# D コマンド

この章では、D で始まる Cisco NX-OS Security コマンドについて説明します。

## deadtime

RADIUS または TACACS+ サーバ グループのデッド タイム間隔を設定するには、**deadtime** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**deadtime** *minutes*

**no deadtime** *minutes*

**シンタックスの説明**

| | |
|---|---|
| *minutes* | 間隔の分数。有効範囲は 0 ～ 1440 分です。 |

**（注）** デッド タイム間隔をゼロ（0）に設定すると、タイマーがディセーブルになります。

**デフォルト**

0 分

**コマンド モード**

RADIUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

**サポートされるユーザ ロール**

network-admin
vdc-admin

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン**

TACACS+ を設定する前に **feature tacacs+** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、RADIUS サーバ グループのデッド タイム間隔を 2 分に設定する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

次に、TACACS+ サーバ グループのデッド タイム間隔を 5 分に設定する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

次に、デッド タイム間隔をデフォルト値に戻す例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa group server** | AAA サーバ グループを設定します。 |
| **radius-server host** | RADIUS サーバを設定します。 |
| **show radius-server groups** | RADIUS サーバ グループ情報を表示します。 |
| **show tacacs-server groups** | TACACS+ サーバ グループ情報を表示します。 |
| **feature tacacs+** | TACACS+ をイネーブルにします。 |
| **tacacs-server host** | TACACS+ サーバを設定します。 |

# deny（ARP）

条件に一致する ARP トラフィックを拒否する ARP ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

### 一般的な構文

[*sequence-number*] **deny ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

[*sequence-number*] **deny request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

[*sequence-number*] **deny response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]

**no** *sequence-number*

**no deny ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

**no deny request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

**no deny response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]

### シンタックスの説明

| | |
|---|---|
| *sequence-number* | （任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。ACL 内のルールの順序は、シーケンス番号によって維持されます。<br><br>シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。<br><br>ACL 内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。<br><br>シーケンス番号を指定しない場合は、デバイスによってそのルールが ACL の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。<br><br>ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。 |
| ***ip*** | ルールの IP アドレス部分を示します。 |
| ***any*** | （任意）任意のホストがルールの ***any*** キーワードが含まれる部分に一致するように指定します。***any*** を使用して、送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレスを指定できます。 |
| ***host*** *sender-IP* | （任意）ARP パケットの送信元 IP アドレスが *sender-IP* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。*sender-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。 |
| *sender-IP*<br>*sender-IP-mask* | （任意）パケットの送信元 IP アドレスが一致する可能性のある IPv4 アドレスおよび IPv4 アドレス セットのマスク。*sender-IP* 引数と *sender-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*sender-IP-mask* 引数に 255.255.255.255 を指定することと、***host*** キーワードを使用することは同じです。 |
| ***mac*** | ルールの MAC アドレス部分を示します。 |

| | |
|---|---|
| ***host*** *sender-MAC* | （任意）ARP パケットの送信元 MAC アドレスが *sender-MAC* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。*sender-MAC* 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。 |
| *sender-MAC* *sender-MAC-mask* | （任意）パケットの送信元 MAC アドレスが一致する可能性のある MAC アドレスおよび MAC アドレス セットのマスク。*sender-MAC* 引数と *sender-MAC-mask* 引数は、ドット付き 16 進表記で指定する必要があります。*sender-MAC-mask* 引数に ffff.ffff.ffff を指定することと、***host*** キーワードを使用することは同じです。 |
| ***log*** | （任意）ルールに一致する ARP パケットをデバイスが記録するように指定します。 |
| ***request*** | （任意）ARP 要求メッセージが含まれるパケットのみにルールが適用されるように指定します。<br><br>**（注）** ***request*** キーワードと ***response*** キーワードの両方を省略すると、すべての ARP メッセージにルールが適用されます。 |
| ***response*** | （任意）ARP 応答メッセージが含まれるパケットのみにルールが適用されるように指定します。<br><br>**（注）** ***request*** キーワードと ***response*** キーワードの両方を省略すると、すべての ARP メッセージにルールが適用されます。 |
| ***host*** *target-IP* | （任意）ARP パケットの宛先 IP アドレスが *target-IP* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。***response*** キーワードを使用する場合にのみ、***host*** *target-IP* を指定できます。*target-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。 |
| *target-IP* *target-IP-mask* | （任意）パケットの宛先 IP アドレスが一致する可能性のある IPv4 アドレスおよび IPv4 アドレス セットのマスク。***response*** キーワードを使用する場合にのみ、*target-IP target-IP-mask* を指定できます。*target-IP* 引数と *target-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*target-IP-mask* 引数に 255.255.255.255 を指定することと、***host*** キーワードを使用することは同じです。 |
| ***host*** *target-MAC* | （任意）ARP パケットの宛先 MAC アドレスが *target-MAC* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。***response*** キーワードを使用する場合にのみ、***host*** *target-MAC* を指定できます。*target-MAC* 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。 |
| *target-MAC* *target-MAC-mask* | （任意）パケットの宛先 MAC アドレスが一致する可能性のある MAC アドレスおよび MAC アドレス セットのマスク。***response*** キーワードを使用する場合にのみ、*target-MAC target-MAC-mask* を指定できます。*target-MAC* 引数と *target-MAC-mask* 引数は、ドット付き 16 進表記で指定する必要があります。*target-MAC-mask* 引数に ffff.ffff.ffff を指定することと、***host*** キーワードを使用することは同じです。 |

**デフォルト**　なし

**コマンド モード**　ARP ACL コンフィギュレーション

**サポートされるユーザ ロール** network-admin
vdc-admin

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン** 新規に作成された ARP ACL にはルールが含まれません。

シーケンス番号を指定しない場合は、デバイスによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます

デバイスは、パケットに ARP ACL を適用する時点で、ACL 内のすべてのルールを使用してパケットを評価します。デバイスは、パケットに一致する条件を持つ最初のルールを実行します。複数のルールの条件が一致した場合、デバイスは最も低いシーケンス番号のルールを実行します。

***response*** キーワードまたは ***request*** キーワードのいずれかを指定しない場合は、ARP メッセージが含まれるパケットにルールが適用されます。

このコマンドにライセンスは必要ありません。

**例** 次に、arp-acl-01 という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始して、10.32.143.0 サブネットに存在する送信元 IP アドレスが含まれる ARP 要求メッセージを拒否するルールを追加する例を示します。

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# deny request ip 10.32.143.0 255.255.255.0 mac any
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **arp access-list** | ARP ACL を設定します。 |
| **ip arp inspection filter** | ARP ACL を VLAN に適用します。 |
| **permit（ARP）** | ARP ACL の許可ルールを設定します。 |
| **remark** | ACL でリマークを設定します。 |
| **show arp access-list** | すべてまたは 1 つの ARP ACL を表示します。 |

# deny（IPv4）

条件に一致するトラフィックを拒否する IPv4 ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

### 一般的な構文

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

**no deny** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

**no** *sequence-number*

### Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

### Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

### IP バージョン 4（IPv4）

[*sequence-number*] **deny ip** *source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

### Transmission Control Protocol（TCP）

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

### User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

**シンタックスの説明**

| | |
|---|---|
| *sequence-number* | （任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。ACL 内のルールの順序は、シーケンス番号によって維持されます。<br><br>シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。<br><br>ACL 内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。<br><br>シーケンス番号を指定しない場合は、デバイスによってそのルールが ACL の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。<br><br>ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。 |
| *protocol* | ルールが一致するパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードのとおりです。<br><br>• ***icmp*** **—** ルールが ICMP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数が使用可能です。<br>• ***igmp*** **—** ルールが IGMP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***igmp-type*** 引数が使用可能です。<br>• ***ip*** **—** ルールがすべての IPv4 トラフィックに適用されるように指定します。このキーワードを使用した場合は、すべての IPv4 プロトコルに適用されるその他のキーワードおよび引数のみが使用可能です。キーワードは次のとおりです。<br>　－ ***dscp***<br>　－ ***fragments***<br>　－ ***log***<br>　－ ***precedence***<br>　－ ***time-range***<br>• ***tcp*** **—** ルールが TCP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***flags*** 引数と ***operator*** 引数、および ***portgroup*** キーワードと ***established*** キーワードが使用可能です。<br>• ***udp*** **—** ルールが UDP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***operator*** 引数および ***portgroup*** キーワードが使用可能です。 |
| *source* | ルールが一致する送信元 IPv4 アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。 |
| *destination* | ルールが一致する宛先 IPv4 アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。 |

| | |
|---|---|
| ***dscp** dscp* | （任意）パケットの IP ヘッダーの DSCP フィールドの値が指定した 6 ビットの Differentiated Service（DiffServ; ディファレンシエーテッド サービス）値である場合にのみ、ルールがパケットに一致するように指定します。*dscp* 引数には、次の数値またはキーワードの 1 つを指定できます。<br>• 0 ～ 63 — DSCP フィールドの 6 ビットと等価の 10 進数。たとえば 10 を指定した場合、ルールは DSCP フィールドのビットが 001010 であるパケットのみに一致します。<br>• ***af11*** — Assured Forwarding（AF; 保証型転送）クラス 1、「低」の廃棄確率（001010）<br>• ***af12*** — AF クラス 1、「中」のドロップ率（001100）<br>• ***af13*** — AF クラス 1、「高」のドロップ率（001110）<br>• ***af21*** — AF クラス 2、「低」のドロップ率（010010）<br>• ***af22*** — AF クラス 2、「中」のドロップ率（010100）<br>• ***af23*** — AF クラス 2、「高」のドロップ率（010110）<br>• ***af31*** — AF クラス 3、「低」のドロップ率（011010）<br>• ***af32*** — AF クラス 3、「中」のドロップ率（011100）<br>• ***af33*** — AF クラス 3、「高」のドロップ率（011110）<br>• ***af41*** — AF クラス 4、「低」のドロップ率（100010）<br>• ***af42*** — AF クラス 4、「中」のドロップ率（100100）<br>• ***af43*** — AF クラス 4、「高」のドロップ率（100110）<br>• ***cs1*** — Class Selector（CS; クラスセレクタ）1、優先度 1（001000）<br>• ***cs2*** — CS2、優先度 2（010000）<br>• ***cs3*** — CS3、優先度 3（011000）<br>• ***cs4*** — CS4、優先度 4（100000）<br>• ***cs5*** — CS5、優先度 5（101000）<br>• ***cs6*** — CS6、優先度 6（110000）<br>• ***cs7*** — CS7、優先度 7（111000）<br>• ***default*** — デフォルト DSCP 値（000000）<br>• ***ef*** — Expedited Forwarding（EF; 緊急転送）（101110） |
| ***precedence** precedence* | （任意）パケットの IP precedence フィールドの値が *precedence* 引数で指定された値である場合にのみ、ルールがパケットに一致するように指定します。*precedence* 引数には、次の番号またはキーワードを指定できます。<br>• 0 ～ 7 — IP precedence フィールドの 3 ビットと等価の 10 進数。たとえば 3 を指定した場合、ルールは DSCP フィールドのビットが 011 であるパケットのみに一致します。<br>• ***critical*** — 優先度 5（101）<br>• ***flash*** — 優先度 3（011）<br>• ***flash-override*** — 優先度 4（100）<br>• ***immediate*** — 優先度 2（010）<br>• ***internet*** — 優先度 6（110）<br>• ***network*** — 優先度 7（111）<br>• ***priority*** — 優先度 1（001）<br>• ***routine*** — 優先度 0（000） |

| | |
|---|---|
| ***fragments*** | （任意）非初期フラグメントであるパケットにのみルールが一致するように指定します。デバイスがレイヤ 4 オプションを評価するために必要な情報は初期フラグメントのみに含まれているため、このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定するのと同じルールで指定することはできません。 |
| ***log*** | （任意）ルールに一致する各パケットについての情報ログ メッセージをデバイスが生成するように指定します。メッセージには、次の情報が含まれます。<br>• ACL 名<br>• パケットが許可されたか拒否されたか<br>• プロトコルが TCP、UDP、ICMP、または番号のいずれであったか<br>• 送信元および宛先アドレス。送信元および宛先ポート番号（該当する場合） |
| ***time-range*** *time-range-name* | （任意）このルールに適用される時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。*time-range-name* 引数には、最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。 |
| *icmp-message* | （ICMP のみ：任意）ルールが一致する ICMP メッセージ タイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」セクションの「ICMP メッセージ タイプ」に記載されているキーワードの 1 つを指定できます。 |
| *igmp-message* | （IGMP のみ：任意）ルールが一致する IGMP メッセージ タイプ。*igmp-message* 引数には、IGMP メッセージ番号（0 ～ 15 の整数）、または次のキーワードのいずれか 1 つを指定できます。<br>• ***dvmrp*** **—** Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル）<br>• ***host-query*** **—** ホスト クエリー<br>• ***host-report*** **—** ホスト レポート<br>• ***pim*** **—** PIM<br>• ***trace*** **—** マルチキャスト トレース |
| *operator port* [*port*] | （任意：TCP および UDP のみ）*operator* 引数および *port* 引数の条件に一致する送信元ポートまたは宛先ポートとの間で送受信されるパケットにのみルールが一致します。これらの引数が送信元ポートまたは宛先ポートのいずれに適用されるかは、*source* または *destination* のどちらの引数の後ろに指定したかにより決まります。<br>*port* 引数には、TCP または UDP ポートの名前または番号を指定できます。有効な番号は、0 ～ 65535 です。有効なポート名のリストについては、「使用上のガイドライン」セクションの「TCP ポート名」および「UDP ポート名」を参照してください。<br>2 番めの *port* 引数は、*operator* 引数が範囲の場合にのみ必要になります。<br>*operator* 引数には、次のキーワードのいずれか 1 つを指定する必要があります。<br>• ***eq*** **—** パケットのポートが *port* 引数の値と同じ場合にのみ一致します。<br>• ***gt*** **—** パケットのポートが *port* 引数の値より大きい場合にのみ一致します。<br>• ***lt*** **—** パケットのポートが *port* 引数の値より小さい場合にのみ一致します。<br>• ***neq*** **—** パケットのポートが *port* 引数の値と同じでない場合にのみ一致します。<br>• ***range*** **—** 2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数の値以上で、2 番めの *port* 引数の値以下である場合にのみ一致します。 |

| | |
|---|---|
| ***portgroup*** *portgroup* | （任意：TCP および UDP のみ）*portgroup* 引数によって指定される IP ポート オブジェクト グループのメンバーである送信元ポートまたは宛先ポートとの間でパケットが送受信される場合にのみ、ルールがパケットに一致するように指定します。portgroup 引数には、64 文字の英数字を使用でき、大文字と小文字が区別されます。IP ポート オブジェクト グループが送信元ポートまたは宛先ポートのいずれに適用されるかは、*source* または *destination* のどちらの引数の後ろに指定したかにより決まります。<br><br>IP ポート オブジェクト グループを作成または変更するには、**object-group ip port** コマンドを使用します。 |
| *flags* | （TCP のみ：任意）ルールが一致する TCP 制御ビット フラグ。*flags* 引数の値には、次のキーワードの 1 つ以上を指定する必要があります。<br><br>• ***ack***<br>• ***fin***<br>• ***psh***<br>• ***rst***<br>• ***syn***<br>• ***urg*** |
| ***established*** | （TCP のみ：任意）確立された TCP 接続に属するパケットのみにルールが一致するように指定します。デバイスは、ACK または RST ビットを持つ TCP パケットは、確立された接続に属するものとみなします。 |

## デフォルト

新規に作成された IPv4 ACL にはルールが含まれません。

シーケンス番号を指定しない場合は、デバイスによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます。

## コマンド モード

IPv4 ACL コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

デバイスは、パケットに IPv4 ACL を適用する時点で、ACL 内のすべてのルールを使用してパケットを評価します。デバイスは、パケットに一致する条件を持つ最初のルールを実行します。複数のルールの条件が一致した場合、デバイスは最も低いシーケンス番号のルールを実行します。

このコマンドにライセンスは必要ありません。

### 送信元および宛先

*source* 引数および *destination* 引数は、複数の方法のいずれか 1 つによって指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールを設定する場合には、次の方法を使って *source* 引数および *destination* 引数を指定します。

- IP アドレス グループ オブジェクト — IPv4 アドレス グループ オブジェクトを使用して、*source* 引数または *destination* 引数を指定できます。IPv4 アドレス グループ オブジェクトを作成または変更するには、**object-group ip address** コマンドを使用します。構文は、次のとおりです。

  ***addrgroup*** *address-group-name*

  次に、lab-gateway-svrs という名前の IPv4 アドレス グループ オブジェクトを使用して *destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
  ```

- アドレスおよびネットワーク ワイルドカード — IPv4 アドレスおよびその後ろに続けてネットワーク ワイルドカードを使用することで、ホストまたはネットワークを送信元または宛先として指定できます。構文は、次のとおりです。

  *IPv4-address network-wildcard*

  次に、192.168.67.0 サブネットの IPv4 アドレスおよびネットワーク ワイルドカードを使用して *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）— IPv4 アドレスおよびその後ろに続けて VLSM を使用することで、ホストまたはネットワークを送信元または宛先として指定できます。構文は、次のとおりです。

  *IPv4-address/prefix-len*

  次に、192.168.67.0 サブネットの IPv4 アドレスおよび VLSM を使用して *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny udp 192.168.67.0/24 any
  ```

- ホスト アドレス — ***host*** キーワードおよび IPv4 アドレスを使用して、ホストを送信元または宛先として指定できます。構文は、次のとおりです。

  ***host*** *IPv4-address*

  この構文は、*IPv4-address*/32 および *IPv4-address* 0.0.0.0 と等価です。

  次に、***host*** キーワードおよび 192.168.67.132 IPv4 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny icmp host 192.168.67.132 any
  ```

- 任意のアドレス — ***any*** キーワードを使用して、送信元または宛先が任意の IPv4 アドレスとなるように指定できます。***any*** キーワードを使用した例については、このセクションの例を参照してください。それぞれの例には、***any*** キーワードを使用して送信元または宛先を指定する方法が示されています。

### ICMP メッセージ タイプ

*icmp-message* 引数には、ICMP メッセージ番号（0 ～ 255 の整数）、または次のキーワードのいずれか 1 つを指定できます。

- ***administratively-prohibited*** — 管理上の禁止
- ***alternate-address*** — 代替アドレス
- ***conversion-error*** — データグラム変換
- ***dod-host-prohibited*** — ホストの拒否
- ***dod-net-prohibited*** — ネットワークの拒否
- ***echo*** — エコー（PING）
- ***echo-reply*** — エコー応答
- ***general-parameter-problem*** — パラメータの問題

- ***host-isolated*** — 分離されているホスト
- ***host-precedence-unreachable*** — 優先度が Host Unreachable
- ***host-redirect*** — ホストへのリダイレクト
- ***host-tos-redirect*** — ToS ベースでのホストへのリダイレクト
- ***host-tos-unreachable*** — ToS ベースでホストに到達不能
- ***host-unknown*** — 未知のホスト
- ***host-unreachable*** — ホストに到達不能
- ***information-reply*** — 応答についての情報
- ***information-request*** — 要求についての情報
- ***mask-reply*** — マスクの応答
- ***mask-request*** — マスクの要求
- ***mobile-redirect*** — モバイル ホストへのリダイレクト
- ***net-redirect*** — ネットワークへのリダイレクト
- ***net-tos-redirect*** — ToS ベースでのネットワークへのリダイレクト
- ***net-tos-unreachable*** — ToS ベースでネットワークに到達不能
- ***net-unreachable*** — ネットワークに到達不能
- ***network-unknown*** — 未知のネットワーク
- ***no-room-for-option*** — パラメータが必須であるが指定する余地がない
- ***option-missing*** — パラメータが必須であるが存在しない
- ***packet-too-big*** — フラグメンテーションが必要だが DF が設定されている
- ***parameter-problem*** — すべてのパラメータの問題
- ***port-unreachable*** — ポートに到達不能
- ***precedence-unreachable*** — 優先順位が使用できない
- ***protocol-unreachable*** — プロトコルに到達不能
- ***reassembly-timeout*** — 再構成時のタイムアウト
- ***redirect*** — すべてリダイレクト
- ***router-advertisement*** — ルータ ディスカバリのためのアドバタイズメント
- ***router-solicitation*** — ルータ ディスカバリのためのソリシテーション
- ***source-quench*** — ソース クエンチ
- ***source-route-failed*** — 送信元ルートの障害
- ***time-exceeded*** — すべての時間超過メッセージ
- ***timestamp-reply*** — タイム スタンプ付きの応答
- ***timestamp-request*** — タイム スタンプ付きの要求
- ***traceroute*** — トレースルート
- ***ttl-exceeded*** — Time-To-Live（TTL; 存続可能時間）を超過
- ***unreachable*** — すべて到達不能

### TCP ポート名

*protocol* 引数に ***tcp*** を指定した場合は、*port* 引数に TCP ポート番号（0 ～ 65535 の整数）または次のキーワードのいずれか 1 つを指定できます。

***bgp*** — Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）

***chargen*** — Character Generator（19）

***cmd*** — リモートコマンド（rcmd、514）

***daytime* —** 日付と時刻（13）

***discard* —** 廃棄（9）

***domain* —** ドメイン ネーム サービス（53）

***drip* —** ダイナミック RIP（3949）

***echo* —** エコー（7）

***exec* —** EXEC（rsh、512）

***finger* —** Finger（79）

***ftp* —** Fingerile Transfer Protocol（FTP; ファイル転送プロトコル）（21）

***ftp-data* —** FTP データ接続（2）

***gopher* —** Gopher（7）

***hostname* —** NIC ホストネーム サーバ（11）

***ident* —** Ident プロトコル（113）

***irc* —** Internet Relay Chat（IRC; インターネット リレー チャット）（194）

***klogin* —** Kerberos ログイン（543）

***kshell* —** Kerberos シェル（544）

***login* —** ログイン（rlogin、513）

***lpd* —** プリンタ サービス（515）

***nntp* —** Network News Transport Protocol（NNTP）（119）

***pim-auto-rp* —** PIM Auto-RP（496）

***pop2* —** POP v2（19）

***pop3* —** POP v3（11）

***smtp* —** Simple Mail Transport Protocol（SMTP）（25）

***sunrpc* —** Sun Remote Procedure Call（SunRPC）（111）

***tacacs* —** TAC Access Control System（TACACS）（49）

***talk* —** Talk（517）

***telnet* —** Telnet（23）

***time* —** Time（37）

***uucp* —** UNIX-to-UNIX Copy Program（54）

***whois* —** WHOIS/NICNAME（43）

***www* —** World Wide Web（HTTP、8）

### UDP ポート名

*protocol* 引数に ***udp*** を指定した場合は、*port* 引数に UDP ポート番号（0 ～ 65535 の整数）または次のキーワードのいずれか 1 つを指定できます。

***biff* —** biff（メール通知、comsat、512）

***bootpc* —** Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）

***bootps*** **—** BOOTP サーバ（67）

***discard*** **—** 廃棄（9）

***dnsix*** **—** DNSIX セキュリティ プロトコル監査（195）

***domain*** **—** ドメイン ネーム サービス（DNS、53）

***echo*** **—** エコー（7）

***isakmp*** **—** Internet Security Association and Key Management Protocol（ISAKMP）（5）

***mobile-ip*** **—** Mobile IP 登録（434）

***nameserver*** **—** IEN116 ネームサービス（廃止、42）

***netbios-dgm*** **—** NetBIOS データグラム サービス（138）

***netbios-ns*** **—** NetBIOS ネーム サービス（137）

***netbios-ss*** **—** NetBIOS セッション サービス（139）

***non500-isakmp*** **—** Internet Security Association and Key Management Protocol（ISAKMP）（45）

***ntp*** **—** Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）

***pim-auto-rp*** **—** PIM Auto-RP（496）

***rip*** **—** RIP（ルータ、in.routed、52）

***snmp*** **—** Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）

***snmptrap*** **—** SNMP トラップ（162）

***sunrpc*** **—** Sun Remote Procedure Call（SunRPC）（111）

***syslog*** **—** システム ロガー（514）

***tacacs*** **—** TAC Access Control System（TACACS）（49）

***talk*** **—** Talk（517）

***tftp*** **—** TFTP（69）

***time*** **—** Time（37）

***who*** **—** who サービス（rwho、513）

***xdmcp*** **—** X DMCP（177）

## 例

次に、10.23.0.0 ～ 10.176.0.0 および 192.168.37.0 ～ 10.176.0.0 ネットワークのすべての TCP と UDP のトラフィックを拒否するルール、およびその他のすべての IPv4 トラフィックを許可する最後のルールを持つ、acl-lab-01 という名前の IPv4 ACL を設定する例を示します。

```
switch# config t
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

次に、eng_workstations という名前の IPv4 アドレス オブジェクト グループから marketing_group という名前の IP アドレス オブジェクト グループまでのすべての IP トラフィックを拒否するルールの後に、その他のすべての IPv4 トラフィックを許可するルールが続く、acl-eng-to-marketing という名前の IPv4 ACL を設定する例を示します。

```
switch# config t
switch(config)# ip access-list acl-eng-to-marketing
switch(config-acl)# deny ip addrgroup eng_workstations addrgroup marketing_group
switch(config-acl)# permit ip any any
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ip access-list** | IPv4 ACL を設定します。 |
| **object-group ip address** | IPv4 アドレス オブジェクト グループを設定します。 |
| **object-group ip port** | IP ポート オブジェクト グループを設定します。 |
| **permit（IPv4）** | IPv4 ACL の許可ルールを設定します。 |
| **remark** | IPv4 ACL でリマークを設定します。 |
| **show ip access-list** | すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。 |
| **statistics per-entry** | ACL の各エントリの統計情報の収集をイネーブルにします。 |
| **time-range** | 時間範囲を設定します。 |

# deny（MAC）

条件に一致するトラフィックを拒否する MAC Access Control List（ACL; アクセス コントロール リスト）+ ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

**no deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

**no** *sequence-number*

## シンタックスの説明

| | |
|---|---|
| *sequence-number* | （任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。ACL 内のルールの順序は、シーケンス番号によって維持されます。<br><br>シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。<br><br>ACL 内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。<br><br>シーケンス番号を指定しない場合は、デバイスによってそのルールが ACL の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。<br><br>ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。 |
| *source* | ルールが一致する送信元 MAC アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。 |
| *destination* | ルールが一致する宛先 MAC アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。 |
| *protocol* | （任意）ルールが一致するプロトコル番号。有効なプロトコル番号は、0x0 ～ 0xffff です。有効なプロトコル名のリストについては、「使用上のガイドライン」セクションの「MAC プロトコル」を参照してください。 |
| ***cos** cos-value* | （任意）*cos-value* 引数に指定された Class of Service（CoS; サービス クラス）値がパケットの IEEE 802.1Q ヘッダーに含まれる場合にのみ、ルールがパケットに一致するように指定します。*cos-value* 引数には、0 ～ 7 の整数を指定できます。 |
| ***vlan** VLAN-ID* | （任意）指定された VLAN ID がパケットの IEEE 802.1Q ヘッダーに含まれる場合にのみ、ルールがパケットに一致するように指定します。*VLAN-ID* 引数には、1 ～ 4094 の整数を指定できます。 |

## デフォルト

新規に作成された MAC ACL にはルールが含まれません。

シーケンス番号を指定しない場合は、デバイスによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます。

## コマンド モード

MAC ACL コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン**

デバイスは、パケットに MAC ACL を適用する時点で、ACL 内のすべてのルールを使用してパケットを評価します。デバイスは、パケットに一致する条件を持つ最初のルールを実行します。複数のルールの条件が一致した場合、デバイスは最も低いシーケンス番号のルールを実行します。

このコマンドにライセンスは必要ありません。

### 送信元および宛先

*source* 引数および *destination* 引数は、2 つの方法のうちのいずれかによって指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールを設定する場合には、次の方法を使って *source* 引数および *destination* 引数を指定します。

- アドレスおよびマスク — MAC アドレスおよびその後ろにマスクを続けて使用して、1 つのアドレスまたはアドレス グループを指定できます。構文は、次のとおりです。

  *MAC-address MAC-mask*

  次に、MAC アドレス 00c0.4f03.0a72 で *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、MAC ベンダー コードが 00603e のすべてのホストに対応する MAC アドレスで *destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス — ***any*** キーワードを使用して、送信元または宛先が任意の MAC アドレスとなるように指定できます。***any*** キーワードを使用した例については、このセクションの例を参照してください。それぞれの例には、***any*** キーワードを使用して送信元または宛先を指定する方法が示されています。

### MAC プロトコル

*protocol* 引数には、MAC プロトコル番号またはキーワードを指定できます。プロトコル番号は、0x というプレフィクスを持つ 4 バイトの 16 進数です。有効なプロトコル番号は、0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- ***aarp*** — AppleTalk ARP（0x80f3）
- ***appletalk*** — AppleTalk（0x809b）
- ***decnet-iv*** — DECnet Phase IV（0x6003）
- ***diagnostic*** — DEC Diagnostic Protocol（0x6005）
- ***etype-6000*** — EtherType 0x6000（0x6000）
- ***etype-8042*** — EtherType 0x8042（0x8042）
- ***ip*** — IPv4（0x0800）
- ***lat*** — DEC LAT（0x6004）
- ***lavc-sca*** — DEC LAVC、SCA（0x6007）
- ***mop-console*** — DEC MOP Remote Console（0x6002）
- ***mop-dump*** — DEC MOP Dump（0x6001）
- ***vines-echo*** — VINES Echo（0x0baf）

## 例

次に、2 つの MAC アドレス グループ間で非 IPv4 トラフィックを許可するルールが含まれる mac-ip-filter という名前の MAC ACL を設定する例を示します。

```
switch# config t
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000
0000.00ff.ffff ip
switch(config-mac-acl)# permit any any
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **mac access-list** | MAC ACL を設定します。 |
| **permit（MAC）** | MAC ACL で拒否ルールを設定します。 |
| **remark** | ACL でリマークを設定します。 |
| **show mac access-list** | すべてまたは 1 つの MAC ACL を表示します。 |
| **statistics per-entry** | ACL の各エントリの統計情報の収集をイネーブルにします。 |

# deny（ロールベース ACL）

SGACL（セキュリティ グループ アクセス コントロール リスト）で拒否アクションを設定するには、**deny** コマンドを使用します。アクションを削除するには、このコマンドの **no** 形式を使用します。

**deny** {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dest**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]}

**no deny** {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dest**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]}

## シンタックスの説明

| | |
|---|---|
| **all** | すべてのトラフィックを指定します。 |
| **icmp** | ICMP トラフィックを指定します。 |
| **igmp** | IGMP トラフィックを指定します。 |
| **ip** | IP トラフィックを指定します。 |
| **tcp** | TCP トラフィックを指定します。 |
| **udp** | UDP トラフィックを指定します。 |
| **src** | 送信元ポート番号を指定します。 |
| **dest** | 宛先ポート番号を指定します。 |
| **eq** | 指定した値と同じポート番号を指定します。 |
| **gt** | 指定した値より大きいポート番号を指定します。 |
| **lt** | 指定した値より小さいポート番号を指定します。 |
| **neq** | 指定した値以外のすべてのポート番号を指定します。 |
| *port-number* | TCP または UDP のポート番号。有効範囲は 0 ～ 65535 です。 |
| **range** | TCP または UDP のポート範囲を指定します。 |
| *port-number1* | 範囲内の最初のポート。有効範囲は 0 ～ 65535 です。 |
| *port-number2* | 範囲内の最後のポート。有効範囲は 0 ～ 65535 です。 |

## デフォルト

なし

## コマンド モード

ロールベース ACL

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

## 例

次に、SGACL に拒否アクションを追加する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp
```

次に、SGACL から拒否アクションを削除する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **cts role-based access-list** | Cisco TrustSec SGACL を設定します。 |
| **feature cts** | Cisco TrustSec 機能をイネーブルにします。 |
| **show cts role-based access-list** | Cisco TrustSec SGACL 設定を表示します。 |

# description（アイデンティティ ポリシー）

アイデンティティ ポリシーの説明を設定するには、**description** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**description "***text***"**

**no description**

## シンタックスの説明

| | |
|---|---|
| "*text*" | アイデンティティ ポリシーについて説明するテキスト ストリング。ストリングには、英数字を使用します。最大 100 文字まで可能です。 |

## デフォルト

なし

## コマンド モード

アイデンティティ ポリシー コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドにライセンスは必要ありません。

## 例

次に、アイデンティティ ポリシーの説明を設定する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# description "Administrator identity policy"
```

次に、アイデンティティ ポリシーから説明を削除する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no description
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **identity policy** | アイデンティティ ポリシーを設定または指定し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。 |
| **show identity policy** | アイデンティティ ポリシー情報を表示します。 |

# description（ユーザ ロール）

ユーザ ロールの説明を設定するには、**description** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**description** *text*

**no description**

## シンタックスの説明

| | |
|---|---|
| *text* | ユーザ ロールについて説明するテキスト ストリング。ストリングには、英数字を使用します。最大 128 文字まで可能です。 |

## デフォルト

なし

## コマンド モード

ユーザ ロール コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

ユーザ ロールの説明テキストには、空白スペースを使用できます。

このコマンドにライセンスは必要ありません。

## 例

次に、ユーザ ロールの説明を設定する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

次に、ユーザ ロールから説明を削除する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no description
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **role name** | ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。 |
| **show role** | ユーザ ロール情報を表示します。 |

# device

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アイデンティティ プロファイルの例外リストにサプリカント デバイスを追加するには、**device** コマンドを使用します。サプリカント デバイスを削除するには、このコマンドの **no** 形式を使用します。

**device** {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*] | **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

**no device** {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*] | **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

## シンタックスの説明

| | |
|---|---|
| **authenticate** | ポリシーを使用するデバイス認証を許可するように指定します。 |
| **not-authenticate** | ポリシーを使用するデバイス認証を許可しないように指定します。 |
| **ip-address** *ipv4-address* | サプリカント デバイスの IPv4 アドレスを A.B.C.D 形式で指定します。 |
| *subnet-mask* | （任意）IPv4 アドレスの IPv4 サブネット マスク |
| **mac-address** *mac-address* | サプリカント デバイスの MAC アドレスを XXXX.XXXX.XXXX 形式で指定します。 |
| *mac-address-mask* | （任意）MAC アドレスのマスク |
| **policy** *policy-name* | サプリカント デバイスに使用するポリシーを指定します。 |

## デフォルト

なし

## コマンド モード

アイデンティティ ポリシー コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドにライセンスは必要ありません。

## 例

次に、EAPoUDP アイデンティティ プロファイルにデバイスを追加する例を示します。

```
switch# config t
switch(config)# identity profile eapoupd
switch(config-id-policy)# device authenticate 10.10.1.1 255.255.255.245 policy
AdminPolicy
```

次に、EAPoUDP アイデンティティ プロファイルからデバイスを削除する例を示します。

```
switch# config t
switch(config)# identity profile eapoupd
switch(config-id-policy)# no device authenticate 10.10.2.2 255.255.255.245 policy
UserPolicy
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **identity policy** | アイデンティティ ポリシーを設定または指定し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。 |
| **show identity policy** | アイデンティティ ポリシー情報を表示します。 |

# dot1x default

802.1X グローバル設定またはインターフェイス設定をデフォルトにリセットするには、**dot1x default** コマンドを使用します。

**dot1x default**

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** なし

**コマンド モード** グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

**サポートされるユーザ ロール** network-admin
vdc-admin

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン** 802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

**例** 次に、グローバル 802.1X パラメータをデフォルトに設定する例を示します。

```
switch# config t
switch(config)# dot1x default
```

次に、インターフェイス 802.1X パラメータをデフォルトに設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x default
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x** | 802.1X 機能ステータス情報を表示します。 |

# dot1x host-mode

インターフェイス上の 1 つまたは複数のサプリカントの 802.1X 認証を許可するには、**dot1x host-mode** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x host-mode** {**multi-host** | **single-host**}

**no dot1x host-mode**

## シンタックスの説明

| | |
|---|---|
| ***mutli-host*** | インターフェイス上の複数のサプリカントの 802.1X 認証を許可します。 |
| ***single-host*** | インターフェイス上の 1 つだけのサプリカントの 802.1X 認証を許可します。 |

## デフォルト

***single-host***

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、インターフェイス上の複数のサプリカントの 802.1X 認証を許可する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x host-mode multi-host
```

次に、インターフェイス上でデフォルトのホスト モードに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x host-mode
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x initialize

サプリカントの 802.1X 認証を初期化するには、**dot1x initialize** コマンドを使用します。

**dot1x initialize** [**interface ethernet** *slot/port*]

**シンタックスの説明**

| | |
|---|---|
| ***interface ethernet*** *slot/port* | （任意）802.1X 認証初期化のインターフェイスを指定します。 |

**デフォルト**

なし

**コマンド モード**

任意のコマンド モード

**サポートされるユーザ ロール**

network-admin
vdc-admin

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン**

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

**例**

NX-OS デバイス上でサプリカントの 802.1X 認証を初期化する例を示します。

```
switch# dot1x initialize
```

次に、インターフェイス上でサプリカントの 802.1X 認証を初期化する例を示します。

```
switch# dot1x initialize interface ethernet 2/1
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x mac-auth-bypass

802.1X サプリカントがないインターフェイス上で MAC アドレス認証バイパスをイネーブルにするには、**dot1x mac-auth-bypass** コマンドを使用します。MAC アドレス認証バイパ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。

**dot1x mac-auth-bypass** [**eap**]

**no dot1x mac-auth-bypass**

## シンタックスの説明

| | |
|---|---|
| **eap** | バイパスで Extensible Authentication Protocol（EAP）を使用するように指定します。 |

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、MAC アドレス認証バイパスをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x mac-auth-bypass
```

次に、MAC アドレス認証バイパスをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x mac-auth-bypass
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x max-reauth-req

セッションがタイムアウトになるまでに NX-OS デバイスがインターフェイス上のサプリカントに再認証要求を再送信する最大回数を変更するには、**dot1x max-reauth-req** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x max-reauth-req** *retry-count*

**no dot1x max-reauth-req**

## シンタックスの説明

| | |
|---|---|
| *retry-count* | 再認証要求リトライ回数。有効範囲は 1 ～ 10 回です。 |

## デフォルト

リトライ 2 回

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、インターフェイスの最大再許可要求リトライ回数を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-reauth-req 3
```

次に、インターフェイスの最大再許可要求リトライ回数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-reauth-req
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x max-req

802.1X 認証が再開するまでに NX-OS デバイスがサプリカントに送信する最大要求回数を変更するには、**dot1x max-req** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x max-req** *retry-count*

**no dot1x max-req**

## シンタックスの説明

| | |
|---|---|
| *retry-count* | 802.1X 再認証が再開するまでにサプリカントに送信する要求リトライ回数。有効範囲は 1 ～ 10 回です。 |

## デフォルト

グローバル コンフィギュレーション：リトライ 2 回

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

## コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、グローバル 802.1X コンフィギュレーションの最大要求リトライ回数を変更する例を示します。

```
switch# config t
switch(config)# dot1x max-req 3
```

次に、グローバル 802.1X コンフィギュレーションの最大要求リトライ回数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no dot1x max-req
```

次に、インターフェイスの最大要求リトライ回数を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-req 4
```

次に、インターフェイスの最大要求リトライ回数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-req
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x port-control

インターフェイス上で実行される 802.1X 認証を制御するには、**dot1x port-control** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}

**no dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}

## シンタックスの説明

| | |
|---|---|
| ***auto*** | インターフェイス上で 802.1X 認証をイネーブルにします。 |
| ***force-authorized*** | インターフェイス上で 802.1X 認証をディセーブルにして、認証なしでインターフェイス上のすべてのトラフィックを許可します。 |
| ***force-unauthorized*** | インターフェイス上ですべての認証をディセーブルにします。 |

## デフォルト

***force-authorized***

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、インターフェイス上で実行される 802.1X 認証処理を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

次に、インターフェイス上で実行される 802.1X 認証処理の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x interface ethernet** | インターフェイスの 802.1X 情報を表示します。 |

# dot1x radius-accounting

802.1X の RADIUS アカウンティングをイネーブルにするには、**dot1x radius-accounting** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x radius-accounting**

**no dot1x radius-accounting**

## シンタックスの説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、802.1X 認証の RADIUS アカウンティングをイネーブルにする例を示します。

```
switch# config t
switch(config)# dot1x radius-accounting
```

次に、802.1X 認証の RADIUS アカウンティングをディセーブルにする例を示します。

```
switch# config t
switch(config)# no dot1x radius-accounting
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show running-config dot1x all** | 実行コンフィギュレーションですべての 802.1X 情報を表示します。 |

# dot1x re-authentication（EXEC）

802.1X サプリカントを手動で再認証するには、**dot1x re-authentication** コマンドを使用します。

**dot1x re-authentication** [**interface ethernet** *slot*/*port*]

## シンタックスの説明

| | |
|---|---|
| ***interface ethernet*** *slot*/*port* | （任意）手動再認証のインターフェイスを指定します。 |

## デフォルト

なし

## コマンド モード

EXEC モード

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、802.1X サプリカントを手動で再認証する例を示します。

```
switch# dot1x re-authentication
```

次に、インターフェイス上の 802.1X サプリカントを手動で再認証する例を示します。

```
switch# dot1x re-authentication interface ethernet 2/1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x re-authentication（グローバル コンフィギュレーション、インターフェイス コンフィギュレーション）

802.1X サプリカントの定期的な再認証をイネーブルにするには、**dot1x re-authentication** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x re-authentication**

**no dot1x re-authentication**

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** グローバル コンフィギュレーション：ディセーブル

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

**コマンド モード** グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

**サポートされるユーザ ロール** network-admin
vdc-admin

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン** 802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドをグローバル コンフィギュレーション モードで使用すると、NX-OS デバイス上のすべてのサプリカントの定期的な再認証が設定されます。このコマンドをインターフェイス コンフィギュレーション モードで使用すると、インターフェイス上のサプリカントのみの定期的な再認証が設定されます。

このコマンドにライセンスは必要ありません。

**例** 次に、802.1X サプリカントの定期的な再認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# dot1x re-authentication
```

次に、802.1X サプリカントの定期的な再認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no dot1x re-authentication
```

次に、インターフェイス上の 802.1X サプリカントの定期的な再認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x re-authentication
```

次に、インターフェイス上の 802.1X サプリカントの定期的な再認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x re-authentication
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x system-auth-control

802.1X 認証をイネーブルにするには、**dot1x system-auth-control** コマンドを使用します。802.1X 認証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。

**dot1x system-auth-control**

**no dot1x system-auth-control**

## シンタックスの説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンド モード

グローバル コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | 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 system-auth-control** コマンドにより 802.1X 設定は削除されません。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

## 例

次に、802.1X 認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no dot1x system-auth-control
```

次に、802.1X 認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# dot1x system-auth-control
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x** | 802.1X 機能ステータス情報を表示します。 |

# dot1x timeout quiet-period

802.1X 待機時間タイムアウトをグローバルに、またはインターフェイス単位で設定するには、**dot1x timeout quiet-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

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

**no dot1x timeout quiet-period**

## シンタックスの説明

| | |
|---|---|
| *seconds* | 802.1X 待機時間タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。 |

## デフォルト

グローバル コンフィギュレーション：60 秒

インターフェイス コンフィギュレーション：グローバル コンフィギュレーションの値

## コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X 待機時間タイムアウトは、サプリカントとの認証の交換に失敗した後で、デバイスが待機状態にとどまる秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

**（注）** 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

## 例

次に、グローバル 802.1X 待機時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# dot1x timeout quiet-period 45
```

次に、グローバル 802.1X 待機時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no dot1x timeout quiet-period
```

次に、インターフェイスの 802.1X 待機時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout quiet-period 50
```

次に、インターフェイスの 802.1X 待機時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout quiet-period
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x timeout ratelimit-period

インターフェイス上のサプリカントの 802.1X レート制限時間タイムアウトを設定するには、**dot1x timeout ratelimit-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x timeout ratelimit-period** *seconds*

**no dot1x timeout ratelimit-period**

## シンタックスの説明

| | |
|---|---|
| *seconds* | 802.1X レート制限時間タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。 |

## デフォルト

0 秒

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X レート制限タイムアウト時間は、オーセンティケータが、正常に認証されたサプリカントの EAPOL-Start パケットを無視する秒数です。この値は、グローバル待機時間タイムアウトを上書きします。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

## 例

次に、インターフェイスの 802.1X レート制限時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

次に、インターフェイスの 802.1X レート制限時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x interface ethernet** | インターフェイスの 802.1X 情報を表示します。 |

# dot1x timeout re-authperiod

802.1X 再認証時間タイムアウトをグローバルに、またはインターフェイス単位で設定するには、**dot1x timeout re-authperiod** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x timeout re-authperiod** *seconds*

**no dot1x timeout re-authperiod**

## シンタックスの説明

| | |
|---|---|
| *seconds* | 802.1X 再認証時間タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。 |

## デフォルト

グローバル コンフィギュレーション：3600 秒

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

## コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X 再認証タイムアウト時間は、再認証の試行間の秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

## 例

次に、グローバル 802.1X 再認証時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# dot1x timeout re-authperiod 3000
```

次に、インターフェイスの 802.1X 再認証時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout re-authperiod 3300
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |

# dot1x timeout server-timeout

インターフェイスの 802.1X サーバ タイムアウトを設定するには、**dot1x timeout server-timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

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

**no dot1x timeout server-timeout**

## シンタックスの説明

| | |
|---|---|
| *seconds* | 802.1X サーバ タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。 |

## デフォルト

30 秒

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

インターフェイスの 802.1X サーバ タイムアウトは、認証サーバにパケットを再送信するまでに NX-OS デバイスが待機する秒数です。この値は、グローバル再認証時間タイムアウトを上書きします。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

**（注）** 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

## 例

次に、グローバル 802.1X サーバ タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

次に、グローバル 802.1X サーバ タイムアウト間隔の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x interface ethernet** | インターフェイスの 802.1X 情報を表示します。 |

# dot1x timeout supp-timeout

インターフェイスの 802.1X サプリカント タイムアウトを設定するには、**dot1x timeout supp-timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

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

**no dot1x timeout supp-timeout**

## シンタックスの説明

| | |
|---|---|
| *seconds* | 802.1X サプリカント タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。 |

## デフォルト

30 秒

## 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

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

インターフェイスの 802.1X サプリカント タイムアウトは、NX-OS デバイスがフレームを再送信するまでに、サプリカントが EAP 要求フレームに応答するのを NX-OS デバイスが待機する秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

**（注）** 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

## 例

次に、インターフェイスの 802.1X サーバ タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout supp-timeout 45
```

次に、インターフェイスの 802.1X サーバ タイムアウト間隔の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x timeout supp-timeout
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x interface ethernet** | インターフェイスの 802.1X 情報を表示します。 |

# dot1x timeout tx-period

802.1X 送信時間タイムアウトをグローバルに、またはインターフェイス単位で設定するには、**dot1x timeout tx-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

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

**no dot1x timeout tx-period**

## シンタックスの説明

| | |
|---|---|
| *seconds* | 802.1X 送信時間タイムアウトの秒数を指定します。有効範囲は 1 ～ 65535 秒です。 |

## デフォルト

グローバル コンフィギュレーション：60 秒

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

## コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

## サポートされるユーザ ロール

network-admin
vdc-admin

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 4.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

802.1X 送信タイムアウト時間は、要求を再送信するまでに、NX-OS デバイスがサプリカントからの EAP 要求 / アイデンティティ フレームへの応答を待機する秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

**（注）** 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

## 例

次に、グローバル 802.1X 送信時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# dot1x timeout tx-period 45
```

次に、グローバル 802.1X 送信時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no dot1x timeout tx-period
```

次に、インターフェイスの 802.1X 送信時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout tx-period 45
```

次に、インターフェイスの 802.1X 送信時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout tx-period
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **feature dot1x** | 802.1X 機能をイネーブルにします。 |
| **show dot1x all** | すべての 802.1X 情報を表示します。 |