



## 802-1x コマンド

---

この章は、次の項で構成されています。

- [aaa authentication dot1x](#) (2 ページ)
- [clear dot1x statistics](#) (3 ページ)
- [dot1x authentication](#) (4 ページ)
- [dot1x guest-vlan](#) (6 ページ)
- [dot1x guest-vlan enable](#) (7 ページ)
- [dot1x guest-vlan timeout](#) (8 ページ)
- [dot1x host-mode](#) (9 ページ)
- [dot1x max-hosts](#) (12 ページ)
- [dot1x max-req](#) (13 ページ)
- [dot1x port-control](#) (14 ページ)
- [dot1x re-authenticate](#) (16 ページ)
- [dot1x system-auth-control](#) (17 ページ)
- [dot1x timeout quiet-period](#) (18 ページ)
- [dot1x timeout reauth-period](#) (19 ページ)
- [dot1x timeout server-timeout](#) (20 ページ)
- [dot1x timeout silence-period](#) (21 ページ)
- [dot1x timeout supp-timeout](#) (22 ページ)
- [dot1x timeout tx-period](#) (23 ページ)
- [dot1x traps authentication failure](#) (24 ページ)
- [dot1x traps authentication quiet](#) (25 ページ)
- [dot1x traps authentication success](#) (26 ページ)
- [dot1x unlock client](#) (27 ページ)
- [dot1x violation-mode](#) (28 ページ)
- [show dot1x](#) (29 ページ)
- [show dot1x statistics](#) (34 ページ)
- [show dot1x users](#) (36 ページ)

# aaa authentication dot1x

802.1X 認証の有効時の認証に使用するサーバを指定するには、グローバル コンフィギュレーションモードで **aaa authentication dot1x** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

## 構文

```
aaa authentication dot1x default {radius | none | {radius none}}
```

```
no aaa authentication dot1x default
```

## パラメータ

- **radius** : すべての RADIUS サーバのリストを認証に使用します。
- **none** : 認証を使用しません。

## デフォルト設定

RADIUS サーバ。

## コマンドモード

グローバル コンフィギュレーションモード

## 使用上のガイドライン

RADIUS サーバによる認証、認証なし (**none**)、または両方の方式を選択できます。

RADIUS サーバ応答が受信されなかったときにも認証を成功させる必要がある場合は、コマンドラインで最後の方式として **none** を指定します。

## 例

次の例では、RADIUS サーバ認証に 802.1X 認証モードを設定しています。応答が受信されなかった場合でも、認証が成功します。

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

# clear dot1x statistics

802.1X 統計情報をクリアするには、特権 EXEC モードで **clear dot1x statistics** コマンドを使用します。

## 構文

**clear dot1x statistics** [*interface-id*]

## パラメータ

- *interface-id* : イーサネット ポート ID を指定します。

## デフォルト設定

すべてのポートの統計がクリアされます。

## コマンドモード

特権 EXEC モード

## 使用上のガイドライン

このコマンドにより、**show dot1x** および **show dot1x statistics** コマンドに表示されるすべてのカウンタがクリアされます。

## 例

```
switchxxxxxx# clear dot1x statistics
```

## dot1x authentication

ポートで認証方式を有効にするには、インターフェイス コンフィギュレーション モードで **dot1x authentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

```
dot1x authentication [802.1x] [mac] [web]
```

```
no dot1x authentication
```

### パラメータ

- **802.1x** : 802.1X に基づく認証 (802.1X ベース認証) を有効にします。
- **mac** : ステーションの MAC アドレスに基づく認証 (MAC ベース認証) を有効にします。
- **web** : Web ベース認証を有効にします。

### デフォルト設定

802.1X ベース認証が有効になっています。

### コマンドモード

インターフェイス (イーサネット) コンフィギュレーション モード

### ユーザガイドライン

スタティック MAC アドレスは、MAC ベースの方式で許可できません。

MAC アドレスが MAC ベース認証によって許可されている場合は、ダイナミック MAC アドレスをスタティック MAC アドレスに変更することや、MAC アドレスを削除することは推奨しません。

1. MAC ベースの認証で認証されたダイナミック MAC アドレスが静的 MAC アドレスに変更された場合は、手動では再認証されません。
2. MAC ベースの認証で認証されたダイナミック MAC アドレスを削除すると、再認証が行われます。

ポートチャネルに関連付けられたポートで有効になっている 802.1X には、次の制限があります。

- 802.1X ベースの認証のみがサポートされます。
- マルチホスト (レガシー 802.1X モード) モードのみがサポートされます。

## 例

次に、ポート gi1/0/1 の 802.1x とステーションの MAC アドレスに基づく認証を有効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/1  
switchxxxxxx(config-if)# dot1x authentication 802.1x mac
```

## dot1x guest-vlan

ゲスト VLAN を定義するには、インターフェイス（VLAN）コンフィギュレーションモードで **dot1x guest-vlan** モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x guest-vlan**

**no dot1x guest-vlan**

### デフォルト設定

ゲスト VLAN として定義されている VLAN はありません。

### コマンドモード

インターフェイス（VLAN）コンフィギュレーションモード

### 使用上のガイドライン

デバイスが持つことができるグローバルゲスト VLAN は1つのみです。

ゲスト VLAN はスタティック VLAN である必要があり、削除することはできません。

未承認 VLAN はゲスト VLAN に設定できません。

### 例

次の例では、ゲスト VLAN として VLAN 2 を定義しています。

```
switchxxxxxxx(config)# interface vlan 2
switchxxxxxxx(config-if)# dot1x guest-vlan
```

## dot1x guest-vlan enable

ゲスト VLAN へのアクセスインターフェイスで未承認ユーザを有効にするには、インターフェイス コンフィギュレーションモードで **dot1x guest-vlan enable** コマンドを使用します。アクセスを無効にするには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x guest-vlan enable**

**no dot1x guest-vlan enable**

### デフォルト設定

デフォルト設定では無効になっています。

### コマンドモード

インターフェイス（イーサネット）コンフィギュレーションモード

### 使用上のガイドライン

ゲスト VLAN と Web ベース認証は、ポートへの同時設定はできません。

モニタリング VLAN がインターフェイスで有効になっている場合、このコマンドを設定できません。

ポートがゲスト VLAN に属していない場合、ゲスト VLAN にタグなし出力ポートとして追加されます。

認証モードがシングルホストまたはマルチホストの場合、PVID の値はゲスト VLAN\_ID に設定されます。

認証モードがマルチセッションモードの場合、PVID は変更されず、許可されていないホストからの非認証 VLAN に属していないすべてのタグなしトラフィックおよびタグ付きトラフィックが、ゲスト VLAN にマッピングされます。

802.1X が無効になっている場合は、ポートのスタティック設定がリセットされます。

### 例

次の例では、gi1/0/1 の未承認ユーザがゲスト VLAN にアクセスできるようにします。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

## dot1x guest-vlan timeout

802.1X の有効化（またはポートのアップ）とポートのゲスト VLAN への追加の間の遅延を設定するには、グローバル コンフィギュレーション モードで **dot1x guest-vlan timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x guest-vlan timeout** *timeout*

**no dot1x guest-vlan timeout**

### パラメータ

- **timeout** : 802.1X を有効にしてから（またはポートがアップ状態になってから）ゲスト VLAN にポートが追加されるまでの時間遅延を秒単位で指定します。（範囲：30～180）。

### デフォルト設定

ゲスト VLAN がただちに適用されます。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

このコマンドは、ポート上でゲスト VLAN が有効になっている場合に関係します。タイムアウトを設定すると、802.1X を有効にしてから（またはポートがアップ状態になってから）デバイスによりゲスト VLAN にポートが追加されるまでの遅延が追加されます。

### 例

次の例では、802.1X を有効にしてからゲスト VLAN にポートが追加されるまでの遅延を 60 秒に設定しています。

```
switchxxxxxx(config)# dot1x guest-vlan timeout 60
```

## dot1x host-mode

IEEE 802.1X 承認済みポートでシングルホスト（クライアント）またはマルチホストを許可するには、インターフェイス コンフィギュレーションモードで **dot1x host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

```
dot1x host-mode {multi-host / single-host / multi-sessions}
```

### パラメータ

- **multi-host** : マルチホスト モードを有効にします。
- **single-host** : シングルホスト モードを有効にします。
- **multi-sessions** : マルチセッション モードを有効にします。

### デフォルト設定

デフォルトのモードはマルチホストです。

### コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

### ユーザ ガイドライン

#### シングルホスト モード

シングルホストモードでは、ポートの認証ステータスが管理されます。許可ホストがある場合、ポートが許可されます。このモードでは、単一のホストのみをポートで許可できます。

ポートが未承認で、ゲスト VLAN が有効な場合、タグなしトラフィックはゲスト VLAN に再マップされます。VLAN タグがゲスト VLAN または未認証 VLAN ではない場合、タグ付きトラフィックはドロップされます。ゲスト VLAN がポートで有効になっていない場合、未認証 VLAN に属するタグ付きトラフィックのみがブリッジされます。

ポートが許可されると、許可ホストからのタグなしトラフィックおよびタグ付きトラフィックが、ポートで設定されたスタティック VLAN メンバーシップに基づいてブリッジされます。他のホストからのトラフィックはドロップされます。

許可ホストからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。この場合、VLAN タグが RADIUS によって割り当てられた VLAN または認証されていない VLAN である場合を除いて、タグ付きトラフィックはドロップされます。

スイッチは、認証ステータスが許可から無許可に変更されたときに、ポートで学習されたすべての MAC アドレスを FDB から削除します。

### マルチホスト モード

マルチホストモードでは、ポートの認証ステータスが管理されます。少なくとも1つのホストが許可された後に、ポートが許可されます。

ポートが未承認で、ゲスト VLAN が有効な場合、タグなしトラフィックはゲスト VLAN に再マップされます。VLAN タグがゲスト VLAN または未認証 VLAN ではない場合、タグ付きトラフィックはドロップされます。ゲスト VLAN がポートで有効になっていない場合、未認証 VLAN に属するタグ付きトラフィックのみがブリッジされます。

ポートが許可されると、ポートに接続されたすべてのホストからのタグなしトラフィックおよびタグ付きトラフィックが、ポートで設定されたスタティック VLAN メンバシップに基づいてブリッジされます。

許可ポートからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。この場合、VLAN タグが RADIUS によって割り当てられた VLAN または認証されていない VLAN である場合を除いて、タグ付きトラフィックはドロップされます。

スイッチは、認証ステータスが許可から無許可に変更されたときに、ポートで学習されたすべての MAC アドレスを FDB から削除します。

### マルチセッション モード

シングルホストモードやマルチホストモード（ポートベースモード）とは異なり、マルチセッションモードでは、ポートに接続された各ホストの認証ステータスが管理されます（セッションベースモード）。ポートでマルチセッションモードが設定されている場合、ポートには認証ステータスがあります。任意の数のホストをポートで許可できます。[dot1x max-hosts](#) コマンドでは、ポートで許可される承認済みホストの最大数を制限できます。

各承認済みクライアントには、TCAM ルールが必要です。TCAM に使用可能な領域がない場合、認証は拒否されます。

認証が有効になっているときに **dot1x host-mode** コマンドを使用してポートモードを **single-host** または **multi-host** に変更すると、ポート ステートが無許可に設定されます。

認証が有効になっているときに **dot1x host-mode** コマンドでポートモードを **multi-session** に変更すると、接続されているすべてのホストのステートが無許可に設定されます。

ポートモードを **single-host** または **multi-host** に変更するには、ポートを **force-unauthorized** に設定し（**dot1x port-control**）、ポートモードを **single-host** または **multi-host** に変更して、ポートを **authorization auto** に設定します。

マルチセッションモードと、次のコマンドで設定されるポリシー ベース VLAN を同時に同じインターフェイスに設定することはできません。

- `switchport general map protocol-group vlans`
- `switchport general map macs-group vlans`

未認証 VLAN に属するタグ付きトラフィックは、ホストが承認済みかどうかに関わらず、常にブリッジされます。

ゲスト VLAN が有効になっている場合、認証されていない VLAN に属していない許可されていないホストからのタグなしトラフィックおよびタグ付きトラフィックは、ゲスト VLAN を介してブリッジされます。

許可ホストからのトラフィックは、ポートのスタティック設定に従ってブリッジされます。認証されていない VLAN に属していない許可ホストからのタグなしトラフィックおよびタグ付きトラフィックが、認証プロセス中に RADIUS サーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。

スイッチは、認証ステータスが許可から無許可に変更されたときに、ポートで学習されたホスト MAC アドレスを FDB から削除しません。エージングタイムアウトになると、MAC アドレスが削除されます。

ポートチャンネルに関連付けられたポートで有効になっている 802.1X には、次の制限があります。

- 802.1X ベースの認証のみがサポートされます。
- マルチホスト（レガシー 802.1X モード）モードのみがサポートされます。

#### 例

```
switchxxxxxx(config)# interface gil/0/1  
switchxxxxxx(config-if)# dot1x host-mode multi-host
```

## dot1x max-hosts

インターフェイスに許可される承認済みホストの最大数を設定するには、インターフェイスコンフィギュレーションモードで **dot1x max-hosts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x max-hosts** *count*

**no dot1x max-hosts**

### パラメータ

- **count** : インターフェイスで許可される許可ホストの最大数を指定します。32 ビットの正の数を使用できます。

### デフォルト設定

制限されていません。

### コマンドモード

インターフェイス（イーサネット）コンフィギュレーションモード

### ユーザガイドライン

デフォルトでは、インターフェイス上で許可される許可ホストの数は制限されていません。インターフェイス上で許可される許可ホストの数を制限するには、**dot1x max-hosts** コマンドを使用します。

このコマンドは、マルチセッションモードにのみ関係します。

### 例

次に、イーサネットポート **gi1/0/1** 上の許可ホストの最大数を **6** に制限する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-hosts 6
```

## dot1x max-req

(応答がない場合) 認証プロセスが再起動されるまでに、デバイスが Extensible Authentication Protocol (EAP) request/identity フレームをクライアントに送信する最大回数を設定するには、インターフェイス コンフィギュレーションモードで **dot1x max-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x max-req** *count*

**no dot1x max-req**

### パラメータ

- **count** : デバイスが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最大回数を設定します。(範囲: 1 ~ 10)。

### デフォルト設定

デフォルトの最大試行回数は 2 回です。

### コマンドモード

インターフェイス (イーサネット、OOB) コンフィギュレーションモード

### 使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

### 例

次の例では、デバイスが EAP Request/Identity フレームを送信する最大回数を 6 回に設定しています。

```
switchxxxxxx(config)# interface gil/0/1
switchxxxxxx(config-if)# dot1x max-req 6
```

# dot1x port-control

ポートの承認状態の手動コントロールを有効にするには、インターフェイスコンフィギュレーションモードで **dot1x port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

## 構文

```
dot1x port-control {auto | force-authorized | force-unauthorized} [time-range time-range-name]
```

```
no dot1x port-control
```

## パラメータ

- **auto** : ポートで 802.1X 認証を有効にし、デバイスおよびクライアント間の 802.1X 認証交換に基づきポートを許可ステートまたは無許可ステートに移行します。
- **force-authorized** : インターフェイスで 802.1X 認証を無効にし、認証交換を必要とせずにポートを許可ステートに移行します。ポートは 802.1X ベースのクライアント認証なしでトラフィックを送受信します。
- **force-unauthorized** : ポートを強制的に無許可ステートに移行し、クライアントからの認証試行をすべて無視して、このポート経由のすべてのアクセスを拒否します。デバイスはこのポートを介してクライアントに認証サービスを提供できません。
- **time-range time-range-name** : 時間範囲を指定します。時間範囲が有効でない場合、ポートは無許可ステートになります。(範囲: 1 ~ 32 文字)。

## デフォルト設定

ポートは **force-authorized** ステートです。

## コマンドモード

インターフェイス (イーサネット、OOB) コンフィギュレーションモード

## 使用上のガイドライン

同じインターフェイスでポートセキュリティ機能がすでに有効になっている場合は、インターフェイスで 802.1X 認証を有効にすることはできません。

スイッチは、認証制御が **force-authorized** から別のものに変更されたときに、ポートで学習されたすべての MAC アドレスを削除します。



- 
- (注) 認証が成功したらただちにフォワーディングステートに進むことができるように、エンドステーションに接続されている **auto** ステートの 802.1X エッジポートでスパニングツリーを無効にするか、スパニングツリー PortFast モードを有効にすることを推奨します。
-

**例**

次に、gi1/0/1 の 802.1X 認証を auto モードに設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1  
switchxxxxxx(config-if)# dot1x port-control auto
```

## dot1x re-authenticate

すべての 802.1X 対応ポートまたは指定した 802.1X 対応ポートの再認証を手動で開始するには、特権 EXEC モードで **dot1x re-authenticate** コマンドを使用します。

### 構文

**dot1x re-authenticate** [*interface-id*]

### パラメータ

- *interface-id* : イーサネットポートまたは OOB ポートを指定します。

### デフォルト設定

ポートが指定されていない場合は、すべてのポートにコマンドが適用されます。

### コマンドモード

特権 EXEC モード

### 例

次に、802.1X 対応の gi1/0/1 の再認証を手動で開始するコマンドを示します。

```
switchxxxxxx# dot1x re-authenticate gi1/0/1
```

## dot1x system-auth-control

802.1X をグローバルに有効にするには、グローバル コンフィギュレーション モードで **dot1x system-auth-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x system-auth-control**

**no dot1x system-auth-control**

### デフォルト設定

ディセーブル

### コマンドモード

グローバル コンフィギュレーション モード

### 例

次の例では、802.1X をグローバルに有効にしています。

```
switchxxxxxx(config)# dot1x system-auth-control
```

## dot1x timeout quiet-period

デバイスが、認証交換に失敗した後に待機状態になる時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout quiet-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x timeout quiet-period** *seconds*

**no dot1x timeout quiet-period**

### パラメータ

- **seconds** : クライアントとの認証交換が失敗した後にデバイスが待機状態を維持する時間間隔を秒単位で指定します。(範囲 : 10 ~ 65535 秒)。

### デフォルト設定

デフォルトの待機時間は 60 秒です。

### コマンドモード

インターフェイス (イーサネット、OOB) コンフィギュレーション モード

### 使用上のガイドライン

待機時間中は、デバイスが認証要求を受け入れることも開始することはありません。

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントまたは認証サーバに特定の動作上の問題がある場合など、異常な状況に適応する場合にのみ変更するようにしてください。

より高速な応答時間をユーザに提供するには、デフォルト値よりも小さい数値を入力する必要があります。

802.1x および MAC ベースの認証の場合、失敗したログインの回数は 1 回です。

Web ベースの認証では、試行が複数回失敗した後に、待機時間が適用されます。

802.1x ベースおよび MAC ベースの認証方式では、試行が失敗するたびに待機時間が適用されます。

### 例

次の例では、認証交換に失敗した後にデバイスが待機状態を維持する時間間隔を、120 秒に設定しています。

```
switchxxxxxx(config)# interface gil/0/1
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

## dot1x timeout reauth-period

再認証の試行間隔を秒単位で指定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout reauth-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x timeout reauth-period** seconds

**no dot1x timeout reauth-period**

### パラメータ

- **reauth-period** seconds : 再認証試行間の秒数。 (範囲 : 300 ~ 4294967295) 。

### デフォルト設定

3600

### コマンドモード

インターフェイス (イーサネット、OOB) コンフィギュレーション モード

### 使用上のガイドライン

このコマンドは、802.1x 認証方式のみに適用されます。

### 例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

## dot1x timeout server-timeout

デバイスが認証サーバからの応答を待つ時間間隔を設定するには、インターフェイスコンフィギュレーションモードで **dot1x timeout server-timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x timeout server-timeout** *seconds*

**no dot1x timeout server-timeout**

### パラメータ

- **server-timeout** *seconds* : デバイスが認証サーバからの応答を待機する時間間隔を秒単位で指定します。(範囲: 1 ~ 65535 秒)。

### デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

### コマンドモード

インターフェイス (イーサネット、OOB) コンフィギュレーションモード

### 使用上のガイドライン

実際のタイムアウト期間は、このコマンドによって指定した値と、**radius-server transmit** コマンドによって指定したタイムアウト期間で **radius-server retransmit** コマンドによって指定した再試行回数を乗算した結果と比較し、この 2 つの値の低い方を選択することで決定されます。

### 例

次の例では、認証サーバへのパケットの再送信の時間間隔を 3600 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

## dot1x timeout silence-period

認証サイレンス時間を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout silence-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x timeout silence-period** *seconds*

no dot1x timeout silence-period

### パラメータ

- **seconds** : サイレンス間隔を秒単位で指定します。有効な範囲は 60 ~ 65535 です。

### デフォルト設定

サイレンス期間は制限されていません。

### コマンドモード

インターフェイス (イーサネット) コンフィギュレーション モード

### 使用上のガイドライン

サイレンス時間は、承認済みクライアントがこの期間にトラフィックを送信しないと、未承認に変更になる期間 (秒単位) です。

承認済みクライアントが、このコマンドで指定したサイレンス期間にトラフィックを送信しないと、クライアントの状態が未承認に変更されます。

このコマンドは、Web ベース認証にのみ適用されます。

### 例

次の例では、認証のサイレンス時間を 100 秒に設定しています。

```
switchxxxxxx(config)# interface gil/0/1
switchxxxxxx(config-if)# dot1x timeout silence-period 100
```

## dot1x timeout supp-timeout

デバイスが要求を再送信するまでに、Extensible Authentication Protocol (EAP) request フレームに対するクライアントの応答を待つ時間間隔を設定するには、インターフェイスコンフィギュレーションモードで **dot1x timeout supp-timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x timeout supp-timeout** *seconds*

**no dot1x timeout supp-timeout**

### パラメータ

- **supp-timeout** *seconds* : 要求を再送信する前にクライアントからの EAP Request フレームへの応答をデバイスが待機する時間間隔を秒単位で指定します。（範囲：1 ~ 65535 秒）。

### デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

### コマンドモード

インターフェイス（イーサネット、OOB）コンフィギュレーションモード

### 使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

このコマンドは、802.1x 認証方式のみに適用されます。

### 例

次の例では、要求を再送信する前にクライアントからの EAP Request フレームへの応答をデバイスが待機する時間間隔を、3600 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

## dot1x timeout tx-period

デバイスが要求を再送信するまでに、Extensible Authentication Protocol (EAP) request/identity フレームに対するクライアントの応答を待つ時間間隔を設定するには、インターフェイスコンフィギュレーションモードで **dot1x timeout tx-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x timeout tx-period** *seconds*

**no dot1x timeout tx-period**

### パラメータ

- *seconds* : 要求を再送信する前にクライアントからの EAP-Request/Identity フレームへの応答をデバイスが待機する時間間隔を秒単位で指定します。(範囲 : 30 ~ 65535 秒)。

### デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

### コマンドモード

インターフェイス (イーサネット、OOB) コンフィギュレーションモード

### 使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

このコマンドは、802.1x 認証方式のみに適用されます。

### 例

次のコマンドでは、EAP Request/Identity フレームへの応答をデバイスが待機する時間間隔を、60 秒に設定しています。

```
switchxxxxxx(config)# interface gil/0/1:  
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

# dot1x traps authentication failure

802.1X 認証方式の失敗時のトラップ送信を有効にするには、グローバルコンフィギュレーションモードで **dot1x traps authentication failure** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

## 構文

**dot1x traps authentication failure** {[802.1x] [mac] [web]}

**no dot1x traps authentication failure**

## パラメータ

- **802.1x** : 802.1X ベース認証のトラップを有効にします。
- **mac** : MAC ベース認証のトラップを有効にします。
- **web** : WEB ベース認証のトラップを有効にします。

## デフォルト設定

すべてのトラップが無効になっています。

## コマンドモード

グローバル コンフィギュレーション モード

## 使用上のガイドライン

キーワードの組み合わせに制限はありません。少なくとも1つのキーワードを設定する必要があります。

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

## 例

次の例では、802.1X MAC 認証アクセス コントロールによる MAC アドレスの許可に失敗した場合のトラップ送信を有効にしています。

```
switchxxxxxx(config)# dot1x traps authentication failure 802.1x
```

## dot1x traps authentication quiet

ログイン試行に最大連続回数失敗した後、ホスト状態が待機状態に設定された場合にトラップ送信を有効にするには、グローバルコンフィギュレーションモードで **dot1x traps authentication quiet** コマンドを使用します。このトラップを無効にするには、このコマンドの **no** 形式を使用します。

### 構文

**dot1x traps authentication quiet**

**no dot1x traps authentication quiet**

### デフォルト設定

待機トラップが無効になっています。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

トラップは、ログインの最大連続試行回数の後に、クライアントが待機状態に設定されると送信されます。

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

### 例

次の例では、ホストが待機状態に設定されたときのトラップ送信を有効にしています。

```
switchxxxxxx(config)# dot1x traps authentication quiet
```

## dot1x traps authentication success

ホストが 802.1X 認証方式によって正常に承認された場合にトラップの送信を有効にするには、グローバル コンフィギュレーション モードで **dot1x traps authentication success** コマンドを使用します。このトラップを無効にするには、このコマンドの **no** 形式を使用します。

### 構文

```
dot1x traps authentication success {[802.1x] [mac] [web]}
```

```
no dot1x traps authentication success
```

### パラメータ

- **802.1x** : 802.1X ベース認証のトラップを有効にします。
- **mac** : MAC ベース認証のトラップを有効にします。
- **web** : WEB ベース認証のトラップを有効にします。

### デフォルト設定

成功トラップが無効になっています。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

キーワードの組み合わせに制限はありません。少なくとも1つのキーワードを設定する必要があります。

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

### 例

次の例では、802.1X MAC 認証アクセス コントロールにより MAC アドレスが正常に許可された場合のトラップ送信を有効にしています。

```
switchxxxxxx(config)# dot1x traps authentication success mac
```

# dot1x unlock client

ロックされた（待機期間中の）クライアントをロック解除するには、特権EXECモードで **dot1x unlock client** コマンドを使用します。

## 構文

**dot1x unlock client** *interface-id mac-address*

## パラメータ

- **interface-id** : クライアントが接続されているインターフェイス ID。
- **mac-address** : クライアント MAC アドレス。

## デフォルト設定

クライアントは、待機時間が終わるまでロックされています。

## コマンドモード

特権 EXEC モード

## 使用上のガイドライン

許可された認証の最大失敗試行回数その後でロックされたクライアントのロックを解除し、待機時間を終了するには、このコマンドを使用します。クライアントが待機時間でない場合、このコマンドは影響を与えません。

## 例

```
switchxxxxx# dot1x unlock client gi1/0/1 00:01:12:af:00:56
```

## dot1x violation-mode

シングルホストモードの承認済みポートの未承認ホストがインターフェイスへのアクセスを試行する場合のアクションを設定するには、インターフェイス コンフィギュレーション モードで **dot1x violation-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

### 構文

```
dot1x violation-mode {restrict | protect | shutdown} [traps seconds]
```

```
no dot1x violation-mode
```

### パラメータ

- **restrict** : MAC アドレスがサブリカント MAC アドレスではないステーションがインターフェイスへのアクセスを試みると、トラップを生成します。トラップ間の最小時間は1秒です。これらのフレームは転送されますが、送信元アドレスは学習されません。
- **protect** : サブリカントアドレスではない送信元アドレスを持つフレームを廃棄します。
- **shutdown** : サブリカントアドレスではない送信元アドレスを持つフレームを廃棄し、ポートをシャットダウンします。
- **trap seconds** : SNMP トラップを送信し、連続するトラップ間の最小時間を指定します。seconds を 0 にした場合、トラップは無効になります。このパラメータを指定しない場合、デフォルトは制限モードでは 1 秒になり、その他のモードでは 0 になります。

### デフォルト設定

Protect

### コマンドモード

インターフェイス (イーサネット) コンフィギュレーション モード

### ユーザ ガイドライン

このコマンドは、シングルホストモードにのみ関係します。

保護モードでは、MAC アドレスがサブリカント MAC アドレスではない BPDU メッセージが廃棄されません。

シャットダウンモードでは、MAC アドレスがサブリカント MAC アドレスではない BPDU メッセージによりシャットダウンが行われます。

### 例

```
switchxxxxxxx(config)# interface gil/0/1  
switchxxxxxxx(config-if)# dot1x violation-mode protect
```

# show dot1x

802.1X インターフェイスまたは指定したインターフェイスのステータスを表示するには、特権 EXEC モードで **show dot1x** コマンドを使用します。

## 構文

**show dot1x** [**interface** interface-id | **detailed**]

## パラメータ

- **interface-id** : イーサネット ポートまたは OOB ポートを指定します。
- **detailed** : 提供ポートと未提供ポートの情報を表示します。

## デフォルト設定

すべてのポートについて表示します。 **detailed** を使用しない場合、現在のポートだけが表示されます。

## コマンドモード

特権 EXEC モード

## 例

次に、802.1x が有効になっているすべてのインターフェイスの認証情報を表示する例を示します。

```
switchxxxxxx# show dot1x
Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius, None
MAC-Based Authentication:
  Type: Radius
  Username Groupsize: 2
  Username Separator: -
  Username case: Lowercase
  Password: MD5 checksum 1238af77aaca17568f12988601fcabed
Unauthenticated VLANs: 100, 1000, 1021
Guest VLAN: VLAN 11, timeout 30 sec
Authentication failure traps are enabled for 802.1x+mac
Authentication success traps are enabled for 802.1x
Authentication quiet traps are enabled for 802.1x
Supplicant Global Configuration:
Supplicant Authentication failure traps are enabled
Supplicant Authentication success traps are enabled
gil/0/1
  Authenticator is enabled
  Supplicant is disabled
Authenticator Configuration:
Host mode: multi-sessions
Authentication methods: 802.1x+mac
Port Adminstrated status: auto
Guest VLAN: enabled
```

```
VLAN Radius Attribute: enabled, static
Open access: disabled
Time range name: work_hours (Active now)
Server-timeout: 30 sec
Maximum Hosts: unlimited
Maximum Login Attempts: 3
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
  EAP Timeout: 30 sec
  EAP Max-Retrans: 2
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  max-req: 2
Authentication success: 9
Authentication fails: 1
Number of Authorized Hosts: 10
Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gil/0/2
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: single-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: enabled
  Open access: enabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
  Mode: restrict
  Trap: enabled
  Trap Min Interval: 20 sec
  Violations were detected: 9
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
  EAP Timeout: 30 sec
  EAP Max-Retrans: 2
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  max-req: 2
  Authentication success: 2
  Authentication fails: 0
gil/0/3
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
```

```
Port Adminstrated status: auto
Port Operational status: authorized
Guest VLAN: disabled
VLAN Radius Attribute: disabled
Time range name: work_hours (Active now)
Open access: disabled
Server-timeout: 30 sec
Applied Authenticating Server: Radius
Applied Authentication method: 802.1x
Session Time (HH:MM:SS): 00:25:22
MAC Address: 00:08:78:32:98:66
Username: Bob
Violation:
  Mode: restrict
  Trap: enabled
  Trap Min Interval: 20 sec
  Violations were detected: 0
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
  EAP Timeout: 30 sec
  EAP Max-Retrans: 2
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  max-req: 2
Authentication success: 20
Authentication fails: 0
Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gil/0/4
Authenticator is disabled
Supplicant is enabled
Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: force-auto
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Applied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
```

```

max-req: 2
Authentication success: 0
Authentication fails: 0
Supplicant Configuration:
retry-max: 2
EAP time period: 15 sec
Supplicant Held Period: 30 sec
Credentials Name: Basic-User
Supplicant Operational status: authorized

```

次に、この出力で表示される重要なフィールドについて説明します。

- **Port** : ポートのインターフェイス ID。
- **Host mode** : ポート認証の設定されたモード。使用される値は、single-host、multi-host、multi-sessions です。
  - single-host
  - multi-host
  - multi-sessions
- **Authentication methods** : ポートで設定されている認証方式。使用される値は、次の方式の組み合わせです。
  - 802.1x
  - mac
  - wba
- **Port Administrated status** : ポートの管理（設定済み）モード。使用可能な値 : **force-auth**、**force-unauth**、**auto**。
- **Port Operational status** : ポートの動作（実際の）モード。使用可能な値 : **authorized** または **unauthorized**。
- **Username** : サプリカントアイデンティティを表すユーザ名。ポート制御が自動の場合は、このフィールドにユーザ名が表示されます。ポートが許可されている場合は、現在のユーザのユーザ名が表示されます。ポートが許可されていない場合は、最後に正常に認証されたユーザが表示されます。
- **Quiet period** : クライアントが無効なパスワードを提供した場合など、認証交換が失敗した後、デバイスが待機状態を維持する秒数。
- **Silence period** : このコマンドにより指定されたサイレンス期間中に許可クライアントがトラフィックを送信しなかった場合、そのクライアントが無許可状態に変更される秒数。
- **EAP timeout** : 要求が再送信されるまで EAP サーバ（EAP オーセンティケータ）が EAP クライアント（EAP ピア）からの応答を待つ時間間隔（秒単位）。
- **EAP Max Retrans** : EAP クライアント（EAP ピア）からの応答がない場合に、EAP サーバ（EAP オーセンティケータ）が EAP 要求を再送信する最大回数。

- **Tx period** : デバイスが Extensible Authentication Protocol (EAP) Request/Identity フレームに対するクライアントからの応答を待機し、要求を再送信するまでの秒数。
- **Max req** : (クライアントから応答が得られなかった場合に) デバイスが認証プロセスを再起動する前に、クライアントに EAP Request フレームを送信する最大回数。
- **Server timeout** : デバイスが認証サーバからの応答を待機し、要求を再送信するまでの秒数。
- **Session Time** : ユーザがログインしている時間の長さ (HH:MM:SS) 。
- **MAC address** : サブリカント MAC アドレス。
- **Authentication success** : ステート マシンが認証サーバから成功メッセージを受信した回数。
- **Authentication fails** : ステート マシンが認証サーバから失敗メッセージを受信した回数。

## show dot1x statistics

指定したポートの 802.1X 統計情報を表示するには、特権 EXEC モードで **show dot1x statistics** コマンドを使用します。

### 構文

```
show dot1x statistics interface interface-id
```

### パラメータ

- **interface-id** : イーサネット ポートまたは OOB ポートを指定します。

### コマンドモード

特権 EXEC モード

### 例

次に、gi1/0/1 の 802.1X 統計情報を表示する例を示します。

```
switchxxxxx# show dot1x statistics interface gi1/0/1
EapolEapFramesRx: 10
EapolStartFramesRx: 0
EapolLogoffFramesRx: 1
EapolAnnouncementFramesRx: 0
EapolAnnouncementReqFramesRx: 0
EapolInvalidFramesRx: 0
EapolEapLengthErrorFramesRx: 0
EapolMkNoCknFramesRx: 0
EapolMkInvalidFramesRx: 0
EapolLastRxFrameVersion: 3
EapolLastRxFrameSource: 00:08:78:32:98:78
EapolSuppEapFramesTx: 0
EapolStartFramesTx: 1
EapolLogoffFramesTx: 0
EapolAnnouncementFramesTx: 0
EapolAnnouncementReqFramesTx: 0
EapolAuthEapFramesTx: 9
EapolMkaFramesTx: 0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
<b>EapolInvalidFramesRx</b>	この PAE で受信したすべてのタイプの無効な EAPOL フレームの数。
EapolEapLengthErrorFramesRx	パケット本文の長さがこの PAE で受信した EAPOL MPDU のオクテット内に含まれているパケット本文と一致しない EAPOL フレームの数。
EapolAnnouncementFramesRx	この PAE で受信した EAPOL-Announcement フレームの数。

フィールド	説明
EapolAnnouncementReqFramesRx	この PAE で受信した EAPOL-Announcement-Req フレームの数。
EapolStartFramesRx	この PAE で受信した EAPOL-Start フレームの数。
EapolEapFramesRx	この PAE で受信した EAPOL-EAP フレームの数。
EapolLogoffFramesRx	この PAE で受信した EAPOL-Logoff フレームの数。
EapolMkNoCknFramesRx	この PAE で MKA が有効になっていないか、CKN が認識されない状態で受信した MKPDU の数。
EapolMkInvalidFramesRx	この PAE の受信プロセスでメッセージ認証が失敗した MKPDU の数。
EapolLastRxFrameVersion	この PAE で最後に受信した EAPOL フレームのバージョン。
EapolLastRxFrameSource	この PAE で最後に受信した EAPOL フレームの送信元 MAC アドレス。
EapolSuppEapFramesTx	この PAE のサブリカントで送信した EAPOL-EAP フレームの数。
EapolLogoffFramesTx	この PAE で送信した EAPOL-Logoff フレームの数。
EapolAnnouncementFramesTx	この PAE で送信した EAPOL-Announcement フレームの数。
EapolAnnouncementReqFramesTx	この PAE で送信した EAPOL-Announcement-Req フレームの数。
EapolStartFramesTx	この PAE で受信した EAPOL-Start フレームの数。
EapolAuthEapFramesTx	この PAE の認証で送信した EAPOL-EAP フレームの数。
EapolMkaFramesTx	この PAE で送信した CKN 情報のない EAPOL-MKA フレームの数。

## show dot1x users

デバイスのアクティブな 802.1X 承認済みユーザを表示するには、特権 EXEC モードで **show dot1x users** コマンドを使用します。

### 構文

```
show dot1x users [username username]
```

### パラメータ

- **username username** : サプリカントユーザ名 (長さ: 1 ~ 160 文字) を指定します。

### デフォルト設定

すべてのユーザを表示します。

### コマンドモード

特権 EXEC モード

**例 1** : 次のコマンドは、すべての 802.1x ユーザを表示します。

```
show dot1x users
```

Port	ユーザ名	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020
gi1/0/2	John	0008.3b79.8787	MAC	Remote	00:11:12	
		0008.3baa.0022	WBA	Remote	00:27:16	

**例 2** : 次の例では、サプリカントユーザ名が Bob の 802.1X ユーザを表示します。

```
switchxxxxxx# show dot1x users username Bob
```

Port	ユーザ名	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。