Configuración para asegurar un Switchport de Flexconnect AP con el dot1x

Contenido

Introducción

Este documento describe la configuración para asegurar los Switchports donde los puntos de acceso de FlexConnect autentican con el dot1x usando el radio VSA del device-traffic-class=switch para permitir el tráfico de la Tecnología inalámbrica localmente conmutada LAN (WLAN).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexConnect en el regulador del Wireless LAN (WLC)
- 802.1x en los switches Cisco
- Topología de la autenticación del borde de la red (ASEADA)

Componentes Utilizados

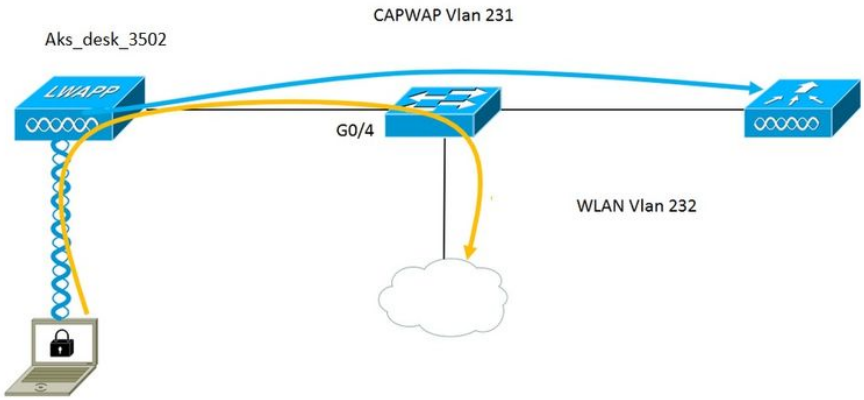
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Motor del servicio de la identidad (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.

Configurar

Diagrama de la red



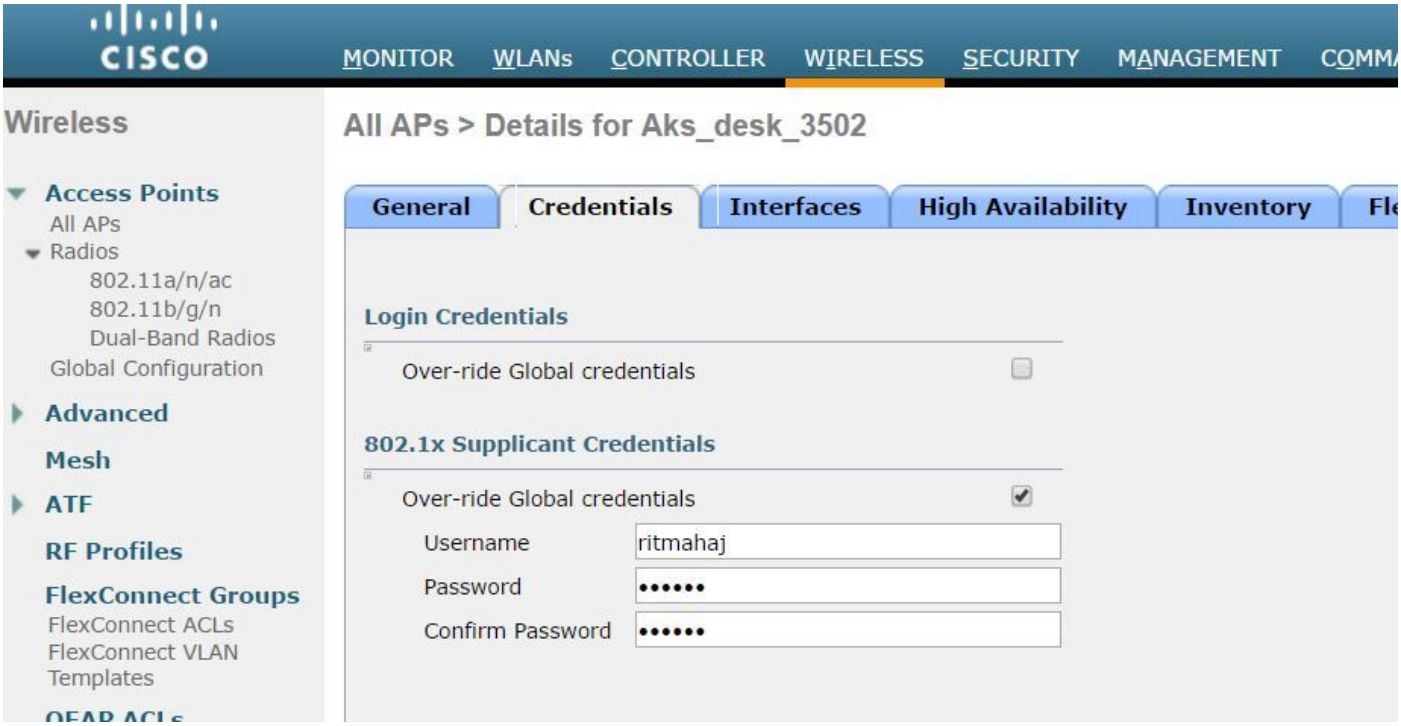
En este puesto el Punto de acceso actúa como el supplicant del 802.1x y es autenticado por el Switch contra el ISE usando el EAP-FAST. El puerto se configura una vez para la autenticación del 802.1x, el Switch no permite que ningún tráfico con excepción del tráfico del 802.1x pase a través del puerto hasta que el dispositivo conectado con el puerto autentique con éxito.

Una vez que el Punto de acceso autentica con éxito contra el ISE, el Switch recibe device-traffic-class=switch del atributo de Cisco VSA “y mueve automáticamente el puerto al trunk.

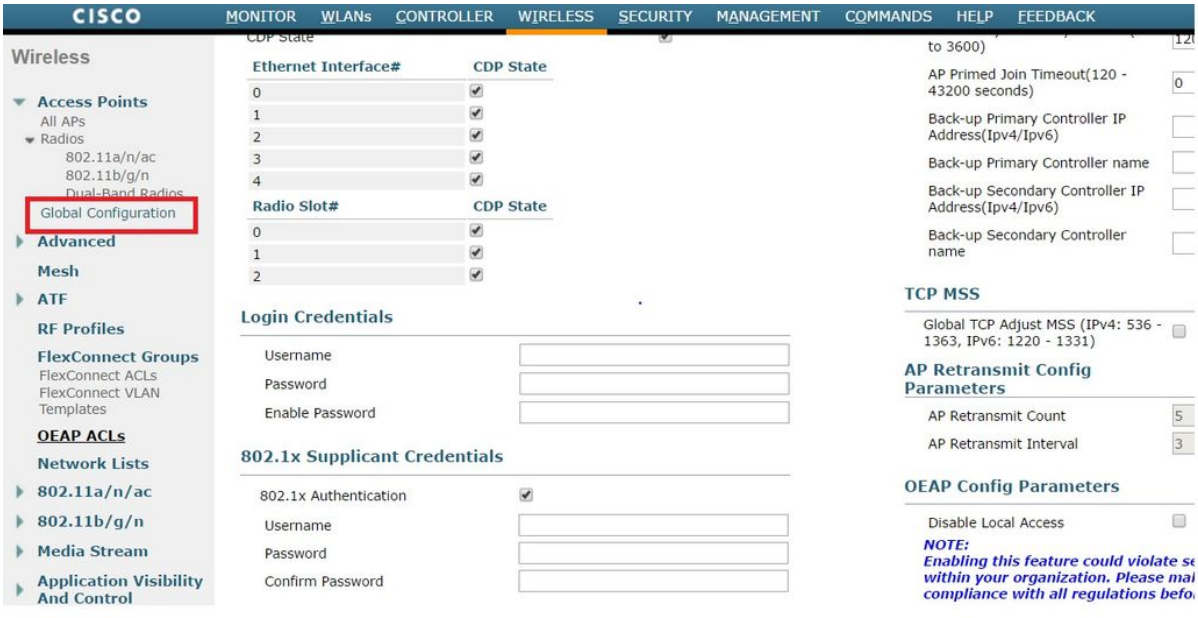
Este los medios, si el AP soporta el modo de FlexConnect y localmente ha conmutado los SSID configurados, podrá enviar el tráfico con Tag. Asegúrese de que el soporte vlan esté habilitado en el AP y el VLAN nativo correcto está configurado.

Configuración AP: -

1. Si el AP se une a ya al WLC, va la lengueta sin hilos y hace clic en el Punto de acceso. Va el campo de Credetials y el nder las credenciales del supplicant del 802.1x que dirigen, marca el cuadro **global de las credenciales de la invalidación** para fijar el nombre de usuario y contraseña del 802.1x para este Punto de acceso.



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



2. Si el Punto de acceso no se ha unido a un WLC todavía, usted debe consolar en el REVESTIMIENTO para fijar las credenciales y para utilizar este comando CLI:

Consola cli del capwap de LAP#debug
<password> de la contraseña del <username> del nombre de usuario del dot1x de LAP#capwap ap

Configuración del switch: -

1. Habilite el dot1x en el Switch global y agregue el servidor ISE para conmutar

```
aaa new-model

¡!
radio del grupo predeterminado del dot1x de la autenticación aaa

¡!
radio del grupo predeterminado de la autorización de red AAA

¡!

sistema-auth-control del dot1x

¡!

servidor de RADIUS ISE
acct-puerto 1646 del auténtico-puerto 1645 del direccionamiento ipv4 10.48.39.161
 clave 7 123A0C0411045D5679
```

2. Ahora configure el puerto del switch AP

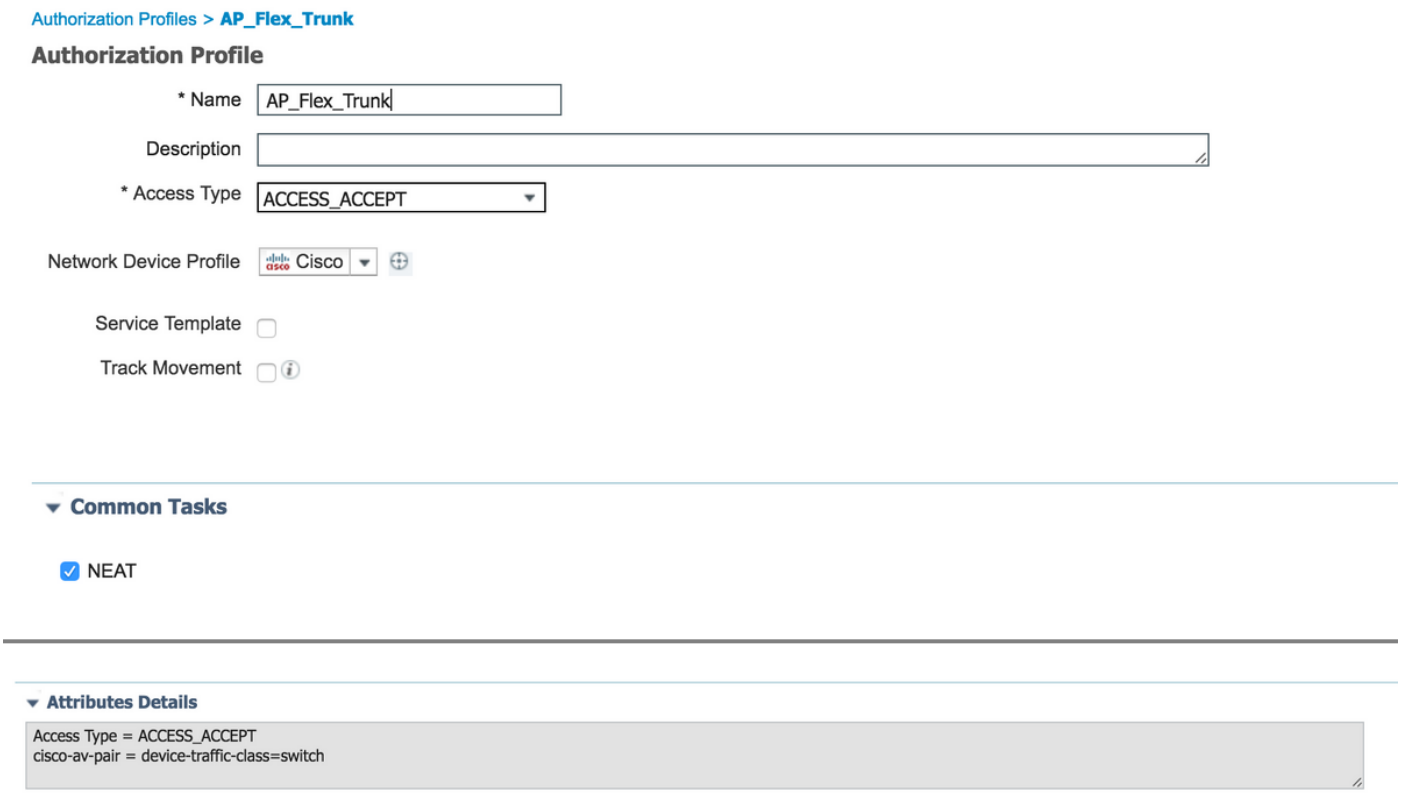
```
interconecte GigabitEthernet0/4
VLAN de acceso al puerto del switch 231
switchport trunk no prohibido 231,232 vlan
acceso de modo del switchport
apagado
multi-host de la autenticación host-MODE
dot1x de la orden de la autenticación
auto del puerto-control de la autenticación
authenticator de los pae del dot1x
borde del árbol de expansión Portfast
```

Si uno quiere configurar el MAB en vez del dot1x entonces el config del puerto parece: -

```
interfaz GigabitEthernet0/4
VLAN de acceso al puerto del switch 231
switchport trunk no prohibido 231,232 vlan
acceso de modo del switchport
apagado
multi-host de la autenticación host-MODE
orden mab de la autenticación
auto del puerto-control de la autenticación
mab
borde del árbol de expansión Portfast
```

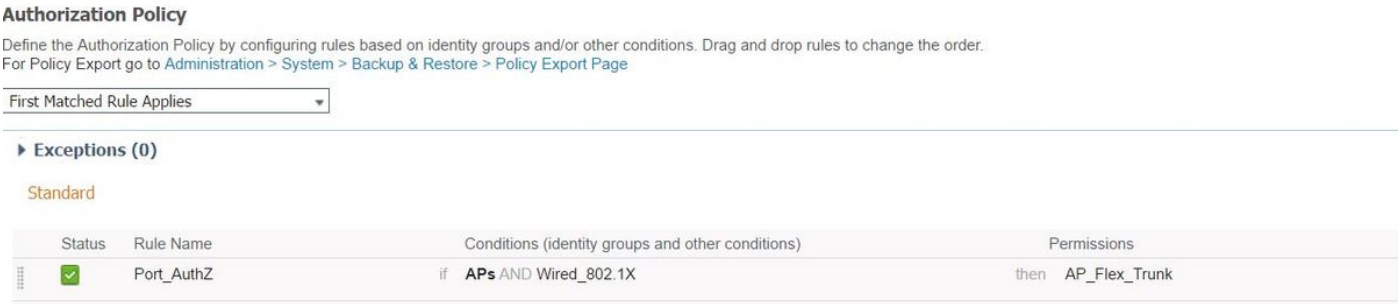
Configuración ISE: -

1. En el ISE, uno puede habilitar simplemente ASEADO para el perfil de la autorización AP para fijar el atributo correcto, sin embargo, en otros servidores de RADIUS, usted puede configurar manualmente.



2. En el ISE, uno también necesita configurar la directiva de la política de autenticación y de la autorización. En este caso golpeamos la regla de la autenticación predeterminada que es dot.1x(wired atado con alambre MAB en caso de MAB) pero uno puede personalizarlo según el requisito.

En cuanto a la directiva de la autorización (Port_AuthZ), en este caso agregamos las credenciales AP a un (APS) del grupo de usuarios y avanzamos el perfil de la autorización (AP_Flex_Trunk) basado en esto.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. En el Switch, puede utilizar una vez el comando “autocfg todo de la característica del debug authentication” de marcar si el puerto se está moviendo al puerto troncal o no.

20 de febrero 12:34:18.119: %LINK-3-UPDOWN: Interfaz GigabitEthernet0/4, estado cambiado a para arriba
20 de febrero 12:34:19.122: %LINEPROTO-5-UPDOWN: Line Protocol en la interfaz GigabitEthernet0/4, estado cambiado a para arriba
akshat_sw#

akshat_sw#
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: En el start_fn de AutoCfg del dot1x, epm_handle: 3372220456
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: [588d.0997.061d, tipo de dispositivo Gi0/4] = Switch
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: [588d.0997.061d, nuevo cliente Gi0/4]
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Estatus macro interno de la aplicación [Gi0/4] Autocfg: 1
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Tipo de dispositivo [Gi0/4]: 2
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Auto-config [Gi0/4]: el stp tiene port_config 0x85777D8
20 de febrero 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Auto-config [Gi0/4]: el port_config del stp tiene guard_config 2 del bpdu
20 de febrero 12:38:11.116: AUTHENTIC-FEAT-AUTOCFG-EVENT: [Gi0/4] que aplica el auto-cfg en el puerto.
20 de febrero 12:38:11.116: AUTHENTIC-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: VLAN-Str 231: 231
20 de febrero 12:38:11.116: AUTHENTIC-FEAT-AUTOCFG-EVENT: [Gi0/4] que aplica la macro dot1x_autocfg_supp
20 de febrero 12:38:11.116: Aplicando el comando… 'ningún VLAN de acceso al puerto del switch 231' en Gi0/4
20 de febrero 12:38:11.127: Aplicando el comando… “ningún switchport nonegocia” en Gi0/4
20 de febrero 12:38:11.127: Aplicando el comando… “modo troncal del switchport” en Gi0/4
20 de febrero 12:38:11.134: Aplicando el comando… 'VLAN nativo 231' del switchport trunk en Gi0/4
20 de febrero 12:38:11.134: Aplicando el comando… “trunk del árbol de expansión Portfast” en Gi0/4
20 de febrero 12:38:12.120: %LINEPROTO-5-UPDOWN: Line Protocol en la interfaz GigabitEthernet0/4, estado cambiado a abajo
20 de febrero 12:38:15.139: %LINEPROTO-5-UPDOWN: Line Protocol en la interfaz GigabitEthernet0/4, estado cambiado a para arriba

2. La salida del “funcionamiento internacional el g0/4" de la demostración mostrará que el puerto ha cambiado a un puerto troncal.

Configuración actual 295 bytes
¡!
interfaz GigabitEthernet0/4
switchport trunk no prohibido 231,232,239 vlan
VLAN nativo 231 del switchport trunk
switchport mode trunk
multi-host de la autenticación host-MODE
dot1x de la orden de la autenticación
auto del puerto-control de la autenticación
authenticator de los pae del dot1x
trunk del borde del árbol de expansión Portfast
Finalizar

3. En el ISE, bajo Operations>>Radius Livelogs uno podemos la autenticación que es acertada y el perfil correcto de la autorización que es avanzado.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-02-20 15:05:48.991			0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4. Si conectamos a un cliente después de que esto entonces su MAC address sea aprendida en el puerto del switch AP en el cliente 232 vlan.

tabla de direcciones internacional g0/4 del mac del akshat_sw#sh
Tabla del MAC address

Puertos del tipo del MAC address de Vlan
---- ----------- -------- -----
231 588d.0997.061d Gi0/4 ESTÁTICOS - AP
232 c0ee.fbd7.8824 Gi0/4 DINÁMICO - Cliente

En el WLC, en el detalle del cliente puede ser visto que pertenece este cliente 232 vlan y el SSID localmente está conmutado. Aquí está un snippet.

(Detalle c0:ee:fb:d7:88:24 del cliente del >show del regulador de Cisco)
MAC Address del cliente c0:ee:fb:d7:88:24
Nombre de usuario del cliente ..... N/A
Dirección MAC ..... b4:14:89:82:cb:90 AP
Nombre AP ..... Aks_desk_3502
Identificación del slot de la radio AP 1
Estado del cliente ..... Asociado
Grupo de usuario de cliente .....
Del cliente del NAC estado OOB ..... Acceso
Identificación del Wireless LAN 2
Nombre de red inalámbrica LAN (SSID) ..... Puerto-auth
Nombre del perfil del Wireless LAN ..... Puerto-auth
Hotspot (802.11u) ..... No soportados
BSSID b4:14:89:82:cb:9f
Conectado por ..... 42 secs
Canal 44
Dirección IP 192.168.232.90
Dirección del gateway 192.168.232.1
Netmask 255.255.255.0
Identificación de la asociación 1
Algoritmo de autenticación ..... Sistema operativo
Código de motivo 1
Código de estado 0

Transferencia de los datos de FlexConnect ..... Local
Estatus DHCP de FlexConnect ..... Local
FlexConnect Vlan basó la transferencia central ..... No
Autenticación de FlexConnect ..... Central
Asociación central de FlexConnect ..... No
NOMBRE ..... 232 vlan del VLA N de FlexConnect
VLA N de la cuarentena 0
VLA N del acceso 232
VLA N local del bridging 232

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Si la autenticación falla, utilice el **dot1x del debug**, el **debug authentication** ordena.
- Si el puerto no se mueve al trunk, ingrese el **comando all del autocfg de la característica del debug authentication**.
- Asegúrese que usted haga el modo del multi-host (multi-host de la autenticación host-MODE) configurar. El Multi-host tiene que ser habilitado para permitir las direcciones MAC de la Tecnología inalámbrica del cliente.
- el comando de la “autorización de red AAA” se debe configurar para que el Switch valide y aplique los atributos enviados por el ISE.