在ISE 3.3中使用單和雙SSID配置ISE BYOD

目錄

簡介

本文檔介紹如何在ISE上配置並排除BYOD問題。

背景

BYOD是一種功能，使使用者能夠在ISE上註冊其個人裝置，以便使用者能夠使用環境中的網路資源。它還可以幫助網路管理員限制使用者從個人裝置訪問關鍵資源。

與訪客流不同，在訪客流中，裝置使用內部儲存或ISE上的Active directory通過Guest頁面進行身份驗證。BYOD允許網路管理員在終端上安裝終端配置檔案以選擇EAP方法的型別。在EAP-TLS等場景中，客戶端證書由ISE本身簽名以在終端和ISE之間建立信任。

必要條件

思科建議您瞭解以下主題：

- WLC控制器
- ISE基礎知識

採用元件

這些使用的裝置不限於BYOD流的一個特定版本：

- Catalyst 9800-CL無線控制器(17.12.3)
- ISE虛擬機器(3.3)

什麼是ISE上的單SSID和雙SSID自帶裝置？

單SSID BYOD

在單SSID BYOD設定中，使用者將其個人裝置直接連線到公司無線網路。自註冊過程發生在同一個SSID上，其中ISE促進裝置註冊、調配和策略實施。此方法簡化了使用者體驗，但需要安全自註冊和適當的身份驗證方法來確保網路安全。

雙SSID BYOD

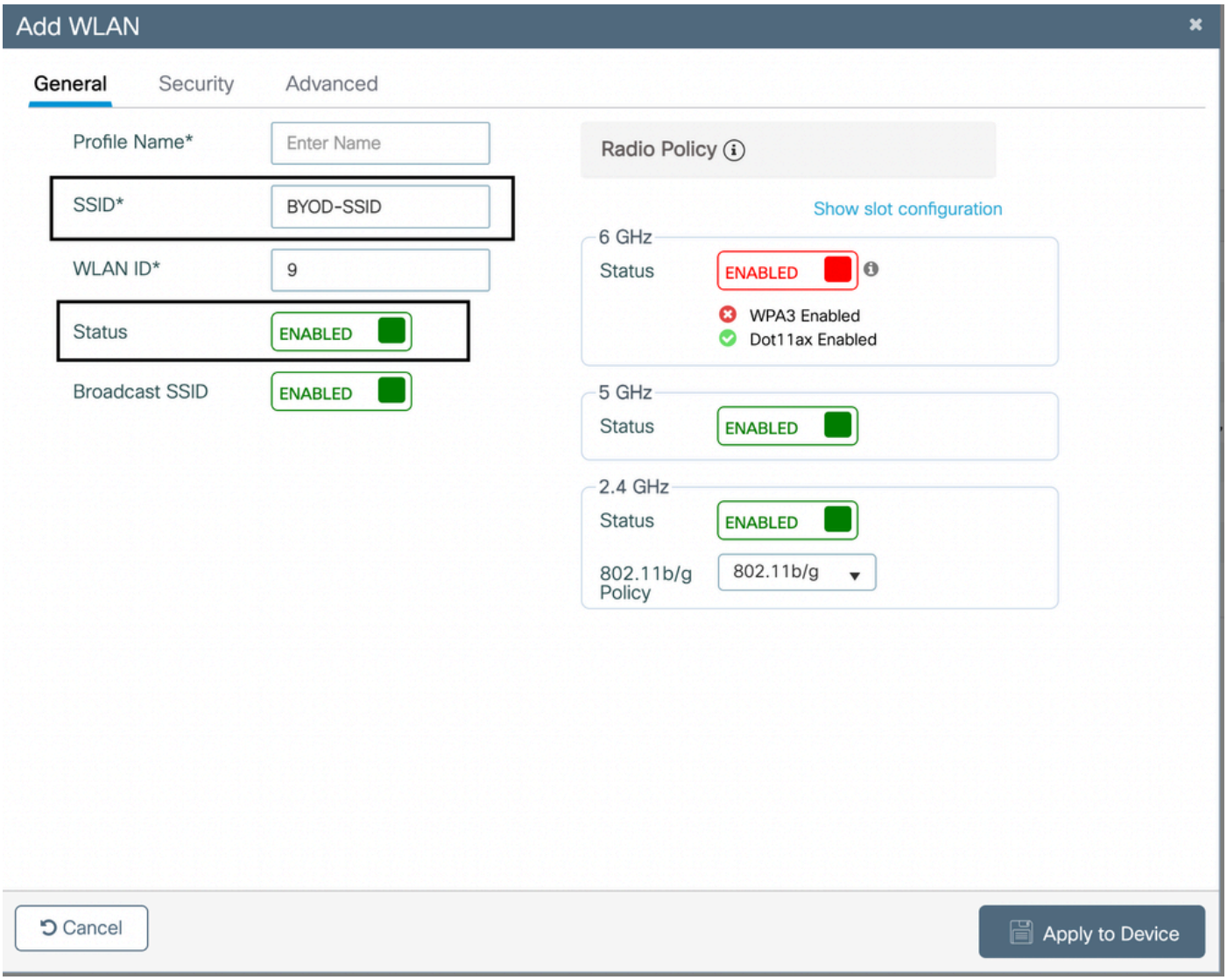
在雙SSID BYOD設定中，使用兩個單獨的SSID:一個用於自註冊（不安全或限制訪問），另一個用於訪問公司網路。使用者最初連線到自註冊SSID，通過ISE完成裝置註冊和調配，然後切換到安全的公司SSID進行網路訪問。這樣通過將自註冊流量與生產流量隔離，提供了額外的安全層。

WLC組態

為CWA建立WLAN

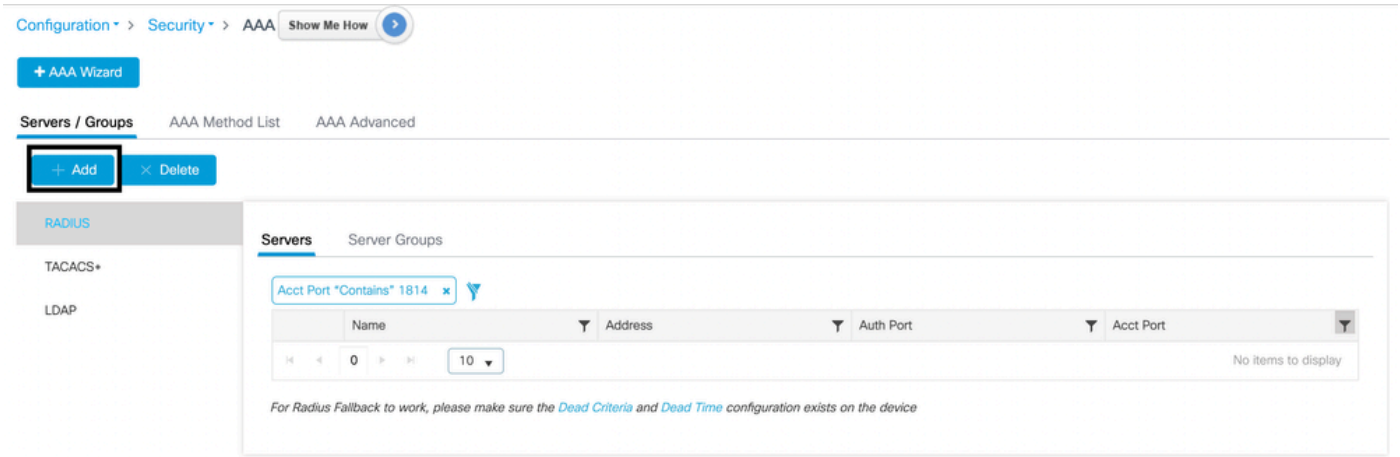
1. 前往Configuration > Tags & Profiles > WLANs。
2. 按一下「Add」以建立一個新的WLAN。

- 設定WLAN名稱和SSID（例如BYOD-WiFi）。
- 啟用WLAN。

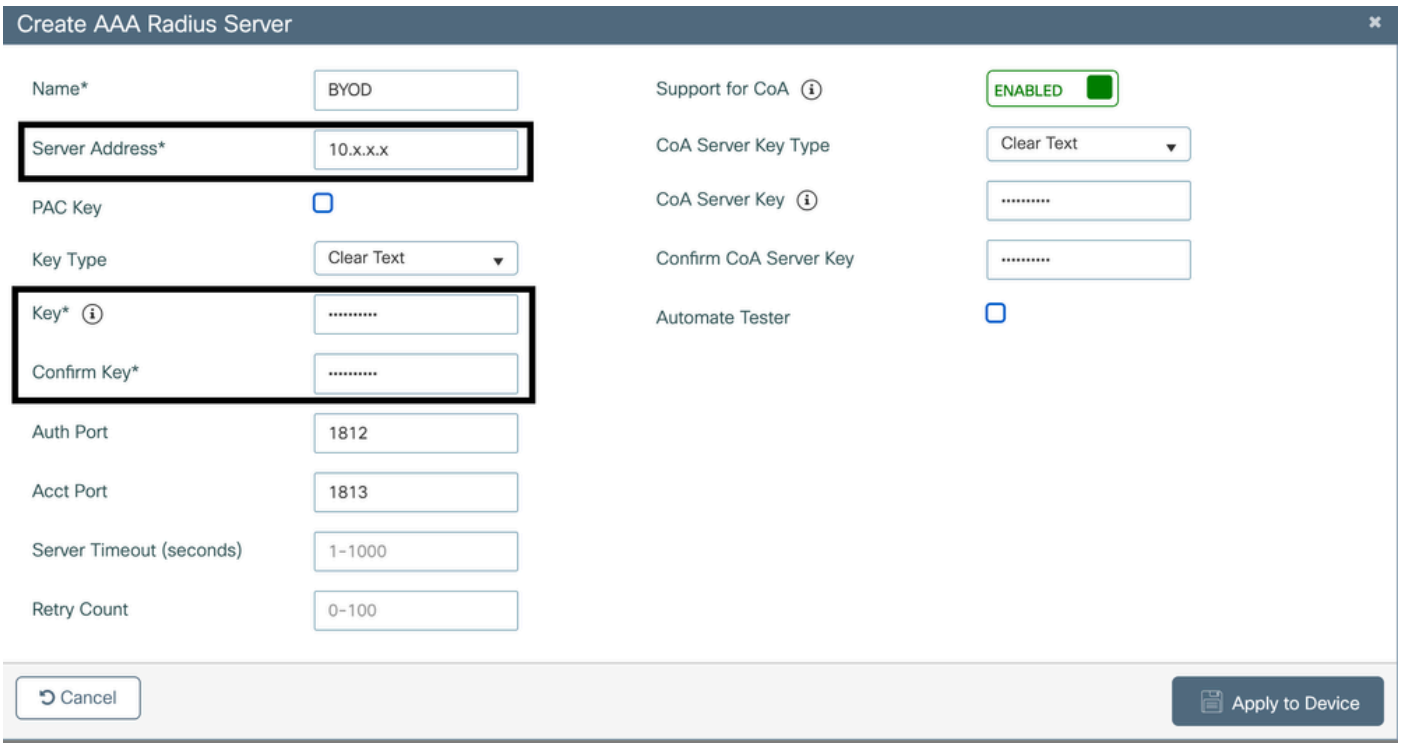


設定RADIUS伺服器

1. 導覽至Configuration > Security > AAA > RADIUS > Servers。

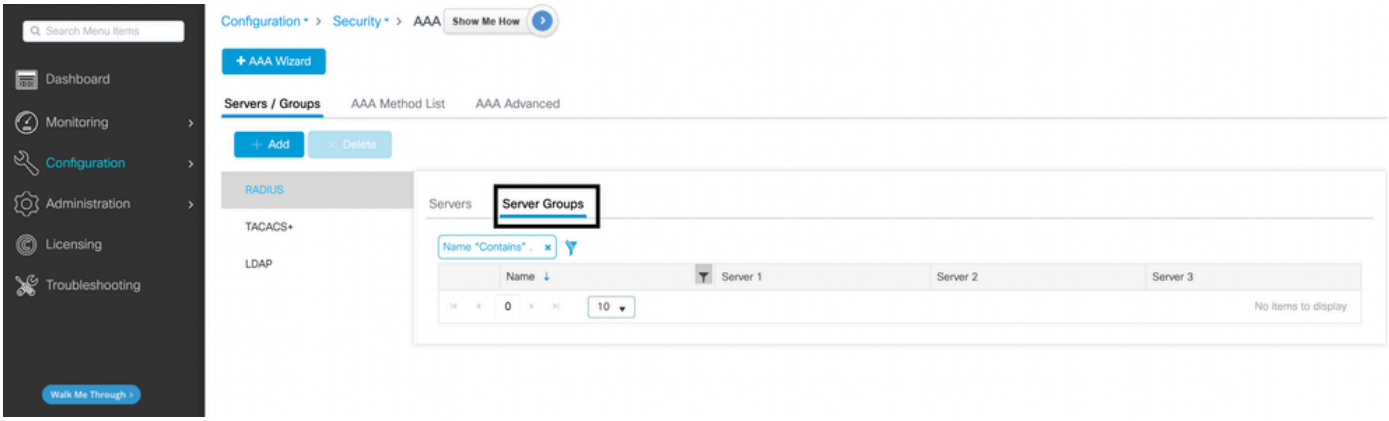


2. 按一下Add將ISE配置為RADIUS伺服器：
    - 伺服器IP：ISE的IP地址
    - 共用金鑰：匹配ISE上配置的共用金鑰。

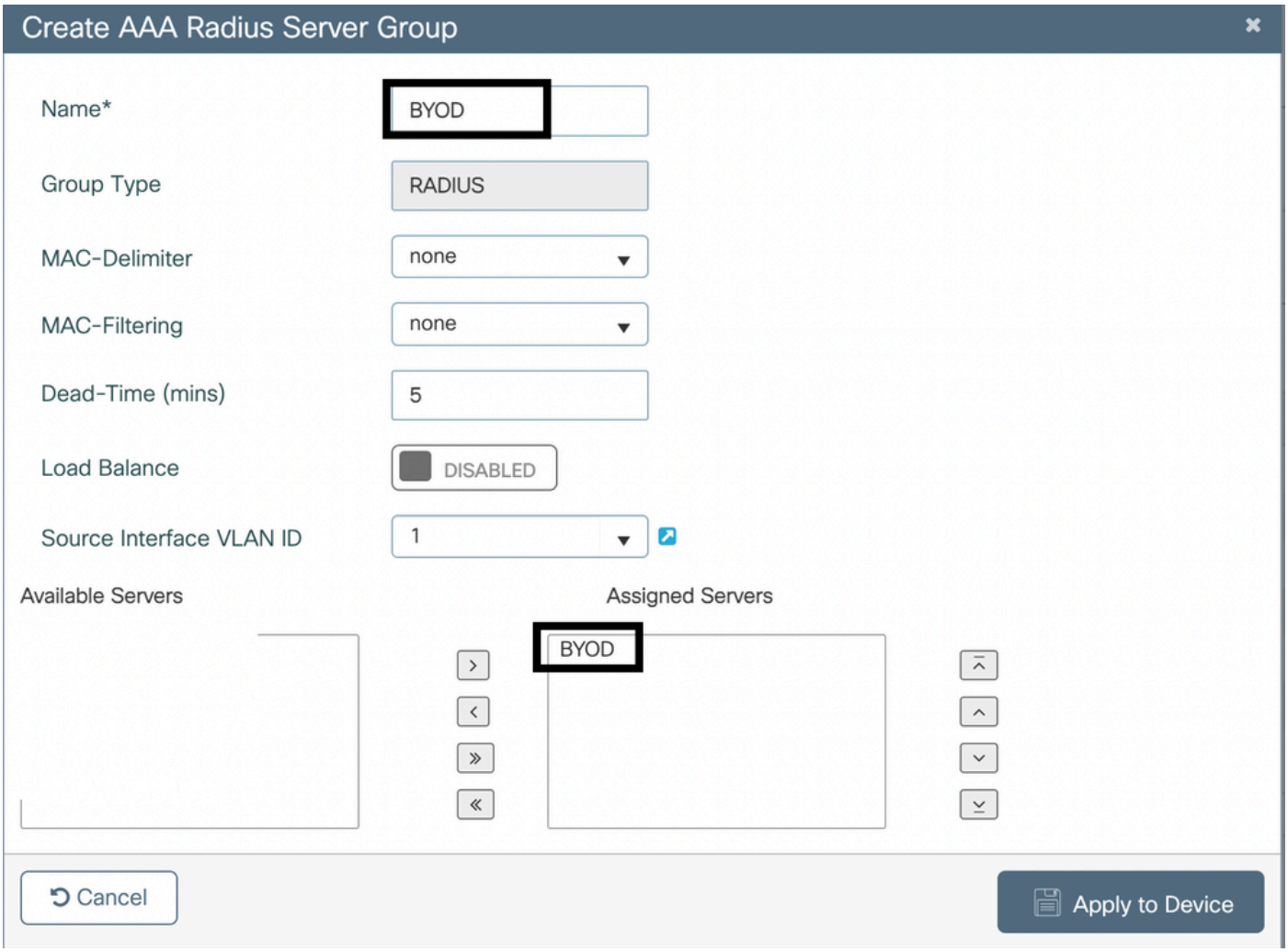


配置AAA伺服器

1. 導覽至Configuration > Security > AAA > Servers/Groups。



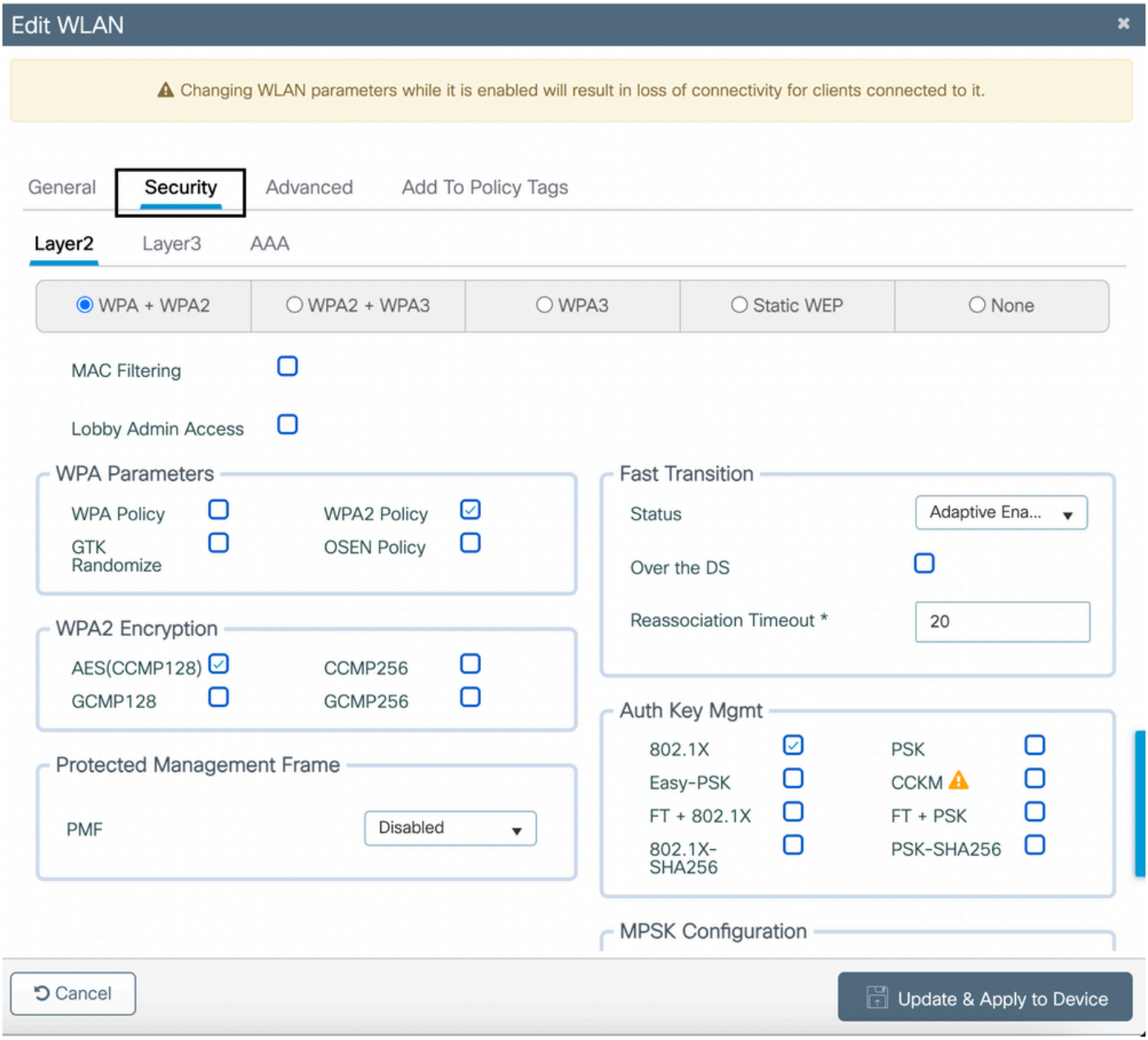
2. 將RADIUS伺服器分配給新的或現有的伺服器組。



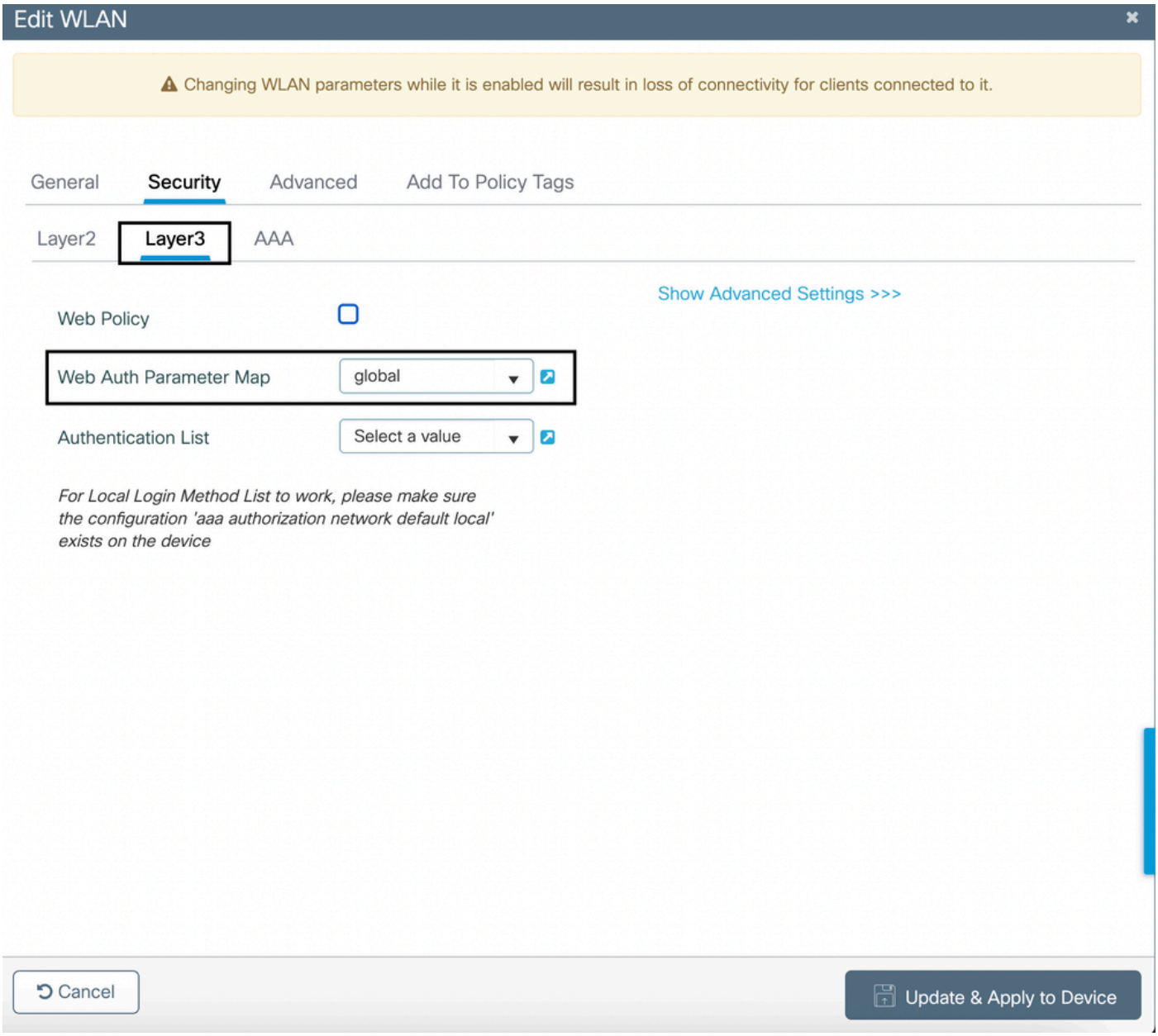
為WLAN配置安全策略

1. 導覽至Configuration > Tags & Profiles > WLANs。編輯先前建立的WLAN。

2. 在Security > Layer 2頁籤下：
   - 啟用WPA+WPA2
   - 在WPA2加密下設定AES(CCMP128)
   - Auth Key Mgmt as 802.1X



3. 在Security > Layer 3索引標籤下，從Web Auth Parameter Map下拉選單中選擇global。



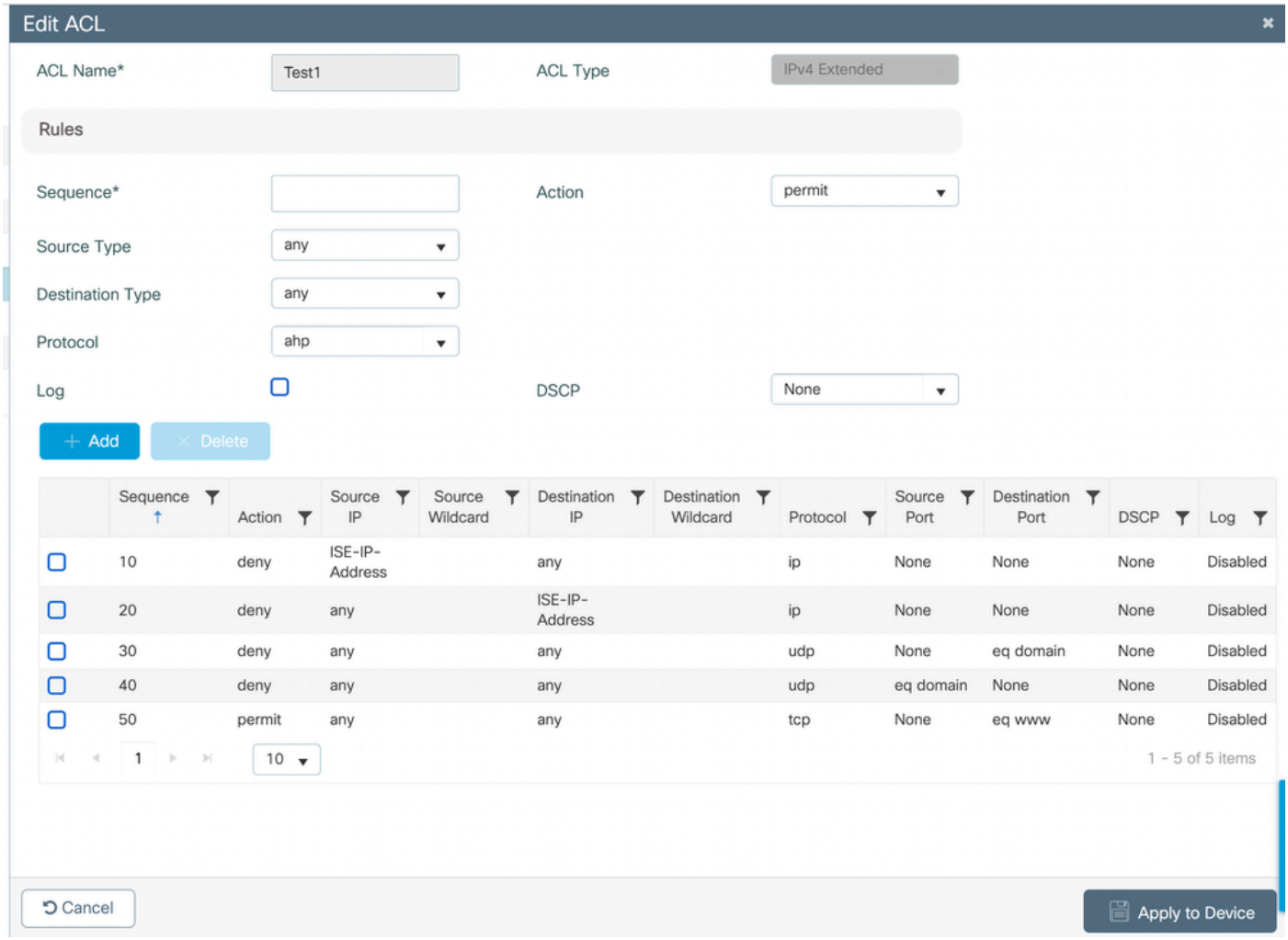
設定預先驗證ACL

建立ACL以允許使用重定向操作：

- DNS流量。
- 通過HTTP/HTTPS連線到ISE門戶。
- 任何所需的後端服務。

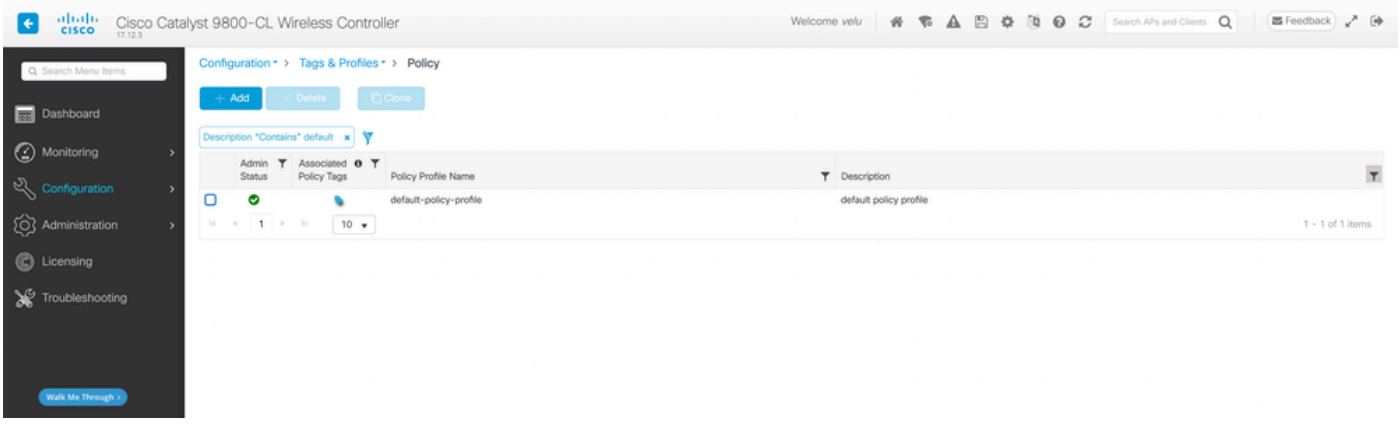
為此，請執行以下操作：

1. 導覽至Configuration > Security > ACLs > Access Control Lists。
2. 建立包含規則的新ACL以允許必要的流量。

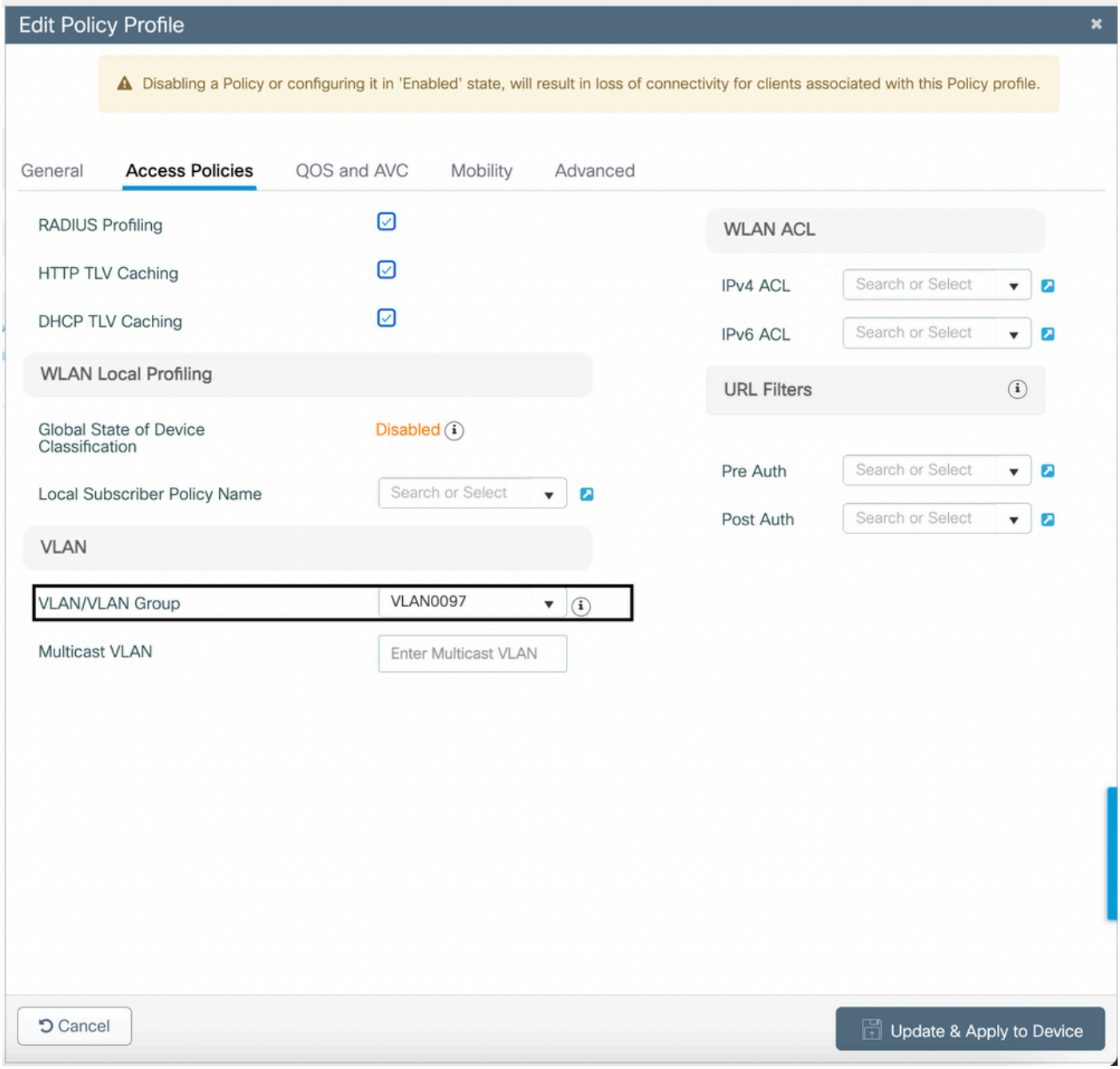


配置策略配置檔案

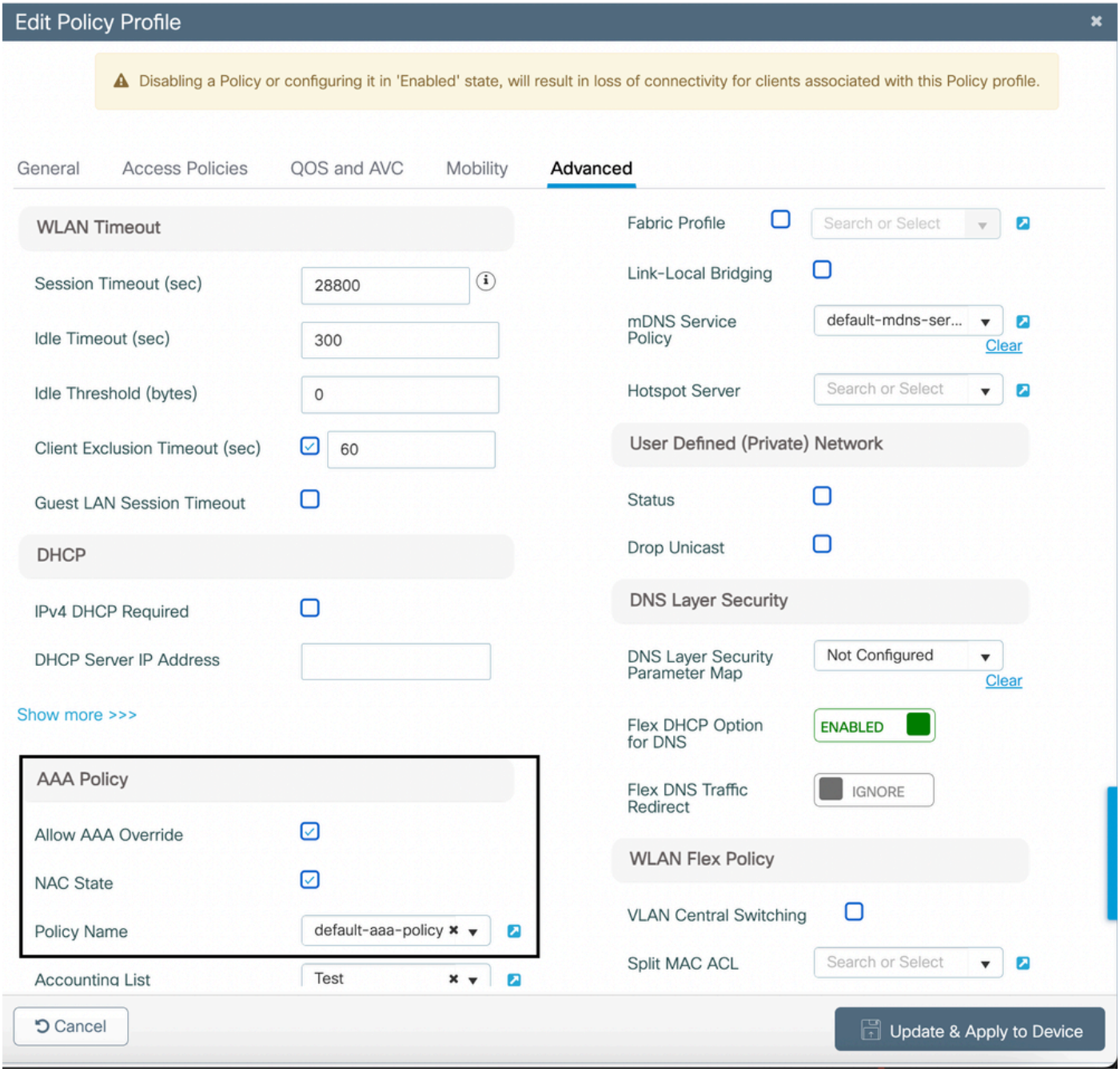
1. 導覽至Configuration > Tags & Profiles > Policy。可以建立或使用預設策略



2. 在Access Policies下分配適當的VLAN

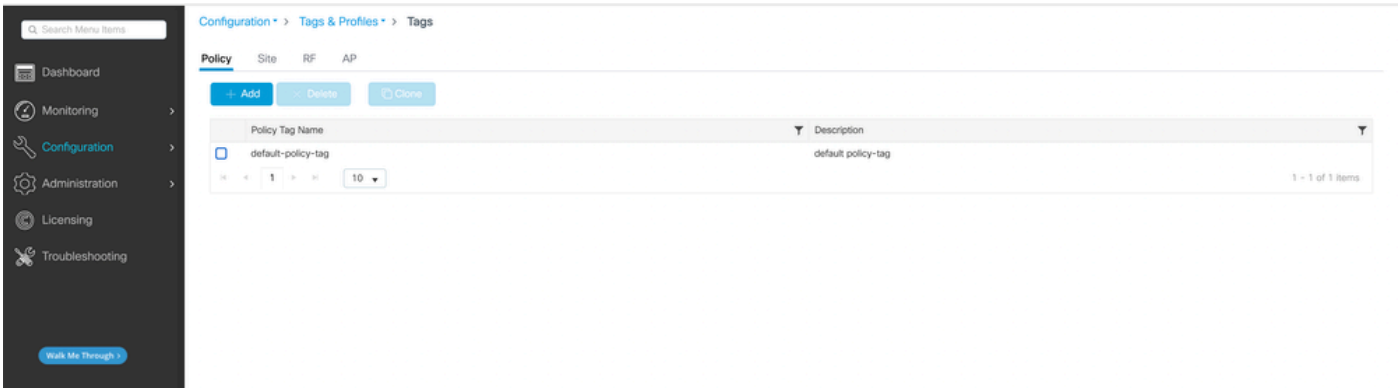


3.還在該策略的高級下啟用Allow AAA Override和NAC state。



應用標籤並進行部署

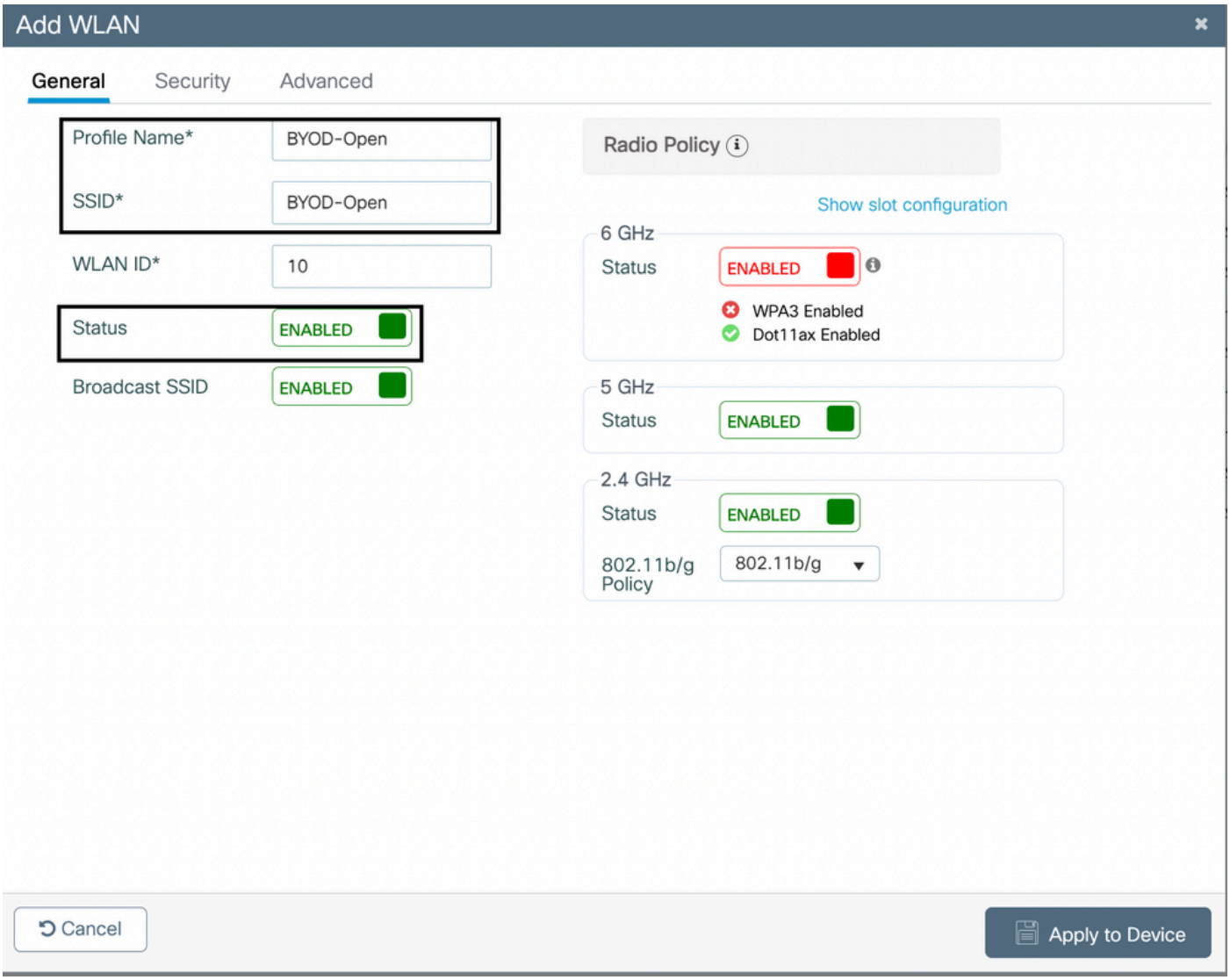
- 導航到Configuration > Tags & Profiles > Tags。
- 建立或編輯標籤，以包括WLAN和策略配置檔案。
- 為接入點分配標籤。



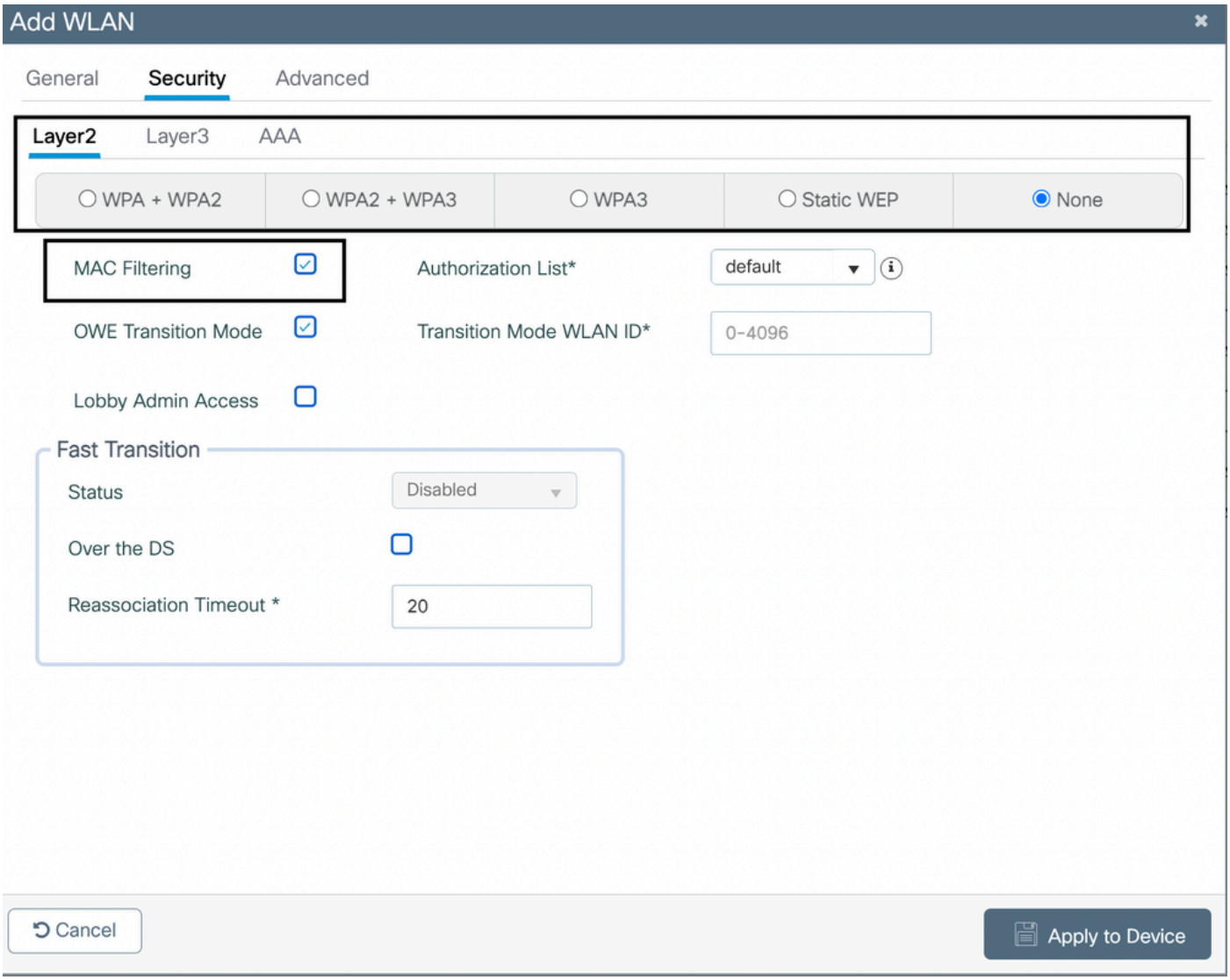
配置開放/不安全SSID

只有在您決定環境中具有雙SSID BYOD配置時，才會建立開放式SSID。

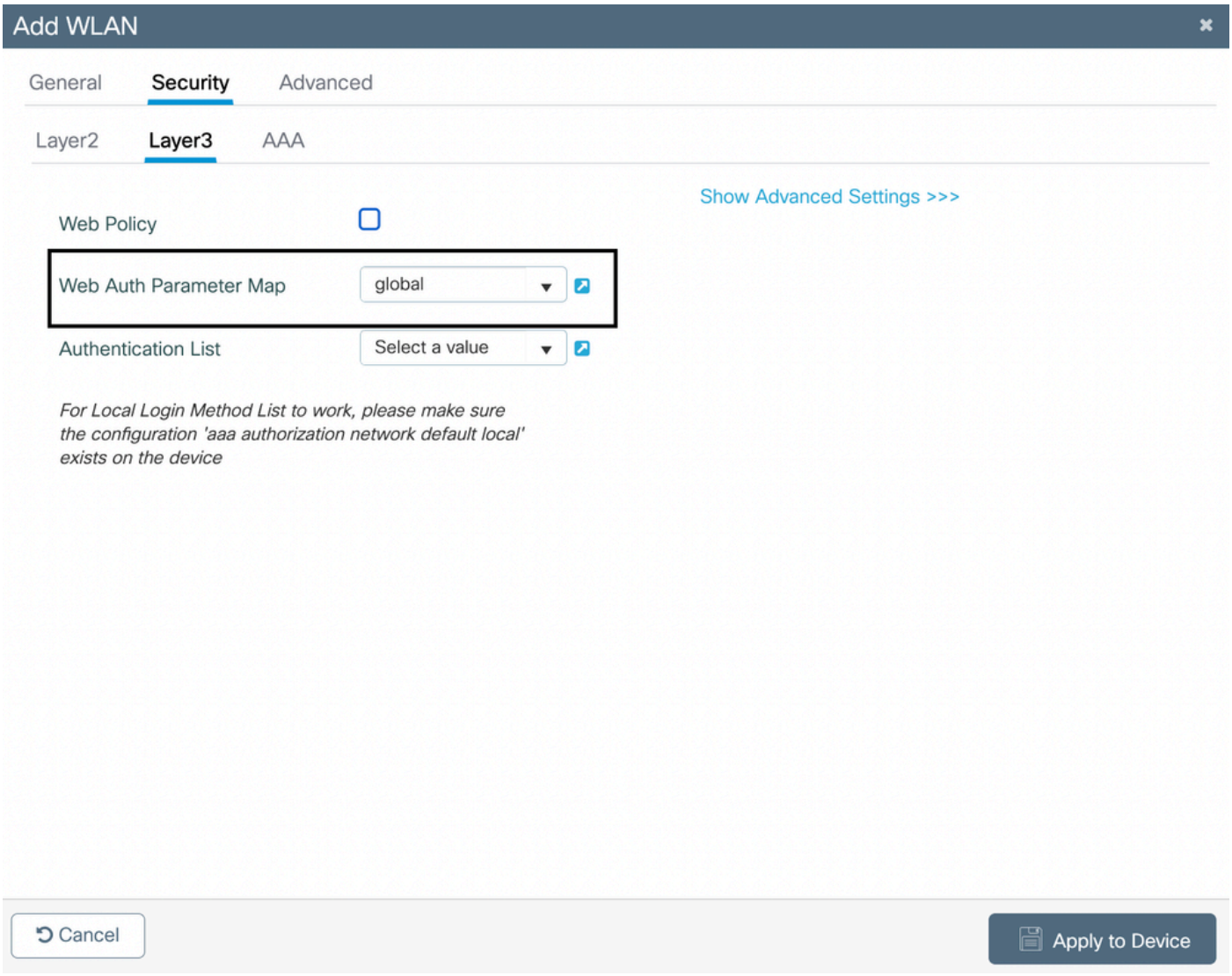
1. 導覽至Configuration > Tags & Profiles > WLANs。按一下Add按鈕。
2. 在General頁籤下提供SSID名稱並啟用WLAN按鈕。



3.從同一視窗中按一下Security標籤。選擇None單選按鈕並啟用Mac過濾。



4.在第3層的Security下，選擇Web Auth Parameter Map的全域性設定。如果您在WLC上設定了任何其他Web驗證設定檔，您還可以將其對映至此處：



ISE 組態

前提條件

- 確保已安裝Cisco ISE並獲得BYOD功能許可。
- 將您的WLC作為具有RADIUS共用金鑰的網路裝置新增到ISE。

憑證

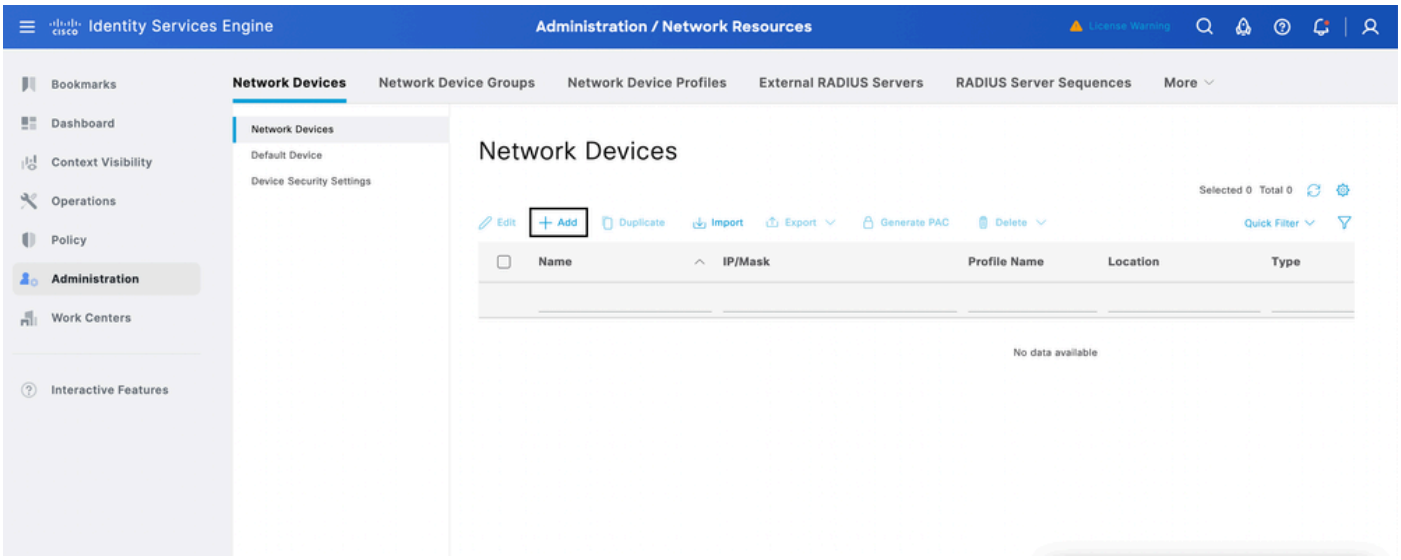
- 在ISE上安裝有效的伺服器證書以避免瀏覽器安全警告。
- 確保證書受端點信任（由已知的CA或具有受信任根的內部的CA簽署）。

DNS配置

- 確保DNS解析BYOD門戶的ISE主機名。

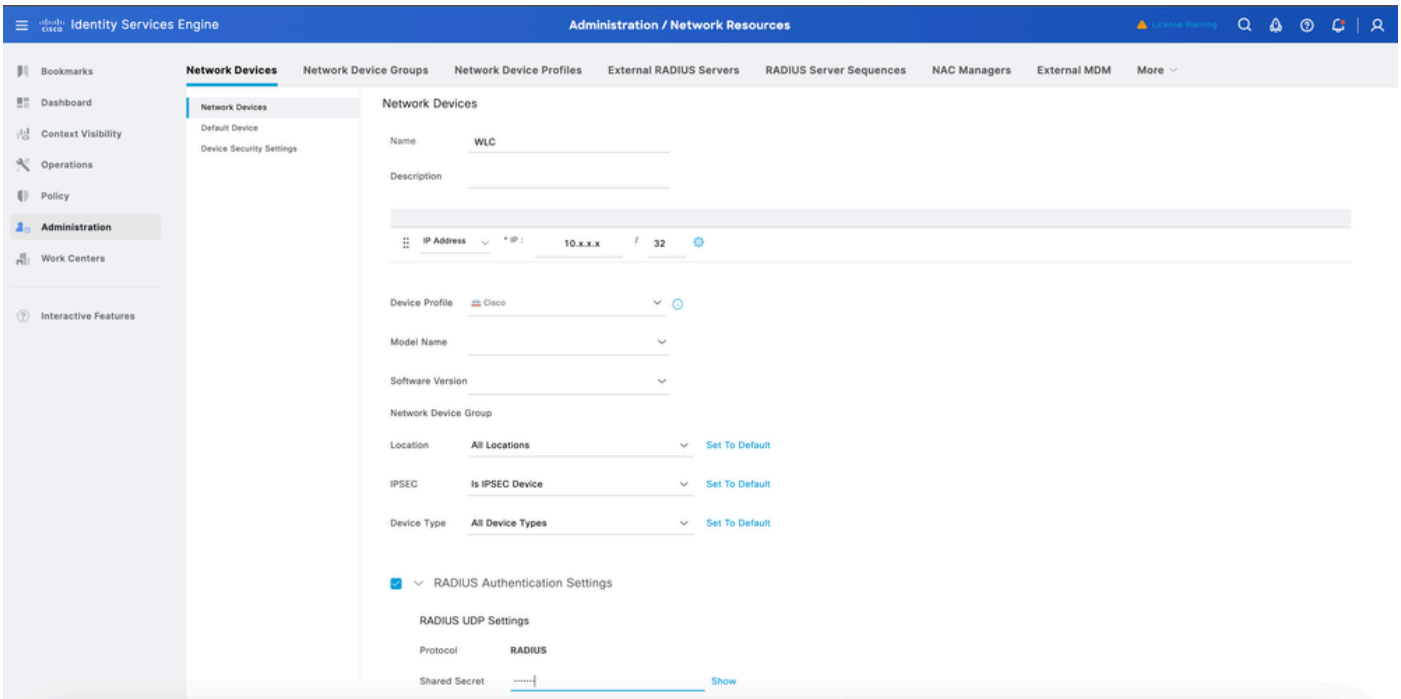
配置ISE網路裝置

1. 登入到ISE Web UI。
2. 導覽至Administration > Network Resources > Network Devices。



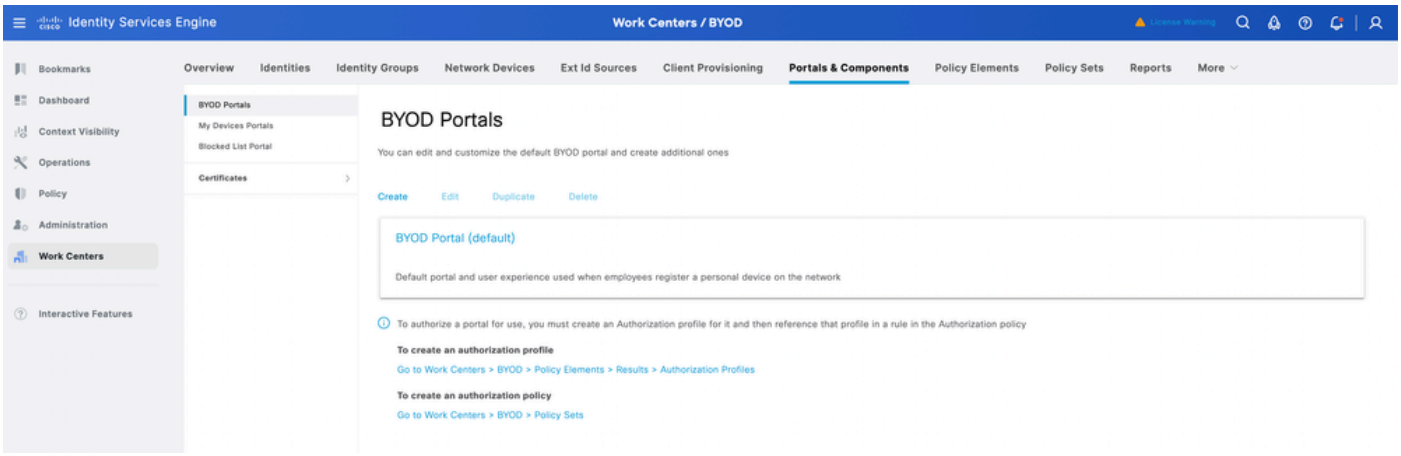
3.將WLC新增為網路裝置：

- 名稱:輸入WLC的名稱。
- IP 位址:輸入WLC管理IP。
- RADIUS共用密碼:輸入與WLC上配置的相同共用金鑰。
- 按一下「Submit」。



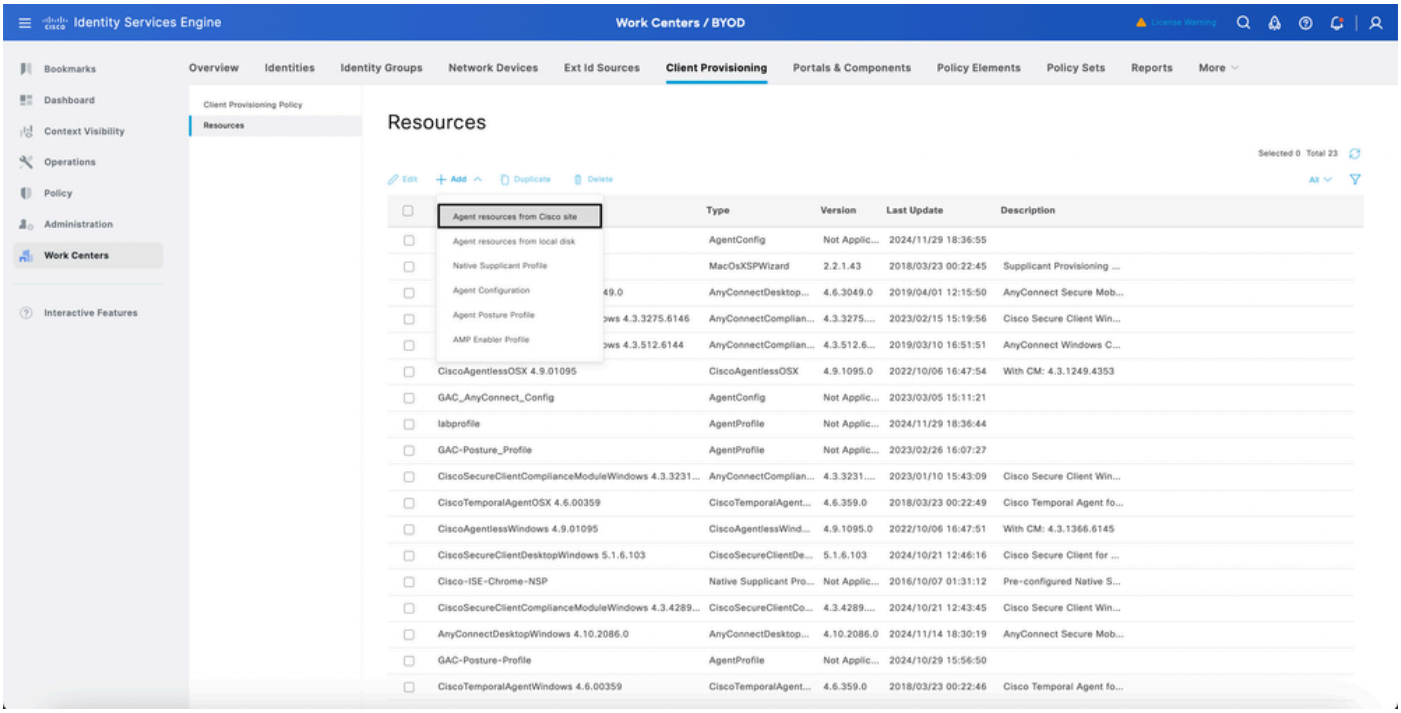
建立BYOD門戶

1. 導航至工作中心> BYOD >設定>門戶和元件> BYOD門戶。
2. 按一下Add建立BYOD門戶，或者可以使用ISE上的現有預設門戶。



下載Cisco IOS®最新版本

1. 導航至工作中心(Work Centers)> BYOD（自帶裝置）>客戶端調配(Client provisioning)>資源(Resources)。
2. 按一下Add按鈕，然後從思科站點中選擇代理資源。



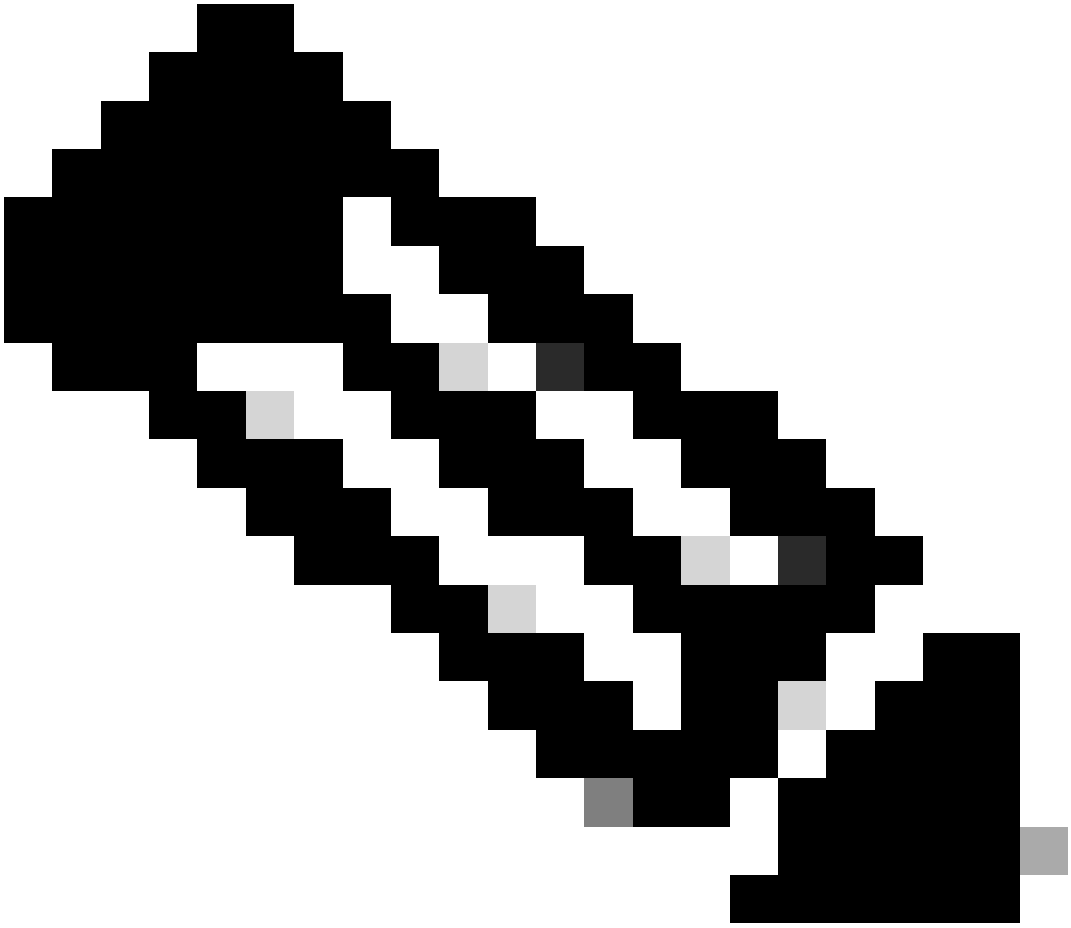
3.在軟體清單中，選擇要下載的最新Cisco IOS版本。

Download Remote Resources

	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☑	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the "Agent resource from local disk" add option, to import into ISE

Cancel Save

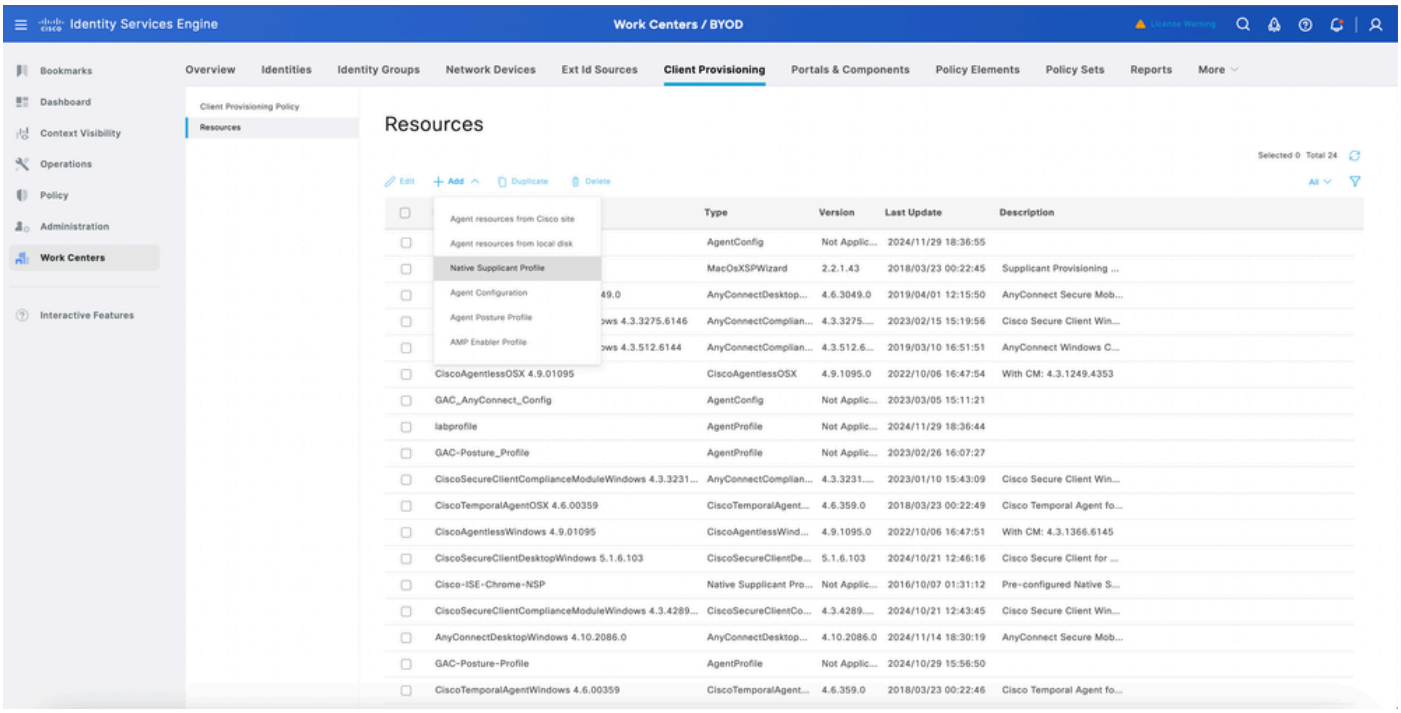


附註：Cisco IOS軟體在Windows和MacOS終端的ISE上下載。對於Apple iPhone IOS，它使用本地請求方來調配裝置；對於android裝置，您有需要從Play Store下載的網路設定助手。

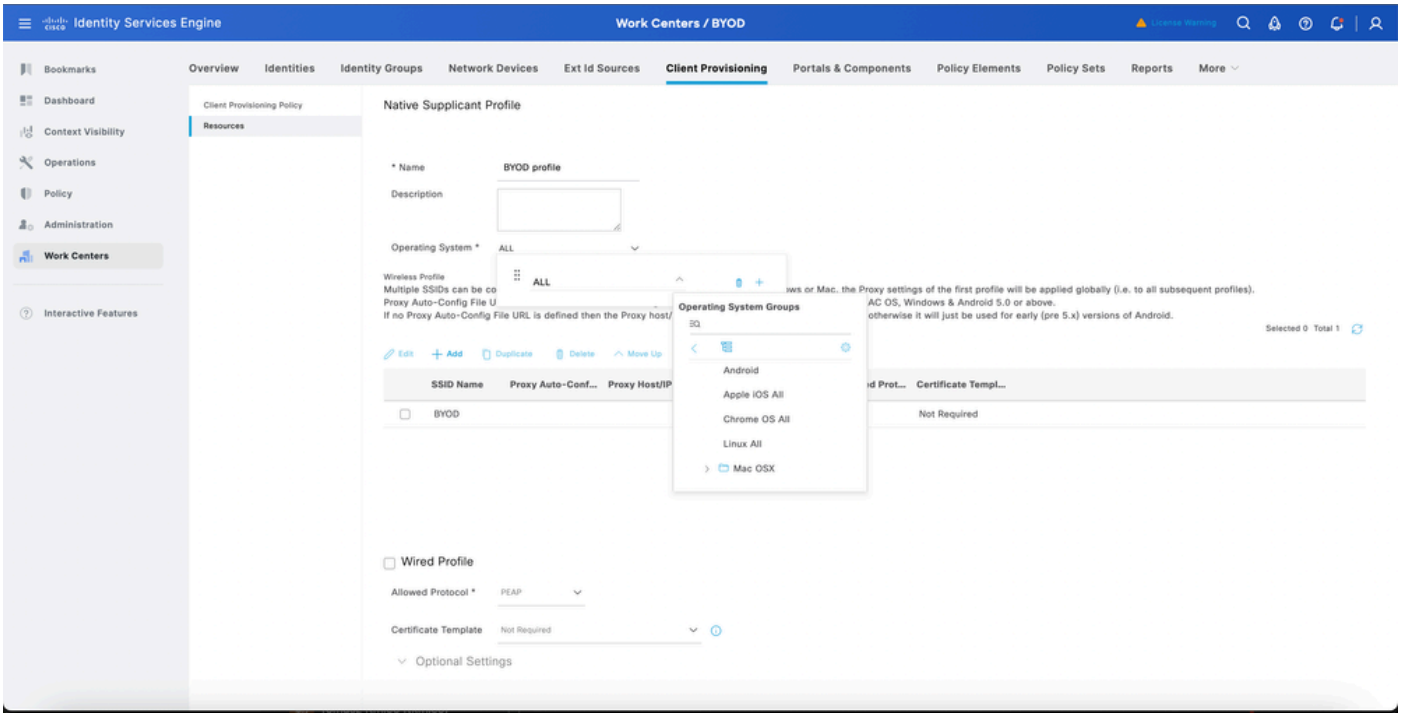
建立終端配置檔案

1.導航至工作中心> BYOD >客戶端調配>資源。

2.按一下Add，從下拉選單中選擇Native supplicant profile。



3.在「Operating system」下拉選單下，選擇要裝入裝置的所需作業系統，或者您可以將環境中所有終端的裝入作業系統設定為「ALL」：



4.從頁面中按一下Add以建立終端配置檔案，為終端配置802.1X:

Wireless Profile(s)

SSID Name * BYOD

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

- [ ] Automatically use logon name and password (and domain if any)
- [x] Enable fast reconnect
- [ ] Enable quarantine checks
- [ ] Disconnect if server does not present cryptobinding TLV
- [ ] Do not prompt user to authorize new servers or trusted certification authorities
- [x] Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- [ ] Enable if target network is hidden

Android Settings

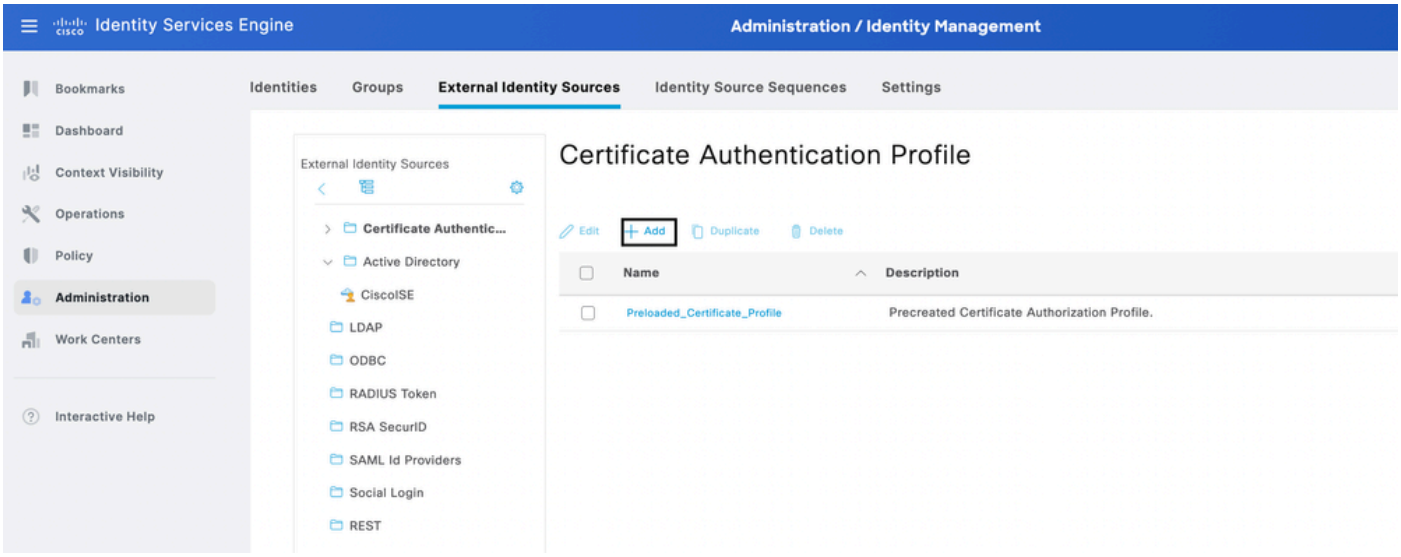
Certificate Enrollment Protocol:

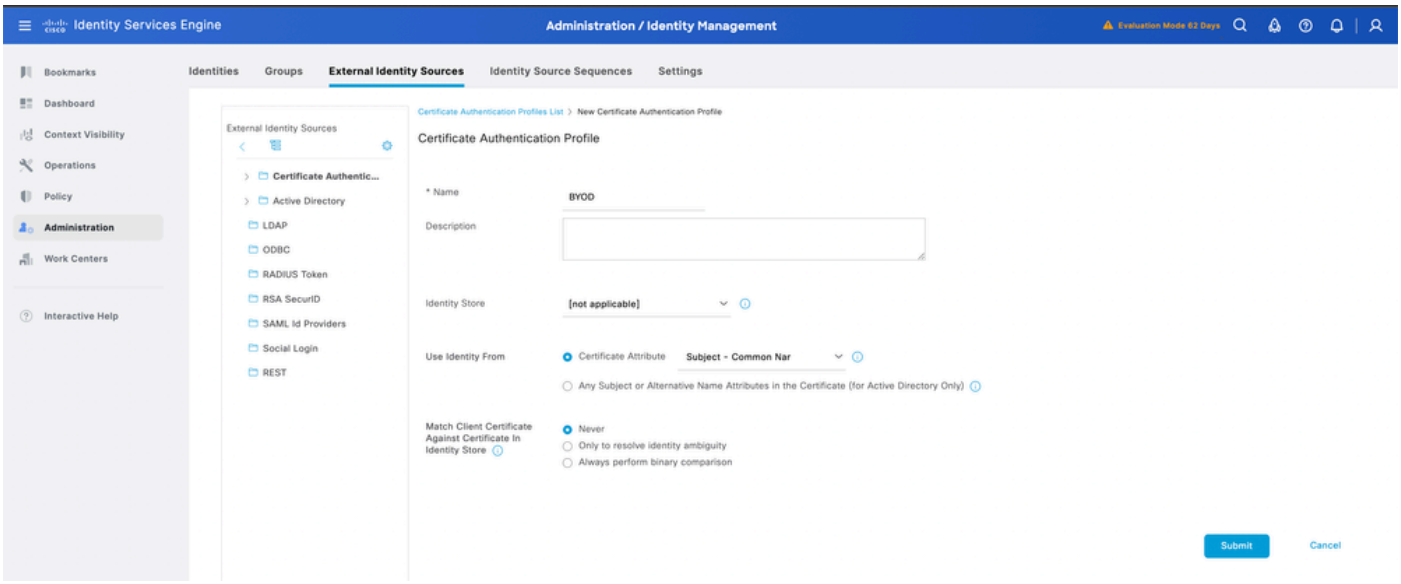
調配，其中「代理配置」部分確定為終端安全評估檢查強制實施的終端安全評估代理和合規性模組，而「本地請求方配置」部分管理BYOD調配流的設定

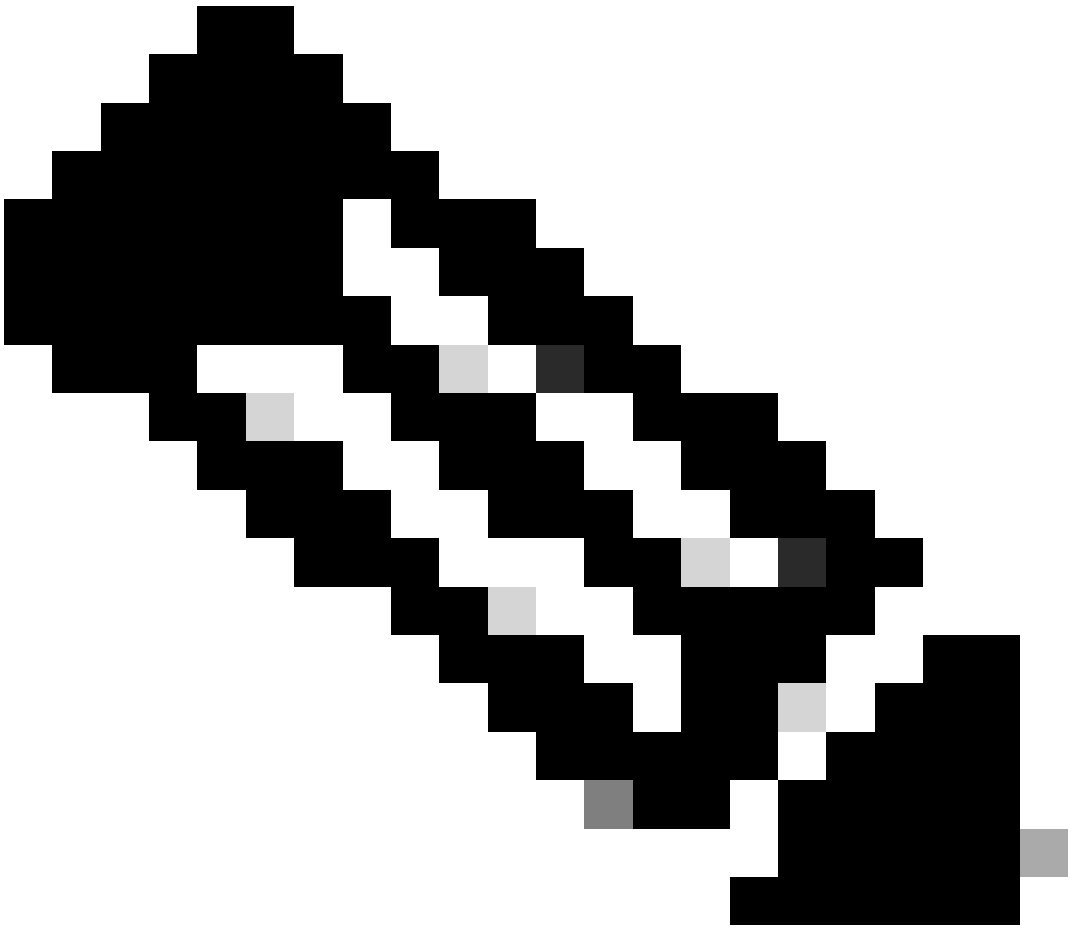
為單SSID BYOD配置ISE策略集

1. 導航到Policy > Policy Set，為ISE上的BYOD流建立策略：

2.然後，導航到管理>身份管理>外部身份源>證書身份驗證配置檔案。按一下Add按鈕建立證書配置檔案：

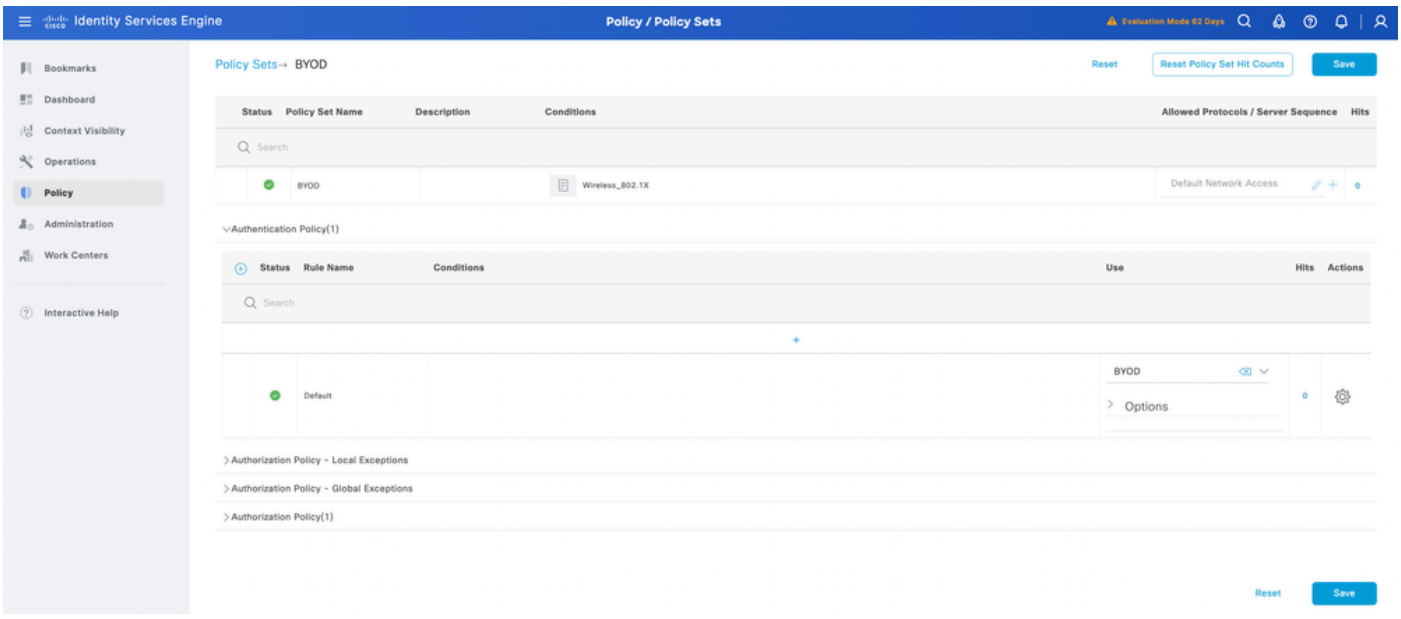






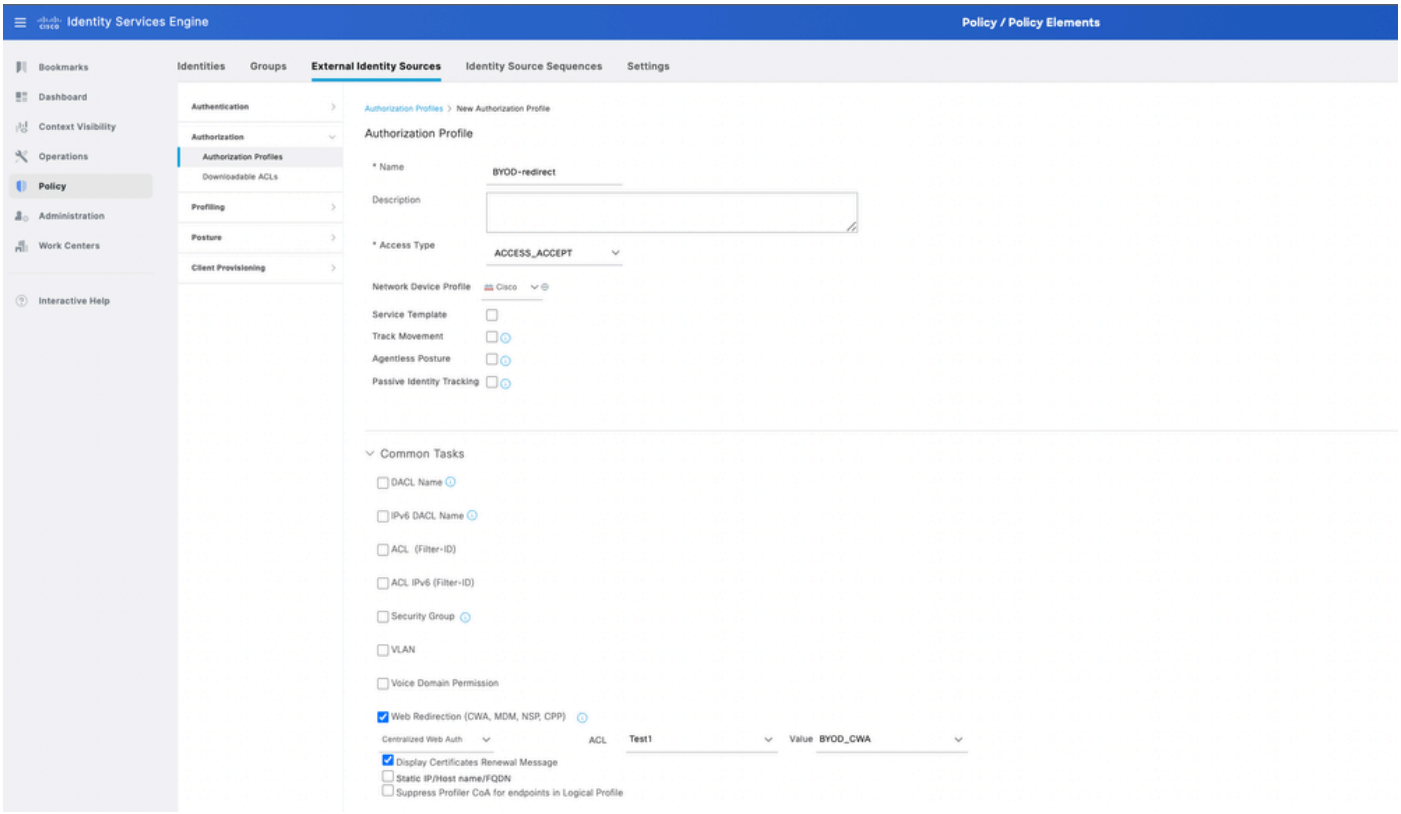
附註：在身份庫中，您可以始終選擇已整合到ISE的Active Directory，以便從證書中執行使用者查詢，從而增強安全性。

3.按一下提交以儲存配置。然後，將證書配置檔案對映到BYOD策略集：



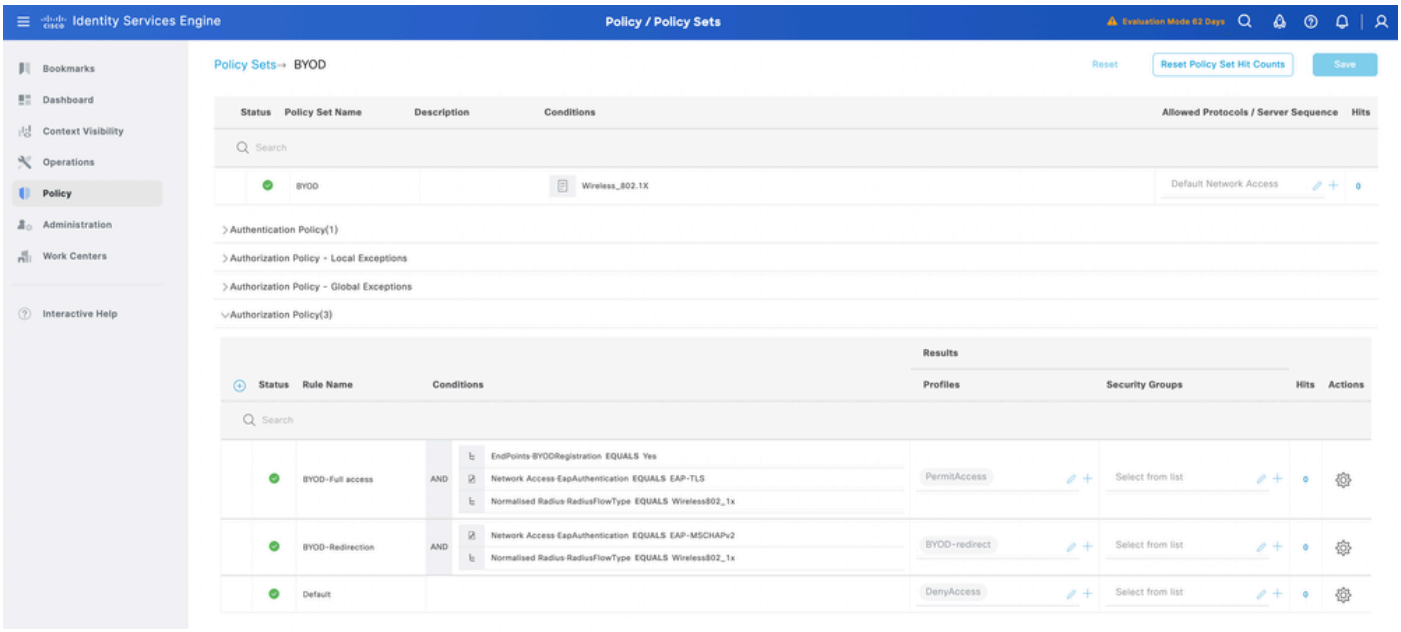
4.為BYOD重定向配置授權配置檔案，並在BYOD流程後進行完全訪問。導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。

5.按一下Add並建立授權配置檔案。檢查Web重定向(CWA、MDM、NSP、CPP)並對映BYOD門戶頁面。此外，將重新導向ACL名稱從WLC新增到設定檔中。對於Full access配置檔案，在配置檔案中配置相應的公司VLAN的允許訪問。



6.將授權配置檔案對映到授權規則。BYOD完全訪問必須使規則EndPoints·BYODegistration等於

yes，以便使用者在BYOD流之後獲得對網路的完全訪問許可權。

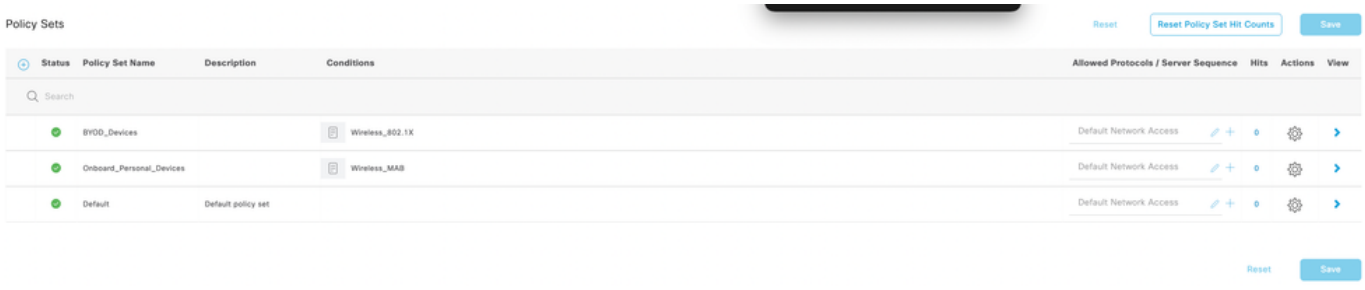


為雙SSID BYOD配置ISE策略集

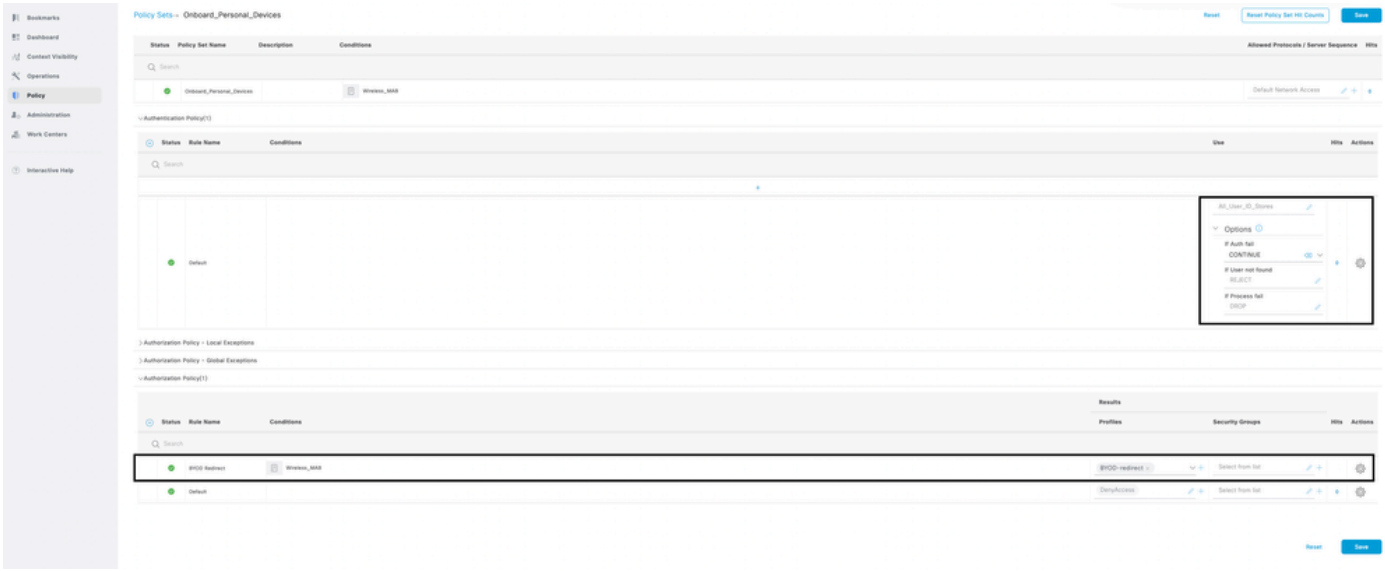
在雙SSID BYOD配置中，在ISE上配置雙策略集。第一個策略集針對開放/不安全SSID，其中策略集配置在連線到開放/不安全SSID時將使用者重定向到BYOD頁面

1. 導航到Policy > Policy Set，並在ISE上為BYOD流建立策略。

2.為開放/不安全SSID和公司SSID建立策略集，對ISE上的註冊BYOD使用者進行身份驗證。

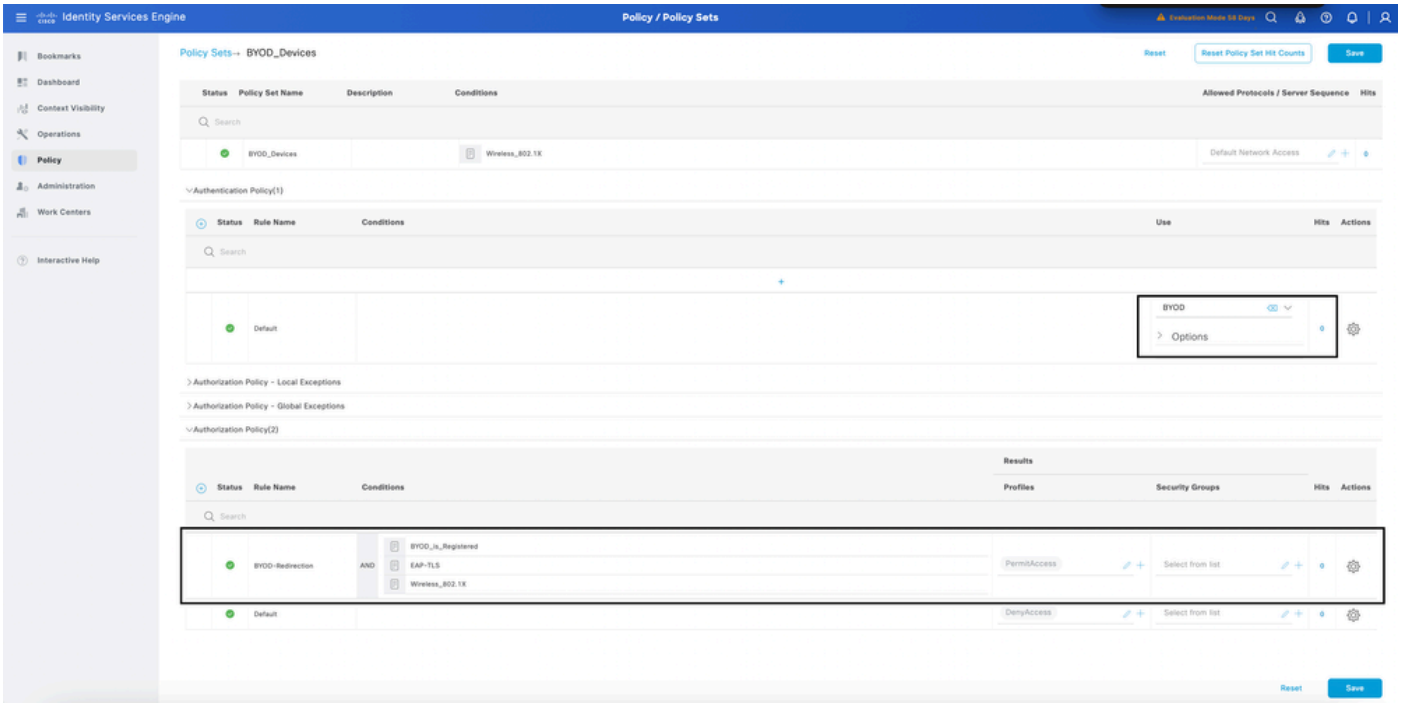


3.在「入職策略」集中，在選項下找到Continue選項。對於授權策略，建立條件並對映重定向授權配置檔案。建立授權配置檔案涉及相同的步驟，可在第4點中找到。



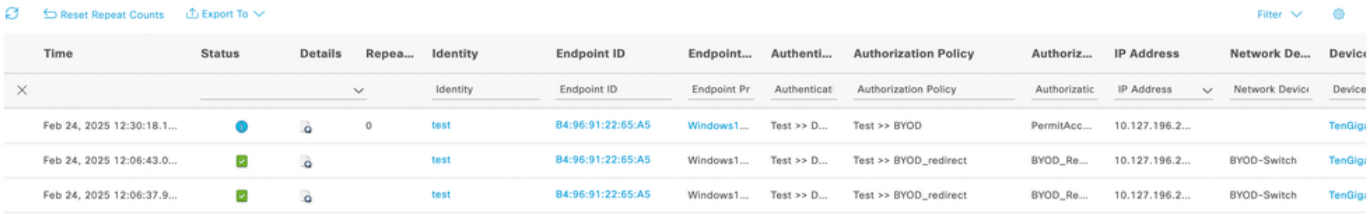
4.在BYOD註冊策略集中，使用找到的證書配置檔案配置身份驗證策略。

在第2點的為單SSID BYOD配置ISE策略集中。也為授權策略建立條件並將完整訪問配置檔案對映到策略。

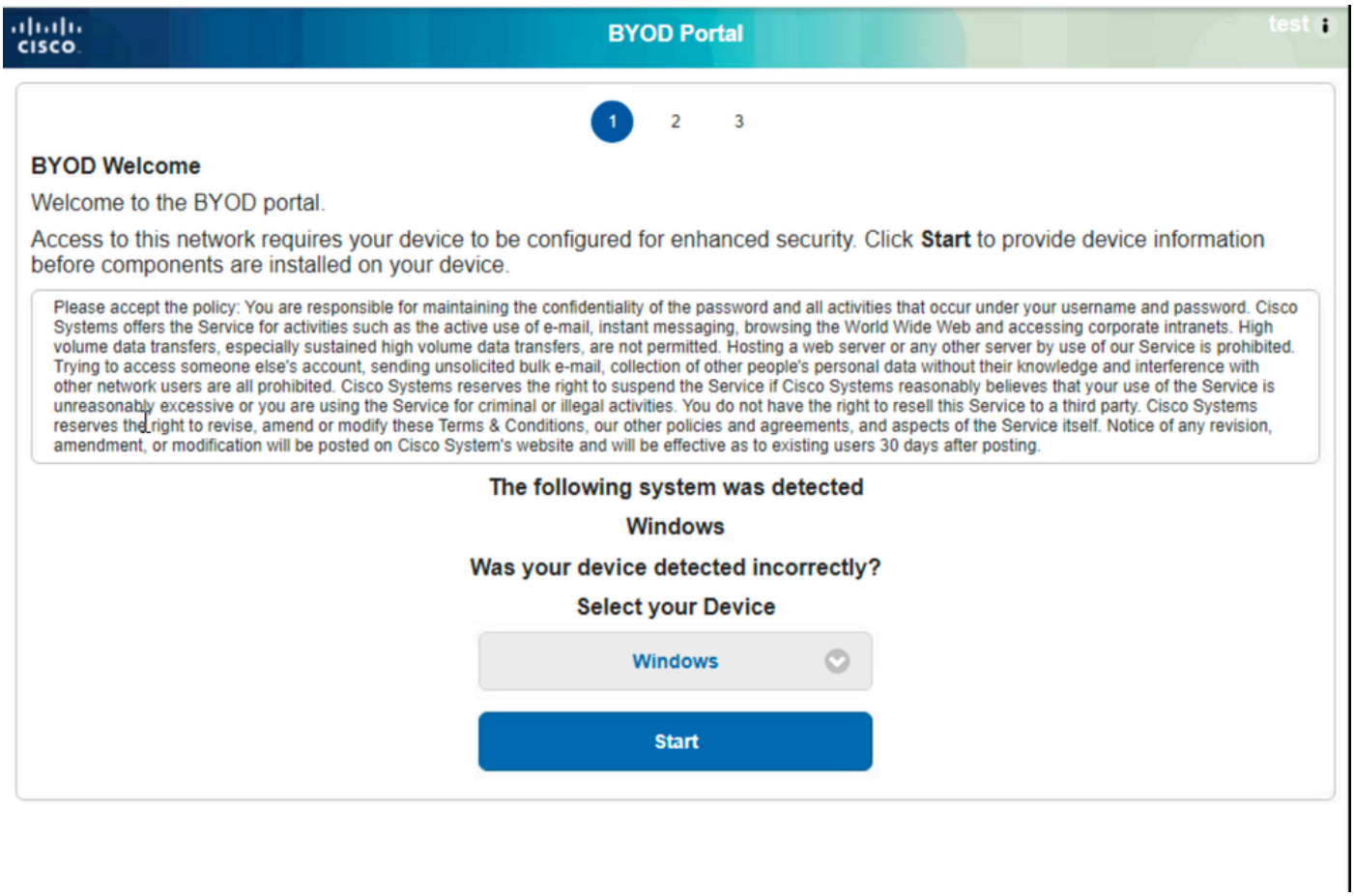


日誌記錄

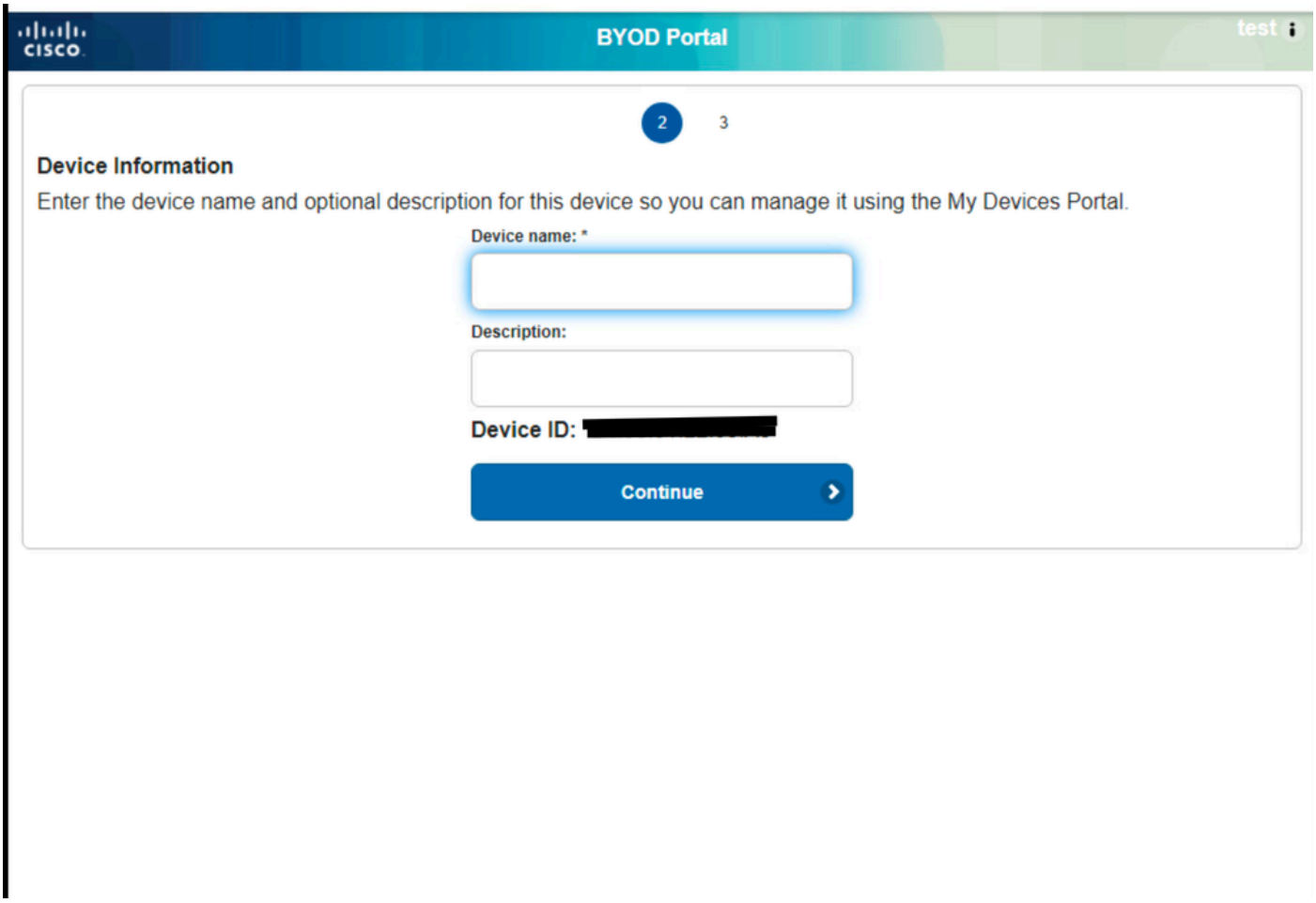
從ISE的即時日誌中，使用者身份驗證將成功，並將重定向到BYOD門戶頁面。完成BYOD流程後，使用者將被授予網路訪問許可權



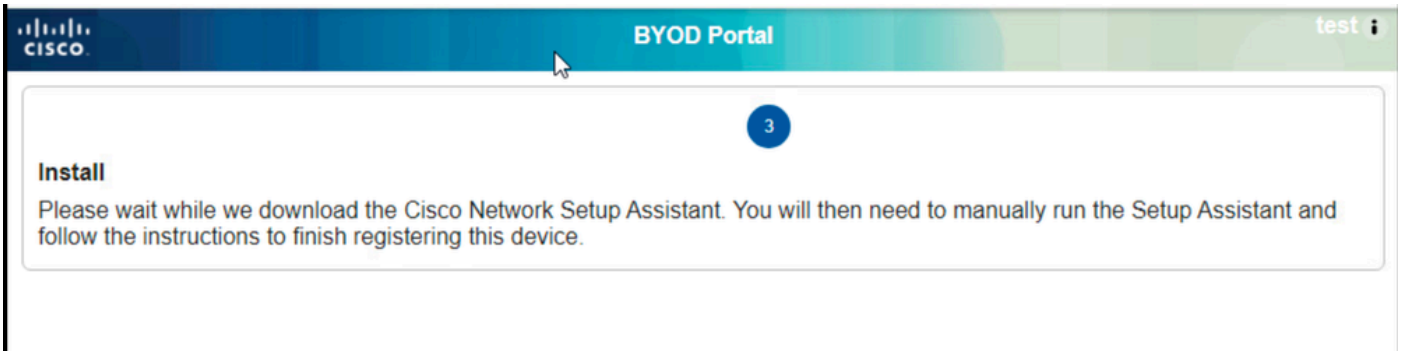
從使用者的角度來說，首先會將它們重定向到BYOD頁面，並且需要從網頁中選擇適當的裝置。為了測試使用Windows 10裝置



按一下「下一步」按鈕後，如果要求使用者輸入裝置的名稱和說明，則會將您引導到一個頁面

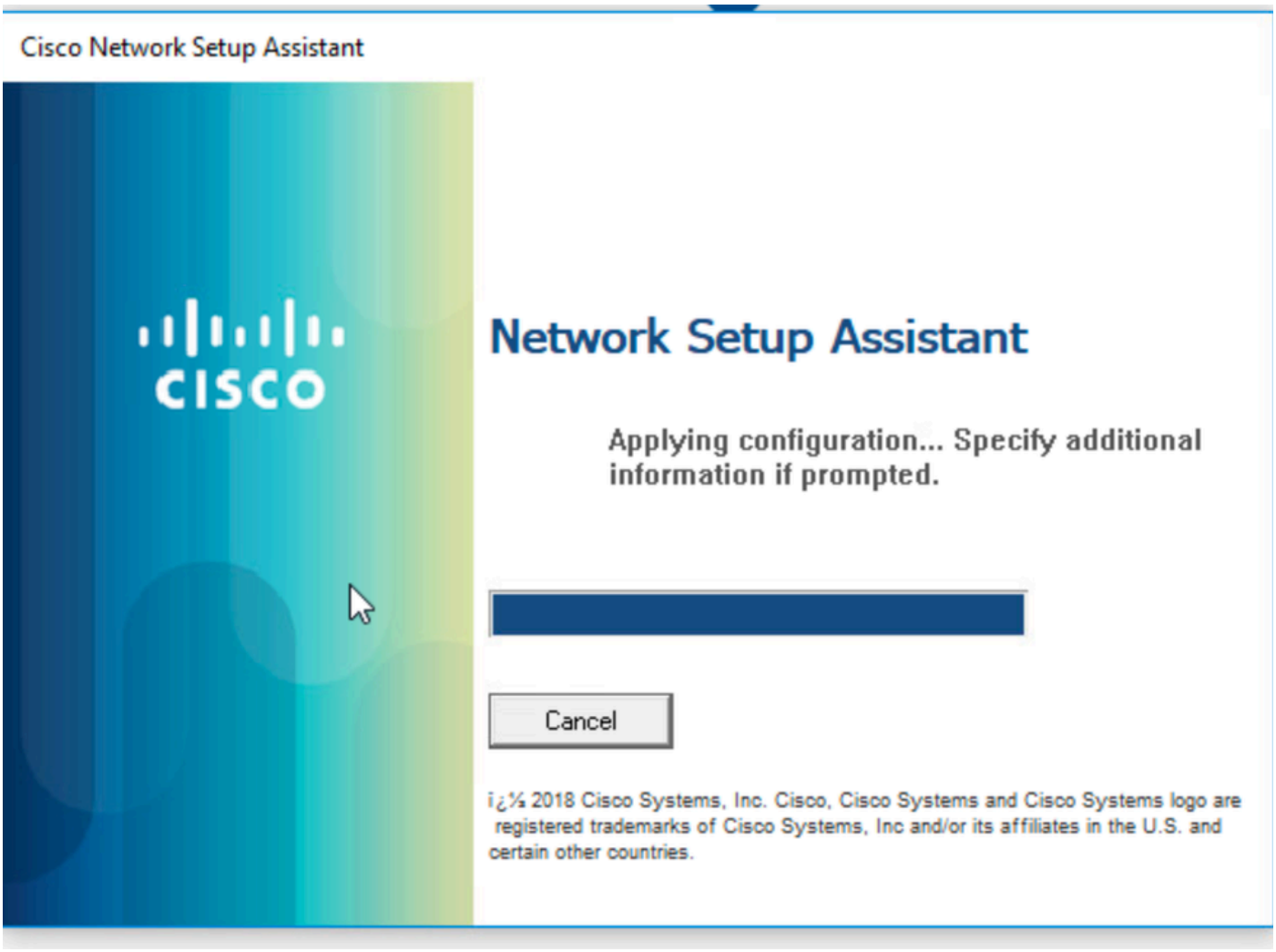


發佈消息，如果配置檔案配置為執行EAP-TLS身份驗證，則使用者將被請求下載Network Assistant工具以下載終端配置檔案和EAP TLS證書以進行身份驗證



以管理員許可權運行Network Assistant應用程式，然後按一下「開始」按鈕以啟動註冊流程：


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 2018 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 certain other countries.



使用者已使用個人裝置成功登入網路以訪問資源。

疑難排解

要解決BYOD問題，請在ISE上啟用此調試

要設定為調試級別的屬性：

- client(guest.log)
- client-webapp(guest.log)
- scep(ise-psc.log)
- ca服務(ise-psc.log)
- admin-ca(ise-psc.log)
- runtime-AAA(prrt-server.log)
- nsf(ise-psc.log)
- nsf-session(ise-psc.log)
- profiler(profiler.log)

日誌片段

訪客日誌

這些日誌表明使用者已成功重定向到該頁面並下載了Network Assistant應用程式：

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5:::::: — 在action-forwarding中找到的對映路徑：pages/byodWelcome.jsp // BYOD歡迎頁面
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- pTranSteps:1的大小
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep， pTranSteps:[id:d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep， stepTran:d2513b7b-722 9-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5:::: — 在操作轉發中找到的對映路徑，轉發到：pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- pTranSteps:1的大小
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep， pTranSteps:[id:f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep， stepTran:f203b8757-9e a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5:::: — 在操作轉發中找到的對映路徑，轉發到：pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::- Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::- portalSessionId =空
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-bbb91e8828da/NetworkSetupAssistant.exe //網路幫助應用程式已傳送到終結點

Ise-Psc日誌

當應用下載到終端時，應用會啟動SCEP流從ISE獲取客戶端證書。

2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore包含4個證書：
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=Certificate Services Root CA -
iseguest;serial=322815127387689606282525327846633020 89]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest;serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::- 3. '[issuer=CN=Certificate Services Root CA -
iseguest;serial=686276201605863086858498187751006982 24]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA -
iseguest;serial=729347676986030971539324822275488749 53]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 正在選擇加密證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 選擇具有keyEncipherment keyUsage的證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 找到1個具有keyEncipherment keyUsage的證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 使用[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest;serial=131900858749761727853768227590303808637]，用於消息加密
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 正在選擇驗證器證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 正在選擇具有數位簽章金鑰的證書用法
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 找到1個具有digitalSignature keyUsage的證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 使用[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest;serial=131900858749761727853768227590303808637]，用於消息驗證
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 選擇頒發者證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 選擇具有基本約束的證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 找到3個具有basicConstraints的證書
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 使用[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest;發行者的serial=131900858749761727853768227590303808637]
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- SCEP伺服器效能度量：name[live/dead， total

reqs， total failures， inflight reqs， Average RTT]
http://127.0.0.1:9444/caservice/scep[live，96444,1,0,120]

終端配置檔案下載

SCEP過程完成且終端安裝證書後，應用程式將下載終端配置檔案，以便將來由裝置執行身份驗證：

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::- Referrer = Windows //已基於網頁檢測到Windows裝置
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::: — 會話= 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::: — 會話= 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::: — 調配nsp配置檔案
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::: — 會話= 000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::- portalSessionId = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::- StreamingServlet URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml//NSP配置檔案已下載到終端
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::: — 流向ip:檔案型別：NativeSPProfile檔名：Cisco-ISE-NSP.xml //The Network Assistant Application
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- userId已設定為測試
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::: — 重定向型別是：SUCCESS_PAGE，重定向URL為：對於mac:

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）。