Configure Local EAP Authentication on Catalyst 9800 WLC

Contents

Introduction

This document describes the configuration of Local EAP on Catalyst 9800 WLCs (Wireless LAN Controllers).

Prerequisites

Requirements

This document describes the configuration of Local EAP (Extensible Authentication Protocol) on Catalyst 9800 WLCs; that is, the WLC perform as RADIUS authentication server for the wireless clients.

This document assumes you are familiar with the basic configuration of a WLAN on the 9800 WLC and only focuses on the WLC operating as Local EAP server for wireless clients.

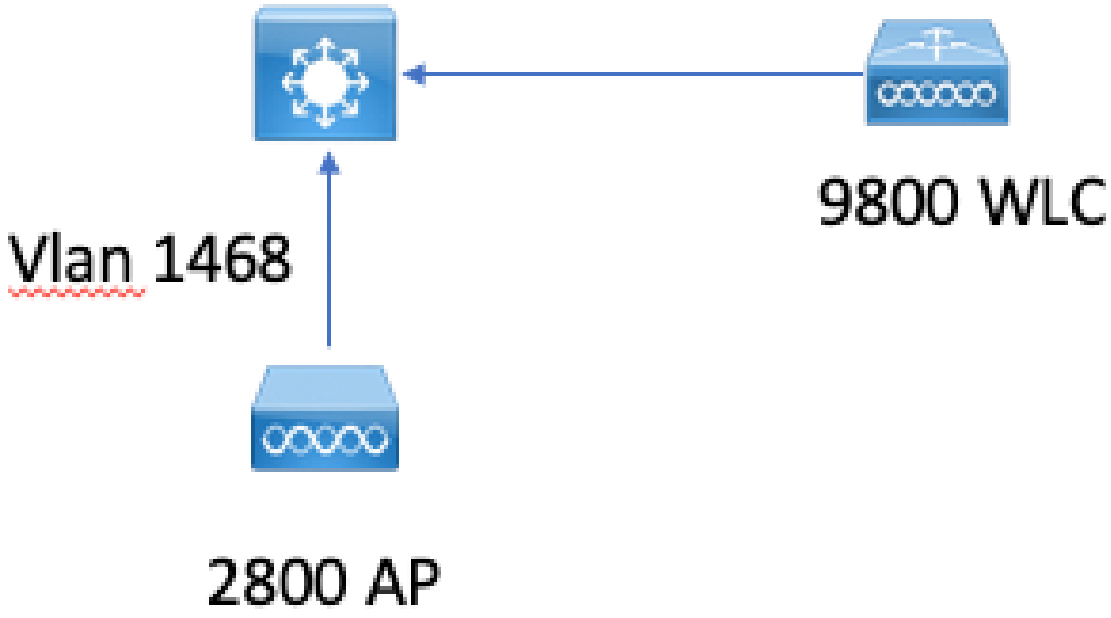
Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Catalyst 9800 on version 17.3.6

Configure

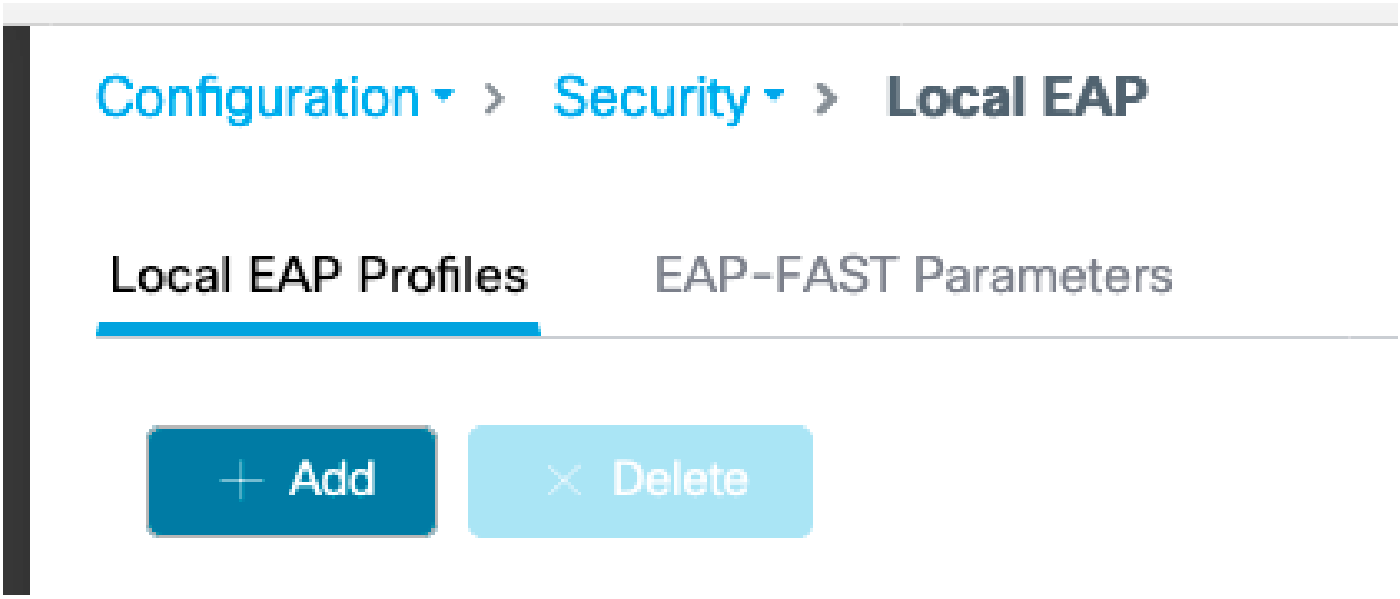
Network Diagram



Main Local EAP configuration

Step 1. Local EAP profile

Go to **Configuration > Security > Local EAP** in the 9800 web UI.

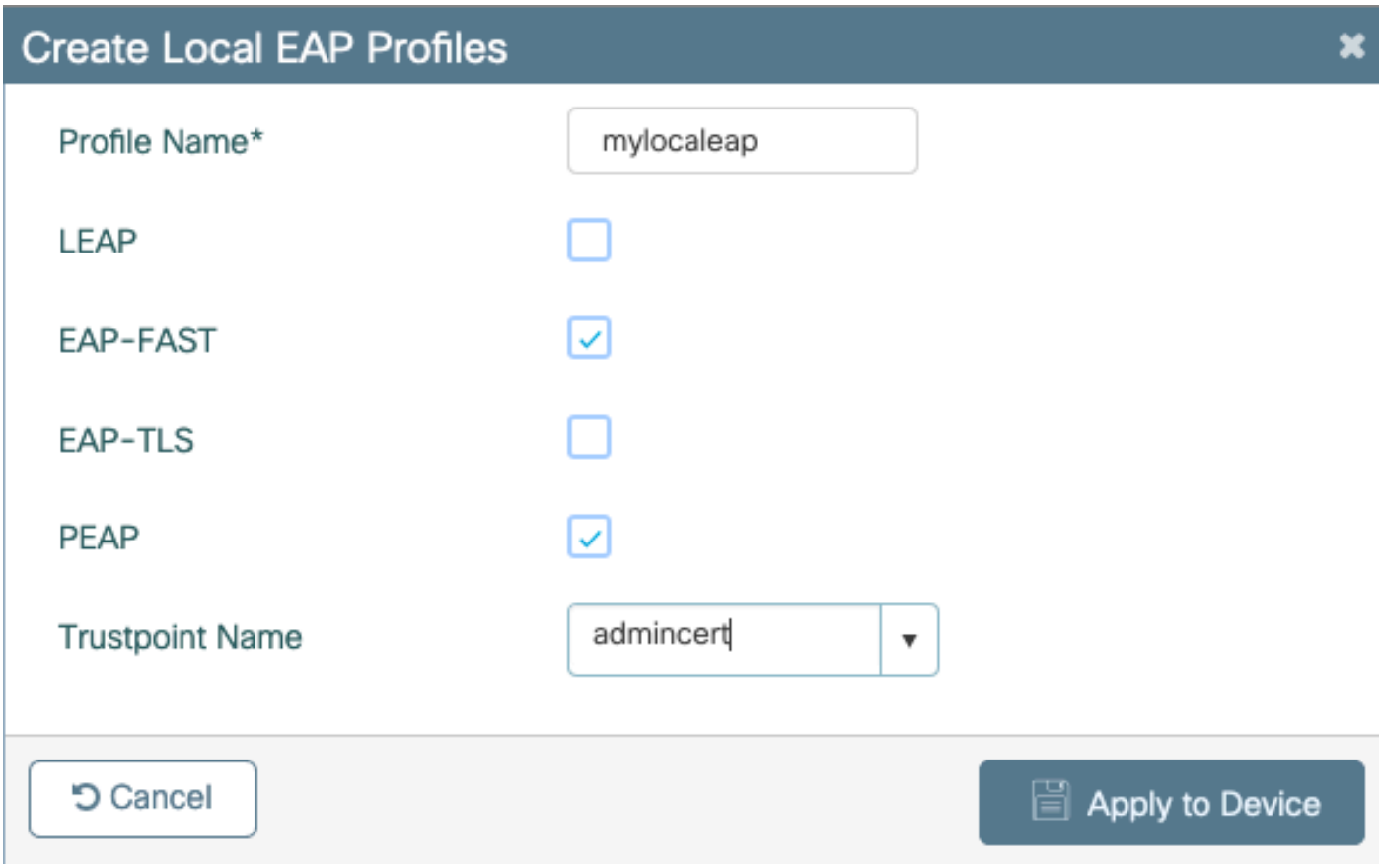


Select **Add**

Enter a profile name.

It is not advised to use LEAP at all due to its weak security. Any of the other 3 EAP methods requires you to configure a trustpoint. This is because the 9800, which acts as authenticator has to send a certificate for the client to trust it.

Clients do not trust the WLC default certificate, so you would need to deactivate server certificate validation on the client side (not advised) or install a certificate trustpoint on the 9800 WLC that the client trusts (or import it manually in the client trust store).



CLI:

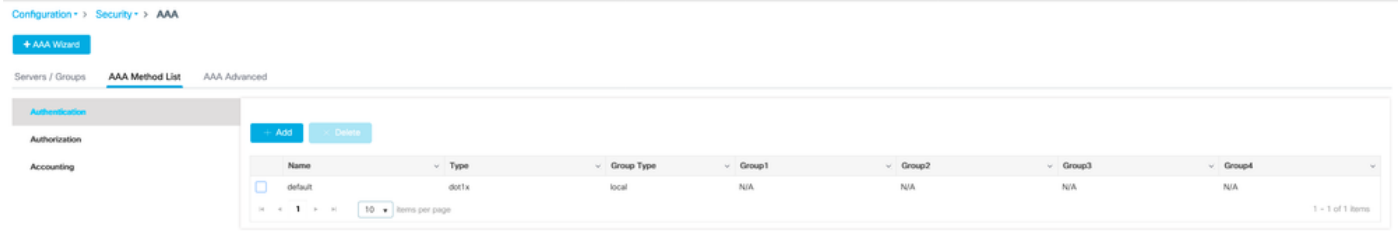
```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Step 2. AAA authentication method

You need to configure a AAA dot1x method that points locally as well in order to use the local database of users (but you could use external LDAP lookup for example).

Go to **Configuration> Security > AAA** and go to the **AAA method list** tab for **Authentication**. Select **Add.**

Choose "dot1x" type and local group type.



Step 3. Configure a AAA authorization method

Go to **Authorization** sub-tab and create a new method for type **credential-download** and point it to local.

Do the same for **network** authorization type

CLI:

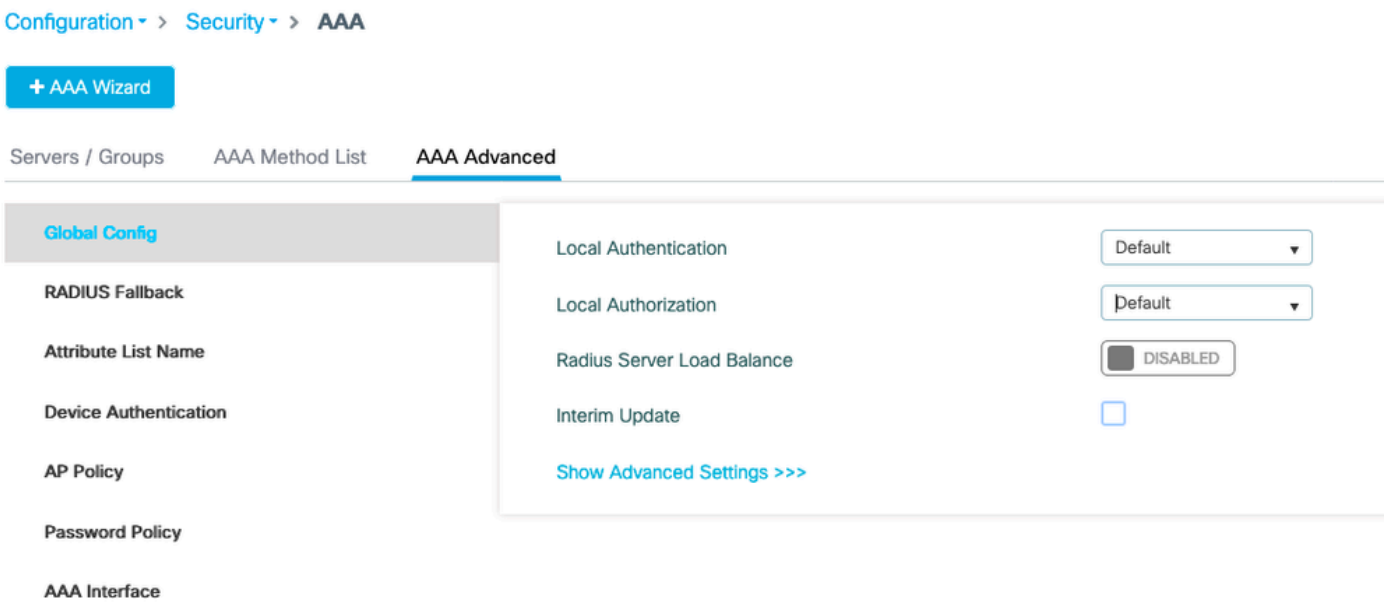
```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

Step 4. Configure local advanced methods

Go to the **AAA advanced** tab.

Define the local authentication and authorization method. Since this exampled used the "default" credential-download and "Default" dot1x method, you need to set default for both local authentication and authorization drop down boxes here.

In case you defined named methods, pick "method list" in the dropdown and another field allows you to enter your method name.



CLI:

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

Step 5. Configure a WLAN

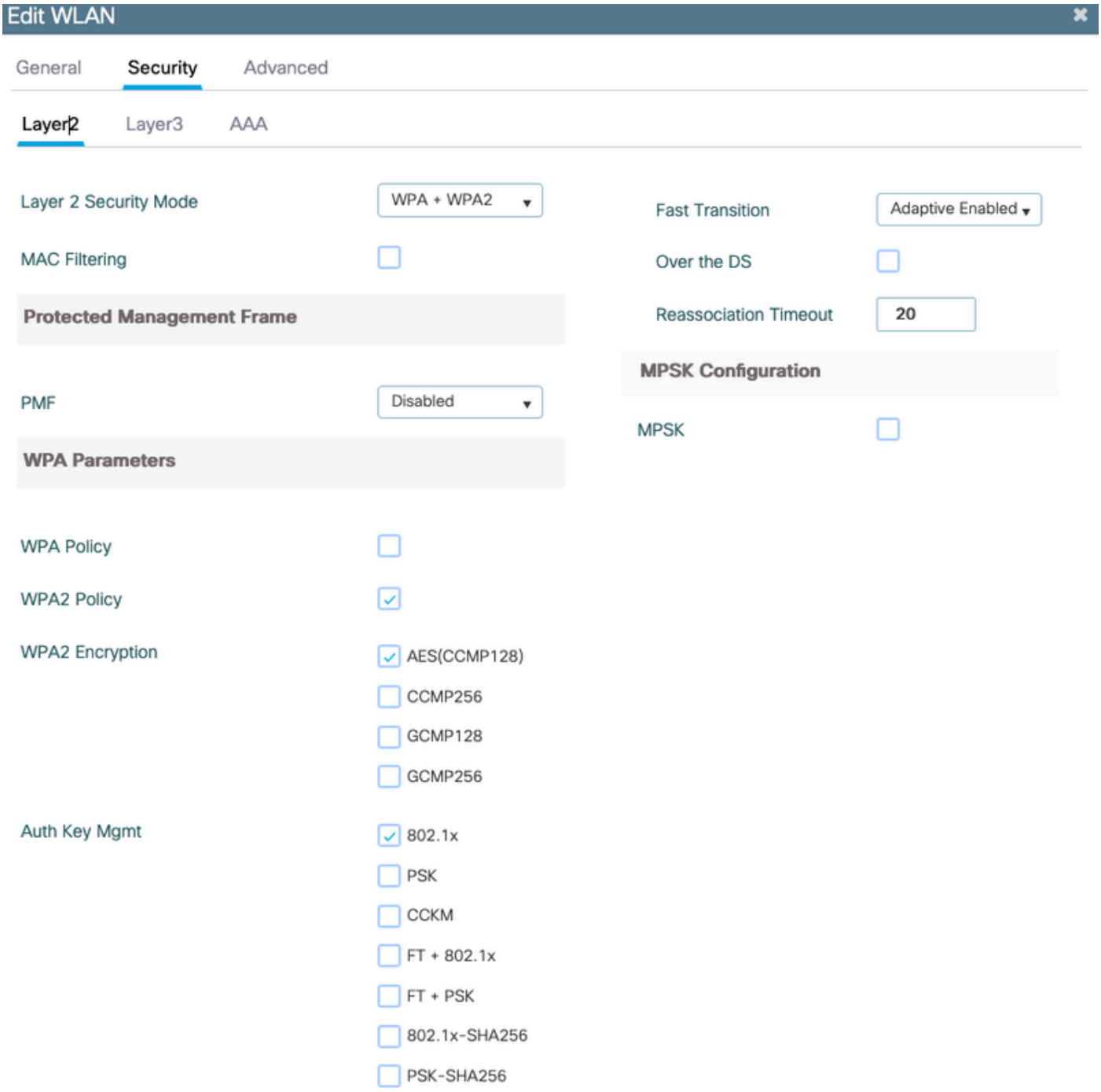
You can then configure your WLAN for 802.1x security against the local EAP profile and AAA authentication method defined in the previous step.

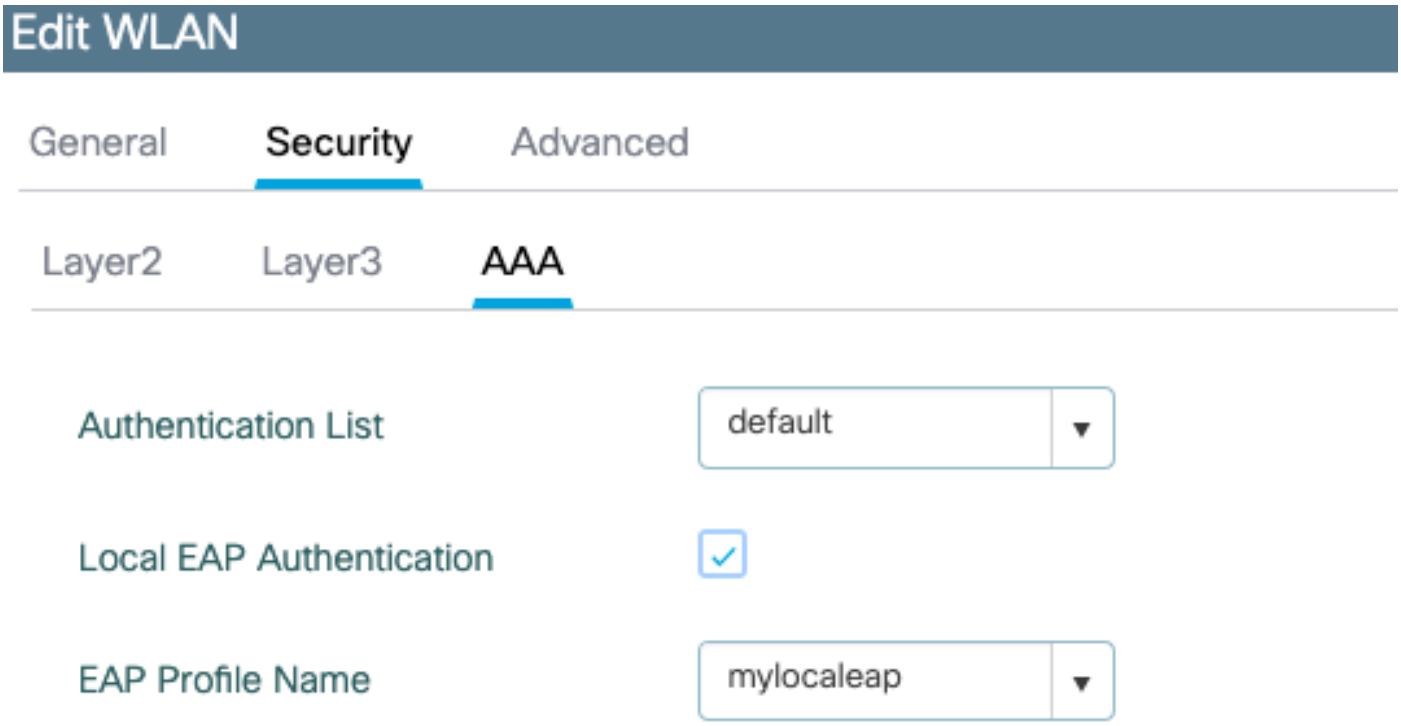
Go to Configuration > Tags and Profiles > WLANs > + Add >

Provide SSID and Profile Name.

Dot1x security is selected by default under Layer 2.

Under AAA, select Local EAP Authentication and choose Local EAP profile and AAA Authentication list from drop-down.


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
```

Step 6. Create one or more users

In CLI, the users have to be of type **network-user.** Here is an example user created in CLI:

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

Once created in CLI, this user is visible in the web UI, but if created in the web UI, there are no methods to make it a **network-user** as of 16.12

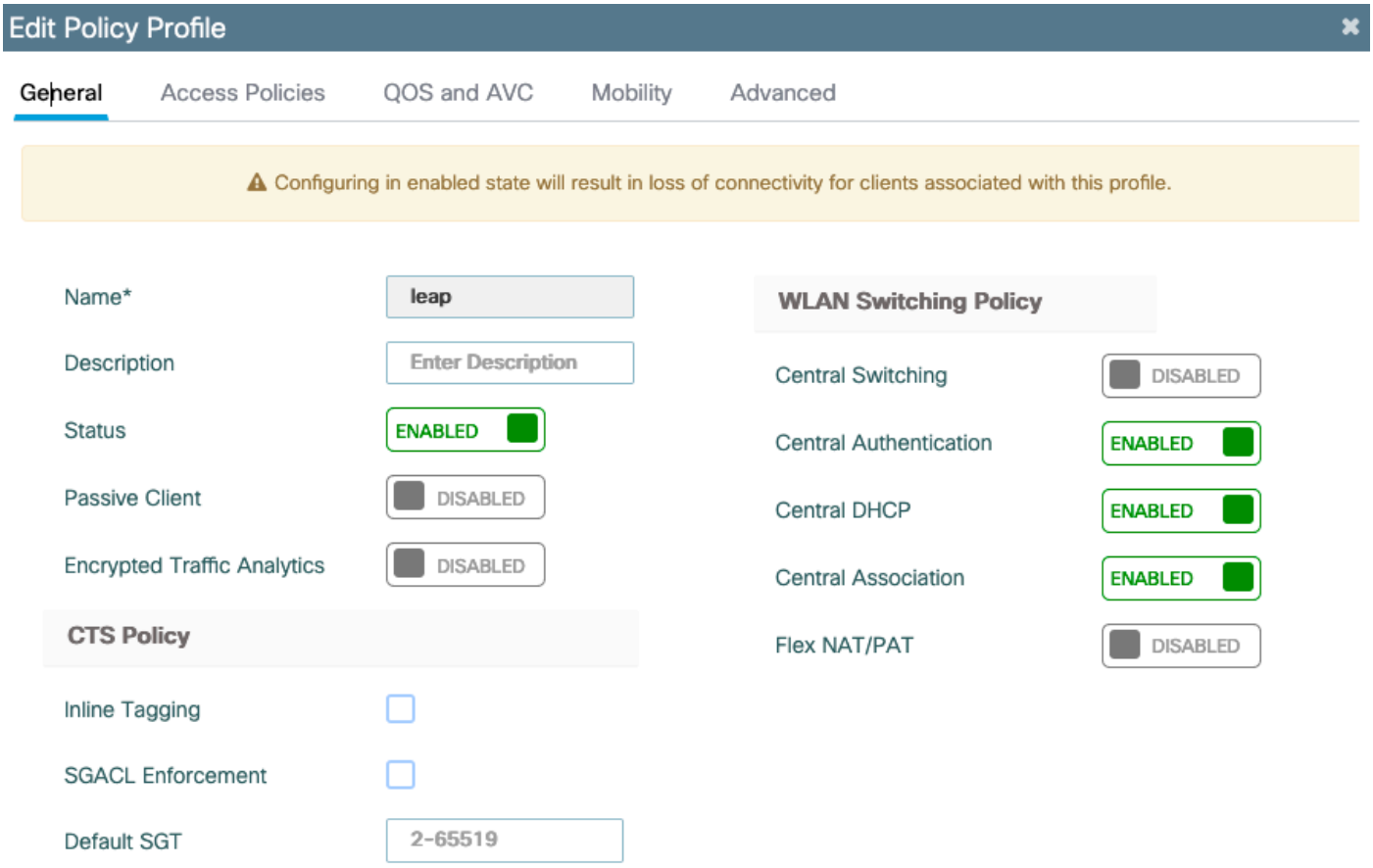
Step 7. Create policy profile. Create policy tag to map this WLAN profile to policy profile

Go **Configuration > Tags and profiles > Policy**

Create a policy profile for your WLAN.

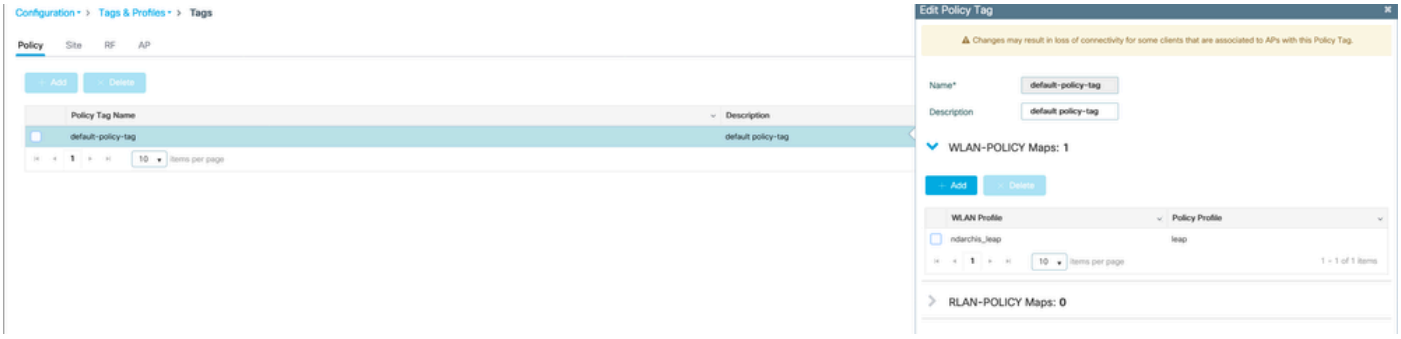
This example shows a flexconnect local switching but central authentication scenario on vlan 1468 but this

depends on your network.



Go to **Configuration> Tags and profiles > Tags**

Assign your WLAN to a policy profile inside your tag.



Step 8. Deploy the policy tag to Access Points.

In this case, for a single AP, you can assign the tags directly on the AP.

Go to **Configuration > Wireless >Access points** and select the AP you want to configure.

Make sure the tags assigned are the ones you configured.

Verify

The main configuration lines are as shown:

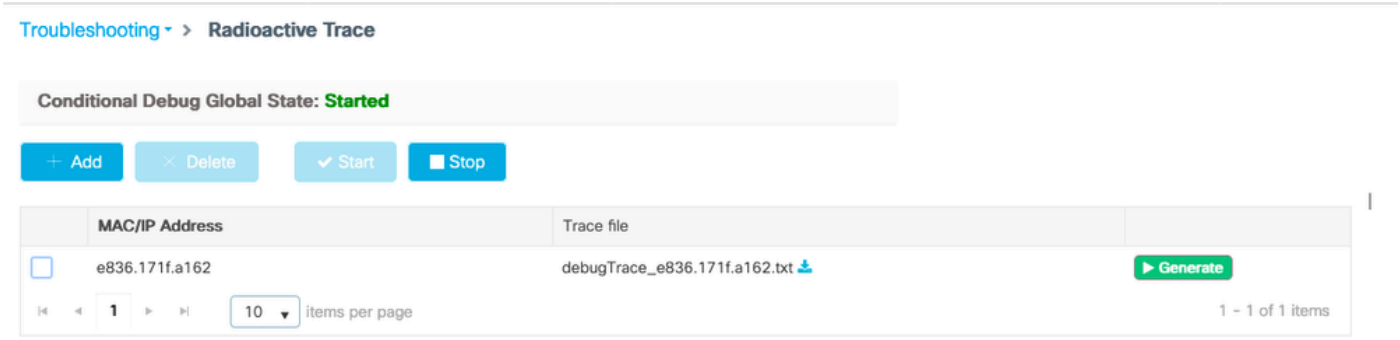
```
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download default local
aaa local authentication default authorization default
eap profile mylocaleap
method peap
pki-trustpoint admincert
user-name 1xuser
creation-time 1572730075 description 1xuser
password 0 Cisco123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

Troubleshoot

Note that Cisco IOS® XE 16.12 and earlier releases only support TLS 1.0 for local eap authentication which could cause issues if your client supports only TLS 1.2 as is more and more the norm. Cisco IOS® XE 17.1 and later support TLS 1.2 and TLS 1.0.

In order to troubleshoot a specific client which has trouble connecting, use RadioActive Tracing. Go to **Troubleshooting > RadioActive Trace** and add the client mac address.

Select **Start** to enable the tracing for that client.



Once the problem is reproduced, you can select the **Generate** button in order to produce a file that contains the debugging output.

Example of a client that fails to connect due to wrong password

```
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:
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 MSCHAP
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-FAS
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
```