

Configuración de la autenticación EAP local en el WLC de Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración EAP local principal](#)

[Paso 1. Perfil EAP local](#)

[Paso 2. método de autenticación AAA](#)

[Paso 3. Configuración de un método de autorización AAA](#)

[Paso 4. Configurar métodos avanzados locales](#)

[Paso 5. Configuración de una WLAN](#)

[Paso 6. Crear uno o varios usuarios](#)

[Paso 7. Crear perfil de directiva. Cree una etiqueta de política para asignar este perfil WLAN al perfil de política](#)

[Paso 8. Implemente la etiqueta de directiva en los puntos de acceso.](#)

[Verificación](#)

[Troubleshoot](#)

[Ejemplo de un cliente que no puede conectarse debido a una contraseña incorrecta](#)

Introducción

Este documento describe la configuración de EAP local en WLC Catalyst 9800 (Wireless LAN Controllers).

Prerequisites

Requirements

Este documento describe la configuración de EAP local (protocolo de autenticación extensible) en WLC Catalyst 9800; es decir, el WLC funciona como servidor de autenticación RADIUS para los clientes inalámbricos.

Este documento asume que usted está familiarizado con la configuración básica de una WLAN en el WLC 9800 y se centra solamente en el WLC que funciona como servidor EAP local para los clientes inalámbricos.

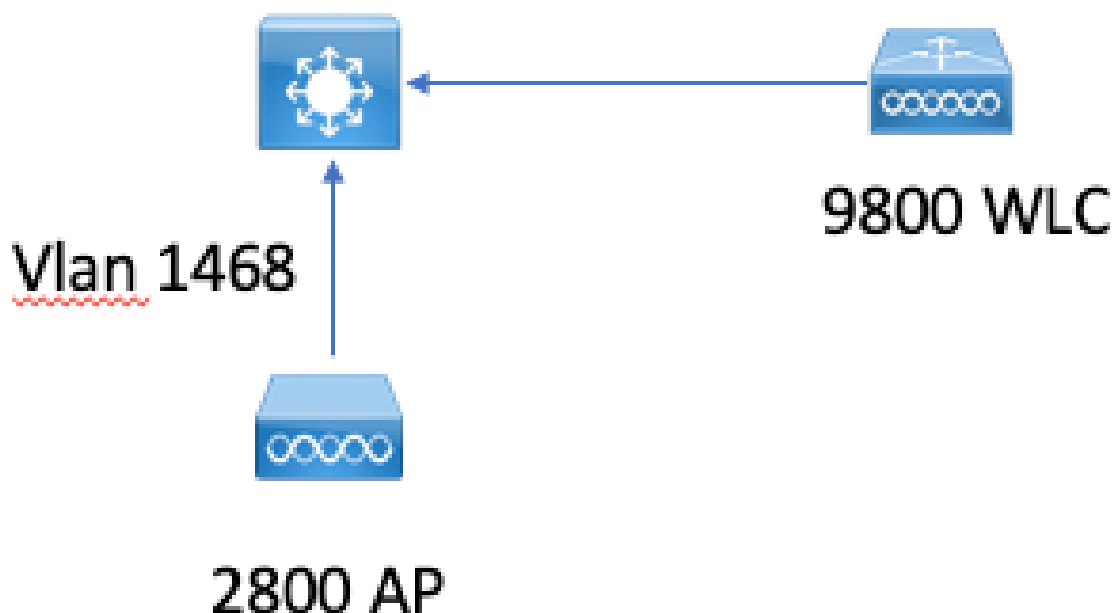
Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Catalyst 9800 en la versión 17.3.6

Configurar

Diagrama de la red



Configuración EAP local principal

Paso 1. Perfil EAP local

Vaya a Configuration > Security > Local EAP en la interfaz de usuario web de 9800.

Configuration > Security > Local EAP

Local EAP Profiles

EAP-FAST Parameters

+ Add

× Delete

Seleccione Agregar

Introduzca un nombre de perfil.

No se recomienda utilizar LEAP en absoluto debido a su débil seguridad. Cualquiera de los otros 3 métodos EAP requiere que configure un punto de confianza. Esto se debe a que el 9800, que actúa como autenticador, tiene que enviar un certificado para que el cliente confíe en él.

Los clientes no confían en el certificado predeterminado del WLC, por lo que tendría que desactivar la validación del certificado del servidor en el lado del cliente (no recomendado) o instalar un punto de confianza del certificado en el WLC 9800 en el que el cliente confía (o importarlo manualmente en el almacén de confianza del cliente).

✕

Create Local EAP Profiles

Profile Name*

LEAP

EAP-FAST

EAP-TLS

PEAP

Trustpoint Name ▼

↶ Cancel

📄
Apply to Device

CLI:

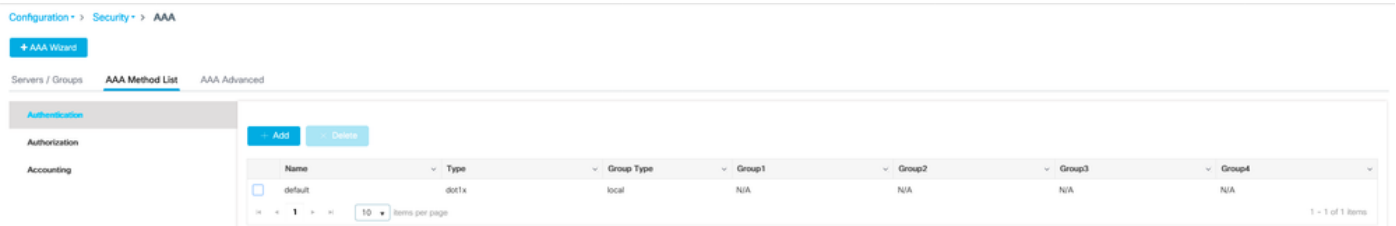
```
(config)#eap profile mylocaleap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Paso 2. método de autenticación AAA

Debe configurar un método dot1x AAA que apunte localmente también para utilizar la base de datos local de usuarios (pero podría utilizar búsqueda LDAP externa, por ejemplo).

Vaya a Configuration > Security > AAA y vaya a la pestaña AAA method list para la autenticación. Seleccione Agregar.

Elija el tipo "dot1x" y el tipo de grupo local.



Paso 3. Configuración de un método de autorización AAA

Vaya a la subficha Authorization y cree un nuevo método para el tipo credential-download y señale al local.

Haga lo mismo para el tipo de autorización de red

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
```

Paso 4. Configurar métodos avanzados locales

Vaya a la pestaña avanzada AAA.

Defina el método de autenticación y autorización local. Dado que en este ejemplo se utilizó el método "default" credential-download y "Default" dot1x, debe establecer el valor predeterminado para los cuadros desplegables de autenticación y autorización locales aquí.

En caso de que haya definido métodos con nombre, seleccione "lista de métodos" en el menú desplegable y otro campo le permitirá introducir el nombre del método.

[Configuration](#) > [Security](#) > [AAA](#)

[+ AAA Wizard](#)

[Servers / Groups](#)

[AAA Method List](#)

[AAA Advanced](#)

[Global Config](#)

[RADIUS Fallback](#)

[Attribute List Name](#)

[Device Authentication](#)

[AP Policy](#)

[Password Policy](#)

[AAA Interface](#)

Local Authentication

Default

Local Authorization

Default

Radius Server Load Balance

DISABLED

Interim Update

[Show Advanced Settings >>>](#)

CLI:

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

Paso 5. Configuración de una WLAN

A continuación, puede configurar su WLAN para la seguridad 802.1x con el perfil EAP local y el método de autenticación AAA definidos en el paso anterior.

Vaya a Configuration > Tags and Profiles > WLAN > + Add >

Proporcione SSID y nombre de perfil.

La seguridad Dot1x está seleccionada de forma predeterminada en la capa 2.

En AAA, seleccione Autenticación EAP local y elija Perfil EAP local y Lista de autenticación AAA en el menú desplegable.

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

Fast Transition Adaptive Enabled ▼

MAC Filtering

Over the DS

Protected Management Frame

Reassociation Timeout 20

PMF Disabled ▼

MPSK Configuration

WPA Parameters

MPSK

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

Edit WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List

default



Local EAP Authentication



EAP Profile Name

mylocaleap



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

Paso 6. Crear uno o varios usuarios

En CLI, los usuarios deben ser del tipo usuario-red. A continuación se muestra un ejemplo de usuario creado en CLI:

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

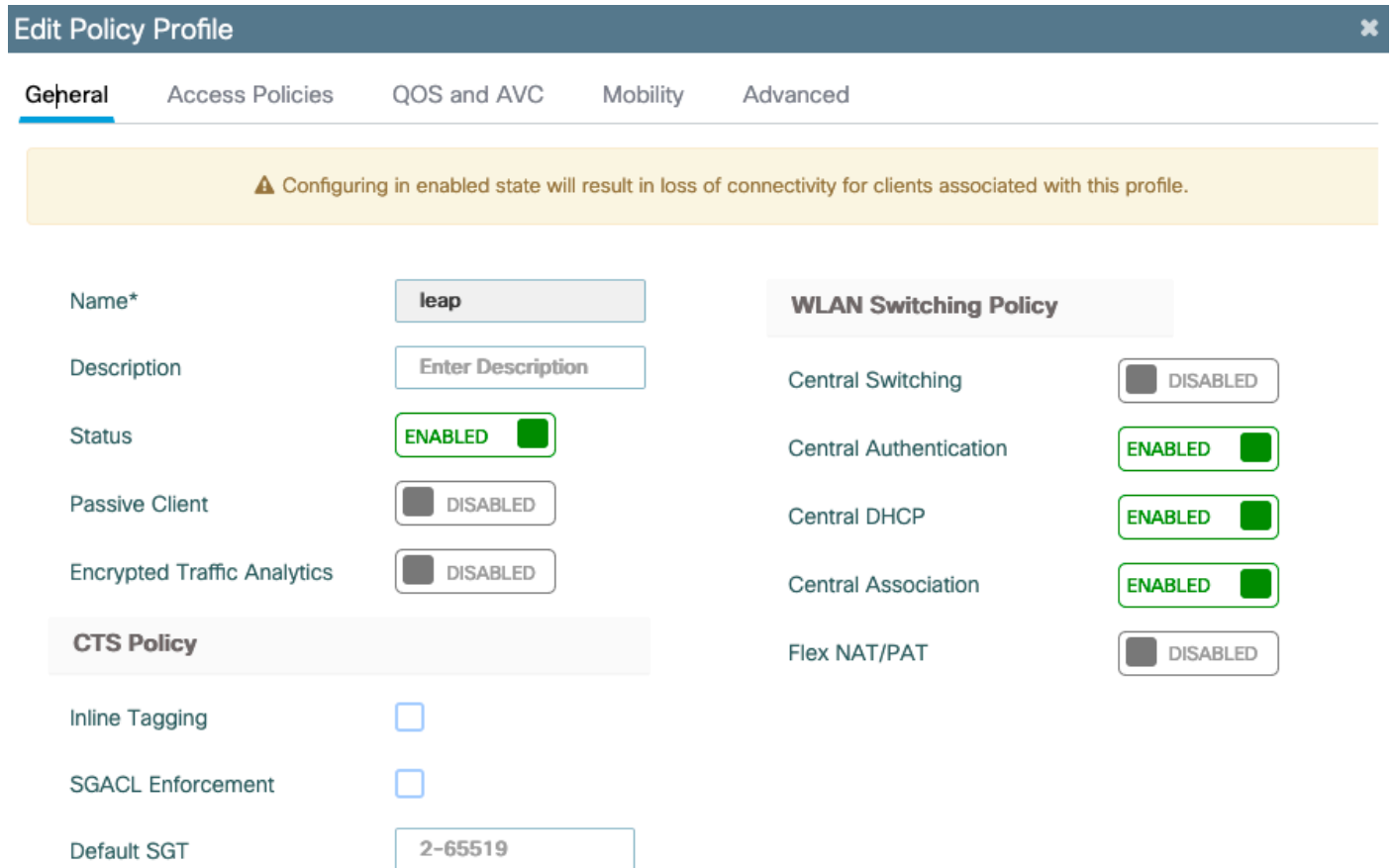
Una vez creado en CLI, este usuario es visible en la interfaz de usuario web, pero si se crea en la interfaz de usuario web, no hay métodos para convertirlo en un usuario de red a partir de 16.12

Paso 7. Crear perfil de directiva. Cree una etiqueta de política para asignar este perfil WLAN al perfil de política

Vaya a Configuration > Tags and profiles > Policy

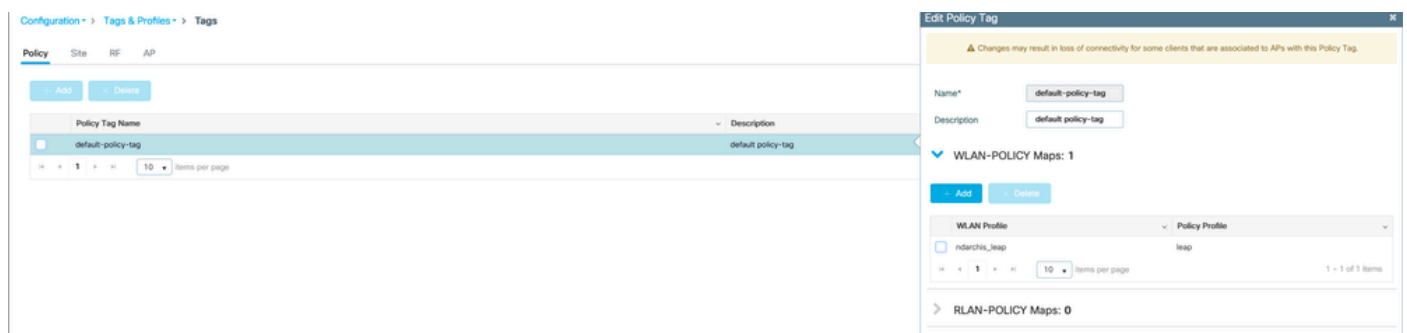
Cree un perfil de políticas para su WLAN.

Este ejemplo muestra un escenario de conmutación local flexconnect pero autenticación central en vlan 1468, pero esto depende de su red.



Vaya a Configuración > Etiquetas y perfiles > Etiquetas

Asigne su WLAN a un perfil de política dentro de su etiqueta.



Paso 8. Implemente la etiqueta de directiva en los puntos de acceso.

En este caso, para un solo AP, puede asignar las etiquetas directamente en el AP.

Vaya a Configuration > Wireless > Access points y seleccione el AP que desea configurar.

Asegúrese de que las etiquetas asignadas son las que ha configurado.

Verificación

Las líneas de configuración principales son las siguientes:

```
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

Tenga en cuenta que Cisco IOS® XE 16.12 y las versiones anteriores sólo admiten TLS 1.0 para la autenticación eap local, lo que podría causar problemas si su cliente sólo admite TLS 1.2, ya que es cada vez más la norma. Cisco IOS® XE 17.1 y versiones posteriores admiten TLS 1.2 y TLS 1.0.

Para resolver problemas de un cliente específico que tiene problemas de conexión, utilice el seguimiento de RadioActive. Vaya a Troubleshooting > RadioActive Trace y agregue la dirección MAC del cliente.

Seleccione Start para habilitar el seguimiento para ese cliente.

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Started**

[+ Add](#) [x Delete](#) [✓ Start](#) [■ Stop](#)

	MAC/IP Address	Trace file	
<input type="checkbox"/>	e836.171f.a162	debugTrace_e836.171f.a162.txt 📄	▶ Generate

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

Una vez que se reproduzca el problema, puede seleccionar el botón Generate para generar un

archivo que contenga el resultado de la depuración.

Ejemplo de un cliente que no puede conectarse debido a una contraseña incorrecta

```
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}: [caaaa-authen] [23294]: (info): [CAAAA: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}: [caaaa-authen] [23294]: (info): [CAAAA: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}: [caaaa-authen] [23294]: (info): [CAAAA: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}: [caaaa-authen] [23294]: (info): [CAAAA: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}: [caaaa-authen] [23294]: (info): [CAAAA: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}: [caaaa-authen] [23294]: (info): [CAAAA: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] /
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).