在Catalyst 9800 WLC上配置本地EAP身份验证

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 主要本地EAP配置
  - 步骤1.本地EAP配置文件
  - 步骤2. AAA身份验证方法
  - 步骤3.配置AAA授权方法
  - 步骤4.配置本地高级方法
  - 步骤5.配置WLAN
  - 步骤6.创建一个或多个用户
  - 步骤7.创建策略配置文件。创建策略标记以将此WLAN配置文件映射到策略配置文件
  - 步骤8.将策略标记部署到接入点。

验证

故障排除

- 由于密码错误而无法连接的客户端示例

简介

本文档介绍在Catalyst 9800 WLC（无线LAN控制器）上配置本地EAP。

先决条件

要求

本文档介绍在Catalyst 9800 WLC上配置本地EAP（可扩展身份验证协议）；即，WLC充当无线客户端的RADIUS身份验证服务器。

本文档假设您熟悉9800 WLC上的WLAN基本配置，并且仅重点介绍作为无线客户端的本地EAP服务器运行的WLC。

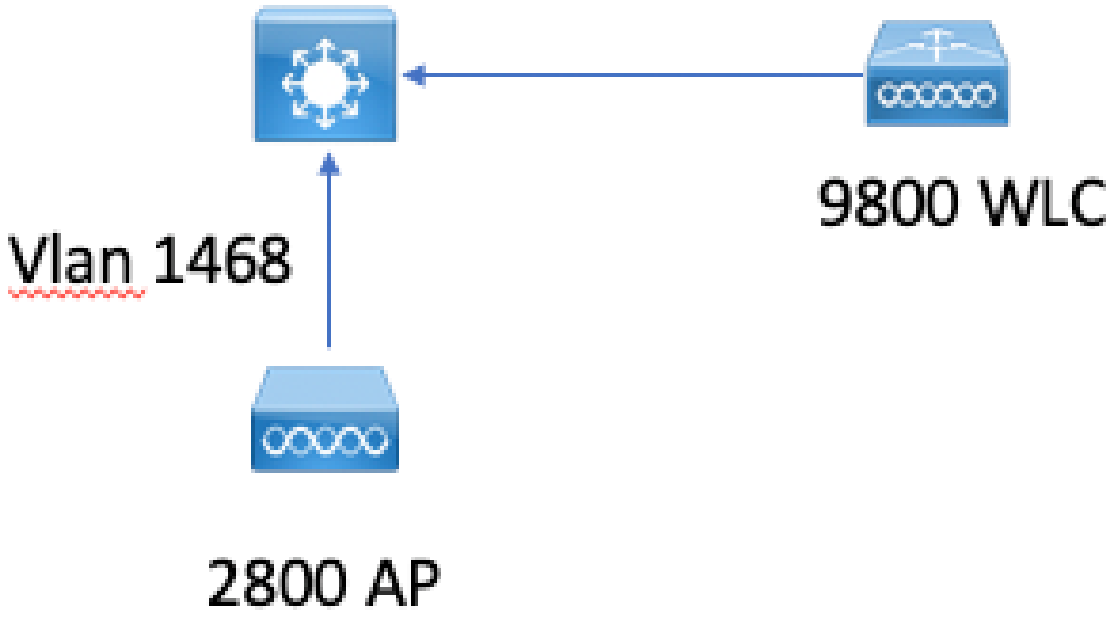
使用的组件

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。

版本17.3.6的Catalyst 9800

配置

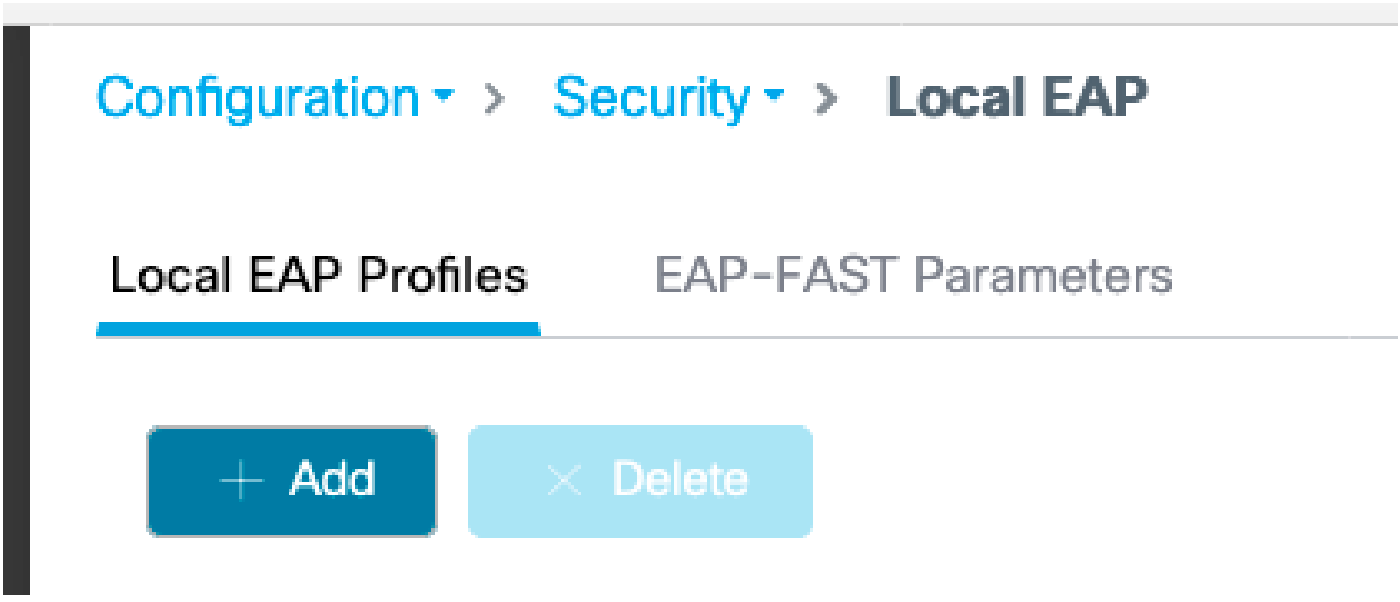
网络图



主要本地EAP配置

步骤1.本地EAP配置文件

转到9800 Web UI中的Configuration > Security > Local EAP。

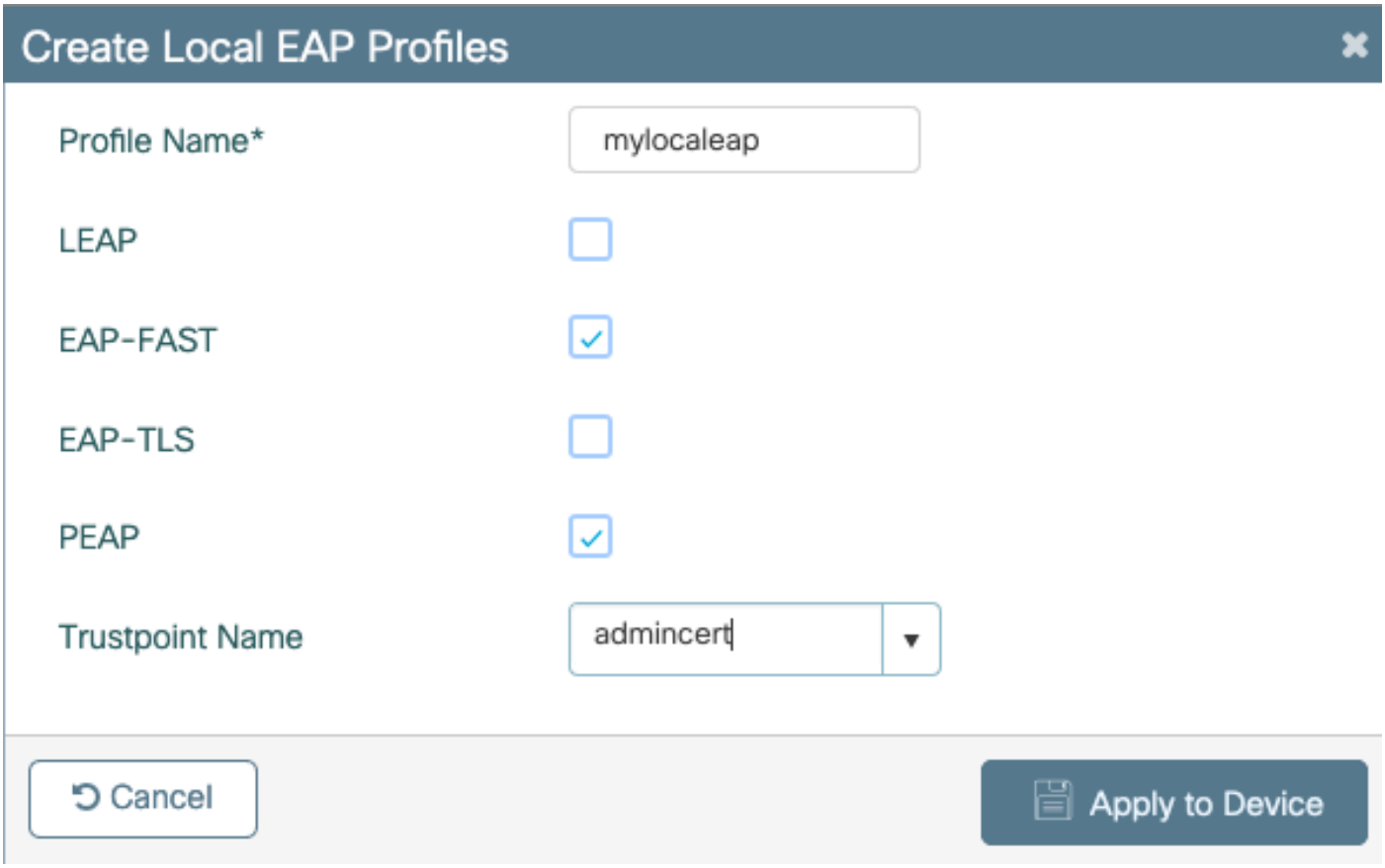


选择Add

输入配置文件名称。

由于安全性较差，不建议使用LEAP。其他3种EAP方法中的任何一种都需要您配置信任点。这是因为9800（充当身份验证器）必须发送证书让客户端信任它。

客户端不信任WLC默认证书，因此您需要在客户端停用服务器证书验证（不建议），或在客户端信任的9800 WLC上安装证书信任点（或在客户端信任存储中手动导入）。



CLI：

```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

步骤2. AAA身份验证方法

您需要配置本地指向的AAA dot1x方法，以便使用用户的本地数据库（但您可以使用外部LDAP查找）。

转至Configuration > Security > AAA，然后转到Authentication的AAA method list选项卡。选择Add。

选择“dot1x”类型和本地组类型。



步骤3.配置AAA授权方法

转至Authorization子选项卡，创建用于键入credential-download的新方法并将其指向本地。

对网络授权类型执行相同操作

CLI：

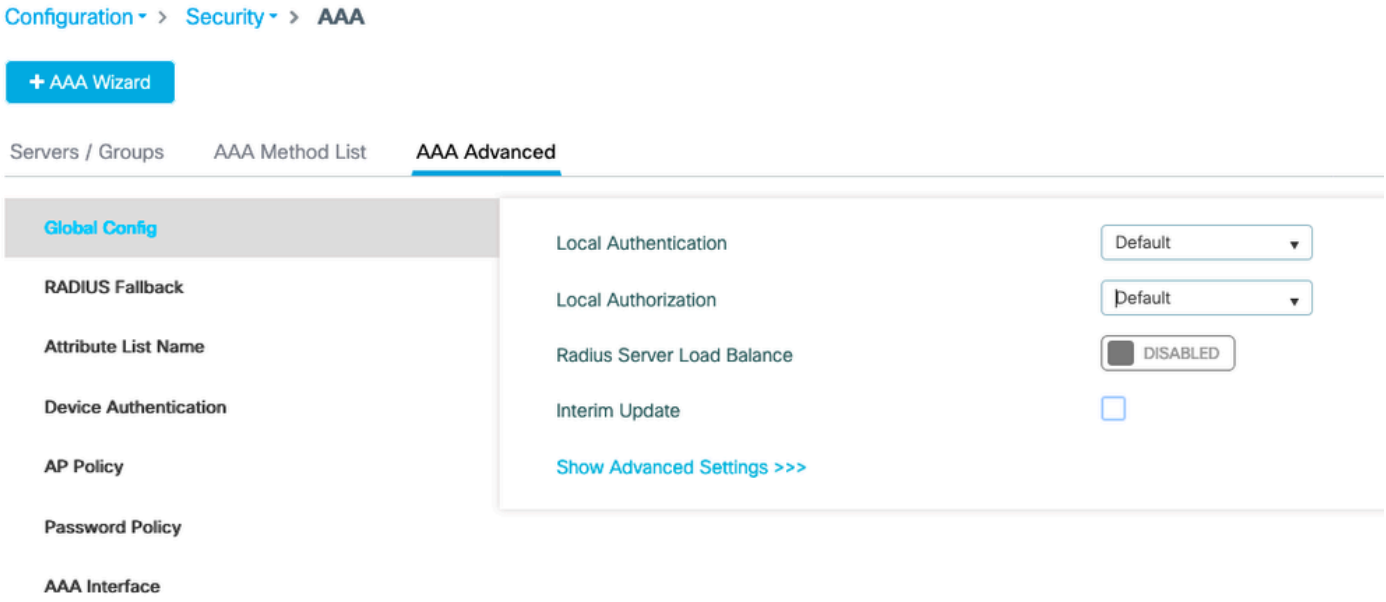
```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

步骤4.配置本地高级方法

转到AAA advanced选项卡。

定义本地身份验证和授权方法。由于此示例使用了“默认”凭证下载和“默认”dot1x方法，您需要在此处为本地身份验证和授权下拉框设置默认值。

如果定义了命名方法，请在下拉列表中选择“方法列表”，然后使用另一个字段输入方法名称。



CLI：

```
aaa local authentication default authorization default
```

步骤5.配置WLAN

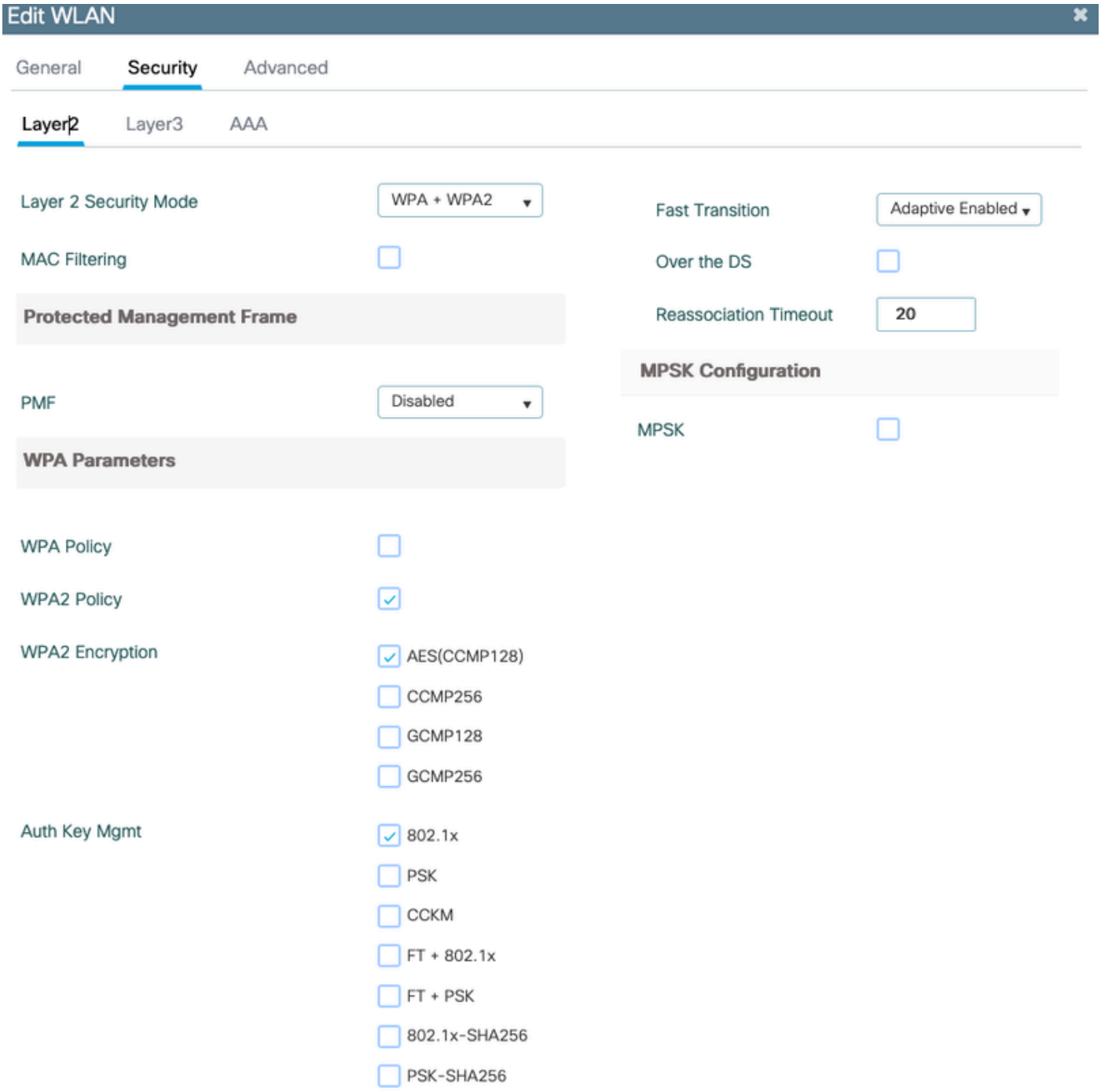
然后，您可以根据上一步中定义的本地EAP配置文件和AAA身份验证方法配置WLAN以实现802.1x安全。

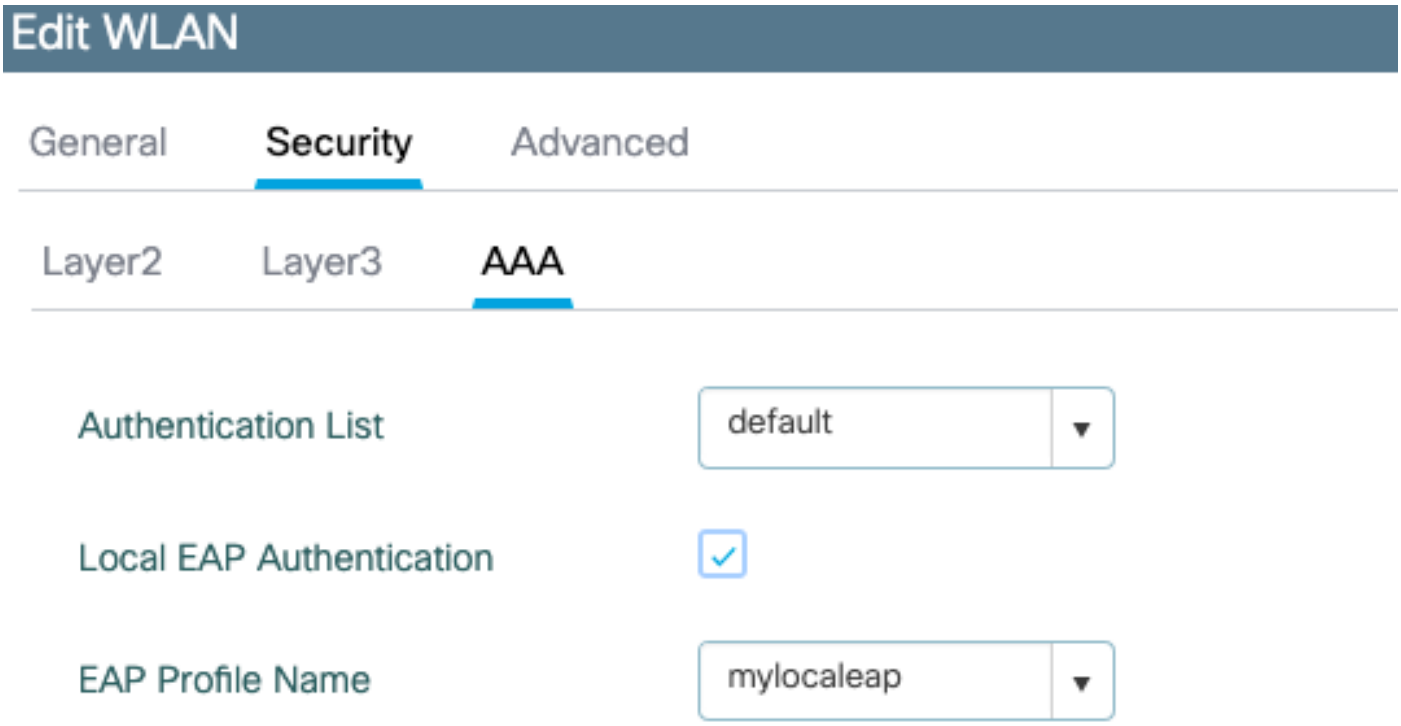
转至Configuration > Tags and Profiles > WLANs > + Add >

提供SSID和配置文件名称。

默认情况下，在第2层下选择Dot1x security。

在AAA下，选择Local EAP Authentication，然后从下拉列表中选择Local EAP profile和AAA Authentication list。


Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Adaptive Enabled
Over the DS
Reassociation Timeout
20
MPSK Configuration
MPSK




```
(config)#wlan localpeapssid 1 localpeapssid
(config-wlan)#security dot1x authentication-list default
(config-wlan)#local-auth mylocaleap
```

步骤6.创建一个或多个用户

在CLI中，用户必须是network-user类型。以下是在CLI中创建的用户示例：

```
(config)#user-name 1xuser
 creation-time 1572730075
 description 1xuser
 password 0 Cisco123
 type network-user description 1xuser
```

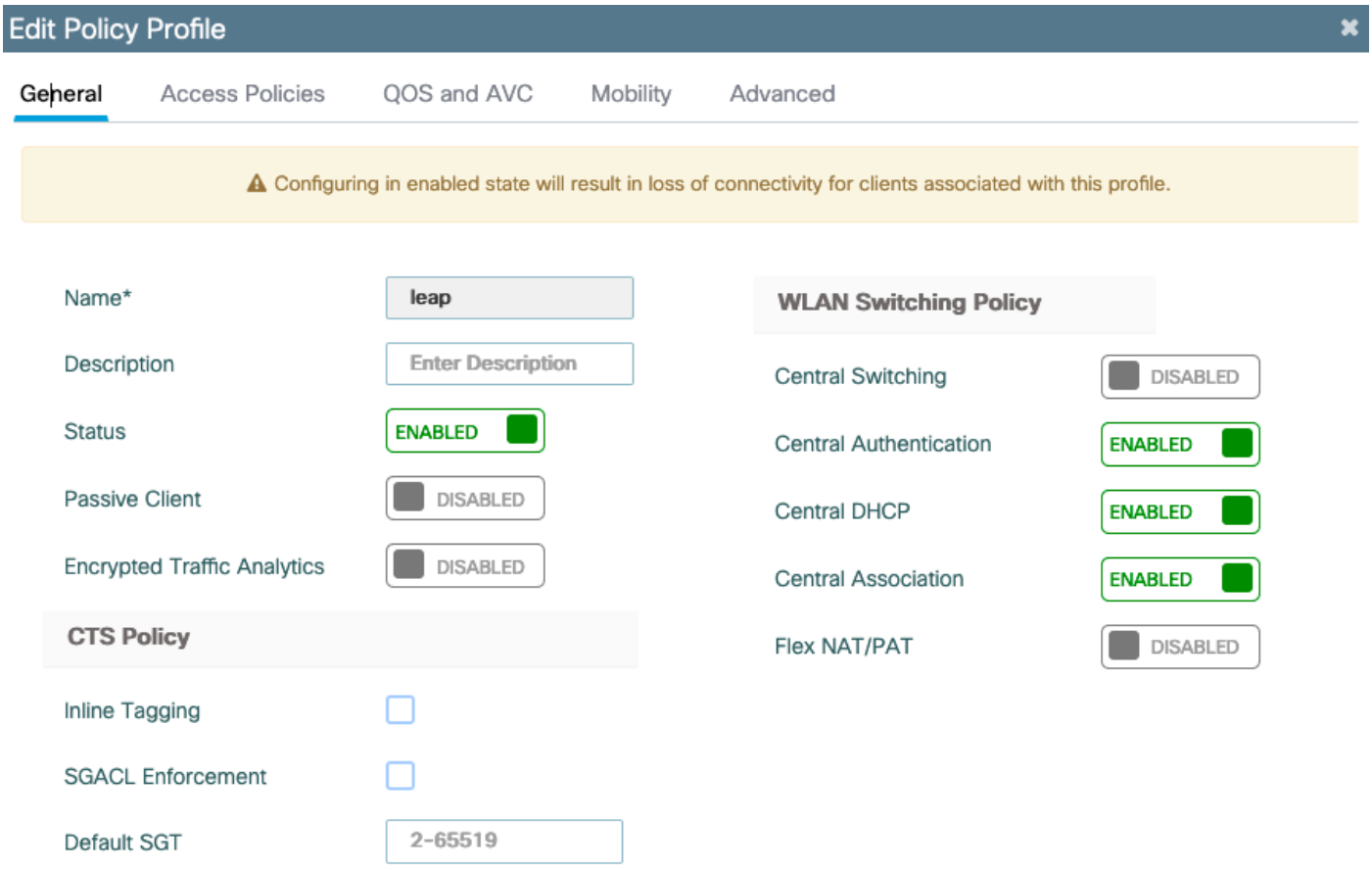
在CLI中创建后，此用户在Web UI中可见，但如果在Web UI中创建，则没有方法使其成为network-user（截至16.12）

步骤7.创建策略配置文件。创建策略标记以将此WLAN配置文件映射到策略配置文件

转到Configuration > Tags and profiles > Policy

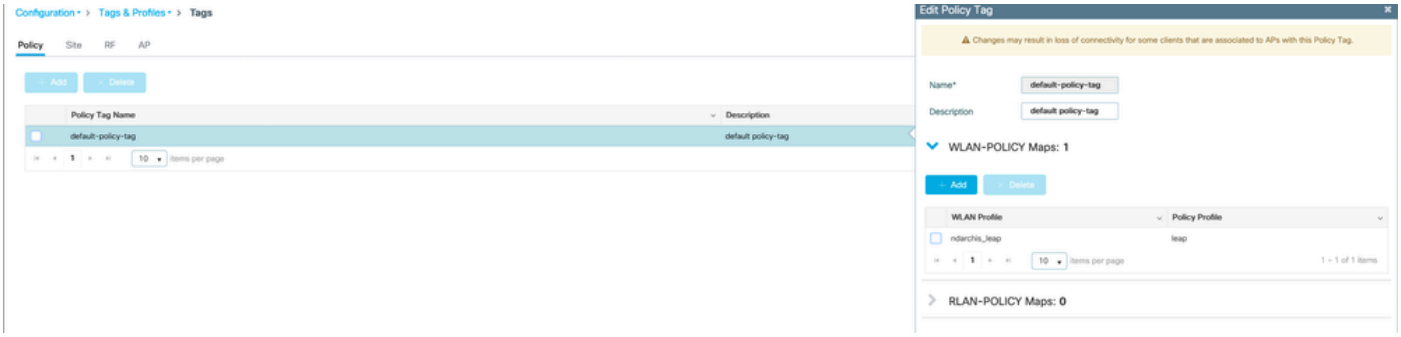
为WLAN创建策略配置文件。

此示例显示了flexconnect本地交换，但vlan 1468上存在中央身份验证方案，但这取决于您的网络。



转至Configuration > Tags and profiles > Tags

将您的WLAN分配给标记内的策略配置文件。



步骤8.将策略标记部署到接入点。

在这种情况下，对于单个AP，您可以直接在AP上分配标记。

转至Configuration > Wireless >Access points，然后选择要配置的AP。

确保分配的标签是您配置的标签。

验证

主要配置行如下所示：

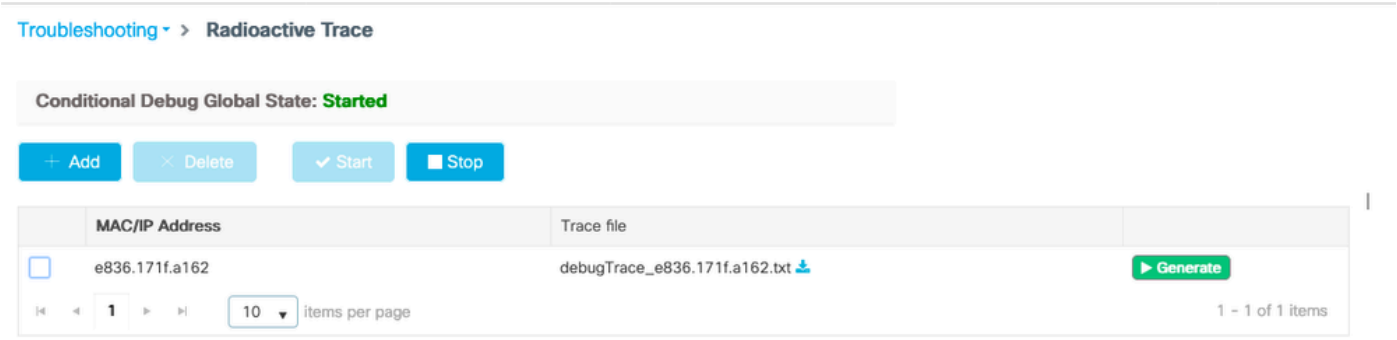
```
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download default local
aaa local authentication default authorization default
eap profile mylocaleap
method peap
pki-trustpoint admincert
user-name 1xuser
creation-time 1572730075 description 1xuser
password 0 Cisco123
type network-user description 1xuser
wlan ndarchis_leap 1 ndarchis_leap
local-auth mylocaleap
security dot1x authentication-list default
no shutdown
```

故障排除

请注意，Cisco IOS® XE 16.12及更早版本仅支持TLS 1.0进行本地EAP身份验证，如果您的客户端越来越常用，仅支持TLS 1.2则可能导致问题。Cisco IOS® XE 17.1及更高版本支持TLS 1.2和TLS 1.0。

要对连接有故障的特定客户端进行故障排除，请使用RadioActive Tracing。转到故障排除>RadioActive跟踪并添加客户端mac地址。

选择Start为该客户端启用跟踪。



重现问题后，可以选择Generate按钮以生成包含调试输出的文件。

由于密码错误而无法连接的客户端示例

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
```

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.785 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAPV
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAST
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rai
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication faile
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

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）。