アクセス ポイントの認証の設定

- 機能情報の確認，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 ポイントの認証を設定する際の制限，2 ページ
- アクセス ポイントに対する認証の設定について，2 ページ
- アクセス ポイントの認証の設定方法，3 ページ
- アクセス ポイントの認証の設定例，9 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

アクセス ポイントの認証を設定するための前提条件

- スイッチに現在 join しているすべてのアクセス ポイント、また今後 join するアクセスポイントがスイッチに join するときに継承するグローバル ユーザ名、パスワード、およびイネーブル パスワードを設定することができます。必要に応じて、このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、およびイネーブル 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。
- アクセス ポイントをスイッチに join すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、コンソール ポートへログインするたびにユーザ名とパスワードの

入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

- スイッチで設定したグローバル資格情報はスイッチやアクセス ポイントをリブートした後も保持されます。この情報が上書きされるのは、アクセス ポイントを、グローバル ユーザ名およびパスワードが設定された新しいスイッチに join した場合のみです。グローバル資格情報を使って新しいスイッチを設定しなかった場合、このアクセス ポイントは最初のスイッチに設定されているグローバル ユーザ名とパスワードをそのまま保持します。
- アクセス ポイントにより使用される資格情報を追跡する必要があります。そうしないと、アクセス ポイントのコンソール ポートにログインできなくなることがあります。アクセス ポイントをデフォルトの *Cisco/Cisco* ユーザ名およびパスワードに戻す必要がある場合は、スイッチの設定をクリアする必要があります。これにより、アクセス ポイントの設定は工場出荷時のデフォルト設定に戻ります。デフォルトのアクセス ポイント設定をリセットするには、**ap name** *Cisco_AP* **mgmtuser username** *Cisco* **password** *Cisco* コマンドを入力します。コマンドを入力しても、アクセス ポイントの固定 IP アドレスはクリアされません。アクセス ポイントがスイッチに再 join すると、デフォルトの *Cisco/Cisco* のユーザ名およびパスワードを適用します。
- 現在スイッチに join している、また、今後 join す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。必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス ポイントに割り当てることができます。
- この機能は、次のハードウェアによりサポートされます。
  - 認証をサポートするすべての Cisco スイッチ。
  - Cisco Aironet 1140、1260、1310、1520、1600、2600、3500、および 3600 アクセス ポイント

アクセス ポイントの認証を設定する際の制限

- AP 設定におけるスイッチ名は、大文字と小文字が区別されます。したがって、AP 設定には、必ず正確なシステム名を設定してください。正確に設定しないと、AP フォールバックが機能しません。

アクセス ポイントに対する認証の設定について

Cisco IOS アクセス ポイントには、工場出荷時にデフォルトの enable パスワード *Cisco* が設定されています。このパスワードを使用して、非特権モードでログインすると、ネットワークのセキュリティに対する脅威となる **show** および **debug** コマンドの入力が許可されます。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートからコンフィギュレーション コマンドを入力できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

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するスイッチにより認証されます。

アクセス ポイントの認証の設定方法

アクセス ポイントのグローバル資格情報の設定（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value*
4. **end**
5. **ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret*
6. **show ap summary**
7. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value* 例： `Switch(config)# ap mgmtuser apusr1 password appass 0 secret 0 appass1`	スイッチに現在 join しているすべてのアクセス ポイント、および今後スイッチに join するアクセス ポイントに対し、グローバル ユーザ名とパスワードを設定し、パスワードをイネーブルにします。このコマンドでは、パラメータ 0 は暗号化されていないパスワードが続くことを指定し、8 は AES 暗号化パスワードが続くことを指定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 5	**ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret* 例： `Switch(config)# ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret`	特定のアクセス ポイントのグローバル資格情報を上書きし、固有のユーザ名とパスワードを割り当て、このアクセス ポイントに対しパスワードをイネーブルにします。 このコマンドに入力した資格情報は、スイッチやアクセス 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スイッチに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スイッチのグローバル資格情報を強制的に使用する必要がある場合は、**ap name** *Cisco_AP* **no mgmtuser** 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 6	**show ap summary** 例： `Switch# show ap summary`	接続されたすべての Cisco AP のサマリーを表示します。
ステップ 7	**show ap name** *Cisco_AP* **config general** 例： `Switch# show ap name AP02 config general`	特定のアクセス ポイントのグローバル資格情報の設定を表示します。 （注） このアクセス ポイントがグローバル クレデンシャル用に設定されている場合は、[AP User Mode] テキスト ボックスに [Automatic] と表示されます。このアクセス ポイントのグローバルクレデンシャルが上書きされている場合は、[AP User Mode] テキスト ボックスに [Customized] と表示されます。

アクセス ポイントの認証の設定（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap dot1x username** *user_name_value* **password 0** *password_value*
4. **end**
5. **ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value*
6. **configure terminal**
7. **no ap dot1x username** *user_name_value* **password 0** *password_value*
8. **end**
9. **show ap summary**
10. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap dot1x username** *user_name_value* **password 0** *password_value* 例： `Switch(config)# ap dot1x username AP3 password 0 password`	にスイッチ現在 join しているすべてのアクセス ポイント、または今後 join するスイッチアクセス ポイントにグローバル認証のユーザ名とパスワードを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **username**：すべてのアクセス ポイントの 802.1X ユーザ名を指定します。 • *user-id*：ユーザ名。 • **password**：すべてのアクセス ポイントの 802.1X パスワードを指定します。 • **0**：暗号化されないパスワードを指定します。 • **8**：AES 暗号化パスワードを指定します。 • *passwd*：パスワード。

	コマンドまたはアクション	目的
		（注） 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長さは少なくとも8文字で、大文字と小文字、数字、および記号の組み合わせを含み、いずれの言語の単語でもありません。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value* 例： `Switch# ap name AP03 dot1x-user username apuser1 password appass`	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ます。このコマンドには、次のキーワードと引数が含まれます。 • **username**：ユーザ名を追加するように指定します。 • *user-id*：ユーザ名。 • **password**：パスワードを追加するように指定します。 • **0**：暗号化されないパスワードを指定します。 • **8**：AES 暗号化パスワードを指定します。 • *passwd*：パスワード。 （注） 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 2 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、スイッチやアクセス ポイントをリブートした後や、アクセス ポイントが新しいスイッチに join された場合でも保持されます。
ステップ 6	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**no ap dot1x username** *user_name_value* **password 0** *password_value* 例： `Switch(config)# no ap dot1x username dot1xusr password 0 dot1xpass`	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 認証をディセーブルにします。 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。 （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。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show ap summary** 例： `Switch# show ap summary`	スイッチに 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。 （注） グローバルな認証が設定されていない場合、[Global AP Dot1x User Name] テキスト ボックスには「Not Configured」と表示されます。
ステップ 10	**show ap name** *Cisco_AP* **config general** 例： `Switch# show ap name AP02 config general`	特定のアクセス ポイントの認証設定を表示します。 （注） このアクセスポイントがグローバル認証用に設定されている場合は、[AP Dot1x User Mode] テキスト ボックスに「Automatic」と表示されます。このアクセス ポイントのグローバル認証設定が上書きされている場合は、[AP Dot1x User Mode] テキスト ボックスに「Customized」と表示されます。

認証のスイッチの設定（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **aaa new-model**
5. **aaa authentication dot1x default group radius**
6. **radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key*
7. **interface TenGigabitEthernet1/0/1**
8. **switch mode access**
9. **dot1x pae authenticator**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	システム認証制御をイネーブルにします。
ステップ 4	**aaa new-model** 例： `Switch(config)# aaa new-model`	新しいアクセス コントロール コマンドと機能をイネーブルにします
ステップ 5	**aaa authentication dot1x default group radius** 例： `Switch(config)# aaa authentication dot1x default group radius`	サーバ グループ内のすべての RADIUS ホストを使用して、IEEE 802.1X のデフォルトの認証リストを設定します。
ステップ 6	**radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key* 例： `Switch(config)# radius-server host 10.1.1.1 acct-port 1813 auth-port 6225 key 0 encryptkey`	RADIUS 認証サーバのクリア テキストの暗号キーを設定します。
ステップ 7	**interface TenGigabitEthernet1/0/1** 例： `Switch(config)# interface TenGigabitEthernet1/0/1`	10 ギガビット イーサネット インターフェイスを設定します。 コマンド プロンプトが Controller(config)# から Controller(config-if)# に変更します。
ステップ 8	**switch mode access** 例： `Switch(config-if)# switch mode access`	インターフェイスへの無条件の truncking モード アクセスを設定します。
ステップ 9	**dot1x pae authenticator** 例： `Switch(config-if)# dot1x pae authenticator`	オーセンティケータとして 802.1X インターフェイスの PAE タイプを設定します。

	コマンドまたはアクション	目的
ステップ **10**	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

アクセス ポイントの認証の設定例

アクセス ポイントの認証設定の表示：例

次に、スイッチに接続するすべてのアクセス ポイントの認証設定を表示する例を示します。

```
Switch# show ap summary
Number of APs.................................. 1
Global AP User Name............................ globalap
Global AP Dot1x User Name...................... globalDot1x
```

次に、特定のアクセス ポイントの認証設定を表示する例を示します。

```
Switch# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier............................ 0
Cisco AP Name.................................. TSIM_AP2
...
AP Dot1x User Mode............................. AUTOMATIC
AP Dot1x User Name............................. globalDot1x
```