使用外部身份验证配置本地Web身份验证

目录

简介

本文档介绍如何在9800 WLC和ISE上配置使用外部身份验证的本地Web身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800无线LAN控制器(WLC)配置
- 轻量接入点(LAP)
- 如何设置和配置外部Web服务器身份服务引擎(ISE)。
- 如何设置和配置DHCP和DNS服务器。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800-40 WLC Cisco IOS® XE版本17.18.4a，带APSP1和APSP2
- 身份服务引擎(ISE)，版本3.2.0.542
- Cisco®无线9172I系列Wi-Fi 7接入点，版本17.18.4.202

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。

Web 身份验证

Web身份验证是允许访客用户访问网络的第3层安全功能。

此功能旨在提供对开放式SSID的简单且安全的访客访问，无需配置用户配置文件，并且还可以与第2层安全方法配合使用。

Web身份验证的目的是允许不受信任的设备（访客）通过可以配置安全机制的访客WLAN以有限的网络访问权限访问网络，并且确保网络的安全不受影响。访客用户若要访问网络，需要成功进行身份验证，即需要提供正确的凭证或接受可接受使用策略(AUP)才能访问网络。

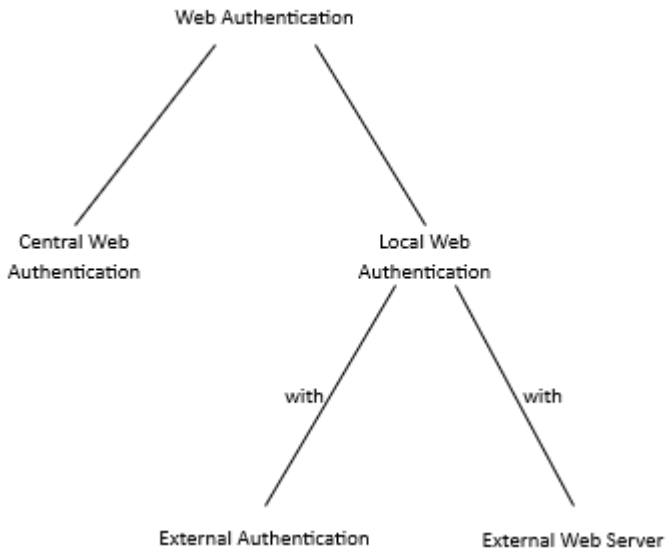
Web身份验证对公司来说是一项优势，因为它提高了用户忠诚度，使公司能够遵守访客用户必须接受的免责声明，并允许公司与访客进行互动。

要部署Web身份验证，必须考虑如何处理访客门户和身份验证。有两种常用方法：

- 本地Web身份验证(LWA):一种将访客用户直接从WLC重定向到门户的方法。重定向和预网络身份验证ACL在WLC上本地配置。
- 集中Web身份验证(CWA):一种访客用户的重定向方法，其中重定向URL和重定向ACL在外部服务器（例如ISE）上集中配置，并通过RADIUS传递到WLC。在集中式Web身份验证中，重定向URL和重定向ACL集中位于外部服务器（例如RADIUS）上。 RADIUS服务器是处理身份验证的服务器，它向WLC发送指令。在CWA中，WLC不需要本地Web身份验证证书，在中心Web门户上只需要一个证书，并且需要中央身份验证服务器，例如ISE。要详细阅读CWA，请导航至在Catalyst 9800 WLC和ISE上配置中心Web身份验证(CWA)。

在本地Web身份验证中，Web门户可以存在于WLC上或外部服务器上。在使用外部身份验证的LWA中，Web门户存在于WLC上。在使用外部Web服务器的LWA中，Web门户存在于外部服务器（例如Cisco DNA空间）上。 有关具有外部Web服务器的LWA的示例，请参阅：使用Catalyst 9800 WLC配置DNA空间强制网络门户。

不同Web身份验证方法的示意图：



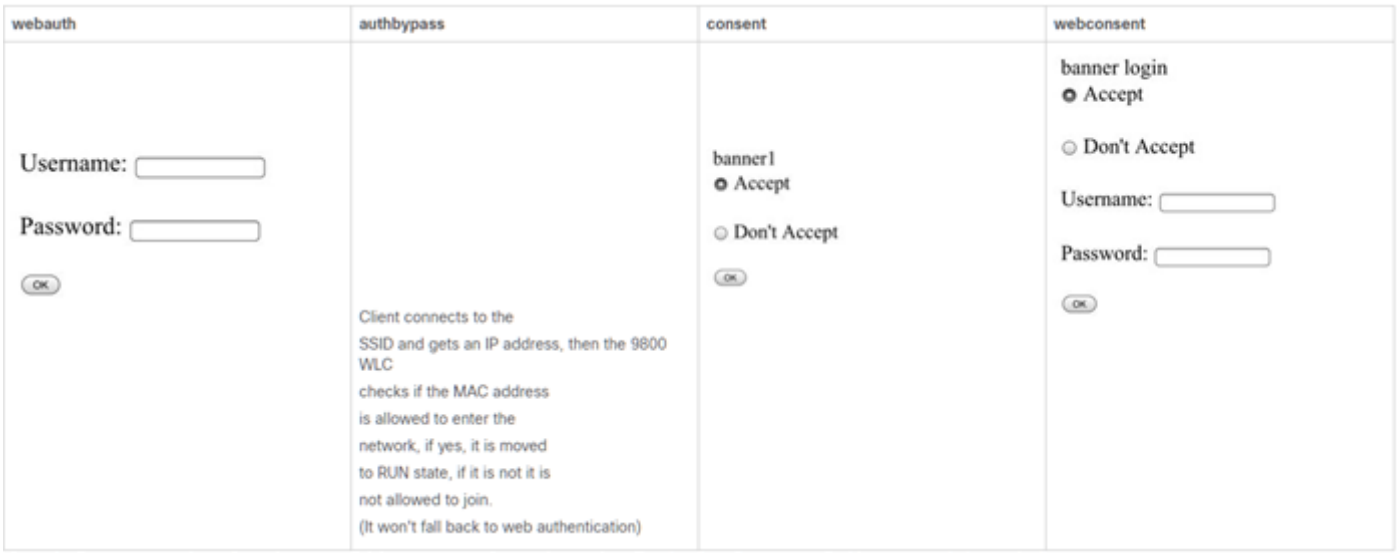
不同的Web身份验证方法图

注意：如果要在9800 WLC上部署具有Web身份验证的Wi-Fi 7 AP，请确保运行推荐的Cisco IOS XE版本，例如17.18.4a或更高版本。

身份验证类型

有四种身份验证类型用于对访客用户进行身份验证：

- Webauth:输入用户名和密码.
- 同意（网络通过）：接受AUP。
- Authbypass:基于访客用户设备的MAC地址的身份验证。
- Web同意：用户名/密码和接受AUP的混合。



用于对访客用户进行身份验证的四种身份验证类型

用于身份验证的数据库

身份验证的凭据可以存储在LDAP服务器上、本地存储在WLC上或RADIUS服务器上。

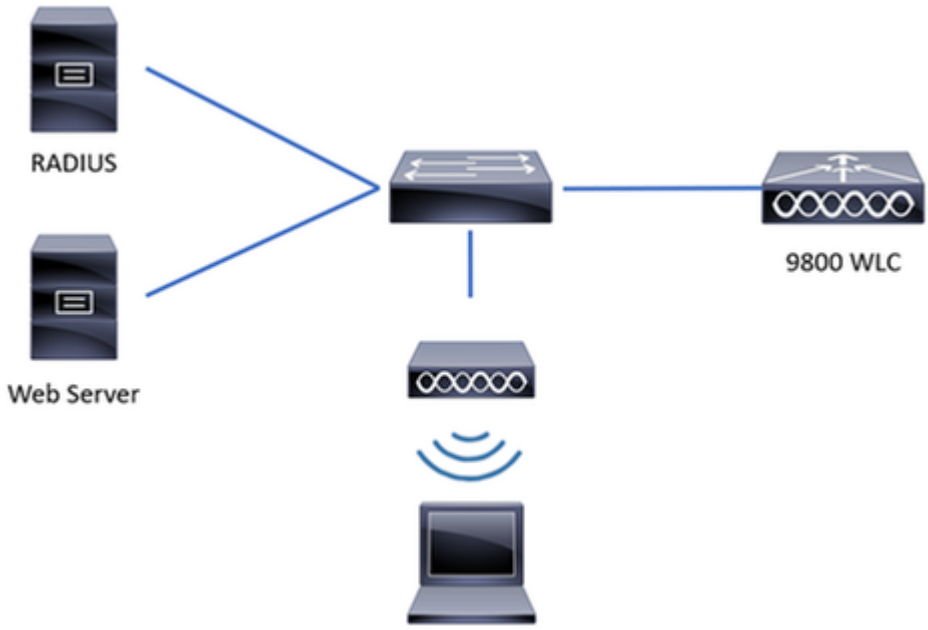
- 本地数据库：凭证（用户名和密码）存储在WLC本地。
- LDAP数据库：凭证存储在LDAP后端数据库中。WLC向LDAP服务器查询数据库中特定用户的凭证。
- RADIUS数据库：凭证存储在RADIUS后端数据库中。WLC向RADIUS服务器查询数据库中特定用户的凭证。

本地Web身份验证

在本地Web身份验证中，访客用户直接从WLC重定向到Web门户。

Web门户可以位于WLC中或其他服务器中。它使本地化的原因是重定向URL和匹配流量的ACL必须位于WLC上（而不是Web门户的位置）。 在LWA中，当访客用户连接到访客WLAN时，WLC会截取来自访客用户的连接，并将它们重定向到Web门户URL，在此请求访客用户进行身份验证。当访客用户输入凭证（用户名和密码）时，WLC会捕获凭证。WLC使用LDAP服务器、RADIUS服务器或本地数据库（WLC上本地存在的数据库）对访客用户进行身份验证。 对于RADIUS服务器（外部服务器，如ISE），它不仅可用于存储凭证，还可用于提供设备注册和自助调配选项。如果是外部Web服务器（例如Cisco DNA Spaces），则存在Web门户。在LWA中，WLC上有一个证书，Web门户上有一个证书。

该图表示LWA的通用拓扑：



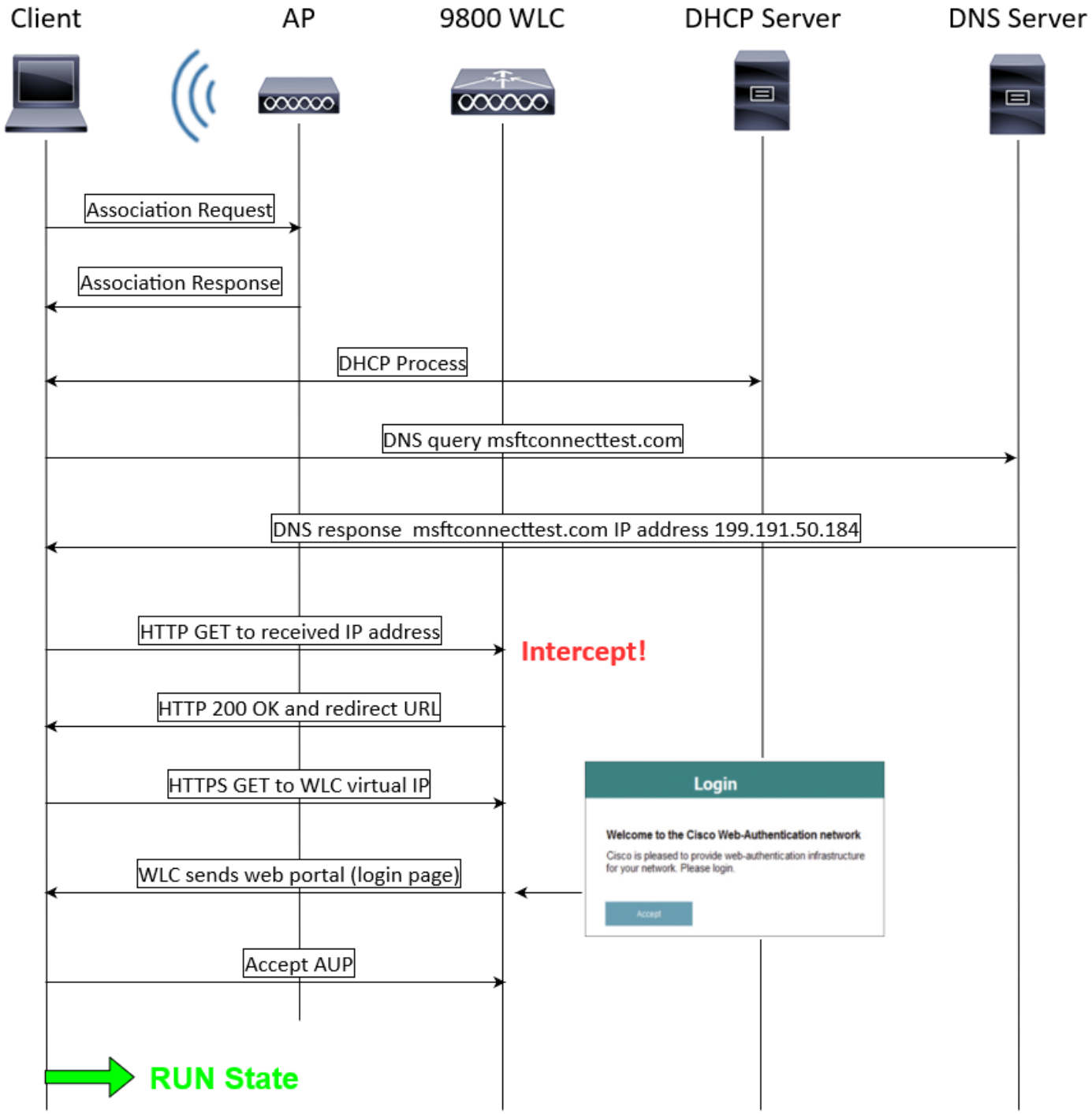
LWA的通用拓扑

LWA网络拓扑中的设备：

- 客户端：向DHCP和DNS服务器发送请求，请求访问访客WLAN，并响应来自WLC的请求。
- 访问点:连接到交换机，广播访客WLAN，并提供与访客用户设备的无线连接。它还允许在访客用户进行身份验证之前（在输入有效凭证之前）使用DHCP和DNS数据包。
- WLC:管理AP和客户端。WLC托管重定向URL和匹配流量的ACL。拦截来自访客用户的HTTP请求，将其重定向到访客用户必须进行身份验证的Web门户（登录页面）。它捕获凭证并对访客用户进行身份验证，并向外部服务器、LDAP服务器或本地数据库发送访问请求以确认凭证是否有效。
- 身份认证服务器：使用访问接受/拒绝来响应来自WLC的访问请求。身份验证服务器验证来自访客用户的凭证，并在凭证有效或无效时通知WLC。如果凭证有效，访客用户有权访问网络（身份验证服务器提供设备注册和自助调配选项）。 如果凭证无效，访客用户将被拒绝访问网络。

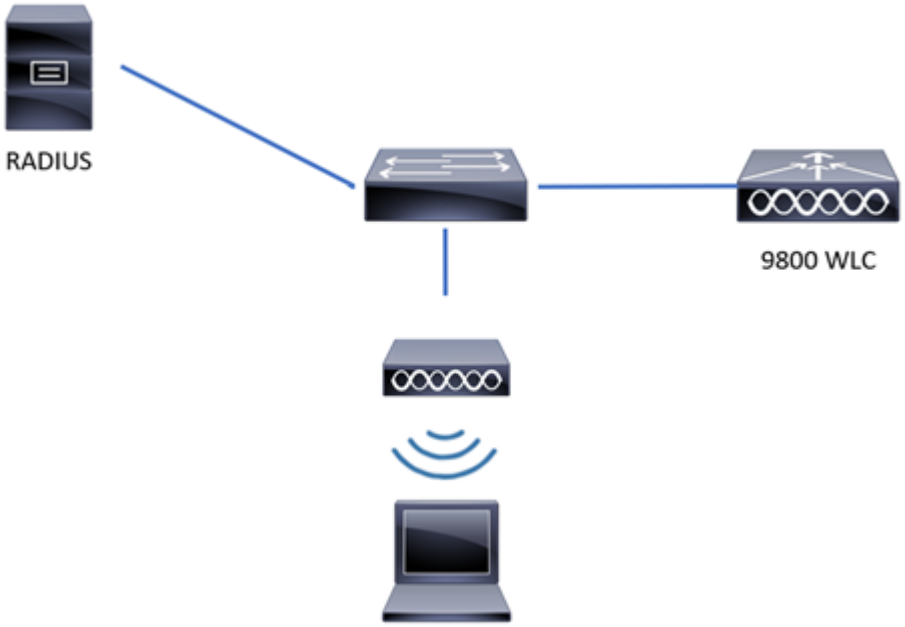
LWA流程：

- 访客用户与广播访客WLAN的AP关联。
- 访客用户通过DHCP过程获取IP地址。
- 访客用户希望对强制网络门户进行Internet连接检查。如果是苹果设备，它会尝试苹果强制网络门户；如果是Android设备，则尝试使用Android强制网络门户；如果是Windows设备，它将尝试Windows连接测试门户。
- 访客用户发送DNS查询请求强制网络门户IP地址。DNS服务器使用对应的IP地址响应查询。
- 访客用户向强制网络门户的IP地址发送HTTP GET消息。
- WLC拦截该消息并使用HTTP 200 OK和重定向URL回复访客用户。
- 访客用户向WLC虚拟IP发送HTTPS GET消息，WLC通过Web门户做出响应。
- 访客用户需要在Web门户上输入身份验证凭证。
- Web门户使用提供的凭证将用户重定向回WLC（如果使用外部Web门户）。
- WLC通过本地数据库对访客用户进行身份验证，或者向RADIUS或LDAP服务器发送查询，以确认凭证是否正确（如果身份验证类型为webconsent或webauth）。
- 如果凭证正确，则WLC对访客用户进行身份验证，并进入RUN状态。如果凭证不正确，WLC将删除访客用户。
- WLC将客户端重定向回在Web浏览器中输入的原始URL。



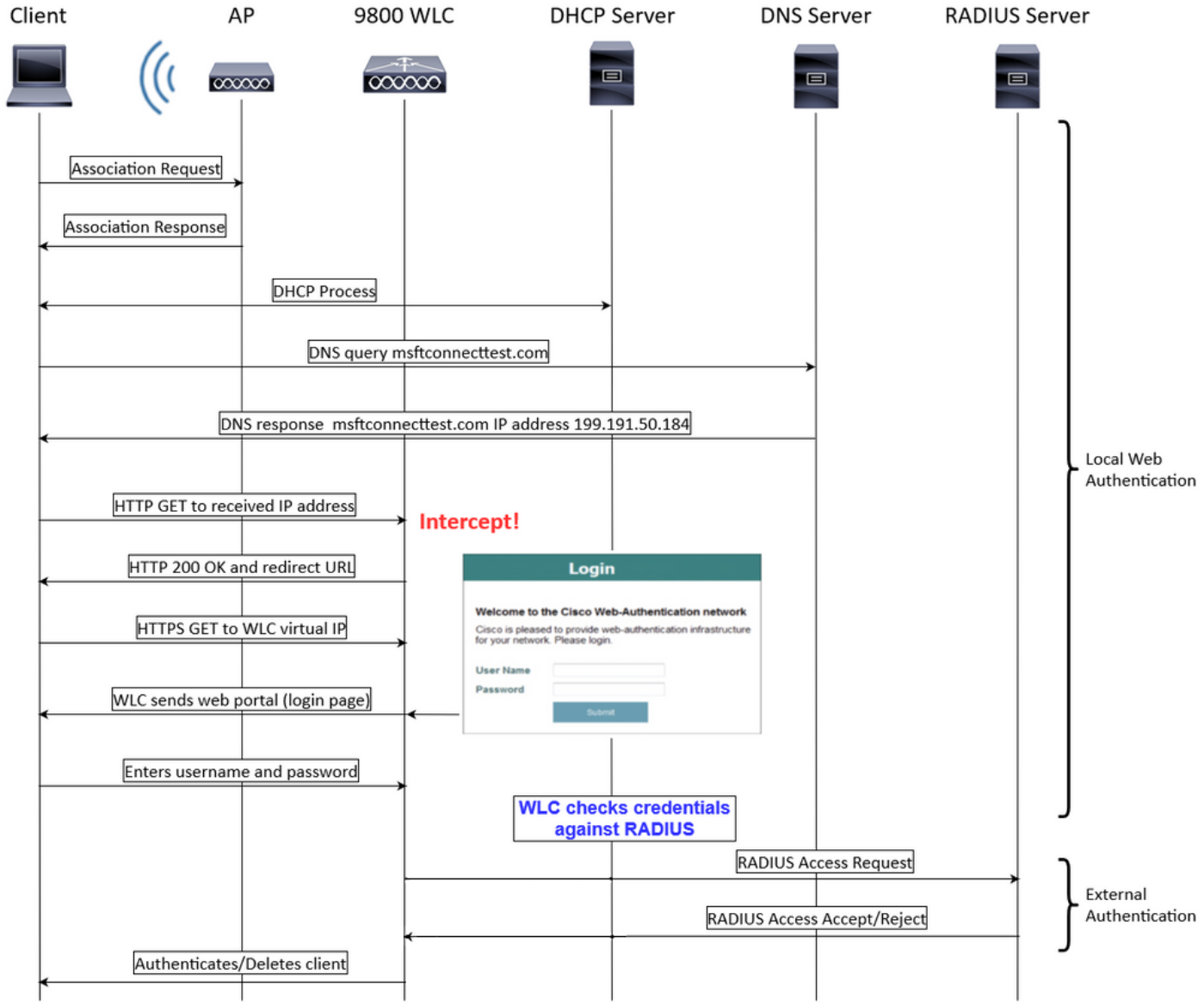
LWA流

使用外部身份验证的本地Web身份验证



LWA-EA的通用拓扑

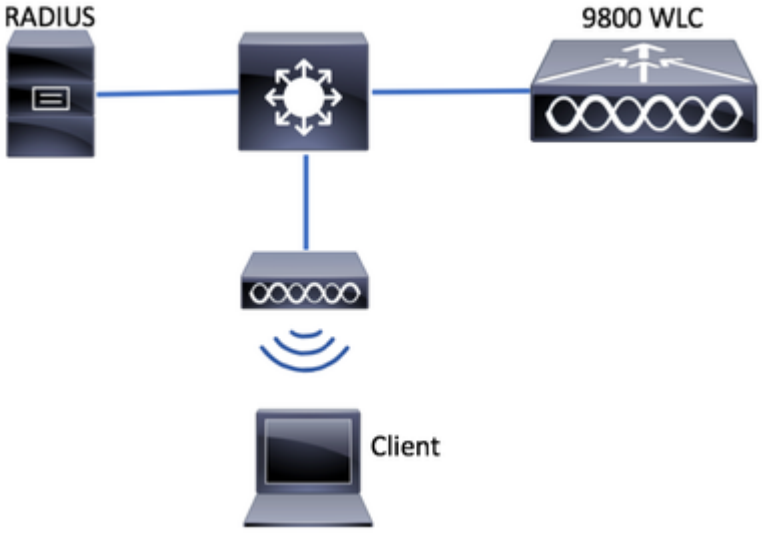
LWA-EA是LWA的一种方法，其中Web门户和重定向URL位于WLC上，凭证存储在外部服务器（例如ISE）上。WLC捕获凭证并通过外部RADIUS服务器对客户端进行身份验证。当访客用户输入凭证时，WLC根据RADIUS检查凭证，它发送RADIUS访问请求并从RADIUS服务器接收RADIUS访问接受/拒绝。然后，如果凭证正确，访客用户将进入RUN状态。如果凭证不正确，访客用户将由WLC删除。



LWA-EA流

配置

网络图



网络图

注意：此配置示例仅涵盖中央交换/身份验证。灵活本地交换配置对配置Web身份验证的要求略有不同。

在CLI上使用外部身份验证配置本地Web身份验证

配置AAA服务器和服务器组

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4


      auth-port 1812 acct-port 1813

9800WLC(config-radius-server)#key cisco

9800WLC(config-radius-server)#exit

9800WLC(config)#aaa group server radius RADIUSGROUP

9800WLC(config-sg-radius)#server name RADIUS

9800WLC(config-sg-radius)#end
```

配置本地身份验证和授权

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#end
```

配置WLAN安全参数

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

创建无线策略配置文件

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan




9800WLC(config-wireless-policy)#no shutdown


9800WLC(config-wireless-policy)#end
```

创建策略标记

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

为AP分配策略标记

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap


     >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

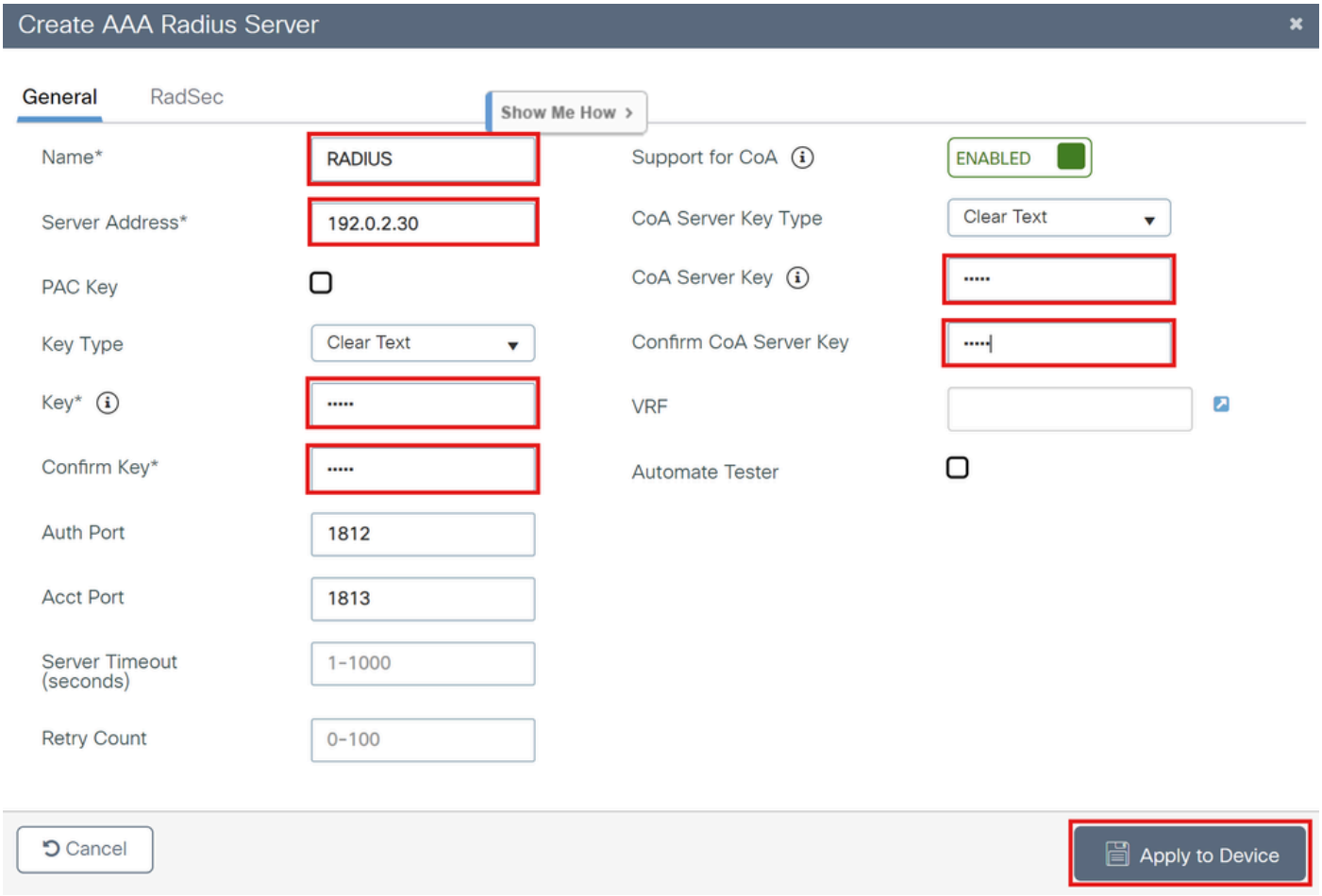
要在ISE端完成配置，请跳至ISE配置部分。

在WebUI上使用外部身份验证配置本地Web身份验证

9800 WLC 上的 AAA 配置

步骤1.将ISE服务器添加到9800 WLC配置。

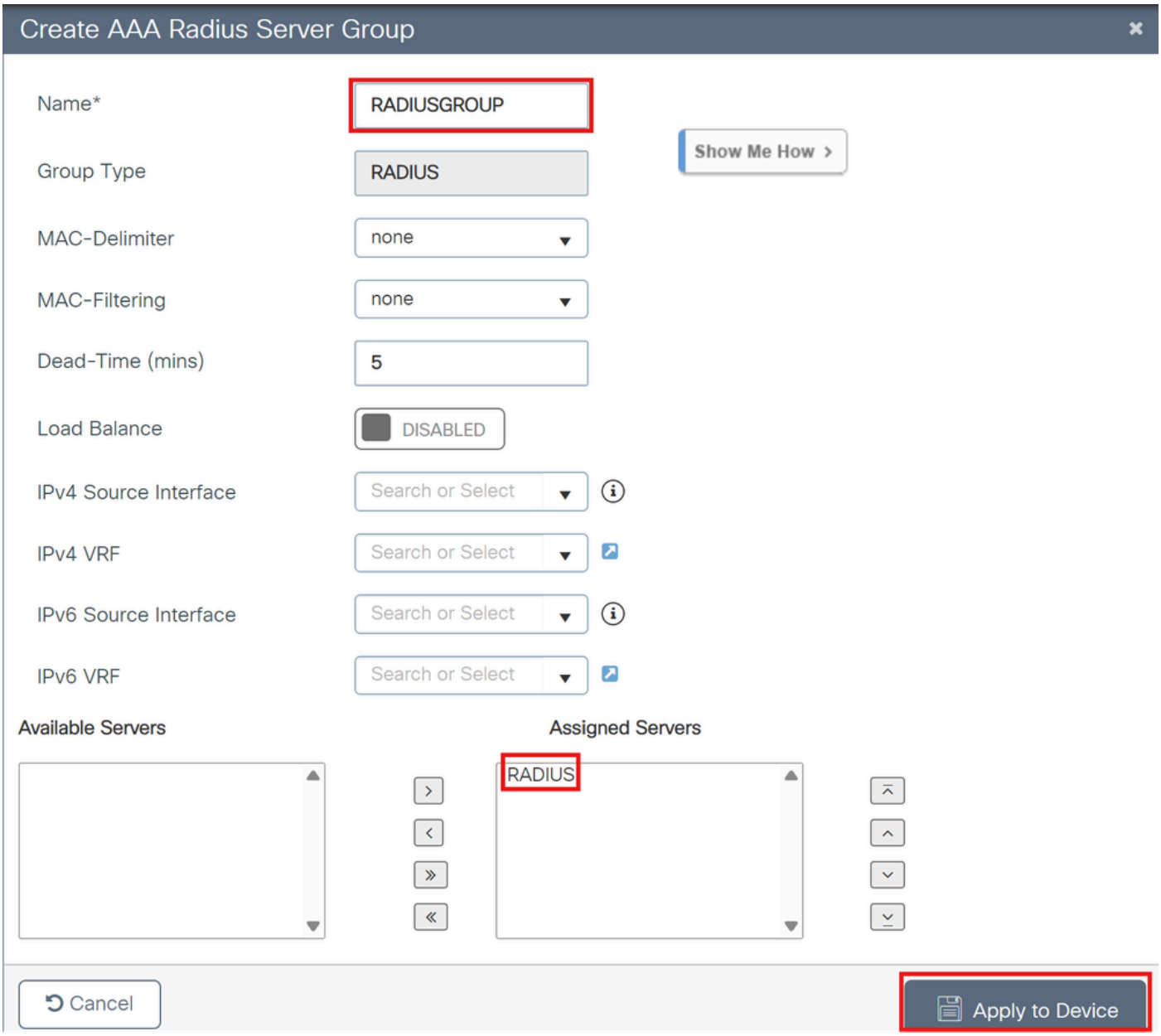
导航到Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add并输入RADIUS服务器信息，如图所示：



9800 WLC 上的 AAA 配置

步骤2.添加RADIUS服务器组。

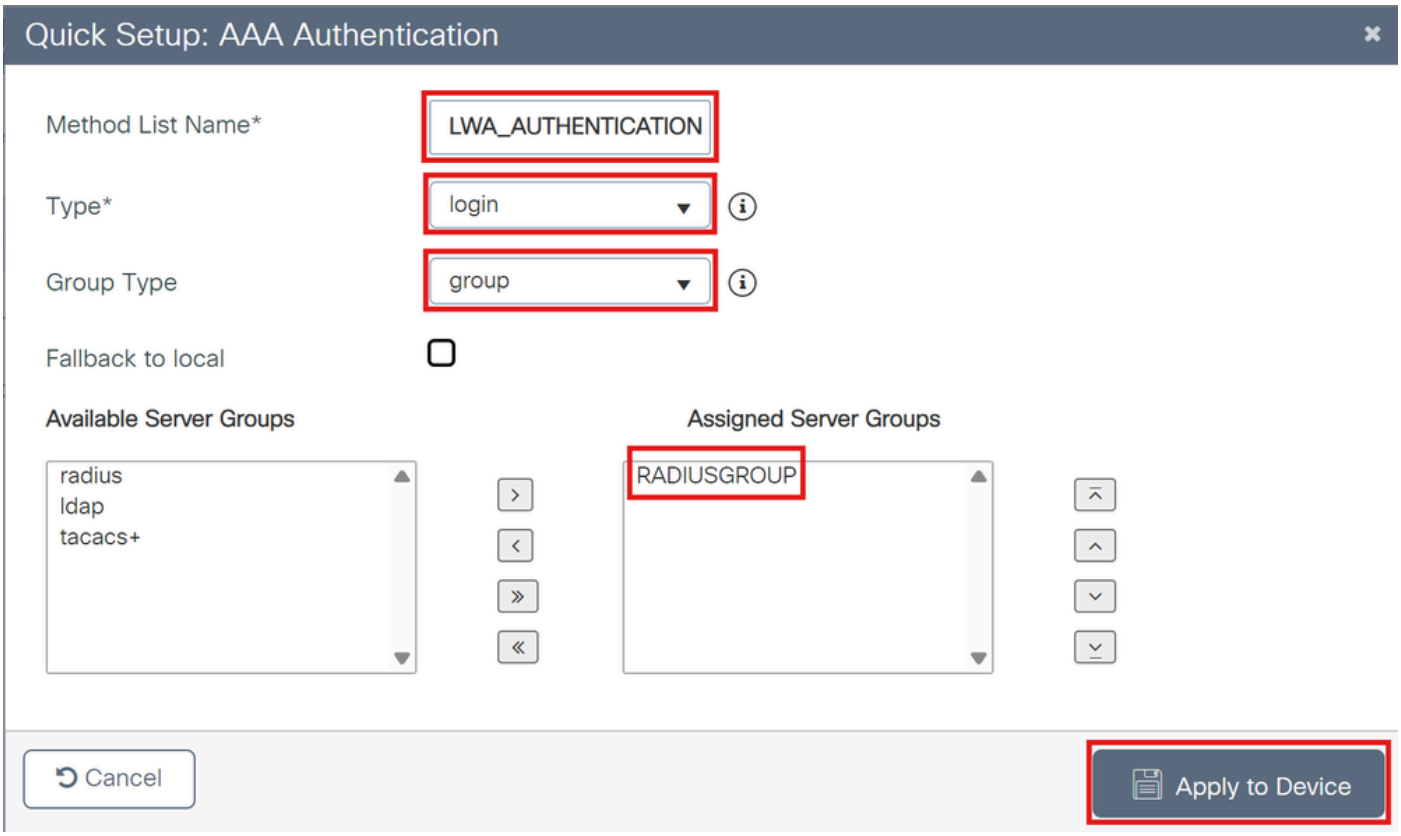
导航到Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add并输入RADIUS服务器组信息：



添加RADIUS服务器组

第 3 步： 创建身份验证方法列表。

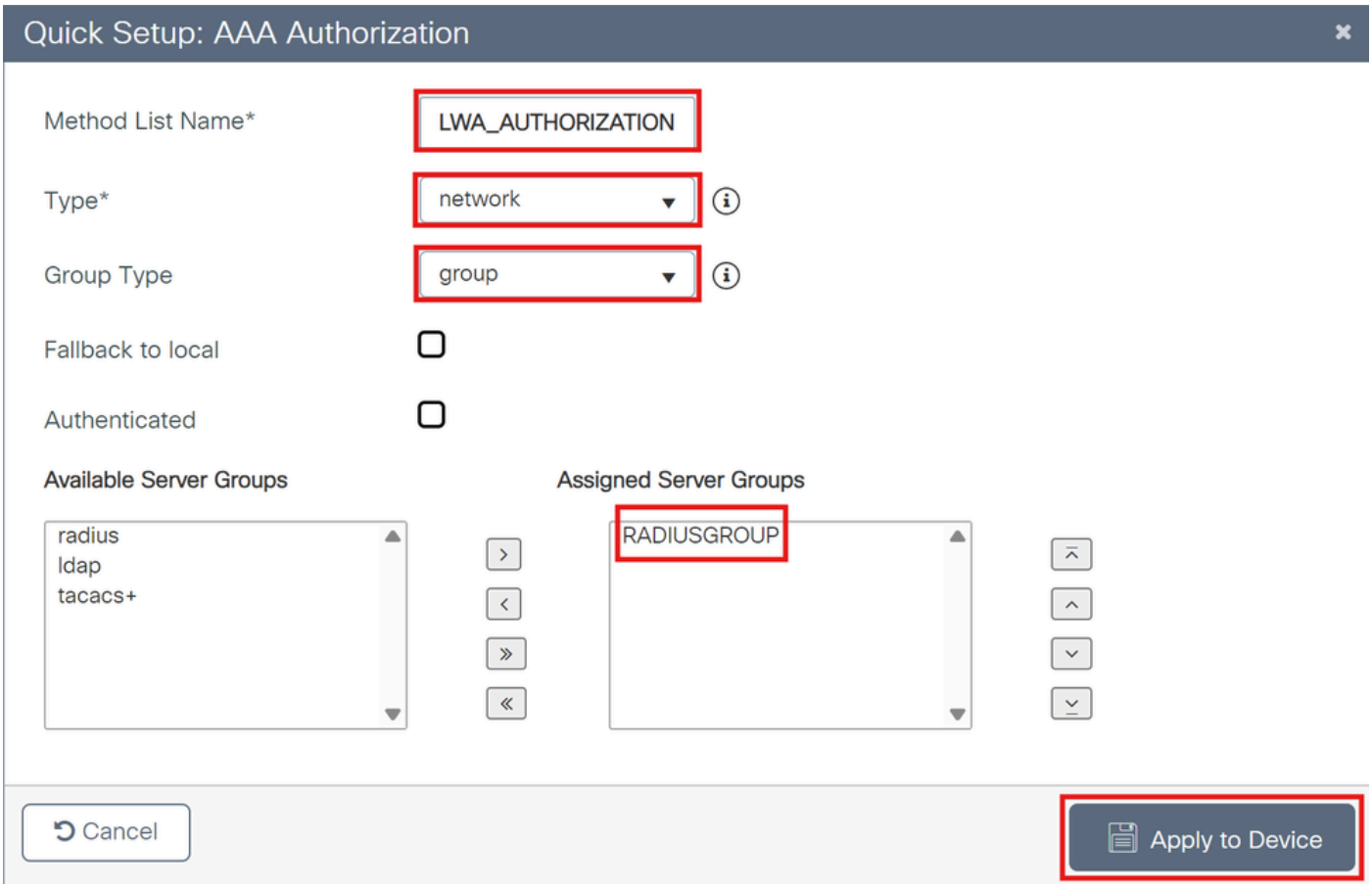
导航到配置>安全> AAA > AAA方法列表>身份验证> +添加：



创建身份验证方法列表

第 4 步： 创建授权方法列表。

导航到Configuration > Security > AAA > AAA Method List > Authorization > + Add:

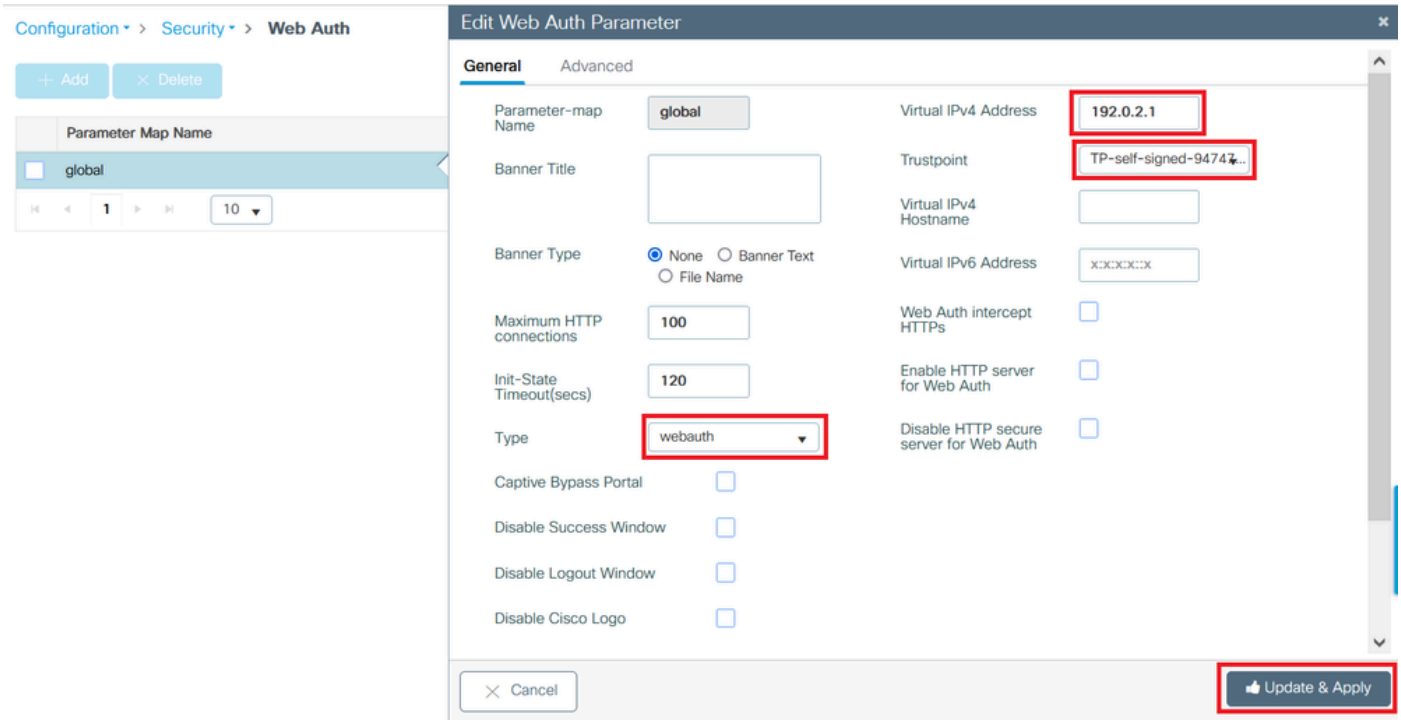


创建授权方法列表

Web身份验证配置

创建或编辑参数映射。选择类型为webauth,虚拟IPv4地址必须是网络中未使用的地址以避免IP地址冲突，然后添加信任点。

导航到配置>安全> Web身份验证> + Add或选择参数映射：

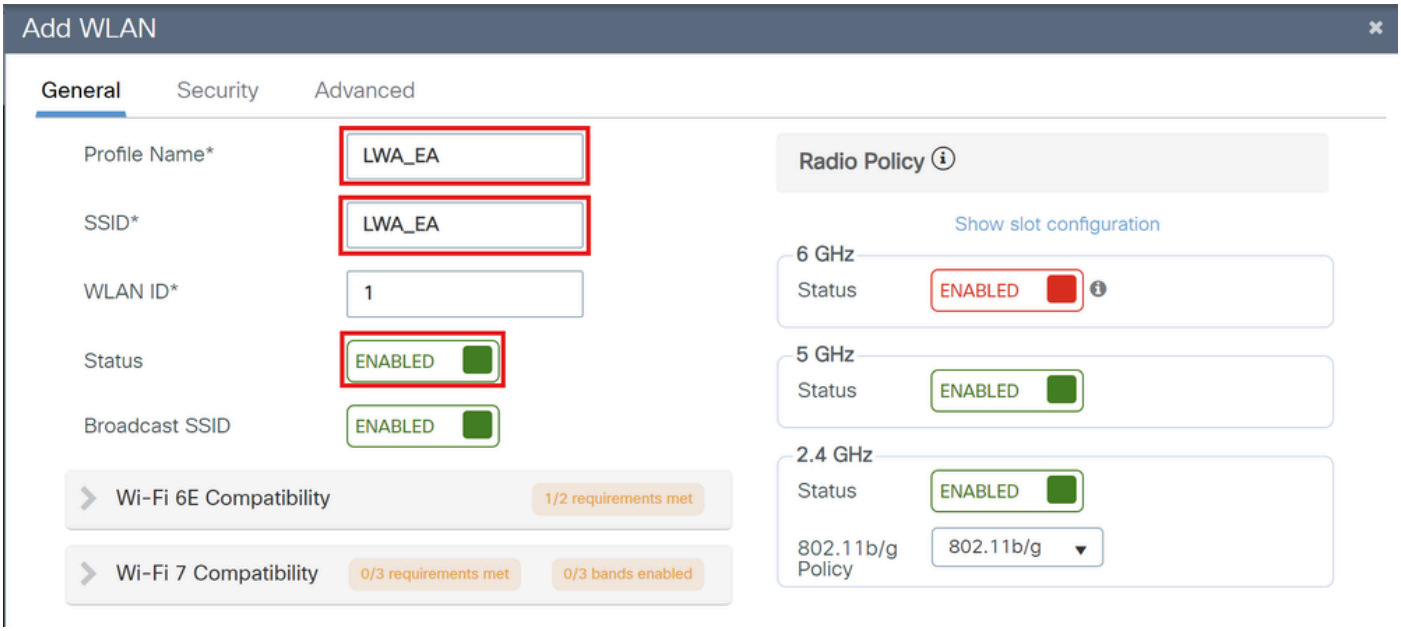


Web身份验证配置

WLAN 配置

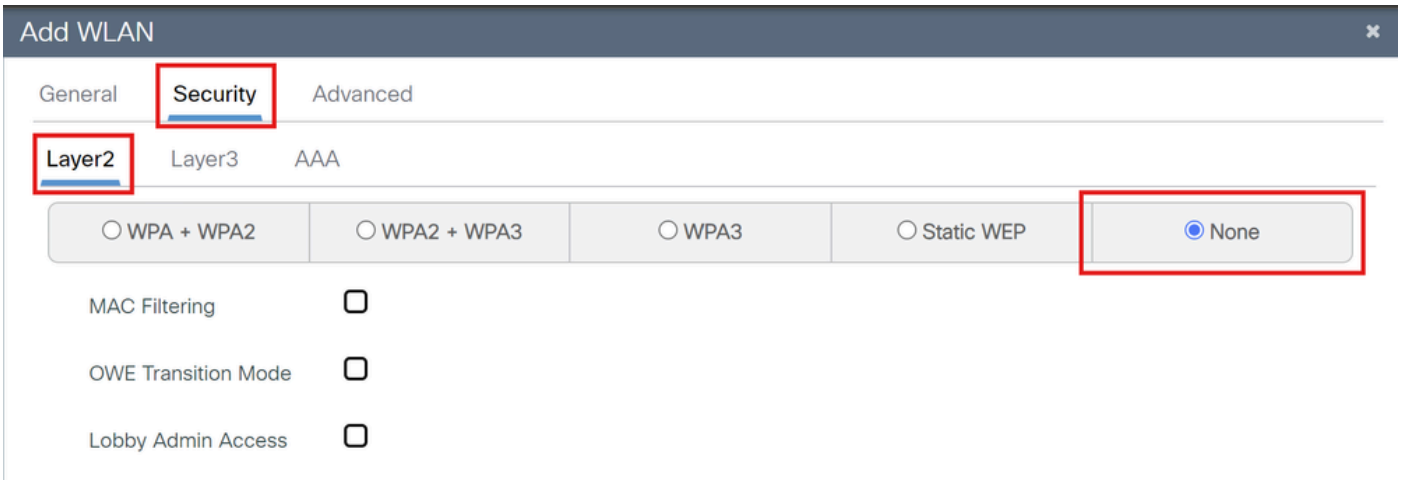
第 1 步： 创建 WLAN.

导航至配置 > 标签和配置文件 > WLAN > +添加，然后根据需要配置网络。



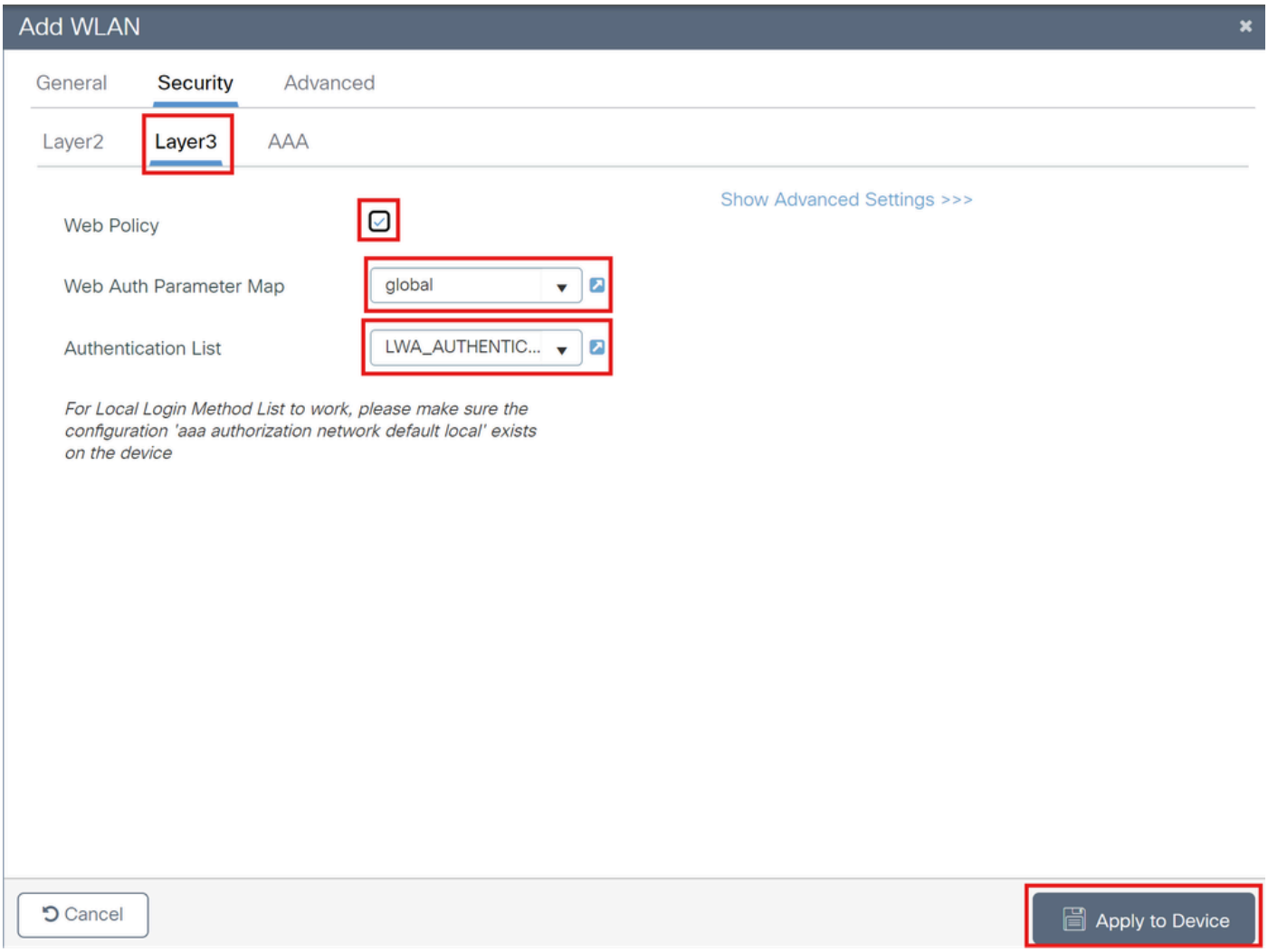
创建WLAN

步骤2.导航到Security > Layer2，并在Layer 2 Security Mode上选择None。



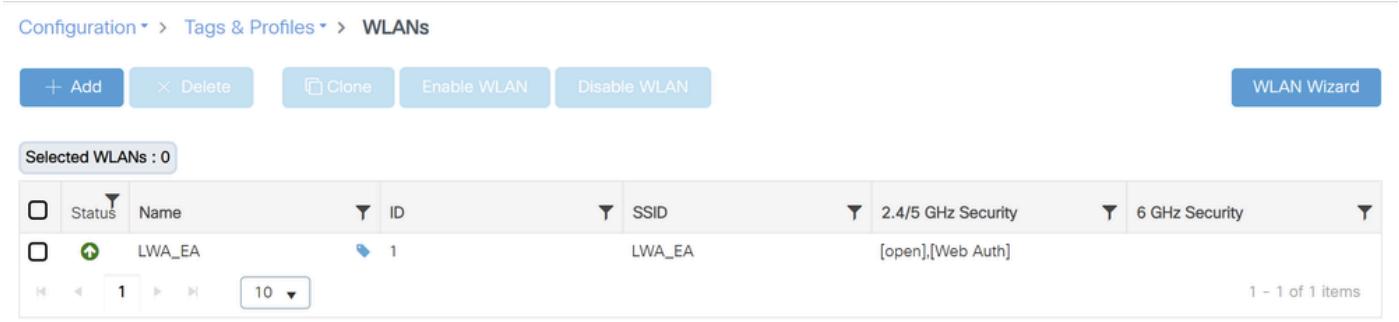
创建WLAN安全

第3步：导航到安全>第3层，在Web策略上勾选该框，在Web身份验证参数映射上选择参数名称，在身份验证列表上选择以前创建的身份验证列表。



创建WLAN身份验证列表

WLAN显示在WLAN列表中：



创建的WLAN

策略配置文件配置

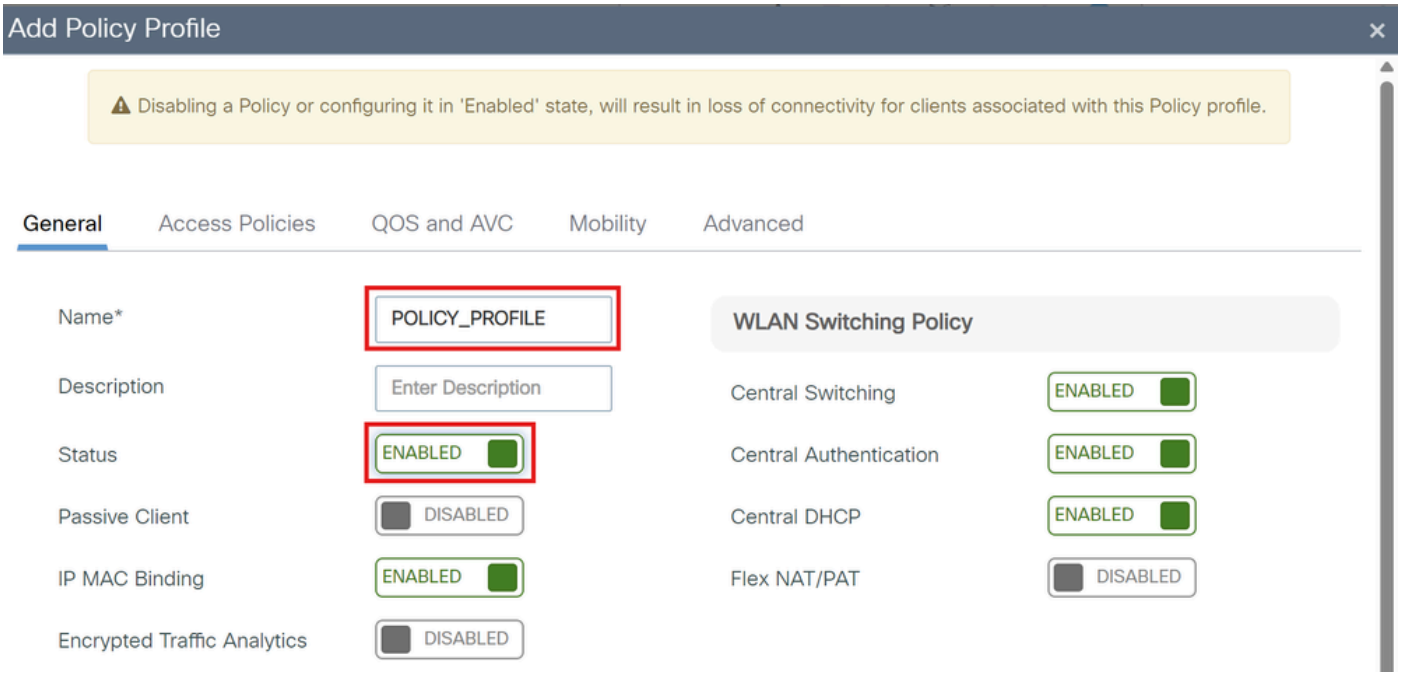
在策略配置文件中，您可以选择分配客户端的VLAN以及其他设置。

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，然后配置默认策略配置文件或创建新配置文件。

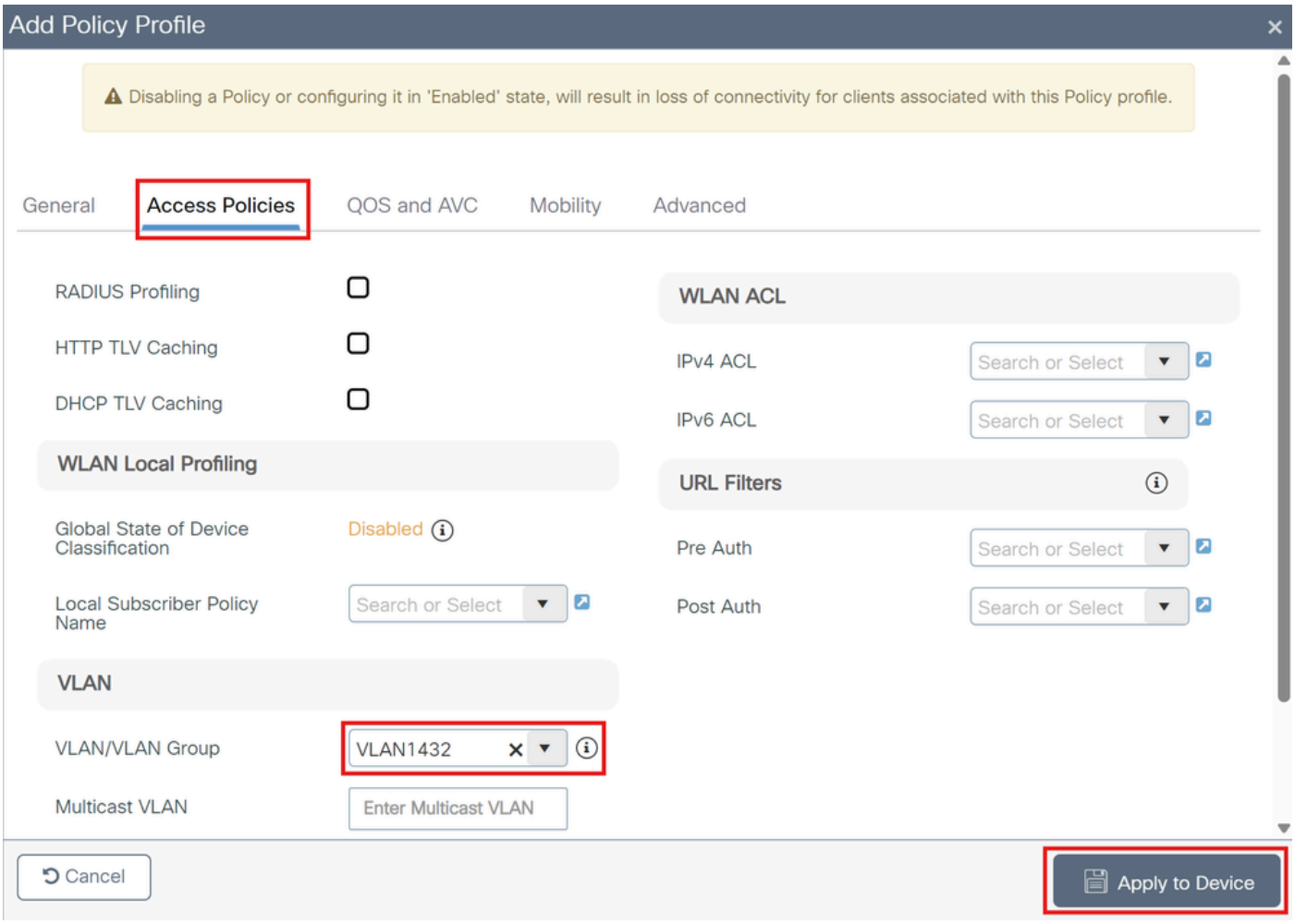
确保已启用配置文件。



创建新策略配置文件

第 2 步： 选择 VLAN。

导航至访问策略选项卡，然后从下拉列表中选择 VLAN 名称，或手动输入 VLAN-ID。



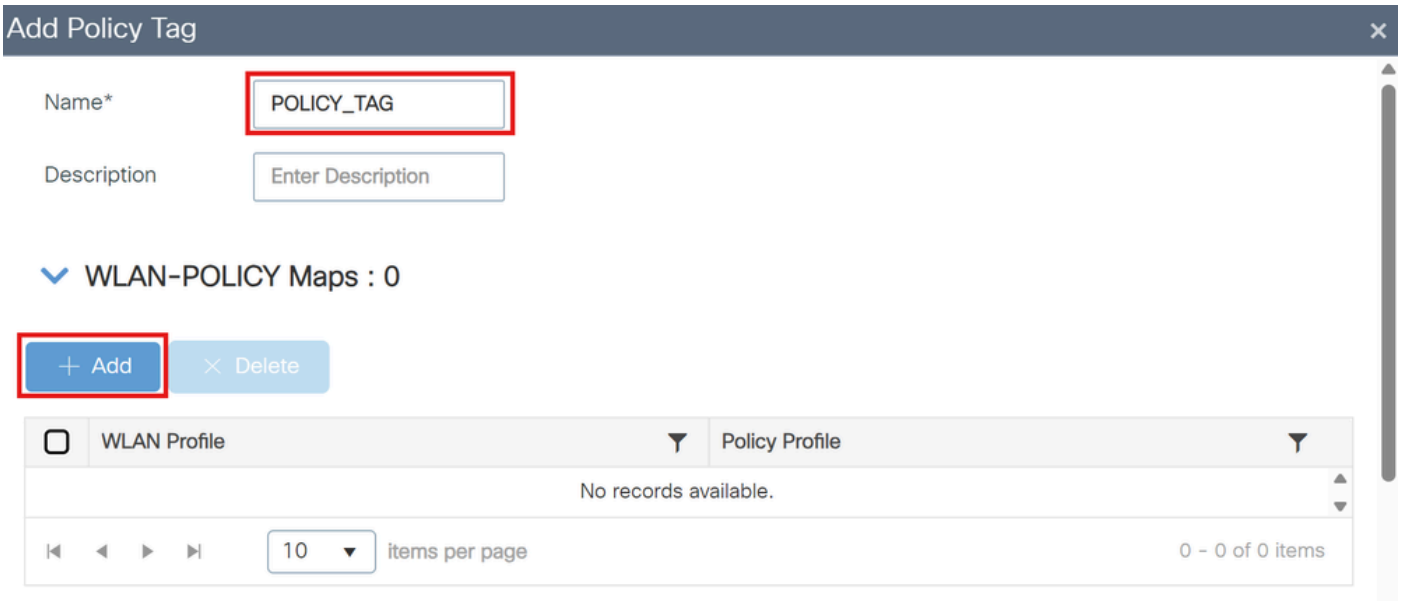
选择VLAN

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。

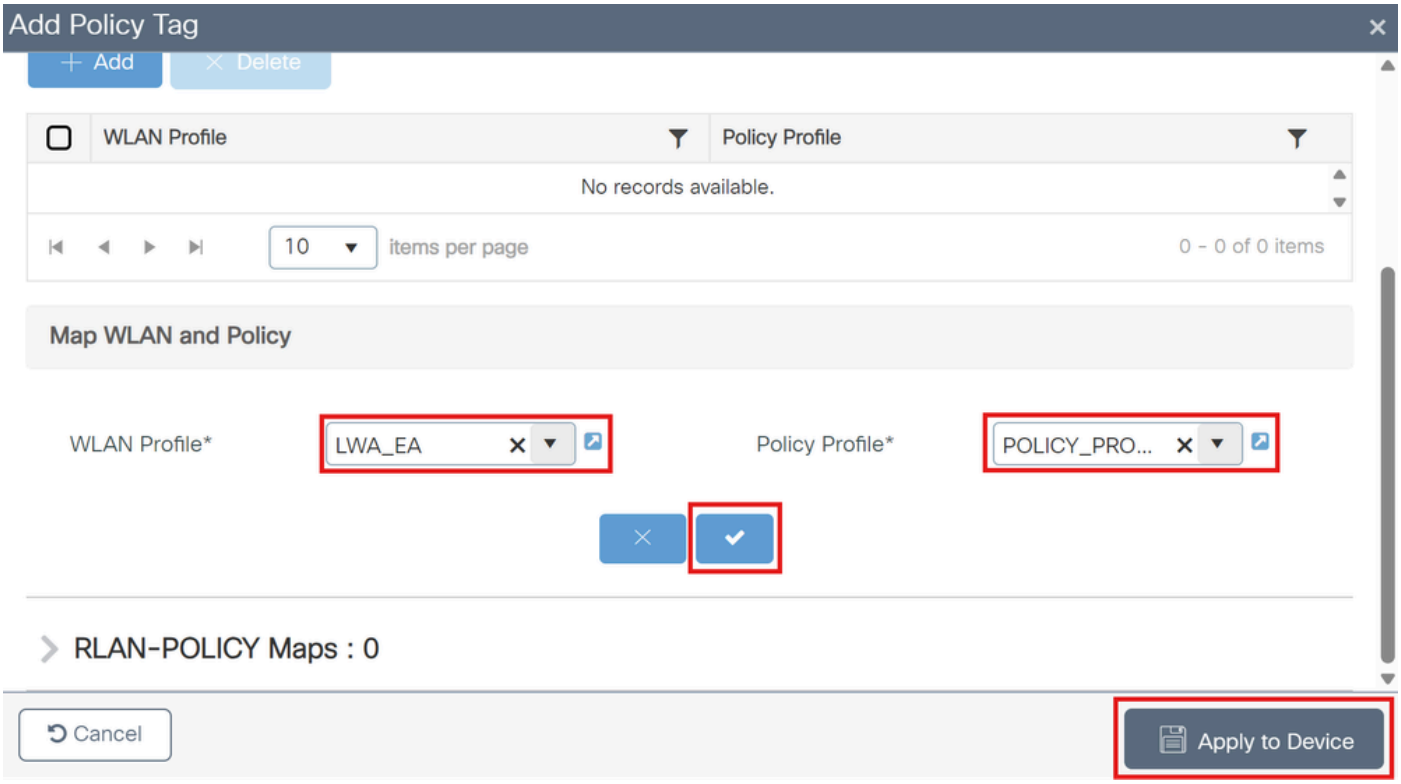
导航至配置 > 标签和配置文件 > 标签 > 策略，根据需要添加新的策略，如图所示。

选择+ Add:



策略标签配置

将您的WLAN配置文件链接到所需的策略配置文件：

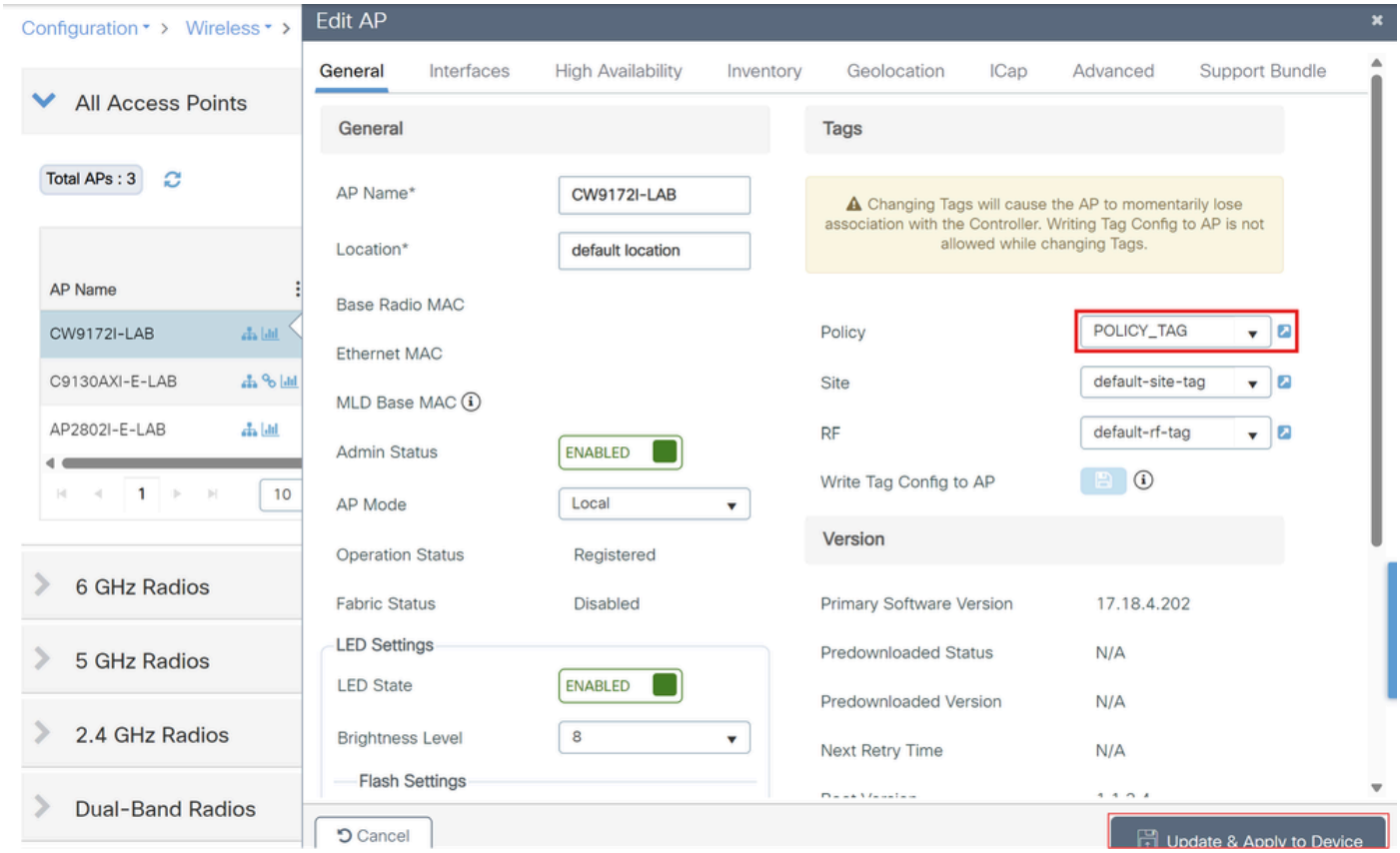


策略标签配置

策略标签分配

将策略标签分配给所需的 AP。

要将标签分配给一个 AP，请导航至配置 > 无线 > 无线接入点 > AP 名称 > 常规标签，按需进行分配，然后点击更新并应用于设备。

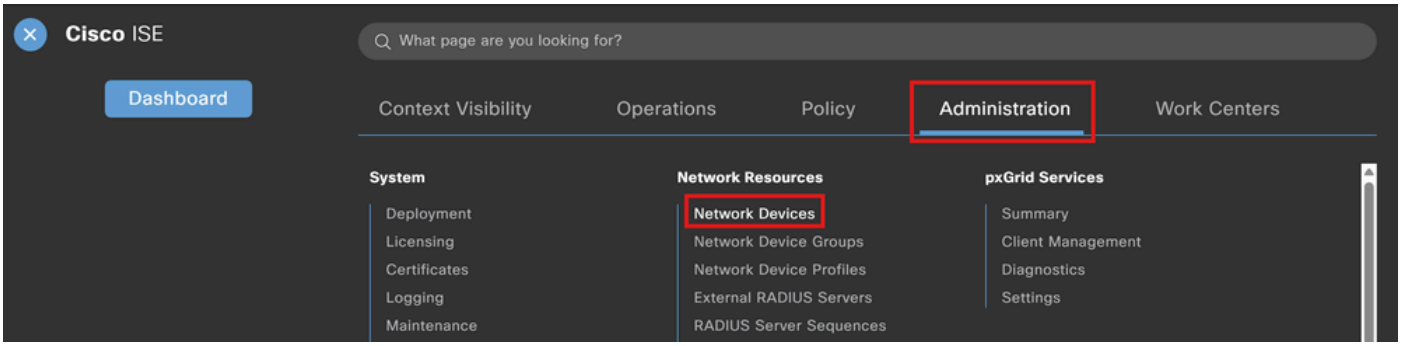


策略标签分配

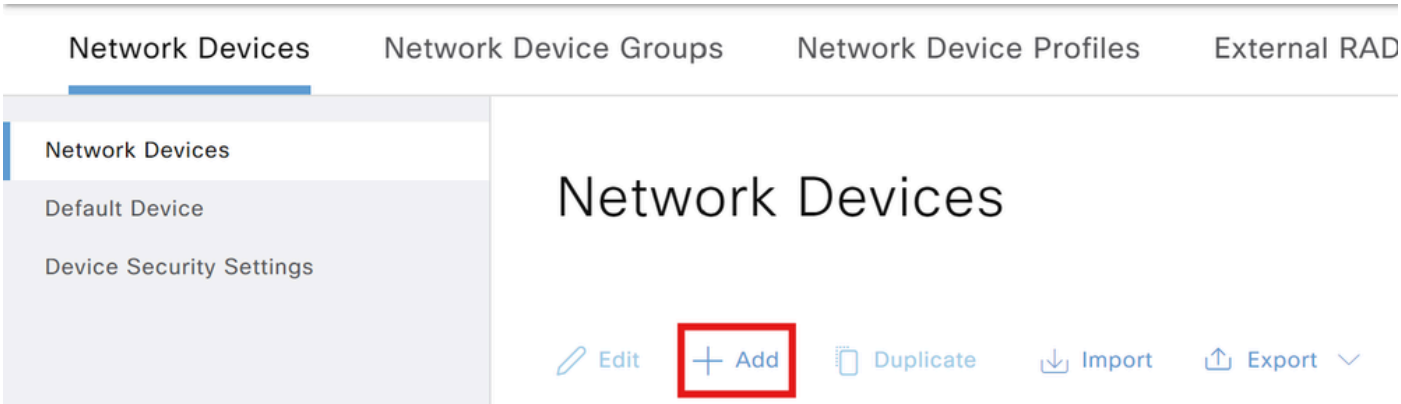
ISE 配置

将 9800 WLC 添加到 ISE

第 1 步： 导航至管理 > 网络资源 > 网络设备，如图所示。



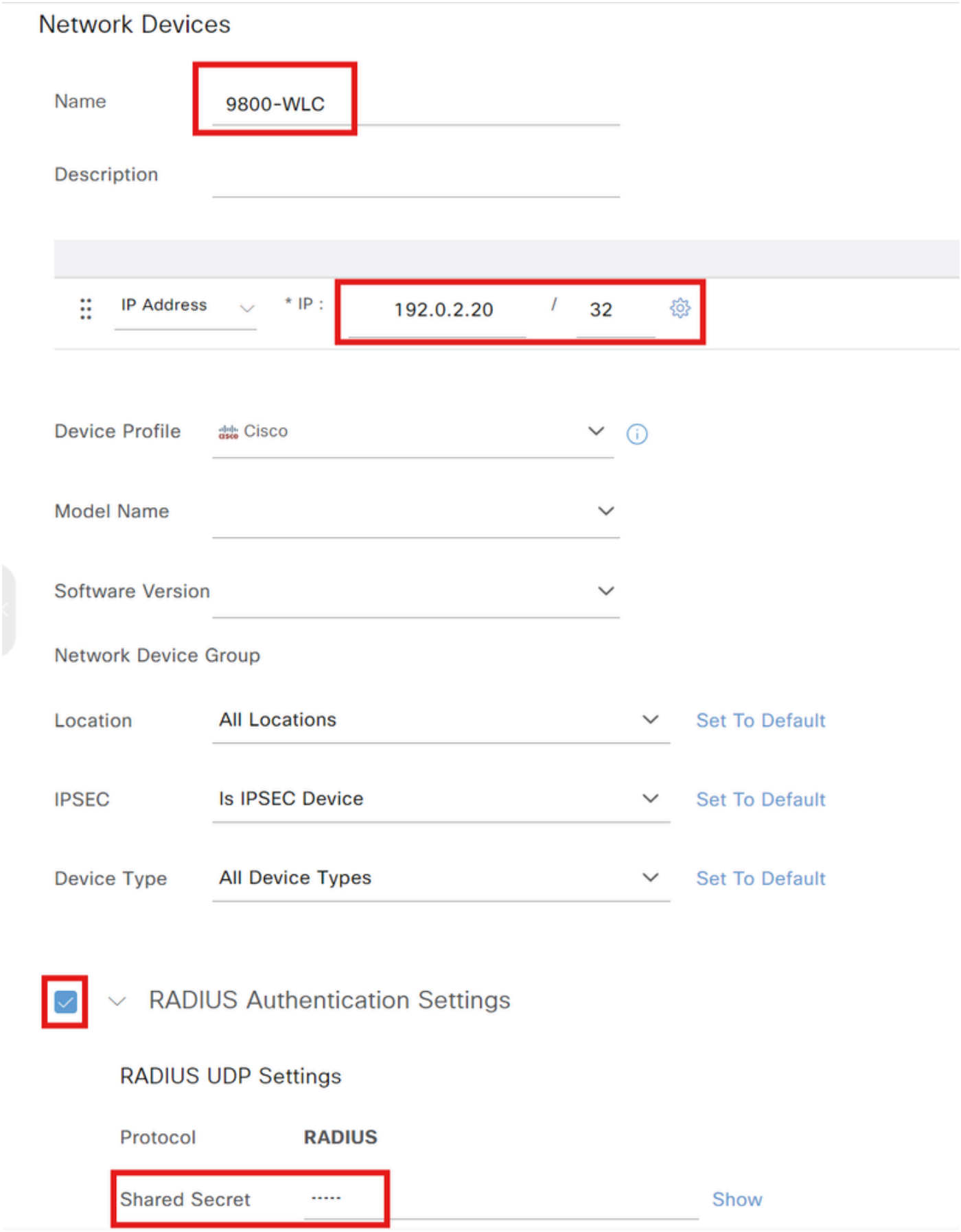
步骤2.单击+Add。



添加网络设备

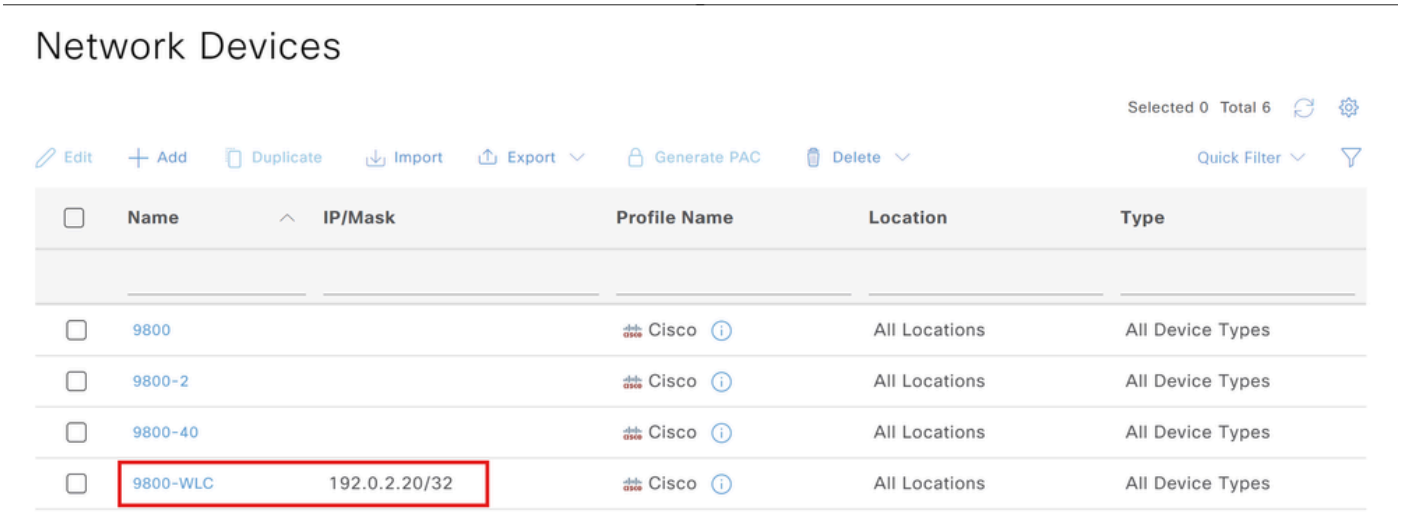
或者，您可以添加指定的型号名称、软件版本、说明，并根据设备类型、位置或 WLC 分配网络设备组。

步骤3.输入9800 WLC设置，如图所示。输入在WLC端创建服务器时定义的相同RADIUS密钥。然后请点击提交。



9800 WLC设置

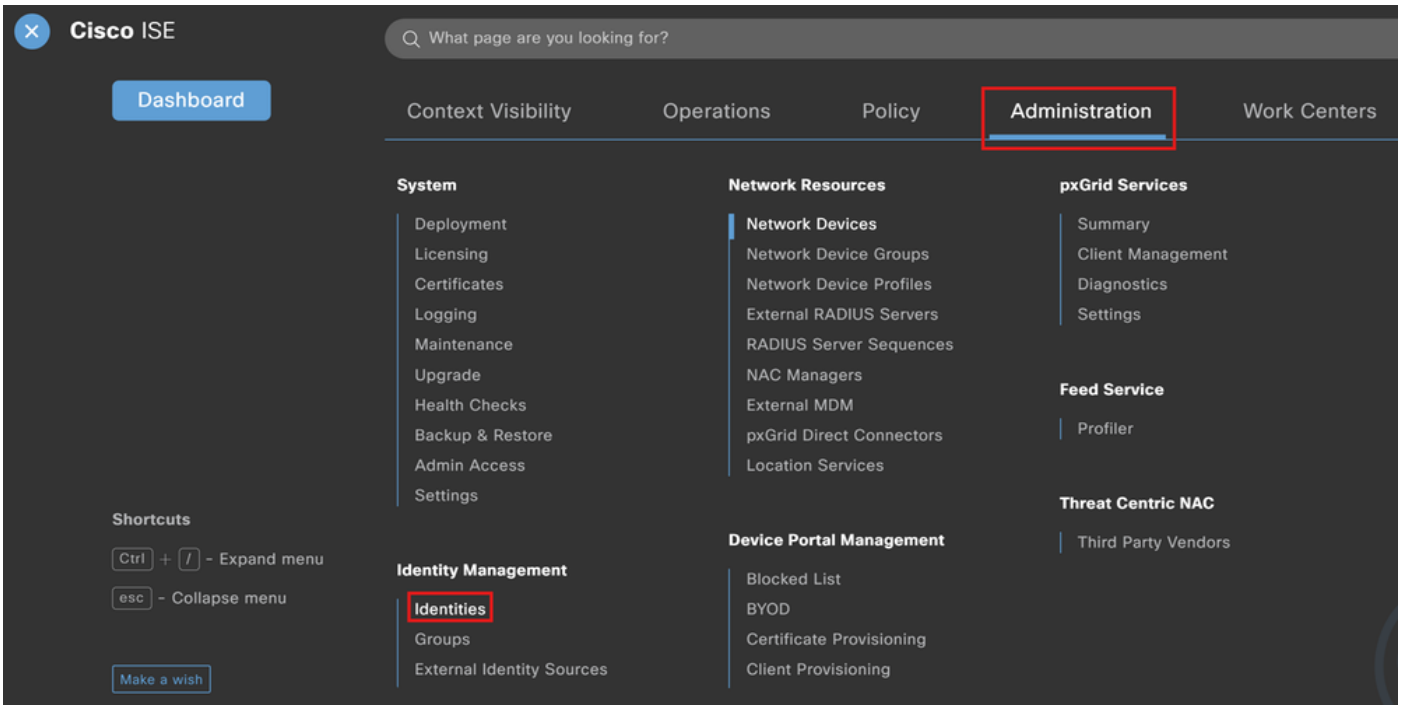
步骤4.导航到管理>网络资源>网络设备，您可以看到网络设备列表。



网络设备列表

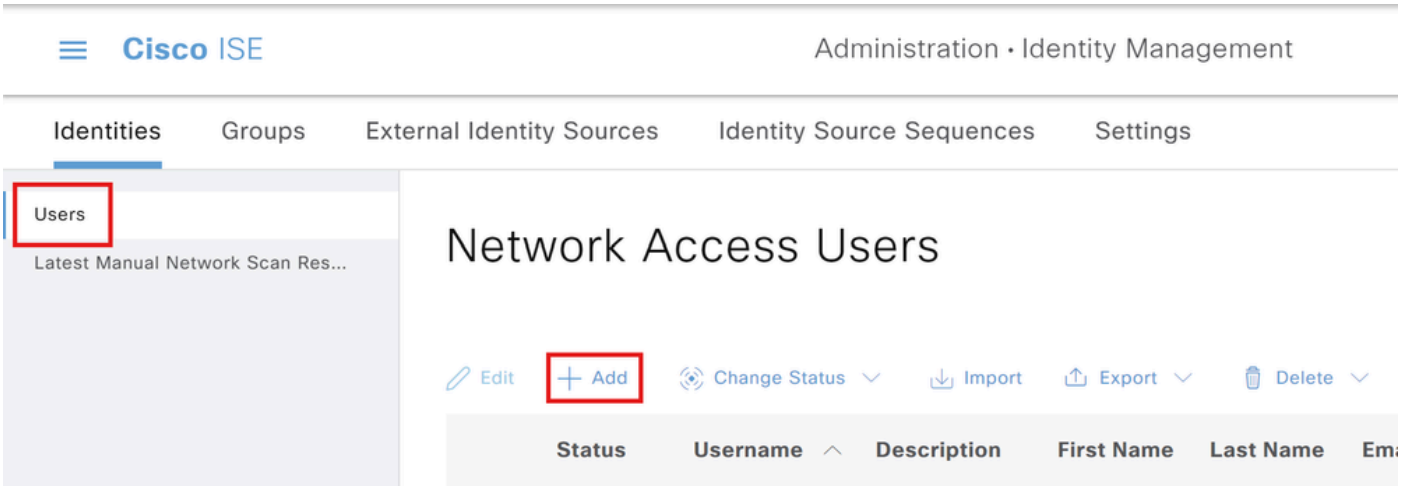
在 ISE 上创建新用户

步骤1.导航到管理>身份管理>身份：



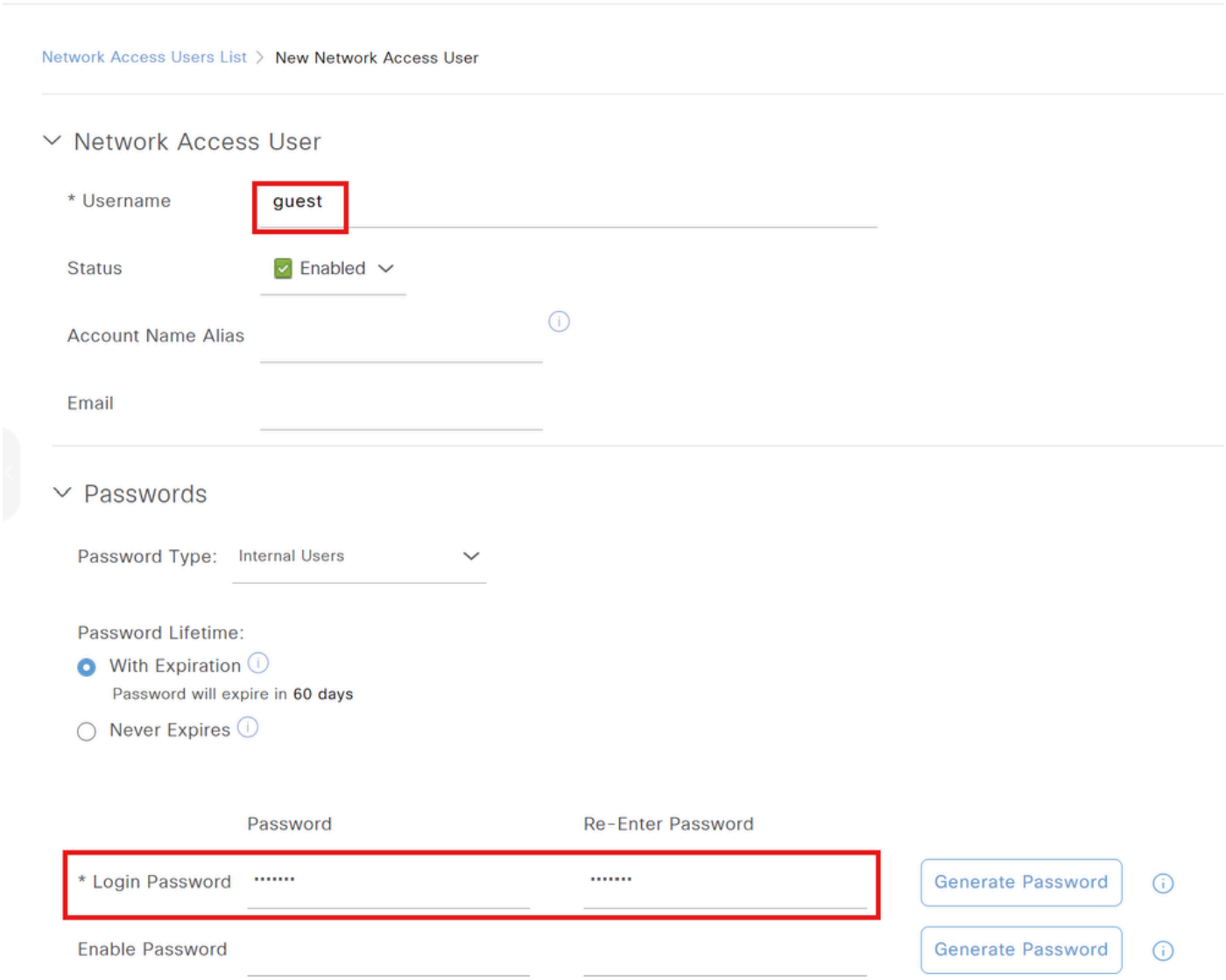
ISE管理 — 身份

步骤2.导航到用户，点击+添加。



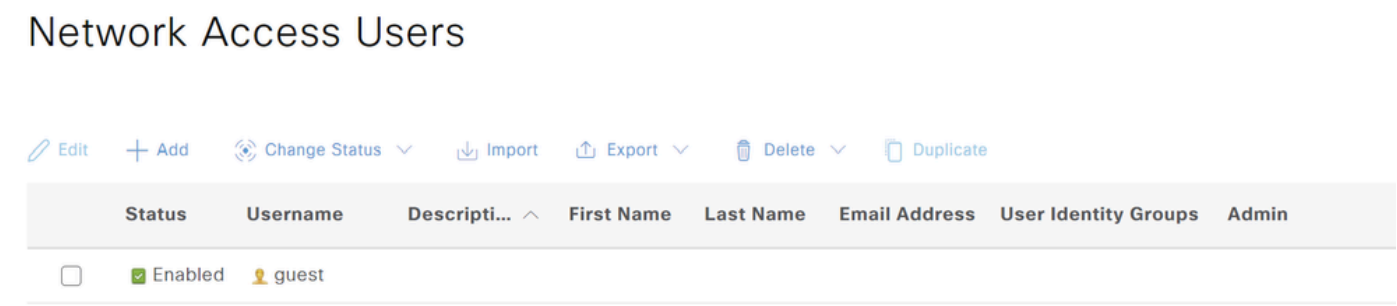
添加用户

步骤3.输入访客用户的用户名和密码，然后单击Submit。



在 ISE 上创建新用户

第4步：导航到管理>身份管理>身份>用户，您可以看到用户列表。



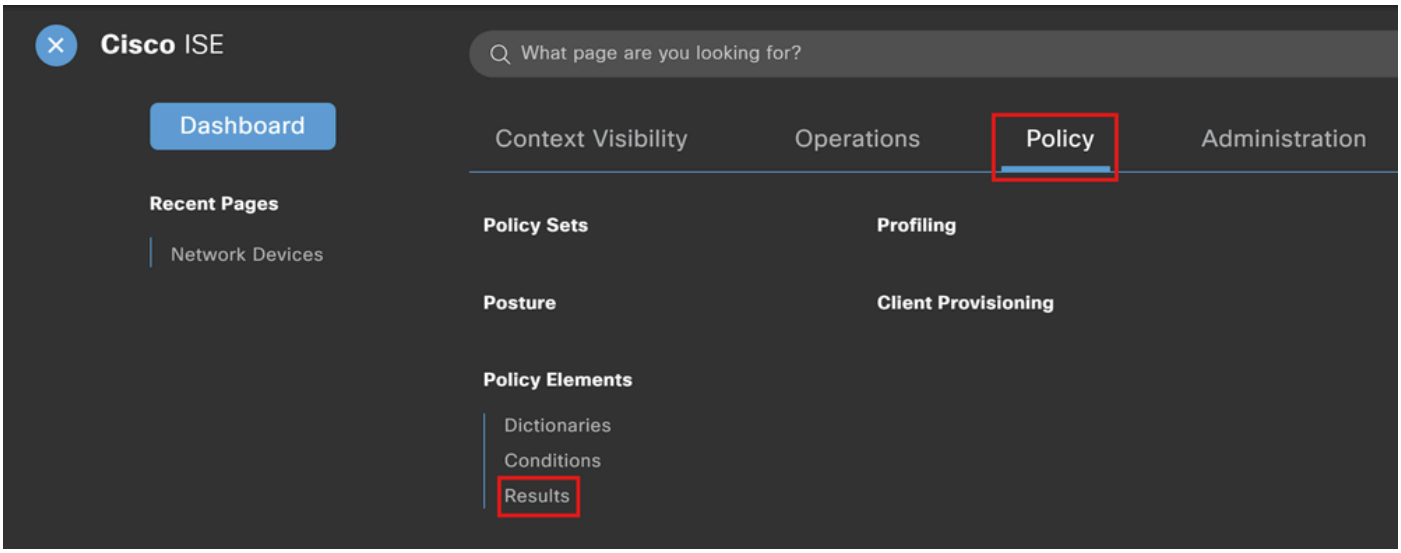
网络访问用户列表

创建授权配置文件

策略配置文件是根据客户端参数（如 MAC 地址、凭证、使用的 WLAN 等）向客户端分配的结果，可以分配特定设置，如虚拟局域网 (VLAN)、访问控制列表 (ACL)、统一资源定位符 (URL) 重定向等。

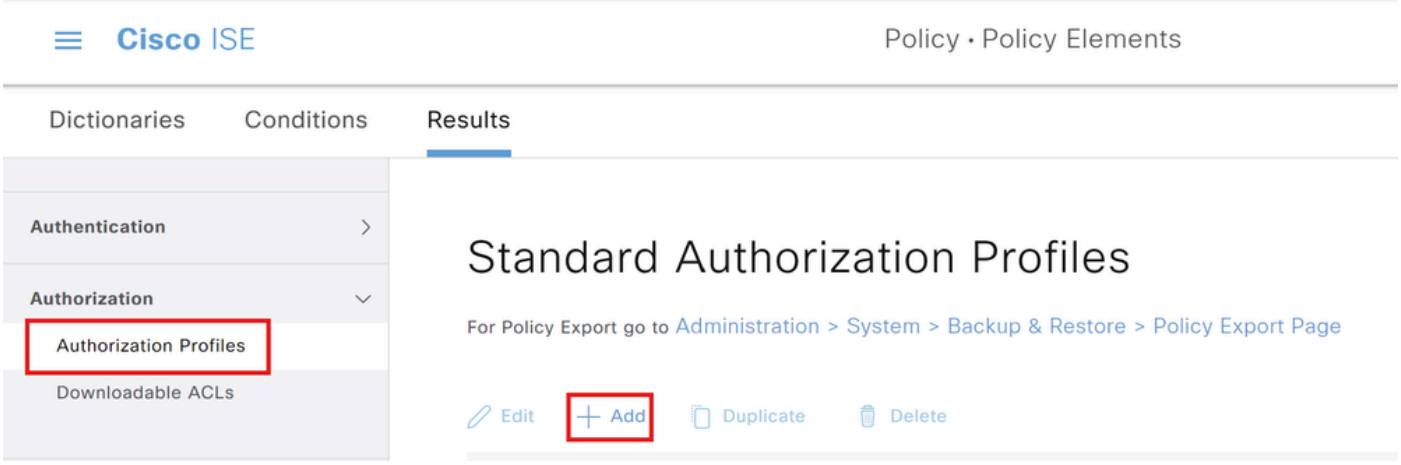
创建授权配置文件以将客户端重定向到身份验证门户的步骤如下。请注意，在最新版本的 ISE 中，已存在 Cisco_Webauth 授权结果。您可以对其进行编辑以修改重定向 ACL 名称，从而与 WLC 上配置的名称相一致。

步骤1.导航到策略>策略元素>结果。



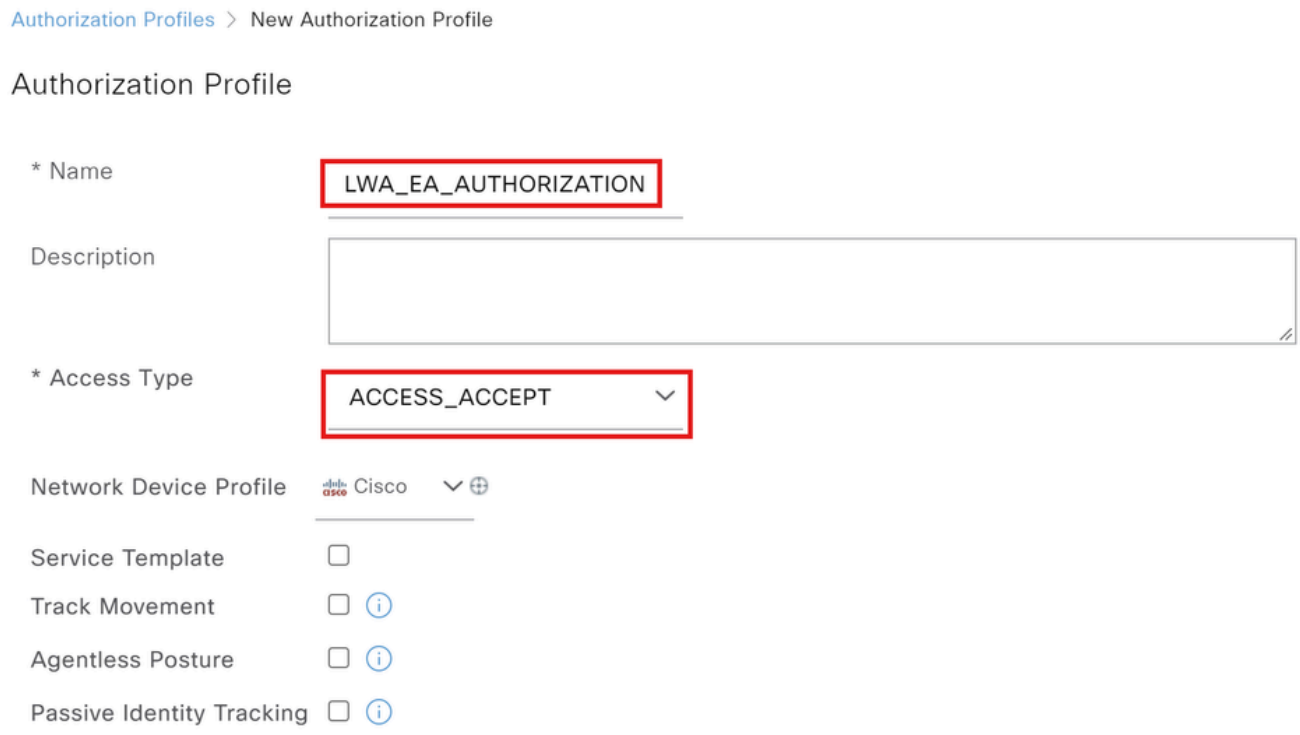
ISE策略 — 结果

步骤2.导航到Authorization > Authorization Profiles。单击+Add以创建授权配置文件。



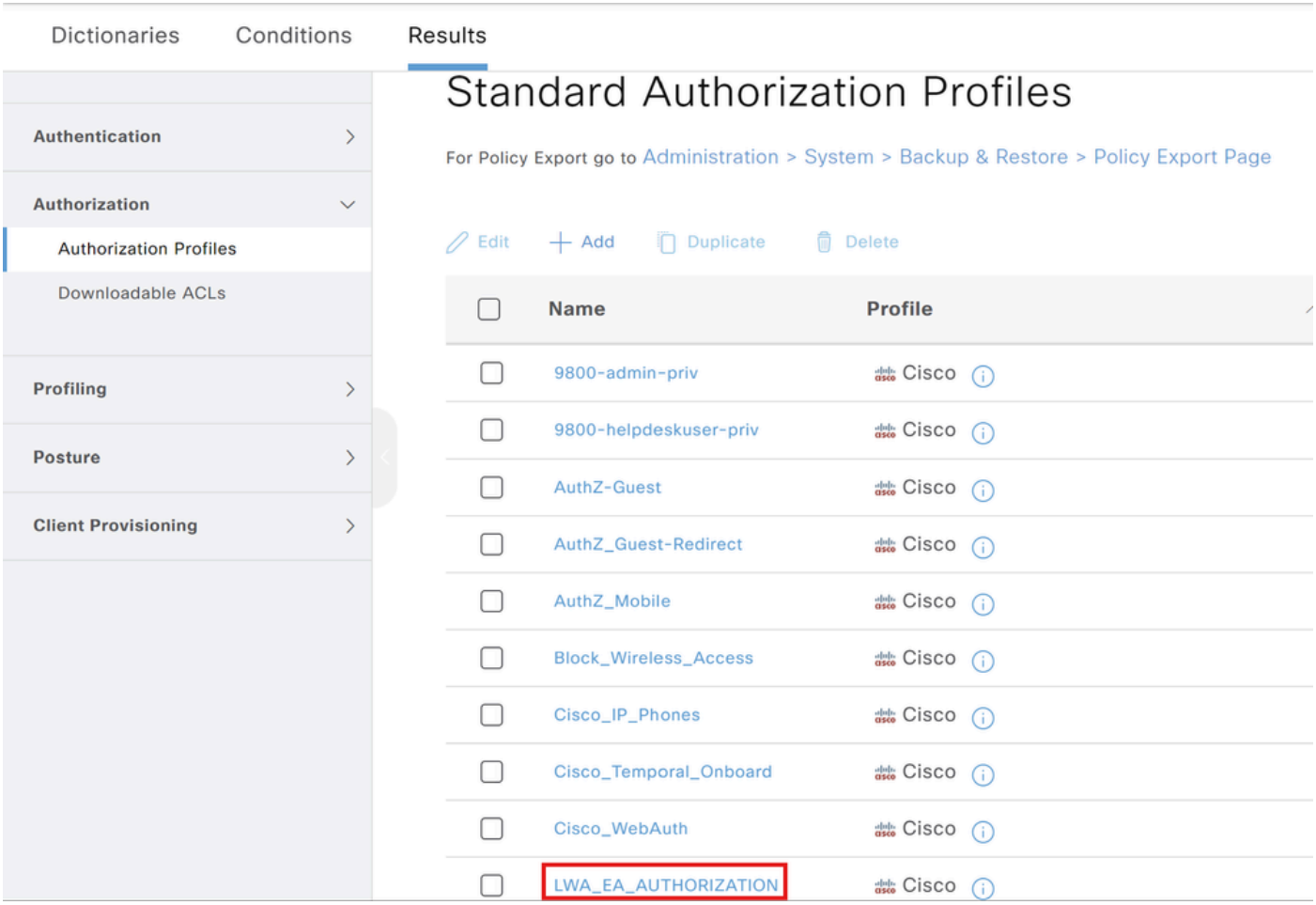
添加授权配置文件

步骤3.创建授权配置文件LWA_EA_AUTHORIZATION。属性详细信息必须为Access Type=ACCESS_ACCEPT。单击 submit。



创建授权配置文件

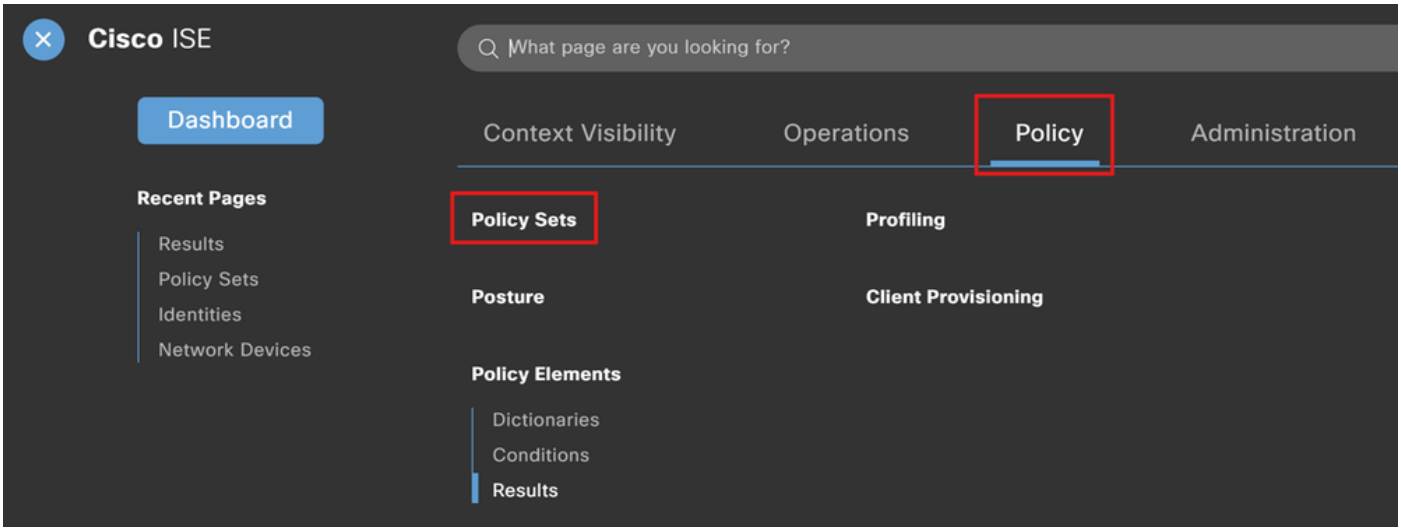
第4步：导航到策略>Policy元素>结果>授权>授权配置文件，您可以看到授权配置文件。



授权配置文件列表

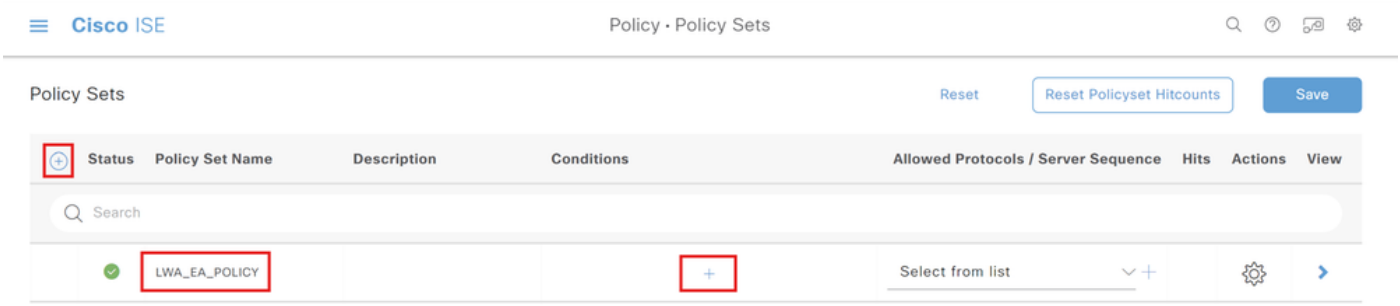
配置身份验证规则

第 1 步： 导航至策略 > 策略集。



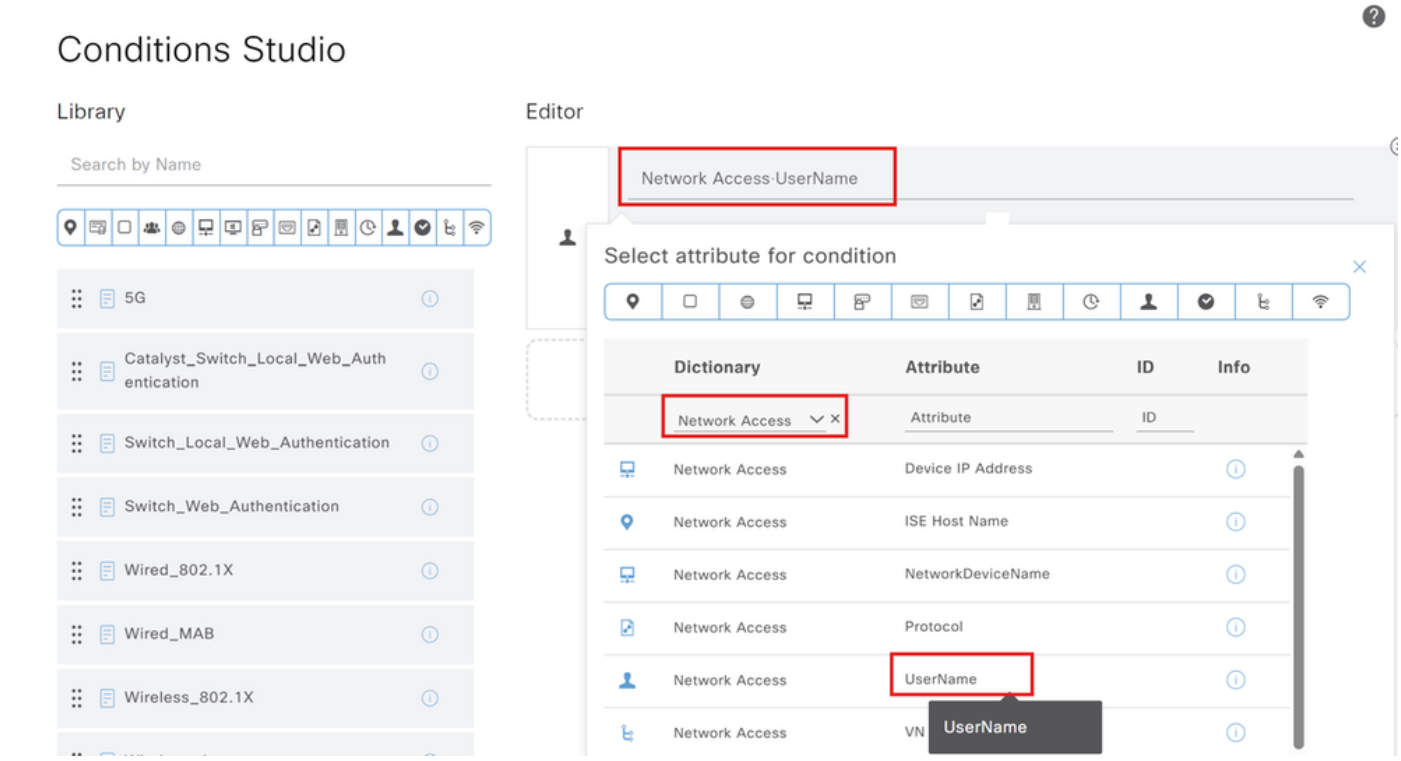
ISE策略 — 策略集

步骤2.选择+号，键入策略集LWA_EA_POLICY的名称。点击Conditions列。



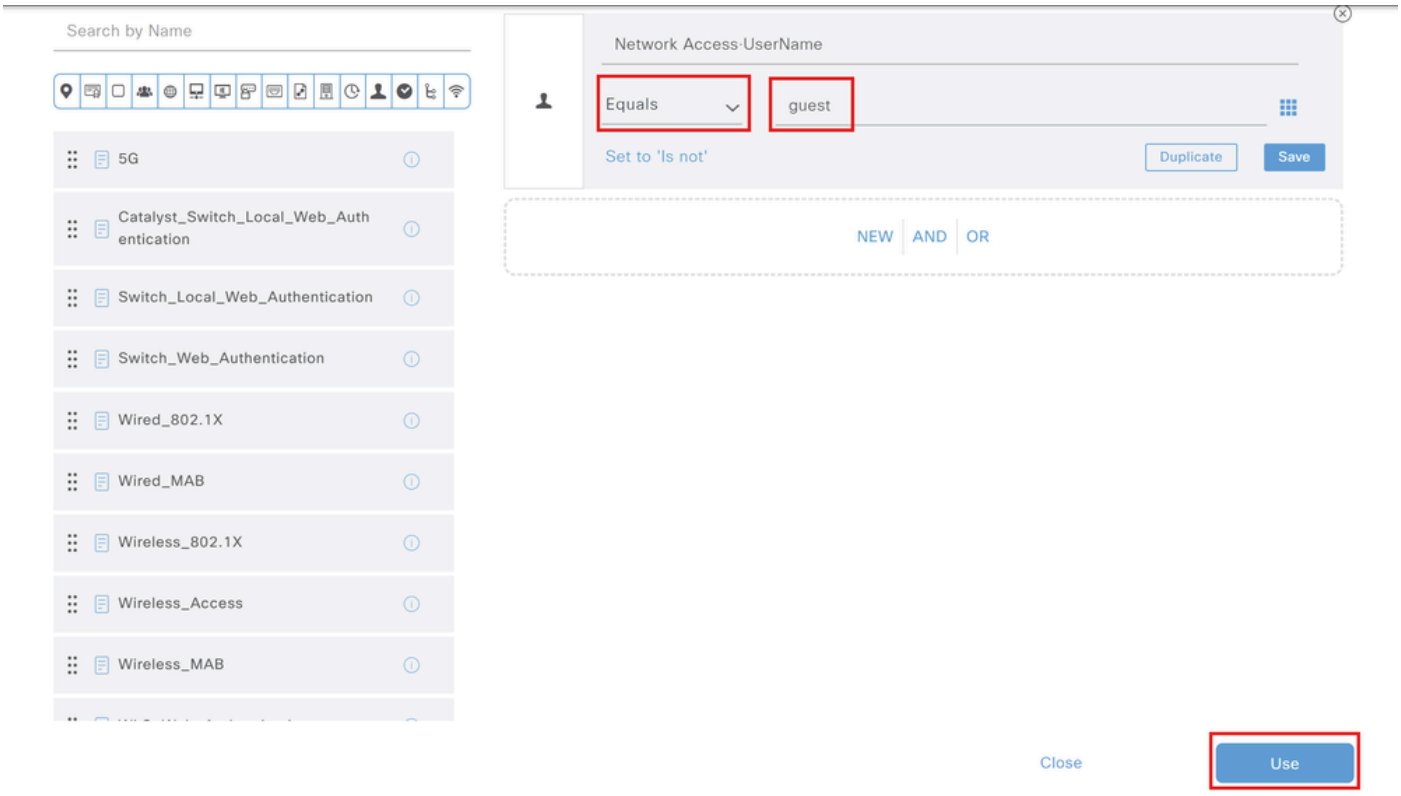
配置身份验证规则

步骤3.在字典上，选择网络访问。在属性上，选择用户名。



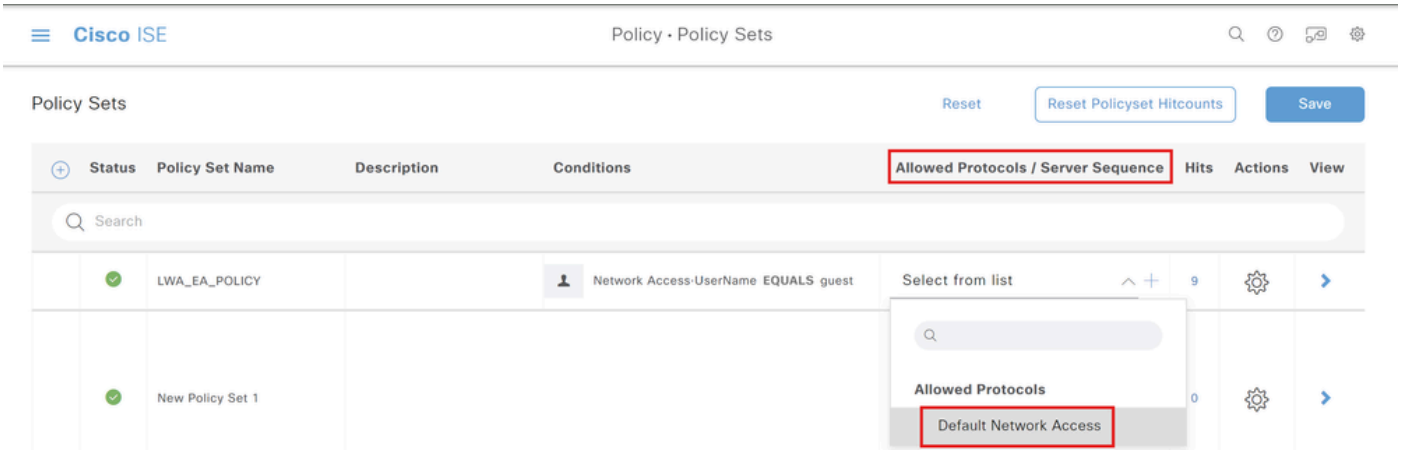
拨号网络访问

步骤4.设置Equals，然后在文本框中键入guest（在Administration > Identity Management > Identities > Users上定义的用户名）。单击Save以保存更改。



用户名访客

第 5 步： 导航至策略 > 策略集。在您创建的策略集上，在Allowed Protocols/Server Sequence列中，选择Default Network Access。



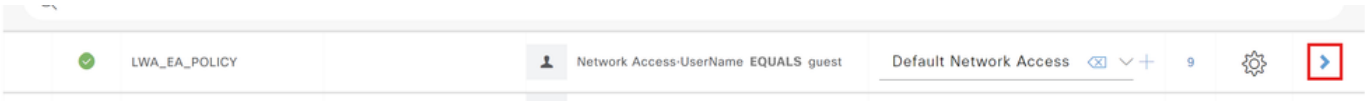
策略集

步骤6.单击Save以保存更改。

配置授权规则

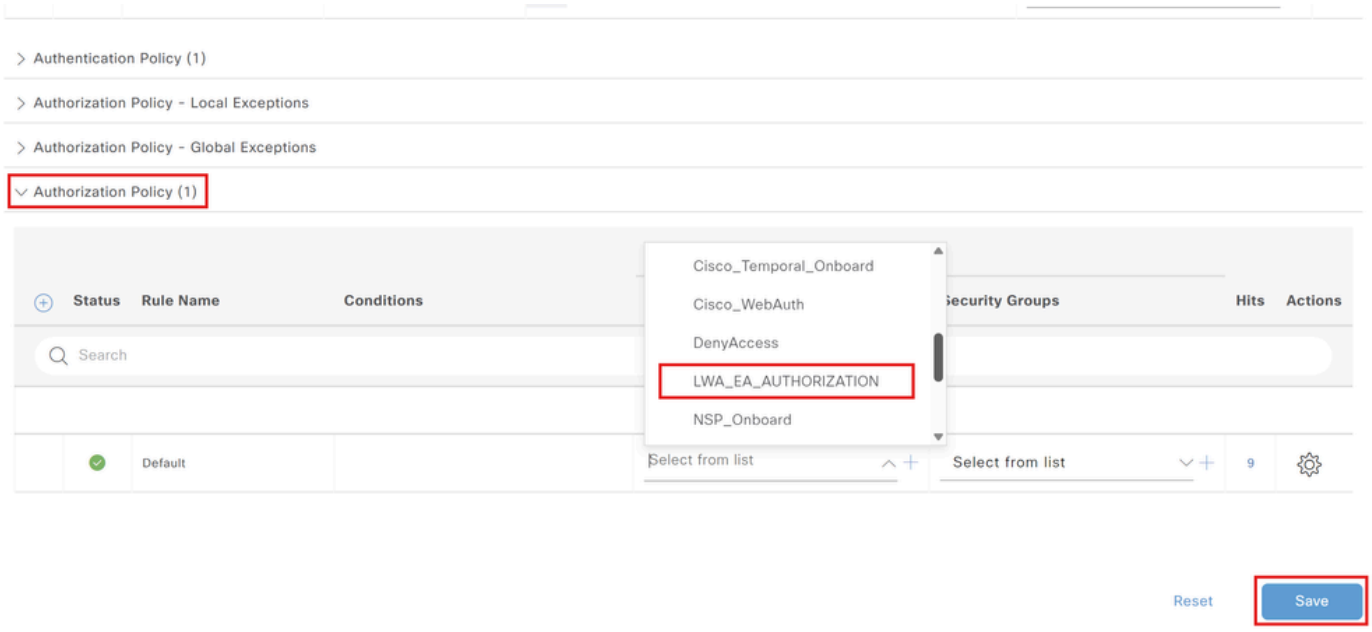
授权规则负责确定将哪些权限（哪个授权配置文件）结果应用于客户端。

第 1 步： 导航至策略 > 策略集。点击您创建的策略集上的箭头图标。



策略集箭头

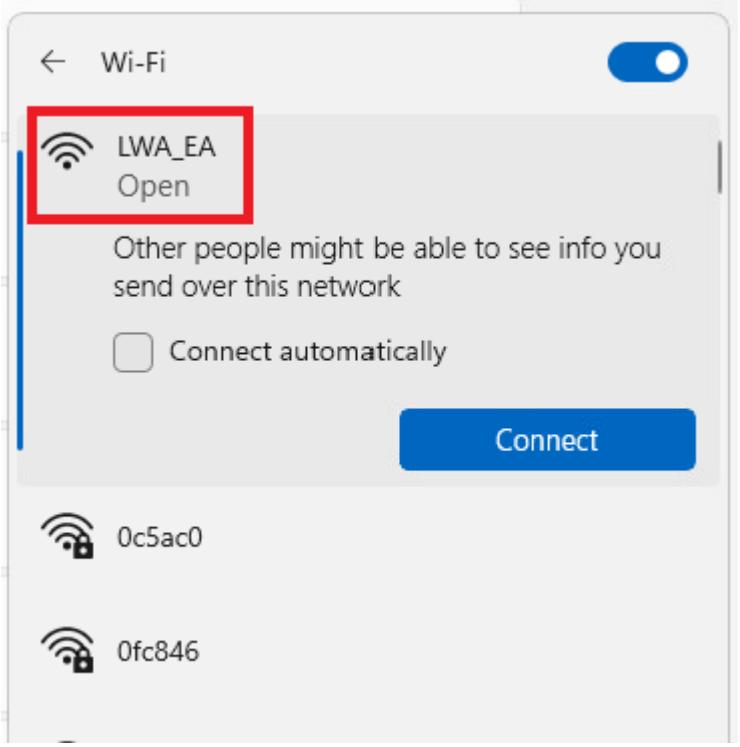
步骤2.在同一Policy set页面上，展开Authorization Policy，如图所示。在Profiles列中，删除DenyAccess并添加LWA_EA_AUTHORIZATION。单击Save以保存更改。



授权策略

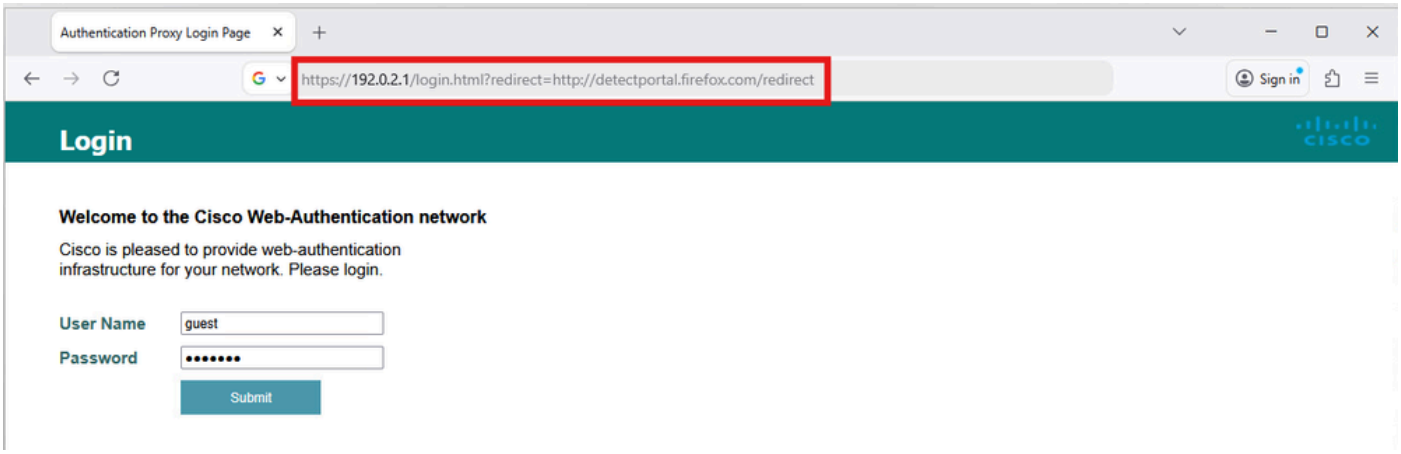
连接访客客户端

步骤1.在您的计算机/电话上导航到Wi-Fi网络，找到SSID LWA_EA并选择连接。



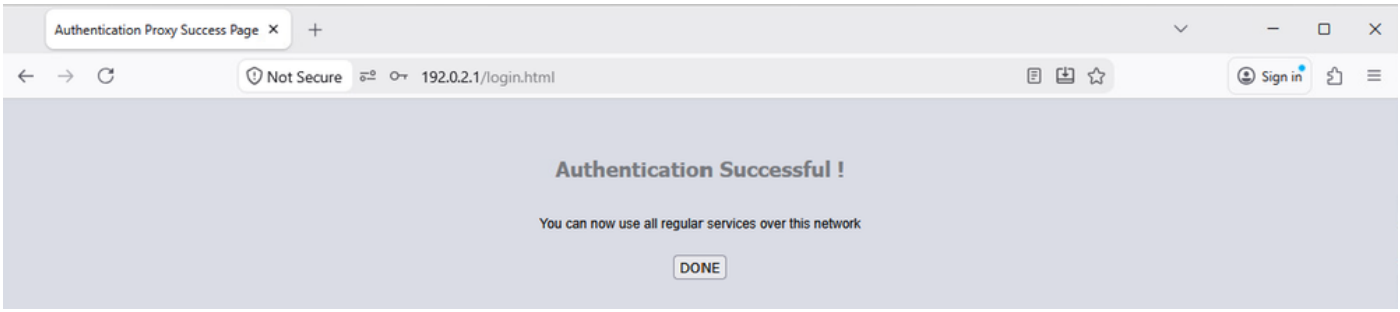
连接访客客户端

步骤2.弹出一个浏览器窗口，其中显示登录页面。重定向URL位于URL框中，您必须键入Username和Password才能访问网络。然后选择Submit。



具有重定向URL的登录页

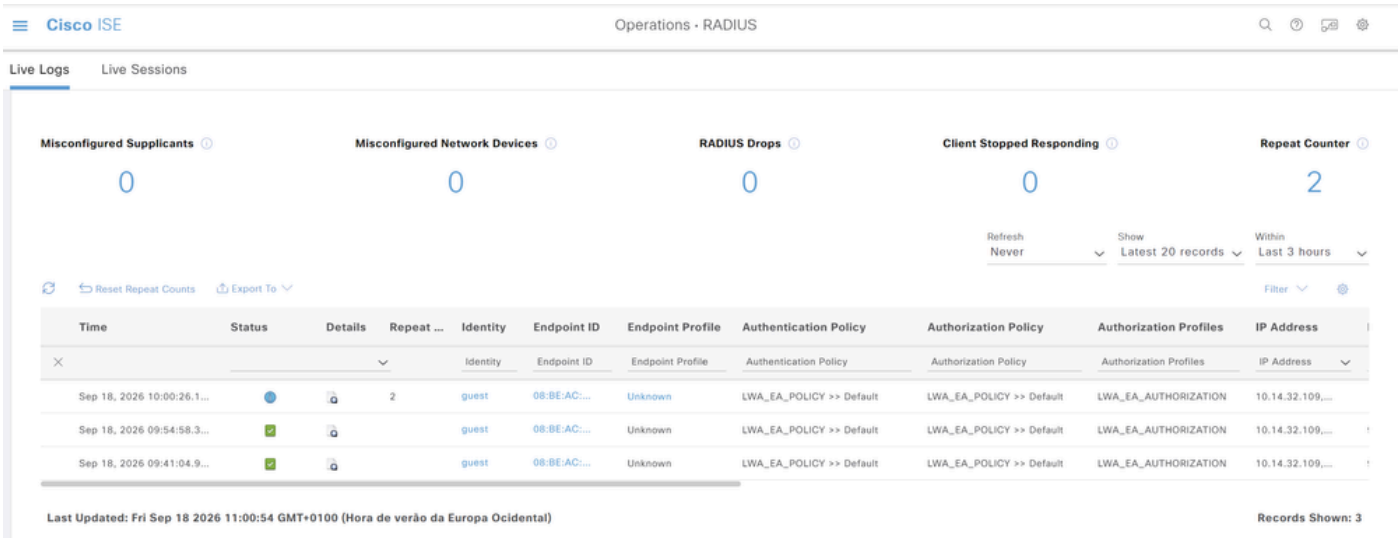
如果凭证正确，系统将显示身份验证成功页面：



“身份验证成功登录”页

注意：提供的URL由WLC提供。它包含WLC虚拟IP和Windows连接测试URL的重定向。

步骤3.导航到操作> RADIUS >实时日志。您可以看到经过身份验证的客户端设备及其身份验证和授权策略。



Radius实时日志

验证

使用本部分可确认配置能否正常运行。

Show WLAN Summary

<#root>

9800WLC#show wlan summary

```
Number of WLANs: 1
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----------------------------------------------
```

1 LWA_EA LWA_EA UP [open],[Web Auth]

9800WLC#

show wlan name LWA_EA

WLAN Profile Name : LWA_EA
==========
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security

Web Based Authentication : Enabled

OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

(...)
Security-2.4GHz/5GHz

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OSEN : Disabled
PMF Support : Disabled

```
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)
```

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

<#root>

9800WLC#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN
```

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)
```

9800WLC#show aaa method-lists authorization

```
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
```

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)
```

9800WLC#show aaa servers

RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS

```
State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (0) : current UP
(...)
```

故障排除

常见问题

以下是有关如何排除Web身份验证问题的几个指南，例如：

- 用户无法进行身份验证。
- 证书问题。
- 重定向URL不起作用。
- 访客用户无法连接到访客WLAN。
- 用户无法获取IP地址。
- 重定向到“Web身份验证登录页面”失败。
- 身份验证成功后，访客用户无法访问互联网。

以下指南详细介绍故障排除步骤：

- 排除Web身份验证的常见问题
- 需要排除的其他情况

条件调试和无线主动跟踪及嵌入式数据包捕获

您可以启用条件调试并捕获无线活动(RA)跟踪，该跟踪为与指定条件（本例中为客户端MAC地址）交互的所有进程提供调试级别跟踪。 要启用条件调试，请使用指南中的步骤Conditional Debug和RadioActive trace。

您还可以收集嵌入式数据包捕获(EPC)。EPC是一种数据包捕获工具，允许查看发往、来自和通过Catalyst 9800 WLC的数据包，即LWA中的DHCP、DNS、HTTP GET数据包。可以使用 Wireshark 导出这些捕获以进行离线分析。有关如何执行此操作的详细步骤，请参阅嵌入式数据包捕获。

成功尝试的示例

这是RA_trace的输出，表示在与RADIUS服务器连接的访客SSID时，尝试在关联/身份验证过程中成功识别每个阶段。

802.11关联/身份验证：

[client-orch-sm] [17062]: (注) : MAC :08be.ac3f收到关联。BSSID cc70.edcf.552f，WLAN LWA_EA，插槽1 AP 2ce3.8eb4,CW9172I-LAB
[client-orch-sm] [17062]: (调试) : MAC :08be.ac3f已收到Dot11关联请求。处理已启动，SSID:LWA_EA，策略配置文件：POLICY_PROFILE、AP名称：CW9172I-LAB，Ap Mac地址：2ce3.8eb4BSSID MAC0000.0000.0000wlan ID:1RSSI:-49,SNR:46
[客户端工作状态] [17062]: (注) : MAC :08be.ac3f客户端状态转换：S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (信息) MAC :08be.ac3f Dot11 ie验证扩展/支持速率。支持费率验证通过 radio_type 2
[dot11-validate] [17062]: (信息) MAC :08be.ac3f WiFi直接连接：Dot11验证P2P IE。P2P IE不存在。
[dot11] [17062]: (调试) : MAC :08be.ac3f dot11发送关联响应。使用resp_status_code建立关联响应：0
[dot11] [17062]: (调试) : MAC :08be.ac3f Dot11功能信息byte1 1,byte2:11
[dot11-frame] [17062]: (信息) MAC :08be.ac3f WiFi直接连接：使用P2P IE跳过构建关联响应：Wifi直接策略已禁用
[dot11] [17062]: (信息) MAC :08be.ac3f dot11发送关联响应。正在发送相关响应，响应长度为：130，带resp_status_code:0,DOT11_STATUS:DOT11_STATUS_SUCCESS
[dot11] [17062]: (注) : MAC :08be.ac3f关联成功。AID 1，漫游=假，WGB =假，11r =假，11w =假快速漫游=假
[dot11] [17062]: (信息) MAC :08be.ac3f DOT11状态转换：S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (调试) : MAC :08be.ac3f站Dot11关联成功。

IP学习过程：

[客户端工作状态] [17062]: (注) : MAC :08be.ac3f客户端状态转换：S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (信息) MAC :08be.ac3f IP-learn状态转换：S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (信息) MAC :08be.ac3f客户端身份验证接口状态转换：S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: (注) : MAC :08be.ac3f客户端IP学习成功。方法：DHCP IP:10.14.32.109
[client-iplearn] [17062]: (信息) MAC :08be.ac3f IP-learn状态转换：S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (调试) : MAC :08be.ac3f已收到ip learn响应。方法：IPLEARN_METHOD_DHCP

第3层身份验证：

[client-orch-sm] [17062]: (调试) : MAC :08be.ac3f触发L3身份验证。状态= 0x0，成功
[客户端工作状态] [17062]: (注) : MAC :08be.ac3f客户端状态转换：S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (注) : MAC :08be.ac3f L3身份验证已启动。LWA
[client-auth] [17062]: (信息) MAC :08be.ac3f客户端身份验证接口状态转换：S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]GET rcvd when in LOGIN state
[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET请求
[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]解析GET，src [10.14.32.109] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]阅读完成：parse_request返回8
[webauth-io] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO状态读取 — >写入
[webauth-io] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO状态写入 — >读

取
[webauth-io] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO状态新 — >读取
[webauth-io] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56539/218读取事件，消息就绪
[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd when in LOGIN state

第3层身份验证成功，将客户端移至RUN状态：

[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004]接收客户端08be.ac3f的用户名访客
[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004] auth mgr attr add/change notification is received for attr auth-domain(954)
[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004]方法webauth将状态从“Running”更改为“Authc Success”
[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004]上下文状态从“正在运行”更改为“授权成功”
[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004] auth mgr attr add/change notification is received for attr method(757)
[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004]引发的事件AUTHZ_SUCCESS(11)
[auth-mgr] [17062]: (信息) [08be.ac3f:capwap_90000004]上下文状态从“Authc Success”更改为“Authz Success”
[webauth-acl] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]通过SVM应用IPv4注销ACL，名称：IP-Adm-V4-LOGOUT-ACL，优先级：51,IIF-ID:0
[webauth-sess] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]使用的参数映射：全局
[webauth-state] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]使用的参数映射：全局
[webauth-state] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]状态AUTHC_SUCCESS -> AUTHZ
[webauth-page] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]发送Webauth成功页
[webauth-io] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO状态身份验证 — >写入
[webauth-io] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO状态写入 — > END
[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.14.32.109]56539/218删除IO交换机和关闭套接字，id [99000029]
[client-auth] [17062]: (注) : MAC :08be.ac3f L3身份验证成功。ACL:[]
[client-auth] [17062]: (信息) MAC :08be.ac3f客户端身份验证接口状态转换
: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062]: (信息) capwap_90000004[08be.ac3f][10.48.39.243]56538/219删除IO时钟并关闭套接字，id [D7000028]
[errmsg] [17062]: (信息) %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:R0/0:wncd:使用MAC的设备的ssid(LWA_EA)加入的用户名条目 (访客) : 08be.ac3f
[aaa-attr-inf] [17062]: (信息) [Applied attribute :bsn-vlan-interface-name 0 "VLAN0039"]
[aaa-attr-inf] [17062]: (信息) [应用的属性：timeout 0 1800(0x708)]
[aaa-attr-inf] [17062]: (信息) [应用的属性：url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (信息) MAC :08be.ac3f客户端QoS运行状态处理程序
[rog-proxy-capwap] [17062]: (调试) : 托管客户端运行状态通知：08be.ac3f
[客户端工作状态] [17062]: (注) : MAC :08be.ac3f客户端状态转换：S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

相关信息

- 思科技术支持和下载

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）。