Proteja un puerto de switch de punto de acceso Flexconnect con Dot1x

Contenido

Introducción

Este documento describe la configuración para proteger los puertos de switch donde los puntos de acceso FlexConnect (AP) se autentican con Dot1x mediante device-traffic-class=switch Radius VSA para permitir el tráfico de las LAN inalámbricas conmutadas localmente (WLAN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexConnect en controlador de LAN inalámbrica (WLC)
- 802.1x en switches Cisco
- Topología de autenticación de extremo de la red (NEAT)

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
- Identity Service Engine (ISE) 2.0
- Puntos de acceso basados en IOS (series x500, x600 y x700).

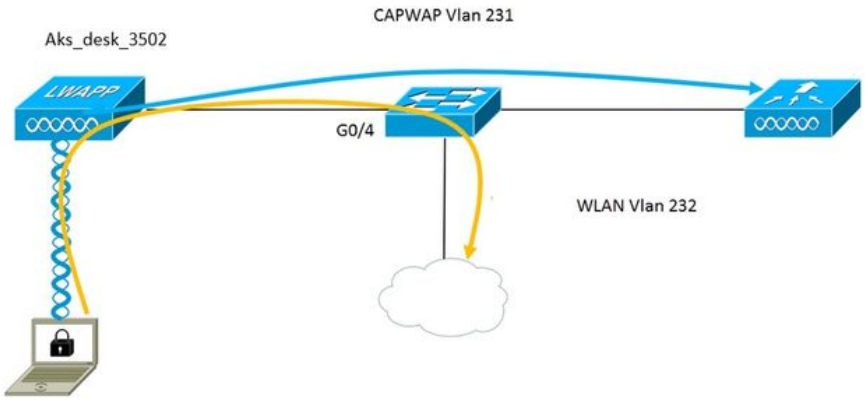
Los AP de Wave 2 basados en el OS AP no soportan el punto 1x troncal de flexconnect al momento de escribir esto.

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. Si tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



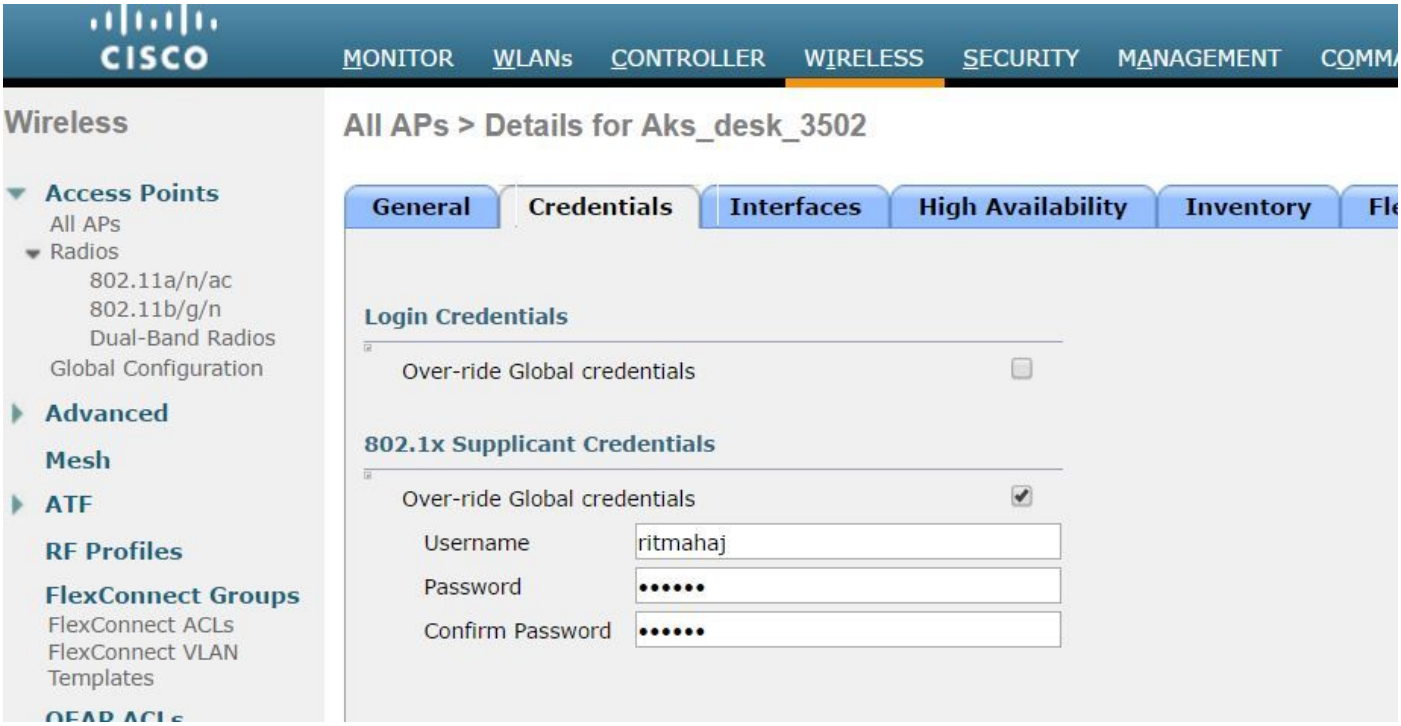
En esta configuración, el punto de acceso actúa como suplicante 802.1x y el switch lo autentica contra ISE mediante EAP-FAST. Una vez que el puerto se configura para la autenticación 802.1x, el switch no permite que ningún tráfico que no sea 802.1x pase a través del puerto hasta que el dispositivo conectado al puerto se autentique correctamente.

Una vez que el punto de acceso se autentica correctamente con ISE, el switch recibe el atributo de VSA de Cisco "device-traffic-class=switch y mueve automáticamente el puerto al trunk.

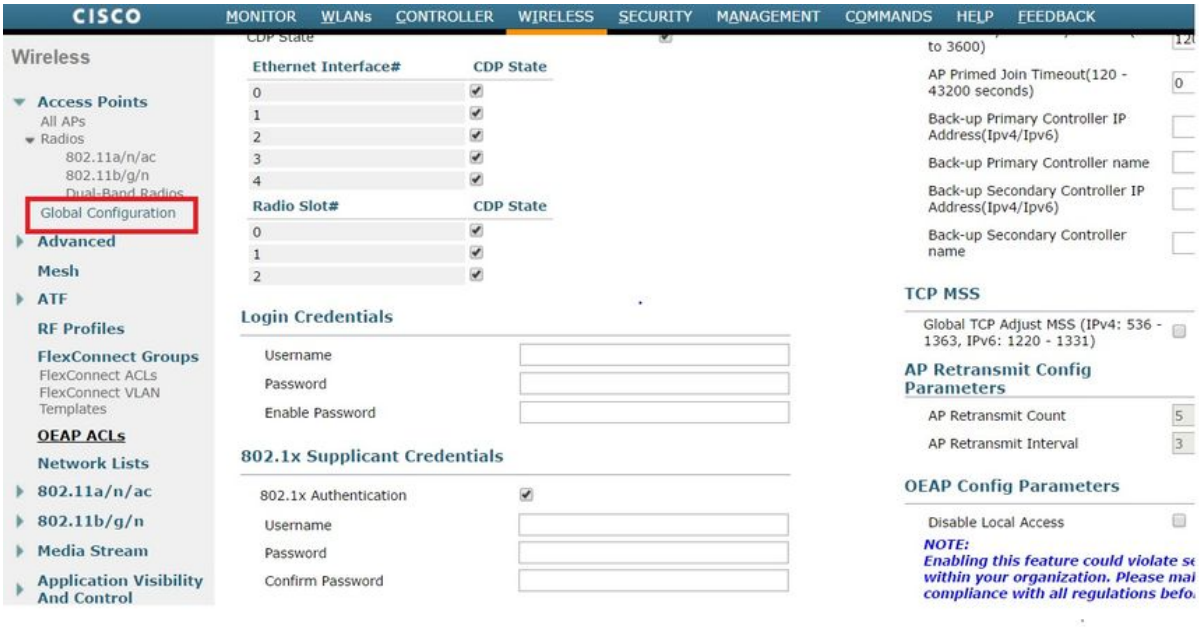
Esto significa que si el AP soporta el modo FlexConnect y tiene configurados SSID conmutados localmente, podrá enviar tráfico etiquetado. Asegúrese de que el soporte de vlan esté habilitado en el AP y que la vlan nativa correcta esté configurada.

Configuración de AP:-

1. Si el AP ya está unido al WLC, vaya a la pestaña Wireless y haga clic en el punto de acceso. Vaya al campo Credenciales y en el encabezado Credenciales de suplicante 802.1x, active la casilla **Sobrescribir credenciales globales** para establecer el nombre de usuario y la contraseña 802.1x para este punto de acceso.



También puede establecer un nombre de usuario y una contraseña de comando para todos los puntos de acceso que se unen al WLC con el menú Global Configuration .



2. Si el punto de acceso aún no se ha unido a un WLC, debe consolar en el LAP para establecer las credenciales y utilizar este comando CLI:

LAP#debug capwap console cli
LAP#capwap ap dot1x username <username> password <password>

Configuración del switch:-

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

aaa new-model

!
aaa authentication dot1x default group radius

!
aaa authorization network default group radius

!

dot1x system-auth-control

!

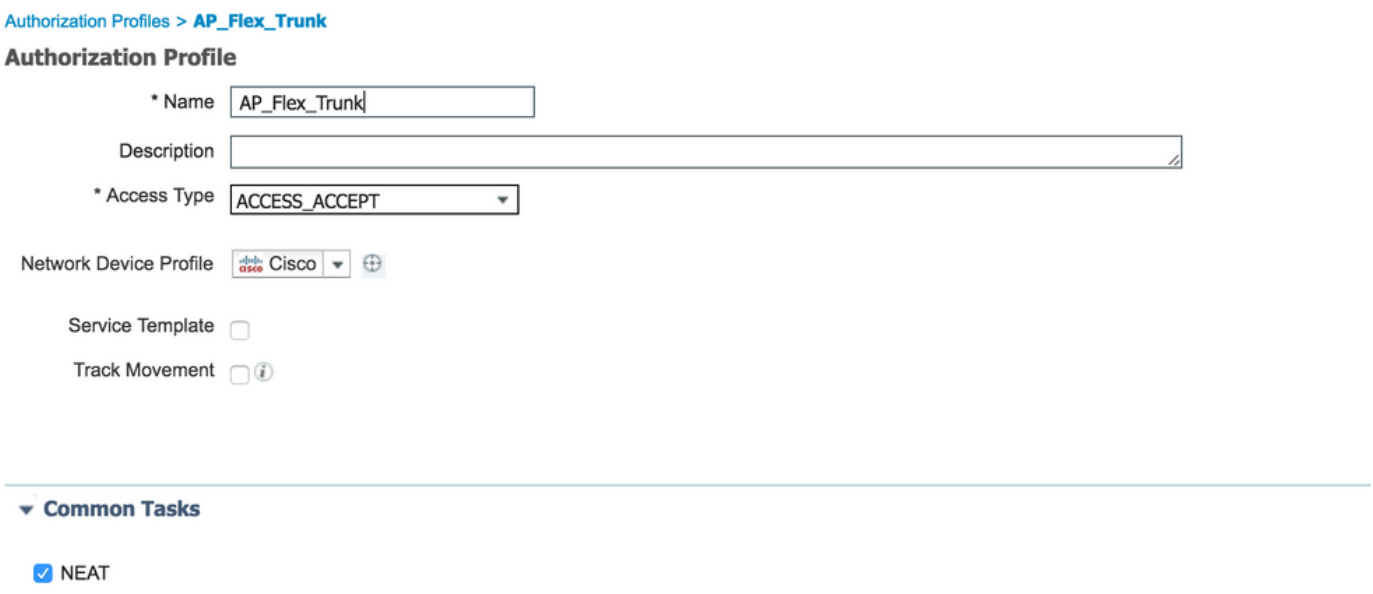
ISE de servidor RADIUS
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
 key 7 123A0C0411045D5679

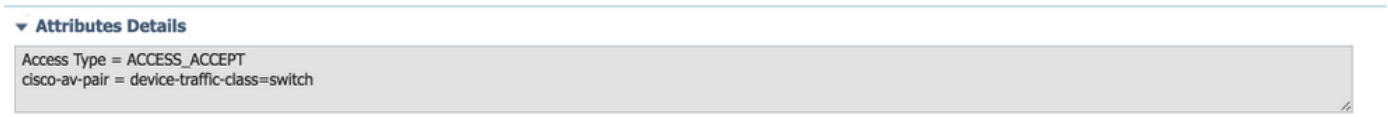
2. Ahora configure el puerto del switch AP

interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication port-control auto
autenticador de la página dot1x
spanning-tree portfast edge

Configuración de ISE:-

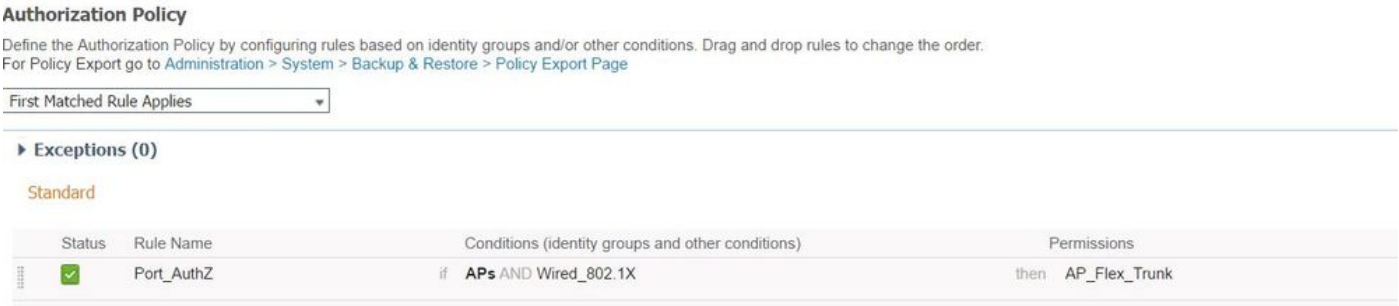
1. En ISE, uno puede simplemente habilitar NEAT para el perfil de Autorización AP para establecer el atributo correcto, sin embargo, en otros servidores RADIUS, usted puede configurar manualmente.





2. En ISE, también es necesario configurar la política de autenticación y la política de autorización. En este caso, se aplicó la regla de autenticación predeterminada que es wired dot1x pero se puede personalizar según el requisito.

En cuanto a la política de autorización (Port_AuthZ), en este caso agregamos las credenciales de AP a un grupo de usuarios (AP) y presionamos el perfil de autorización (AP_Flex_Trunk) basándose en esto.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. En el switch, una vez puede utilizar el comando "debug authentication feature autocfg all" para verificar si el puerto se está moviendo o no al puerto trunk.

20 feb 12:34:18.119: %LINK-3-UPDOWN: Interfaz GigabitEthernet0/4, estado cambiado a activo
20 feb 12:34:19.122: %LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz GigabitEthernet0/4, estado cambiado a activo
akshat_sw#
akshat_sw#
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: En dot1x AutoCfg start_fn, epm_handle: 3372220456
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: [588d.0997.061d, Gi0/4] Tipo de dispositivo = Switch
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: [588d.0997.061d, Gi0/4] nuevo cliente
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: [Gi0/4] Estado interno de la aplicación de macro Autocfg: 1
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: [Gi0/4] Tipo de dispositivo: 2
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: [Gi0/4] Configuración automática: stp tiene port_config 0x85777D8
20 feb 12:38:11.113: EVENTO AUTH-FEAT-AUTOCFG: [Gi0/4] Configuración automática: stp port_config tiene bpdu guard_config 2
20 feb 12:38:11.116: EVENTO AUTH-FEAT-AUTOCFG: [Gi0/4] Aplicando auto-cfg en el puerto.
20 feb 12:38:11.116: EVENTO AUTH-FEAT-AUTOCFG: Vlan [Gi0/4]: 231 Vlan-Str: 231
20 feb 12:38:11.116: EVENTO AUTH-FEAT-AUTOCFG: [Gi0/4] Aplicación de la macro dot1x_autocfg_supp
20 feb 12:38:11.116: Aplicando comando... 'no switchport access vlan 231' en Gi0/4
20 feb 12:38:11.127: Aplicando comando... 'no switchport nonegotiate' en Gi0/4

20 feb 12:38:11.127: Aplicando comando... 'switchport mode trunk' en Gi0/4
20 feb 12:38:11.134: Aplicando comando... 'switchport trunk native vlan 231' en Gi0/4
20 feb 12:38:11.134: Aplicando comando... 'spanning-tree portfast trunk' en Gi0/4
20 feb 12:38:12.120: %LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz GigabitEthernet0/4, estado cambiado a inactivo
20 feb 12:38:15.139: %LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz GigabitEthernet0/4, estado cambiado a activo

2. El resultado de "show run int g0/4" mostrará que el puerto ha cambiado a un puerto trunk.

Configuración actual 295 bytes
!
interface GigabitEthernet0/4
switchport trunk allowed vlan 231,232,239
switchport trunk native vlan 231
switchport mode trunk
authentication host-mode multi-host
authentication order dot1x
authentication port-control auto
autenticador de la página dot1x
tronco de borde Portfast del árbol de expansión
Finalizar

3. En ISE, en Operations>>Radius Livelogs se puede ver si la autenticación es exitosa y si se envía el perfil de autorización correcto.

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 un cliente después de esto, su dirección mac será aprendida en el puerto del switch AP en la vlan cliente 232.

akshat_sw#sh mac address-table int g0/4
Tabla de dirección MAC
—

Puertos de tipo de dirección Vlan Mac
— —
— —
— —
— —
— —
— —
— —
— — — — — — — — — — — — — — — — — —
231 588d.0997.061d STATIC Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Cliente

En el WLC, en los detalles del cliente se puede ver que este cliente pertenece a vlan 232 y el SSID se conmuta localmente. Aquí hay un fragmento.

(Controlador de Cisco) >show client detail c0:ee:fb:d7:88:24
Dirección MAC del cliente..... c0:ee:fb:d7:88:24
Nombre de usuario del cliente..... N/A
Dirección MAC de AP..... b4:14:89:82:cb:90
Nombre de AP..... Aks_desk_3502
ID de ranura de radio AP..... 1
Estado del cliente..... Asociado
Grupo de usuarios del cliente.....
Estado OOB de NAC del cliente..... Acceso
ID de LAN inalámbrica..... 2
Nombre de la red LAN inalámbrica (SSID)..... Port-Auth
Nombre del perfil de LAN inalámbrica..... Port-auth
Hotspot (802.11u)..... Not Supported
BSSID..... b4:14:89:82:cb:9f
Conectado para..... 42 segundos
Canal..... 44
IP Address..... 192.168.232.90
Dirección de puerta de enlace..... 192.168.232.1
Máscara de red..... 255.255.255.0
ID de asociación..... 1
Algoritmo de autenticación..... Sistema abierto
Código de motivo..... 1
Código de estado..... 0

FlexConnect Data Switching..... Local
Estado Dhcp De FlexConnect..... Local
Switching central basado en Vlan de FlexConnect..... No
Autenticación de FlexConnect..... Central
FlexConnect Central Association..... No
NOMBRE DE VLAN de FlexConnect..... vlan 232
VLAN de cuarentena..... 0
Acceso a VLAN..... 232
VLAN de conexión en puente local..... 232

Troubleshoot

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

- Si la autenticación falla, utilice los comandos **debug dot1x**, **debug authentication**.
- Si el puerto no se mueve al trunk, ingrese el comando **debug authentication feature autocfg all**.
- Asegúrese de tener configurado el modo de host múltiple (host de autenticación multihost). Multi-Host debe estar habilitado para permitir las direcciones MAC inalámbricas del cliente.
- "aaa authorization network" se debe configurar para que el switch acepte y aplique los atributos enviados por ISE.

Los puntos de acceso basados en Cisco IOS sólo admiten TLS 1.0. Esto puede causar un problema si su servidor RADIUS está configurado para permitir solamente las autenticaciones de TLS 1.2 802.1X