在SD-Access上配置集中式Web身份验证

目录

简介

本文档介绍配置中央Web身份验证(CWA)的逐步指南，并概述所有组件的验证过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Catalyst中心
- 思科身份服务引擎(ISE)
- Catalyst 9800无线控制器架构
- 验证、授权和记帐 (AAA)

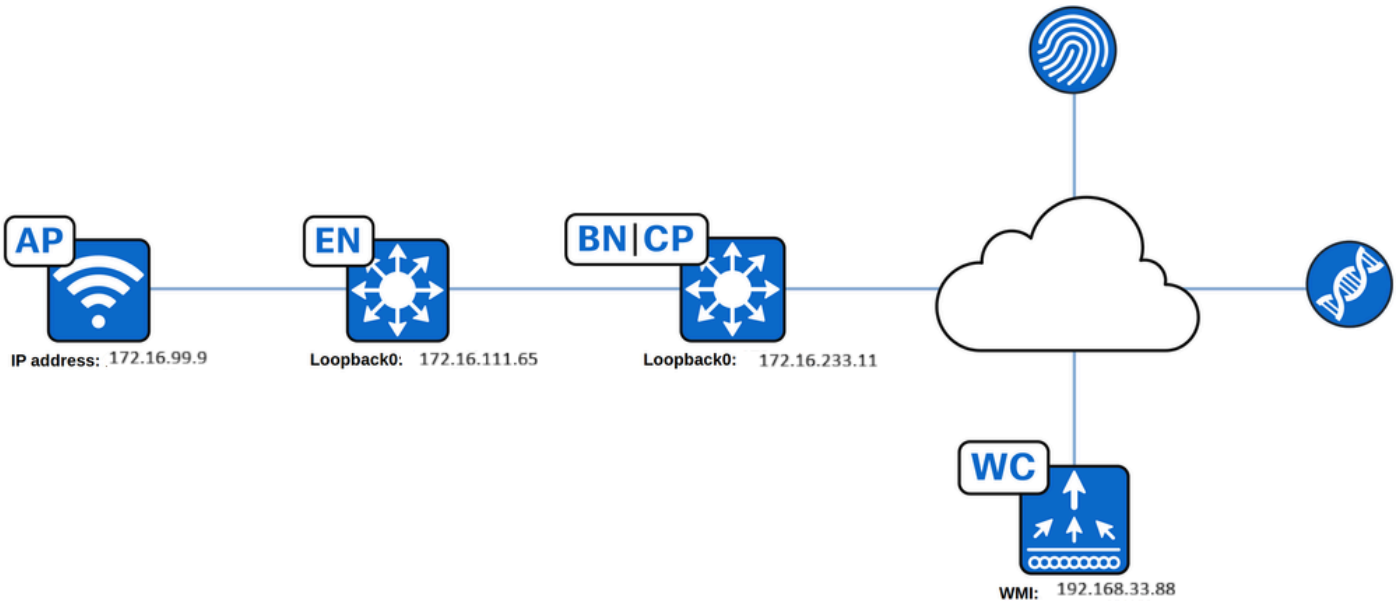
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科无线局域网控制器(WLC)- C9800-CL、Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - 2.3.7.7版
- 思科身份服务引擎(ISE)- 3.0.0.458版
- SDA边缘节点 — C9300-48P、Cisco IOS® XE 17.12.05
- SDA边界节点/控制平面 — C9500-48P、Cisco IOS® XE17.12.05
- 思科接入点 — C9130AXI-A，版本17.9.5.47

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。

拓扑



概述

中心网络身份验证(CWA)使用访客类型SSID将用户的Web浏览器重定向到由思科ISE托管的强制网络门户，使用配置的重定向ACL。强制网络门户允许用户注册和身份验证，在身份验证成功后，无线LAN控制器(WLC)应用适当的授权以授予完整网络访问权限。本指南提供使用Cisco Catalyst Center配置CWA的分步说明。

在Cisco Catalyst Center上配置CWA

创建网络配置文件

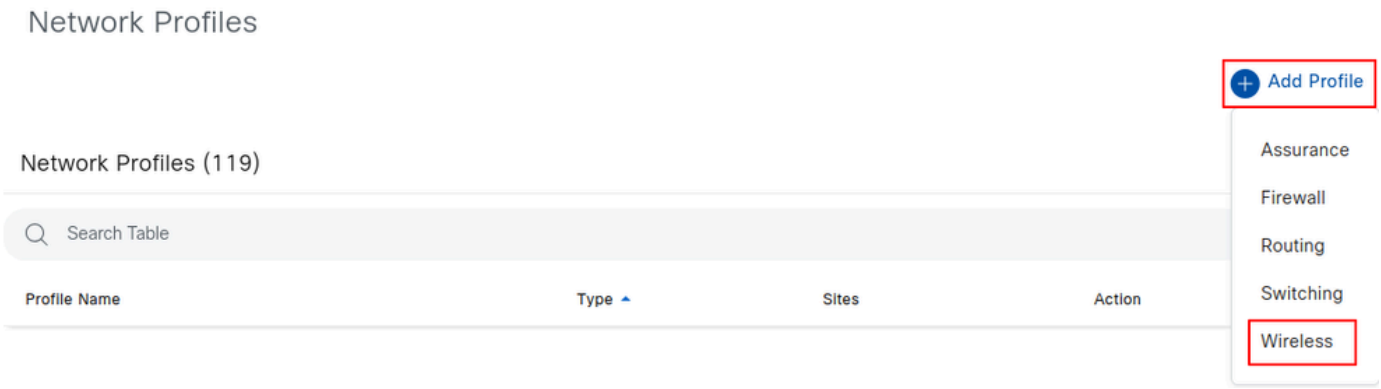
网络配置文件允许配置可应用于特定站点的设置。可以为Cisco Catalyst Center中的各种元素创建网络配置文件，包括：

- 保证
- 防火墙
- 路由
- 交换
- 遥测设备

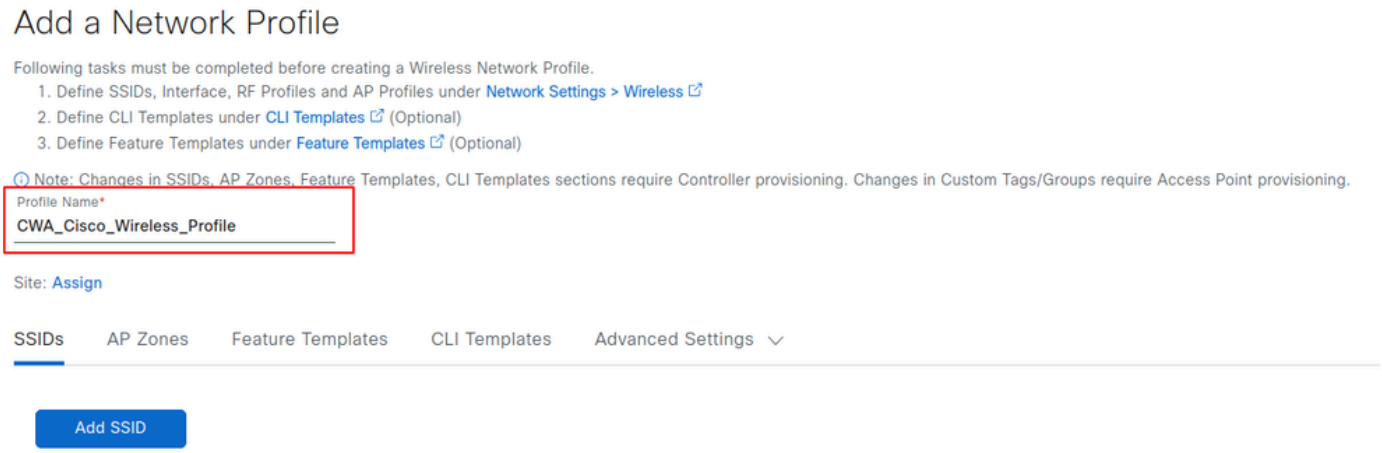
- 无线

对于CWA，必须配置无线配置文件。

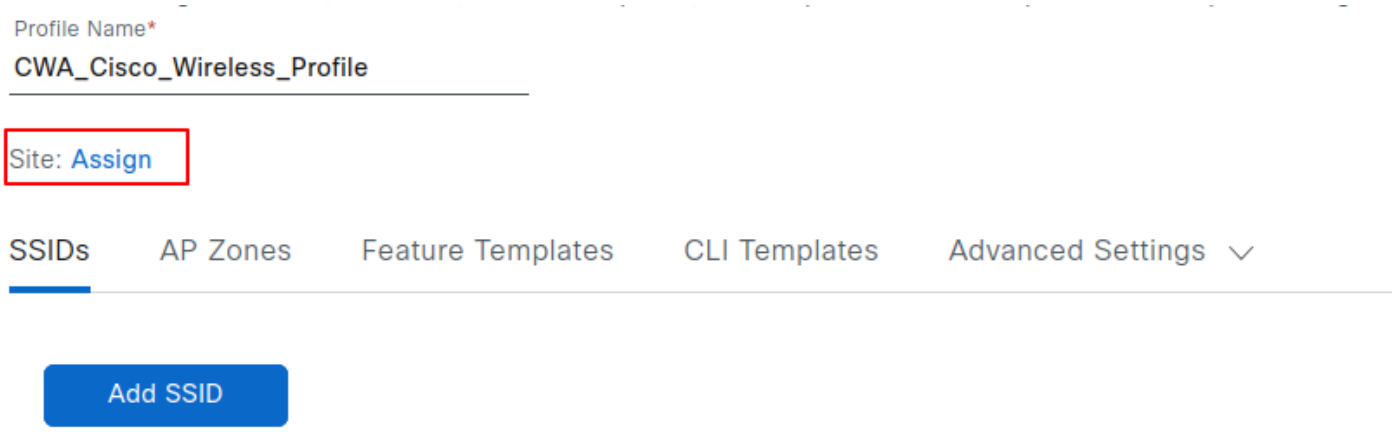
要配置无线配置文件，请导航到设计>网络配置文件，单击添加配置文件，然后选择无线。



根据需要命名配置文件。在本示例中，无线配置文件命名为CWA_Cisco_Wireless_Profile。您可以通过选择Add SSID将任何现有SSID添加到此配置文件中。SSID创建将在下一节介绍。

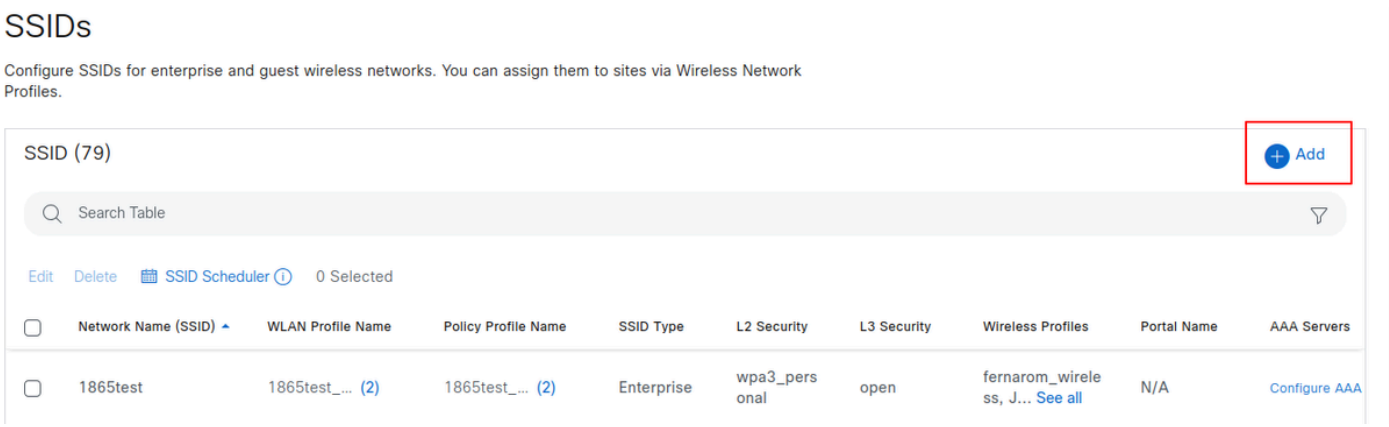


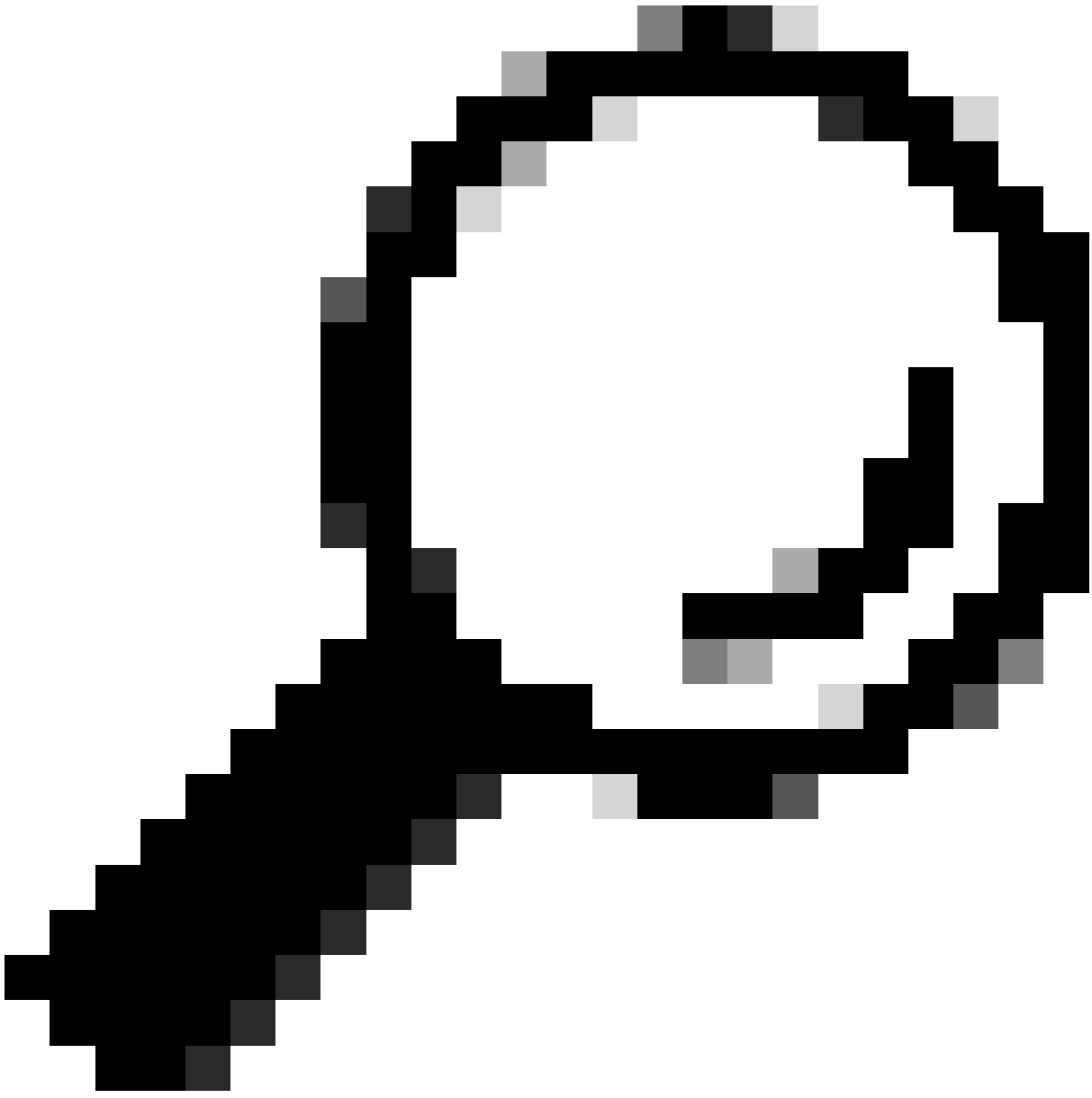
选择Assign以选择要应用此配置文件的站点，然后选择所需的站点。选择站点后，单击Save。



创建SSID

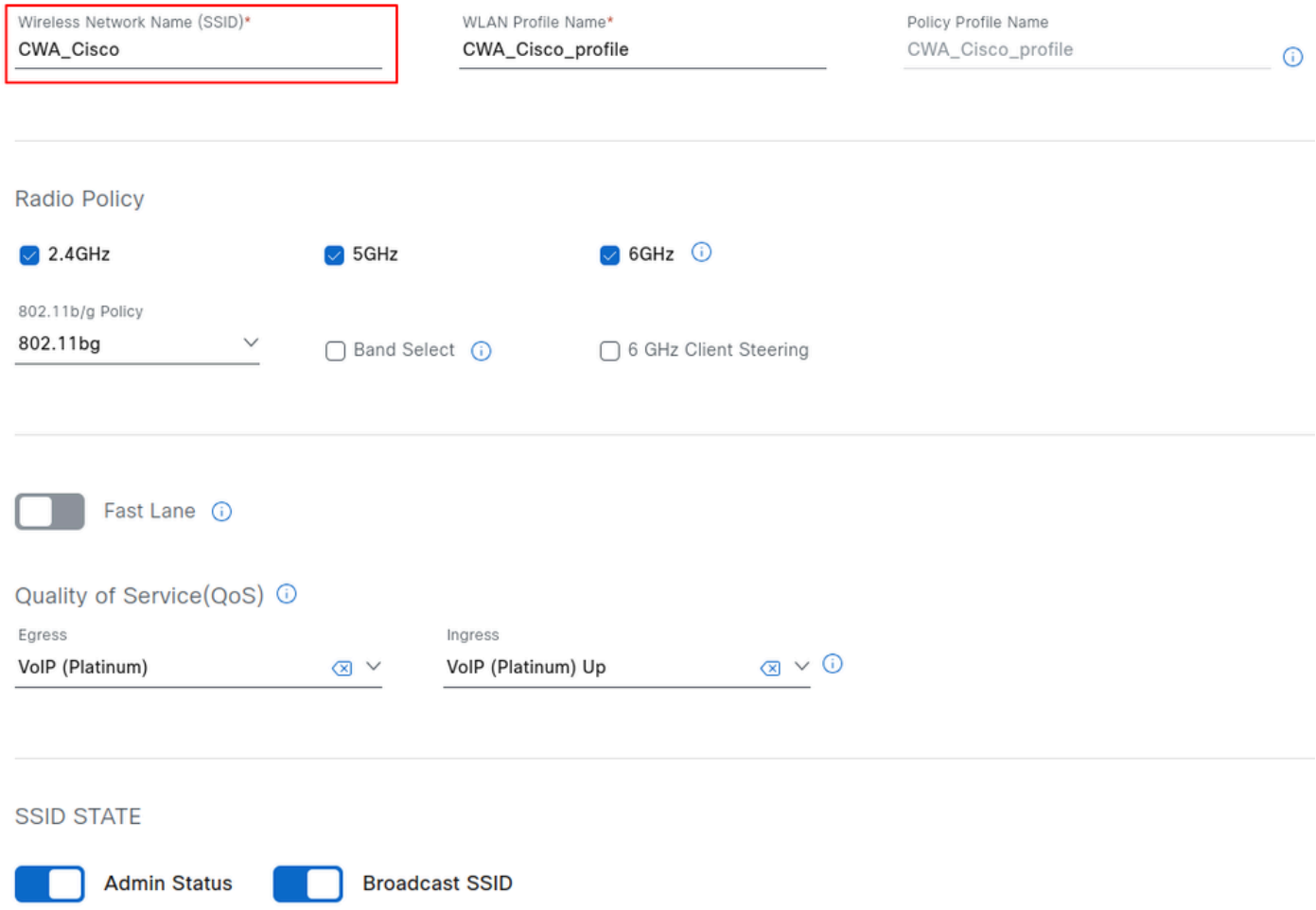
导航到Design > Network Settings > Wireless > SSIDs，然后单击Add。



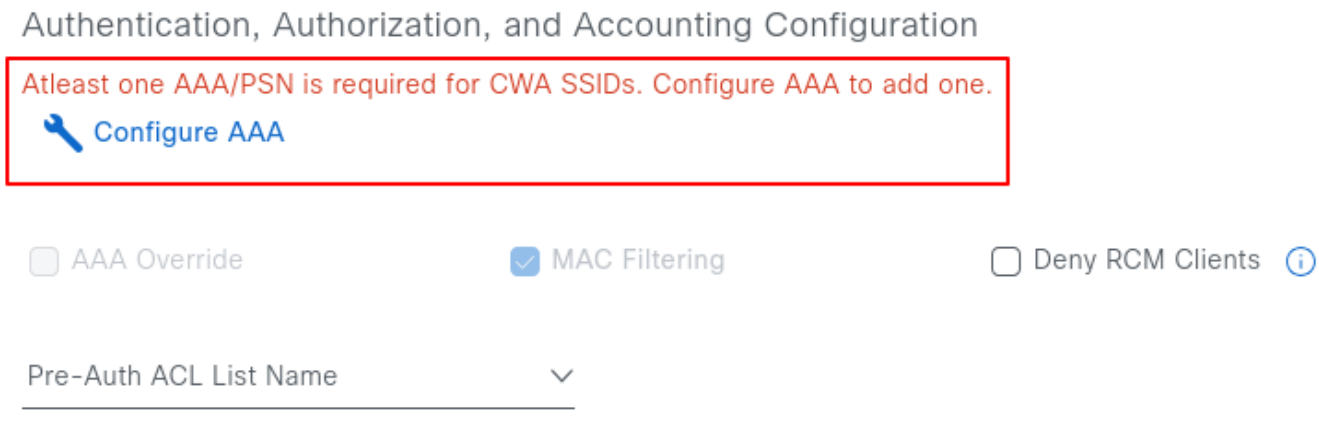


提示：为CWA创建SSID时，选择Guest type至关重要。此选择向WLC上的SSID无线策略配置文件添加命令 — nac命令 — 允许用户在强制网络门户上注册后使用CoA进行重新身份验证。如果没有此配置，用户可能会遇到无休止的循环注册和重复重定向到门户。

选择Add后，继续执行SSID配置工作流程。在第一页上，配置SSID名称，您还可以选择radio policy band，并定义SSID状态，包括管理状态和广播设置。在本配置指南中，SSID命名为CWA_Cisco。

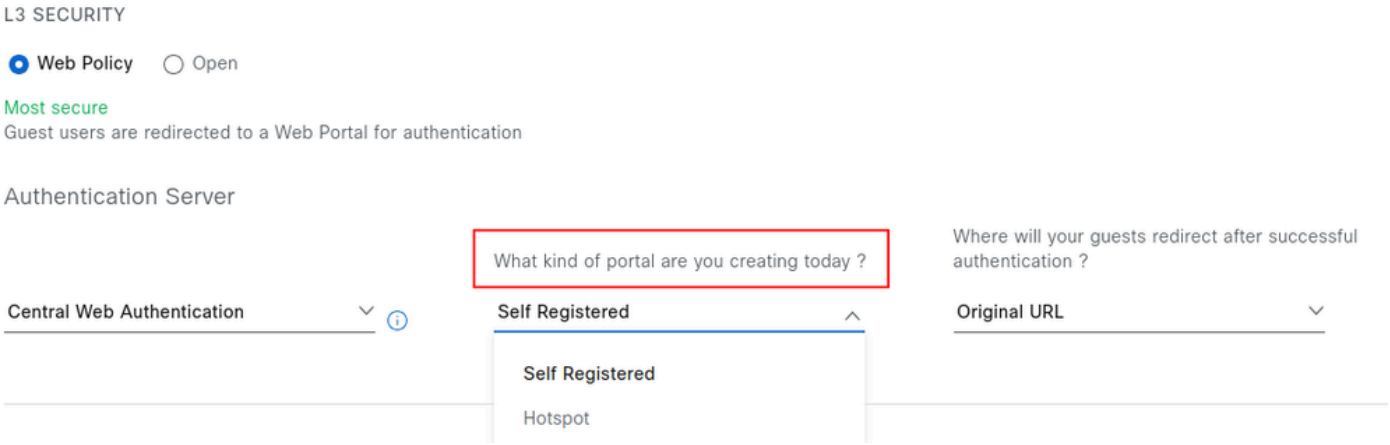


输入SSID名称后，将自动生成WLAN配置文件名称和策略配置文件名称。选择Next继续。
必须至少为CWA SSID配置一个AAA/PSN。如果未配置任何协议，请选择Configure AAA，然后从下拉列表中选择PSN IP address。

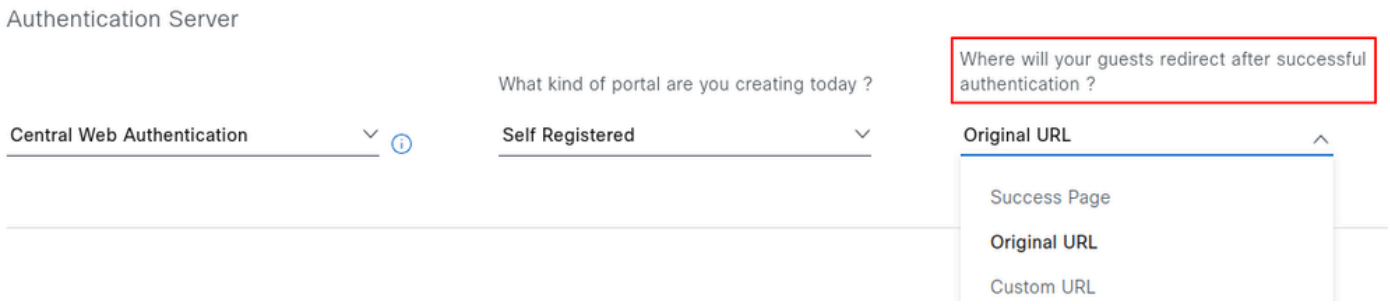


选择AAA服务器后，设置第3层安全参数并选择门户类型：Self-Registered或Hotspot。

热点访客门户：热点访客门户为访客提供网络访问，无需用户名和密码。在此，用户必须接受可接受的使用策略(AUP)才能访问网络，进而访问后续的Internet。需要提供凭证的访客门户：通过需要提供凭证的访客门户进行访问，需要访客具有用户名和密码。



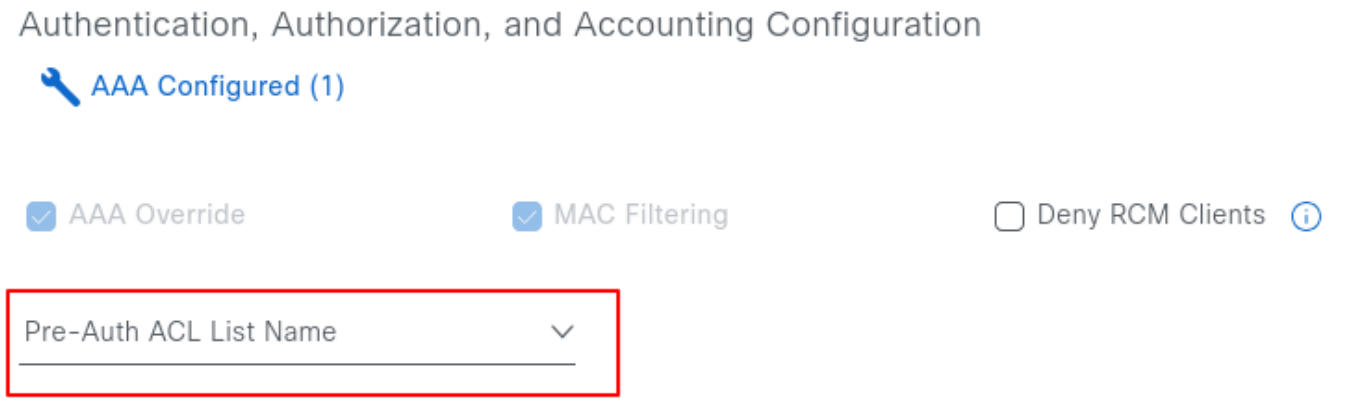
用户注册或接受使用策略后发生的操作也可以配置。有三种选项可供选择：Success Page、Original URL和Custom URL。



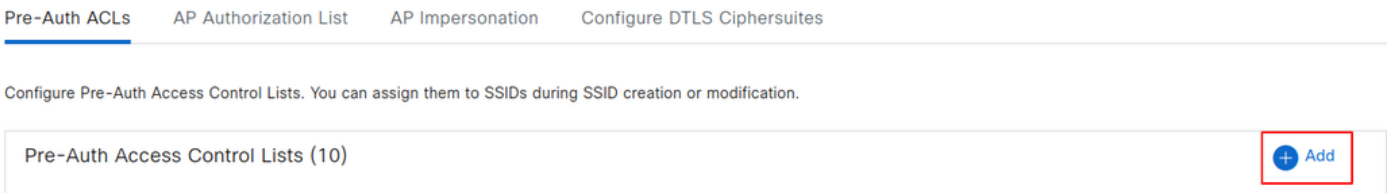
以下说明每个选项的行为：

成功页面：将用户重定向到指示身份验证成功的确认页面。
原始URL：将用户重定向到强制网络门户截获之前请求的原始URL。
自定义URL：将用户重定向到指定的自定义URL。选择此选项可启用其他字段来定义目标URL

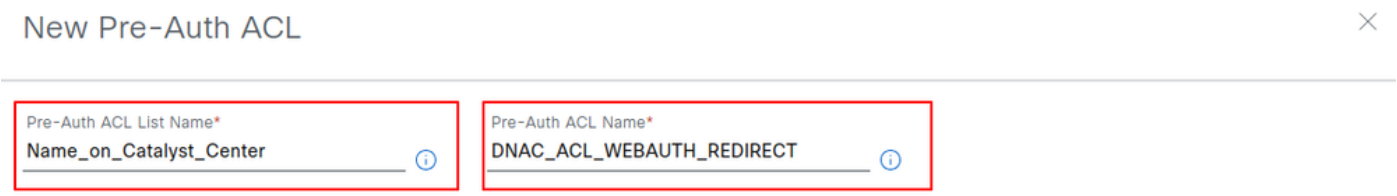
在同一页上，在身份验证、授权和记账配置下，还可以配置预身份验证ACL。此ACL允许为DHCP、DNS或PSN IP地址以外的协议添加额外条目，这些条目从网络设置中获取，并在调配过程中附加到重定向ACL。此功能在Cisco Catalyst Center版本2.3.3.x及更高版本中可用。



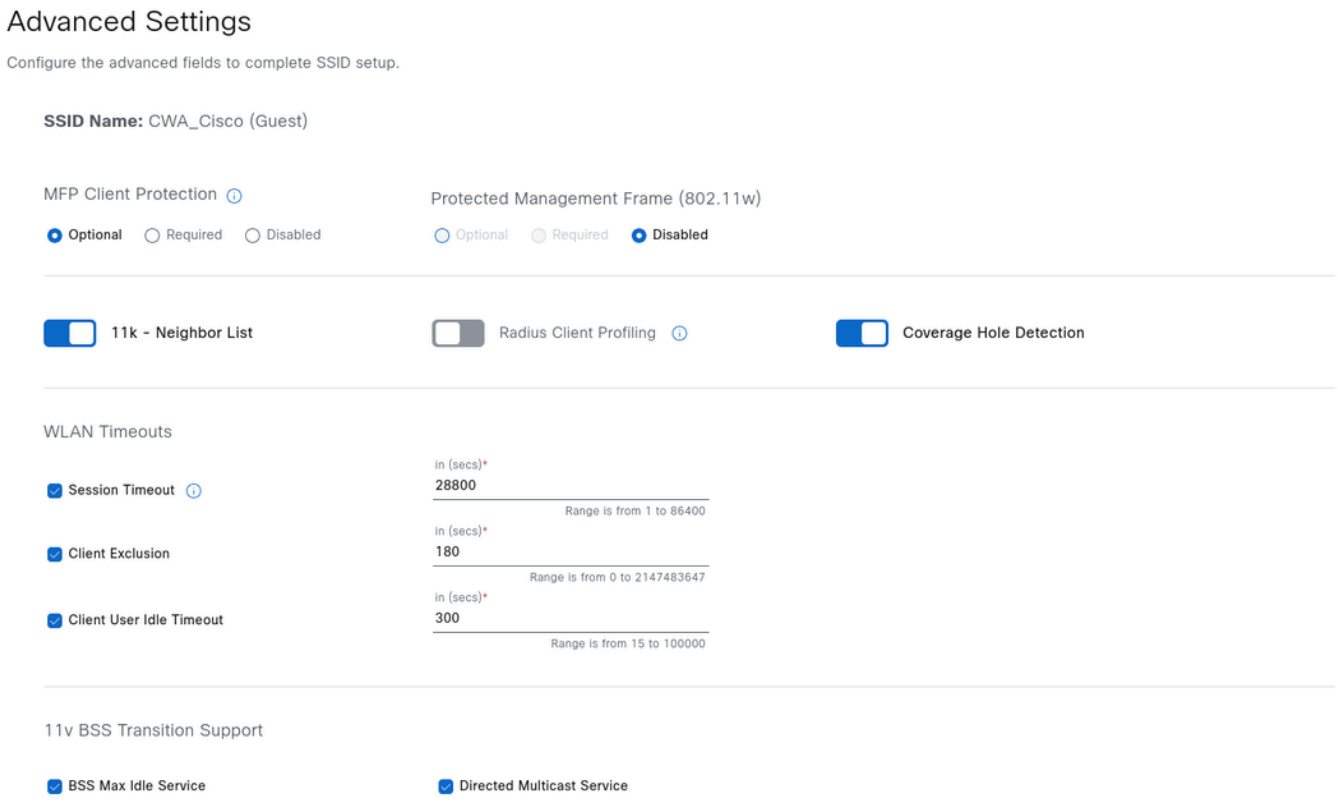
要配置预身份验证ACL，请导航到设计>网络设置>无线>安全设置，然后单击添加。



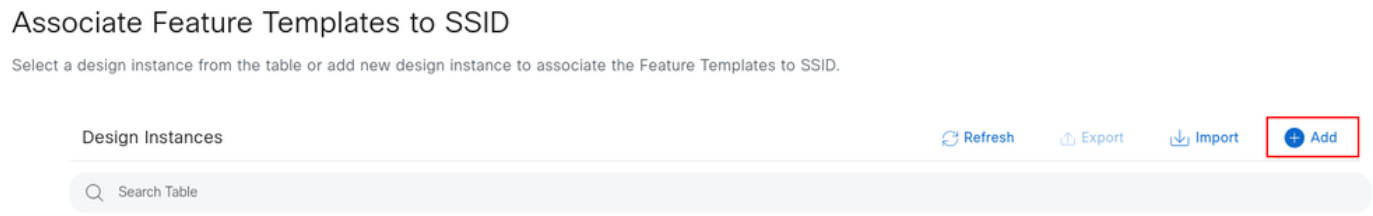
第一个名称标识Catalyst Center中的ACL，而第二个名称对应于WLC上的ACL名称。第二个名称可以与WLC上配置的现有重定向ACL匹配。作为参考，Catalyst Center将名称Cisco DNA_ACL_WEBAUTH_REDIRECT调配到WLC。预先身份验证ACL中的条目会附加到现有条目之后。



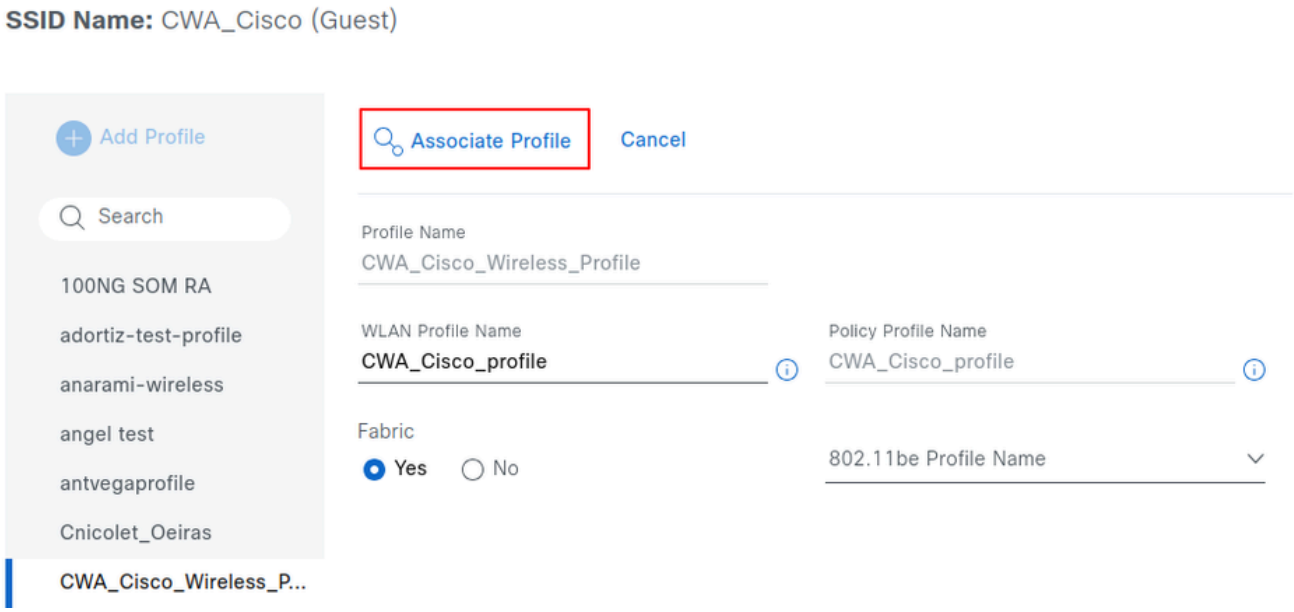
返回SSID创建工作流程，选择下一步将显示高级设置，包括快速转换、会话超时、客户端用户超时和速率限制。根据需要调整参数，然后选择下一步继续。在本配置指南中，本示例保留默认设置。



选择Next后，系统将显示提示以将任何功能模板与SSID关联。如果适用，通过点击添加选择所需的模板，完成后点击下一步。



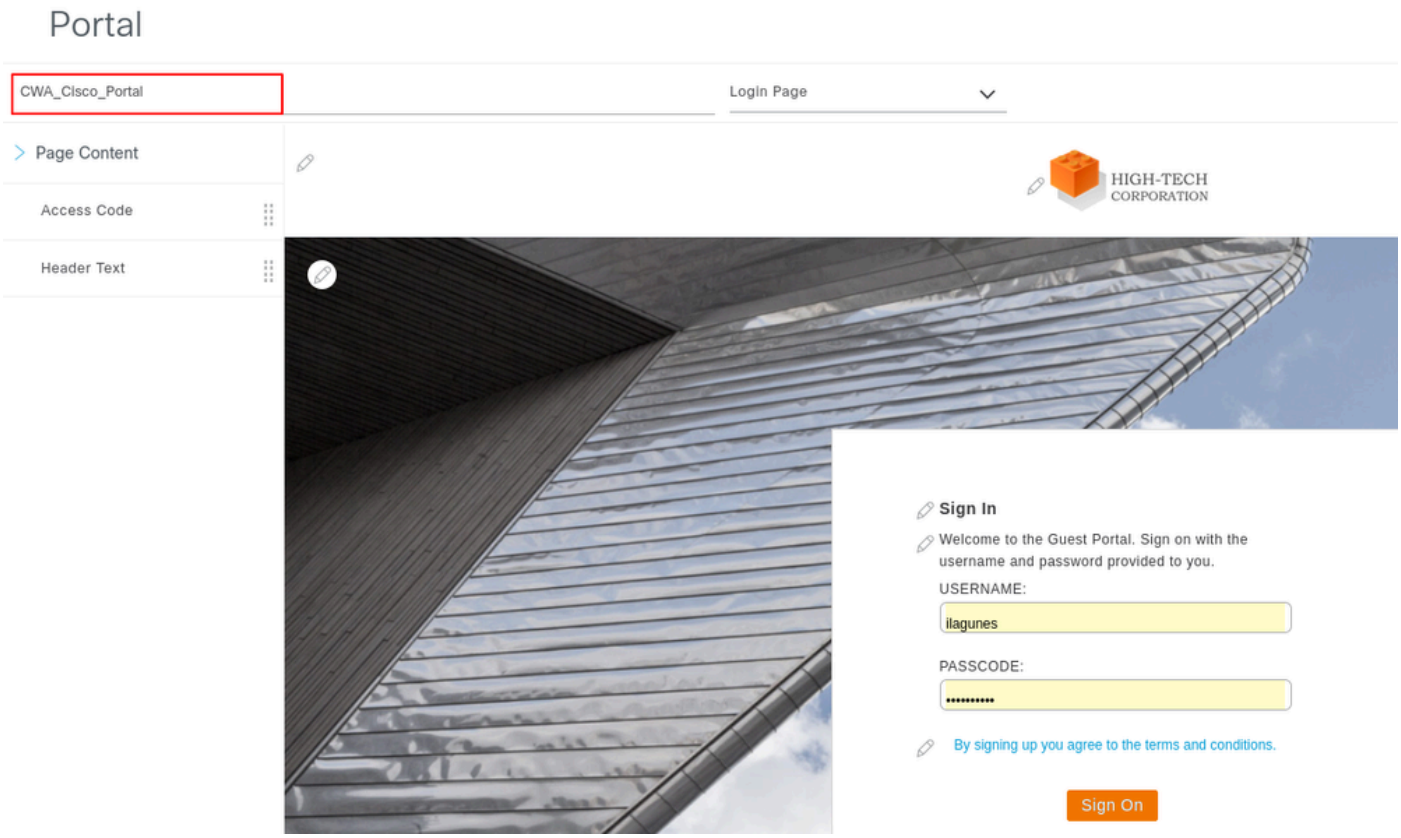
将SSID与先前创建的无线配置文件关联。有关参考，请参阅创建无线网络配置文件部分。在此部分中，您还可以选择是否启用了SSID交换矩阵。完成后，单击Associate profile。



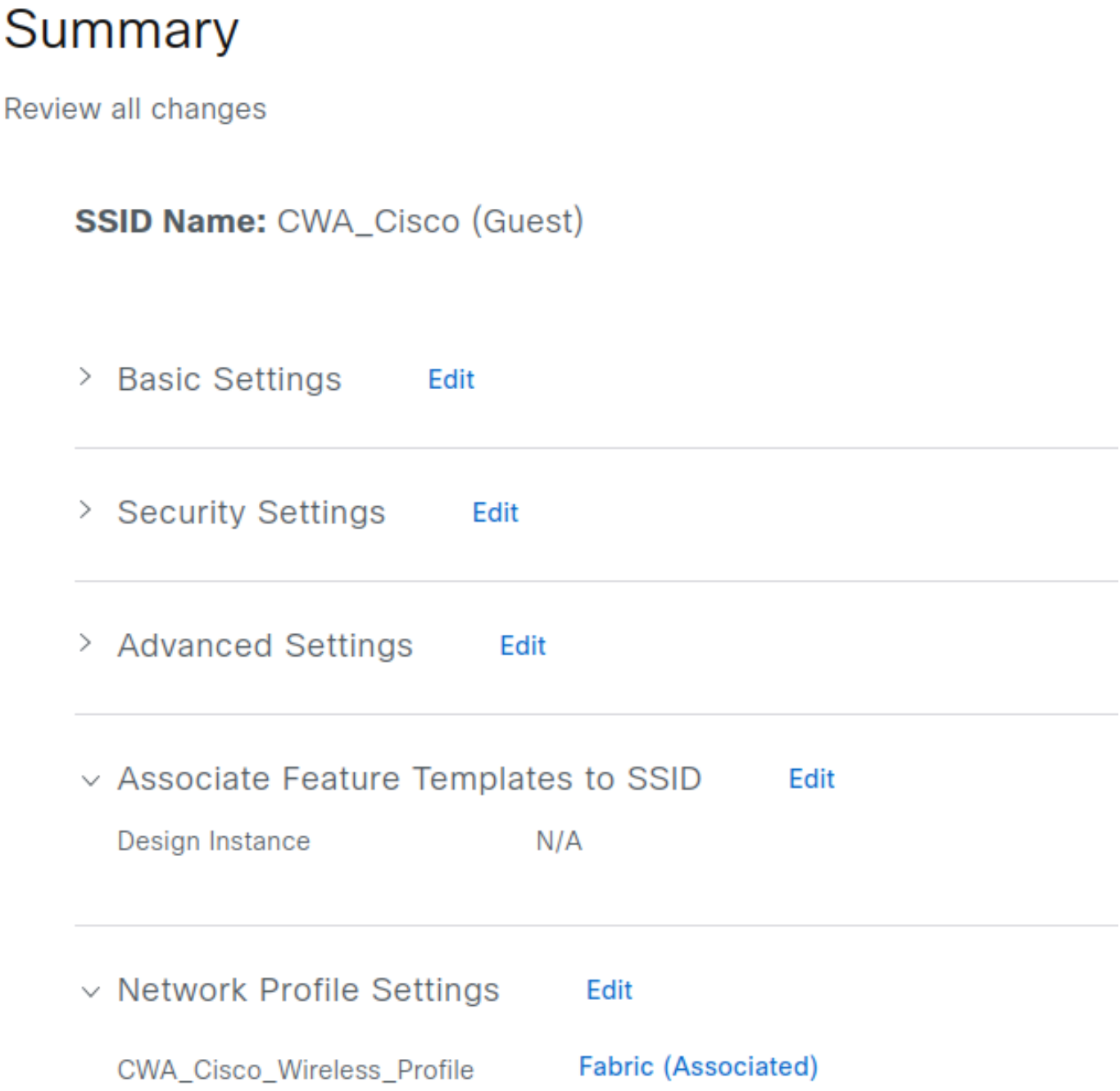
show wireless management trustpoint

配置文件与SSID关联后，单击Next以创建和设计强制网络门户，要启动，请单击Create Portal。

门户名称定义FQDN中的域名和ISE上的策略集名称。完成后单击Save。门户保持可编辑状态，必要时可将其删除。



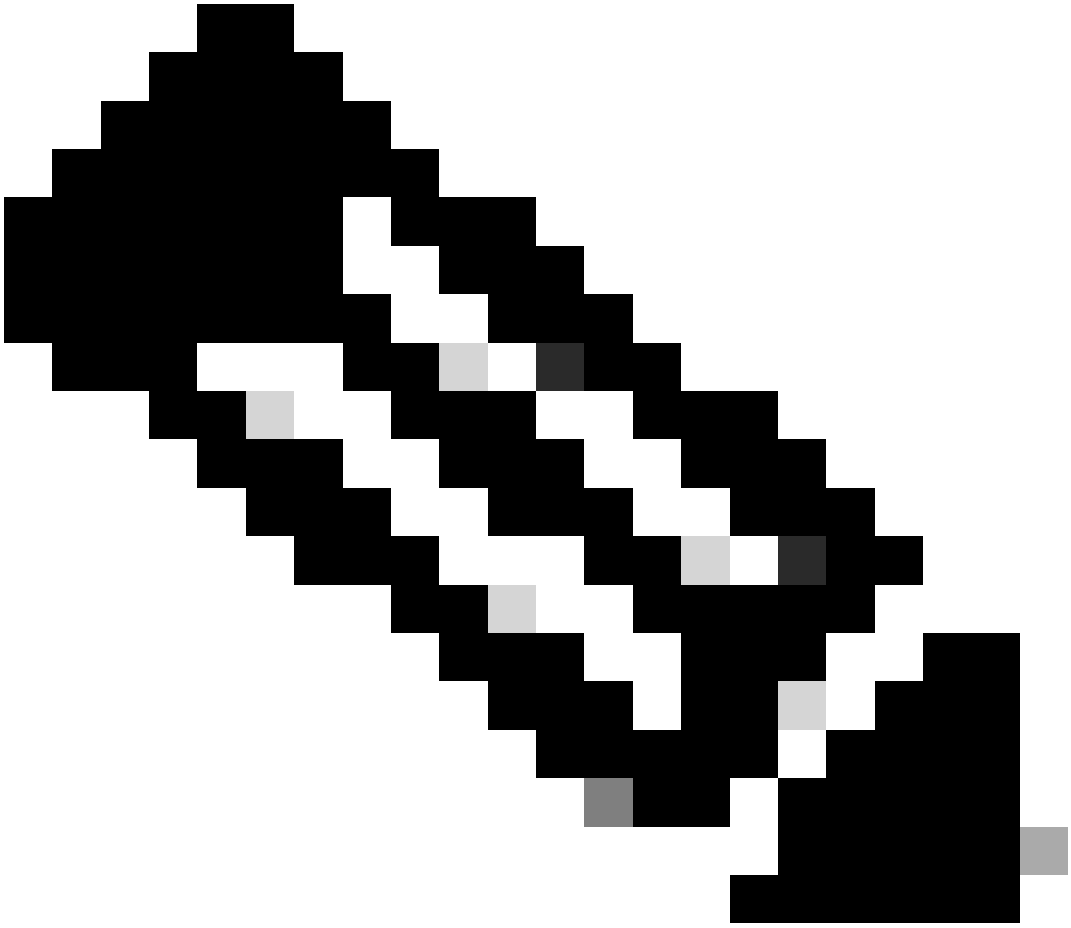
选择Next以显示之前步骤中定义的所有配置参数的摘要。



确认配置详细信息，然后选择保存以应用更改。

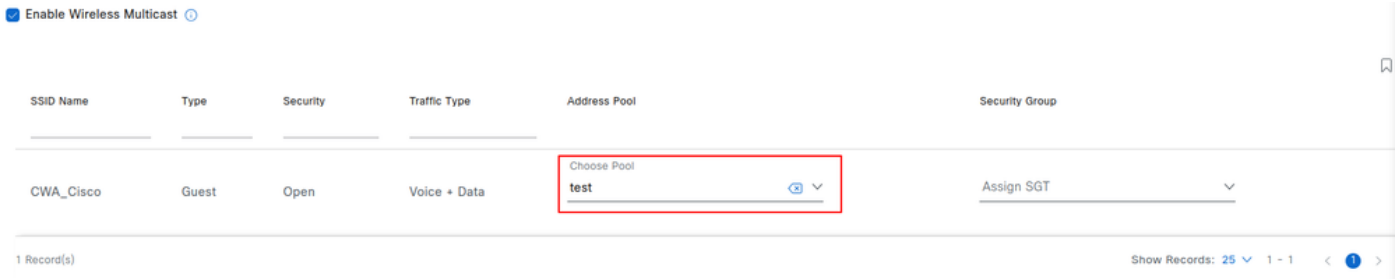
交换矩阵调配

将无线网络配置文件与交换矩阵站点关联后，SSID将显示在调配>交换矩阵站点>（您的站点）>无线SSID下。

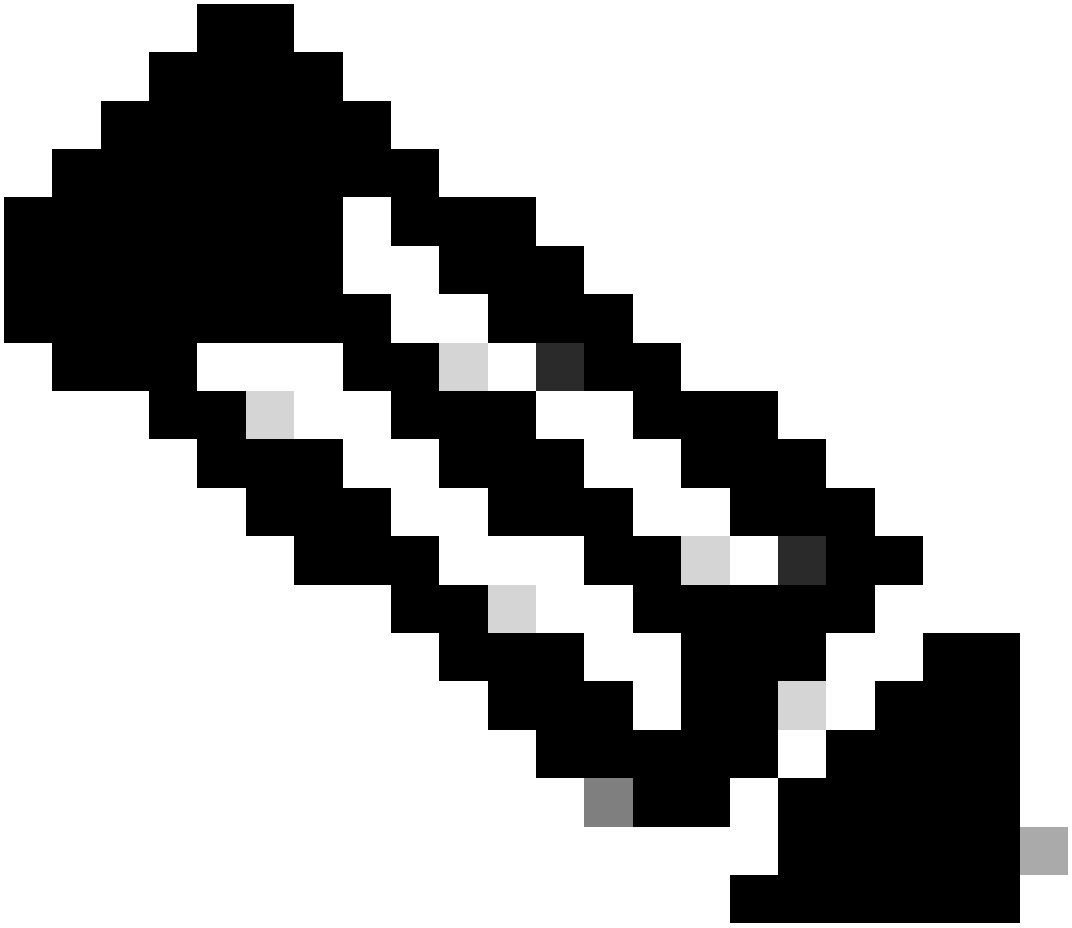


注意：您需要为站点配置无线LAN控制器，以便在“无线SSID”下显示SSID

选择SSID池，或者关联一个安全组标记，然后单击部署。仅当分配了池时，接入点才会广播SSID。



在AireOS和Catalyst 9800控制器上，在Network Settings中的任何SSID配置更改后重新调配无线局域网控制器。



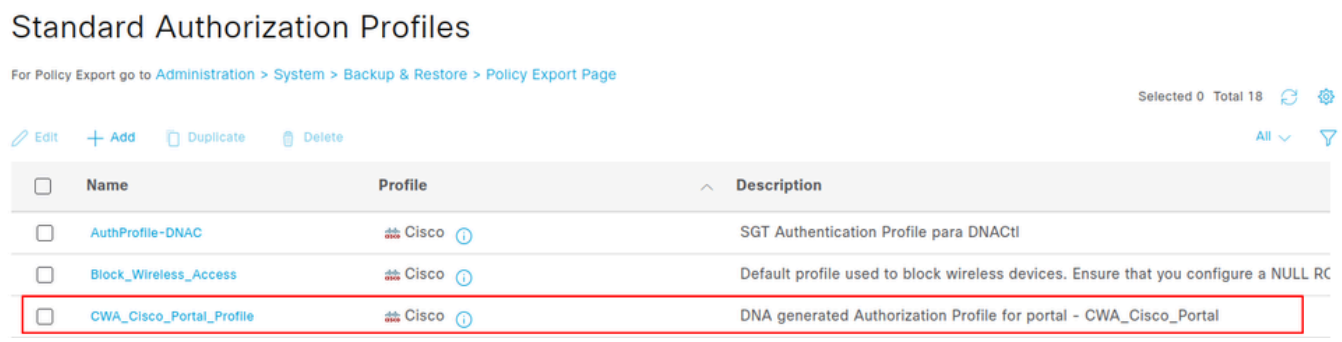
注意：如果没有为SSID分配池，则预计AP不会广播该池。仅在分配池后广播SSID。分配池后，无需重新调配控制器。

查看调配到思科ISE的配置

本部分检查Catalyst Center调配到Cisco ISE的配置。

授权配置文件

Catalyst Center在Cisco ISE上调配的部分配置是Authorization Profile。此配置文件根据客户端的参数定义分配给客户端的结果，并且可以包含特定设置，例如VLAN分配、ACL或URL重定向。
要在ISE中查看授权配置文件，请导航到策略>策略元素>结果。如果门户名称为CWA_Cisco_Portal，则配置文件名称为CWA_Cisco_Portal_Profile。说明字段显示文本：DNA为门户 — CWA_Cisco_Portal生成授权配置文件。



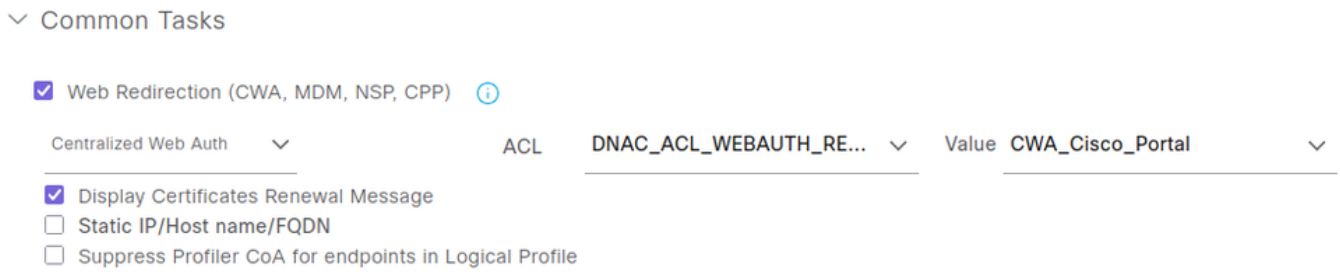
要查看通过此授权配置文件发送到无线LAN控制器的属性，请点击授权配置文件名称并参阅常见任务部分。
此授权配置文件提供重定向ACL和重定向URL。

Web重定向属性包括两个参数：

1. ACL名称：设置为Cisco DNA_ACL_WEBAUTH_REDIRECT。
2. 值：是指强制网络门户的名称，在本例中为CWA_Cisco_Portal。

Display Certificates Renewal Message选项使门户可用于续订终端当前使用的证书。

Display Certificates Renewal Message下提供了另一个选项Static IP/Host Name/FQDN。此功能允许传递门户的IP地址而不是FQDN，当强制网络门户因无法到达DNS服务器而无法加载时，此功能非常有用。

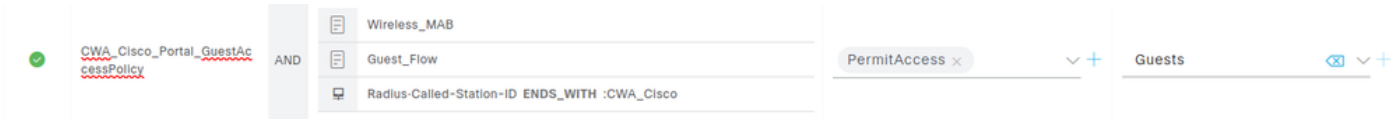


策略集

导航到Policy > Policy Sets > Default > Authorization Policy，查看为名为CWA_Cisco_Portal的门户创建的两个策略集。这些策略集包括：

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

当客户端已通过自助注册或通过热点门户完成Web身份验证过程时，将应用CWA_Cisco_Portal_GuestAccessPolicy策略。

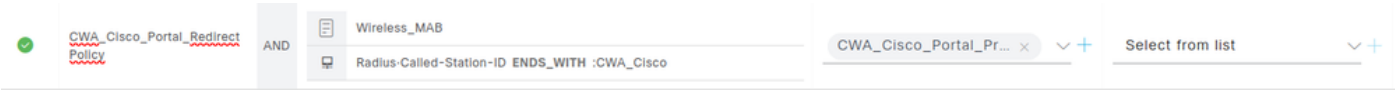


此策略集符合三个条件：

- Wireless_MAB：当思科ISE收到来自无线局域网控制器的MAC身份验证绕行(MAB)身份验证请求时使用。
- Guest_Flow:表示根据GuestEndpoints身份组检查终端的MAC地址的ISE。如果该组中不存在终端MAC地址，则不应用策略。
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco:Called-Station-ID是ISE中的RADIUS属性，它以ASCII格式存储网桥或接入点MAC地址并附加正在访问的SSID，以分号(:)分隔。 在本示例中，CWA_Cisco表示SSID名称。

在列配置文件下，您看到名称PermitAccess，这是不能编辑的保留授权配置文件，为网络提供完全访问权限，您也可以在Security Groups列下分配SGT，在本例中为Guests。

使用PermitAccess配置文件。这是保留的授权配置文件，无法编辑和授予对网络的完全访问权限。也可以在Security Groups列下分配SGT;在本例中，SGT设置为Guests。
下一个要审核的策略是CWA_Cisco_Portal_RedirectPolicy。



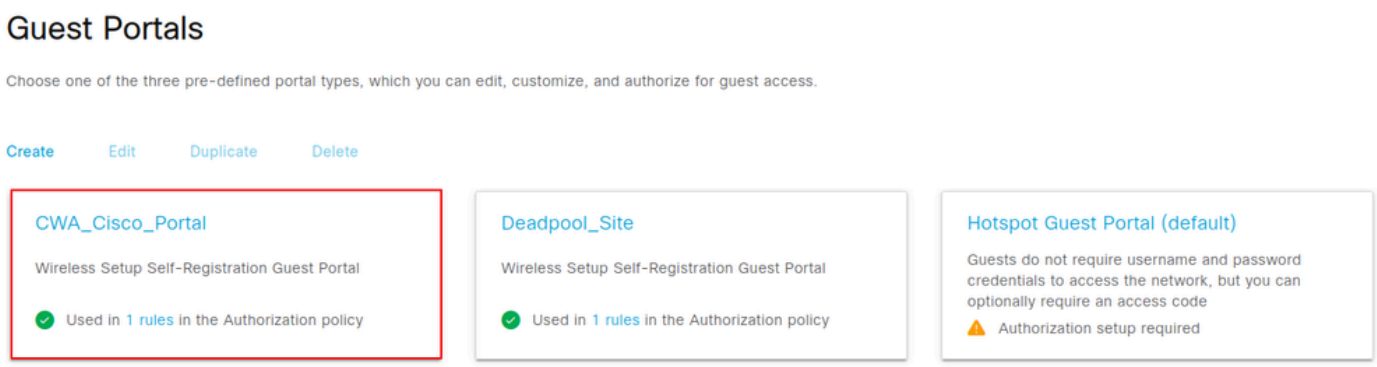
此策略集符合以下两个条件：

- Wireless_MAB：当Cisco ISE收到来自无线LAN控制器的MAB身份验证请求时使用。
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco:Called-Station-ID是ISE中的RADIUS属性，它以ASCII格式存储网桥或接入点MAC地址并附加正在访问的SSID，以分号(:)分隔。 在本示例中:CWA_Cisco表示SSID名称。

这些策略的顺序至关重要。如果CWA_Cisco_Portal_RedirectPolicy在列表中首先出现，则它仅使用RADIUS属性Called-Station-ID ENDS_WITH :CWA_Training匹配MAB身份验证和SSID名称。在此配置中，即使终端已通过门户进行身份验证，它仍将无限期地与此策略匹配。因此，永远无法通过PermitAccess配置文件授予完全访问权限，并且客户端仍然卡在身份验证和重定向到门户的连续循环中。

访客门户配置

导航到工作中心(Work Centers)>访客接入(Guest Access)>门户和组件(Portals & Components)以查看门户。
此处创建的访客门户使用与Catalyst Center CWA_Cisco_Portal中相同的名称。如果要查看其他详细信息，请选择门户名称。

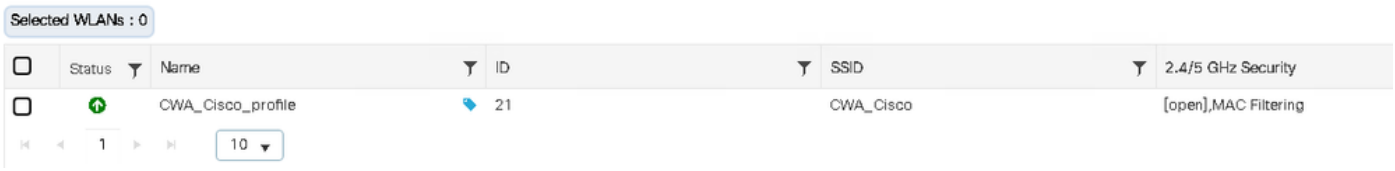


查看调配到WLC的配置

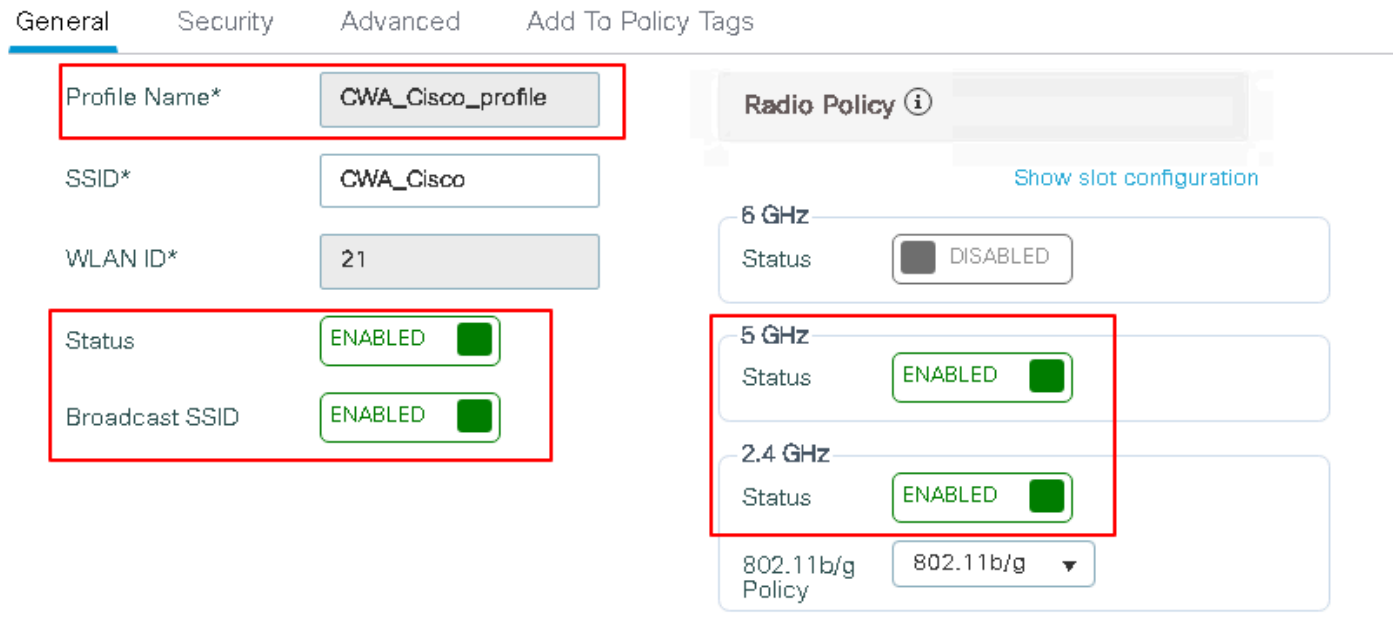
本部分检查Catalyst Center调配到无线LAN控制器的配置。

SSID 配置

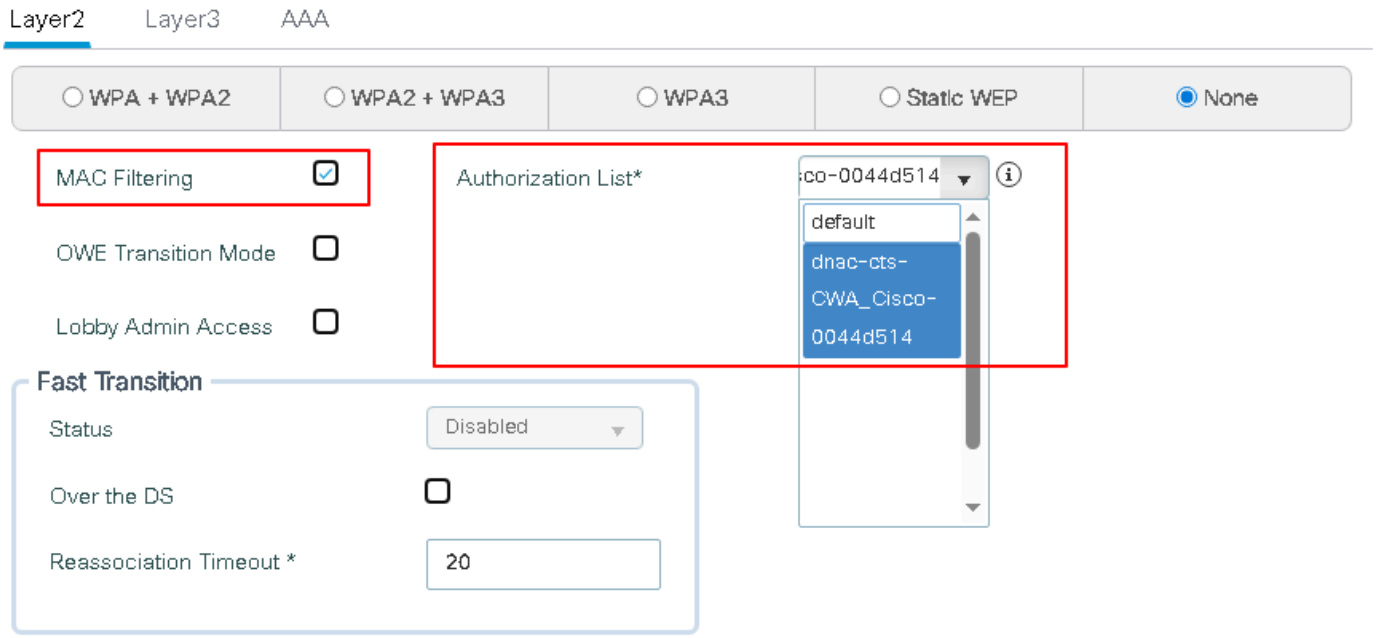
在WLC GUI中，导航到Configuration > Tags & Profiles > WLANs以查看SSID配置。



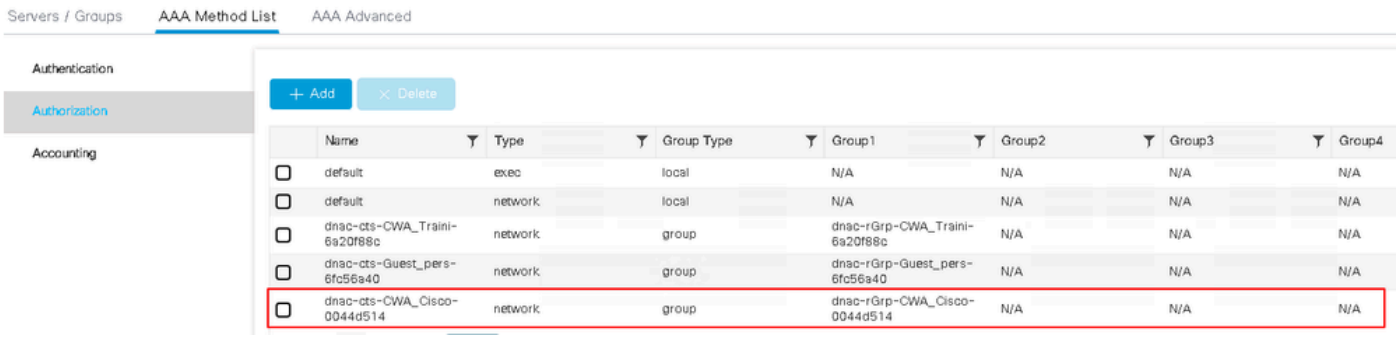
SSID CWA_Cisco在WLC上的名称为CWA_Cisco_profile，ID为21，使用MAC过滤的Open安全类型。双击SSID查看其配置。



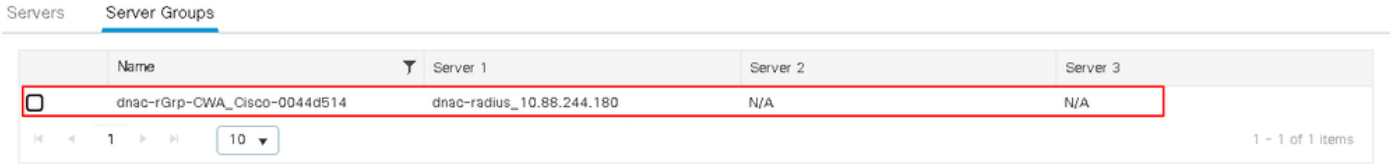
SSID为UP，并在5 GHz和2.4 GHz信道上广播，并且已连接到策略配置文件CWA_CIsco_Profile。单击Security选项卡查看设置。



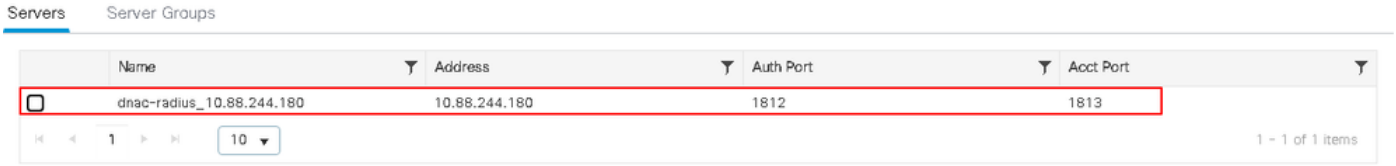
密钥设置包括第2层安全方法（MAC过滤）和AAA授权列表(Cisco DNA-cts-CWA_Cisco-0044d514)。 要查看其配置，请导航到Configuration > Security > AAA > AAA Method List > Authorization。



方法列表指向Group1列中的RADIUS组Cisco DNA-rGrp-CWA_Cisco-0044d514。要查看其配置，请导航到Configuration > Security > AAA > Server/Groups > Server Groups。



服务器组组Cisco DNA-rGrp-CWA_Cisco-0044d514指向Server 1列中的Cisco DNA-radius_10.88.244.180。在Servers选项卡中查看其配置。



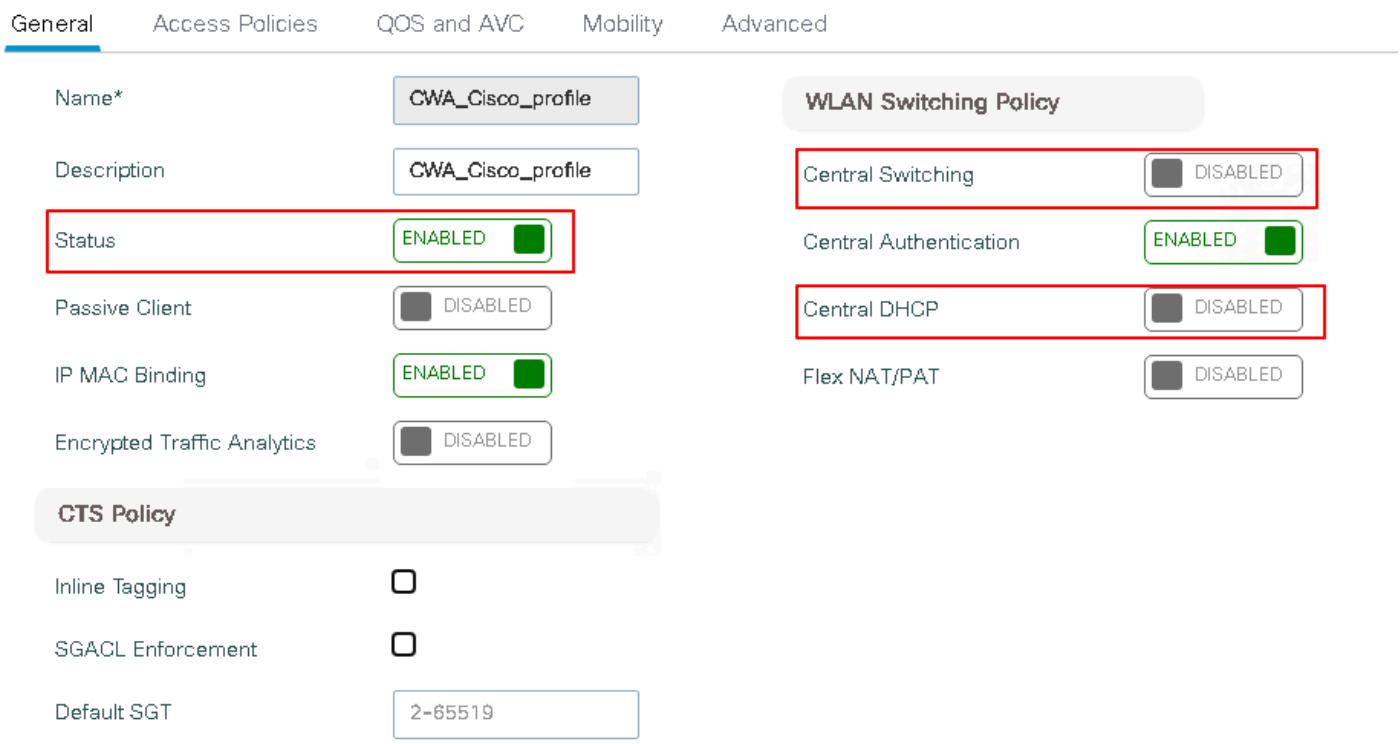
服务器Cisco DNA-radius_10.88.244.180的IP地址为10.88.244.180，单击其名称查看其配置

关键配置是授权更改(CoA)，它提供一种机制，用于在强制网络门户上验证身份验证、授权和记帐(AAA)会话后，修改其属性。如果没有此功能，终端即使在完成门户上的注册后仍处于web-auth pending状态。

无线策略配置文件配置

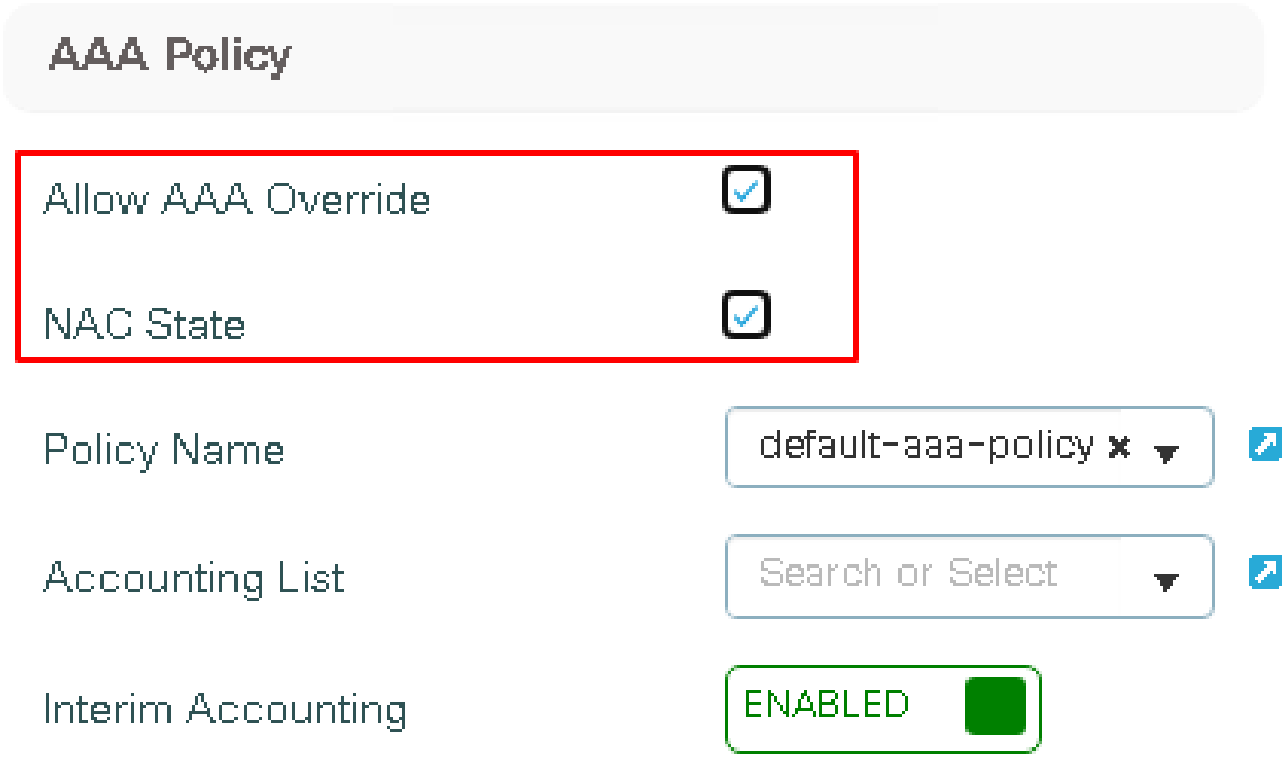
在策略配置文件中，可以为客户端分配设置，例如VLAN、ACL、QoS、移动锚点和计时器。要查看策略配置文件的配置，请导航到配置>标记和配置文件>策略。

单击policy name查看其配置。



策略状态为Enabled，与任何交换矩阵SSID一样，中心交换和中心DHCP被禁用。单击Advanced选

项卡，然后导航到AAA Policy部分以查看其他配置详细信息。



可以启用AAA覆盖和网络访问控制(NAC)。AAA覆盖允许控制器接受RADIUS服务器返回的属性（如ACL或URL），并将这些属性应用于客户端。在客户端在门户上注册后，NAC启用授权更改(CoA)。
也可以通过WLC上的CLI查看此配置。
要验证策略配置文件，已连接SSID以运行以下命令：

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21
CWA_Cisco_profile
  CWA_Cisco  UP
```

要查看策略配置文件CWA_Cisco_profile的配置，请运行命令：

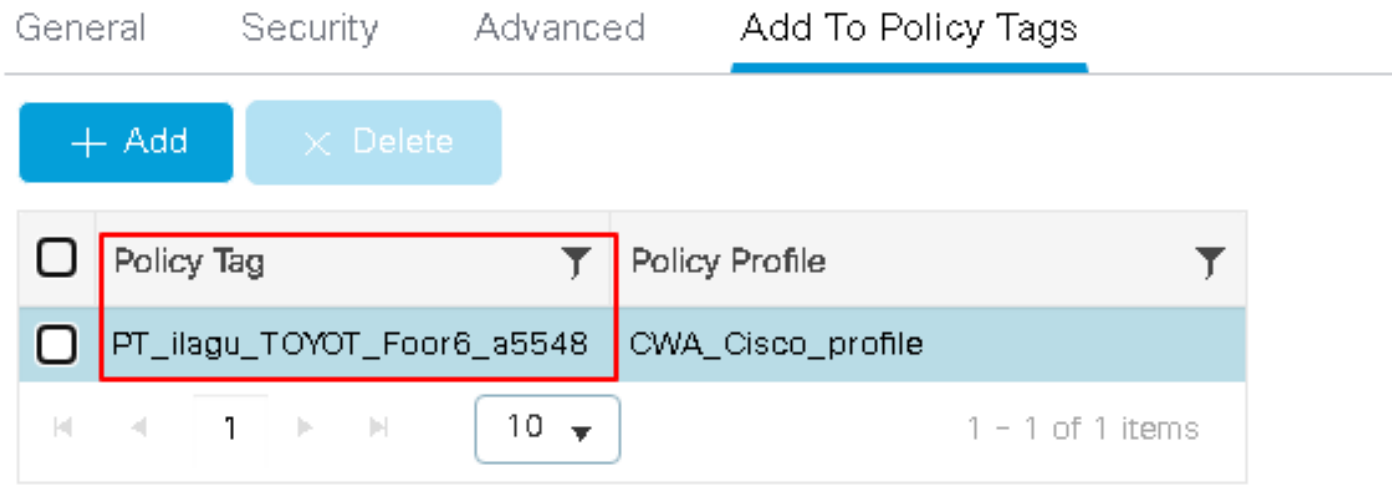
<#root>

```
WLC#show running-config | section policy CWA_Cisco_profile


wireless profile policy CWA_Cisco_profile
 aaa-override
```

```
no central dhcp


no central switching


description CWA_Cisco_profile
dhcp-tlv-caching
exclusionlist timeout 180
fabric CWA_Cisco_profile
http-tlv-caching

nac


service-policy input platinum-up
service-policy output platinum
no shutdown
```

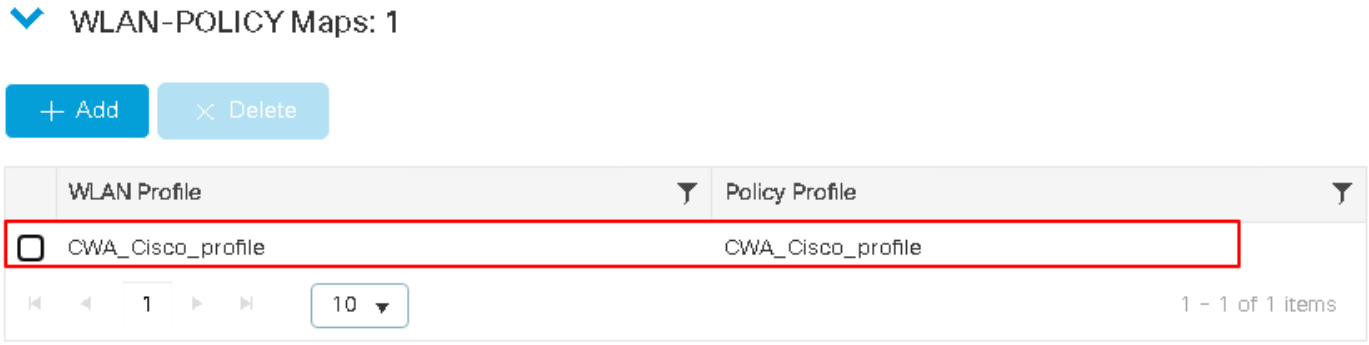
策略标签配置

策略标记是将WLAN与策略配置文件链接的方式，导航到Configuration > Tags & Profiles > WLANs，点击WLAN name，然后导航到Add to Policy Tags以标识分配给SSID的策略标记。



对于SSID CWA_Cisco_profile，策略标记PT_ilagu_TOYOT_Foor6_a5548用于验证此配置，导航到Configuration > Tags & Profiles > Tags > Policy。

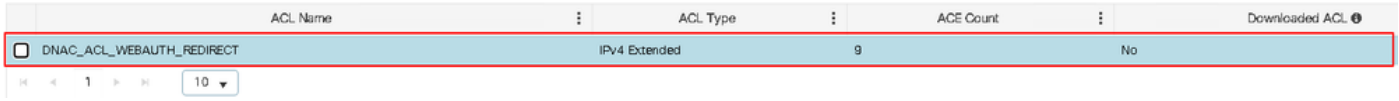
单击name查看其详细信息。策略标记PT_ilagu_TOYOT_Foor6_a5548将与WLC上的名称CWA_Cisco_profile关联的WLAN CWA_Cisco链接到策略配置文件CWA_Cisco_profile（请参阅WLANs页面以获得参考）。



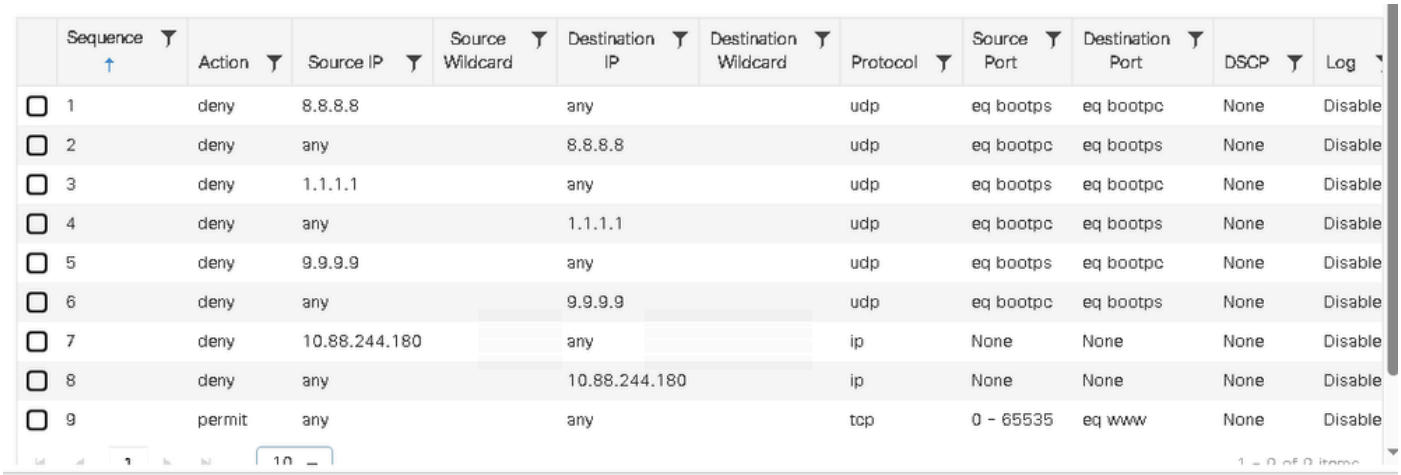
WLAN名称CWA_Cisco_profile引用WLAN CWA_Cisco。

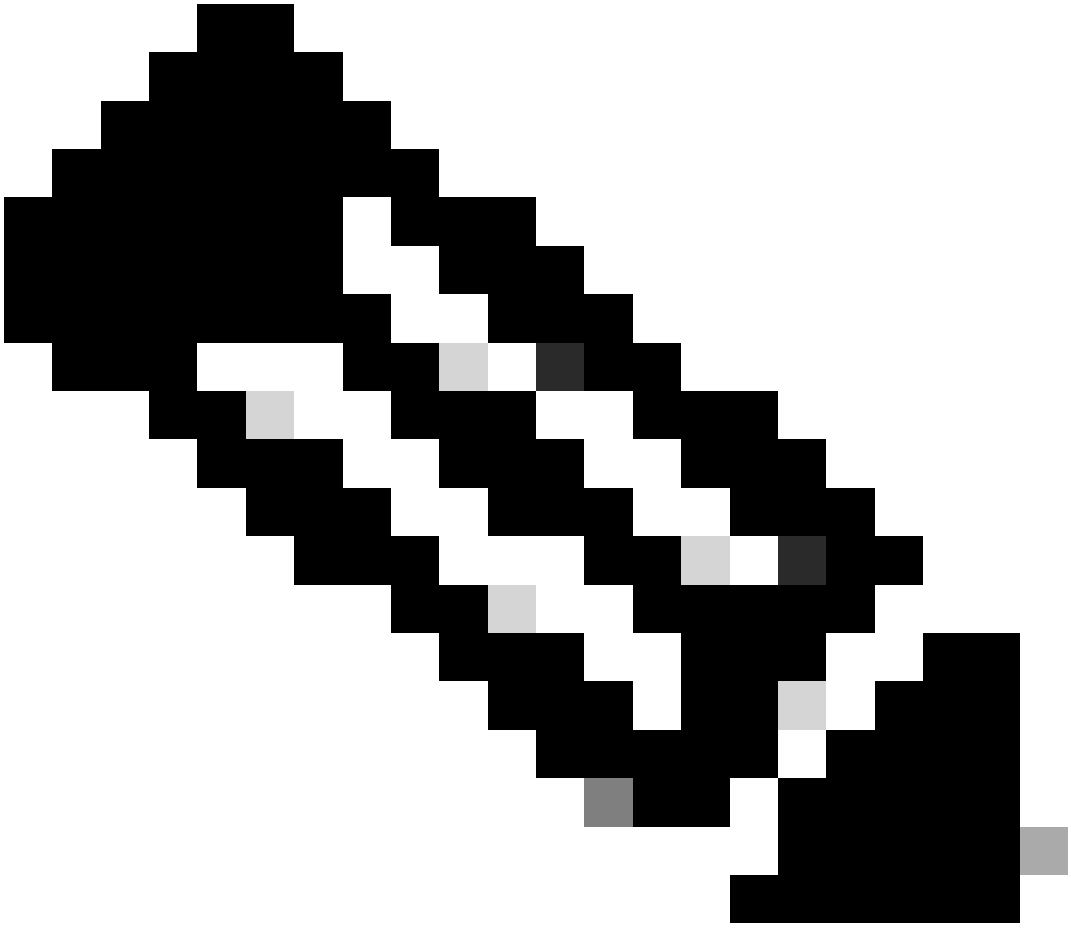
重定向 ACL 配置

在CWA中，重定向访问控制列表定义将哪些流量重定向到WLC以进行进一步处理，以及哪些流量绕过重定向
在创建SSID并从资产调配WLC之后，此配置将被推送到WLC。要查看该列表，请导航到Configuration > Security >ACL,Catalyst Center用于重定向ACL的ACL名称为Cisco DNA_ACL_WEBAUTH_REDIRECT。



单击name查看其配置。这些值来自Catalyst Center上站点的网络设置的网络设置。





注意：这些值从Catalyst Center中配置的站点网络设置获得，而DHCP/DNS值源自WLAN中配置的池。在SSID工作流程中的AAA配置中引用ISE PSN IP地址。

要在WLC CLI上查看重定向ACL，请运行以下命令：

<#root>

```
WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

重定向ACL可以应用于Flex配置文件，以便将其发送到接入点。运行此命令以确认此配置

<#root>

```
WLC#show running-config | section flex

wireless profile flex default-flex-profile
 acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT


central-webauth


urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

在接入点上重定向ACL

在接入点上，允许值和拒绝值颠倒：permit表示转发流量，deny表示重定向。要检查AP上的重定向ACL配置，请运行以下命令：

<#root>

```
AP#sh ip access-lists

Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
7 permit ip 10.88.244.180 0.0.0.0 any
8 permit ip any 10.88.244.180 0.0.0.0
9 deny tcp any range 0 65535 any eq 80
```

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）。