Herunterladbare ACL für Catalyst Switches der Serie 1300

Ziel

In diesem Artikel wird erläutert, wie die herunterladbare Zugriffskontrollliste (Access Control List, DACL) auf Cisco Catalyst 1300-Switches mit der Cisco Identity Service Engine (ISE) funktioniert.

Unterstützte Geräte | Software-Version

- Catalyst 1300-Serie | 4.1.6.54

Einleitung

Dynamische ACLs sind ACLs, die einem Switch-Port anhand einer Richtlinie oder bestimmter Kriterien (z. B. Mitgliedschaft in einer Benutzergruppe, Tageszeit usw.) zugewiesen werden. Dabei kann es sich um lokale ACLs handeln, die durch die Filter-ID oder durch herunterladbare ACLs (DACLs) angegeben werden.

Herunterladbare ACLs sind dynamische ACLs, die vom Cisco ISE-Server erstellt und heruntergeladen werden. Sie wenden Zugriffskontrollregeln basierend auf der Benutzeridentität und dem Gerätetyp dynamisch an. DACL bietet den Vorteil, dass Sie über ein zentrales Repository für ACLs verfügen, sodass Sie diese nicht auf jedem Switch manuell erstellen müssen. Wenn ein Benutzer eine Verbindung zu einem Switch herstellt, muss er sich lediglich authentifizieren, und der Switch lädt die entsprechenden ACLs vom Cisco ISE-Server herunter.

Anwendungsbeispiele für herunterladbare ACL

1. Verschiedene Benutzer erhalten unterschiedliche ACLs, wenn sie eine Verbindung zu einem Switch herstellen (lokale ISE-Benutzer).
2. Benutzer mit eingeschränkter Netzwerkkonnektivität können sich bei einem zentralen Webportal anmelden, um vollständigen Netzwerkzugriff zu erhalten (zentrale Webauthentifizierung).
3. Erweitert - Verwendung von MAB (MAC Authentication Bypass), um die Kommunikation mit Windows Active Directory (AD) und einigen verwandten Diensten zu ermöglichen, während der ISE-Server mit AD verbunden wird und die Benutzerauthentifizierung überwacht wird. Vor der Windows AD-Anmeldung ermöglicht das Netzwerk nur den Zugriff auf sehr eingeschränkte Ressourcen. Bei der AD-Authentifizierung werden jedoch unterschiedliche, auf Windows-Gruppen basierende ACLs heruntergeladen, und der Netzwerkzugriff ist vollständig.
4. Erweitert - Benutzer erhalten aufgrund von Richtlinien auf dem ISE-Server unterschiedliche

Zugriffskontrolllisten, basierend auf dem Wochentag, der Tageszeit oder einem anderen Faktor.

In diesem Artikel wird der erste Anwendungsfall ausführlich behandelt.

Inhalt

Voraussetzungen

- Vergewissern Sie sich, dass für Ihren Catalyst 1300 Switch ein Upgrade auf die neueste Firmware durchgeführt wird (Switch-Firmware sollte 4.1.6 oder höher sein).
- Weisen Sie dem Switch zu Verwaltungszwecken eine statische IP zu.

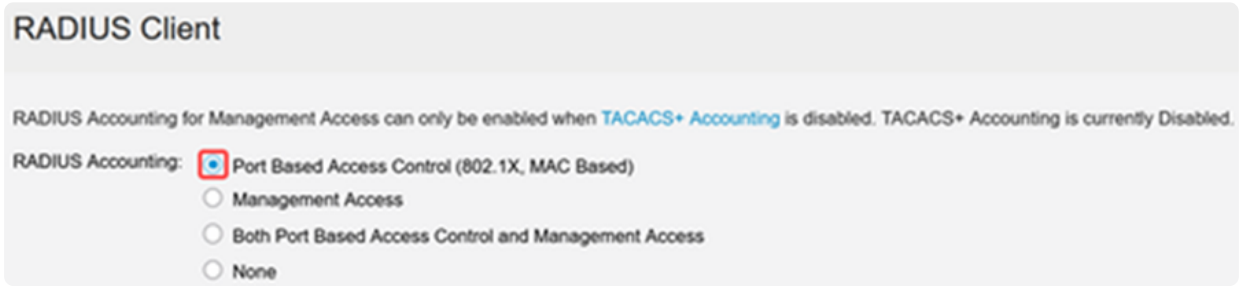
RADIUS-Client konfigurieren

Schritt 1

Melden Sie sich beim Catalyst 1300 Switch an, und navigieren Sie zum Menü Security > RADIUS Client (Sicherheit > RADIUS-Client).

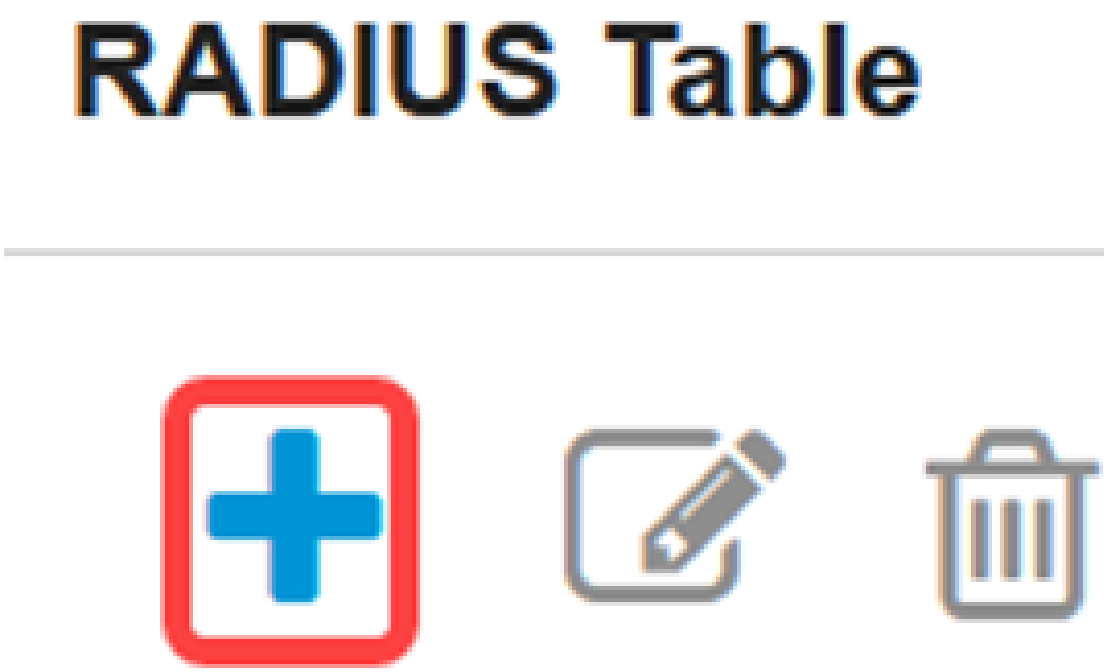
Schritt 2

Wählen Sie für die RADIUS-Abrechnung die Option Port Based Access Control (Port-basierte Zugriffskontrolle) aus.



Schritt 3

Klicken Sie unter RADIUS Table (RADIUS-Tabelle) auf das Pluszeichen, um den Cisco ISE-Server hinzuzufügen.



Schritt 4

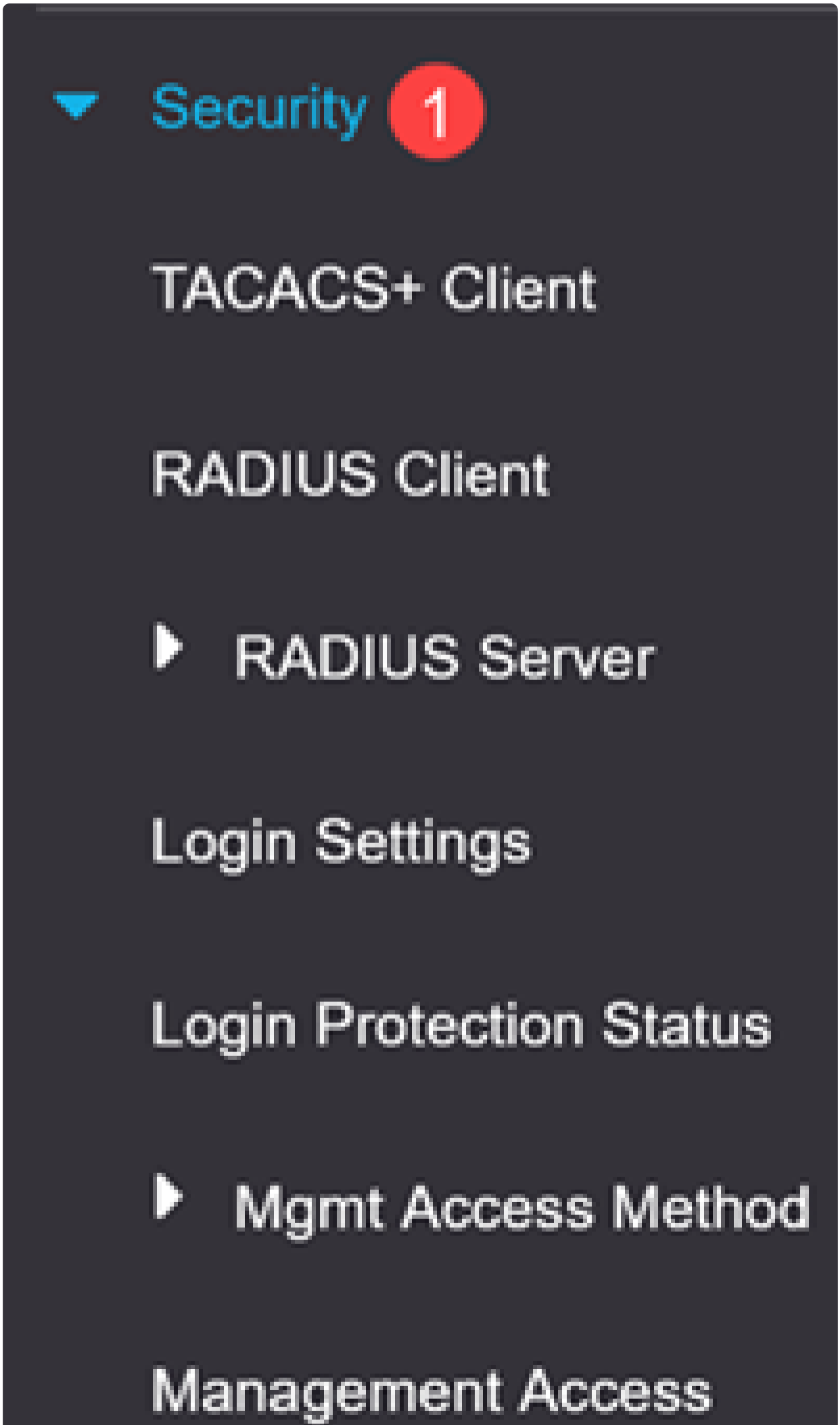
Geben Sie die Details zum Cisco ISE-Server ein, und klicken Sie auf Apply.

> **Note:**
> Als Verwendungstyp muss 802.1x ausgewählt sein.

Konfigurieren der 802.1x-Authentifizierung

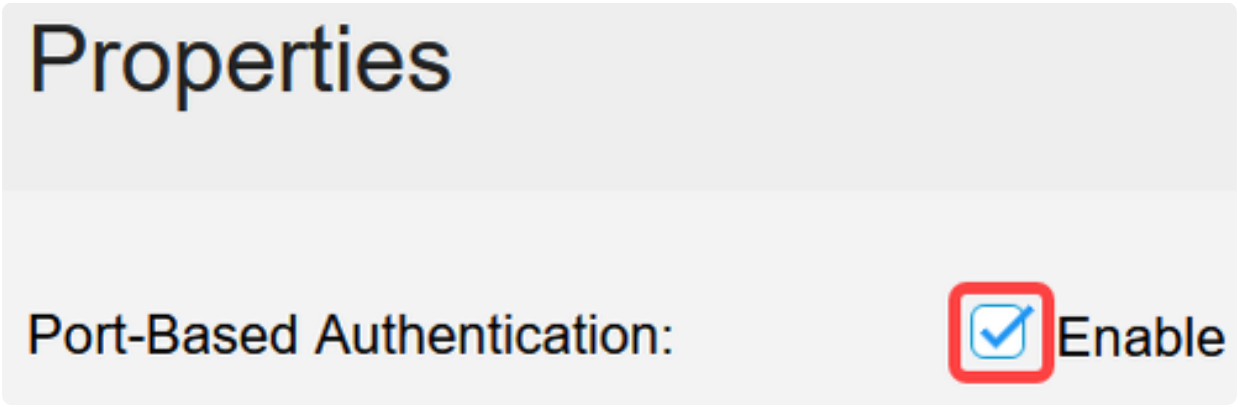
Schritt 1

Navigieren Sie zu Security > 802.1X Authentication > Properties (Sicherheit > 802.1X-Authentifizierung > Eigenschaften).


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

Schritt 2

Klicken Sie auf das Kontrollkästchen, um Port-Based Authentication zu aktivieren.

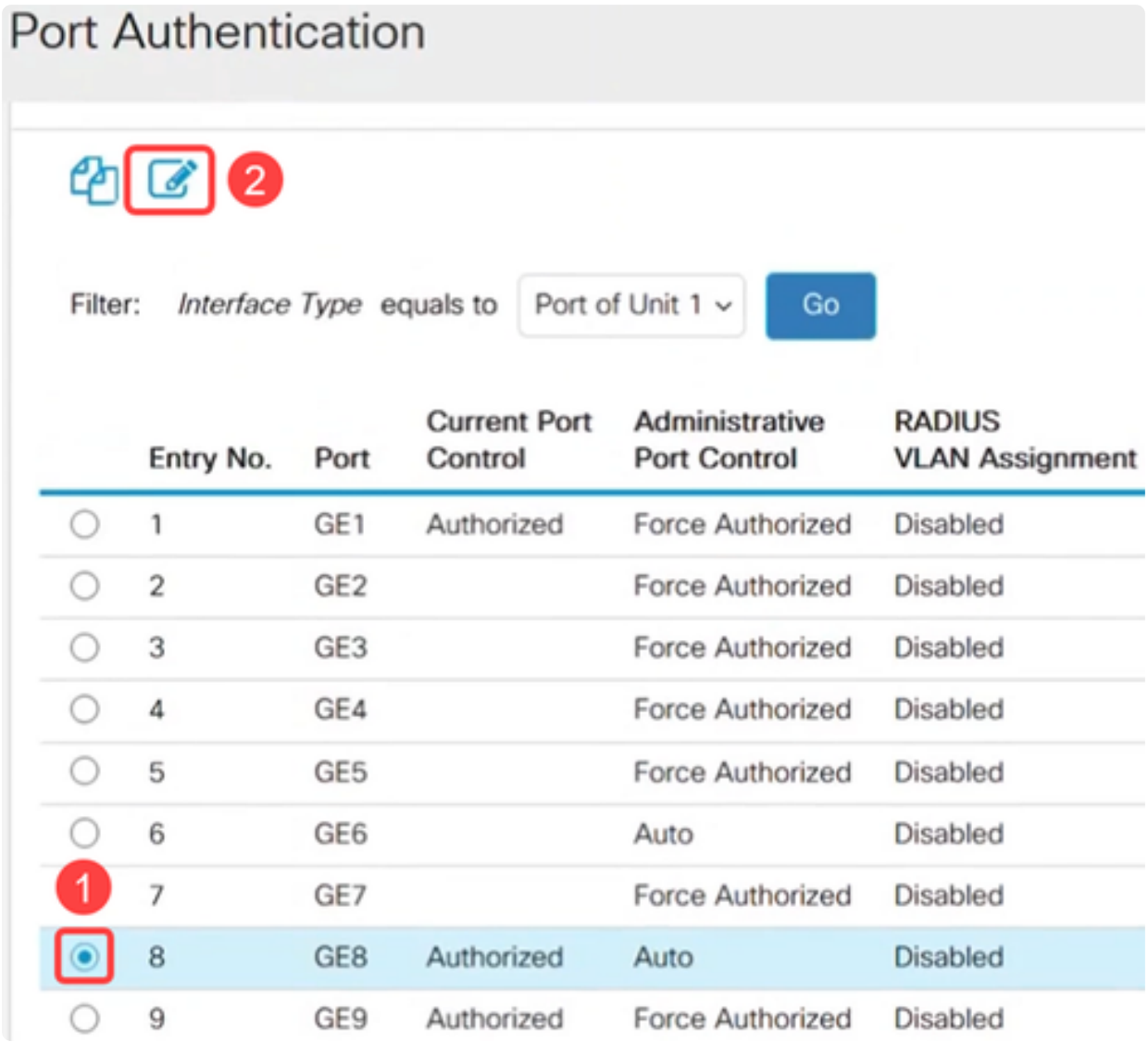


Schritt 3

Wählen Sie unter Authentication Method die Option RADIUS aus, und klicken Sie auf Apply.

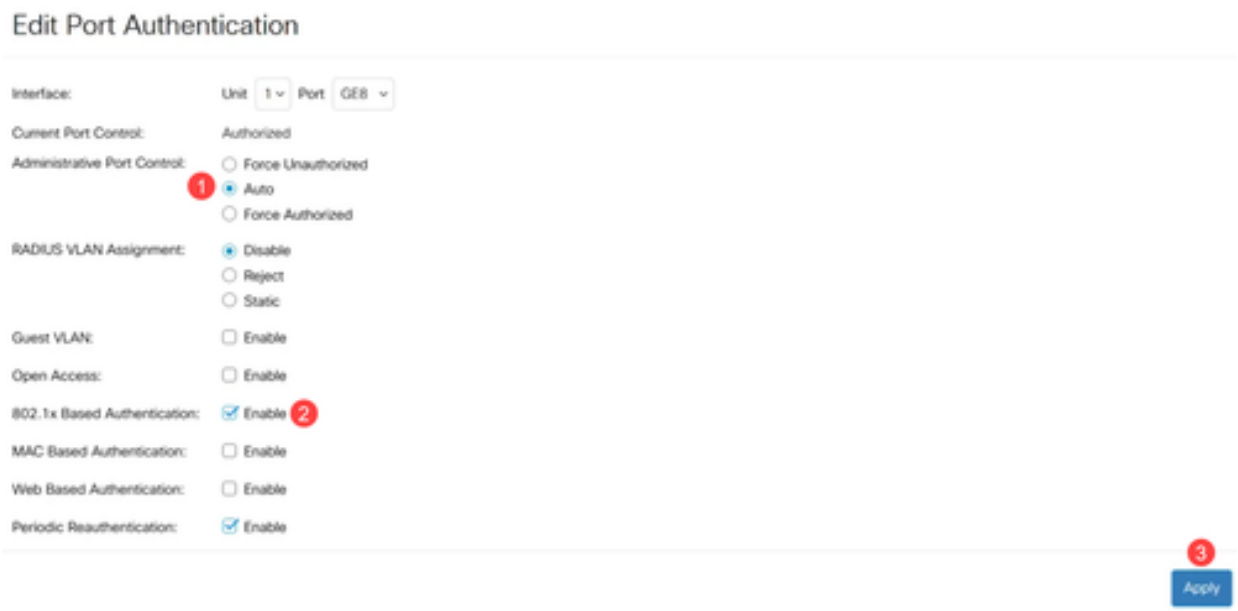
Schritt 4

Gehen Sie zu Security > 802.1X Authentication > Port Authentication menu. Wählen Sie den Port aus, mit dem Ihr Laptop verbunden ist, und klicken Sie auf das Symbol Bearbeiten. In diesem Beispiel ist GE8 ausgewählt.



Schritt 5

Wählen Sie Administrative Port Control als Auto aus, und aktivieren Sie die 802.1x-basierte Authentifizierung. Klicken Sie auf Apply (Anwenden).



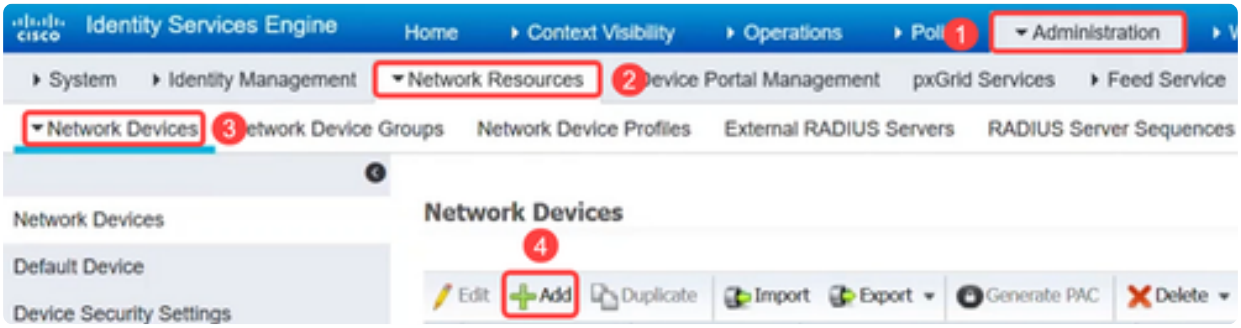
Cisco ISE-Serverkonfiguration für herunterladbare ACLs

> **Note:**
> Die ISE-Konfiguration geht über den Cisco Business Support hinaus. Weitere Informationen finden Sie im ISE-Administratorhandbuch.

Die in diesem Artikel gezeigten Konfigurationen sind ein Beispiel für herunterladbare ACLs, die mit Cisco Catalyst Switches der Serie 1300 verwendet werden können.

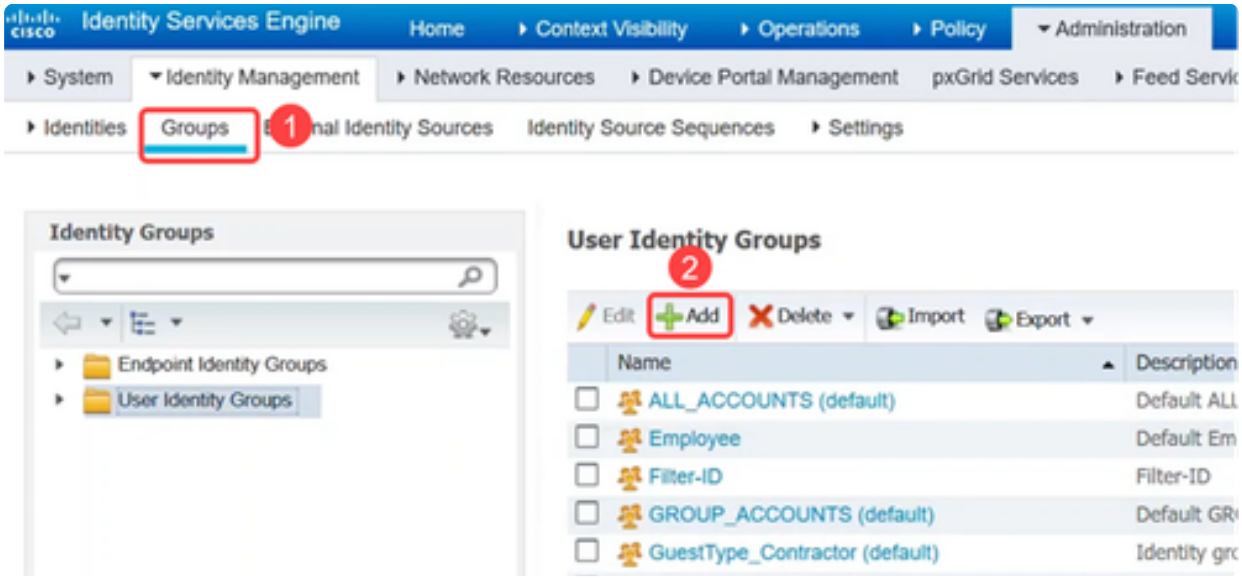
Schritt 1

Melden Sie sich bei Ihrem Cisco ISE-Server an, navigieren Sie zu Administration > Network Resources > Network Devices, und fügen Sie das Catalyst Switch-Gerät hinzu.



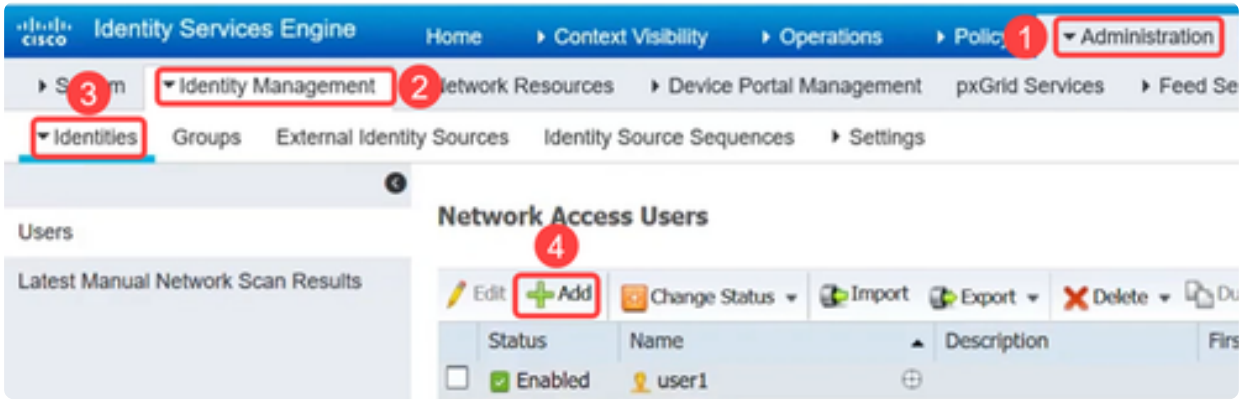
Schritt 2

Um Benutzeridentitätsgruppen zu erstellen, navigieren Sie zur Registerkarte Gruppen, und fügen Sie die Benutzeridentitätsgruppen hinzu.



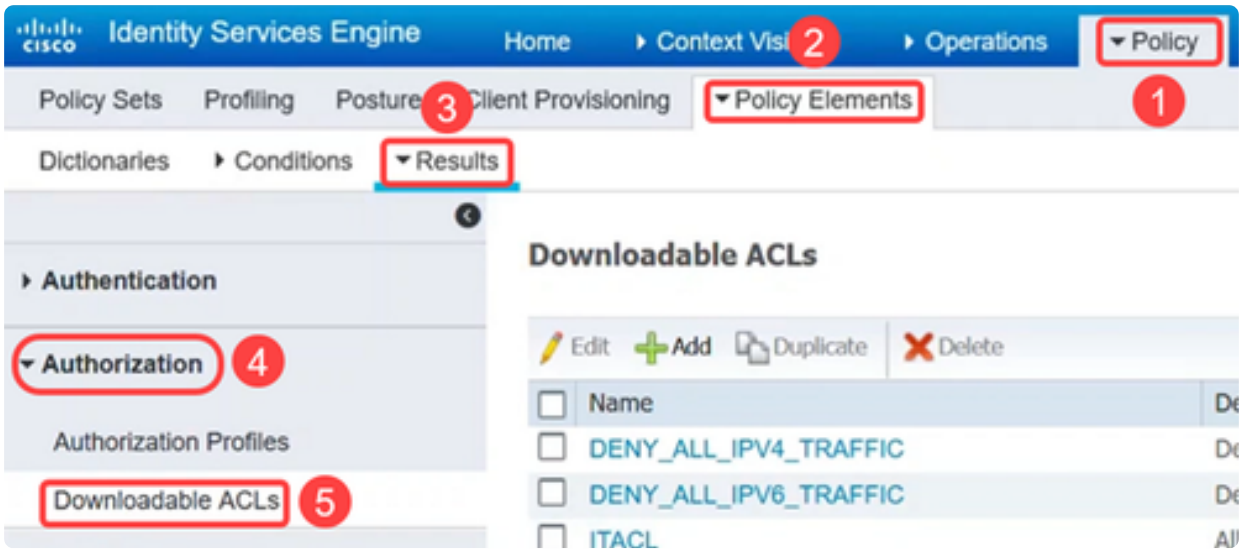
Schritt 3

Gehen Sie zum Menü Administration > Identity Management > Identities, um die Benutzer zu definieren und die Benutzer den Gruppen zuzuordnen.



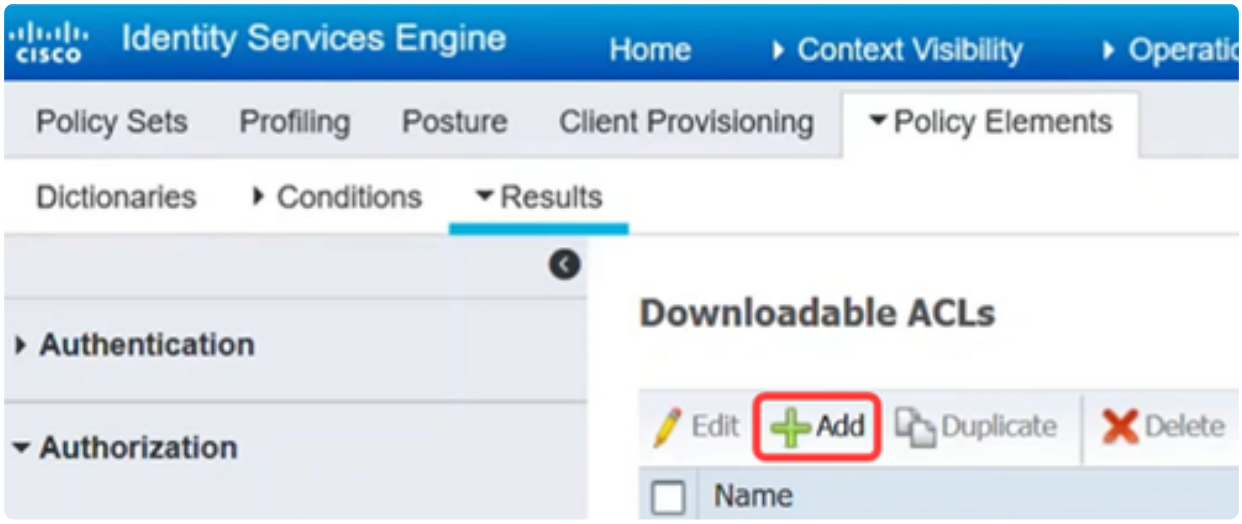
Schritt 4

Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse. Klicken Sie unter Autorisierung auf Herunterladbare ACLs.



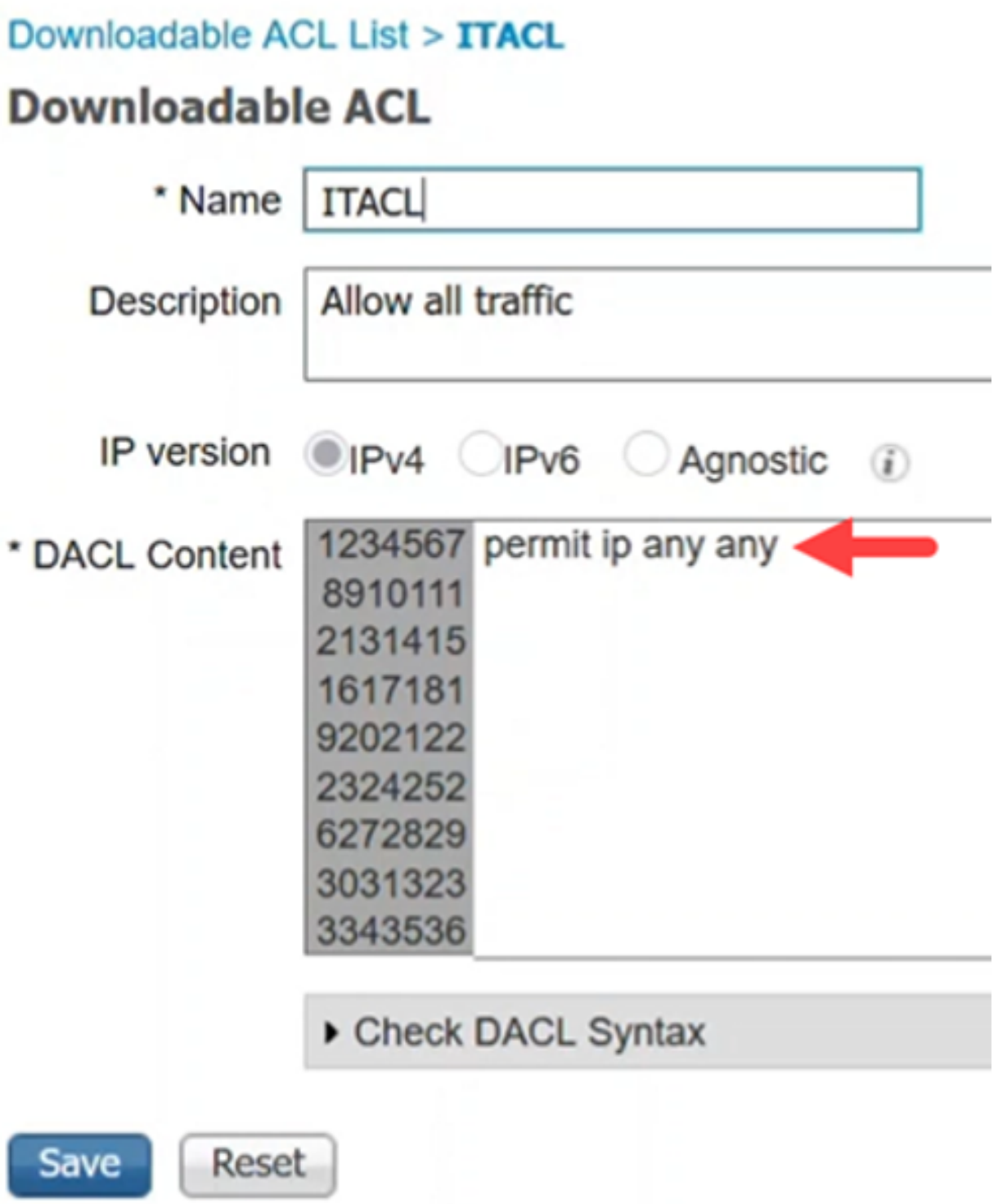
Schritt 5

Klicken Sie auf das Symbol Add (Hinzufügen), um die herunterladbare ACL zu erstellen.



Schritt 6

Konfigurieren Sie den Namen, die Beschreibung, wählen Sie die IP-Version aus, und geben Sie die Zugriffssteuerungseinträge (ACEs) ein, aus denen die herunterladbare ACL besteht. Diese werden in das Feld DACL-Inhalt eingegeben. Klicken Sie auf Speichern.



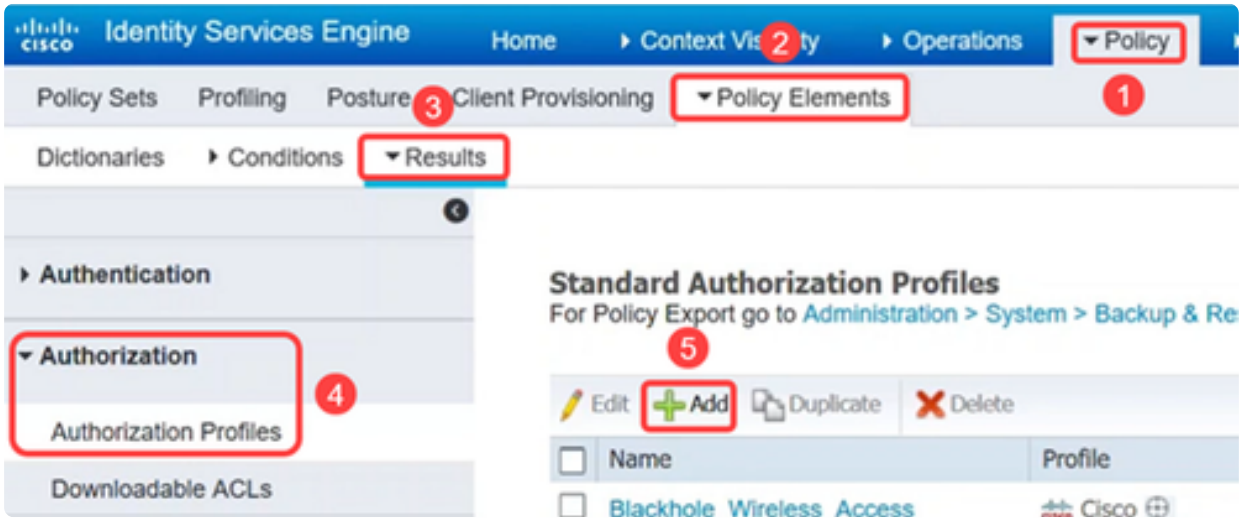
Note:

Nur IP-Zugriffskontrolllisten werden unterstützt, und die Quelle muss ANY sein. Für ACLs auf der ISE wird jetzt nur IPv4 unterstützt. Wenn eine ACL mit einer anderen Quelle eingegeben wird, die Syntax für ISE zwar in Ordnung ist, bei Anwendung auf den Switch jedoch fehlschlägt.

Schritt 7

Erstellen Sie Autorisierungsprofile, die verwendet werden, um Ihre DACL und andere Richtlinien innerhalb der ISE-Richtliniensätze logisch miteinander zu verknüpfen.

Navigieren Sie dazu zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile, und klicken Sie auf Hinzufügen.

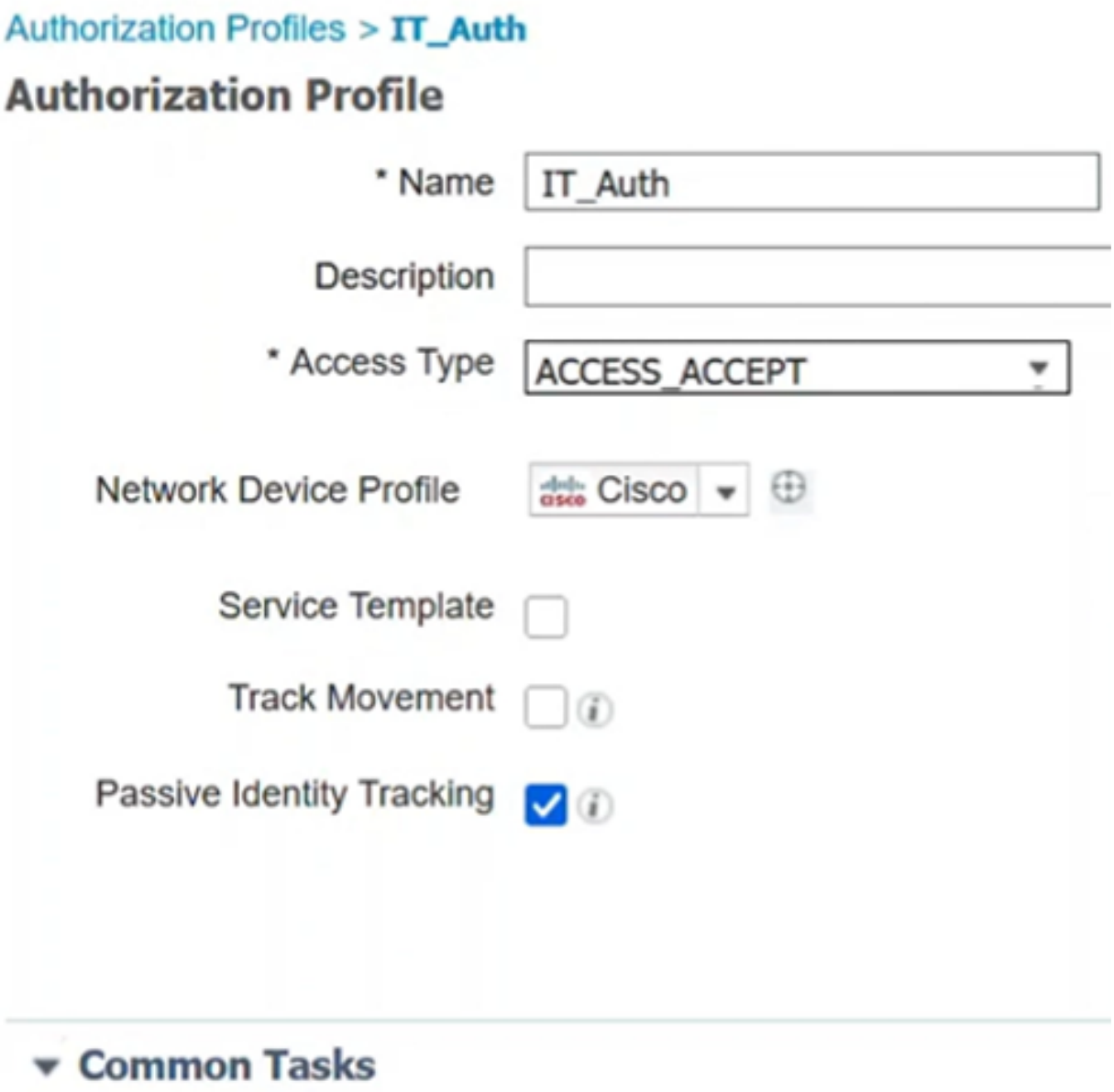


Schritt 8

Konfigurieren Sie auf der Seite Authorization Profile (Autorisierungsprofil) Folgendes:

- Name
- Beschreibung
- Zugriffstyp: Legen Sie hier ACCESS_ACCEPT fest. Bei ACCESS_REJECT wird die Authentifizierung zurückgewiesen.
- Netzwerkgeräteprofil - Wählen Sie dieses als Cisco aus.
- Passive Identitätsnachverfolgung - muss möglicherweise für einige Authentifizierungsszenarien aktiviert werden. Dies ist für EasyConnect_PassiveID-Szenarien erforderlich, die mit AD verknüpft sind.
- Allgemeine Aufgaben - Dieser Abschnitt hat viele Optionen. In diesem Beispiel wird DACL Name konfiguriert.

Klicken Sie auf Speichern.



Schritt 9

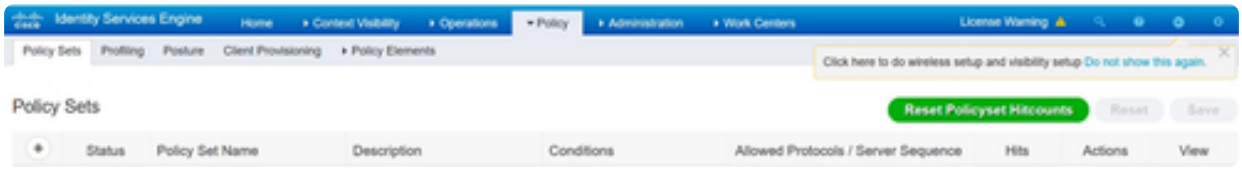
Um Richtliniensätze zu konfigurieren, die logische Gruppierungen von Authentifizierungs- und Autorisierungsrichtlinien darstellen, klicken Sie auf Richtlinie > Menü Richtliniensätze.

Eine Liste der Richtliniensätze enthält folgende Informationen:

- Status: Eine grüne Markierung steht für "aktiviert", ein leerer weißer Kreis für "deaktiviert" und ein Augensymbol für eine reine Monitorkonfiguration.
- Name und Beschreibung des Richtliniensatzes - selbsterklärend
- Bedingungen: Hier wird festgelegt, wo die festgelegten Richtlinien gelten.
- Zugelassene Protokolle/Serversequenz - Legt erweiterte Steuerelemente fest.
- Treffer - Zeigt an, wie oft der Richtliniensatz verwendet wurde.
- Aktionen: Sie können die Reihenfolge ändern, in der Richtliniensätze angewendet werden

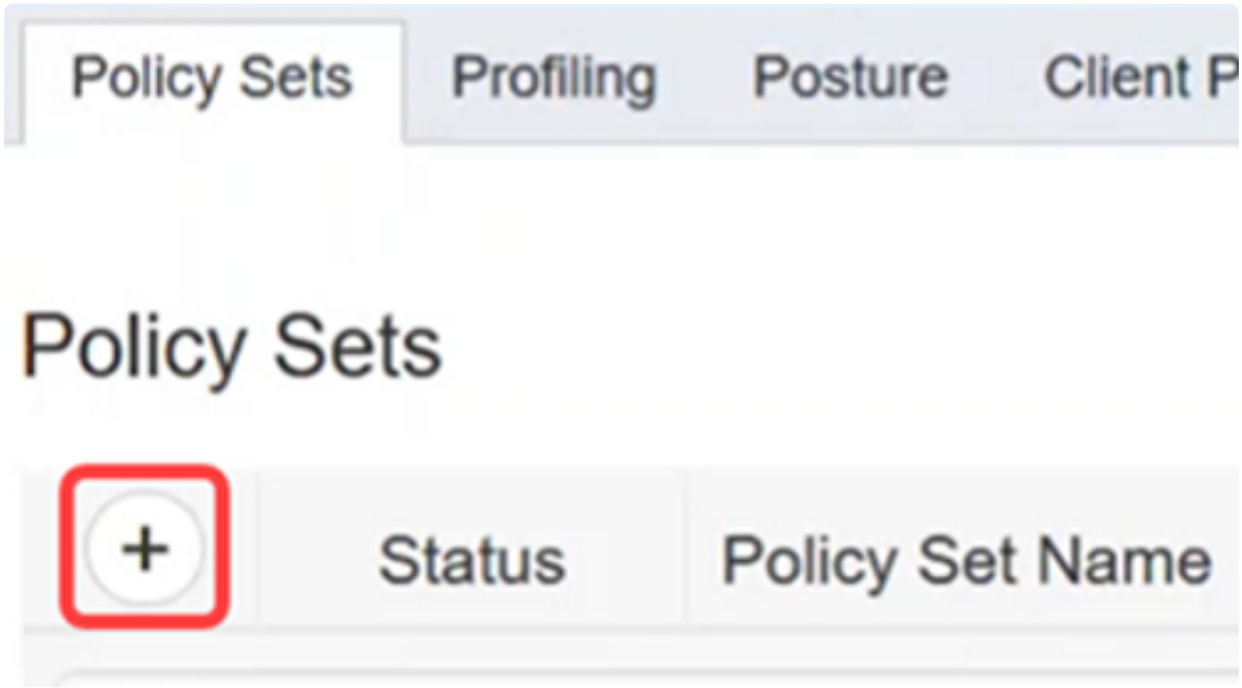
können, einen vorhandenen Richtliniensatz kopieren oder einen vorhandenen Richtliniensatz löschen.

- Anzeigen: Hier können Sie die Details des Richtliniensatzes bearbeiten.



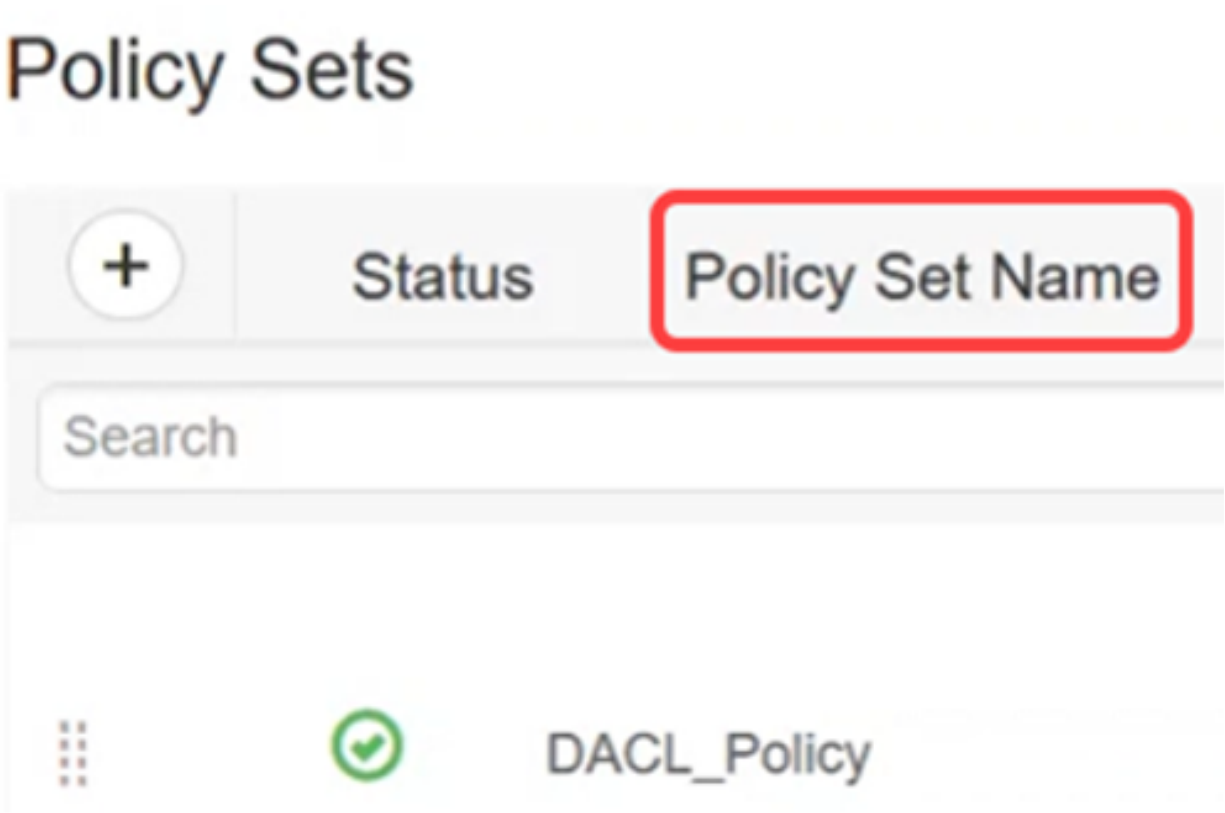
Schritt 10

Klicken Sie zum Erstellen eines Richtliniensatzes auf die Schaltfläche Hinzufügen.



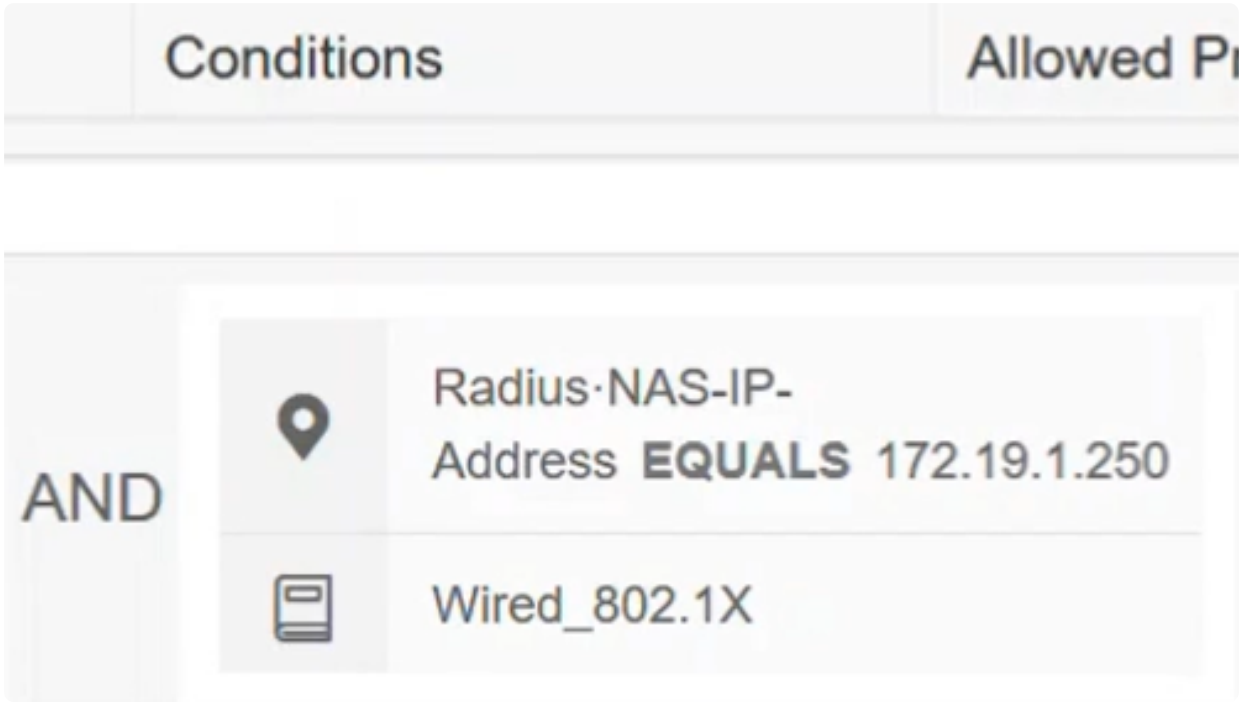
Schritt 11

Definieren Sie einen Richtliniensatznamen.



Schritt 12

Klicken Sie unter Bedingungen auf die Schaltfläche Hinzufügen. Dadurch wird das Bedingungsstudio geöffnet, in dem Sie festlegen können, wo dieses Authentifizierungsprofil verwendet werden soll. In diesem Beispiel wurde sie auf die Radius-NAS-IP-Adresse (den Switch) angewendet, die den Datenverkehr "172.19.1.250" und "wired_802.1x" umfasst.

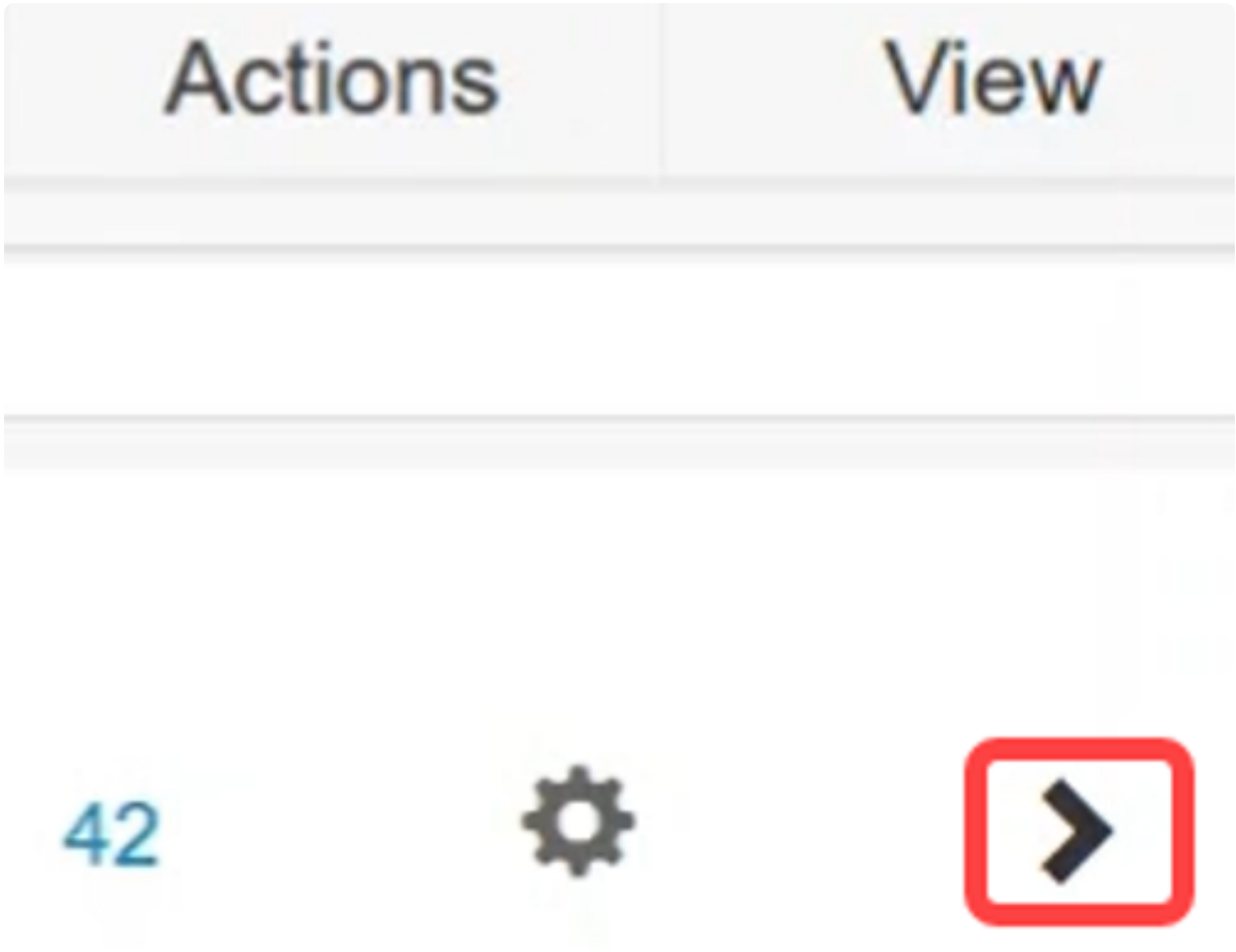


Schritt 13

Konfigurieren Sie die zulässigen Protokolle für den Standardnetzwerkzugriff, und klicken Sie auf Speichern.

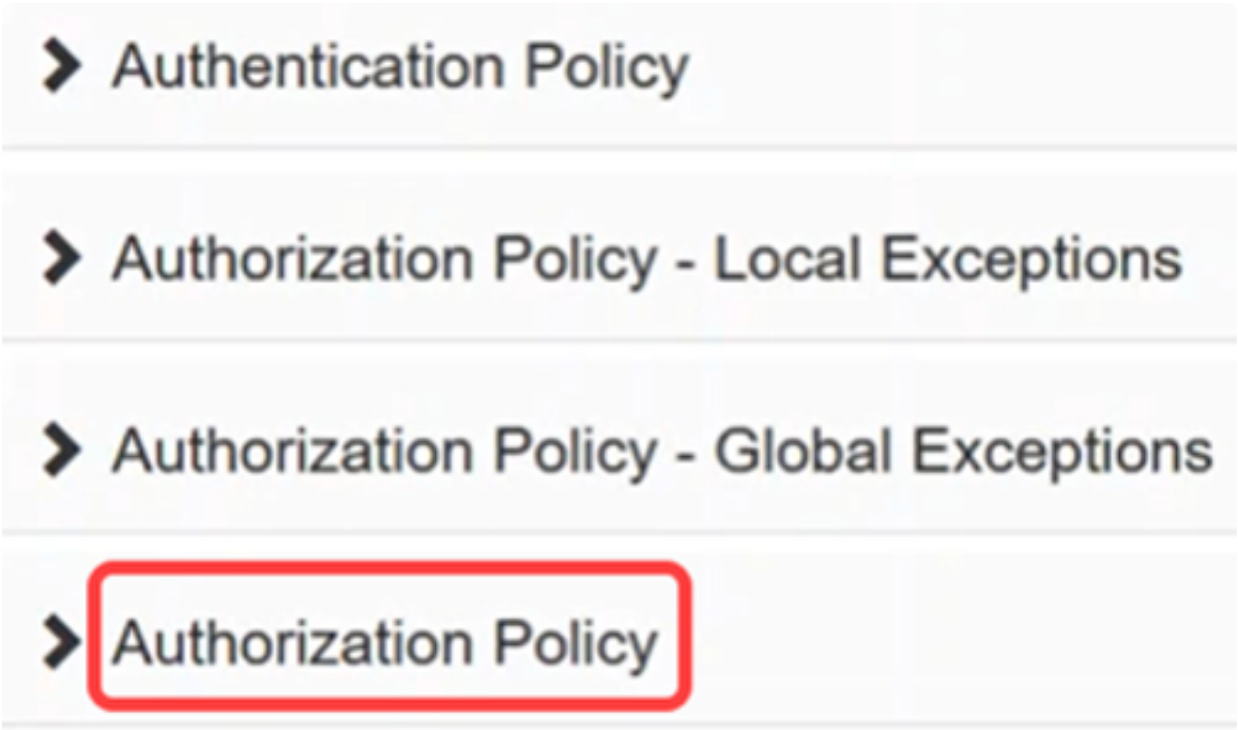
Schritt 14

Klicken Sie unter Ansicht auf das Pfeilsymbol, um Authentifizierungs- und Autorisierungsrichtlinien basierend auf den Einstellungen und Anforderungen Ihres Netzwerks zu konfigurieren, oder wählen Sie die Standardeinstellungen aus. Klicken Sie in diesem Beispiel auf die Autorisierungsrichtlinie.



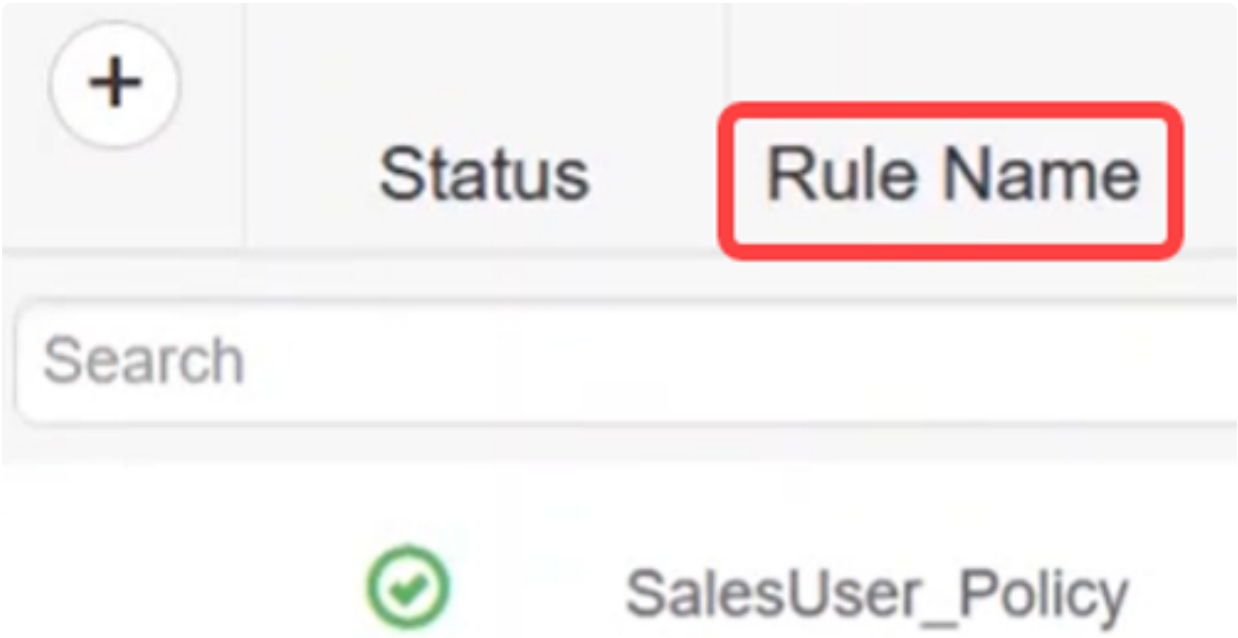
Schritt 15

Klicken Sie auf das Pluszeichen, um eine Richtlinie hinzuzufügen.



Schritt 16

Geben Sie den Regelnamen ein.



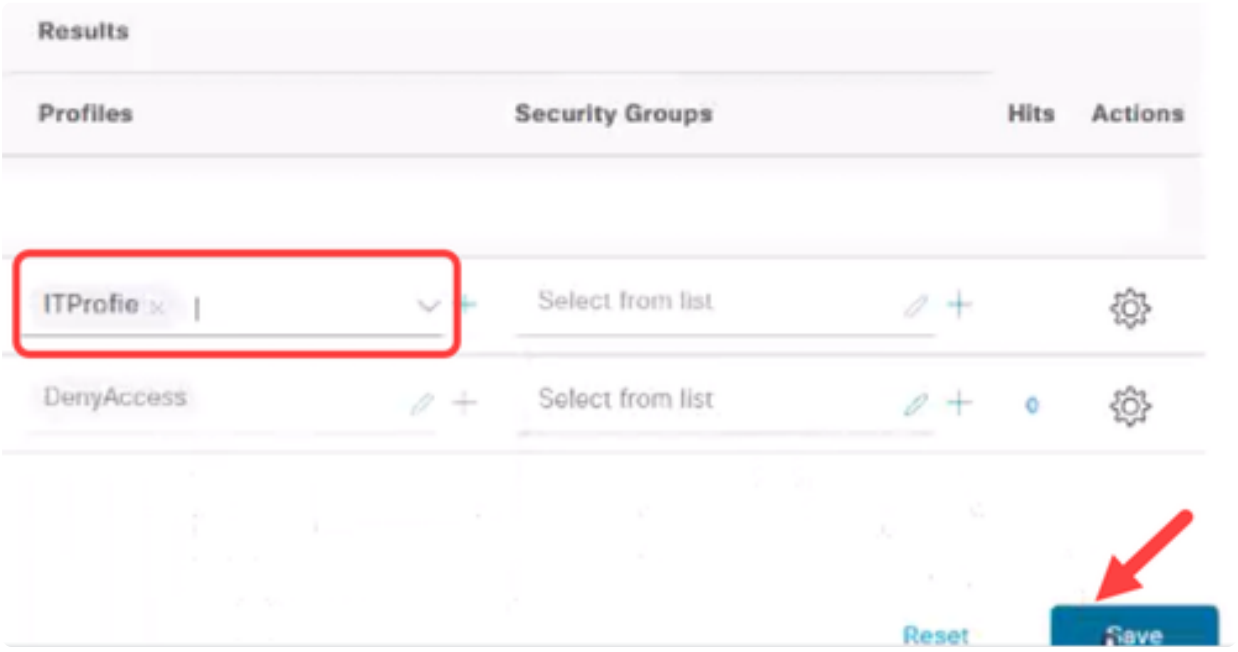
Schritt 17

Klicken Sie unter Bedingungen auf das Pluszeichen, und wählen Sie die

Identitätsgruppe aus. Klicken Sie auf Verwenden.

Schritt 18

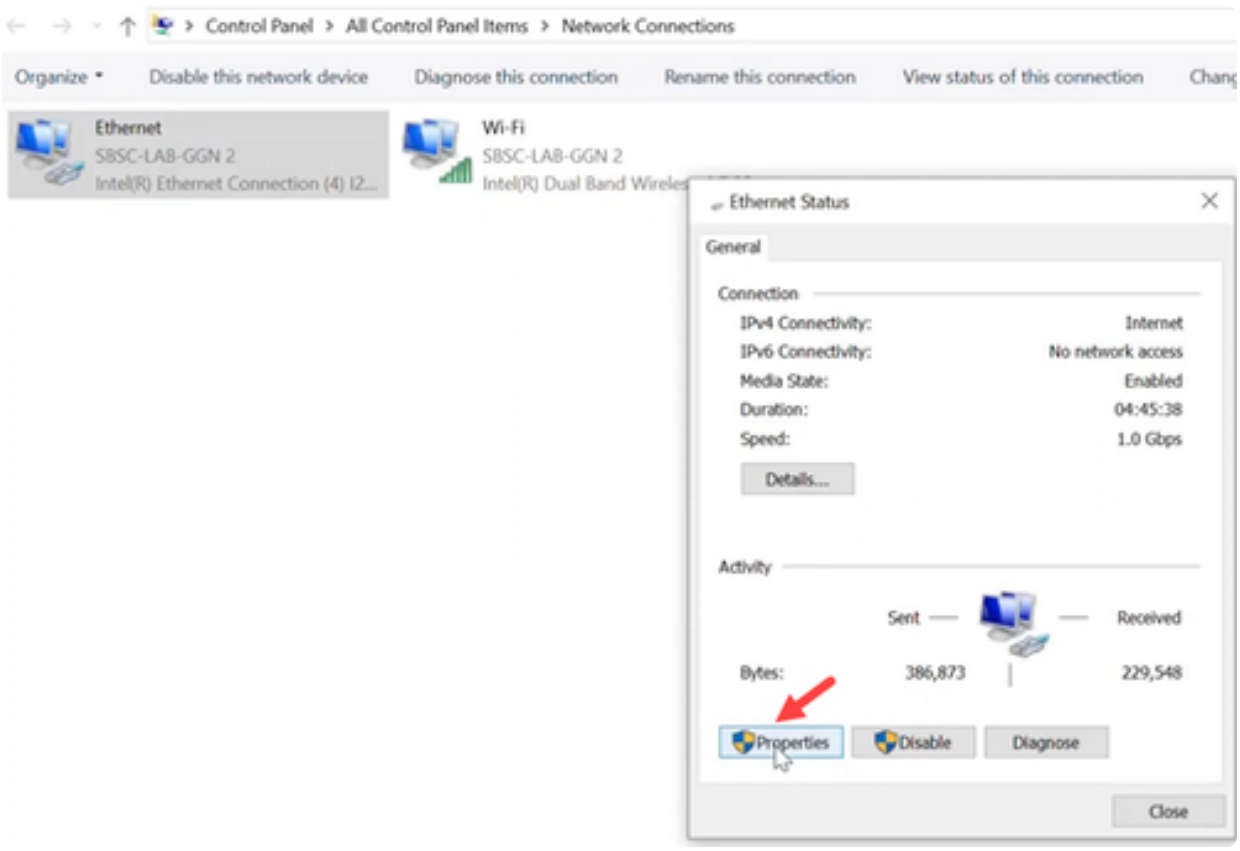
Wenden Sie das erforderliche Profil an, und klicken Sie auf Speichern.



Client-Konfigurationen

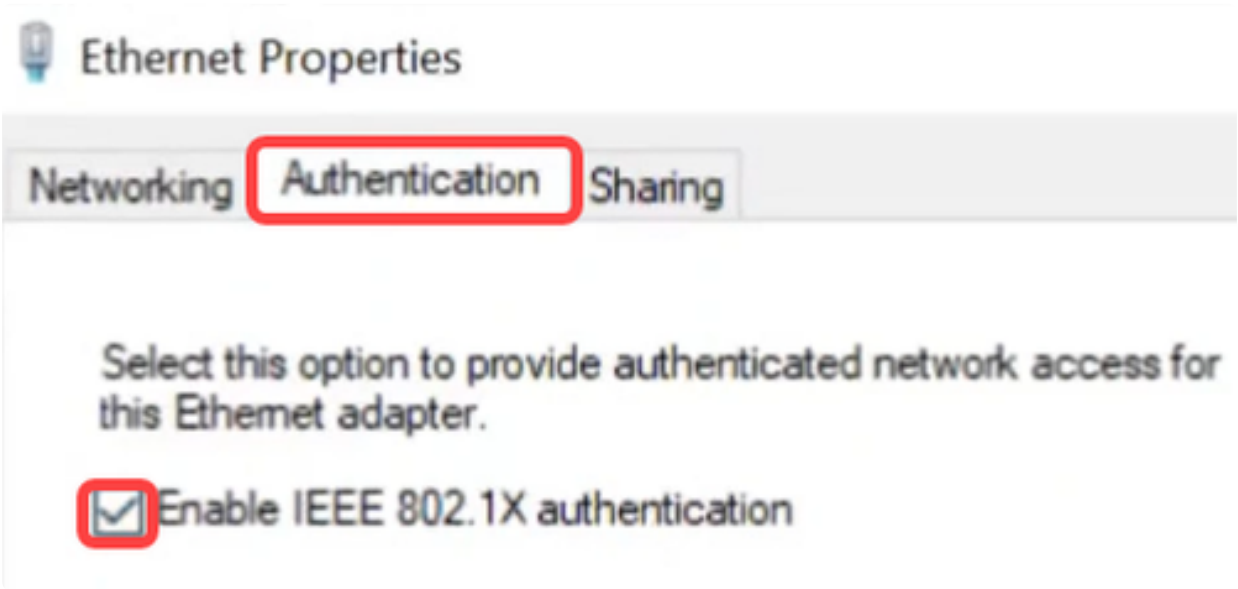
Schritt 1

Navigieren Sie auf dem Client-Laptop zu Netzwerkverbindungen > Ethernet, und klicken Sie auf Eigenschaften.



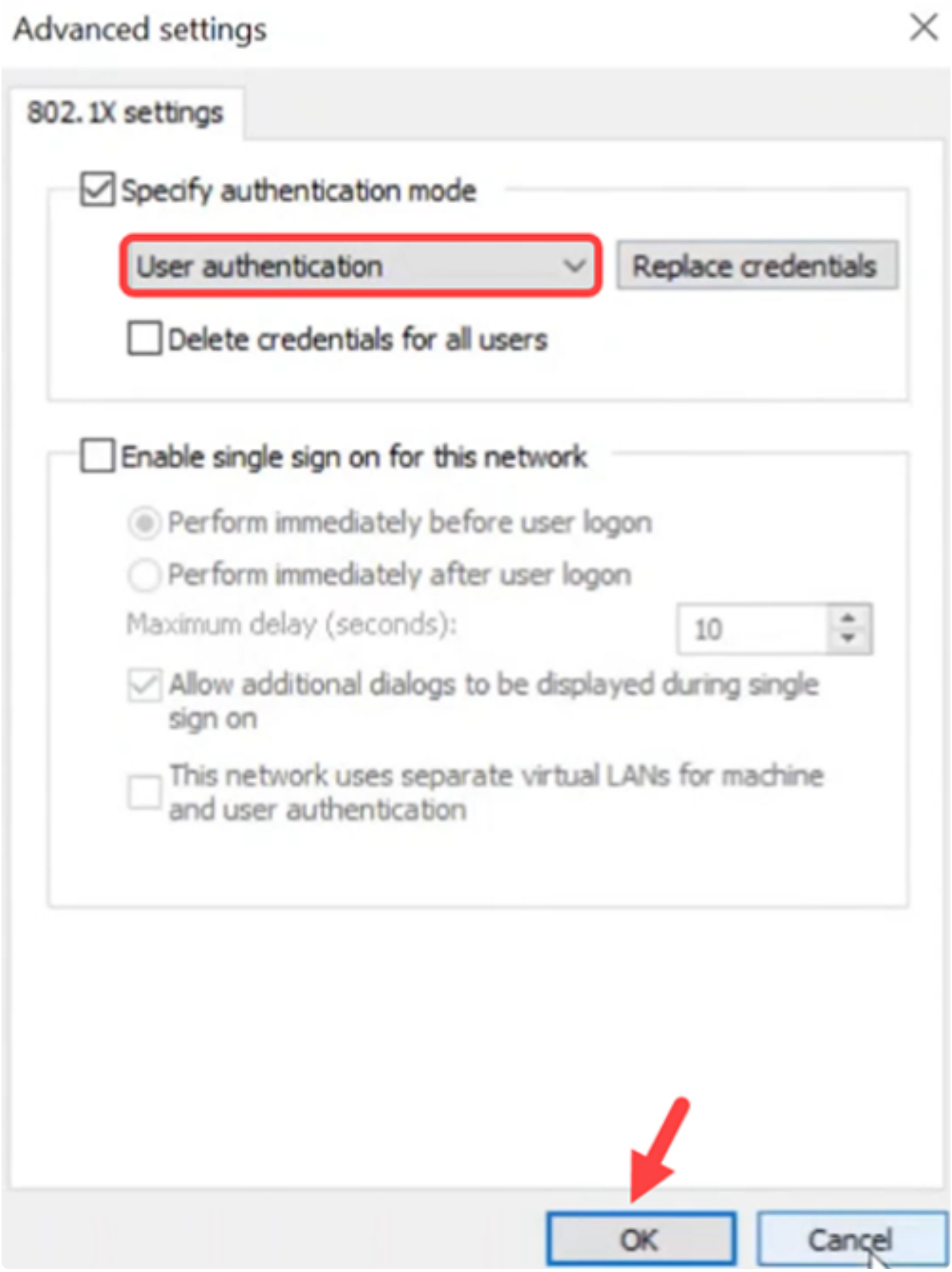
Schritt 2

Klicken Sie auf die Registerkarte "Authentifizierung", und stellen Sie sicher, dass die 802.1X-Authentifizierung aktiviert ist.



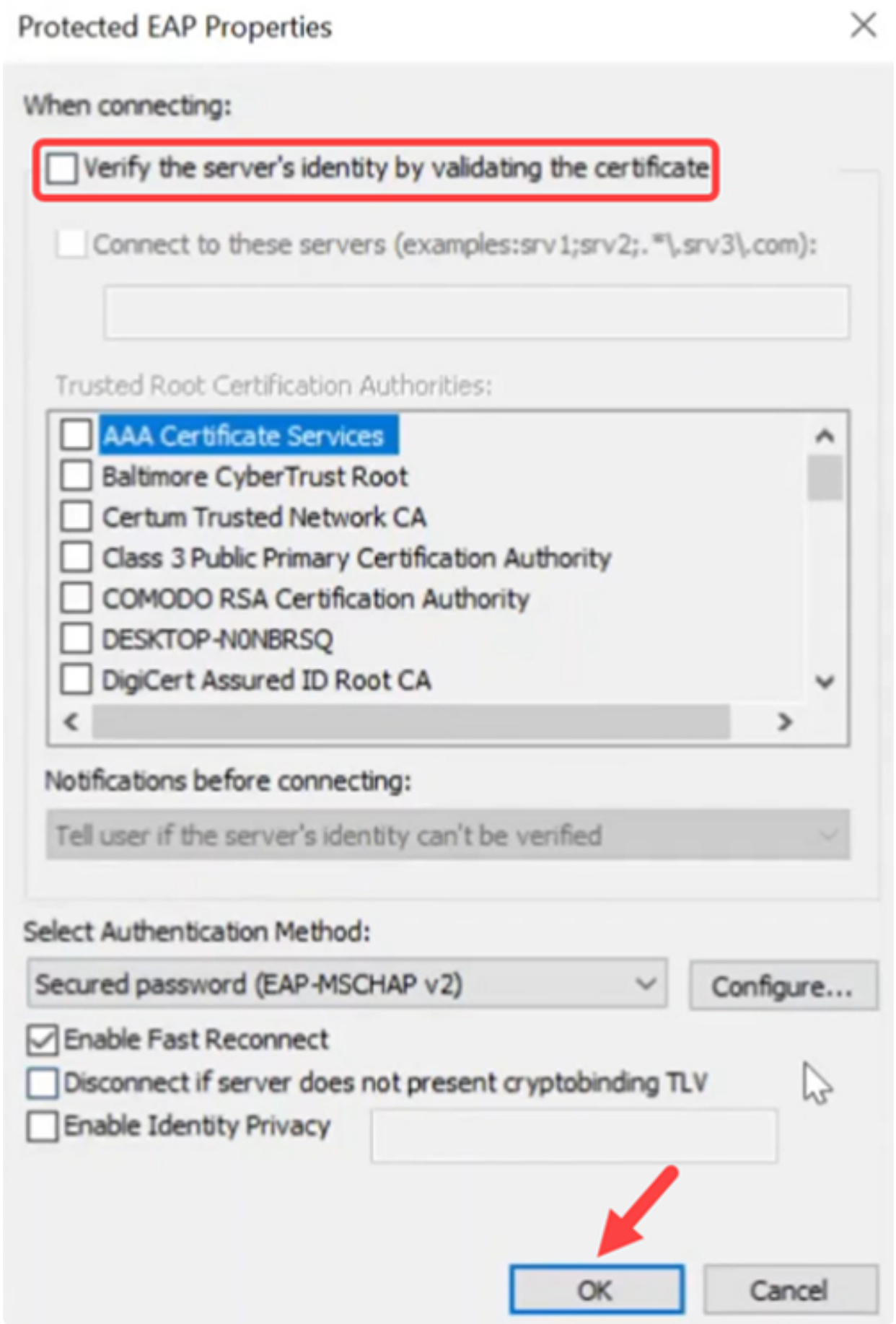
Schritt 3

Wählen Sie unter Zusätzliche Einstellungen die Option Benutzerauthentifizierung als Authentifizierungsmodus aus. Klicken Sie auf Anmeldeinformationen speichern und dann auf OK.



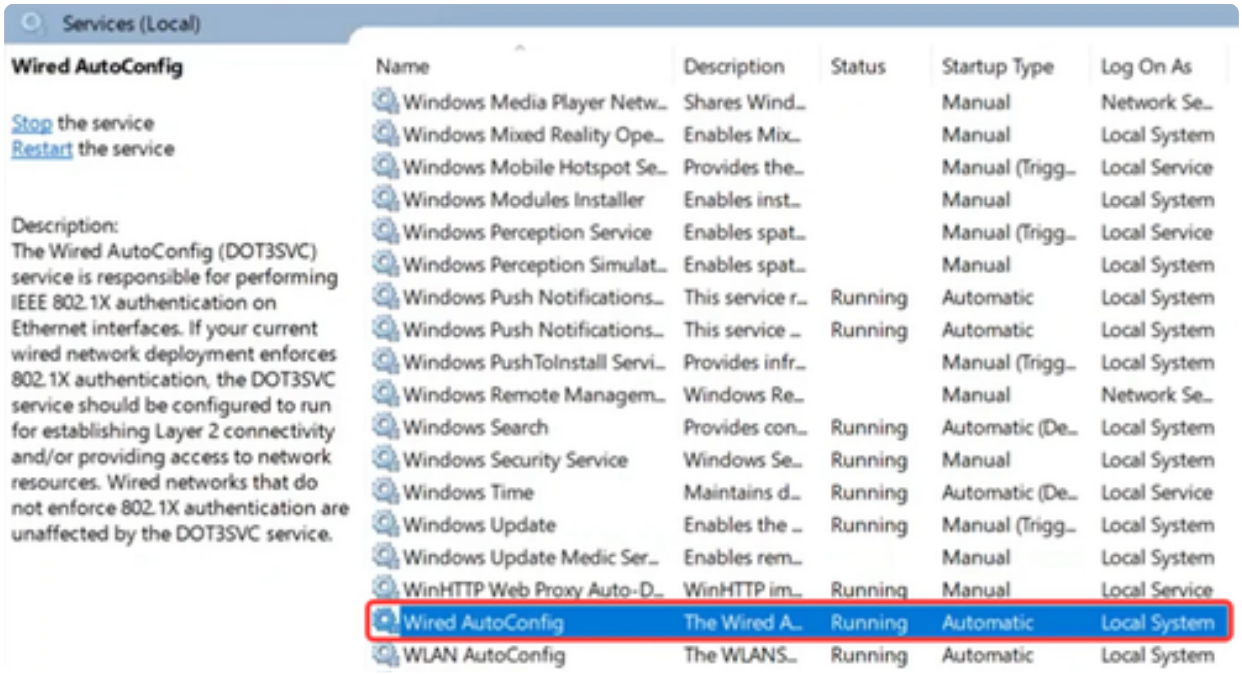
Schritt 4

Klicken Sie auf Einstellungen und stellen Sie sicher, dass das Kästchen neben Identität des Servers durch Validierung des Zertifikats überprüfen deaktiviert ist. Klicken Sie auf OK.


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

Schritt 5

Aktivieren Sie unter Services die Einstellungen für die kabelgebundene Autokonfiguration.

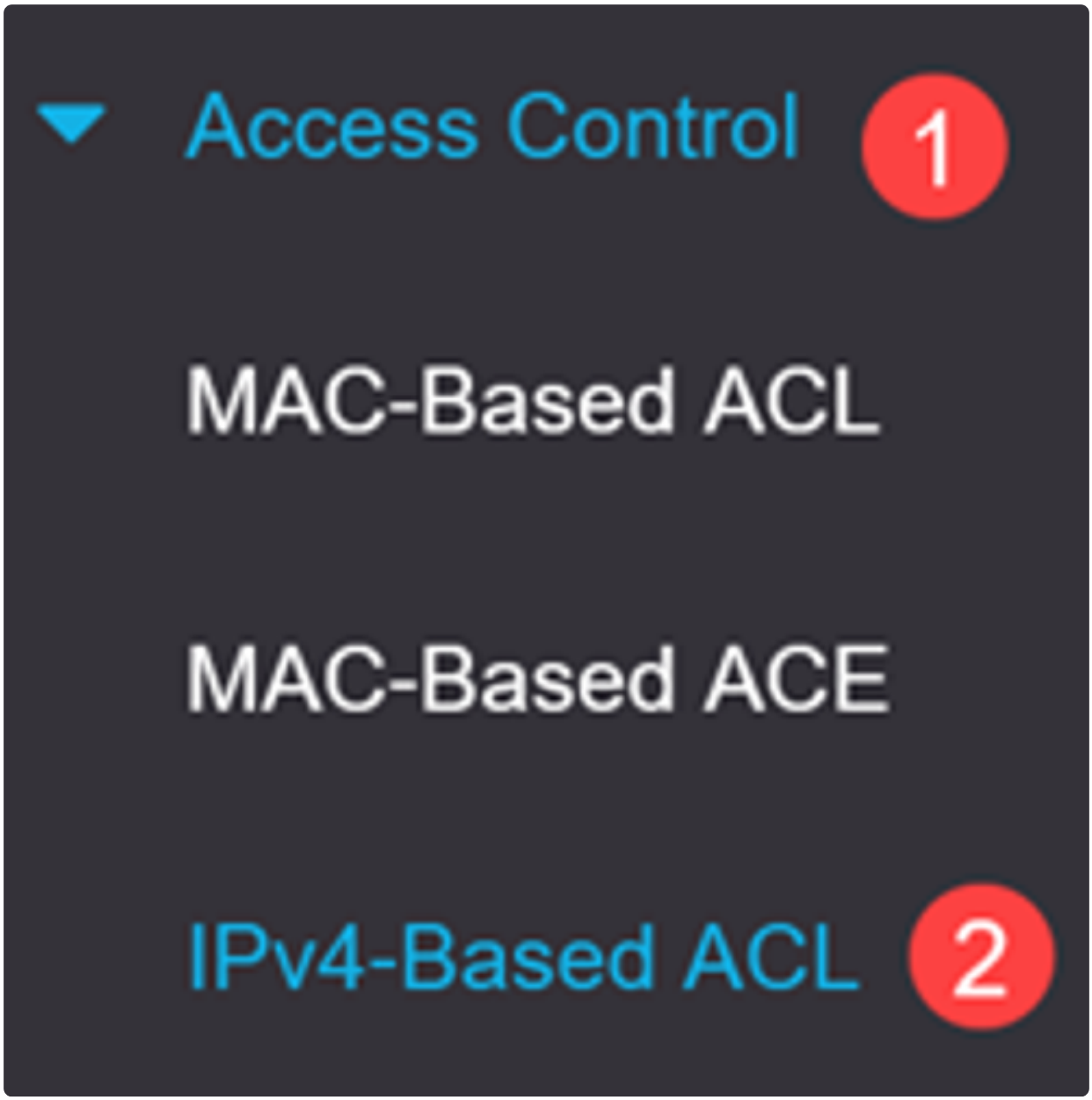


DACL-Verifizierung

Nachdem der Benutzer authentifiziert wurde, können Sie die herunterladbare ACL überprüfen.

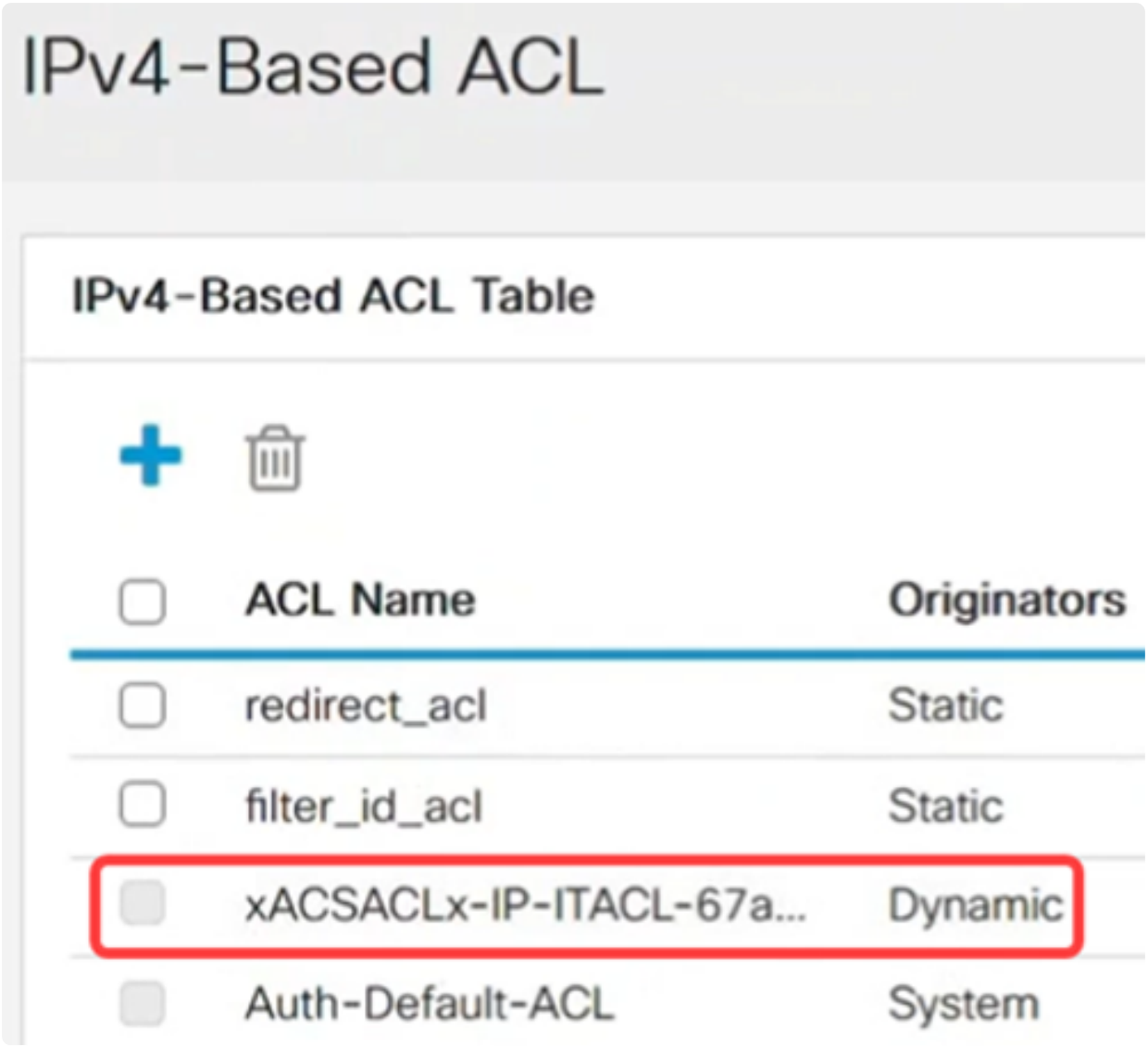
Schritt 1

Melden Sie sich beim Catalyst 1300 Switch an, und navigieren Sie zum Menü Access Control > IPv4-Based ACL (Zugriffskontrolle > IPv4-basierte ACL).



Schritt 2

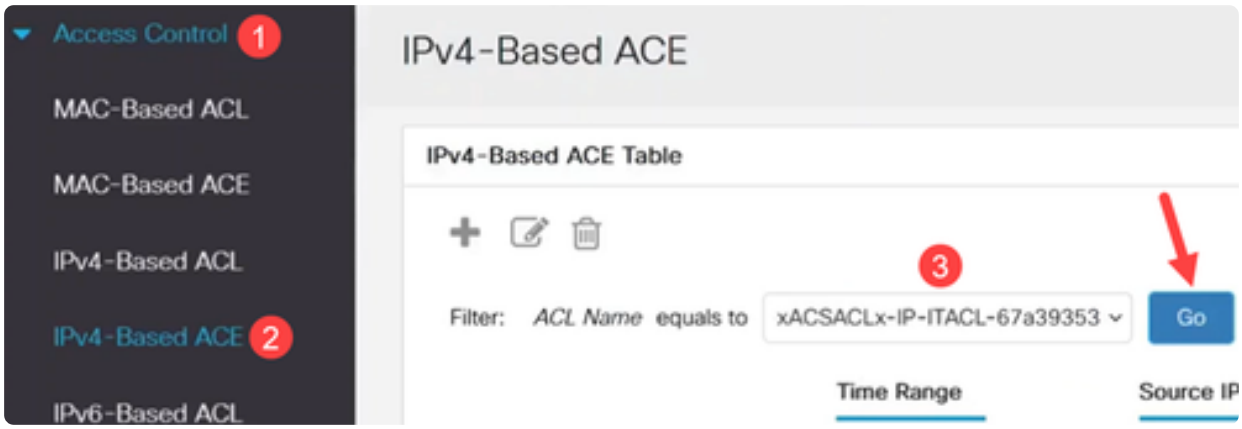
In der Tabelle mit IPv4-basierten ACLs wird die heruntergeladene ACL angezeigt.



Note:
Herunterladbare ACLs können nicht bearbeitet werden.

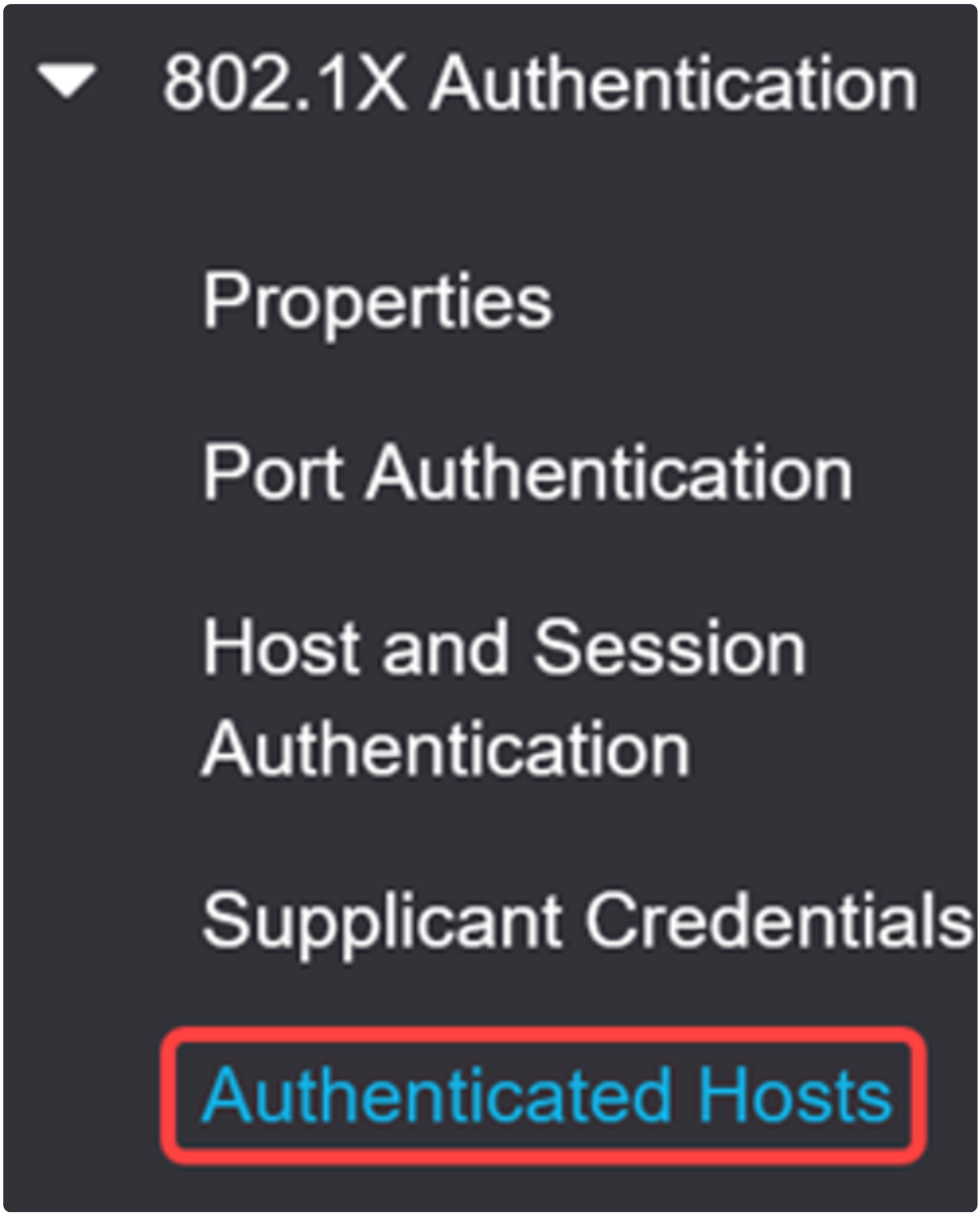
Schritt 3

Sie können auch überprüfen, ob Sie zum IPv4-basierten ACE navigieren, die herunterladbare ACL aus dem Dropdown-Menü ACL Name auswählen und auf Go klicken. Die in der ISE konfigurierten Regeln werden angezeigt.



Schritt 4

Navigieren Sie zum Menü Security > 802.1 Authentication > Authenticated Hosts (Sicherheit > 802.1 Authentifizierung > Authentifizierte Hosts). Sie können die authentifizierten Benutzer überprüfen. Klicken Sie auf Authenticated Sessions, um weitere Details anzuzeigen.



Schritt 5

Führen Sie in der CLI den Befehl show ip access-lists interface gefolgt von der Schnittstellen-ID aus.

In diesem Beispiel werden die auf Gigabit Ethernet 3 angewendeten ACLs und ACEs angezeigt.

```
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
```

Schritt 6

Sie können auch die Einstellungen für die ISE-Verbindung und ACL-Downloads mithilfe des Befehls

show dot1x sessions interface <ID> detailliert. Sie können den Status, den 802.1x-Authentifizierungsstatus und die heruntergeladenen ACLs anzeigen.

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

          Interface: gi1/0/3
        MAC Address: e4:           :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
```

Schlussfolgerung

Da haben Sie es! Jetzt wissen Sie, wie herunterladbare ACL auf Cisco Catalyst 1300-Switches mit der Cisco ISE funktioniert.

Weitere Informationen finden Sie im Administratorhandbuch für Catalyst 1300 und auf der Support-Seite für Cisco Catalyst Switches der Serie 1300.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.