

Dot1x の Flexconnect AP スイッチポートを保護するために設定して下さい

目次

[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](#)

—

[確認](#)

[トラブルシューティング](#)

概要

この資料はローカルでスイッチド ワイヤレス LAN (WLAN) からのトラフィックを可能にするために FlexConnect Access Points (AP) が device-traffic-class=switch Radius VSA を使用して Dot1x と認証するスイッチポートを保護するために設定を説明したものです。

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) の FlexConnect
- 802.1X on Cisco スイッチ
- ネットワークエッジ 認証 トポロジー (端正な)

使用するコンポーネント

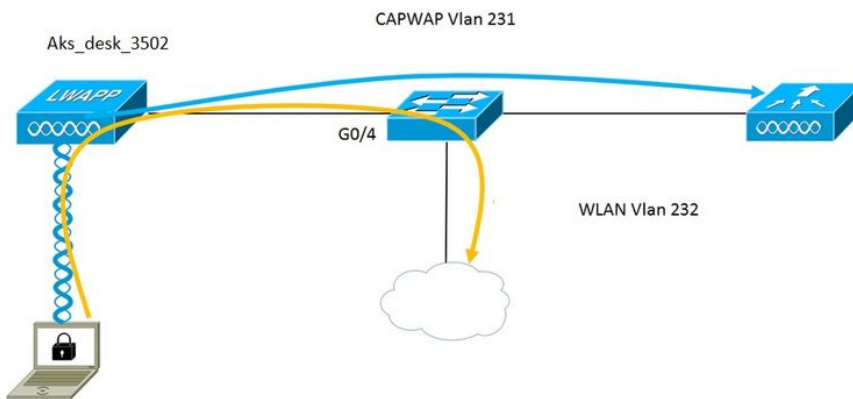
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- WS-C3560CX-8PC-S、15.2(4)E1
- AIR-CT-2504-K9、8.2.141.0
- 識別 サービス エンジン (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



アクセス ポイント設定されることで 802.1X 要求元として機能し、ISE に対するスイッチによって EAP-FAST を使用して認証されます。ポートが 802.1X 認証のために設定されれば、スイッチはパススルーに 802.1X トラフィック以外ポートに接続されるデバイスが認証に成功するまであらゆるトラフィックにポートを与えません。

アクセス ポイントが ISE に対して認証に成功すれば、スイッチは Cisco VSA 属性「device-traffic-class=switch 受け取り、トランキングするために自動的にポートを移動します。

AP が FlexConnect モードをサポートし、ローカルで設定される SSID を切り替えたらこの、それできますタグ付きトラフィックを送信こと意味します。VLANサポートが AP でイネーブルになり、正しいネイティブ VLAN が設定されるようにして下さい。

AP 設定: -

1. AP が WLC に既に加わっている場合、Wireless タブは行き、アクセス ポイントをクリックします。Credentials フィールドは行き、nder は先頭に立つ 802.1X 要求元信任状このアクセス ポイントのための 802.1X ユーザ名 および パスワードを設定するために上書きグローバルな信任状ボックスをチェックします。

The screenshot shows the Cisco WLC configuration interface for an Access Point (Aks_desk_3502). The '802.1x Supplicant Credentials' tab is active, and the 'Over-ride Global credentials' checkbox is checked. The Username field is set to 'ritmahaj', and the Password and Confirm Password fields are masked with dots.

またグローバルコンフィギュレーションメニューとのWLCに加入されるすべてのアクセスポイントのためのcommandユーザ名およびパスワードを設定できます。

The screenshot shows the Cisco WLC configuration interface with the 'Global Configuration' menu item highlighted in red. The page displays various configuration options including CDP State, Login Credentials, 802.1x Supplicant Credentials, TCP MSS, AP Retransmit Config Parameters, and OEAP Config Parameters.

2. アクセスポイントがWLCにまだ加入しない場合信任状を設定し、このCLIコマンドを使用するために、LAPにコンソール接続を行って下さい:

```
LAP#debug capwap コンソール cli
LAP#capwap ap dot1x username <username> password <password>
```

スイッチ設定: -

1. スイッチの dot1x をグローバルに有効にし、切り替えるために ISE サーバを追加して下さい

```
aaa new-model
```

```
!!
```

```
AAA認証 dot1x デフォルト グループ半径
```

```
!!
```

```
AAA認証ネットワーク デフォルト グループ半径
```

```
!!
```

```
dot1x システム auth 制御
```

```
!!
```

```
RADIUSサーバ ISE
```

```
アドレス ipv4 10.48.39.161 auth-port 1645 acct-port 1646
```

```
キー 7 123A0C0411045D5679
```

2. この場合 AP スイッチポートを設定して下さい

GigabitEthernet0/4 をインターフェイスさせて下さい

スイッチポートアクセスVLAN 231

スイッチポートトランクによって許可される VLAN 231,232

```
switchport mode access
```

```
shutdown
```

認証ホスト モード複数のホスト

認証順序 dot1x

認証ポート制御自動

dot1x pae オーセンティケータ

スパニングツリーポートファスト エッジ

1 つがそしてポート構成外観のような dot1x の代わりに MAB を設定したいと思えば: -

インターフェイス GigabitEthernet0/4

スイッチポートアクセスVLAN 231

スイッチポートトランクによって許可される VLAN 231,232

```
switchport mode access
```

```
shutdown
```

認証ホスト モード複数のホスト

認証順序 mab

認証ポート制御自動

```
mab
```

スパニングツリーポートファスト エッジ

ISE 設定: -

1. ISE で正しい属性を設定するために、1 つは AP 許可プロファイルのために端正単に有効になることができますが、他の RADIUSサーバで、手動で設定することができます。

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、1 つはまた認証 ポリシーおよび承認ポリシーを設定する必要があります。この場合 MAB の場合には配線された dot.1x(wired MAB であるデフォルトの認証ルールを見つけます)しかし 1 つは要件によってそれをカスタマイズできます。

承認ポリシー (Port_AuthZ) に関しては、この場合ユーザグループ (APS) に AP 信任状を追加し、これに基づいて許可プロファイル (AP_Flex_Trunk) を押しました。

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、一度ポートがトランク ポートに移動されるかどうか確認するコマンドを「debug authentication 機能 autocfg すべて」使用できます。

```
2月20日 12:34:18.119: %LINK-3-UPDOWN: インターフェイス GigabitEthernet0/4、への変更された状態
```

```
2月20日 12:34:19.122: %LINEPROTO-5-UPDOWN: インターフェイス GigabitEthernet0/4 の行プロトコル、への変更された状態
```

```
akshat_sw#
```

```
akshat_sw#
```

```
2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: dot1x AutoCfg start_fn では、epm_handle: 3372220456
```

2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d、Gi0/4] デバイスの種類 = スイッチ
 2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d、Gi0/4] 新しいクライアント
 2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 内部 Autocfg マクロ アプリケーション ステータス: 1
 2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] デバイスの種類: 2
 2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 自動設定: STP に port_config 0x85777D8 があります
 2月20日 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 自動設定: STP port_config に BPDU (ブリッジ・プロトコル・データ・ユニット) guard_config 2 があります
 2月20日 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: ポートの自動cfg を適用する方法 [Gi0/4]。
 2月20日 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] VLAN: 231 VLAN Str: 231
 2月20日 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: dot1x_autocfg_supp マクロを適用する方法 [Gi0/4]
 2月20日 12:38:11.116: コマンドを適用する方法... 「Gi0/4 のスイッチポートアクセスVLAN 無し 231」
 2月20日 12:38:11.127: コマンドを適用する方法... Gi0/4 の「スイッチポート nonegotiate 無し」
 2月20日 12:38:11.127: コマンドを適用する方法... Gi0/4 の「switchport mode trunk」
 2月20日 12:38:11.134: コマンドを適用する方法... 「Gi0/4 の switchport trunk native vlan 231」
 2月20日 12:38:11.134: コマンドを適用する方法... Gi0/4 の「スパニングツリーポートファストトランク」
 2月20日 12:38:12.120: %LINEPROTO-5-UPDOWN: インターフェイス GigabitEthernet0/4 の行プロトコル、への変更された状態
 2月20日 12:38:15.139: %LINEPROTO-5-UPDOWN: インターフェイス GigabitEthernet0/4 の行プロトコル、への変更された状態

2. 「show run int g0/4」の出力はポートがトランクポートに変更したことを示したものです。

現在の設定 : 295 バイト

!!

```

インターフェイス GigabitEthernet0/4
スイッチポートトランクによって許可される VLAN 231,232,239
switchport trunk native vlan 231
switchport mode trunk
認証ホスト モード複数のホスト
認証順序 dot1x
認証ポート制御自動
dot1x pae オーセンティケータ
スパニングツリーポートファスト エッジ トランク
end
  
```

3. Operations>>Radius Livelogs 1 の下の ISE で、正常である認証および押される正しい許可プロファイルできます。

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. これがクライアント VLAN 232 の AP スイッチポートでそれから MAC アドレス学ばれた後ク

クライアントを接続すれば。

```
akshat_sw#sh MACアドレステーブル int g0/4  
Mac Address Table
```

```
-----  
Vlan  Mac Address      Type      Ports  
-----  
231 588d.0997.061d  静的な Gi0/4 - AP  
232 c0ee.fbd7.8824  ダイナミック Gi0/4 -クライアント
```

クライアント 詳細の WLC で、このクライアントが VLAN 232 属し、SSID がローカルで切り替えられることが見られる場合があります。断片はここにあります。

```
( Cisco コントローラ ) >show クライアント 詳細 c0:ee:fb:d7:88:24  
クライアントのMACアドレス..... c0:ee:fb:d7:88:24  
N/A クライアント ユーザ名.....  
AP MAC アドレス..... b4:14:89:82:cb:90  
AP 名前..... Aks_desk_3502  
AP Radio スロット ID ..... 1  
クライアント ステート..... Associated  
クライアントのユーザ グループ.....  
クライアント NAC OOB 状態..... access  
Wireless LAN ID ..... 2  
ワイヤレスLANネットワーク名前 ( SSID ) ..... ポートAuth  
Wireless LAN Profile Name ..... ポートauth  
ホットスポット ( 802.11u ) ..... サポート対象外  
BSSID ..... b4:14:89:82:cb:9f  
..... 42 秒の間接続される  
チャンネル..... 44  
IP アドレス..... 192.168.232.90  
ゲートウェイアドレス..... 192.168.232.1  
ネットマスク..... 255.255.255.0  
アソシエーション ID ..... 1  
認証アルゴリズム..... オープンシステム  
理由コード..... 1  
ステータス・コード..... 0
```

```
FlexConnect データ・スイッチ..... 「ワイヤ  
FlexConnect Dhcp ステータス..... Local  
FlexConnect VLAN は基づかせていました中央切り替えを..... なし  
FlexConnect 認証..... セントラル  
FlexConnect 中央アソシエーション..... なし  
FlexConnect VLAN NAME ..... VLAN 232  
検疫 VLAN ..... 0  
アクセスして下さい VLAN に..... 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。

- 認証が失敗した場合、デバッグ dot1x を、debug authentication コマンド使用して下さい。
- ポートがトランッキングするために移動されない場合 debug authentication 機能 autocfg をすべてのコマンド入力して下さい。
- 設定してもらいます複数のホスト モード (認証ホスト モード複数のホスト) を確認して下さい。複数のホストはクライアント ワイヤレス MAC アドレスを可能にするためイネーブルにならなければなりません。
- 「AAA認証ネットワーク」コマンドは受け入れ、ISE によって送信された属性を適用することができるスイッチがように設定する必要があります。