

ACL in Catalyst 1300 Switches

Doel

Het doel van dit artikel is om aan te tonen hoe de downloadbare Access Control List (DACL) werkt op Cisco Catalyst 1300-switches met Cisco Identity Service Engine (ISE).

Toepasselijke apparaten | Softwareversie

- Katalysator 1300-serie | 4.1.6.54

Inleiding

ACL's zijn ACL's die aan een switch-poort zijn toegewezen op basis van een beleid of criteria zoals gebruikersaccountgroep, lidmaatschap, tijdstip van de dag en meer. Dit kunnen lokale ACL's zijn die zijn opgegeven door filter-ID of downloadbare ACL's (DACL).

Downloadbare ACL's zijn dynamische ACL's die worden gemaakt en gedownload van de Cisco ISE-server. Ze passen dynamisch toegangscontroleregels toe op basis van gebruikersidentiteit en apparaattype. DACL heeft het voordeel dat u één centrale repository voor ACL's kunt hebben, dus u hoeft ze niet handmatig op elke switch te maken. Wanneer een gebruiker verbinding maakt met een switch, hoeft deze alleen maar te worden geverifieerd en de switch downloadt de toepasselijke ACL's van de Cisco ISE-server.

Gebruik van downloadbare ACL

- 1 Verschillende gebruikers ontvangen verschillende ACL's wanneer ze verbinding maken met een switch (lokale ISE-gebruikers).
- 2 Gebruikers met beperkte netwerkconnectiviteit kunnen zich aanmelden bij een centraal webportaal voor volledige netwerktoegang (centrale webverificatie).
- 3 Geavanceerd - gebruik van MAC Authentication Bypass (MAB) om communicatie met Windows Active Directory (AD) en enkele gerelateerde services mogelijk te maken terwijl uw ISE-server wordt verbonden met AD en de gebruikersverificatie wordt gecontroleerd. Voordat u zich aanmeldt bij Windows AD, biedt het netwerk alleen toegang tot zeer beperkte bronnen, maar de AD-verificatie downloadt verschillende ACL's op basis van Windows-groepen en biedt volledige netwerktoegang.
- 4 Geavanceerd - Gebruikers ontvangen verschillende ACL's op basis van de dag van de week, het tijdstip van de dag of een andere factor vanwege het beleid op de ISE-server.

In dit artikel wordt de eerste use case uitvoerig besproken.

Inhoud

- [RADIUS-client configureren](#)
- [802.1x-verificatie configureren](#)
- [Cisco ISE-serverconfiguratie voor downloadbare ACL](#)
- [Clientconfiguraties](#)
- [DACL-verificatie](#)

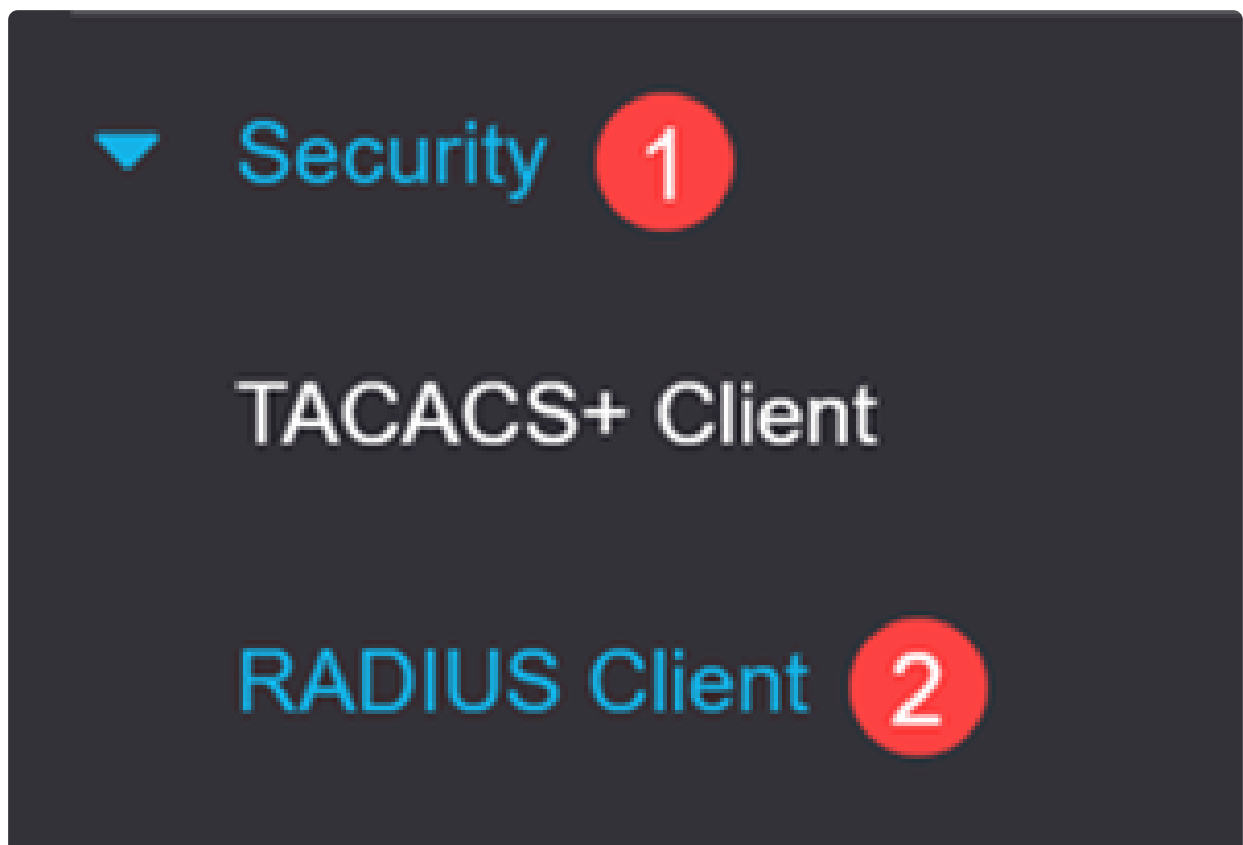
Voorwaarden

- Zorg ervoor dat uw Catalyst 1300-switch is bijgewerkt naar de nieuwste firmware (de firmware van de switch moet 4.1.6 of hoger zijn).
- Wijs een statisch IP-adres toe aan de switch voor beheerdoeleinden.

RADIUS-client configureren

Stap 1

Meld u aan bij de Catalyst 1300-switch en navigeer naar Beveiliging > RADIUS-clientmenu.



Stap 2

Selecteer voor RADIUS-boekhouding de optie Port Based Access Control (Toegangsbeheer op basis van poort).

RADIUS Client

RADIUS Accounting for Management Access can only be enabled when **TACACS+ Accounting** is disabled. TACACS+ Accounting is currently Disabled.

RADIUS Accounting: ☒ Port Based Access Control (802.1X, MAC Based)

☐ Management Access

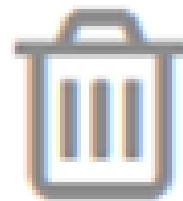
☐ Both Port Based Access Control and Management Access

☐ None

Stap 3

Klik onder RADIUS-tabel op het pluspictogram om de Cisco ISE-server toe te voegen.

RADIUS Table



Stap 4

Voer de Cisco ISE Server-gegevens in en klik op Toepassen.

Add RADIUS Server

X

Server Definition:

☒ By IP address ☐ By name

IP Version:

☐ Version 6 ☒ Version 4

IPv6 Address Type:

☒ Link Local ☐ Global

Link Local Interface:

Gi3

Server IP Address/Name:

Priority:

(Range: 0 - 65535)

Key String:

☒ Use Default

☐ User Defined (Encrypted)

☐ User Defined (Plaintext)

(0-128 characters used)

Timeout for Reply:

☒ Use Default

☐ User Defined

Default

 sec (Range: 1 - 30, Default: 3)

Authentication Port:

1812

(Range: 0 - 65535, Default: 1812)

Retries:

☒ Use Default

☐ User Defined

Default

 (Range: 1 - 15, Default: 3)

Dead Time:

☒ Use Default

☐ User Defined

Default

 min (Range: 0 - 2000, Default: 0)

Usage Type:

☐ Login

☐ 802.1x

☒ All

Apply

Close

Note:

Het gebruikstype moet zijn geselecteerd als 802.1x.

802.1x-verificatie configureren

Stap 1

Navigeer naar Beveiliging > 802.1X-verificatie > menu Eigenschappen.

▼ Security **1**

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Login Settings

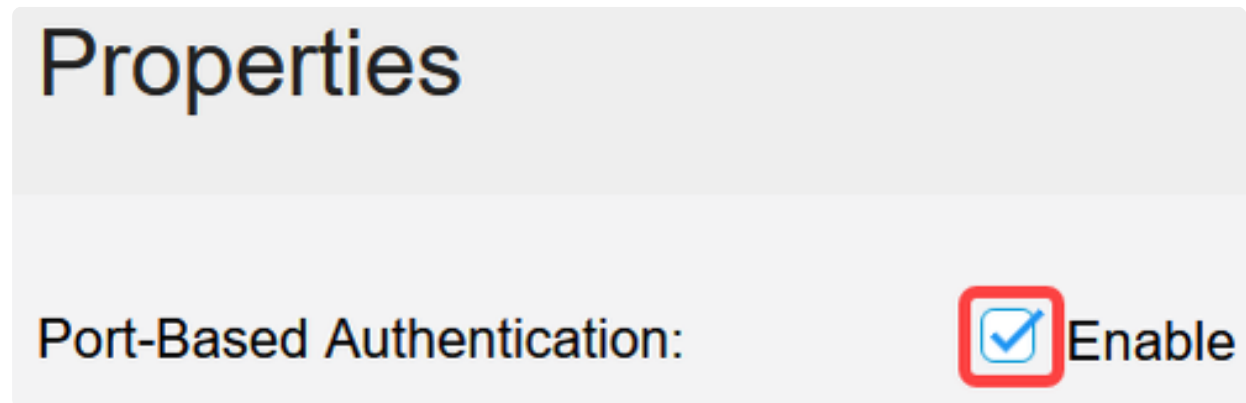
Login Protection Status

▶ Mgmt Access Method

Management Access

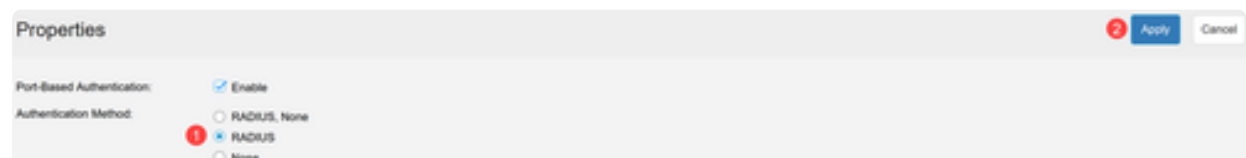
Stap 2

Klik op het selectievakje om Port-Based Authentication (Poortgebaseerde verificatie) in te schakelen.



Stap 3

Selecteer onder Verificatiemethode de optie RADIUS en klik op Toepassen.



Stap 4

Ga naar Beveiliging > 802.1X-verificatie > Poortverificatie menu. Selecteer de poort waarop uw laptop is aangesloten en klik op het pictogram Bewerken. In dit voorbeeld wordt GE8 geselecteerd.

Port Authentication



Filter: *Interface Type* equals to

Port of Unit 1 ▾

Go

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment
☐	1	GE1	Authorized	Force Authorized	Disabled
☐	2	GE2		Force Authorized	Disabled
☐	3	GE3		Force Authorized	Disabled
☐	4	GE4		Force Authorized	Disabled
☐	5	GE5		Force Authorized	Disabled
☐	6	GE6		Auto	Disabled
☒	7	GE7		Force Authorized	Disabled
☒	8	GE8	Authorized	Auto	Disabled
☐	9	GE9	Authorized	Force Authorized	Disabled

Stap 5

Selecteer het beheerpoortbesturingselement als automatisch en schakel 802.1x-gebaseerde verificatie in. Klik op Apply (Toepassen).

Edit Port Authentication

Interface: Unit Port

Current Port Control: Authorized

Administrative Port Control: ☐ Force Unauthorized ☒ Auto ☐ Force Authorized

RADIUS VLAN Assignment: ☒ Disable ☐ Reject ☐ Static

Guest VLAN: ☐ Enable

Open Access: ☐ Enable

802.1x Based Authentication: ☒ Enable ☐ Disable

MAC Based Authentication: ☐ Enable

Web Based Authentication: ☐ Enable

Periodic Reauthentication: ☒ Enable

Cisco ISE-serverconfiguratie voor downloadbare ACL

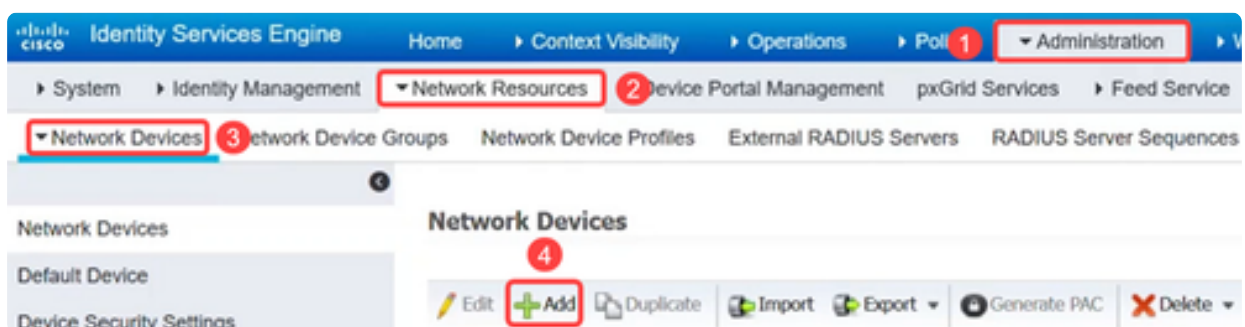
Note:

ISE-configuratie valt buiten het bereik van Cisco Business Support. Raadpleeg de [ISE-beheerdershandleiding](#) voor meer informatie.

De configuraties in dit artikel zijn een voorbeeld voor downloadbare ACL om te werken met Cisco Catalyst 1300-serie switch.

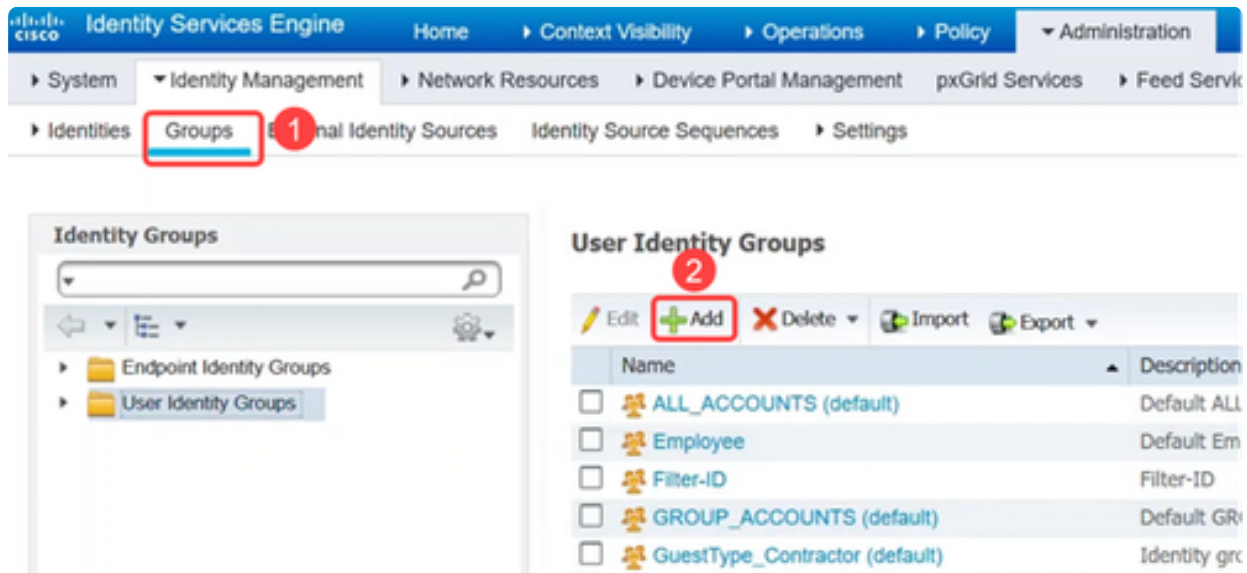
Stap 1

Meld u aan bij uw Cisco ISE-server en navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten en voeg het Catalyst switch-apparaat toe.



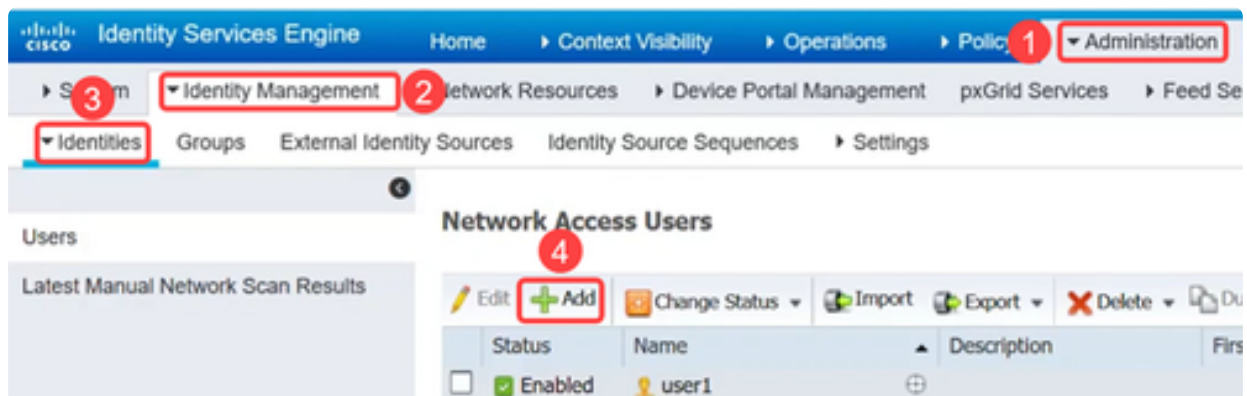
Stap 2

Om gebruikersidentiteitsgroepen te maken, bladert u naar het tabblad Groepen en voegt u de gebruikersidentiteitsgroepen toe.



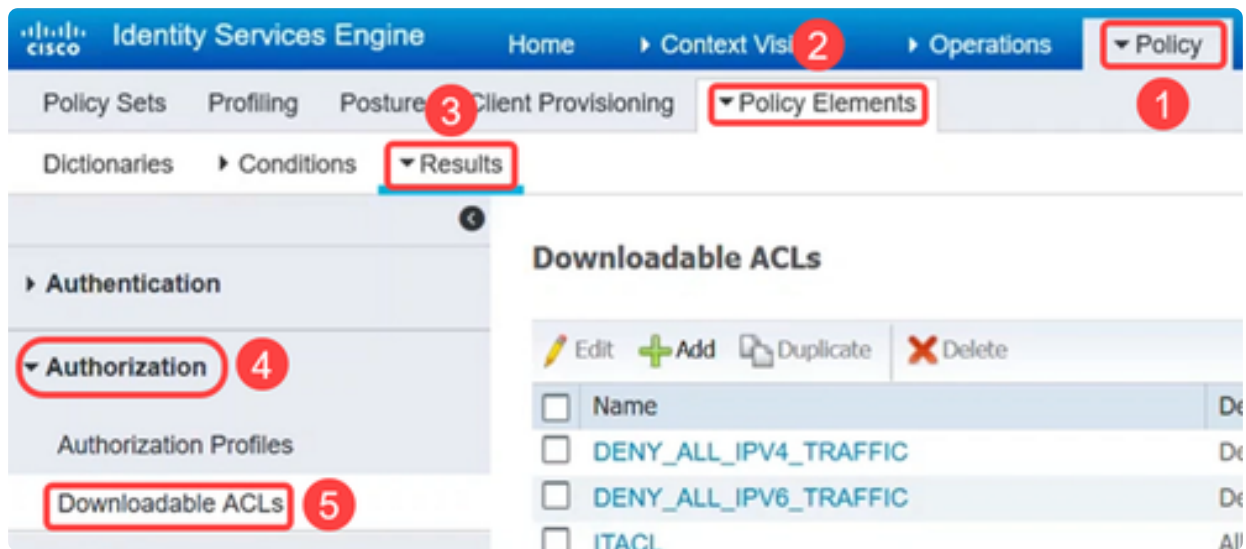
Stap 3

Ga naar het menu Beheer > Identiteitsbeheer > Identiteiten om de gebruikers te definiëren en de gebruikers aan de groepen toe te wijzen.



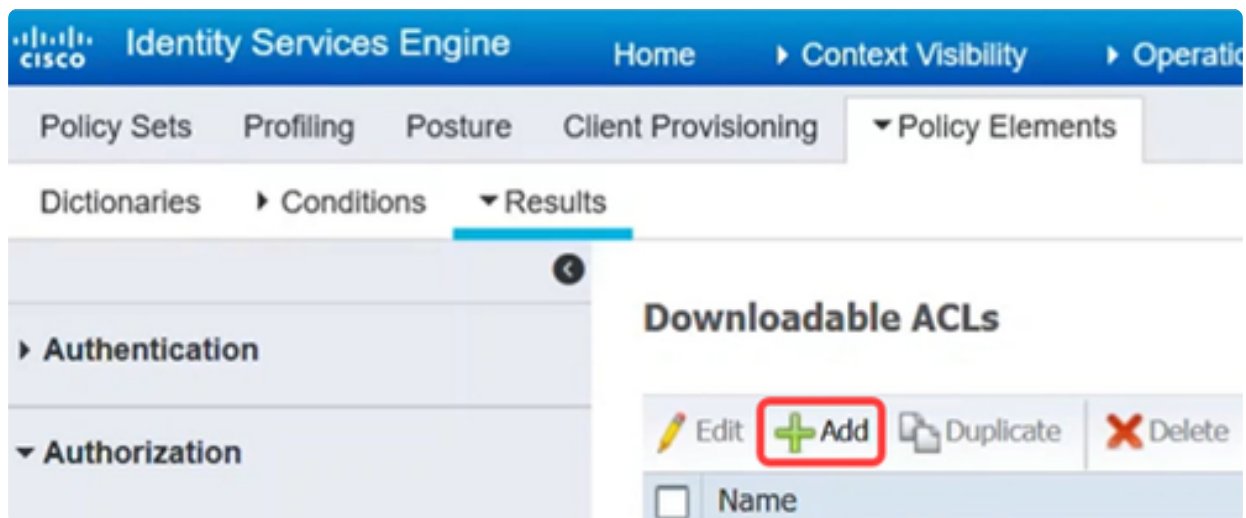
Stap 4

Navigeer naar Beleid > Beleidselementen > Resultaten menu. Klik onder Autorisatie op Downloadbare ACL's.



Stap 5

Klik op het pictogram Toevoegen om de downloadbare ACL te maken.



Stap 6

Configureer de naam, beschrijving, selecteer de IP-versie en voer de toegangscontrole-items (ACE's) in waaruit de downloadbare ACL bestaat in het veld DACL-inhoud. Klik op Save (Opslaan).

Downloadable ACL

* Name

Description

IP version ☒ IPv4 ☐ IPv6 ☐ Agnostic 

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	



► Check DACL Syntax

Save

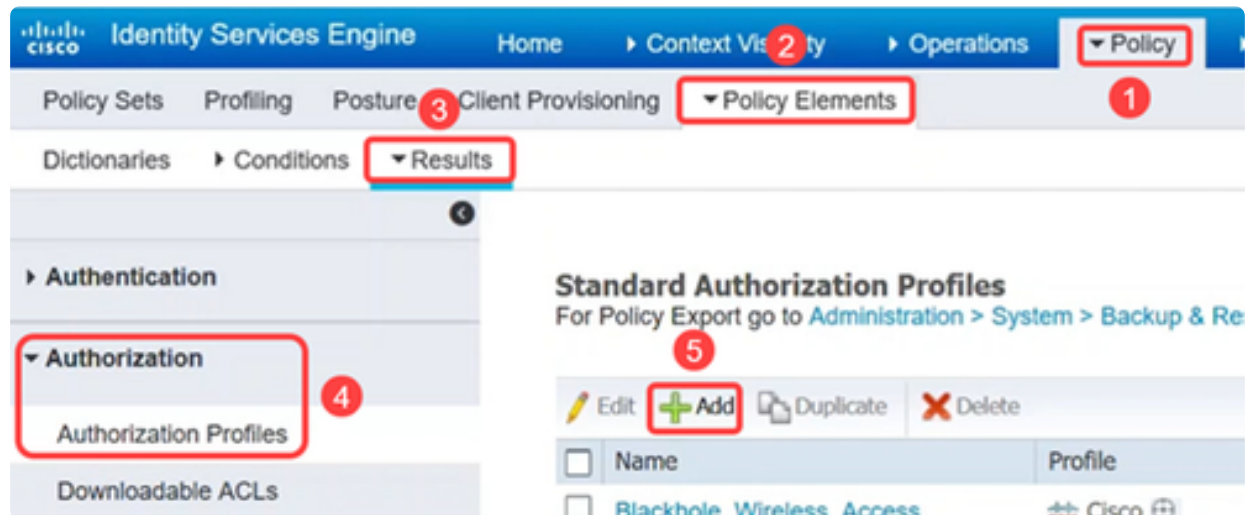
Reset

Note:

Alleen IP-ACL's worden ondersteund en de bron moet ELKE zijn. Voor ACL op ISE wordt nu alleen IPv4 ondersteund. Als een ACL wordt ingevoerd met een andere bron, terwijl de syntaxis prima kan zijn wat ISE betreft, zal het falen wanneer toegepast op de switch.

Machtigingsprofielen maken die worden gebruikt om uw DACL en andere beleidsregels logisch aan elkaar te koppelen binnen de ISE-beleidssets.

Ga hiervoor naar **Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen** en klik op **Toevoegen**.



Stap 8

Configureer op de pagina Autorisatieprofiel het volgende:

- Naam
- Beschrijving
- Toegangstype - dit moet worden ingesteld op ACCESS_ACCEPT. Als deze optie is ingesteld op ACCESS_REJECT, wordt de verificatie geweigerd.
- Netwerkkapparaatprofiel – dit moet worden geselecteerd als Cisco.
- Passive Identity Tracking - moet mogelijk worden ingeschakeld voor bepaalde verificatiescenario's. Het is vereist voor EasyConnect_PassiveID-scenario's die zijn gekoppeld aan AD.
- Algemene taken – Deze sectie heeft veel opties. In dit voorbeeld is DACL Name geconfigureerd.

Klik op **Save (Opslaan)**.

Authorization Profile

* Name	IT_Auth
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	 Cisco 
Service Template	☐
Track Movement	☐ 
Passive Identity Tracking	☒ 

▼ Common Tasks

Stap 9

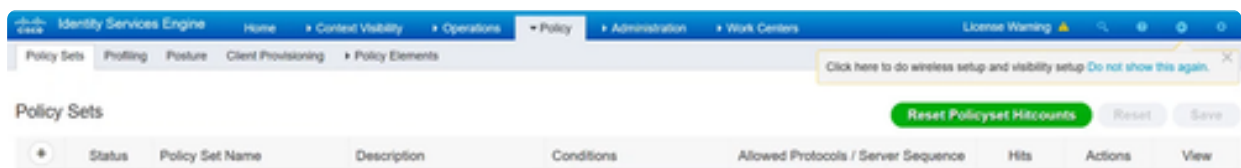
Als u beleidssets wilt configureren die logische groepen van verificatie- en autorisatiebeleid zijn, klikt u op **Beleid > Beleidsreeksen** in het menu.

U kunt het volgende bekijken bij het bekijken van een lijst met beleidssets:

- Status - Een groen vinkje geeft aan dat het is ingeschakeld, een leeg wit cirkeltje geeft aan dat het is uitgeschakeld en een oogpictogram is voor een configuratie die alleen op de monitor wordt weergegeven.
- Naam en beschrijving van beleidsset - spreken voor zich
- Voorwaarden - bepalen waar de beleidsset van toepassing is.
- Toegestane protocollen/serverreeks - stelt meer geavanceerde besturingselementen in.
- Hits - het aantal keren weergegeven dat de beleidsset is gebruikt.
- Acties - hiermee kunt u de volgorde wijzigen waarin beleidssets kunnen worden toegepast, een

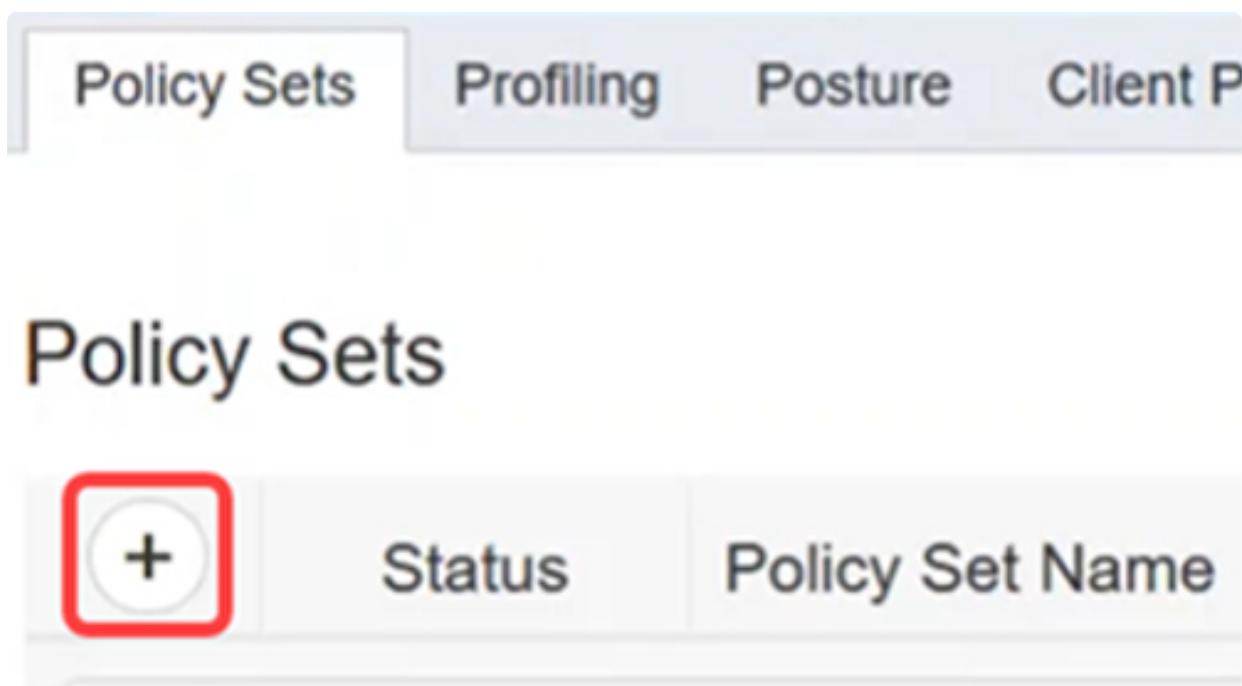
bestaande beleidsset kopiëren of een bestaande beleidsset verwijderen.

- Bekijken - hiermee kunt u de details van de beleidsset bewerken.



Stap 10

Als u een beleidsset wilt maken, klikt u op de knop Toevoegen.



Stap 11

Definieer een naam voor de beleidsset.

Policy Sets

	Status	Policy Set Name
Search		
		DACL_Policy

Stap 12

Klik onder Voorwaarden op de knop Toevoegen. Dit opent de Conditions Studio waar u kunt definiëren waar dit verificatieprofiel wordt gebruikt. In dit voorbeeld is het toegepast op het Radius-NAS-IP-adres (de switch) dat 172.19.1.250 en bekabeld_802.1x-verkeer is.

	Conditions	Allowed P
AND	 Radius-NAS-IP-Address EQUALS 172.19.1.250  Wired_802.1X	

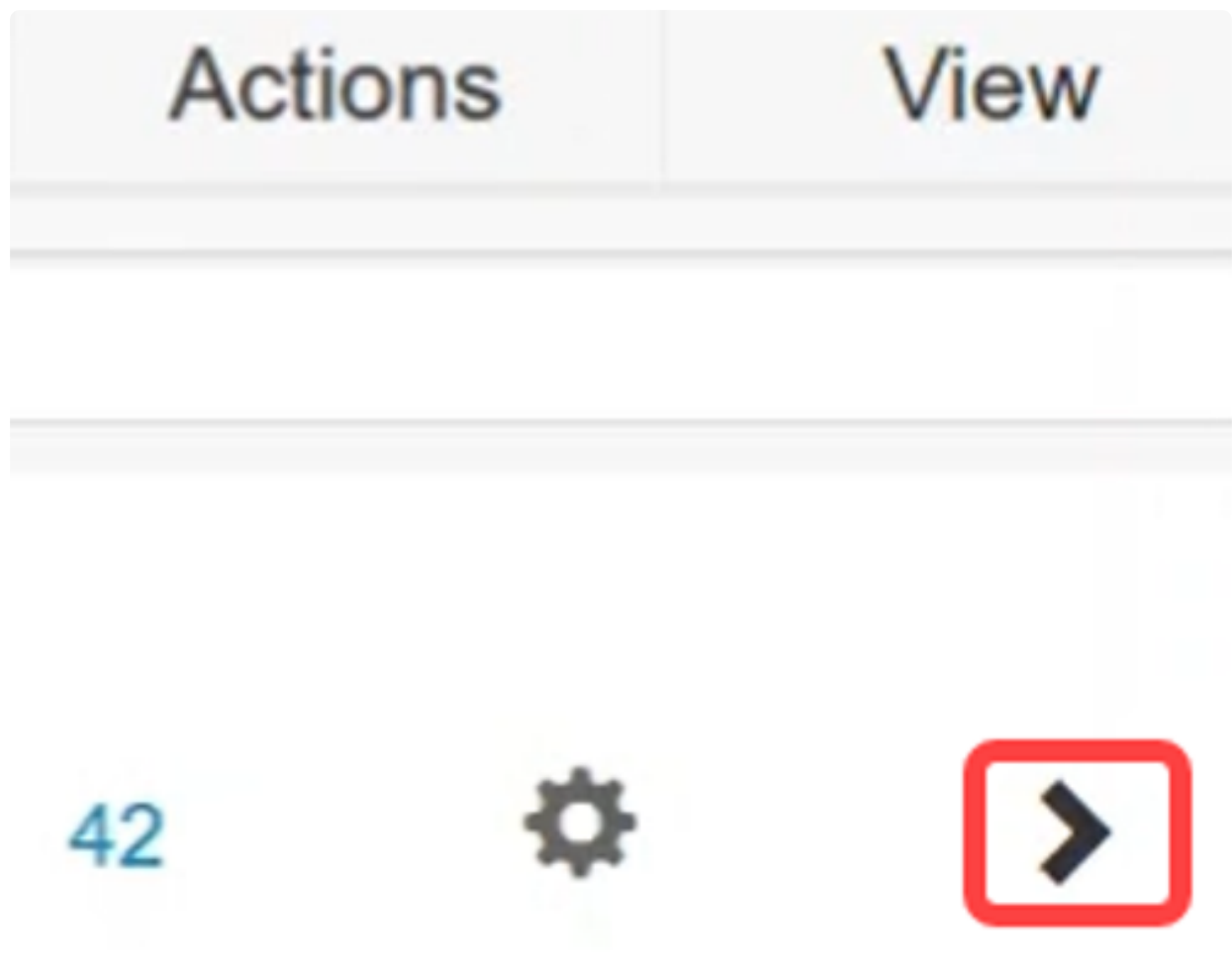
Stap 13

Configureer de toegestane protocollen voor de standaardnetwerktogang en klik op Opslaan.



Stap 14

Klik onder Weergave op het pijltje om het verificatie- en autorisatiebeleid te configureren op basis van de netwerkconfiguratie en -vereisten of u kunt de standaardinstellingen kiezen. Klik in dit voorbeeld op Autorisatiebeleid.



Stap 15

Klik op het plus-pictogram om een beleid toe te voegen.

➤	Authentication Policy
➤	Authorization Policy - Local Exceptions
➤	Authorization Policy - Global Exceptions
➤	Authorization Policy

Stap 16

Voer de naam van de regel in.

+	Status	Rule Name
Search		



SalesUser_Policy

Stap 17

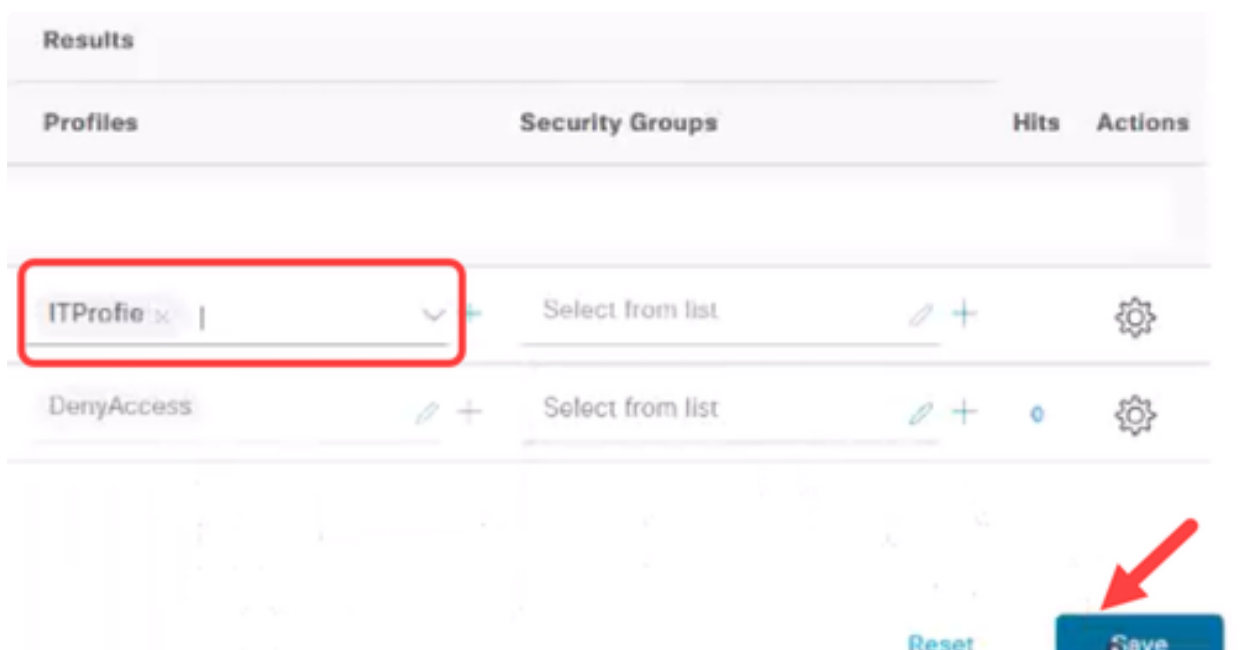
Klik onder Voorwaarden op het plus-pictogram en selecteer de identiteitsgroep. Klik op

Gebruiken.



Stap 18

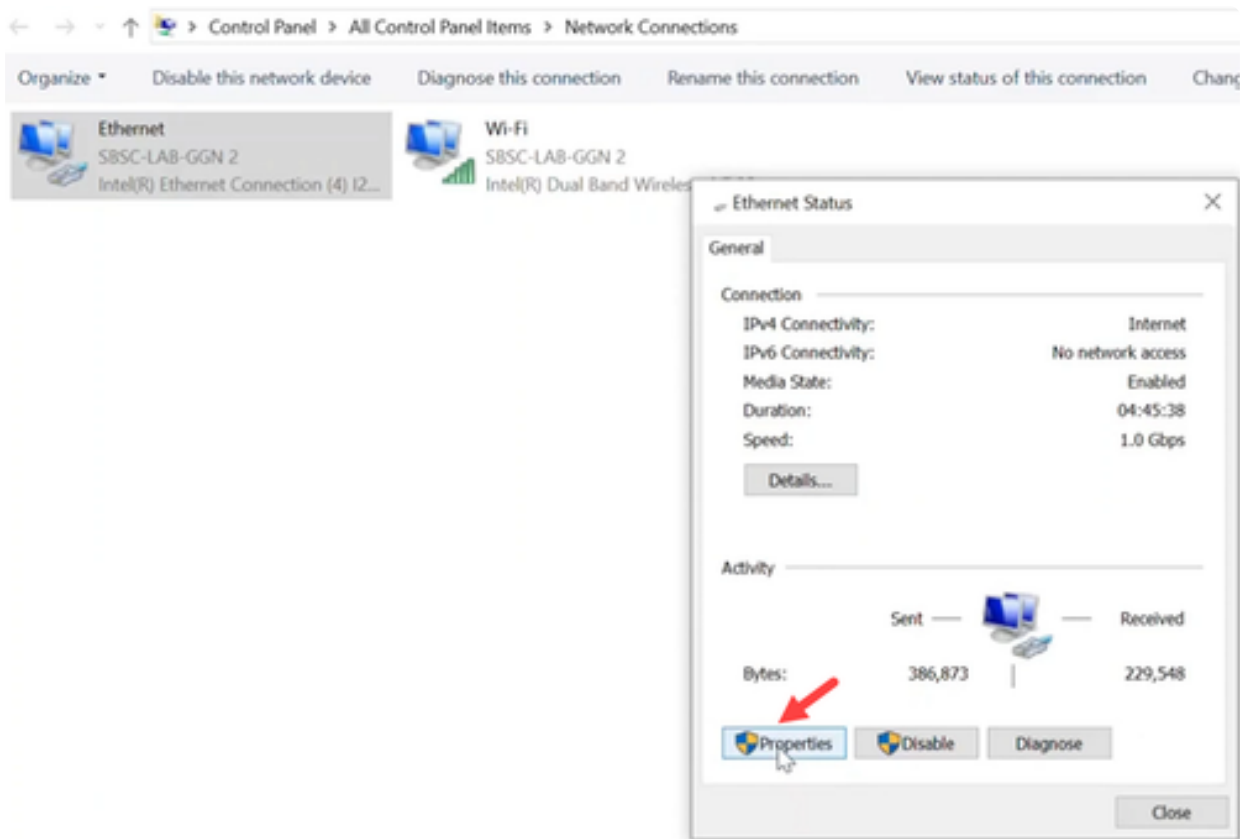
Pas het gewenste profiel toe en klik op Opslaan.



Clientconfiguraties

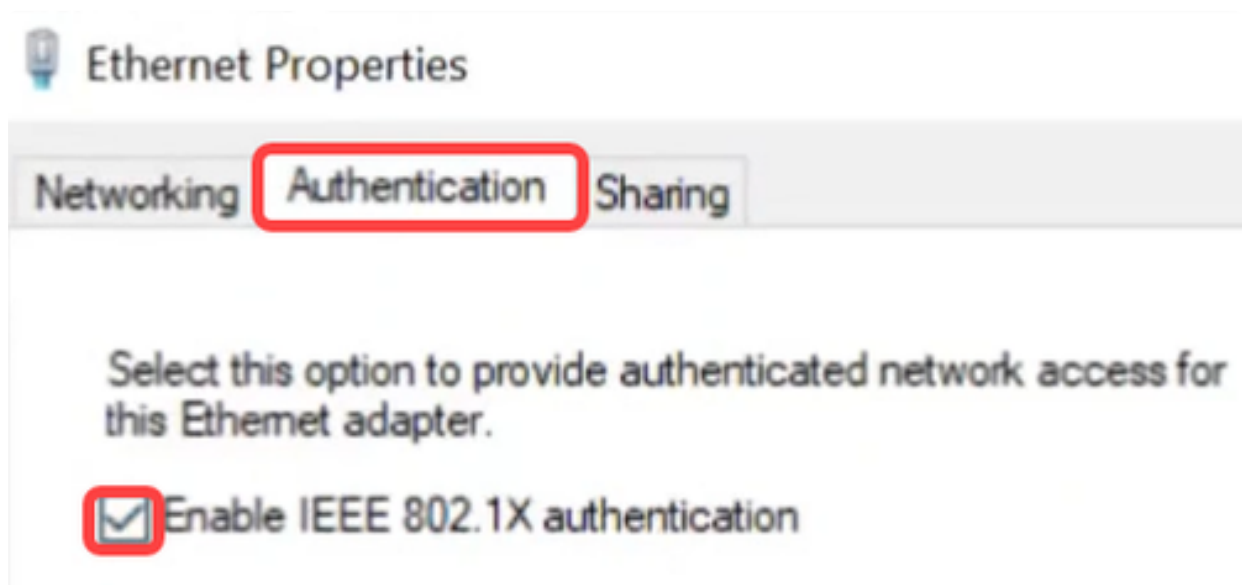
Stap 1

Navigeer op de clientlaptop naar Netwerkverbindingen > Ethernet en klik op Eigenschappen.



Stap 2

Klik op het tabblad Verificatie en controleer of 802.1X-verificatie is ingeschakeld.



Stap 3

Selecteer onder Aanvullende instellingen de optie Gebruikersverificatie als verificatiemodus. Klik op Inloggegevens opslaan en vervolgens op OK.

Advanced settings ✕

802.1X settings

☒ Specify authentication mode

User authentication Replace credentials

☐ Delete credentials for all users

☐ Enable single sign on for this network

☒ Perform immediately before user logon

☐ Perform immediately after user logon

Maximum delay (seconds): 10

☒ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication

OK Cancel



Stap 4

Klik op Instellingen en zorg ervoor dat het vakje naast Verifiëren van de identiteit van de server door het valideren van het certificaat is uitgeschakeld. Klik op 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

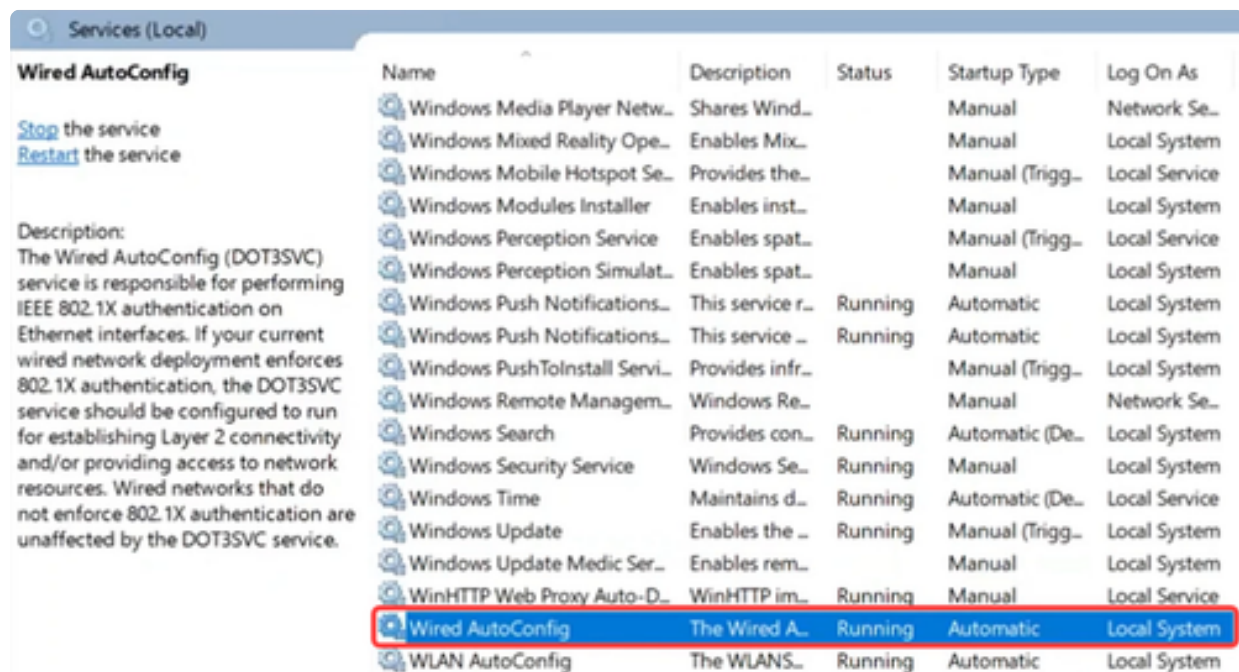
☐ Enable Identity Privacy

OK

Cancel

Stap 5

Schakel onder Services de instellingen voor bekabelde automatische configuratie in.



DACL-verificatie

Zodra de gebruiker is geverifieerd, kunt u de downloadbare ACL controleren.

Stap 1

Meld u aan bij de Catalyst 1300-switch en navigeer naar Toegangscontrole > Op IPv4 gebaseerde ACL-menu.



Access Control

1

MAC-Based ACL

MAC-Based ACE

IPv4-Based ACL

2

Stap 2

De ACL-tabel op basis van IPv4 geeft de gedownloade ACL weer.

IPv4-Based ACL

IPv4-Based ACL Table



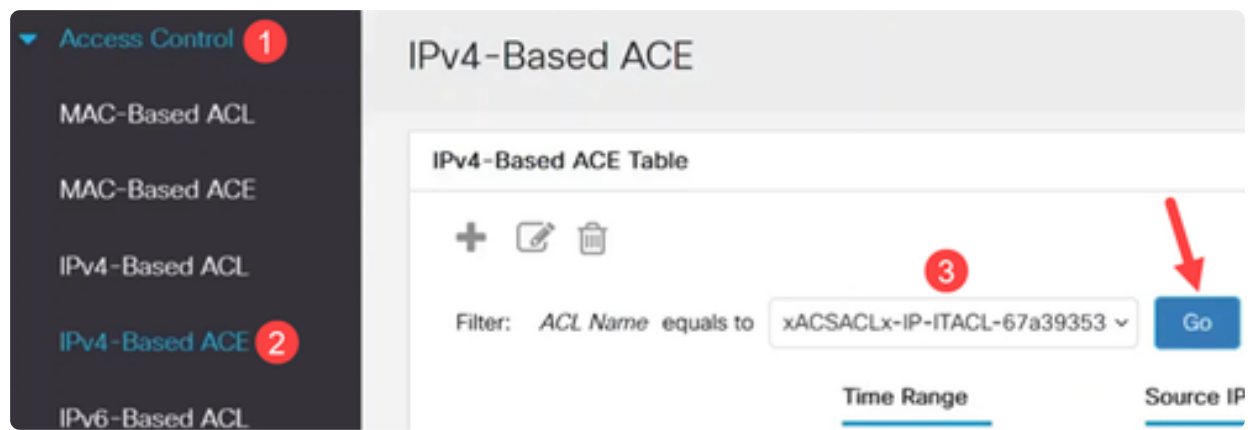
☐	ACL Name	Originators
☐	redirect_acl	Static
☐	filter_id_acl	Static
☐	xACSACLx-IP-ITACL-67a...	Dynamic
☐	Auth-Default-ACL	System

Note:

Downloadbare ACL's kunnen niet worden bewerkt.

Stap 3

Een andere manier om te controleren is om naar IPv4-gebaseerde ACE te navigeren, selecteer de downloadbare ACL in het vervolgkeuzemenu ACL-naam en klik op Go. De regels die in ISE zijn geconfigureerd, worden weergegeven.



Stap 4

Navigeer naar Beveiliging > 802.1-verificatie > Het menu Geverifieerde hosts. U kunt controleren welke gebruikers zijn geverifieerd. Klik op Authenticated Sessions voor meer informatie.

▼ 802.1X Authentication

Properties

Port Authentication

Host and Session
Authentication

Supplicant Credentials

Authenticated Hosts

Stap 5

Voer vanuit de CLI de opdracht `show ip access-lists interface` uit, gevolgd door de interface-ID.

In dit voorbeeld zijn ACL's en ACE's toegepast op Gigabit Ethernet 3 te zien.

```
switch4a7d55#show ip access-lists interface gel/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
```

Stap 6

U kunt ook instellingen zien met betrekking tot de ISE-verbinding en ACL-downloads met behulp van de opdracht

tonen dot1x sessies interface <ID> gedetailleerd. U kunt de status, de 802.1x-verificatiestatus en de gedownload ACL's bekijken.

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

Interface: gil/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
```

Conclusie

Daar ga je! Nu weet u hoe downloadbare ACL werkt op Cisco Catalyst 1300-switches met Cisco ISE.

Raadpleeg de [Catalyst 1300-beheerdershandleiding](#) en de [ondersteuningspagina](#) van de [Cisco Catalyst 1300-reeks voor](#) meer informatie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.