



## 802.1X

---

この章は、次の項で構成されています。

- [802.1X の概要 \(1 ページ\)](#)
- [ホスト サポート \(1 ページ\)](#)
- [認証モード \(2 ページ\)](#)
- [注意事項と制約事項 \(3 ページ\)](#)
- [コンフィギュレーションの概要 \(4 ページ\)](#)
- [NX-OS スタイル CLI を使用した 802.1X ノード認証の設定 \(7 ページ\)](#)
- [REST API を使用した 802.1X ポート認証の設定 \(8 ページ\)](#)
- [REST API を使用した 802.1X ノード認証の設定 \(9 ページ\)](#)

### 802.1X の概要

802.1X では、クライアント サーバベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL) トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

RADIUS 分散クライアント/サーバシステムを使用すると、不正アクセスからネットワークを保護できます。Cisco ACI 実装では、RADIUS クライアントは ToR で稼働し、すべてのユーザー認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウントング要求を送信します。

### ホスト サポート

802.1X 機能は、次のモードでポート上のトラフィックを制限できます。

- **単一ホストモード**：802.1Xポートで1台のエンドポイントデバイスのみからのトラフィックが許可されます。エンドポイントデバイスが認証されると、APICはポートを許可状態にします。エンドポイントデバイスがログオフすると、OSはポートを無許可状態に戻します。802.1Xのセキュリティ違反とは、認証に成功して許可された単一のMACアドレスとは異なるMACアドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティアソシエーション（SA）違反（他のMACアドレスからのEAPOLフレーム）が検出されたインターフェイスはディセーブルにされます。シングルホストモードは、ホストツースイッチ型トポロジで1台のホストがAPICのレイヤ2ポート（イーサネットアクセスポート）またはレイヤ3ポート（ルーテッドポート）に接続されている場合にだけ適用できます。
- **複数のホストモード**：ポートごとに複数のホストを使用できますが、最初の1つだけが認証されます。最初のホストの許可に成功すると、ポートは許可状態に移行します。ポートが許可状態になると、後続のホストがネットワークアクセスの許可を受ける必要はありません。再認証に失敗したり、またはEAPOLログオフメッセージを受信して、ポートが無許可状態になった場合には、接続しているすべてのクライアントはネットワークアクセスを拒否されます。マルチホストモードでは、SA違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。このモードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます
- **マルチ認証モード**：複数のホストとすべてのホストを個別に認証を使用できます。



(注) 各ホストには、同じ EPG/VLAN 情報を必須です。

- **マルチドメインモード**：別のデータおよび音声ドメイン。IP電話で使用します。

## 認証モード

ACI 802.1x は次の認証モードをサポートしています。

- **EAP**：オーセンティケータはEAP-Request/Identityフレームをサブリカントに送信して識別情報を要求します（通常、オーセンティケータは1つまたは複数の識別情報の要求のあとに、最初のIdentity/Requestフレームを送信します）。サブリカントはフレームを受信すると、EAP-Response/Identityフレームで応答します。
- **MAB**：フォールバック認証モードとしてMAC認証バイパス（MAB）がサポートされています。MABにより、エンドポイントのMACアドレスを使用してポートベースのアクセスコントロールが有効になります。MABが有効なポートは接続するデバイスのMACアドレスに基づいて、動的に有効または無効にできます。MABの前に、エンドポイントのIDが不明であり、すべてのトラフィックがブロックされます。スイッチでは、単一のパケットを検査して送信元MACアドレスを学習および認証します。MABが成功するとエンドポイントのIDが判明し、エンドポイントからのすべてのトラフィックが許可されます。スイッチは送信元MACアドレスフィルタリングを実行し、MABの認証されたエンドポイントのみがトラフィックの送信を許可されます。

## 注意事項と制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- Cisco ACI が 802.1X 認証をサポートするのは、物理ポート上だけです。
- Cisco ACI は、ポートチャネルまたはサブインターフェイスでは 802.1X 認証をサポートしません。
- Cisco ACI は、ポートチャネルのメンバポートでは 802.1X 認証をサポートしますが、ポートチャネル自体ではサポートしません。
- 802.1X 設定を含むメンバポートと含まないメンバポートはポートチャネルで共存できません。ただし、チャネリングと 802.1X が連携して動作するためには、すべてのメンバポートで 802.1X 設定を同一にする必要があります。
- 802.1X 認証を有効にした場合、サブリカントが認証されてから、イーサネットインターフェイス上のレイヤ 2 またはレイヤ 3 のすべての機能が有効になります。
- 802.1X は、EX または FX タイプのリーフシャーシでのみサポートされています。
- 802.1X は、ファブリックアクセスポートでのみサポートされています。802.1X は、ポートチャネルまたは仮想ポートチャネルではサポートされていません。
- IPv6 は、dot1x クライアント 3.2(1) リリースではサポートされていません。
- 特に特定のインターフェイス設定（ホストモードおよび認証タイプ）がそのリリースでサポートされていない場合に以前のリリースにダウングレードすると、dot1x 認証タイプはデフォルトでなしになります。ホストモードは希望に応じて単一のホストか複数のホストのどちらかに手動で再設定する必要があります。これで、ユーザーがそのリリースでのみサポートされているモード/認証タイプを設定し、サポートされていないシナリオで実行していないことを確認します。
- マルチ認証では、1 音声クライアントと複数のデータクライアント（すべて同じデータ vlan/epg に属する）をサポートします。
- 802.1X ノード認証ポリシーでの障害 epg/vlan は必須設定です。
- 1 音声および 1 データクライアント以上のマルチドメインは、ポートをセキュリティ無効の状態にします。
- 次のプラットフォームでは 802.1X はサポートされていません。
  - N9K-C9396PX
  - N9K-M12PQ
  - N9K-C93128TX
  - N9K-M12PQ

- 強力な暗号化が有効になっている ACI ファブリックで 802.1x を使用すると、証明書を含む IP パケットが 1500 バイトを超えることがあります。アウトオブバンド (OOB) インターフェイスを介してオーセンティケータに到達できるように構成すると、パケットは自動的にフラグメント化されます。ただし、ACI ファブリックはパケットのフラグメント化をサポートしていません。インバンド管理の使用時に 1500 バイトを超えるパケットの転送を許可するには、次の 2 つのオプションを使用します。

- **[コントロールプレーンの MTU の変更 (Control Plane MTU Change)]**: コントロールプレーンの MTU 設定を調整します。詳細な手順については、『Cisco APIC システム管理構成ガイド』を参照してください。



(注) これは、他のすべてのプロトコルでも使用されるグローバルなファブリック全体の値です。

- **ジャンボ MTU サポートの確認**: 経路上のすべてのデバイスがジャンボ MTU パケットを転送できることを確認してください。

## コンフィギュレーションの概要

APIC で有効になっている場合にのみ、802.1X および RADIUS プロセスが開始されます。内部的にこれは、radius エンティティの作成時に 802.1X Inst MO が作成され radius プロセスが作成されたときに、dot1x プロセスが開始されることを意味します。そのインターフェイスに接続しているユーザーを認証するため、Dot1x ベースの認証が各インターフェイスで有効になっている必要があります。そうでない場合、動作が変更されません。

RADIUS サーバの設定は、dot1x 設定とは別に行われます。RADIUS の設定は、RADIUS サーバのリストとそれらに到達する方法を定義します。Dot1x 設定には、認証に使用する RADIUS グループ (またはデフォルト グループ) への参照が含まれています。

正常に認証を行うには 802.1X と RADIUS の両方を設定する必要があります。設定の順序は重要ではありませんが、RADIUS 設定がない場合は、802.1X 認証は正常に行われません。

## APIC GUI を使用した 802.1X ポート認証の設定

始める前に

RADIUS プロバイダのポリシーを設定します。

## 手順

**ステップ 1** メニューバーで、**[Fabric] > [External Access Policies] > [Policies] > [Interface] > [802.1X Port Authentication]** をクリックし、次の操作を行います。

- a) [802.1X Port Authentication] を右クリックして、[Create 802.1X Port Authentication Policy] を開きます。
- b) [Name] フィールドにポリシーの名前を入力します。
- c) [ホスト モード] フィールドで、ポリシー モードを選択します。使用可能なモードを次に示します。

- [マルチ認証]: 複数のホストおよびすべてのホストを個別に認証できます。

(注)

各ホストには、同じ EPG/VLAN 情報が必須です。

- [マルチ ドメイン]: 別のデータおよび音声ドメインです。IP 電話で使用します。
- [マルチホスト]: ポートごとに複数のホストを使用できますが、最初の1つだけが認証されます。
- [単一ホスト]: ポートごとに1個のホストのみ許可します。

- d) デバイスが 802.1X をサポートしていない場合は、[MAC Auth] フィールドで [EAP\_FALLBACK\_MAB] を選択し、[Submit] をクリックします。

**ステップ 2** 802.1X ポート認証ポリシーをファブリック アクセスグループに関連付けるには、**[Fabric] > [External Access Policies] > [Interfaces] > [Leaf Interfaces] > [Policy Groups] > [Leaf Access Port]** に移動し、次の操作を行います。

- a) [リーフ アクセス ポート] を右クリックして、[リーフ アクセス ポート ポリシー グループの作成] を開きます。
- b) [Name] フィールドにポリシーの名前を入力します。
- c) [802.1X Port Authentication Policy] フィールドで、以前に作成したポリシーを選択し、[Submit] をクリックします。

## APIC GUI を使用した 802.1X ノード認証の設定

始める前に

RADIUS プロバイダのポリシーを設定します。

## 手順

**ステップ 1** メニューバーで、**[Fabric] > [External Access Policies] > [Policies] > [Switch] > [802.1X Node Authentication]** をクリックし、次の操作を行います。

- [802.1X Node Authentication] を右クリックして、[Create 802.1X Node Authentication Policy] を開きます。
- [Name] フィールドにポリシーの名前を入力します。
- [EPG 認証の失敗] フィールドで、認証が失敗した場合に展開するテナント、アプリケーションプロファイル、EPG を選択します。
- [VLAN 認証の失敗] で、認証が失敗した場合に展開する VLAN を選択します。

**ステップ 2** 802.1X ノード認証ポリシーをリーフ スイッチ ポリシー グループに関連付けるには、[Fabric]>[External AccessPolicies]>[Switches]>[Leaf Switches]>[Policy Groups] に移動し、次の操作を行います。

- [ポリシー グループ] を右クリックして、[アクセス スイッチ ポリシー グループの作成] を開きます。
- [Name] フィールドにポリシーの名前を入力します。
- [802.1X Node Authentication Policy] フィールドで、以前に作成したポリシーを選択し、[Submit] をクリックします。

**ステップ 3** 802.1X ノード認証ポリシーをリーフ インターフェイス プロファイルに関連付けるには、[Fabric]>[External AccessPolicies]>[Interfaces]>[Leaf Interfaces]>[Profiles] に移動し、次の操作を行います。

- [プロファイル] を右クリックして、[リーフ インターフェイス プロファイルの作成] を開きます。
- [Name] フィールドにポリシーの名前を入力します。
- [インターフェイス セレクタ] 表を展開し、[アクセス ポートセレクタの作成] ダイアログボックスを開き、[名前] および [インターフェイス ID] 情報を入力します。
- [インターフェイス ポリシー グループ] フィールドで、以前に作成されたポリシーを選択し、[OK] および [送信] をクリックします。

## NX-OS スタイル CLI を使用した 802.1X ポート認証の設定

### 手順

**ステップ 1** ポリシー グループを設定します。

例 :

```
apic1# configure
apic1(config)#
apic1(config)# template policy-group mypol
apic1(config-pol-grp-if)# switchport port-authentication mydot1x
apic1(config-port-authentication)# host-mode multi-host
apic1(config-port-authentication)# no shutdown
apic1(config-port-authentication)# exit
apic1(config-pol-grp-if)# exit
```

**ステップ 2** リーフ インターフェイス ポリシーを設定します。

例 :

```
apic1(config)#
apic1(config)# leaf-interface-profile myprofile
apic1(config-leaf-if-profile)# leaf-interface-group mygroup
apic1(config-leaf-if-group)# interface ethernet 1/10-12
apic1(config-leaf-if-group)# policy-group mypol
```

```
apicl(config-leaf-if-group)# exit
apicl(config-leaf-if-profile)# exit
```

**ステップ3** リーフ プロファイルを設定します。

例：

```
apicl(config)#
apicl(config)# leaf-profile myleafprofile
apicl(config-leaf-profile)# leaf-group myleafgrp
apicl(config-leaf-group)# leaf 101
apicl(config-leaf-group)# exit
```

**ステップ4** リーフ スイッチ プロファイルにインターフェイス ポリシーを適用します。

例：

```
apicl(config-leaf-profile)# leaf-interface-profile myprofile
apicl(config-leaf-group)# exit
```

---

## NX-OS スタイル CLI を使用した 802.1X ノード認証の設定

手順

---

**ステップ1** Radius 認証グループを設定します。

例：

```
apicl# configure
apicl(config)#
apicl(config)# aaa group server radius myradiusgrp
apicl(config-radius)#server 192.168.0.100 priority 1
apicl(config-radius)#exit
```

**ステップ2** ノード レベル ポート認証ポリシーを設定します。

例：

```
apicl(config)# policy-map type port-authentication mydot1x
apicl(config-pmap-port-authentication)#radius-provider-group myradiusgrp
apicl(config-pmap-port-authentication)#fail-auth-vlan 2001
apicl(config-pmap-port-authentication)#fail-auth-epg tenant tn1 application ap1 epg epg256
apicl(config)# exit
```

**ステップ3** ポリシー グループを設定し、グループ内でポート認証ポリシーを指定します。

例：

```
apicl(config)#template leaf-policy-group lpg2
apicl(config-leaf-policy-group)# port-authentication mydot1x
apicl(config-leaf-policy-group)#exit
```

**ステップ4** リーフ スイッチ プロファイルを設定します。

例 :

```
apic1(config)# leaf-profile mylp2
apic1(config-leaf-profile)#leaf-group mylg2
apic1(config-leaf-group)# leaf-policy-group lpg2
apic1(config-leaf-group)#exit
```

## REST API を使用した 802.1X ポート認証の設定

### 手順

802.1X ポート認証ポリシーを作成します。

例 :

```
<polUni>
<infraInfra>
  <l2PortAuthPol adminSt="enabled" annotation="" descr="" dn="uni/infra/portauthpol-test21"
hostMode="multi-auth" name="test21" nameAlias="" ownerKey="" ownerTag="">
  <l2PortAuthCfgPol annotation="" macAuth="bypass" maxReauthReq="2" maxReq="2" reAuthPeriod="3600"
serverTimeout="30" suppTimeout="30" txPeriod="30"/>
  </l2PortAuthPol>
</infraInfra>
</polUni>
```

Modify:

```
<polUni>
<infraInfra>
  <l2PortAuthPol adminSt="enabled" annotation="" descr="" dn="uni/infra/portauthpol-test21"
hostMode="multi-domain" name="test21" nameAlias="" ownerKey="" ownerTag="" >
  <l2PortAuthCfgPol annotation="" macAuth="eap" maxReauthReq="2" maxReq="2" reAuthPeriod="3600"
serverTimeout="30" suppTimeout="30" txPeriod="30"/>
  </l2PortAuthPol>
</infraInfra>
</polUni>
```

Delete:

```
<polUni>
<infraInfra>
  <l2PortAuthPol adminSt="enabled" annotation="" descr="" dn="uni/infra/portauthpol-test21"
hostMode="multi-host" name="test21" nameAlias="" ownerKey="" ownerTag="" status="deleted">
  <l2PortAuthCfgPol annotation="" macAuth="bypass" maxReauthReq="2" maxReq="2" reAuthPeriod="3600"
serverTimeout="30" suppTimeout="30" txPeriod="30" status="deleted"/>
  </l2PortAuthPol>
</infraInfra>
</polUni>
```

# REST API を使用した 802.1X ノード認証の設定

## 手順

---

802.1X ノード認証ポリシーを設定します。

例：

```
<polUni>
<infraInfra>
  <l2NodeAuthPol annotation="" descr="" dn="uni/infra/nodeauthpol-802-node-2"
failAuthEpg="tn-t2,ap-ap,epg-epg1" failAuthVlan="vlan-2078" name="802-node-2" nameAlias="" ownerKey=""
ownerTag="">
<l2RsAaaRadiusProviderGroup annotation="" tDn="uni/userext/radiusext/radiusprovidergroup-radius-grp"/>
</l2NodeAuthPol>
</infraInfra>
</polUni>
```

Modify:

```
<polUni>
<infraInfra>
  <l2NodeAuthPol annotation="" descr="" dn="uni/infra/nodeauthpol-802-node-2"
failAuthEpg="tn-t2,ap-ap,epg-epg1" failAuthVlan="vlan-2066" name="802-node-2" nameAlias="" ownerKey=""
ownerTag="" status="deleted">
<l2RsAaaRadiusProviderGroup annotation="" tDn="uni/userext/radiusext/radiusprovidergroup-radius-grp"/>
</l2NodeAuthPol>
</infraInfra>
</polUni>
```

Delete:

```
<polUni>
<infraInfra>
  <l2NodeAuthPol annotation="" descr="" dn="uni/infra/nodeauthpol-802-node-2"
failAuthEpg="tn-t2,ap-ap,epg-epg1" failAuthVlan="vlan-2078" name="802-node-2" nameAlias="" ownerKey=""
ownerTag="" status="deleted">
<l2RsAaaRadiusProviderGroup annotation="" tDn="uni/userext/radiusext/radiusprovidergroup-radius-grp"
status="deleted"/>
</l2NodeAuthPol>
</infraInfra>
</polUni>
```

---



## 翻訳について

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