

ポート認証

概要・基本設定	2
概要	2
802.1X 認証方式	3
基本設定	3
Authenticator	3
Authenticator (ダイナミック VLAN)	4
Supplicant	6
認証サーバー	6
Supplicant MAC 透過機能	7
コマンドリファレンス編	8
機能別コマンド索引	8
ADD PORTAUTH PORT SUPPLICANTMAC	9
DELETE PORTAUTH PORT SUPPLICANTMAC	11
DISABLE PORTAUTH	12
ENABLE PORTAUTH	13
SET PORTAUTH AUTHMETHOD	14
SET PORTAUTH PORT	15
SET PORTAUTH PORT SUPPLICANTMAC	19
SHOW PORTAUTH	21
SHOW PORTAUTH PORT AUTHENTICATOR	24
SHOW PORTAUTH PORT SUPPLICANT	28

概要・基本設定

本製品は、スイッチポート単位で LAN 上のユーザーや機器を認証するポート認証機能を実装しています。ポートに接続された機器（および機器を使用するユーザー。以下同様）の認証方法としては、次の方式をサポートしています。

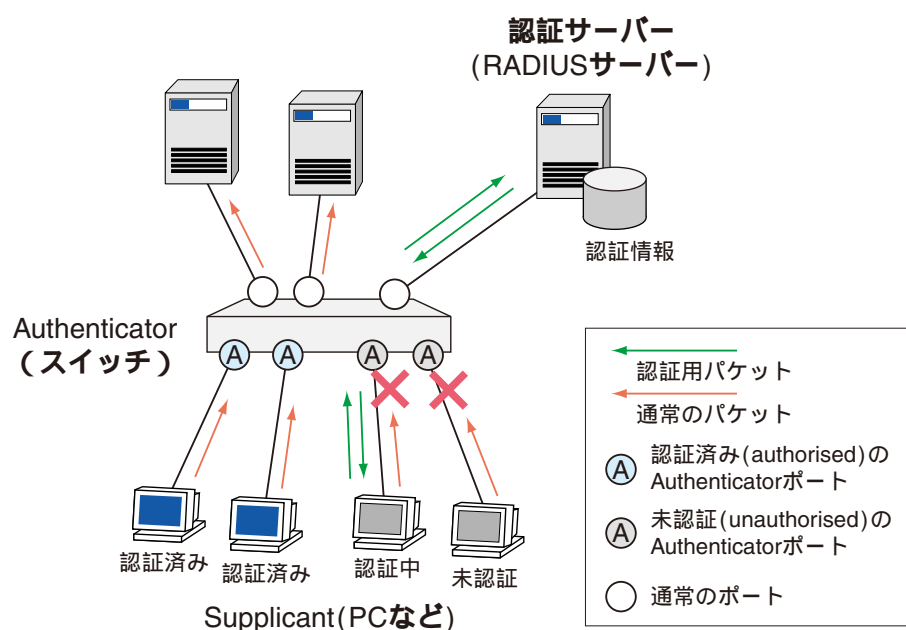
- IEEE 802.1X 認証（以下、802.1X 認証）

802.1X 認証は、EAP（Extensible Authentication Protocol）というプロトコルを使って、ユーザー単位で認証を行うしくみです。802.1X 認証を利用するには、認証する側と認証される側の両方が 802.1X に対応している必要があります。

ポート認証機能を使用すれば、スイッチポートに接続された機器を認証し、認証に成功したときだけ同機器からの通信、および、同機器への通信を許可するよう設定できます。また、認証に成功した機器を特定の VLAN にアサインすることも可能です（ダイナミック VLAN）。さらに、本製品は Supplicant 機能にも対応しているため、他の機器から認証を受けるよう設定することもできます。

概要

ポート認証のシステムは、下記の 3 要素から成り立っています。



- Authenticator（認証者）: ポートに接続してきた Supplicant（クライアント）を認証する機器またはソフトウェア。認証に成功した場合はポート経由の通信を許可、失敗した場合はポート経由の通信を拒否する。認証処理そのものは、認証サーバー（RADIUS サーバー）に依頼する（Supplicant の情報を認証サーバーに中継して、認証結果を受け取る）。
- 認証サーバー（RADIUS サーバー）: Authenticator の要求に応じて、Supplicant を認証する機器またはソフトウェア。認証情報を一元管理している。Authenticator との間の認証情報の受け渡しには

RADIUS プロトコルを用いる。

- Supplicant (クライアント): ポートへの接続時に Authenticator から認証を受ける機器またはソフトウェア。一部の OS に標準装備されているほか、単体のクライアントソフトウェアとして用意されていることもある。

本製品の各スイッチポートは、上記のうち、Authenticator と Supplicant になることができます。認証サーバー (RADIUS サーバー) は別途用意する必要があります。

- ✧ Authenticator ポートと Supplicant ポートは、ミラーポートに設定することはできません。
- ✧ Authenticator ポートと Supplicant ポートは、トランクグループに所属させることはできません。
- ✧ ポート認証有効のポートがある場合、EAP 透過機能は使用できません。
- ✧ コンボポートとポートセキュリティが有効なポートは、Authenticator ポートに設定することはできません。
- ✧ Authenticator ポートにはスタティックエントリは追加できません。
- ✧ Authenticator ポートでは、LDF 検出を併用できません。

802.1X 認証方式

802.1X 認証では、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP など様々な認証方式が使用されています。このうち、本製品の 802.1X 認証モジュールが現在サポートしている EAP 認証方式は以下のとおりです。

- Authenticator 時: EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP
- Supplicant 時: EAP-MD5

基本設定

本製品を使ってポート認証のシステムを運用するための基本的な設定例を示します。以下の例では、認証方式として「EAP-MD5」を使うものと仮定します。

Authenticator

本製品を Authenticator として使用する場合の基本設定を示します。ここでは、ポート 5 で認証を行うものとします。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

1. ポート認証では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。VLAN default に IP アドレスを設定します。

```
ADD IP IPADDRESS=192.168.10.5 MASK=255.255.255.0 ↵
```

2. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
SECRET=himitsu ↵
```

3. ポート認証モジュールを有効にします。

```
ENABLE PORTAUTH ↵
```

4. ポート 5 を Authenticator ポートに指定します。

```
SET PORTAUTH PORT=5 TYPE=AUTHENTICATOR ↵
```

- ※ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、SET PORTAUTH PORT コマンド (15 ページ) の CONTROL パラメーターを AUTHORISED に設定してください。

Authenticator (ダイナミック VLAN)

ダイナミック VLAN (Dynamic VLAN Assignemnt) は、RADIUS サーバーから受け取った認証情報に基づいてポートの所属 VLAN を動的に変更する機能です。

以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

ここでは、利用者機器のために 3 つの VLAN 「A」、「B」、「C」を用意します。また、RADIUS サーバーを接続するための VLAN 「R」も作成します。各ポートに接続された機器は、認証成功後、RADIUS サーバー側から返された VLAN («A」、「B」、「C」のどれか) に自動的にアサインされます。

1. VLAN を作成します

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
CREATE VLAN=R VID=1000 ↵
```

2. RADIUS サーバーを接続するポート 16 を VLAN 「R」に割り当てます。

```
ADD VLAN=R PORT=16 ↵
```

3. 802.1X では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。VLAN 「R」に IP アドレスを設定します。

```
ADD IP INT=R IP=192.168.10.5 MASK=255.255.255.0 ↵
```

4. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813  
SECRET=himitsu ↵
```

5. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

6. ポート 1～8 で 802.1X 認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 1～8 は Authenticator ポートとなります。また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
SET PORTAUTH=8021X PORT=1-8 TYPE=AUTHENTICATOR  
VLANASSIGNMENT=ENABLED ↵
```

- ※ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、SET PORTAUTH PORT コマンド (15 ページ) の CONTROL パラメーターを AUTHORISED に設定してください。

ダイナミック VLAN の動作仕様は次のとおりです。

- Supplicant の認証に失敗した場合、ポートは本来の VLAN (ADD VLAN PORT コマンド (「バーチャル LAN」の 12 ページ) で指定した VLAN) の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、ポートはその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、ポートは本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから VLAN の情報が返ってこなかった場合、ポートは本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、ポートは本来の VLAN 所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。
- 未認証のポート、および、CONTROL=UNAUTHORISED (未認証固定) または CONTROL=AUTHORISED (認証済み固定) に設定されたポートは、本来の VLAN 所属となります。

ポートがダイナミック VLAN にアサインされているときは、ADD VLAN PORT コマンド (「バーチャル LAN」の 12 ページ) で該当ポートの所属 VLAN を変更しても、設定変更は直ちには反映されません。ポートがダイナミック VLAN から本来の VLAN に戻るのは、次のときです。

- 認証済みの Supplicant がなくなったとき。

- リンクがダウンしたとき。
- システム上でポート認証が無効にされたとき（DISABLE PORTAUTH コマンド（12 ページ））。

Supplicant

本製品を Supplicant として使用する場合の基本設定を示します。ここでは、ポート 1 が認証を受けるものとし、802.1X Supplicant としての動作には IP の設定が必須です。

1. ポート認証モジュールを有効にします。

```
ENABLE PORTAUTH ↵
```

2. ポート 1 を Supplicant ポートに指定します。

```
SET PORTAUTH PORT=1 TYPE=SUPPLICANT USERNAME=user1 PASSWORD=himitsu ↵
```

- ※ ポート認証機能でゲスト VLAN やダイナミック VLAN を使用し、Supplicant が DHCP サーバーから IP アドレスを取得する場合は、認証前の VLAN において DHCP サーバーのリースタイムを短く設定する必要があります。

認証サーバー

ポート認証機能を利用するために必要な認証サーバー（RADIUS サーバー）の設定項目について簡単に説明します。

- ※ 認証サーバーの詳細な設定方法については、ご使用のサーバー製品のマニュアルをご参照ください。
- 802.1X 認証において、ダイナミック VLAN を使用しないときは、ユーザーごとに下記の属性を定義してください。

属性名	属性値	備考
User-Name	ユーザー名	認証対象のユーザー名（例：“user1”，“userB”）
User-Password	パスワード	（EAP-MD5、PEAP(EAP-MSCHAPv2)、TTLS使用時）ユーザー名に対応するパスワード（例：“dbf8a9hve”，“h1mi2uDa4o”）。EAP-TLS 使用時は不要（別途、ユーザー電子証明書の用意が必要）

表 1: 802.1X 認証（ダイナミック VLAN なし）

- ※ 認証方式として EAP-TLS を使う場合は、RADIUS サーバーの電子証明書と各ユーザーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。認証方式として EAP-PEAP、EAP-TTLS を使う場合は、RADIUS サーバーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。詳細は RADIUS サーバーおよび Supplicant（OS や専用ソフトウェアなど）のマニュアルをご参照ください。

- また、802.1X 認証でダイナミック VLAN を使用するときは、前述の諸属性に加え、下記の 3 属性を追加設定してください。

属性名	属性値	備考
Tunnel-Type	VLAN (13)	固定値。指定方法はサーバーに依存
Tunnel-Medium-Type	IEEE-802 (6)	固定値。指定方法はサーバーに依存
Tunnel-Private-Group-ID	VLAN 名 か VLAN ID	認証対象のユーザーや機器が認証をパスした後に所属させる VLAN の名前か VLAN ID (例: "sales", 10)

表 2: ダイナミック VLAN 用の属性

Supplicant MAC 透過機能

本製品は、特定の MAC アドレスを送信元アドレスに持つフレームのみを常に認証済みの Supplicant として通信可能にする Supplicant MAC 透過機能にも対応しています。

Supplicant MAC 透過アドレスを登録する場合は、SET PORTAUTH PORT SUPPLICANTMAC コマンド (19 ページ) を使います。

```
SET PORTAUTH PORT=5 SUPPLICANTMAC=00-00-F4-11-11-11 CONTROL=AUTHORISED ↵
```

登録済みの Supplicant MAC 透過アドレスを削除する場合は、DELETE PORTAUTH PORT SUPPLICANTMAC コマンド (11 ページ) を使います。

```
DELETE PORTAUTH PORT=5 SUPPLICANTMAC=00-00-F4-11-11-11 ↵
```

コマンドリファレンス編

機能別コマンド索引

概要・基本設定

ADD PORTAUTH PORT SUPPLICANTMAC	9
DELETE PORTAUTH PORT SUPPLICANTMAC	11
DISABLE PORTAUTH	12
ENABLE PORTAUTH	13
SET PORTAUTH AUTHMETHOD	14
SET PORTAUTH PORT	15
SET PORTAUTH PORT SUPPLICANTMAC	19
SHOW PORTAUTH	21
SHOW PORTAUTH PORT AUTHENTICATOR	24
SHOW PORTAUTH PORT SUPPLICANT	28

ADD PORTAUTH PORT SUPPLICANTMAC

カテゴリー：ポート認証

ADD PORTAUTH PORT=port-number SUPPLICANTMAC=macadd [CONTROL=AUTHORISED]

port-number: スイッチポート番号（1～。単一ポートのみ指定可）

macadd: MAC アドレス。xx-xx-xx-xx-xx-xx の形式

解説

Supplicant MAC 透過アドレスを登録する。Supplicant MAC 透過アドレスは、Single-Supplicant モード、Multi-Supplicant モードのどちらの場合も 1 ポートに対して 10 個まで登録できる

パラメーター

PORT スイッチポート番号

SUPPLICANTMAC Supplicant MAC 透過アドレスとして登録する MAC アドレス。ブロードキャストアドレス、マルチキャストアドレスは設定できない

CONTROL 手動設定による Authenticator ポートの状態。AUTHORISED（認証済み固定）のみを指定可能

入力・出力・画面例

```
Manager > add portauth port=1 supplicantmac=00-00-f4-11-11-11 control=authorised
```

例

Supplicant MAC 透過アドレスを追加する

```
ADD PORTAUTH PORT=1 SUPPLICANTMAC=00-00-f4-11-11-11 CONTROL=AUTHORISED
```

備考・注意事項

ポート認証設定において、TYPE が Authenticator、かつ、CONTROL が Auto に指定されているポートに対して、Supplicant MAC 透過アドレスを登録できる

ポート認証が有効に設定されていないポートに対して実行した場合、指定された MAC アドレスは本製品の設定にのみ登録され、FDB には登録されない

すでにフィルター対象として登録されているアドレス、他ポートで認証済みの Supplicant の MAC アドレスは、Supplicant MAC 透過アドレスに登録できない

ポート認証設定において TYPE を Authenticator 以外に変更した場合、または、CONTROL を AUTO 以外に変更した場合、すでに登録されている MAC アドレスは設定および FDB から削除される
本コマンドで登録した MAC アドレスを違う VLAN でダイナミックエントリーとして登録すると、設定したエージングタイムと関係なく、約 30 秒で削除される

関連コマンド

DELETE PORTAUTH PORT SUPPLICANTMAC (11 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (19 ページ)

DELETE PORTAUTH PORT SUPPLICANTMAC

カテゴリー：ポート認証

DELETE PORTAUTH PORT=*port-number* [**SUPPLICANTMAC=***macadd*]

port-number: スイッチポート番号（1～。単一ポートのみ指定可）

macadd: MAC アドレス。xx-xx-xx-xx-xx-xx の形式

解説

Supplicant MAC 透過アドレスを削除する

パラメーター

PORT スイッチポート番号

SUPPLICANTMAC 削除する Supplicant MAC 透過アドレス。省略した場合は、指定ポートに登録されている全 Supplicant MAC 透過アドレスを削除する

入力・出力・画面例

```
Manager > delete portauth port=1 supplicantmac=00-00-f4-11-11-11

Operation successful.
```

例

登録されている Supplicant MAC 透過アドレスを削除する

```
DELETE PORTAUTH PORT=1 SUPPLICANTMAC=00-00-f4-11-11-11
```

関連コマンド

ADD PORTAUTH PORT SUPPLICANTMAC (9 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (19 ページ)

DISABLE PORTAUTH

カテゴリー：ポート認証

DISABLE PORTAUTH

解説

ポート認証モジュールを無効にする。デフォルトは無効

入力・出力・画面例

```
Manager > disable portauth  
  
Operation successful.
```

例

ポート認証機能を無効にする

DISABLE PORTAUTH

関連コマンド

ENABLE PORTAUTH (13 ページ)

SET PORTAUTH AUTHMETHOD (14 ページ)

SET PORTAUTH PORT (15 ページ)

SHOW PORTAUTH (21 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (24 ページ)

SHOW PORTAUTH PORT SUPPLICANT (28 ページ)

ENABLE PORTAUTH

カテゴリー：ポート認証

ENABLE PORTAUTH

解説

ポート認証モジュールを有効にする。デフォルトは無効

入力・出力・画面例

```
Manager > enable portauth  
  
Operation successful.
```

例

ポート認証機能を有効にする

ENABLE PORTAUTH

備考・注意事項

Authenticator ポートと Supplicant ポートではポートセキュリティは使用できない

Authenticator ポートと Supplicant ポートはトランクグループに所属することはできない

Authenticator ポートと Supplicant ポートはミラーポートに設定できない

ポート認証有効の場合、EAP 透過機能は使用できない

Combo ポートはポート認証の Authenticator ポートに設定することはできない

Authenticator ポートにはスタティックエントリーは追加できない

関連コマンド

DISABLE PORTAUTH (12 ページ)

SET PORTAUTH AUTHMETHOD (14 ページ)

SET PORTAUTH PORT (15 ページ)

SHOW PORTAUTH (21 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (24 ページ)

SHOW PORTAUTH PORT SUPPLICANT (28 ページ)

SET PORTAUTH AUTHMETHOD

カテゴリー：ポート認証

SET PORTAUTH AUTHMETHOD=RADIUSSEAP

解説

ポート認証モジュールの認証プロトコルを設定する

パラメーター

AUTHMETHOD RadiusEAP のみ

入力・出力・画面例

```
Manager > set portauth authmethod=radiusseap

Operation successful.
```

例

認証プロトコルを RadiusEAP に設定する

SET PORTAUTH AUTHMETHOD=RADIUSSEAP

関連コマンド

DISABLE PORTAUTH (12 ページ)

ENABLE PORTAUTH (13 ページ)

SET PORTAUTH PORT (15 ページ)

SHOW PORTAUTH (21 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (24 ページ)

SHOW PORTAUTH PORT SUPPLICANT (28 ページ)

SET PORTAUTH PORT

カテゴリ：ポート認証

Authenticator 時

```
SET PORTAUTH [=8021X] PORT={port-list|ALL} TYPE=AUTHENTICATOR
[MODE={SINGLE|MULTI}] [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}]
[SERVERTIMEOUT=1..600] [QUIETPERIOD=0..65535] [TXPERIOD=1..65535]
[REAUTHPERIOD=1..86400] [SUPPTIMEOUT=1..600] [MAXREQ=1..10]
[REAUTHENABLED={ENABLED|DISABLED}] [PIGGYBACK={ENABLED|DISABLED}]
[GUESTVLAN={vlan-name|1..4094|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}]
```

Supplicant 時

```
SET PORTAUTH [=8021X] PORT={port-list|ALL} TYPE=SUPPLICANT
[AUTHPERIOD=1..300] [HELDPERIOD=0..65535] [MAXSTART=1..10]
[STARTPERIOD=1..60] [USERNAME=login-name] [PASSWORD=password]
```

認証ポートの解除

```
SET PORTAUTH PORT={port-list|ALL} TYPE=NONE
```

port-list: スイッチポート番号 (1~。ハイフン [-]、カンマ [,] を使った複数指定も可能)

login-name: ログイン名 (1~63 文字。英数字のみ使用可能)

password: パスワード (1~63 文字。英数字のみ使用可能)

vlan-name: VLAN 名

解説

指定ポートのポート認証設定を変更する

パラメーター

PORTAUTH 8021X(802.1X 認証) のみ選択可能

PORT 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

TYPE スイッチポートのタイプ (ポート認証における役割)。AUTHENTICATOR (Authenticator ポート)、SUPPLICANT (Supplicant ポート)、NONE (ポート認証機能無効) のいずれかを指定する

MODE (Authenticator ポートのみ) Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード (MODE=SINGLE) と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード (MODE=MULTI) がある。Single-Supplicant モードでは、該当ポート配

下に最初に接続された Supplicant だけが認証対象となる。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。

CONTROL (Authenticator ポートのみ) 手動設定による Authenticator ポートの状態。AUTO (認証結果に応じて変動)、UNAUTHORISED (未認証固定)、AUTHORISED (認証済み固定) から選択する。デフォルトは AUTO。通常は AUTO のままでよい

SERVERTIMEOUT (Authenticator ポートのみ) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)。デフォルトは 30 秒

QUIETPERIOD (Authenticator ポートのみ) Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間 (秒)。この期間中は受信した EAPOL パケットをすべて破棄する。デフォルトは 60 秒。0 指定時はすぐに通信を許可する

TXPERIOD (Authenticator ポートのみ) Supplicant に EAPOL パケットを再送信する間隔 (秒)。デフォルトは 30 秒

REAUTHPERIOD (Authenticator ポートのみ) Supplicant の再認証間隔 (秒)。デフォルトは 3600 秒

SUPPTIMEOUT (Authenticator ポートのみ) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒

MAXREQ (Authenticator ポートのみ) Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回

REAUTHENABLED (Authenticator ポートのみ) Supplicant ポートの再認証を行うかどうかを選択する。ENABLED (再認証を行う) または DISABLED (再認証を行わない) から選択する。デフォルトは、ENABLED

PIGGYBACK (Authenticator ポートのみ) Single-Supplicant モード (MODE=SINGLE) において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。ENABLED (有効) または DISABLED (無効) から選択する。デフォルトは、DISABLED

AUTHPERIOD (Supplicant ポートのみ) Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間 (秒)。デフォルトは 30 秒

GUESTVLAN (Authenticator ポートのみ) ゲスト VLAN を指定する。VLAN 名または VLAN ID を指定する。NONE はゲスト VLAN を使用しないことを意味する。NONE 以外を指定すると直ちにゲスト VLAN の所属となる。認証が成功するとゲスト VLAN から他の VLAN の所属となる。認証に失敗すると、またゲスト VLAN の所属となる。Multi-Supplicant モード (MODE=MULTI) では NONE 以外に指定できない。デフォルトは NONE

SECUREVLAN (Authenticator ポートのみ) Multi-Supplicant モード (MODE=MULTI) でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートでのみ有効。デフォルトは ON

VLANASSIGNMENT (Authenticator ポートのみ) ダイナミック VLAN の有効/無効を選択する。有効時は、指定ポートの所属 VLAN を動的に変更する。マルチプル VLAN モード時は ENABLED に設定できない。デフォルトは 802.1Q タグ VLAN モード時は ENABLED、マルチプル VLAN 時は DISABLED

HELDPERIOD (Supplicant ポートのみ) 認証失敗後、Authenticator との通信を試みない期間 (秒)。

デフォルトは 60 秒

MAXSTART (**Supplicant** ポートのみ) EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する。デフォルトは 3 回

STARTPERIOD (**Supplicant** ポートのみ) Authenticator に EAPOL-Start パケットを再送信する間隔 (秒)。デフォルトは 30 秒

USERNAME (**Supplicant** ポートのみ) 指定スイッチポートが Supplicant として動作する場合に使うユーザー名。必ず PASSWORD パラメーターと組で指定すること

PASSWORD (**Supplicant** ポートのみ) 指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること

入力・出力・画面例

```
Manager > set portauth port=1-8 type=authenticator

Operation successful.
```

例

ポート番号 1～8 を Authenticator ポートに設定する

```
SET PORTAUTH PORT=1-8 TYPE=AUTHENTICATOR
```

備考・注意事項

ポートセキュリティを有効に設定したポートは TYPE=AUTHENTICATOR に設定できない

タグつきポートに設定されたポートには、ポート認証は併用不可

VLAN が 802.1Q タグ VLAN の時、本コマンドのダイナミック VLAN を無効 (VLANASSIGNMENT=DISABLED)

に設定したあと、VLAN モードをマルチプル VLAN に変更すると、本コマンドによるダイナミック VLAN の無効の指定は設定から消去される。この状態で VLAN モードを再度 802.1Q タグ VLAN に戻すと、ダイナミック VLAN はデフォルトの有効として動作する

ゲスト VLAN を使用する場合、実際にポートに適用されている VLAN を確認するときは、SHOW VLAN コマンドを使用する。SHOW SWITCH PORT コマンドでは、Supplicant が認証を通ったときに所属する VLAN の設定が表示される

トランクポート、ミラーポートに指定したポートは TYPE=AUTHENTICATOR、TYPE=SUPPLICANT に設定できない

関連コマンド

DISABLE PORTAUTH (12 ページ)

ENABLE PORTAUTH (13 ページ)

SET PORTAUTH AUTHMETHOD (14 ページ)

SHOW PORTAUTH (21 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (24 ページ)

SHOW PORTAUTH PORT SUPPLICANT (28 ページ)

SET PORTAUTH PORT SUPPLICANTMAC

カテゴリー：ポート認証

SET PORTAUTH PORT=*port-number* **SUPPLICANTMAC=***macadd* [CONTROL=AUTHORISED]

port-number: スイッチポート番号（1～。単一ポートのみ指定可）

macadd: MAC アドレス。xx-xx-xx-xx-xx-xx の形式

解説

Supplicant MAC 透過アドレスを登録する。Supplicant MAC 透過アドレスは、Single-Supplicant モード、Multi-Supplicant モードのどちらの場合も 1 ポートに対して 10 個まで登録できる

パラメーター

PORT 対象となるポート番号

SUPPLICANTMAC Supplicant MAC 透過アドレスとして登録する MAC アドレス。ブロードキャストアドレス、マルチキャストアドレスは設定できない

CONTROL 手動設定による Authenticator ポートの状態。AUTHORISED（認証済み固定）のみを指定可能

入力・出力・画面例

```
Manager > set portauth port=1 supplicantmac=00-00-f4-11-11-11 control=authorised
```

例

Supplicant MAC 透過アドレスを追加する

```
SET PORTAUTH PORT=1 SUPPLICANTMAC=00-00-f4-11-11-11 CONTROL=AUTHORISED
```

備考・注意事項

ポート認証設定において、TYPE が Authenticator、かつ、CONTROL が Auto に指定されているポートに対して、Supplicant MAC 透過アドレスを登録できる

ポート認証が有効に設定されていないポートに対して実行した場合、指定された MAC アドレスは本製品の設定にのみ登録され、FDB には登録されない

すでにフィルター対象として登録されているアドレス、他ポートで認証済みの Supplicant の MAC アドレスは、Supplicant MAC 透過アドレスに登録できない

ポート認証設定において TYPE を Authenticator 以外に変更した場合、または、CONTROL を AUTO 以外に変更した場合、すでに登録されている MAC アドレスは設定および FDB から削除される
本コマンドで登録した MAC アドレスを違う VLAN でダイナミックエントリーとして登録すると、設定したエージングタイムと関係なく、約 30 秒で削除される

関連コマンド

ADD PORTAUTH PORT SUPPLICANTMAC (9 ページ)

DELETE PORTAUTH PORT SUPPLICANTMAC (11 ページ)

SHOW PORTAUTH

カテゴリー：ポート認証

SHOW PORTAUTH [=8021X] [{CONFIG|STATUS}]

解説

ポート認証モジュールの設定と情報を表示する

パラメーター

PORTAUTH 8021X(802.1X 認証) のみ指定可。省略時は 8021X とみなされる

CONFIG ポート認証モジュールの設定を表示する

STATUS ポート認証モジュールの状態を表示する

入力・出力・画面例

```
Manager > show portauth config
```

```
Port Access Configuration Information:
```

```
Port Access Control..... Disabled
```

```
Authentication Method ..... RADIUS EAP
```

```
Manager > show portauth status
```

```
-----
Port AuthMode PortRole  VLAN  PortStatus  Status  Additional Info
-----
1      -----  None           -----  -----  -----
2      -----  None           -----  -----  -----
3      -----  None           -----  -----  -----
4      8021x    Auth          10     Unauthorized Held      00:09:16:00:02:06
5      8021x    Auth          1000   Authorized  Authenticating 00:60:97:37:72:6E
6      8021x    Auth          1000   Authorized  Authenticated 00:03:47:B5:79:89
7      -----  None           -----  -----  -----
8      -----  None           -----  -----  -----
9      -----  None           -----  -----  -----
10     -----  None           -----  -----  -----
11     -----  None           -----  -----  -----
12     -----  None           -----  -----  -----
13     -----  None           -----  -----  -----
14     -----  None           -----  -----  -----
15     -----  None           -----  -----  -----
16     -----  None           -----  -----  -----
```

Port Access Control	ポート認証モジュールの有効/無効。Enabled か Disabled
Authentication Method	認証方式

表 3: CONFIG 指定時

Port	ポート番号
AuthMode	使用認証モード 802.1X (ポート認証)
Port Role	スイッチポートのタイプ(ポート認証における役割)。Authenticator、Supplicant、None のいずれか
VLAN	現在割り当てられている VLAN ID
PortStatus	ポートの状態 Unauthorized (未認証) または、Authorized(認証済)。Multi-Supplicant 有効時は、各 SUPPLICANT の状態を表示
Status	認証状態。(ポートのタイプが設定され、Port 認証モジュールが有効の場合に、次のステータスを表示する。) AUTHENTICATOR ポートの場合は、Initialize (初期化) Connecting (接続中) Authenticating (認証中) Authenticated (認証済み) Aborting (認証断念中) Held (待機中) Force_Auth (「認証済み」に固定設定) Force_Unauth (「未認証」に固定設定) のいずれか。SUPPLICANT ポートの場合は、Acquired (要求中) Connecting (接続中) Authenticating (認証中) Authenticated (認証済み) Held (待機中) Logoff (ログオフ) のいずれか
Additional Info	AUTHENTICATOR ポートで、Authenticated 状態のときに、サブリカントの MAC アドレスを表示する

表 4: STATUS 指定時

例

ポート認証モジュールの設定を表示する

```
SHOW PORTAUTH CONFIG
```

ポート認証モジュールの状態を表示する

```
SHOW PORTAUTH STATUS
```

関連コマンド

DISABLE PORTAUTH (12 ページ)

ENABLE PORTAUTH (13 ページ)

SET PORTAUTH AUTHMETHOD (14 ページ)

SET PORTAUTH PORT (15 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (24 ページ)

SHOW PORTAUTH PORT SUPPLICANT (28 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR

カテゴリー：ポート認証

SHOW PORTAUTH [=8021X] **PORT**=*{port-list|ALL}* [AUTHENTICATOR] [{CONFIG|STATUS}]

port-list: スイッチポート番号（1～）。ハイフン [-]、カンマ [,] を使った複数指定も可能）

解説

指定ポートのポート認証モジュールの設定と情報を表示する

パラメーター

PORTAUTH 8021X(802.1X 認証)

PORT 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

CONFIG ポート認証モジュールの設定を表示する

STATUS ポート認証モジュールの状態を表示する

入力・出力・画面例

```
Manager > show portauth port=4-6 authenticator
```

```
-----All Authenticator Configuration -----
```

```
-----
Port Number           4
Auth Mode             8021X
Port Control          Auto
Supplicant Mode       Single
Quiet Period          60
Tx Period             30
Reauth Enabled        Enabled
Reauth Period         3600
Supplicant Timeout    30
Server Timeout        30
Max Requests          2
Piggyback Mode        Disabled
vlanAssignment        Enabled
secureVlan            On
guestVlan             None

Port Number           5
Auth Mode             8021X
Port Control          Auto
```


Supplicant Mode	Single					
Quiet Period	60					
Tx Period	30					
Reauth Enabled	Enabled					
Reauth Period	3600					
Supplicant Timeout	30					
Server Timeout	30					
Max Requests	2					
Piggyback Mode	Disabled					
vlanAssignment	Enabled					
secureVlan	On					
guestVlan	None					
Port Number	6					
Auth Mode	8021X					
Port Control	Auto					
Supplicant Mode	Single					
Quiet Period	60					
Tx Period	30					
Reauth Enabled	Enabled					
Reauth Period	3600					
Supplicant Timeout	30					
Server Timeout	30					
Max Requests	2					
Piggyback Mode	Disabled					
vlanAssignment	Enabled					
secureVlan	On					
guestVlan	None					
Attached Supplicant(s)	00-00-11-11-11-11					
	00-00-22-22-22-22					

Port	AuthMode	PortRole	VLAN	PortStatus	Status	Additional Info

4	8021x	Auth	10	Unauthorized	Held	00:09:16:00:02:06
5	8021x	Auth	1000	Authorized	Authenticating	00:60:97:37:72:6E
6	8021x	Auth	1000	Authorized	Authenticated	00:03:47:B5:79:89

Auth Mode	認証モード。802.1x
Port Control	(Authenticator ポート) 手動設定による Authenticator ポートの状態。 AUTO (認証結果に応じて変動) UNAUTHORISED (未認証固定) AUTHORISED (認証済み固定) のいずれか
Supplicant Mode	Single(Single-Supplicant モード)、Multi(Multi-Supplicant モード) のいずれか
Quiet Period	(Authenticator ポート) Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間 (秒)

Tx Period	(Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒)
Reauth Enabled	(Authenticator ポート) Supplicant ポートの再認証を行うかどうか。Enabled (再認証を行う) または Disabled (再認証を行わない) のいずれか
Reauth Period	(Authenticator ポート) Supplicant の再認証間隔 (秒)
Supplicant Timeout	(Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)
Server Timeout	(Authenticator ポート) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)
Max Requests	(Authenticator ポート) Supplicant に対する EAPOL-Request パケットの最大再送回数
Piggyback Mode	(Authenticator ポート) Piggy back モードの有効/無効。
vlanAssignment	ダイナミック VLAN の有効・無効
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないとは認証を許可しない機能の有効・無効
guestVlan	ゲスト VLAN に指定した VLAN 名と VLAN ID
Attached Supplicant(s)	Supplicant MAC 透過アドレス

表 5: CONFIG 指定時

Port	ポート番号
AuthMode	使用認証モード 802.1x
PortRole	スイッチポートのタイプ (ポート認証における役割) Authenticator
VLAN	現在割り当てられている VLAN ID
PortStatus	ポートの状態 Unauthorized (未認証) または、Authorized(認証済)。Multi-Supplicant 有効時は、各サブリカントの状態を、上記のいずれかで表示する。
Status	認証状態。(ポートのタイプが設定され、Port 認証モジュールが有効の場合に、次のステータスを表示する。) AUTHENTICATOR ポートの場合は、Initialize (初期化) Connecting (接続中) Authenticating (認証中) Authenticated (認証済み) Aborting (認証断念中) Held (待機中) Force_Auth (「 認証済み 」 に固定設定) Force_Unauth (「 未認証 」 に固定設定) のいずれか。SUPPLICANT ポートの場合は、Acquired (要求中) Connecting (接続中) Authenticating (認証中) Authenticated (認証済み) Held (待機中) Logoff (ログオフ) のいずれか

Additional Info	Authenticator ポートで、Authenticated 状態のときに、サブリカントの MAC アドレスを表示する。MultiSupplicant が有効な場合は、各サブリカントの MAC アドレスを表示
-----------------	--

表 6: STATUS 指定時

例

ポート 1 のポート認証モジュールの設定を表示する

SHOW PORTAUTH PORT=1 AUTHENTICATOR CONFIG

ポート 1 のポート認証モジュールの状態を表示する

SHOW PORTAUTH PORT=1 AUTHENTICATOR STATUS

関連コマンド

DISABLE PORTAUTH (12 ページ)

ENABLE PORTAUTH (13 ページ)

SET PORTAUTH AUTHMETHOD (14 ページ)

SET PORTAUTH PORT (15 ページ)

SHOW PORTAUTH (21 ページ)

SHOW PORTAUTH PORT SUPPLICANT (28 ページ)

SHOW PORTAUTH PORT SUPPLICANT

カテゴリー：ポート認証

SHOW PORTAUTH [=8021X] **PORT**=*{port-list|ALL}* **SUPPLICANT** [{CONFIG|STATUS}]

port-list: スイッチポート番号（1～。ハイフン [-]、カンマ [,] を使った複数指定も可能）

解説

指定ポートのポート認証モジュールの設定と情報を表示する

パラメーター

PORTAUTH 8021X(802.1X 認証)

PORT 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

CONFIG ポート認証モジュールの設定を表示する

STATUS ポート認証モジュールの状態を表示する

入力・出力・画面例

```
Manager > show portauth port=1 supplicant config
```

```
-----Supplicant Configuration -----
```

```
Port Number      1
Auth Period      30
Held Period      60
Max Start        3
Start Period     30
User Name
User Password
```

```
Manager > show portauth port=2 supplicant status
```

```
-----
Port  PortRole      Status      Additional Info
-----
2     Supplicant    -----
```

Port Number	ポート番号
Auth Period	Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）

Held Period	認証失敗後、Authenticator との通信を試みない期間（秒）
Max Start	EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する
Start Period	Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
User Name	ユーザー名
User Password	パスワード

表 7: CONFIG 指定時

Port	ポート番号
PortRole	スイッチポートのタイプ（ポート認証における役割）。Supplicant
VLAN	Supplicant 指定時は表示されない
PortStatus	Supplicant 指定時は表示されない
Status	ポートの状態。（ポートのタイプが設定され、ポート認証モジュールが有効の場合に、次のステータスを表示する。）Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか
Additional Info	Authenticator ポートで、Authenticated 状態のときに、サブリカントの MAC アドレスを表示する。MultiSupplicant が有効な場合は、各サブリカントの MAC アドレスを表示

表 8: STATUS 指定時

例

ポート 1 のポート認証モジュールの設定を表示する

```
SHOW PORTAUTH PORT=1 SUPPLICANT CONFIG
```

ポート 2 のポート認証モジュールの状態を表示する

```
SHOW PORTAUTH PORT=2 SUPPLICANT STATUS
```

関連コマンド

DISABLE PORTAUTH（12 ページ）

ENABLE PORTAUTH（13 ページ）

SET PORTAUTH AUTHMETHOD（14 ページ）

SET PORTAUTH PORT（15 ページ）

SHOW PORTAUTH（21 ページ）

SHOW PORTAUTH PORT AUTHENTICATOR（24 ページ）