

Configuración del punto de acceso ligero como suplicante 802.1x

Introducción

Este documento describe cómo configurar un Lightweight Access Point (LAP) como suplicante 802.1x para autenticarse con el servidor de Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Wireless Lan Controller (WLC) y LAP
- 802.1x en switches Cisco
- ISE
- Protocolo de autenticación extensible (EAP): autenticación flexible mediante tunelación segura (FAST)

Componentes Utilizados

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

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE 2.0

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, make sure that you understand the potential impact of any command.

Antecedentes

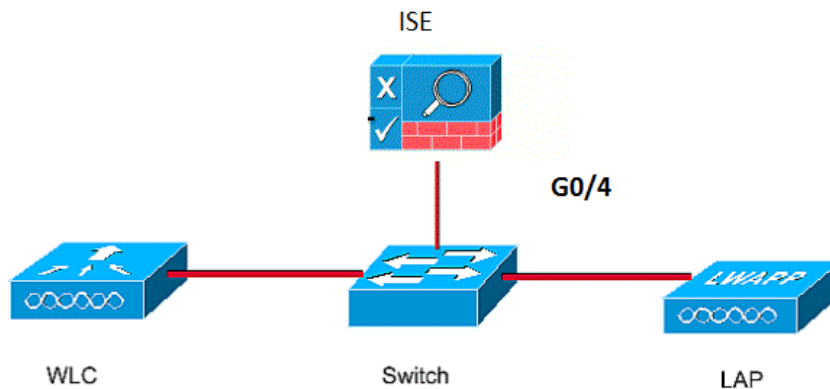
En esta configuración, el punto de acceso (AP) actúa como suplicante 802.1x y el switch lo autentica con respecto al ISE que utiliza EAP-FAST con aprovisionamiento de credenciales de acceso protegido (PAC) anónimas. Una vez que el puerto se configura para la autenticación 802.1x, el switch no permite que ningún tráfico que no sea 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 ha 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:



Configuraciones

Este documento utiliza estas direcciones IP:

- La dirección IP del switch es 10.48.39.141
- La dirección IP del servidor ISE es 10.48.39.161
- La dirección IP del WLC es 10.48.39.142

Configuración del LAP

En esta sección, se le presenta la información para configurar el LAP como un suplicante 802.1x.

1. Si el AP ya está unido al WLC, vaya a la pestaña Wireless y haga clic en el AP, vaya al campo Credentials y debajo del encabezado 802.1x Supplicant Credentials, marque la casilla de verificación **Over-ride Global Credentials** para establecer el nombre de usuario y la contraseña 802.1x para este AP.

The screenshot shows the Cisco WLC configuration interface for an AP. The 'Credentials' tab is selected, and the '802.1x Supplicant Credentials' section is expanded. The 'Over-ride Global credentials' checkbox is checked. The 'Username' field contains 'ritmahaj', and the 'Password' and 'Confirm Password' fields are masked with dots.

También puede establecer un nombre de usuario y una contraseña comunes para todos los AP que se unen al WLC con el menú Global Configuration

The screenshot shows the Cisco WLC configuration interface with the 'Global Configuration' menu item highlighted in the left sidebar. The main content area displays various configuration options for the AP, including 'Login Credentials', '802.1x Supplicant Credentials', 'TCP MSS', 'AP Retransmit Config Parameters', and 'OEAP Config Parameters'.

2. Si el AP todavía no se ha unido a un WLC, debe consolar en el LAP para establecer las credenciales y utilizar estos comandos CLI:

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

Configuración del switch

1. Active dot1x en el switch globalmente y agregue el servidor ISE al switch.

```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123A0C0411045D5679
```

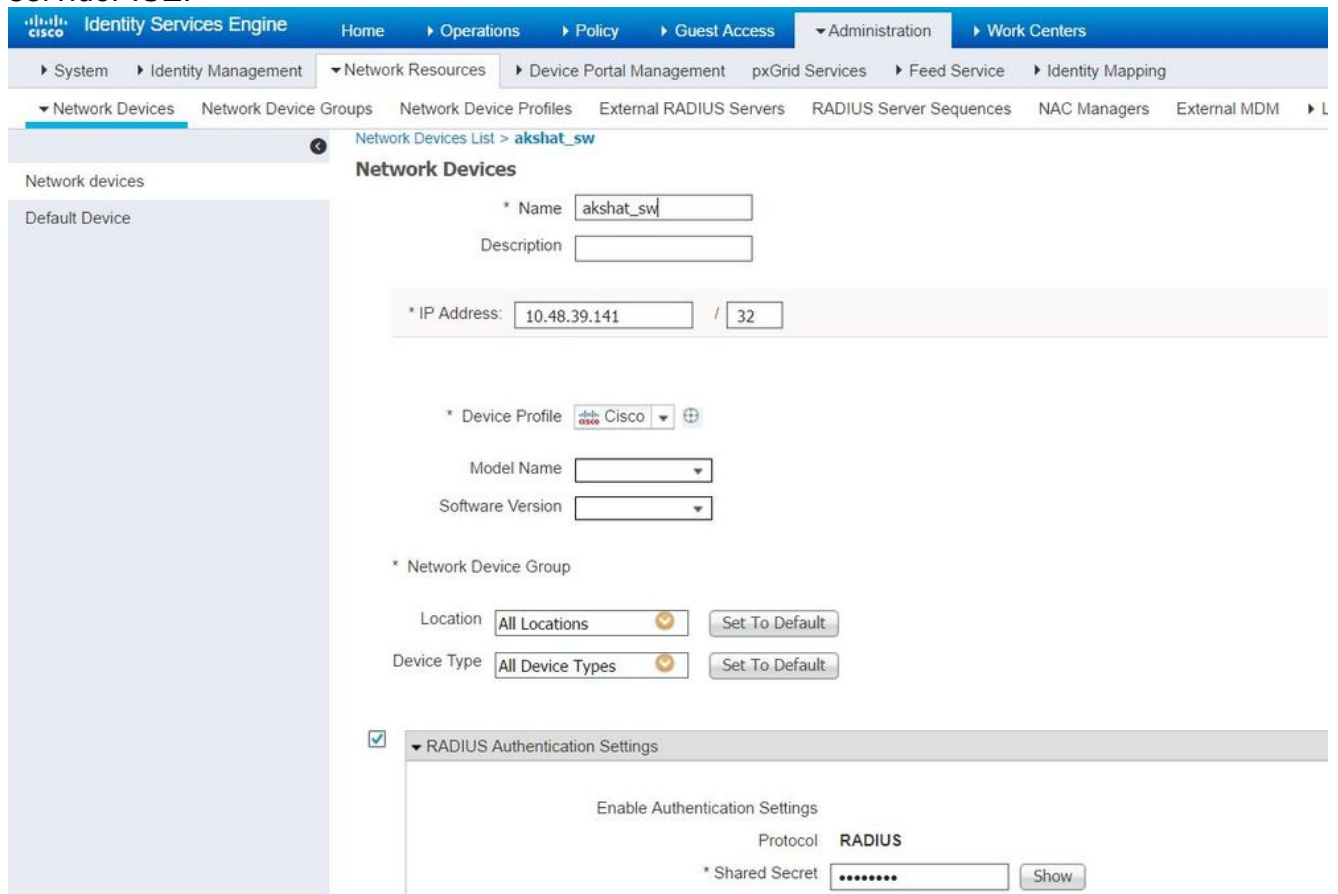
2. Ahora, configure el puerto del switch AP.

```
interface GigabitEthernet0/4

switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configuración del servidor ISE

1. Agregue el switch como cliente de autenticación, autorización y contabilidad (AAA) en el servidor ISE.



The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a Network Device. The page is titled "Network Devices" and shows the configuration for a device named "akshat_sw".

Configuration details include:

- Name: akshat_sw
- Description: (empty)
- IP Address: 10.48.39.141 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: Location: All Locations, Device Type: All Device Types
- RADIUS Authentication Settings: Enable Authentication Settings, Protocol: RADIUS, Shared Secret: (masked)

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location

Network devices

Default Device

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> GurpWLC1	10.48.39.155/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> GurpWLC2	10.48.39.156/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> akshat_sw	10.48.39.141/32	Cisco	All Locations	All Device Types

2. En ISE, configure la política de autenticación y la política de autorización. En este caso, se utiliza la regla de autenticación predeterminada que es Wired dot.1x, pero se puede personalizar según el requisito.

Identity Services Engine Home Operations Policy Guest Access Administration Work

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MAB Allow Protocols	: Default Network Access and
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X Allow Protocols	: Default Network Access and
<input checked="" type="checkbox"/>	Default	: use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

Asegúrese de que en los protocolos permitidos que Default Network Access , EAP-FAST esté permitido.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allow EAP-FAST

EAP-FAST Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries 3 (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries 3 (Valid Range 0 to 3)

Allow EAP-TLS

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

Use PACs Don't Use PACs

Tunnel PAC Time To Live 90 Days

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

Allow Anonymous In-Band PAC Provisioning

Allow Authenticated In-Band PAC Provisioning

Server Returns Access Accept After Authenticated Provisioning

Accept Client Certificate For Provisioning

3. En cuanto a la política de autorización (Port_AuthZ), en este caso se agregaron credenciales de AP a un grupo de usuarios (AP). La condición utilizada era "Si el usuario pertenece al grupo AP y hace un dot1x cableado, presione el acceso de permiso predeterminado del perfil de autorización". Una vez más, esto se puede personalizar según los requisitos.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

Create a New Rule

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > APs

Identity Group

Name APs

Description Credentials for APs

Save Reset

Member Users

Users Selected 0 | Total 1

Add Delete Show All

Status	Email	Username	First Name	Last Name
✓ Enabled		ritmahaj		

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Una vez que se habilita 802.1x en el puerto del switch, todo el tráfico, excepto el tráfico 802.1x, se bloquea a través del puerto. El LAP, que si ya está registrado en el WLC, se desasocia. Sólo después de una autenticación 802.1x exitosa se permite el paso de otro tráfico. El registro exitoso del LAP en el WLC después de que el 802.1x esté habilitado en el switch indica que la autenticación del LAP es exitosa. También puede utilizar estos métodos para verificar si el LAP se autenticó.

1. En el switch, ingrese uno de los comandos **show** para verificar si el puerto ha sido autenticado o no.

```
akshat_sw#show dot1x interface g0/4
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
akshat_sw#show dot1x interface g0/4 details
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
Dot1x Authenticator Client List
-----
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
```

```
akshat_sw#show authentication sessions
```

```
Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. En ISE, elija **Operations > Radius Livelogs** y vea que la autenticación es exitosa y que se presiona el perfil de autorización correcto.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below this, there are tabs for 'RADIUS Live Log', 'TACACS Live Log', 'Reports', 'Troubleshoot', and 'Adaptive Network Control'. The main content area displays several summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (0), 'Client Stopped Responding' (3), and 'Repeat Counts' (0). Below these cards is a table of RADIUS sessions. The table has columns for Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, and Authorization Profiles. Two sessions are listed, both with a status of 'Success' and a repeat count of 0.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-03-09 10:32:28.956	Success		0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess
2017-03-09 10:31:29.227	Success		0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	

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 un cliente AAA en el servidor ISE.
3. Asegúrese de que el secreto compartido sea el mismo entre el switch y el servidor ACS.
4. Verifique si EAP-FAST está habilitado en el servidor ISE.
5. Verifique si las credenciales 802.1x están configuradas para el LAP y son iguales en el servidor ISE. **Nota:** El nombre de usuario y la contraseña distinguen entre mayúsculas y minúsculas.
6. Si falla la autenticación, ingrese estos comandos en el switch: **debug dot1x** y **debug authentication**.