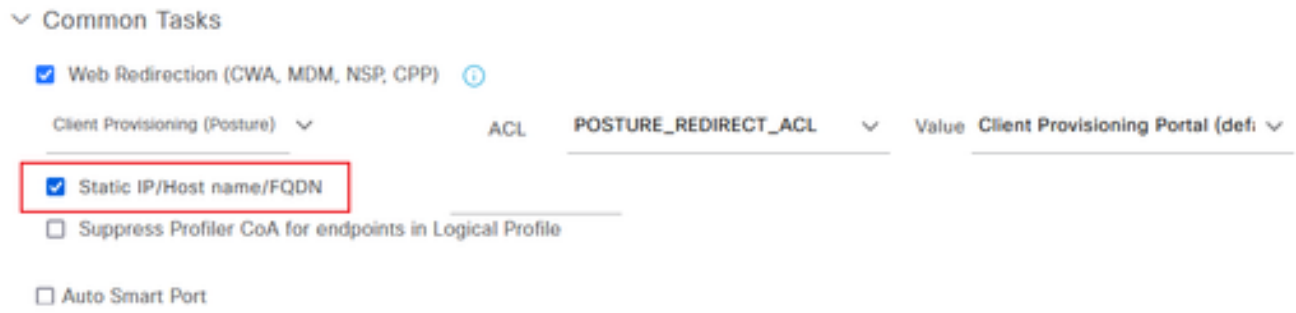
疑難排解

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）。