Configurar para fixar um Switchport de Flexconnect AP com dot1x

Índice

Introdução

Este documento descreve a configuração para fixar os Switchports onde os Access point de FlexConnect (AP) autenticam com dot1x usando o raio VSA do device-traffic-class=switch para permitir o tráfego do Sem fio localmente comutado LAN (WLAN).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexConnect no controlador do Wireless LAN (WLC)
- 802.1x em switch Cisco
- Topologia da autenticação da margem de rede (PURA)

Componentes Utilizados

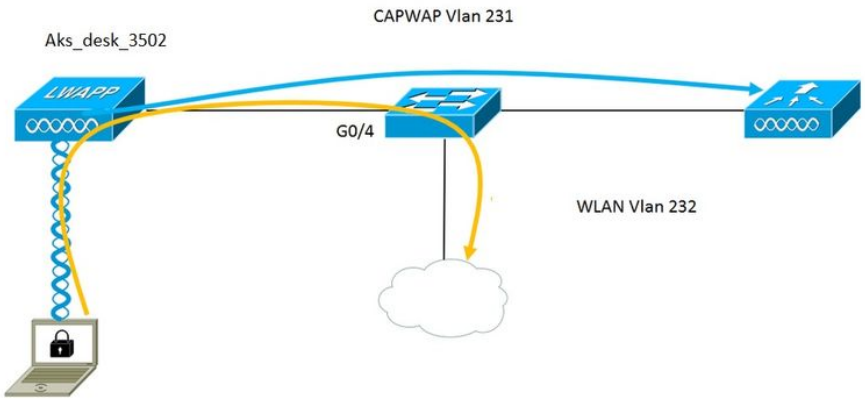
As informações neste documento são baseadas nestas versões de software e hardware:

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Motor do serviço da identidade (ISE) 2.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



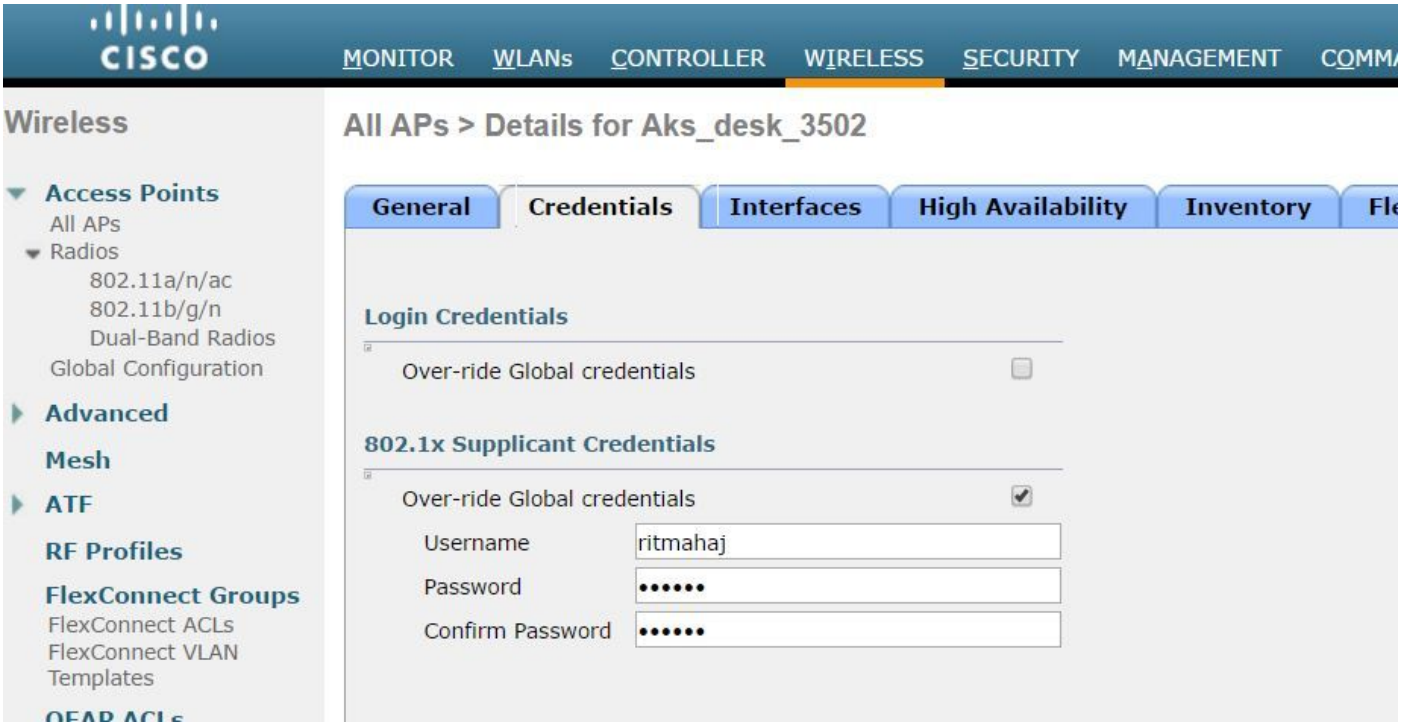
No este setup o Access point atua como o suplicante do 802.1x e é autenticado pelo interruptor contra a utilização ISE EAP-FAST. Uma vez que a porta é configurada para a autenticação do 802.1x, o interruptor não permite que nenhum tráfego a não ser o tráfego do 802.1x passe através da porta até que o dispositivo conectado à porta autentique com sucesso.

Uma vez que o Access point autentica com sucesso contra o ISE, o interruptor recebe device-traffic-class=switch do atributo de Cisco VSA “e move automaticamente a porta para o tronco.

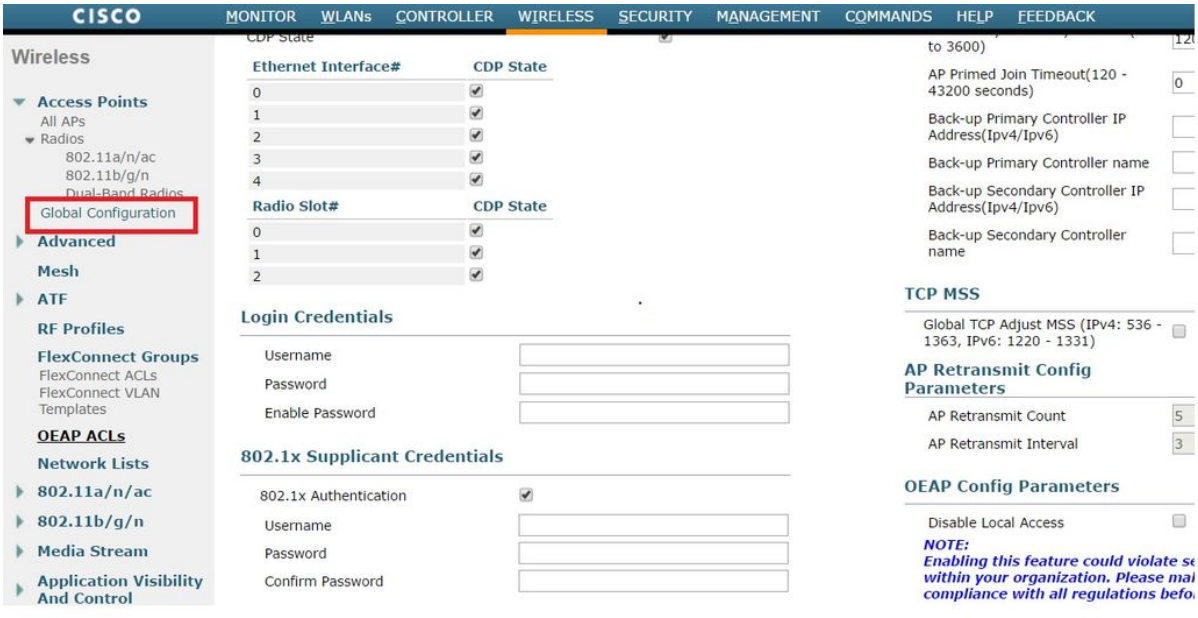
Este meios, se o AP apoia o modo de FlexConnect e comutou localmente os SSID configurados, poderá enviar o tráfego rotulado. Assegure-se de que o apoio vlan esteja permitido no AP e o vlan nativo correto esteja configurado.

Configuração AP: -

1. Se o AP é juntado já ao WLC, vai a aba wireless e clica sobre o Access point. Vai o campo de Credetials e o nder as credenciais do suplicante do 802.1x que dirigem, verifica a caixa **global das credenciais da ultrapassagem** para ajustar o nome de usuário e senha do 802.1x para este Access point.



Você pode igualmente ajustar um nome de usuário e senha do comman para todos os Access point que são juntados ao WLC com o menu da configuração global.



2. Se o Access point não se juntou a um WLC ainda, você deve consolar no REGAÇO para ajustar as credenciais e para usar este comando CLI:

Console CLI do capwap de LAP#debug
<password> da senha do <username> username do dot1x de LAP#capwap ap

Configuração de switch: -

1. Permita o dot1x no interruptor globalmente e adicionar o server ISE para comutar

aaa new-model

!
raio do grupo padrão do dot1x da autenticação aaa

!
raio do grupo padrão da rede de autorização AAA

!

sistema-AUTH-controle do dot1x

!

servidor Radius ISE
acct-porta 1646 da autêntico-porta 1645 de 10.48.39.161 do IPv4 do endereço
 7 chave 123A0C0411045D5679

2. Configurar agora a porta de switch AP

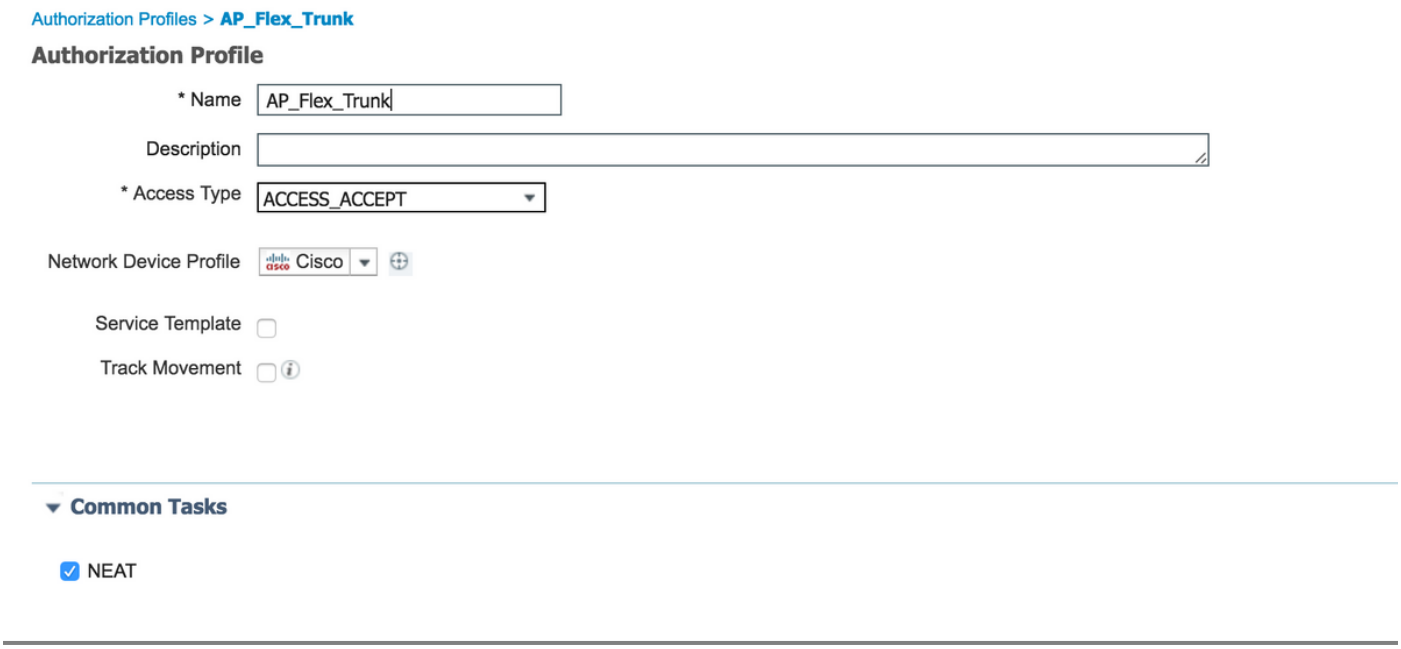
conecte GigabitEthernet0/4
switchport access vlan 231
tronco de switchport permitido 231,232 vlan
acesso de modo do switchport
fechamento
multi-host da autenticação host-MODE
dot1x da ordem da autenticação
automóvel do porta-controle da autenticação
autenticador dos pae do dot1x
borda do portfast de Spanning Tree

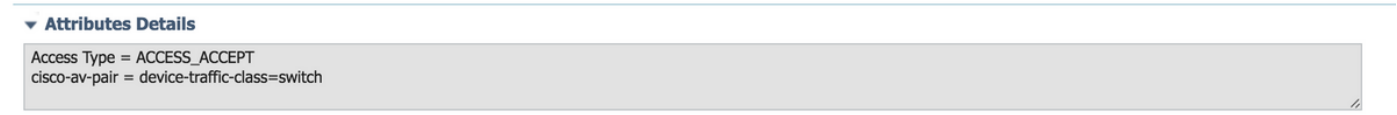
Se um quer configurar o MAB em vez do dot1x então a configuração da porta olha como: -

relação GigabitEthernet0/4
switchport access vlan 231
tronco de switchport permitido 231,232 vlan
acesso de modo do switchport
fechamento
multi-host da autenticação host-MODE
ordem mab da autenticação
automóvel do porta-controle da autenticação
mab
borda do portfast de Spanning Tree

Configuração ISE: -

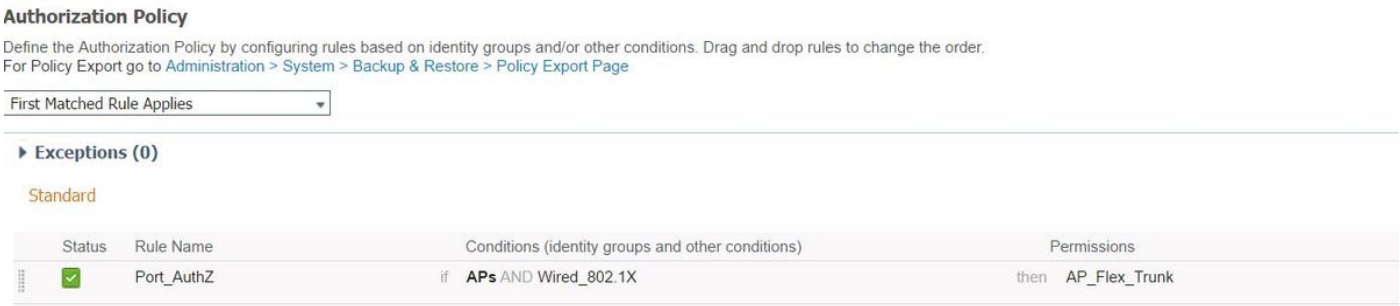
1. No ISE, um pode simplesmente permitir PURO para o perfil da autorização AP a fim ajustar o atributo correto, contudo, em outros servidores Radius, você pode configurar manualmente.





2. No ISE, um igualmente precisa de configurar a política da política de autenticação e da autorização. Neste caso nós batemos a regra da autenticação padrão que é dot.1x(wired prendido MAB em caso do MAB) mas um pode personalizá-lo conforme a exigência.

Quanto para à política da autorização (Port_AuthZ), neste caso nós adicionamos as credenciais AP a um grupo de usuário (AP) e empurramos o perfil da autorização (AP_Flex_Trunk) baseado neste.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. No interruptor, uma vez pode usar o comando do “autocfg todo da característica debug authentication” verificar se a porta está sendo movida para a porta de tronco ou não.

20 de fevereiro 12:34:18.119: %LINK-3-UPDOWN: Relação GigabitEthernet0/4, estado mudado a acima
20 de fevereiro 12:34:19.122: %LINEPROTO-5-UPDOWN: Protocolo de linha na relação GigabitEthernet0/4, estado mudado a acima
akshat_sw#
akshat_sw#
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: No start_fn de AutoCfg do

dot1x, epm_handle: 3372220456
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: [588d.0997.061d, tipo de dispositivo Gi0/4] = interruptor
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: [588d.0997.061d, cliente novo Gi0/4]
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Estado macro interno do aplicativo [Gi0/4] Autocfg: 1
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Tipo de dispositivo [Gi0/4]: 2
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Auto-configuração [Gi0/4]: o stp tem o port_config 0x85777D8
20 de fevereiro 12:38:11.113: AUTHENTIC-FEAT-AUTOCFG-EVENT: Auto-configuração [Gi0/4]: o port_config do stp tem o guard_config 2 do bpdu
20 de fevereiro 12:38:11.116: AUTHENTIC-FEAT-AUTOCFG-EVENT: [Gi0/4] que aplica o auto-CFG na porta.
20 de fevereiro 12:38:11.116: AUTHENTIC-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: VLAN-estreptococo 231: 231
20 de fevereiro 12:38:11.116: AUTHENTIC-FEAT-AUTOCFG-EVENT: [Gi0/4] que aplica o macro dot1x_autocfg_supp
20 de fevereiro 12:38:11.116: Aplicando o comando… 'nenhum switchport access vlan 231' em Gi0/4
20 de fevereiro 12:38:11.127: Aplicando o comando… “nenhuma não-negociação do switchport” em Gi0/4
20 de fevereiro 12:38:11.127: Aplicando o comando… do “tronco de modo switchport” em Gi0/4
20 de fevereiro 12:38:11.134: Aplicando o comando… 'tronco de switchport 231' vlan nativo em Gi0/4
20 de fevereiro 12:38:11.134: Aplicando o comando… do “tronco portfast de Spanning Tree” em Gi0/4
20 de fevereiro 12:38:12.120: %LINEPROTO-5-UPDOWN: Protocolo de linha na relação GigabitEthernet0/4, estado mudado a para baixo
20 de fevereiro 12:38:15.139: %LINEPROTO-5-UPDOWN: Protocolo de linha na relação GigabitEthernet0/4, estado mudado a acima

2. A saída da “da corrida int g0/4" mostra mostrará que a porta mudou a uma porta de tronco.

Configuração atual: 295 bytes
!
relação GigabitEthernet0/4
tronco de switchport permitido 231,232,239 vlan
tronco de switchport 231 vlan nativos
tronco de modo de porta de comutação
multi-host da autenticação host-MODE
dot1x da ordem da autenticação
automóvel do porta-controle da autenticação
autenticador dos pae do dot1x
tronco da borda do portfast de Spanning Tree
fim

3. No ISE, sob Operations>>Radius Livelogs um podemos nós a autenticação que são bem sucedida e o perfil correto da autorização que está sendo empurrado.

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. Se nós conectamos um cliente depois que este seu MAC address estará aprendido então na porta de switch AP no cliente 232 vlan.

tabela de endereços MAC int g0/4 do akshat_sw#sh
Tabela de endereços MAC

Tipo portas do MAC address de Vlan
---- ----------- -------- -----
231 588d.0997.061d Gi0/4 ESTÁTICOS - AP
232 c0ee.fbd7.8824 Gi0/4 DINÂMICO - Cliente

No WLC, no detalhe do cliente pode-se ver que este cliente pertence 232 vlan e o SSID está comutado localmente. Está aqui um snippet.

(Detalhe c0:ee:fb:d7:88:24 do cliente do >show do controlador de Cisco)
Endereço MAC de cliente c0:ee:fb:d7:88:24
Nome de usuário do cliente ..... N/A
MAC address ..... b4:14:89:82:cb:90 AP
Nome AP ..... Aks_desk_3502
Identificação do entalhe do rádio AP 1
Estado do cliente ..... Associado
Grupo de usuário cliente .....
Estado do cliente NAC OOB ..... Acesso
Identificação do Wireless LAN 2
Nome de rede de Wireless LAN (SSID) ..... Porta-AUTH
Nome de perfil do Wireless LAN ..... Porta-AUTH
Ponto quente (802.11u) ..... não suportado
BSSID b4:14:89:82:cb:9f
Conectado por ..... 42 segundos
Canal 44
Endereço IP de Um ou Mais Servidores Cisco ICM NT 192.168.232.90
Endereço de gateway 192.168.232.1
Máscara de rede 255.255.255.0
Identificação da associação 1
Algoritmo de autenticação ..... Sistema aberto
Código de motivo 1
Código de status 0

Interruptor dos dados de FlexConnect ..... Local
Estado DHCP de FlexConnect ..... Local
FlexConnect Vlan baseou o interruptor central ..... No
Autenticação de FlexConnect ..... Central
Associação central de FlexConnect ..... No
NOME ..... 232 vlan de FlexConnect VLAN
Quarentena VLAN 0
Alcance o VLAN 232
VLAN de construção de uma ponte sobre local 232

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Se a autenticação falha, o uso **debuga o dot1x**, o **debug authentication** comanda.
- Se a porta não é movida para o tronco, inscreva o **comando all do autocfg da característica do debug authentication**.
- Assegure-se de que você tenha o modo do multi-host (multi-host da autenticação host-MODE) configurado. O Multi-host tem que ser permitido a fim permitir a cliente endereços wireless MAC.
- o comando da “rede de autorização AAA” deve ser configurado para que o interruptor aceite e aplique os atributos enviados pelo ISE.