Machine tweefactorverificatie configureren voor toegang door aanvrager

Inhoud

Inleiding

Dit document beschrijft de stappen die nodig zijn om Twee-Factor-verificatie te configureren met machine- en dot1x-verificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco Identity Services Engine
- Configuratie van Cisco Catalyst
- IEEE 802.1X

Gebruikte componenten

- Identity Services Engine virtuele 3.3-patch 1
- C100-48FP-4G-L 15.2(7)E9 switch

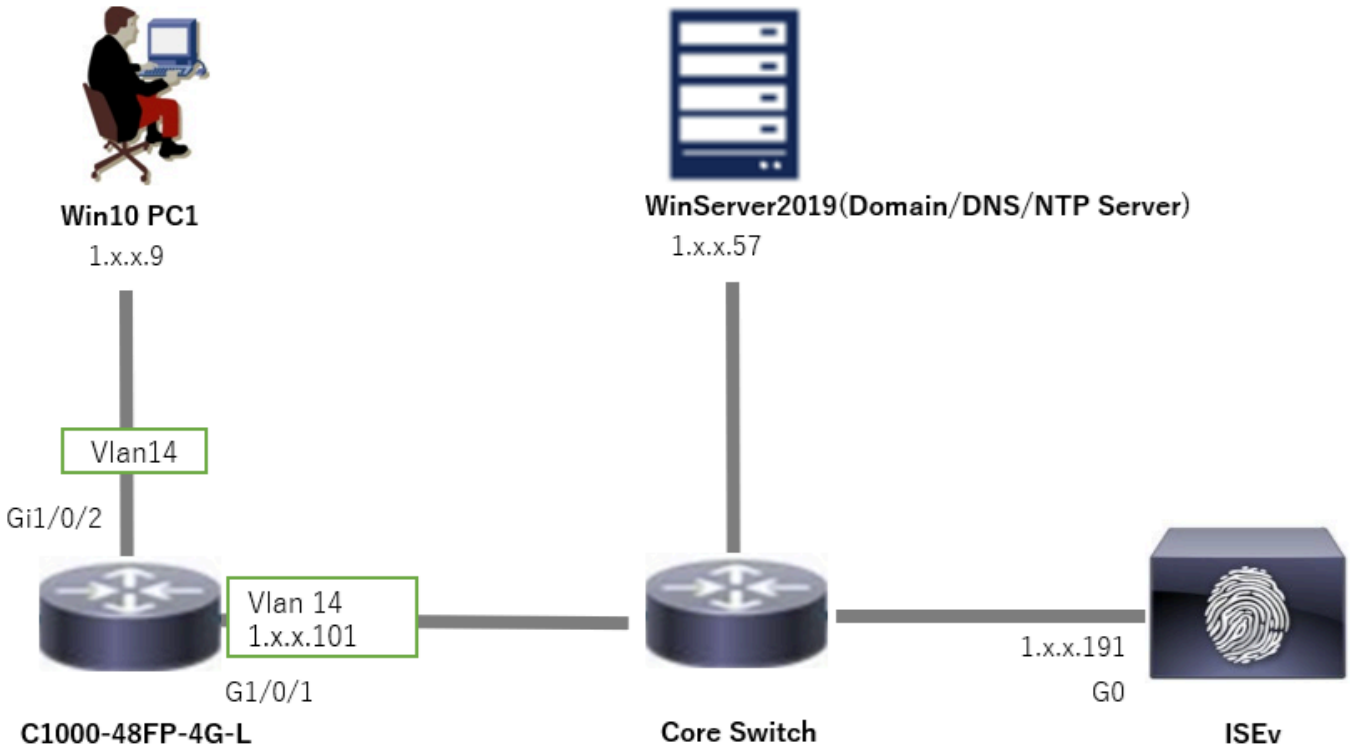
- Windows Server 2019

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.

Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.

De domeinnaam ingesteld op Windows Server 2019 is ad.rem-xxx.com, die wordt gebruikt als voorbeeld in dit document.



Netwerkdiagram

Achtergrondinformatie

Machineverificatie is een beveiligingsproces dat de identiteit verifieert van een apparaat dat toegang zoekt tot een netwerk of systeem. In tegenstelling tot gebruikersverificatie, die de identiteit van een persoon verifieert op basis van referenties zoals een gebruikersnaam en wachtwoord, concentreert de machine-verificatie zich op het valideren van het apparaat zelf. Dit gebeurt vaak met behulp van digitale certificaten of beveiligingssleutels die uniek zijn voor het apparaat.

Door machine- en gebruikersverificatie samen te gebruiken, kan een organisatie ervoor zorgen dat alleen bevoegde apparaten en gebruikers toegang hebben tot haar netwerk, waardoor een veiligere omgeving wordt gecreëerd. Deze tweeledige verificatiemethode is bijzonder nuttig voor het beschermen van gevoelige informatie en het voldoen aan strikte regulerende normen.

Configuraties

Configuratie in C1000

Dit is de minimale configuratie in C1000 CLI.

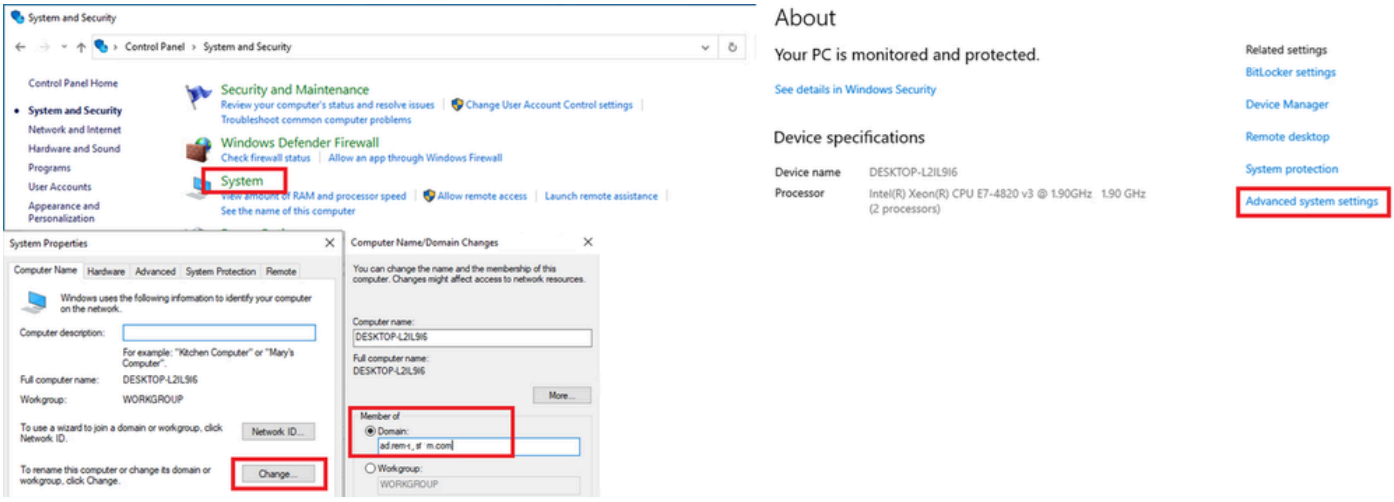
```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
key cisco123
```

```
aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configuratie in Windows-pc

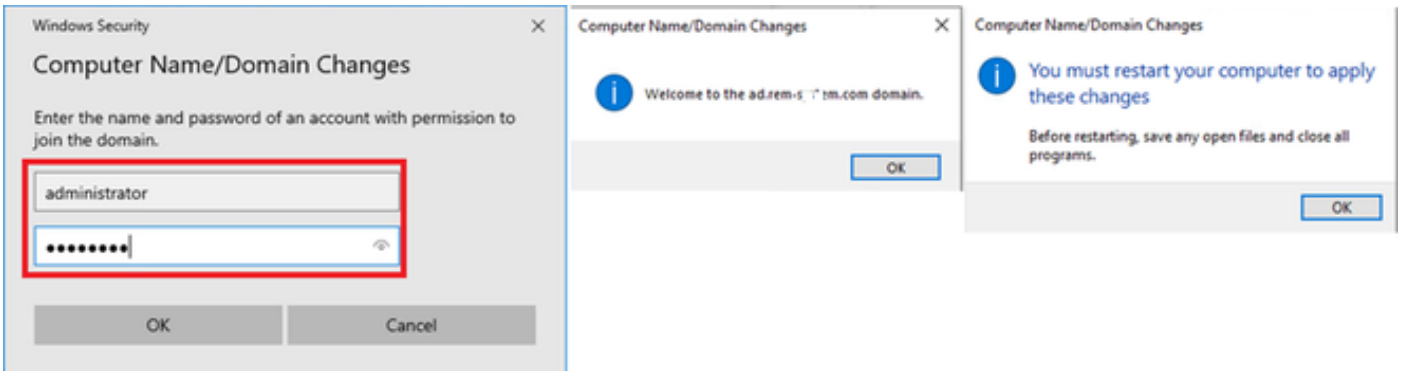
Stap 1. PC toevoegen aan AD-domein

Navigeer naar Configuratiescherm > Systeem en beveiliging, klik op Systeem en klik vervolgens op Geavanceerde systeeminstellingen. Klik in het venster Systeemeigenschappen op Wijzigen, selecteer Domein en voer de domeinnaam in.



PC toevoegen aan AD-domein

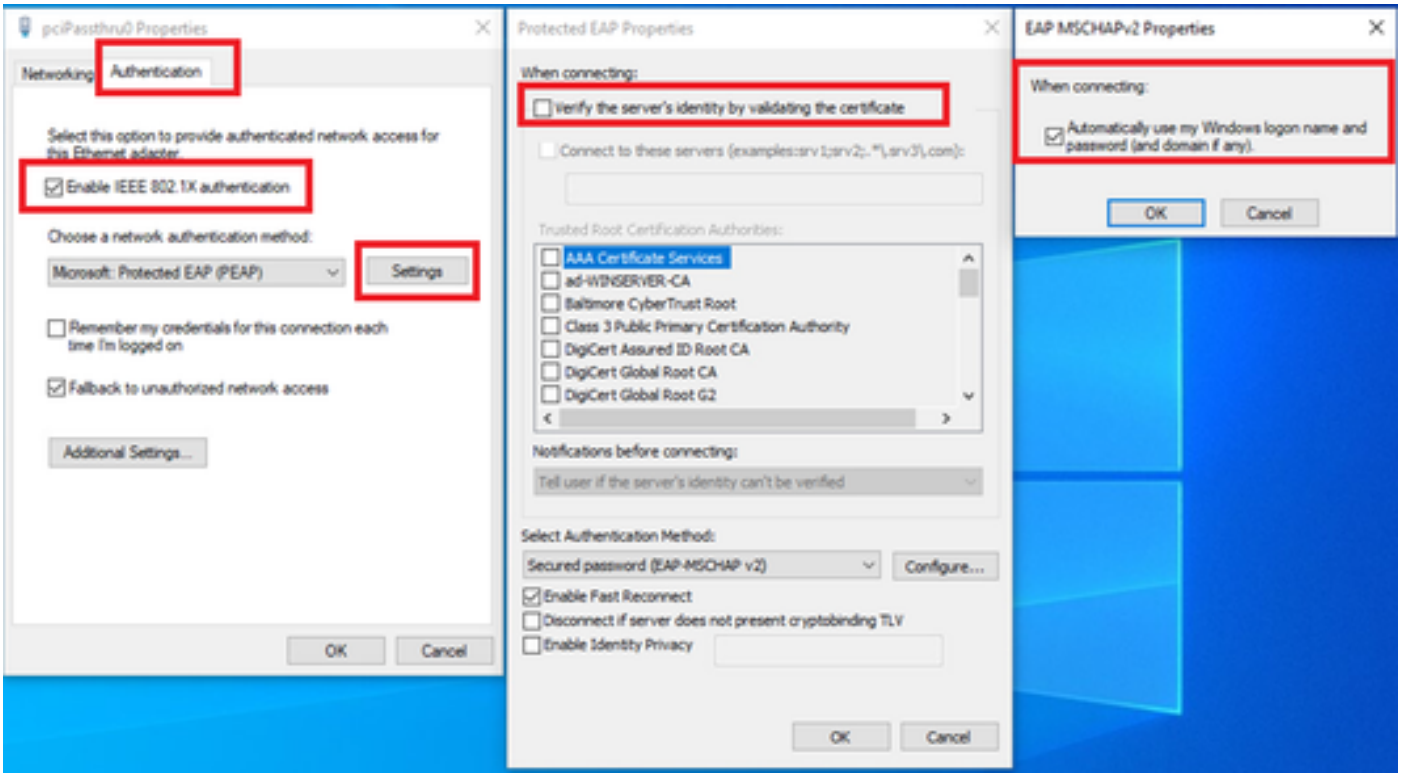
Voer in het venster Windows Beveiliging de gebruikersnaam en het wachtwoord van de domeinserver in.



Gebruikersnaam en wachtwoord invoeren

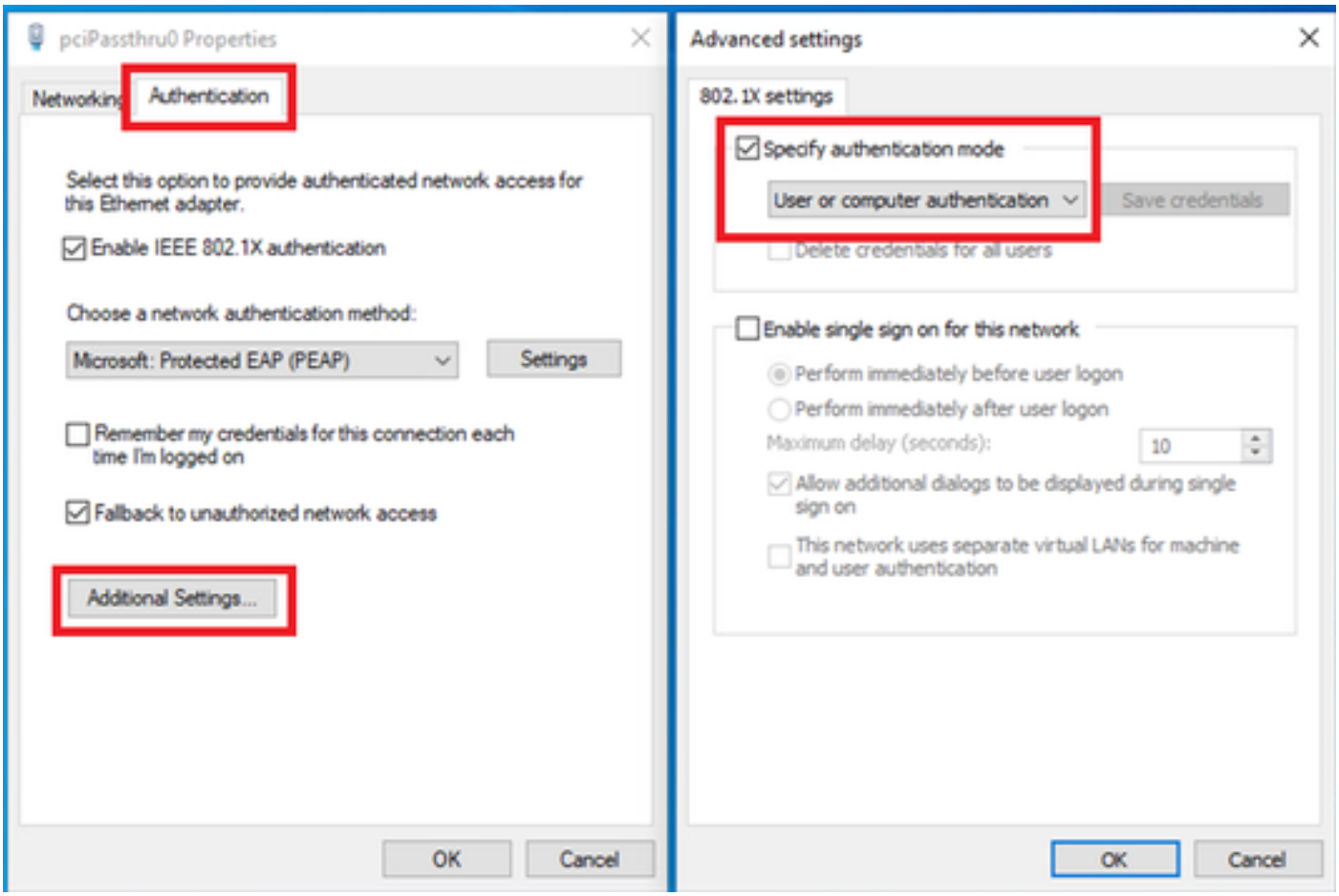
Stap 2. Gebruikersverificatie configureren

Navigeer naar verificatie en controleer IEEE 802.1X-verificatie inschakelen. Klik op Instellingen in het venster met beschermde EAP-eigenschappen, uncheck Controleer de identiteit van de server door het certificaat te valideren en klik vervolgens op Configureren. Selecteer in het venster EAP MSCHAPv2 Properties de optie Automatisch mijn Windows-aanmeldingsnaam en -wachtwoord (en eventueel een domein) om de gebruikersnaam te gebruiken die is ingevoerd tijdens de aanmelding bij de Windows-machine voor gebruikersverificatie.



Gebruikersverificatie inschakelen

Navigeer naar Verificatie en controleer Extra instellingen. Selecteer Gebruiker- of computerverificatie in de vervolgkeuzelijst.

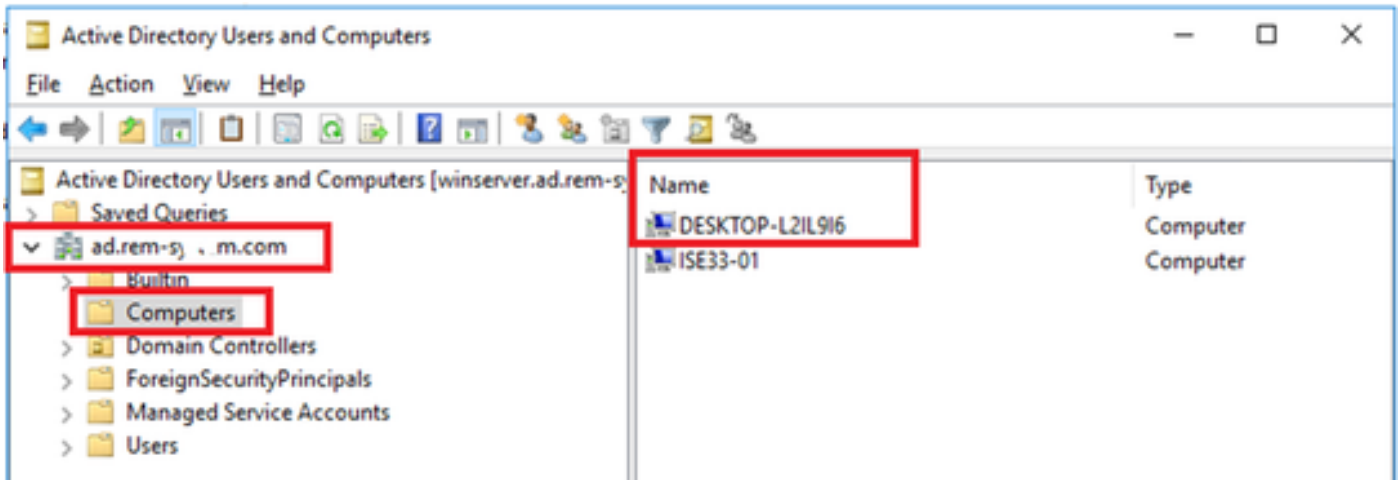


Verificatiemodus opgeven

Configuratie in Windows-server

Stap 1. Domeincomputers bevestigen

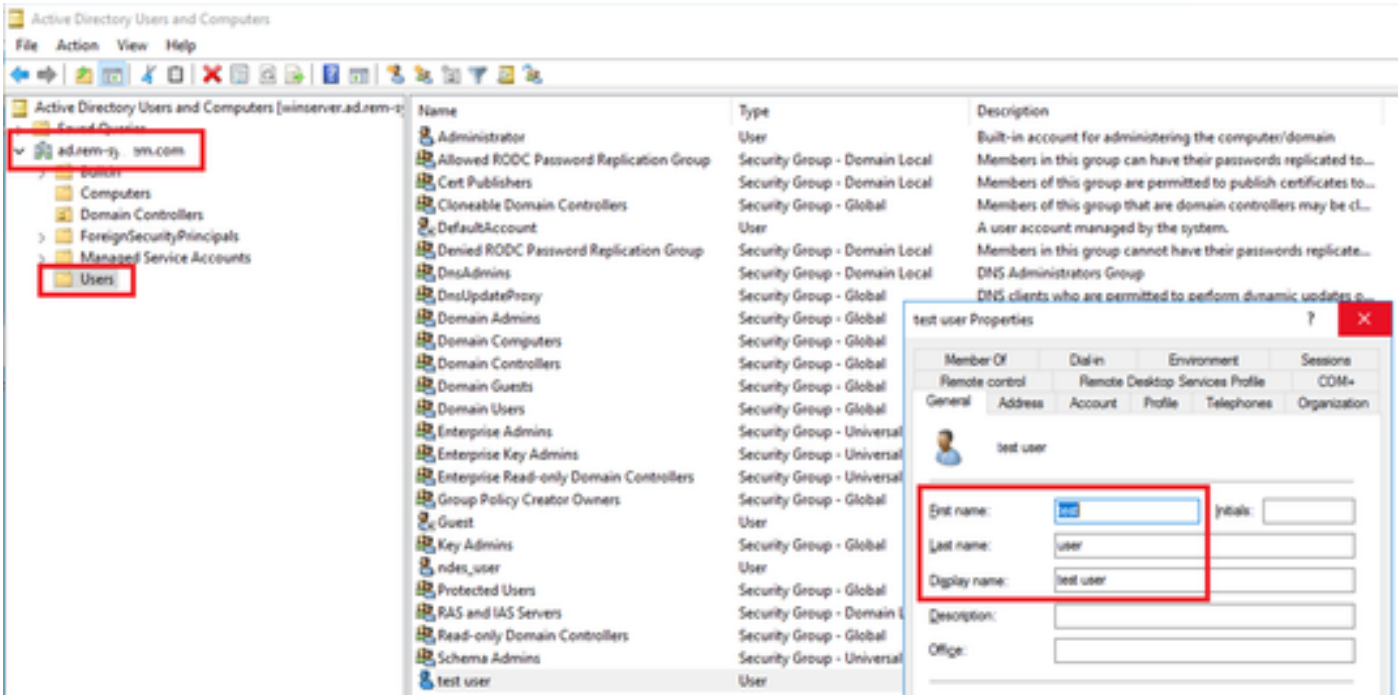
Navigeer naar Active Directory-gebruikers en -computers, klik op Computers. Bevestig dat Win10 PC1 in het domein wordt vermeld.



Domain Computer bevestigen

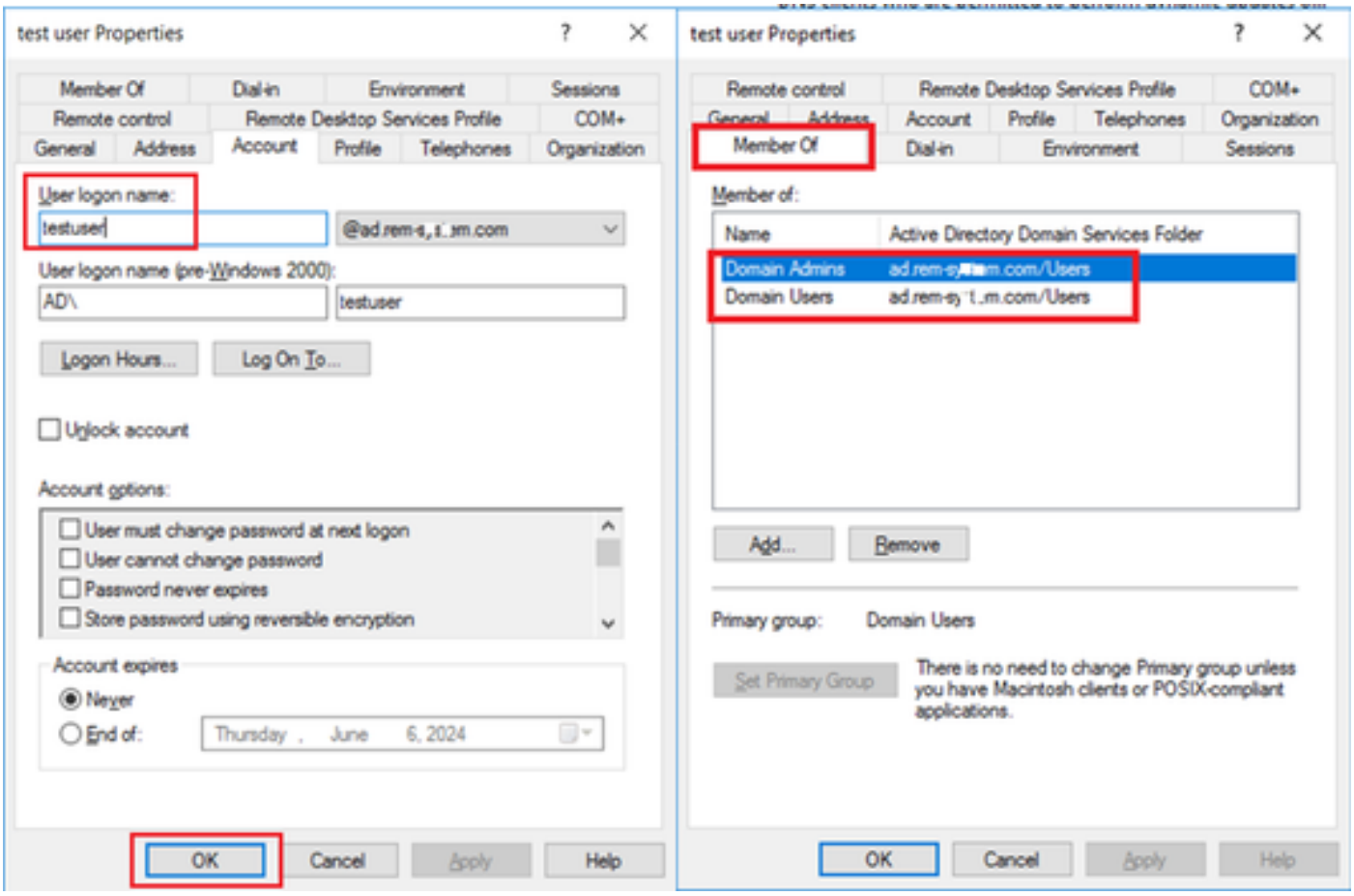
Stap 2. Domeingebruiker toevoegen

Navigeer naar Active Directory-gebruikers en -computers, klik op Gebruikers. Voeg testuser toe als domeingebruiker.



Domeingebruiker toevoegen

Voeg de domeingebruiker toe aan lid van Domain Admins en Domain Gebruikers.

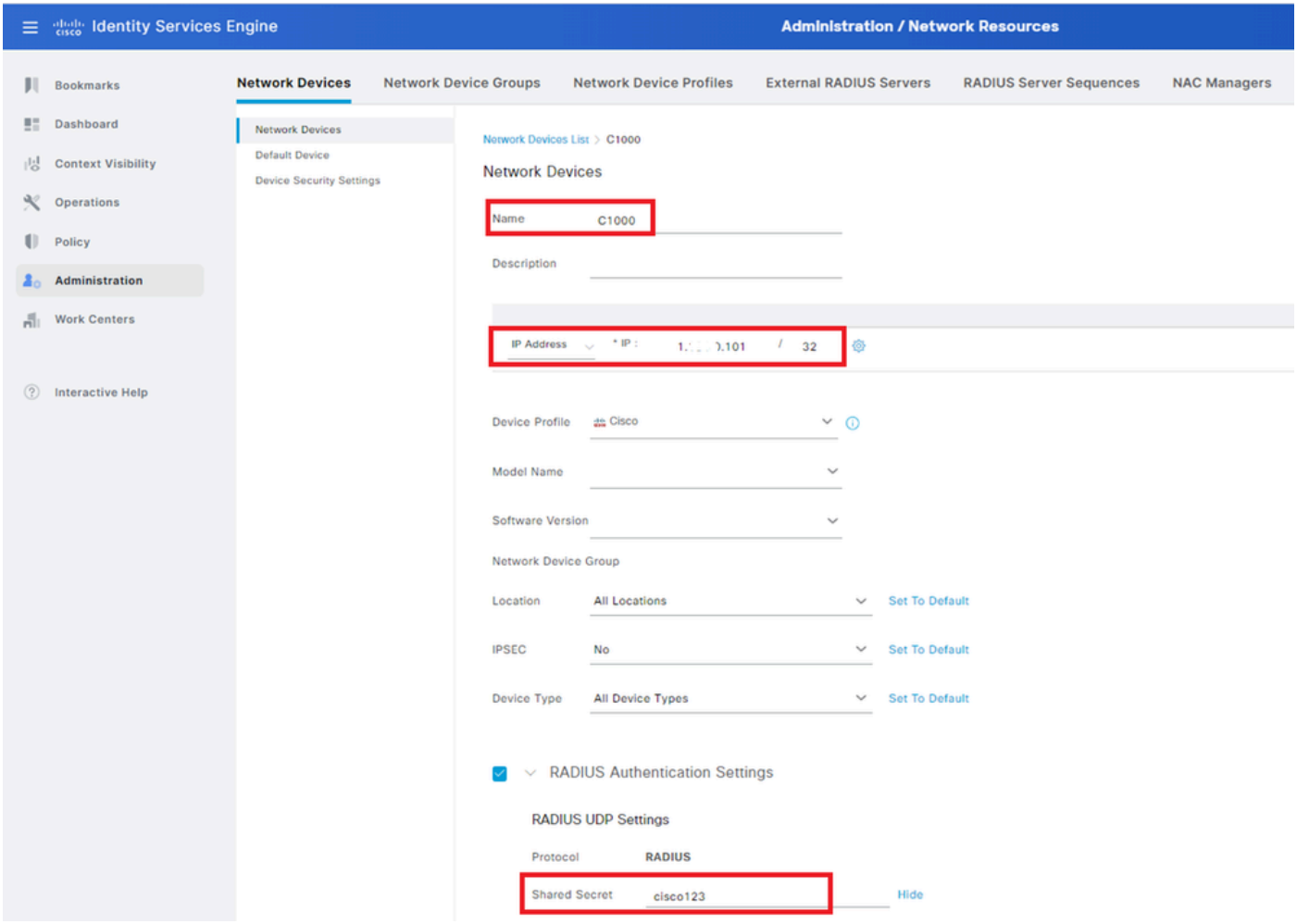


Domain Admins en domeingebruikers

Configuratie in ISE

Stap 1. Apparaat toevoegen

Navigeer naar Beheer > Netwerkapparaten en klik op de knop Toevoegen om C1000-apparaat toe te voegen.

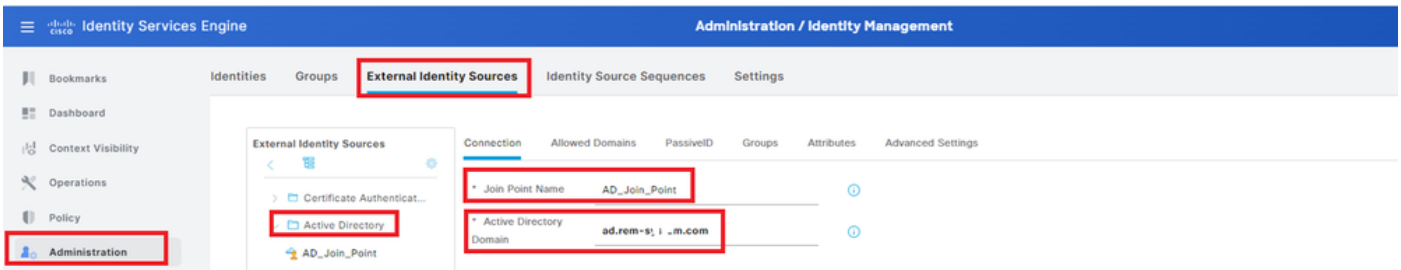


Apparaat toevoegen

Stap 2. Actieve map toevoegen

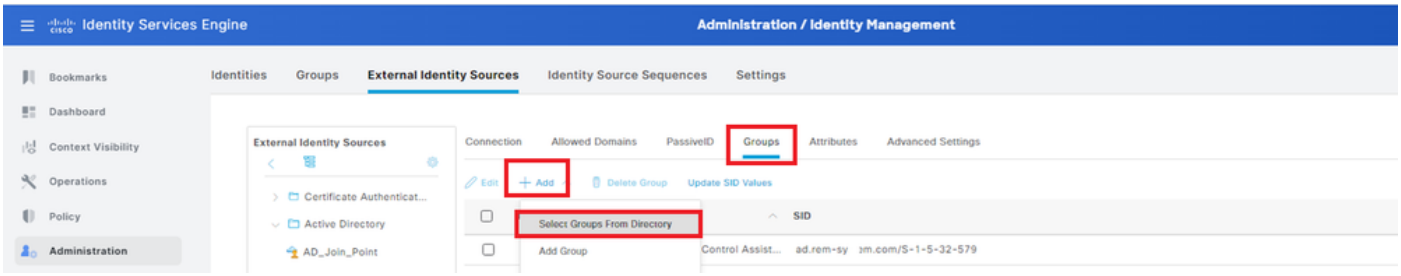
Navigeer naar Beheer > Externe Identiteitsbronnen > Active Directory, klik op tabblad Connection en voeg Active Directory toe aan ISE.

- Lid worden Naam: AD_Join_Point
- Active Directory-domein: ad.rem-xxx.com



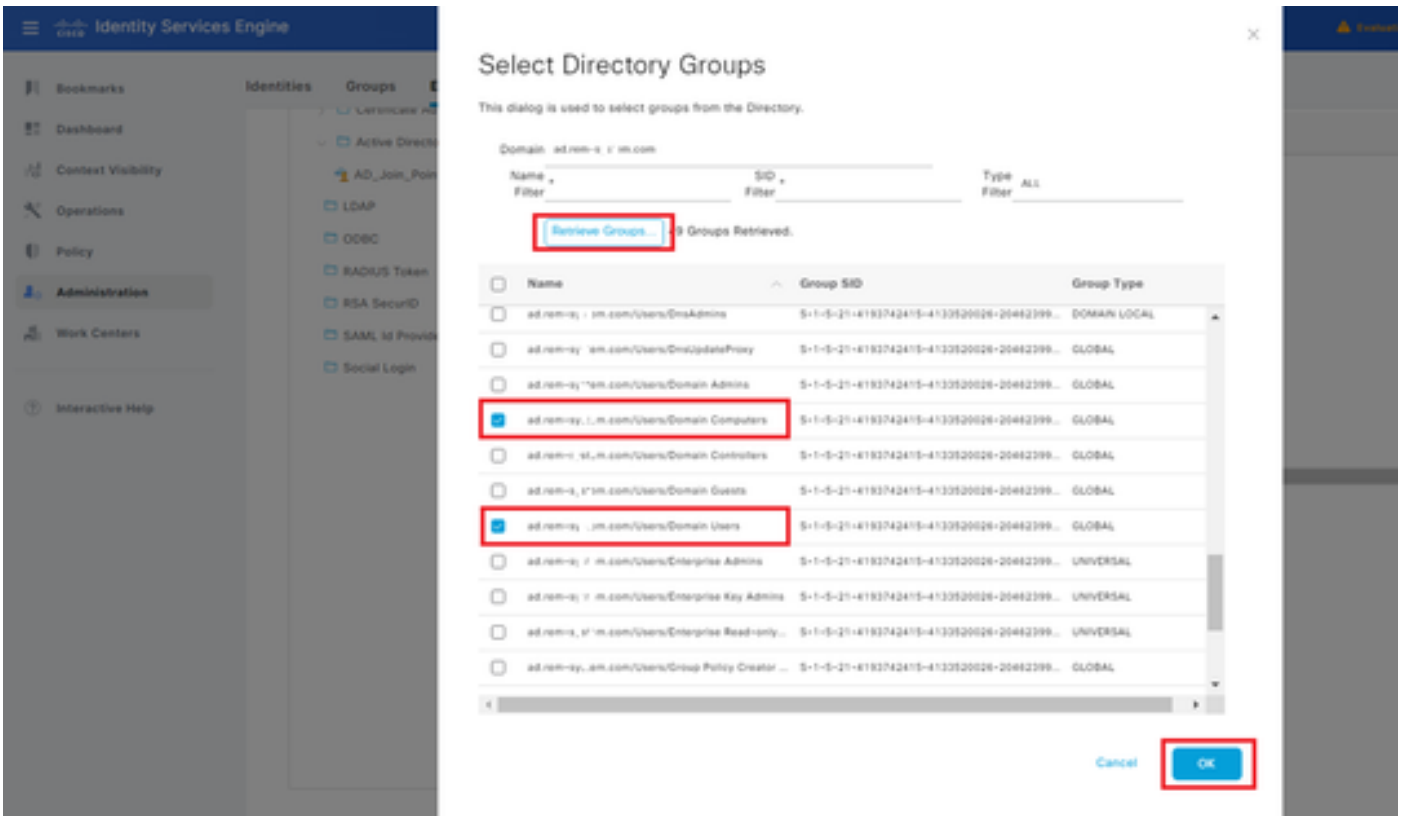
Actieve map toevoegen

Navigeer naar het tabblad Groepen en selecteer Groepen uit map uit vervolgkeuzelijst.



Groepen uit map selecteren

Klik op Groepen ophalen uit vervolgkeuzelijst. Controleer ad.rem-xxx.com/Users/Domain Computers en ad.rem-xxx.com/Users/Domain Gebruikers en klik op OK.



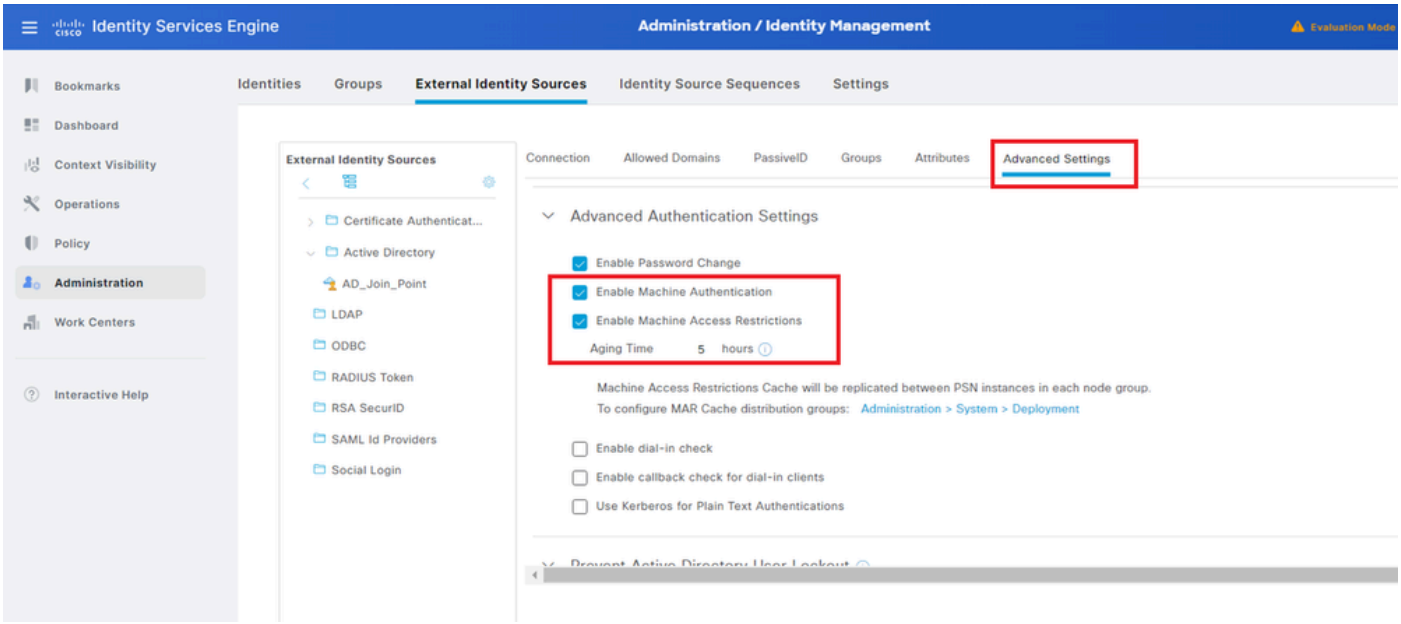
Domeincomputers en -gebruikers toevoegen

Stap 3. Instellingen voor machineverificatie bevestigen

Navigeer naar het tabblad Geavanceerde instellingen en bevestig de instelling van de verificatie van de machine.

- Machine-verificatie inschakelen: automatische verificatie inschakelen
- Beperking machinetoegang inschakelen: gebruikers- en machineverificatie combineren vóór autorisatie

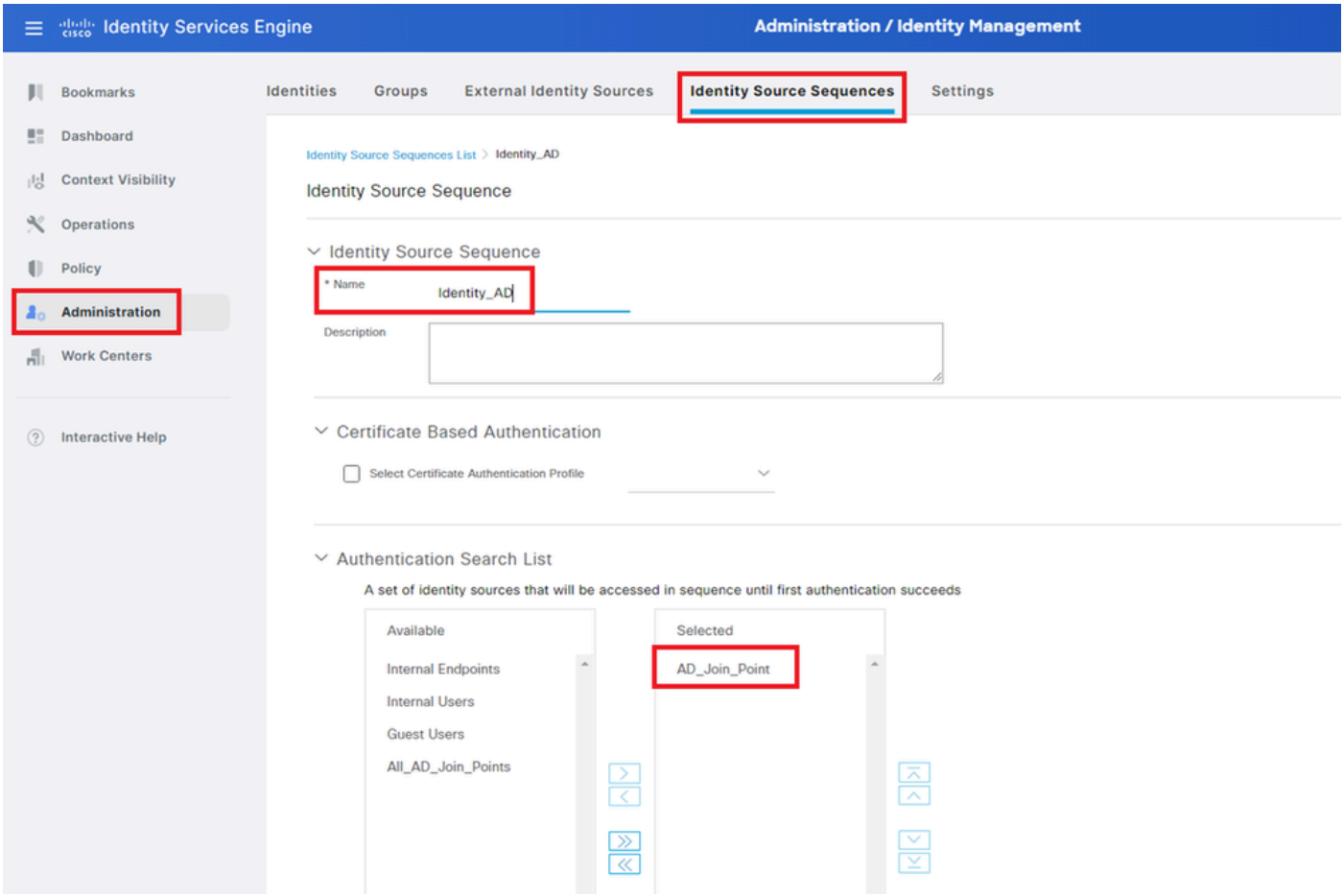
Opmerking: Het geldige bereik van de verouderingstijd is 1 tot 8760.



Stap 4. Identity Source Sequences toevoegen

Ga naar Beheer > Identity Source Sequences en voeg een Identity Source Sequence toe.

- Naam: Identity_AD
- Verificatie Zoeklijst: AD_Join_Point

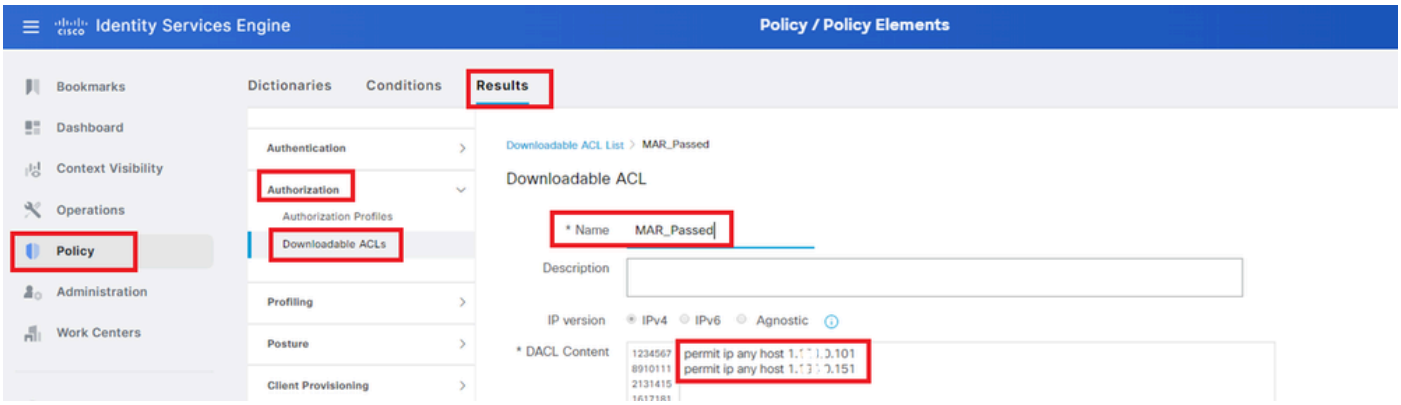


Identity Source Sequences toevoegen

Stap 5. DACL-profiel en autorisatieprofiel toevoegen

Navigeer naar Beleid > Resultaten > Autorisatie > Downloadbare ACL's, voeg een DACL toe.

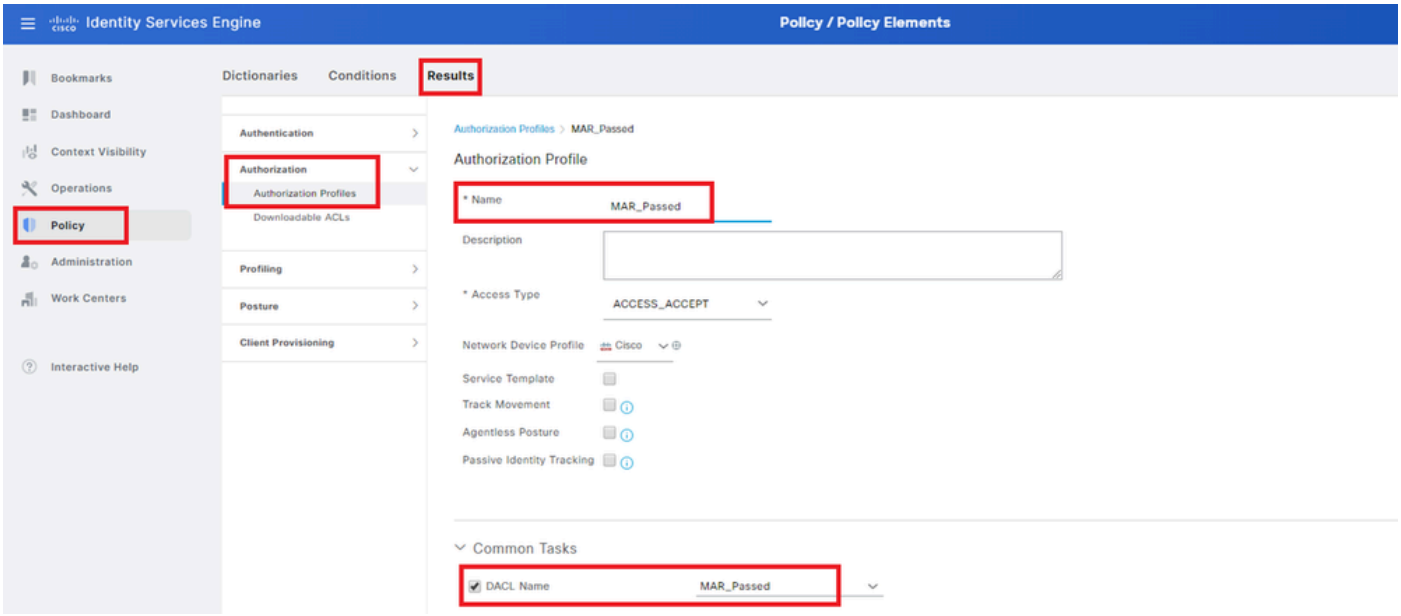
- Naam: MAR_Passed
- DACL-inhoud: laat ip elke host 1.x.x.101 toe en laat ip elke host 1.x.x.105 toe



DACL toevoegen

Navigeer naar Beleid > Resultaten > Autorisatie > Autorisatieprofielen en voeg een autorisatieprofiel toe.

- Naam: MAR_Passed
- DACL-naam: MAR_Passed

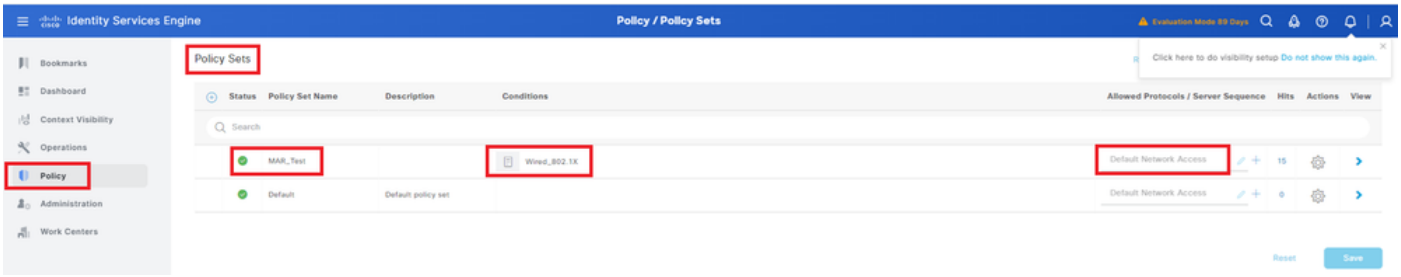


Vergunningsprofiel toevoegen

Stap 6. Beleidsset toevoegen

Navigeer naar Policy > Policy Sets, klik op + om een policy set toe te voegen.

- Naam van de beleidsreeks: MAR_Test
- Voorwaarden: Wired_802.1x
- Toegestane protocollen/serverreeks: standaard netwerktoegang

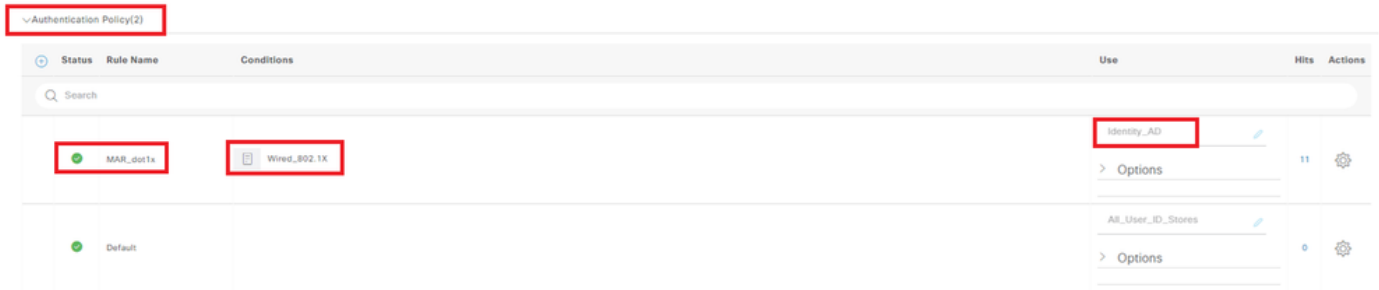


Beleidsset toevoegen

Stap 7. Verificatiebeleid toevoegen

Navigeer naar Policy Sets, klik op MAR_Test om een verificatiebeleid toe te voegen.

- Regel Naam: MAR_dot1x
- Voorwaarden: Wired_802.1x
- Gebruik: Identity_AD



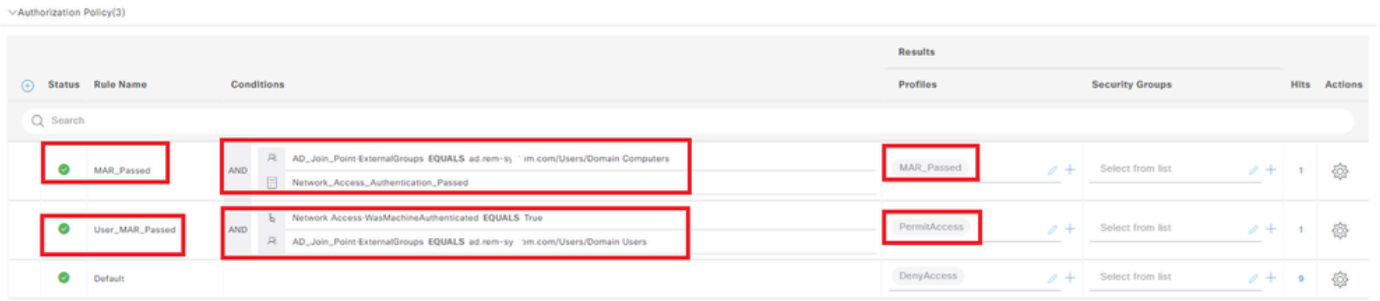
Verificatiebeleid toevoegen

Stap 8. Toepassingsbeleid toevoegen

Navigeren naar Policy Sets, klik op MAR_Test om een autorisatiebeleid toe te voegen.

- Regel Naam: MAR_Passed
- Voorwaarden: AD_Join_Point·ExterneGroepen EQUALS ad.rem-xxx.com/Users/Domain Computers EN Network_Access_Verification_Passed
- Resultaten: MAR_Passed

- Regel Naam: Gebruiker_MAR_Passed
- Voorwaarden: Network Access·WasMachineAuthenticated EQUALS True en AD_Join_Point·ExterneGroepen GELIJKT ad.rem-xxx.com/Users/Domain Gebruikers
- Resultaten: PermitAccess



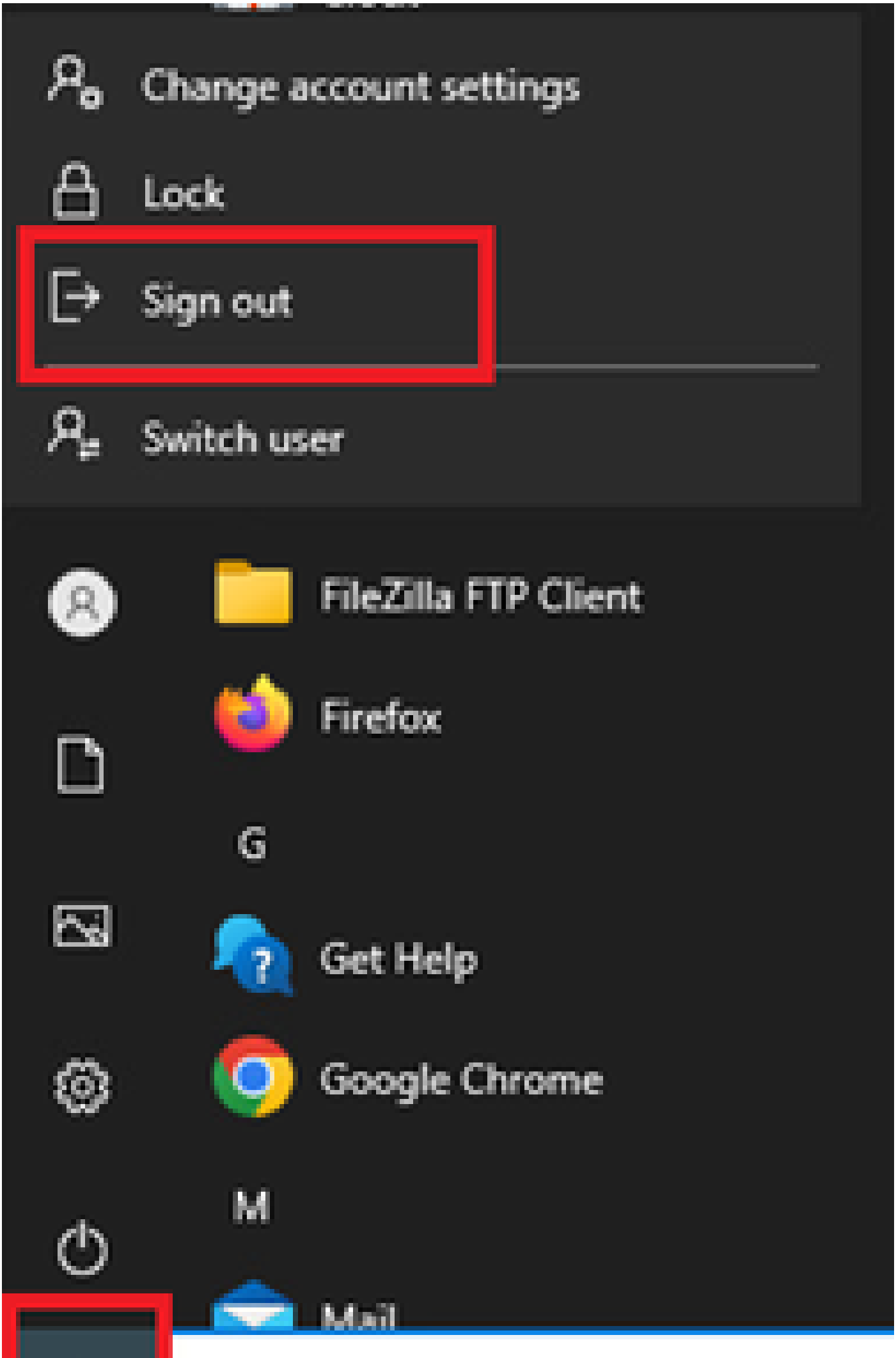
Toepassingsbeleid toevoegen

Verifiëren

Patroon 1. Machine-verificatie en gebruikersverificatie

Stap 1. Uitloggen op Windows-pc

Klik op de knop Uitloggen vanaf Win10 PC1 om de machine-verificatie te activeren.


Change account settings
Lock
Sign out
Switch user
FileZilla FTP Client
Firefox
G
Get Help
Google Chrome
M
Mail

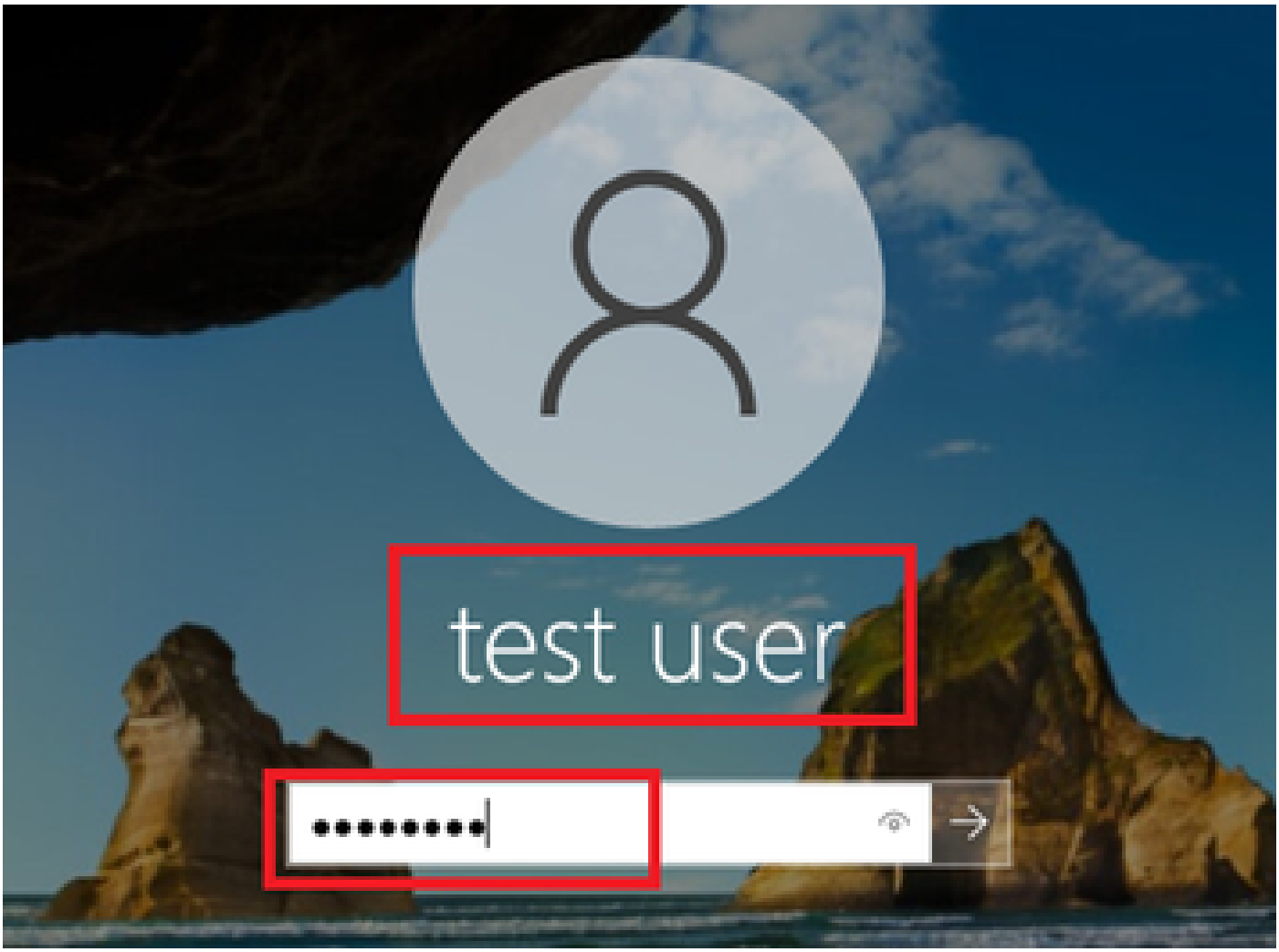
```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

host/DESKTOP-L2IL9I6.ad.rem-xxx.com

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 5s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003C
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success
```

Stap 3. Aanmelden bij Windows-pc

Login Win10 PC1, voer gebruikersnaam en wachtwoord in om gebruikersverificatie te activeren.



Aanmelden bij Windows-pc

Stap 4. Verificatiesessie bevestigen

show authentication sessions interface GigabitEthernet1/0/2 details Voer de opdracht uit om de gebruikersverificatiesessie in C1000 te bevestigen.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

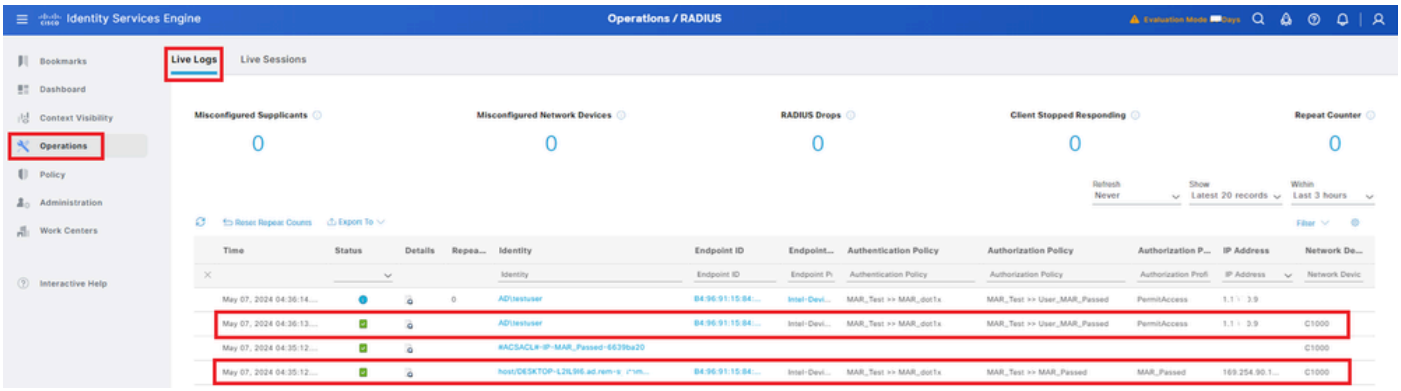
AD\testuser

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
```

```
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 85s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

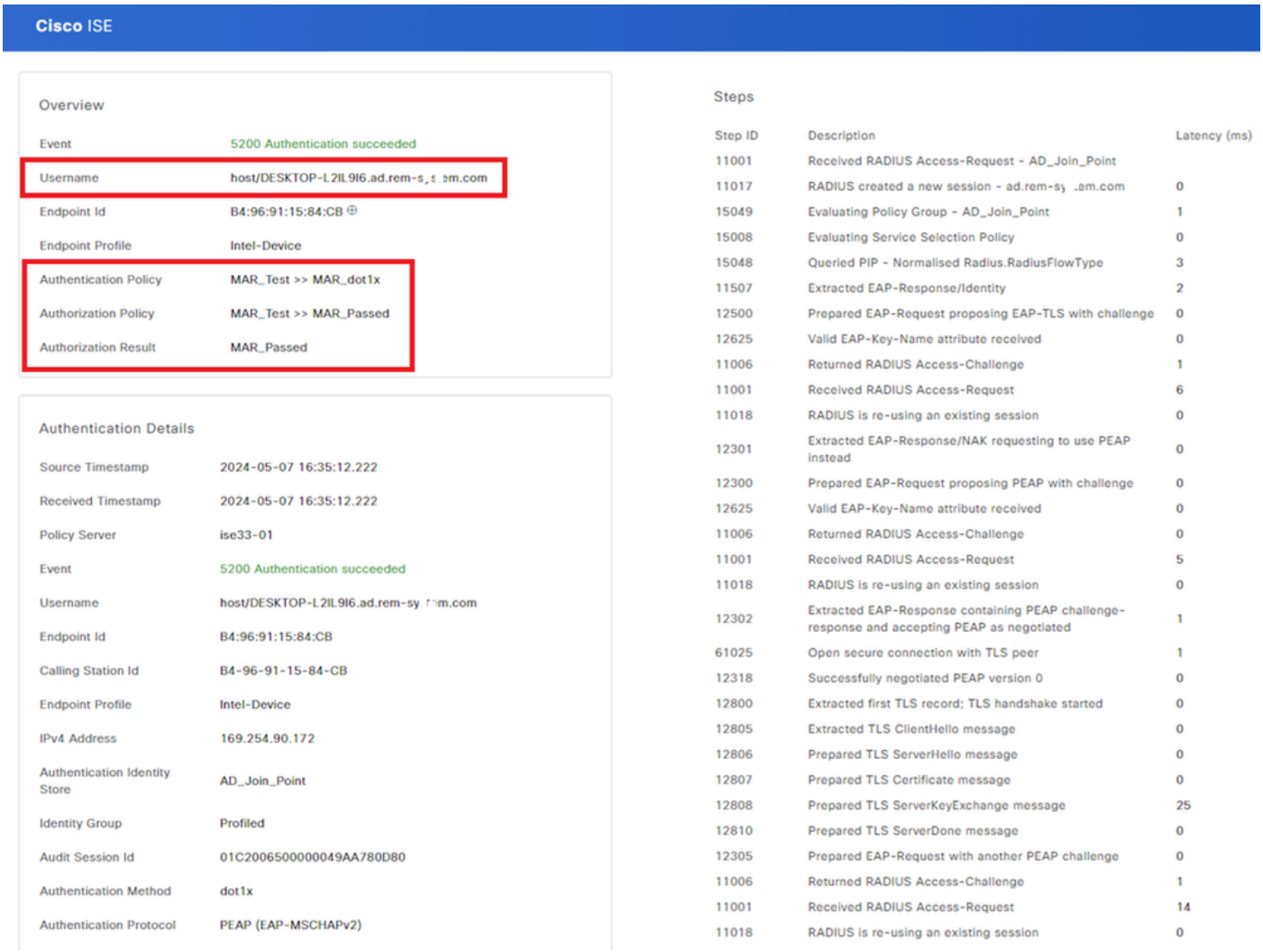
Stap 5. Radius live log bevestigen

Navigeer naar **Operations > RADIUS > Live logs** in ISE GUI, bevestig het bewegende logbestand voor machine-verificatie en gebruikersverificatie.



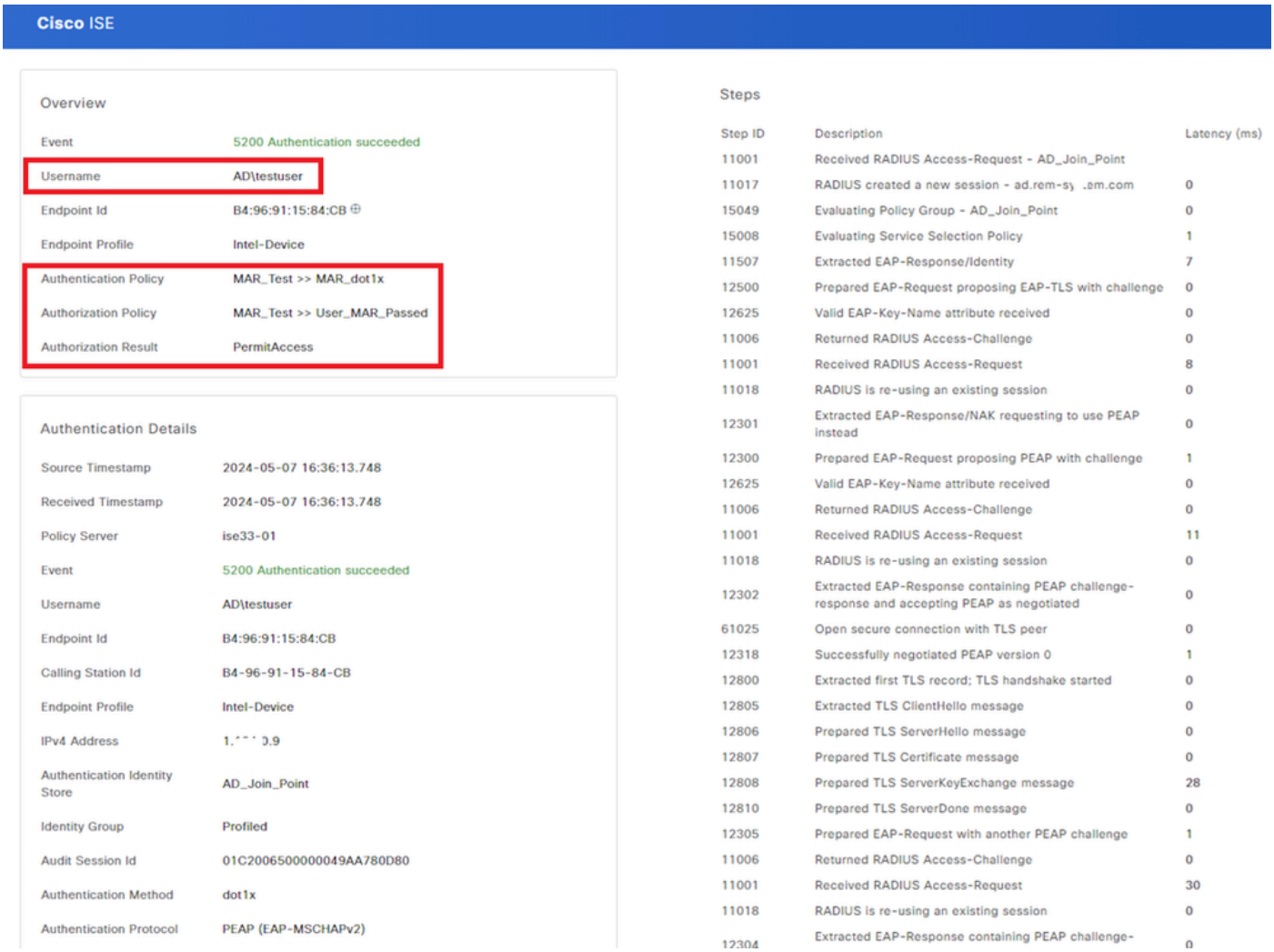
Radius live log

Bevestig het gedetailleerde bewegende logbestand voor machinale authenticatie.



Gedetailleerde beschrijving van de machineverificatie

Bevestig het gedetailleerde live logbestand van gebruikersverificatie.



Details van gebruikersverificatie

Patroon 2. Alleen gebruikersverificatie

Stap 1. NIC van Windows-pc uitschakelen en inschakelen

Om gebruikersverificatie te activeren, schakelt u de NIC van Win10 PC1 uit en schakelt u deze in.

Stap 2. Verificatiesessie bevestigen

show authentication sessions interface GigabitEthernet1/0/2 details Voer de opdracht uit om de gebruikersverificatiesessie in C1000 te bevestigen.

<#root>

Switch#

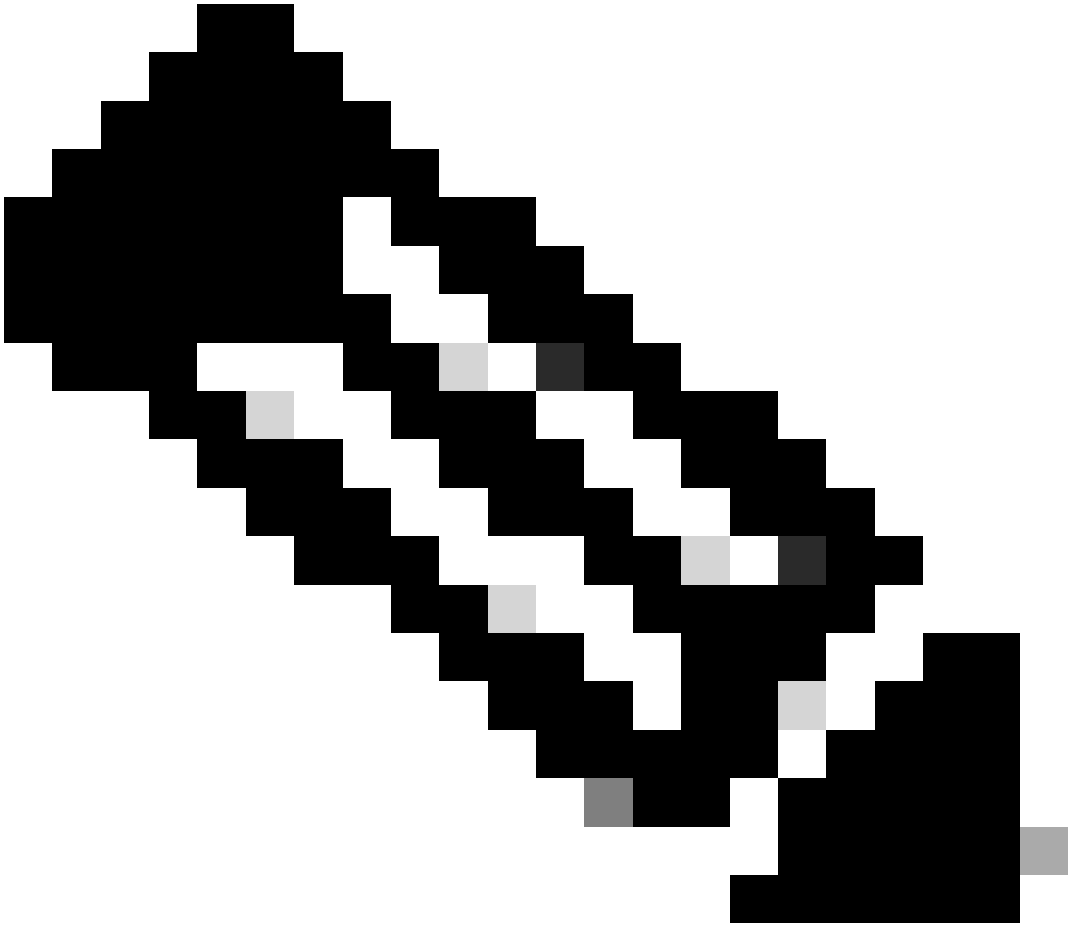
show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
```

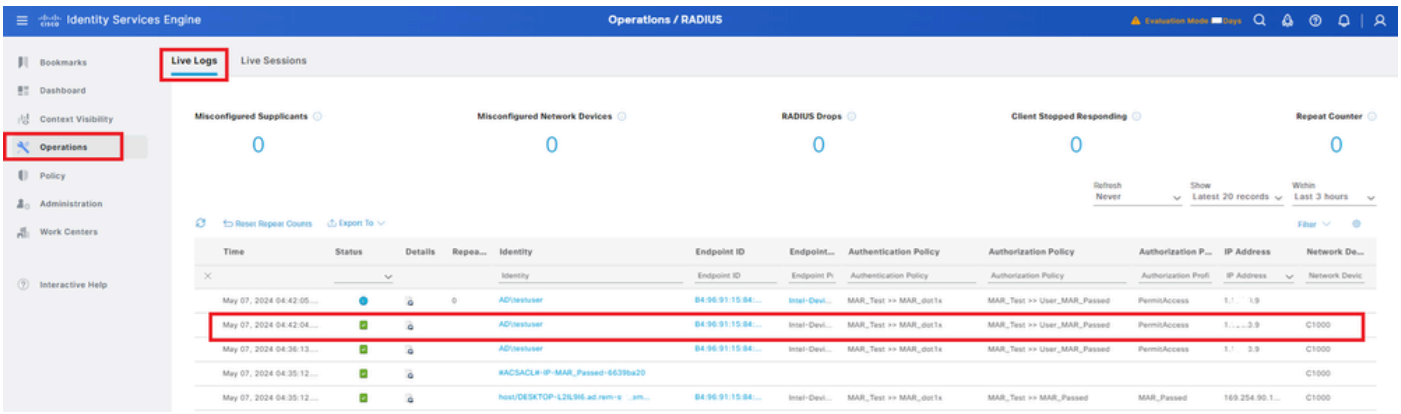
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

Stap 3. Radius live log bevestigen

Navigeer naar **Operations > RADIUS > Live logs** in ISE GUI en bevestig het live log voor gebruikersverificatie.

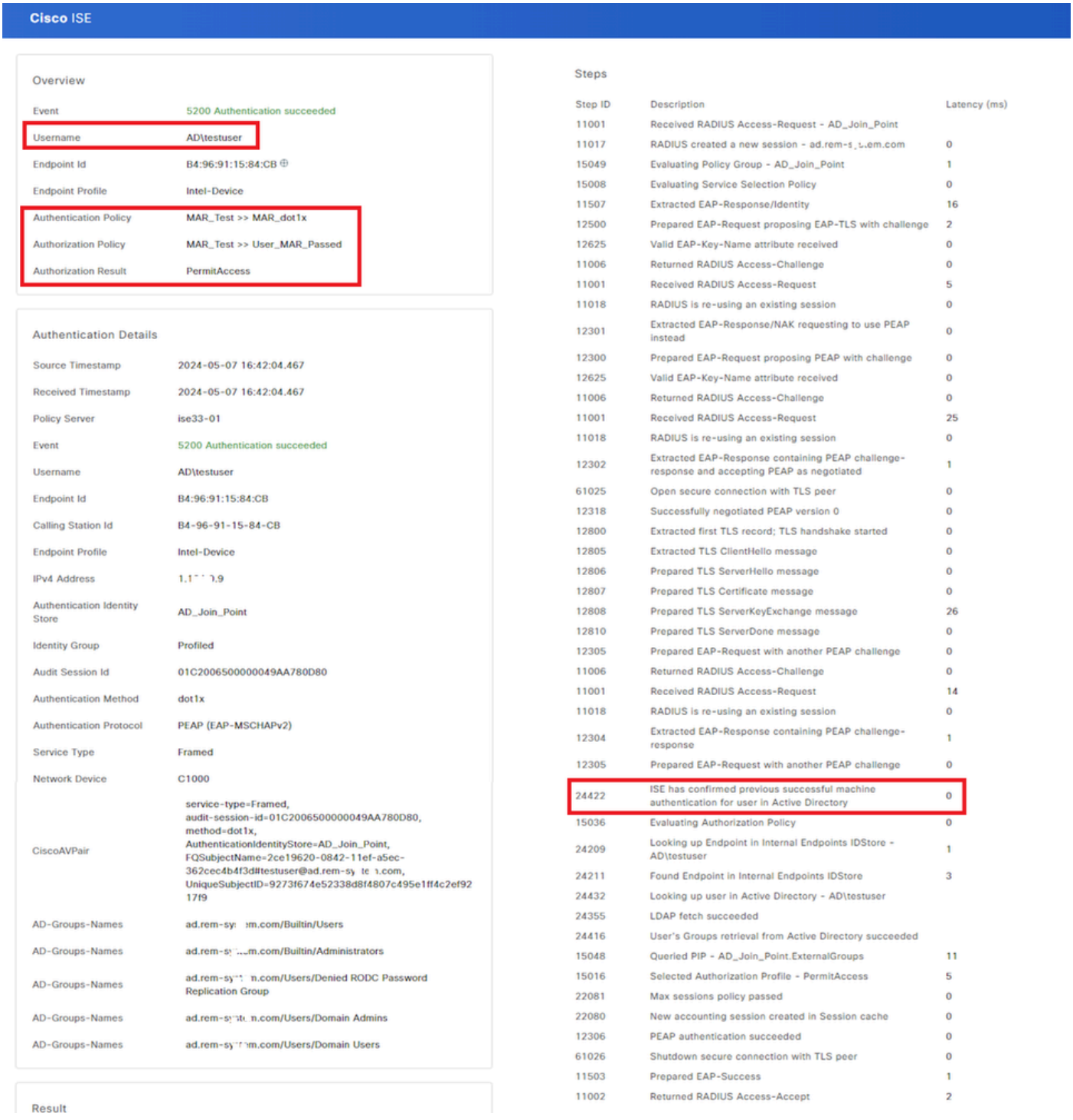


Opmerking: omdat de MAR cache is opgeslagen in ISE, is alleen gebruikersverificatie nodig.



Radius live log

Bevestig het gedetailleerde live logbestand van gebruikersverificatie.



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:42:04.467
Received Timestamp	2024-05-07 16:42:04.467
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.1[illegible]9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	C1000
CiscoAVPair	service-type=Framed, audit-session-id=01C2006500000049AA780D80, method=dot1x, AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d#testuser@ad.rem-sy[illegible].com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9
AD-Groups-Names	ad.rem-sy[illegible]m.com/Builtin/Users
AD-Groups-Names	ad.rem-s[illegible].m.com/Builtin/Administrators
AD-Groups-Names	ad.rem-sy[illegible]n.com/Users/Denied RODC Password Replication Group
AD-Groups-Names	ad.rem-sy[illegible]n.com/Users/Domain Admins
AD-Groups-Names	ad.rem-sy[illegible]m.com/Users/Domain Users

Result

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-s[illegible].em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
11507	Extracted EAP-Response/Identity	16
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	25
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	26
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
24211	Found Endpoint in Internal Endpoints IDStore	3
24432	Looking up user in Active Directory - AD\testuser	
24355	LDAP fetch succeeded	
24416	User's Groups retrieval from Active Directory succeeded	
15048	Queried PIP - AD_Join_Point.ExternalGroups	11
15016	Selected Authorization Profile - PermitAccess	5
22081	Max sessions policy passed	0
22080	New accounting session created in Session cache	0
12306	PEAP authentication succeeded	0
61026	Shutdown secure connection with TLS peer	0
11503	Prepared EAP-Success	1
11002	Returned RADIUS Access-Accept	2

Details van gebruikersverificatie

Problemen oplossen

Deze debug logbestanden (poortserver.log) helpen u het gedetailleerde gedrag van verificatie in ISE te bevestigen.

- tijdens uitvoering configureren

- runtime-vastlegging
- runtime-AAA

Dit is een voorbeeld van het debug log voor **Patroon 1. Machine-verificatie en gebruikersverificatie** in dit document.

<#root>

// machine authentication
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com, IDStore=AD_Join_Point an
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222
MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

Gerelateerde informatie

Voordelen en voordelen van toegangsbeperkingen voor machines

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.