

Problemen met bekabelde Dot1x oplossen in ISE 3.2 en Windows

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

Inleiding

Dit document beschrijft hoe u een 802.1X PEAP-verificatie kunt configureren voor Identity Services Engine (ISE) 3.2 en een Windows-native applicatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Protected Extensible Verification Protocol (PEAP)
- PEAP 802.1x

Gebruikte componenten

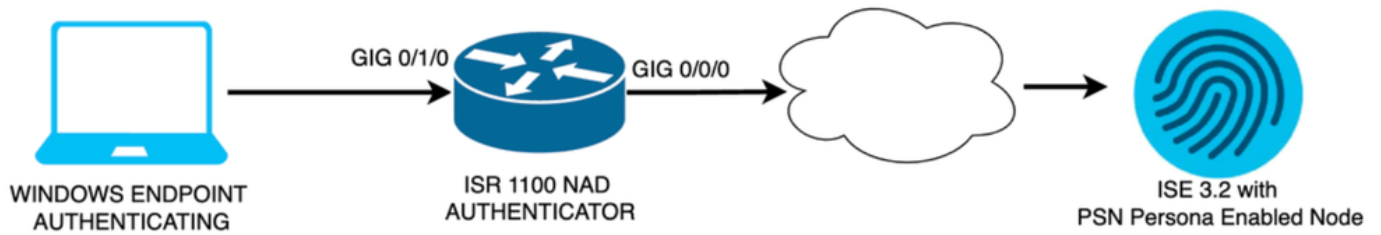
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine (ISE) versie
- Cisco C117 Cisco IOS® XE-software, versie 17.12.02
- Laptop met Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdigram



Netwerkdigram

Configuraties

Voer de volgende stappen uit om te configureren:

Stap 1. Configureer ISR 1100 router.

Stap 2. Identity Service Engine configureren 3.2.

Stap 3. Configureer de Windows-native applicatie.

Stap 1. ISR 1100 router configureren

In dit gedeelte wordt de basisconfiguratie uitgelegd die de NAD minimaal moet hebben om dot1x te kunnen laten werken.



Opmerking: voor ISE-implementatie met meerdere knooppunten moet u het IP van het knooppunt configureren waarvoor de PSN-persoonlijkheid is ingeschakeld. Dit kan worden ingeschakeld als u naar ISE navigeert onder het tabblad Beheer > Systeem > Implementatie.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
```

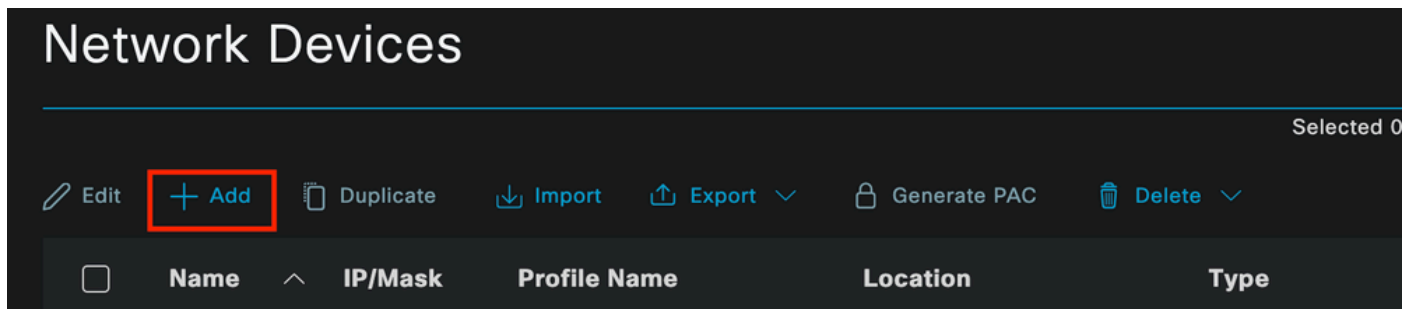
```
key <Your shared secret>
!  
!  
aaa group server radius ISE-CLUSTER  
server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
description "Endpoint that supports dot1x"  
switchport access vlan 15  
switchport mode access  
authentication host-mode multi-auth  
authentication order dot1x mab  
authentication priority dot1x mab  
authentication port-control auto  
dot1x pae authenticator  
spanning-tree portfast
```

Stap 2. Identity Service Engine configureren 3.2.

2. a. Het te gebruiken netwerkapparaat configureren en toevoegen voor de verificatie.

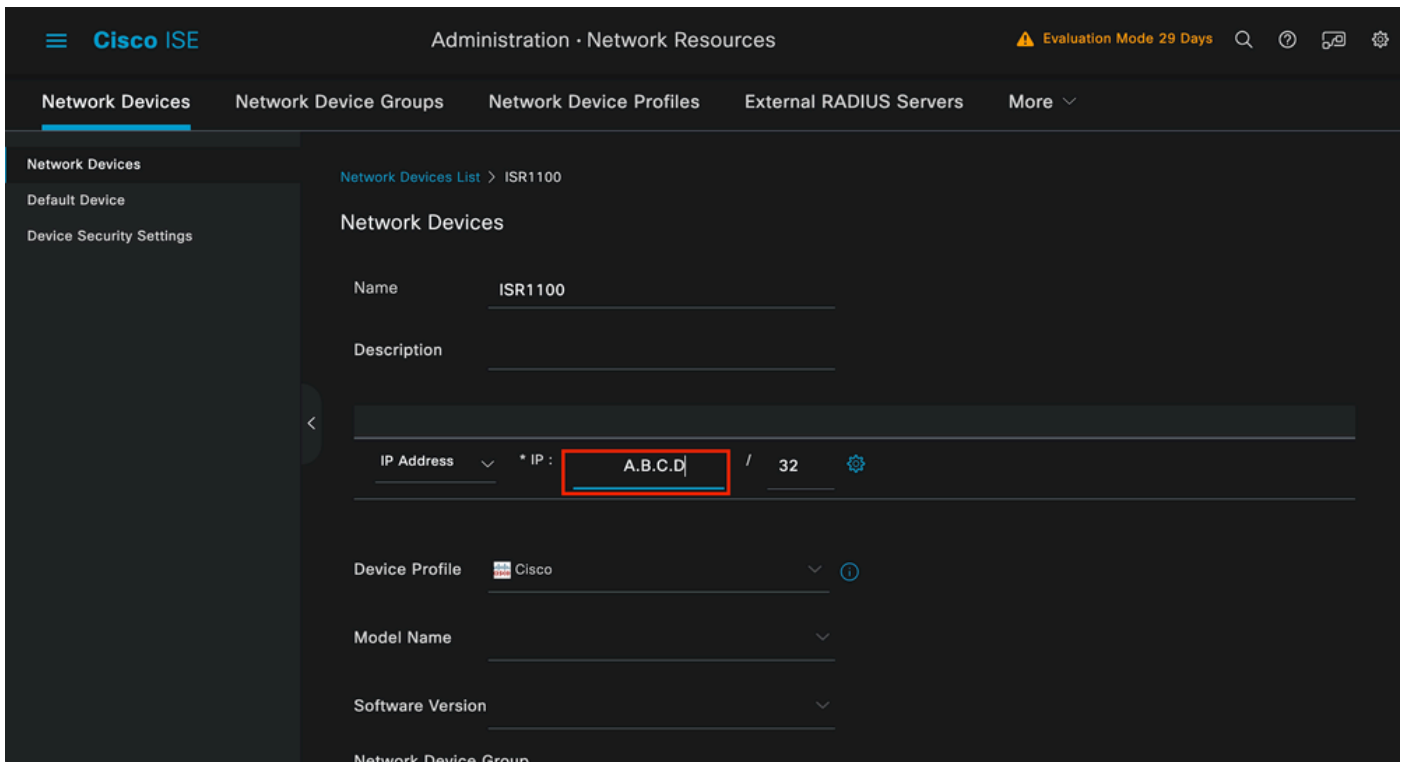
Voeg het gedeelte Netwerkapparaat toe aan het gedeelte ISE-netwerkapparaten.

Klik op de knop Toevoegen om te beginnen.



ISE-netwerkapparaten

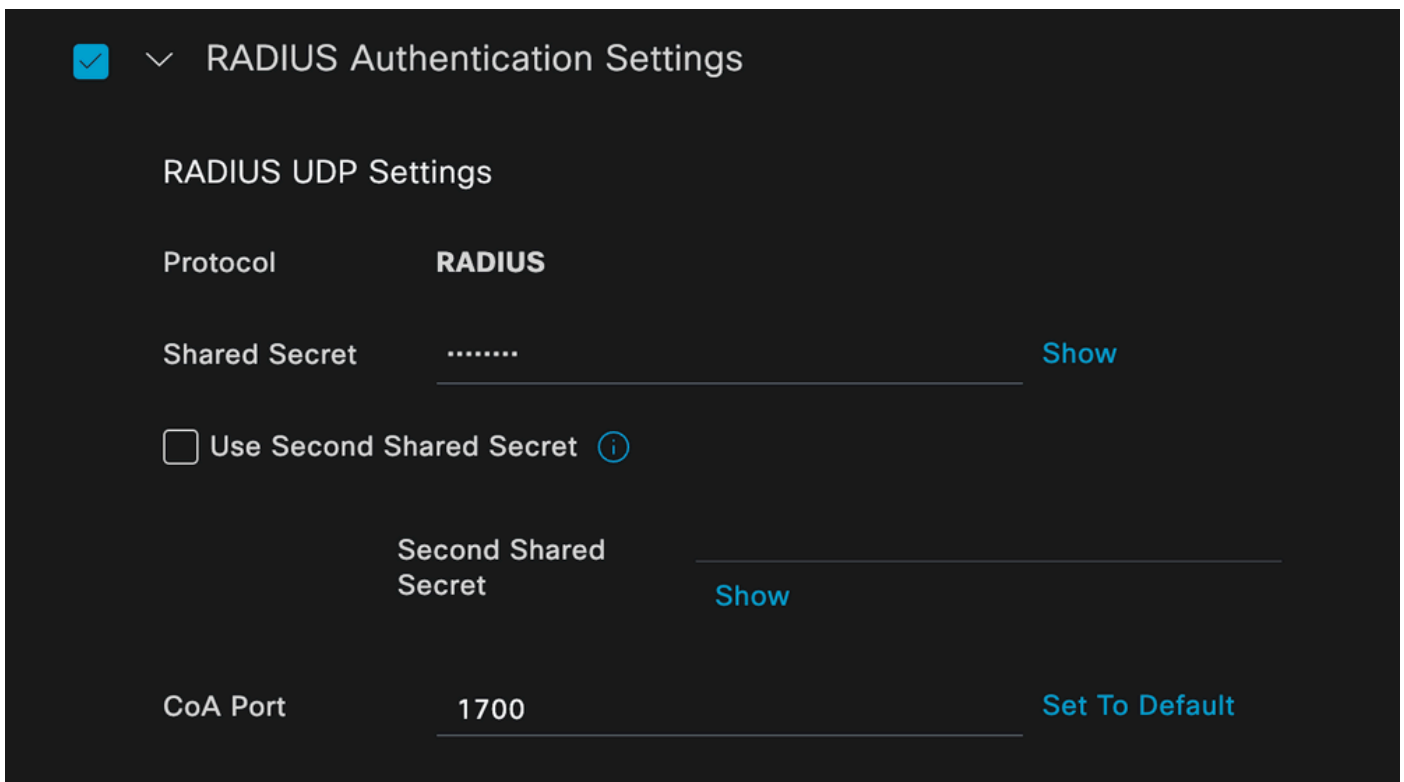
Voer de waarden in, wijs een naam toe aan de NAD die u maakt en voeg ook de IP toe die het netwerkapparaat gebruikt om contact op te nemen met ISE.



Creatiepagina voor netwerkkapparaat

Blader op dezelfde pagina naar beneden om de Radius-verificatie-instellingen te vinden. Zoals in de volgende afbeelding.

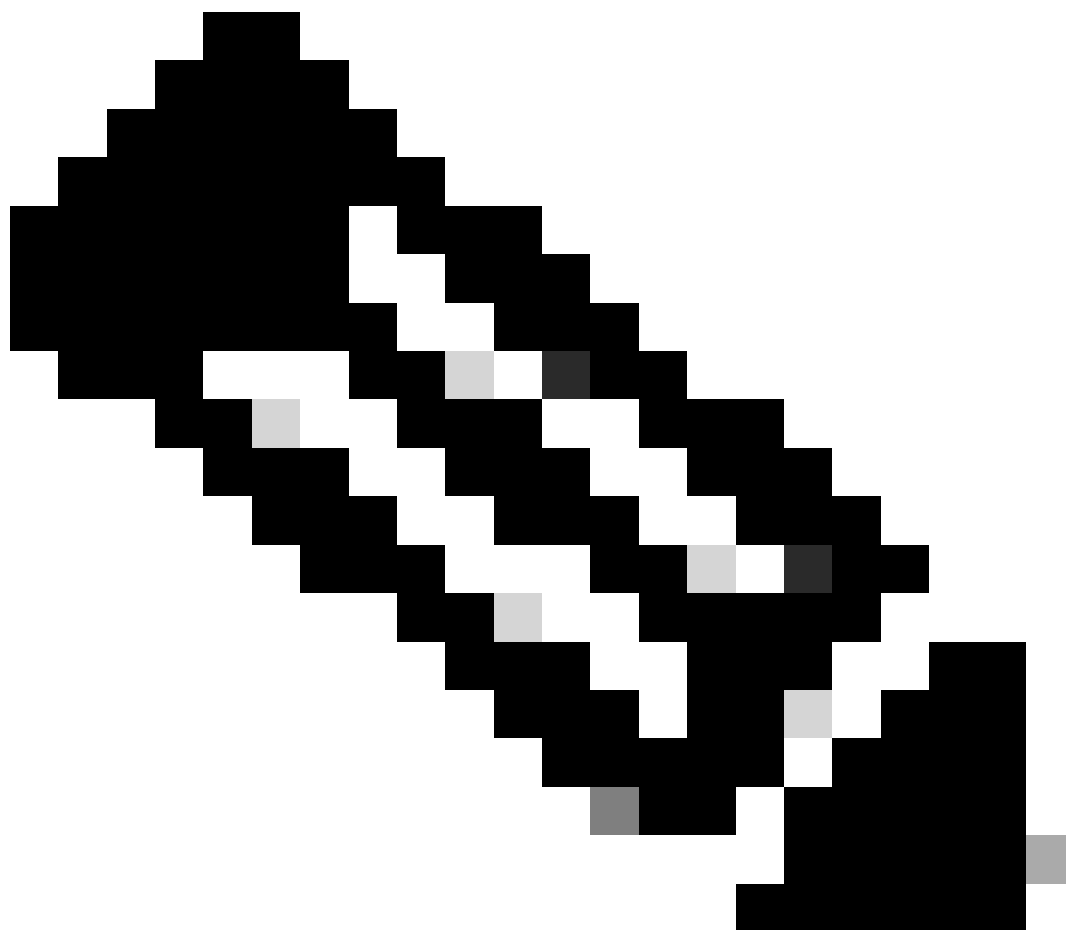
Voeg het gedeelde geheim toe dat u onder uw NAD-configuratie hebt gebruikt.



Radiusconfiguratie

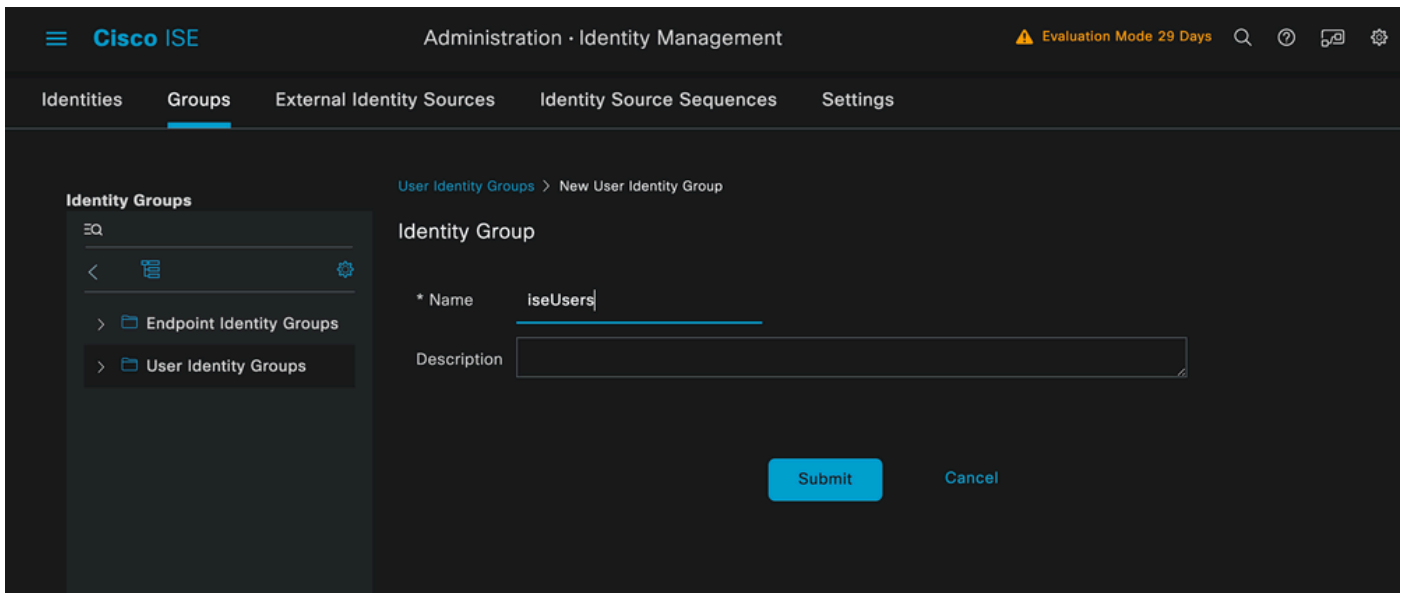
Sla de wijzigingen op.

2. b. Configureer de identiteit die wordt gebruikt om het eindpunt te authenticeren.



Opmerking: om deze configuratiehandleiding te behouden, wordt eenvoudige lokale ISE-verificatie gebruikt.

Navigeer naar het tabblad Beheer > Identity Management > Groepen. Creëer de groep en de identiteit, de groep die voor deze demonstratie is gemaakt is iseUser.

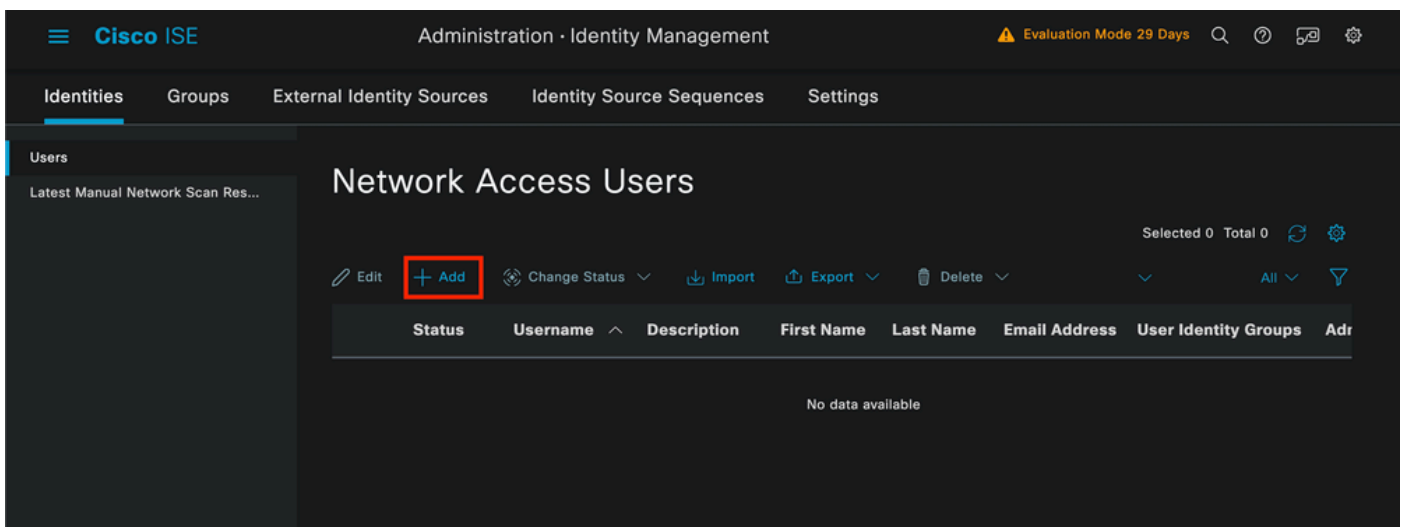


Creatiepagina voor identiteitsgroep

Klik op de knop Verzenden.

Navigeer vervolgens naar Beheer > Identity Management > Identity tabblad.

Klik op Toevoegen.



Creatiepagina voor gebruikers

Als onderdeel van de verplichte velden begint de naam van de gebruiker. De gebruikersnaam isisisecool wordt in dit voorbeeld gebruikt.

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Naam die aan de gebruikersnaam is toegewezen

De volgende stap is om een wachtwoord toe te wijzen aan de gebruikersnaam die is gemaakt. VainillaISE97 wordt gebruikt in deze demonstratie.

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ
Password will expire in 60 days

Never Expires ⓘ

Password

Re-Enter Password

* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Wachtwoord maken

Wijs de gebruiker toe aan de groep ISEusers.

User Groups

ⓘ



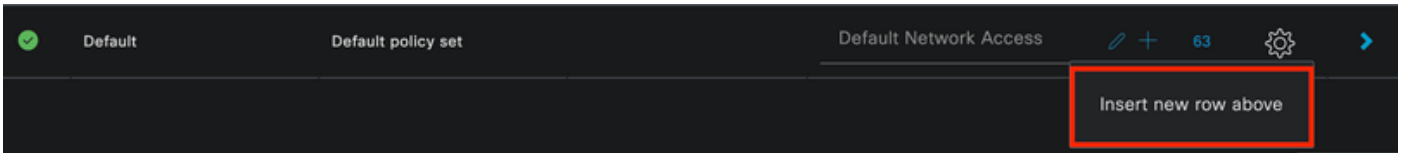
Toewijzing van gebruikersgroep

2. c. De beleidsset configureren

Navigeer naar het ISE-menu > Beleidssets > Beleidssets.

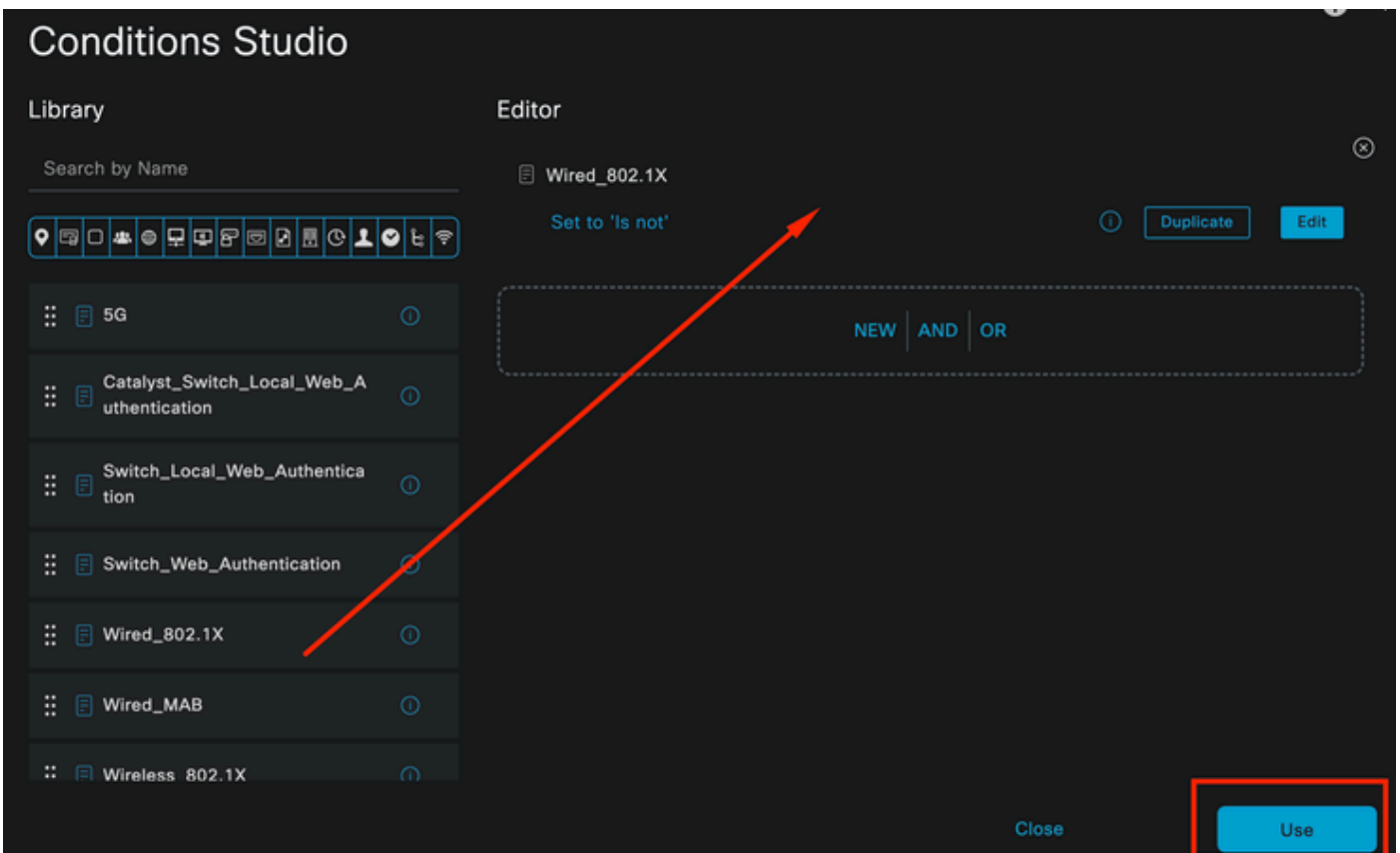
De standaardbeleidsset kan worden gebruikt. In dit voorbeeld wordt echter een beleidsset gemaakt en deze wordt Wired genoemd. Het classificeren en differentiëren van de beleidsreeksen helpt bij het oplossen van problemen,

Als het pictogram add of plus niet zichtbaar is, kan op het tandwielpictogram van een beleidsset worden geklikt. Selecteer het tandwielpictogram en selecteer vervolgens Nieuwe rij invoegen hierboven.



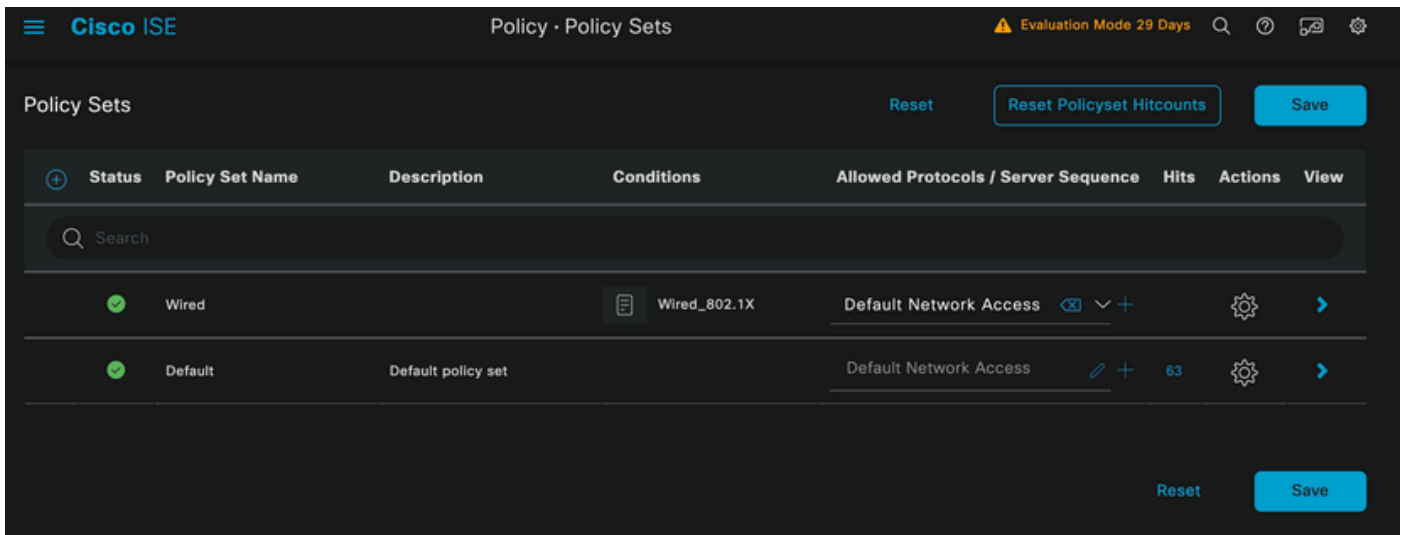
Beleidsvorming

De voorwaarde die in dit voorbeeld is geconfigureerd, is Wired 8021x, een voorwaarde die vooraf is geconfigureerd in ISE verse implementaties. Sleep het bestand en klik op Gebruik.



Condition Studio

Selecteer tot slot Default Network Access, voorgeconfigureerd, toegestane protocolservice.

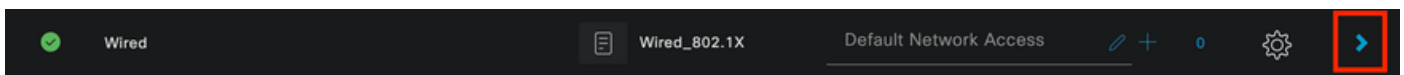


Reeksweergave Beleid

Klik op Save (Opslaan).

2. d. Configureer het verificatie- en autorisatiebeleid.

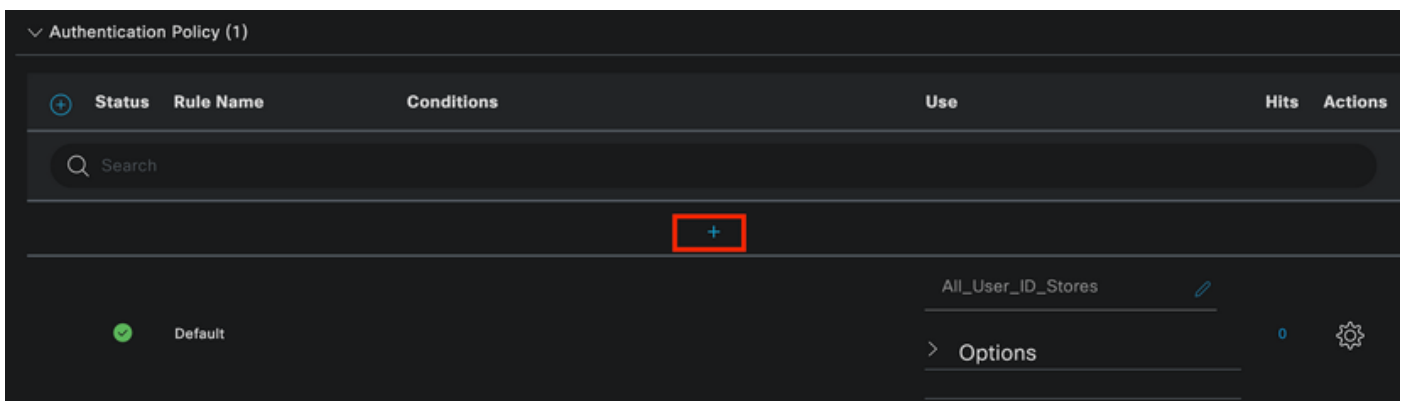
Klik op de pijl die rechts staat van de Beleidsset die zojuist is gemaakt.



Bedrade beleidsset

Het verificatiebeleid uitbreiden

Klik op het pictogram +.



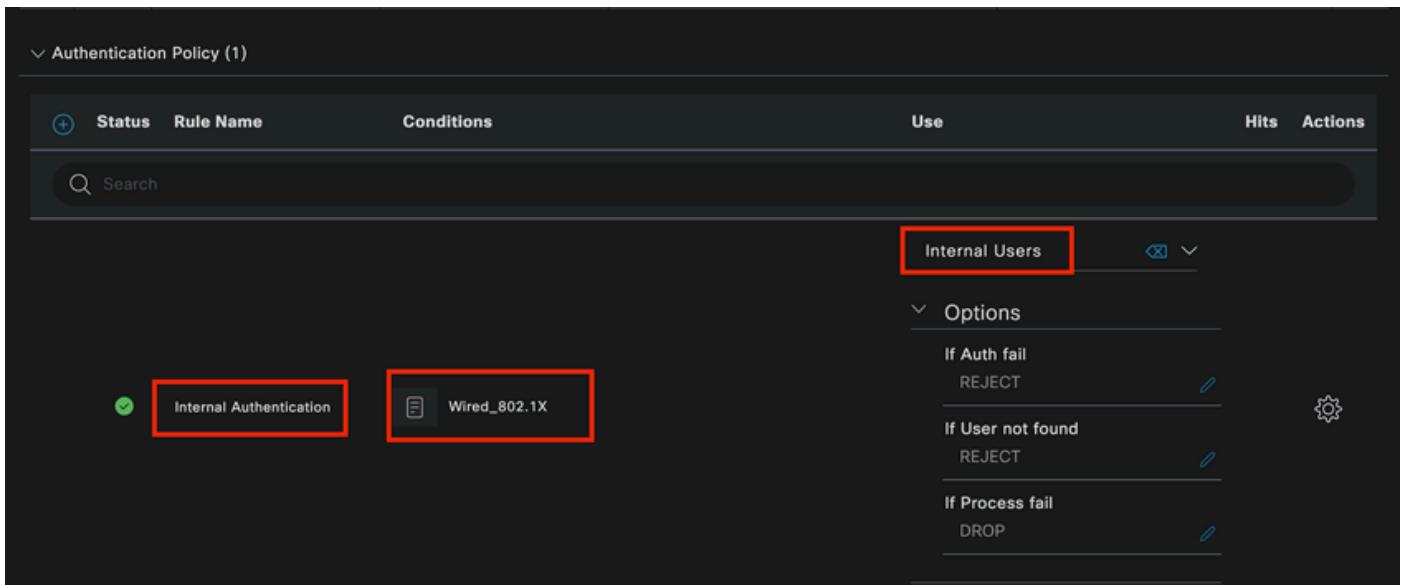
Verificatiebeleid toevoegen

Wijs een naam toe aan het verificatiebeleid, bijvoorbeeld Interne verificatie wordt gebruikt.

Klik op het + pictogram in de kolom Voorwaarden voor dit nieuwe verificatiebeleid.

De vooraf ingestelde voorwaarde Bedrade Dot1x ISE kan worden gebruikt.

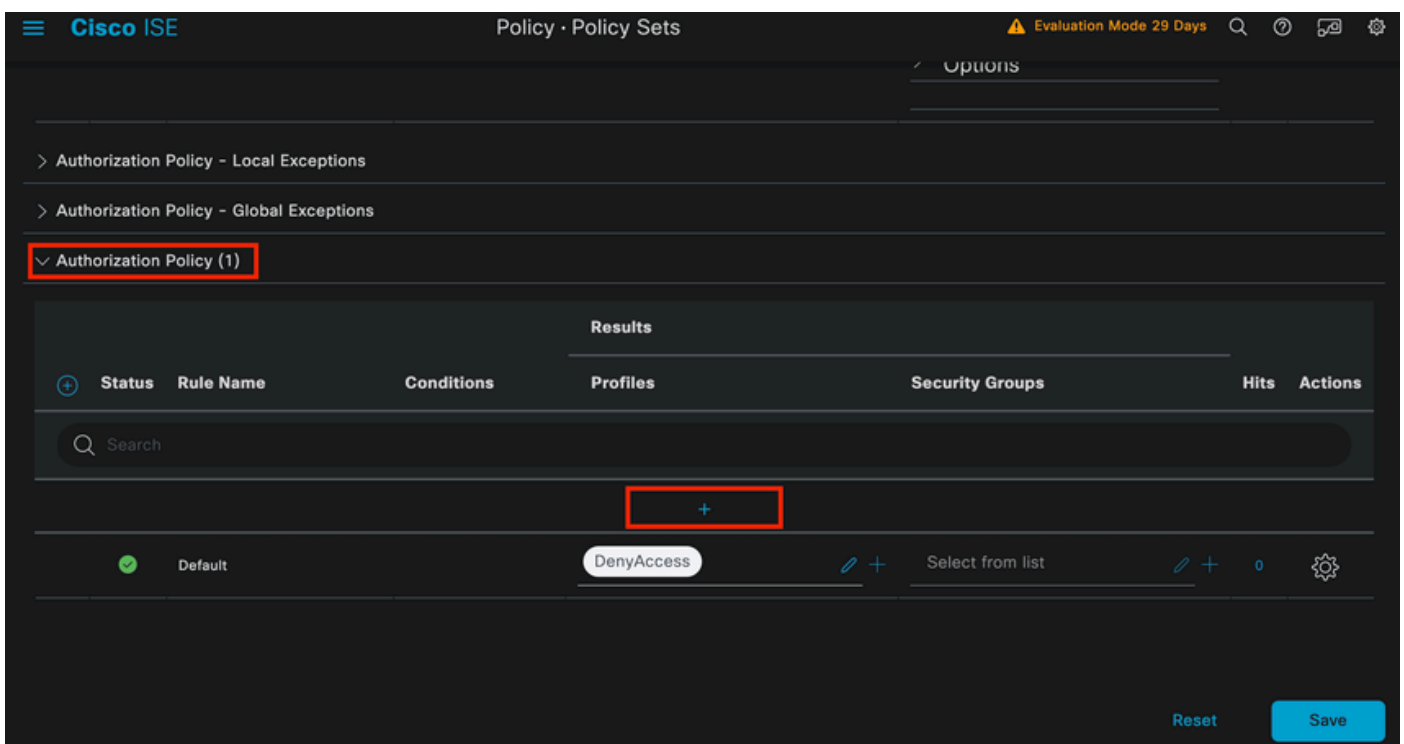
Selecteer onder de kolom Gebruik tot slot de optie Interne gebruikers uit de vervolgkeuzelijst.



Verificatiebeleid

Vergunningsbeleid

De sectie Autorisatiebeleid staat onderaan de pagina. Breid het uit en klik op het + pictogram.



Vergunningsbeleid

Noem het Autorisatiebeleid dat u zojuist hebt toegevoegd, in dit configuratievoorbeeld wordt de naam Interne ISE-gebruikers gebruikt.

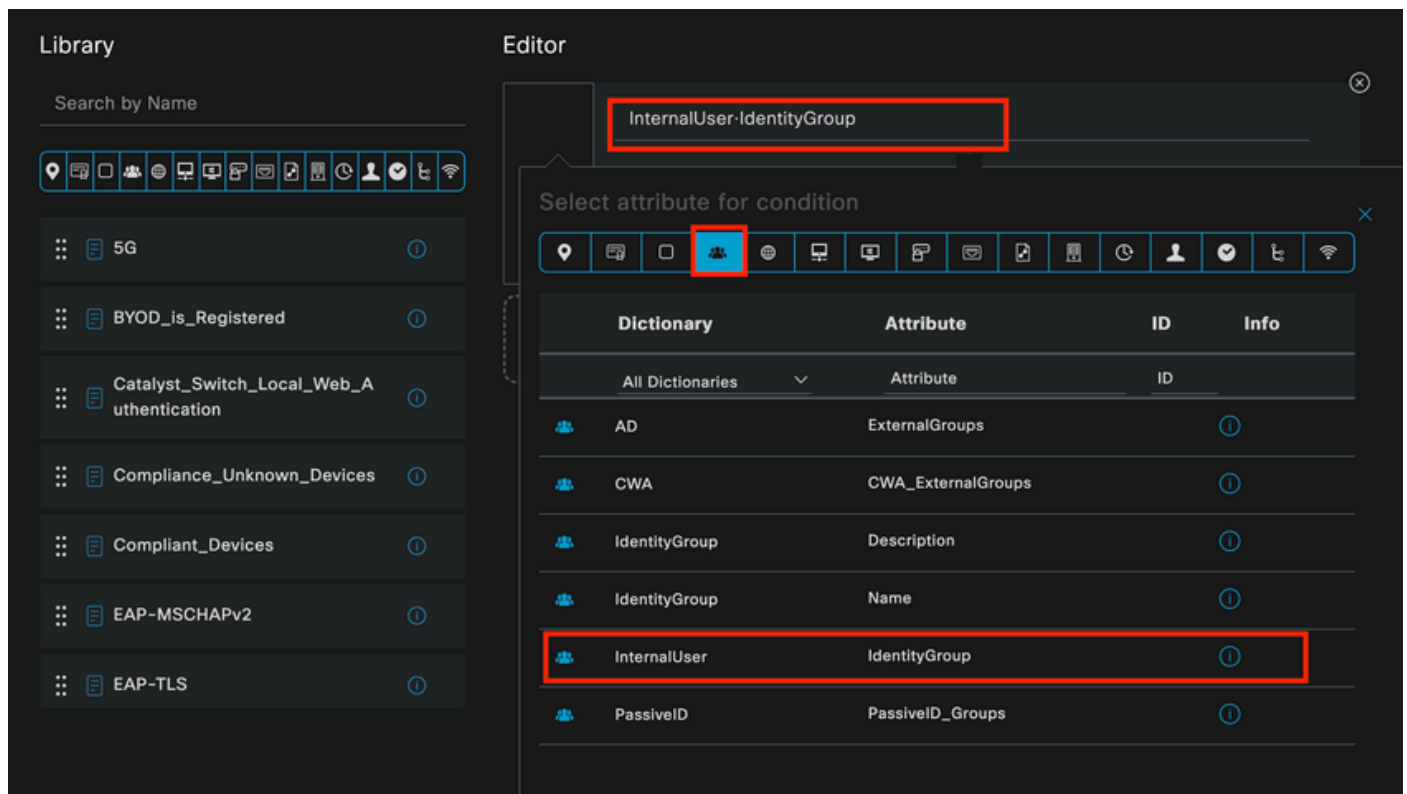
Als u een voorwaarde voor dit autorisatiebeleid wilt maken, klikt u op het +-pictogram in de kolom Voorwaarden.

De eerder gemaakte gebruiker maakt deel uit van de IseUser-groep.

Eenmaal in de editor, klik op de Klik om een attribuut sectie toe te voegen.

Selecteer het pictogram Identity group.

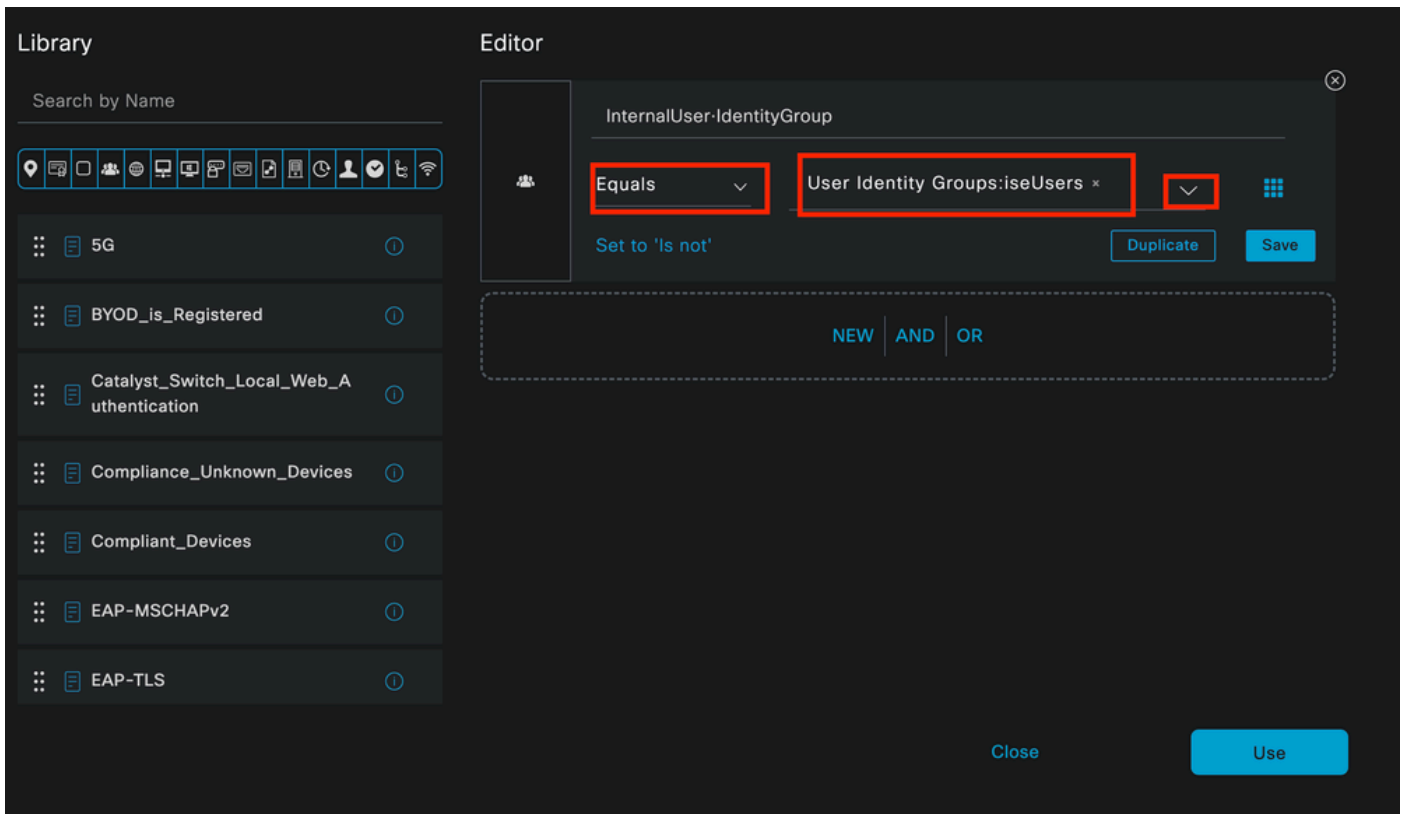
Selecteer in het woordenboek het interne gebruikerswoordenboek dat bij het kenmerk Identity Group wordt geleverd.



Condition Studio voor autorisatiebeleid

Selecteer de operator Gelijk.

Selecteer de groep IseGebruikers in de vervolgkeuzelijst Gebruikersidentiteitsgroepen.



Voorwaarden voor autorisatiebeleid voltooid

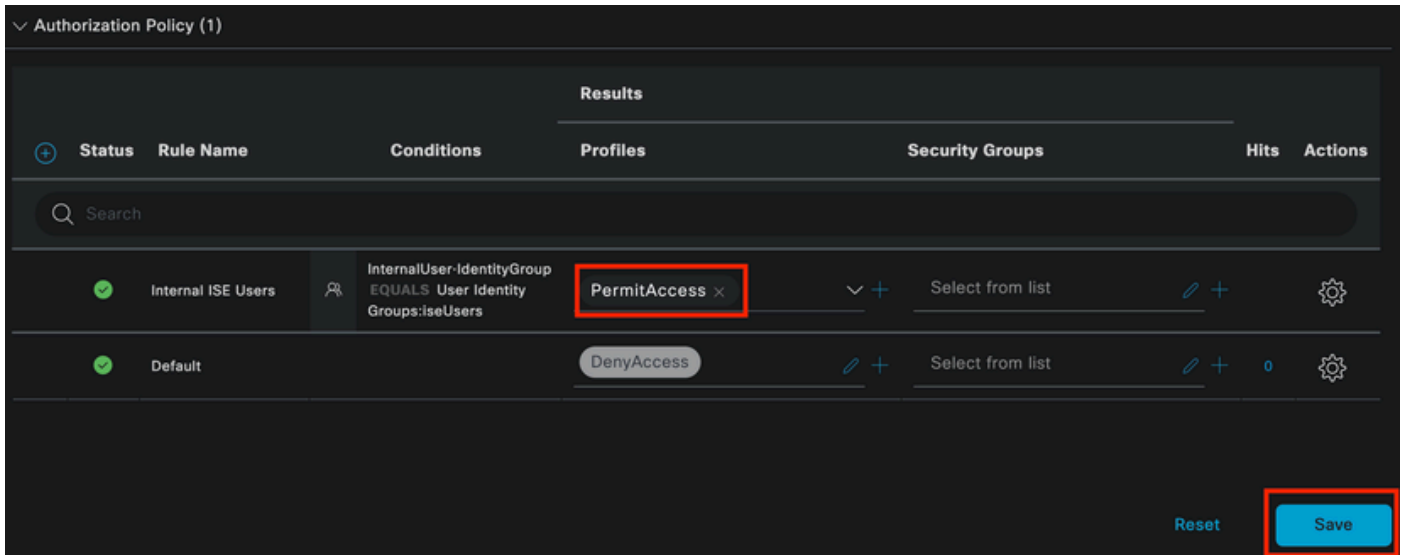
Klik op Gebruik.

Selecteer tot slot het Resultaatautorisatieprofiel dat het verificatiegedeelte van deze groep Identity ontvangt.



Opmerking: melding dat de authenticaties die naar ISE komen en deze Wired Dot1x Policy-set raken die geen deel uitmaken van de User Identity Group ISEUgebruikers, nu de standaard autorisatie beleid. Dit heeft het profielresultaat DenyAccess.

ISE is vooraf geconfigureerd met het profiel Toegang tot toegangsrechten. Selecteer het.



Vergunningsbeleid voltooid

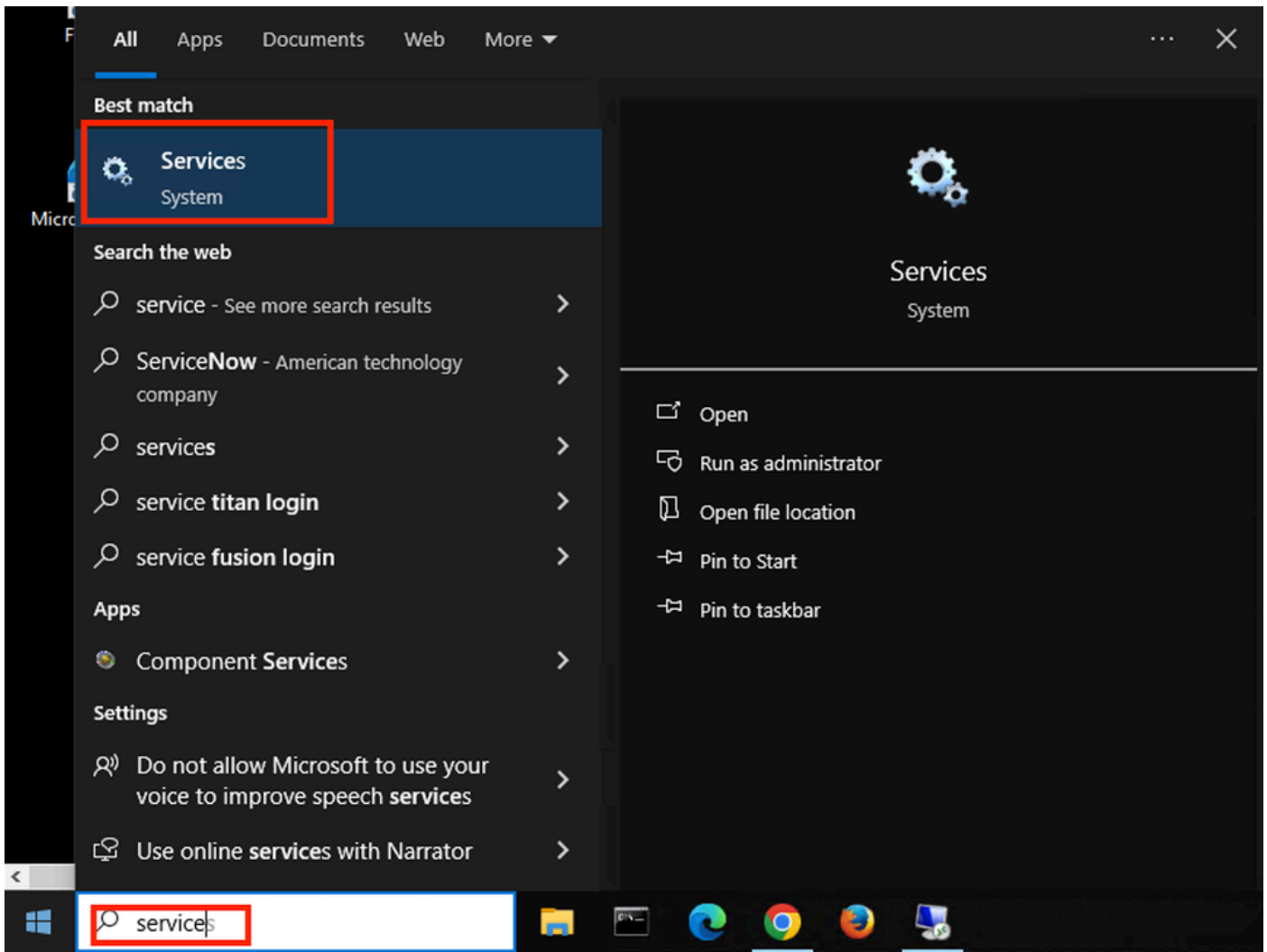
Klik op Save (Opslaan).

De configuratie voor ISE is voltooid.

Stap 3. Configuratie van Windows-native applicatie

3. a. Schakel bekabelde dot1x in onder Windows.

Open Services vanuit de Windows-zoekbalk.



Windows-zoekbalk

Zoek in de onderkant van de lijst met services bekabelde automatische configuratie.

Klik met de rechtermuisknop op Wired AutoConfig en selecteer Eigenschappen.

Wired AutoConfig Properties (Local Computer)



General Log On Recovery Dependencies

Service name: dot3svc

Display name: Wired AutoConfig

Description: responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X

Path to executable:

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Manual

Service status: Stopped

Start

Stop

Pause

Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK

Cancel

Apply



Opmerking: de service Wired AutoConfig (DOT3SVC) is verantwoordelijk voor het uitvoeren van IEEE 802.1X-verificatie op Ethernet-interfaces.

Het handmatige opstarttype is geselecteerd.

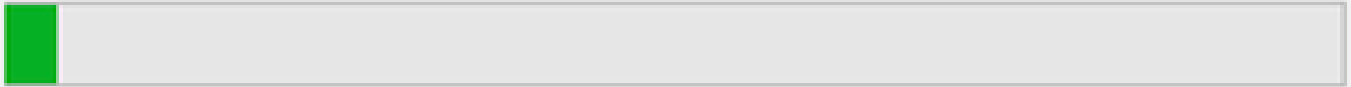
Aangezien de servicestatus is gestopt. Klik op Start.

Service Control



Windows is attempting to start the following service on Local Computer...

Wired AutoConfig



Close

Servicebeheer

Klik vervolgens op OK.

Hierna wordt de dienst uitgevoerd.

	Windows Update	Enables the ...	Running	Manual (Trig...	Local System...
	Windows Update Medic Service	Enables rem...		Manual	Local System...
	WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
	Wired AutoConfig	The Wired A...	Running	Manual	Local System...
	WLAN AutoConfig	The WLANS...		Manual	Local System...
	WMI Performance Adapter	Provides pe...		Manual	Local System...
	Work Folders	This service ...		Manual	Local Service

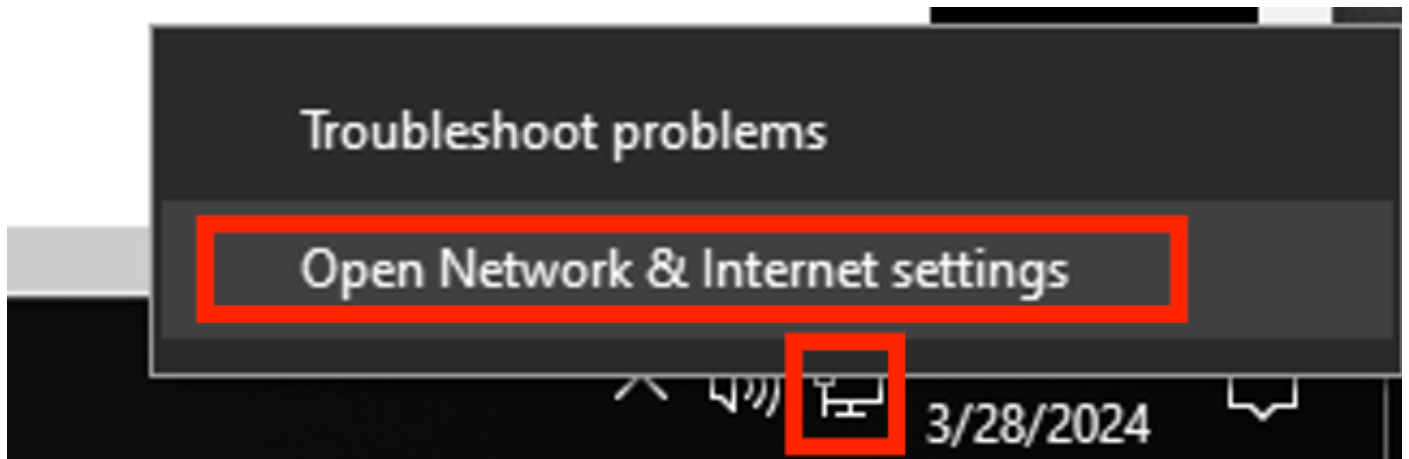
Bedrade AutoConfig-service

3. b. Configureer de Windows-laptopinterface die is aangesloten op de NAD Authenticator (ISR 1100).

Lokaliseer vanuit de taakbalk de rechterhoek en gebruik vervolgens het computerpictogram.

Dubbelklik op het pictogram van de computer.

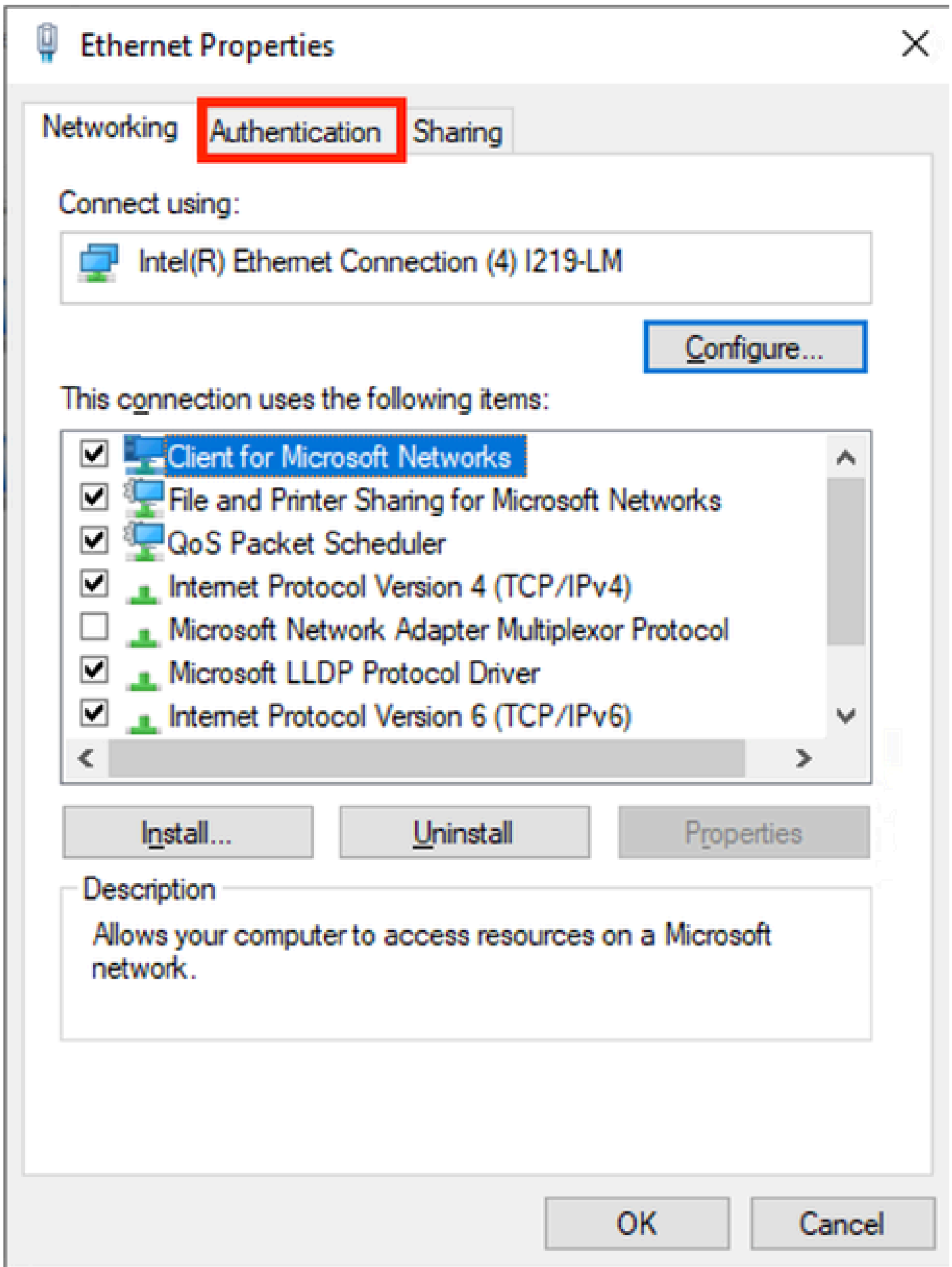
Selecteer Netwerk- en internetinstellingen openen.



Windows-taakbalk

Wanneer het venster Network Connections is geopend, klikt u met de rechtermuisknop op de Ethernet-interface die is aangesloten op de ISR Gig 0/1/0. Klik op de optie Eigenschappen.

Klik op het tabblad verificatie.



Ethernet-eigenschappen interface

Schakel het selectievakje IEEE 802.1X-verificatie inschakelen in.



Ethernet Properties



Networking

Authentication

Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) ▾

Settings

Remember my credentials for this connection each time I'm logged on

Fallback to unauthorized network access

Additional Settings...

OK

Cancel

Ethernet-eigenschappen voor verificatie

Selecteer Protected EAP (PEAP).

Schakel de optie Onthoud mijn referenties voor deze verbinding telkens wanneer ik ben aangemeld.

Klik op Instellingen.

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
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2

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

geeft gedetailleerde informatie weer over de dot1x-sessie(s) die op de opgegeven poort wordt (worden) uitgevoerd.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
```

```
    Interface: GigabitEthernet0/1/0
      IIF-ID: 0x08767C0D
    MAC Address: 8c16.450d.f42b
    IPv6 Address: Unknown
    IPv4 Address: Unknown
    User-Name: iseiscool <----- The username configured for Windows Native Supplicant
      Status: Authorized <----- An indication that this session was authorized by the PSN
      Domain: DATA
    Oper host mode: multi-auth
    Oper control dir: both
    Session timeout: N/A
    Common Session ID: 22781F0A0000000C83E28461
    Acct Session ID: 0x00000003
      Handle: 0xc6000002
    Current Policy: POLICY_Gi0/1/0
```

Local Policies:

```
    Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
    Security Policy: Should Secure
```

Server Policies:

Method status list:

Method	State
dot1x	Authc Success <----- An indication that dot1x is used for this authentication

Router#

ISE-logbestanden

Ga naar Operations > Radius > Live logs tabblad.

Filter door de gebruikersnaam identiteit, in dit voorbeeld wordt de gebruikersnaam iseCool gebruikt.

The screenshot displays the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, a summary section shows five metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (0). Below the summary, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 3 hours). There are also buttons for 'Reset Repeat Counts' and 'Export To', and a 'Filter' dropdown menu.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authc	
×		↓		iseiscool	×	Endpoint ID	Endpoint Pr	Authentication Policy	Autho
Mar 28, 2024 07:04:35.4...	●	📄	0	iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired	
Mar 28, 2024 07:04:35.3...	✓	📄		iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired	

Last Updated: Thu Mar 28 2024 01:29:12 GMT-0600 (Central Standard Time) Records Shown: 2

ISE-livelogs

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs interface. At the top, there are summary cards for Misconfigured Suppliants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (0). Below these are controls for Refresh (Never), Show (Latest 20 records), and Within (Last 3 hours). A table of log entries is displayed with columns: Authorization Policy, Authoriz..., IP Address, Network De..., Device Port, Identity Group, Posture..., and Server. The second row of the table is highlighted with red boxes around the following values: 'Wired >> Internal ISE Users', 'PermitAcc...', 'ISR1100', 'GigabitEthernet0/1/0', 'User Identity Groups:iseUsers', and 'PSN01'. The bottom of the interface shows 'Last Updated: Thu Mar 28 2024 01:34:19 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

ISE-livelogs

Merk op dat vanuit deze snelle weergave, live logs bieden belangrijke informatie:

- Tijdstempel van de verificatie.
- Identiteit gebruikt.
- Adres eindpunt snijpad
- De beleidsreeks en het Verificatiebeleid dat werd geraakt.
- Beleidsset en autorisatiebeleid dat is geraakt.
- Resultaat van het autorisatieprofiel.
- Het netwerkapparaat dat het Radius-verzoek naar ISE verstuurt.
- De interface waar het eindpunt aan wordt verbonden.
- De Identity Group van de gebruiker die is geverifieerd.
- Het Policy Server-knooppunt (PSN) dat de verificatie heeft verwerkt.

Problemen oplossen

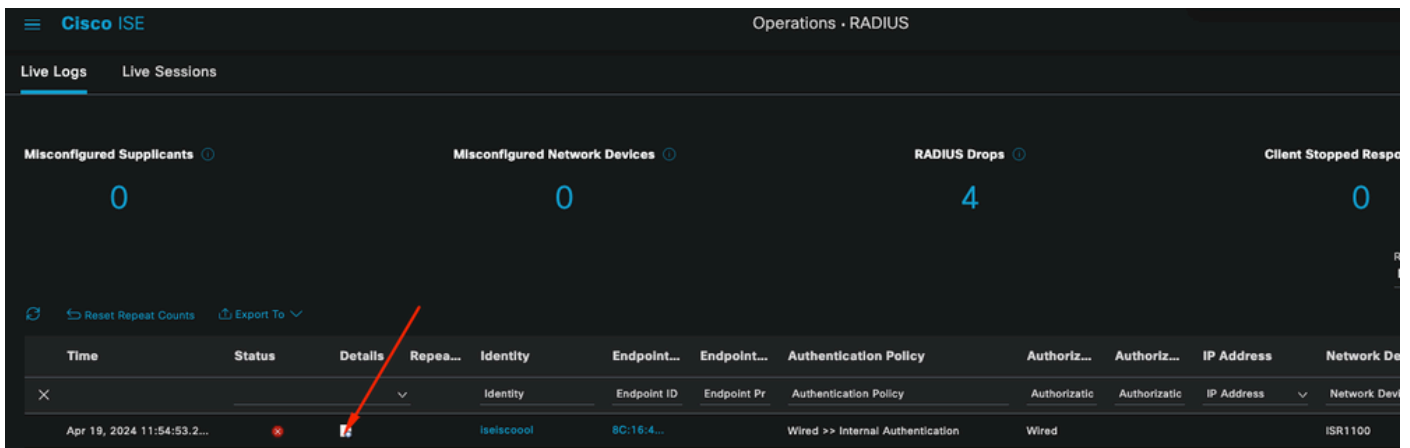
1 - Reading ISE Live Log Details

Navigeer naar Operations > Radius > Live logs tabblad, filter door Autorstatus: Mislukt OF door de gebruikersnaam die wordt gebruikt OF door het MAC-adres OF door het gebruikte Network Access Device.

Toegang tot de Operations > Radius > Live logs > Gewenste verificatie > Live log details.

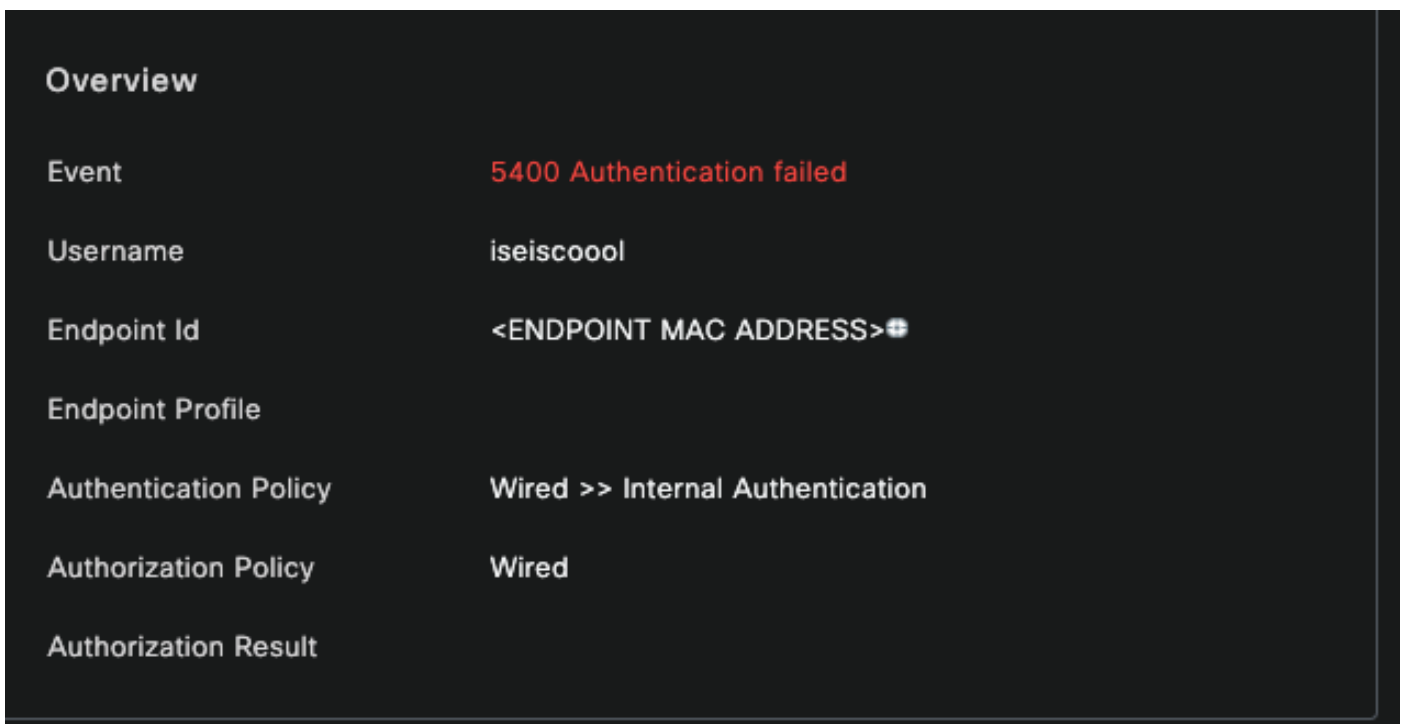
Klik op dezelfde pagina op het pictogram Zoeken nadat de verificatie is gefilterd.

Eerste scenario: De gebruiker voert zijn gebruikersnaam in met een typo.



Gegevens bewegend logboek openen

Zodra het live log detail is geopend, kunt u zien dat de verificatie is mislukt ook de gebruikte gebruikersnaam wordt vermeld.



Sectie Overzicht

Dan op dezelfde live logdetails, in de sectie Verificatiedetails, kan het de faillietreden, worteloorzaak, en Resolutie van de fout worden gevonden.

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resolution settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).
Username	iseiscool

Verificatiedetails

In dit scenario is de reden waarom de authenticatie mislukt omdat de gebruikersnaam een typo heeft, maar deze zelfde fout wordt gepresenteerd, als de gebruiker niet is aangemaakt in ISE, of als ISE niet in staat was om te valideren dat de gebruiker bestaat in andere identiteitswinkels, bijvoorbeeld LDAP of AD.

Stappen

15041 Evaluating Identity Policy

15013 Selected Identity Source - Internal Users ←

24210 Looking up User in Internal Users IDStore - iseiscoool ←

24216 The user is not found in the internal users identity store ←

22056 Subject not found in the applicable identity store(s) ←

22058 The advanced option that is configured for an unknown user is used

22061 The 'Reject' advanced option is configured in case of a failed authentication request ←

11815 Inner EAP-MSCHAP authentication failed ←

11520 Prepared EAP-Failure for inner EAP method

22028 Authentication failed and the advanced options are ignored

12305 Prepared EAP-Request with another PEAP challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12304 Extracted EAP-Response containing PEAP challenge-response

61025 Open secure connection with TLS peer

12307 PEAP authentication failed ←

11504 Prepared EAP-Failure

11003 Returned RADIUS Access-Reject ←

Stappendeel Details bewegend logboek

In het gedeelte Stappen wordt in detail beschreven hoe de ISE-processen tijdens het RADIUS-

gesprek zijn uitgevoerd.

U vindt hier informatie zoals:

- Hoe het gesprek is begonnen.
- SSL-handshake.
- De EAP-methode waarover is onderhandeld.
- EAP-methodeproces.

In dit voorbeeld is te zien dat ISE zojuist de interne identiteiten voor deze authenticatie heeft ingecheckt. De gebruiker is niet gevonden en daarom wordt ISE als antwoord op een Access-Reject verzonden.

Tweede scenario: de ISE-beheerder heeft PEAP uitgeschakeld uit de Beleidsset Toegestane protocollen.

2 - PEAP uitgeschakeld

Als de bewegende loggegevens van de mislukte sessie zijn geopend, wordt de foutmelding "PEAP is niet toegestaan in de toegestane protocollen" weergegeven.

Event	5400 Authentication failed
Failure Reason	12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols
Resolution	Ensure that the PEAP protocol is allowed by ISE in Allowed Protocols.
Root cause	The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols.
Username	iseiscool

Detailrapport bewegend logboek

Deze fout is gemakkelijk op te lossen, de resolutie is te navigeren naar **Beleid > Beleidselementen > Verificatie > Toegestane Protocollen**. Controleer of de optie PEAP toestaan is uitgeschakeld.

The screenshot shows the Cisco ISE configuration interface for a policy named "Allow EAP-TLS". The "Results" tab is selected, and the "Allowed Protocols" section is expanded. The "Allow PEAP" checkbox is highlighted with a red box. Other protocols and their settings are as follows:

- Allow LEAP
- Allow PEAP
- PEAP Inner Methods**
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries 1 (Valid Range 0 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries 1 (Valid Range 0 to 3)
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ
 - Require cryptobinding TLV ⓘ
 - Allow PEAPv0 only for legacy clients

Sectie Toegestane protocollen

Derde scenario: de verificatie mislukt omdat het eindpunt niet vertrouwt op het ISE-certificaat.

Navigeer naar de gegevens van het bewegende logboek. Vind de record voor de verificatie die mislukt en controleer de gegevens van het live logboek.

Authentication Details

Source Timestamp 2024-04-20 04:37:42.007

Received Timestamp 2024-04-20 04:37:42.007

Policy Server ISE PSN

Event 5411 Supplicant stopped responding to ISE

Failure Reason 12934 Supplicant stopped responding to ISE during PEAP tunnel establishment

Resolution Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page (Administration > System > Certificates > Local Certificates). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.

Root cause PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

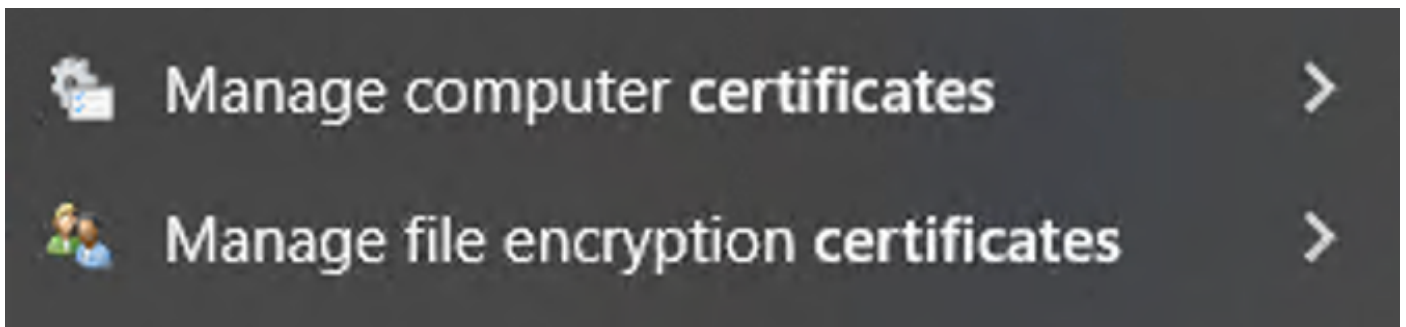
Username iseiscool

Details bewegend logboek

Het eindpunt is het afwijzen van het certificaat dat wordt gebruikt voor de PEAP-tunnelinrichting.

Om dit probleem op te lossen, in het Windows-eindpunt waar u het probleem hebt verifiëren dat de CA-keten die het ISE-certificaat heeft ondertekend, zich bevindt in de sectie Windows Gebruikerscertificaten beheren > Trusted Root-certificeringsinstanties OF Computercertificaten beheren > Trusted Root-certificeringsinstanties.

U kunt deze configuratiesectie op uw Windows-apparaat openen door deze in de zoekbalk van Windows te zoeken.



Resultaten in Windows-zoekbalk

3 - ISE-TCP-dommeltool (pakketvastlegging)

De pakketvaststellingsanalyse is essentieel bij het oplossen van problemen. Direct vanaf ISE-pakketopnamen kunnen op alle knooppunten en op elke interface van de knooppunten worden genomen.

Ga om toegang te krijgen tot dit gereedschap naar Operations > Diagnostische tools > Algemene tools > TCP Dump.

Operations · Troubleshoot

Evaluation Mode 9 Days

Diagnostic Tools | Download Logs | Debug Wizard

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug
- TCP Dump**
- Session Trace Tests

TrustSec Tools

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 0 / << 0 / >> | Go 0 Total Rows

Refresh Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number
No data found.						

Sectie TCP-pomp

Klik op de knop Add om te beginnen met het configureren van een pcap.

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*

ISE PSN

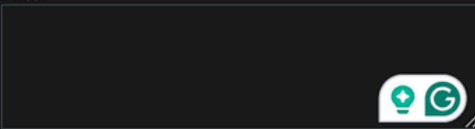


Network Interface*

GigabitEthernet 0 [Up, Running]



Filter





E.g: ip host 10.77.122.123 and not
10.177.122.119

File Name

ISEPCAP

Creatie van TCP-dump

Repository

File Size
10
Mb

Limit to
1
File(s)

Time Limit
5
Minute(s)

Promiscuous Mode

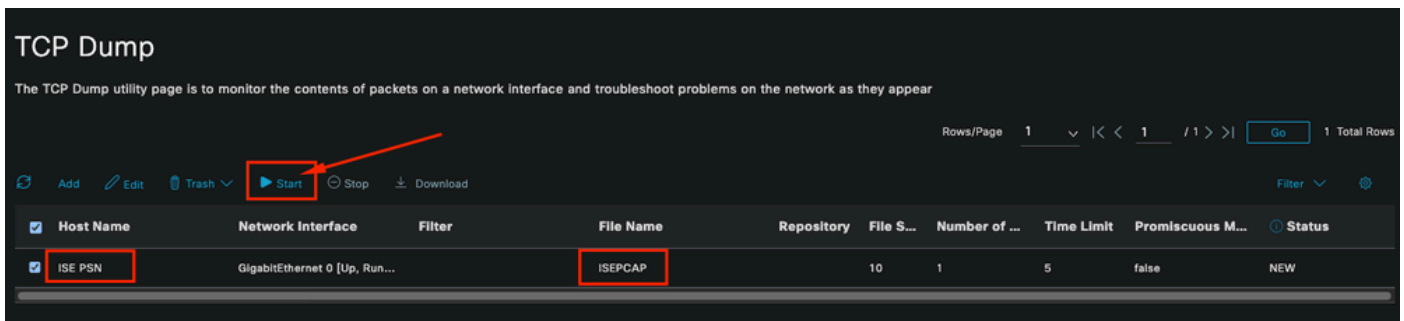
Cancel Save Save and Run

Sectie TCP-pomp

Om een cap in ISE te maken, zijn dit de gegevens die u moet invoeren:

- Selecteer het knooppunt waarin u de pcap moet nemen.
- Selecteer de ISE-knoopinterface die voor de pcap wordt gebruikt.
- Als u bepaald verkeer moet opnemen, gebruikt u de filters, geeft ISE u enkele voorbeelden.
- Geef de dop een naam. In dit scenario hebben we ISEPCAP gebruikt.
- Selecteer de repository als er geen repository is geselecteerd, dan wordt de opname opgeslagen op de lokale schijf van ISE en kan worden gedownload van de GUI.
- Indien nodig kunt u ook de grootte van het pcap-bestand wijzigen.
- Gebruik indien nodig meer dan 1 bestand, dus als de pcap groter is dan de bestandsgrootte, wordt er vervolgens een nieuw bestand gemaakt.
- Breid indien nodig de tijd voor het opnameverkeer voor de dop uit.

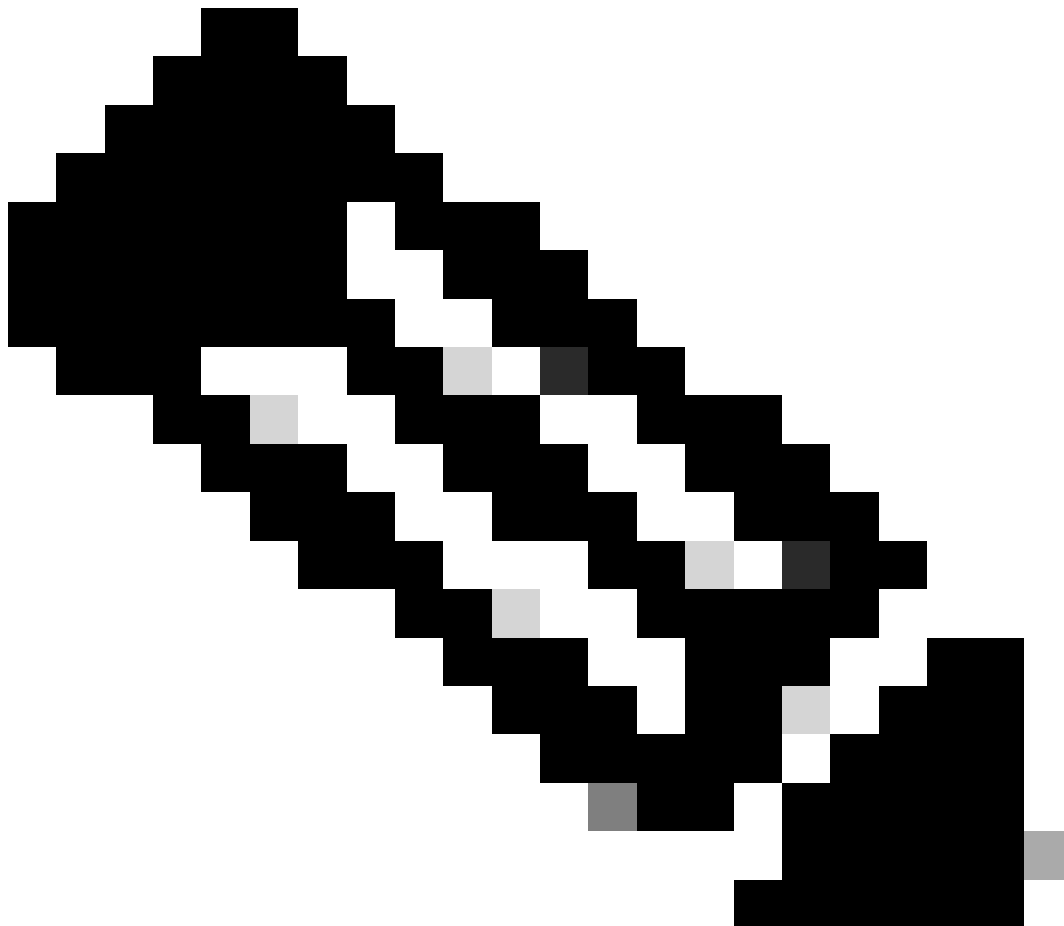
Klik tot slot op de knop Opslaan.



Sectie TCP-pomp

Selecteer vervolgens de pcap en klik op de knop Start.

Nadat u op Start hebt geklikt, wordt de kolom Status gewijzigd in actieve status.



Opmerking: terwijl de PCAP in RUN-staat is, repliceer het falende scenario of het gedrag dat u moet opnemen. Na voltooiing zijn de details van de RADIUS, het gesprek zichtbaar in de PCAP.

Zodra de gegevens die u nodig hebt, worden opgenomen terwijl de PCAP wordt uitgevoerd, moet u de afsluitdop voltooiën. Selecteer het nogmaals en klik op Stoppen.

3 - 1 ISE-verslagen

Indien een diepgaandere analyse vereist is, biedt ISE nuttige rapporten om gebeurtenissen uit het verleden te onderzoeken.

Om ze te vinden, navigeer je naar Operations > Rapporten > Rapporten > Endpoints en Gebruikers

The screenshot displays the Cisco ISE interface. The top right corner shows 'Operations · Reports'. The left sidebar contains a navigation menu with 'Reports' and 'Endpoints and Users' highlighted in red. The main content area is titled 'RADIUS Authentications' and shows a table of authentication logs. The table has columns for 'Logged At', 'RADIUS Status', 'Details', and 'Identity'. The 'Logged At' column is filtered to 'Last 7 Days'. The 'RADIUS Status' column shows 'x' for all entries. The 'Identity' column shows 'iselscool' for all entries.

Logged At	RADIUS Status	Details	Identity
2024-04-20 05:10:59.176	x	[icon]	iselscool
2024-04-20 05:00:59.153	x	[icon]	iselscool
2024-04-20 04:50:59.135	x	[icon]	iselscool
2024-04-20 04:40:59.097	x	[icon]	iselscool

ISE-rapportgedeelte

Endpoints and Users



Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

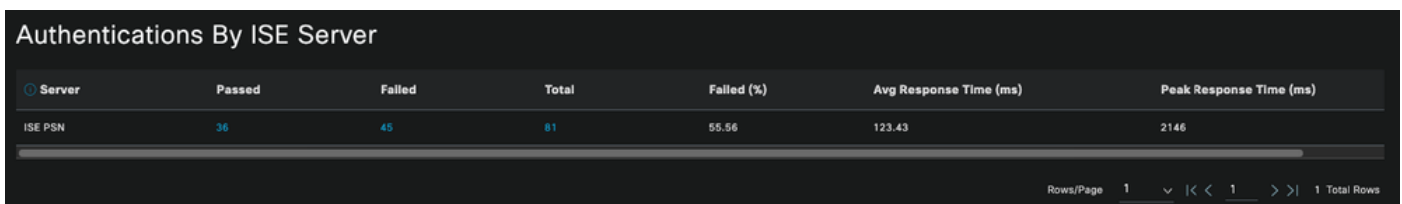
Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

: in de implementatie die voor dit document wordt gebruikt, is slechts één PSN gebruikt. Voor grotere implementaties zijn deze gegevens echter nuttig om te zien of taakverdeling nodig is.



Server	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
ISE PSN	36	45	81	55.56	123.43	2146

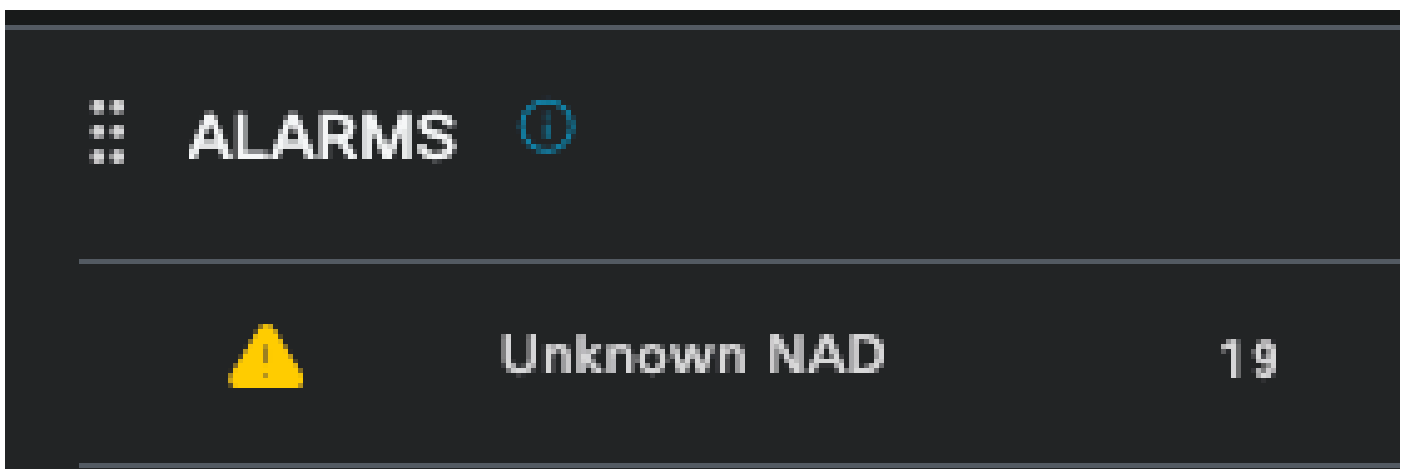
Verificaties door ISE-server

4 - ISE-alarmen

In het Dashboard van ISE worden in het gedeelte Alarmen de implementatieproblemen weergegeven.

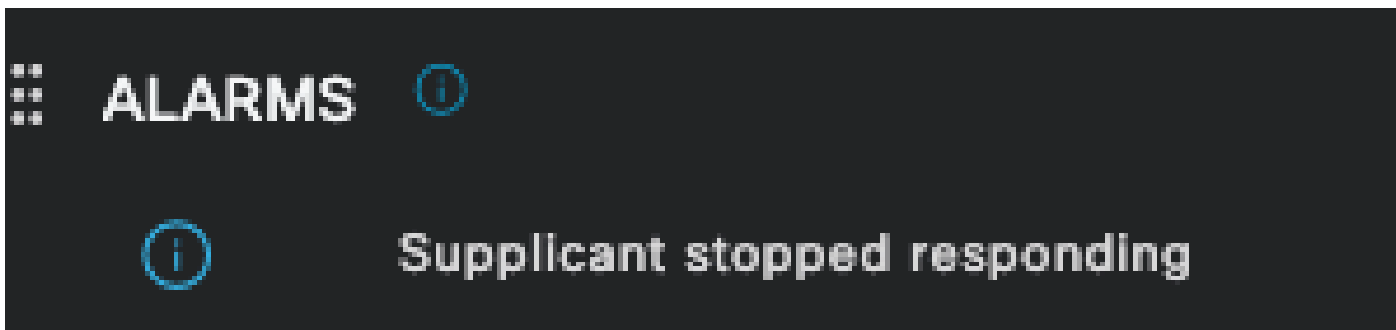
Hier zijn verscheidene alarmen van ISE die met het oplossen van problemen helpen.

Onbekend NAD — Dit alarm wordt weergegeven wanneer er een netwerkapparaat is dat een eindpunt authenticceert en naar ISE reikt. Maar ISE vertrouwt het niet en de RADIUS-verbinding wordt verbroken. De meest voorkomende redenen zijn dat het netwerkapparaat niet is gemaakt of dat het IP dat het netwerkapparaat gebruikt niet hetzelfde is als dat ISE heeft geregistreerd.



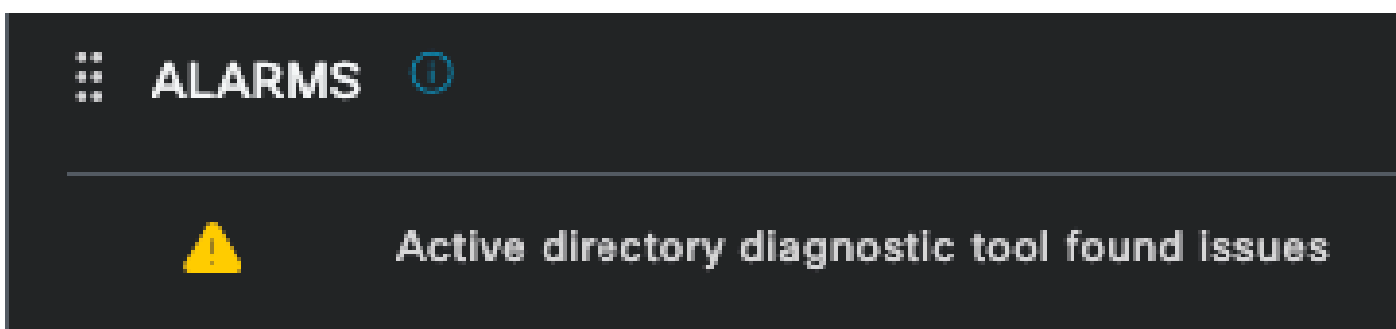
Onbekend NAD

Supplicant gestopt met reageren — Dit alarm doet zich voor wanneer er een probleem is met de communicatie tussen de aanvrager, meestal als gevolg van een verkeerde configuratie in de aanvrager die moet worden gecontroleerd en onderzocht aan de kant van het eindpunt.



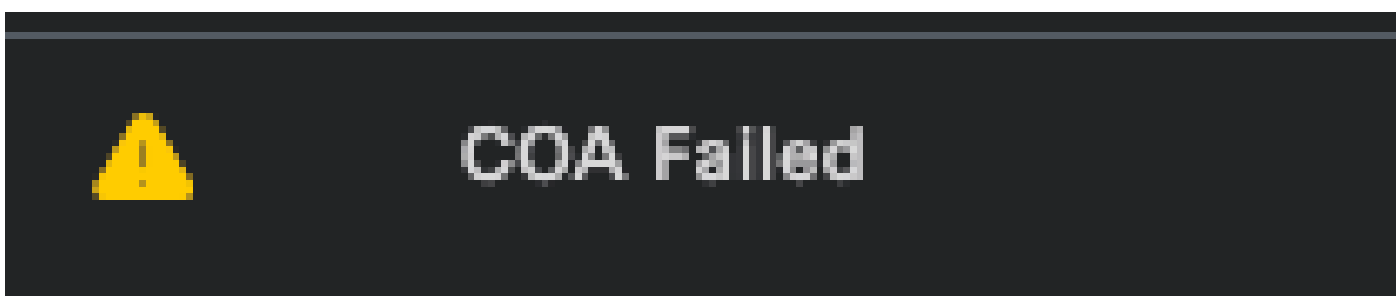
Supplicant stopt met reageren

Active Directory diagnostische tool gevonden problemen — Wanneer Active Directory wordt gebruikt om de gebruikersidentiteit te valideren, als het begint met problemen met het communicatieproces, of als de verbinding is verbroken, zou u dit alarm zien. Dan zou je realiseren waarom de authenticaties dat de identiteit bestaat op de AD falen.



AD-diagnostiek mislukt

COA (Verandering van Vergunning) is mislukt — Meervoudige stromen in ISE gebruiken CoA, dit alarm informeert u of er problemen zijn opgetreden tijdens de CoA poortcommunicatie naar een netwerkapparaat.



Coa is mislukt

5 - ISE-debugconfiguratie en -logverzameling

Om verder te gaan met de details van het verificatieproces, moet u de volgende componenten in DEBUG inschakelen voor mab- en dot1x-problemen:

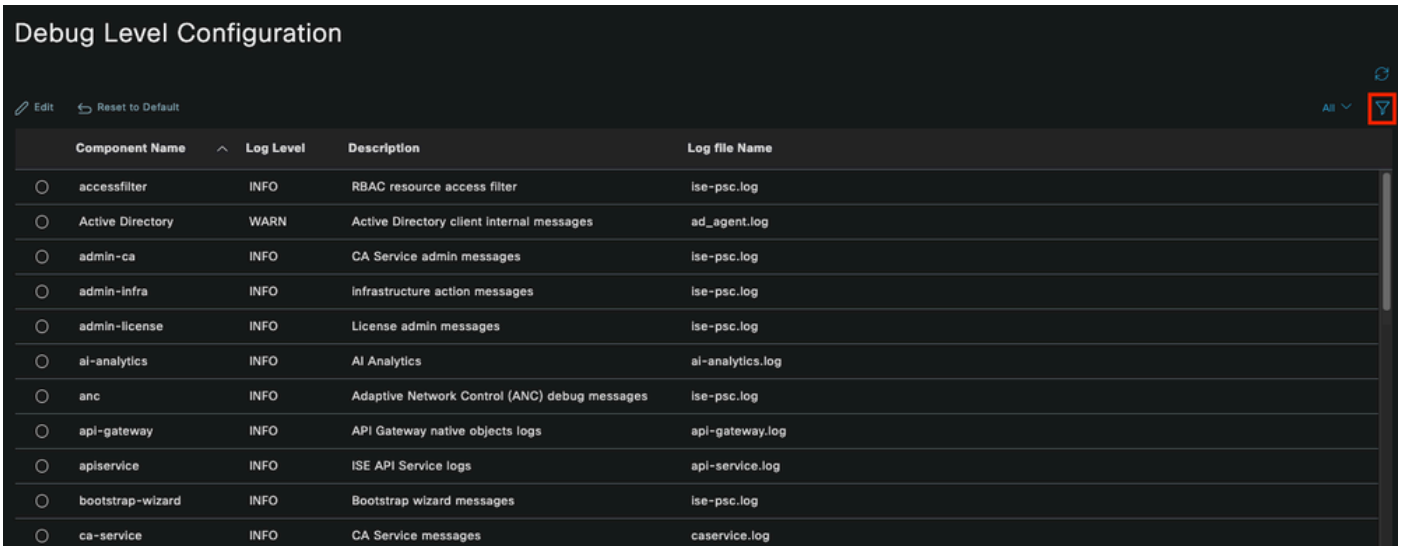
Probleem: dot1x/mab

Attributen die moeten worden ingesteld op debug-niveau.

- runtime-AAA (poortserver.log)
- nsf (ise-psc.log)
- nsf-sessie (ise-psc.log)

Om de componenten op DEBUG-niveau te laten, moet eerst worden vastgesteld welke PSN de authenticatie ontvangt die faalt of moet worden onderzocht. U kunt deze informatie uit de live logs krijgen. Daarna moet u naar het ISE-menu > Probleemoplossing > Wizard Debug > Configuratie debug log > Selecteer de PSN > Klik op de knop Bewerken.

Het volgende menu wordt weergegeven. Klik op het filterpictogram:



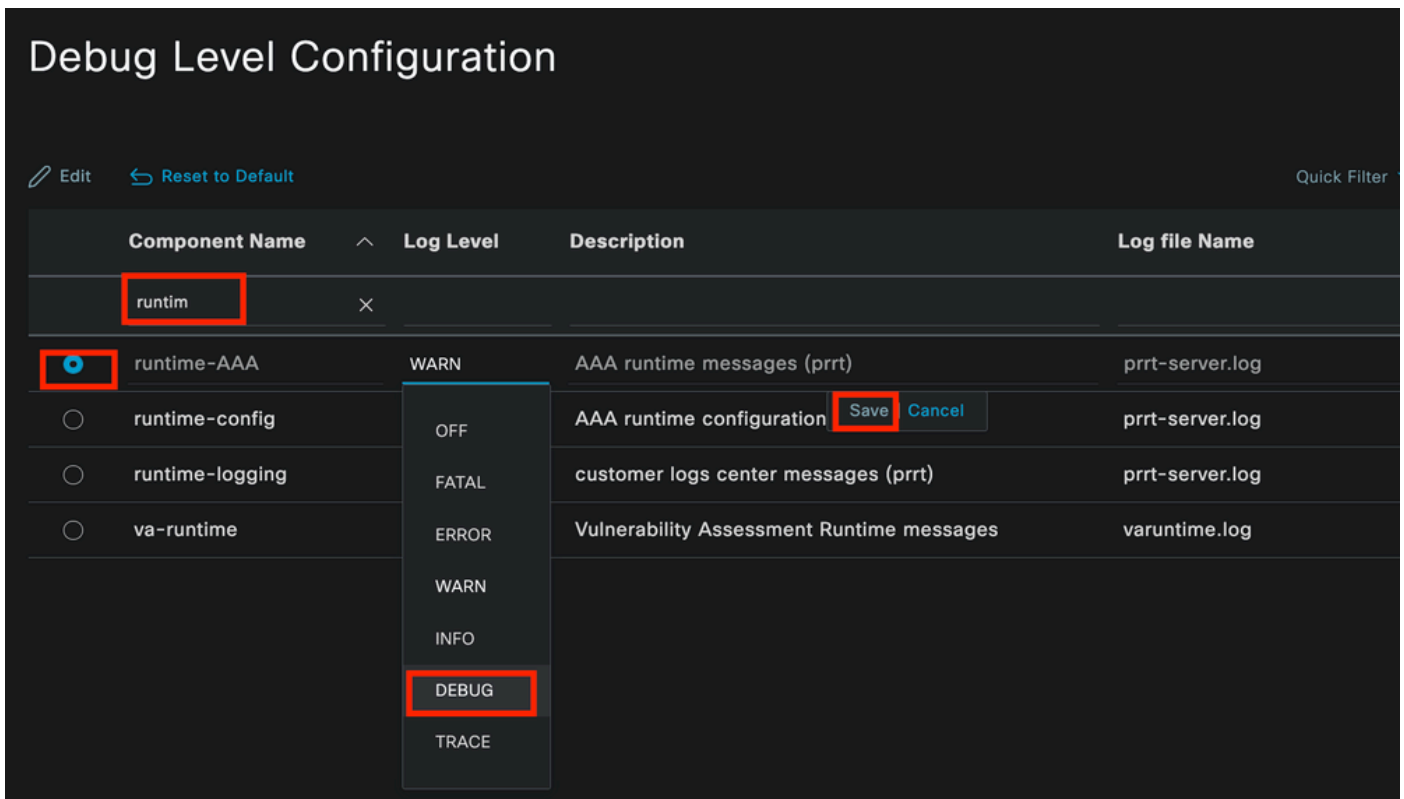
Debug Level Configuration

Edit Reset to Default

Component Name	Log Level	Description	Log file Name
<input type="radio"/> accessfilter	INFO	RBAC resource access filter	ise-psc.log
<input type="radio"/> Active Directory	WARN	Active Directory client internal messages	ad_agent.log
<input type="radio"/> admin-ca	INFO	CA Service admin messages	ise-psc.log
<input type="radio"/> admin-Infra	INFO	Infrastructure action messages	ise-psc.log
<input type="radio"/> admin-license	INFO	License admin messages	ise-psc.log
<input type="radio"/> ai-analytics	INFO	AI Analytics	ai-analytics.log
<input type="radio"/> anc	INFO	Adaptive Network Control (ANC) debug messages	ise-psc.log
<input type="radio"/> api-gateway	INFO	API Gateway native objects logs	api-gateway.log
<input type="radio"/> apiservice	INFO	ISE API Service logs	api-service.log
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log

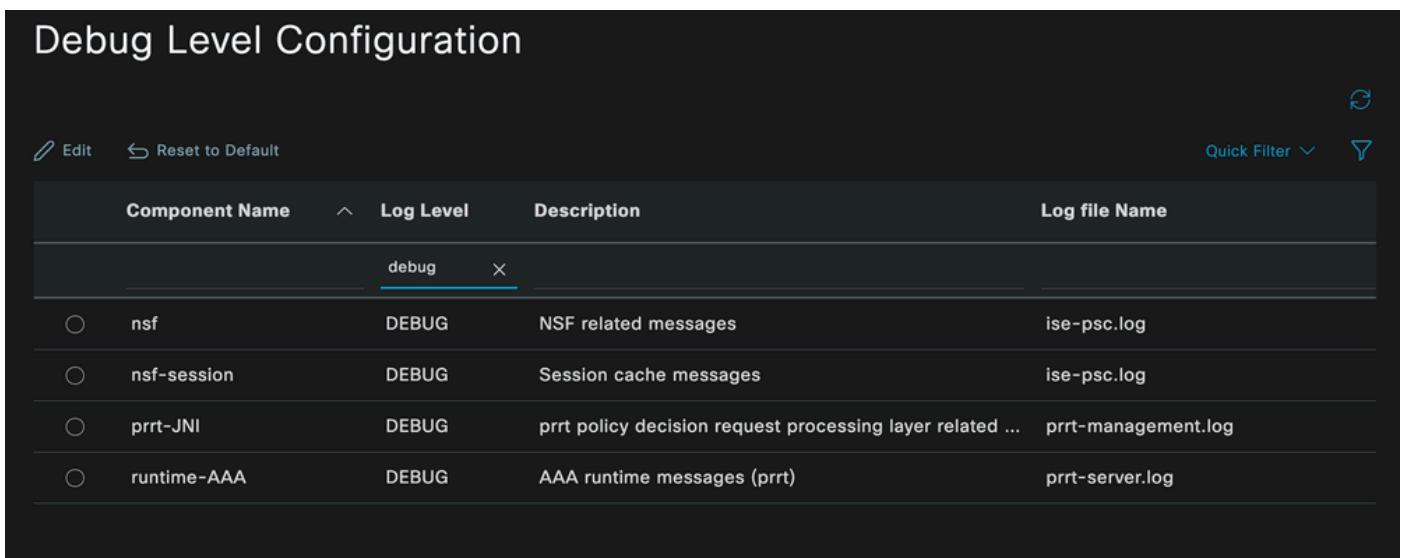
Configuratie debug-log

Zoek in de kolom Naam van component naar de eerder genoemde kenmerken. Selecteer elk logniveau en verander het om te ZUIVEREN. Sla de wijzigingen op.



Instellen van AAA-component tijdens uitvoering

Nadat u elke component hebt geconfigureerd, filtert u deze met DEBUG zodat u kunt zien of alle componenten correct zijn geconfigureerd.



Configuratie debug-log

Mocht het nodig zijn om de logbestanden onmiddellijk te analyseren, dan kunt u ze downloaden door te navigeren naar het pad ISE Menu > Operations > Probleemoplossing > Logbestanden downloaden > Knooplijst applicatie > PSN en de DEBUGS > Debug Logs ingeschakeld.

In dit geval, moet u downloaden voor dot1x en mab problemen in de prt-server.log en ise-psc.log. Het logbestand dat u moet downloaden is het logboek met de datum van uw laatste test.

Klik op het logbestand dat in deze afbeelding wordt weergegeven en download het (weergegeven

in blauwe tekst).

Debug Log Type	Log File	Description	Size
ise-psc (16) (111 MB)			
<input type="checkbox"/>	ise-psc (all logs)	Main ise debug log messages	111 MB
<input type="checkbox"/>	ise-psc.log		5.8 MB
<input type="checkbox"/>	ise-psc.log.2024-04-03-1		7.0 MB
<input type="checkbox"/>	ise-psc.log.2024-04-04-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-05-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-06-1		7.0 MB
<input type="checkbox"/>	ise-psc.log.2024-04-07-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-08-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-09-1		7.6 MB
<input type="checkbox"/>	ise-psc.log.2024-04-10-1		8.0 MB

Debug logbestanden vanaf het PSN-knooppunt

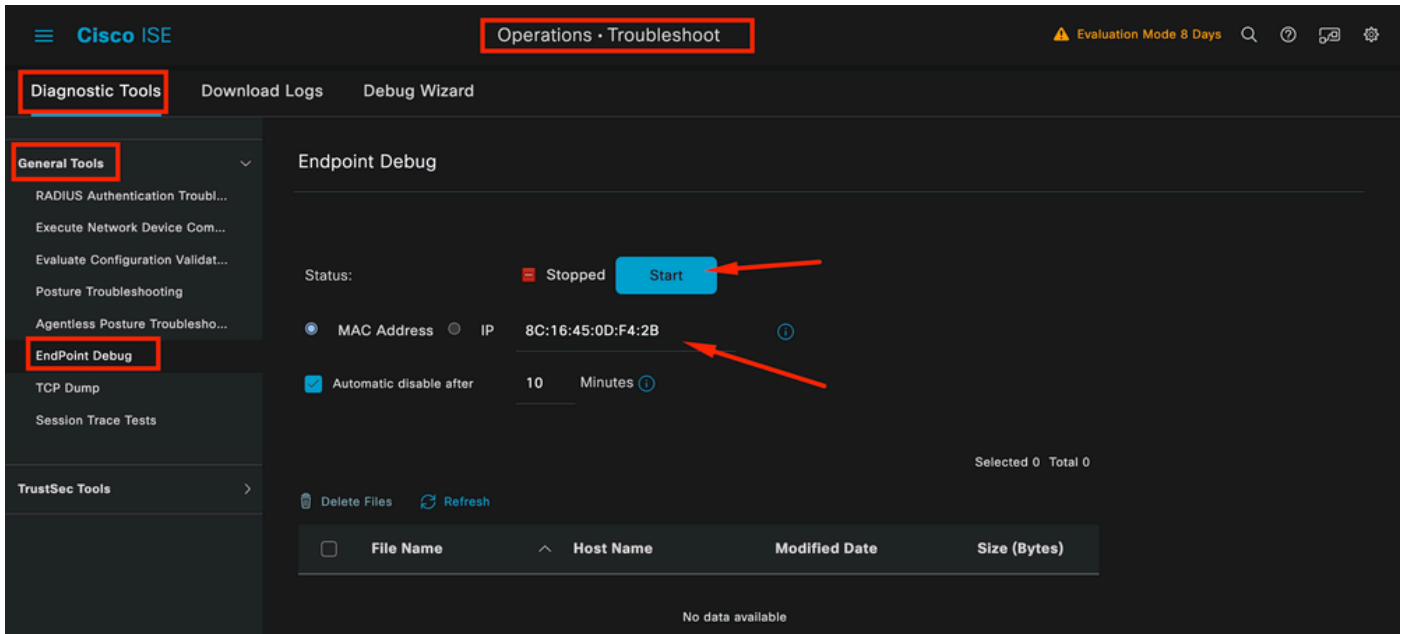
Debug Log Type	Log File	Description	Size
prrt-server (1) (7.8 MB)			
<input type="checkbox"/>	prrt-server (all logs)	Protocol Runtime runtime configuration, debug and customer logs messages	7.8 MB
<input type="checkbox"/>	prrt-server.log		7.8 MB
> pxcloud (4) (20 KB)			

Sectie Debug Logs

6 - ISE per endpoint debug

Er is ook een andere optie om te krijgen DEBUG logs, per endpoint debug logs gebaseerd op mac adres of IP. U kunt de Endpoint Debug ISE-tool gebruiken.

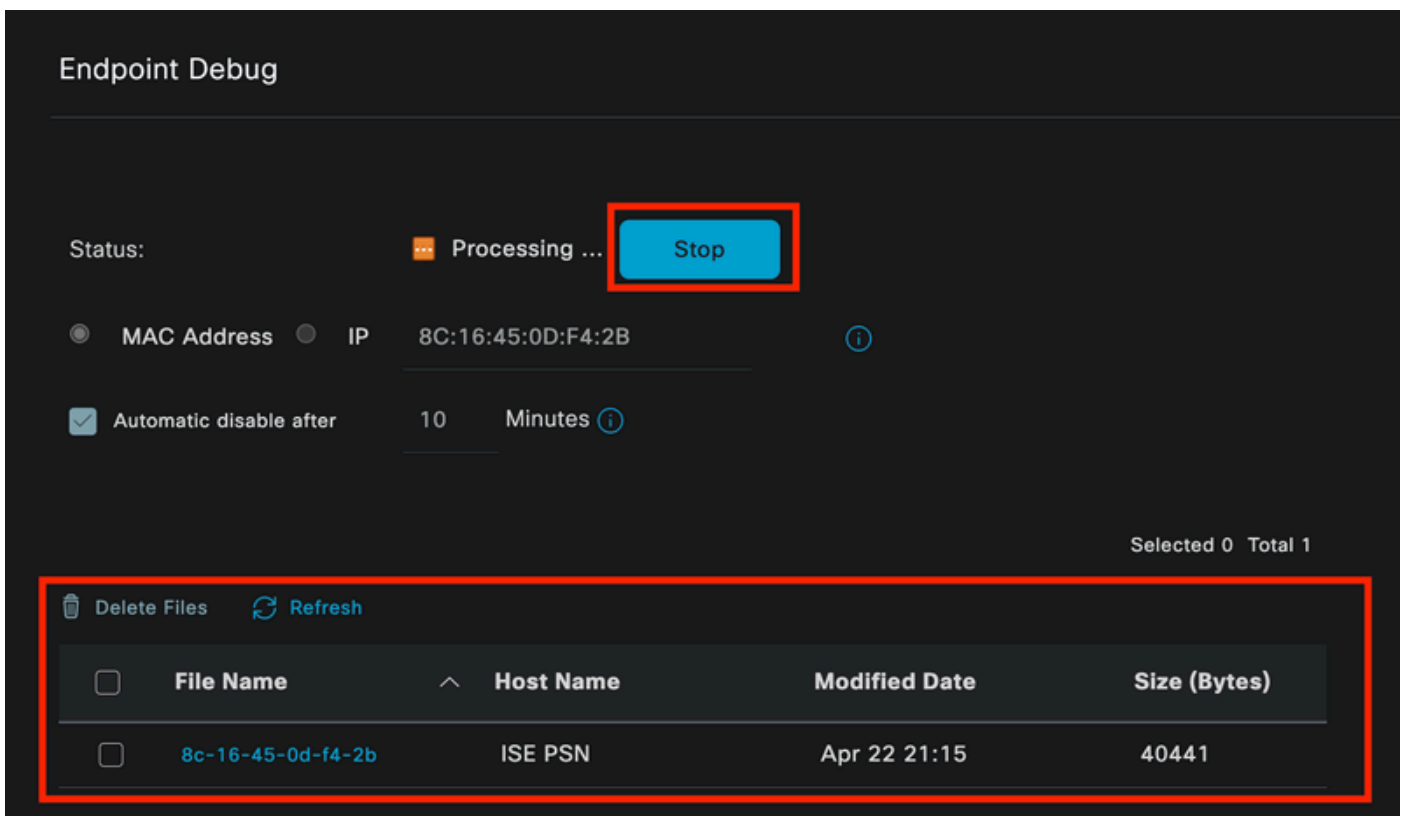
Navigeer naar het menu ISE > Operations > Probleemoplossing > Diagnostische tools > Algemene tools > Endpoint Debug.



Endpoint debug

Voer vervolgens de gewenste eindpuntinformatie in om te beginnen met het opnemen van logbestanden. Klik op Start.

Klik vervolgens op Doorgaan in het waarschuwingsbericht.



Endpoint debug

Klik na het opnemen van de informatie op Stoppen.

Klik op de blauwe bestandsnaam. in deze afbeelding.

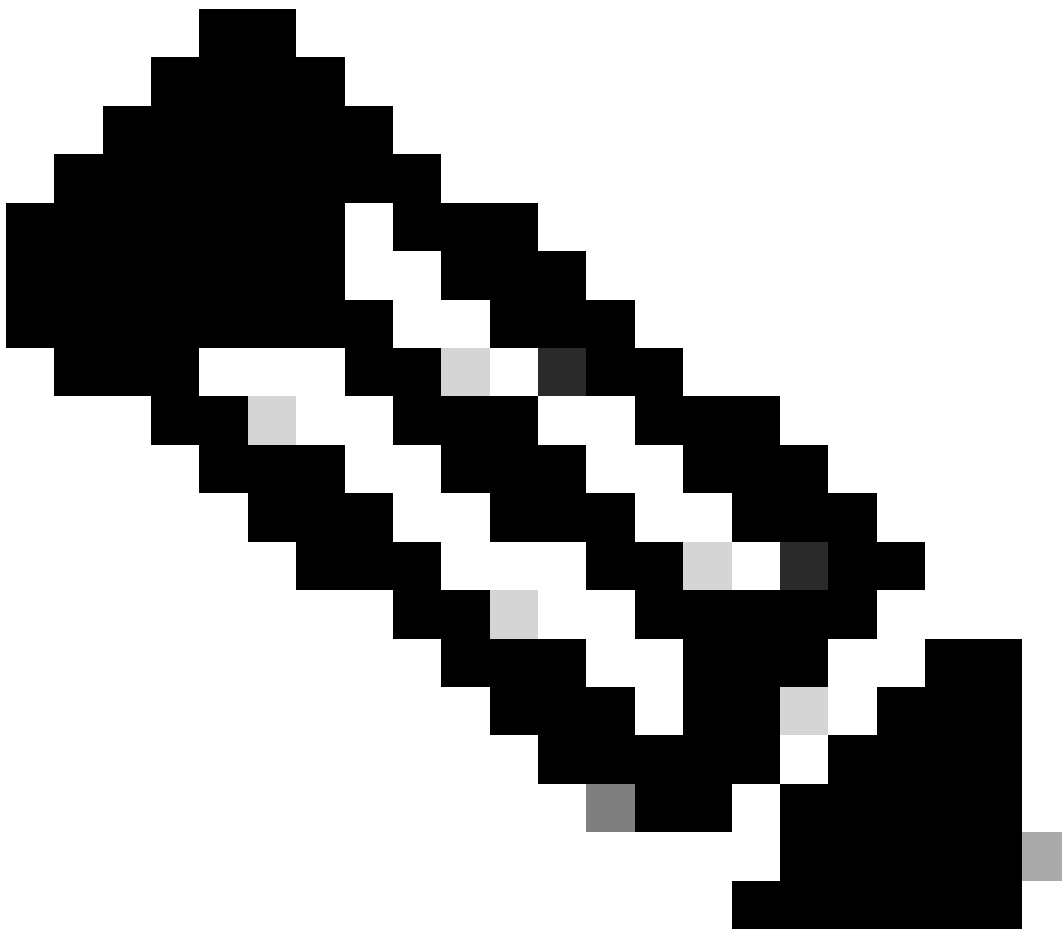
Selected 1 Total 1

Delete Files Refresh

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input checked="" type="checkbox"/>	8c-16-45-0d-f4-2b	ISE PSN	Apr 22 21:17	67959712

Endpoint debug

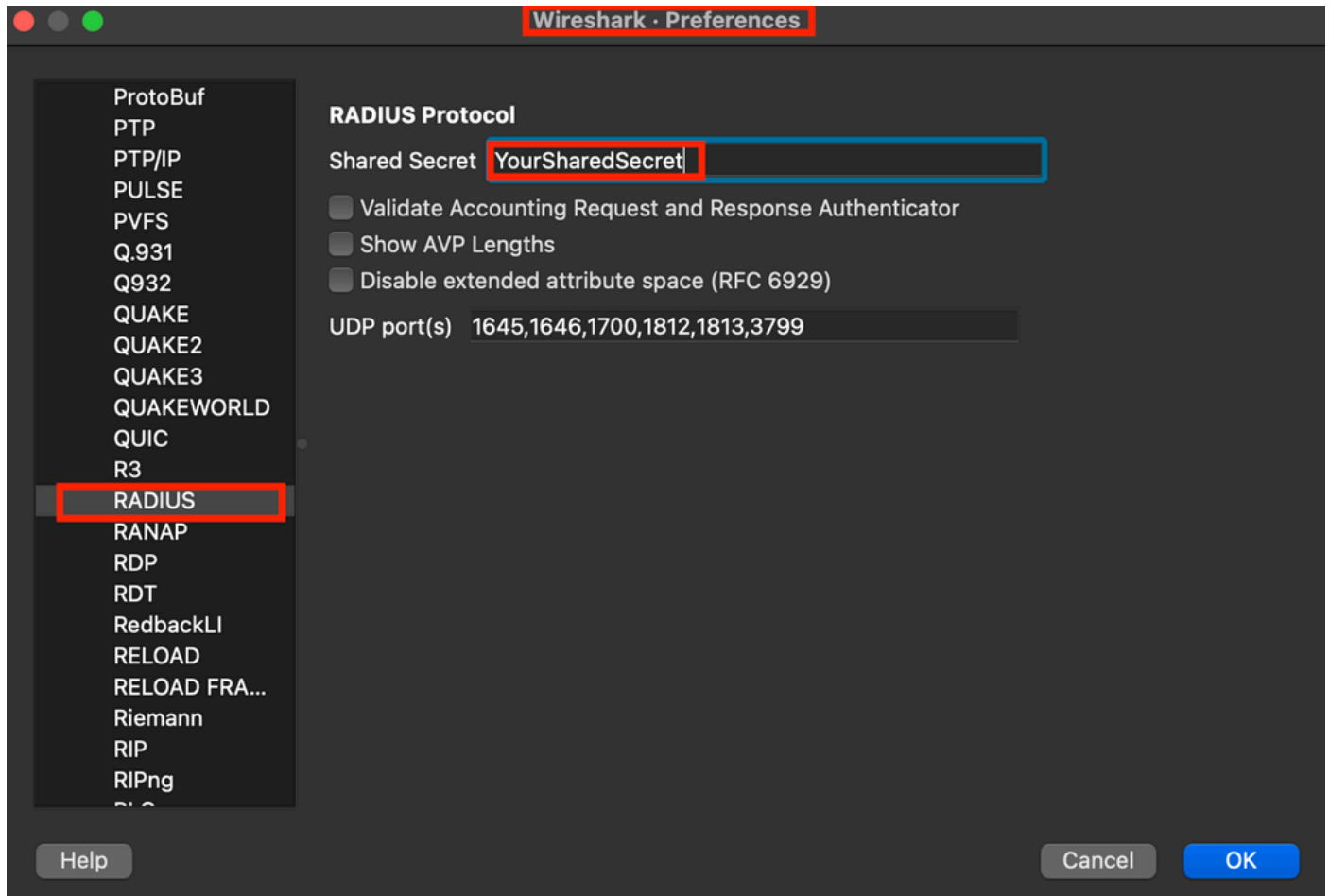
U moet de verificatielogboeken met DEBUG-logboeken kunnen zien zonder ze rechtstreeks in te schakelen vanuit de Debug Log Configuration.



Opmerking: omdat sommige dingen in de Endpoint Debug-uitvoer kunnen worden weggelaten, zou u een volledig logbestand genereren met de Debug Log Configuration en alle vereiste logbestanden downloaden van elk bestand dat u nodig hebt. Zoals uitgelegd in de vorige sectie van ISE-debugconfiguratie en -logboekverzameling.

7 - RADIUS-pakketten decrypteren

Radius-pakketten worden niet versleuteld, behalve in het veld gebruikerswachtwoord. U moet echter het verzonden wachtwoord controleren. U kunt het pakket zien dat de gebruiker door te navigeren naar Wireshark > Voorkeuren > Protocollen > RADIUS verstuurt en vervolgens de RADIUS gedeelde sleutel toevoegen die door ISE en het netwerkapparaat wordt gebruikt. Daarna worden de RADIUS-pakketten gedecrypteerd weergegeven.



Opties voor draadloze haaien

8 - Opdrachten voor probleemoplossing voor netwerkapparaten

De volgende opdracht helpt bij het oplossen van problemen met het ISR 1100- of Wired NAD-apparaat.

8 - 1 Om te zien of de AAA-server of ISE beschikbaar en bereikbaar is via het netwerkapparaat, toont u aaa-servers.

```
Router>show aaa servers
```

```
RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname  
State: current UP, duration 2876s, previous duration 0s  
Dead: total time 0s, count 0
```

```
Platform State from SMD: current UP, duration 2876s, previous duration 0s  
SMD Platform Dead: total time 0s, count 0
```

Platform State from WNCN (1) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (2) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (3) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (4) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (5) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (6) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (7) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (8) : current UP, duration 3015s, previous duration 0s

WNCN Platform Dead: total time 0s, count 0UP

Quarantined: No

Authn: request 11, timeouts 0, failover 0, retransmission 0

Response: accept 1, reject 0, challenge 10
Response: unexpected 0, server error 0, incorrect 0, time 33ms
Transaction: success 11, failure 0
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
Dot1x transactions:

Response: total responses: 11, avg response time: 33ms
Transaction: timeouts 0, failover 0
Transaction: total 1, success 1, failure 0

MAC auth transactions:
Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0

Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
MAC author transactions:

Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
Request: start 1, interim 0, stop 0
Response: start 1, interim 0, stop 0

Response: unexpected 0, server error 0, incorrect 0, time 27ms
Transaction: success 2, failure 1
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0

Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0


```
Consecutive Response Failures: total 0
  SMD Platform : max 0, current 0 total 0
  WNCN Platform: max 0, current 0 total 0
  IOSN Platform : max 0, current 0 total 0

Consecutive Timeouts: total 3
  SMD Platform : max 0, current 0 total 0
  WNCN Platform: max 0, current 0 total 0
  IOSN Platform : max 3, current 0 total 3

Requests per minute past 24 hours:
  high - 0 hours, 47 minutes ago: 4
  low  - 0 hours, 45 minutes ago: 0
  average: 0
```

Router>

8-2 Om de poortstatus, de details, de op de sessie toegepaste ACL's, de verificatiemethode en meer nuttige informatie te zien, gebruikt u de opdracht tonen de interface van verificatiesessies <interface waar de laptop is aangesloten> details.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781FOA0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0
```

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
```

```
Server Policies:
```

```
Method status list:
Method State
dot1x Authc Success
```

Router#

8-3 Om te verifiëren dat u alle vereiste opdrachten voor aaa in de globale configuratie hebt, voert u tonen in werking stellen-configuratie aaa.

```

Router#sh run aaa
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
client <A.B.C.D> server-key Cisc0123
!
!
radius server COHVSRAISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRAISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#

```

8-4 Een andere handige opdracht is test aaa groep radius server <A.B.C.D> isisecool VainillaISE97 legacy.

```

Router#test aaa group radius server <A.B.C.D> isisecool VainillaISE97 legacy
User was successfully authenticated.

Router#

```

9 - Relevante debugs van netwerkapparaten

- debug dot1x all - Hier worden alle dot1x EAP-berichten weergegeven
- debug aaa-verificatie - Hier wordt informatie over debuggen van verificaties van AAA-toepassingen weergegeven
- debug aaa-autorisatie - Informatie over debug voor AAA-autorisatie
- debug radius authenticatie - Hier vindt u gedetailleerde informatie over activiteiten op protocolniveau, alleen voor de verificatie
- debug radius - Hier vindt u gedetailleerde informatie over activiteiten op protocolniveau

Gerelateerde informatie

- [Cisco Technical Support en downloads](#)

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.