



アクセスポイントの認証の設定

- [アクセスポイントに対する認証の設定について, 1 ページ](#)
- [アクセスポイントの認証を設定するための前提条件, 1 ページ](#)
- [アクセスポイントの認証に関する制約事項, 2 ページ](#)
- [アクセスポイントの認証の設定 \(GUI\) , 2 ページ](#)
- [アクセスポイントの認証の設定 \(CLI\) , 3 ページ](#)
- [スイッチの認証の設定, 4 ページ](#)

アクセスポイントに対する認証の設定について

Lightweight アクセスポイントとシスコのスイッチの間で 802.1X 認証を設定できます。アクセスポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。

コントローラに現在関連付けられている、または今後関連付けられるすべてのアクセスポイントにグローバル認証を設定できます。グローバル認証設定を上書きし、特定のアクセスポイントに一意の認証設定を割り当てることもできます。

アクセスポイントの認証を設定するための前提条件

ステップ 1 アクセスポイントが新しい場合は、次を実行します。

- a) アクセスポイントを、インストールされたリカバリイメージでブートします。
- b) この提案フローに従わず、アクセスポイントがコントローラに join する前にアクセスポイントに接続されたスイッチポートで 802.1X 認証を有効化するには、次のコマンドを入力します。

lwapp ap dot1x username username password password

(注) この提案フローに従って、アクセスポイントがコントローラに join されて設定済みの 802.1X 資格情報を受信してからスイッチポートで 802.1X 認証を有効化する場合は、このコマンドを入力する必要はありません。

(注) このコマンドは、5.1、5.2、6.0、または 7.0 リカバリ イメージを実行しているアクセスポイントでのみ使用できます。

アクセスポイントをスイッチポートに接続します。

ステップ 2 5.1、5.2、6.0、または 7.0 イメージをコントローラにインストールし、コントローラをリブートします。

ステップ 3 すべてのアクセスポイントによるコントローラへの join を許可します。

ステップ 4 コントローラ上で認証を設定します。コントローラの認証の設定に関する情報については、「[アクセスポイントの認証の設定 \(GUI\)](#)」の項、または「[アクセスポイントの認証の設定 \(CLI\)](#)」の項を参照してください。

ステップ 5 スイッチを設定して認証を許可します。スイッチの認証の設定については、「[スイッチの認証の設定](#)」の項を参照してください。

アクセスポイントの認証に関する制約事項

- OEAP 600 シリーズアクセスポイントでは、LEAP はサポートされません。

アクセスポイントの認証の設定 (GUI)

ステップ 1 [Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます。

ステップ 2 [802.1x Supplicant Credentials] で、[802.1x Authentication] チェックボックスをオンにします。

ステップ 3 [Username] テキストボックスに、そのコントローラに join するすべてのアクセスポイントが継承するユーザ名を入力します。

ステップ 4 [Password] ボックスと [Confirm Password] ボックスに、コントローラに join するすべてのアクセスポイントによって継承されるパスワードを入力します。

(注) これらのテキストボックスには、強力なパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

- ステップ 5** [Apply] をクリックして、グローバル認証ユーザ名およびパスワードを、コントローラに現在 join しているアクセスポイント、および今後 join するすべてのアクセスポイントに送信します。
- ステップ 6** [Save Configuration] をクリックして、変更を保存します。
- ステップ 7** 必要に応じて、次の手順に従って、グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセスポイントに割り当てることができます。
- [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
 - 認証設定を無効にするアクセスポイントの名前をクリックします。
 - [Credentials] タブをクリックして [All APs > Details for] (Credentials) ページを開きます。
 - [802.1x Supplicant Credentials] で [Over-ride Global Credentials] チェックボックスをオンにして、このアクセスポイントがグローバル認証のユーザ名およびパスワードをコントローラから継承しないようにします。デフォルト値はオフです。
 - [Username]、[Password]、および [Confirm Password] テキストボックスに、このアクセスポイントに割り当てて一意のユーザ名およびパスワードを入力します。
(注) 入力した情報は、コントローラやアクセスポイントをリブートした後や、アクセスポイントが新しいコントローラに join された場合でも保持されます。
 - [Apply] をクリックして、変更を確定します。
 - [Save Configuration] をクリックして、変更を保存します。
(注) このアクセスポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

アクセスポイントの認証の設定 (CLI)

- ステップ 1** 次のコマンドを入力して、コントローラに現在 join しているアクセスポイント、および今後 join するすべてのアクセスポイントについて、グローバル認証のユーザ名とパスワードを設定します。
- ```
config ap 802.1Xuser add username ap-username password ap-password all
```
- (注) *ap-password* パラメータには強力なパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。
- 少なくとも 8 文字の長さである。
  - 小文字と大文字、数字、および記号の組み合わせ。
  - どの言語の単語でもない。
- ステップ 2** (任意) グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセスポイントに割り当てることができます。そのためには、次のコマンドを入力します。

```
config ap 802.1Xuser add username ap-username password ap-password Cisco_AP
```

(注) *ap-password* パラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴については、[ステップ 1](#) の注記を参照してください。

このコマンドに入力した認証設定は、コントローラやアクセスポイントをリブートした後や、アクセスポイントが新しいコントローラに join された場合でも保持されます。

- (注) このアクセスポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、**config ap 802.1Xuser delete Cisco\_AP** コマンドを入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

**ステップ 3** **save config** コマンドを入力して、変更を保存します。

**ステップ 4** (任意) 次のコマンドを入力して、すべてのアクセスポイントまたは特定のアクセスポイントに対して 802.1X 認証を無効にします。

**config ap 802.1Xuser disable {all | Cisco\_AP}**

- (注) 特定のアクセスポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセスポイントに対してだけ 802.1X を無効にできます。

**ステップ 5** 次のコマンドを入力して、コントローラに join するすべてのアクセスポイントの認証設定を表示します。  
**show ap summary**

以下に類似した情報が表示されます。

```
Number of APs..... 1
Global AP User Name..... globalap
Global AP Dot1x User Name..... globalDot1x
```

**ステップ 6** 次のコマンドを入力して、特定のアクセスポイントの認証設定を表示します。

**show ap config general Cisco\_AP**

- (注) アクセスポイントの名前では、大文字と小文字が区別されません。
- (注) このアクセスポイントがグローバル認証を使用するよう設定されている場合は、[APDot1xUser Mode] テキストボックスに「Automatic」と表示されます。このアクセスポイントでグローバル認証設定が無効にされている場合は、[AP Dot1x User Mode] テキストボックスに「Customized」と表示されます。

## スイッチの認証の設定

スイッチポートで 802.1X 認証を有効にするには、スイッチ CLI で次のコマンドを入力します。

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**

- Switch(config)# **radius-server host** *ip\_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**

