

# 9800コントローラを使用したアクセスポイント用の802.1Xサブリカントの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[LAPを802.1xサブリカントとして設定する](#)

[APがすでにWLCに加入している場合：](#)

[APがまだWLCに加入していない場合：](#)

[スイッチの設定](#)

[ISEサーバの設定](#)

[確認](#)

[認証タイプの確認](#)

[スイッチポートでの802.1xの確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、RADIUSサーバに対してスイッチポートで認証される802.1xサブリカントとしてCiscoアクセスポイント(AP)を設定する方法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)とLAP ( Lightweightアクセスポイント )。
- CiscoスイッチおよびISE上の802.1x
- Extensible Authentication Protocol ( EAP )
- Remote Authentication Dial-In User Service ( RADIUS )

## 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、Cisco IOS® XE、15.2(3r)E2

- C9800-CL-K9、Cisco IOS® XE、17.6.1
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

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、初期（デフォルト）設定の状態から起動しています。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。

## 背景説明

この設定では、アクセスポイント(AP)が802.1xサブリカントとして機能し、EAP方式EAP-FASTを使用してISEに対してスイッチによって認証されます。

ポートが802.1X認証用に設定されると、スイッチは、ポートに接続されたデバイスが正常に認証されるまで、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。

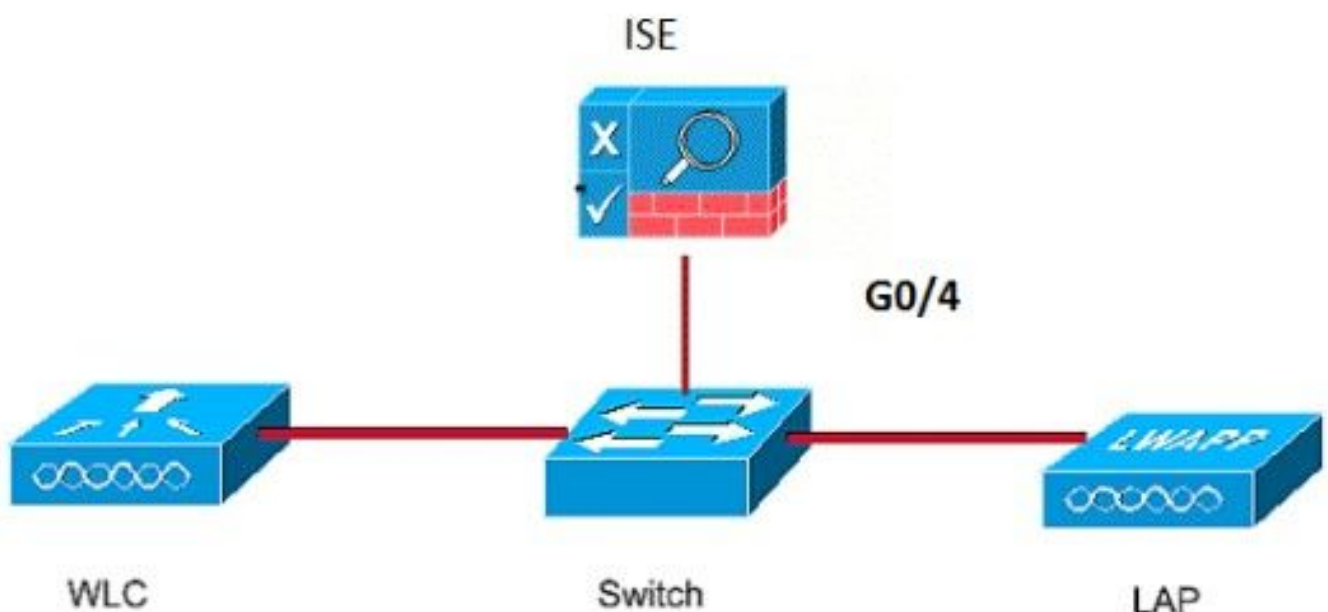
APは、WLCに加入する前に、またはWLCに加入した後に認証できます。この場合、LAPがWLCに加入した後で、スイッチに802.1Xを設定します。

## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

## ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。

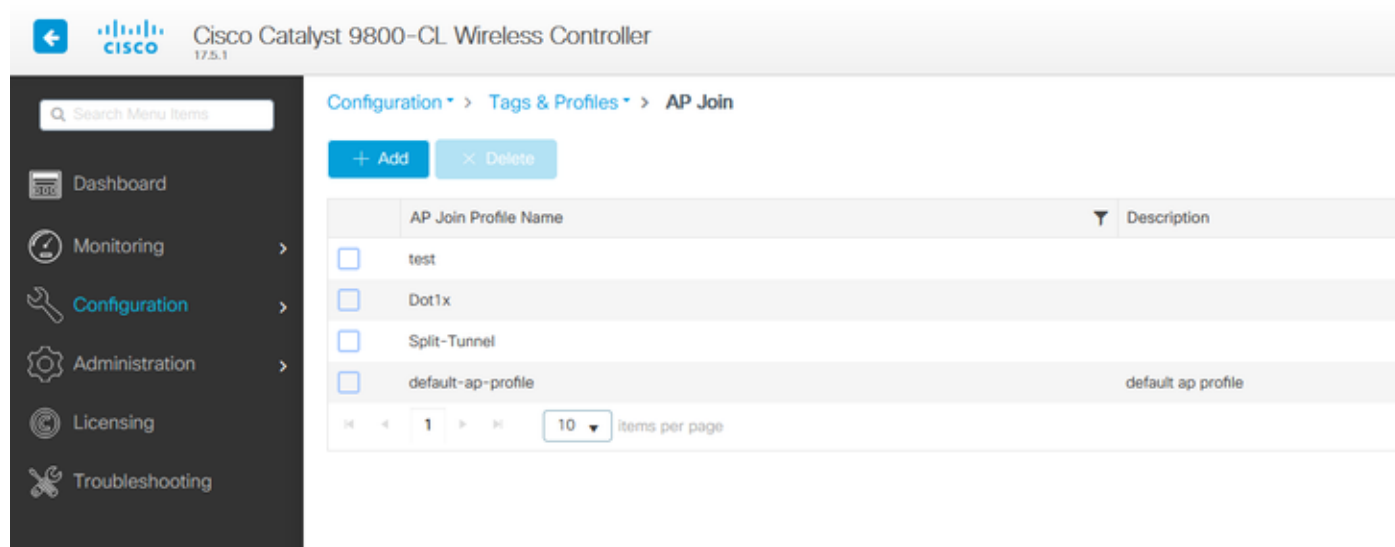


## LAPを802.1xサブリカントとして設定する

APがすでにWLCに加入している場合：

802.1x認証タイプとローカルで有効な証明書(LSC)AP認証タイプを設定します。

ステップ 1：[Configuration] > [Tags & Profiles] > [AP Join] に移動し、[AP Join Profile] ページで [Add] をクリックして新しい参加プロファイルを追加するか、名前をクリックしてAP参加プロファイル編集します。



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > AP Join. There are '+ Add' and 'X Delete' buttons. A table lists AP Join Profile Names and their descriptions:

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing '1' of 10 items per page.

ステップ 2：[AP Join Profile]ページで、[AP] > [General] の順に選択し、[AP EAP Auth Configuration] セクションに移動します。 [EAP Type] ドロップダウンリストから、[EAP type]として[EAP-FAST]、[EAP-TLS]、または[EAP-PEAP]を選択し、dot1x認証タイプを設定します。

Edit AP Join Profile ×

General Client CAPWAP **AP** Management Security ICap QoS

**General** Hyperlocation Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type Unknown ▾

Injector Switch MAC 00:00:00:00:00:00

**Client Statistics Reporting Interval**

5 GHz (sec) 90

2.4 GHz (sec) 90

**AP EAP Auth Configuration**

EAP Type EAP-FAST ▾

AP Authorization Type

- EAP-FAST
- EAP-TLS
- EAP-PEAP

**Extended Module**

Enable

**Mesh**

Profile Name mesh-profile ▾ [Clear](#)

↶ Cancel 🔄 Update & Apply to Device

ステップ 3 : [AP Authorization Type] ドロップダウンリストから、タイプとして[CAPWAP DTLS +]または[CAPWAP DTLS]を選択し、[Update & Apply to Device] をクリックします。

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

**General** Hyperlocation Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

**Client Statistics Reporting Interval**

5 GHz (sec)

2.4 GHz (sec)

**AP EAP Auth Configuration**

EAP Type

AP Authorization Type

- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

**Extended Module**

Enable

**Mesh**

Profile Name  [Clear](#)

802.1xのユーザ名とパスワードを設定します。

ステップ 1 : [Management] > [Credentials] > [Enter Dot1x username and password details] >適切な802.1xパスワードタイプを選択> [Update & Apply to Device] をクリックします

Edit AP Join Profile ×

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

**Dot1x Credentials**

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

**APがまだWLCに加入していない場合：**

クレデンシャルを設定し、次のCLIコマンドを使用するには、LAPにコンソール接続する必要があります(Cheetah OSおよびCisco IOS® APの場合)。

CLI：

```
LAP# debug capwap console cli  
LAP# capwap ap dot1x username
```

**APのDot1xクレデンシャルをクリアするには (必要な場合)**

Cisco IOS® APの場合は、リロード後にAPを次のようにリロードします。

CLI :

```
LAP# clear capwap ap dot1x
```

Cisco COS APの場合、リロード後にAPを次のようにリロードします。

CLI :

```
LAP# capwap ap dot1x disable
```

## スイッチの設定

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します。

CLI :

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

APスイッチポートを設定します。

CLI :

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

APがFlex Connectモード、ローカルスイッチングの場合、クライアントトラフィックはAPレベルで解放されるため（APレベルで解放される）、ポートで複数のMACアドレスを許可するには、スイッチインターフェイスで追加の設定を行う必要があります。

```
authentication host-mode multi-host
```

**注：読者が注意を持つことを意味します。** 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

**注：**マルチホストモードでは、最初のMACアドレスが認証されてから、無制限の数の他のMACアドレスが許可されます。接続されたAPがローカルスイッチングモードで設定されている場合は、スイッチポートでホストモードを有効にします。クライアントのトラフィックがスイッチポートを通過することを許可します。セキュアなトラフィックパスが必要な場合は、WLANでdot1xを有効にしてクライアントデータを保護します

## ISEサーバの設定

ステップ 1：スイッチをISEサーバ上のネットワークデバイスとして追加します。

[Administration] > [Network Resources] > [Network Devices] > [Add] > [Enter Device name, IP address, enable RADIUS Authentication Settings] > [Specify Shared Secret Value, COA port] (またはデフォルトのままにします) に移動し、[Submit] をクリックします。

The screenshot displays the Cisco ISE Administration interface for configuring a new network device. The breadcrumb trail is Administration > Network Resources > Network Devices > Add > Enter Device name, IP address, enable RADIUS Authentication Settings > Specify Shared Secret Value, COA port. The 'Network Devices' menu item is highlighted in the left sidebar. The main form includes the following fields and options:

- Name: MySwitch
- Description: (empty)
- IP Address: 10.48.39.100 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: Is IPSEC Device (Set To Default)
- Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings
  - RADIUS LDP Settings
    - Protocol: RADIUS
    - Shared Secret: (masked) (Show)
    - Use Second Shared Secret:  (Show)
    - CoA Port: 1700 (Set To Default)
  - RADIUS DTLS Settings
    - DTLS Required:  (Show)
    - Shared Secret: radius/dtls (Show)

ステップ 2：APクレデンシャルをISEに追加します。[Administration] > [Identity Management] > [Identities] > [Users] に移動し、[Add] ボタンをクリックしてユーザを追加します。ここで、WLCのAP加入プロファイルで設定したクレデンシャルを入力する必要があります。ユーザはデフォルトのグループに配置されますが、これは要件に応じて調整できます。



Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users  
Latest Manual Network Scan Res...

Network Access User

Name dot1x

Status  Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

Login Password ..... Generate Password

Enable Password ..... Generate Password

User Information

Account Options

Account Disable Policy

User Groups

ALL\_ACCOUNTS (default)

ステップ 3 : ISEで、**認証ポリシー**と**認可ポリシー**を設定します。 [Policy] > [Policy Sets] に移動し、設定するポリシーセットと右側の青い矢印を選択します。この場合、デフォルトのポリシーセットが使用されますが、要件に従ってカスタマイズできます。

Cisco ISE Policy - Policy Sets

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	6		

次に、**認証ポリシー**と**認可ポリシー**を設定します。ここに示すポリシーは、ISEサーバ上で作成されたデフォルトポリシーですが、要件に応じて調整およびカスタマイズできます。この例では、設定を次のように変換できます。「有線802.1Xが使用され、ユーザがISEサーバで認識されている場合、認証に成功したユーザへのアクセスを許可します」その後、APはISEサーバに対して認証されます。

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
<input checked="" type="checkbox"/>	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	
<input checked="" type="checkbox"/>	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	
<input checked="" type="checkbox"/>	Default		All_User_ID_Stores > Options	0	

Authorization Policy (12)			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	Select from list	6	⚙️
●	Default		DenyAccess x	Select from list	0	⚙️

ステップ 4 : 許可されているプロトコルで、Default Network AccessにEAP-FASTが許可されていることを確認します。[Policy] > [Policy Elements] > [Authentication] > [Results] > [Allowed Protocols] > [Default Network Access] > [Enable Allow EAP-TLS] > [Save] に移動します。

The screenshot shows the Cisco ISE interface for configuring the 'Default Network Access' policy element. The 'Results' tab is active, and the 'Allowed Protocols' section is expanded. Under 'Authentication Protocols', the following options are checked: Allow PAP/ASCII, Allow EAP-MD5, Allow EAP-TLS, Allow PEAP, Allow EAP-FAST, Allow EAP-TTLS, and Allow TEAP. A red arrow points to the 'Allow EAP-TLS' checkbox. The 'Allowed Protocols' section also includes 'Authentication Bypass' (Process Host Lookup checked) and 'Enable Stateless Session Resume' (unchecked).

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

## 認証タイプの確認

showコマンドは、APプロファイルの認証情報を表示します。

CLI :

```
9800WLC#show ap profile name <profile-name> detailed
例 :
```

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
```

```
...
Dot1x EAP Method      : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE     : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

## スイッチポートでの802.1xの確認

showコマンドは、スイッチポートの802.1xの認証状態を表示します。

CLI :

```
Switch# show dot1x all
```

出力例 :

```
Sysauthcontrol          Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                        = AUTHENTICATOR
QuietPeriod                = 60
ServerTimeout              = 0
SuppTimeout                = 30
ReAuthMax                  = 2
MaxReq                      = 2
TxPeriod                    = 30
```

ポートが認証されているかどうかを確認します

CLI :

```
Switch#show dot1x interface <AP switch port number> details
```

出力例 :

```
Dot1x Info for GigabitEthernet0/8
-----
PAE                        = AUTHENTICATOR
QuietPeriod                = 60
ServerTimeout              = 0
SuppTimeout                = 30
ReAuthMax                  = 2
MaxReq                      = 2
TxPeriod                    = 30

Dot1x Authenticator Client List
-----
EAP Method                  = FAST
Supplicant                  = f4db.e67e.dd16
Session ID                  = 0A30279E00000BB7411A6BC4
  Auth SM State              = AUTHENTICATED
  Auth BEND SM State         = IDLE
ED
Auth BEND SM State = IDLE
```

CLI から :

```
Switch#show authentication sessions
```

出力例：

```
Interface      MAC Address      Method  Domain  Status Fg Session ID
Gi0/8         f4db.e67e.dd16  dot1x   DATA   Auth    0A30279E00000BB7411A6BC4
```

ISEで、[Operations] > [Radius Livelogs] の順に選択し、認証が成功して正しい認可プロファイルがプッシュされたことを確認します。

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	✓	🔒		dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access			nschyns-SW-...	FastEther
Nov 28, 2022 08:33:34.4...	✓	🔒		dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess		nschyns-SW-...	FastEther

## 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使用できる情報を示します。

1. pingコマンドを入力して、ISEサーバがスイッチから到達可能かどうかを確認します。
2. スイッチがISEサーバ上でAAAクライアントとして設定されていることを確認します。
3. 共有秘密がスイッチとISEサーバの間で同じであることを確認します。
4. ISEサーバでEAP-FASTが有効になっているかどうかを確認します。
5. 802.1xクレデンシャルがLAP用に設定されていて、ISEサーバ上で同じであることを確認します。

注：ユーザ名とパスワードでは大文字と小文字が区別されます。

6. 認証が失敗した場合は、スイッチでdebug dot1xコマンドとdebug authenticationコマンドを入力します。

Cisco IOSベースのアクセスポイント(802.11ac wave 1)は、TLSバージョン1.1および1.2をサポートしていないことに注意してください。ISEまたはRADIUSサーバが802.1X認証の内部でTLS 1.2のみを許可するように設定されている場合、この問題が発生する可能性があります。

## 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。