authentication command bounce-port ignore ～ auth-type

- authentication command bounce-port ignore, 2 ページ
- authentication command disable-port ignore, 4 ページ
- authentication control-direction, 6 ページ
- authentication event fail, 8 ページ
- authentication event server alive action reinitialize, 10 ページ
- authentication event server dead action authorize, 12 ページ
- authentication fallback, 14 ページ
- authentication host-mode, 16 ページ
- authentication open, 18 ページ
- authentication order, 20 ページ
- authentication periodic, 22 ページ
- authentication port-control, 24 ページ
- authentication priority, 26 ページ
- authentication timer inactivity, 28 ページ
- authentication timer reauthenticate, 30 ページ
- authentication timer restart, 32 ページ
- authentication violation, 34 ページ
- auth-type, 36 ページ

authentication command bounce-port ignore

ルータが RADIUS 許可変更（CoA）bounce port コマンドを無視するように設定するには、グローバル コンフィギュレーション モードで **authentication command bounce-port ignore** コマンドを使用します。 デフォルト ステータスに戻すには、このコマンドの **no** 形式を使用します。

authentication command bounce-port ignore

no authentication command bounce-port ignore

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ルータが RADIUS CoA bounce port コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが導入されました。
12.2(33)SXI4	このコマンドが、Cisco IOS Release 12.2(33)SXI4 に統合されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

RADIUS CoA bounce port コマンドが RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）の再ネゴシエーションが開始されます。 この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。

authentication command bounce-port ignore コマンドは、ルータが RADIUS CoA bounce port コマンドを無視し、認証ポートに接続されているホストのリンク フラップの発生を防ぐように設定します。

例

次に、ルータが RADIUS CoA bounce port コマンドを無視するように設定する例を示します。

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

関連コマンド

コマンド	説明
authentication command disable-port ignore	ルータが RADIUS サーバの CoA **disable port** コマンドを無視するように設定します。

authentication command disable-port ignore

ルータがRADIUSサーバの許可変更（CoA）disable portコマンドを無視するように設定するには、グローバル コンフィギュレーション モードで **authentication command disable-port ignore** コマンドを使用します。 デフォルト ステータスに戻すには、このコマンドの **no** 形式を使用します。

authentication command disable-port ignore

no authentication command disable-port ignore

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ルータが RADIUS CoA disable port コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが導入されました。
12.2(33)SXI4	このコマンドが、Cisco IOS Release 12.2(33)SXI4に統合されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)Tに統合されました。

使用上のガイドライン

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。 ルータが RADIUS サーバの CoA disable port コマンドを無視し、この認証ポートの認証ポートおよびその他のホストが切断されないように設定するには、**authentication command disable-port ignore** コマンドを使用します。

例

次に、ルータが CoA **disable port** コマンドを無視するように設定する例を示します。

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

関連コマンド

コマンド	説明
authentication command bounce-port ignore	ルータが RADIUS サーバの CoA bounce port コマンドを無視するように設定します。

authentication control-direction

ポートの認証制御の方向を設定するには、インターフェイス コンフィギュレーション モードで **authentication control-direction** 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。

authentication control-direction {**both**| **in**}

no authentication control-direction

構文の説明

both	ポートで双方向制御をイネーブルにします。
in	ポートで単方向制御をイネーブルにします。

コマンド デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

IEEE 802.1x 標準は、nonauthenticated クライアントとネットワーク リソース間のトラフィックをブロックするために実装されます。 これは、nonauthenticated クライアントがオーセンティケータ以外のネットワーク上のデバイスと通信できないことを意味します。 リバースは true です。ただし、ポートが単方向制御ポートとして設定されている場合を除きます。

単方向ステート

IEEE 802.1x 標準は、ネットワーク上のデバイスがクライアントを「起動」してクライアントが再認証され続けるように、単方向制御ポートを定義します。 **authentication control-direction in** コマンドを使用してポートを単方向に設定すると、ポートはスパニングツリー フォワーディング ステートに変更され、ネットワーク上のデバイスがクライアントを起動して強制的に再認証を行わせることが許可されます。

双方向ステート

authentication control-direction both コマンドを使用してポートを双方向に設定すると、ポートへのアクセスが両方向で制御されます。 この場合、ポートはパケットを送受信しません。

例

次の例では、単方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# authentication control-direction in
```

次に、双方向制御をイネーブルにする例を示します。

```
Switch(config-if)# authentication control-direction both
```

authentication event fail

ユーザ クレデンシャルが認識されないときの認証エラーを Auth Manager が処理する方法を指定するには、インターフェイス コンフィギュレーション モードで **authentication event fail** 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。

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id*| **next-method**}

no authentication event fail

構文の説明

retry *retry-count*	（任意）認証が最初に失敗した後に試行される認証方式の回数を指定します。
action	不正なユーザ クレデンシャルによって認証が失敗した後に実行するアクションを指定します。
authorize vlan *vlan-id*	認証の試行が失敗した後に、ポートの制限付き VLAN を許可します。
next-method	認証の試行が失敗した後に呼び出される次の認証方式を指定します。 認証方式の順序は、**authentication order** コマンドによって指定されます。

コマンド デフォルト

認証は最初の試行が失敗した後に 2 回試行されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

dot1x 認証方式だけが、この認証失敗のタイプをシグナリングできます。

例

次に、認証試行に 3 回失敗した後、ポートが制限付き VLAN に割り当てられるように指定する例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event fail retry 3 action authorize vlan 40

Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication event no-response action	ホストが応答しないことにより認証が失敗した場合に実行するアクションを指定します。
authentication order	試行する認証方式の順序を指定します。

authentication event server alive action reinitialize

以前は到達不能だった認証、許可、アカウンティング（AAA）サーバが使用可能になった場合に、許可された Auth Manager セッションを再初期化するには、インターフェイス コンフィギュレーション モードで **authentication event server alive action reinitialize** 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。

authentication event server alive action reinitialize

no authentication event server alive action reinitialize

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

セッションは再初期化されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

以前は到達不能だった AAA サーバが使用可能になった場合は、**authentication event server alive action reinitialize** コマンドを使用して、許可されたセッションを再初期化します。

例

次に、以前は到達不能だったAAAサーバが使用可能になった場合に、許可されたセッションが再初期化されるように指定する例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication event server dead action authorize	AAA サーバが到達不能の場合に、許可されたセッションの処理方法を指定します。

authentication event server dead action authorize

認証、許可、アカウンティング（AAA）サーバが到達不能になった場合にAuth Managerセッションを許可するには、インターフェイス コンフィギュレーション モードで **authentication event server dead action authorize** 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。

authentication event server dead action authorize vlan *vlan-id*

no authentication event server dead action authorize

構文の説明

vlan *vlan-id*	認証の試行が失敗した後に、ポートの制限付きVLAN を許可します。

コマンド デフォルト

セッションは許可されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

AAA サーバが使用できない場合でも、**authentication event server dead action authorize** コマンドを使用してセッションを許可できます。

例

次に、AAAサーバが到達不能になった場合に、ポートがVLANに割り当てられるように指定する例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server dead action authorize vlan 40

Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication event server alive action reinitialize	以前は到達不能だった AAA サーバが使用可能になったときに、許可されたセッションを再初期化します。

authentication fallback

Web 認証フォールバック方式をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication fallback** コマンドを使用します。 Web 認証フォールバックをディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication fallback *fallback-profile*

no authentication fallback

構文の説明

fallback-profile	Web 認証フォールバック プロファイルの名前。

コマンド デフォルト

Web 認証フォールバックはイネーブルではありません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

Web 認証フォールバック プロファイルを指定するには、**authentication fallback** コマンドを使用します。 プロファイルの詳細を指定するには、**fallback profile** コマンドを使用します。

例

次に、ポートにフォールバック プロファイルを指定する例を示します。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet1/0/3
Router(config-if)# authentication fallback profile1
Router(config-if)# end
```

関連コマンド

コマンド	説明
fallback profile	Web 認証のプロファイルを指定します。

authentication host-mode

ホストの制御ポートへのアクセスを許可するには、インターフェイス コンフィギュレーション モードで**authentication 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。

authentication host-mode {**single-host**| **multi-auth**| **multi-domain**| **multi-host**} **[open]**

no authentication host-mode

構文の説明

single-host	常に 1 つのクライアントだけがポートで認証できるように指定します。複数のクライアントが検出された場合、セキュリティ違反が発生します。
multi-auth	常に複数のクライアントがポートで認証できるように指定します。
multi-domain	ドメイン（DATA または VOICE）ごとに、一度に 1 つのクライアントだけが認証できるように指定します。
multi-host	最初のクライアントが認証されると、それ以降のすべてのクライアントのアクセスが許可されるように指定します。
open	（任意）ポートが開くように指定します。つまり、アクセス制限はありません。

コマンド デフォルト

ポートへのアクセスは許可されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

このコマンドを使用する前に、**authentication port-control** コマンドをキーワード **auto** で使用する必要があります。

multi-host モードでは、すべてのホストのネットワーク アクセスが許可されるように、接続されたホストのうち 1 つだけが正常に許可される必要があります。 ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）は、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

例

次に、**multi-host** モードで認証をイネーブルにする例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# authentication port-control auto

Switch(config-if)# authentication host-mode multi-host
```

関連コマンド

コマンド	説明
authentication port-control	インターフェイスに関する情報を表示します。

authentication open

このポートでオープン アクセスをイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication open** コマンドを使用します。 このポートでオープン アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication open

no authentication open

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドがサポートされるようになりました。

使用上のガイドライン

オープン アクセスを使用すると、認証の実行前にクライアントまたはデバイスがネットワークにアクセスできます。

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

このコマンドは、ポートに対してのみ **authentication host-mode** *session-type* **open** グローバル コンフィギュレーション コマンドよりも優先されます。

例

次の例では、ポートに対してオープン アクセスをイネーブルにする方法を示します。

```
Router(config-if)# authentication open
Router(config-if)#
```

次の例では、ポートに対してオープン アクセスをイネーブルにする方法を示します。

```
Router(config-if)# no authentication open
Router(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication order

ポートで Auth Manager がクライアントの認証を試行する順序を指定するには、インターフェイス コンフィギュレーション モードで **authentication order** コマンドを使用します。 デフォルトの認証順序に戻すには、このコマンドの **no** 形式を使用します。

authentication order {**dot1x** [**mab**| **webauth**] **[webauth]**| **mab** [**dot1x**| **webauth**] **[webauth]**| **webauth**}

no authentication order

構文の説明

dot1x	IEEE 802.1X 認証を指定します。
mab	MAC ベースの認証（MAB）を指定します。
webauth	Web ベースの認証を指定します。

コマンド デフォルト

デフォルトの認証順序は **dot1x**、**mab**、および **webauth** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

authentication order コマンドを使用して、実行する認証方式を明示的に指定し、その実行する順序を指定します。 各方式は一度だけリストに入力できます。**webauth** の後に方式をリストすることはできません。

例

次に、ポートに認証順序を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet0/1
```

```
Router(config-if)# authentication order mab dot1x
Router(config-if)# end
Router#
```

関連コマンド

コマンド	説明
authentication priority	ポートでの認証方式のプライオリティを指定します。

authentication periodic

ポートの自動再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication periodic** コマンドを使用します。 ディセーブルにするには、このコマンドの **no** 形式を使用します。

（注） Cisco IOS Release 12.2(33)SXI から、**dot1x reauthentication** コマンドが、**authentication periodic** コマンドに置き換えられました。

authentication periodic

no authentication periodic

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

再認証はディセーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ポートの自動再認証をイネーブルにするには、**authentication periodic** コマンドを使用します。 再認証の試行間隔を設定するには、**authentication timer reauthenticate** コマンドを使用します。

例

次に、再認証をイネーブルにし、試行間隔を 1800 秒に設定する例を示します。

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 1800
```

関連コマンド

コマンド	説明
authentication timer reauthenticate	許可ポートの再認証の試行間隔を指定します。

authentication port-control

制御ポートの許可ステートを設定するには、インターフェイスコンフィギュレーションモードで **authentication port-control** コマンドを使用します。 ポート制御値をディセーブルにするには、このコマンドの **no** 形式を使用します。

（注） Cisco IOS Release 12.2(33)SXI から、**dot1x port-control** コマンドが、**authentication port-control** コマンドに置き換えられました。

authentication port-control {**auto**| **force-authorized**| **force-unauthorized**}

no authentication port-control

構文の説明

auto	ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのは Extensible Authentication Protocol over LAN（EAPOL）フレームだけです。
force-authorized	インターフェイスの IEEE 802.1X をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。**force-authorized** キーワードはデフォルトです。
force-unauthorized	クライアントからの認証試行をすべて無視し、ポートを強制的に無許可ステートに変更して、このインターフェイス経由のすべてのアクセスを拒否します。

コマンド デフォルト

ポートは認証情報の交換なしで許可されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ポート制御の設定を確認するには、**show interfaces** コマンドを使用するか、ディスプレイの 802.1X Port Summary セクションの Status カラムを確認します。 enabled ステータスは、ポート制御値が auto または force-unauthorized に設定されていることを意味します。

ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。 システムはクライアントの識別情報を要求して、クライアントと認証サーバ間で認証メッセージのリレーを開始します。

例

次に、クライアントの許可ステータスが認証プロセスによって決定されるように指定するコマンドの例を示します。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface ethernet0/2

Router(config-if)# authentication port-control auto
```

関連コマンド

コマンド	説明
show interfaces	制御ポートの許可ステートを設定します。

authentication priority

ポートで認証方式のプライオリティを指定するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。 デフォルトに戻るには、**no** 形式のコマンドを使用します。

authentication priority {**dot1x** [**mab**| **webauth**] [**webauth**]| **mab** [**dot1x**| **webauth**] [**webauth**]| **webauth**}

no authentication priority

構文の説明

dot1x	IEEE 802.1X 認証を指定します。
mab	MAC ベースの認証を指定します。
webauth	Web ベースの認証を指定します。

コマンド デフォルト

デフォルトのプライオリティ順は **dot1x**、**mab**、および **webauth** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

authentication order コマンドは、認証方式を試行する順序を指定します。 これはデフォルトのプライオリティ順です。 デフォルトのプライオリティを上書きし、高いプライオリティの方式が認証方式の実行に割り込むことを許可するには、**authentication priority** コマンドを使用します。

例

次に、ポートで認証順序と認証のプライオリティの設定に使用するコマンドの例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet0/1
```

```
Router(config-if)# authentication order mab dot1x webauth
Router(config-if)# authentication priority dot1x mab
Router(config-if)# end
Router#
```

関連コマンド

コマンド	説明
authentication order	ポートでAuth Managerがクライアントの認証を試行する順序を指定します。

authentication timer inactivity

非アクティブな Auth Manager セッションが終了するまでの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 **authentication timer inactivity** コマンドを使用します。 非アクティビティ タイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication timer inactivity {*seconds*| **server**}

no authentication timer inactivity

構文の説明

seconds	Auth Manager セッションが終了してポートが無許可になる前に許可される非アクティビティ期間（秒単位）。 有効な範囲は 1 ～ 65535 です。
server	非アクティビティ期間が認証、許可、アカウンティング（AAA）サーバのアイドル タイムアウト値（RADIUS 属性 28）によって定義されるように指定します。

コマンド デフォルト

非アクティビティ タイマーはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

非アクティブ セッションの再認証を回避するには、**authentication timer inactivity** コマンドを使用して、非アクティビティ タイマーを、**authentication timer reauthenticate** コマンドで設定された再認証間隔よりも短い間隔に設定します。

例

次に、ポートの非アクティビティ間隔を 900 秒に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer inactivity 900

Switch(config-if)# end
```

関連コマンド

コマンド	説明
configuration timer reauthenticate	Auth Manager が、許可ポートの再認証の試行を開始するまでの時間を指定します。
authentication timer restart	Auth Manager が無許可ポートの認証の試行を開始するまでの間隔を指定します。

authentication timer reauthenticate

Auth Manager が許可ポートの再認証を試行する間隔を指定するには、インターフェイス コンフィギュレーション モードで **authentication timer reauthenticate** コマンドを使用します。 再認証間隔をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

authentication timer reauthenticate {*seconds*| **server**}

no authentication timer reauthenticate

構文の説明

seconds	再認証間隔（秒単位）。 デフォルト値は 3600 です。
server	再認証の試行間隔が、認証、許可、アカウンティング（AAA）サーバのセッション タイムアウト値（RADIUS 属性 27）で定義されるように指定します。

コマンド デフォルト

自動再認証間隔は 3600 秒に設定されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

許可ポートの自動再認証間隔を設定するには、**authentication timer reauthenticate** コマンドを使用します。 **authentication timer inactivity** コマンドを使用して非アクティビティ間隔を設定する場合は、再認証間隔を非アクティビティ間隔よりも長く設定します。

例

次に、ポートの再認証間隔を 1800 秒に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer reauthenticate 1800

Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication periodic	自動再認証をイネーブルにします。
authentication timer inactivity	Auth Manager が非アクティブ セッションを終了するまでの間隔を指定します。
authentication timer restart	Auth Manager が無許可ポートの認証の試行を開始するまでの間隔を指定します。

authentication timer restart

Auth Manager が無許可ポートの認証の試行を開始するまでの期間を指定するには、インターフェイス コンフィギュレーション モードで **authentication timer restart** コマンドを使用します。 間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

authentication timer restart *seconds*

no authentication timer restart

構文の説明

seconds	無許可ポートの認証試行間隔（秒単位）。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 60 です。

コマンド デフォルト

無許可ポートの認証の試行は行われません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

無許可ポートの認証試行間隔を指定するには、**authentication timer restart** コマンドを使用します。 デフォルト インターバルは 60 秒です。

例

次に、認証タイマーの間隔を 120 秒に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet6/0

Router(config-if)# authentication timer restart 120

Router(config-if)# end
```

関連コマンド

コマンド	説明
authentication timer inactivity	Auth Manager が無許可ポートの認証の試行を開始するまでの期間を指定します。
configuration timer reauthenticate	Auth Manager が、許可ポートの再認証の試行を開始するまでの時間を指定します。

authentication violation

ポートでセキュリティ違反が発生したときに実行するアクションを指定するには、インターフェイス コンフィギュレーション モードで **authentication violation** コマンドを使用します。 デフォルトのアクションに戻すには、このコマンドの **no** 形式を使用します。

authentication violation {**restrict**| **shutdown**}

no authentication violation

構文の説明

restrict	セキュリティ違反が発生したドメインに対してポートがトラフィックを制限するように指定します。
shutdown	セキュリティ違反に対してポートがシャットダウンするように指定します。

コマンド デフォルト

セキュリティ違反が発生すると、ポートはシャット ダウンします。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ポートでセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

例

次に、セキュリティ違反が発生したときに GigabitEthernet インターフェイスがトラフィックを制限するように設定する例を示します。

```
Switch(config)# interface GigabitEthernet6/2
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict

Switch(config-if)# end
```

auth-type

動的に認証または認証解除されるデバイスにポリシーを設定するには、アイデンティティ プロファイル コンフィギュレーション モードで **auth-type** コマンドを使用します。 指定されたポリシーを削除するには、このコマンドの **no** 形式を使用します。

auth-type {**authorize| not-authorize**} **policy** *policy-name*

no auth-type {**authorize| not-authorize**} **policy** *policy-name*

構文の説明

authorize	ポリシーは、すべての許可済みデバイスに指定されます。
not-authorize	ポリシーは、すべての許可されていないデバイスに指定されます。
policy *policy-name*	アイデンティティ ポリシー名が、関連付けられた認証結果に適用されるように指定します。

コマンド デフォルト

ポリシーは、許可済みまたは許可されていないデバイスには設定されません。

コマンド モード

アイデンティティ プロファイルの設定

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

使用上のガイドライン

このコマンドは、ネットワーク アクセス デバイスによってデバイスが動的に認証または認証解除される場合、およびデバイスにその認証結果に適用する必要があるポリシーの名前が必要である場合に使用されます。

例

次に、すべての動的に認証されたホストに対してアイデンティティ ポリシー「grant」に802.1x認証を適用する例を示します。

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit
Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit
Router (config)# identity profile dot1x

Router (config-identity-prof)# auth-type authorize policy grant
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを作成します。
identity profile dot1x	802.1xアイデンティティ プロファイルを作成します。