

Lightweight Access Point de la configuración como supplicant del 802.1x

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configure el REVESTIMIENTO](#)

[Configure el Switch](#)

[Configure el servidor ISE](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar un Lightweight Access Point (REVESTIMIENTO) mientras que un supplicant del 802.1x para autenticar contra el servidor del Identity Services Engine (ISE).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Regulador del Wireless LAN (WLC) y REVESTIMIENTO
- 802.1x en los switches Cisco
- ISE
- Protocolo de Autenticación Extensible (EAP) - Autenticación flexible vía el Tunelización seguro (RÁPIDO)

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

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

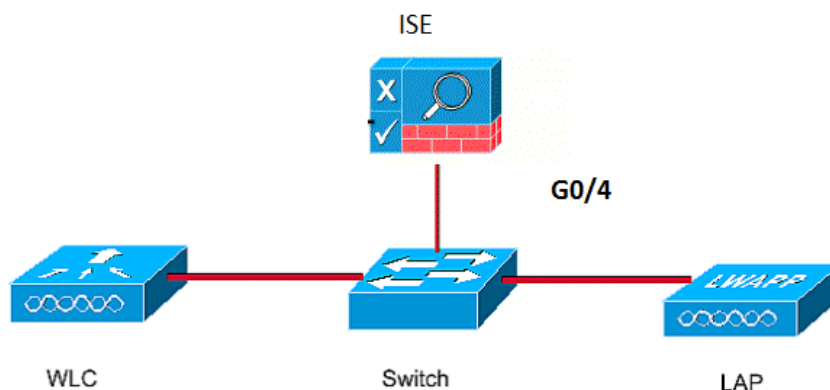
En este puesto el punto de acceso actúa como el supplicant del 802.1x y es autenticado por el Switch contra el ISE que utiliza el EAP-FAST con la disposición protegida anónima de las credenciales del acceso (PAC). El puerto se configura una vez para la autenticación del 802.1x, el Switch no permite que ningún tráfico con excepción del tráfico del 802.1x pase a través del puerto hasta que el dispositivo conectado con el puerto autentique con éxito. Un AP se puede autenticar o antes de que se una a un WLC o después de que se ha unido a un WLC, en este caso usted configura el 802.1x en el Switch después de que el REVESTIMIENTO se una 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

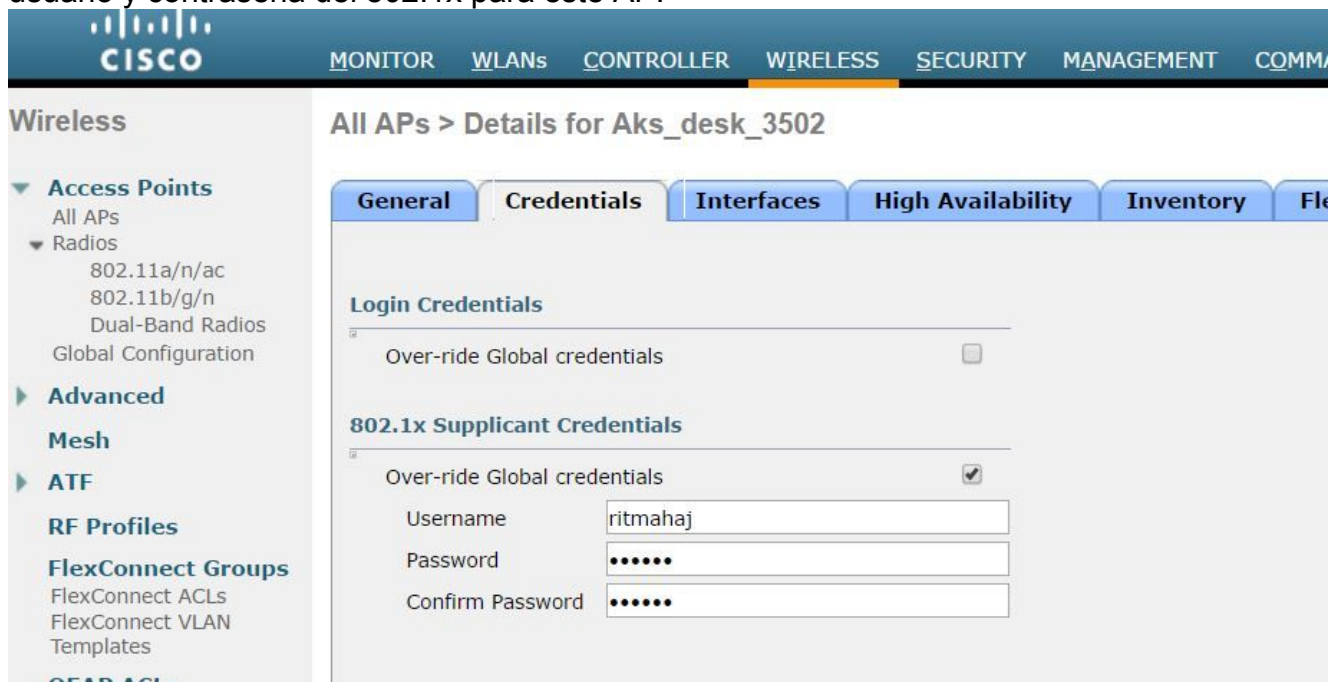
Este documento utiliza estos IP Addresses:

- 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

Configure el REVESTIMIENTO

En esta sección, le presentan con la información para configurar el REVESTIMIENTO como suppliant del 802.1x.

1. Si el AP se une a ya al WLC, va la lengüeta sin hilos y hace clic en el AP, va las credenciales coloca y bajo las credenciales del suppliant del 802.1x que dirigen, marca el rectángulo de **verificación de credenciales global de la invalidación** para fijar el nombre de usuario y contraseña del 802.1x para este AP.



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMM. The left sidebar shows the 'Wireless' menu with options like Access Points, Radios, Advanced, Mesh, ATF, RF Profiles, and FlexConnect Groups. The main content area is titled 'All APs > Details for Aks_desk_3502'. It features several tabs: General, Credentials, Interfaces, High Availability, Inventory, and Flex. The 'Credentials' tab is active, showing 'Login Credentials' and '802.1x Supplicant Credentials' sections. In the '802.1x Supplicant Credentials' section, the 'Over-ride Global credentials' checkbox is checked. The 'Username' field contains 'ritmahaj', and the 'Password' and 'Confirm Password' fields are masked with dots.

Usted puede también fijar un nombre de usuario y contraseña común para todos los AP que se unen a al WLC con el menú de la configuración global.

The screenshot shows the Cisco Wireless configuration interface. The 'Global Configuration' link under 'Dual-Band Radios' is highlighted with a red box. The page displays various configuration sections:

- Ethernet Interface# CDP State:** A table showing CDP status for interfaces 0 through 4, all with checkmarks.
- Radio Slot# CDP State:** A table showing CDP status for radio slots 0 through 2, all with checkmarks.
- Login Credentials:** Fields for Username, Password, and Enable Password.
- 802.1x Supplicant Credentials:** A checkbox for 802.1x Authentication (checked) and fields for Username, Password, and Confirm Password.
- TCP MSS:** A section for Global TCP Adjust MSS (IPV4: 536 - 1363, IPV6: 1220 - 1331).
- AP Retransmit Config Parameters:** Fields for AP Retransmit Count (5) and AP Retransmit Interval (3).
- OEAP Config Parameters:** A checkbox for Disable Local Access.

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

```
LAP#debug capwap console cli
```

```
LAP#capwap ap dot1x username <username> password <password>
```

Configure el Switch

1. Habilite el dot1x en el Switch global 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
```

Configure el servidor ISE

1. Agregue el Switch como cliente del Authentication, Authorization, and Accounting (AAA) en el servidor ISE.

Identity Services Engine 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

Network Devices List > akshat_sw

Network devices

Default Device

Network Devices

* Name: akshat_sw

Description: []

* IP Address: 10.48.39.141 / 32

* Device Profile: Cisco

Model Name: []

Software Version: []

* Network Device Group

Location: All Locations [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: [] [Show]

Identity Services Engine 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

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 el ISE, configure la directiva de la política de autenticación y de la autorización. En este caso, se utiliza la regla de la autenticación predeterminada que es dot.1x atado con alambre, solamente uno puede personalizarlo 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

Asegure eso en los protocolos permitidos que el acceso de red predeterminada, EAP-FAST no se prohíbe.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Allow EAP-FAST

EAP-FAST Inner Methods

- Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
- Allow EAP-GTC
 - Allow Password Change Retries (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
 - Proactive PAC update will occur after % 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

- En cuanto a la directiva de la autorización (Port_AuthZ), en este caso las credenciales AP fueron agregadas a un (APS) del grupo de usuarios. La condición usada era “si el usuario pertenece al grupo AP y hacer el dot1x atado con alambre, después avanza el acceso predeterminado del permiso del perfil de la autorización.” Una vez más esto se puede personalizar según el requisito.

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
<input checked="" type="checkbox"/>	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

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
<input checked="" type="checkbox"/> Enabled		ritmahaj		

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Una vez que el 802.1x se habilita en el puerto del switch, todo el tráfico a menos que el tráfico del 802.1x se bloquee a través del puerto. El REVESTIMIENTO, que si está registrado ya al WLC, consigue desasociado. Solamente después que una autenticación acertada del 802.1x es el otro tráfico permitido pasar a través. El registro exitoso del REVESTIMIENTO al WLC después de que el 802.1x se habilita en el Switch indica que la autenticación del REVESTIMIENTO es acertada. Usted puede también utilizar estos métodos para verificar si el REVESTIMIENTO autenticó.

1. En el Switch, ingrese uno de los **comandos show** para verificar si se ha autenticado el puerto 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 el ISE, elija las **operaciones > el radio Livelogs** y vea que la autenticación es acertada y el perfil correcto de la autorización está avanzado.

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

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

1. Ingrese el **comando ping** para marcar si el servidor ISE es accesible del Switch.
2. Asegúrese que el Switch está configurado como cliente AAA en el servidor ISE.
3. Asegúrese de que el secreto compartido sea lo mismo entre el Switch y el servidor ACS.
4. Marque si el EAP-FAST se habilita en el servidor ISE.
5. Marque si las credenciales del 802.1x se configuran para el REVESTIMIENTO y son lo mismo en el servidor ISE. **Note:** El nombre de usuario y contraseña es con diferenciación entre mayúsculas y minúsculas.
6. Si la autenticación falla, ingrese estos comandos en el Switch: **haga el debug del dot1x y el debug authentication.**