在Catalyst 9800 WLC和ISE上配置终端安全评估

目录

简介

本文档介绍如何通过图形用户界面(GUI)在Catalyst 9800 WLC和ISE上配置终端安全评估WLAN。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC常规配置
- ISE策略和配置文件配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- 身份服务引擎(ISE)v3.2
- 笔记本电脑Windows 10企业版

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。

背景信息

无线LAN控制器RADIUS NAC和CoA功能流

1.客户端使用dot1x身份验证进行身份验证。

2. RADIUS Access Accept传输端口80的重定向URL和包括允许IP地址和端口或隔离VLAN的预身份验证ACL。

3.客户端被重定向到access accept中提供的URL，并进入新状态，直到完成状态验证。处于此状态的客户端与ISE服务器通信，并根据ISE NAC服务器上配置的策略验证自身。

4.客户端上的NAC代理启动状态验证（流向端口80的流量）：代理将HTTP发现请求发送到端口80，控制器会重定向到访问接受中提供的URL。ISE知道客户端尝试访问并直接响应客户端。这样，客户端即可了解ISE服务器IP，从现在起，客户端将直接与ISE服务器进行通信。

5. WLC允许此流量，因为ACL配置为允许此流量。如果发生VLAN覆盖，流量会桥接以便到达ISE服务器。

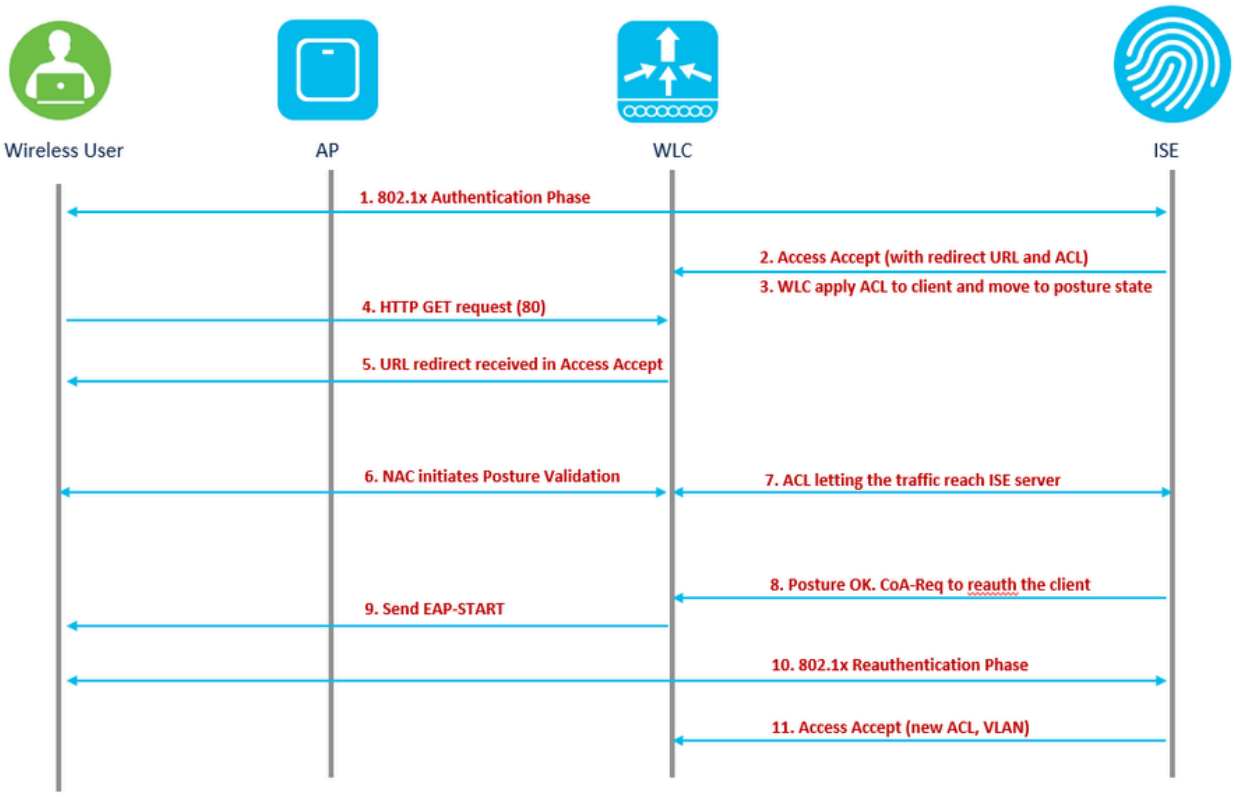
6.当ISE客户端完成评估后，RADIUS CoA-Req with reauth service将发送到WLC。这将启动客户端的重新身份验证（通过发送EAP-START）。 重新身份验证成功后，ISE会发送包含新ACL（如果有）和无URL重定向或访问VLAN的访问接受。

7.根据RFC 3576,WLC支持CoA-Req和Disconnect-Req。根据RFC 5176,WLC需要支持重新身份验证服务的CoA-Req。

8.在WLC上使用预配置的ACL，而不是可下载的ACL。ISE服务器仅发送ACL名称，该名称已在控制器中配置。

9.此设计适用于VLAN和ACL两种情况。如果发生VLAN覆盖，我们只需重定向端口80，并允许（桥接）隔离VLAN上的其余流量。对于ACL，应用访问接受中收到的预身份验证ACL。

此图直观地显示了此功能流：



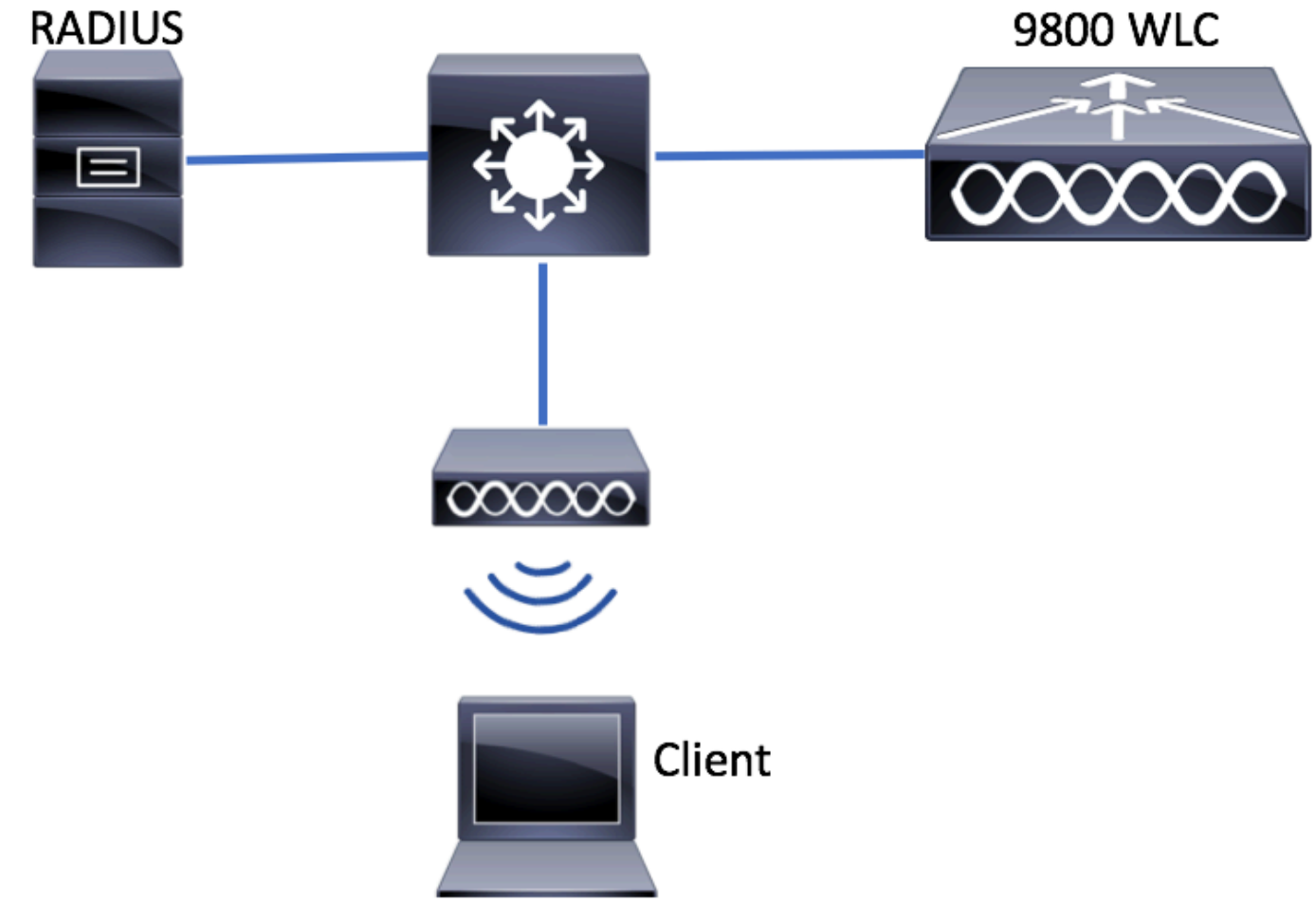
功能工作流程

对于此使用案例，仅用于企业用户的SSID将启用安全评估。此SSID上不存在其他使用案例，例如BYOD、访客或任何其他使用案例。

当无线客户端首次连接到终端安全评估SSID时，它必须下载终端安全评估模块并将其安装在ISE的重定向门户上，最后根据终端安全评估检查结果（兼容/不兼容）应用相关ACL。

配置

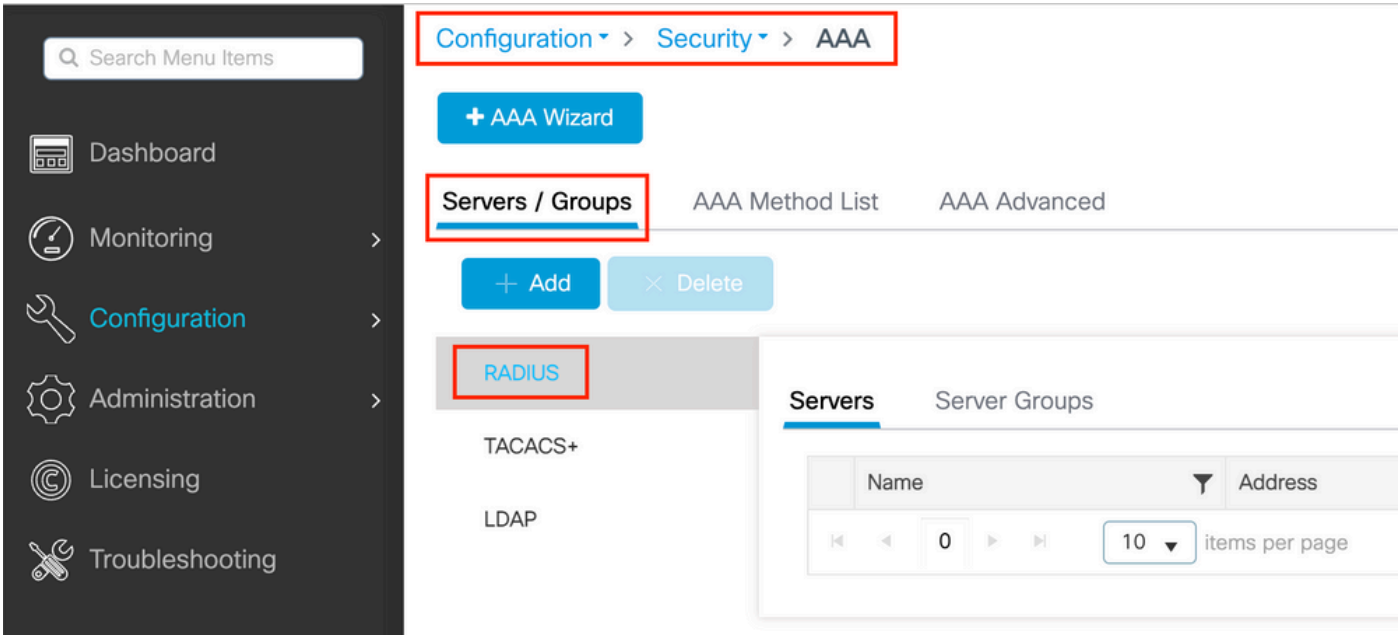
网络图



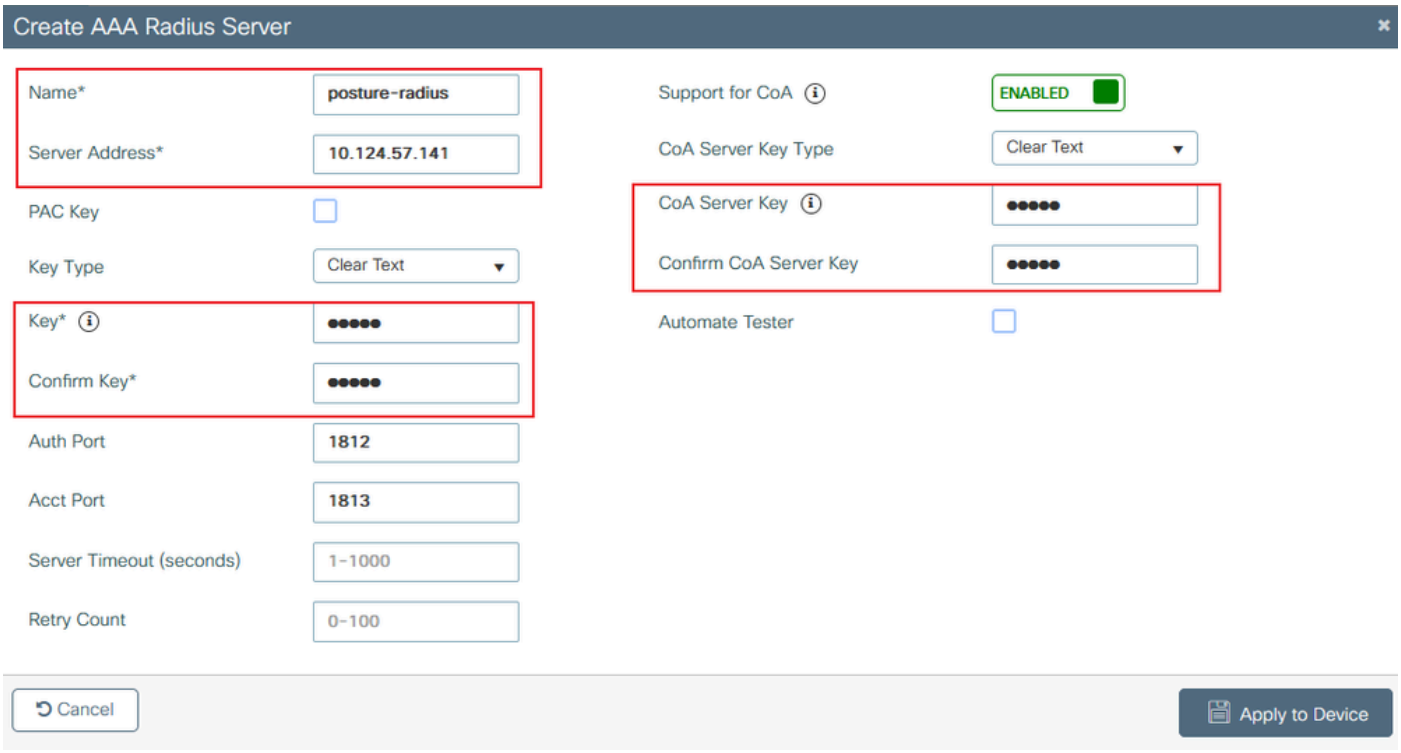
网络图

9800 WLC 上的 AAA 配置

步骤1.将ISE服务器添加到9800 WLC配置。导航到Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add并输入RADIUS服务器信息，如图所示。确保为状态NAC启用对CoA的支持。

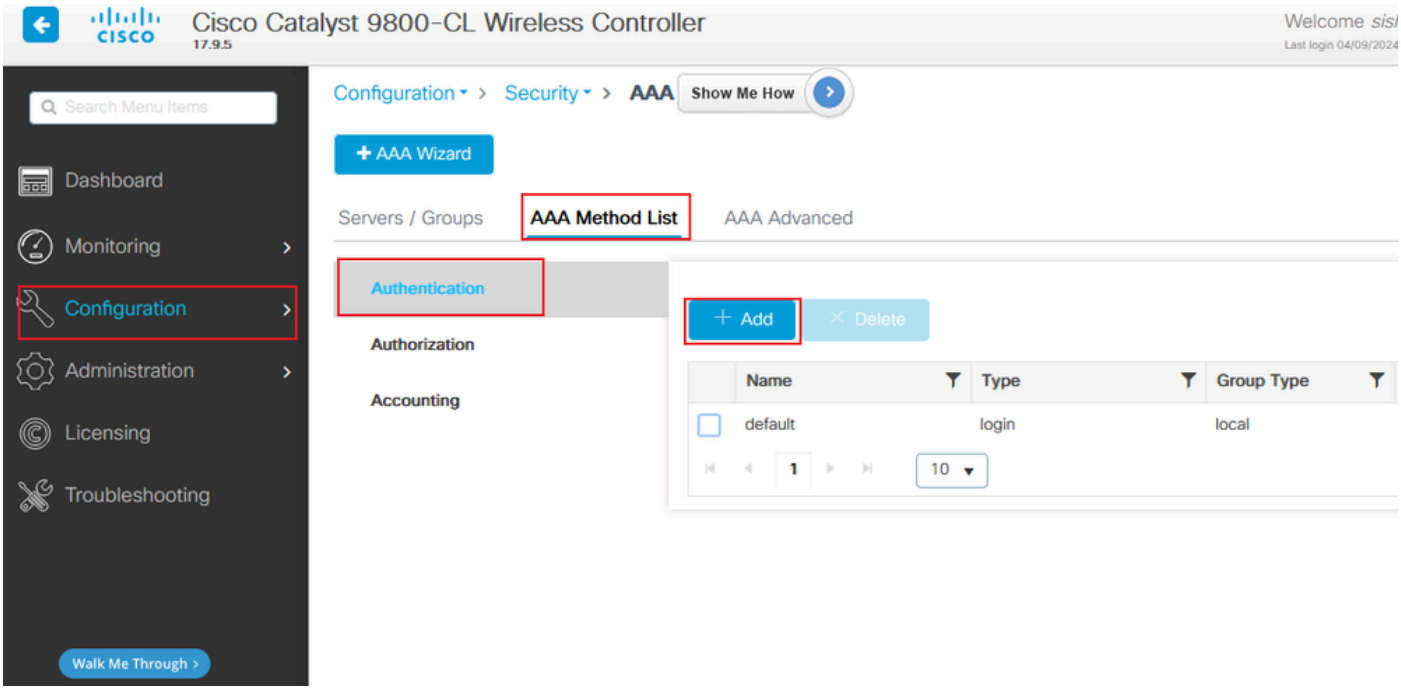


9800创建radius服务器

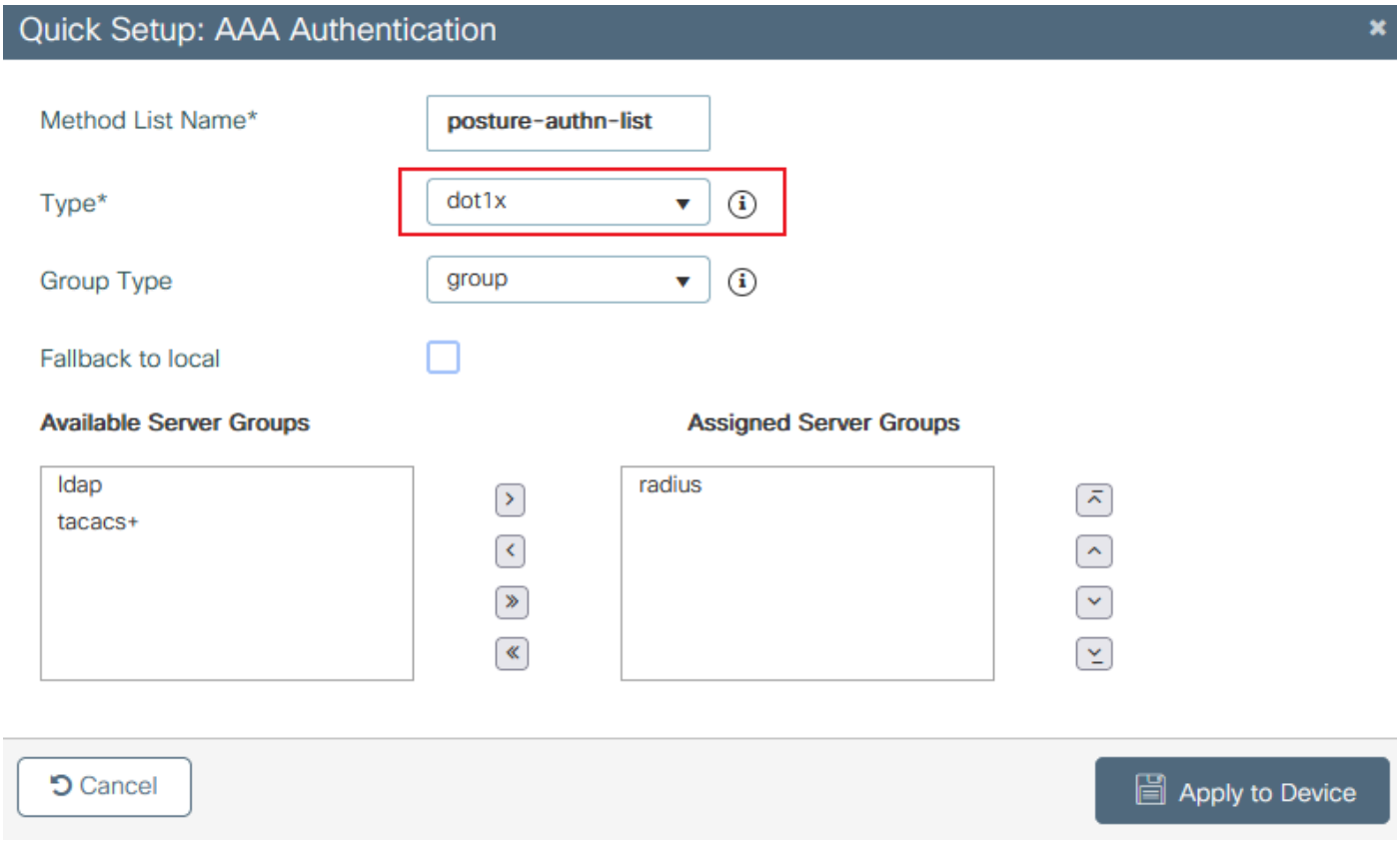


9800创建radius详细信息

步骤2.创建身份验证方法列表。导航到Configuration > Security > AAA > AAA Method List > Authentication > + Add，如图所示：

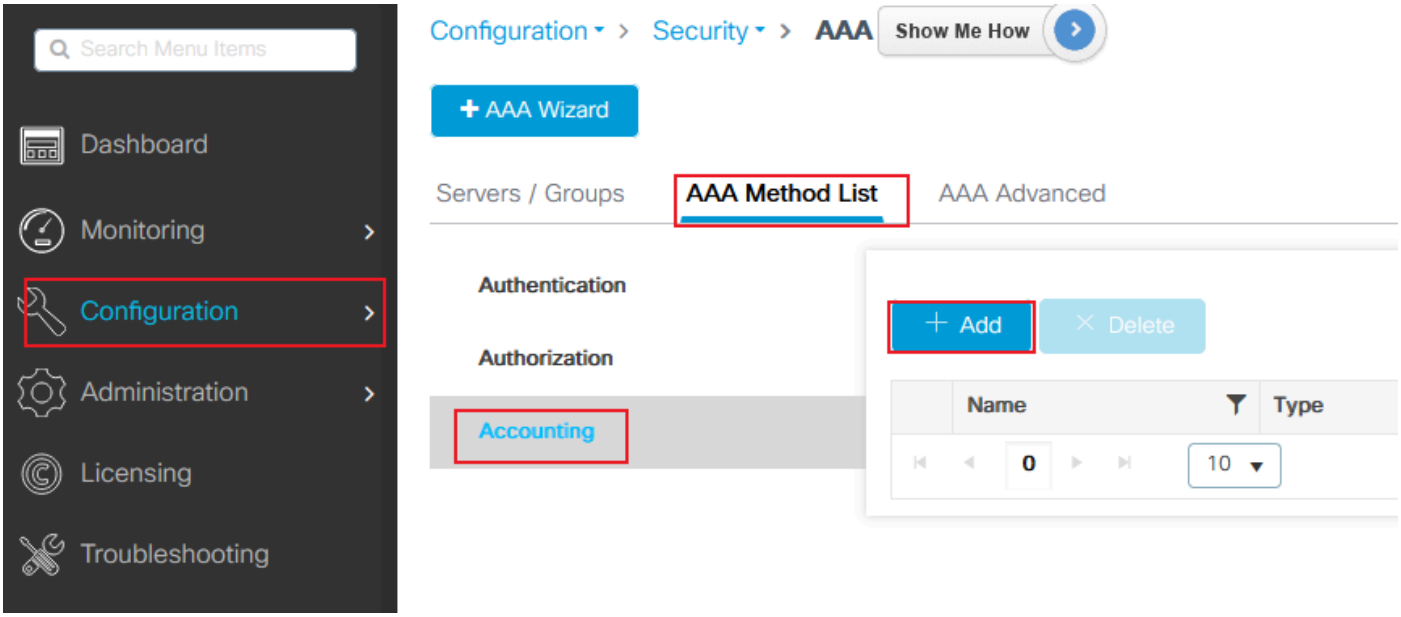


9800添加身份验证列表

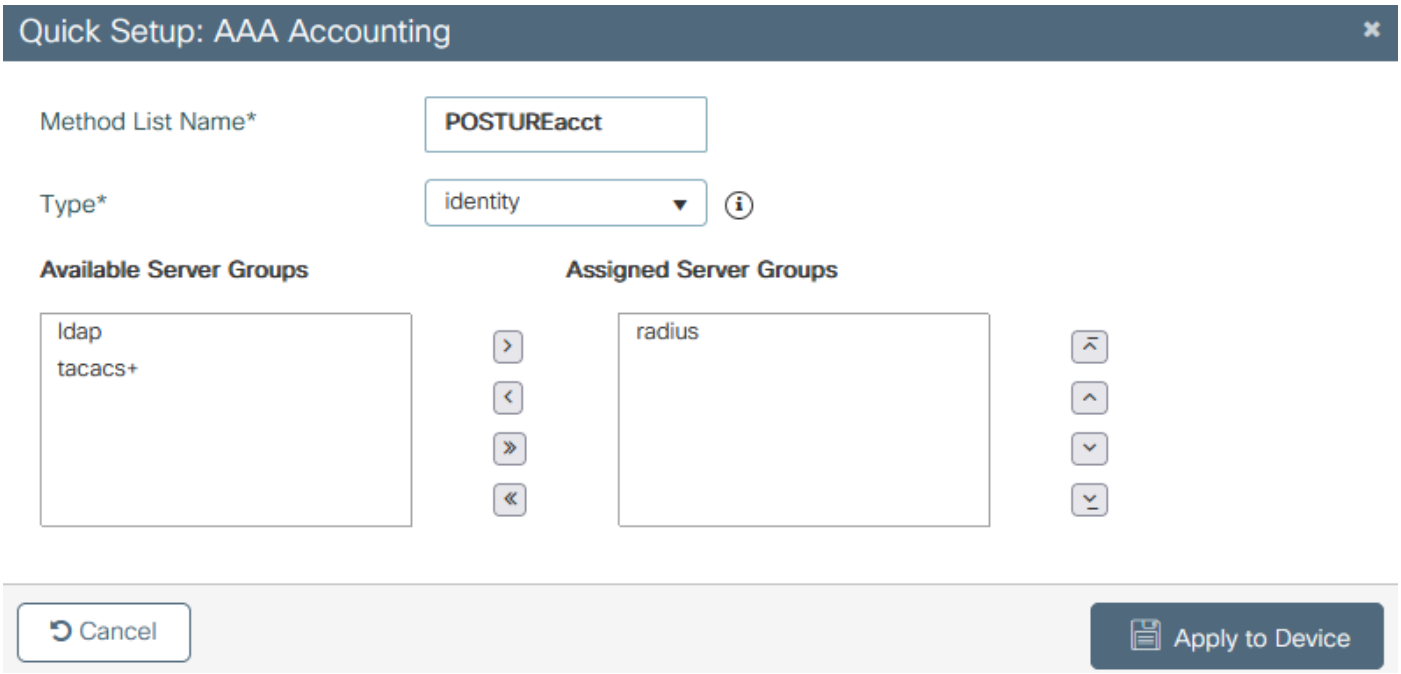


9800创建身份验证列表详细信息

步骤3.（可选）创建记账方法列表，如图所示：



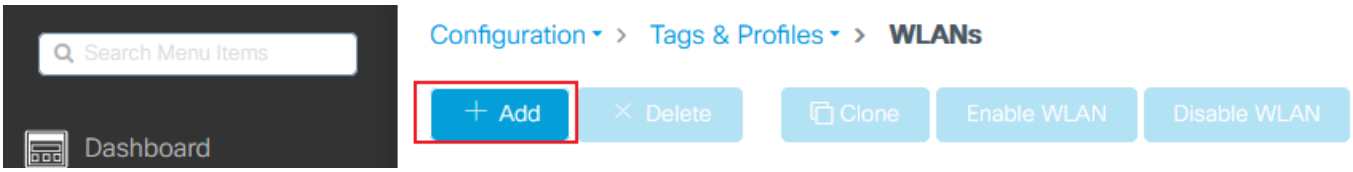
9800添加帐户列表



9800创建客户列表详细信息

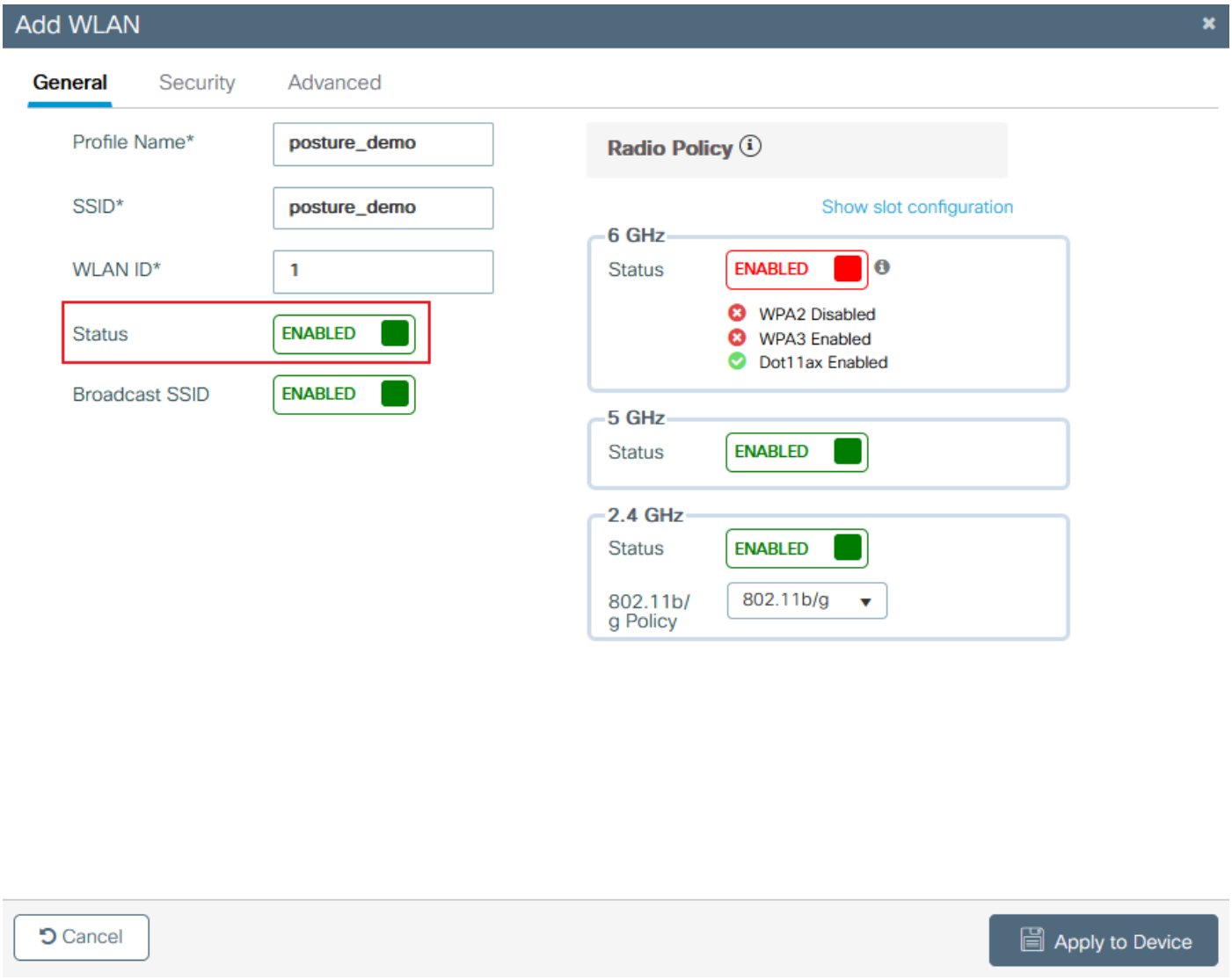
WLAN 配置

第 1 步： 创建 WLAN.导航到Configuration > Tags & Profiles > WLANs > + Add并根据需要配置网络：



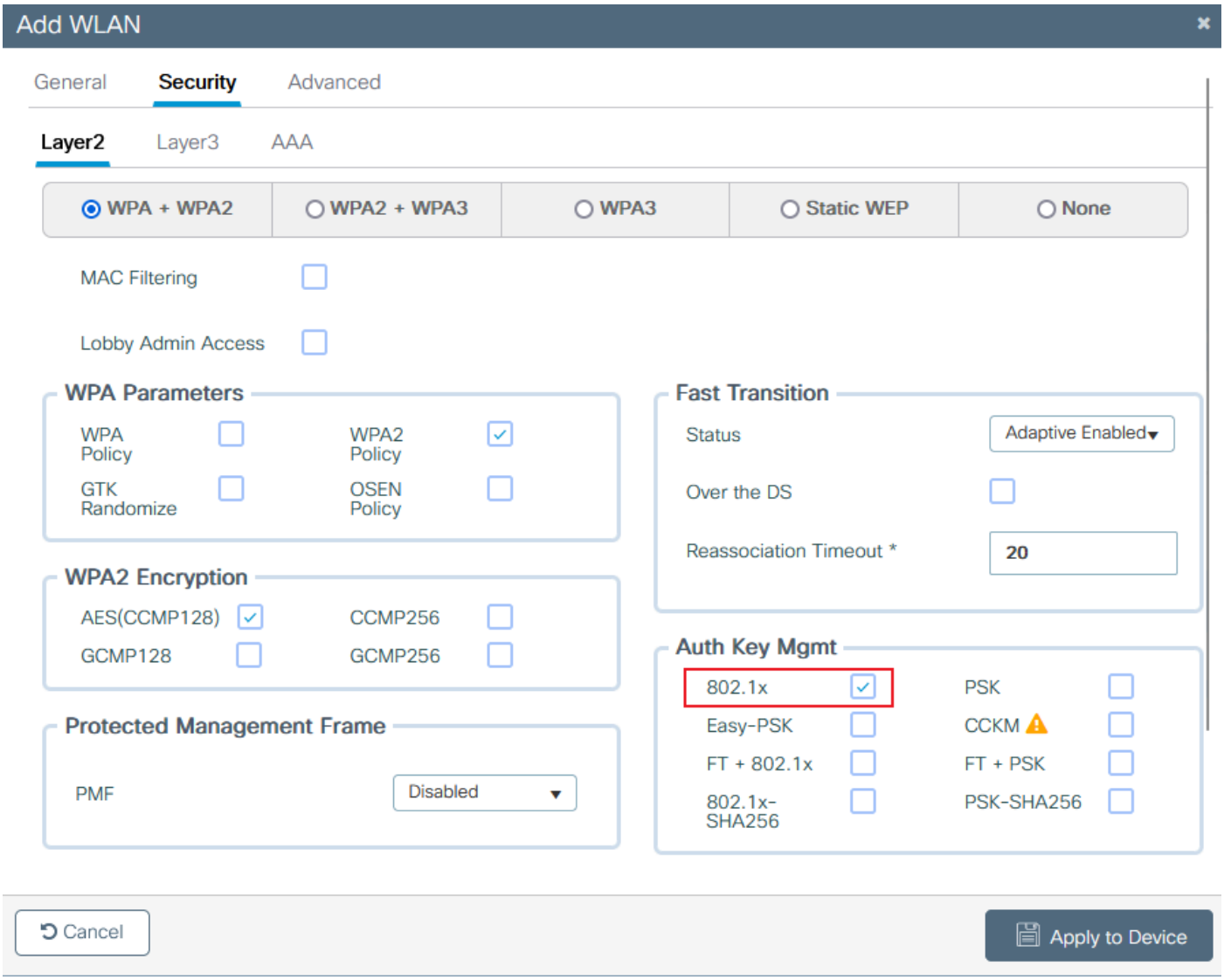
9800 WLAN添加

步骤2.输入WLAN一般信息。

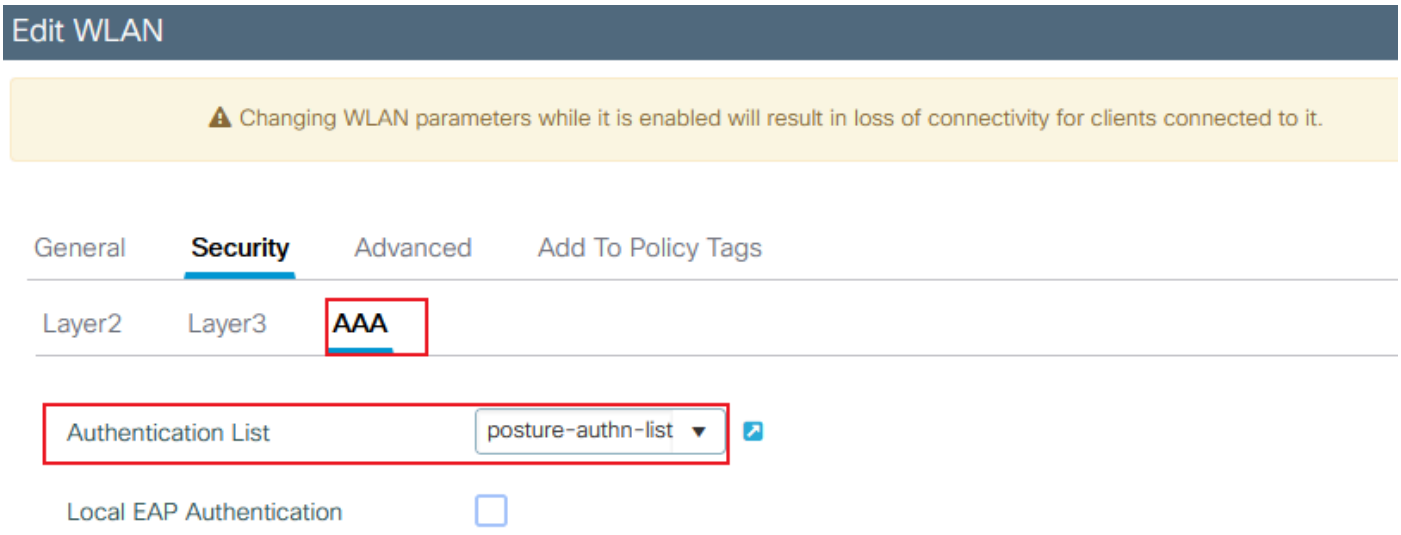


9800创建WLAN常规

步骤3.导航到安全选项卡并选择所需的安全方法。在这种情况下，请选择“802.1x”，并且需要AAA身份验证列表(在AAA配置部分中的步骤2中创建):



9800创建WLAN安全L2

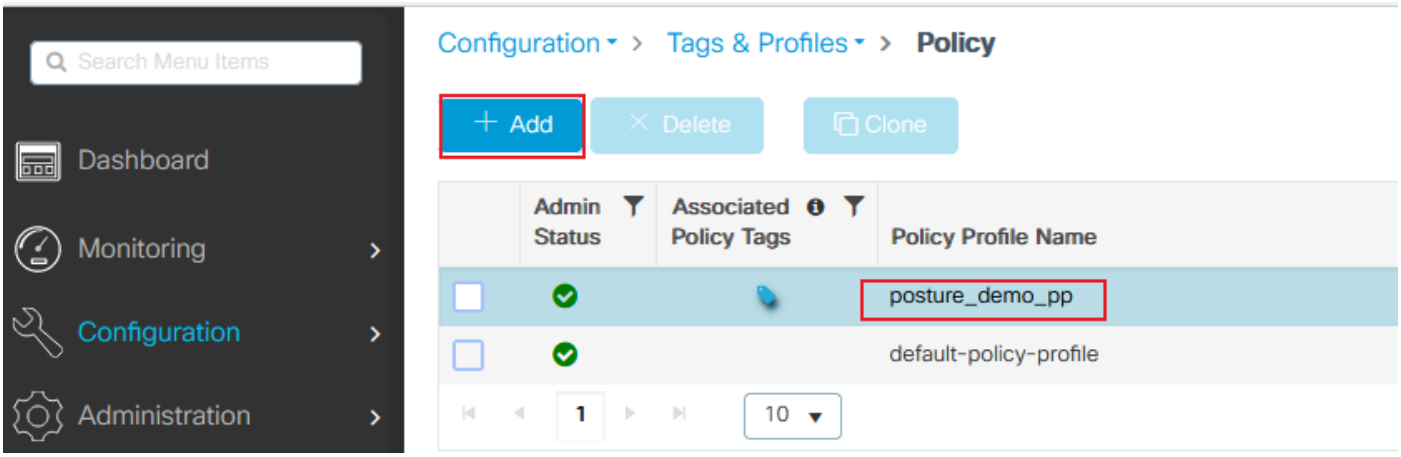


9800创建WLAN安全AAA

策略配置文件配置

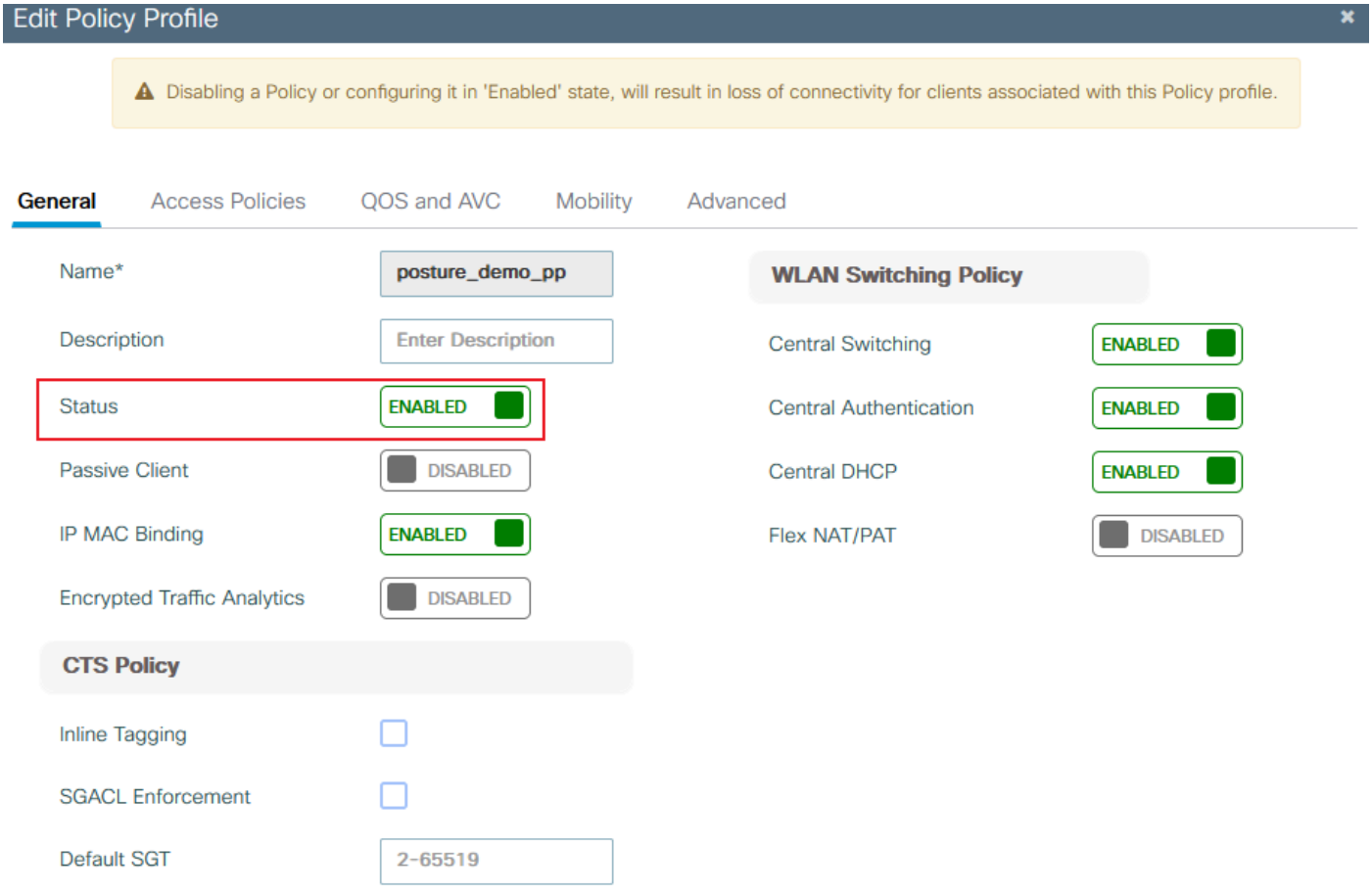
在策略配置文件中，您可以决定分配客户端到哪个VLAN，以及其他设置(如访问控制列表(ACL)、服务质量(QoS)、移动锚点、计时器等)。 您可以使用默认策略配置文件，也可以新建策略配置文件。

第 1 步： 新建策略配置文件。导航到Configuration > Tags & Profiles > Policy并创建一个新的：



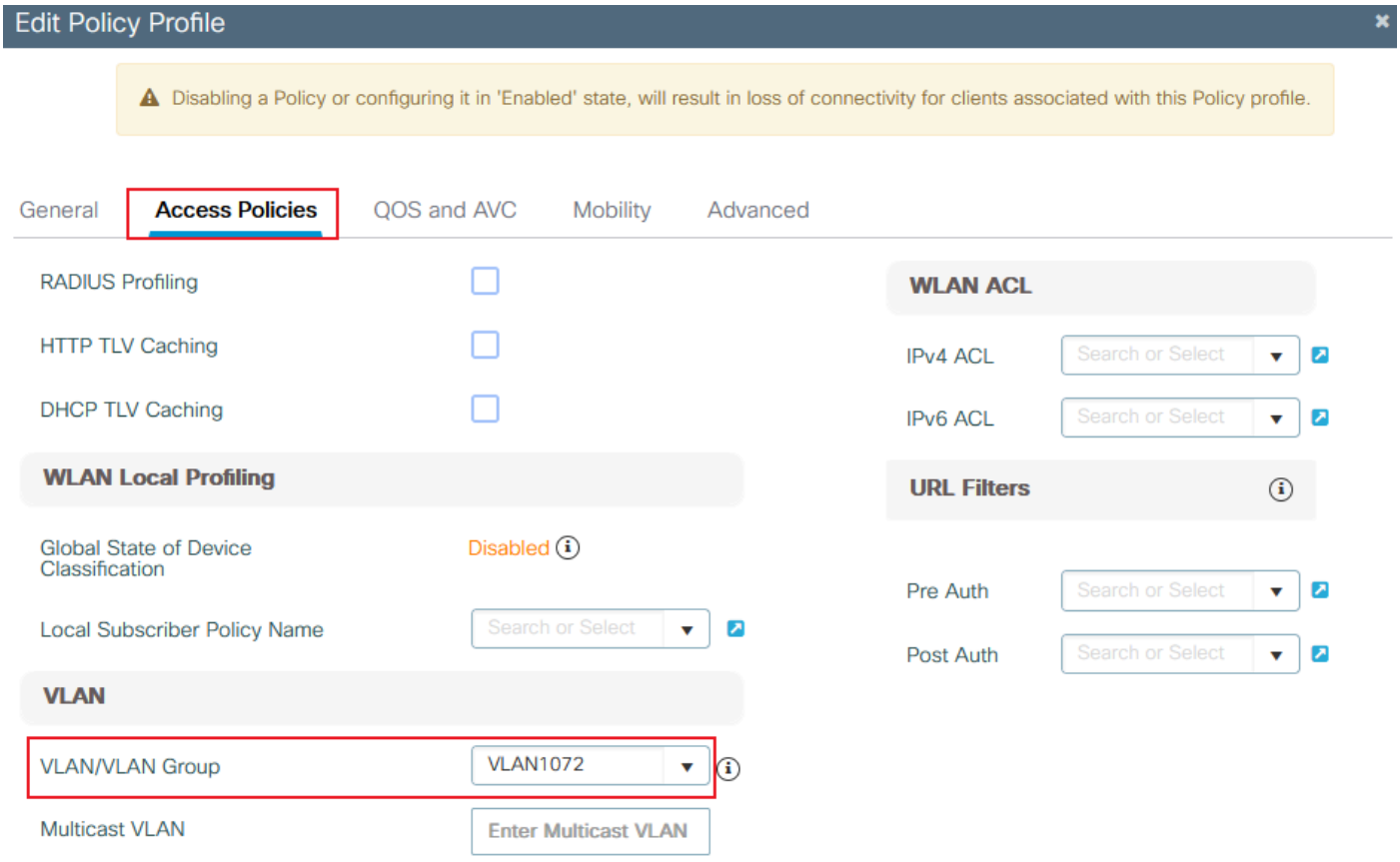
9800添加策略配置文件

确保已启用配置文件。



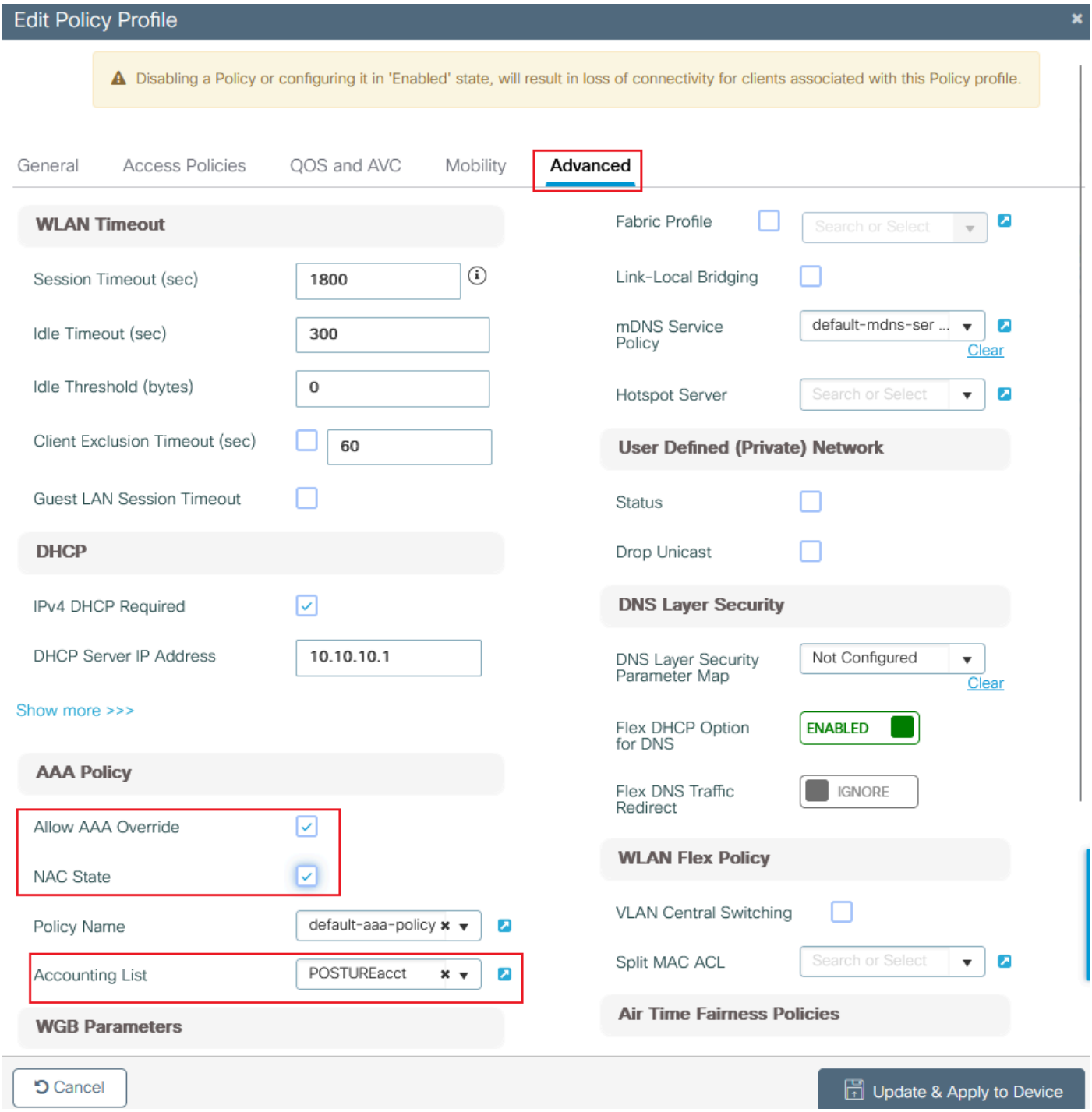
9800 create policy profile general

步骤2.选择VLAN。导航到访问策略选项卡，然后从下拉列表中选择VLAN名称或手动键入VLAN-ID。请勿在策略配置文件中配置ACL:



9800创建策略配置文件VLAN

第 3 步：配置策略配置文件，接受 ISE 覆盖（“允许 AAA 覆盖”）和授权更改 (CoA)（“NAC 状态”）。 您也可以选择指定会计方法：

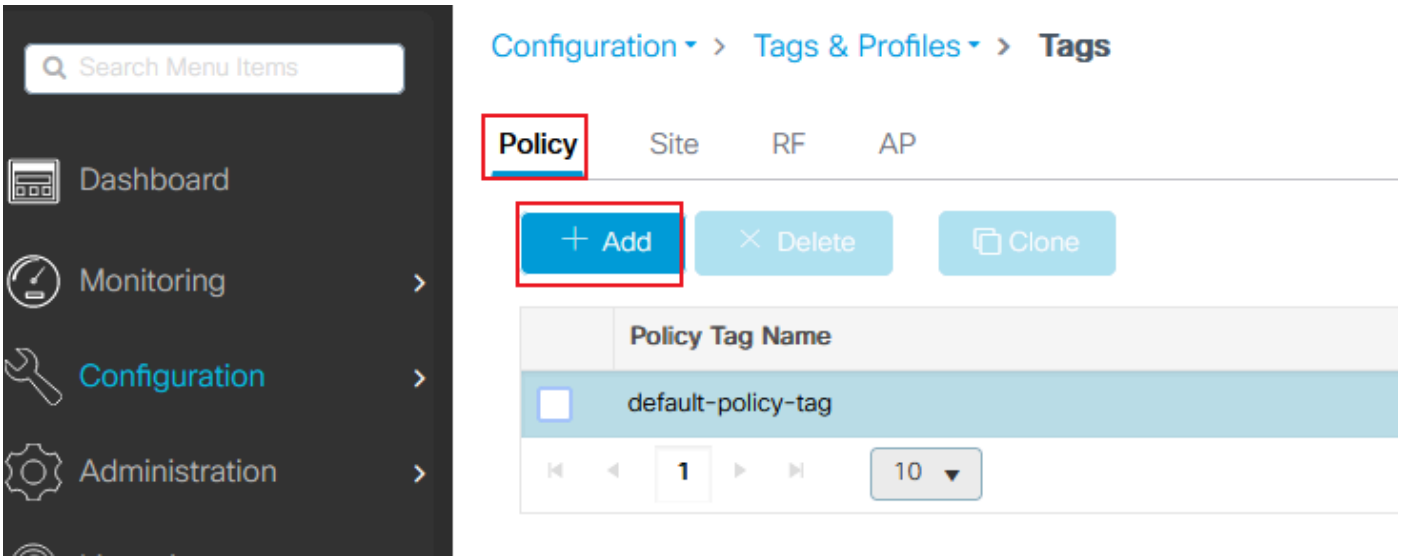


9800创建策略配置文件高级

策略标签配置

在策略标签中，您可以将 SSID 与策略配置文件相关联。您可以新建策略标签，也可以使用 default-policy 标签。

导航到Configuration > Tags & Profiles > Tags > Policy，并根据需要添加新标签，如图所示：



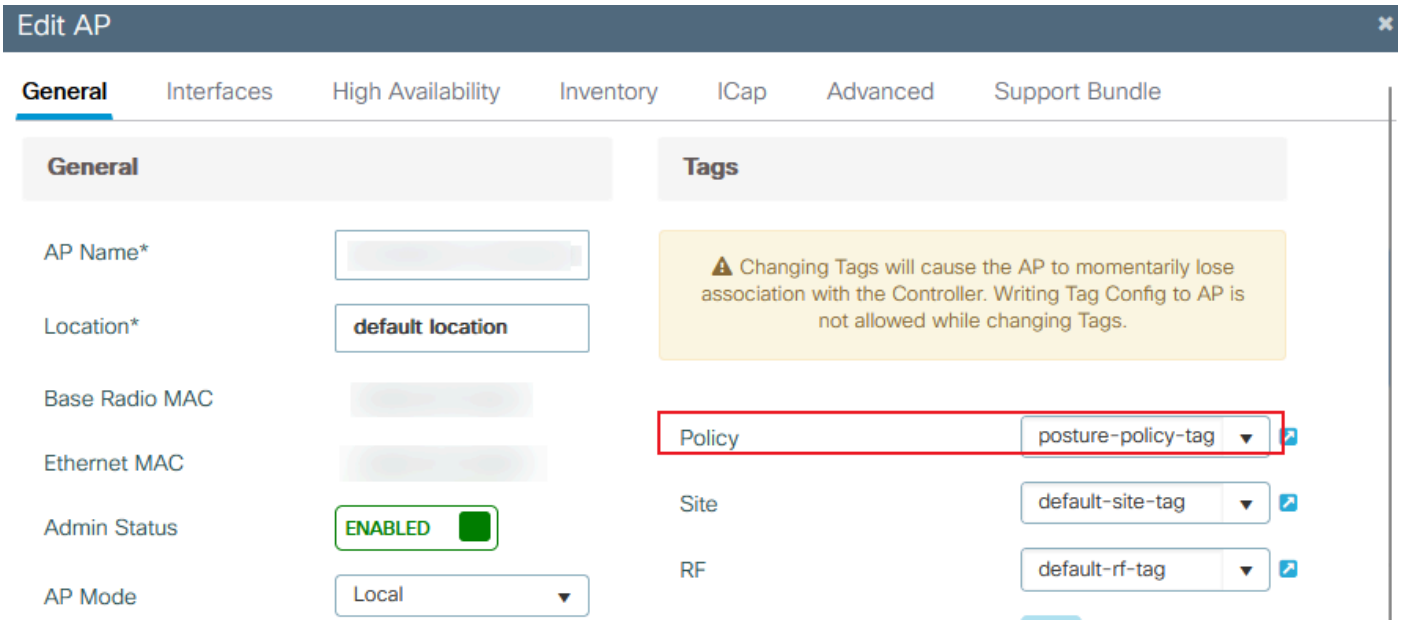
9800策略标记添加

将您的WLAN配置文件链接到所需的策略配置文件：

9800策略标记详细信息

策略标签分配

将策略标签分配给所需的 AP。导航到Configuration > Wireless > Access Points > AP Name > General Tags，进行所需的分配，然后点击Update & Apply to Device。



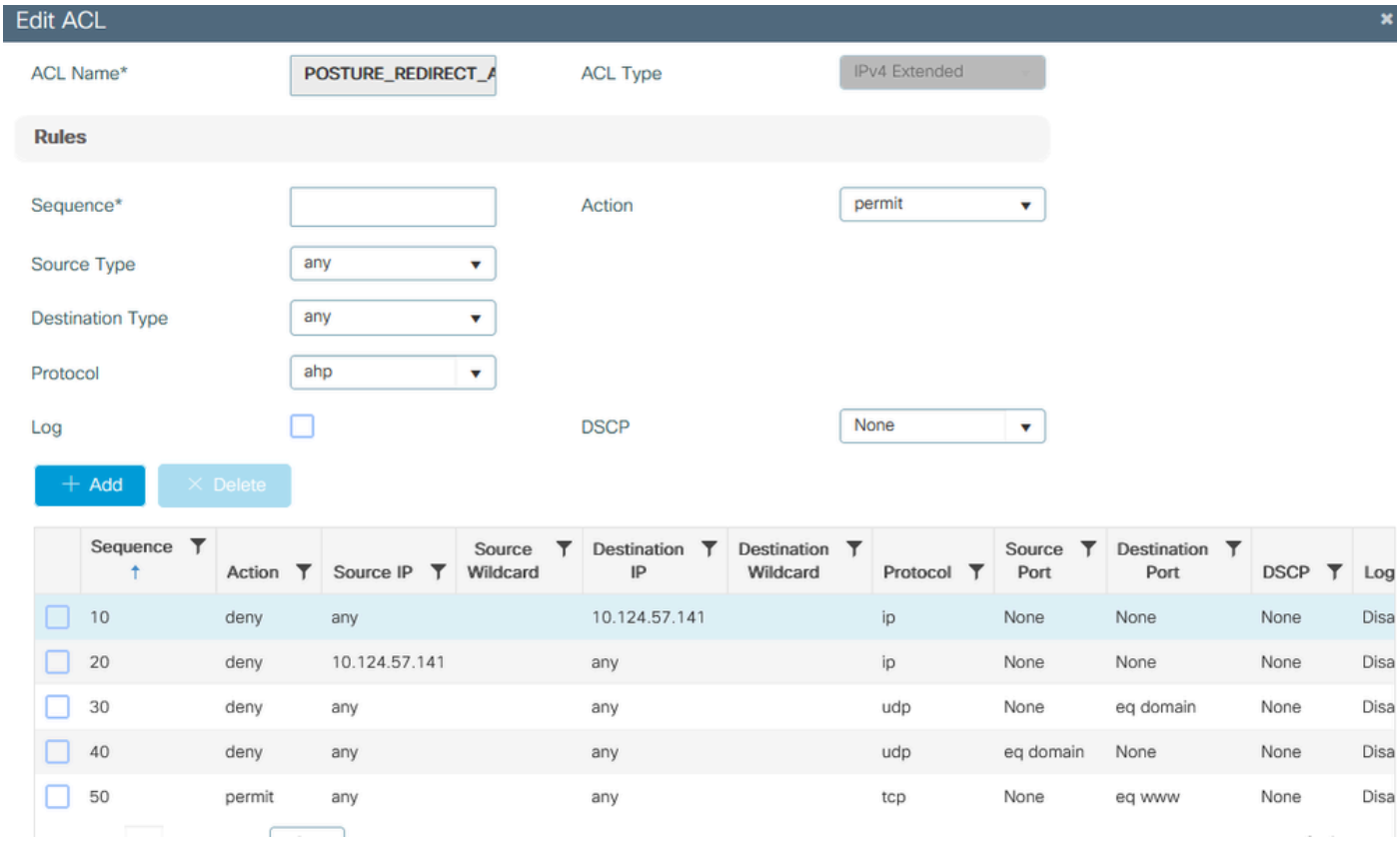
9800策略标记分配

重定向 ACL 配置

导航到Configuration > Security > ACL > + Add以创建新的ACL。

用于安全评估门户重定向的ACL与CWA（集中式Web身份验证）的要求相同。

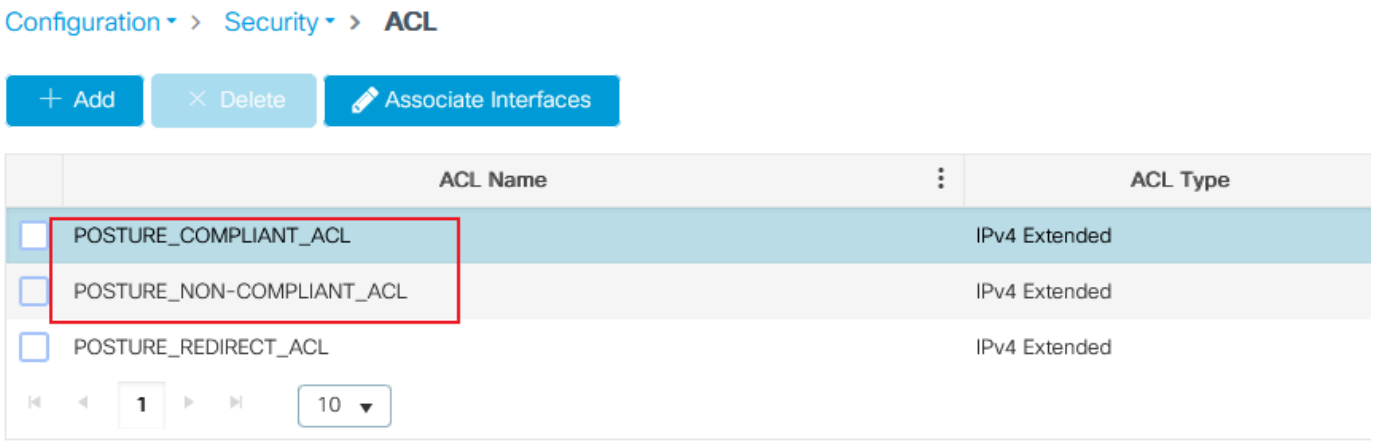
您需要拒绝流向 ISE PSN 节点的流量以及 DNS，同时允许所有其余流量。此重定向ACL不是安全ACL，而是弃用ACL，它定义哪些流量进入CPU（在允许的情况下）进行进一步处理（如重定向）以及哪些流量停留在数据平面上（在拒绝时）并避免重定向。ACL必须如下所示（在本例中用您的ISE IP地址替换10.124.57.141）：



9800重定向ACL详细信息

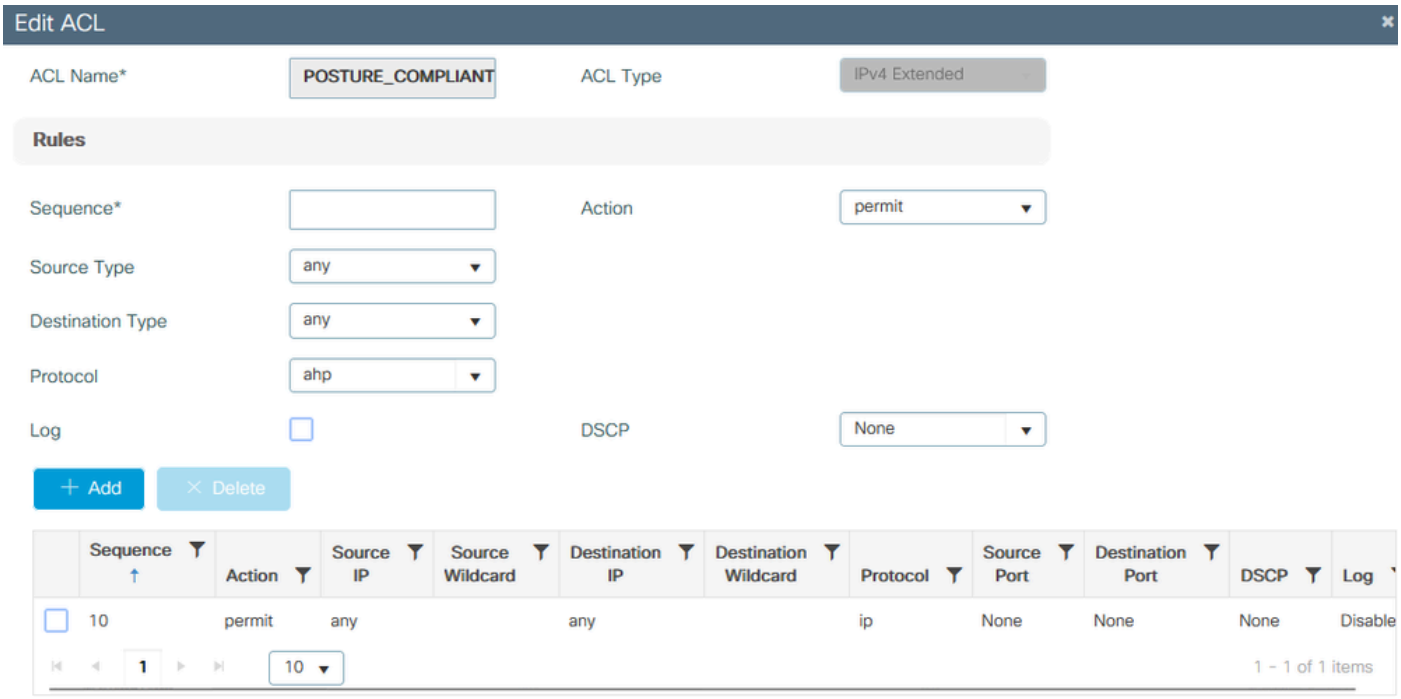
策略ACL配置

在这种情况下，您需要在9800 WLC上为ISE定义单独的ACL，以根据状态检查结果授权合规和不合规方案。



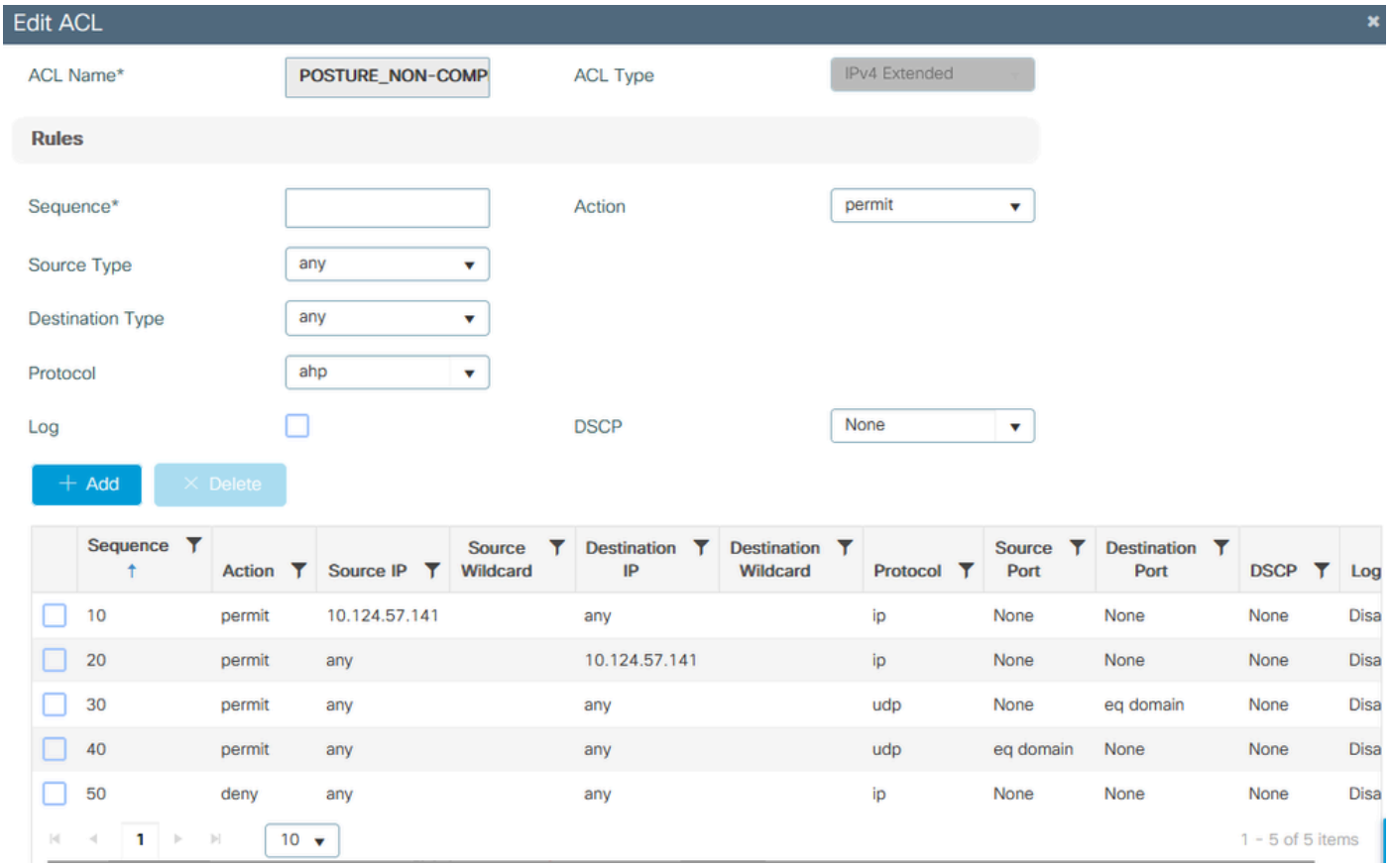
9800 ACL一般信息

对于兼容方案，在本例中只需使用permit all。作为另一种常见配置，您还可以让ISE不授权合规结果中的任何ACL，这相当于permit all在9800端：



9800 ACL — 兼容

对于不合规情况，客户端仅允许访问特定网络，通常访问补救服务器（本例中为ISE自身）：



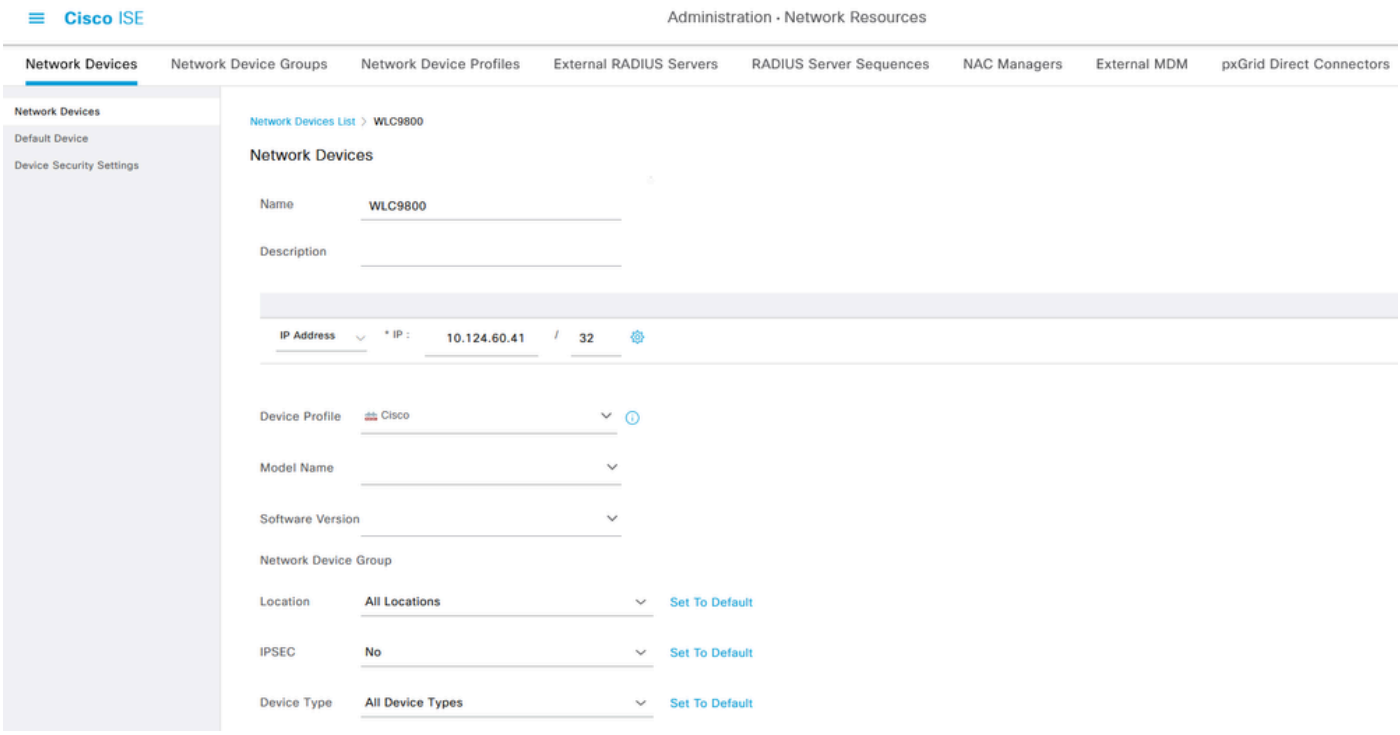
9800 ACL — 不合规

ISE上的AAA配置和状态设置

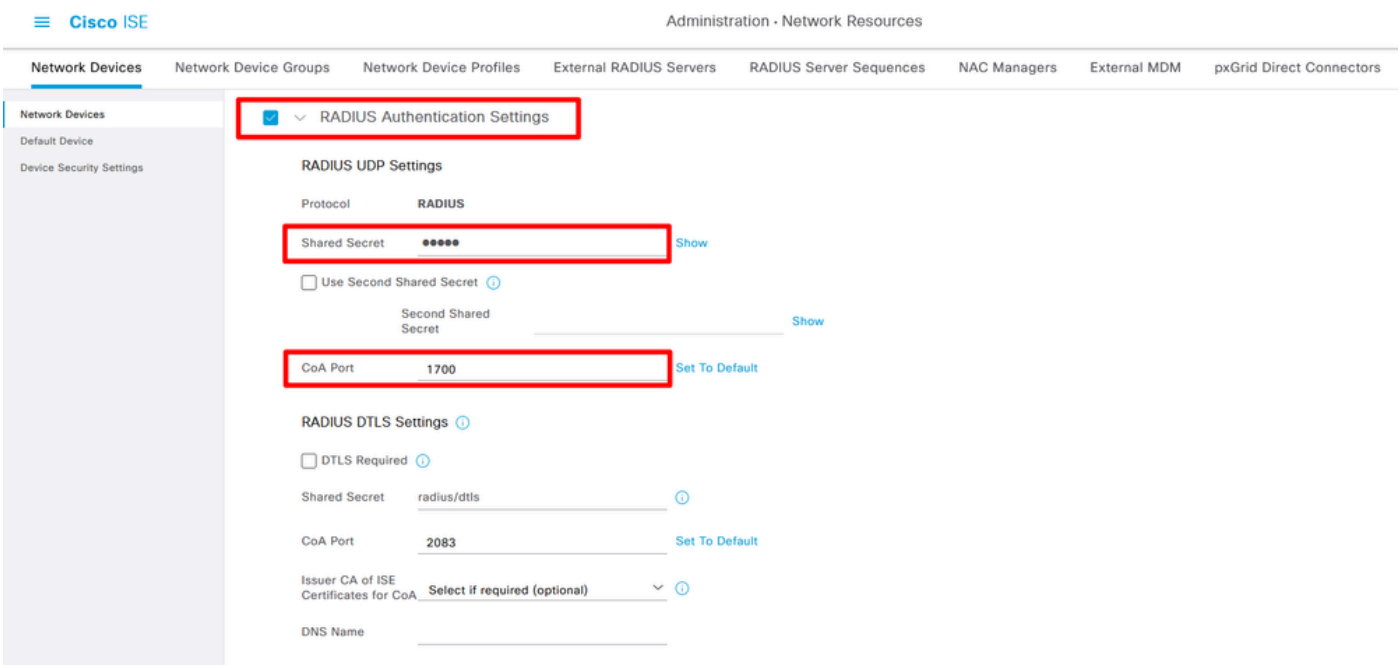
状态要求：在本示例中，确定合规性的要求是检测用于测试Windows PC的桌面上是否存在特定测

试文件。

步骤1.将WLC 9800添加为ISE上的NAD。导航到管理>网络资源>网络设备>添加:



添加网络设备01



添加网络设备02

步骤2.在思科软件CCO网站上下载思科安全客户端前端部署包和合规性模块。

访问和搜索Cisco Secure Client:

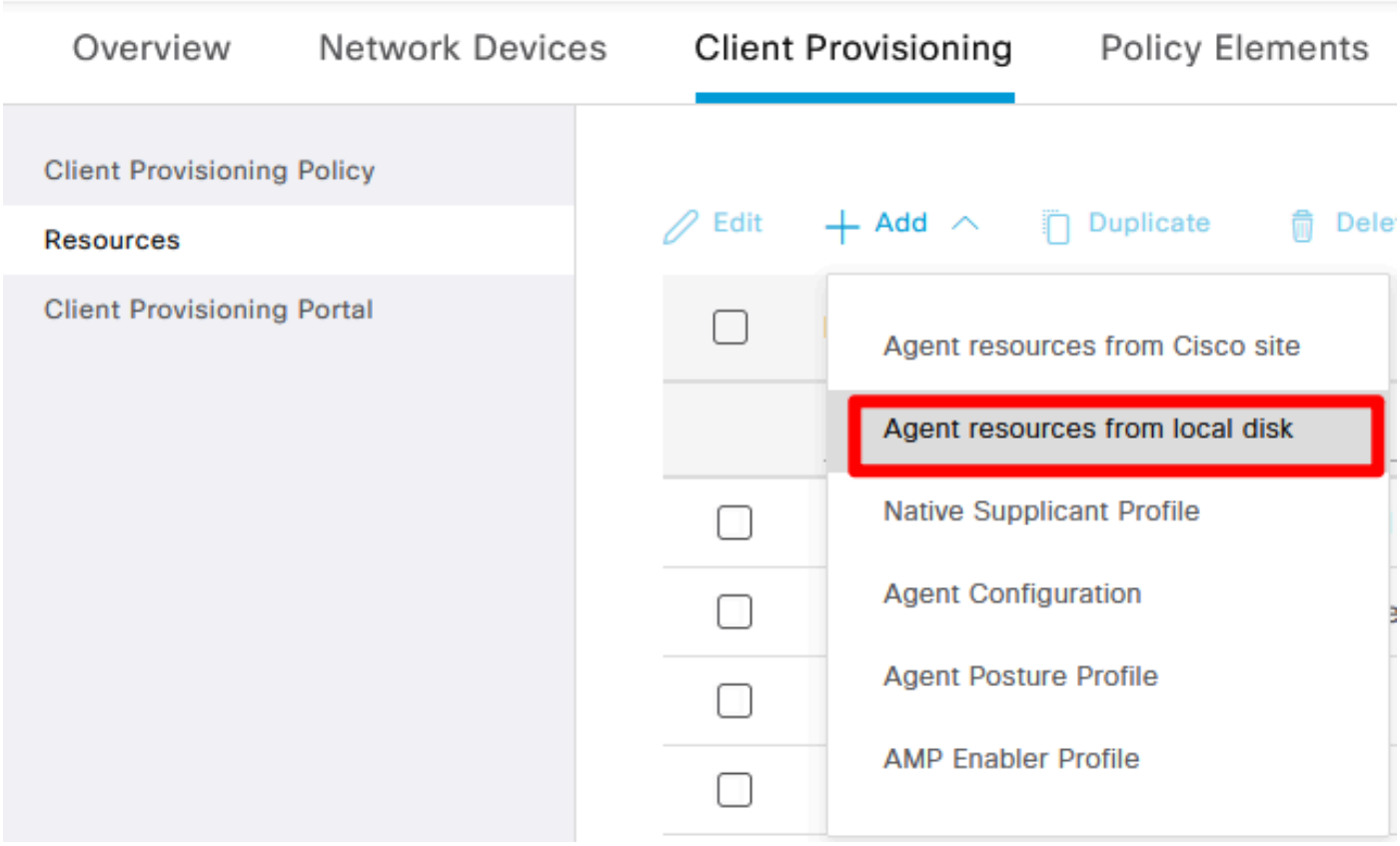
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB

安全客户端5.1.2.42

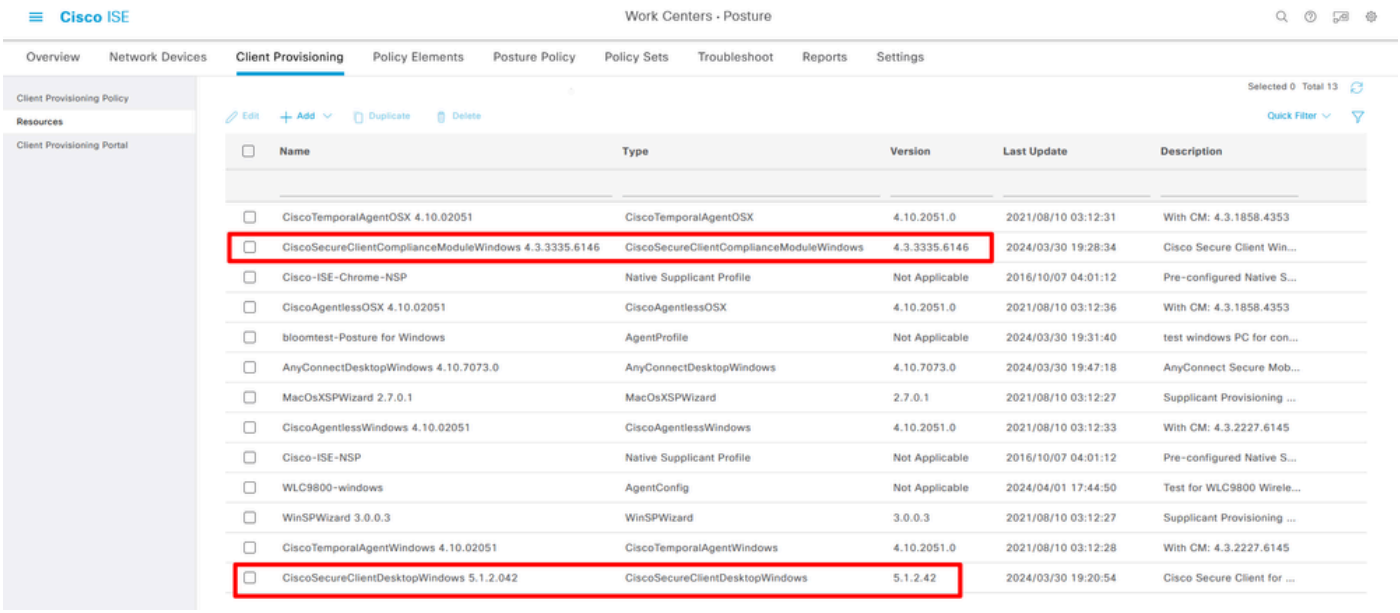
ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later. cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg Advisories	30-Jan-2023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

ISE合规性模块4.3

步骤3.将Cisco安全客户端头端部署包和合规性模块包上传到ISE客户端调配。导航到工作中心>状态>客户端调配>资源。单击添加，从下拉框中选择从本地磁盘选择代理资源:

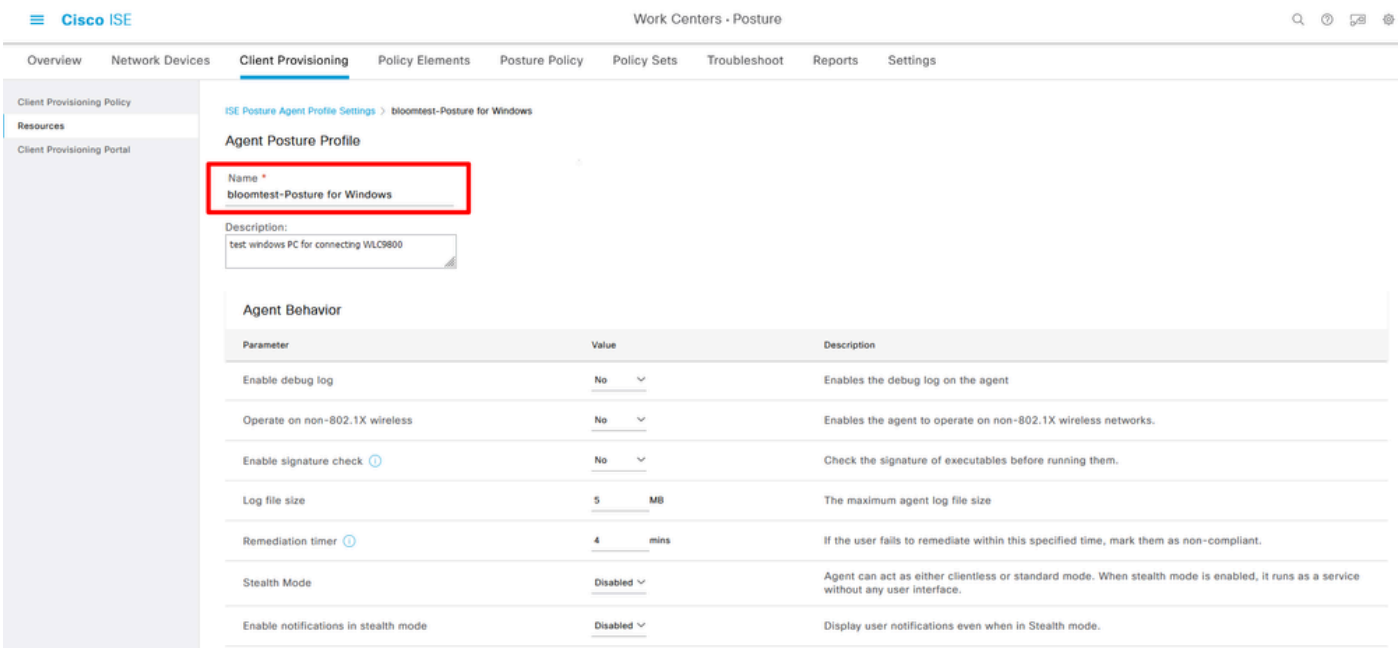


上传安全客户端



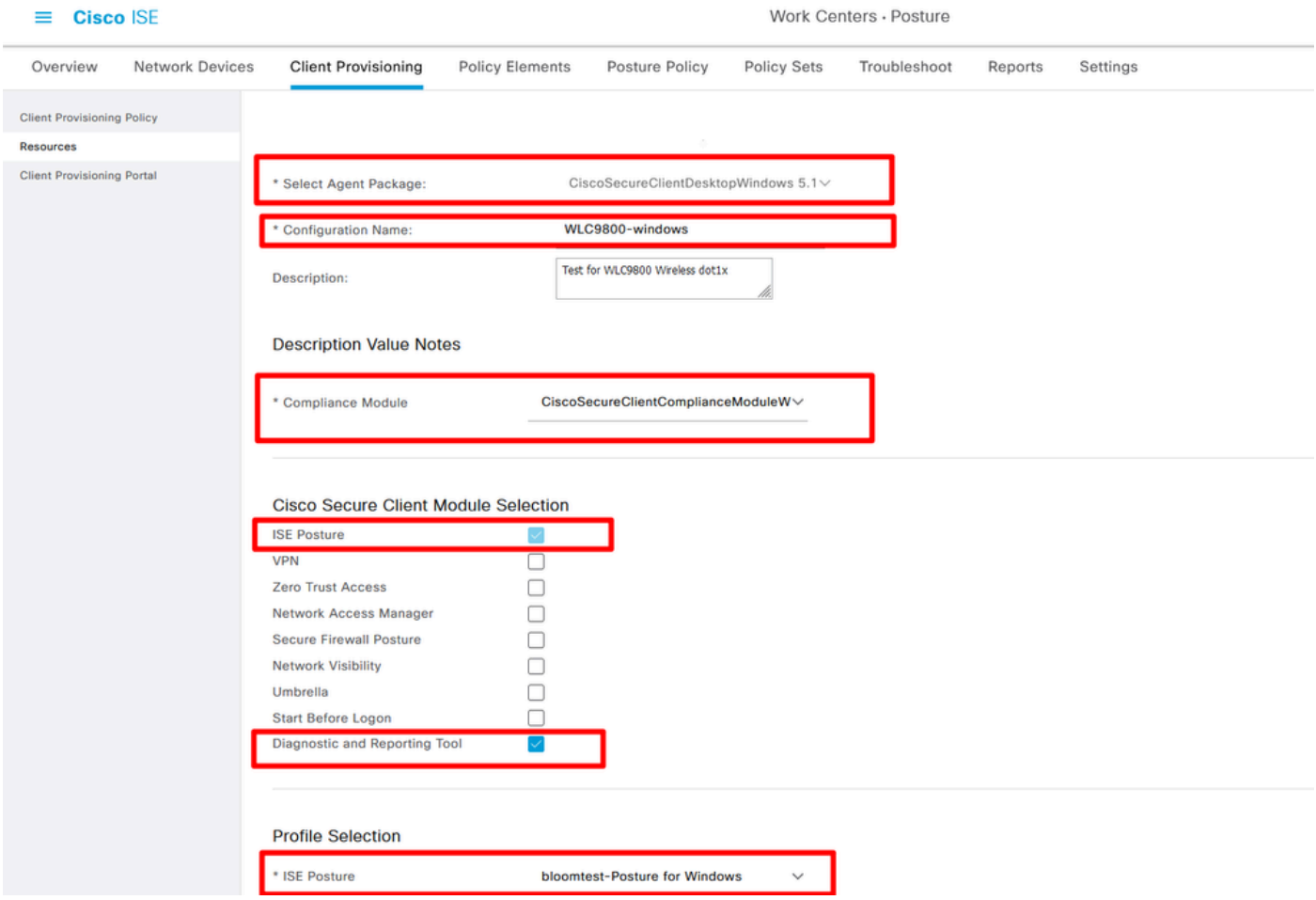
成功上传安全客户端和合规性模块

第4步：创建座席状态配置文件导航到工作中心>状态>客户端调配>资源>添加>座席状态配置文件:



座席状态配置文件

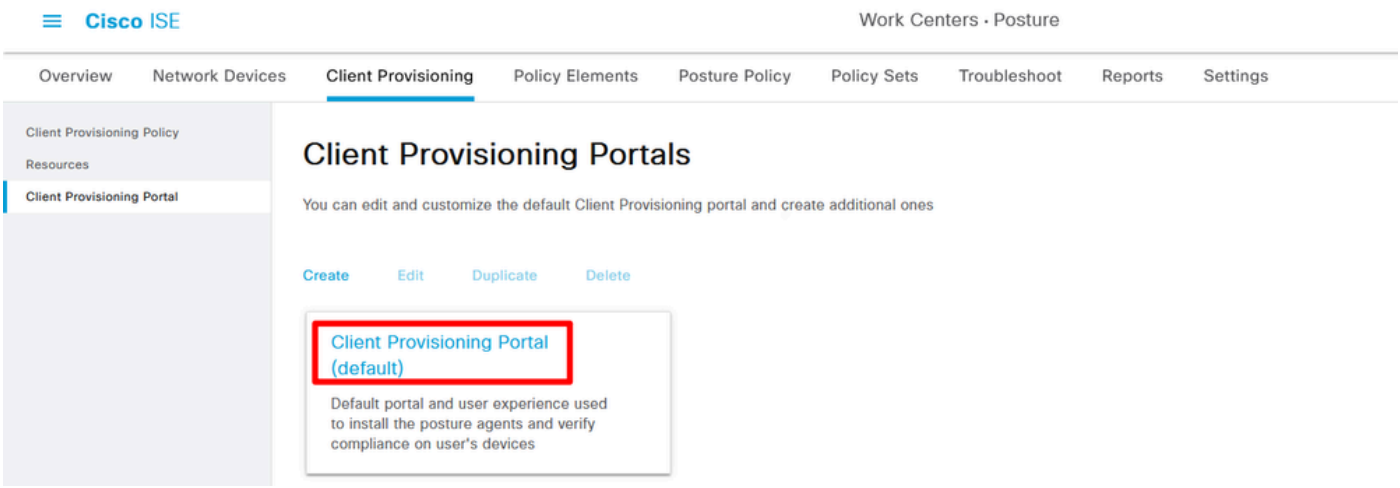
第5步：创建代理配置导航到工作中心>状态>客户端调配>资源>添加>代理配置:



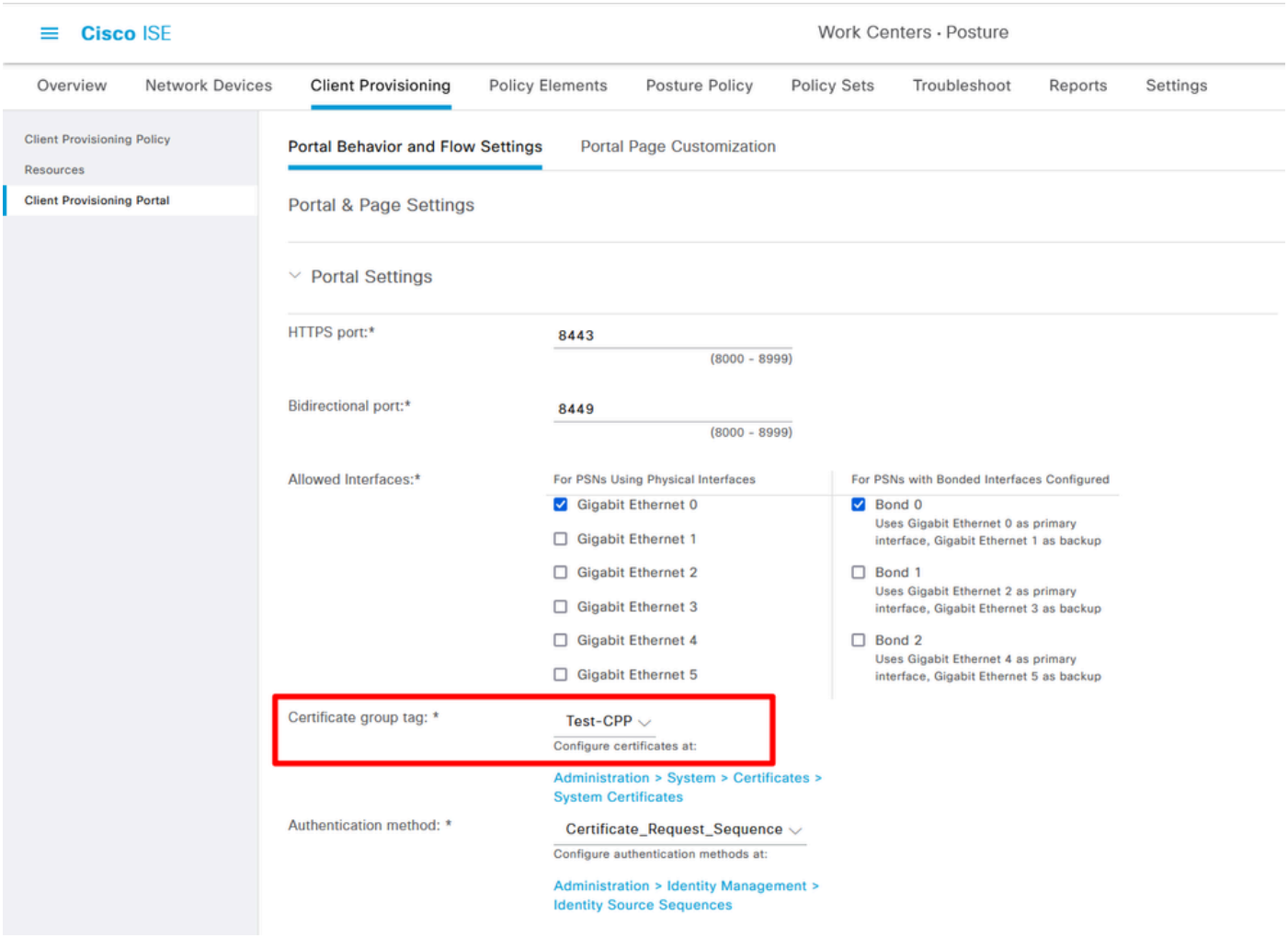
添加代理配置

步骤6.确认客户端调配门户，使用默认门户进行测试。（请从CA服务器生成CSR并申请SSL证书，并替换此门户设置上的证书组标记。否则，在测试过程中会出现证书不受信任警告。）

导航至工作中心>状态>客户端调配>客户端调配门户:

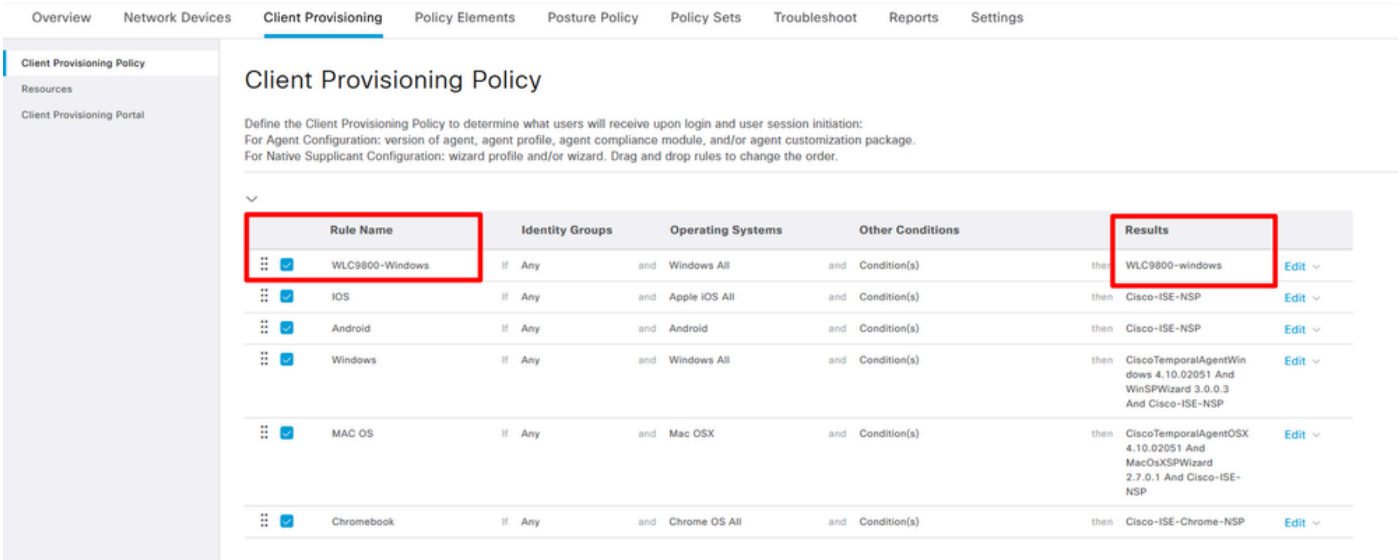


选择Client Provisioning Portal 01



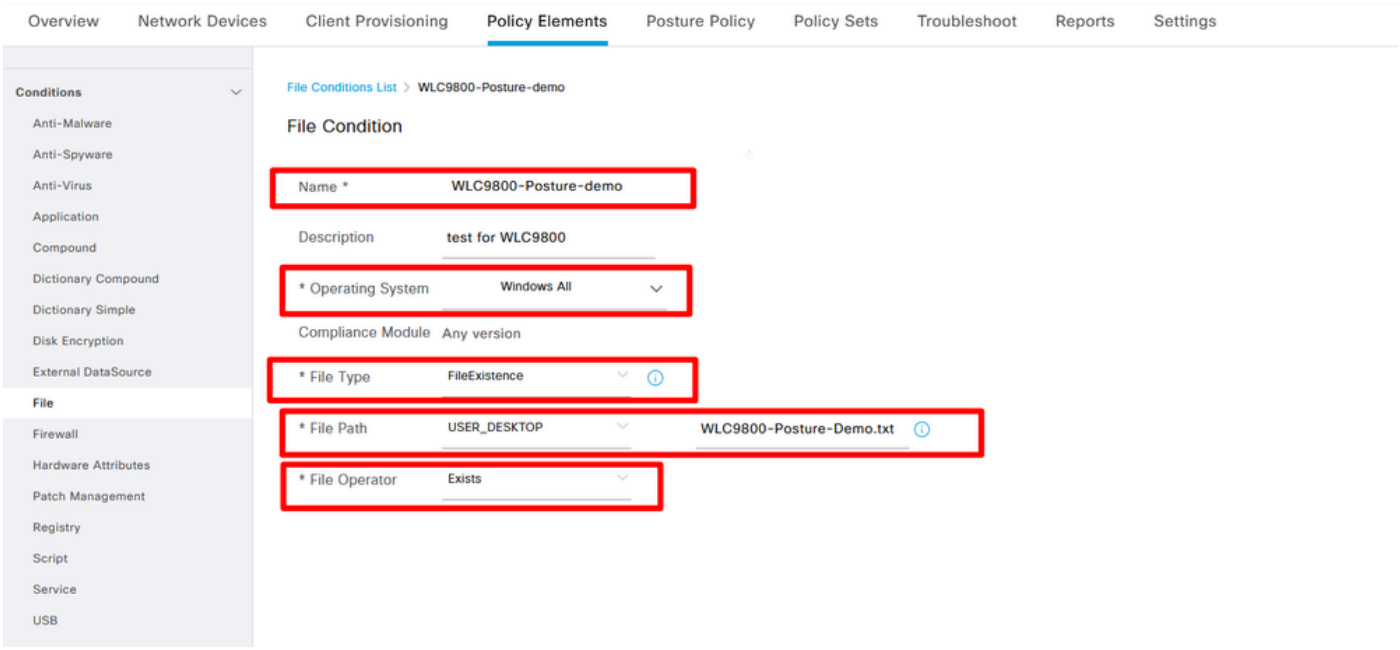
选择Client Provisioning Portal 02

步骤7.创建客户端调配策略。导航到Work Centers> Posture> Client Provisioning> Client Provisioning Policy > Edit>插入上述新策略。



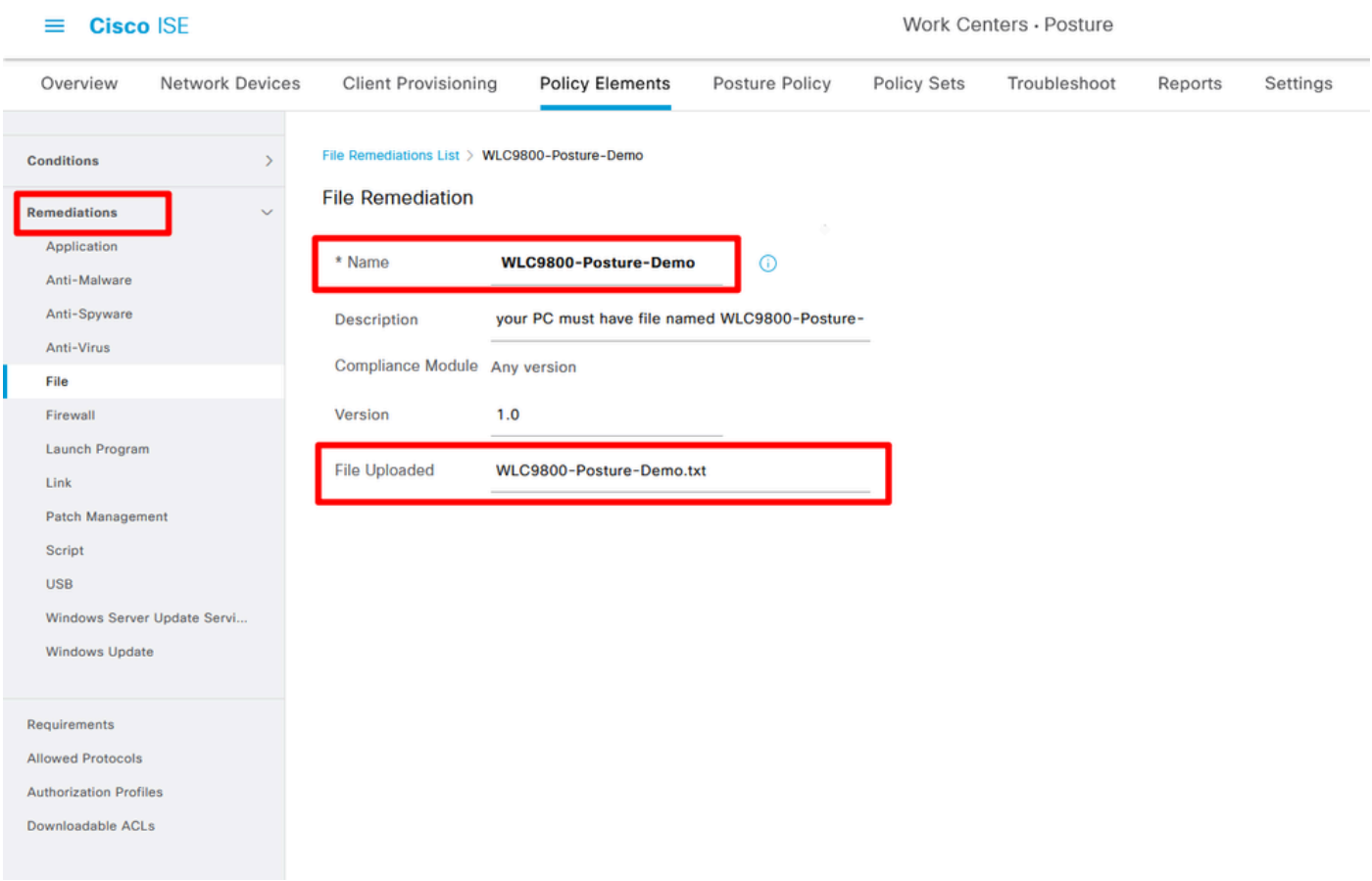
创建客户端调配策略

步骤8.创建文件条件。导航至工作中心>状态>策略元素>条件>文件>文件条件>添加:



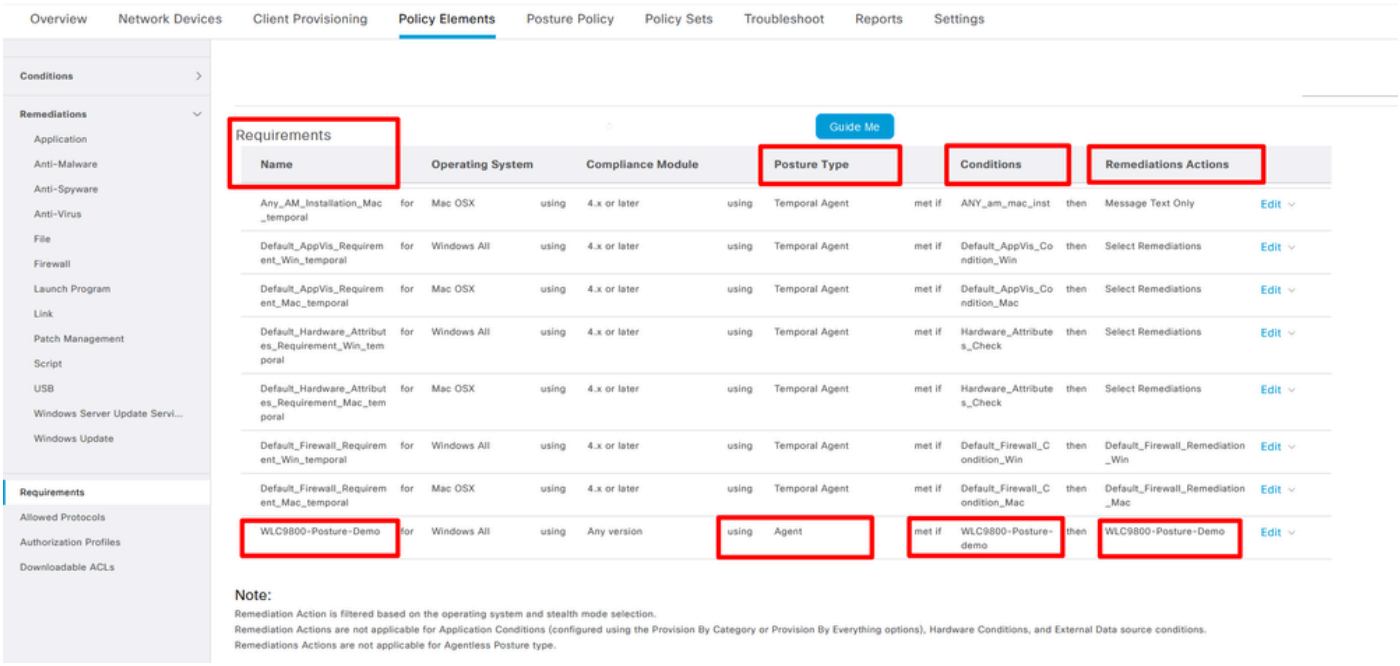
创建文件条件

第9步：创建补救(Create Remediations)导航到工作中心(Work Centers)>状态(Posture)>策略元素(Policy Elements)>补救(Remediations)>文件(File)>添加(Add):



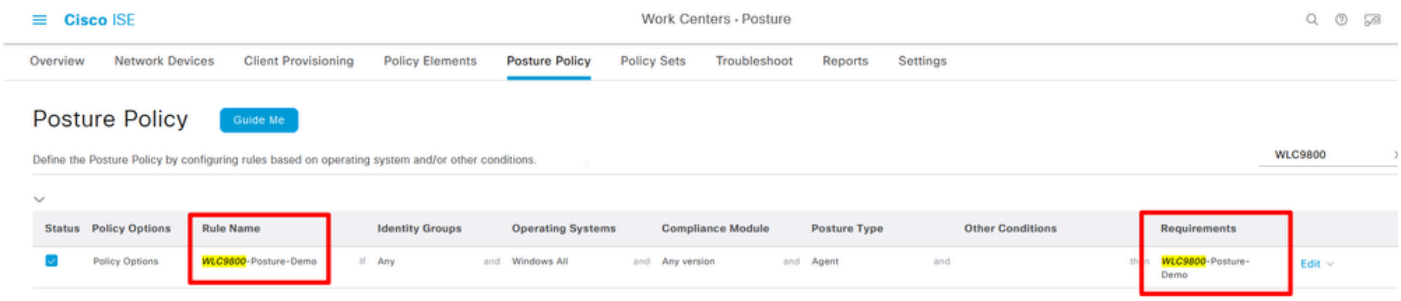
创建文件补救

步骤10.创建需求。导航至工作中心>状态>策略元素>要求>插入新要求:



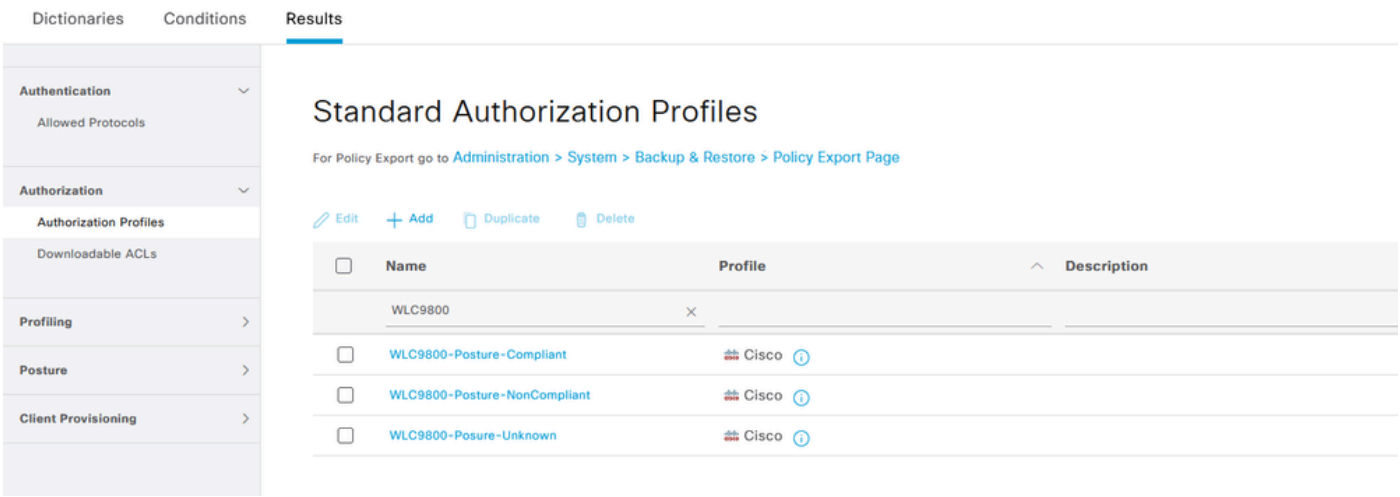
创建状况要求

步骤11.创建状态策略。导航到工作中心>状态>插入新策略:

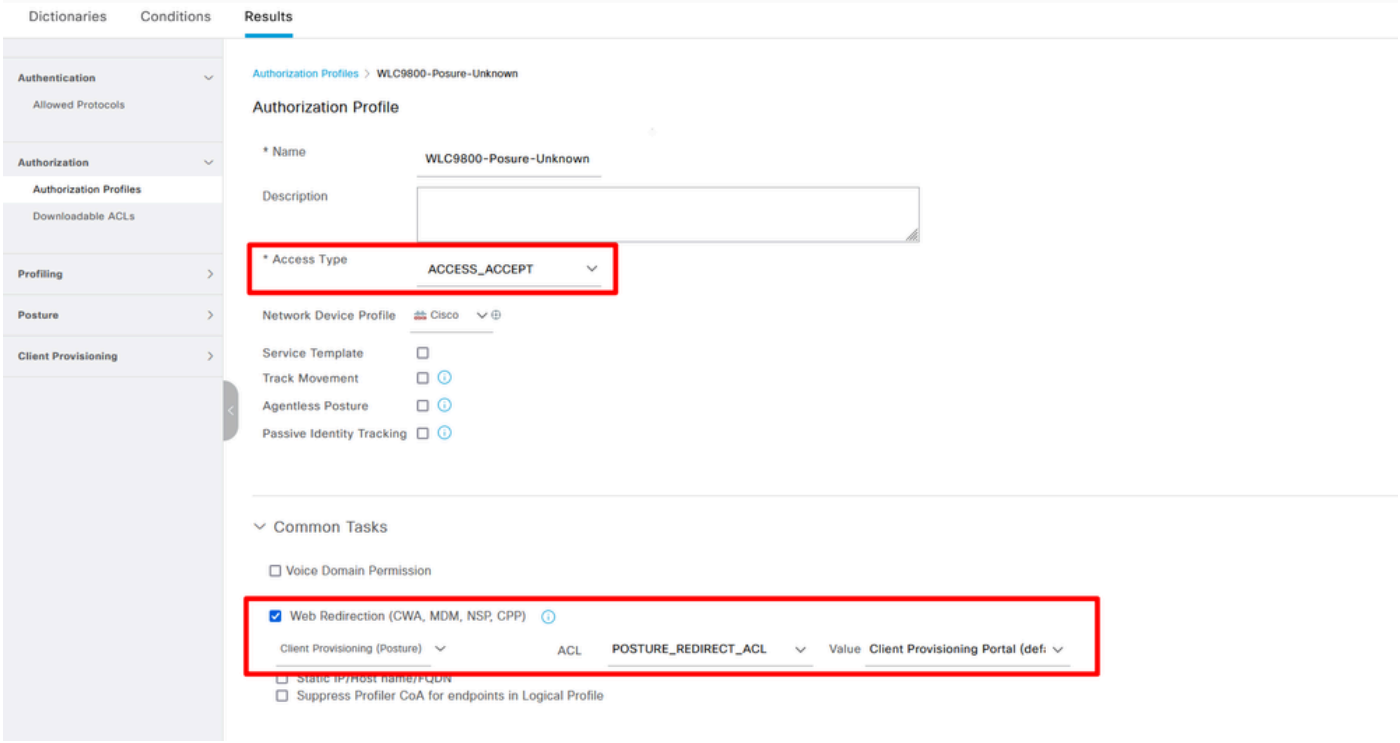


创建状态策略

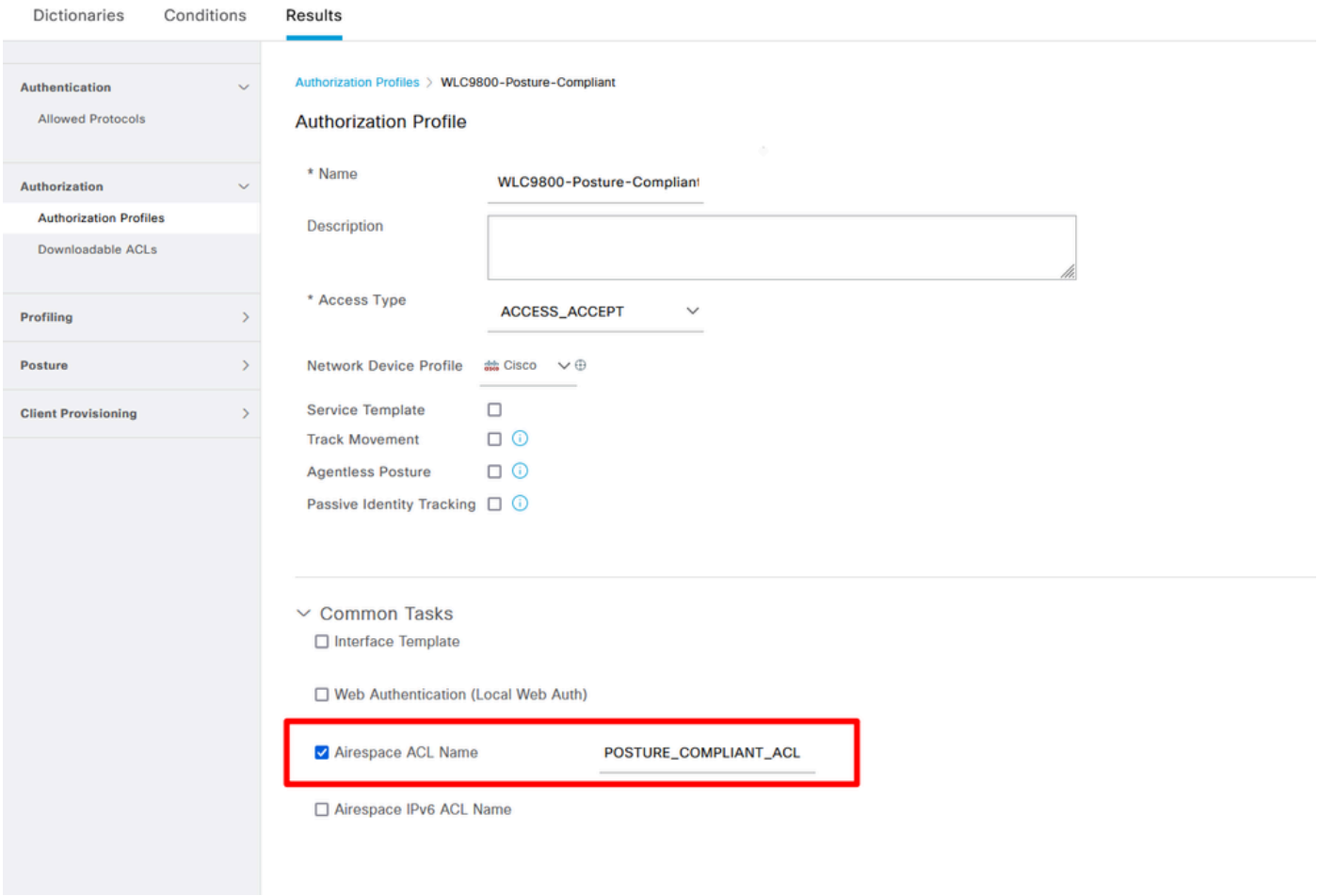
步骤12.创建三个授权配置文件：状态未知；安全评估状态为“不兼容”；安全评估状态是合规的。导航到Policy > Policy Elements> Results> Authorization> Authorization Profiles> Add:



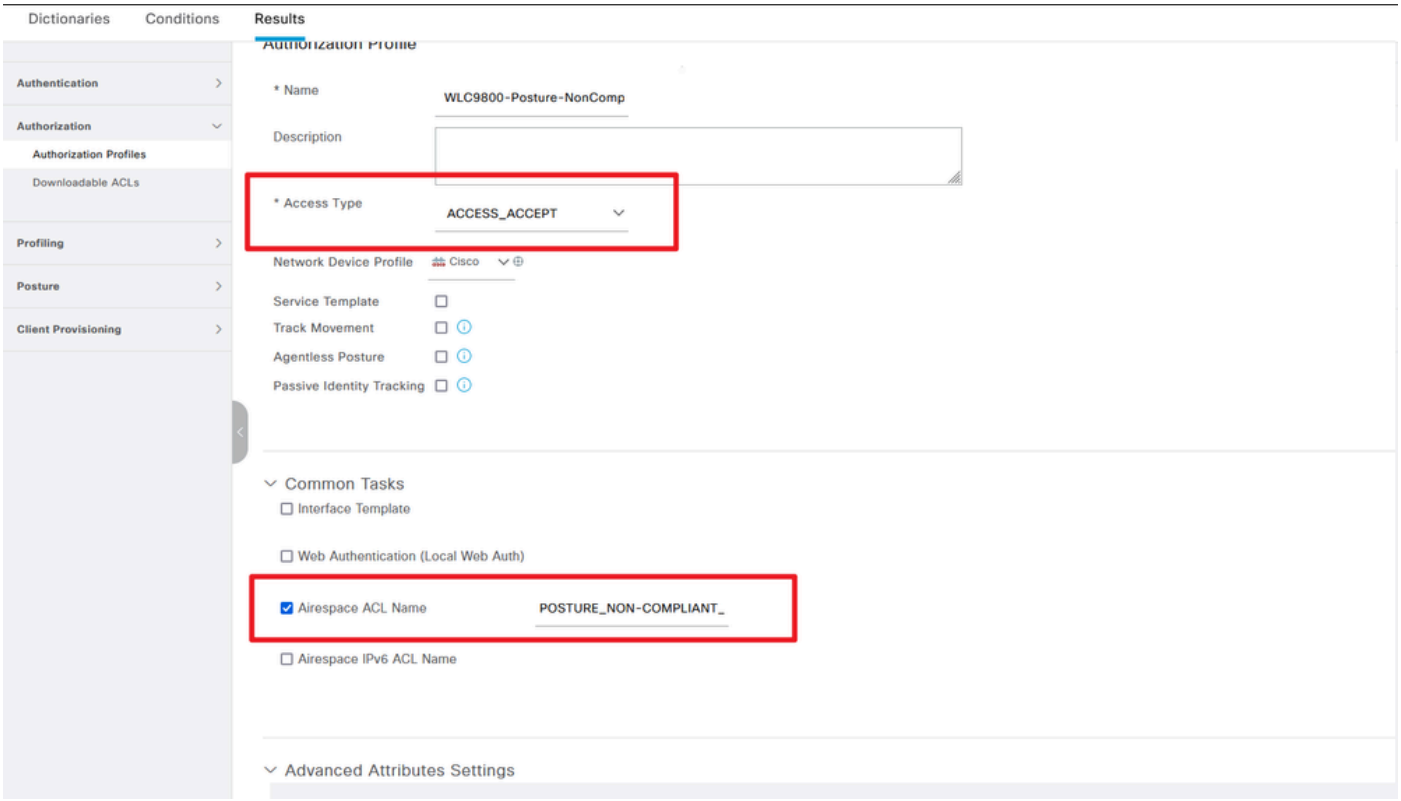
创建授权配置文件01



创建授权配置文件02



创建授权配置文件03

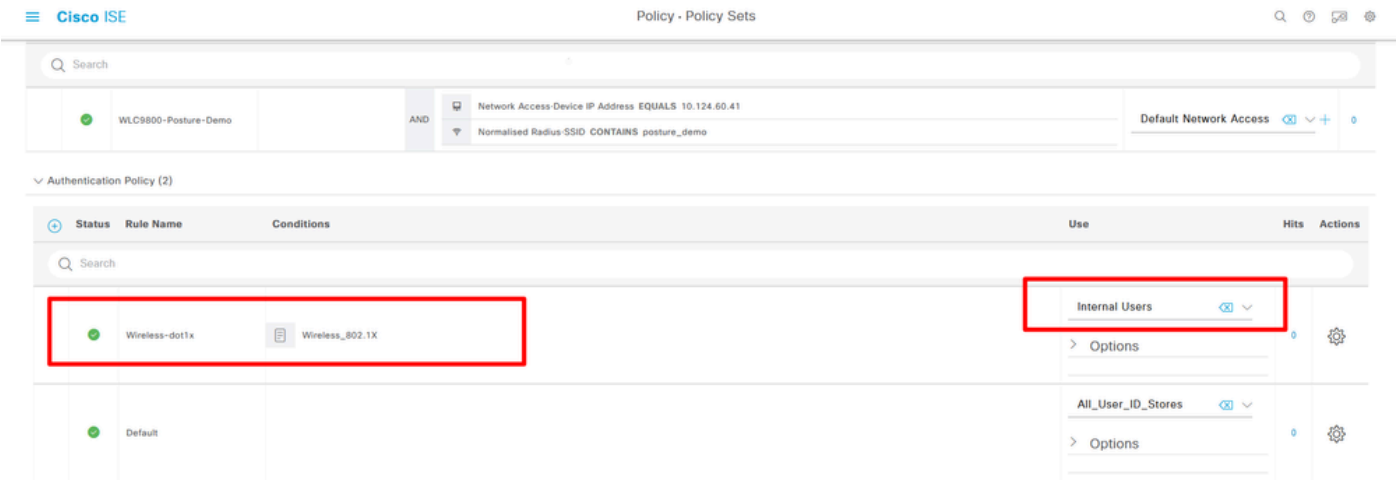


步骤13.创建策略集。导航到Policy> Policy

创建策略集

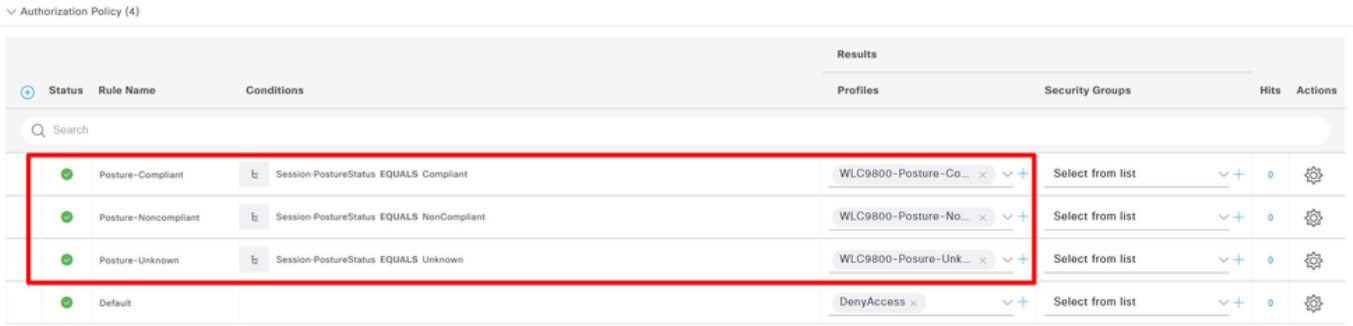
集>添加图标:

步骤14.创建身份验证策略导航到策略>策略集>展开"WLC9800-Posture-Demo">身份验证策略>添加:



创建身份验证策略

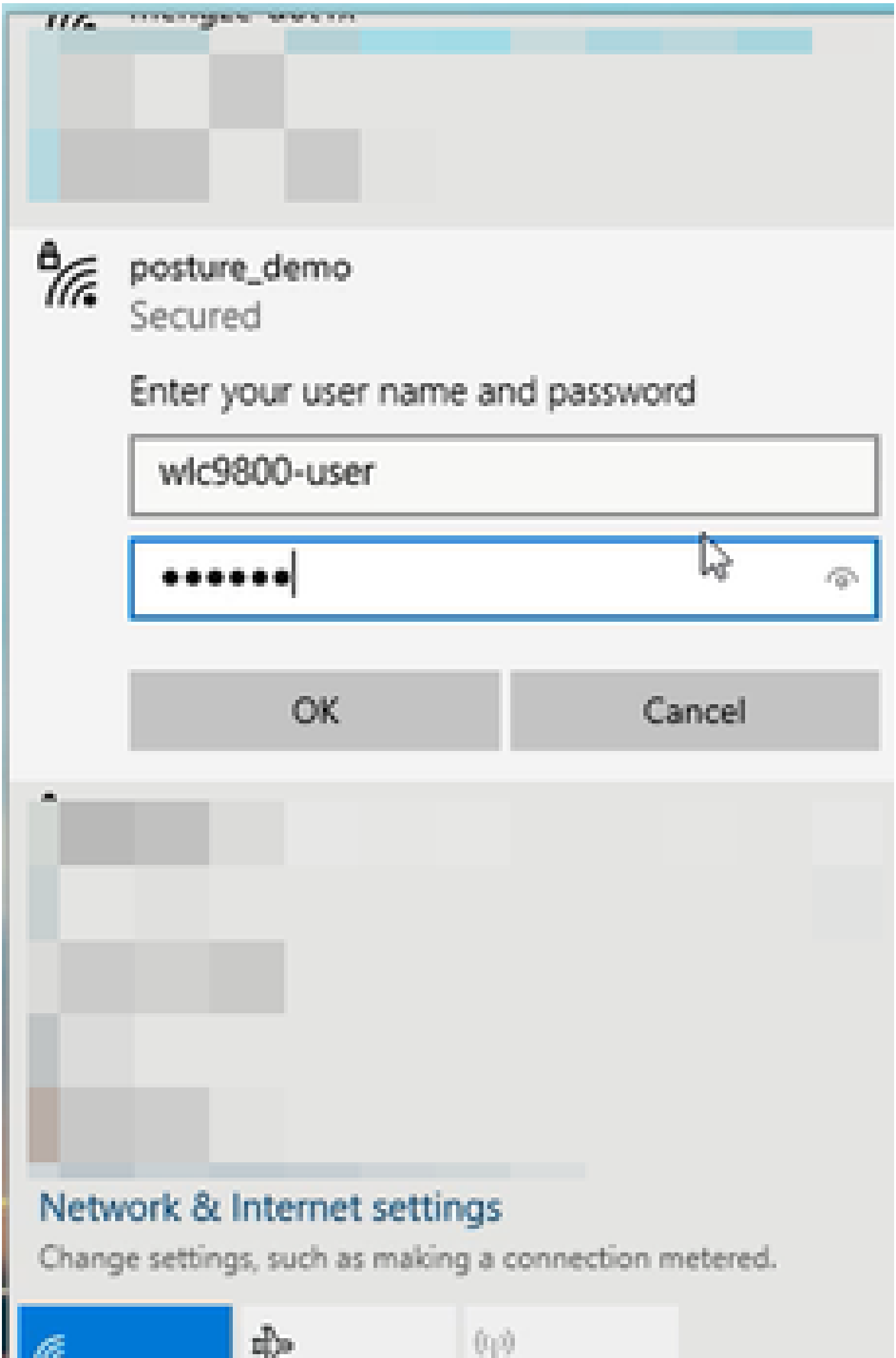
第15步：创建授权策略导航到Policy> Policy Sets>展开“WLC9800-Posture-Demo”> Authorization Policy>添加:



创建授权策略

Examples

1.使用正确的802.1X凭证连接测试SSID posture_demo。


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

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）。