802.1x サポート

802.1x 認証の概要

IEEE 802.1x ポートベースの認証は、不正なデバイスによるネットワーク アクセスを防止するためにデバイスに設定されます。デバイスでは、固定された構成に基づいて、ルータ、スイッチ、およびアクセス ポイントの機能を組み合わせることができます。802.1x 認証が有効になっているスイッチ ポートに接続しているデバイスはすべて、トラフィックの交換を開始する場合に、関連する EAP 認証モデルを実行する必要があります。

現在、Cisco Wave 2 AP および Wi-Fi 6（802.11ax）APは、EAP-FAST、EAP-TLS、および EAP-PEAP 方式のスイッチポートを使用した 802.1x 認証をサポートしています。そのため、設定を有効にして組み込みコントローラから AP にクレデンシャルを提供できます。

EAP-FAST プロトコル

シスコが開発した EAP-FAST プロトコルでは、RADIUS を使用したセキュアな TLS トンネルを確立するために、AP では、インバンドプロビジョニング（セキュア チャネル内）またはアウトバンドプロビジョニング（手動）を介して提供される強力な共有キー（PAC）を必要とします。

（注） AP では MSCHAP バージョン 2 方式の EAP-FAST が使用されるため、EAP-FAST タイプの設定では AP に対して Dot1x クレデンシャルの設定が必要です。

（注） ローカル EAP は、Cisco 7925 電話ではサポートされていません。

EAP-TLS/EAP-PEAP プロトコル

EAP-TLS プロトコルまたは EAP-PEAP プロトコルは、証明書ベースの相互 EAP 認証を提供します。

EAP-TLS では、サーバー側証明書とクライアント側証明書の両方が必要であり、特定のセッションに対してデータを暗号化または復号化するために、セキュリティ保護された共有キーが導出されます。一方、EAP-PEAP ではサーバー側証明書のみ必要であり、クライアントはセキュリティ保護されたチャネルでパスワードベースのプロトコルを使用して認証を行います。

（注） EAP-PEAP タイプの設定では AP に対して Dot1x クレデンシャルの設定が必要です。また、AP では LSC のプロビジョニングを実行する必要もあります。AP では MSCHAP バージョン 2 方式の PEAP プロトコルが使用されます。

802.1x 認証の制限事項

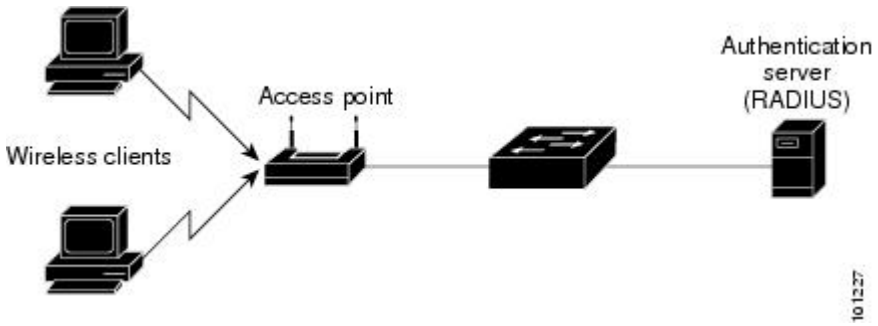
- 802.1x はダイナミック ポートまたはイーサチャネル ポートではサポートされていません。
- 802.1x はメッシュ AP のシナリオではサポートされていません。
- クレデンシャルの不一致、または AP 上の証明書の期限切れ/無効が生じた場合、組み込みコントローラから回復することはありません。設定を修正するために再び AP に接続するには、スイッチ ポートで 802.1x 認証を無効にする必要があります。
- AP にインストールされた証明書では証明書失効チェックは実装されません。
- AP では ローカルで有効な証明書（LSC）を 1 つだけプロビジョニングでき、組み込みコントローラによる CAPWAP DTLS セッションの確立と、スイッチによる 802.1x 認証では、これと同じ証明書を使用する必要があります。組み込みコントローラのグローバル LSC 設定が無効になった場合、AP では、すでにプロビジョニングされている LSC が削除されます。
- AP に設定のクリアが適用された場合、AP では 802.1x EAP タイプの設定と LSC 証明書が失われます。802.1x が必要な場合、AP では再度ステージング プロセスを実行する必要があります。
- マルチホスト認証モードのトランクポート AP の 802.1x がサポートされています。Network Edge Authentication Topology（NEAT）は COS AP ではサポートされていません。

トポロジ - 概要

802.1x 認証のイベントは次のとおりです。

1. AP は 802.1x サプリカントとして機能し、RADIUS サーバーに対してスイッチによって認証されます。RADIUS サーバーは、EAP-FAST とともに EAP-TLS と EAP-PEAP も サポートします。dot1x 認証がスイッチ ポートで有効になっている場合、そのポートに接続しているデバイスは、802.1x トラフィック以外のデータを受信して転送するために自分自身を認証します。
2. EAP-FAST 方式による認証を行うには、AP で RADIUS サーバーのクレデンシャルが必要になります。クレデンシャルは組み込みコントローラで設定でき、そこから設定更新要求を介して AP に渡されます。EAP-TLS または EAP-PEAP の場合、AP では、ローカル CA サーバーによって重要扱いにされた証明書（デバイス/ID および CA）が使用されます。

図 *1* : 図 *1* : *802.1x* 認証のトポロジ



802.1x 認証タイプと LSC AP 認証タイプの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[AP Join]** を選択します。

ステップ 2 [AP Join Profile] ページで、[Add] をクリックします。

[Add AP Join Profile] ページが表示されます。

ステップ 3 **[AP]** > **[General]** タブで、[AP EAP Auth Configuration] セクションに移動します。

ステップ 4 [EAP Type] ドロップダウン リストから、EAP タイプとして [EAP-FAST]、[EAP-TLS]、または [EAP-PEAP] を選択して、dot1x 認証タイプを設定します。

ステップ 5 [AP Authorization Type] ドロップダウン リストから、タイプとして [CAPWAP DTLS +] または [CAPWAP DTLS] のいずれかを選択します。

ステップ 6 [Save & Apply to Device] をクリックします。

802.1x 認証タイプと LSC AP 認証タイプの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	特権 EXEC モードを有効にし、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap profile** <profile-name> 例： `Device(config)# ap profile new-profile`	プロファイル名を指定します。
ステップ 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプを設定します。 **max-sessions**：AP ごとに開始される 802.1x セッションの最大数を設定します。 **username**：すべての AP の 802.1x ユーザー名を設定します。 **eap-type**：スイッチ ポートを使用した dot1x 認証タイプを設定します。 **lsc-ap-auth-state**：AP での LSC 認証状態を設定します。
ステップ 5	**dot1x eap-type {EAP-FAST | EAP-TLS | EAP-PEAP}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプ（EAP-FAST、EAP-TLS、または EAP-PEAP）を設定します。
ステップ 6	**dot1x lsc-ap-auth-state {CAPWAP-DTLS | Dot1x-port-auth | Both}** 例： `Device(config-ap-profile)#dot1x lsc-ap-auth-state Dot1x-port-auth`	AP での LSC 認証状態を設定します。 **CAPWAP-DTLS**：CAPWAP DTLS にのみ LSC を使用します。

	コマンドまたはアクション	目的
		Dot1x-port-auth：ポートでの dot1x 認証にのみ LSC を使用します。 **Both**：CAPWAP-DTLS とポートでの Dot1x 認証の両方に LSC を使用します。
ステップ 7	**end** 例： `Device(config-ap-profile)# end`	AP プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

802.1x ユーザー名とパスワードの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 [AP Join] ページで、 AP Join プロファイルの名前をクリックするか、[Add] をクリックして新規に作成します。

ステップ 3 [Management] タブをクリックし、[Credentials] タブをクリックします。

ステップ 4 ローカルのユーザ名とパスワードの詳細を入力します。

ステップ 5 適切なローカル パスワード タイプを選択します。

ステップ 6 802.1x ユーザー名とパスワードの詳細を入力します。

ステップ 7 適切な 802.1x パスワード タイプを選択します。

ステップ 8 セッションが期限切れになるまでの時間を秒単位で入力します。

ステップ 9 必要に応じて、ローカル クレデンシャルや 802.1 x クレデンシャルを有効にします。

ステップ 10 [Update & Apply to Device] をクリックします。

802.1x ユーザー名とパスワードの設定（CLI）

次の手順では、すべての AP の 802.1x パスワードを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	特権 EXEC モードを有効にし、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap profile** <profile-name> 例： `Device(config)# ap profile new-profile`	プロファイル名を指定します。
ステップ 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプを設定します。 **max-sessions**：AP ごとに開始される 802.1x セッションの最大数を設定します。 **username**：すべての AP の 802.1x ユーザー名を設定します。 **eap-type**：スイッチ ポートを使用した dot1x 認証タイプを設定します。 **lsc-ap-auth-state**：AP での LSC 認証状態を設定します。
ステップ 5	**dot1x username** <username> **password {0 | 8}** <password> 例： `Device(config-ap-profile)#dot1x username` *`username`* `password 0` *`password`*	すべての AP の dot1x パスワードを設定します。 0：暗号化されていないパスワードに従うことを指定します。 8：AES で暗号化されたパスワードに従うことを指定します。

スイッチ ポートでの 802.1x の有効化

次の手順では、スイッチ ポートで 802.1x を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	特権 EXEC モードを有効にし、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	**aaa authentication dot1x {default | listname} method1[method2...]** 例： `Device(config)# aaa authentication dot1x default group radius`	デバイスが AAA サーバーと通信できるように、特権コマンド レベルにアクセスするユーザー権限の決定に使用される一連の認証方式を作成します。
ステップ 5	**aaa authourization network group** 例： `aaa authourization network group`	802.1X でのネットワーク サービスの AAA 認証を有効にします。
ステップ 6	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 7	**interface type slot/port** 例： `Device(config)# interface fastethernet2/1`	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。
ステップ 8	**authentication port-control {auto | force-authorized | force-unauthorized}** 例： `Device(config-if)# authentication port-control auto`	インターフェイス上で 802.1x ポートベースの認証をイネーブルにします。 auto：IEEE 802.1x 認証をイネーブルにし、ポートを無許可ステートで開始します。ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。デバイスはサプリカントの識別を要求し、サプリカ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。デバイスはサプリカントの MAC アドレスを使用して、ネットワーク アクセスを試みる各サプリカントを一意に識別します。

	コマンドまたはアクション	目的
		force-authorized：IEEE802.1x 認証をディセーブルにし、その結果、認証の交換を必要とせずにポートが許可済みステートに変更されます。ポートは、クライアントの IEEE 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。これがデフォルト設定です。 force unauthorized：ポートが無許可ステートのままになり、サプリカントからの認証の試みをすべて無視します。デバイスは、このポートを介してサプリカントに認証サービスを提供することはできません。
ステップ 9	**dot1x pae [supplicant | authenticator | both]** 例： `Device(config-if)# dot1x pae authenticator`	
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

スイッチ ポートでの 802.1x の確認

次の show コマンドは、スイッチ ポートでの 802.1x の認証状態を表示します。

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version      2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                         = AUTHENTICATOR
PortControl                 = AUTO
ControlDirection            = Both
HostMode                    = MULTI_HOST
ReAuthentication            = Disabled
QuietPeriod                 = 60
ServerTimeout               = 30
SuppTimeout                 = 30
ReAuthPeriod                = 3600 (Locally configured)
ReAuthMax                   = 2
MaxReq                      = 2
TxPeriod                    = 30
RateLimitPeriod             = 0
Device#
```

認証タイプの確認

次の show コマンドは、AP プロファイルの認証状態を表示します。

```
Device#show ap profile <profile-name> detailed ?
  chassis  Chassis
  |        Output modifiers
  <cr>

Device#show ap profile <profile-name> detailed

  AP Profile Name        : default-ap-profile
  Description            : default ap profile
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port
auth
```