

Dot1xを使用したFlexconnect APスイッチポートの保護

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[APの設定:](#)

[スイッチの設定](#)

[ISEの設定:](#)

[確認](#)

[トラブルシューティング](#)

[参考資料](#)

概要

このドキュメントでは、FlexConnectアクセスポイント(AP)がDot1xで認証されるスイッチポートを保護するための設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 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いています。

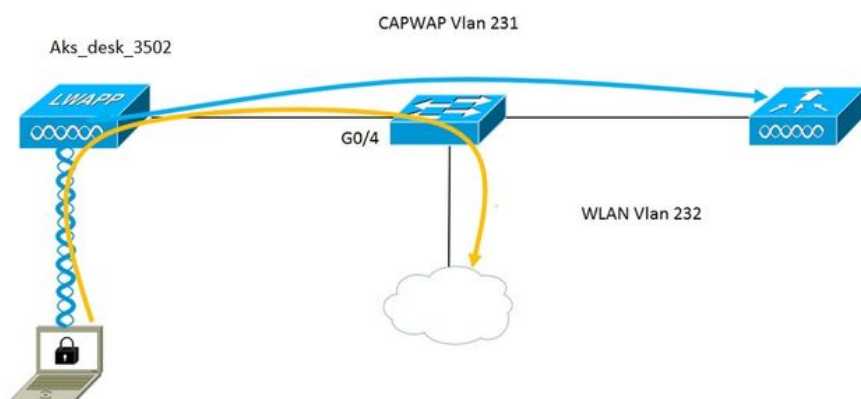
- WS-C3560CX-8PC-S、15.2(4)E1
- AIR-CT-2504-K9、8.2.141.0
- Identity Service Engine (ISE) 2.0
- IOSベースのアクセスポイント (x500、x600、x700シリーズ)

このドキュメントの作成時点では、AP OSに基づくWave 2 APはflexconnectトランクdot1xをサポートしていません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



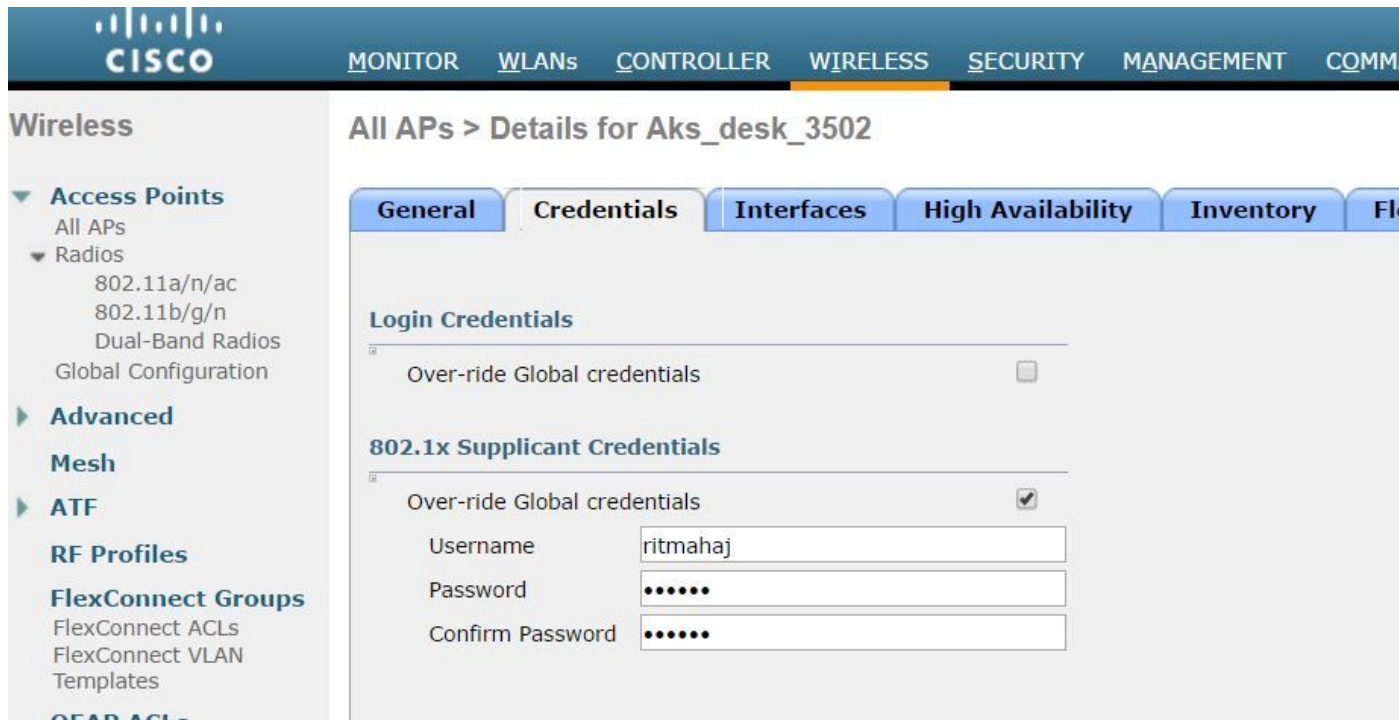
この設定では、アクセスポイントが 802.1x サブリカントとして機能します。スイッチは ISE に対し、EAP-FAST を使用してアクセスポイントを認証します。802.1x 認証用のポートが設定されると、スイッチは、ポートに接続されたデバイスが正しく認証されるまでは、802.1x トラフィック以外のトラフィックがポートを通過することを許可しません。

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、APがFlexConnectモードをサポートし、ローカルでスイッチされるSSIDが設定されている場合、タグ付きトラフィックを送信できます。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に加入している場合は、Wirelessタブに移動してアクセスポイントをクリックします。[Credentials] 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。



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMM'. The left sidebar shows the 'Wireless' menu with options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'All APs > Details for Aks_desk_3502' and has tabs for 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', and 'Flex'. The 'Credentials' tab is active, showing 'Login Credentials' and '802.1x Supplicant Credentials' sections. In the '802.1x Supplicant Credentials' section, the 'Over-ride Global credentials' checkbox is checked, and the 'Username' field contains 'ritmahaj', while the 'Password' and 'Confirm Password' fields are masked with dots.

[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。

The screenshot shows the Cisco Wireless configuration interface. The left sidebar contains a navigation menu with 'Global Configuration' highlighted. The main content area is divided into several sections:

- Ethernet Interface# CDP State:** A table with columns for Ethernet Interface# (0-4) and CDP State (checked).
- Radio Slot# CDP State:** A table with columns for Radio Slot# (0-2) and CDP State (checked).
- Login Credentials:** Fields for Username, Password, and Enable Password.
- 802.1x Supplicant Credentials:** A checkbox for 802.1x Authentication (checked) and fields for Username, Password, and Confirm Password.
- TCP MSS:** A section for Global TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331).
- AP Retransmit Config Parameters:** Fields for AP Retransmit Count (5) and AP Retransmit Interval (3).
- OEAP Config Parameters:** A checkbox for Disable Local Access.

A note at the bottom states: **NOTE:** Enabling this feature could violate security within your organization. Please maintain compliance with all regulations before.

2. アクセスポイントがまだWLCに参加していない場合、LAPにコンソール接続してクレデンシャルを設定し、次のCLIコマンドを使用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サーバをスイッチに追加する

```
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. 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
```

ISE の設定 :

1. ISEでは、AP認可プロファイルのNEATを有効にするだけで正しい属性を設定できますが、他のRADIUSサーバでは手動で設定できます。

[Authorization Profiles > AP_Flex_Trunk](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile 

Service Template

Track Movement 

▼ Common Tasks

NEAT

▼ Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = device-traffic-class=switch

2. ISEでは、認証ポリシーと認可ポリシーも設定する必要があります。この場合、デフォルトの認証ルールである有線dot1xに一致しますが、要件に応じてカスタマイズできます。

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。

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Port_AuthZ	if APs AND Wired_802.1X	then AP_Flex_Trunk

確認

このセクションでは、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」を使用して、ポートがトランクポートに移動されているかどうかを確認します。

```
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#
2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: 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」の出力は、ポートがトランクポートに変更されたことを示しています。

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のOperations>>Radius Livelogsで、認証が成功し、正しい認可プロファイルがプッシュされた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
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.この後でクライアントを接続すると、そのMACアドレスがクライアントVLAN 232のAPスイッチポートで学習されます。

```
akshat_sw#sh mac address-table int g0/4
MACアドレステーブル
```

```
-----
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
クライアントユーザ名.....N/A
AP MAC Address.....b4:14:89:82:cb:90
AP Name.....Aks_desk_3502
AP無線スロットID..... 1
Client State.....Associated
Client User Group.....
Client NAC OOB State.....Access
ワイヤレス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 For42 secs
チャネル..... 44
IPアドレス..... 192.168.232.90
Gateway Address.....192.168.232.1
ネットマスク..... 255.255.255.0
関連付けId..... 1
Authentication Algorithm.....Open System
理由コード..... 1
ステータスコード..... 0

FlexConnect Data Switching.....Local
FlexConnect Dhcp Status.....Local
FlexConnect Vlan Based Central Switching.....いいえ
FlexConnect Authentication.....Central
FlexConnect Central Association.....いいえ
FlexConnect VLAN NAME.....vlan 232
検疫VLAN.....0
アクセスVLAN..... 232
ローカルブリッジングVLAN..... 232

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

- 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には、「aaa authorization network」コマンドを設定する必要があります。

Cisco IOSベースのアクセスポイントは、TLS 1.0のみをサポートしています。RADIUSサーバが TLS 1.2 802.1X認証のみを許可するように設定されている場合、これが問題を引き起こす可能性があります

参考資料

[APと9800 WLCを使用したdot1xサブリカントの設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。