Catalyst 1300スイッチのダウンロード可能ACL

目的

この記事の目的は、Cisco Identity Service Engine(ISE)を搭載したCisco Catalyst 1300スイッチで、ダウンロード可能アクセスコントロールリスト(DACL)がどのように機能するかを説明することです。

該当するデバイス|ソフトウェアバージョン

- Catalyst 1300シリーズ| 4.1.6.54

はじめに

ダイナミックACLは、ポリシーまたはユーザアカウントグループメンバーシップ、時間帯などの基準に基づいて、スイッチポートに割り当てられるACLです。これらは、filter-IDまたはdownloadable ACL(DACL)で指定されたローカルACLである可能性があります。

ダウンロード可能ACLは、Cisco ISEサーバから作成およびダウンロードされるダイナミックACLです。ユーザIDとデバイスタイプに基づいて、アクセスコントロールルールを動的に適用するDACLには、ACLの中央リポジトリを1つ作成できるという利点があるため、各スイッチでACLを手動で作成する必要はありません。ユーザがスイッチに接続する際に必要なのは認証だけで、スイッチはCisco ISEサーバから該当するACLをダウンロードします。

ダウンロード可能ACLの使用例

1. ユーザが異なると、スイッチに接続する際に異なるACLを受信します（ローカルISEユーザ）。
2. ネットワーク接続が制限されているユーザは、中央Webポータルにサインインしてフルネットワークアクセスを行うことができます（中央Web認証）。
3. 拡張：MAC認証バイパス(MAB)を使用して、ISEサーバをADに接続し、ユーザ認証を監視しながら、Windows Active Directory(AD)および一部の関連サービスへの通信を可能にします。Windows ADログインの前は、ネットワークでは非常に限られたリソースへのアクセスのみが許可されますが、AD認証ではWindowsグループに基づいて異なるACLがダウンロードされ、完全なネットワークアクセスが許可されます。
4. Advanced:ISEサーバ上のポリシーにより、ユーザは曜日、時刻、またはその他の要因に基づいて異なるACLを受信します。

この記事では、最初の使用例について詳しく説明します。

目次

前提条件

- Catalyst 1300スイッチが最新のファームウェアにアップグレードされていることを確認します（スイッチファームウェアは4.1.6以降である必要があります）。
- 管理目的でスイッチにスタティックIPを割り当てます。

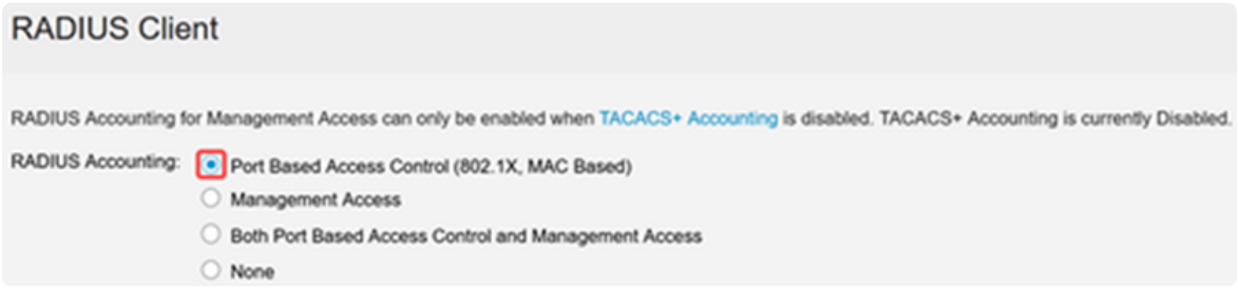
RADIUSクライアントの設定

手順 1

Catalyst 1300スイッチにログインし、Security > RADIUS Clientメニューに移動します。

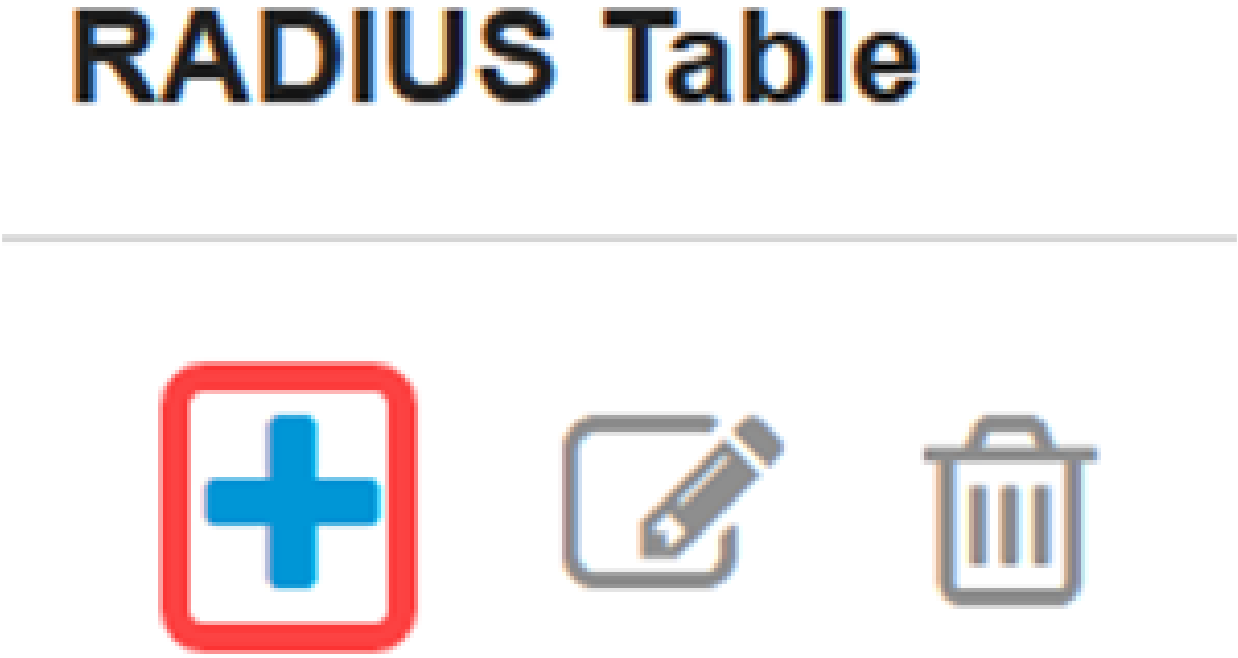
手順 2

RADIUS Accountingでは、Port Based Access Controlオプションを選択します。



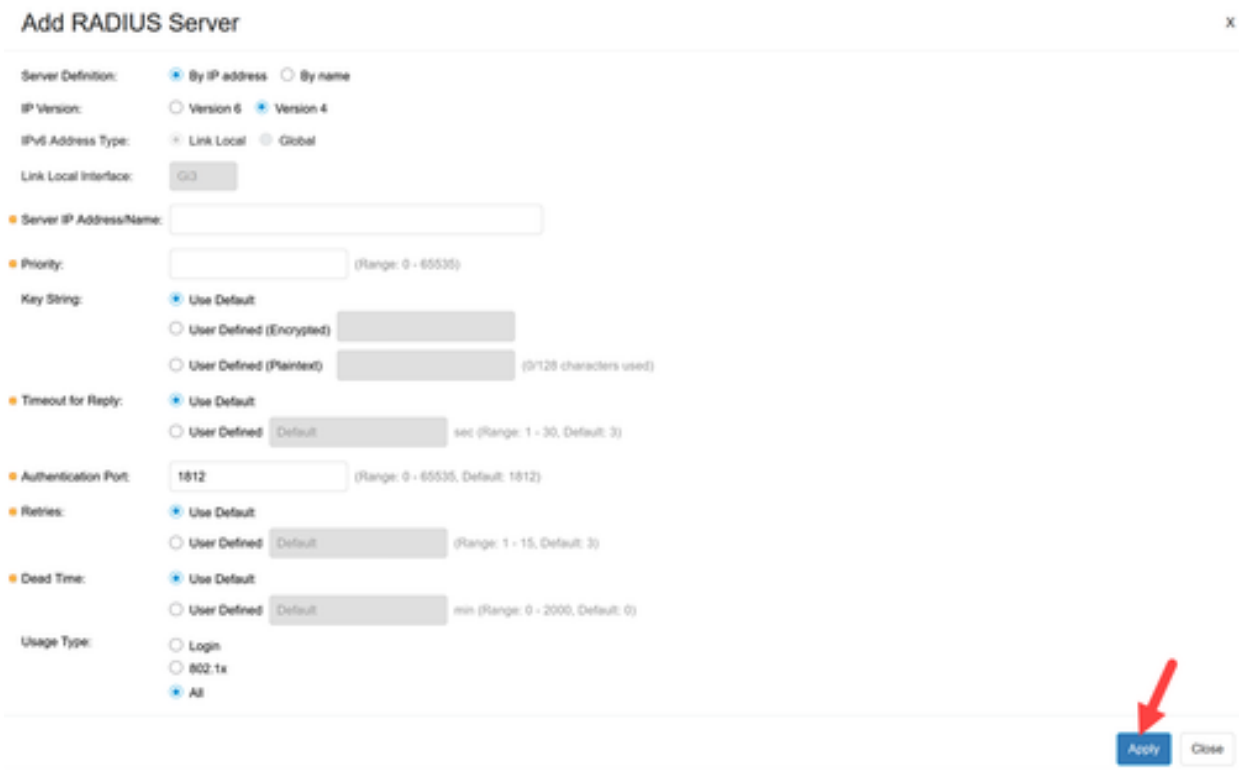
手順 3

RADIUSテーブルの下のプラスアイコンをクリックして、Cisco ISEサーバを追加します。



手順 4

Cisco ISEサーバの詳細を入力し、Applyをクリックします。

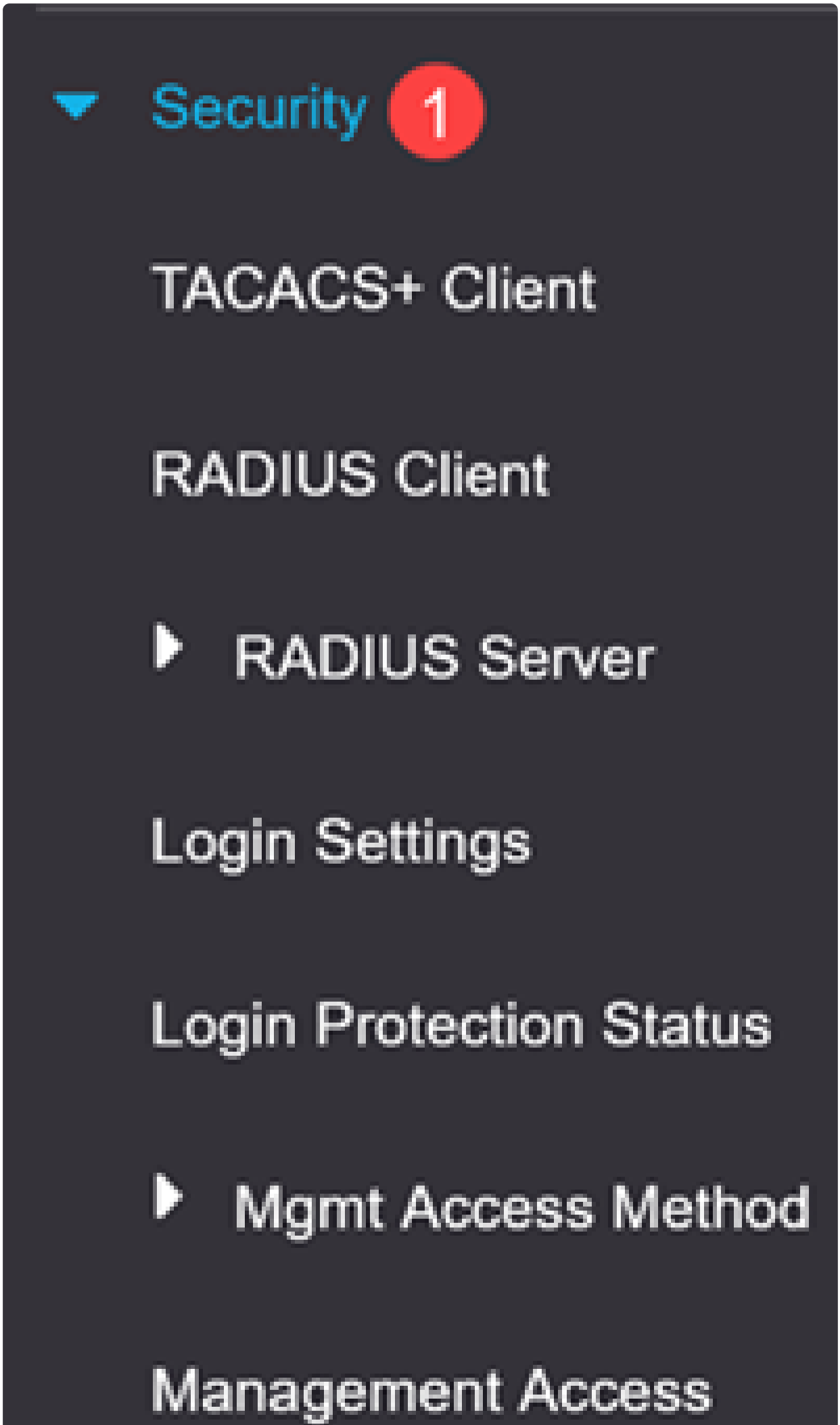


> **Note:**
> Usage Typeは802.1xとして選択する必要があります。

802.1x認証の設定

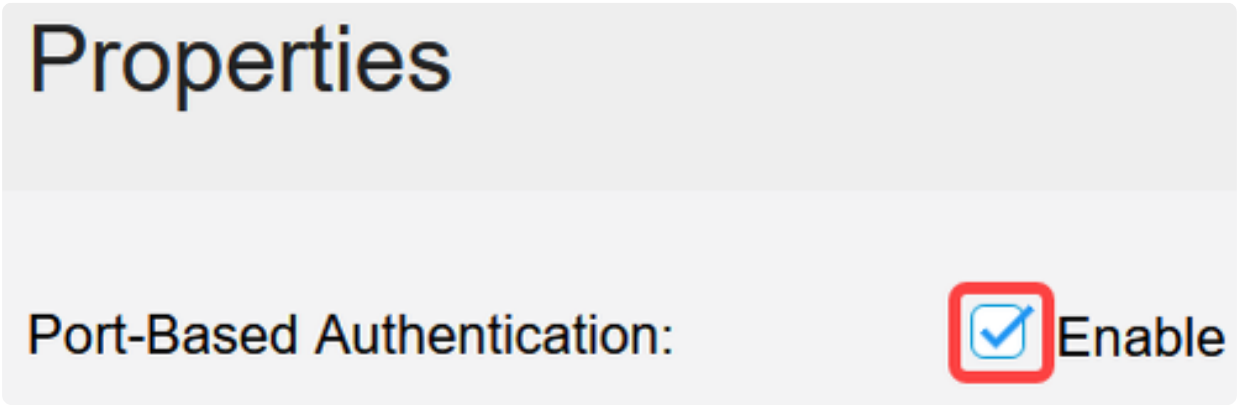
手順 1

Security > 802.1X Authentication > Propertiesメニューの順に移動します。


Security 1
TACACS+ Client
RADIUS Client
RADIUS Server
Login Settings
Login Protection Status
Mgmt Access Method
Management Access

手順 2

ポートベース認証を有効にするには、このチェックボックスをオンにします。

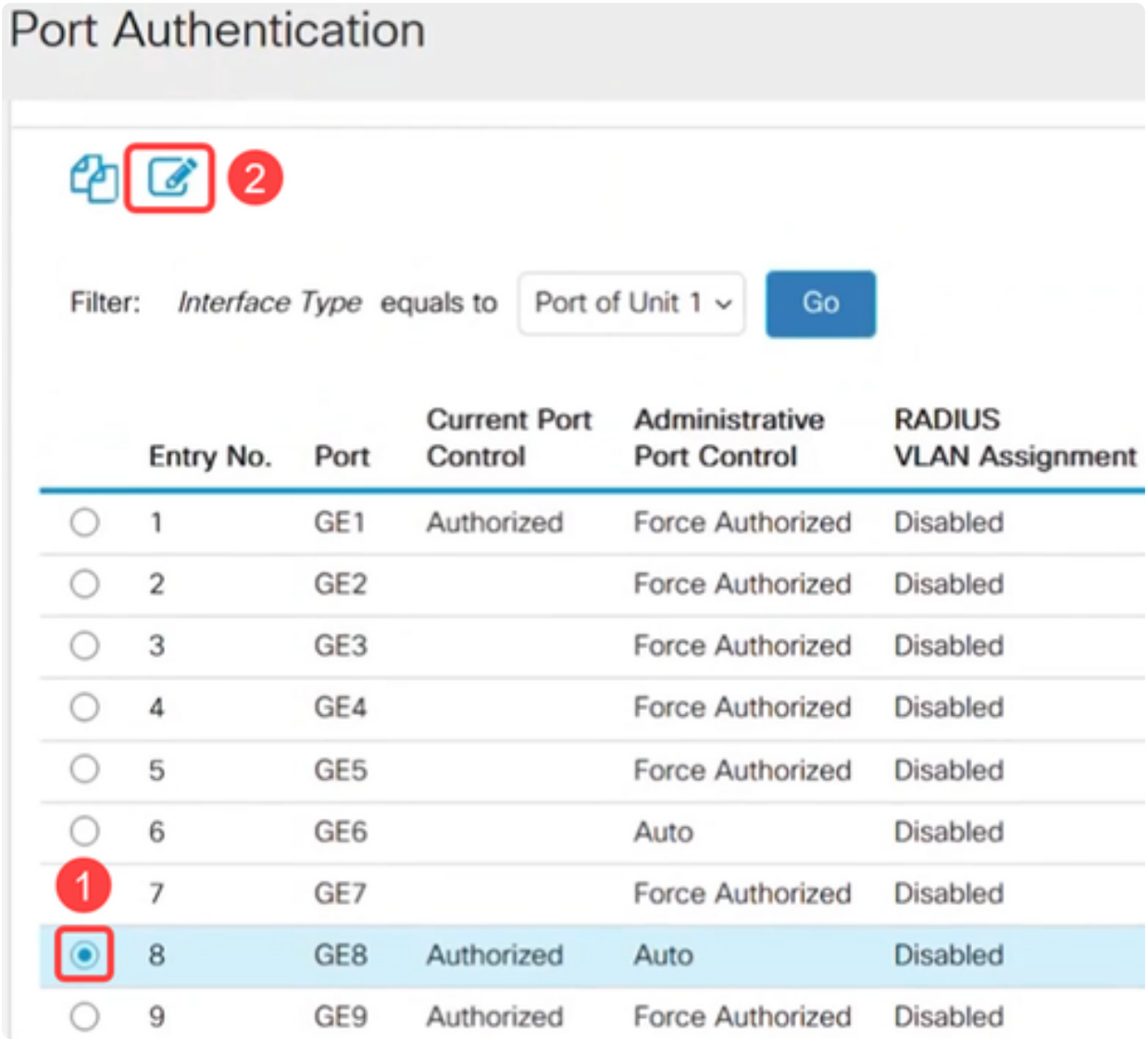


手順 3

Authentication Methodの下で、RADIUSを選択し、Applyをクリックします。

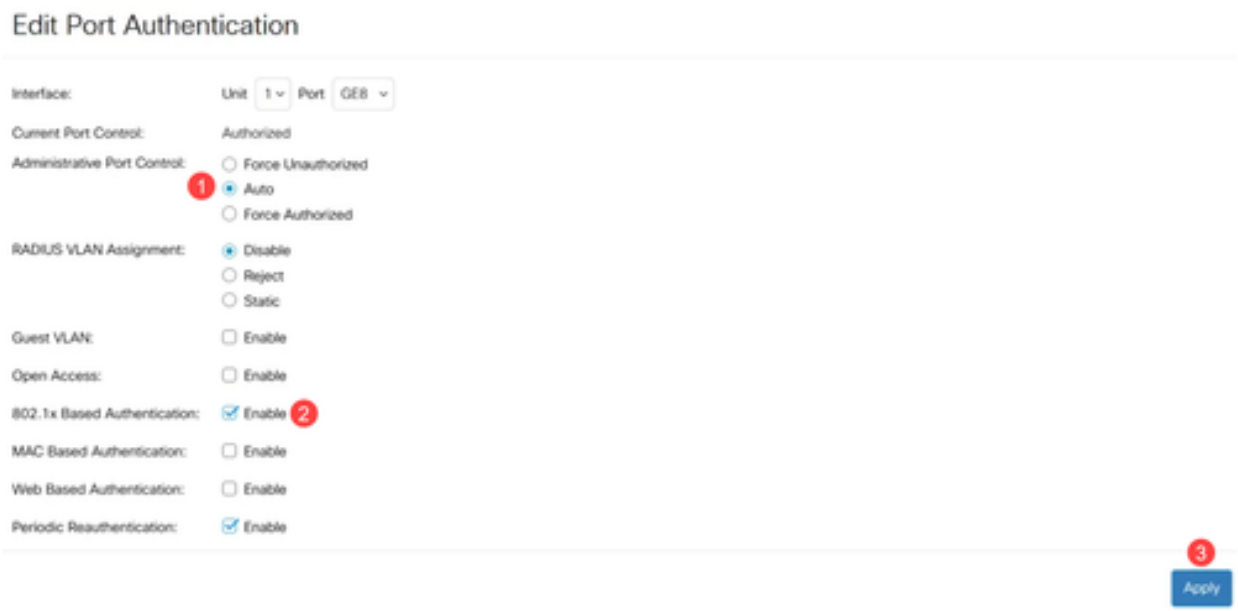
手順 4

Security > 802.1X Authentication > Port Authenticationメニューの順に選択します。ラップトップが接続されているポートを選択し、editアイコンをクリックします。この例では、GE8が選択されています。



手順 5

Administrative Port ControlをAutoとして選択し、802.1xベースの認証をイネーブルにします。[APPLY] をクリックします。



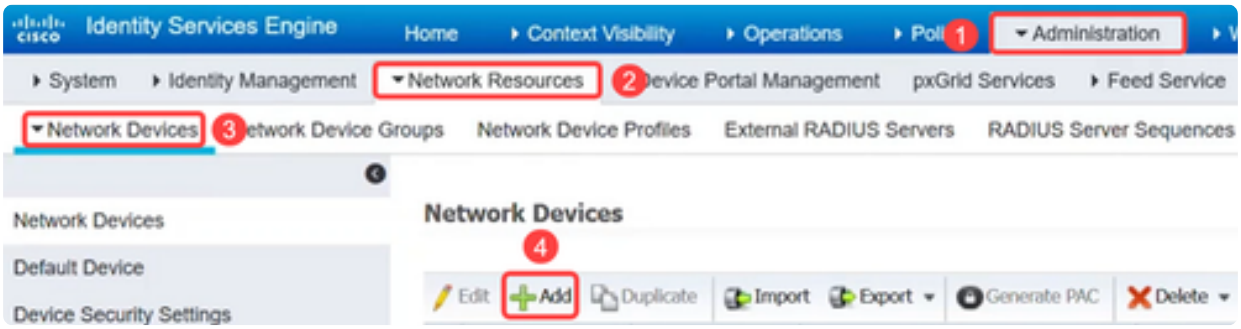
ダウンロード可能ACL用のCisco ISEサーバの設定

> **Note:**
> ISEの設定は、シスコのビジネスサポートの範囲外です。詳細については、『ISE管理ガイド』を参照してください。

この記事に示す設定は、Cisco Catalyst 1300シリーズスイッチで動作するダウンロード可能ACLの例です。

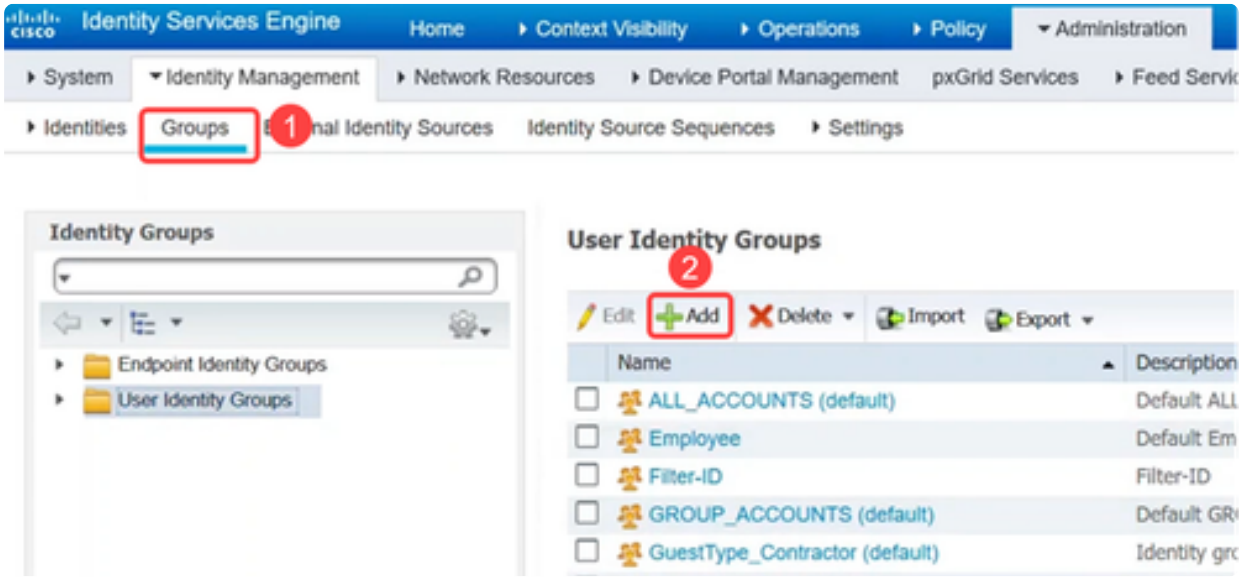
手順 1

Cisco ISEサーバにログインし、Administration > Network Resources > Network Devicesの順に選択して、Catalystスイッチデバイスを追加します。



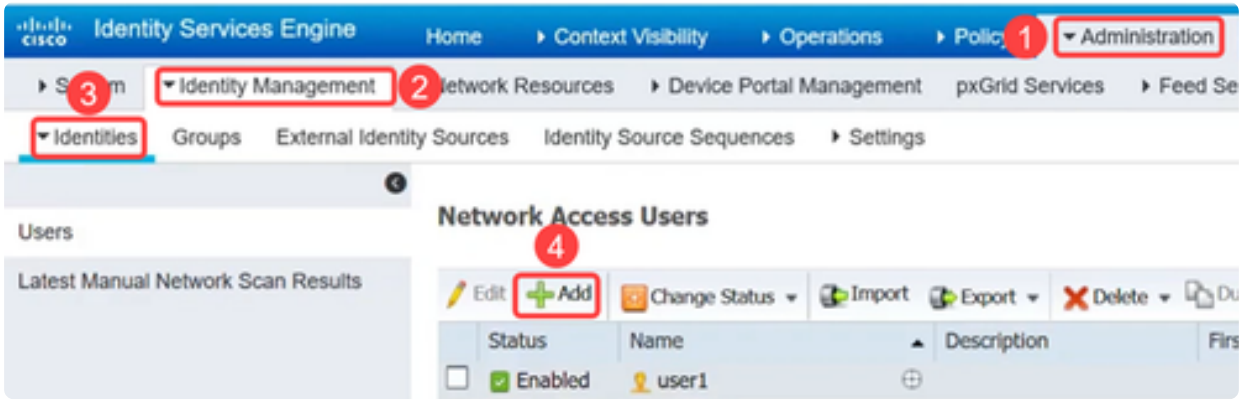
手順 2

ユーザIDグループを作成するには、グループタブに移動し、ユーザIDグループを追加します。



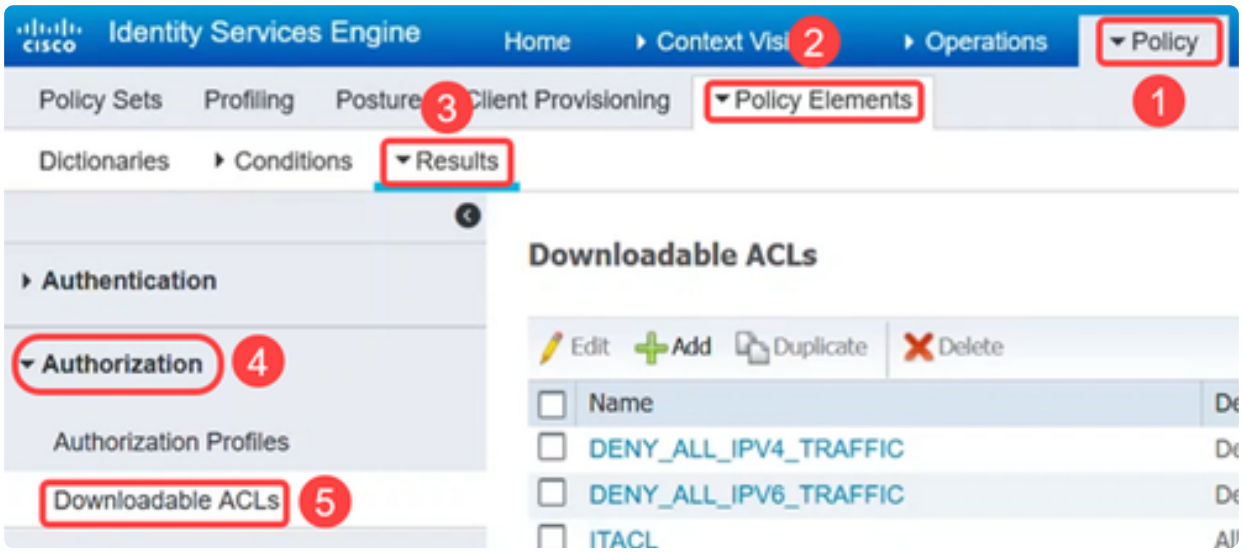
手順 3

Administration > Identity Management > Identitiesメニューに移動し、ユーザを定義して、そのユーザをグループにマッピングします。



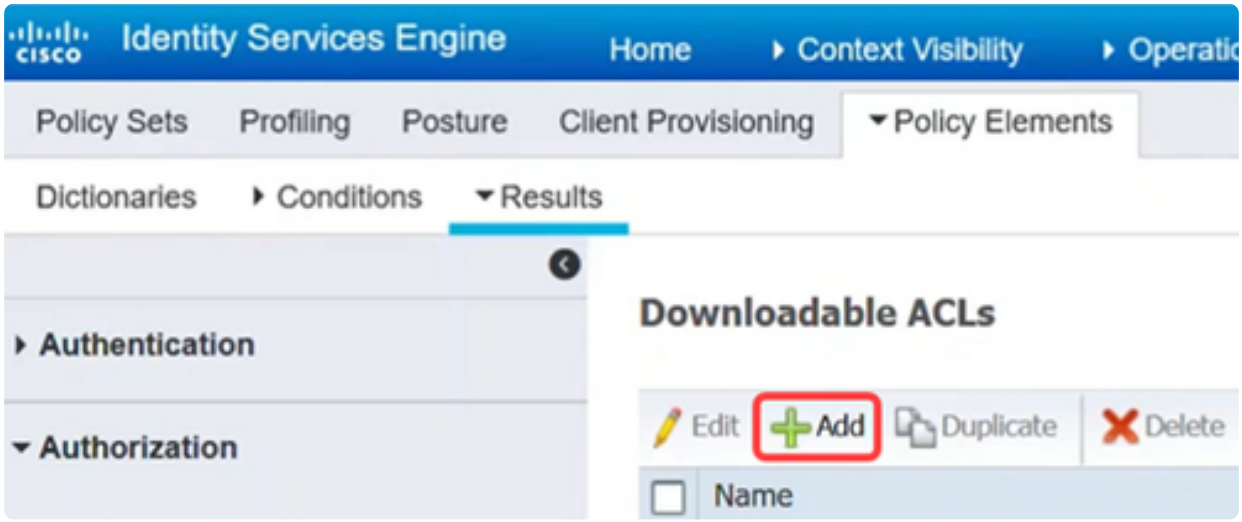
手順 4

Policy > Policy Elements > Resultsメニューに移動します。Authorizationの下で、Downloadable ACLsをクリックします。



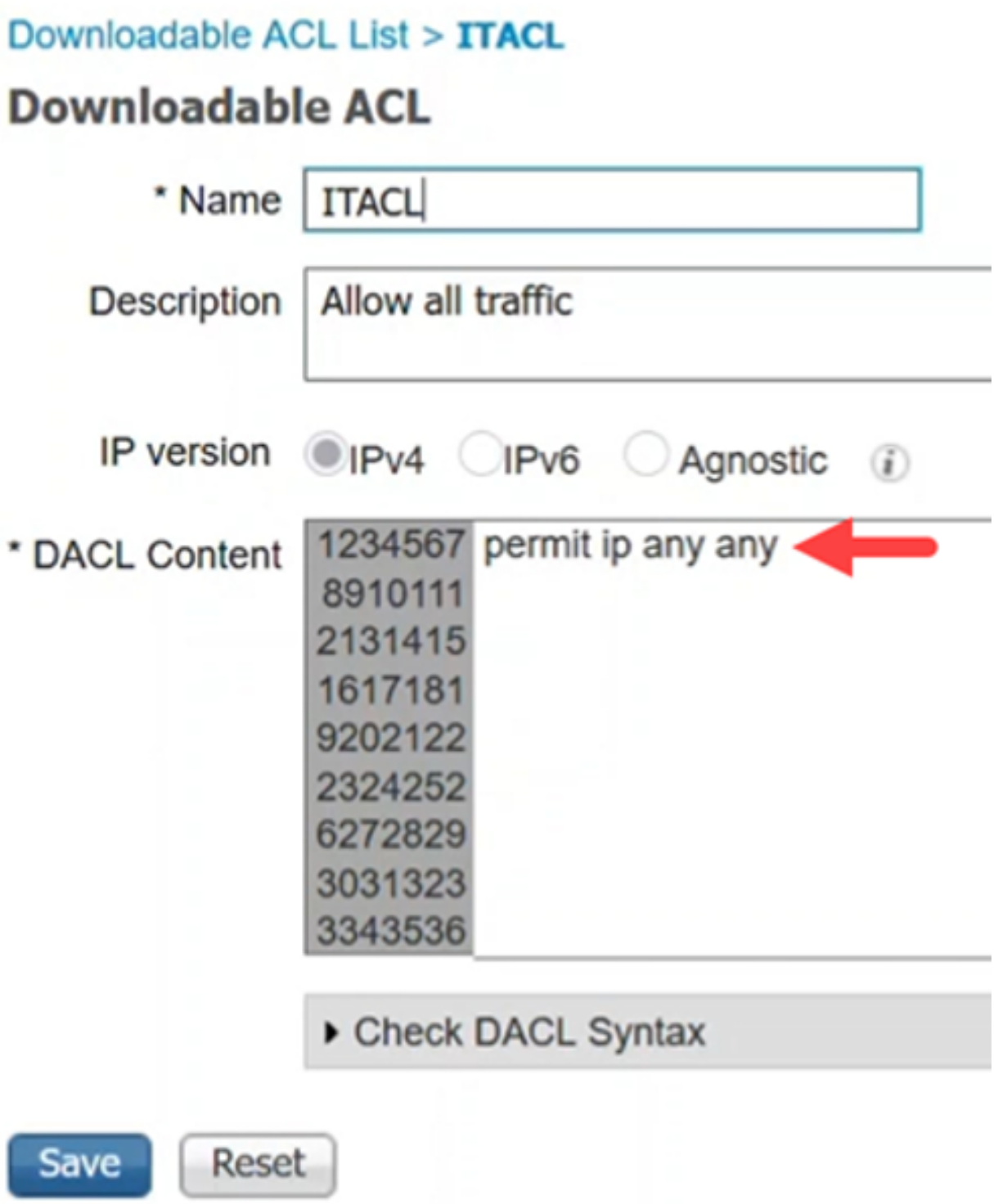
手順 5

Addアイコンをクリックして、ダウンロード可能なACLを作成します。



手順 6

Name, Descriptionを設定し、IPバージョンを選択して、ダウンロード可能ACLを構成するアクセスコントロールエントリ(ACE)をDACL Contentフィールドに入力します。[Save] をクリックします。



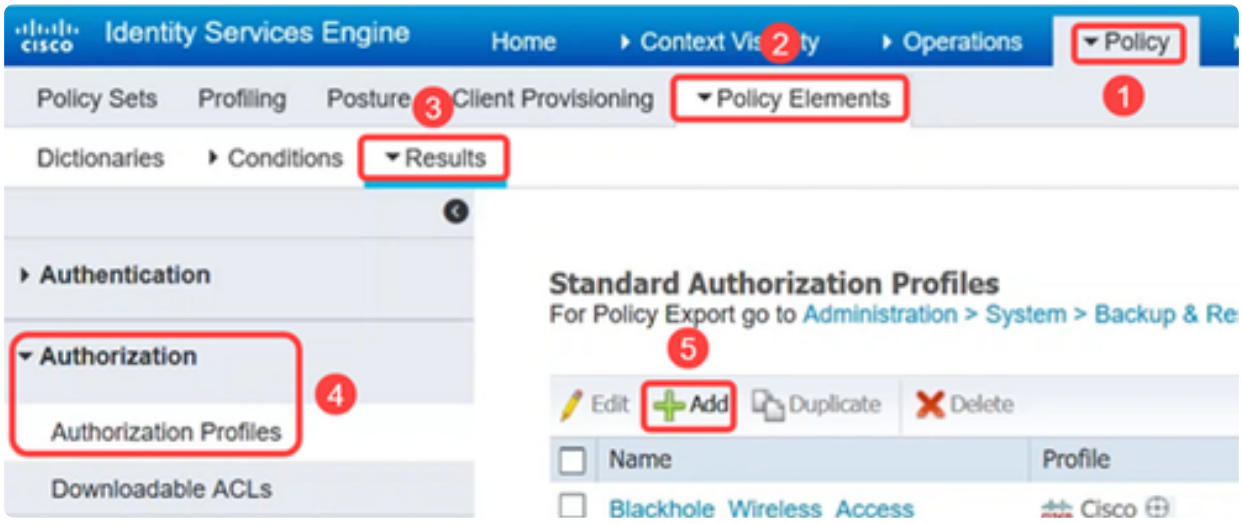
Note:

IP ACLだけがサポートされ、送信元はANYである必要があります。ISEのACLでは、現在IPv4のみがサポートされています。ISEに関する限り構文に問題がなくても、別の送信元を使用してACLを入力すると、スイッチに適用したときにACLが失敗します。

ステップ7

DACLと他のポリシーをISEポリシーセット内で論理的に関連付けるために使用される認可プロファイルを作成します。

これを行うには、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動し、Addをクリックします。

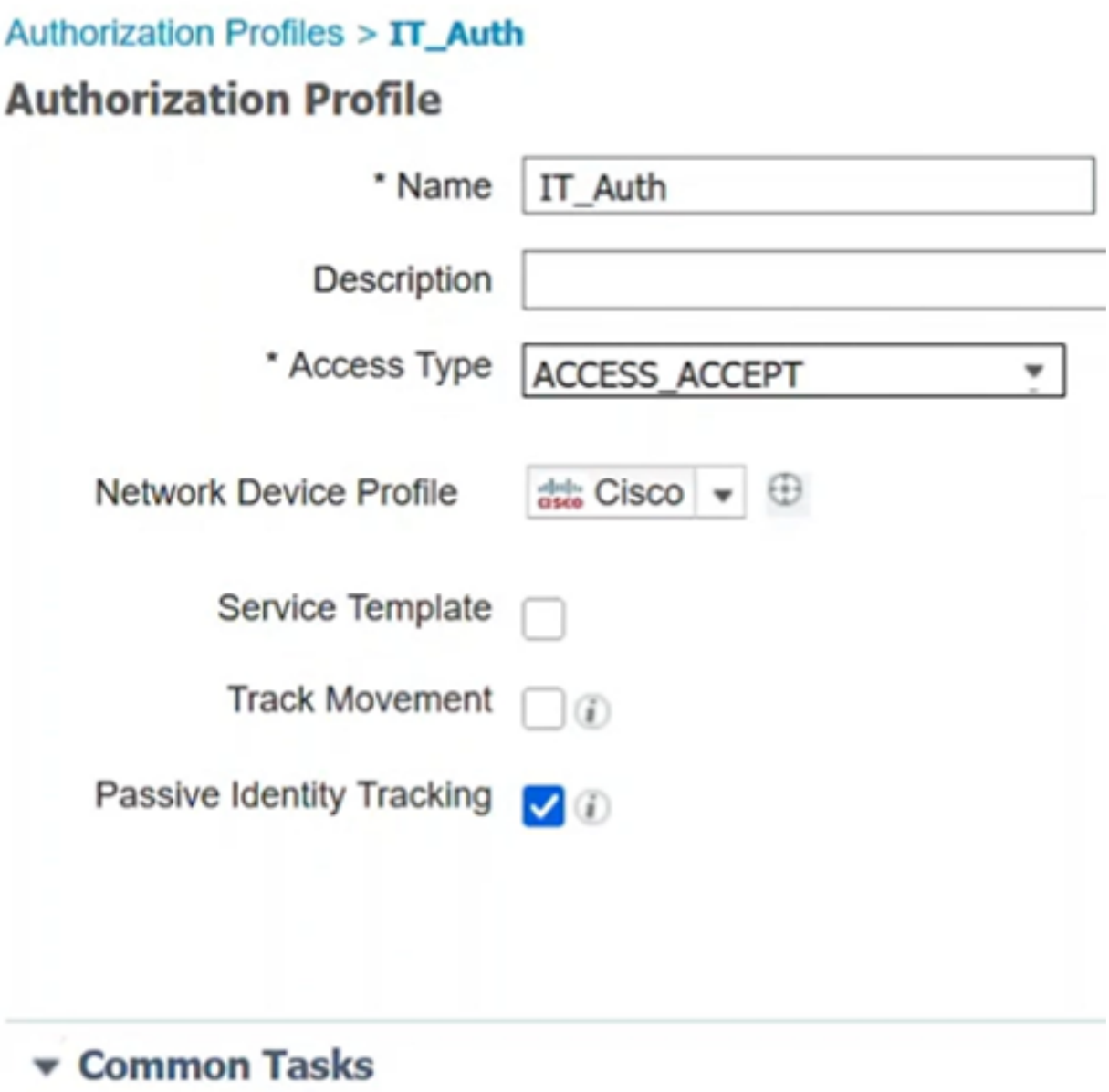


手順 8

Authorization Profileページで、次のように設定します。

- [名前(Name)]
- 説明
- Access Type：これはACCESS_ACCEPTに設定する必要があります。ACCESS_REJECTに設定すると、認証を拒否します。
- Network Device Profile：これはCiscoとして選択する必要があります。
- パッシブIDトラッキング：認証シナリオによっては有効にすることが必要な場合があります。これは、ADにリンクされているEasyConnect_PassiveIDのシナリオで必要です。
- 共通タスク：このセクションには多くのオプションがあります。この例では、DACL Nameが設定されています。

[Save] をクリックします。



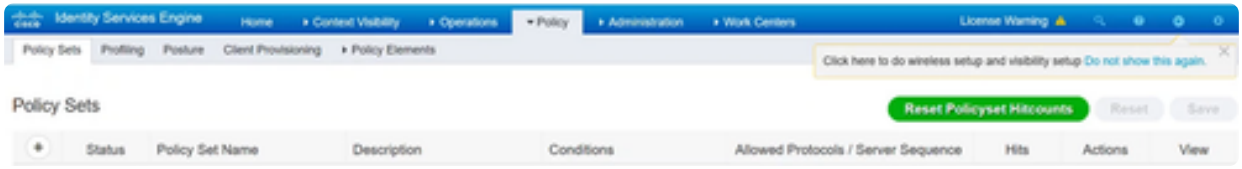
手順 9

認証ポリシーと認可ポリシーの論理グループであるポリシーセットを設定するには、Policy > Policy Setsメニューをクリックします。

ポリシーセットのリストを表示すると、次の項目を確認できます。

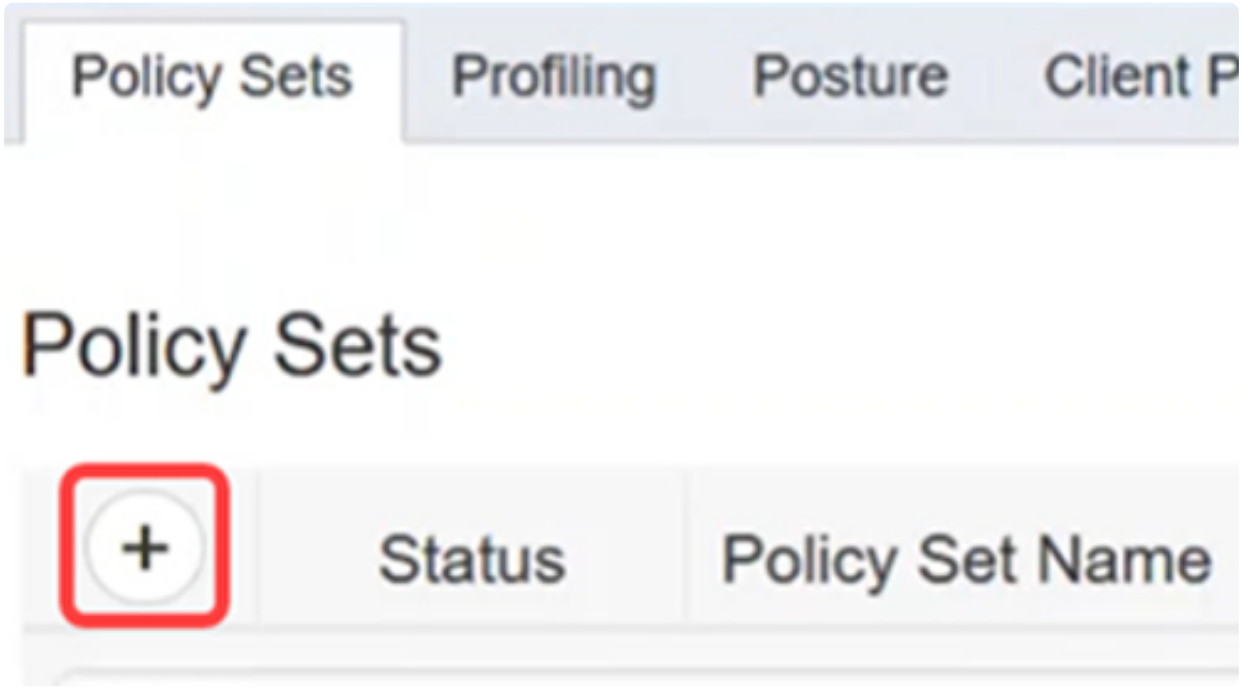
- ステータス：緑色のチェックマークは有効であることを示し、空の白い円は無効であることを示し、目のアイコンはモニタのみの構成であることを示します。
- ポリシーセットの名前と説明：読んで字のとおりです。
- 条件：ポリシーセットを適用する場所を定義します。
- Allowed Protocols/Server Sequence：より高度な制御を設定します。
- Hits：ポリシーセットが使用された回数を示します。
- アクション：ポリシーセットを適用できる順序の変更、既存のポリシーセットのコピー、または既存のポリシーセットの削除を行うことができます。

- 表示：ポリシーセットの詳細を編集できます。



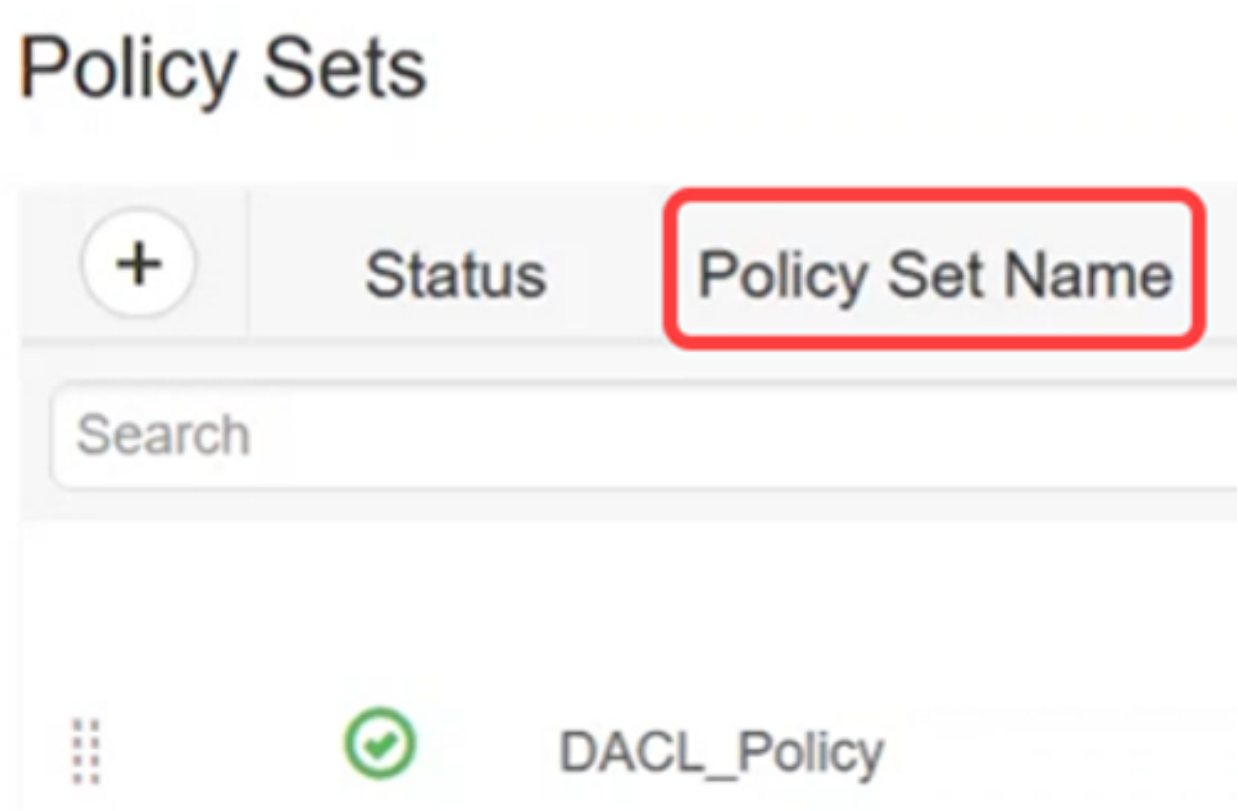
手順 10

ポリシーセットを作成するには、addボタンをクリックします。



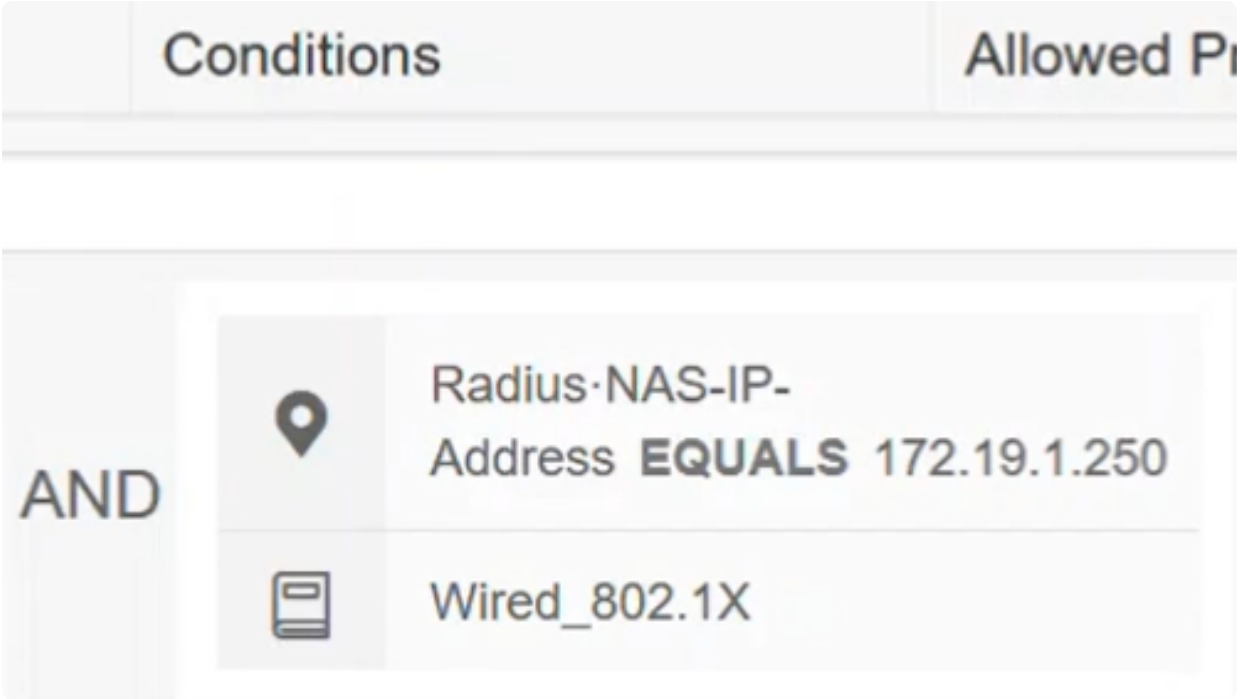
手順 11

ポリシーセット名を定義する



手順 12

Conditionsの下で、addボタンをクリックします。これにより、Conditions Studioが開き、この認証プロファイルを使用する場所を定義できます。この例では、172.19.1.250およびwired_802.1xトラフィックのRadius-NAS-IP-Address（スイッチ）に適用されています。

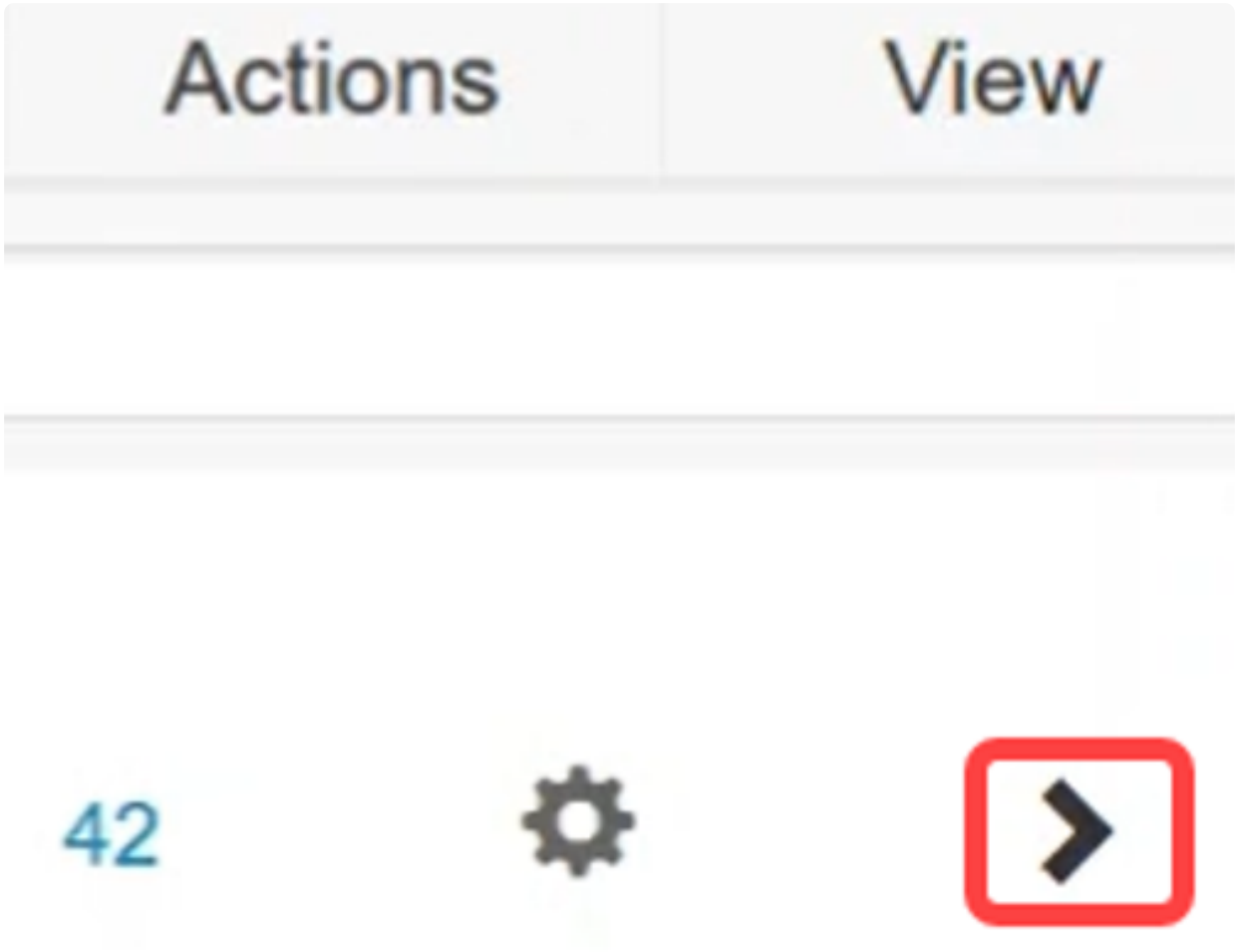


手順 13

Allowed ProtocolsをDefault Network Accessに設定して、Saveをクリックします。

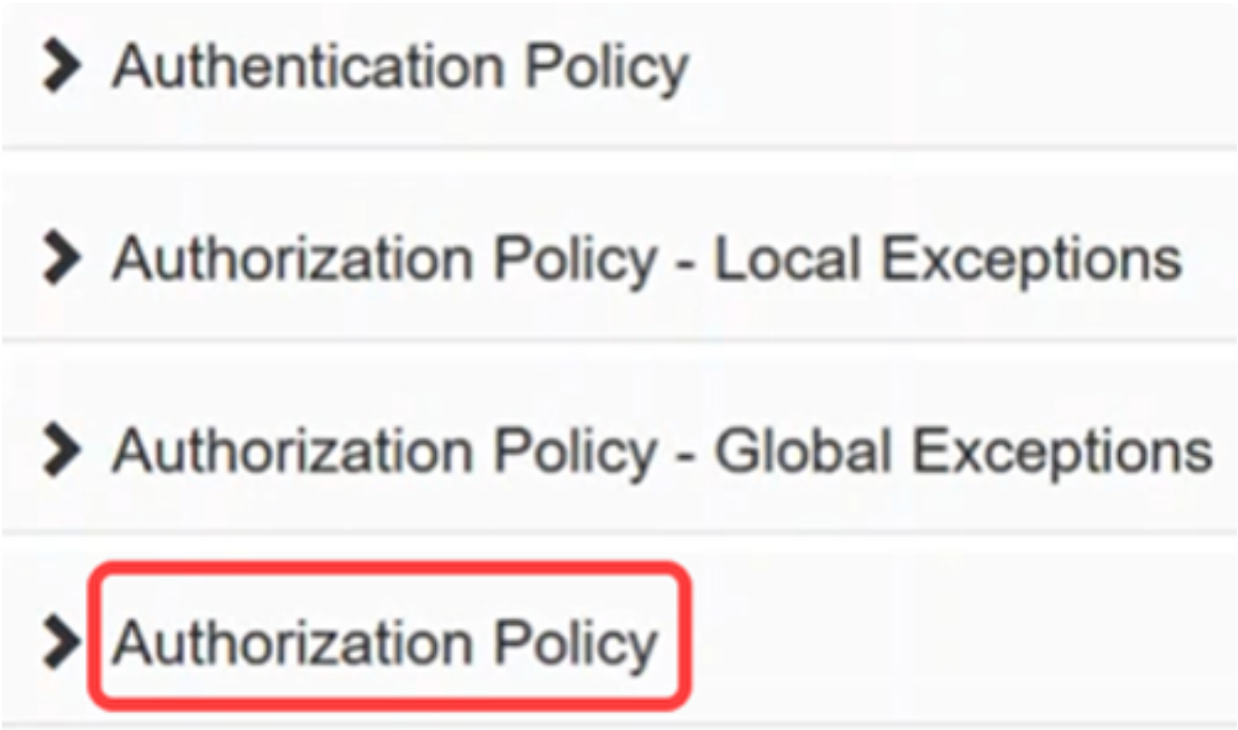
手順 14

Viewの下にある矢印アイコンをクリックして、ネットワークの設定と要件に基づいて認証ポリシーと認可ポリシーを設定するか、デフォルト設定を選択できます。この例では、Authorization policyをクリックします。



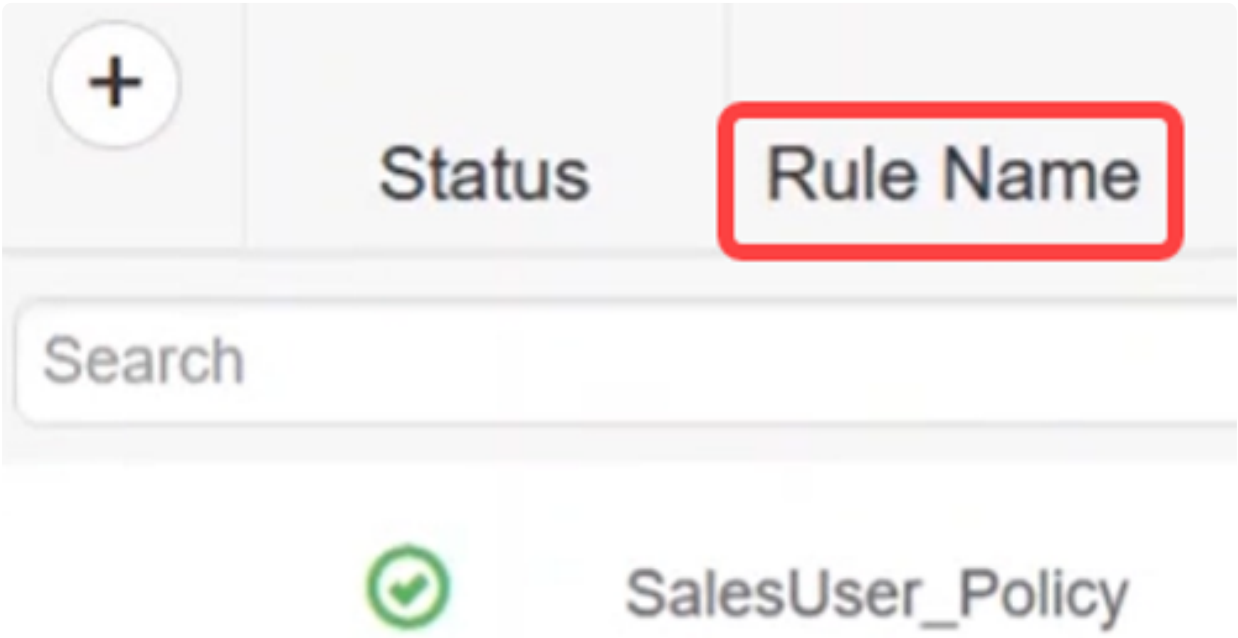
手順 15

プラスアイコンをクリックして、ポリシーを追加します。



手順 16

Rule Nameを入力します。



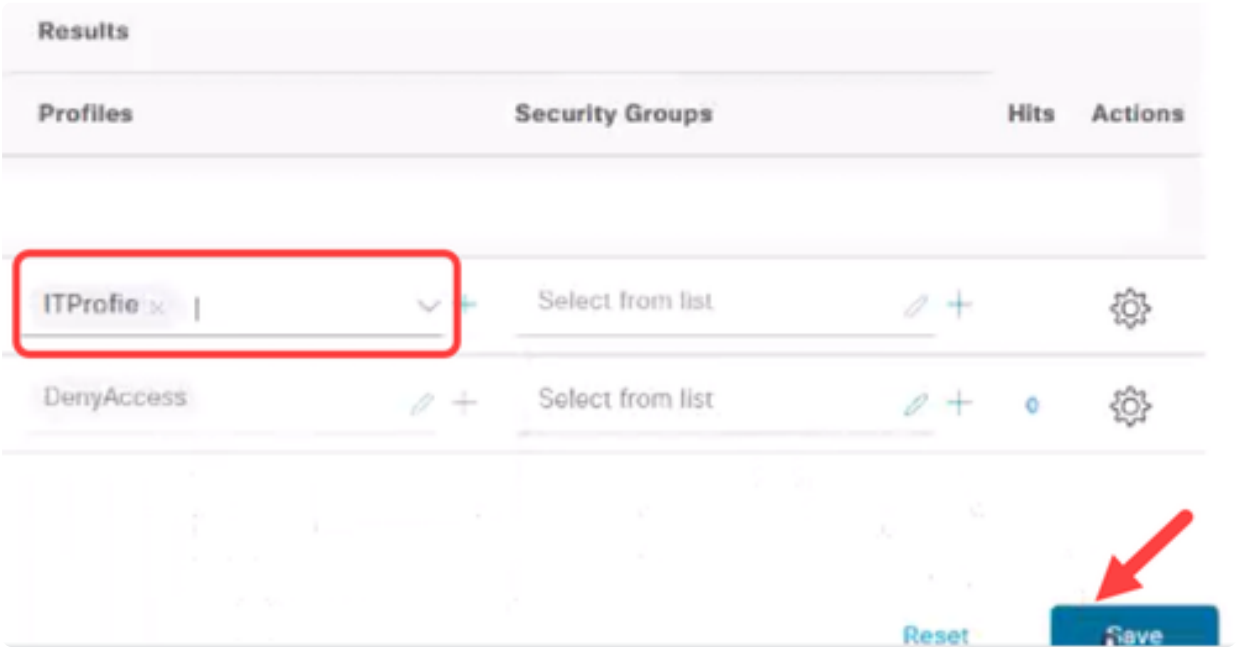
手順 17

Conditionsの下で、plusアイコンをクリックして、アイデンティティグループを選択し

ます。Useをクリックします。

手順 18

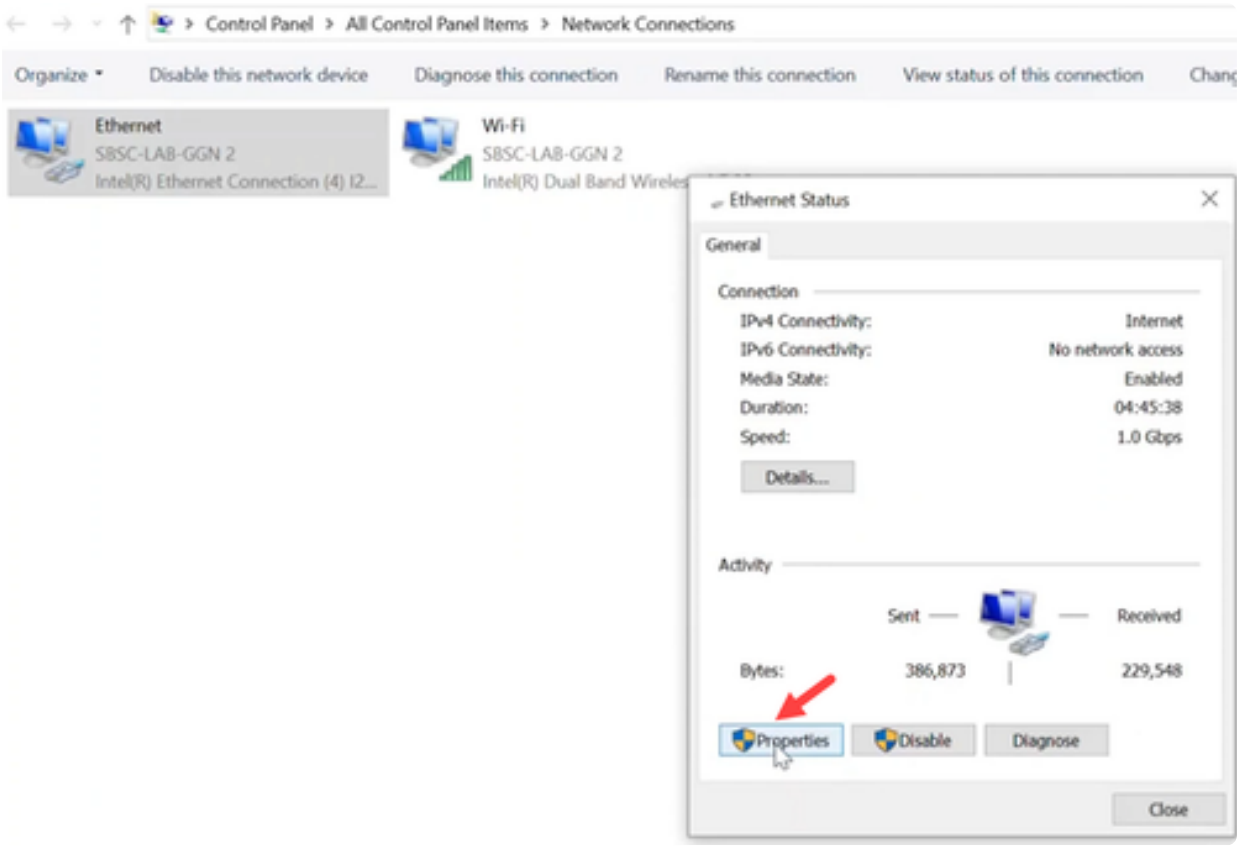
必要なプロファイルを適用し、Saveをクリックします。



クライアントの設定

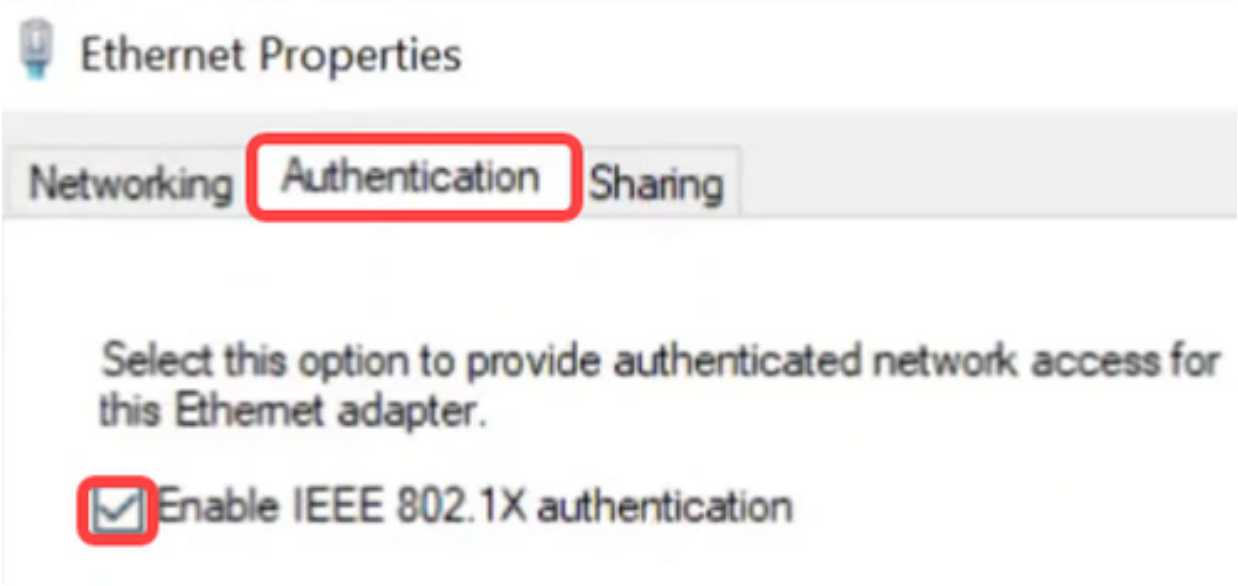
手順 1

クライアントラップトップで、Network Connections > Ethernetの順に移動し、Propertiesをクリックします。



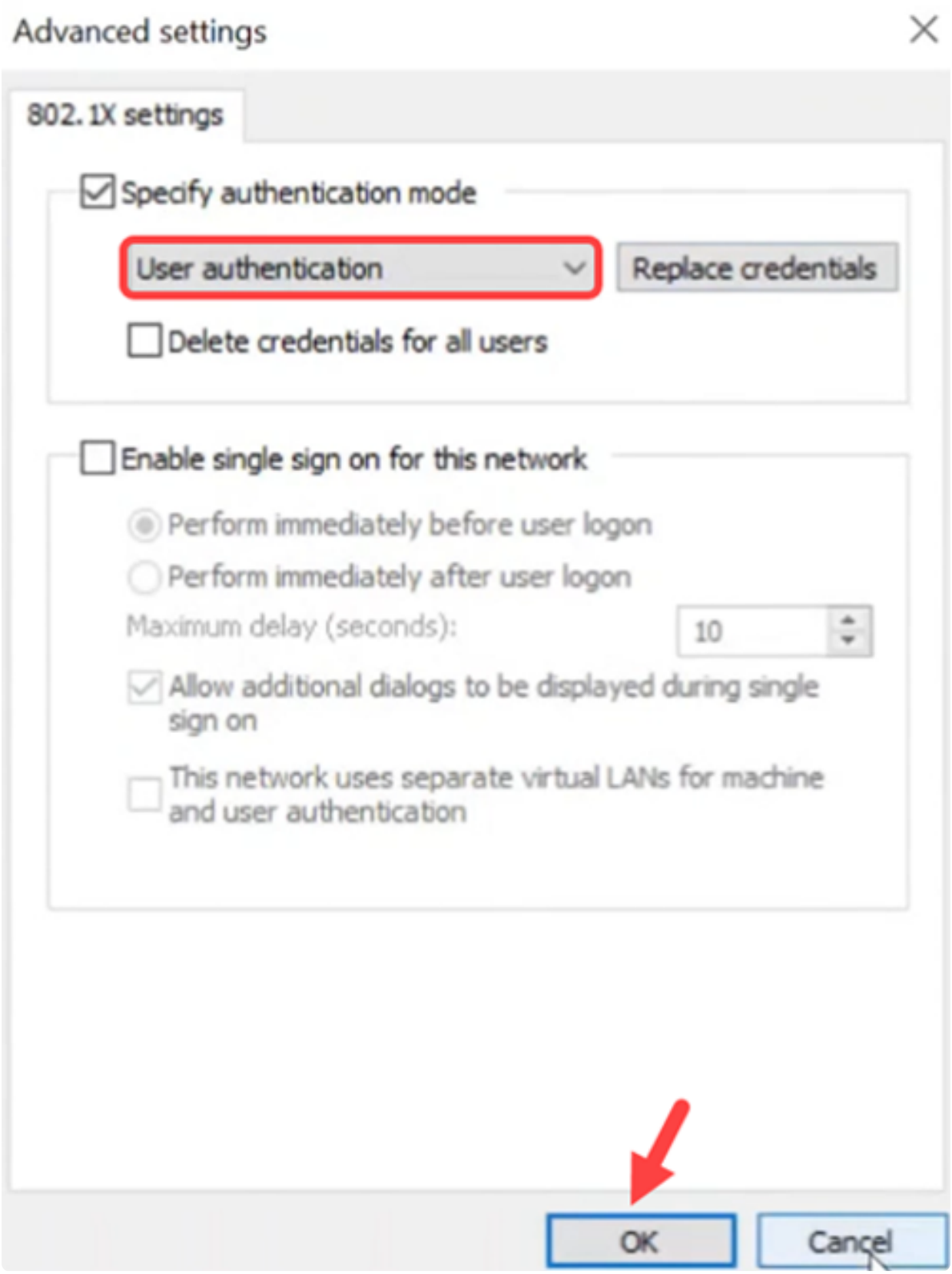
手順 2

Authenticationタブをクリックし、802.1X authenticationがイネーブルになっていることを確認します。



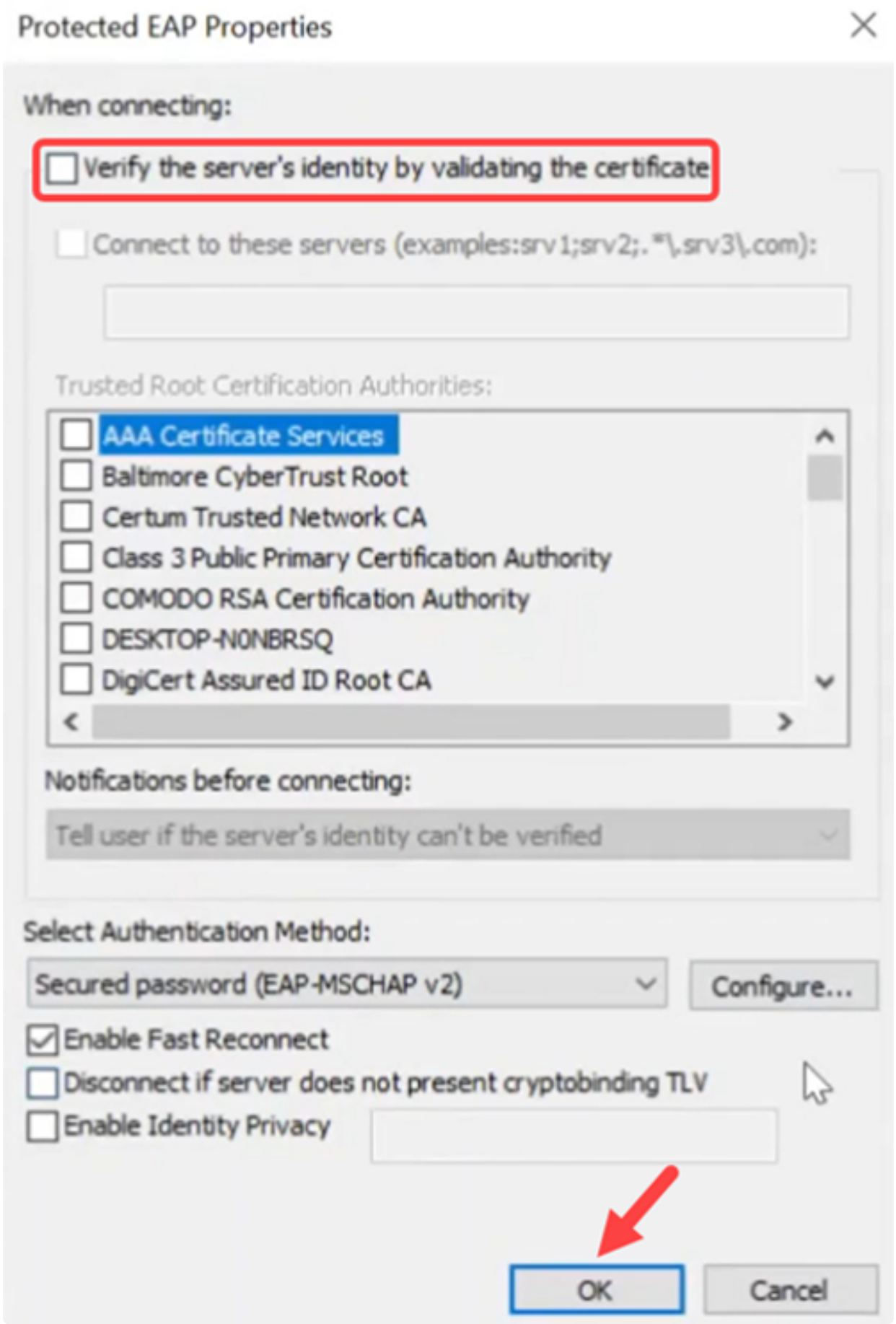
手順 3

Additional Settingsで、認証モードとしてUser authenticationを選択します。Save Credentialsをクリックし、次にOKをクリックします。



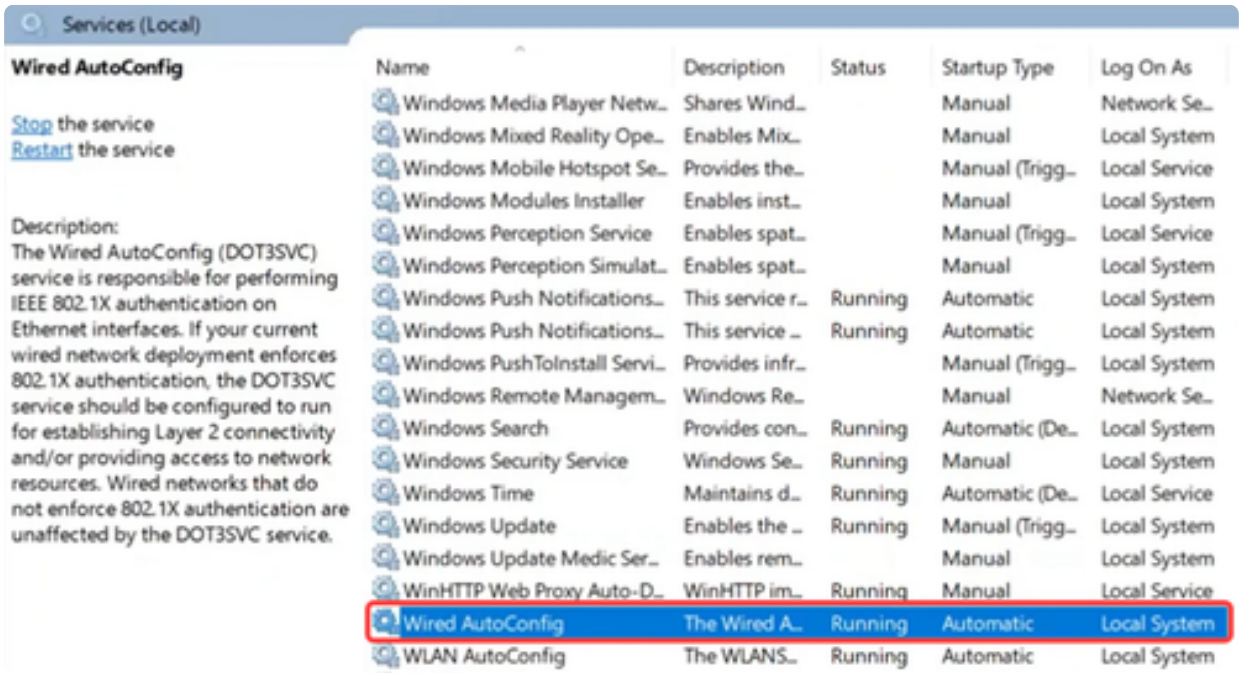
手順 4

Settingsをクリックし、Verify the server's identity by validating the certificateの横にあるボックスがオフになっていることを確認します。[OK] をクリックします。


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
Baltimore CyberTrust Root
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DESKTOP-N0NBRSQ
DigiCert Assured ID Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

手順 5

Servicesで、Wired AutoConfig 設定を有効にします。

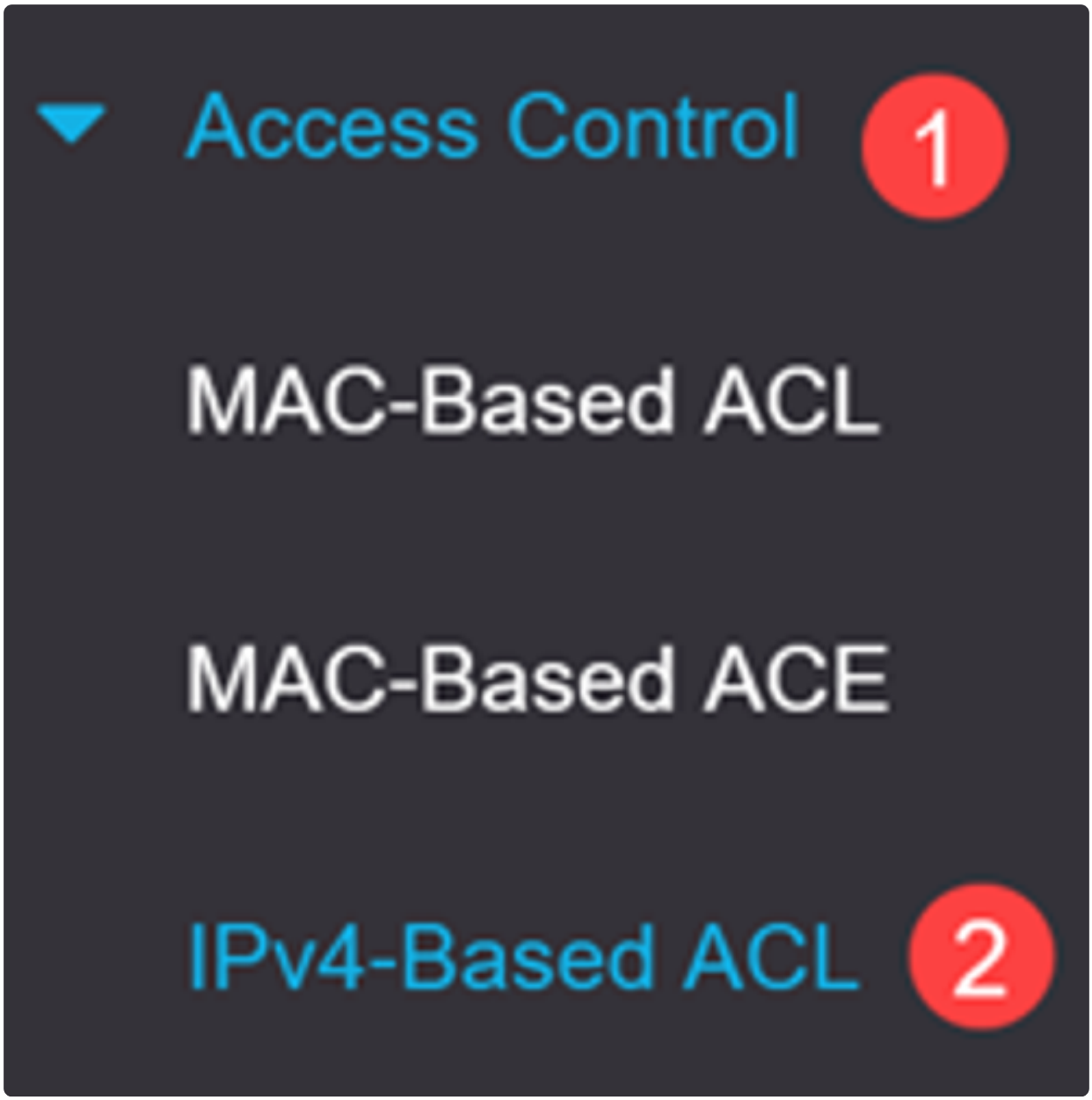


DACLの検証

ユーザが認証されると、ダウンロード可能なACLを確認できます。

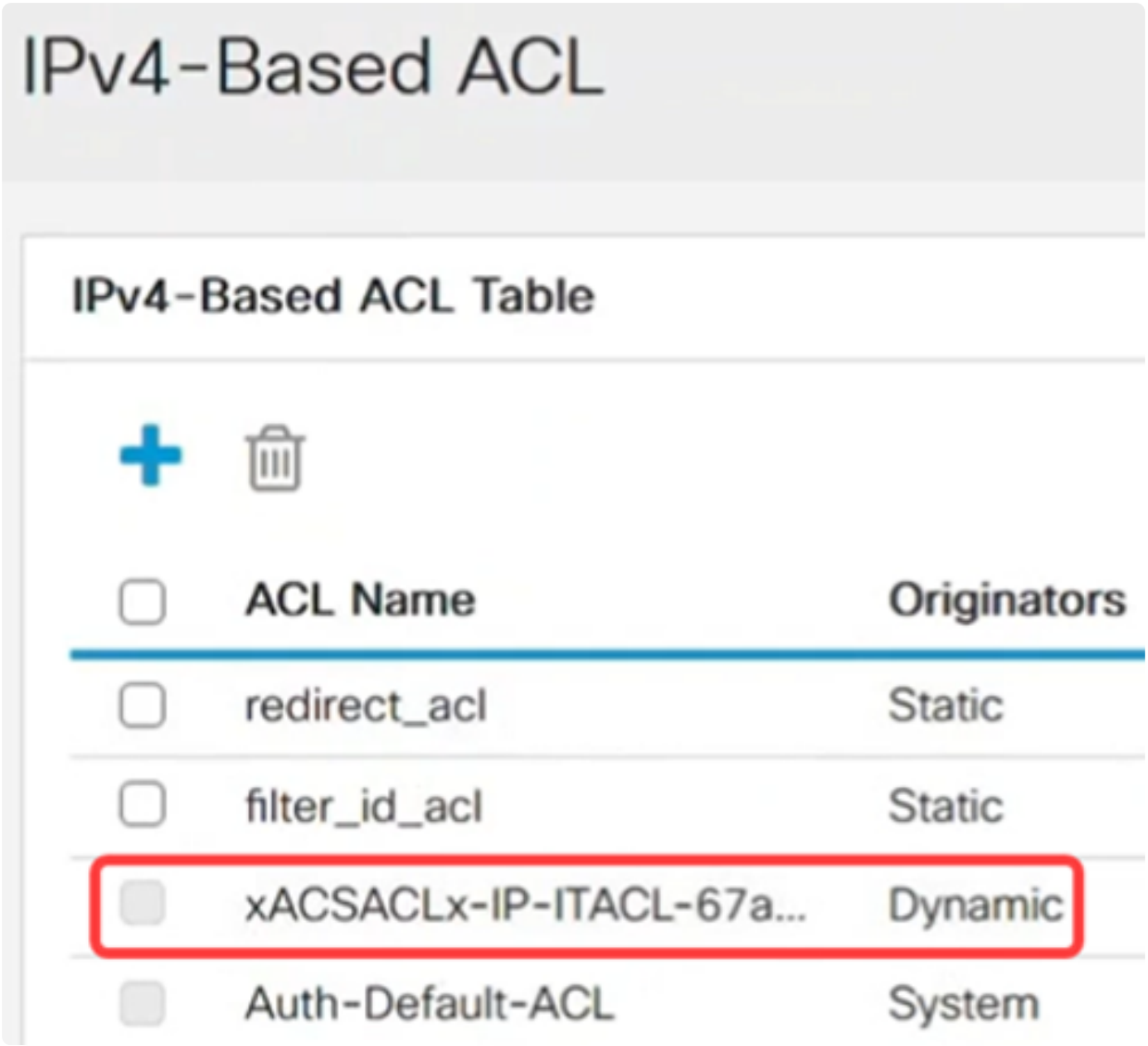
手順 1

Catalyst 1300スイッチにログインし、Access Control > IPv4-Based ACLメニューに移動します。



手順 2

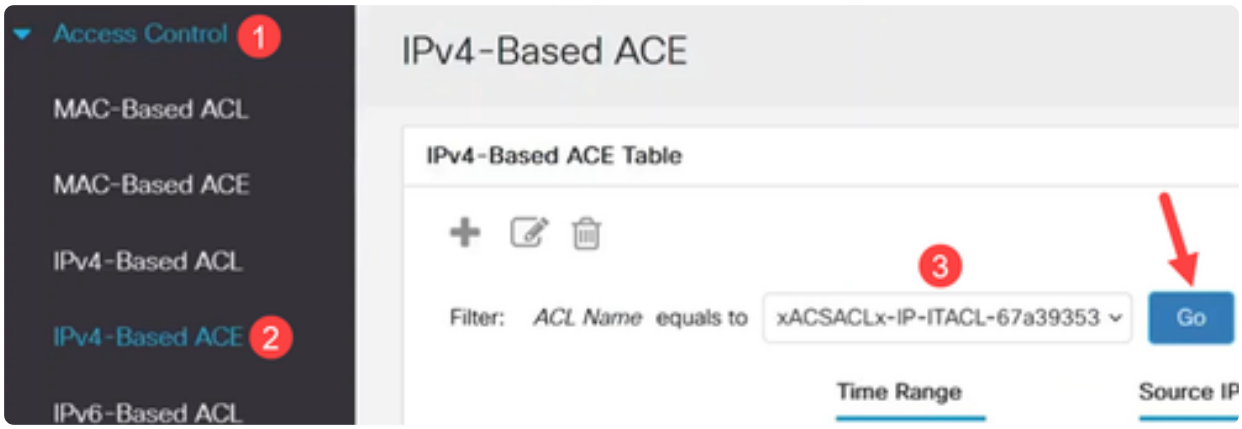
IPv4ベースのACLテーブルに、ダウンロードしたACLが表示されます。



Note:
ダウンロード可能なACLは編集できません。

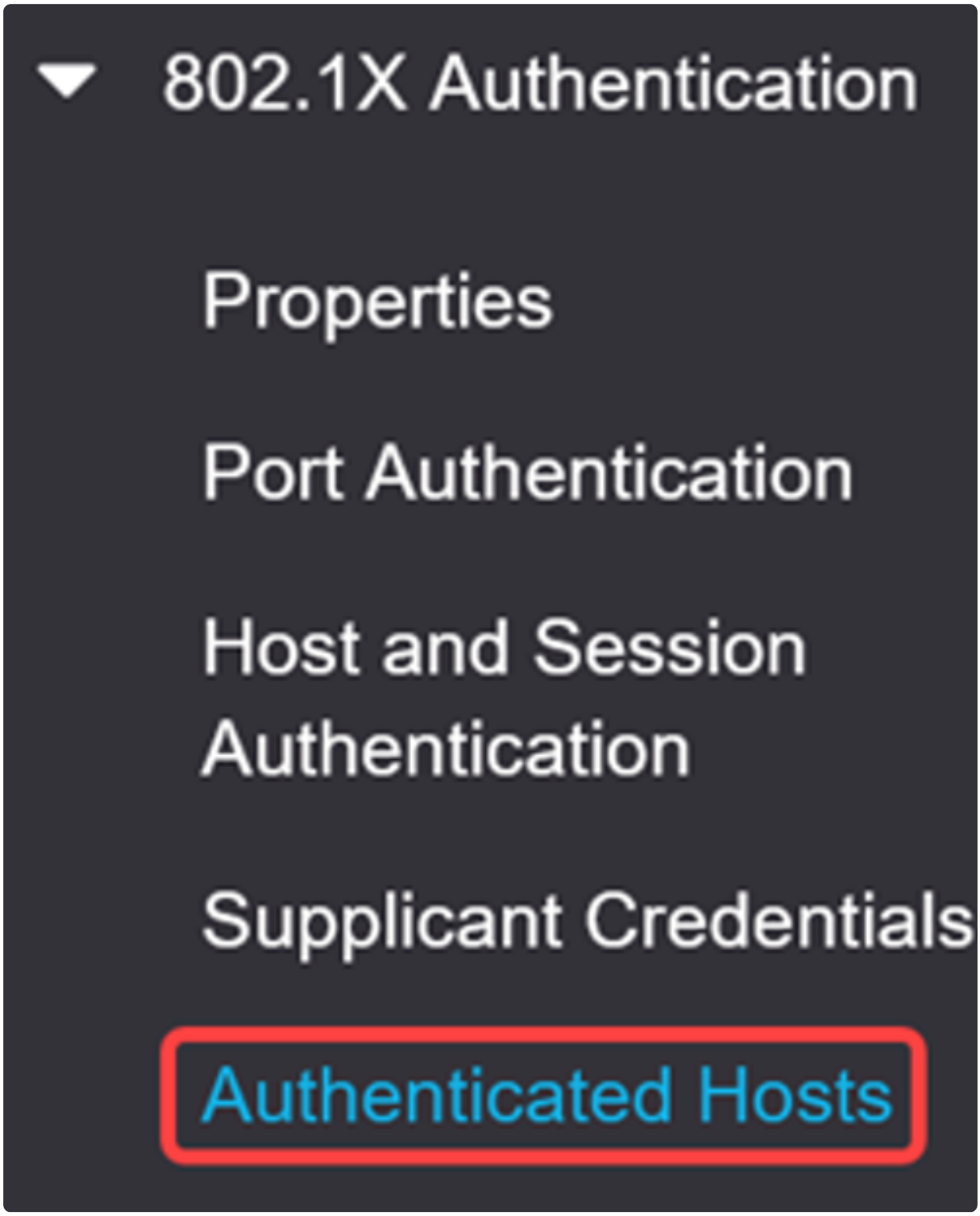
手順 3

IPv4ベースのACEに移動して、ACL Nameドロップダウンメニューからダウンロード可能なACLを選択し、Goをクリックするという方法でも確認できます。ISEで設定されたルールが表示されます。



手順 4

Security > 802.1 Authentication > Authenticated Hostsの順にメニューします。認証されたユーザを確認できます。Authenticated Sessionsをクリックすると、詳細が表示されます。



手順 5

CLIでは、コマンドshow ip access-lists interfaceの後にinterface IDを続けて実行します。

この例では、ギガビットイーサネット3に適用されたACLとACEを確認できます。

```
switch4a7d55#show ip access-lists interface ge1/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
    deny    ip any host 192.168.251.10 ace-priority 1
    permit  ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
    permit  udp any any any domain ace-priority 20
    permit  tcp any any any domain ace-priority 40
    permit  udp any bootps any any ace-priority 60
    permit  udp any any any bootpc ace-priority 80
    permit  udp any bootpc any any ace-priority 100
    deny    ip any any ace-priority 120
```

手順 6

また、コマンドを使用して、ISE接続とACLダウンロードに関連する設定を確認することもできます

show dot1x sessions interface <ID>詳細ステータス、802.1x認証状態、およびダウンロードされたACLを表示できます。

```
switch4a7d55#show dot1x sessions interface ge1/0/3 detailed

          Interface: gi1/0/3
        MAC Address: e4:[redacted]:31
       IPv4 Address: 192.168.251.11
          User-Name: user5
             Status: Authorized
     Oper host mode: multi-host
    Session timeout: N/A
     Session Uptime: 196 sec
  Common Session ID: 14FBA8C00500032222C35D9E
    Acct Session ID: 0x05000322
 Server Policies:
            ACS ACL: xACSACLx-IP-SalesACL-6760399d

 Method status list:
    Method                  State
    802.1x                  Authentication success
```

結論

行くぞ！これで、Cisco ISEを使用したCisco Catalyst 1300スイッチでダウンロード可能ACLがどのように機能するかについて理解できました。

詳細については、『Catalyst 1300管理ガイド』および『Cisco Catalyst 1300シリーズサポートページ』を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。