Sichern Sie einen FlexConnect AP-Switchport mit Dot1x.

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration zur Sicherung von Switchports beschrieben, bei denen FlexConnect Access Points (AP) mit Dot1x authentifiziert werden. Dabei wird die Device-Traffic-Class=Switch Radius VSA verwendet, um den Datenverkehr von lokal geswitchten WLANs zuzulassen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FlexConnect auf Wireless LAN Controller (WLC)
- 802.1x auf Cisco Switches
- NetzwerkEdge-Authentifizierungstopologie (NEAT)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Identity Service Engine (ISE) 2.0
- IOS-basierte Access Points (Serie x500, x600, x700)

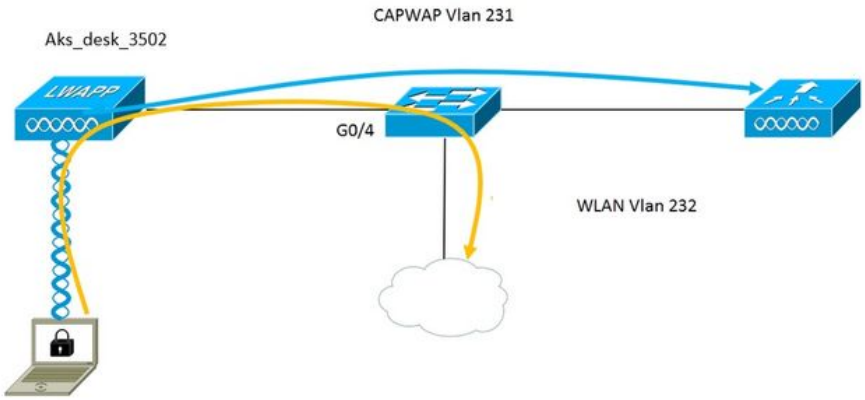
Wave 2 APs mit AP-Betriebssystem unterstützen zum Zeitpunkt der Erstellung dieses Dokuments nicht den Flexconnect-Trunk1x.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



In dieser Konfiguration fungiert der Access Point als 802.1x-Komponente und wird vom Switch mithilfe von EAP-FAST gegen ISE authentifiziert. Nachdem der Port für die 802.1x-Authentifizierung konfiguriert wurde, lässt der Switch zu, dass außer 802.1x-Datenverkehr kein Datenverkehr den Port durchläuft, bis das mit dem Port verbundene Gerät erfolgreich authentifiziert wird.

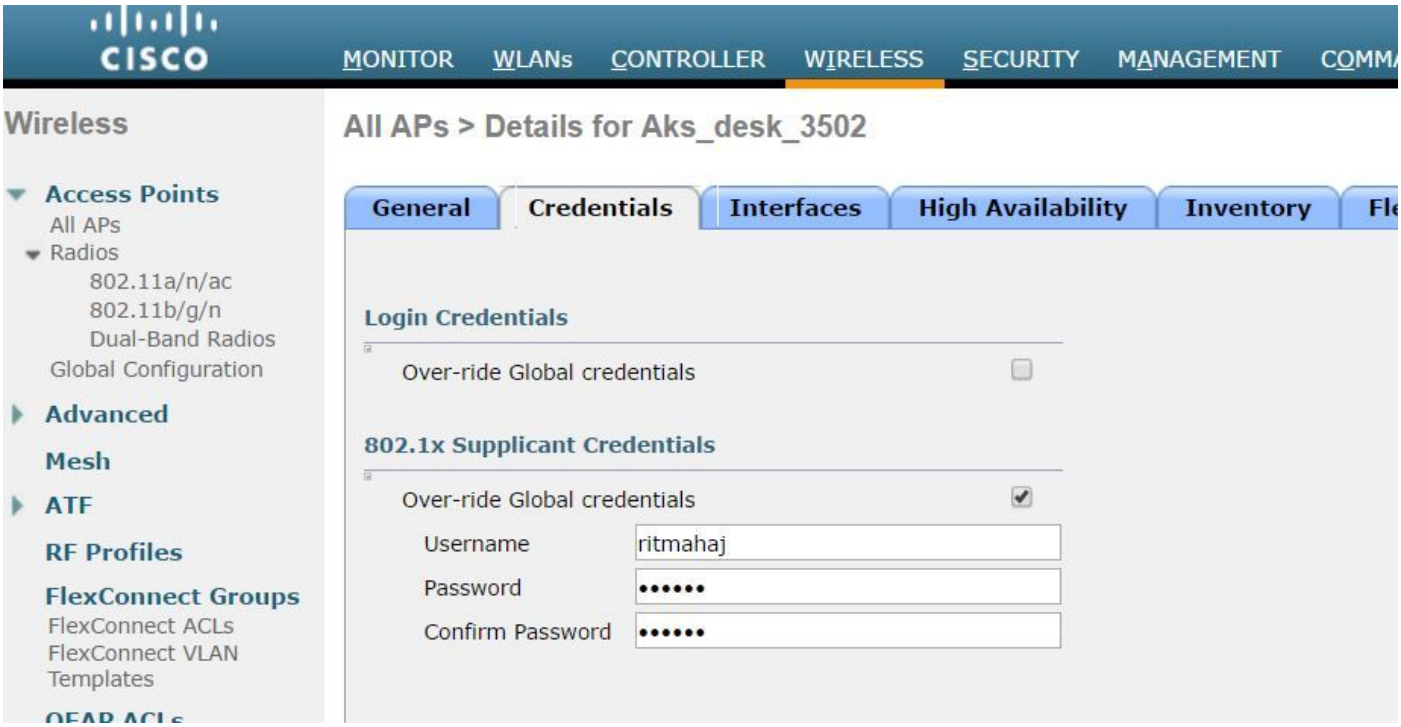
Sobald sich der Access Point erfolgreich gegen die ISE authentifiziert, erhält der Switch das Cisco VSA-Attribut "device-traffic-class=switch" und verschiebt den Port automatisch in den Trunk.

Wenn der Access Point den FlexConnect-Modus unterstützt und lokal geswitchte SSIDs konfiguriert hat, kann er getaggten Datenverkehr senden. Stellen Sie sicher, dass die VLAN-Unterstützung für den AP aktiviert ist und das richtige native VLAN konfiguriert ist.

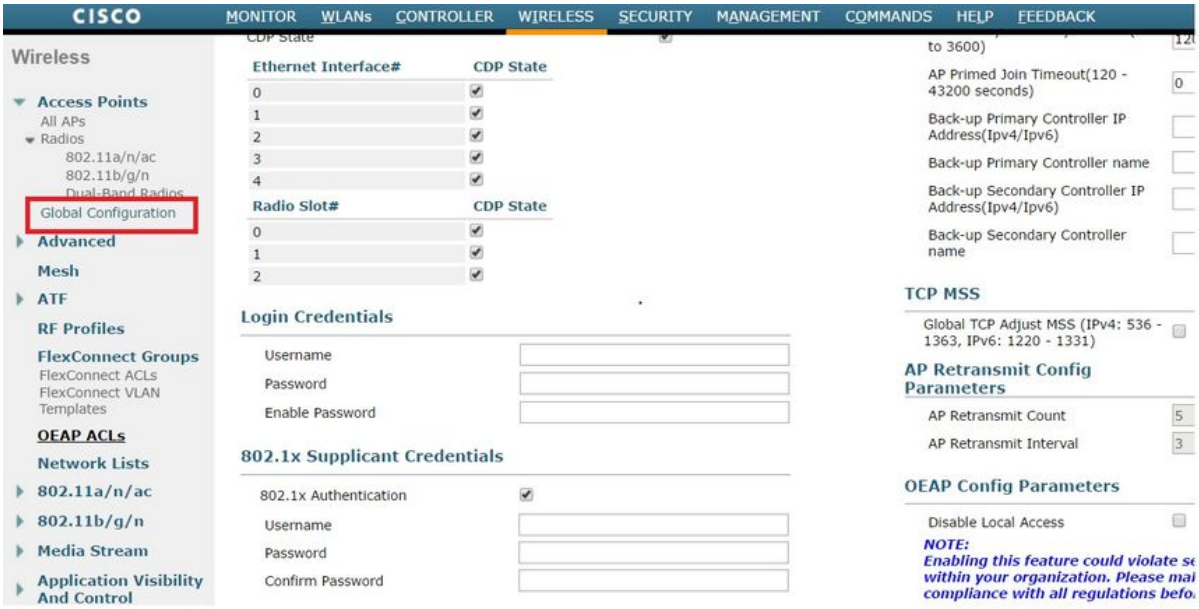
AP-Konfiguration:-

1. Wenn der Access Point bereits dem WLC beigetreten ist, wechseln Sie zur Registerkarte Wireless und klicken Sie auf den Access Point. Aktivieren Sie im Feld "Credetials" unter der Überschrift "802.1x Supplicant Credentials" das Feld **Over-ride Global Credentials (Globale Anmeldeinformationen für** 802.1x), um den 802.1x-Benutzernamen und das Kennwort für diesen

Access Point festzulegen.



Sie können auch einen Befehlsbenutzernamen und ein Kennwort für alle Access Points festlegen, die mit dem Menü "Global Configuration" (Globale Konfiguration) zum WLC hinzugefügt werden.



2. Wenn der Access Point noch nicht zu einem WLC hinzugefügt wurde, müssen Sie sich in die LAP einwählen, um die Anmeldeinformationen festzulegen, und den folgenden CLI-Befehl verwenden:

LAP#debug CAWAP-Konsolencli
LAP#capwap AP dot1x Benutzername <Benutzername> Kennwort <Kennwort>

Switch-Konfiguration:-

1. Aktivieren Sie dot1x auf dem Switch global und fügen Sie den ISE-Server zum Switch hinzu

aaa neues Modell

!
aaa authentication dot1x Standardgruppenradius

!
aaaa-Autorisierungsnetzwerk-Standardgruppenradius

!

802.1x-System-Auth-Control

!

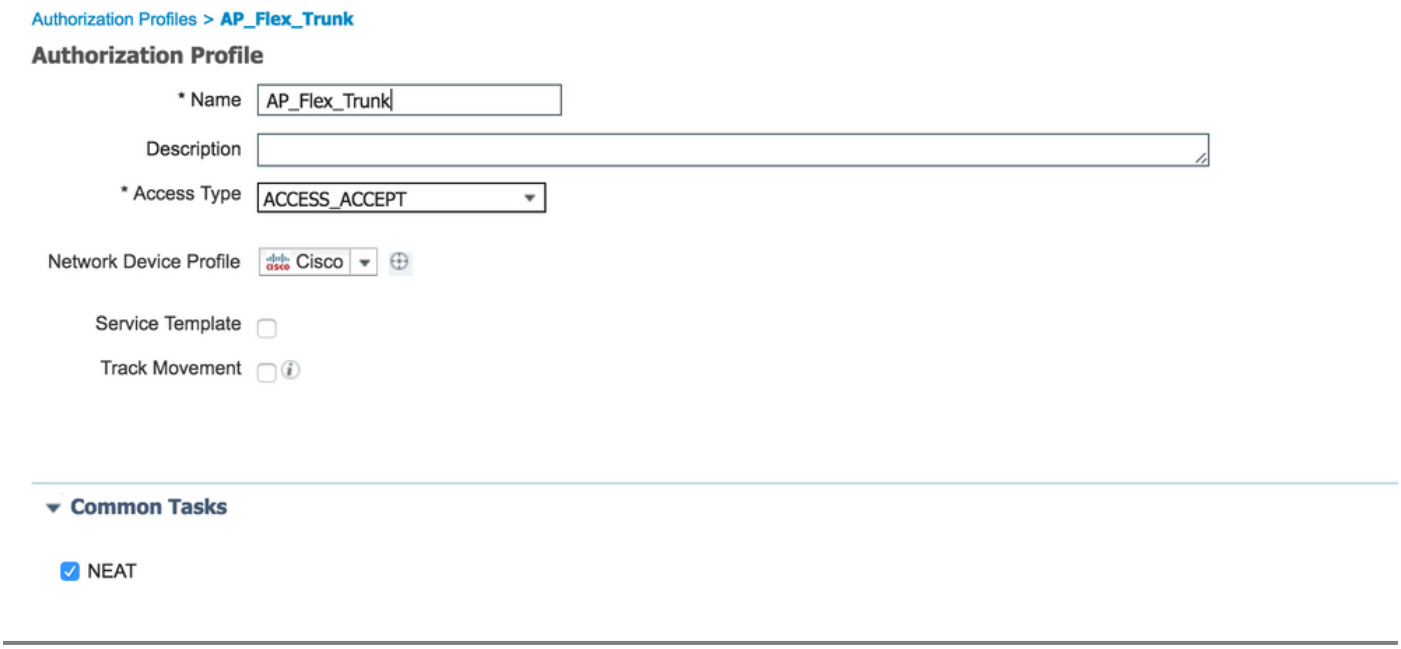
Radius-Server-ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
 Taste 7 123A0C0411045D5679

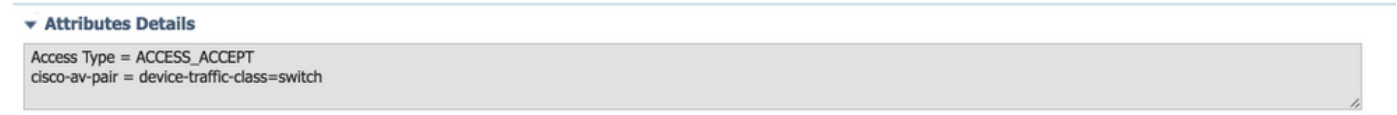
2. Konfigurieren Sie jetzt den AP-Switch-Port.

interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231.232
Switchport-Moduszugriff
Authentifizierung im Host-Modus Multi-Host
Authentifizierungsart dot1x
Authentifizierung Port Control Auto
dot1x page-Authentifizierer
Spanning-Tree-Port-Fast-Edge

ISE-Konfiguration:-

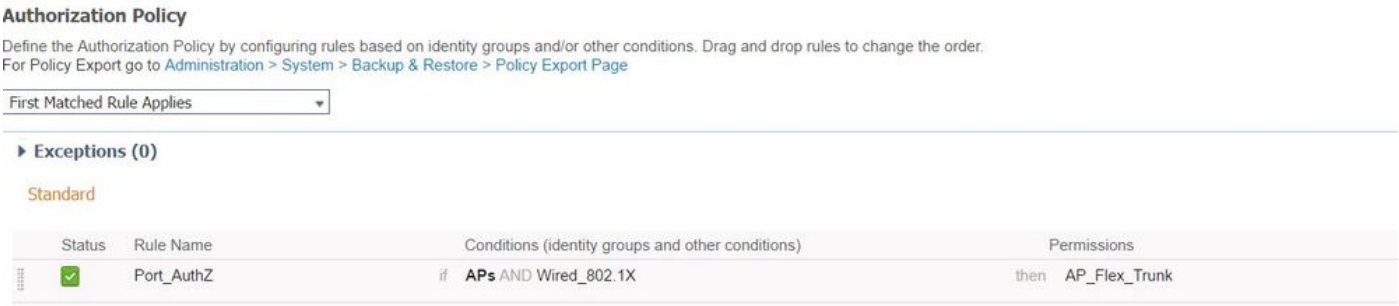
1. Auf der ISE kann man einfach NEAT für das AP-Autorisierungsprofil aktivieren, um das richtige Attribut festzulegen. Auf anderen RADIUS-Servern können Sie die Konfiguration jedoch manuell vornehmen.





2. Auf der ISE müssen außerdem die Authentifizierungsrichtlinie und die Autorisierungsrichtlinie konfiguriert werden. In diesem Fall haben wir die Standardauthentifizierungsregel getroffen, die 802.1x-800-800-800-1000-1000-1000-100-1000-100-100-100 ist. Sie können sie jedoch je nach Bedarf anpassen.

Was die Autorisierungsrichtlinie (Port_AuthZ) angeht, haben wir die AP-Anmeldeinformationen einer Benutzergruppe (APs) hinzugefügt und das darauf basierende Authorization Profile (AP_Flex_Trunk) weitergeleitet.



Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Auf dem Switch kann einmal mit dem Befehl "debug authentication feature autocfg all" überprüfen, ob der Port an den Trunk-Port verschoben wird oder nicht.

20.02.2012:34:18.119: %LINK-3-UPDOWN: Schnittstelle GigabitEthernet0/4, Status geändert auf aktiv
20.02.2012:34:19.122: %LINEPROTO-5-UPDOWN: Leitungsprotokoll auf Schnittstelle GigabitEthernet0/4, Status geändert zu aktiv
akshat_sw#
akshat_sw#

20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle: 3372220456
20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Gerätetyp = Switch
20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] neuer Client
20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Interner Autocfg-Makro-Anwendungsstatus: 1
20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Gerätetyp: 2
20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Automatische Konfiguration: stp hat port_config 0x85777D8
20.02.12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Automatische Konfiguration: stp port_config hat bpdu guard_config 2
20.02.2012:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Anwendung von Auto-cfg auf den Port.
20.02.2012:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] VLAN: 231 VLAN-Str.: 231
20.02.2012:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Anwenden des 80.1x_autocfg_supp-Makros
20.02.2012:38:11.16: Anwendung von Befehl.. "no switchport access vlan 231" bei Gi0/4
20.02.2012:38:11.127: Anwendung von Befehl.. "no switchport nonegotiate" bei Gi0/4
20.02.2012:38:11.127: Anwendung von Befehl.. 'switchport mode trunk' an Gi0/4
20.02.2012:38:11.134: Anwendung von Befehl.. 'switchport trunk native vlan 231' at Gi0/4
20.02.2012:38:11.134: Anwendung von Befehl.. "spanning-tree portfast trunk" bei Gi0/4
20.02.2012:38:12.120: %LINEPROTO-5-UPDOWN: Leitungsprotokoll auf Schnittstelle GigabitEthernet0/4, Status auf "Down" eingestellt
20.02.2012:38:15.139: %LINEPROTO-5-UPDOWN: Leitungsprotokoll auf Schnittstelle GigabitEthernet0/4, Status geändert zu aktiv

2. Die Ausgabe von "show run int g0/4" zeigt an, dass der Port zu einem Trunk-Port geändert wurde.

Aktuelle Konfiguration: 295 Byte
!
interface GigabitEthernet0/4
switchport trunk allowed vlan 231.232.239
switchport trunk native vlan 231
Trunk im Switch-Port-Modus
Authentifizierung im Host-Modus Multi-Host
Authentifizierungsart dot1x
Authentifizierung Port Control Auto
dot1x page-Authentifizierer
Spanning-Tree-Port-Fast-Edge-Trunk
Ende

3. Auf der ISE kann unter Operations>>Radius Livelogs die Authentifizierung erfolgreich durchgeführt und das richtige Autorisierungsprofil gesendet werden.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
	All								
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. Wenn wir danach einen Client anschließen, wird seine MAC-Adresse auf dem AP-Switch-Port im Client-VLAN 232 gelernt.

akshat_sw#sh mac-Adresstabelle int g0/4
MAC-Adresstabelle
—

VLAN MAC-Adresstyp-Ports
— — — — — —
231 588d.0997.061d STATIC Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Client

Auf dem WLC ist im Client-Detail zu erkennen, dass dieser Client VLAN 232 gehört und die SSID lokal geschaltet ist. Hier ist ein Ausschnitt.

(Cisco Controller) >show client detail c0:ee:fb:d7:88:24
MAC-Adresse des Clients..... c0:ee:fb:d7:88:24
Client-Benutzername ..... –
AP-MAC-Adresse..... b4:14:89:82:cb:90
AP-Name..... OK_desk_3502
AP-Funksteckplatz-ID..... 1
Status des Kunden..... Zugeordnet
Client-Benutzergruppe.....
Status des Client NAC OOB ..... Zugriff
Wireless LAN-ID..... 2
Name des Wireless LAN-Netzwerks (SSID)..... Port-Auth
WLAN-Profilname..... Port-Authentifizierung
Hotspot (802.11u)..... Nicht unterstützt
BSSID..... b4:14:89:82:cb:9f
Verbunden für ..... 42 s
Kanal..... 44
IP-Adresse..... 192.168.232.90
Gateway-Adresse..... 192.168.232.1
Netzmaske..... 255.255.255.0
Zuordnungs-ID..... 1
Authentifizierungsalgorithmus..... Offenes System
Ursachencode..... 1
Statuscode..... 0

FlexConnect Data Switching..... Lokal
FlexConnect DHCP-Status..... Lokal
FlexConnect VLAN-basiertes zentrales Switching..... Nein
FlexConnect-Authentifizierung..... Zentral
FlexConnect Central Association..... Nein
FlexConnect VLAN NAME..... VLAN 232
Quarantäne-VLAN..... 0
Zugriffs-VLAN..... 232
Lokales Bridging-VLAN..... 232

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

- Wenn die Authentifizierung fehlschlägt, verwenden Sie die Befehle **debug dot1x**, **debug authentication**.

- Wenn der Port nicht in den Trunk verschoben wird, geben Sie den Befehl **debug authentication feature autocfg all** ein.
- Stellen Sie sicher, dass der Multi-Host-Modus (Authentifizierung Host-Modus Multi-Host) konfiguriert ist. Multi-Host muss aktiviert sein, um Client-Wireless-MAC-Adressen zuzulassen.
- Der Befehl "aaa authorized network" muss konfiguriert werden, damit der Switch die von der ISE gesendeten Attribute akzeptiert und anwendet.

Cisco IOS-basierte Access Points unterstützen nur TLS 1.0. Dies kann zu einem Problem führen, wenn Ihr RADIUS-Server so konfiguriert ist, dass nur TLS 1.2 802.1X-Authentifizierungen zugelassen werden.