在Windows和ISE上配置单SSID无线BYOD

目录

简介

本文档介绍如何使用单SSID和双SSID在Windows计算机的思科身份服务引擎(ISE)上配置自带设备(BYOD)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE版本3.0的配置
- Cisco WLC的配置
- 自带设备工作

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.0
- Windows 10
- WLC和AP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

理论

在单SSID BYOD中，设备的板载和以后授予注册设备的完全访问权限时，仅使用一个SSID。首先，用户使用用户名和密码(MSCHAPv2)连接到SSID。 在ISE上成功进行身份验证后，用户将重定向到BYOD门户。设备注册完成后，终端客户端从ISE下载本地请求方助理(NSA)。NSA安装在终端客户端上，从ISE下载配置文件和证书。NSA配置无线请求方，客户端安装证书。终端使用下载的证书使用EAP-TLS对同一SSID执行另一身份验证。ISE检查来自客户端的新请求并验证EAP方法和设备注册并授予对设备的完全访问权限。

Windows BYOD单SSID步骤 —

- 初始EAP-MSCHAPv2身份验证
- 重定向到BYOD门户
- 设备注册
- NSA下载
- 配置文件下载
- 证书下载
- EAP-TLS身份验证

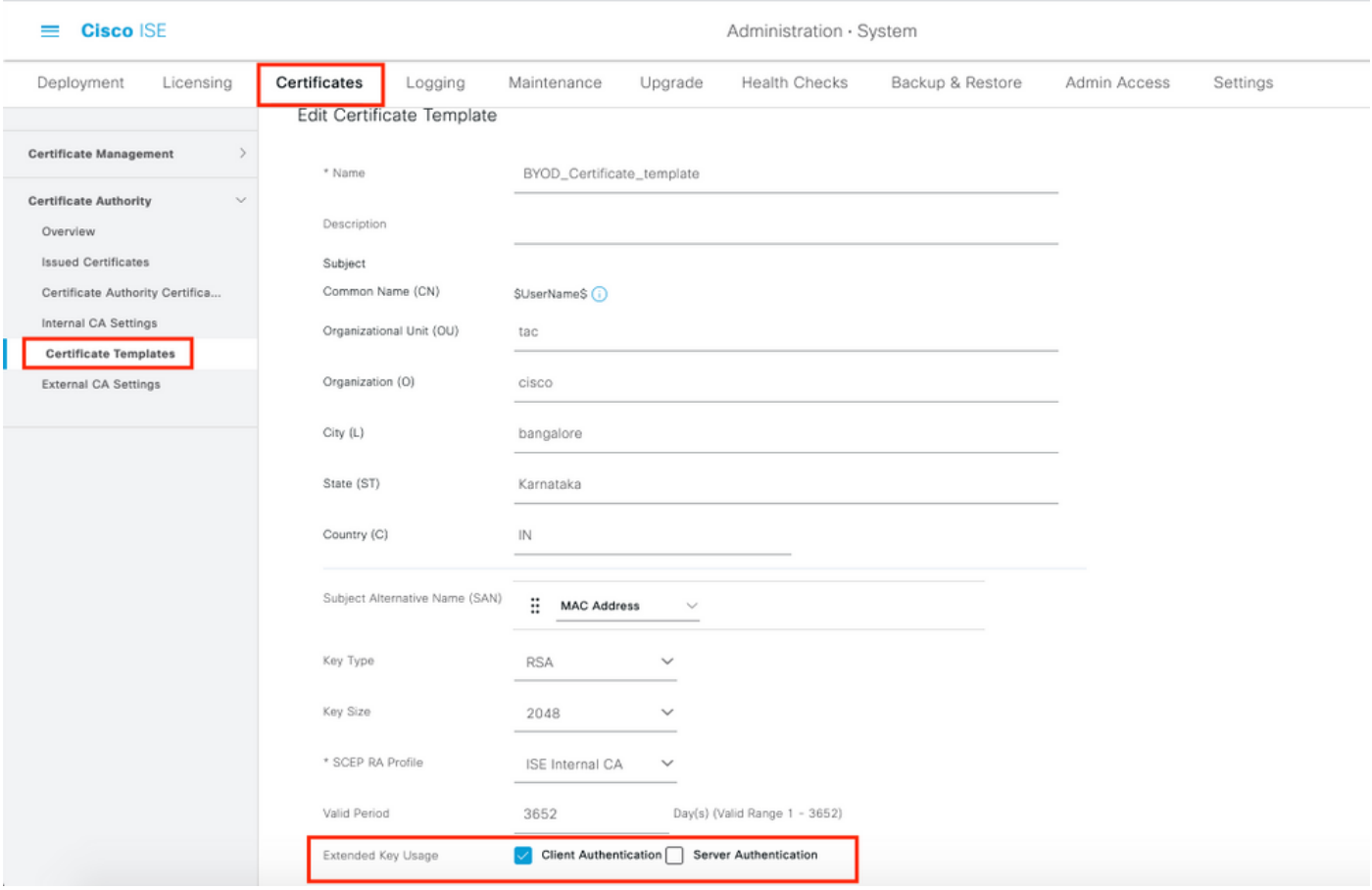
配置

ISE配置

步骤1.在ISE上添加网络设备并配置RADIUS和共享密钥。

导航至**ISE >管理>网络设备>添加网络设备**。

步骤2.为BYOD用户创建证书模板。模板必须具有客户端身份验证增强密钥使用。您可以使用默认的EAP_Certificate_Template。

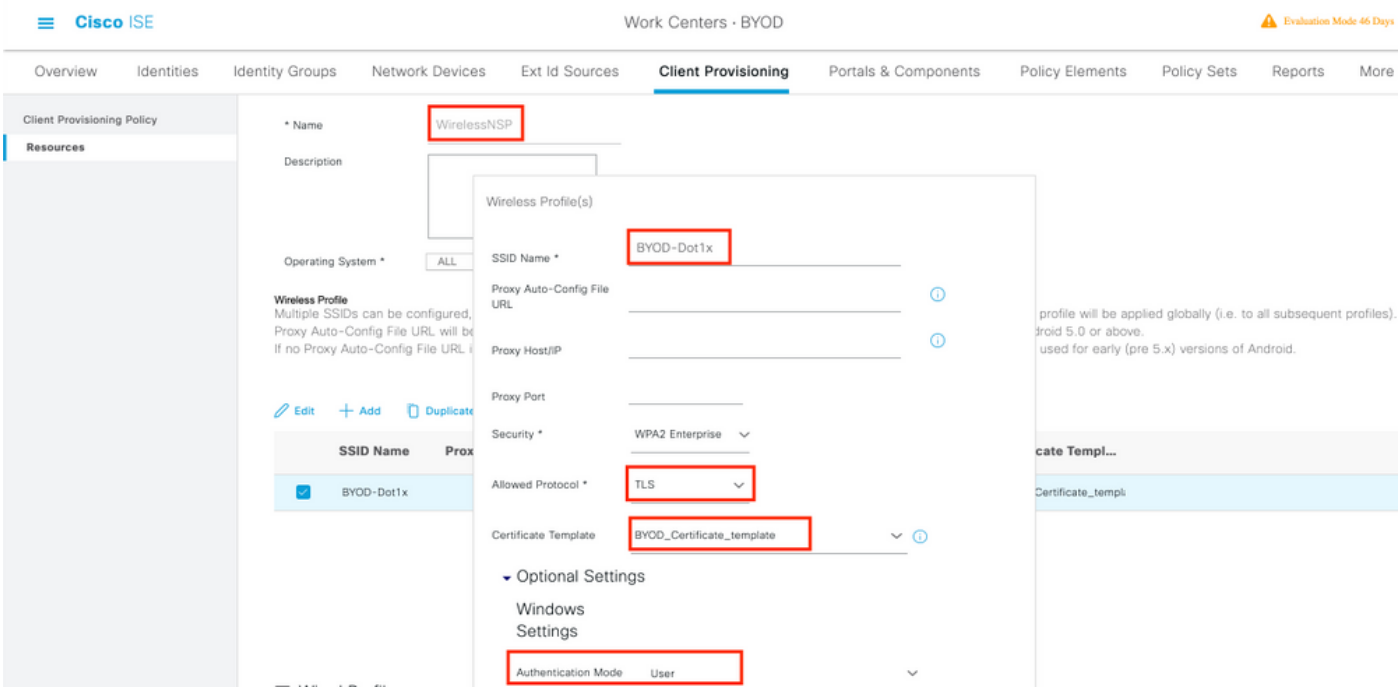


步骤3.为无线配置文件创建本地请求方配置文件。

导航至**ISE >工作中心> BYOD >客户端调配**。单击Add并从下**拉菜单中选择Native Supplicant Profile(NSP)**。

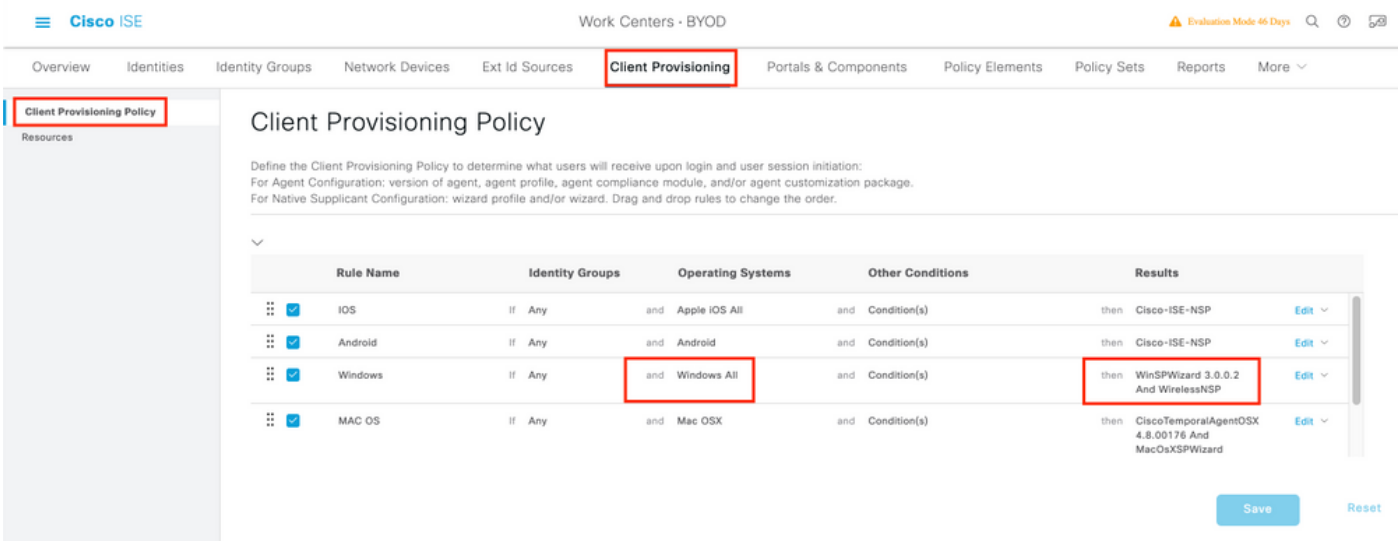
在这里，SSID名称必须与您连接的名称相同，然后您才能执行单SSID BYOD。选择协议作为TLS。选择在上一步中创建的证书模板，或者您可以使用默认EAP_Certificate_Template 。

在可选设置下，根据您的要求选择用户或用户和计算机身份验证。在本例中，它配置为用户身份验证。保留其他设置为默认值。



步骤4.为Windows设备创建客户端调配策略。

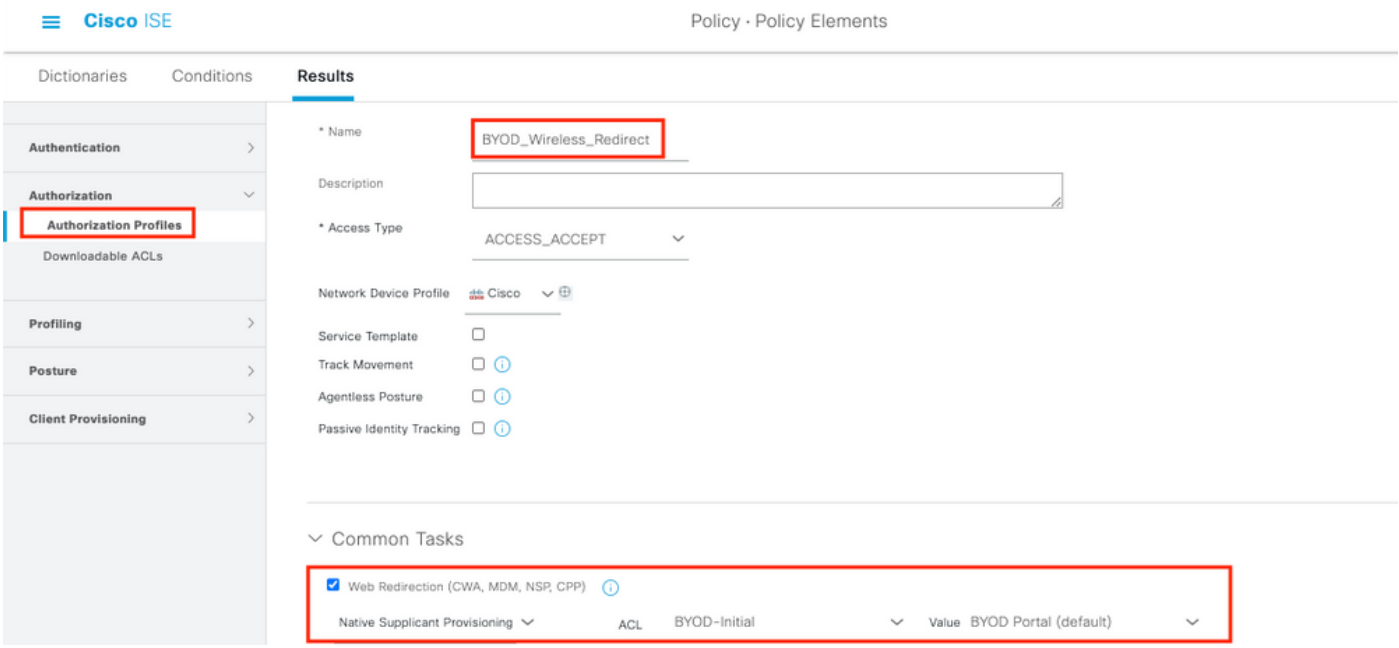
导航至**ISE >工作中心> BYOD >客户端调配>客户端调配策略**。选择操作系统作为**Windows ALL**。选择**WinSPWizard 3.0.0.2和在上一步**中创建的NSP。



步骤5.为未注册为**BYOD设**备的设备创建授权配置文件。

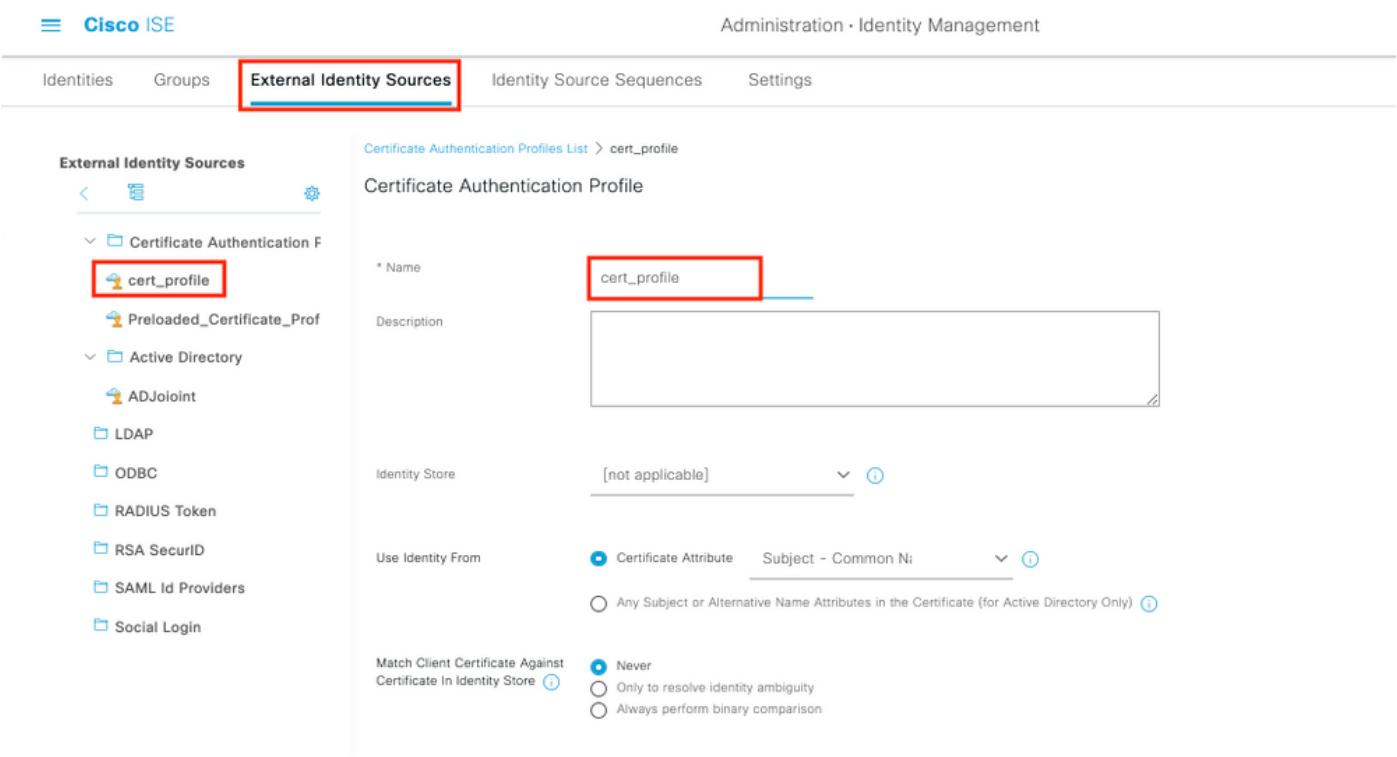
导航至**ISE > Policy > Policy Elements > Results> Authorization > Authorization Profiles > Add**。

在“常**见任务**”下，选**择“本地请求方调配**”。定义在WLC上创建的重定向ACL名称并选择BYOD门户。此处使用默认门户。您可以创建自定义BYOD门户。导航至**ISE >工作中心> BYOD >门户**和组件，然后点**击添加**。

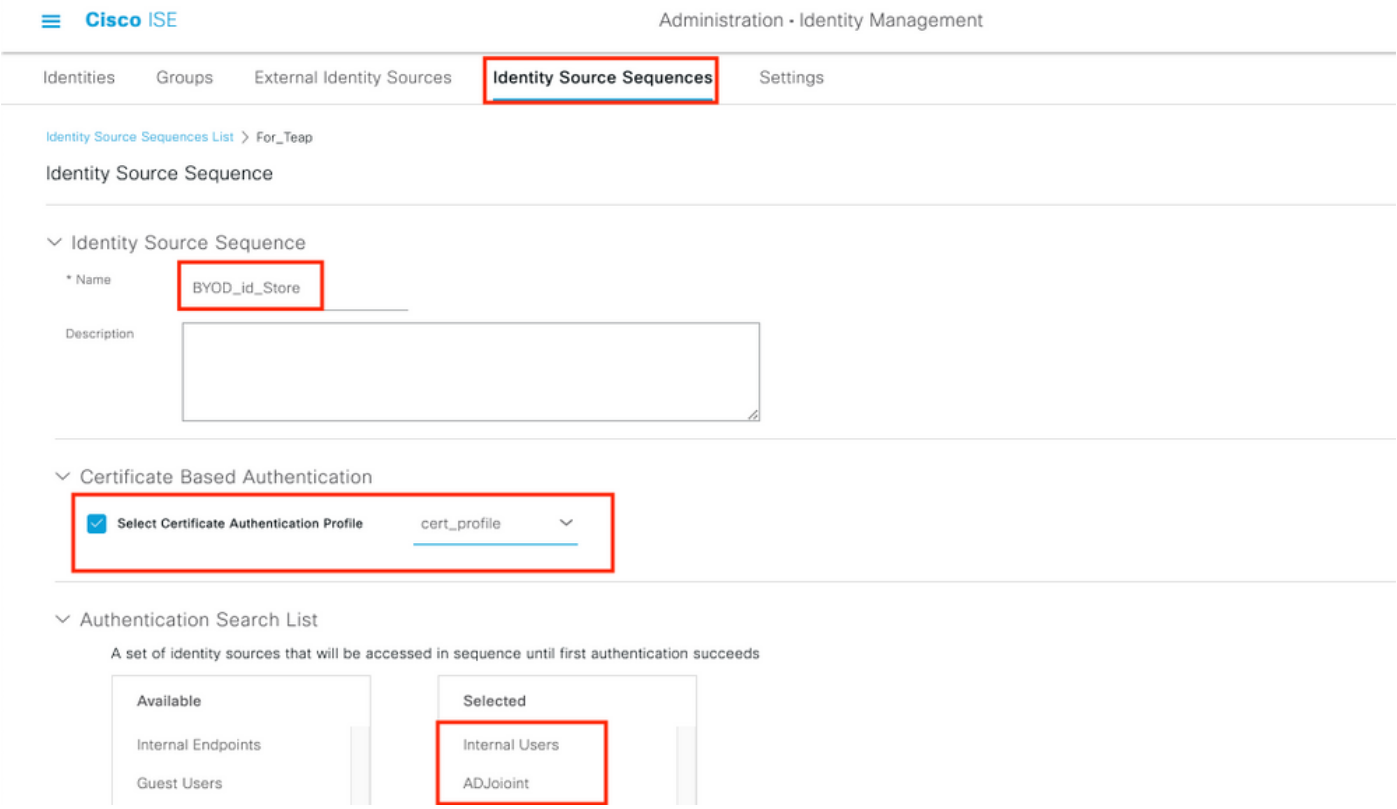


步骤6.创建证书配置文件。

导航至**ISE >管理>外部身份源>证书配置文件**。此处创建新证书配置文件或使用默认证书配置文件。



步骤7.创建身份源序列并选择在上一步中创建的证书配置文件或使用默认证书配置文件。当用户在BYOD注册后执行EAP-TLS以获得完全访问权时，需要执行此操作。



步骤8.创建策略集、身份验证策略和授权策略。

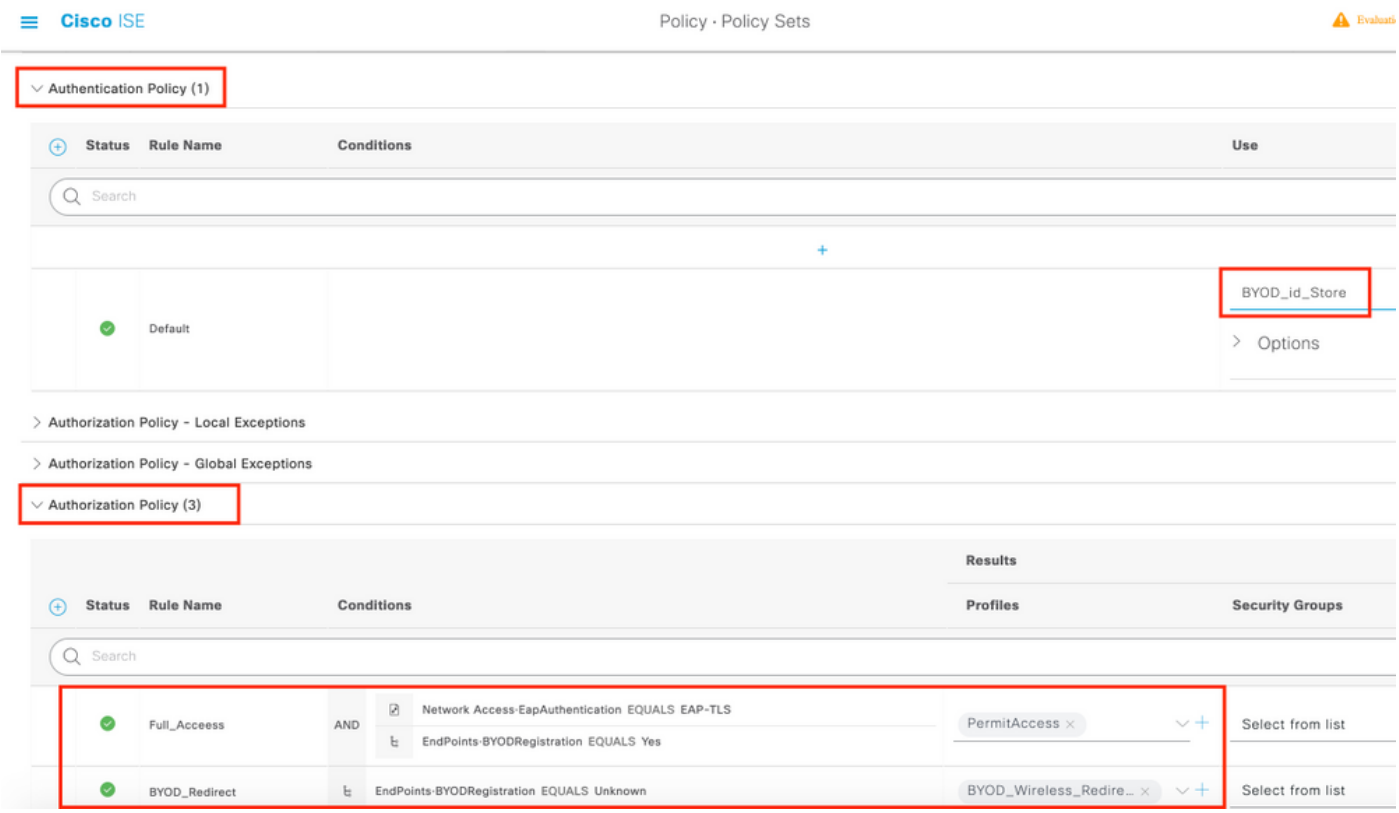
导航到**ISE > Policy > Policy Sets**。创建策略集并**保存**。

创建身份验证策略并选择在上一步中创建的身份源序列。

创建授权策略。您必须创建两个策略。

1.对于未注册BYOD的设备。提供在步骤5中创建的重定向配置文件。

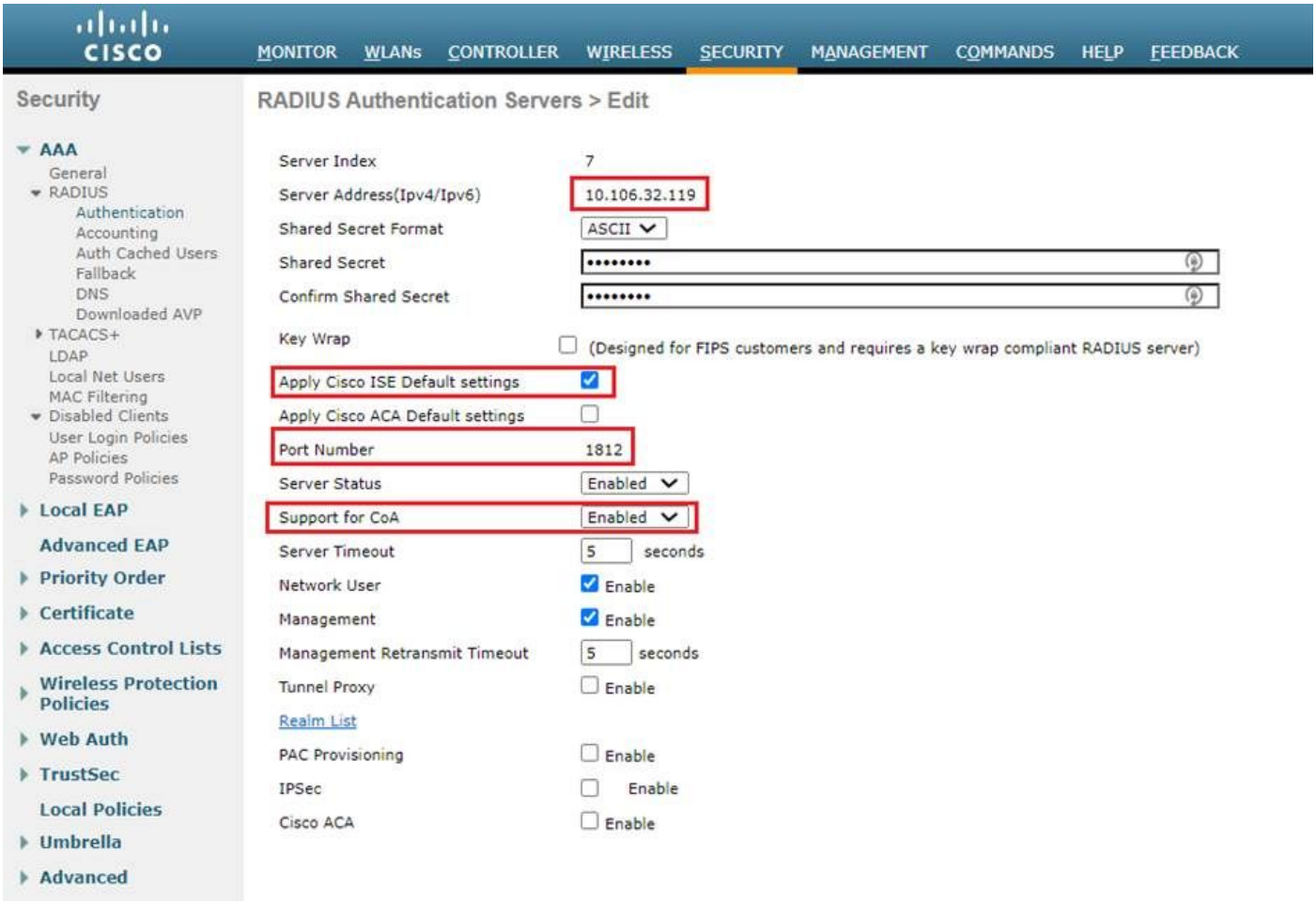
2.注册了BYOD并执行EAP-TLS的设备。提供对这些设备的完全访问权限。



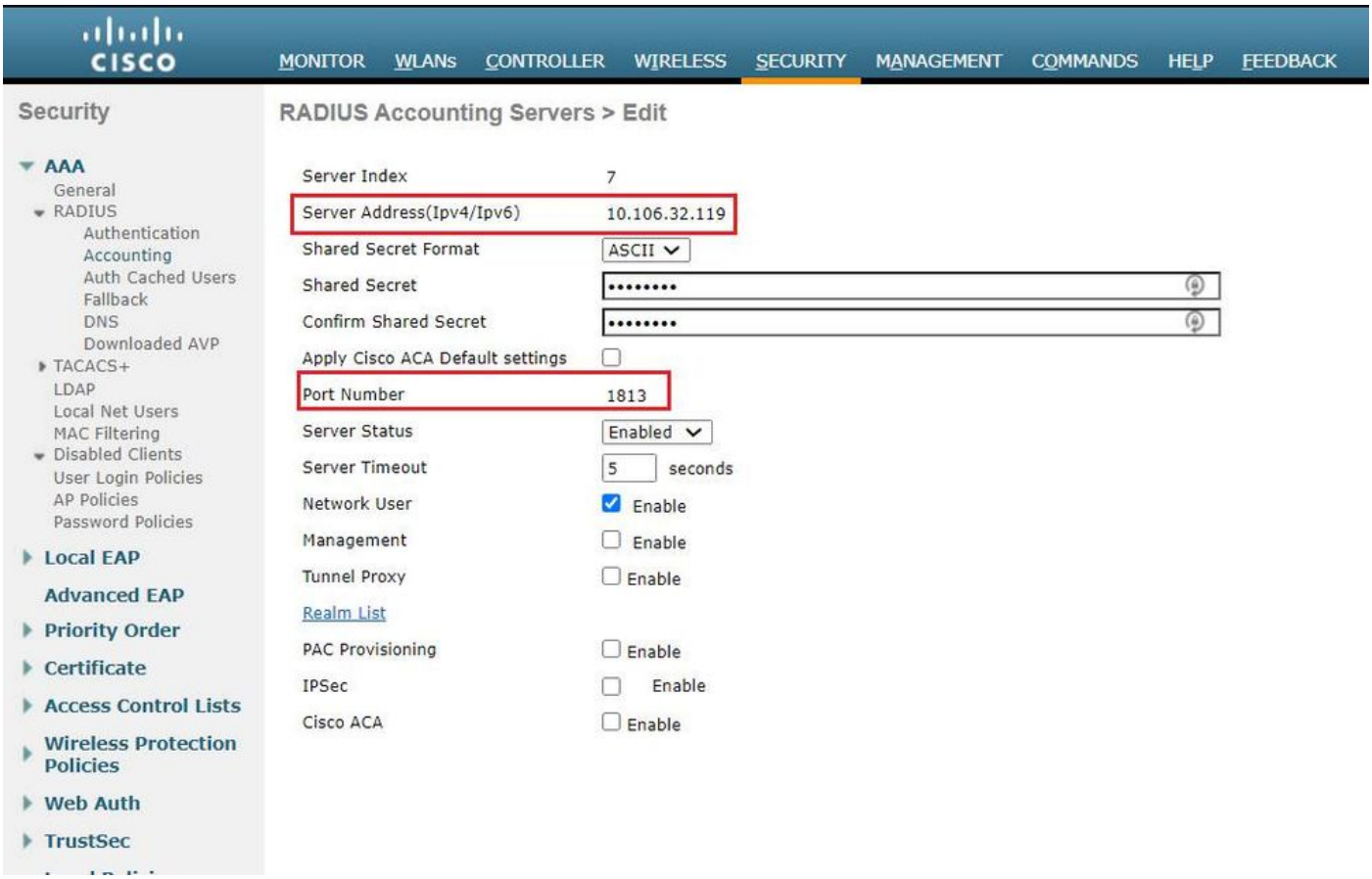
WLC 配置

步骤1.在WLC上配置Radius服务器。

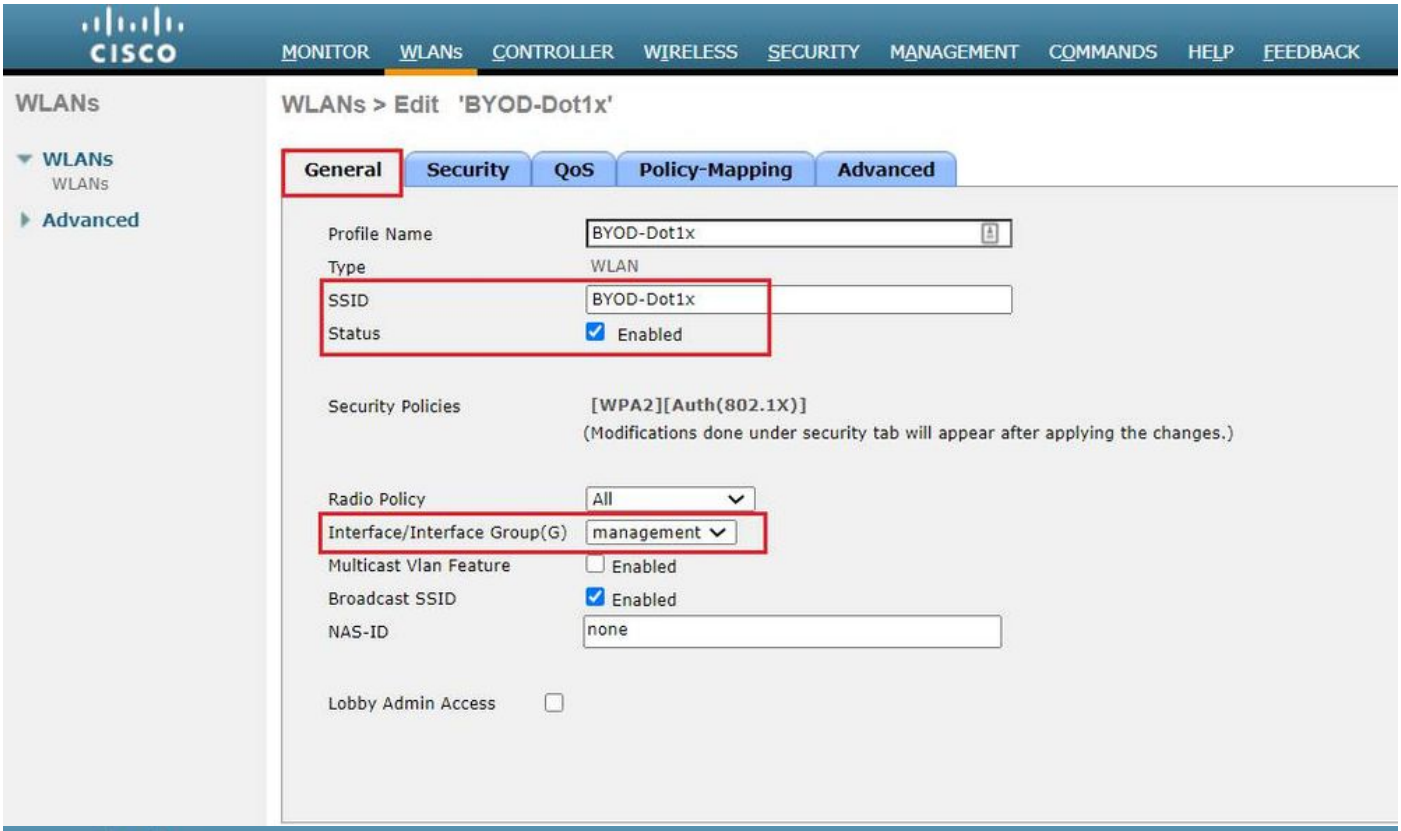
导航至**Security > AAA > Radius > Authentication**。

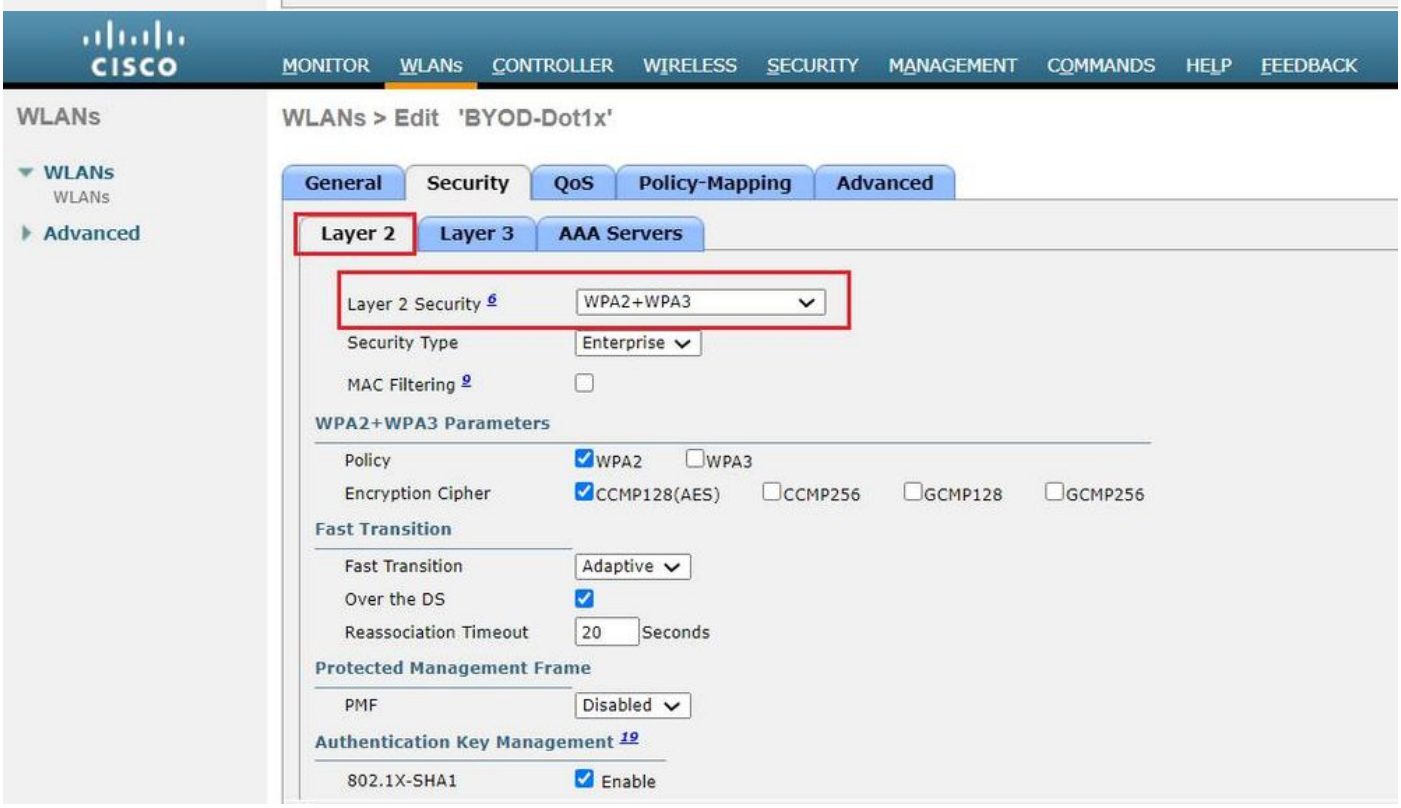


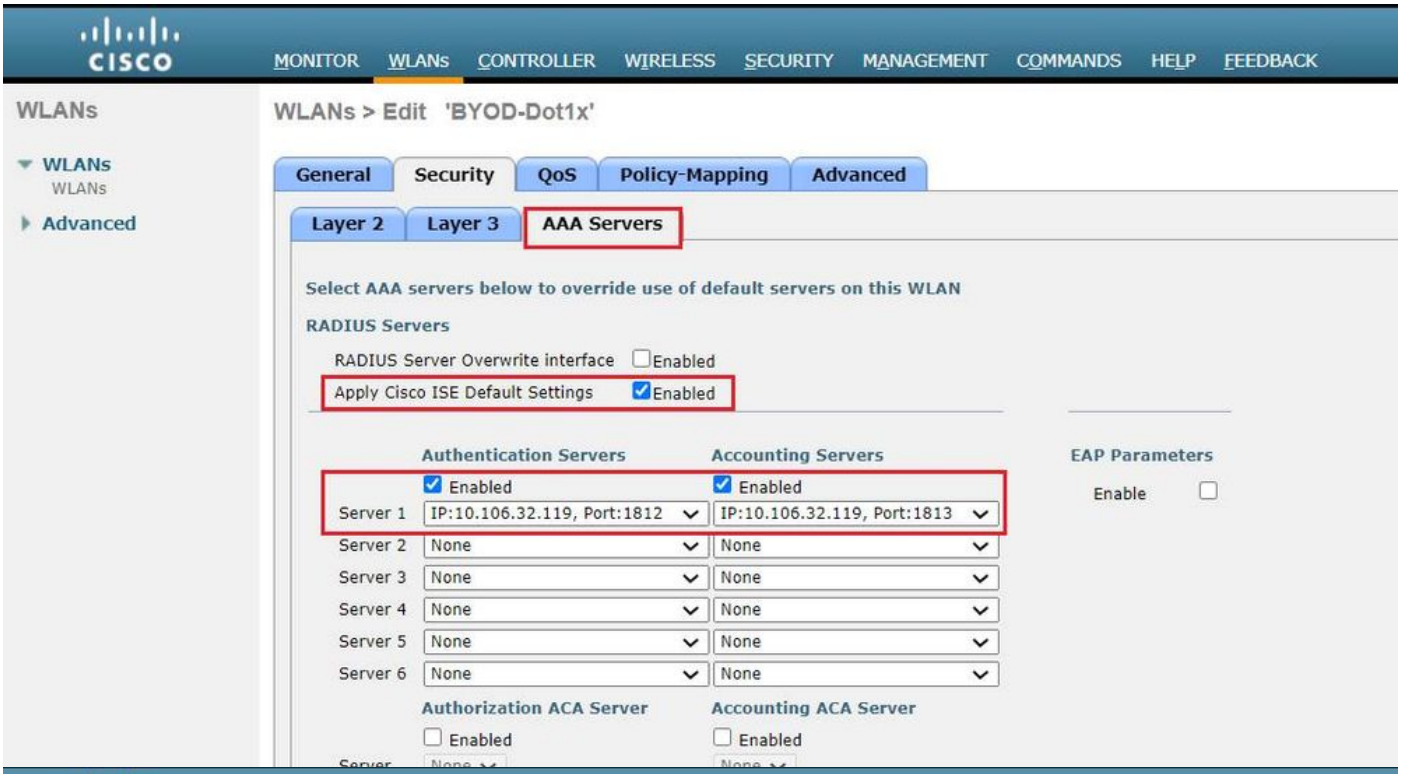
导航至Security > AAA > Radius > Accounting。

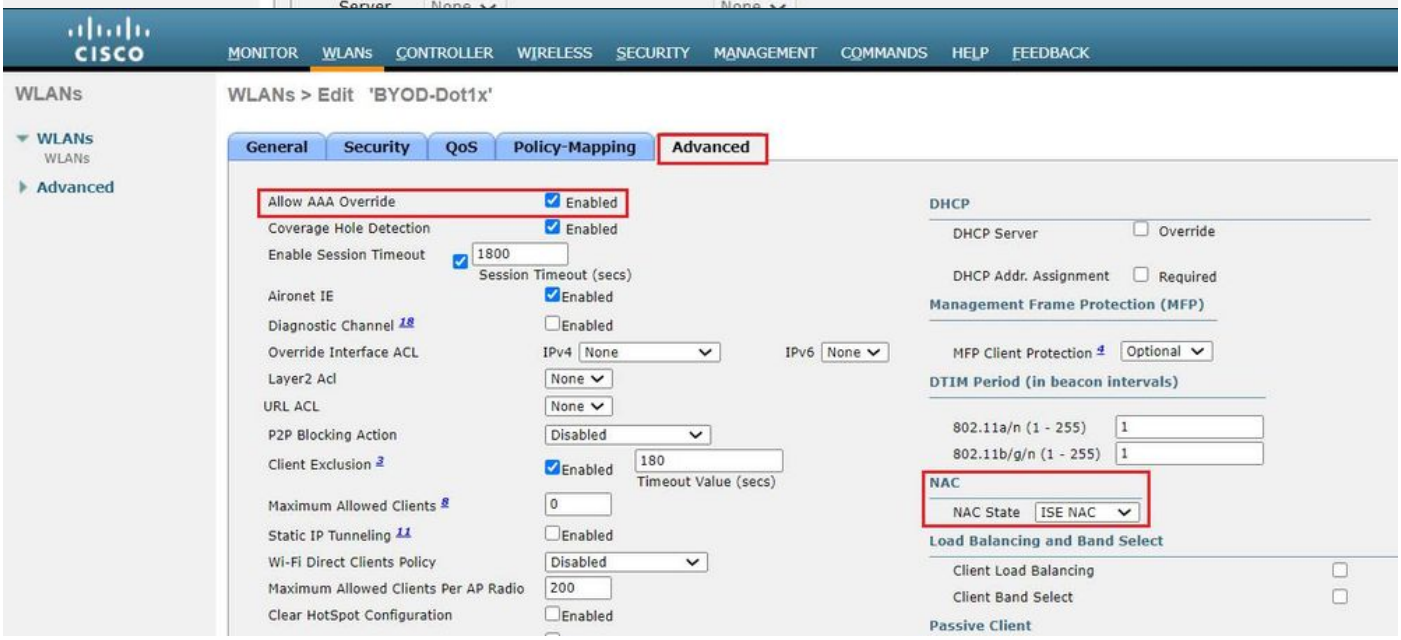


步骤2.配置Dot1x SSID。


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 6 WPA2+WPA3
Security Type Enterprise
MAC Filtering 9
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 19
802.1X-SHA1 Enable

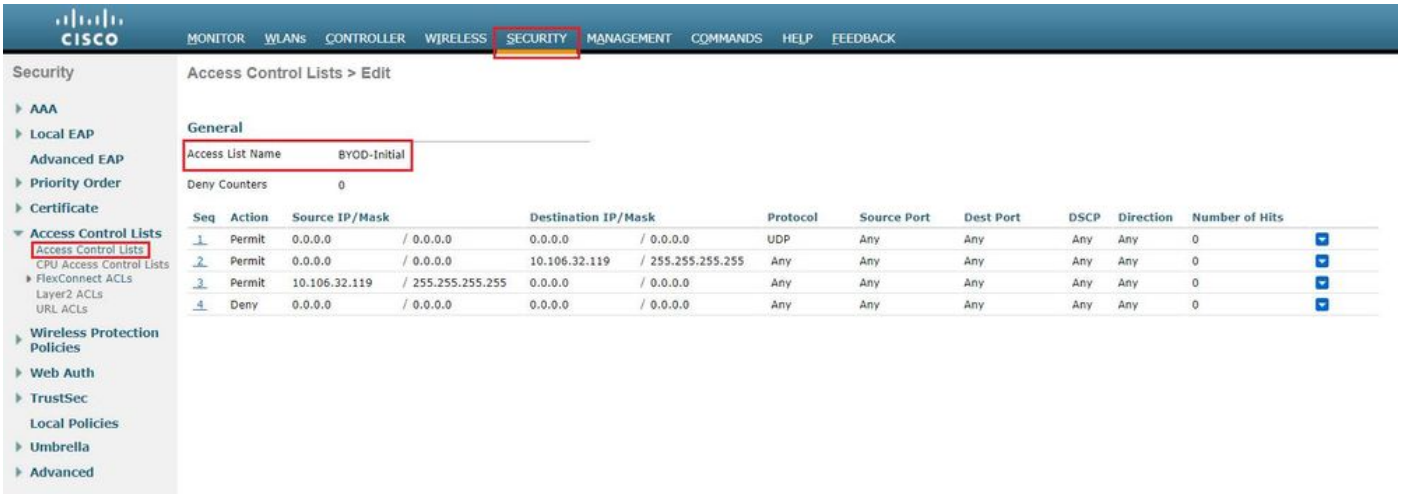




步骤3.配置重定向ACL，以提供调配设备的有限访问。

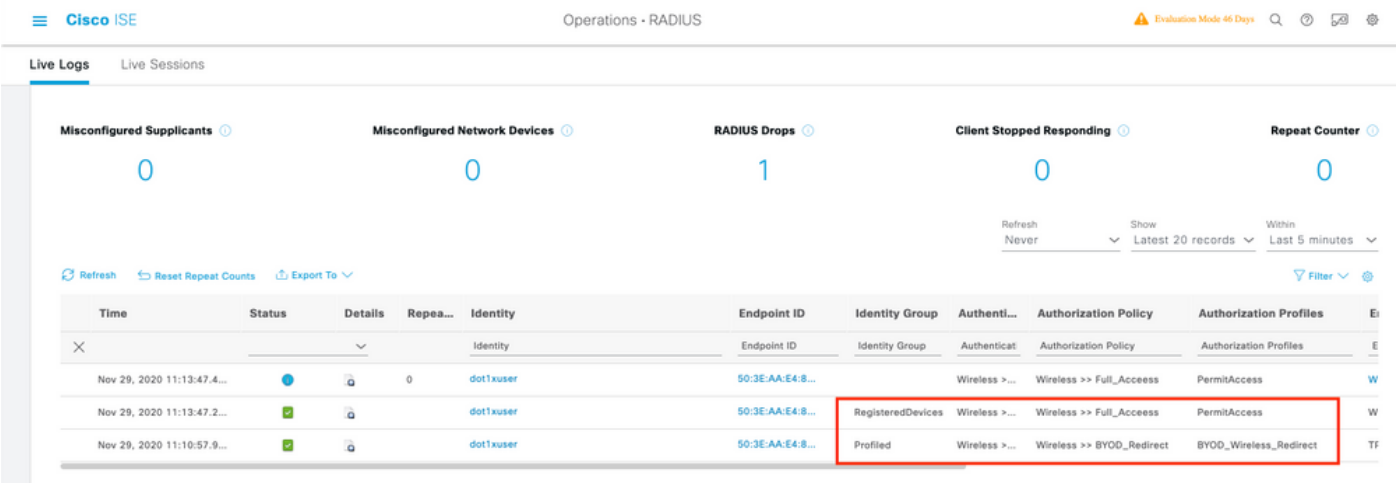
- 允许UDP流量到DHCP和DNS（默认允许DHCP）。
- 与ISE的通信。
- 拒绝其他流量。

名称：BYOD-Initial（或您在授权配置文件中手动命名的ACL）



验证

身份验证流验证



1.首次登录时，用户使用用户名和密码执行PEAP身份验证。在ISE上，用户点击重定向规则BYOD重定向。

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

Cisco ISE

Authentication Details

Source Timestamp	2020-11-29 11:10:57.955
Received Timestamp	2020-11-29 11:10:57.955
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
User Type	User
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	TP-LINK-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC1

2.在BYOD注册后，用户被添加到注册设备，现在执行EAP-TLS并获得完全访问权限。

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

Cisco ISE

Authentication Details

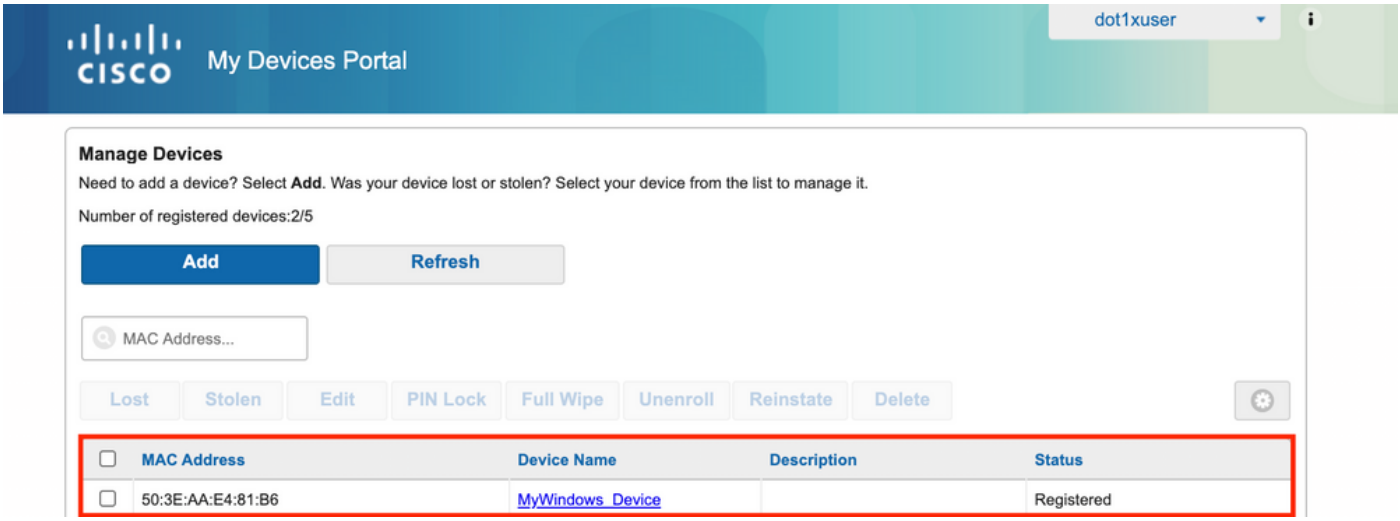
Source Timestamp	2020-11-29 11:13:47.246
Received Timestamp	2020-11-29 11:13:47.246
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	Windows10-Workstation
Identity Group	RegisteredDevices
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	WLC1

检查我的设备门户

导航至MyDevices Portal（我的设备门户）并使用凭证登录。 您可以看到设备名称和注册状态。

您可以为MyDevices门户创建URL。

导航至**ISE >工作中心> BYOD >门户和组件>我的设备门户>登录设置**，然后输入完全限定URL。



故障排除

一般信息

对于BYOD流程，这些ISE组件必须在PSN节点的调试中启用 —

scep - scep日志消息。目标日**志fileguest.log和ise-psc.log**。

client-webapp — 负责基础设施消息的组件。目标日志文件 — **ise-psc.log**

portal-web-action — 负责客户端调配策略处理的组件。目标日志文件 — **guest.log**。

portal — 所有与门户相关的事件。目标日志文件 — **guest.log**

portal-session-manager — 目标日志文件 — **门户会话相关调试消息 — gues.log**

ca-service - ca-service消息 — 目标日志文件 — **caservice.log和caservice-misc.log**

ca-service-cert- ca-service certificate messages — 目标日志文件**- caservice.log和caservice-misc.log**

admin-ca- ca-service admin消息 — 目标日志文**件ise-psc.log**、**caservice.log和casrvice-misc.log**

certprovisioningportal — 证书调配门户消息 — 目标日**志文件ise-psc.log**

nsf - NSF相关消息 — 目标日志文**件ise-psc.log**

nsf-session — 会话缓存相关消息 — 目标日志文**件ise-psc.log**

runtime-AAA — 所有运行时事件。目标日志文件**-prrt-server.log**。

对于客户端日志：

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

工作日志分析

ISE日志

使用重定向ACL和BYOD门户重定向URL的初始访问 — 接受。

Prrt-server.log-

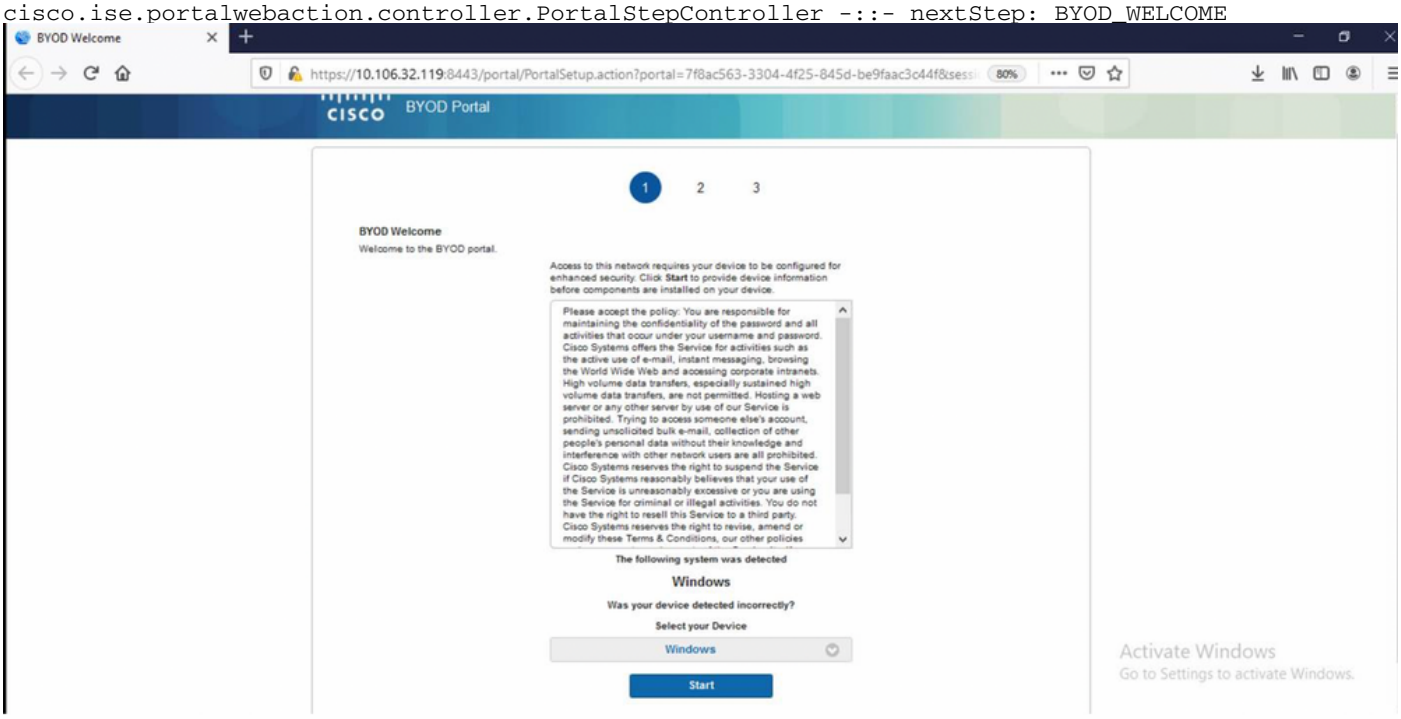
```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-
primary/392215758/699,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -
value: [dot1xuser] [25] Class - 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
```

当最终用户尝试导航到网站并被WLC重定向到ISE重定向URL时。

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
```



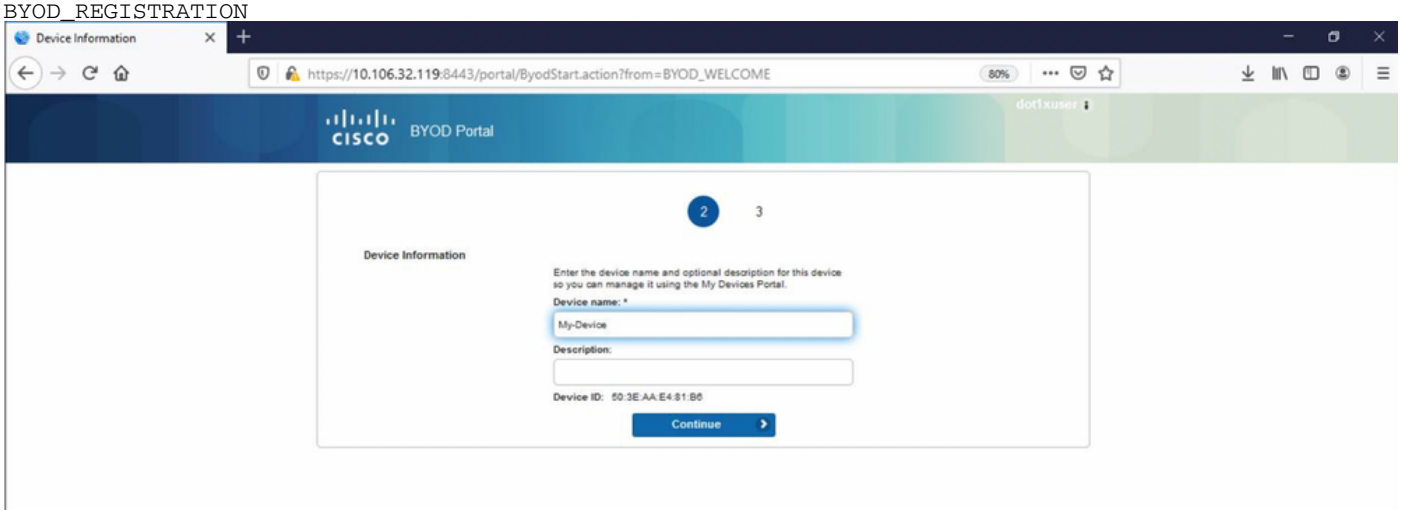
点击BYOD欢迎页面上的开始。

```
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
```

此时，ISE评估BYOD所需的必要文件/资源是否存在，并将自身设置为BYOD INIT状态。

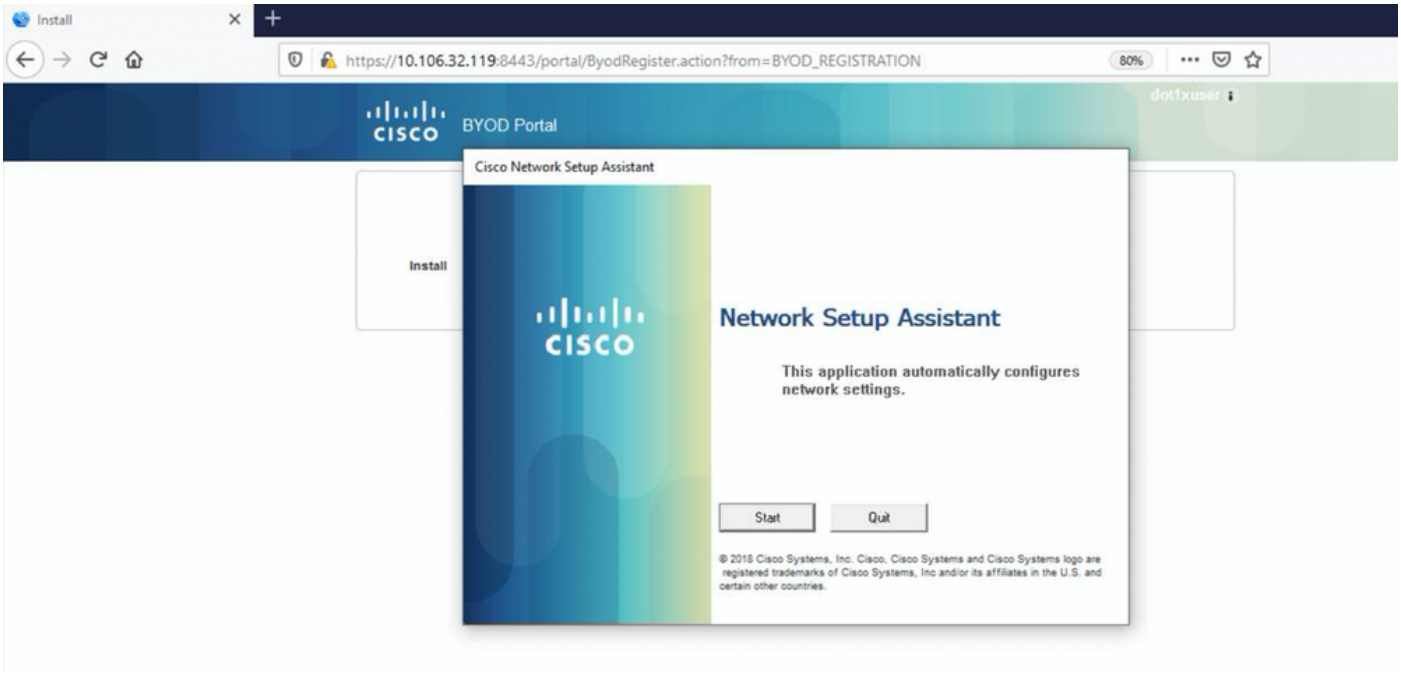
```
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All), nspStatus=SUCCESS 2020-12-02 05:44:01,936 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
```



输入设备名称，然后点击注册。

```
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
```

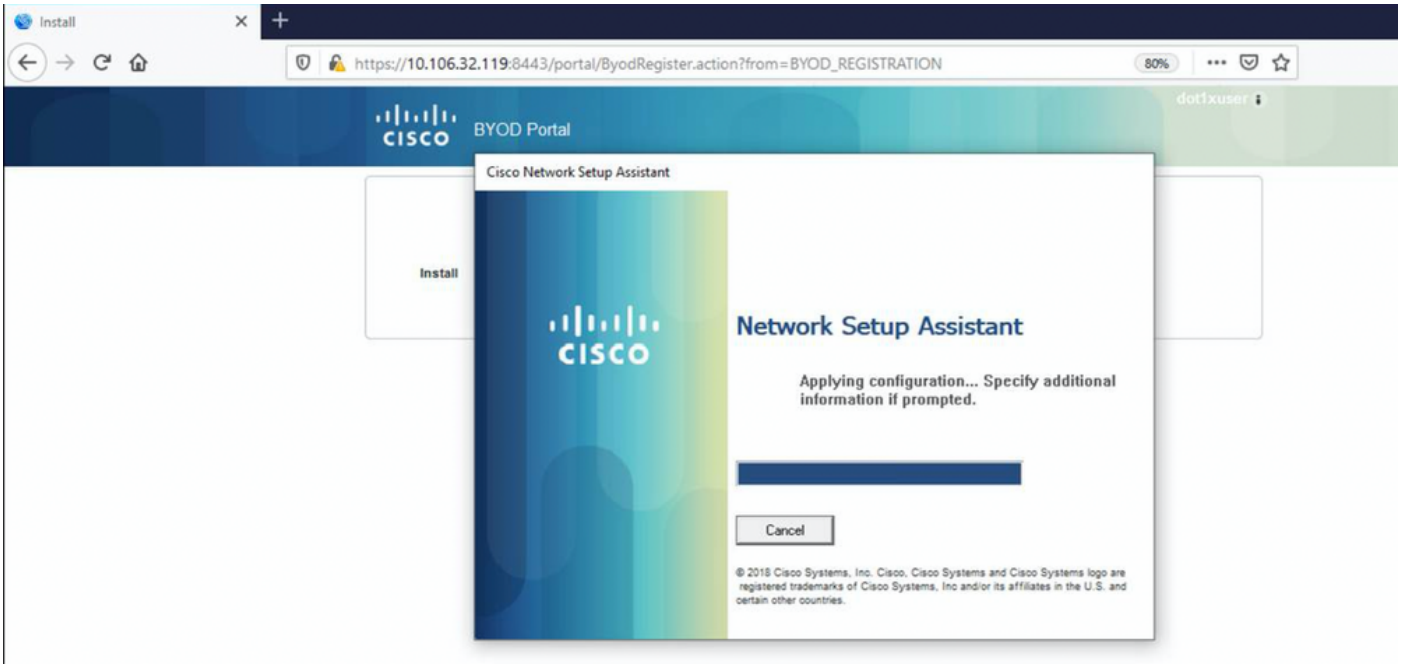


现在，当用户点击NSA上的Start时，在客户端上临时创建名为**spwProfile.xml**的文件，该文件从TCP端口8905上下载的Cisco-ISE-NSP.xml复制内容。

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 -::-
```

从**spwProfile.xml**中读取内容后，NSA配置网络配置文件并生成CSR，并将其发送到ISE以使用URL https://10.106.32.119:8443/auth/pkiclient.exe获取证书



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 ]
```

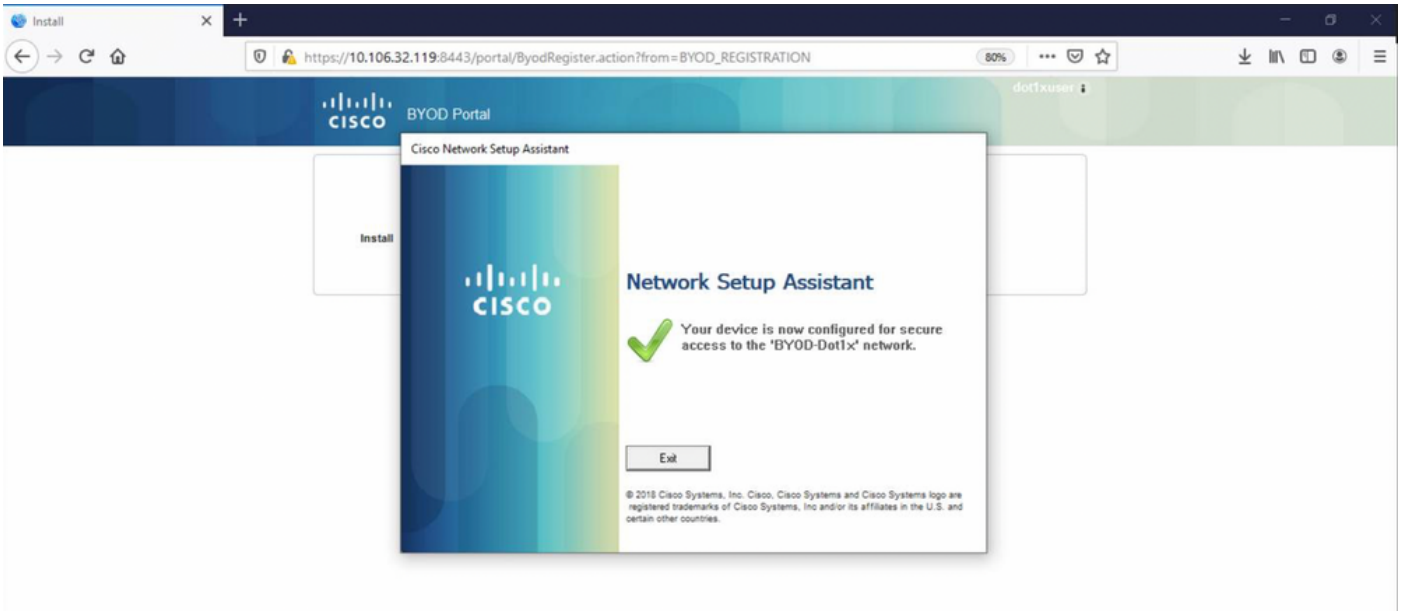
ise-psc.log -

```
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
```

在证书安装后，客户端使用EAP-TLS启动另一个身份验证并获得完全访问权限。

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
```

客户端日志（spw日志）

客户端启动下载配置文件。

```
[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
```

客户端检查WLAN服务是否正在运行。

```
[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]
```

客户端开始应用配置文件 —

```
[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]
```

客户端安装证书。

```
[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配置无线配置文件

```
[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]
```

配置文件

```
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.
```