Secure a Flexconnect AP-switch met Dot1x

Inhoud

Inleiding

Dit document beschrijft de configuratie om switches te beveiligen wanneer FlexConnect Access Point (AP) authentiek is met Dot1x met machine-verkeer-klasse=switch Radius VSA om verkeer van lokaal switched draadloze LAN's (WLAN's) toe te staan.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexConnect op draadloze LAN-controller (WLC)
- 802.1x op Cisco-Switches
- Network Edge-verificatietopologie (NEAT)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

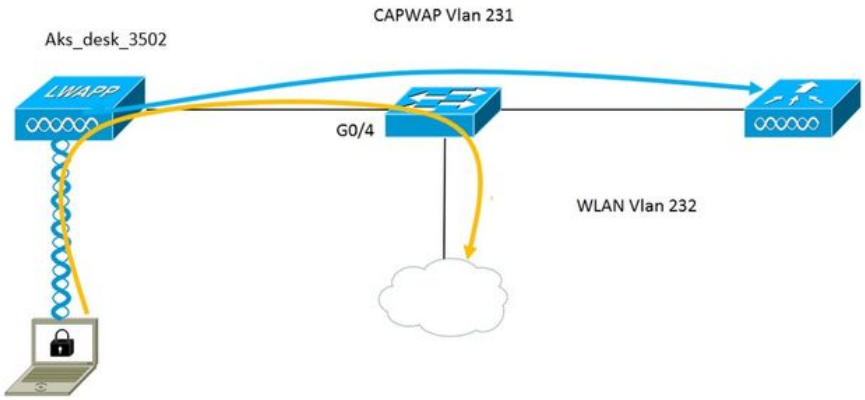
- WS-C3560CX-8PC-S, 15.2(4)E1
- LUCHT-CT-2504-K9, 8.2.141.0
- Identity Services Engine (ISE) 2.0
- IOS-gebaseerde access points (x500,x600,x700 Series).

Wave 2 AP's gebaseerd op AP OS ondersteunen flexiconnect hoofdpunt1x niet vanaf het tijdstip van dit schrijven.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerkdiagram



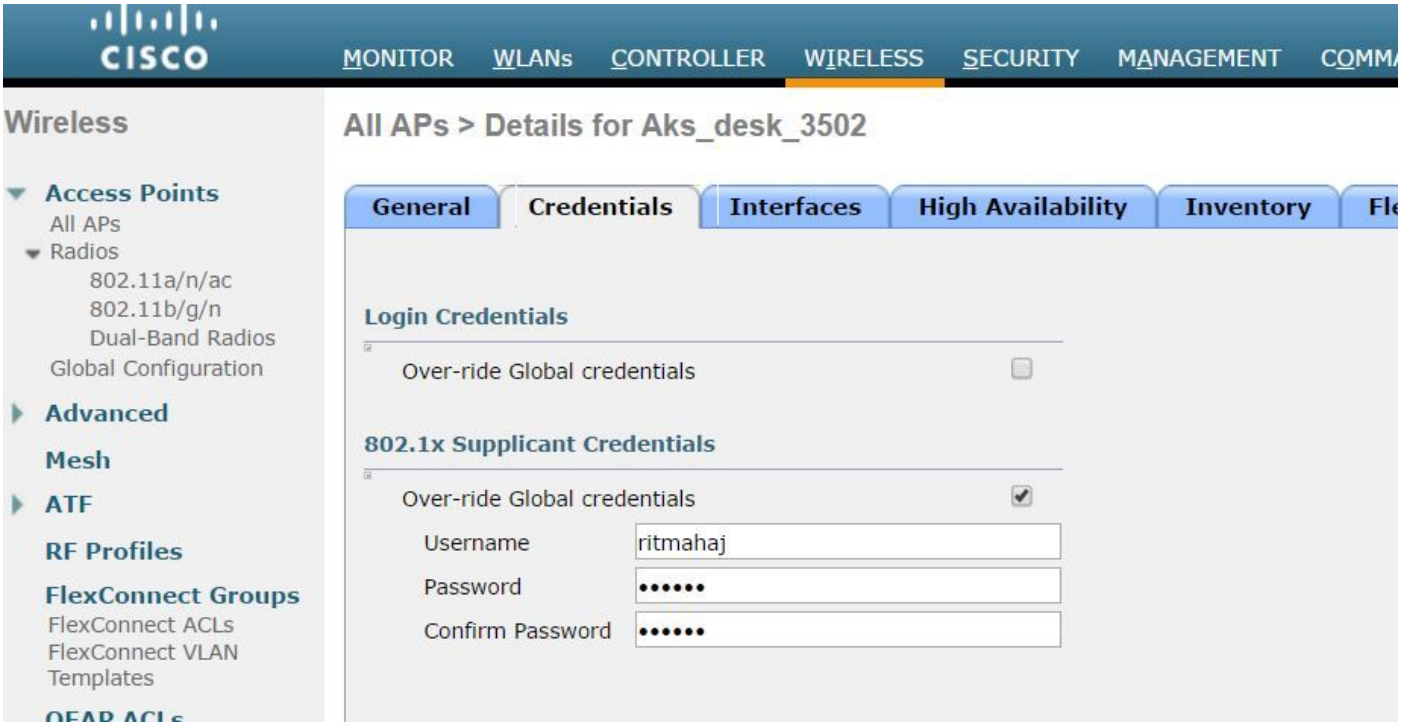
Bij deze instelling fungeert het toegangspunt als de 802.1x-smeekbede en wordt geauthentiseerd door de switch tegen ISE met behulp van EAP-FAST. Zodra de poort is ingesteld voor 802.1x-verificatie, laat de switch geen ander verkeer dan 802.1x-verkeer door de poort lopen totdat het apparaat dat is aangesloten op de poort authentiek verklaard heeft.

Zodra het toegangspunt voor authentiek verklaard tegen ISE is, ontvangt de switch "device-traffic-class=switch van Cisco VSA-kenmerk en beweegt hij automatisch de poort naar de romp.

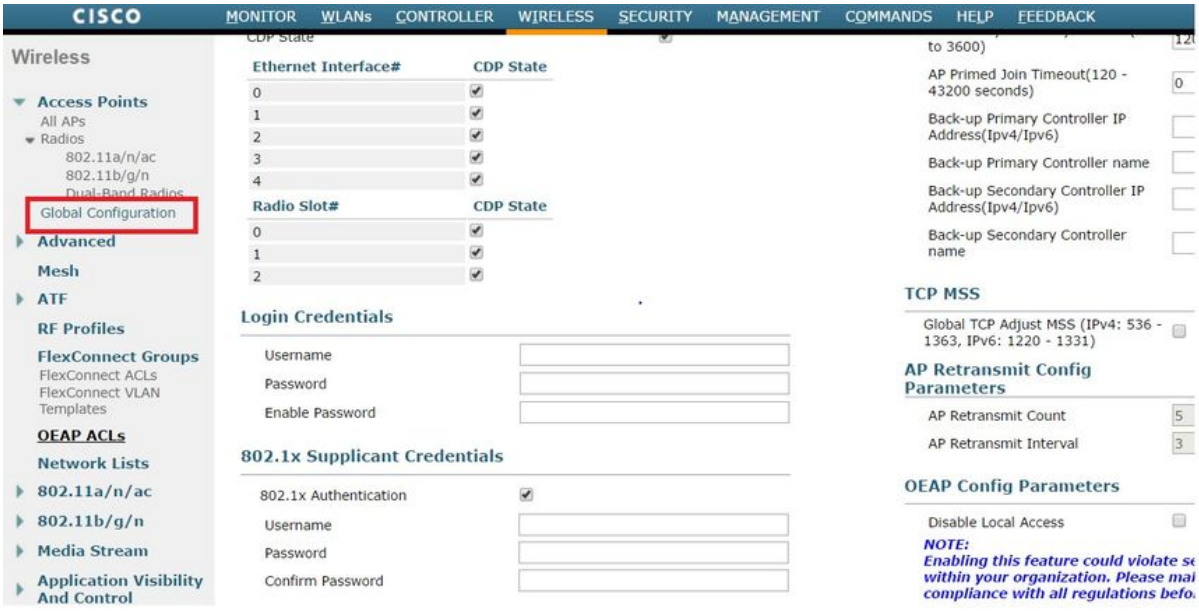
Dit betekent dat als AP de modus FlexConnect ondersteunt en SSID's lokaal is ingesteld, het gelabeld verkeer kan verzenden. Zorg ervoor dat de VLAN-ondersteuning is ingeschakeld op het AP en dat het juiste native VLAN is geconfigureerd.

AP configuratie:-

1. Als het AP reeds aan WLC is aangesloten, ga het tabblad Draadloos en klik op het access point. Gebruik het veld Gereedschappen en gebruik de optie 802.1x plus extra krediet, controleer het vakje **Gratis Global** aanmeldingsgegevens om de 802.1x-gebruikersnaam en het wachtwoord voor dit access point in te stellen.



U kunt ook een veel te gebruiken naam en wachtwoord instellen voor alle access points die aangesloten zijn op de WLC in het menu Global Configuration.



2. Als het access point nog niet bij een WLC is aangesloten, moet u console in de LAP troosten om de aanmeldingsgegevens in te stellen en deze CLI-opdracht te gebruiken:

CLI voor LAP#debug-kapconsole
LAP#capwap dot1x gebruikersnaam <gebruikersnaam> <wachtwoord>

Configuratie switch:-

1. Schakel punt1x in op de switch en voeg ISE-server aan switch toe

nieuw model

!
aaa authenticatiedot1x standaardgroepsstraal

!
Standaard autorisatienetwerk groepsstraal

!

dot1x systeem-automatische controle

!

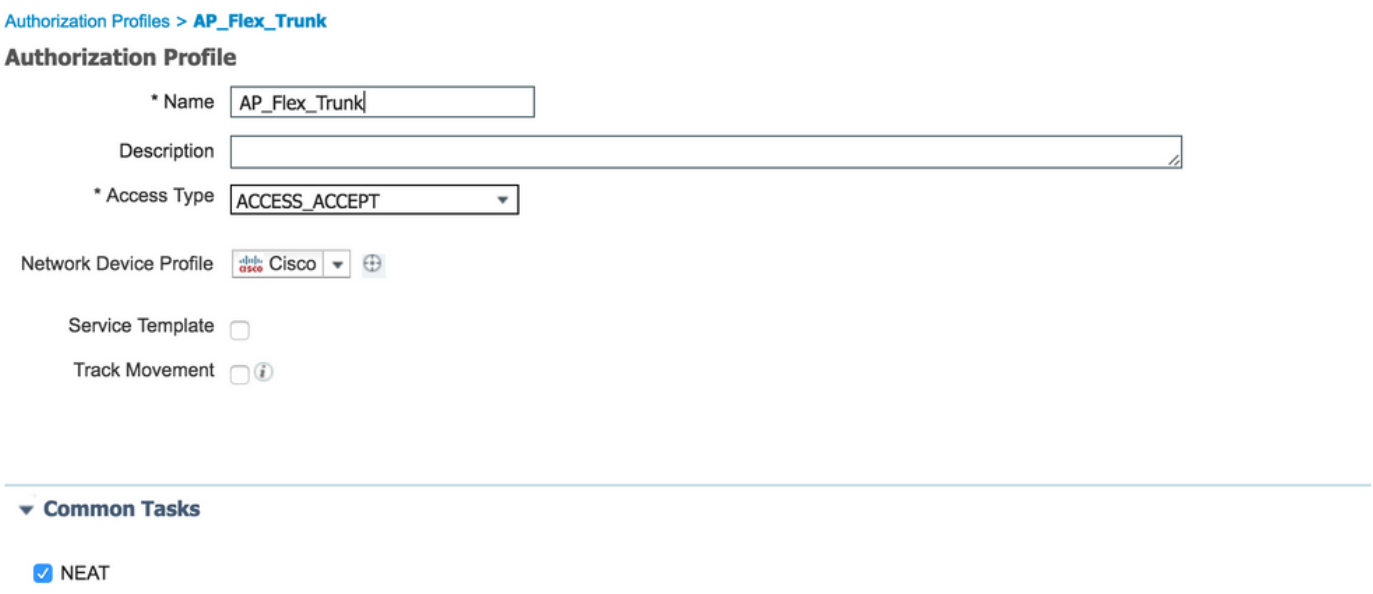
Straalserver ISE
adres ipv4 10.48.39.161 16-poorts 1645 poort 1646
 sleutel 7 123A0C0411045D5679

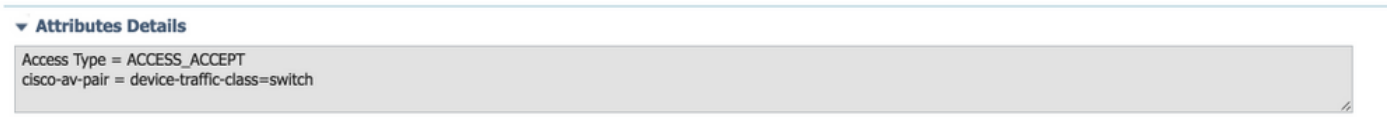
2. Stel nu de AP switch poort in

interface Gigabit Ethernet0/4
schakelpoort-toegangsnetwerk 231
schakelpoort-stam toegestaan VLAN 231.232
toegang tot de switchingmodus
authenticatie host-mode multi-host
echtheidscontrole dot1x
Verificatie van poortregelaar
dot1x pae-authenticator
over-boom draagrand

ISE-configuratie:-

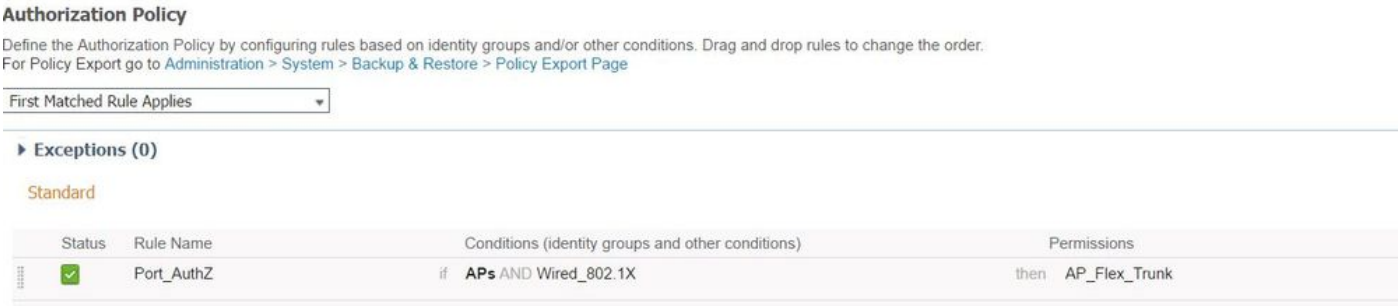
1. Op ISE kan NEAT voor het profiel met AP Authorization eenvoudig worden ingeschakeld om de juiste eigenschap op andere RADIUS-servers in te stellen. U kunt deze echter handmatig configureren.





2. Op ISE moet men ook het verificatiebeleid en het autorisatiebeleid configureren. In dit geval passen we de standaard authenticatieregel aan die wordt aangesloten op punt 1x, maar je kunt de regel aanpassen aan de eisen.

Wat betreft het autorisatiebeleid (Port_AuthZ) hebben we in dit geval de AP-referenties toegevoegd aan een gebruikersgroep (APs) en op basis hiervan het autorisatieprofiel (AP_Flex_Trunk) geduwd.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. In de switch, kan eens de opdracht "debug authenticatie optie autocfg all" gebruiken om te controleren of de poort al dan niet naar de boompoort wordt verplaatst.

20 feb. 12:34:18.19: %LINK-3-UPDOWN: Interface Gigabit Ethernet0/4, veranderde status in omhoog
20 feb. 12:34:19.122: %LINEPROTO-5-UPDOWN: Het protocol van de lijn op interface Gigabit Ethernet0/4, veranderde staat aan omhoog
akshat_sw#
akshat_sw#
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle: 3372220456
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Apparaattype = Switch
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] nieuwe client
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [GI0/4] Interne automatische afschermingsmacrotoepassingsstatus: 1
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Apparaattype: 2
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Automatische configuratie: stp heeft port_fig 0x8577D8
20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Automatische configuratie: stp port_fig heeft bpdu Guard_fig 2
20 feb. 12:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Op de poort van toepassing.
20 feb. 12:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] VLAN: VLAN-Str: 231
20 feb. 12:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Toepassing van dot1x_autocfg_supp macro
20 feb. 12:38:11.16: Bestellen toepassen... 'geen switchport toegang VLAN 231' bij Gi0/4

20 feb. 12:38:11.127: Bestellen toepassen... 'geen switchport nonegotiate' bij Gi0/4
20 feb. 12:38:11.127: Op bevel van toepassing... 'schakelport mode boomstam' op Gi0/4
20 feb. 12:38:11.134: Bezoek opdracht... 'switchport stam native vlan 231' bij Gi0/4
20 feb. 12:38:11.134: Op bevel toepassen... 'over-boom draagsnelle boomstam' bij Gi0/4
20 feb. 12:38:12.120: %LINEPROTO-5-UPDOWN: Het protocol van de lijn op interface Gigabit Ethernet0/4, veranderde staat in beneden
20 feb. 12:38:15.139: %LINEPROTO-5-UPDOWN: Het protocol van de lijn op interface Gigabit Ethernet0/4, veranderde staat aan omhoog

2. De output van "show run int g0/4" toont aan dat de poort is veranderd in een boomstampoort.

Huidige configuratie: 295 bytes
!
interface Gigabit Ethernet0/4
schakelpoort-stam toegestaan VLAN 231.232.239
switchport - moedertaal vlan 231
verbindingsmodems
authenticatie host-mode multi-host
echtheidscontrole dot1x
Verificatie van poortregelaar
dot1x pae-authenticator
boomstam
einde

3. Op ISE kan onder Operations> Radius Livelogs de echtheidscontrole succesvol zijn en kan het juiste autorisatieprofiel worden geduwd.

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. Als we een client daarna verbinden, wordt het mac-adres geleerd op de AP switch poort in client VLAN 232.

akshat_sw#sh mac adres-tabel int g0/4
Mac-adrestabel
—

VLAN-adrespoorten
— — — —
231 588d.0997.061d STATISCH Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC RGB0/4 - client

Op de WLC, in de details van de cliënt kan men zien dat deze cliënt vlan 232 behoort en SSID lokaal wordt geschakeld. Hier is een fragment.

(Cisco Controller) >Show client detail c0:ee:fb:d7:88:24
MAC-adres van client..... c0:ee:fb:d7:88:24
Gebruikersnaam client ..... N.v.t.
AP MAC-adres.....b4:14:89:82:cb:90
AP Naam..... Aks_desk_3502
Identificatie van AP-radiogateway.....1

Clientstaat..... geassocieerd
Clientgebruikersgroep.....
ClientNAC OOB-status..... Toegang
Draadloze LAN-id.....2
Draadloze LAN-netwerknaam (SSID)..... Poortaugustus
Naam draadloos LAN-profiel..... Poortkantoor
Hotspot (802.11u)..... Niet ondersteund
BSSID.....b4:14:89:82:cb:9f
Verbonden voor .....42 seconden
Kanaal.....44
IP-adres..... 192.168.232.90
Gateway-adres..... 192.168.232.1
Netmasker..... 255.255.255.0
Associatie-id.....
Verificatiealgoritme..... Open systeem
Reden code.....
Statuscode.....

FlexConnect Data Switching..... Lokaal
FlexConnect DHCP-status..... Lokaal
FlexConnect VLAN-gebaseerde Central-switching..... Nee
FlexConnect-verificatie..... Centraal
FlexConnect Central Association..... Nee
FlexConnect VLAN-NAAM..... VLAN 232
Quarantine VLAN.....0
Toegang tot VLAN.....232
Local Bridging VLAN.....232

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- Als de authenticatie faalt, gebruik **debug dot1x**, **debug authenticatie** opdrachten.
- Als de poort niet naar romp is verplaatst, voer de **debug authenticatie optie in die alle** opdracht **heeft** geautoriseerd.
- Verzeker u hebt multi-host modus (authenticatie host-mode multi-host) ingesteld. Multi-Host moet worden ingeschakeld om client draadloze MAC-adressen toe te staan.
- De opdracht "een autorisatienetwerk" moet zodanig zijn geconfigureerd dat de switch de door ISE verzonden eigenschappen accepteert en toepast.

Cisco IOS-gebaseerde access points ondersteunen alleen TLS 1.0. Dit kan een probleem veroorzaken als uw RADIUS-server is geconfigureerd om alleen TLS 1.2 802.1X-authenticaties toe te staan