

Configuración de suplicante 802.1X para puntos de acceso con controlador 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración del LAP como Suplicante 802.1x](#)

[Si el AP ya está unido al WLC:](#)

[Si el AP no se ha unido a un WLC todavía:](#)

[Configuración del switch](#)

[Configuración del servidor ISE](#)

[Verificación](#)

[Verifique el tipo de autenticación](#)

[Verifique 802.1x en el puerto del switch](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar un punto de acceso (AP) de Cisco como un suplicante 802.1x para ser autorizado en un puerto de switch contra un servidor RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de LAN inalámbrica (WLC) y LAP (Lightweight Access Point).
- 802.1x en switches Cisco e ISE
- Protocolo de autenticación extensible (EAP)
- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WS-C3560CX, Cisco IOS® XE, 15.2(3r)E2
- C9800-CL-K9, Cisco IOS® XE, 17.6.1
- ISE 3.0
- AIR-CAP3702
- AP3802 AIR

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.

Antecedentes

En esta configuración, el punto de acceso (AP) actúa como suplicante de 802.1x y el switch lo autentica frente a ISE con el método EAP-FAST.

Una vez configurado el puerto para la autenticación 802.1X, el switch no permite que ningún tráfico que no sea el tráfico 802.1X pase a través del puerto hasta que el dispositivo conectado al puerto se autentique correctamente.

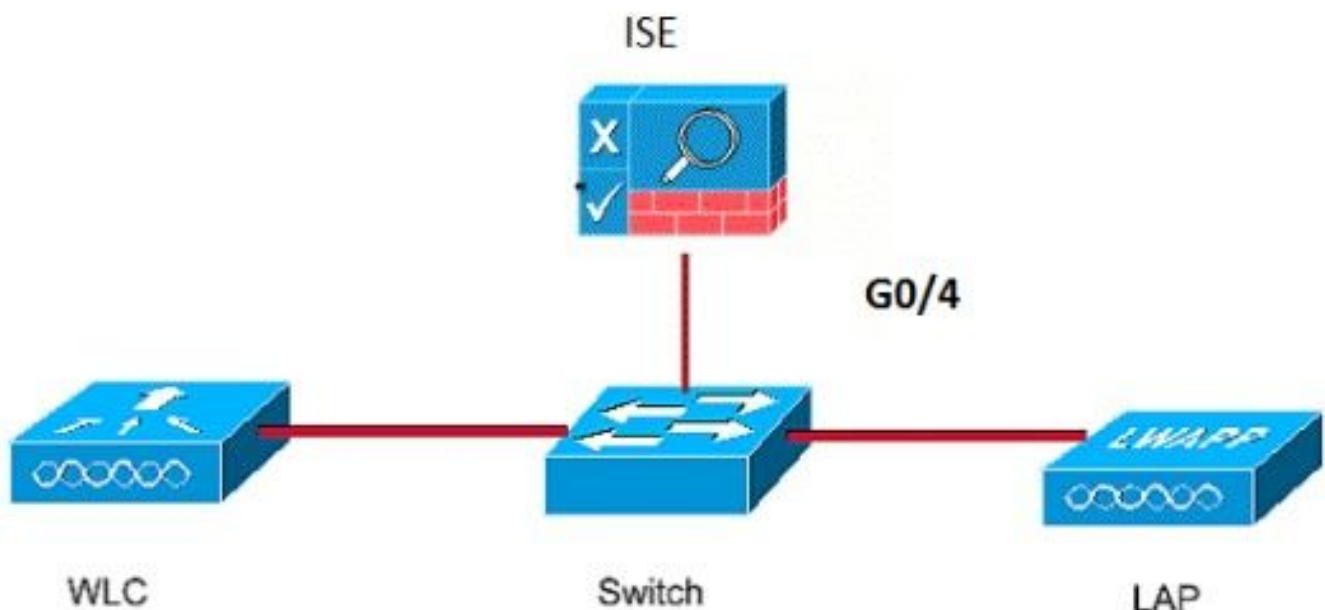
Un AP se puede autenticar antes de que se una a un WLC o después de que se haya unido a un WLC, en cuyo caso usted configura 802.1X en el switch después de que el LAP se une al WLC.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

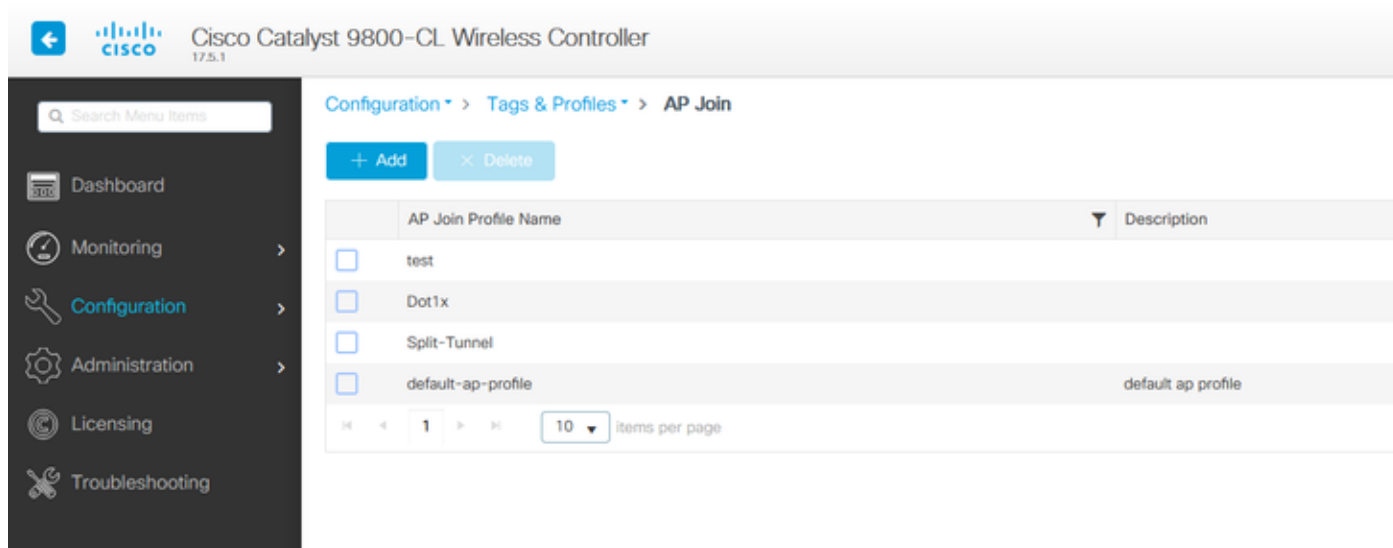


Configuración del LAP como Suplicante 802.1x

Si el AP ya está unido al WLC:

Configure el tipo de autenticación 802.1x y el tipo de autenticación de AP de certificado de significación local (LSC):

Paso 1. Navegue hasta Configuration > Tags & Profiles > AP Join > En la página AP Join Profile, haga clic en Add para agregar un nuevo perfil de unión o editar un perfil de unión AP cuando haga clic en su nombre.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The breadcrumb navigation is Configuration > Tags & Profiles > AP Join. There are '+ Add' and 'X Delete' buttons. A table lists AP Join Profiles:

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing '1' of 10 items per page.

Paso 2. En la página AP Join Profile, en AP > General, navegue hasta la sección AP EAP Auth Configuration. En la lista desplegable EAP Type, elija el tipo de EAP como EAP-FAST, EAP-TLS o EAP-PEAP para configurar el tipo de autenticación dot1x.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type Unknown ▾

Injector Switch MAC 00:00:00:00:00:00

Client Statistics Reporting Interval

5 GHz (sec) 90

2.4 GHz (sec) 90

AP EAP Auth Configuration

EAP Type EAP-FAST ▾

AP Authorization Type

- EAP-FAST
- EAP-TLS
- EAP-PEAP

Extended Module

Enable

Mesh

Profile Name mesh-profile ▾ [Clear](#)

Cancel Update & Apply to Device

Paso 3. En la lista desplegable **AP Authorization Type**, elija el tipo como CAPWAP DTLS + o CAPWAP DTLS > haga clic en **Update & Apply to Device**.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

AP EAP Auth Configuration

EAP Type

AP Authorization Type

- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

Extended Module

Enable

Mesh

Profile Name [Clear](#)

Configure el nombre de usuario y la contraseña de 802.1x:

Paso 1. Desde **Administración > Credenciales > Ingrese el nombre de usuario y la contraseña Dot1x > Elija el tipo de contraseña 802.1x apropiado > Haga clic en Actualizar y aplicar al dispositivo**

Edit AP Join Profile

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

Dot1x Credentials

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

Si el AP no se ha unido a un WLC todavía:

Usted debe consolar en el LAP para establecer las credenciales y utilizar estos comandos de CLI:
(para los APs Cheetah OS y Cisco IOS®)

CLI:

```
LAP# debug capwap console cli  
LAP# capwap ap dot1x username
```

Para Borrar Las Credenciales Dot1x En El AP (Si Es Necesario)

Para Cisco IOS® AP, después de eso recargue el AP:

CLI:

```
LAP# clear capwap ap dot1x
```

Para Cisco COS AP, después de eso recargue el AP:

CLI:

```
LAP# capwap ap dot1x disable
```

Configuración del switch

Habilite dot1x en el switch globalmente y agregue el servidor ISE al switch.

CLI:

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

Configure el puerto del switch AP.

CLI:

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

Si el AP está en el **modo Flex Connect, conmutación local**, se debe realizar una configuración adicional en la interfaz del switch para permitir varias direcciones MAC en el puerto, ya que el tráfico del cliente se libera en el nivel AP :

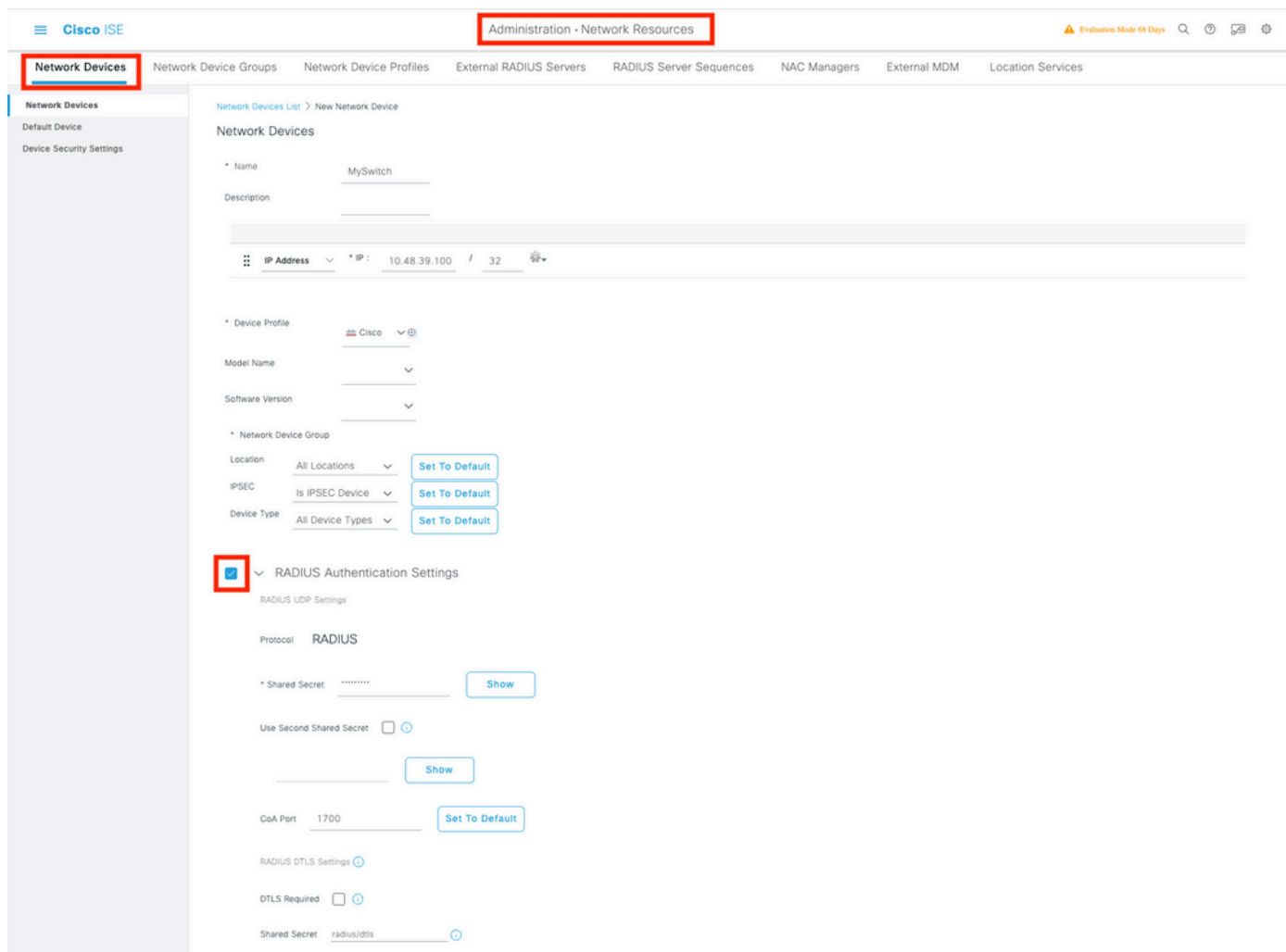
```
authentication host-mode multi-host
```

Nota: Significa que el lector toma nota. Las notas contienen sugerencias de gran ayuda o referencias a material que no se encuentra en el documento.

Nota: El modo de host múltiple autentica la primera dirección MAC y luego permite un número ilimitado de otras direcciones MAC. Habilite el modo de host en los puertos del switch si el AP conectado se ha configurado con el modo de conmutación local. Permite que el tráfico del cliente pase por el puerto del switch. Si desea una ruta de tráfico segura, habilite dot1x en la WLAN para proteger los datos del cliente

Configuración del servidor ISE

Paso 1. Agregue el switch como un dispositivo de red en el servidor ISE. Vaya a Administration > Network Resources > Network Devices > Click Add > Enter Device name, IP address, enable RADIUS Authentication Settings, Specify Shared Secret Value, COA port (o déjelo como predeterminado) > Submit.



Paso 2. Agregue las credenciales del punto de acceso a ISE. Navegue hasta Administration > Identity Management > Identities > Users y haga clic en el botón Add para agregar un usuario. Aquí debe ingresar las credenciales que configuró en su perfil de unión AP en su WLC. Tenga en cuenta que el usuario se coloca en el grupo predeterminado aquí, pero esto se puede ajustar según sus requisitos.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb navigation is 'Administration > Identity Management'. The 'Identities' tab is selected. On the left, the 'Users' section is visible. The main area shows the configuration for a user named 'dot1x' under the 'Network Access User' group. The user's status is 'Enabled'. Under the 'Passwords' section, the 'Password Type' is set to 'Internal Users'. The 'Login Password' field is highlighted with a red box. There are 'Generate Password' buttons for both the password and the 'Enable Password' field. Below the password section, there are expandable sections for 'User Information', 'Account Options', 'Account Disable Policy', and 'User Groups'. The 'User Groups' section shows 'ALL_ACCOUNTS (default)' selected.

Paso 3. En ISE, configure la **política de autenticación** y la **política de autorización**. Vaya a **Policy > Policy Sets** y seleccione el conjunto de políticas que desea configurar y la flecha azul a la derecha. En este caso, se utiliza el conjunto de políticas predeterminado, pero se puede personalizar según el requisito.

The screenshot shows the Cisco ISE Administration interface for Policy - Policy Sets. The breadcrumb navigation is 'Policy - Policy Sets'. The 'Policy Sets' section is visible. A table lists the policy sets. The 'Default' policy set is selected, and a blue arrow points to the right of its name. The table has columns for 'Status', 'Policy Set Name', 'Description', 'Conditions', 'Allowed Protocols / Server Sequence', 'Hits', 'Actions', and 'View'. The 'Default' policy set has a status of 'Default', a description of 'Default policy set', and is associated with 'Default Network Access'. There are 'Reset', 'Reset Policyset Hitcounts', and 'Save' buttons at the top and bottom of the table.

A continuación, configure la **política de autenticación** y la **política de autorización**. Las políticas que se muestran aquí son las políticas predeterminadas creadas en el servidor ISE, pero se pueden adaptar y personalizar según sus necesidades. En este ejemplo, la configuración se puede traducir a: "Si se utiliza 802.1X con cables y el usuario es conocido en el servidor ISE, entonces permitimos el acceso a los usuarios para los que la autenticación fue exitosa". El punto de acceso se autorizará entonces en el servidor ISE.

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	⚙️
●	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy (12)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions	
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	+	Select from list	+	6	⚙️
●	Default		DenyAccess x	+	Select from list	+	0	⚙️

Paso 4. Asegúrese de que en los protocolos permitidos en el acceso predeterminado a la red, EAP-FAST esté permitido. Vaya a Directiva > Elementos de directiva > Autenticación > Resultados > Protocolos permitidos > Acceso de red predeterminado > Habilitar EAP-TLS > Guardar.

Cisco ISE Policy - Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

- Authentication Bypass
 - Process Host Lookup
- Authentication Protocols
 - Allow PAP/ASCII
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - Allow EAP-MD5
 - Allow EAP-TLS

Expand: Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verifique el tipo de autenticación

El comando show muestra la información de autenticación de un perfil AP:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

Ejemplo:

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE   : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

Verifique 802.1x en el puerto del switch

El comando show muestra el estado de autenticación de 802.1x en el puerto del switch:

CLI:

```
Switch# show dot1x all
```

Ejemplo de salida:

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout         = 0
SuppTimeout           = 30
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
```

Verifique si el puerto ha sido autenticado o no

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

Ejemplo de salida:

```
Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout         = 0
SuppTimeout           = 30
ReAuthMax              = 2
MaxReq                 = 2
```

TxPeriod = 30

Dot1x Authenticator Client List

```
-----  
EAP Method = FAST  
Supplicant = f4db.e67e.dd16  
Session ID = 0A30279E00000BB7411A6BC4  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE
```

ED

Auth BEND SM State = IDLE

Desde CLI:

Switch#show authentication sessions

Ejemplo de salida:

```
Interface MAC Address Method Domain Status Fg Session ID  
Gi0/8 f4db.e67e.dd16 dot1x DATA Auth 0A30279E00000BB7411A6BC4
```

En ISE, elija **Operations > Radius LiveLogs** y confirme que la autenticación es correcta y que se envía el perfil de autorización correcto.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are several summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (0). Below these cards is a table of live logs. The table has columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, Authorization Profiles, IP Address, Network Device, and Device Port. One row is highlighted with a red border, showing a successful authentication session on Nov 28, 2022 at 08:33:34.4... with a status of 'Success' and a 'PermitAccess' authorization profile.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

1. Ingrese el comando **ping** para verificar si el servidor ISE es accesible desde el switch.
2. Asegúrese de que el switch esté configurado como cliente AAA en el servidor ISE.
3. Asegúrese de que el secreto compartido sea el mismo entre el switch y el servidor ISE.
4. Compruebe si EAP-FAST está activado en el servidor ISE.
5. Verifique si las credenciales 802.1x están configuradas para el LAP y son las mismas en el servidor ISE.

Nota: El nombre de usuario y la contraseña distinguen entre mayúsculas y minúsculas.

6. Si la autenticación falla, ingrese estos comandos en el switch: **debug dot1x** y **debug authentication**.

Tenga en cuenta que los puntos de acceso basados en Cisco IOS (802.11ac wave 1) no admiten las versiones 1.1 y 1.2 de TLS. Esto puede causar un problema si su servidor ISE o RADIUS está configurado para permitir solo TLS 1.2 dentro de la autenticación 802.1X.

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).