

# Cisco Business 220シリーズスイッチでの802.1x認証の設定

## 目的

この記事の目的は、Cisco Business 220シリーズスマートスイッチで802.1x認証を設定する方法を説明することです。

## 該当するデバイス | ファームウェアのバージョン

- CBS220シリーズ ([データシート](#)) | 2.0.0.17

## 概要

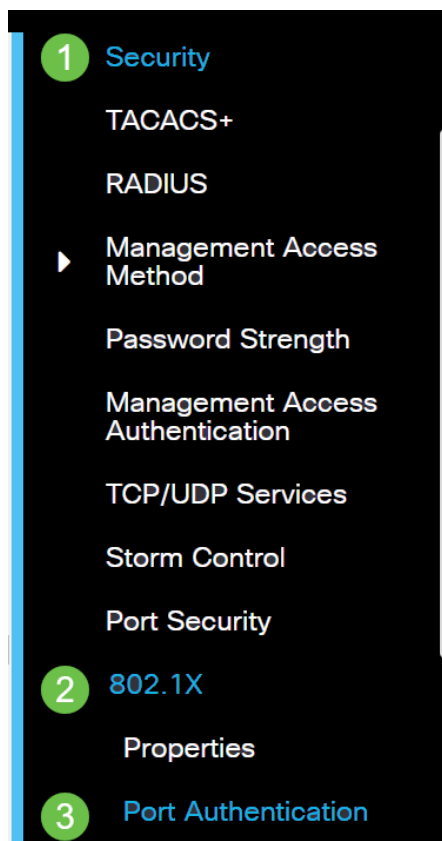
ポート認証を使用すると、各ポートのパラメータを設定できます。設定の変更の一部は、ポート認証など、ポートが強制承認済み状態である場合にのみ可能であるため、変更を行う前にポート制御を[強制承認済み(Force Authorized)]に変更することをお勧めします。設定が完了したら、ポート制御を以前の状態に戻します。

802.1xが定義されたポートは、LAGのメンバになれません。802.1xとポートセキュリティを同じポートで同時に有効にすることはできません。インターフェイスでポートセキュリティを有効にすると、管理ポート制御を自動モードに変更できません。

## ポート認証の設定

### 手順 1

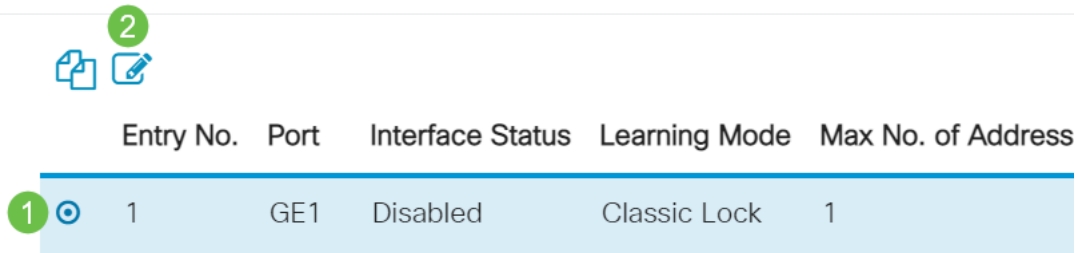
スイッチのWebユーザインターフェイス(UI)にログインし、[Security] > [802.1x] > [Port Authentication]を選択します。



## 手順 2

設定するポートのオプションボタンをクリックし、編集アイコンをクリックします。

### Port Security Table

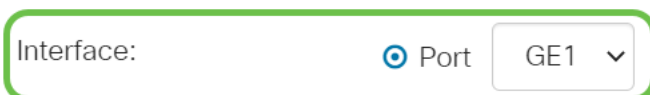


Entry No.	Port	Interface	Status	Learning Mode	Max No. of Address
1	GE1	Disabled	Classic Lock	1	

## 手順 3

[Edit Port Authentication]ウィンドウがポップアップ表示されます。[Interface]ドロップダウンリストから、指定したポートがステップ2で選択したポートであることを確認します。そうでない場合は、ドロップダウン矢印をクリックし、正しいポートを選択します。

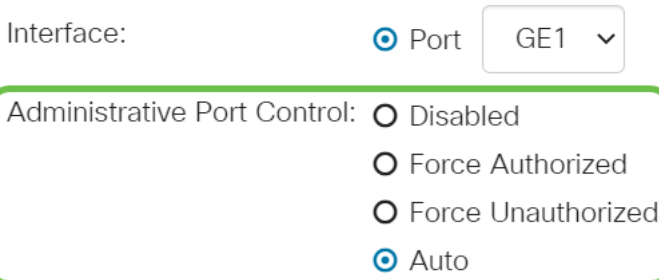
### Edit Port Authentication



## 手順 4

[Administrative Port Control]のオプションボタンを選択します。これにより、ポート認証状態が決定されます。次のオプションがあります。

- **Disabled:**802.1xを無効にします。これはデフォルトの状態です。
- **Force Unauthorized:** インターフェイスを不正な状態に移行することによって、インターフェイスアクセスを拒否します。スイッチは、インターフェイスを介してクライアントに認証サービスを提供しません。
- **Auto:** スイッチでポートベースの認証と許可を有効にします。インターフェイスは、スイッチとクライアント間の認証交換に基づいて、認可された状態または不正な状態の間を移動します。
- **Force Authorized:** 認証なしでインターフェイスを承認します。



## 手順 5 ( オプション )

[RADIUS VLAN Assignment]のオプションボタンを選択します。これにより、指定されたポートでダイナミックVLAN割り当てが有効になります。次のオプションがあります。

- **Disabled:** VLAN許可結果を無視し、ホストの元のVLANを保持します。これがデフォルトのアクションです。
- **Reject :** 指定されたポートがVLAN認定情報を受信すると、その情報を使用します。ただし、VLAN承認済み情報がない場合は、ホストを拒否し、不正にします。
- **Static :** 指定されたポートがVLAN認定情報を受信した場合、その情報が使用されます。ただし、VLAN承認済み情報がない場合は、ホストの元のVLANが保持されます。

RADIUSからVLAN承認済み情報が存在するが、VLANがDevice Under Test(DUT)で管理上作成されていない場合、VLANは自動的に作成されます。

RADIUS VLAN Assignment:  Disabled  
 Reject  
 Static

ヒント : ダイナミックVLAN割り当て機能を動作させるには、スイッチでRADIUSサーバから次のVLAN属性を送信する必要があります。

- [64] Tunnel-Type = VLAN ( タイプ13 )
- [65] Tunnel-Medium-Type = 802 ( タイプ6 )
- [81] Tunnel-Private-Group-Id = VLAN ID

## ステップ 6 ( オプション )

ゲストVLANが不正ポートにゲストVLANを使用するには、ゲストVLANの[Enable] チェックボックスをオンにします。

Guest VLAN:  Enable

## ステップ7

[Periodic Reauthentication]の[Enable]チェックボックスをオンにします。これにより、指定された再認証期間の後にポート再認証が試行されます。

Periodic Reauthentication:  Enable

## 手順 8

[再認証期間]フィールドに値を入力します。これは、ポートの再認証にかかる時間 ( 秒 ) です。

Reauthentication Period: 3600

## 手順 9 ( オプション )

[Reauthenticate Now] チェックボックスをオンにして、即時のポート再認証を有効にします。

[Authenticator State]フィールドには、認証の現在の状態が表示されます。

Reauthenticate Now:  Enable

Authenticator State: Initialize

ポートが[Force Authorized]または[Force Unauthorized]状態でない場合は、ポートは自動モードで

あり、オーセンティケータは認証中の状態を表示します。ポートが認証されると、状態は [Authenticated] と表示されます。

#### 手順 10

[Max Hosts] フィールドに、特定のポートで許可される認証済みホストの最大数を入力します。この値は、マルチセッションモードでのみ有効です。

Max Hosts: 256 (Range: 1 - 256, Default: 256)

#### 手順 11

[Quiet Period] フィールドに、認証交換の失敗の後にスイッチが Quiet 状態のままになる秒数を入力します。スイッチが静音状態の場合は、スイッチがクライアントからの新しい認証要求をリッスンしていないことを意味します。

Quiet Period: 60 sec (Range: 0 - 65535)

#### ステップ 12

[Resending EAP] フィールドに、スイッチがサブリカント (クライアント) からの Extensible Authentication Protocol (EAP) 要求またはアイデンティティフレームへの応答を待機する秒数を入力してから要求を再送信します。

Resending EAP: 30 (Range: 1 - 65535, Default: 30)

#### 手順 13

[Max EAP Requests] フィールドに、送信可能な EAP 要求の最大数を入力します。定義された期間 (サブリカントタイムアウト) 後に応答が受信されない場合、認証プロセスが再起動されます。

Max EAP Requests: 2 (Range: 1 - 10, Default: 2)

#### ステップ 14

[Supplicant Timeout] フィールドに、EAP 要求がサブリカントに再送信されるまでの経過時間を秒数で入力します。

Supplicant Timeout: 30 sec (Range: 1 - 65535, Default: 30)

#### ステップ 15

[サーバのタイムアウト] フィールドに、スイッチが認証サーバに要求を再送信するまでの経過時間を秒数で入力します。

Server Timeout: 30 sec (Range: 1 - 65535, Default: 30)

#### ステップ 16

[Apply] をクリックします。

Apply

Close

これで、スイッチで802.1x認証が正常に設定されました。

その他の設定については、『[Cisco Business 220シリーズスイッチアドミニストレーションガイド](#)』を参照してください。

その他の記事を見るには、『[Cisco Business 220 Series Switch Support Page](#)』を参照してください