Dot1x を使用して FlexConnect AP スイッチポートを保護するための設定

目次

概要

このドキュメントで説明するスイッチポートを保護するための設定では、FlexConnect アクセスポイント（AP）がローカルでスイッチされるワイヤレス LAN（WLAN）からのトラフィックを許可するために、Dot1x で device-traffic-class=switch Radius VSA を使用して認証を行います。

前提条件

要件

次の項目に関する知識が推奨されます。

- ワイヤレス LAN コントローラ（WLC）上の FlexConnect
- Cisco スイッチ上の 802.1x
- ネットワーク エッジ認証トポロジ（NEAT）

使用するコンポーネント

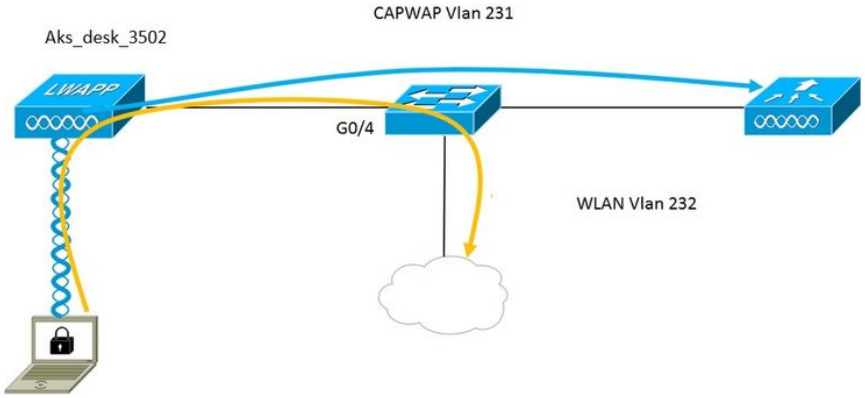
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- WS-C3560CX-8PC-S、15.2(4)E1
- AIR-CT-2504-K9、8.2.141.0
- Identity Service Engine（ISE）2.0

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

ネットワーク図



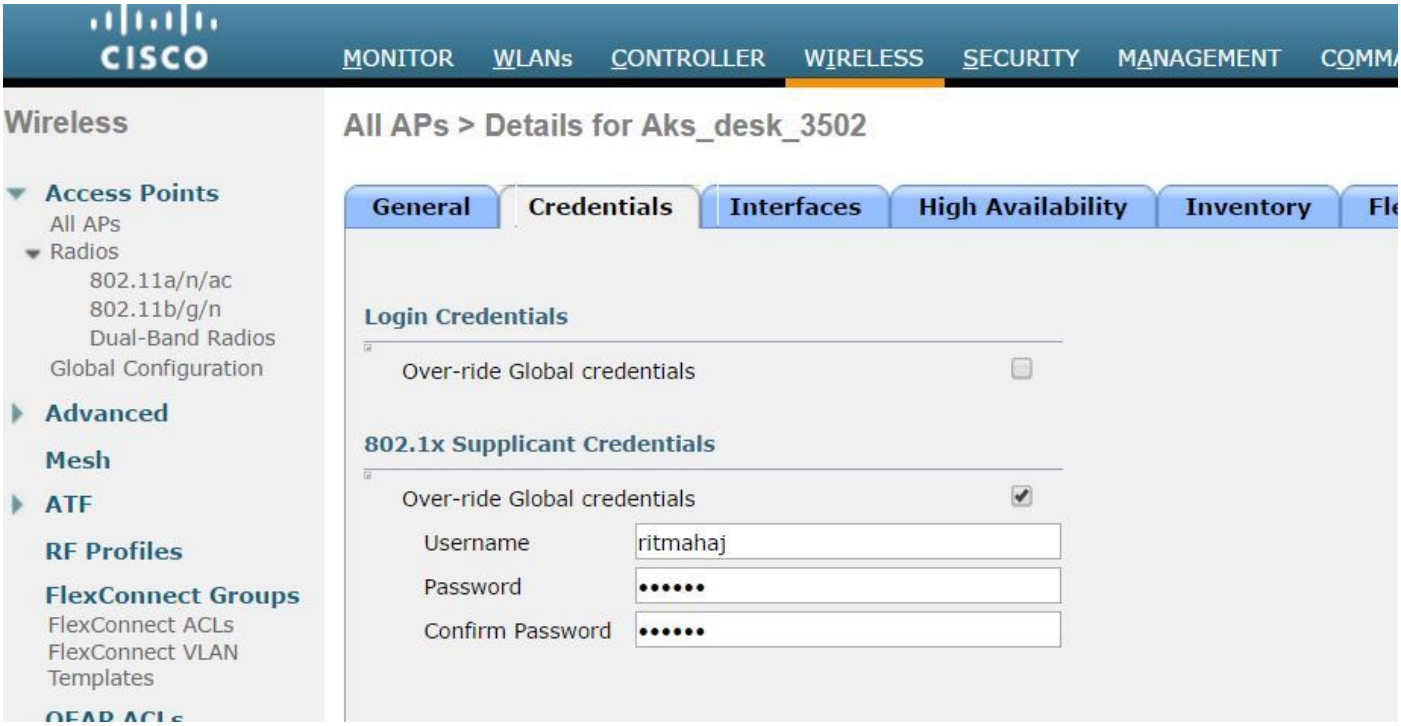
この設定では、アクセス ポイントが 802.1x サプリカントとして機能します。スイッチは ISE に対し、EAP-FAST を使用してアクセス ポイントを認証します。 802.1x 認証用のポートが設定されると、スイッチは、ポートに接続されたデバイスが正しく認証されるまでは、802.1x トラフィック以外のトラフィックがポートを通過することを許可しません。

ISE に対するアクセス ポイントの認証が成功すると、スイッチは Cisco VSA 属性 device-traffic-class=switch を受け取り、自動的にポートをトランクに移動します。

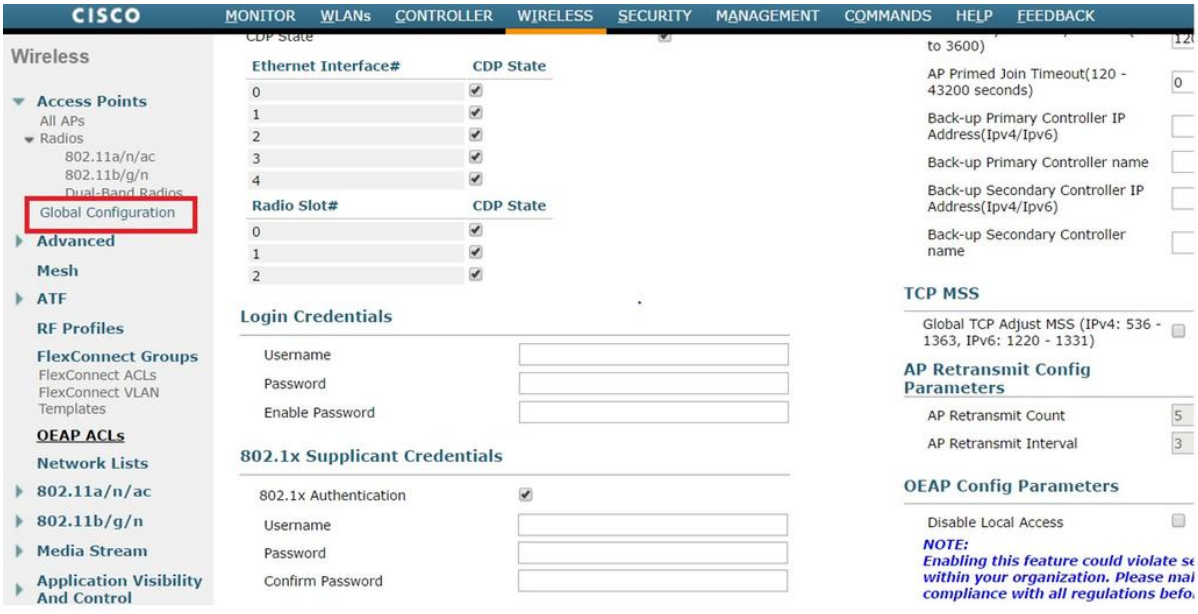
つまり、FlexConnect モードをサポートする AP に、ローカルでスイッチされる SSID が設定されている場合、その AP はタグ付けされたトラフィックを送信することができます。 AP で VLAN サポートが有効にされて、正しいネイティブ VLAN が設定されていることを確認してください。

AP の設定： -

1. AP がすでに WLC に参加している場合は、[Wireless] タブに移動し、該当するアクセス ポイントをクリックします。 [Credetials] フィールドに移動し、[802.1x Supplicant Credentials]見出しの下にある [Over-ride Global credentials] ボックスをクリックして、このアクセス ポイントの 802.1x ユーザ名およびパスワードを設定します。



[Global Configuration] メニューを使用して、WLC に参加しているすべてのアクセス ポイントに共通のユーザ名とパスワードを設定することもできます。



2. アクセスポイントがまだ WLC に参加していない場合、以下のコマンドを使用して、LAP のコンソールに移動して、クレデンシャルを設定する必要があります。

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

スイッチの設定： -

1. スイッチで dot1x をグローバルに有効にし、ISE サーバを追加します

```
aaa new-model

!!
aaa authentication dot1x default group radius

!!
aaa authorization network default group radius

!!

dot1x system-auth-control

!!

radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
 key 7 123A0C0411045D5679
```

2. 次に、AP スイッチ ポートを設定します。

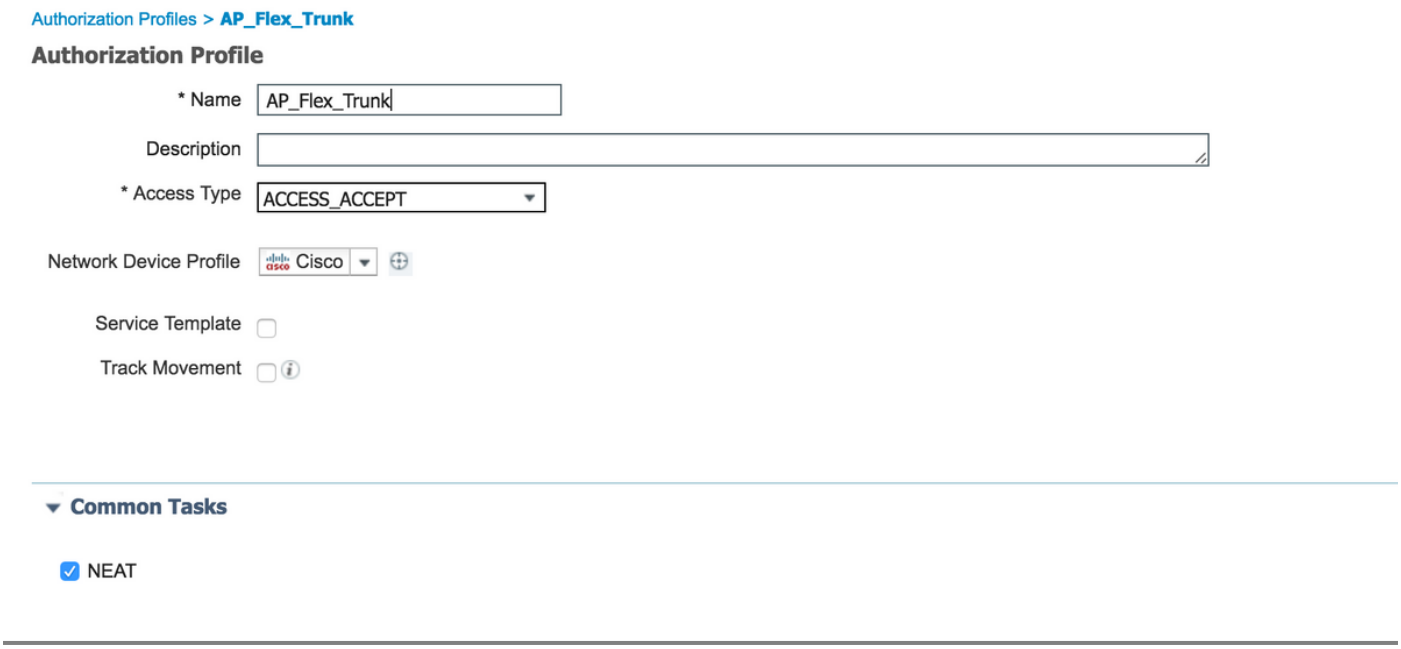
```
interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231232
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfastedge
```

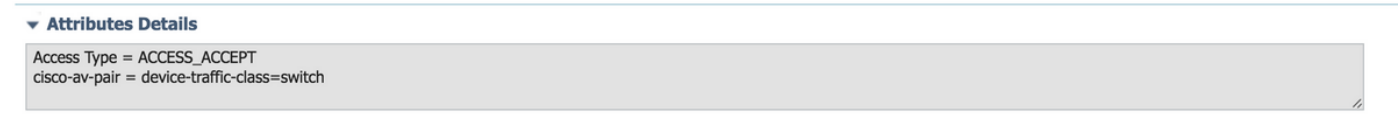
dot1x ではなく MAB を設定する場合、ポートの設定は以下のようになります。 -

```
interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231232
switchport mode access
authentication host-mode multi-host
authentication order mab
authentication port-control auto
mab
spanning-tree portfastedge
```

ISE の設定： -

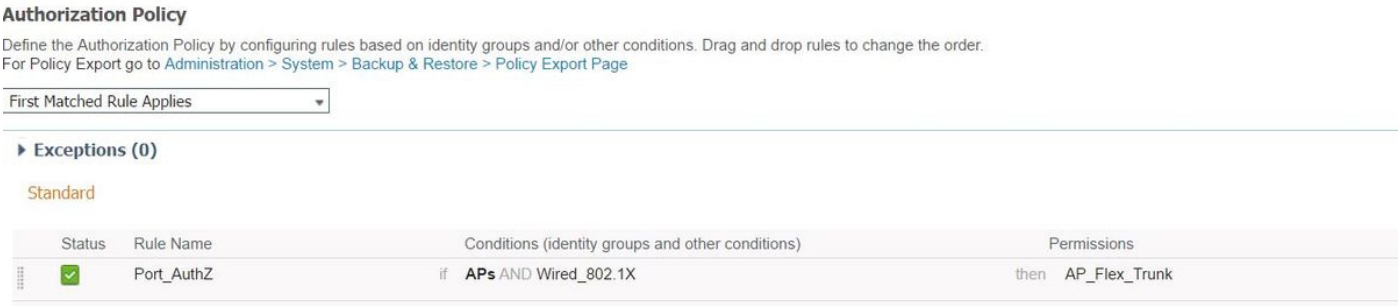
1. ISE では、AP 許可プロファイルに NEAT を有効にするだけで正しい属性を設定できます。一方、その他の RADIUS サーバでは手動で設定することができます。





2. ISE では、認証ポリシーと許可ポリシーを設定する必要もあります。 この例では有線 dot.1x（MAB の場合は有線 MAB）であるデフォルトの認証ルールを見つけましたが、要件に応じて認証ポリシーをカスタマイズすることもできます。

AP 許可ポリシー（Port_AuthZ）については、この例では AP クレデンシャルをユーザ グループ（AP）に追加し、それをベースに許可プロファイル（AP_Flex_Trunk）をプッシュしました。



確認

ここでは、設定が正常に動作していることを確認します。

1. スイッチで、コマンド「debug authentication feature autocfg all」を使用することで、ポートがトランク ポートに移動しているかどうかを確認できます。

Feb 20 12:34:18.119: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changed state to up
Feb 20 12:34:19.122: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4, changed state to up
akshat_sw#
akshat_sw#
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle: 3372220456
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Device Type =

Switch
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] new client
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Internal Autocfg Macro Application Status : 1
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Device type : 2
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp has port_config 0x85777D8
Feb 20 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp port_config has bpdu guard_config 2
Feb 20 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Applying auto-cfg on the port.
Feb 20 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: 231 Vlan-Str: 231
Feb 20 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Applying dot1x_autocfg_supp macro
Feb 20 12:38:11.116: Applying command... "no switchport access vlan 231' at Gi0/4
Feb 20 12:38:11.127: Applying command... "no switchport nonegotiate' at Gi0/4
Feb 20 12:38:11.127: Applying command... "switchport mode trunk' at Gi0/4
Feb 20 12:38:11.134: Applying command... "switchport trunk native vlan 231' at Gi0/4
Feb 20 12:38:11.134: Applying command... "spanning-tree portfast trunk' at Gi0/4
Feb 20 12:38:12.120: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4, changed state to down
Feb 20 12:38:15.139: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4, changed state to up

2. 「show run int g0/4」の出力に、ポートがトランク ポートに変更されたことが示されます。

Current configuration : 295 bytes
!!
interface GigabitEthernet0/4
switchport trunk allowed vlan 231232239
switchport trunk native vlan 231
switchport mode trunk
authentication host-mode multi-host
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfastedge trunk
最後

3. ISE で、[Operations] > [Radius Livelogs] に移動すると、認証が成功し、正しい許可プロファイルがプッシュされていることを確認できます。

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. これを確認した後、クライアントを接続すると、クライアント VLAN 232 の AP スイッチ ポートでその AMC アドレスが学習されます。

akshat_sw#sh mac address-table int g0/4
Mac Address Table

```
Vlan    Mac Address       Type        Ports
---- ----------- -------- -----
231 588d.0997.061d STATIC Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Client
```

WLC 上のクライアント詳細で、このクライアントが VLAN 232 に属していること、SSID ローカルでスイッチされることを確認できます。 以下にスニペットを記載します。

```
(Cisco Controller) >show client detail c0:ee:fb:d7:88:24
Client MAC Address.....c0:ee:fb:d7:88:24
Client Username .....N/A
AP MAC Address.....b4:14:89:82:cb:90
AP Name..... Aks_desk_3502
AP radio slot Id..... 1
Client State..... Associated
Client User Group.....
Client NAC OOB State..... access
Wireless LAN Id..... 2
Wireless LAN Network Name (SSID)..... Port-Auth
Wireless LAN Profile Name..... Port-auth
Hotspot (802.11u)..... サポート対象外
BSSID.....b4:14:89:82:cb:9f
Connected For .....42 secs
Channel..... 44
IP Address..... 192.168.232.90
Gateway Address..... 192.168.232.1
Netmask..... 255.255.255.0
Association Id..... 1
Authentication Algorithm..... Open System
Reason Code..... 1
Status Code..... 0

FlexConnect Data Switching..... Local
FlexConnect Dhcp Status..... Local
FlexConnect Vlan Based Central Switching..... なし
FlexConnect Authentication..... セントラル
FlexConnect Central Association..... なし
FlexConnect VLAN NAME.....vlan 232
Quarantine VLAN..... 0
Access VLAN..... 232
Local Bridging VLAN..... 232
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- 認証が失敗する場合は、**debug dot1x** コマンドおよび **debug authentication** コマンドを使用します。
- ポートがトランクに移動しない場合は、**debug authentication feature autocfg all** コマンドを入力します。
- マルチホスト モード（ authentication host-mode multi-host ）が設定されていることを確認します。 クライアント ワイヤレス MAC アドレスを許可するためには、マルチホストが有効にされている必要があります。

- "スイッチが ISE から送信された属性を受け入れて適用するようにするためには、「aaa authorization network」コマンドを設定する必要があります。