在ISE 3.3中使用单和双SSID配置ISE BYOD

目录

简介

本文档介绍如何在ISE上配置并排除BYOD问题。

背景

BYOD功能允许用户在ISE上注册其个人设备，以便用户可以在环境中使用网络资源。它还可以帮助网络管理员限制用户从个人设备访问关键资源。

与访客流不同，访客页面使用内部存储或ISE上的Active directory对设备进行身份验证。BYOD允许网络管理员在终端上安装终端配置文件，以选择EAP方法的类型。在EAP-TLS等场景中，客户端证书由ISE自身签名以在终端和ISE之间创建信任。

先决条件

Cisco 建议您了解以下主题：

- WLC控制器
- ISE基础知识

使用的组件

这些使用的设备不限于BYOD流程的一个特定版本：

- Catalyst 9800-CL无线控制器(17.12.3)
- ISE虚拟机(3.3)

什么是ISE上的单SSID和双SSID BYOD?

单SSID BYOD

在单SSID BYOD设置中，用户将其个人设备直接连接到公司无线网络。自注册过程发生在同一SSID上，其中ISE促进设备注册、调配和策略实施。此方法可简化用户体验，但需要安全自注册和适当的身份验证方法来确保网络安全。

双SSID BYOD

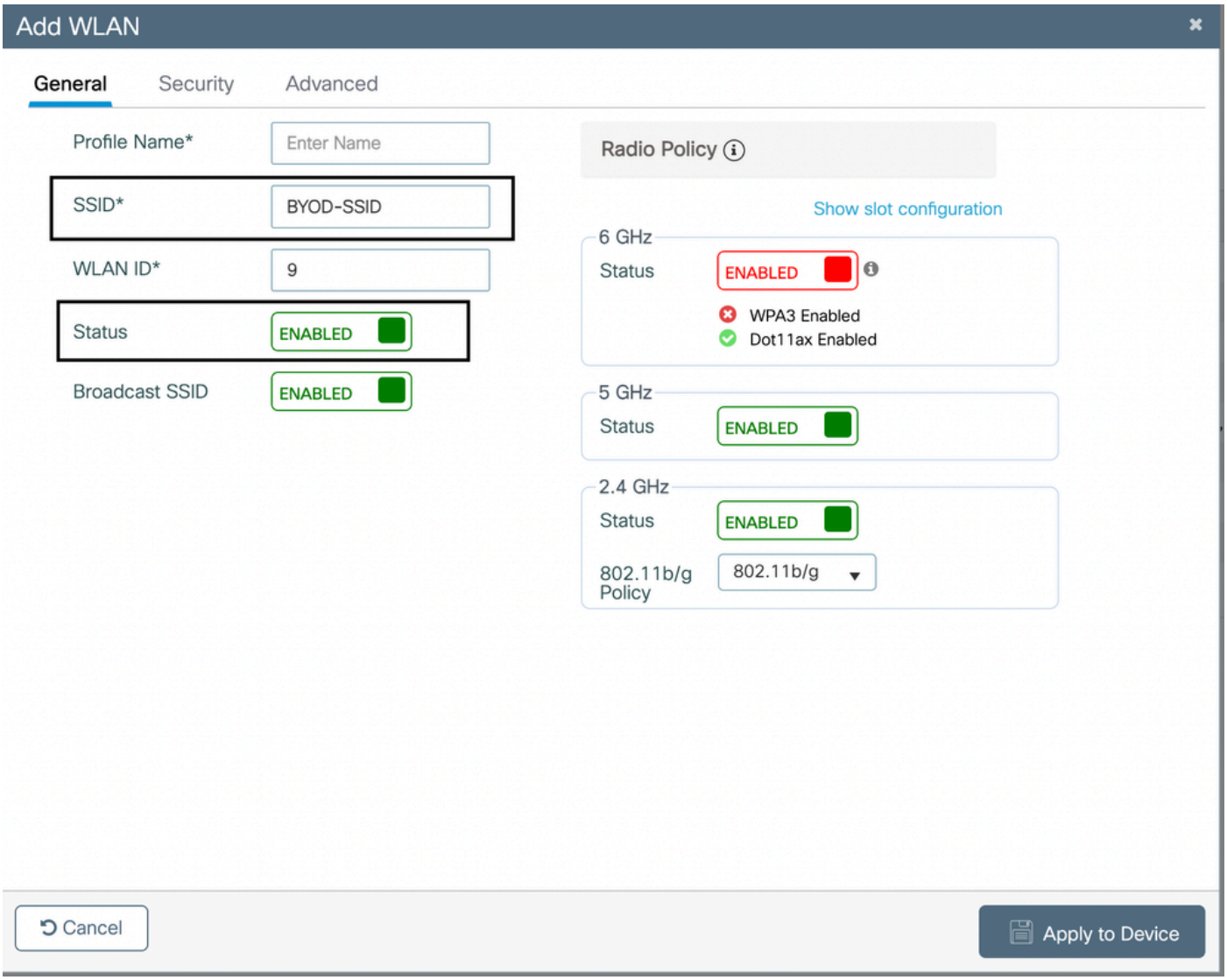
在双SSID BYOD设置中，使用两个单独的SSID:一个用于自注册（不安全或受限访问），另一个用于访问公司网络。用户最初连接到自注册SSID，通过ISE完成设备注册和调配，然后切换到安全的企业SSID进行网络访问。这样可以将入网流量与生产流量隔离，从而提供额外的安全层。

WLC 配置

为CWA创建WLAN

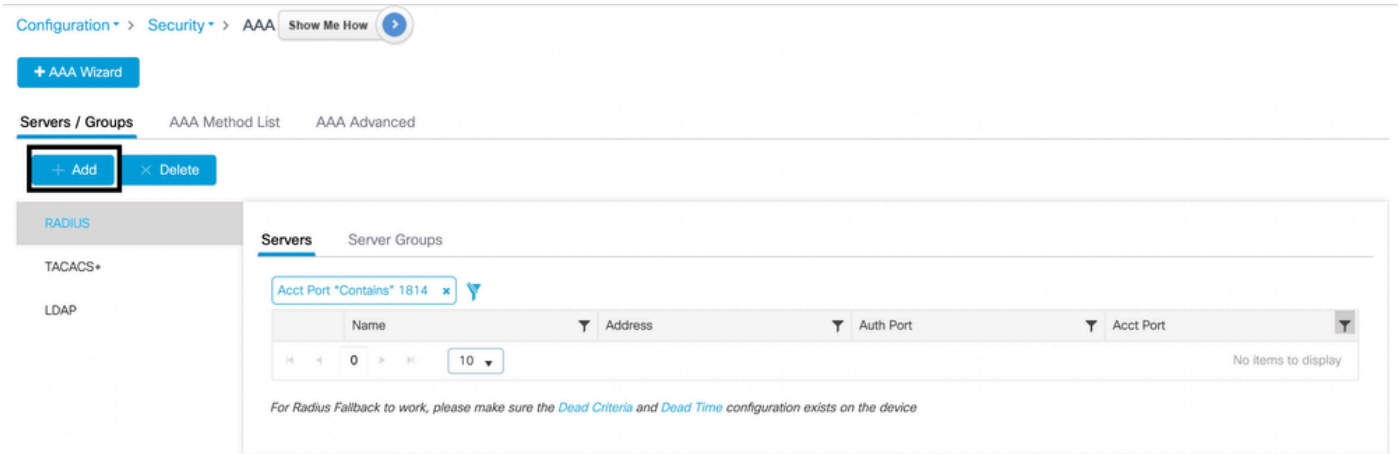
1. 转至Configuration > Tags & Profiles > WLANs。
2. 单击Add以创建新的WLAN。

- 设置WLAN名称和SSID（例如，BYOD-WiFi）。
- 启用WLAN。

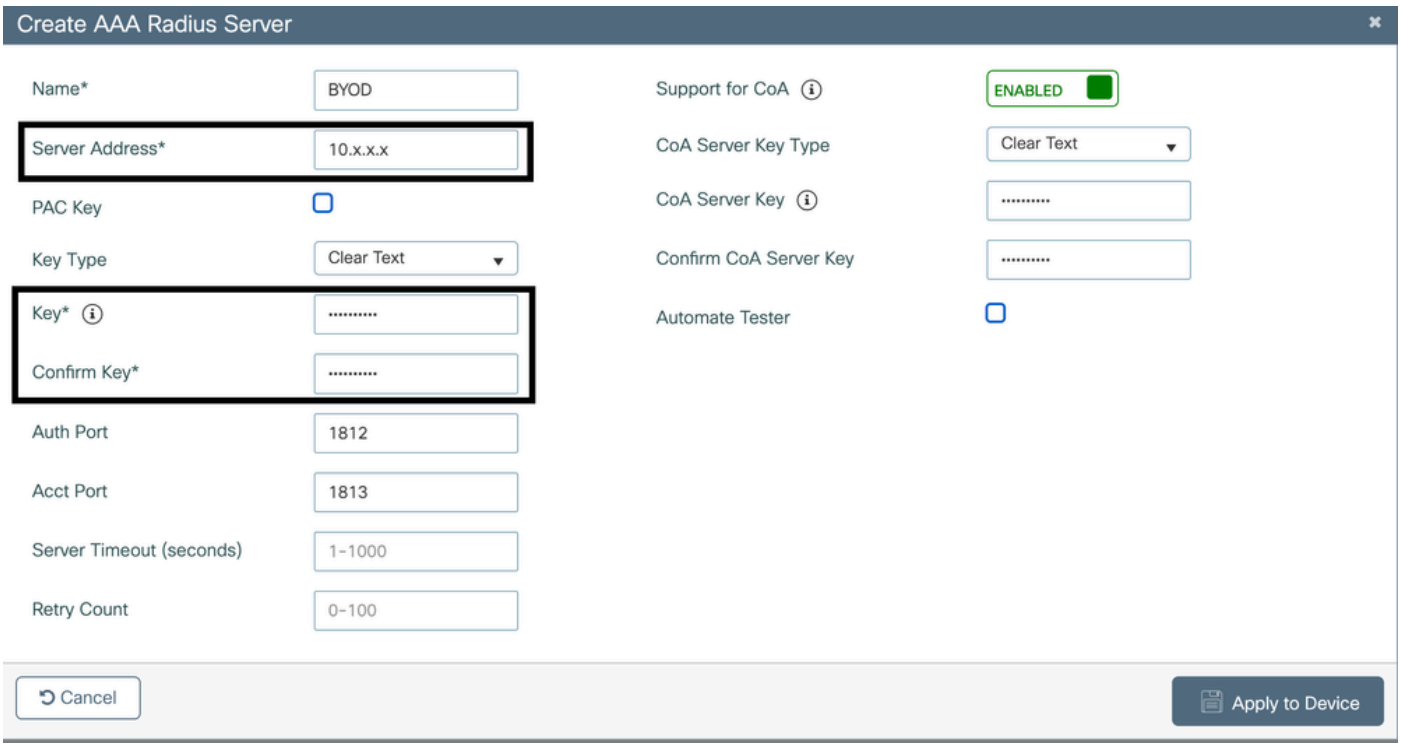


配置 RADIUS 服务器

1. 导航到Configuration > Security > AAA > RADIUS > Servers。

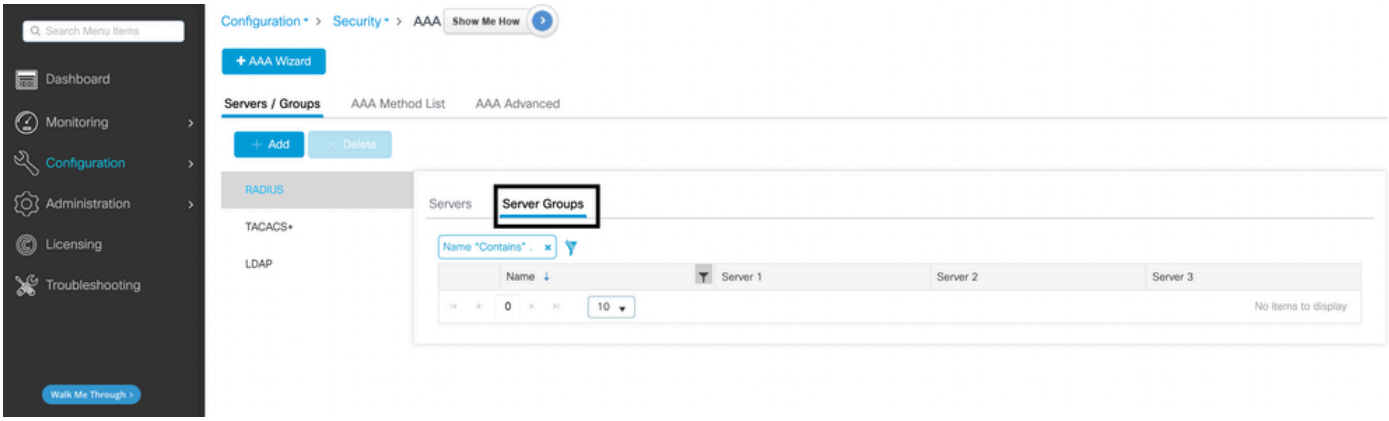


2. 单击Add将ISE配置为RADIUS服务器：
    - 服务器 IP: ISE的IP地址
    - 共享密钥:匹配ISE上配置的共享密钥。

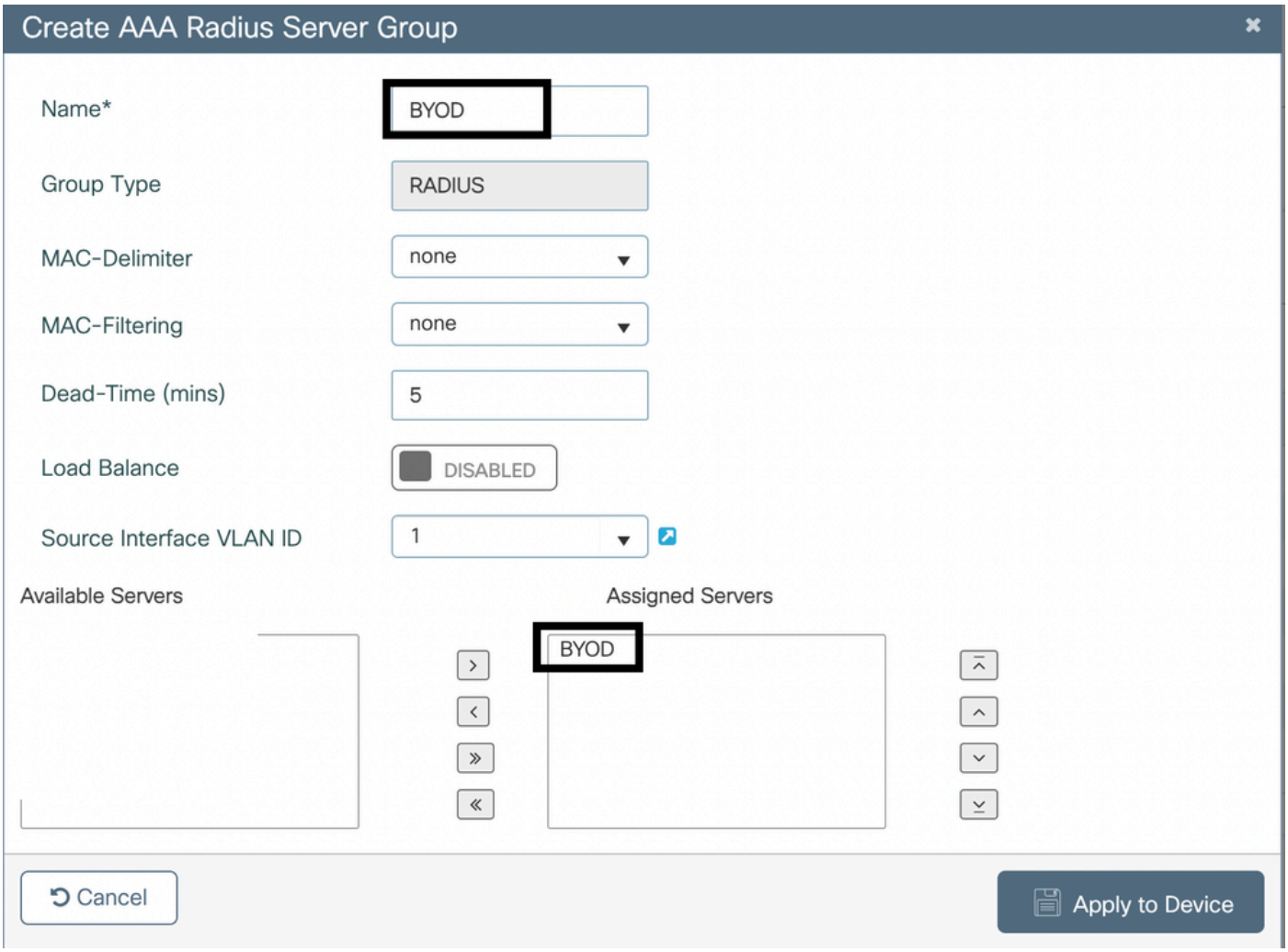


配置AAA服务器

1. 导航到配置>安全> AAA >服务器/组。



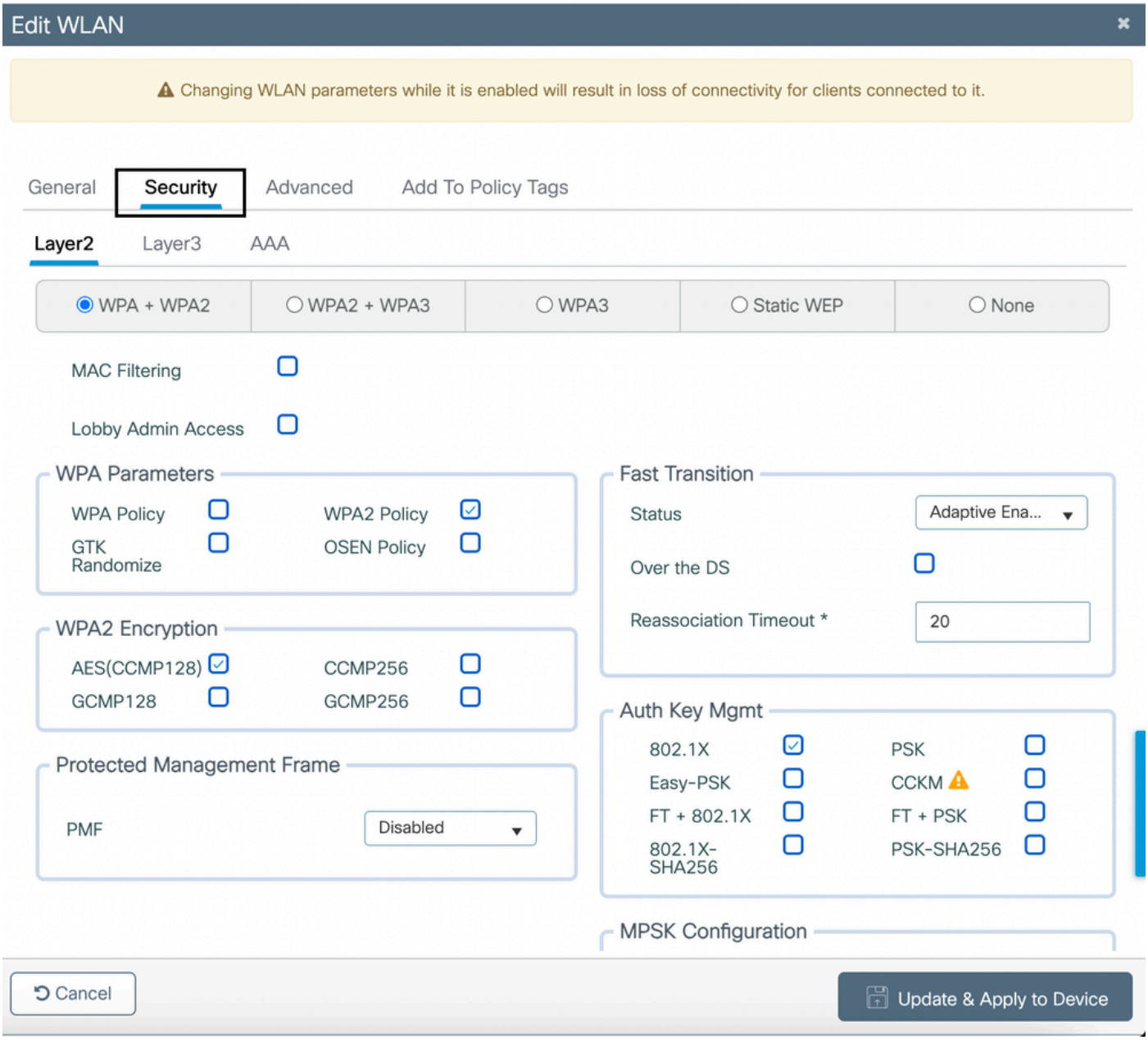
2. 将RADIUS服务器分配给新的或现有的服务器组。



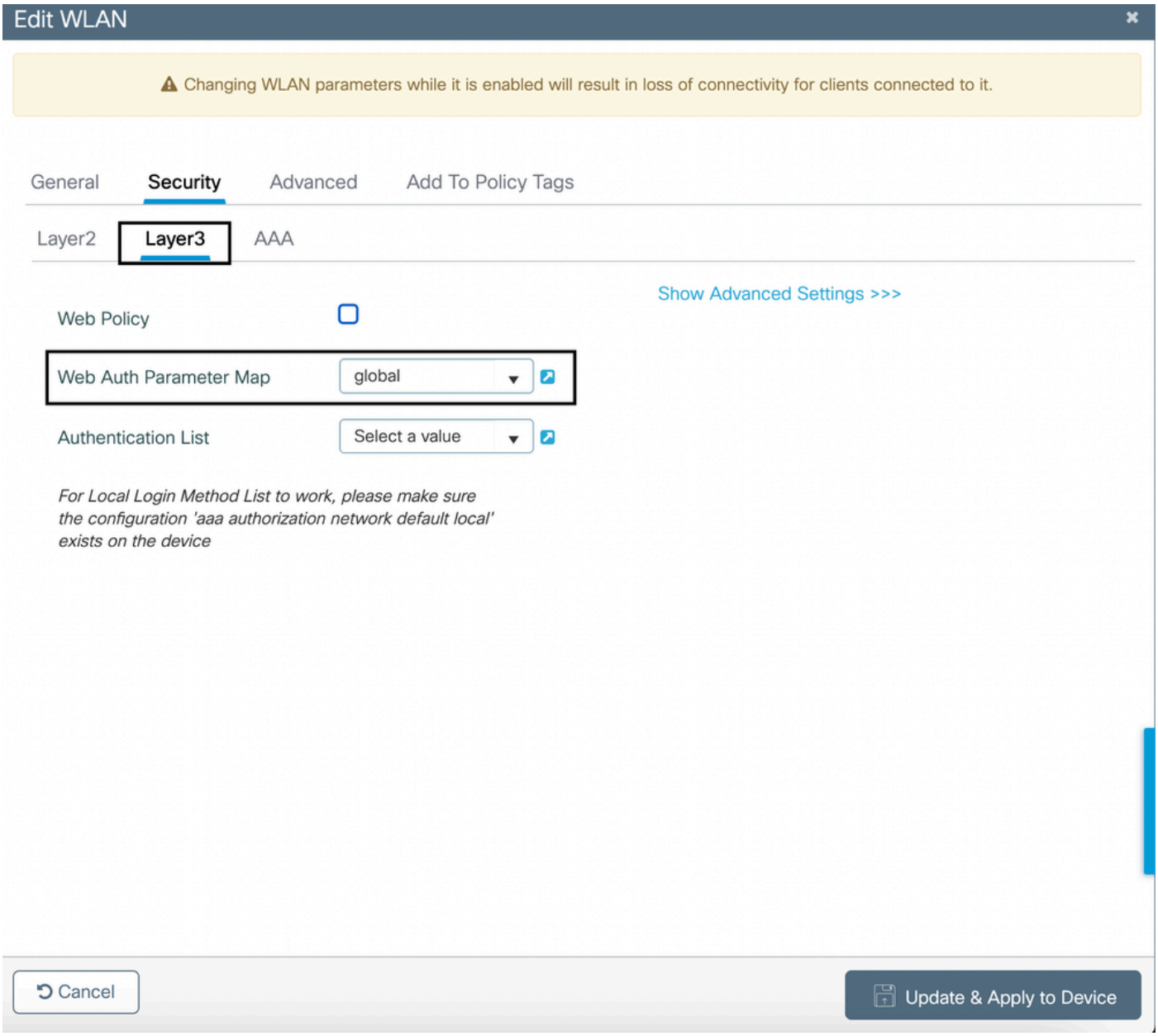
配置WLAN的安全策略

1. 导航到配置>标签和配置文件> WLAN。编辑之前创建的WLAN。

2. 在Security > Layer 2选项卡下：
   - 启用WPA+WPA2
   - 在WPA2加密下设置AES(CCMP128)
   - 身份验证密钥管理为802.1X



3. 在Security > Layer 3选项卡下，从Web Auth Parameter Map下拉列表中选择全局。



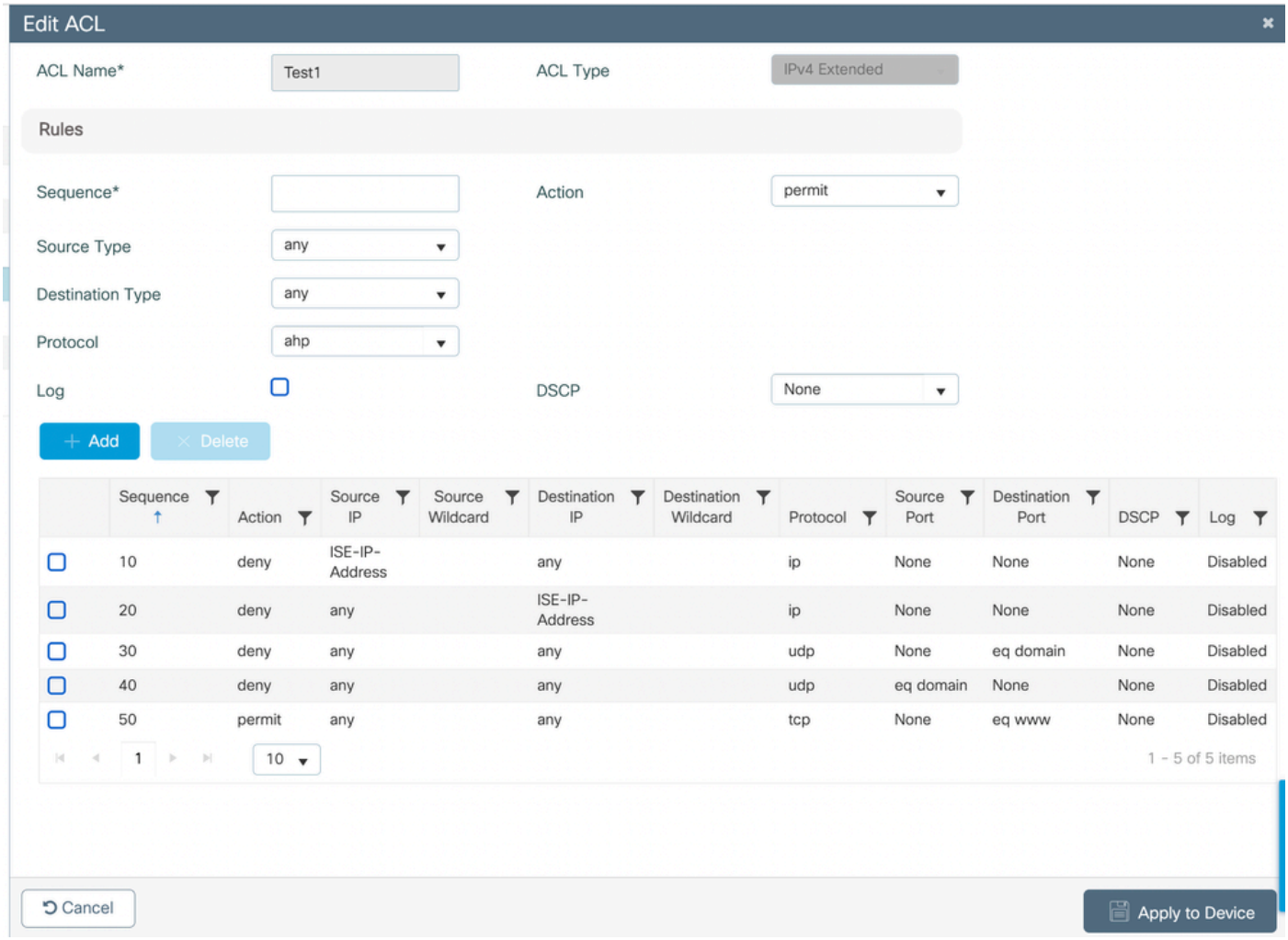
配置预身份验证ACL

创建ACL以允许使用重定向操作：

- DNS流量。
- 通过HTTP/HTTPS连接到ISE门户。
- 任何所需的后端服务。

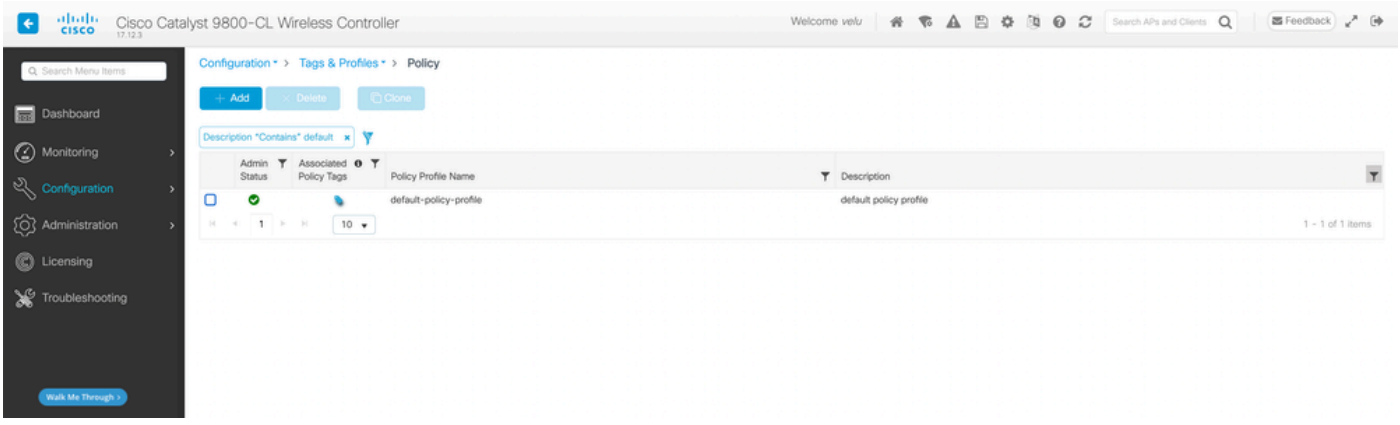
为此，请执行以下操作：

1. 导航到配置>安全> ACL >访问控制列表。
2. 创建包含规则的新ACL以允许必要的流量。

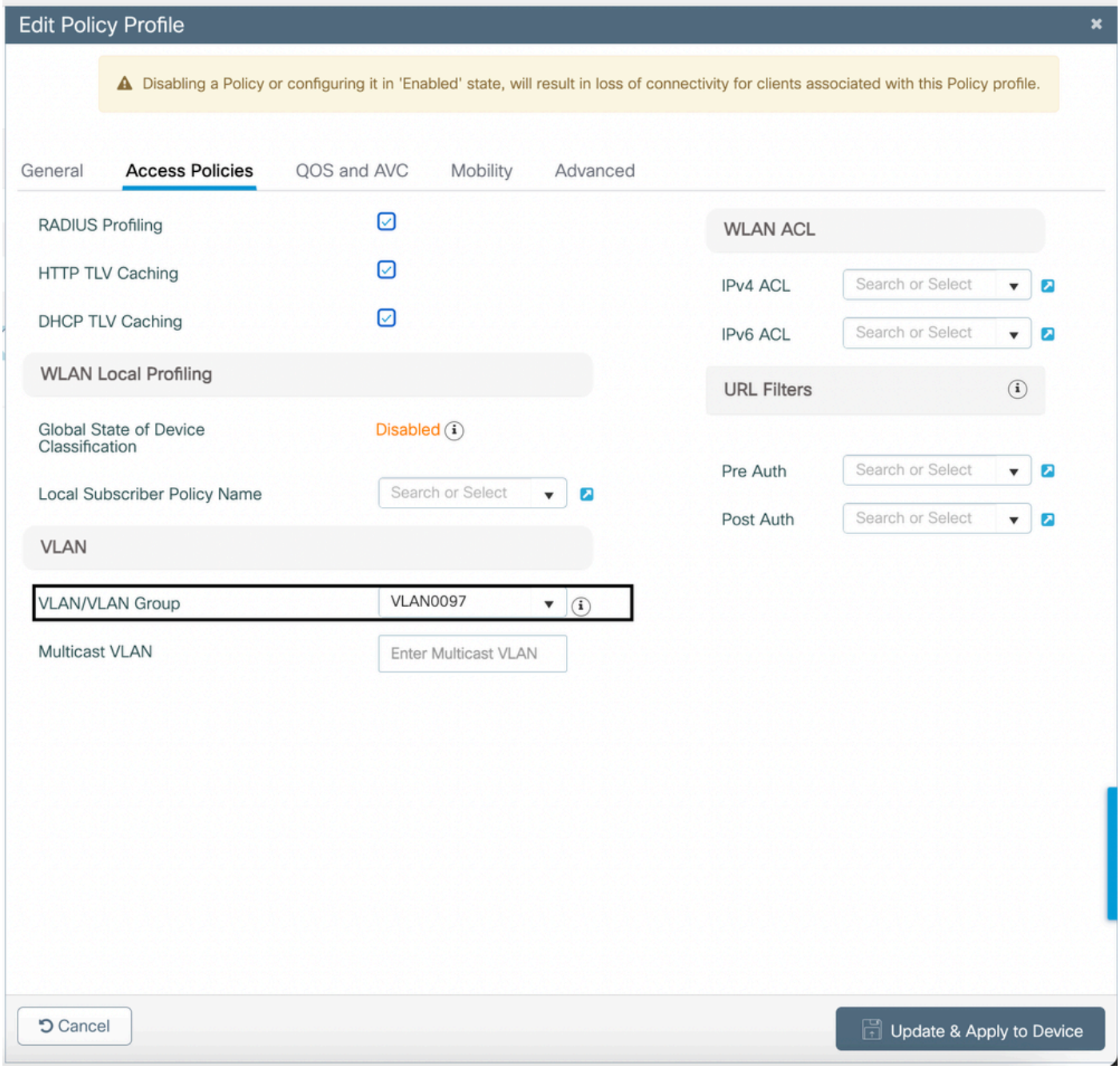


配置策略配置文件

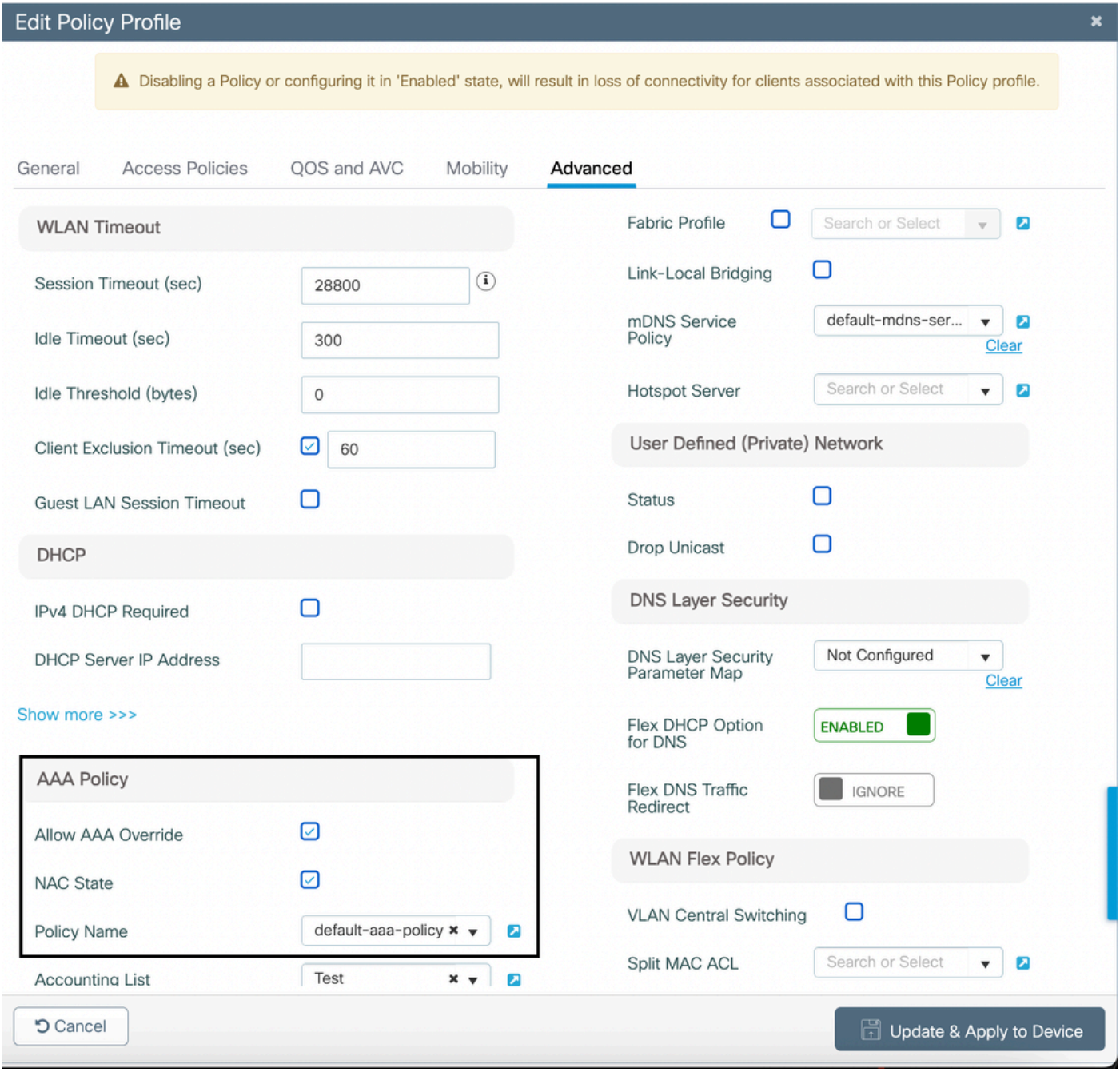
1. 导航至配置 > 标签和配置文件 > 策略。您可以创建或使用默认策略



2. 在Access Policies下分配适当的VLAN

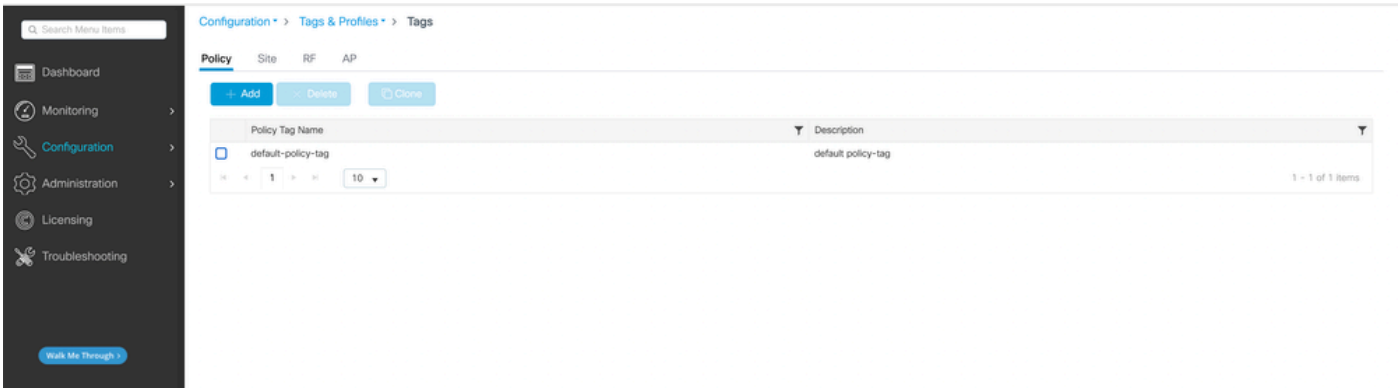


3.还要在策略的高级下启用允许AAA覆盖和NAC状态。



应用标记和部署

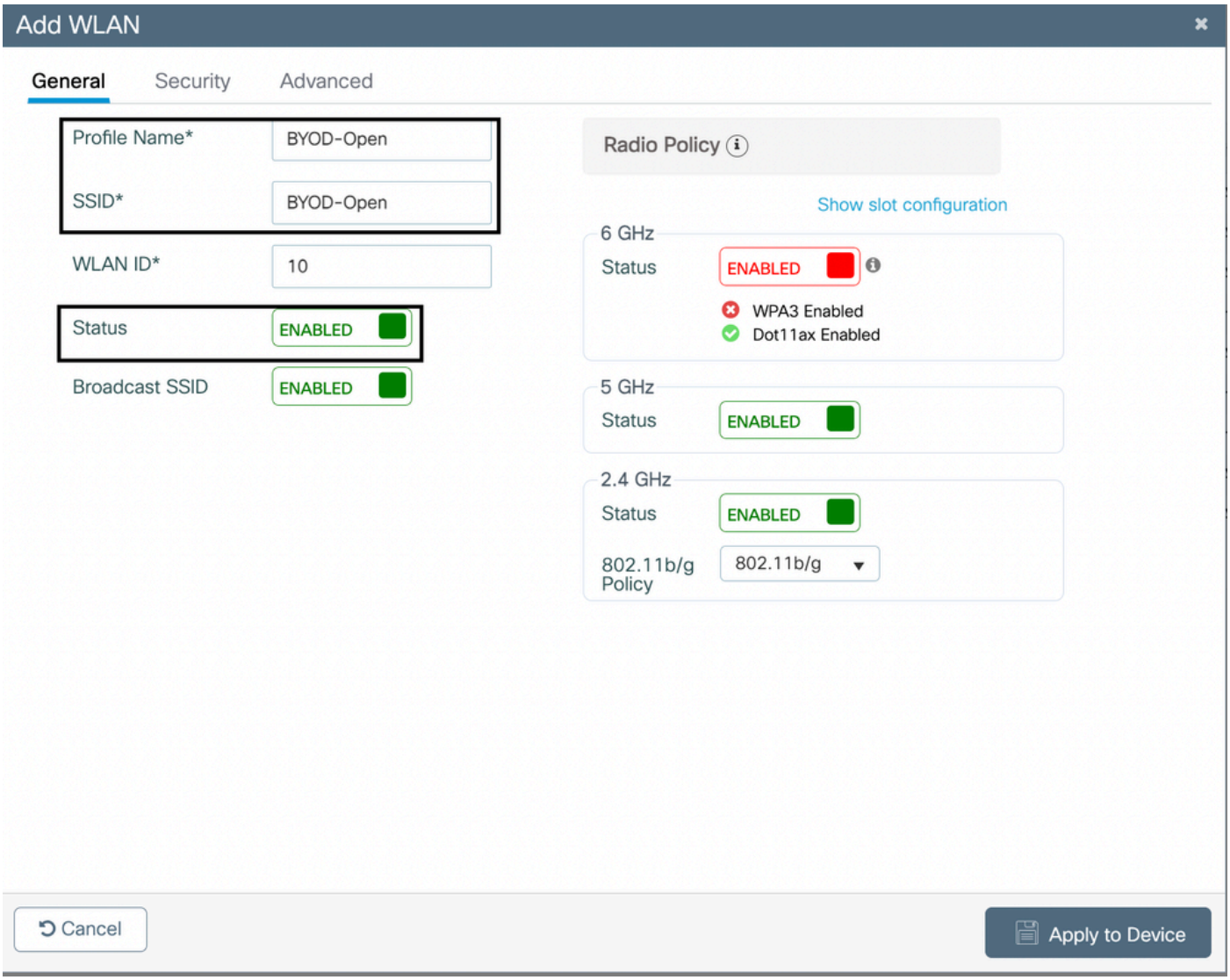
- 导航到配置>标签和配置文件>标签。
- 创建或编辑标记以包括WLAN和策略配置文件。
- 将标签分配给接入点。



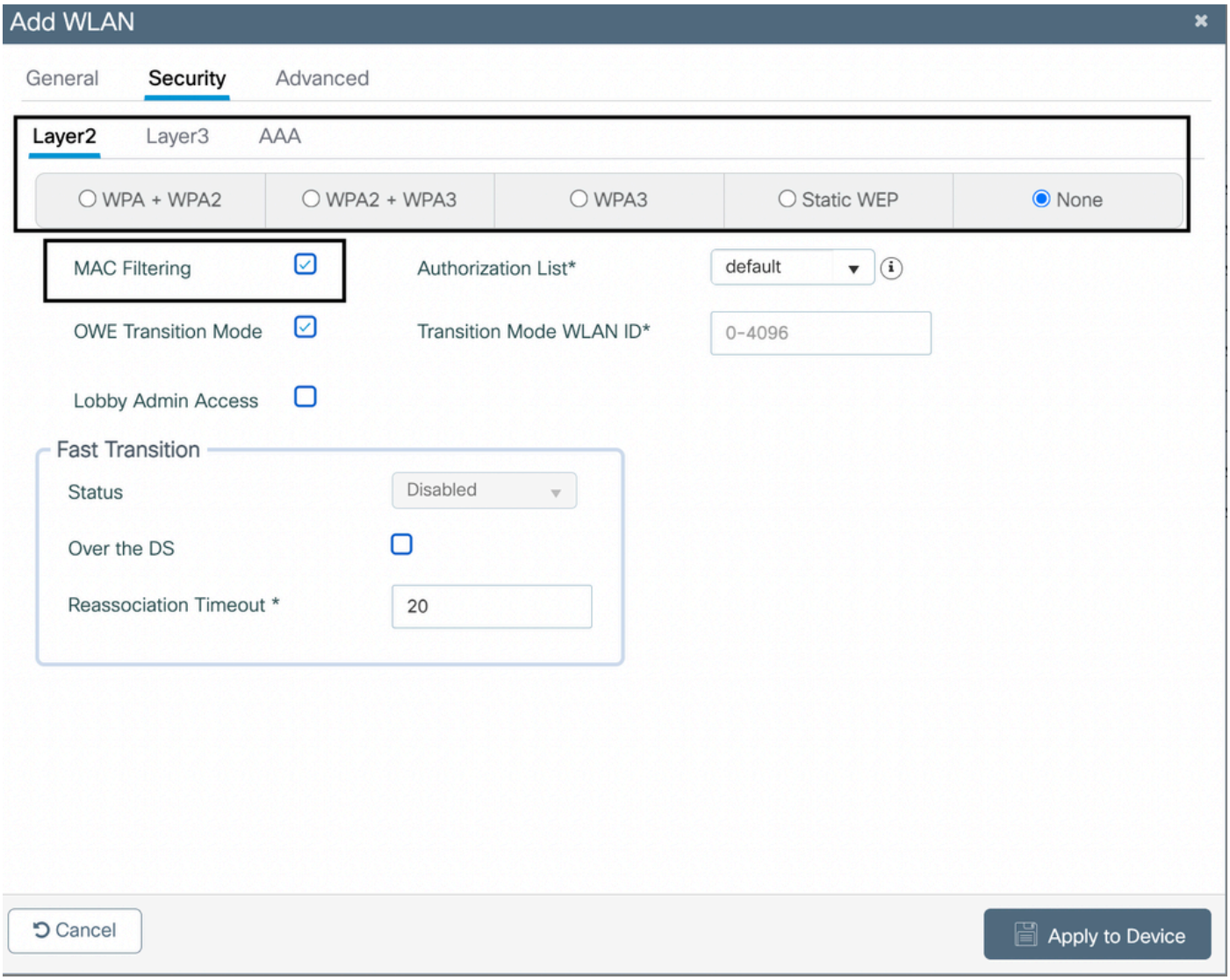
配置开放/不安全SSID

只有在您决定环境中使用双SSID BYOD配置时，才会创建开放SSID。

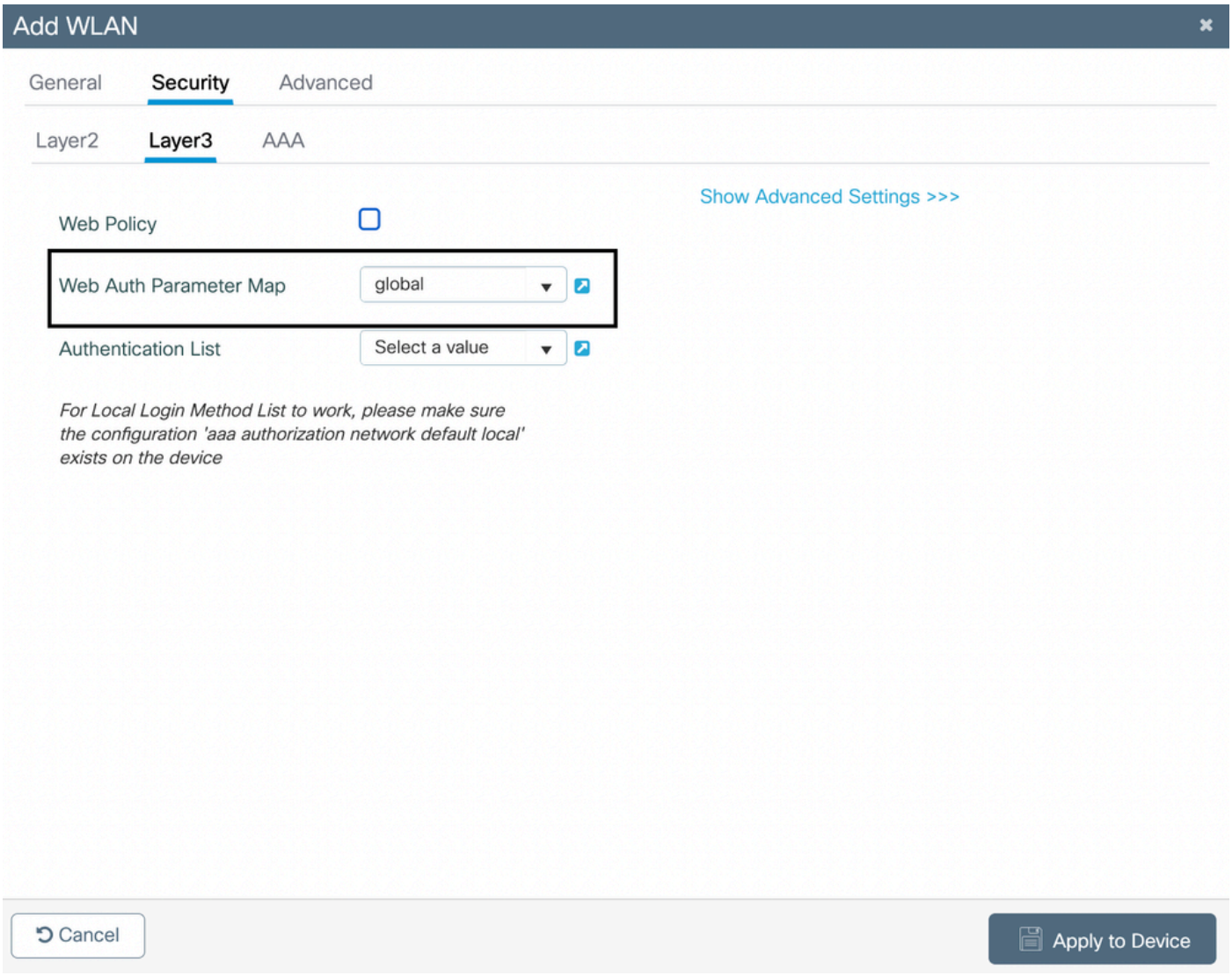
1. 导航到配置>标签和配置文件> WLAN。单击 Add 按钮。
2. 在General选项卡下提供SSID名称并启用WLAN按钮。



3.从同一窗口中单击Security选项卡。选择None单选按钮并启用Mac过滤。



4.在Layer 3中的Security下，选择Web Auth Parameter Map的全局设置。如果您在WLC上配置了任何其他网络身份验证配置文件，也可以将其映射到此处：



ISE 配置

前提条件

- 确保Cisco ISE已安装并获得BYOD功能许可。
- 将您的WLC作为具有RADIUS共享密钥的网络设备添加到ISE。

证书

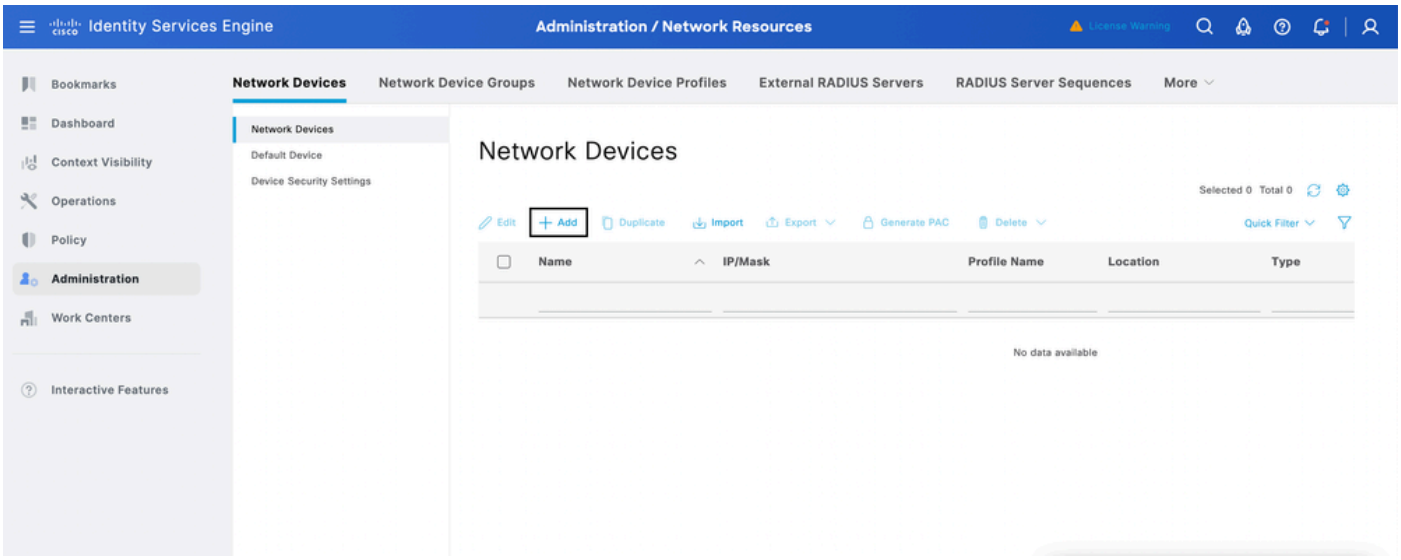
- 在ISE上安装有效的服务器证书以避免浏览器安全警告。
- 确保证书受终端信任（由已知CA或具有受信任根的内部CA签名）。

DNS 配置

- 确保DNS解析BYOD门户的ISE主机名。

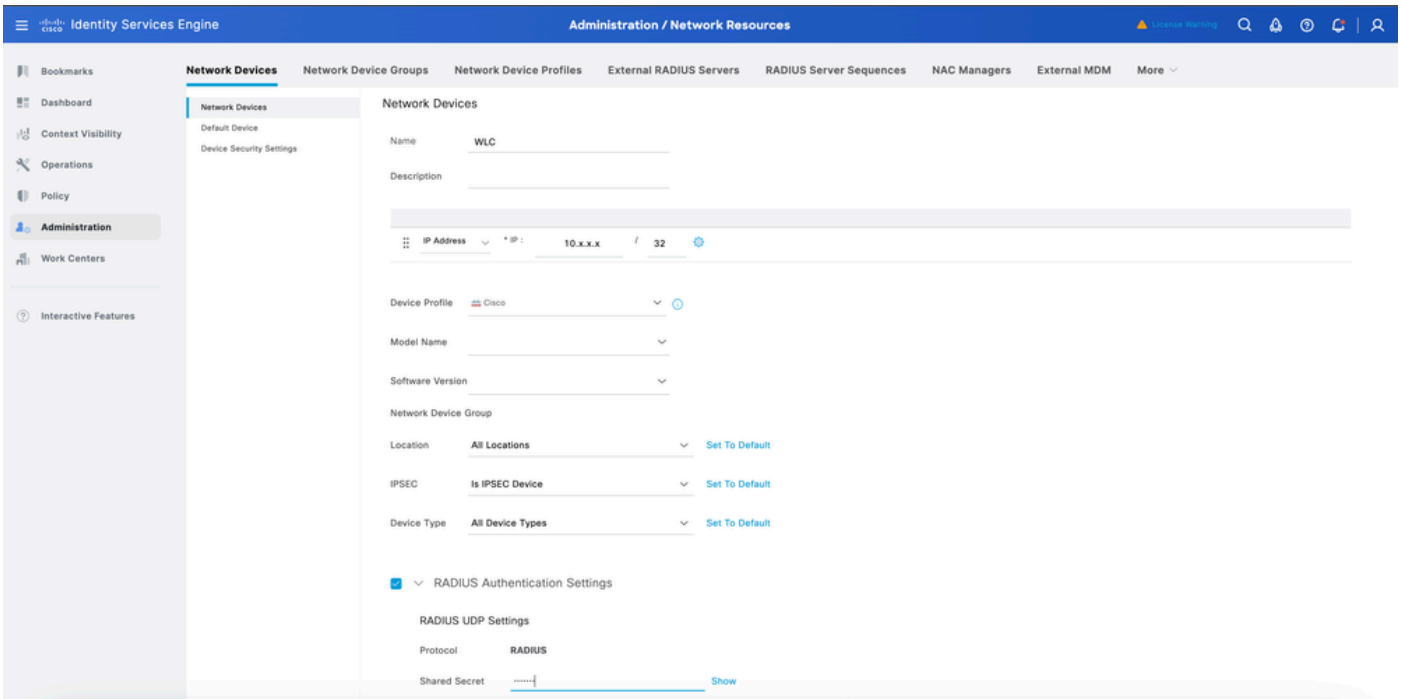
配置ISE网络设备

1. 登录到ISE Web UI。
2. 导航到Administration > Network Resources > Network Devices。



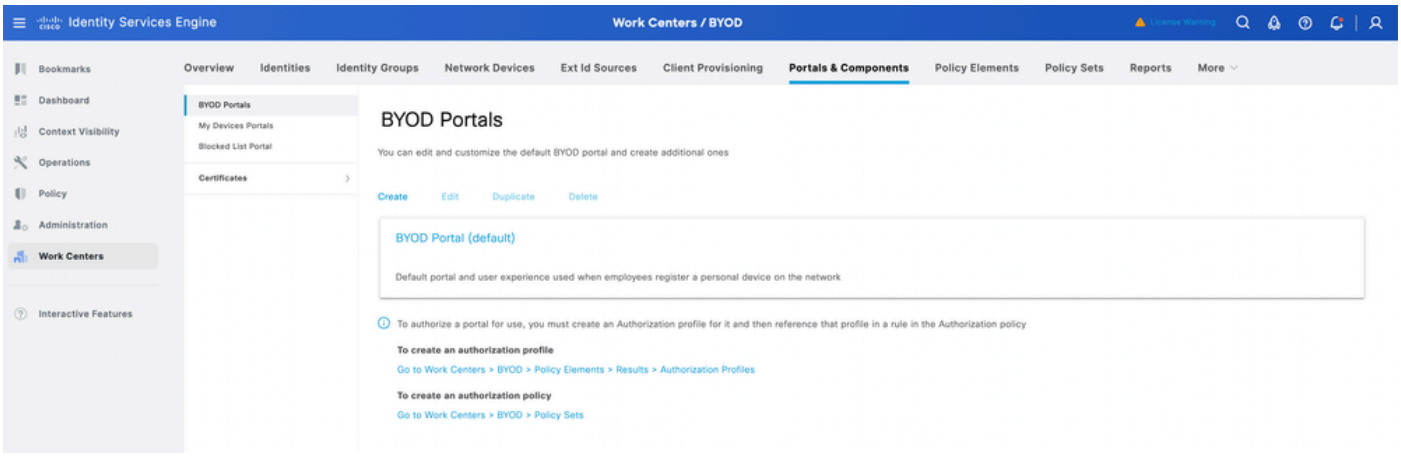
3.将WLC添加为网络设备：

- 名称：输入WLC的名称。
- IP Address:输入WLC管理IP。
- RADIUS共享密钥:输入与WLC上配置的共享密钥。
- 单击 submit。



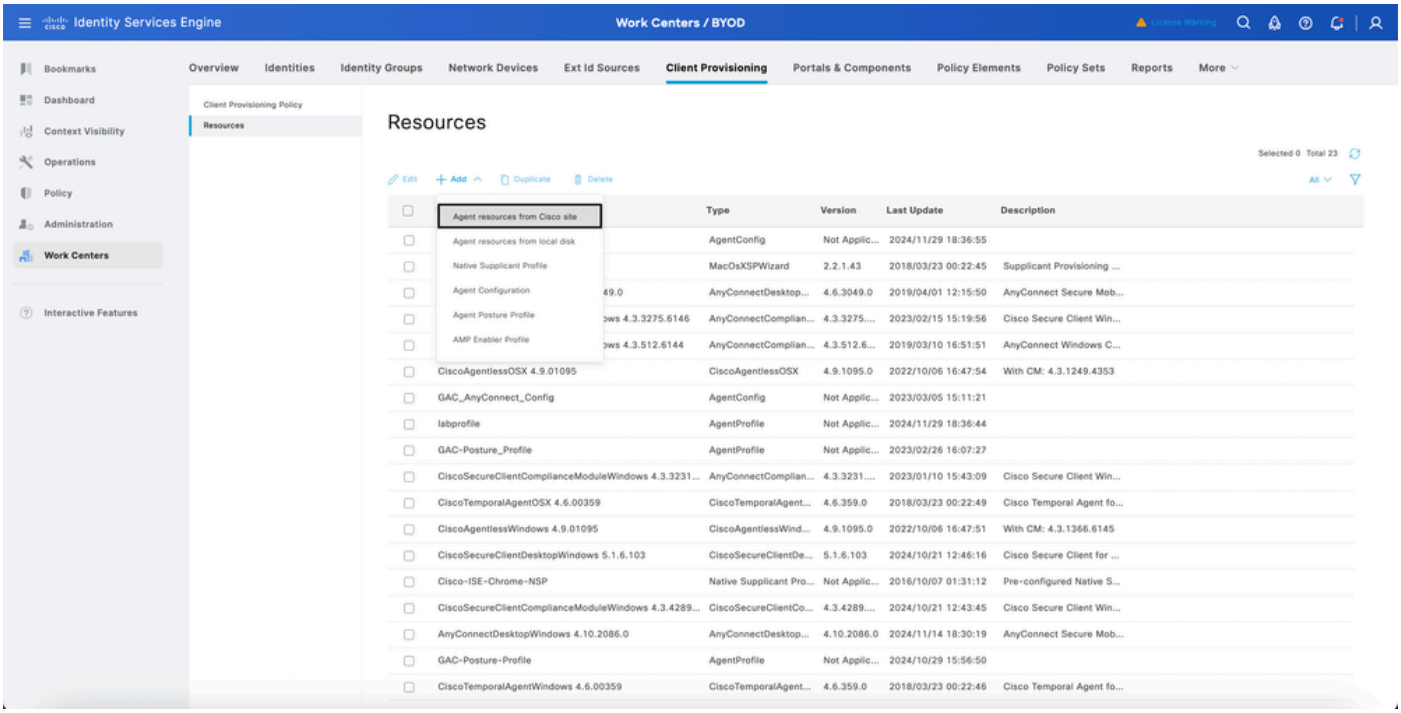
创建BYOD门户

1. 导航至工作中心> BYOD >设置>门户和组件> BYOD门户。
2. 点击Add以创建BYOD门户，或者您可以在ISE上使用现有默认门户。



下载Cisco IOS®最新版本

1. 导航到工作中心> BYOD >客户端调配>资源。
2. 单击Add按钮，然后从思科站点中选择座席资源。



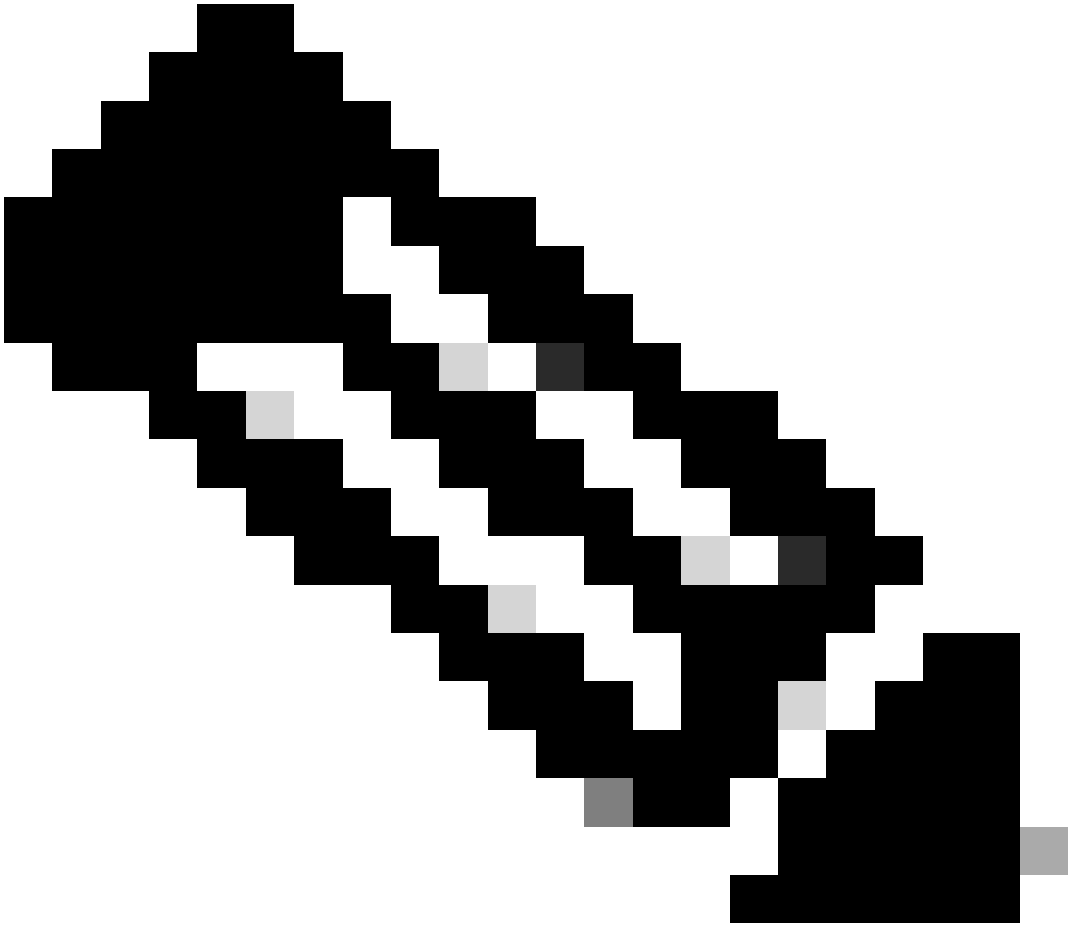
3.在软件列表中，选择要下载的最新Cisco IOS版本。

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

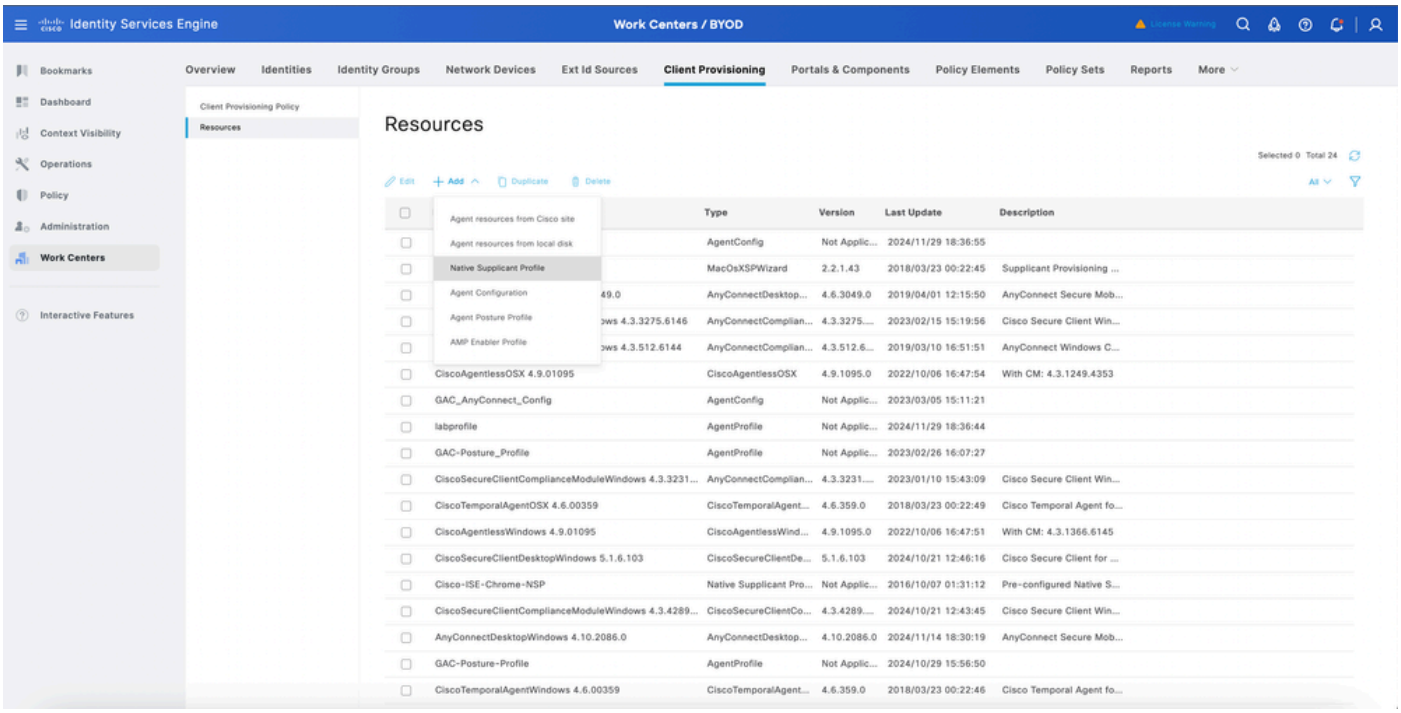


注意：思科IOS软件在适用于Windows和MacOS终端的ISE上下载。对于Apple iPhone IOS，它使用本地请求方来调配设备；对于android设备，您需要从Play Store下载网络设置助手。

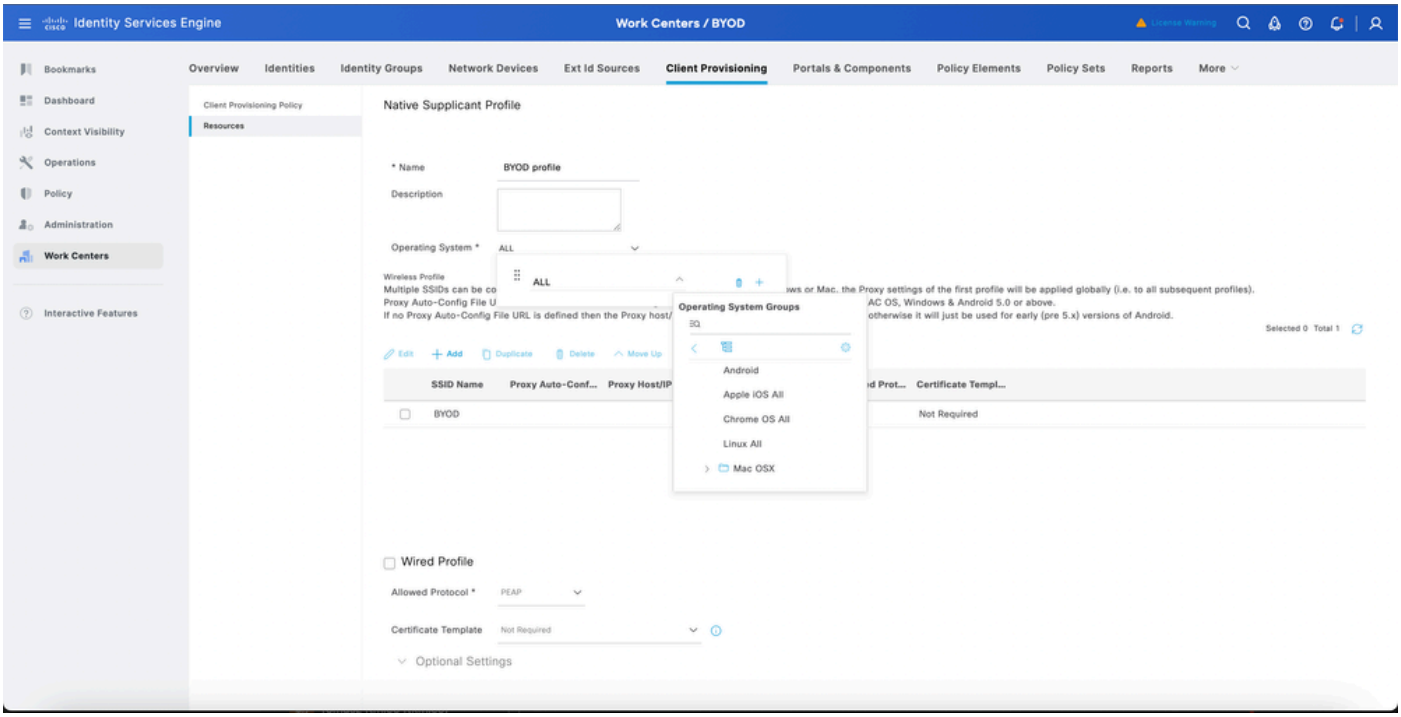
创建终端配置文件

1.导航至工作中心> BYOD >客户端调配>资源。

2.单击Add，从下拉菜单中选择Native supplicant profile。



3.在Operating system下拉菜单下，请选择您要装入设备的所需操作系统，或者您可以将其设置为ALL以装入环境中的所有终端：



4.从页面点击Add以创建终端配置文件，为终端配置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

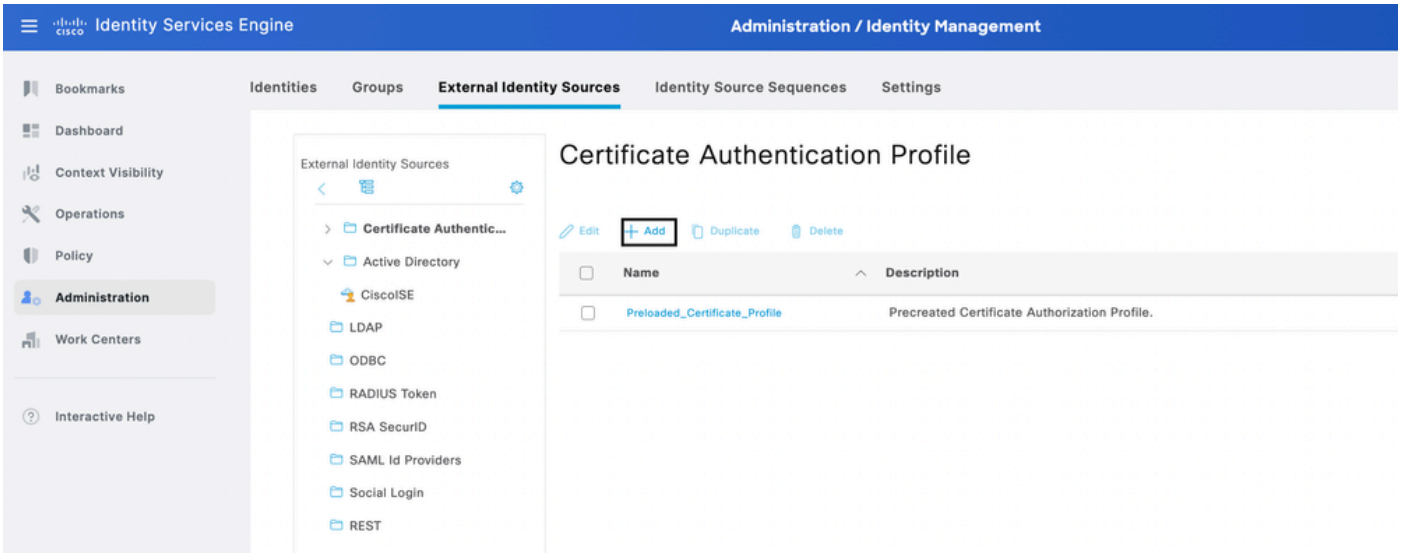
Certificate Enrollment Protocol:

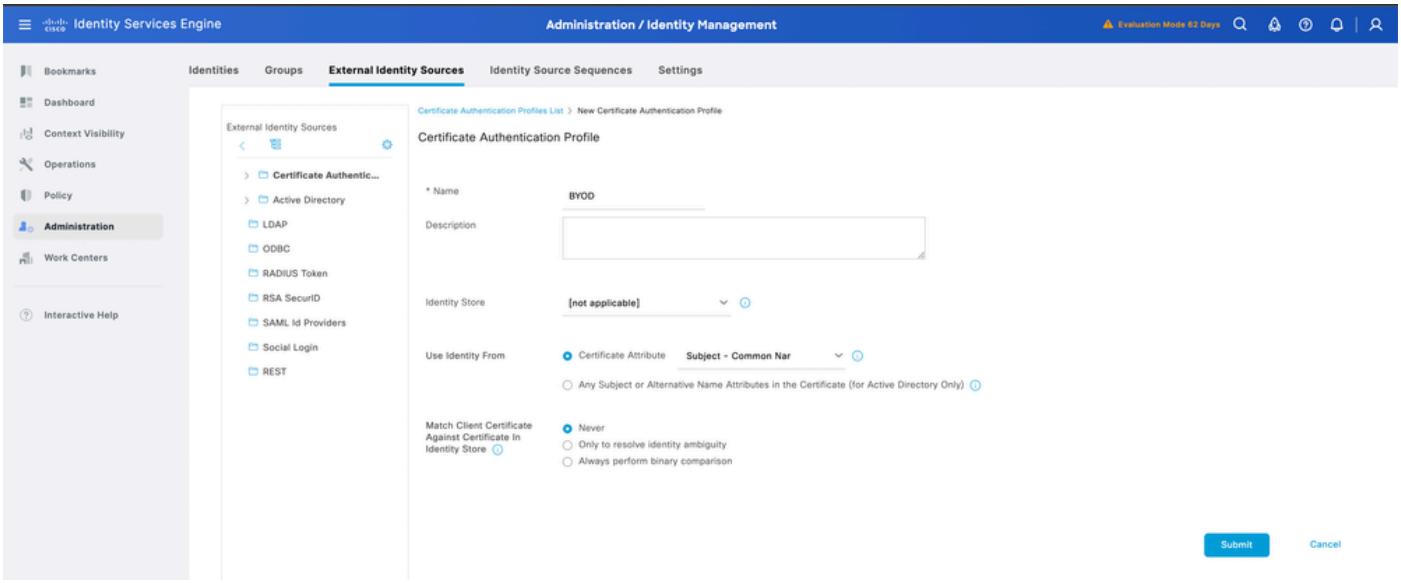
调配，其中“代理配置”部分确定为终端安全评估检查实施的终端安全评估代理和合规性模块，而“本地请求方配置”部分管理BYOD调配流的设置

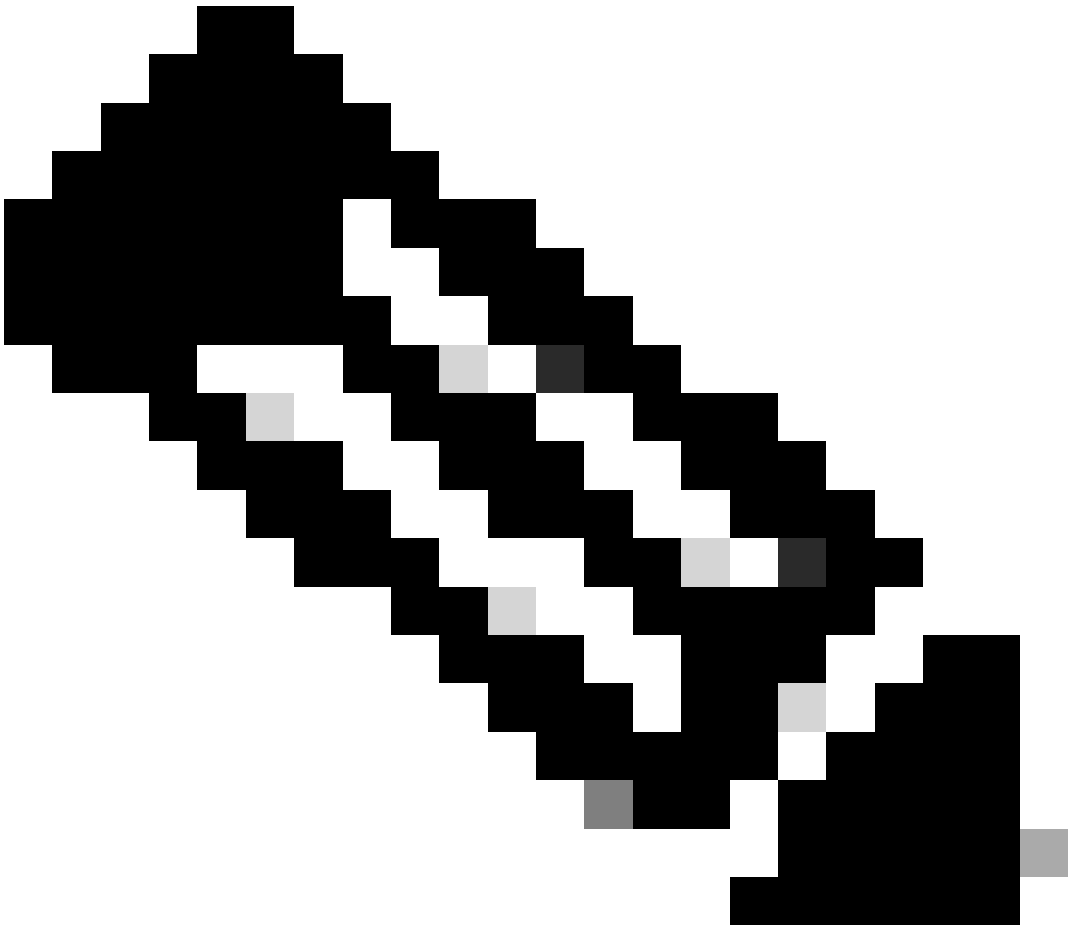
为单SSID BYOD配置ISE策略集

1. 导航到Policy > Policy Set，并在ISE上为BYOD流创建策略：

2.然后，导航到管理>身份管理>外部身份源>证书身份验证配置文件。单击Add按钮以创建证书配置文件：

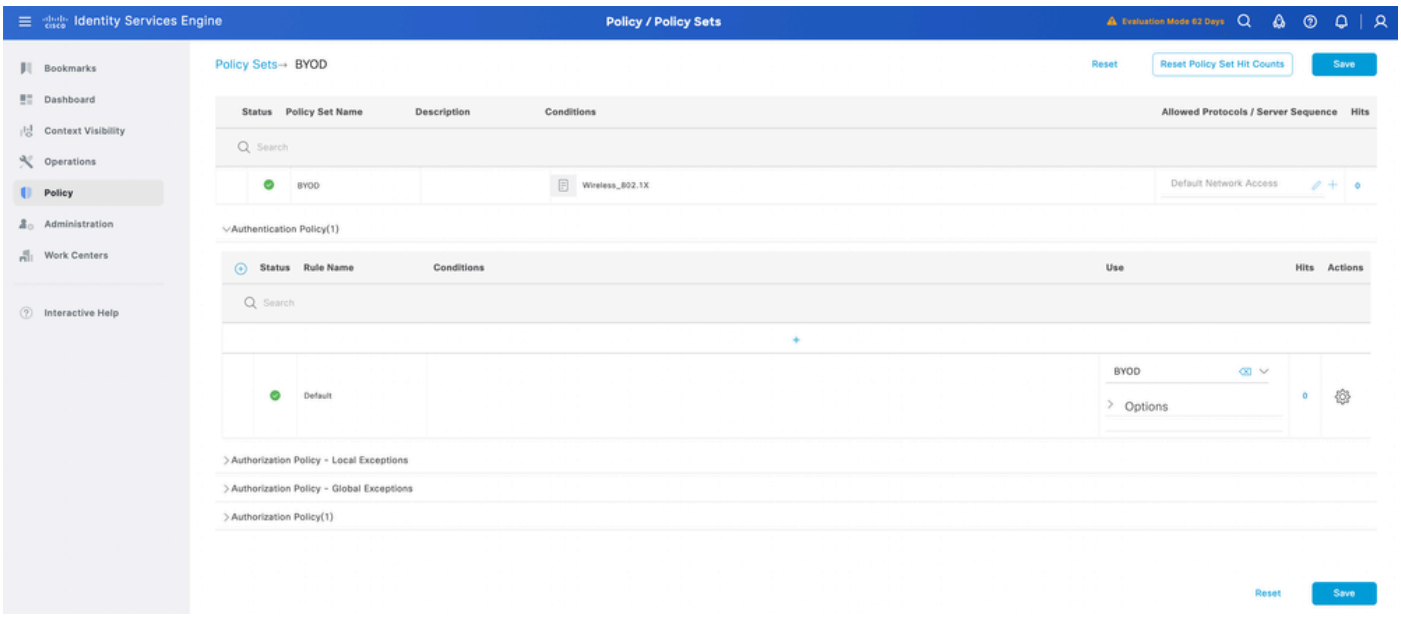






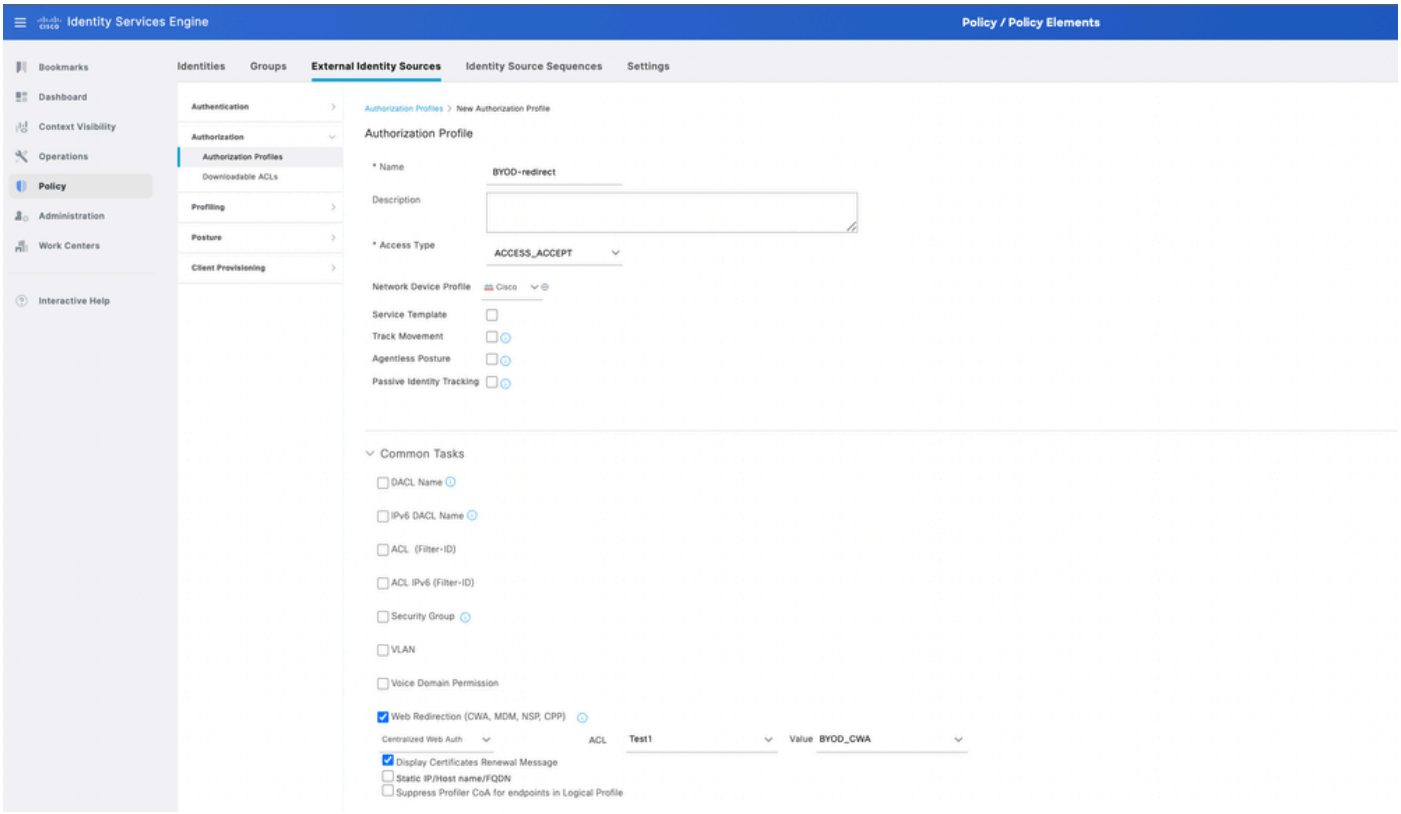
注意：在身份库中，您可以始终选择已集成到ISE的Active Directory，以从证书执行用户查找来获得附加安全性。

3.单击Submit保存配置。然后，将证书配置文件映射到为BYOD设置的策略：



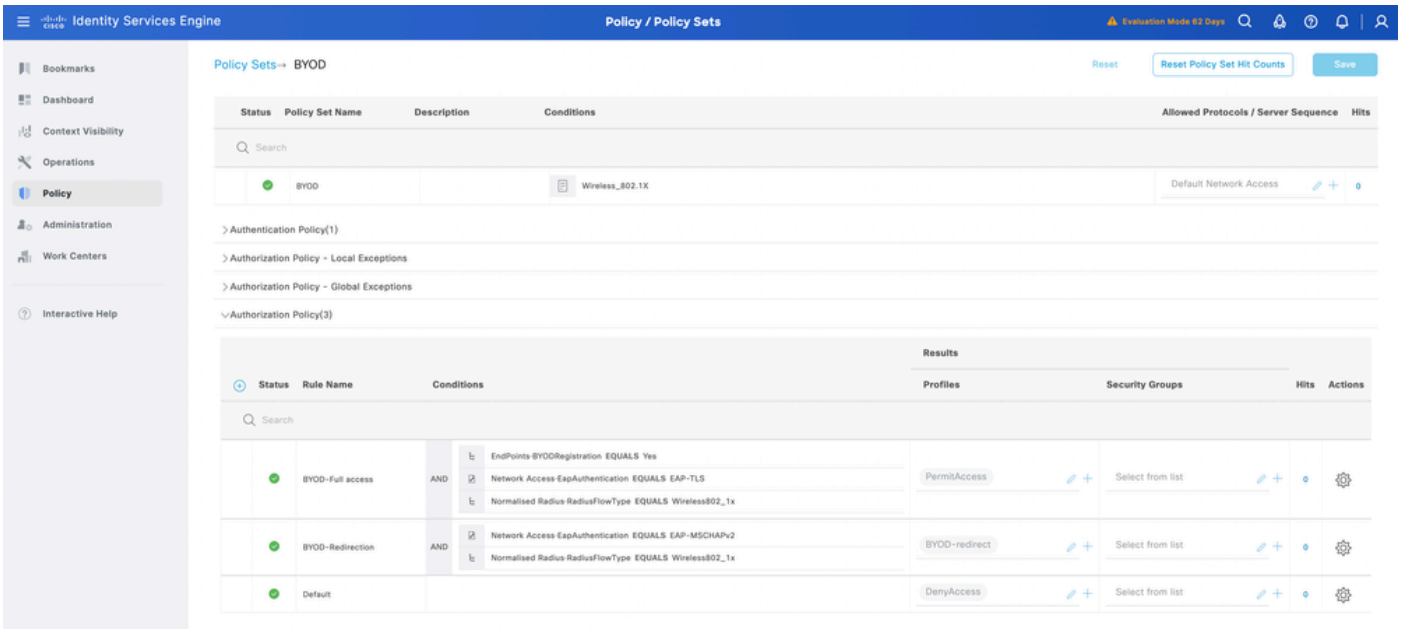
4.配置BYOD重定向的授权配置文件和BYOD流程后的完全访问权限。导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。

5.单击Add并创建授权配置文件。检查Web重定向(CWA、MDM、NSP、CPP)并映射BYOD门户页面。此外，将重定向ACL名称从WLC添加到配置文件。对于Full access配置文件，使用配置文件中的各个公司VLAN配置允许访问。



6.将授权配置文件映射到授权规则。BYOD完全访问权限必须具有EndPoints·BYODegistration相等

的规则yes，以便用户在BYOD流程后获得网络的完全访问权限。

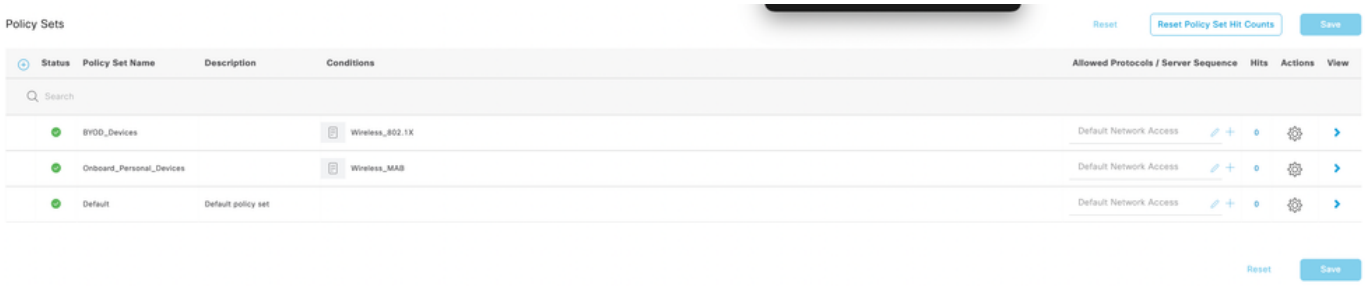


为双SSID BYOD配置ISE策略集

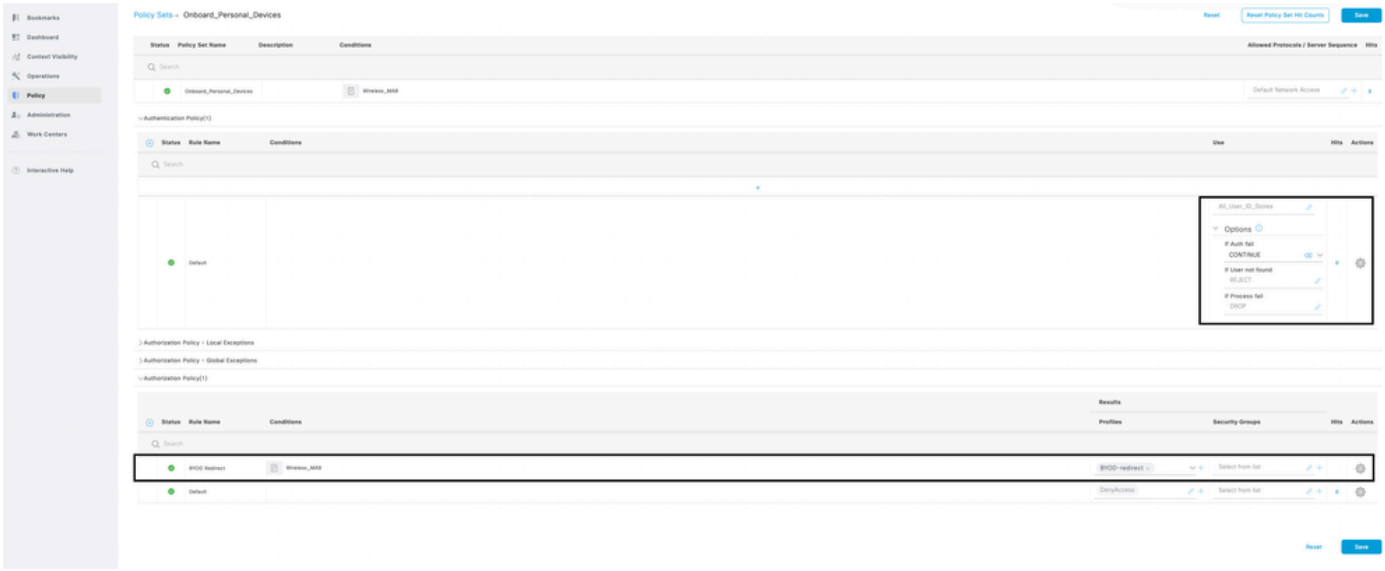
在双SSID BYOD配置中，在ISE上配置双策略集。第一个策略集用于开放/不安全SSID，其中策略集配置在连接到开放/不安全SSID时将用户重定向到BYOD页面

1. 导航到Policy > Policy Set并在ISE上为BYOD流创建策略。

2.为开放/不安全SSID和企业SSID创建策略集，对ISE上的注册BYOD用户进行身份验证。

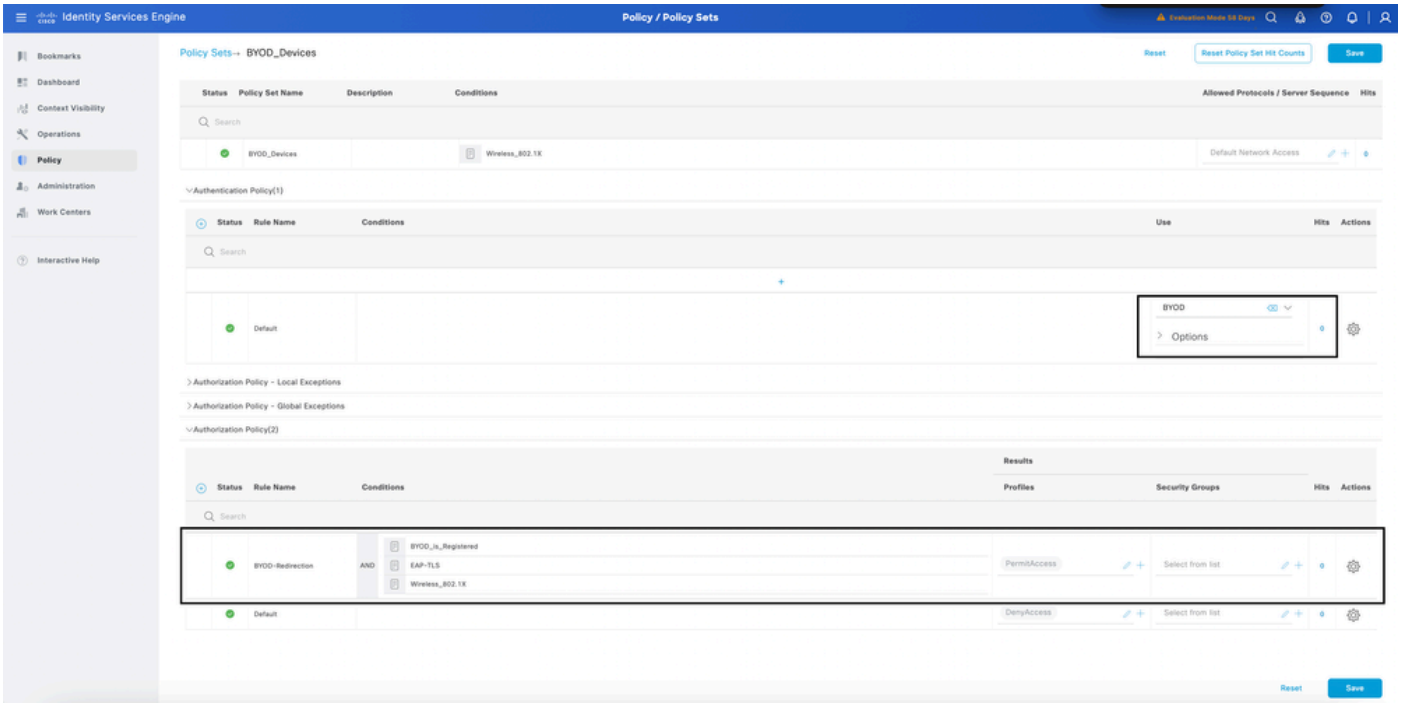


3.在“入职策略”集中，在选项下找到Continue选项。对于授权策略，创建条件并映射重定向授权配置文件。创建授权配置文件时也会涉及相同的步骤，可在第4点中找到。



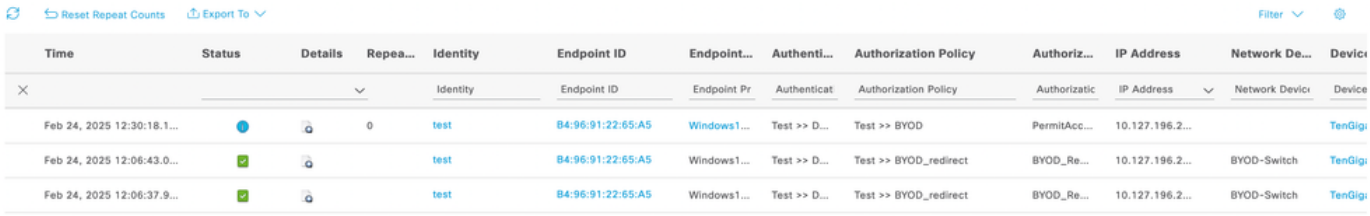
4.在BYOD注册策略集中，使用找到的证书配置文件配置身份验证策略。

在第2点的为单SSID BYOD配置ISE策略集中。还要为授权策略创建条件并将完整访问配置文件映射到策略。

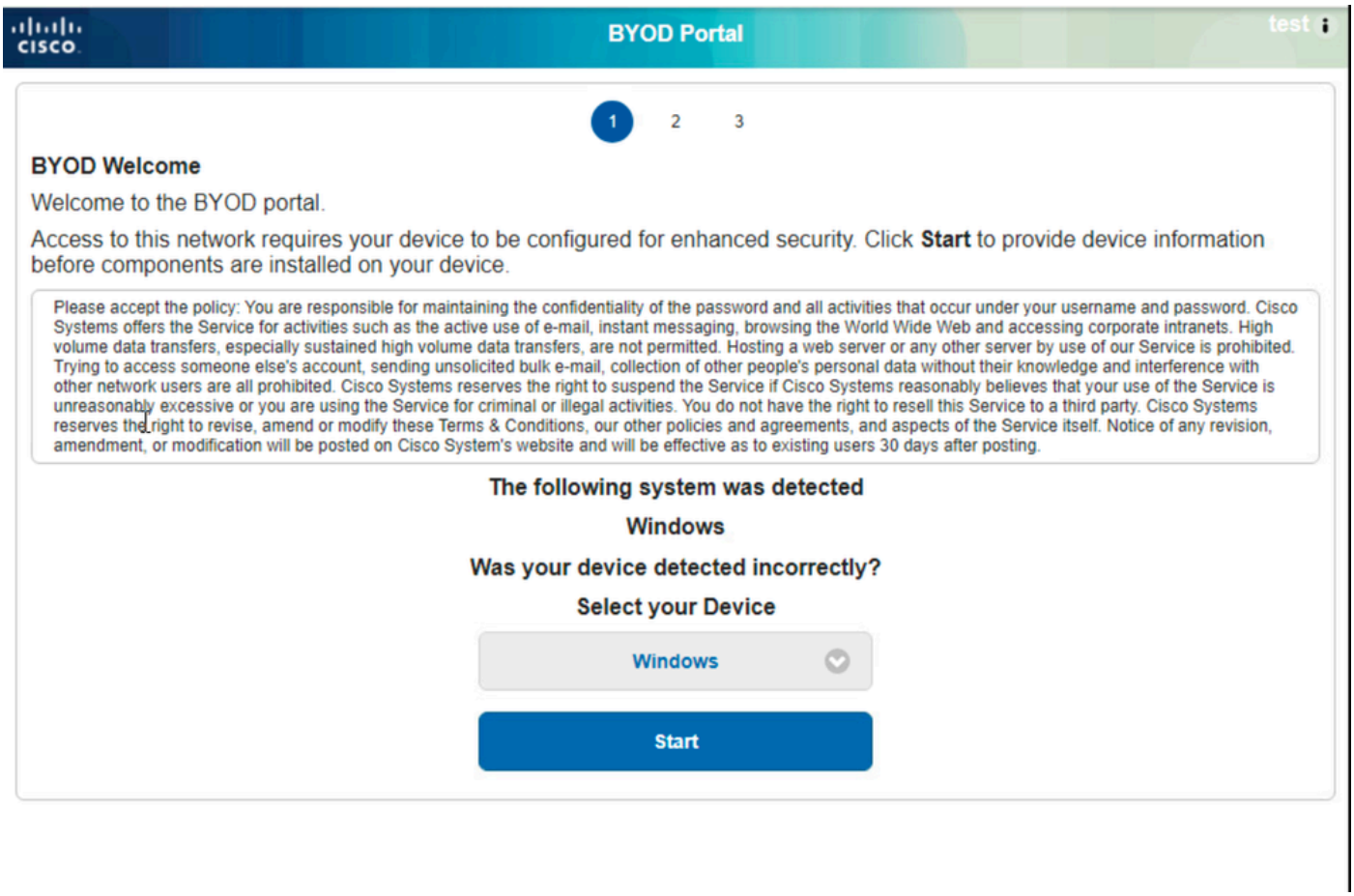


日志记录

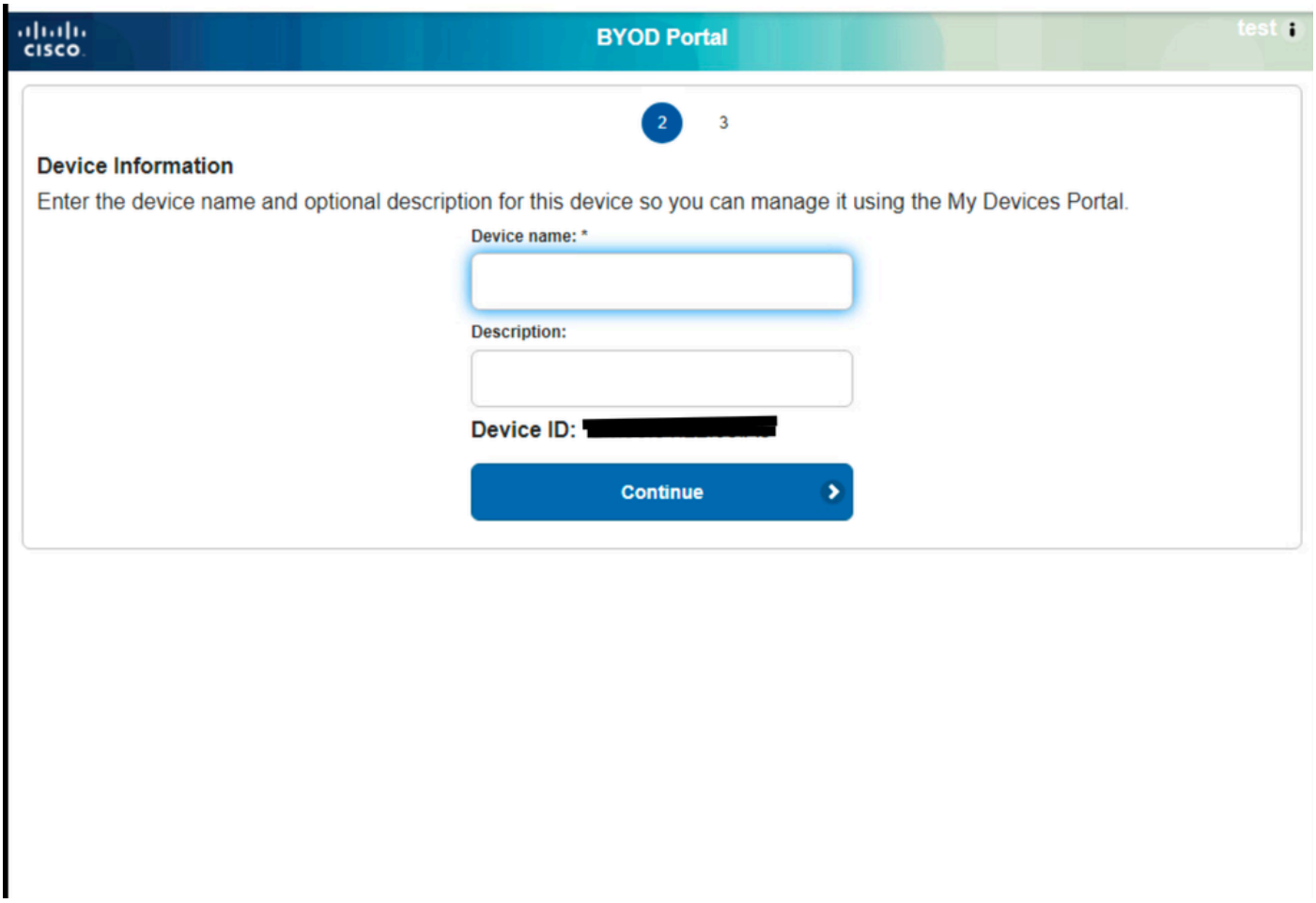
从ISE的实时日志中，用户身份验证将成功，并将重定向到BYOD门户页面。完成BYOD流程后，用户将被授予网络访问权限



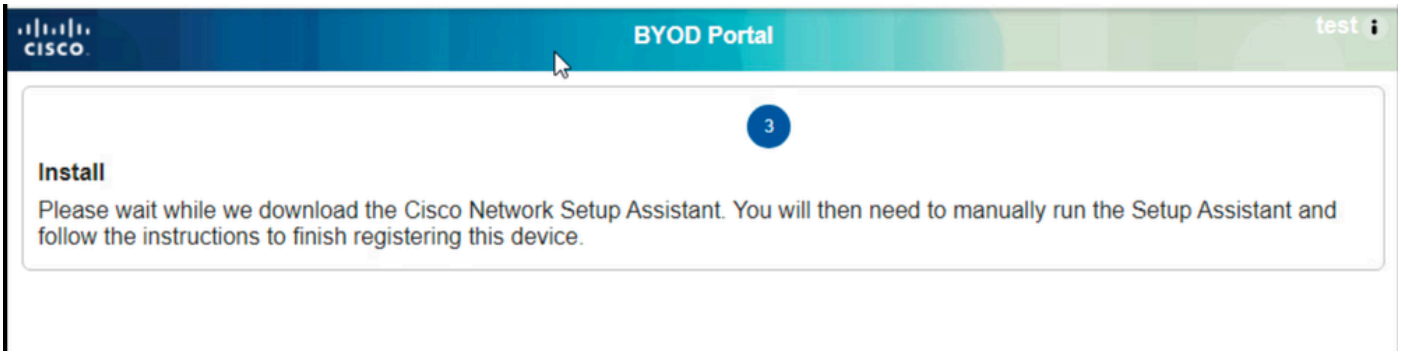
从用户的角度来看，首先会将它们重定向到BYOD页面，并且需要从网页中选择适当的设备。用于测试Windows 10设备



点击Next按钮后，如果要求用户输入设备名称和说明，您会转到相应页面

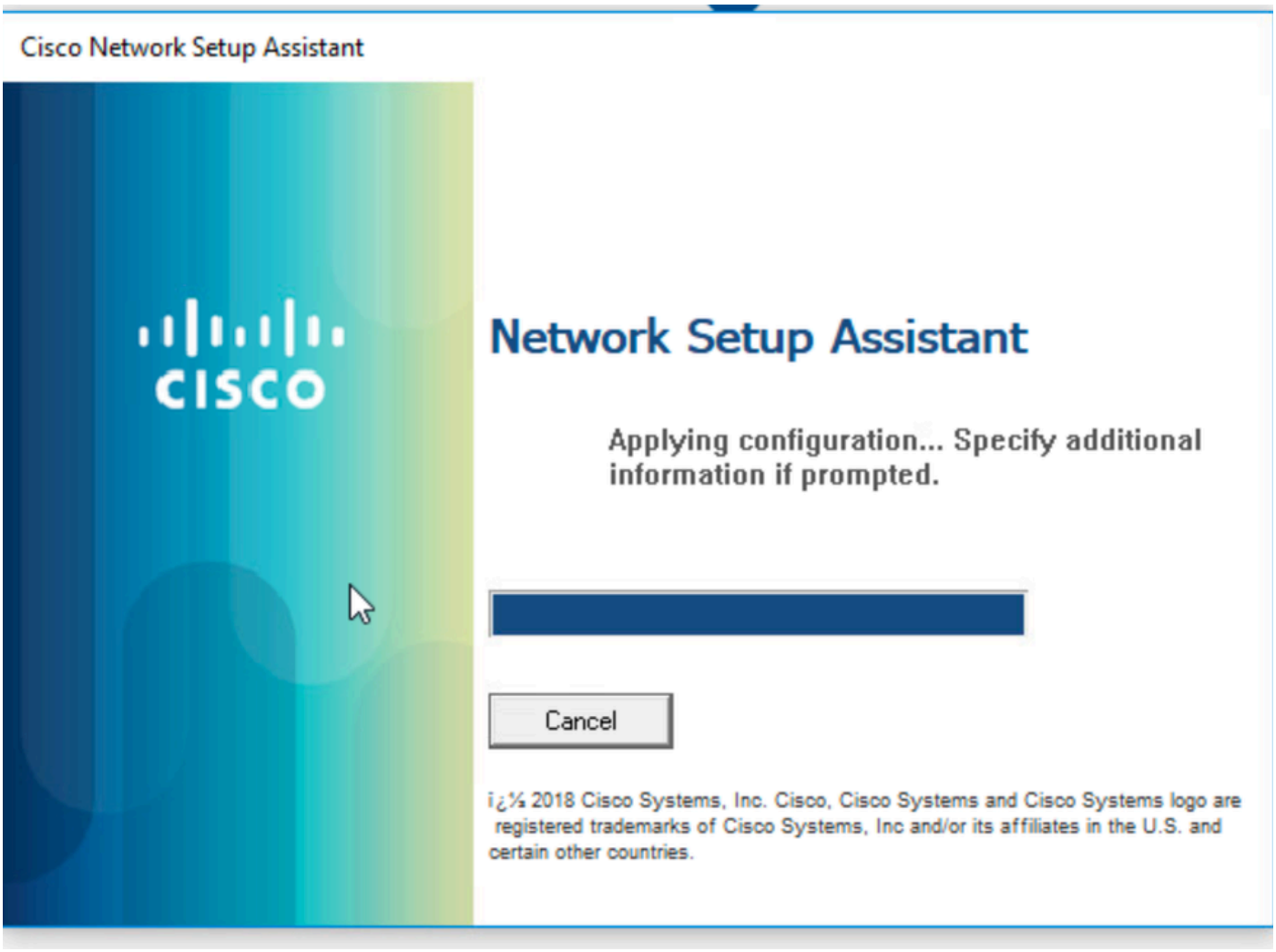


发布消息，如果配置文件配置为执行EAP-TLS身份验证，则用户将被请求下载Network Assistant工具以下载终端配置文件和EAP TLS证书以进行身份验证



以管理员权限运行Network Assistant应用程序，然后点击start（开始）按钮以启动自行激活流程：


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.



用户已使用个人设备成功登录网络以访问资源。

故障排除

要排除BYOD问题，请在ISE上启用此调试

要设置为调试级别的属性：

- client(guest.log)
- client-webapp(guest.log)
- scep(ise-psc.log)
- ca-service(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)

日志片段

访客日志

这些日志表明用户已成功重定向到该页面并已下载Network Assistant应用程序：

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中找到的映射路径，转发到：pages/byodWelcome.jsp // BYOD欢迎页面
2025-02-24 12:06:09,968信息[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信息[https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.Step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep， pTranSteps:[id:d2513b7b-7249-4bc3-a423-0e7d9a0b250]
2025-02-24 12:06:09,968信息[https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.Step.Step执行器 — :000000000000000B30D59CC5::test:- getNextFlowStep，stepTran:d2513b7b-72 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::: — 在操作转发中找到的映射路径，转发到：pages/byodRegistration.jsp
2025-02-24 12:06:14,643信息[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信息[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信息[https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.Step.Step执行器 — :000000000000000B30D59CC5::test:- getNextFlowStep，stepTran:f203b8757-9e a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647信息[https-jsse-nio-10.127.196.172-8443-exec-2][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::: — 在操作转发中找到的映射路径，转发到：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::: — 会话=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::- 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 //网络协助应用程序已发送到终端

Ise-Psc日志

当应用下载到终端时，应用会启动SCEP流从ISE获取客户端证书。

2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore包含4个证书：
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 -:::: — 选择加密证书
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 选择具有keyEncipherment keyUsage的证书
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 找到1个证书和keyEncipherment keyUsage
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]，用于消息加密
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 选择验证者证书
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 选择具有数字签名密钥的证书用法
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 找到1个使用digitalSignature keyUsage的证书
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]用于消息验证
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 选择颁发者证书
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 选择具有基本限制的证书
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::: — 找到3个具有基本限制的证书
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]（对于颁发者）
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- SCEP服务器性能度量：name[live/dead， total

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

终端配置文件下载

完成SCEP过程且终端安装证书后，应用下载终端配置文件以供将来由设备执行的身份验证：

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Referer = Windows //已根据网页检测到Windows设备
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::: — 会话= 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::: — 会话= 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::: — 调配nsp配置文件
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::: — 会话= 000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId =空
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配置文件已下载到终端
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::: — 流向ip:文件类型:NativeSPProfile文件名：Cisco-ISE-NSP.xml //The Network Assistant应用
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已设置为测试
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::: — 重定向类型是：SUCCESS_PAGE，重定向URL为：对于mac:

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。