在Windows和ISE上配置單SSID無線BYOD

目錄

簡介

本文檔介紹如何使用單SSID和雙SSID在Windows電腦的Cisco身份服務引擎(ISE)上配置自帶裝置(BYOD)。

必要條件

需求

思科建議您瞭解以下主題：

- 思科ISE版本3.0的配置
- Cisco WLC的組態
- 自帶裝置工作

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.0
- Windows 10
- WLC和AP

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。

理論

在單SSID BYOD中，只有一個SSID用於兩台裝置並隨後授予對已註冊裝置的完全訪問許可權。首先，使用者使用使用者名稱和密碼(MSCHAPv2)連線到SSID。 在ISE上成功通過身份驗證後，使用者將被重定向到BYOD門戶。裝置註冊完成後，終端客戶端從ISE下載本地請求者助手(NSA)。NSA安裝在終端客戶端上，從ISE下載配置檔案和證書。NSA配置無線請求方，客戶端安裝證書。終端使用EAP-TLS使用下載的證書對同一個SSID執行另一個身份驗證。ISE檢查來自客戶端的新請求並驗證EAP方法和裝置註冊，並授予裝置的完全訪問許可權。

Windows BYOD單SSID步驟 —

- 初始EAP-MSCHAPv2身份驗證
- 重定向至BYOD門戶
- 裝置註冊
- NSA下載
- 配置檔案下載
- 證書下載
- EAP-TLS身份驗證

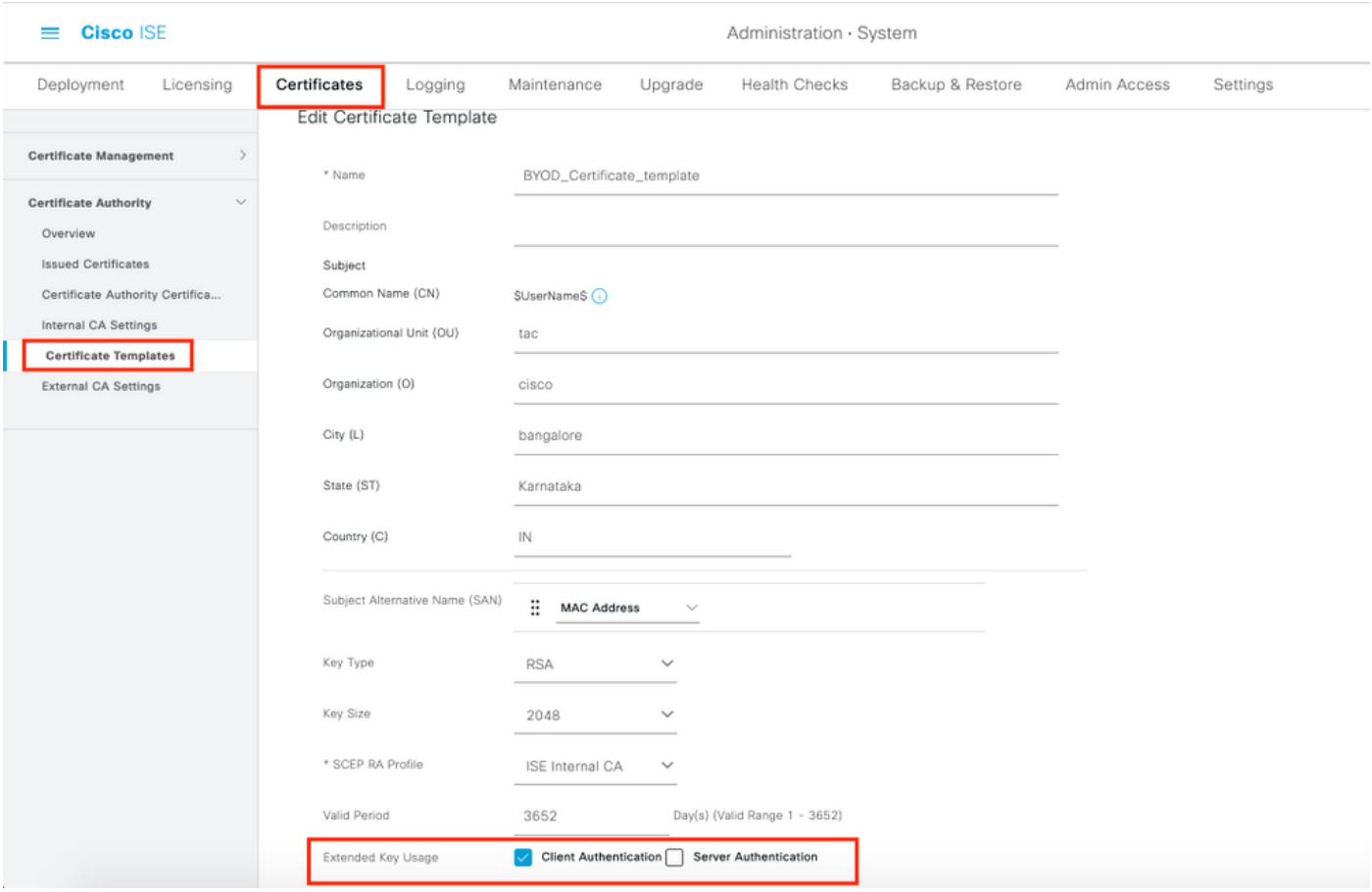
設定

ISE 組態

步驟1.在ISE上新增網路裝置並配置RADIUS和共用金鑰。

導航到**ISE >管理>網路裝置>新增網路裝置**。

步驟2.為BYOD使用者建立證書模板。模板必須具有Client Authentication Enhanced Key Usage。您可以使用預設的EAP_Certificate_Template。

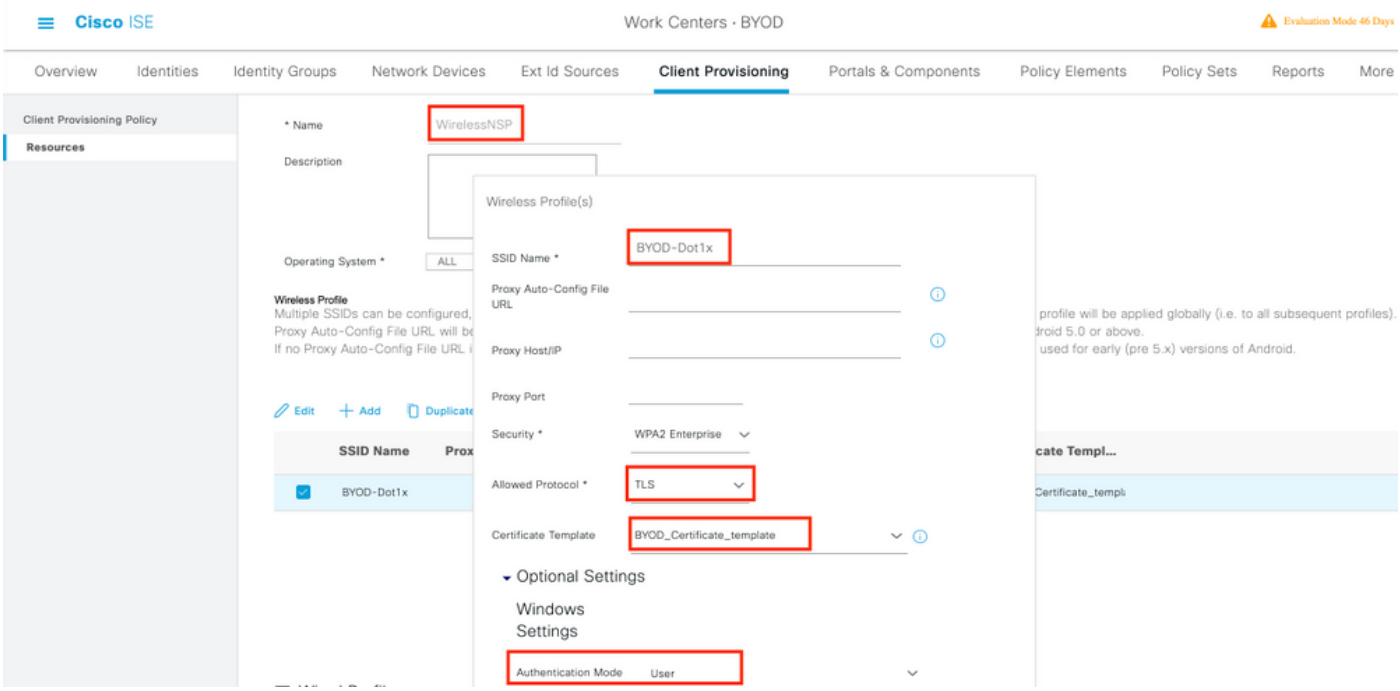


步驟3.為無線配置檔案建立本地請求方配置檔案。

導航到**ISE >工作中心> BYOD >客戶端調配**。按一下**Add**，然後從下拉選單中選擇**Native Supplicant Profile(NSP)**。

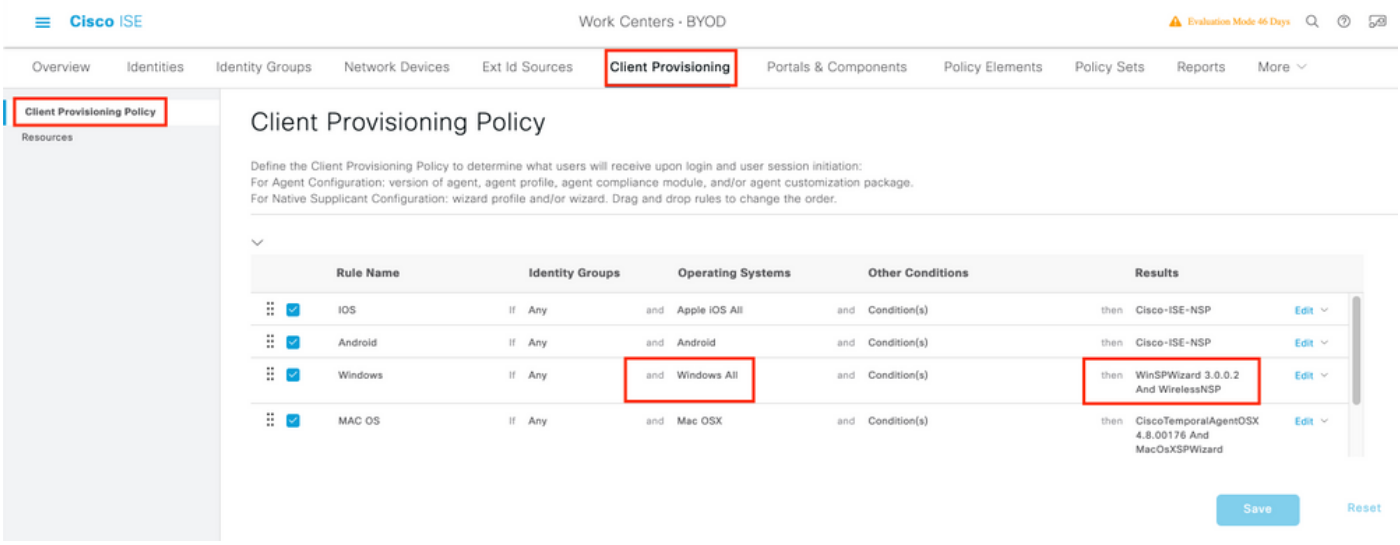
執行單SSID BYOD操作之前，此SSID名稱必須與您連線的名稱相同。選擇協定作為TLS。選擇在上一步中建立的證書模板，或者您可以使用預設的EAP_Certificate_Template。

在可選設定下，根據需要選擇使用者或使用者和電腦身份驗證。在本示例中，它配置為使用者身份驗證。將其他設定保留為預設值。



步驟4.為Windows裝置建立客戶端調配策略。

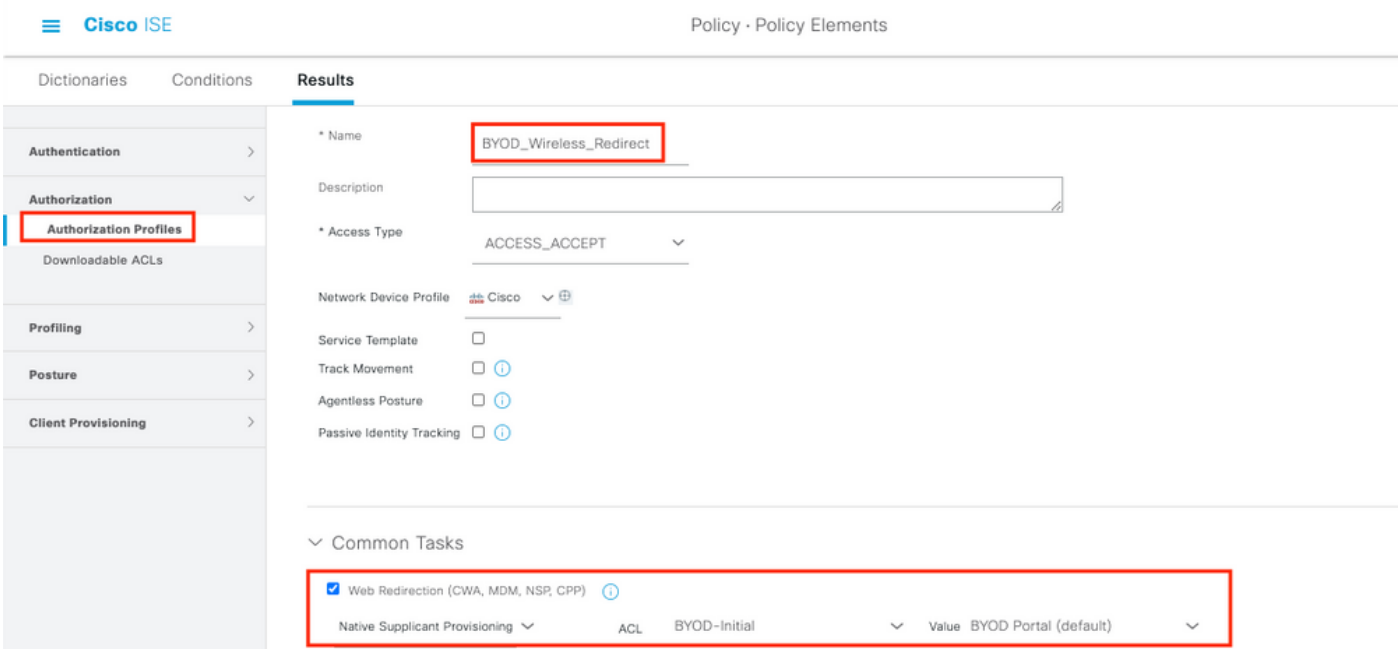
導航到**ISE >工作中心> BYOD >客戶端調配>客戶端調配策略**。選擇作業系統作為**Windows ALL**。選擇**WinSPWizard 3.0.0.2和上一步中建立的NSP**。



步驟5.為未註冊為BYOD裝置的裝置建立**授權配置檔案**。

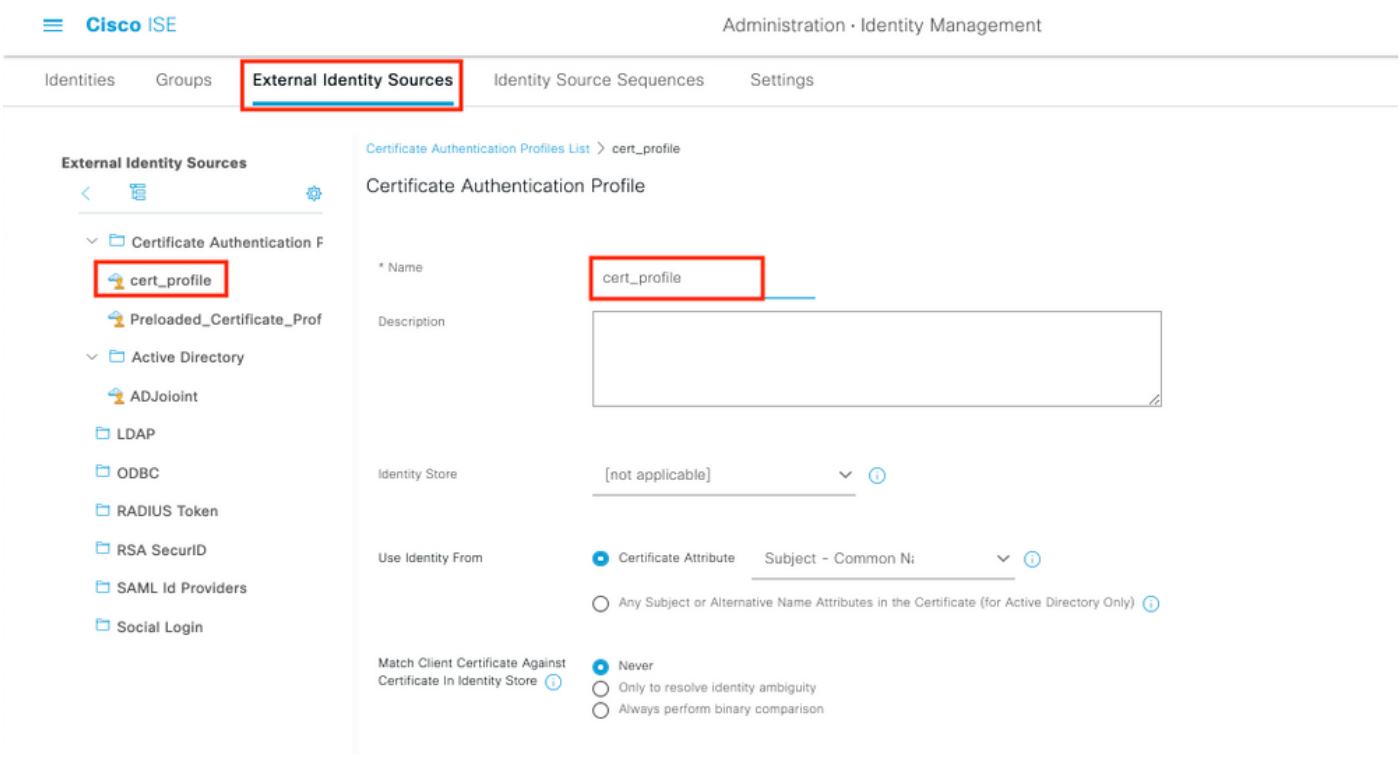
導航至**ISE > Policy > Policy Elements > Results> Authorization > Authorization Profiles > Add**。

在**Common Task**下，選擇**Native Supplicant Provisioning**。定義在WLC上建立的重定向ACL名稱並選擇BYOD門戶。此處使用預設門戶。您可以建立自定義BYOD門戶。導航到**ISE >工作中心> BYOD >門戶和**元件，然後點選**Add**。

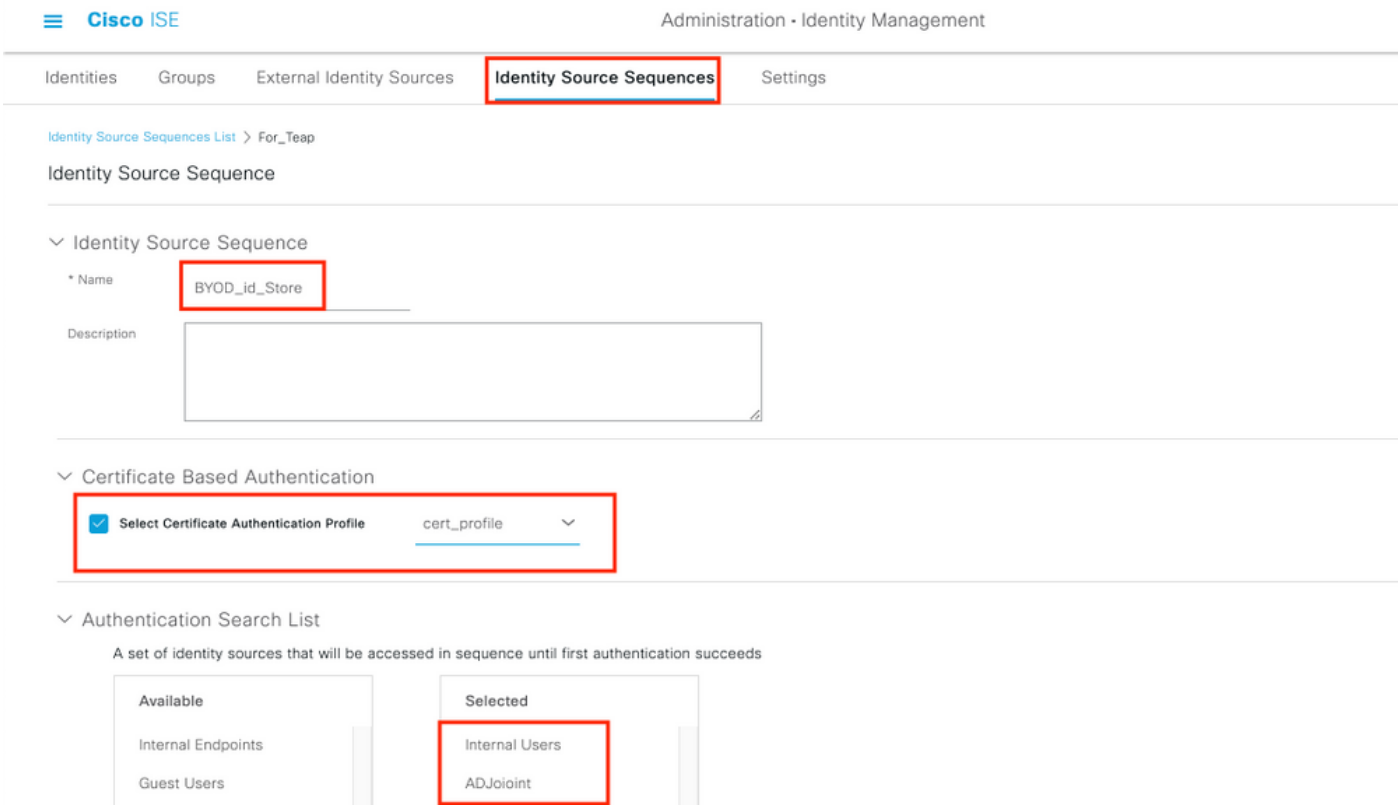


步驟6.建立證書配置檔案。

導航到**ISE >管理>外部身份源>證書配置檔案**。在此處建立新的證書配置檔案或使用預設證書配置檔案。



步驟7.建立身份源序列並選擇在上一步中建立的證書配置檔案或使用預設證書配置檔案。當使用者在BYOD註冊後執行EAP-TLS以獲得完全訪問許可權時，這是必需的。



步驟8.建立策略集、身份驗證策略和授權策略。

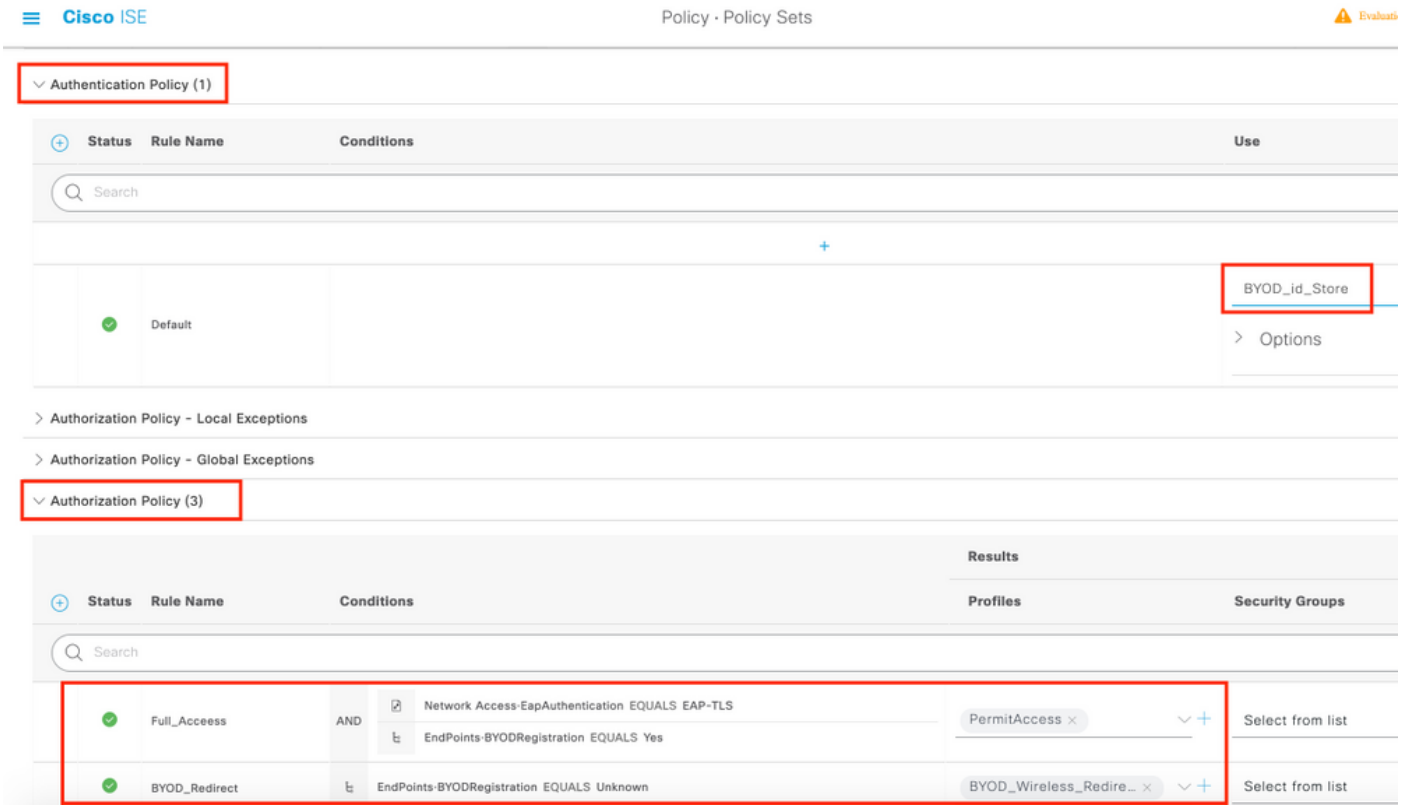
導航到**ISE > Policy > Policy Sets**。建立策略集並**儲存**。

建立身份驗證策略並選擇在上一步中建立的身份源序列。

建立授權策略。您必須建立兩個策略。

1.對於未註冊BYOD的裝置。提供在步驟5中建立的重定向配置檔案。

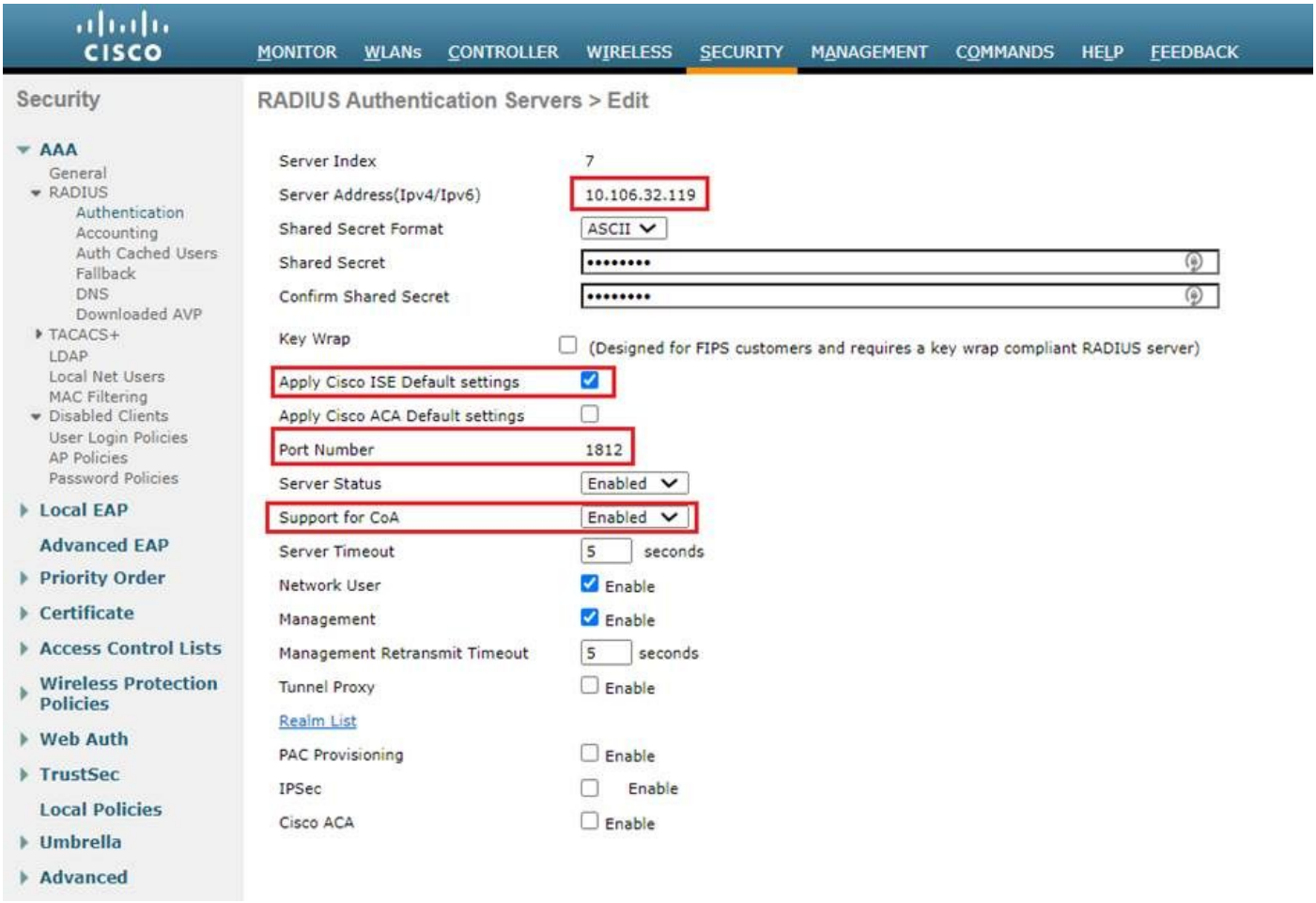
2.已註冊BYOD並執行EAP-TLS的裝置。授予對這些裝置的完全訪問許可權。



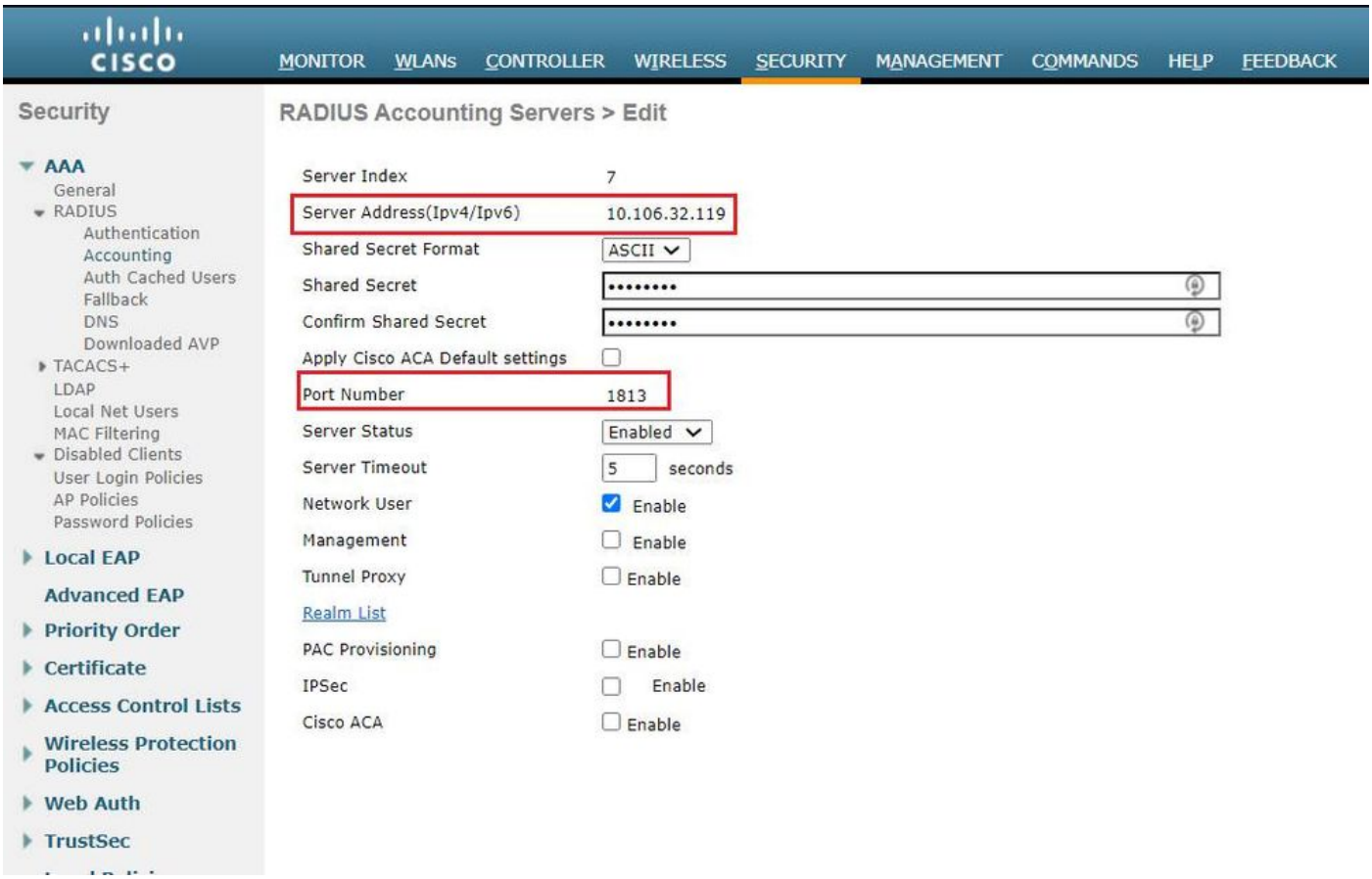
WLC組態

步驟1.在WLC上設定Radius伺服器。

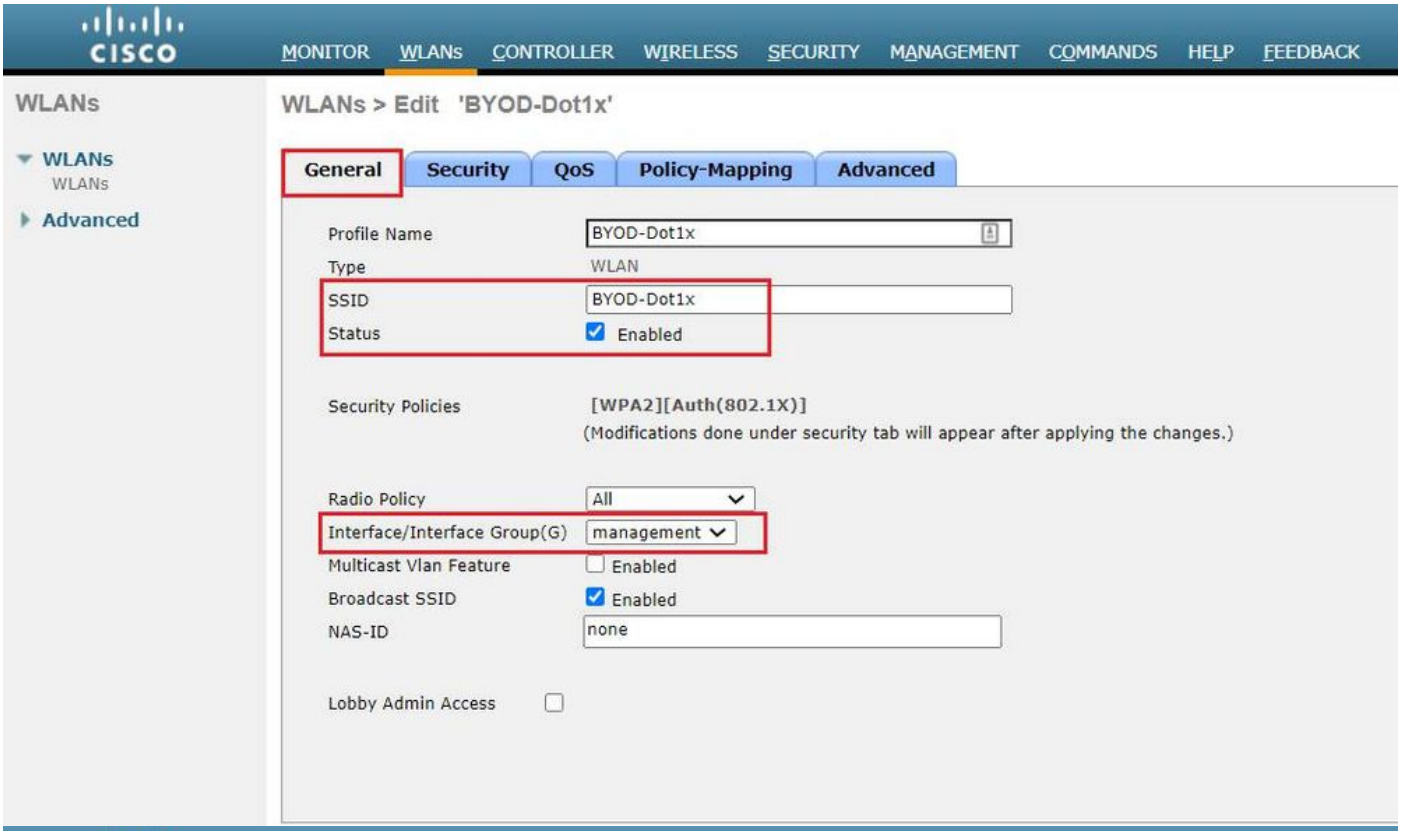
導覽至**Security > AAA > Radius > Authentication**。

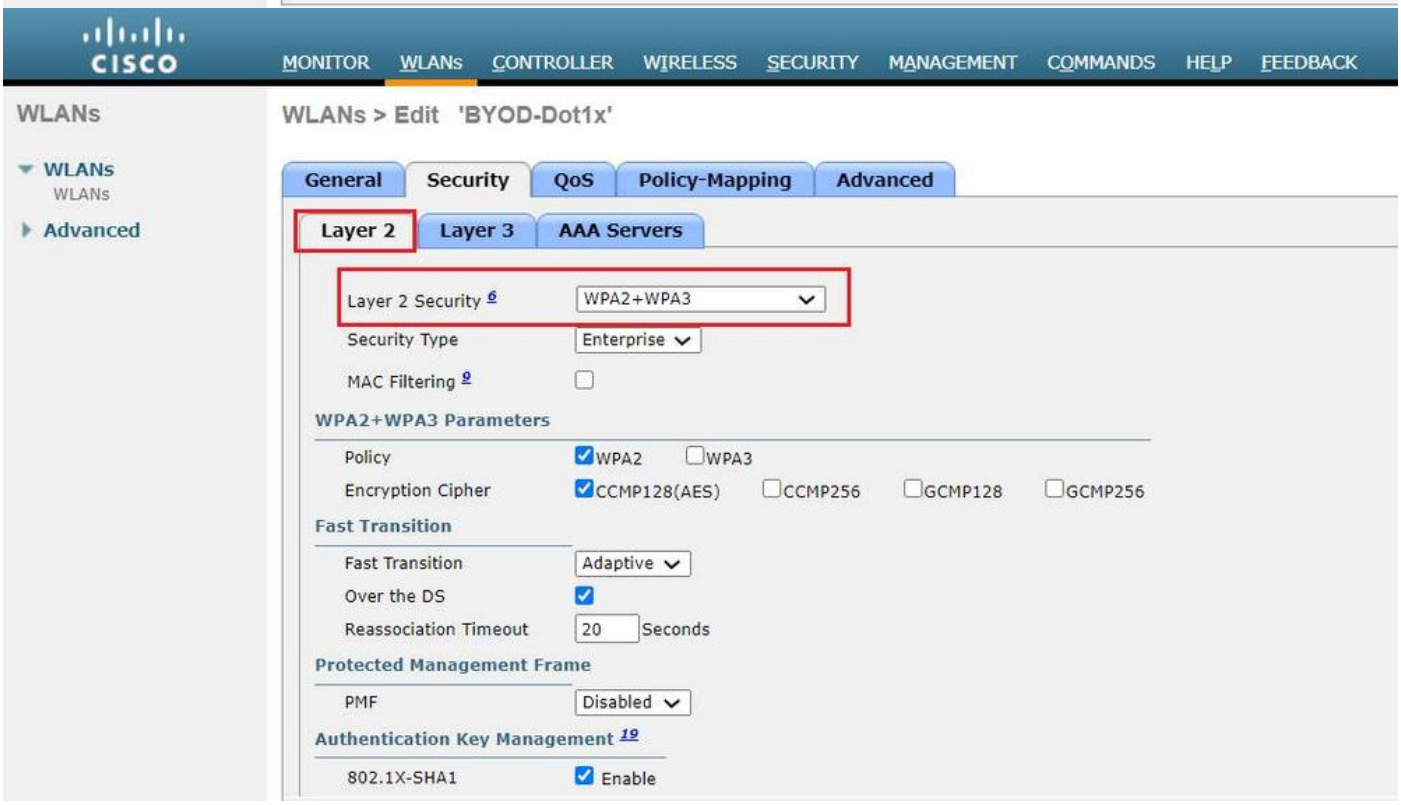


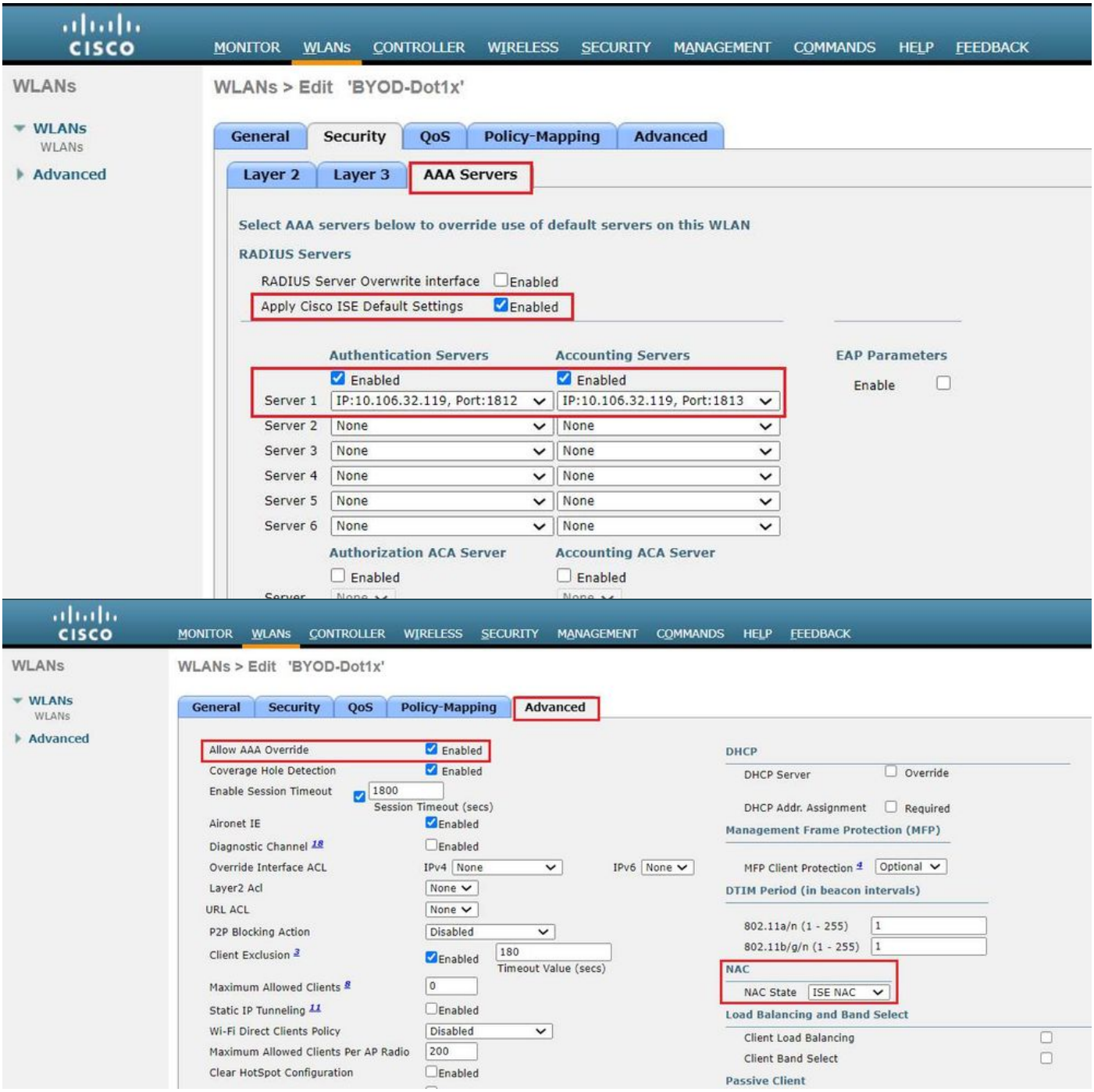
導覽至Security > AAA > Radius > Accounting。



步驟2.配置Dot1x SSID。


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'BYOD-Dot1x'
General Security QoS Policy-Mapping Advanced
Profile Name BYOD-Dot1x
Type WLAN
SSID BYOD-Dot1x
Status Enabled
Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface/Interface Group(G) management
Multicast Vlan Feature Enabled
Broadcast SSID Enabled
NAS-ID none
Lobby Admin Access

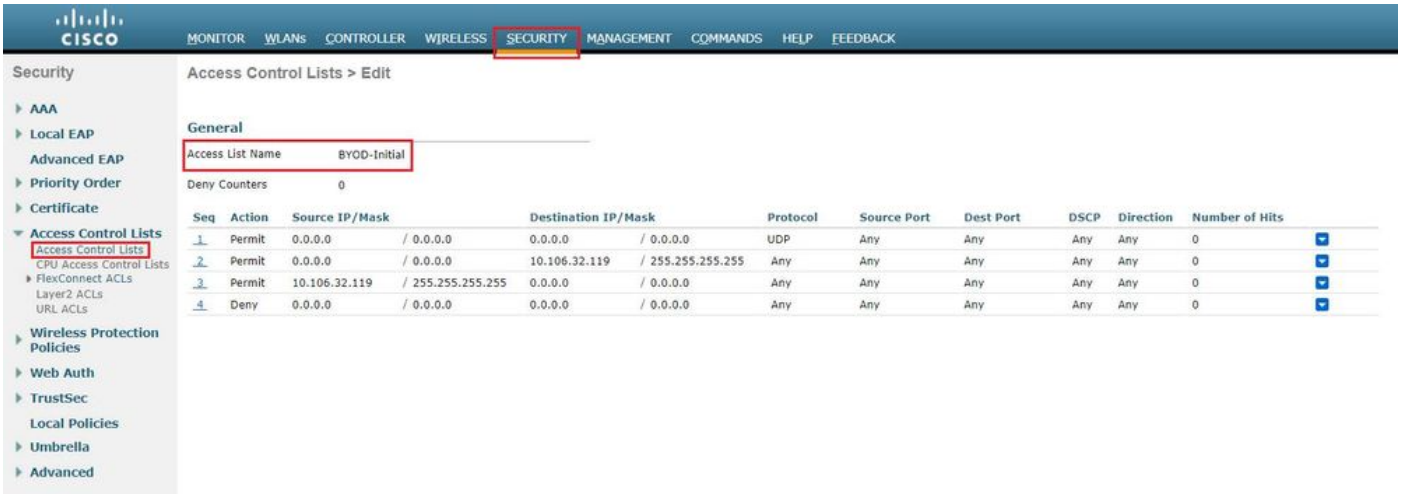

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'BYOD-Dot1x'
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security WPA2+WPA3
Security Type Enterprise
MAC Filtering
WPA2+WPA3 Parameters
Policy WPA2 WPA3
Encryption Cipher CCMP128(AES) CCMP256 GCMP128 GCMP256
Fast Transition
Fast Transition Adaptive
Over the DS
Reassociation Timeout 20 Seconds
Protected Management Frame
PMF Disabled
Authentication Key Management
802.1X-SHA1 Enable



步驟3.配置重定向ACL以提供有限的裝置調配訪問許可權。

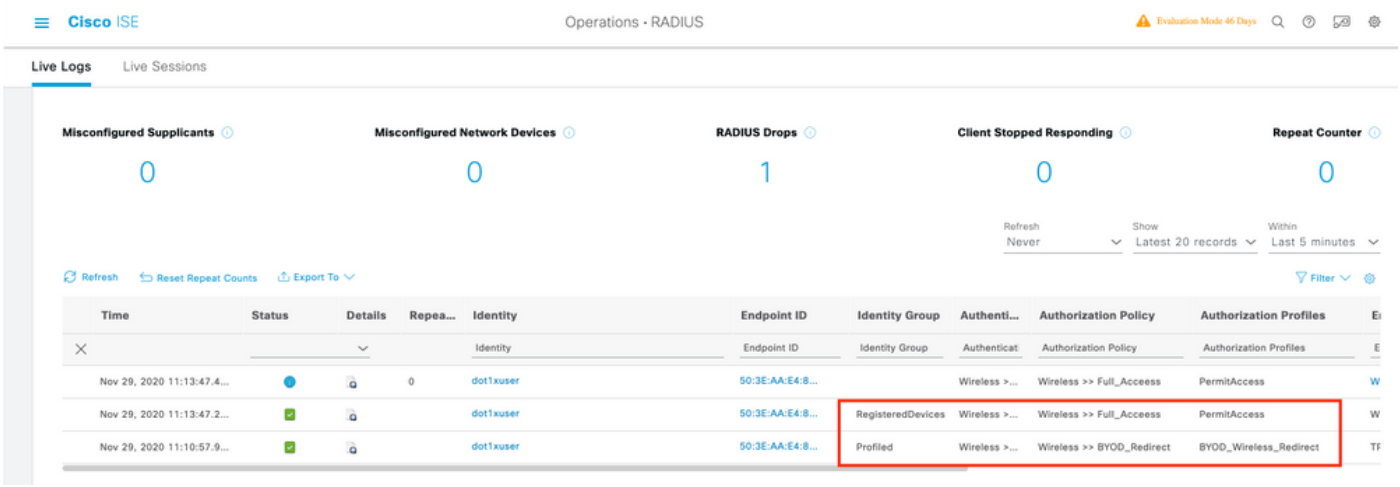
- 允許到DHCP和DNS的UDP流量（預設情況下允許DHCP）。
- 與ISE通訊。
- 拒絕其他流量。

名稱:BYOD-Initial（或在授權配置檔案中手動命名ACL的任何裝置）



驗證

驗證流程驗證

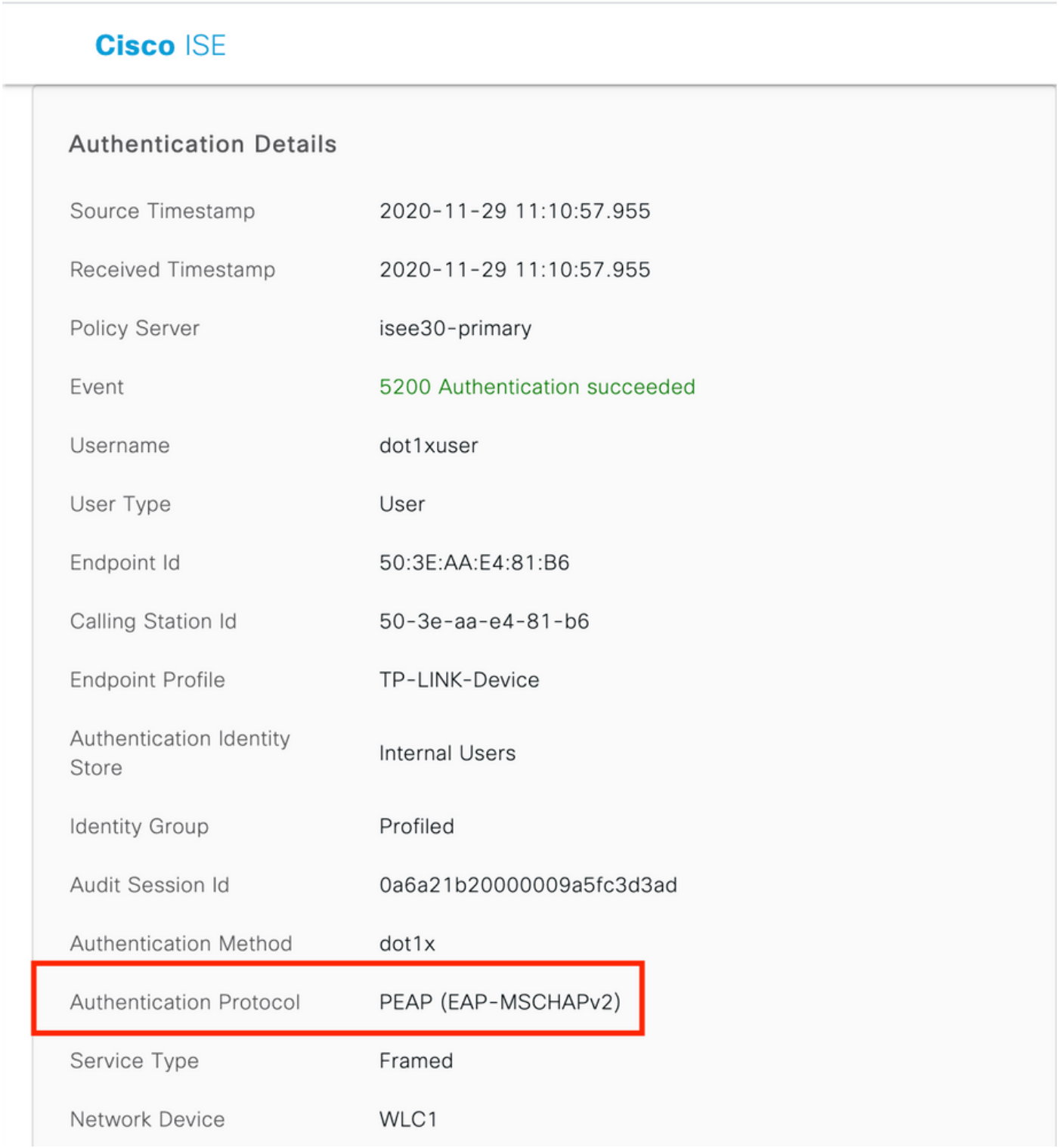


1.首次登入時，使用者使用使用者名稱和密碼執行PEAP身份驗證。在ISE上，使用者點選重定向規則BYOD-Redirect。

Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	TP-LINK-Device
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> BYOD_Redirect
Authorization Result	BYOD_Wireless_Redirect

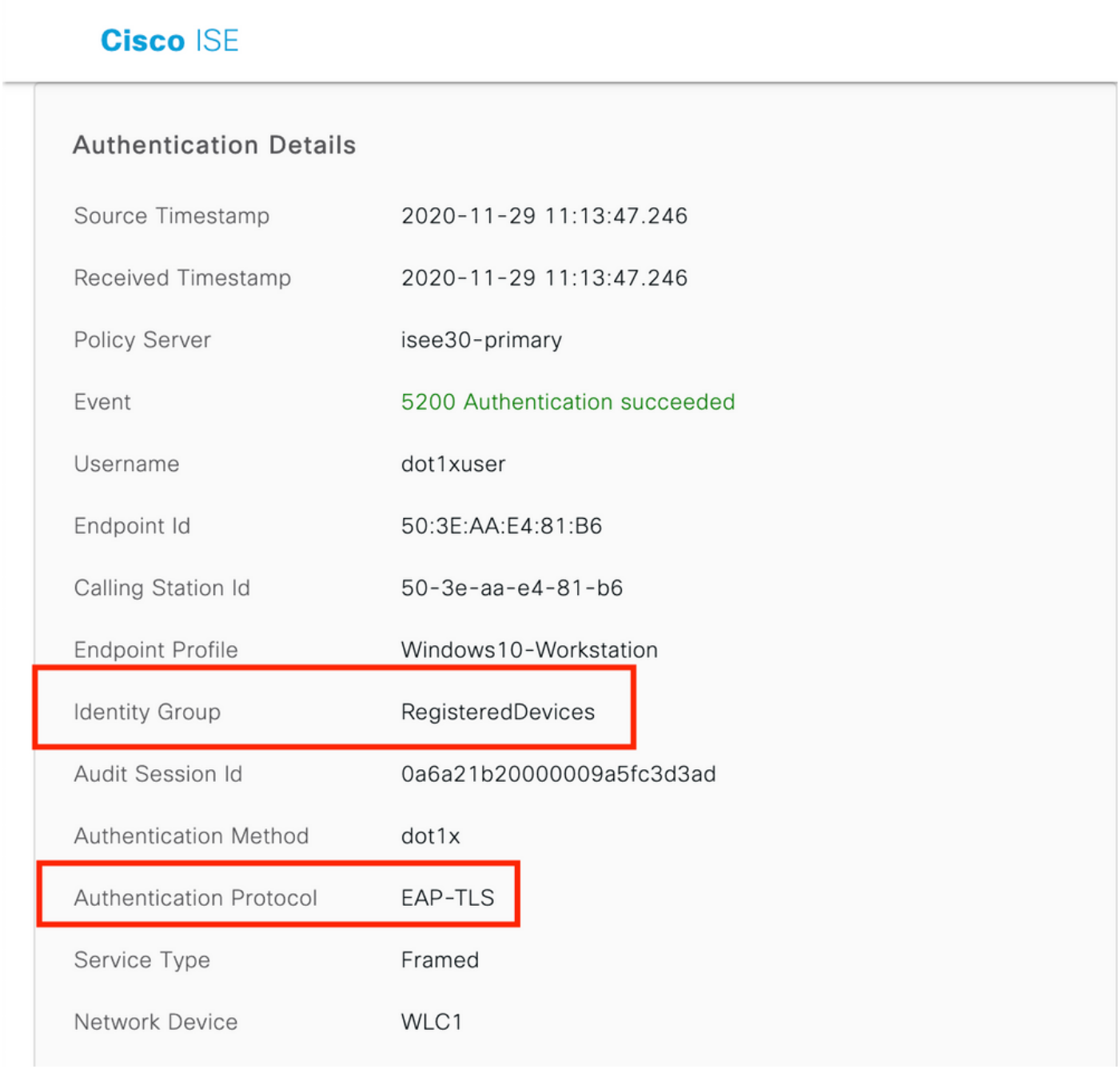


2.在BYOD註冊後，使用者被新增到註冊裝置，現在執行EAP-TLS並獲得完全訪問許可權。

Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	Windows10-Workstation
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> Full_Acceess
Authorization Result	PermitAccess

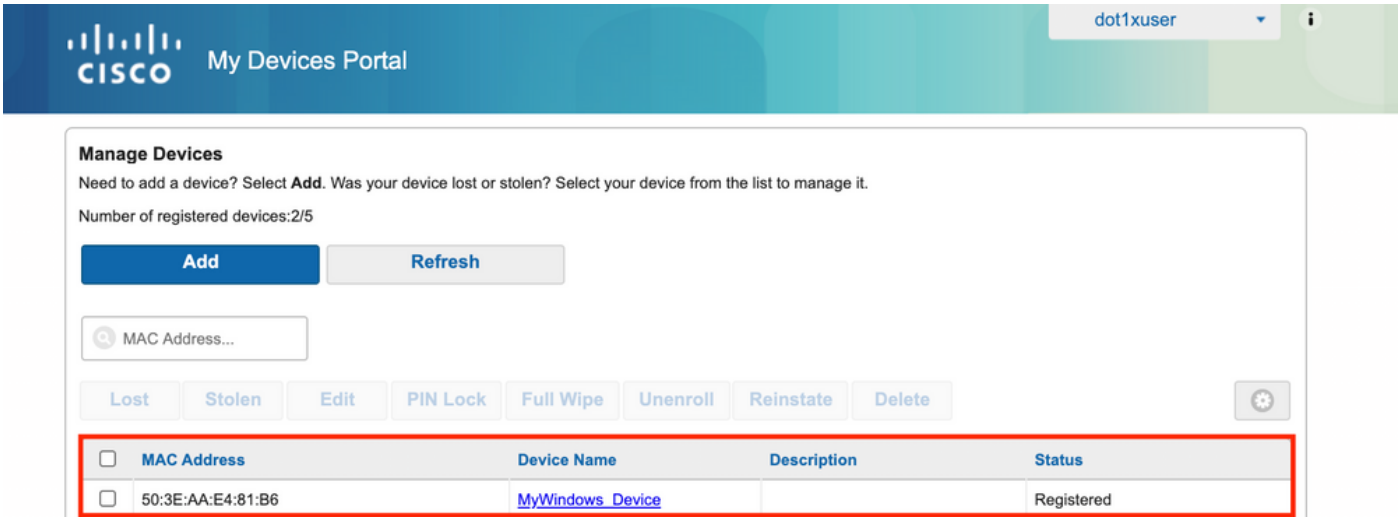


檢查我的裝置門戶

導航到MyDevices Portal並使用憑證登入。 您可以看到裝置名稱和註冊狀態。

您可以為MyDevices門戶建立URL。

導航到**ISE >工作中心> BYOD >門戶和元件>我的裝置門戶>登入設定**，然後輸入完全限定的URL。



疑難排解

一般資訊

對於BYOD流程，必須在PSN節點上的調試中啟用這些ISE元件 —

scep - scep日誌消息。目標日**志filesguest.log和ise-psc.log**。

client-webapp -負責基礎設施消息的元件。目標日誌檔案**-ise-psc.log**

portal-web-action — 負責客戶端調配策略處理的元件。目標日誌檔案**-guest.log**。

portal — 所有門戶相關事件。目標日誌檔案**-guest.log**

portal-session-manager — 目標日志檔案 — 門戶會**話相關的調試消息 — gues.log**

ca-service- ca-service messages — 目標日誌檔案 — **caservice.log和caservice-misc.log**

ca-service-cert- ca-service certificate messages — 目標日誌檔案 — **caservice.log和caservice-misc.log**

admin-ca- ca-service admin messages — 目標日誌檔案**ise-psc.log、caservice.log和casrvice-misc.log**

certprovisioningportal — 證書調配門戶消息 — 目**標日誌檔案ise-psc.log**

nsf- NSF相關消息 — 目標日誌**檔案ise-psc.log**

nsf-session — 會話快取相關的消息 — 目標日誌**檔案ise-psc.log**

運行時 — AAA — 所有運行時事件。目標日誌檔案**-prrt-server.log**。

對於客戶端日誌：

查詢%temp%\spwProfileLog.txt(例如
：C:\Users\<username>\AppData\Local\Temp\spwProfileLog.txt)

工作日誌分析

ISE日誌

Initial Access-Accept with redirect ACL和Redirect URL for BYOD Portal。

Prrt-server.log-

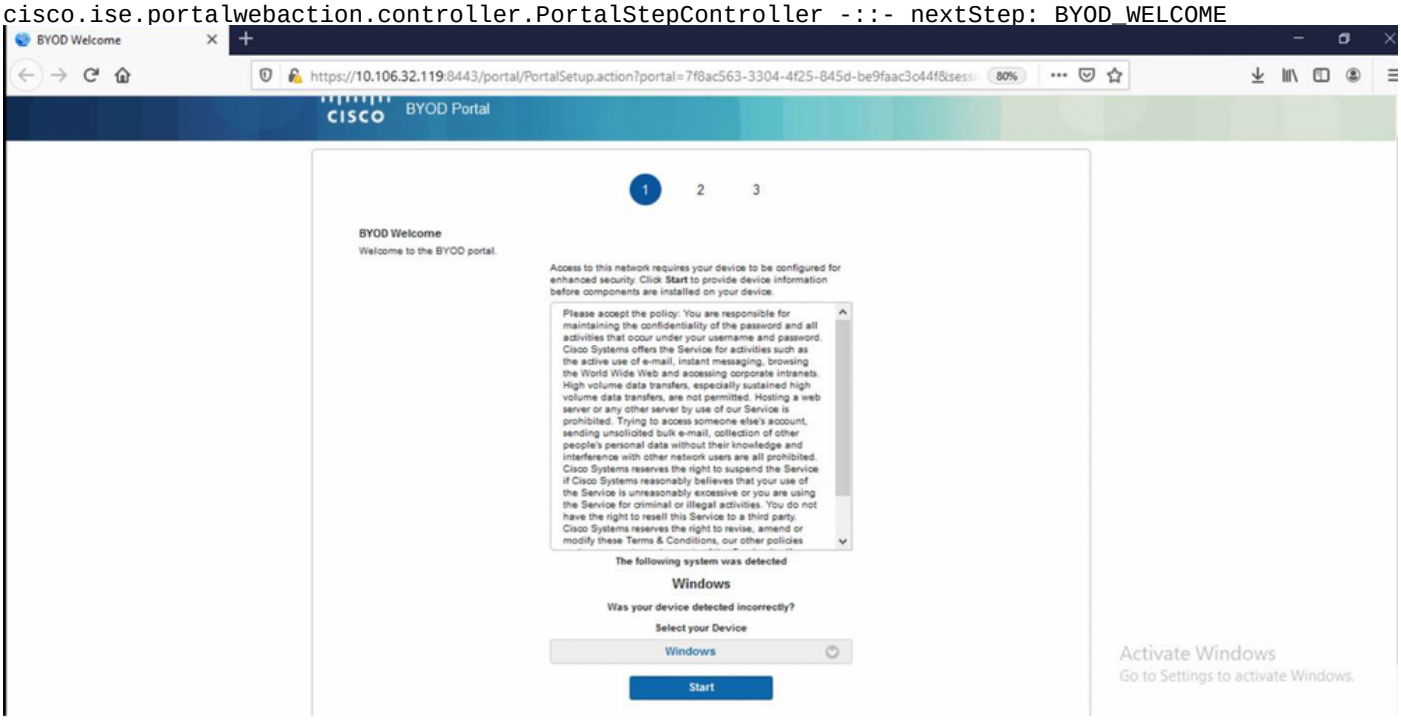
```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-
primary/392215758/699,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -
value: [dot1xuser] [25] Class - value: [****] [79] EAP-Message - value: [ñ [80] Message-
Authenticator - value: [.2{wëbÙ¨ÅþO5‹Z] [26] cisco-av-pair - value: [url-redirect-acl=BYOD-
Initial] [26] cisco-av-pair - value: [url-
redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009f5fc770c7&portal=7f8
ac563-3304-4f25-845d-be9faac3c44f&action=nsp&token=53a2119de6893df6c6fca25c8d6bd061] [26] MS-
MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

當終端使用者嘗試導航到網站並被WLC重定向到ISE重定向URL時。

Guest.log -

```
2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
com.cisco.ise.portal.Gateway -::- Gateway Params (after update):
redirect=www.msftconnecttest.com/redirect client_mac=null daysToExpiry=null ap_mac=null
switch_url=null wlan=null action=nsp sessionId=0a6a21b20000009f5fc770c7 portal=7f8ac563-3304-
4f25-845d-be9faac3c44f isExpired=null token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02
05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- sessionId=0a6a21b20000009f5fc770c7 :
token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- Session
token successfully validated. 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-5][] cisco.ise.portal.util.PortalUtils -::- UserAgent : Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portal.util.PortalUtils -::- isMozilla: true 2020-12-02
05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gateway -
::- url: /portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-
be9faac3c44f&sessionId=0a6a21b20000009f5fc770c7&action=nsp&redirect=www.msftconnecttest.com%2Fre
direct 2020-12-02 05:43:58,355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -::- start guest flow interceptor...
2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Executing action PortalSetup via request
/portal/PortalSetup.action 2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.actions.PortalSetupAction -::- executeAction... 2020-12-02
05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Result from action, PortalSetup: success
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Action PortalSetup Complete for request
/portal/PortalSetup.action 2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- Current flow step:
INIT, otherInfo=id: 226ea25b-5e45-43f5-b79d-fb59cab96def 2020-12-02 05:43:58,361 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- Getting
next flow step for INIT with TranEnum=PROCEED 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- StepTran for
Step=INIT=> tranEnum=PROCEED, toStep=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- Find Next
Step=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Step : BYOD_WELCOME will be visible! 2020-12-
02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
```

```
cpm.guestaccess.flowmanager.step.StepExecutor -::- Returning next step =BYOD_WELCOME 2020-12-02
05:43:58,362 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -::- Looking up Guest user with
uniqueSubjectId=5f5592a4f67552b855ecc56160112db42cf7074e 2020-12-02 05:43:58,365 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -::- Found Guest user 'dot1xuserin
DB using uniqueSubjectID '5f5592a4f67552b855ecc56160112db42cf7074e'. authStoreName in
DB=Internal Users, authStoreGUID in DB=9273fe30-8c01-11e6-996c-525400b48521. DB ID=bab8f27d-
c44a-48f5-9fe4-5187047bffc0 2020-12-02 05:43:58,366 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.controller.PortalStepController -::- ++++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is INITIATED and current step
is BYOD_WELCOME 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][]
com.cisco.ise.portalSessionManager.PortalSession -::- Setting the portal session state to ACTIVE
2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][]
cisco.ise.portalwebaction.controller.PortalStepController -::- nextStep: BYOD_WELCOME
```



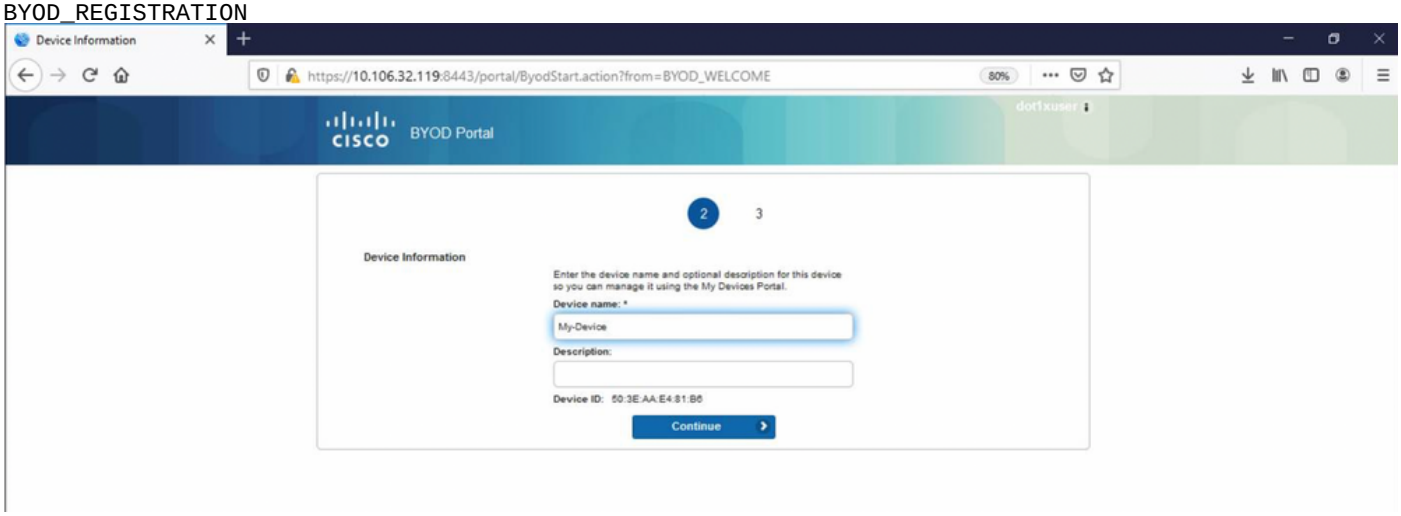
在BYOD歡迎頁面上按一下**Start**。

```
020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodStart via
request /portal/ByodStart.action 2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalPreResultListener -:dot1xuser:-
currentStep: BYOD_WELCOME
```

此時，ISE評估是否存在BYOD所需的必要檔案/資源，並將自身設定為BYOD INIT狀態。

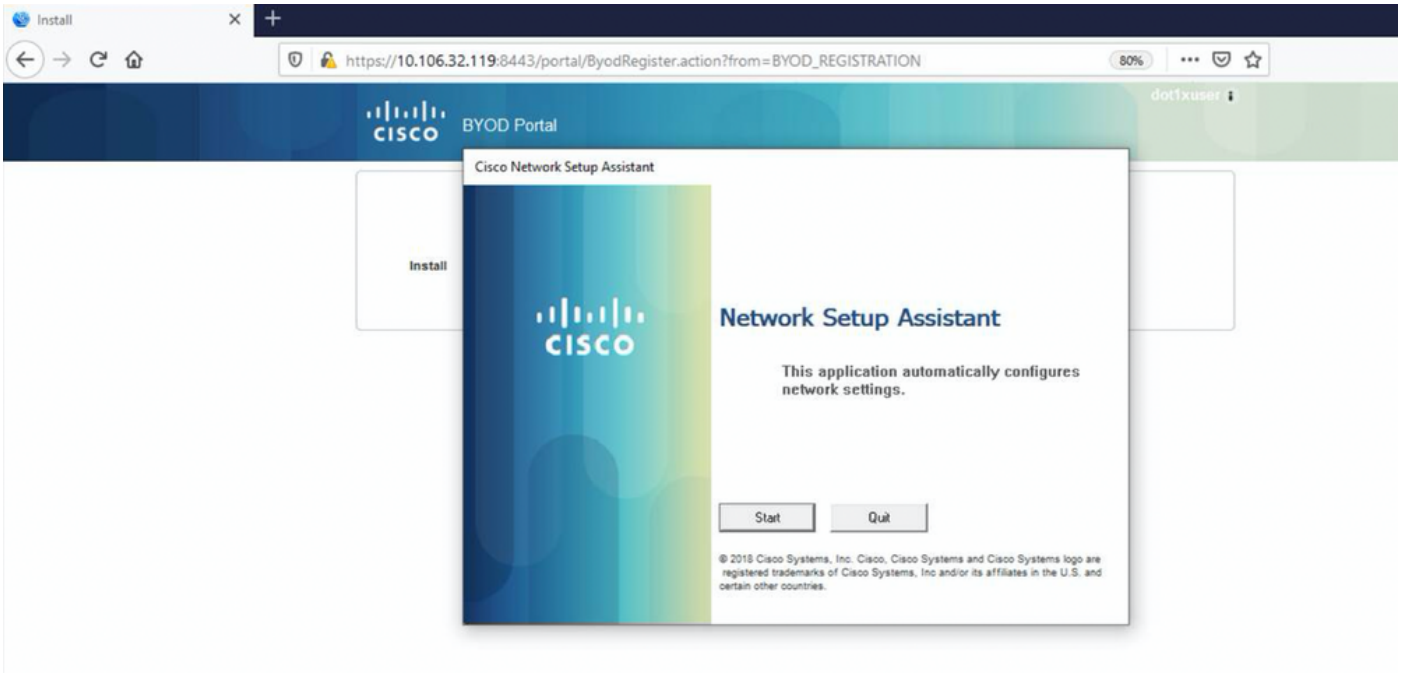
```
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- NSP Downloadalble
Resource data=>, resource=DownloadableResourceInfo :WINDOWS_10_ALL
https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009f5fc770c7&os=WINDOWS_10_ALL null null
https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/ null
null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-
81141ec42d2d/NetworkSetupAssistant.exe, coaType=NoCoa 2020-12-02 05:44:01,936 DEBUG [https-jsse-
nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.utils.NSPProvAccess -:dot1xuser:-
It is a WIN/MAC! 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
```

cpm.guestaccess.flowmanager.step.StepExecutor -:dot1xuser:- Returning next step =BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++ updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- nextStep: BYOD_REGISTRATION



輸入裝置名稱，然後按一下註冊。

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodRegister via request /portal/ByodRegister.action Request Parameters: from=BYOD_REGISTRATION token=PZBMFBHX3FBPXT8QF98U717ILNOTD68D device.name=My-Device device.description= 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portal.actions.ByodRegisterAction -:dot1xuser:- executeAction... 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Result from action, ByodRegister: success 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Action ByodRegister Complete for request /portal/ByodRegister.action 2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices.mydevices.MyDevicesServiceImpl -:dot1xuser:- Register Device : 50:3E:AA:E4:81:B6 username= dot1xuser idGroupID= aa13bb40-8bff-11e6-996c-525400b48521 authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521 nadAddress= 10.106.33.178 isSameDeviceRegistered = false 2020-12-02 05:44:14,900 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager.step.StepExecutor -:dot1xuser:- Returning next step =BYOD_INSTALL 2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++ updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is BYOD_INSTALL 2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:dot1xuser:- result: success 2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe

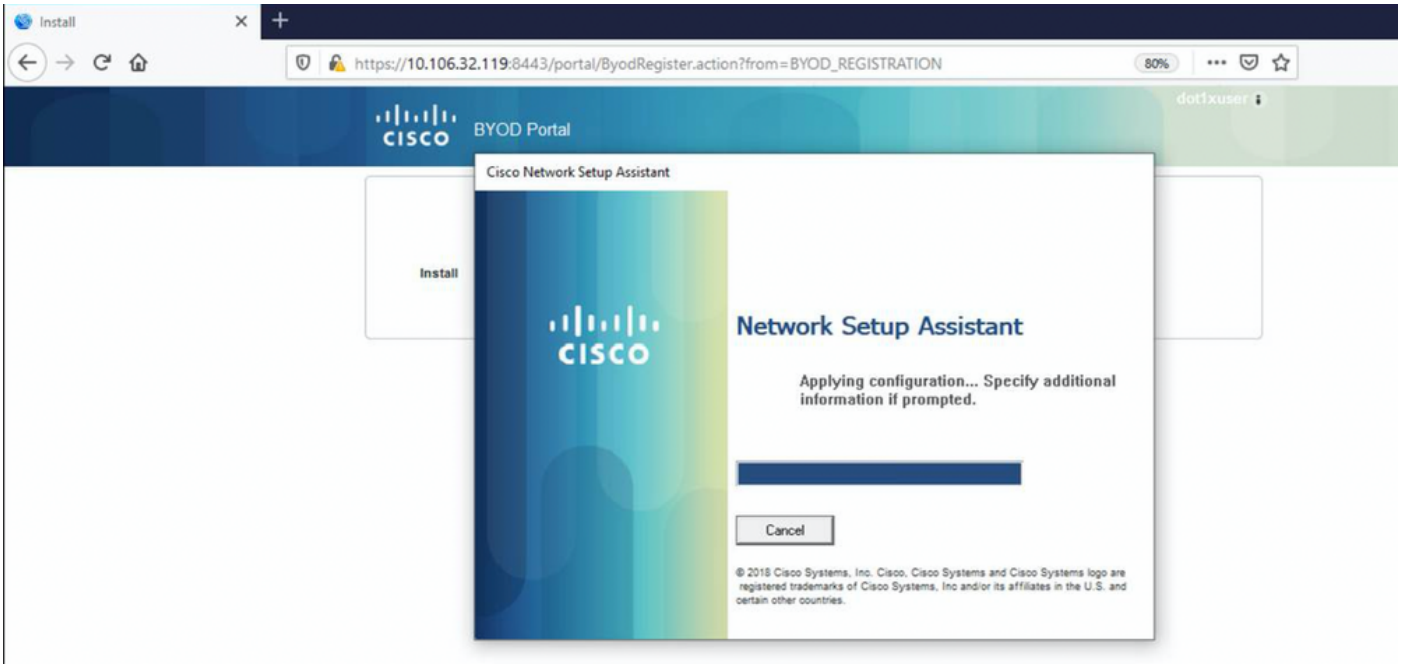


現在，當使用者在NSA上按一下「開始」時，會在客戶端上臨時建立名為**spwProfile.xml**的檔案，該檔案會複製在TCP埠8905上下載的Cisco-ISE-NSP.xml中的內容。

Guest.log -

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-e4ec38ee188c/WirelessNSP.xml 2020-12-02
05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-
Streaming to ip:10.106.33.167 file type: NativeSPProfile file name:WirelessNSP.xml 2020-12-02
05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-
SPW profile :: 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][]
cisco.cpm.client.provisioning.StreamingServlet -::-
```

從**spwProfile.xml**讀取內容後，NSA配置網路配置檔案並生成CSR，然後將其傳送到ISE以使用URL https://10.106.32.119:8443/auth/pkiclient.exe獲取證書



ise-psc.log-

```
2020-12-02 05:45:11,298 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Found incoming certifcate request for
internal CA. Increasing Cert Request counter. 2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Key type
is RSA, retrieving ScepCertRequestProcessor for caProfileName=ISE Internal CA 2020-12-02
05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertRequestValidator -::::- Session user has been set to = dot1xuser
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02
05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][]
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- About to forward certificate request
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser with transaction id n@P~N6E to server
http://127.0.0.1:9444/caservice/scep 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Encoding message:
org.jscep.message.PkcsReq@5c1649c2[transId=4d22d2e256a247a302e900ffa71c35d75610de67,messageType=
PKCS_REQ,senderNonce=Nonce
[7d9092a9fab204bd7600357e38309ee8],messageData=org.bouncycastle.pkcs.PKCS10CertificationRequest@
4662a5b0] 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkcsPkiEnvelopeEncoder -::::- Encrypting session key using key belonging to
[issuer=CN=Certificate Services Endpoint Sub CA - isee30-primary;
serial=162233386180991315074159441535479499152] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Signing message using
key belonging to [issuer=CN=isee30-primary.anshsinh.local;
serial=126990069826611188711089996345828696375] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- SignatureAlgorithm
SHA1withRSA 2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkiMessageEncoder -::::- Signing
org.bouncycastle.cms.CMSProcessableByteArray@5aa9dfcc content
```

ca-service.log -

```
2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -::::::- performing certificate request
validation: version [0] subject [C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser] ---
output omitted--- 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request validation]
com.cisco.cpm.caservice.CrValidator -::::::- RDN value = dot1xuser 2020-12-02 05:45:11,379 DEBUG
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request]
com.cisco.cpm.caservice.CrValidator -::::::- request validation result CA_OK
```

caservice-misc.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request issuance] cisco.cpm.scep.util.ScepUtil -::::::- Algorithm OID in CSR:
1.2.840.113549.1.1.1 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.scep.CertRequestInfo -::::::- Found challenge password with cert template ID.
```

caservice.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -::::::- Checking cache for
certificate template with ID: e2c32ce0-313d-11eb-b19e-e60300a810d5 2020-12-02 05:45:11,380 DEBUG
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -::::::- CA SAN Extensions = GeneralNames: 1: 50-3E-
AA-E4-81-B6 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -::::::- CA : add SAN extension... 2020-12-02
05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5
request issuance] com.cisco.cpm.caservice.CertificateAuthority -::::::- CA Cert Template name =
```

```
BYOD_Certificate_template 2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
cisco.cpm.caservice.util.CaServiceUtil -::::::- Storing certificate via REST for serial number:
518fa73a4c654df282ffdb026080de8d 2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -::::::- issuing Certificate Services Endpoint
Certificate: class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_OK]
subject [CN=dot1xuser, OU=tac, O=cisco, L=bangalore, ST=Karnataka, C=IN] version [3] serial
[0x518fa73a-4c654df2-82ffdb02-6080de8d] validity [after [2020-12-01T05:45:11+0000] before [2030-
11-27T07:35:10+0000]] keyUsages [ digitalSignature nonRepudiation keyEncipherment ]
```

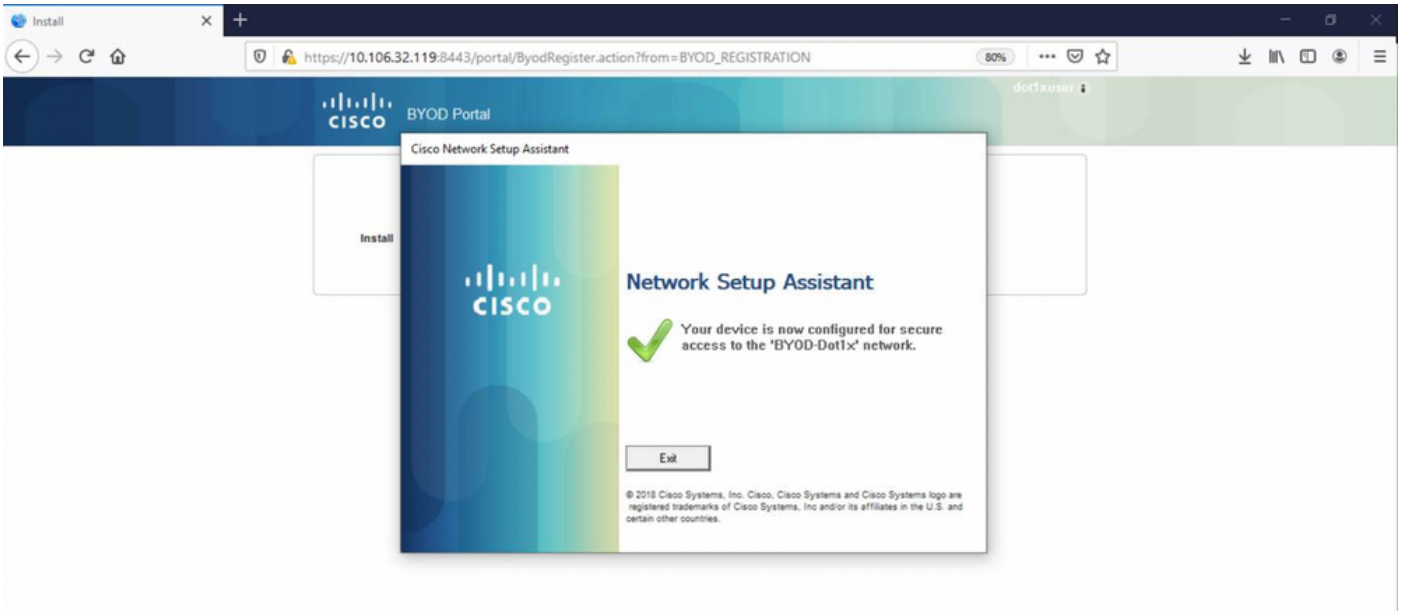
ise-psc.log -

```
2020-12-02 05:45:11,407 DEBUG [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -
::::- Verifying message using key belonging to 'CN=Certificate Services Endpoint RA - isee30-
primary'
```

caservice.log -

```
2020-12-02 05:45:11,570 DEBUG [Infra-CAServiceUtil-Thread][]
cisco.cpm.caservice.util.CaServiceUtil -::::::- Successfully stored endpoint certificate.
```

ise-psc.log -




```
2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Performing doGetCertInitial found
Scep certificate processor for txn id n@P~N6E 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Polling
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser for certificate request n@P~N6E with
id {} 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][]
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Certificate request Complete for
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser Trx Idn@P~N6E 2020-12-02 05:45:13,596
DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- BYODStatus:COMPLETE_OTA_NSP
```

證書安裝後，客戶端使用EAP-TLS啟動另一個身份驗證並獲得完全訪問許可權。

prrt-server.log -

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-
```

```
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,CallingStationID=50-3e-aa-e4-81-
b6,EAP: Recv EAP packet, code=Response, identifier=64, type=EAP-TLS, length=166
,EapParser.cpp:150 Radius,2020-12-02
05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [1] User-Name -
value: [dot1xuser] [25] Class - value: [****] [79] EAP-Message - value: [E [80] Message-
Authenticator - value: [Ù(ØyËöžö|kÔ,¸}] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216
```

客戶端日誌（spw日誌）

客戶端發起下載配置檔案。

```
[Mon Nov 30 03:34:27 2020] Downloading profile configuration... [Mon Nov 30 03:34:27 2020]
Discovering ISE using default gateway [Mon Nov 30 03:34:27 2020] Identifying wired and wireless
network interfaces, total active interfaces: 1 [Mon Nov 30 03:34:27 2020] Network interface -
mac:50-3E-AA-E4-81-B6, name: Wi-Fi 2, type: unknown [Mon Nov 30 03:34:27 2020] Identified
default gateway: 10.106.33.1 [Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1,
mac address: 50-3E-AA-E4-81-B6 [Mon Nov 30 03:34:27 2020] DiscoverISE - start [Mon Nov 30
03:34:27 2020] DiscoverISE input parameter : strUrl [http://10.106.33.1/auth/discovery] [Mon Nov
30 03:34:27 2020] [HTTPConnection] CrackUrl: host = 10.106.33.1, path = /auth/discovery, user =
, port = 80, scheme = 3, flags = 0 [Mon Nov 30 03:34:27 2020] [HTTPConnection] HttpSendRequest:
header = Accept: */* headerLength = 12 data = dataLength = 0 [Mon Nov 30 03:34:27 2020] HTTP
Response header: [HTTP/1.1 200 OK Location:
https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-
3304-4f25-845d-
be9faac3c44f&action=nsp&token=29354d43962243bcb72193cbf9dc3260&redirect=10.106.33.1/auth/discove
ry [Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path =
/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009c5fc4fb5e&os=WINDOWS_10_ALL, user = , port
= 8443, scheme = 4, flags = 8388608 Mon Nov 30 03:34:36 2020] parsing wireless connection
setting [Mon Nov 30 03:34:36 2020] Certificate template: [keytype:RSA, keysize:2048,
subject:OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN, SAN:MAC] [Mon Nov 30 03:34:36 2020] set
ChallengePwd
```

客戶端檢查WLAN服務是否正在運行。

```
[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - Start [Mon Nov 30 03:34:36 2020]
Wlansvc service is in Auto mode ... [Mon Nov 30 03:34:36 2020] Wlansvc is running in auto
mode... [Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - End [Mon Nov 30 03:34:36
2020] Wireless interface 1 - Desc: [TP-Link Wireless USB Adapter], Guid: [{65E78DDE-E3F1-4640-
906B-15215F986CAA}]... [Mon Nov 30 03:34:36 2020] Wireless interface - Mac address: 50-3E-AA-E4-
81-B6 [Mon Nov 30 03:34:36 2020] Identifying wired and wireless interfaces... [Mon Nov 30
03:34:36 2020] Found wireless interface - [ name:Wi-Fi 2, mac address:50-3E-AA-E4-81-B6] [Mon
Nov 30 03:34:36 2020] Wireless interface [Wi-Fi 2] will be configured... [Mon Nov 30 03:34:37
2020] Host - [ name:DESKTOP-965F94U, mac addresses:50-3E-AA-E4-81-B6]
```

客戶端開始應用配置檔案 —

```
[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id:
dot1xuser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81-B6, profile: WirelessNSP
[Mon Nov 30 03:34:37 2020] number of wireless connections to configure: 1 [Mon Nov 30 03:34:37
2020] starting configuration for SSID : [BYOD-Dot1x] [Mon Nov 30 03:34:37 2020] applying
certificate for ssid [BYOD-Dot1x]
```

客戶端安裝證書。

```
[Mon Nov 30 03:34:37 2020] ApplyCert - Start... [Mon Nov 30 03:34:37 2020] using ChallengePwd
[Mon Nov 30 03:34:37 2020] creating certificate with subject = dot1xuser and subjectSuffix =
```

OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN [Mon Nov 30 03:34:38 2020] Self signed certificate [Mon Nov 30 03:34:44 2020] Installed [isee30-primary.anshsinh.local, hash: 5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b] as rootCA [Mon Nov 30 03:34:44 2020] Installed CA cert for authMode machineOrUser - Success Certificate is downloaded . Omitted for brevity - [Mon Nov 30 03:34:50 2020] creating response file name C:\Users\admin\AppData\Local\Temp\response.cer [Mon Nov 30 03:34:50 2020] Certificate issued - successfully [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert start [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert: Reading scep response file [C:\Users\admin\AppData\Local\Temp\response.cer]. [Mon Nov 30 03:34:51 2020] ScepWrapper::InstallCert GetCertHash -- return val 1 [Mon Nov 30 03:34:51 2020] ScepWrapper::InstallCert end [Mon Nov 30 03:34:51 2020] ApplyCert - End... [Mon Nov 30 03:34:51 2020] applied user certificate using template id e2c32ce0-313d-11eb-b19e-e60300a810d5

ISE配置無線配置檔案

[Mon Nov 30 03:34:51 2020] Configuring wireless profiles... [Mon Nov 30 03:34:51 2020] Configuring ssid [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile - Start [Mon Nov 30 03:34:51 2020] TLS - TrustedRootCA Hash: [5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b]

配置檔案

Wireless interface succesfully initiated, continuing to configure SSID [Mon Nov 30 03:34:51 2020] Currently connected to SSID: [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] Wireless profile: [BYOD-Dot1x] configured successfully [Mon Nov 30 03:34:51 2020] Connect to SSID [Mon Nov 30 03:34:51 2020] Successfully connected profile: [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile. - End [Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - Start [Mon Nov 30 03:35:21 2020] Currently connected to SSID: [BYOD-Dot1x], profile ssid: [BYOD-Dot1x], Single SSID [Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - End [Mon Nov 30 03:36:07 2020] Device configured successfully.