

# Configureer statische IP-adrestoewijzing aan AnyConnect-gebruikers via RADIUS-autorisatie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Remote Access VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren  
machtigingsbeleid op ISE \(RADIUS-server\) configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft hoe u RADIUS-autorisatie met een ISE-server (Identity Services Engine) kunt configureren, zodat altijd hetzelfde IP-adres naar het Firepower Threat Defense (FTD) wordt verzonden voor een specifieke Cisco AnyConnect Secure Mobility Client-gebruiker via het RADIUS-kenmerk 8 framed-IP-adres.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FTD
- FireSIGHT Management Center (FMC)
- ISE
- Cisco AnyConnect beveiligde mobiliteit-client
- RADIUS-protocol

### Gebruikte componenten

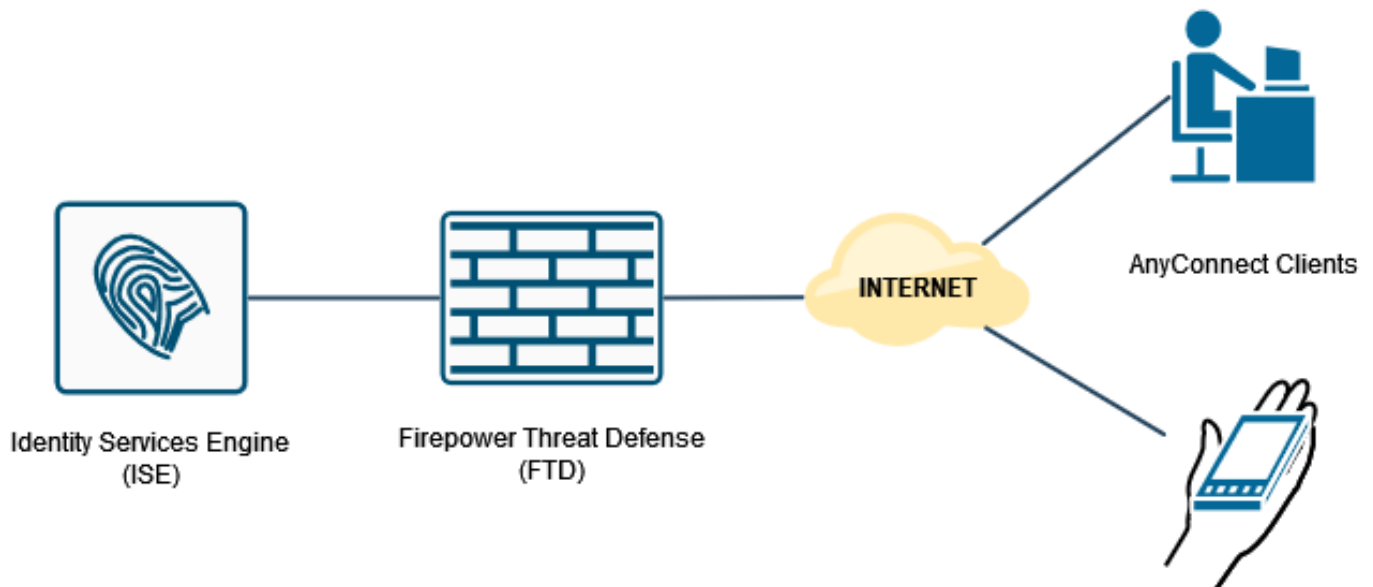
De informatie in dit document is gebaseerd op deze softwareversies:

- FMCv - 7.0.0 (bouw 94)
- FTDv - 7.0.0 (gebouwd 94)
- ISE - 2.7.0.356
- AnyConnect - 4.10.2086
- Windows 10 Pro

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Configureren

### Netwerkdigram



### Remote Access VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren

Verwijs voor een stap voor stap naar dit document en deze video:

- [AnyConnect Remote Access VPN-configuratie op FTD](#)
- [Initiële AnyConnect-configuratie voor FTD beheerde door FMC](#)

Remote Access VPN-configuratie op de FTD CLI is:

```
ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0

interface GigabitEthernet0/0
nameif Outside_Int
security-level 0
ip address 192.168.0.100 255.255.255.0

aaa-server ISE_Server protocol radius
aaa-server ISE_Server host 172.16.0.8
key *****
authentication-port 1812
accounting-port 1813

crypto ca trustpoint RAVPN_Self-Signed_Cert
enrollment self
fqdn none
subject-name CN=192.168.0.100
keypair <Default-RSA-Key>
crl configure
```

```
ssl trust-point RAVPN_Self-Signed_Cert

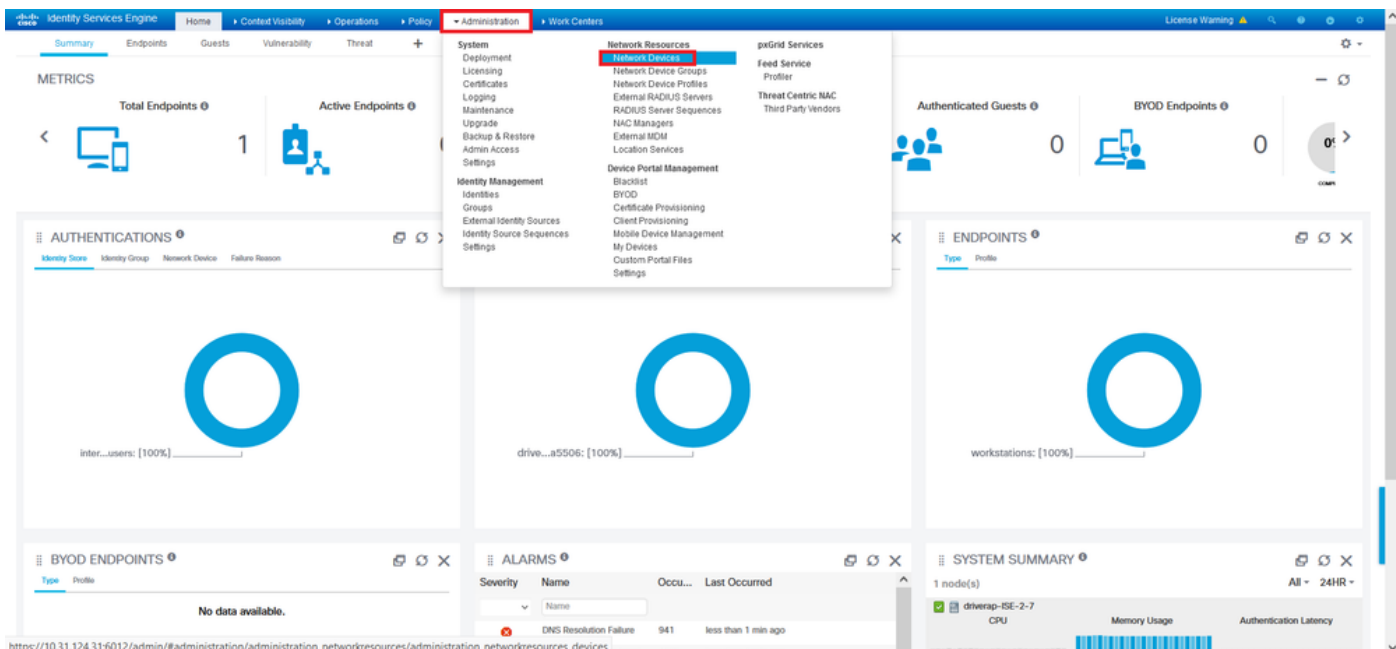
webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
no disable
error-recovery disable

group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev2 ssl-client
user-authentication-idle-timeout none
webvpn
anyconnect keep-installer none
anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none

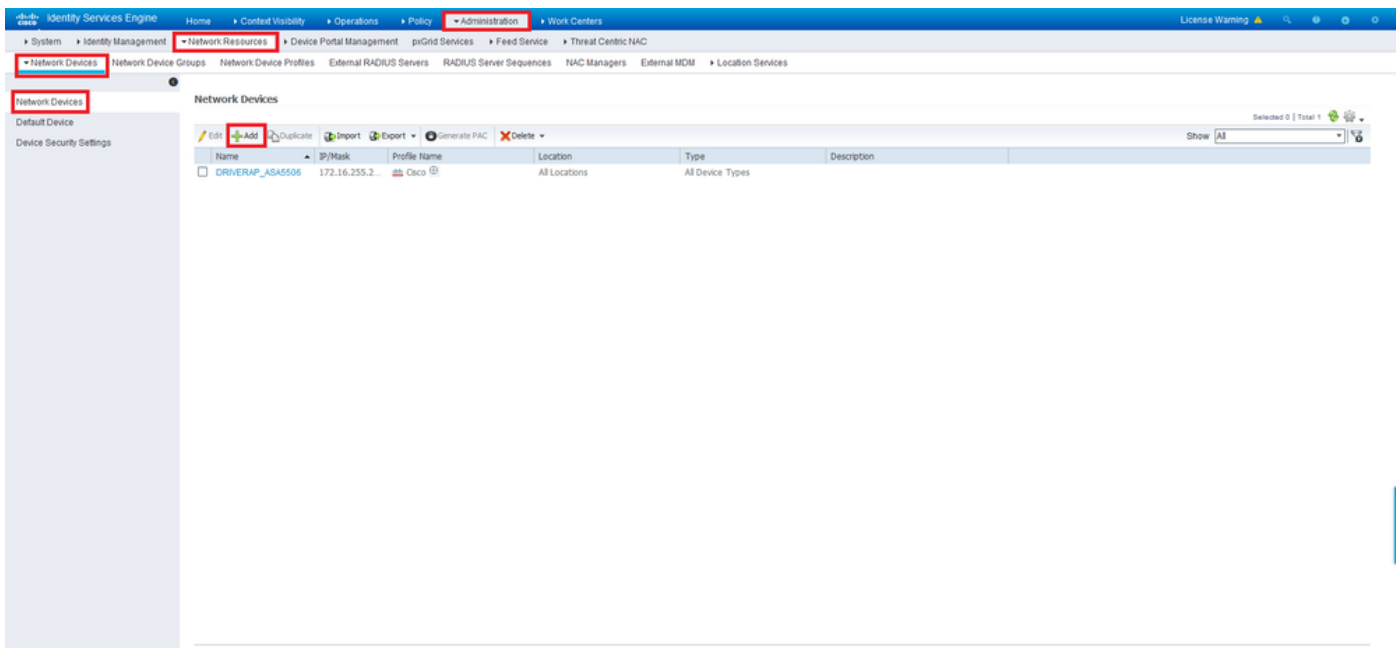
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

## **machtigingsbeleid op ISE (RADIUS-server) configureren**

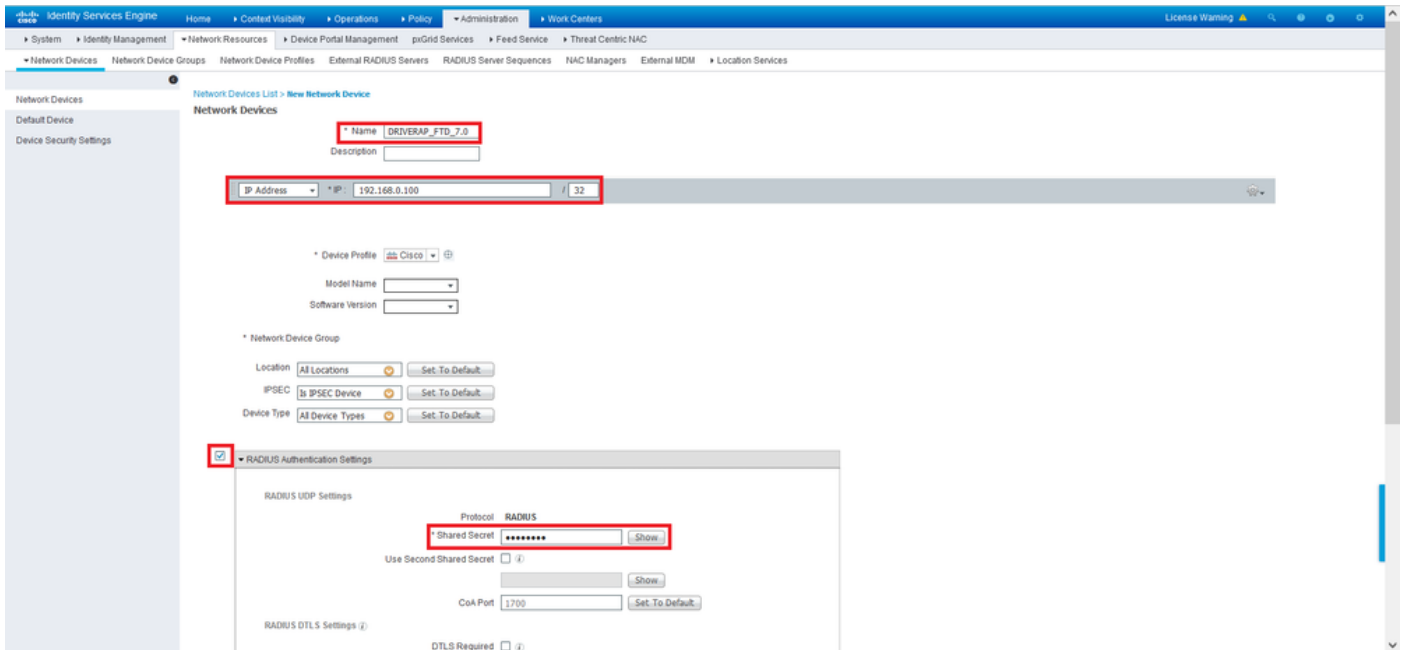
Stap 1. Meld u aan bij de ISE-server en navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**.



Stap 2. Klik in het gedeelte Network Devices op **Add** zodat ISE RADIUS-toegangs aanvragen van de FTD kan verwerken.

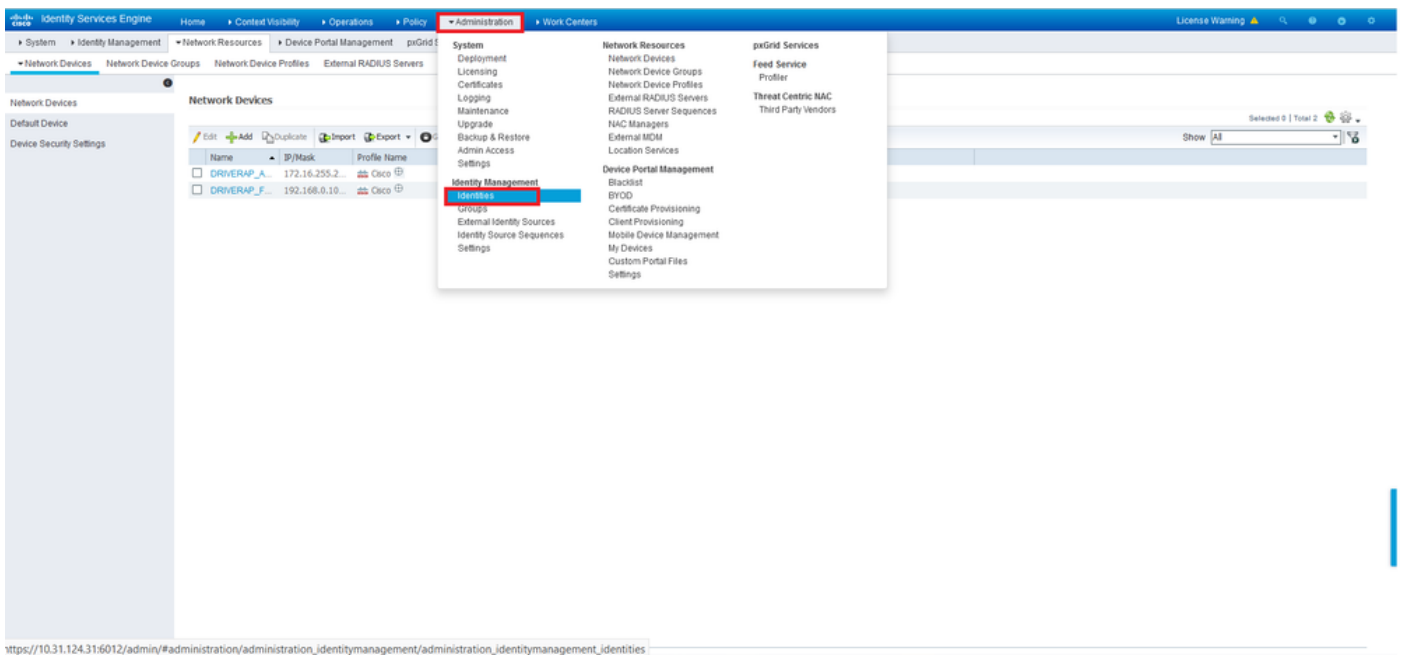


Voer de velden **Naam** en **IP-adres** van het netwerkapparaat in en controleer vervolgens **RADIUS-verificatie-instellingen**. Het **Gedeeld Gebied** moet dezelfde waarde zijn die is gebruikt toen het object RADIUS Server op FMC is gemaakt.

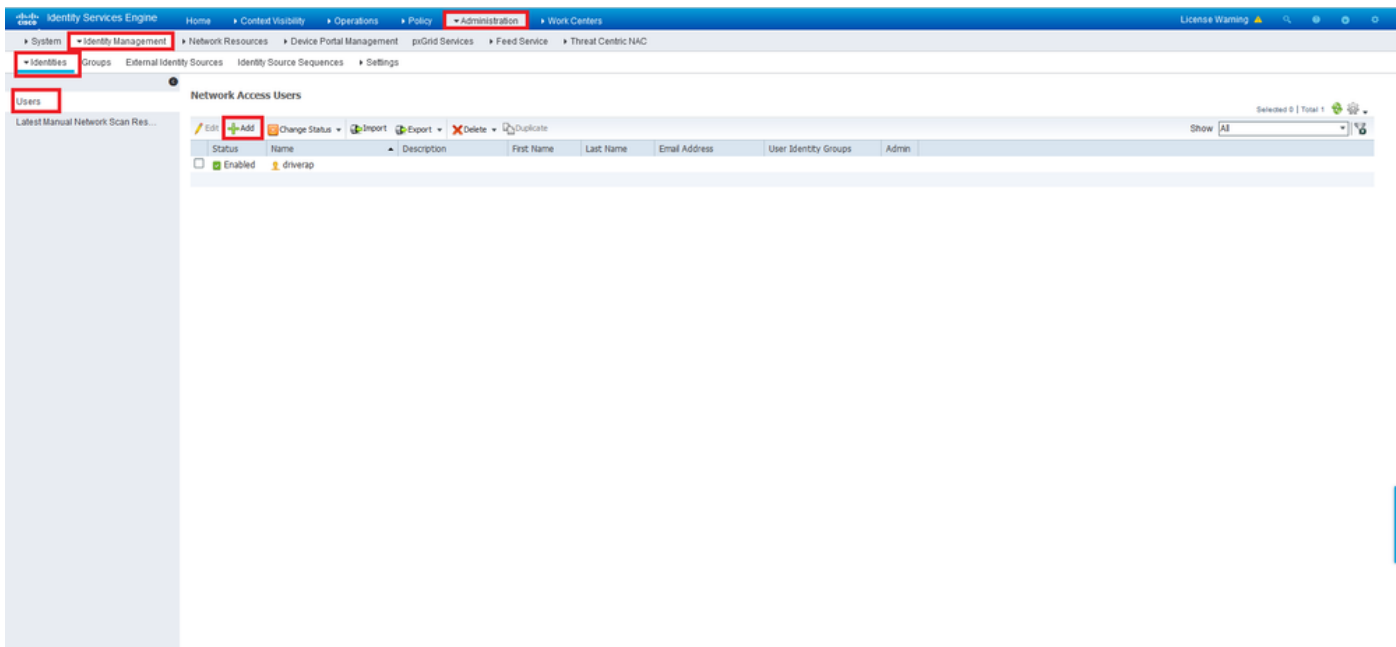


Sla deze op met de knop aan het einde van deze pagina.

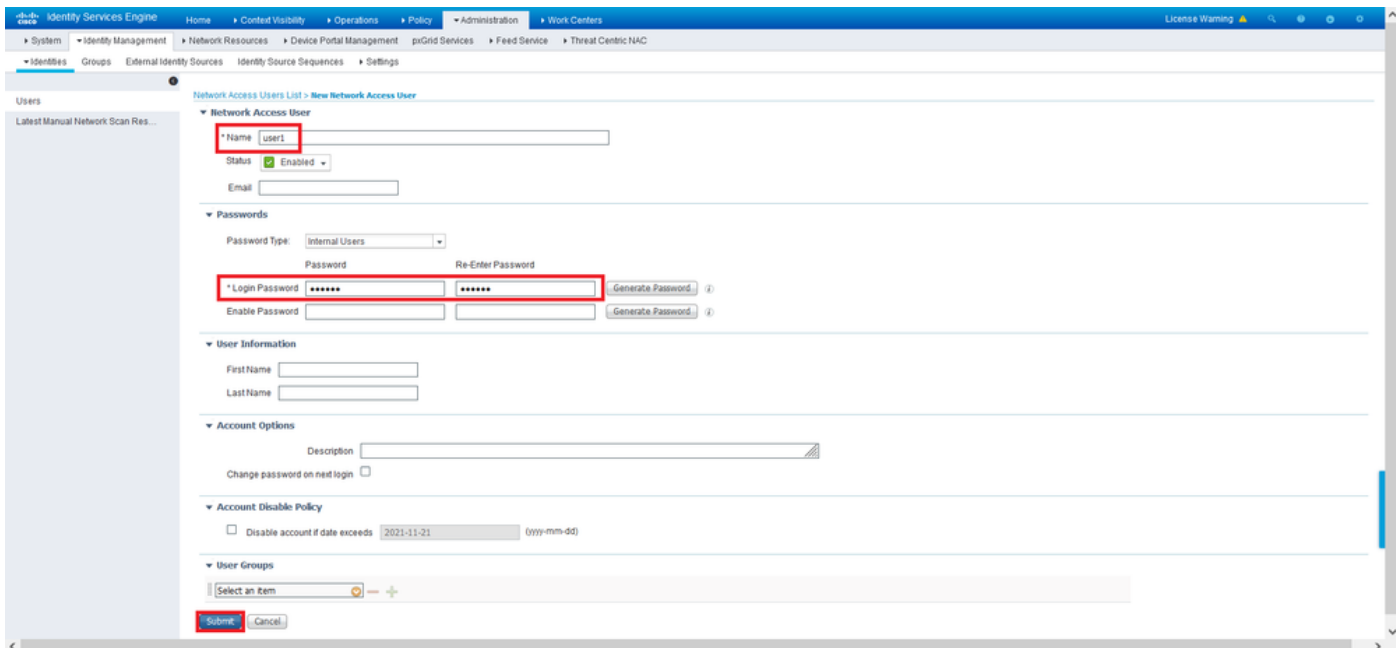
Stap 3. Navigeer naar **Administratie** > **identiteitsbeheer** > **Identificatiegegevens**.



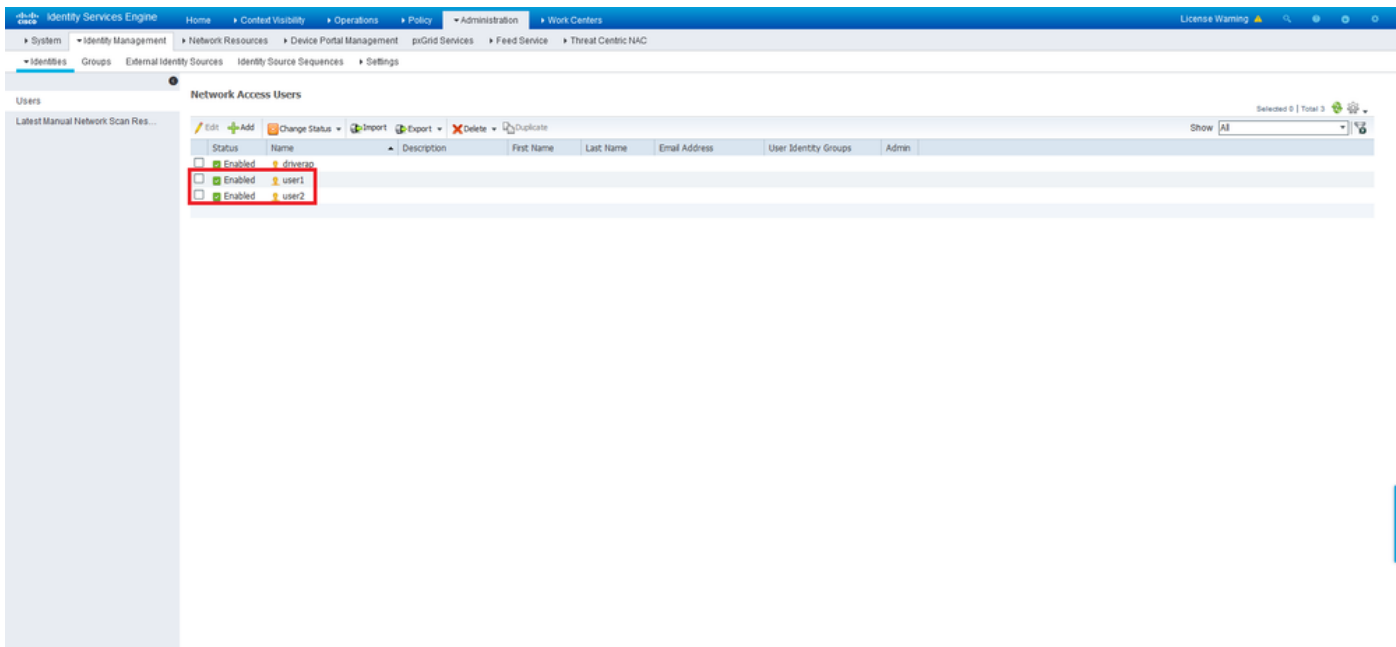
Stap 4. Klik in het gedeelte Gebruikers van netwerktoegang op **Add** om *user1* te maken in de lokale database van ISE.



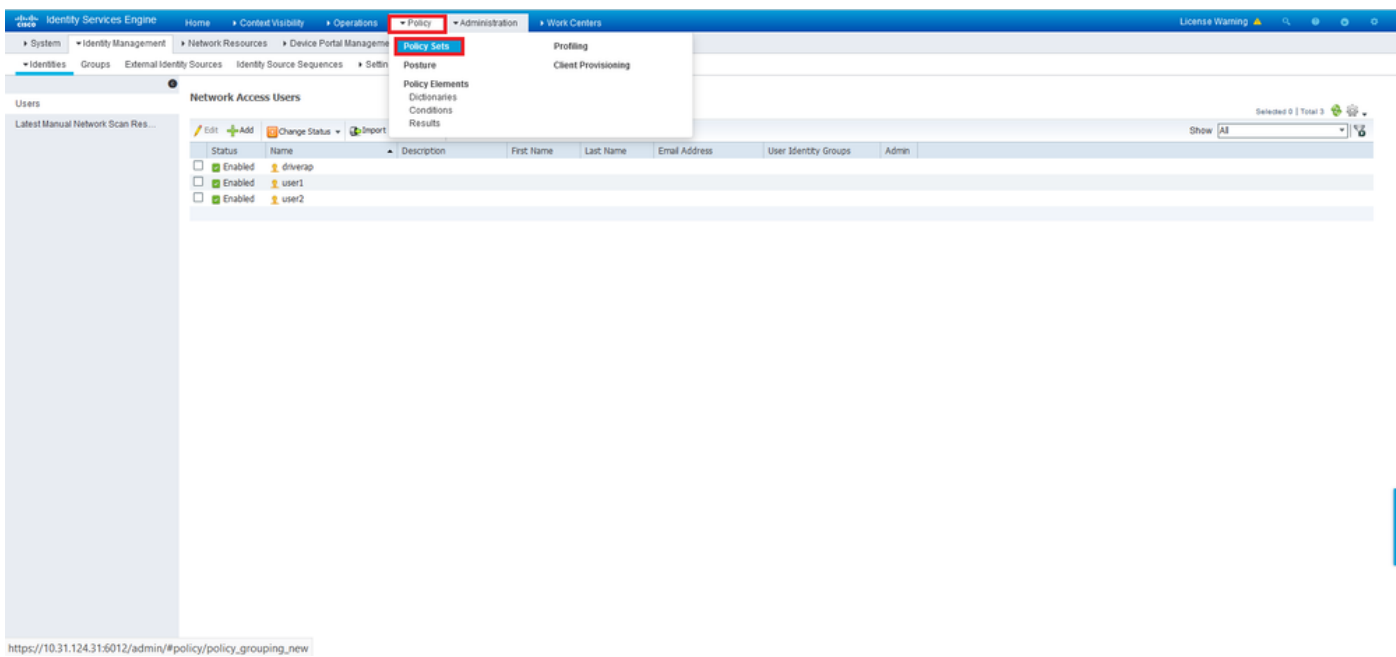
Voer een gebruikersnaam en wachtwoord in in de velden **Naam** en **Wachtwoord** voor aanmelding en klik vervolgens op **Indienen**.



Stap 5. Herhaal de vorige stappen om *gebruiker2* te maken.

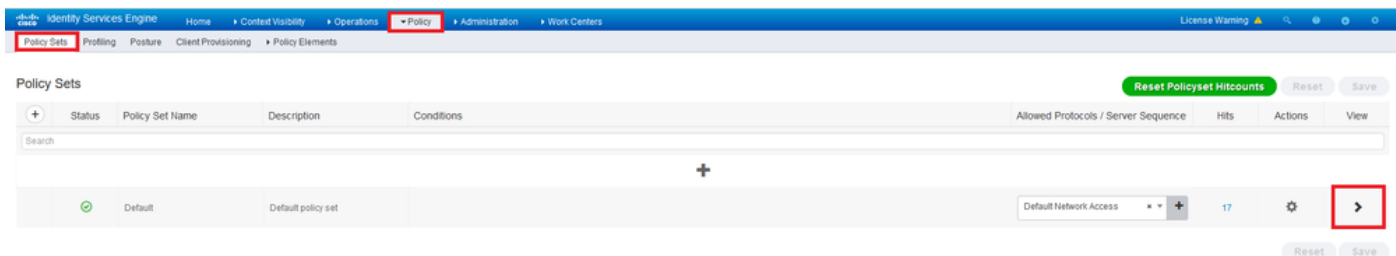


Stap 6. Navigeer naar beleid > Beleidsformaten.

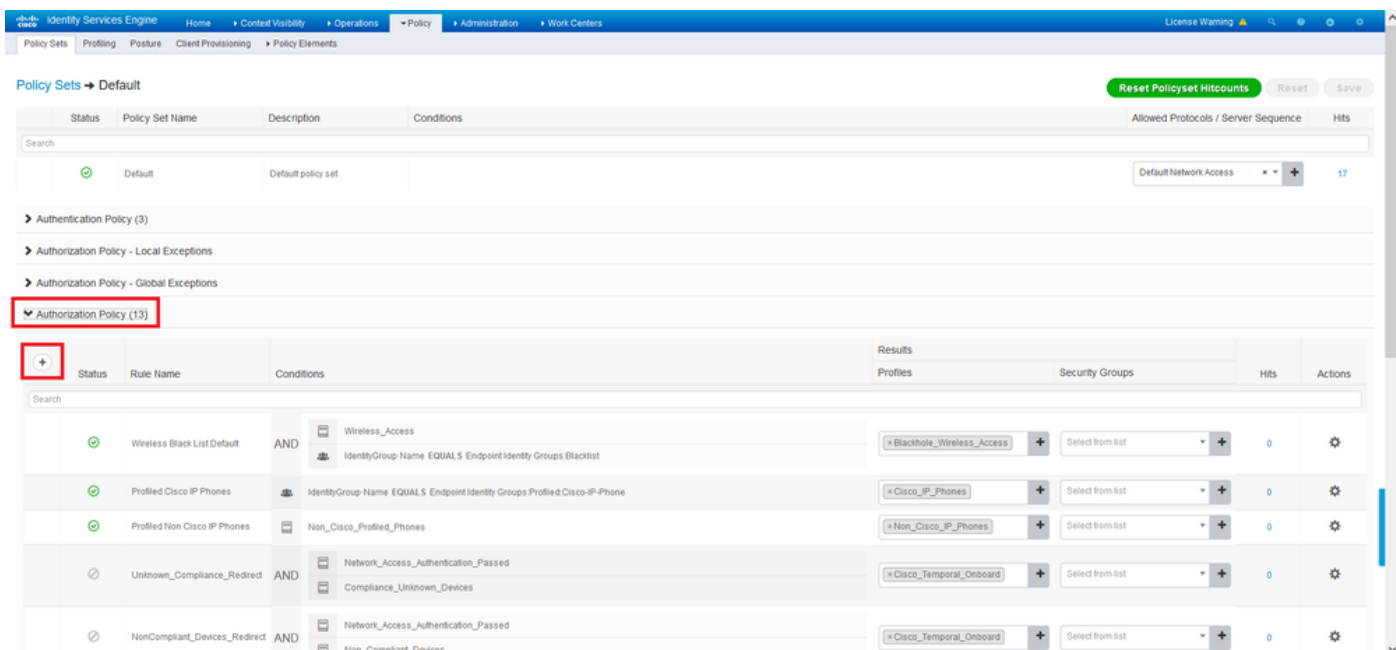


[https://10.31.124.31:6012/admin/#policy/policy\\_grouping\\_new](https://10.31.124.31:6012/admin/#policy/policy_grouping_new)

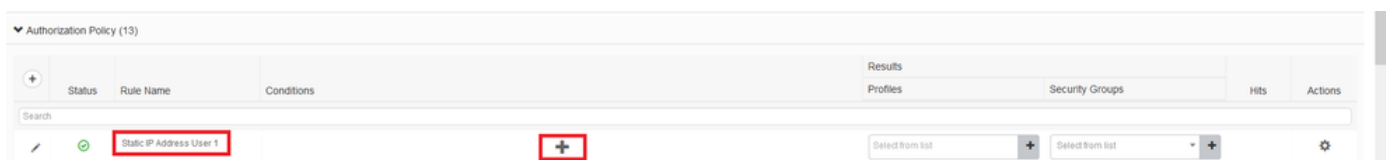
Stap 7. Klik op de pijl >rechts van het scherm.



Stap 8. Klik op de pijl > naast **Authorized Policy** om deze uit te vouwen. Klik nu op het + symbool om een nieuwe regel toe te voegen.



Typ een naam voor de regel en selecteer het + symbool in de kolom **Voorwaarden**.



Klik in het Tekstvenster van de Lijst en klik op het pictogram **Onderwerp**. Scrolt naar beneden tot u **RADIUS User-Name** attribuut vindt en kiest deze.



# Conditions Studio



## Library

- Search by Name
- BYOD\_is\_Registered
  - Catalyst\_Switch\_Local\_Web\_Authentication
  - Compliance\_Unknown\_Devices
  - Compliant\_Devices
  - EAP-MSCHAPv2
  - EAP-TLS
  - Guest\_Flow
  - MAC\_in\_SAN
  - Network\_Access\_Authentication\_Passwd
  - Non\_Cisco\_Profiled\_Phones
  - Non\_Compliant\_Devices
  - Switch\_Local\_Web\_Authentication
  - Switch\_Web\_Authentication

## Editor

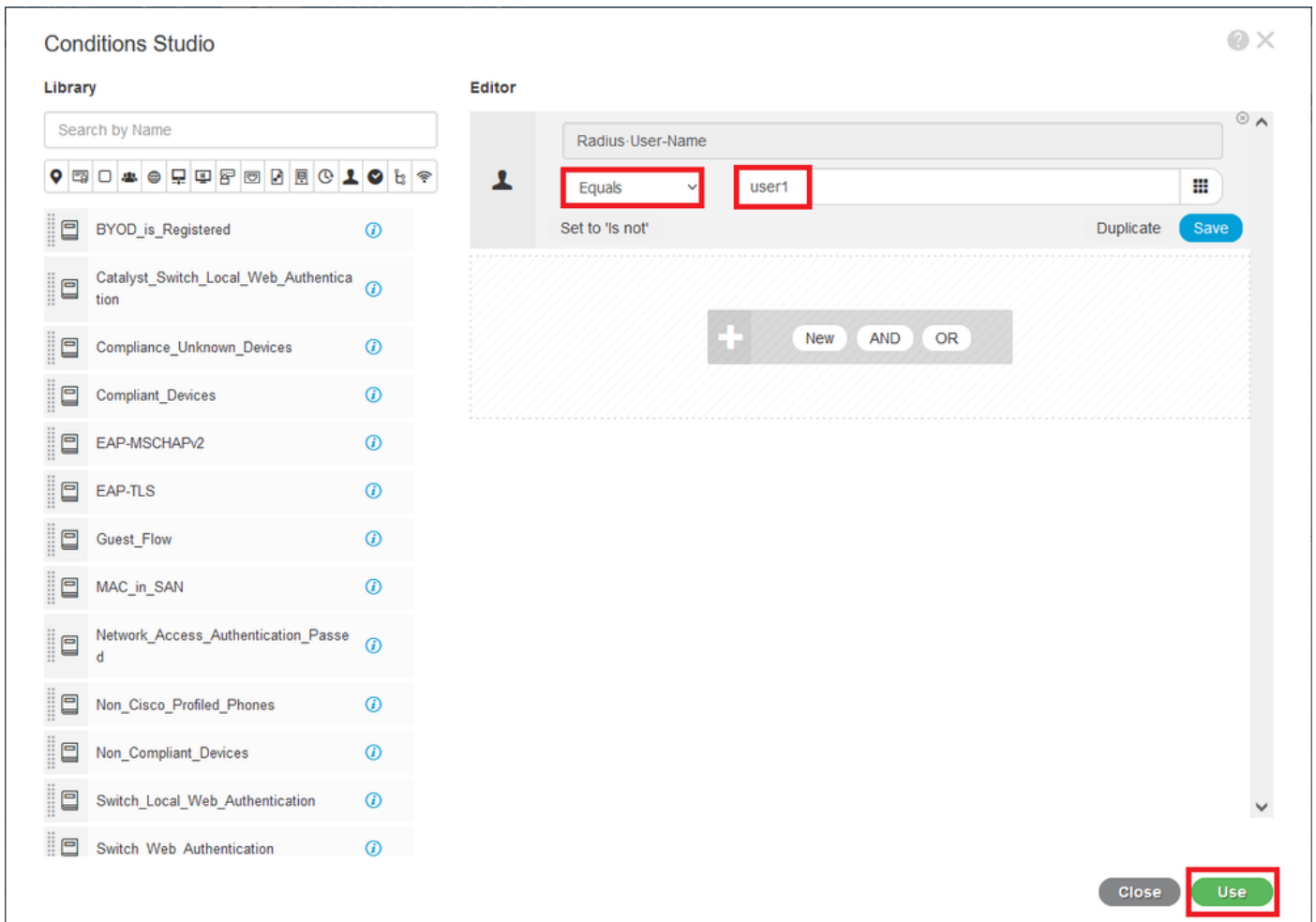
Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Microsoft	MS-HCAP-User-Name	60	<a href="#">i</a>
Motorola-Symbol	Symbol-User-Group	12	<a href="#">i</a>
Network Access	AD-User-DNS-Domain		<a href="#">i</a>
Network Access	AD-User-Join-Point		<a href="#">i</a>
Network Access	UserName		<a href="#">i</a>
PassiveID	PassiveID_Username		<a href="#">i</a>
Radius	User-Name	1	<a href="#">i</a>
Radius	User-Password	2	<a href="#">i</a>
Ruckus	Ruckus-User-Groups	1	<a href="#">i</a>

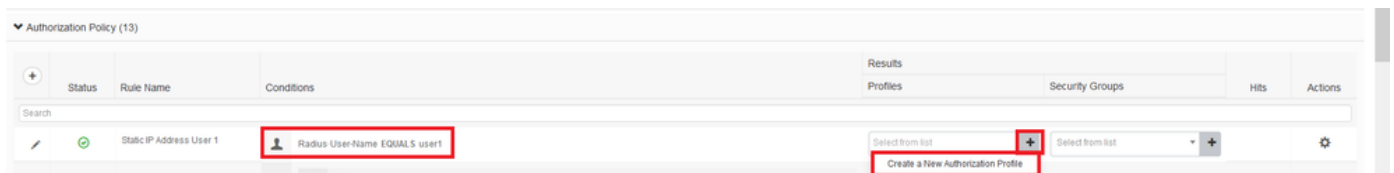
Close Use

Bewaar **gelijken** als de operator en voer *user1* in het tekstvak naast deze in. Klik op **Gebruik** om de eigenschap op te slaan.



De voorwaarde voor deze regel is nu ingesteld.

Stap 9. In de kolom **Resultaten/profielen** klikt u op het symbool + en vervolgens kiest u **een nieuw autorisatieprofiel maken**.



Geef het een **Naam** op en bewaar **ACCESS\_ACCEPT** als het **Access Type**. Scrollt naar het gedeelte **Advance Attributes**.

Add New Standard Profile

Authorization Profile

\* Name StaticIPaddressUser1

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement  (i)

Passive Identity Tracking  (i)

Common Tasks

DAACL Name

IPv6 DAACL Name

ACL (Filter-ID)

ACL IPv6 (Filter-ID)

Advanced Attributes Settings

Save Cancel

Klik op de oranje pijl en kies **Straal > framed-IP-Address**—[8].

Add New Standard Profile

Service Template

Track Movement  (i)

Passive Identity Tracking  (i)

Common Tasks

DAACL Name

IPv6 DAACL Name

ACL (Filter-ID)

ACL IPv6 (Filter-ID)

Advanced Attributes Setting

Radius:Framed-IP-Address

Attributes Details

Access Type = ACCESS\_ACCEPT

Framed-IP-Address =

Save Cancel

Typ het IP-adres dat u automatisch aan deze gebruiker wilt toewijzen en klik op **Opslaan**.

**Add New Standard Profile**

Service Template

Track Movement  ⓘ

Passive Identity Tracking  ⓘ

---

**Common Tasks**

Airespace IPv6 ACL Name

ASA VPN

AVC Profile Name

UPN Lookup

---

**Advanced Attributes Settings**

Radius:Framed-IP-Address = 10.0.50.101

---

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Framed-IP-Address = 10.0.50.101

**Save** Cancel

Stap 10. Kies nu het nieuwe vergunningsprofiel.

**Authorization Policy (13)**

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✓	Static IP Address User 1	Radius-User-Name EQUALS user1	Select from list	Select from list		⚙️
✓	Wireless Black List Default	AND Wireless_Access IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	Static_IP_Address	Select from list	0	⚙️
✓	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco IP-Phone	Static_IP_Address/User1	Select from list	0	⚙️
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Static_IP_Address	Select from list	0	⚙️

De autorisatieregel is nu helemaal ingesteld. Klik op Opslaan.

**Policy Sets → Default**

Reset Policyset Hitcounts Reset **Save**

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	17

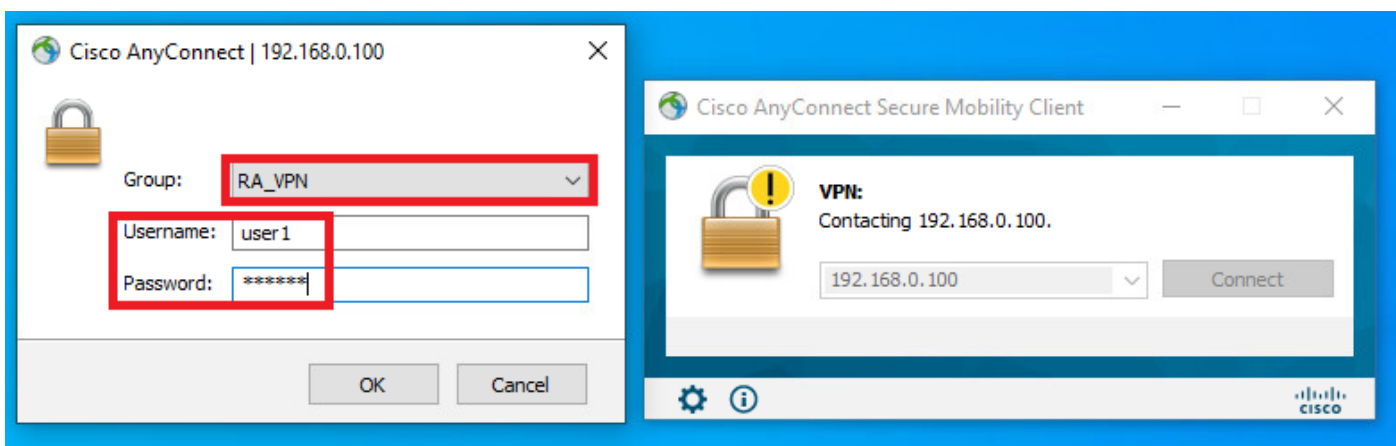
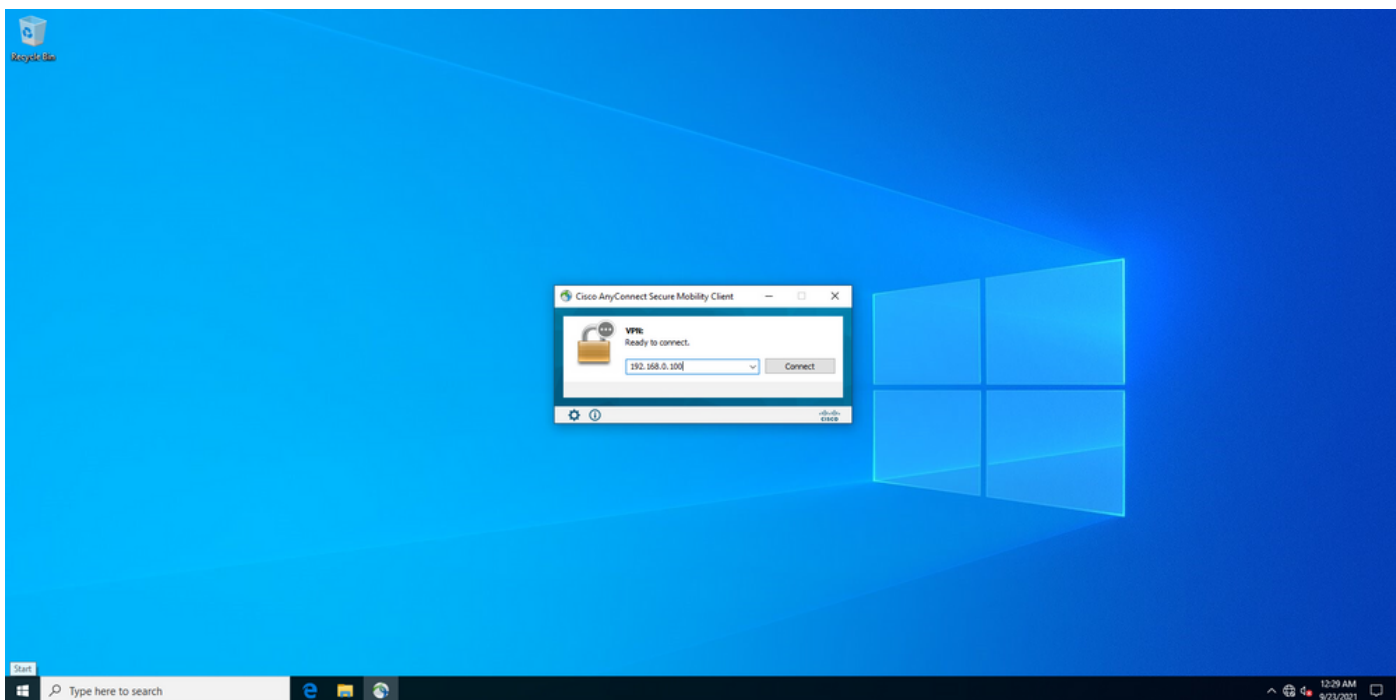
---

**Authorization Policy (13)**

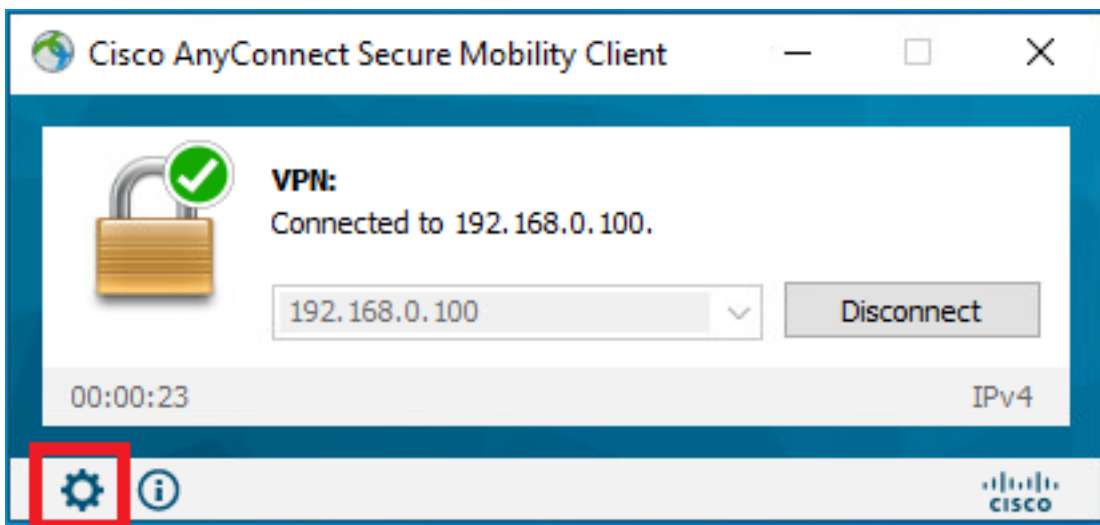
Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✓	Static IP Address User 1	Radius-User-Name EQUALS user1	StaticIPAddressUser1	Select from list		⚙️

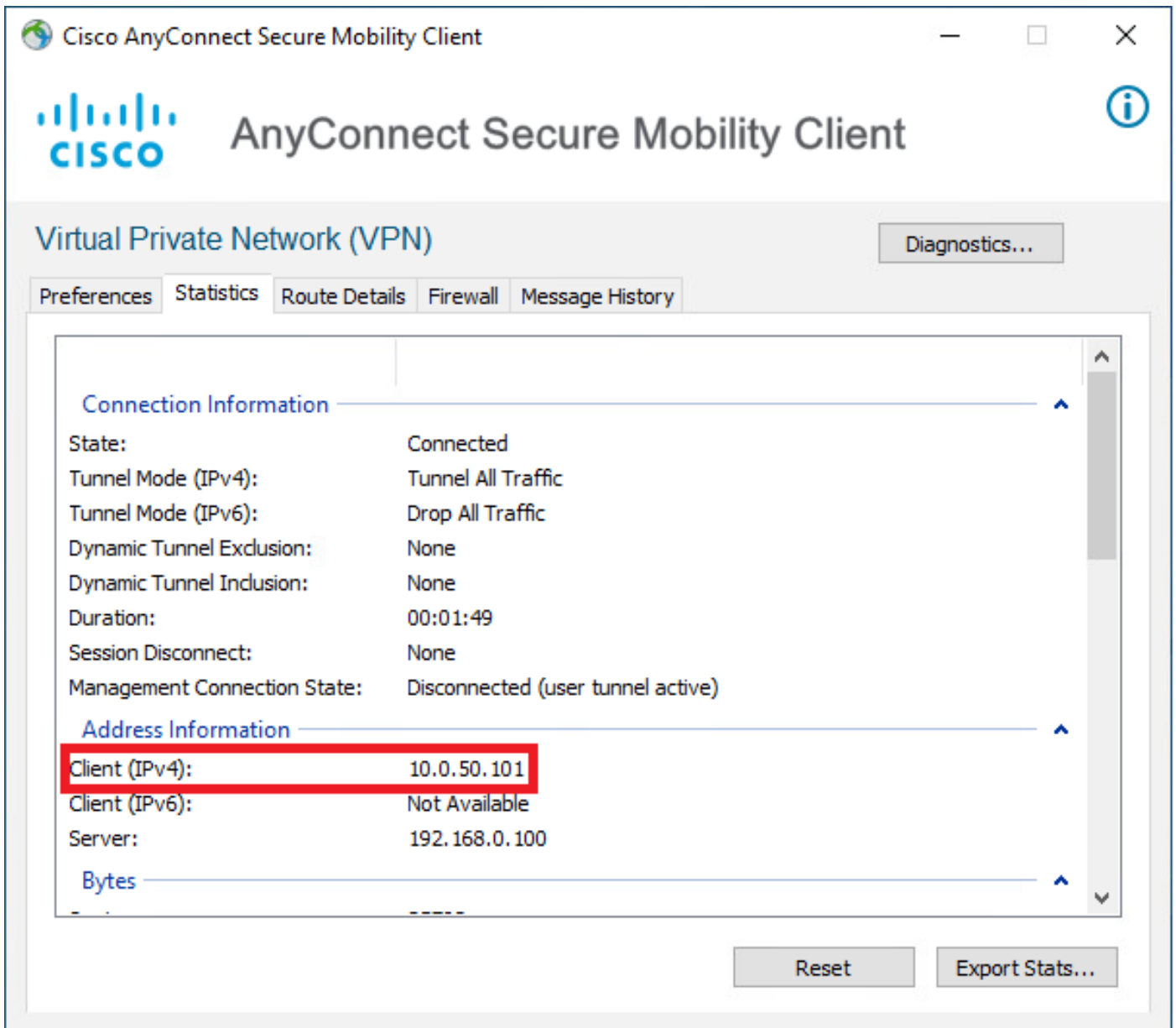
## Verifiëren

Stap 1. Navigeer naar uw clientmachine waar Cisco AnyConnect Secure Mobility-client is geïnstalleerd. Sluit aan op uw FTD head-end (hier wordt een Windows-machine gebruikt) en voer de *user1* aanmeldingsgegevens in.



Klik op het pictogram versnelling (linker benedenhoek) en navigeer naar het tabblad **Statistieken**. Bevestig in het gedeelte **Adres Information** dat het IP-adres is toegewezen, dat is ingesteld op ISE Authorization policy voor deze gebruiker.





De debug straal straalt alle opdrachtvoer op FTD toont:

```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0x9000)
radius mkreq: 0x13
alloc_rip 0x0000145d043b6460
new request 0x13 --> 3 (0x0000145d043b6460)
got user 'user1'
got password
add_req 0x0000145d043b6460 session 0x13 id 3
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.0.101

RADIUS packet decode (authentication request)
```

**RADIUS packet decode (response)**

-----  
Raw packet data (length = 136).....

```
02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 | .....AK..X...1
7d aa 38 1e 01 07 75 73 65 72 31 08 06 0a 00 32 | }.8...user1....2
65 19 3d 43 41 43 53 3a 63 30 61 38 30 30 36 34 | e.=CACS:c0a80064
30 30 30 30 61 30 30 30 36 31 34 62 63 30 32 64 | 0000a000614bc02d
3a 64 72 69 76 65 72 61 70 2d 49 53 45 2d 32 2d | :driverap-ISE-2-
37 2f 34 31 37 34 39 34 39 37 38 2f 32 31 1a 2a | 7/417494978/21.*
00 00 00 09 01 24 70 72 6f 66 69 6c 65 2d 6e 61 | .....$profile-na
6d 65 3d 57 69 6e 64 6f 77 73 31 30 2d 57 6f 72 | me=Windows10-Wor
6b 73 74 61 74 69 6f 6e | kstation
```

Parsed packet data.....

Radius: Code = 2 (0x02)

Radius: Identifier = 3 (0x03)

Radius: Length = 136 (0x0088)

Radius: Vector: 0CAF1C414BC4A658DEF392317DAA381E

**Radius: Type = 1 (0x01) User-Name**

Radius: Length = 7 (0x07)

**Radius: Value (String) =**

**75 73 65 72 31 | user1**

**Radius: Type = 8 (0x08) Framed-IP-Address**

Radius: Length = 6 (0x06)

**Radius: Value (IP Address) = 10.0.50.101 (0x0A003265)**

Radius: Type = 25 (0x19) Class

Radius: Length = 61 (0x3D)

Radius: Value (String) =

43 41 43 53 3a 63 30 61 38 30 30 36 34 30 30 30 | CACS:c0a80064000

30 61 30 30 30 36 31 34 62 63 30 32 64 3a 64 72 | 0a000614bc02d:dr

69 76 65 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 | iverap-ISE-2-7/4

31 37 34 39 34 39 37 38 2f 32 31 | 17494978/21

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 42 (0x2A)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 36 (0x24)

Radius: Value (String) =

70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win

64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati

6f 6e | on

**rad\_procpkt: ACCEPT**

Got AV-Pair with value profile-name=Windows10-Workstation

RADIUS\_ACCESS\_ACCEPT: normal termination

RADIUS\_DELETE

remove\_req 0x0000145d043b6460 session 0x13 id 3

free\_rip 0x0000145d043b6460

radius: send queue empty

De FTD-logboeken tonen:

firepower#

<omitted output>

Sep 22 2021 23:52:40: %FTD-6-725002: Device completed SSL handshake with client

Outside\_Int:192.168.0.101/60405 to 192.168.0.100/443 for TLSv1.2 session

Sep 22 2021 23:52:48: %FTD-7-609001: Built local-host Outside\_Int:172.16.0.8

Sep 22 2021 23:52:48: %FTD-6-113004: AAA user authentication Successful : server = 172.16.0.8 :

user = user1

Sep 22 2021 23:52:48: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user

= user1

Sep 22 2021 23:52:48: %FTD-6-113008: **AAA transaction status ACCEPT : user = user1**

Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute

aaa.radius["1"]["1"] = user1

Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute

aaa.radius["8"]["1"] = 167785061

Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute

```
aaa.radius["25"]["1"] = CACS:c0a800640000c000614bcd0:driverap-ISE-2-7/417494978/23
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.grouppolicy = DfltGrpPolicy
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.ipaddress = 10.0.50.101
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.username = user1
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.username1 = user1
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.username2 =
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.tunnelgroup = RA_VPN
Sep 22 2021 23:52:48: %FTD-6-734001: DAP: User user1, Addr 192.168.0.101, Connection AnyConnect:
The following DAP records were selected for this connection: DfltAccessPolicy
Sep 22 2021 23:52:48: %FTD-6-113039: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101>
AnyConnect parent session started.
<omitted output>
Sep 22 2021 23:53:17: %FTD-6-725002: Device completed SSL handshake with client
Outside_Int:192.168.0.101/60412 to 192.168.0.100/443 for TLSv1.2 session
Sep 22 2021 23:53:17: %FTD-7-737035: IPAA: Session=0x0000c000, 'IPv4 address request' message
queued
Sep 22 2021 23:53:17: %FTD-7-737035: IPAA: Session=0x0000c000, 'IPv6 address request' message
queued
Sep 22 2021 23:53:17: %FTD-7-737001: IPAA: Session=0x0000c000, Received message 'IPv4 address
request'
Sep 22 2021 23:53:17: %FTD-6-737010: IPAA: Session=0x0000c000, AAA assigned address 10.0.50.101,
succeeded
Sep 22 2021 23:53:17: %FTD-7-737001: IPAA: Session=0x0000c000, Received message 'IPv6 address
request'
Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: no IPv6 address
available from local pools
Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: callback failed
during IPv6 request
Sep 22 2021 23:53:17: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User
<user1> IP <192.168.0.101> No IPv6 address available for SVC connection
Sep 22 2021 23:53:17: %FTD-7-609001: Built local-host Outside_Int:10.0.50.101
Sep 22 2021 23:53:17: %FTD-5-722033: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> First
TCP SVC connection established for SVC session.
Sep 22 2021 23:53:17: %FTD-6-722022: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> TCP
SVC connection established without compression
Sep 22 2021 23:53:17: %FTD-7-746012: user-identity: Add IP-User mapping 10.0.50.101 -
LOCAL\user1 Succeeded - VPN user
Sep 22 2021 23:53:17: %FTD-6-722055: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101>
Client Type: Cisco AnyConnect VPN Agent for Windows 4.10.02086
Sep 22 2021 23:53:17: %FTD-4-722051: Group
```

De RADIUS Live-logbestanden op ISE tonen:



**Identity Services Engine**

### Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:00:56:96:45:0F (0)
Endpoint Profile	Windows10-Workstation
Authorization Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPAddressUser1

### Authentication Details

Source Timestamp	2021-09-22 23:53:19.72
Received Timestamp	2021-09-22 23:53:19.72
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00:00:56:96:45:0F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	d8a800540000d00014bc1d0
Authentication Method	PAP_ASCM
Authentication Protocol	PAP_ASCM
Network Device	DRIVERAP_FT0_7-0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

### Steps

```

11001 Returned RADIUS AccessRequest
11017 RADIUS created a new session
15049 Evaluating Policy Group
15058 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15040 Queried PIP - Normalized Radius RadiusType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
24716 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15030 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user1
24211 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - Radius User Name
15016 Selected Authorization Profile - StaticIPAddressUser1
22081 Max sessions policy passed
22080 New accounting session created in Session cache
11002 Returned RADIUS AccessAccept
  
```

**Identity Services Engine**

NAS Port Type	Virtual
Authorization Profile	StaticIPAddressUser1
Response Time	51 milliseconds

### Other Attributes

ConfigVersionId	146
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPR3000ASAPPOX-Tunnel-Group-Name	RA_VPN
OriginalUsername	user1
NetworkDeviceProfileId	b0699005-3150-4210-a80a-6753445d850c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPPOX-Client-Type	2
Acx-SessionID	driverap-ISE-2-71417494978-23
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_Ad_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLS-Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	LocationAll Locations
Device Type	Device TypeAll Device Types

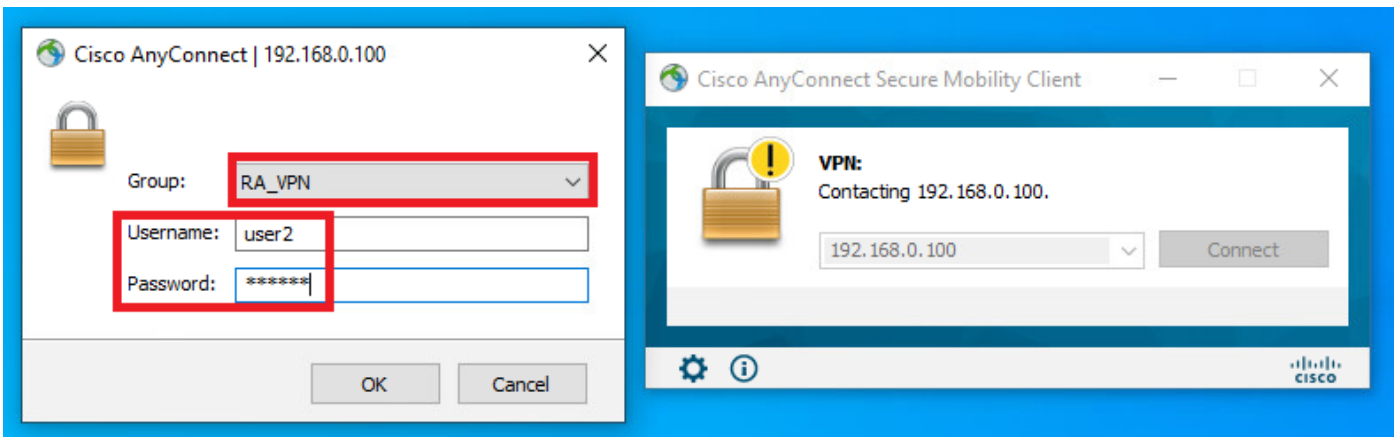
IPSEC	IPSECOnly IPSEC Device#0
EnabledFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM SessionID	d8a800540000d00014bc1d0
Called-Station-ID	192.168.0.100
CiscoAVPair	mdm-dmdevice-platform=win, mdm-dmdevice-manufacturer=56-96-45-0f, mdm-dmdevice-platform-version=10.0.13522, mdm-dmdevice-publicname=00:00:56:96:45:0f, mdm-dmdevice-agent=AnyConnect Windows 4 10.02086, mdm-dmdevice-type=VMware, Inc VMware Virtual Platform, mdm-dmdevice-uid=glbactm158788E0CF62F3F2CDE241409F4BA2AE2C583, mdm-dmdevice-uid=3C28427071F90782F810F124621184A08598C717E370386CC03F8443C880244, audit-session-id=d8a800540000d00014bc1d0, ip-source-ip=192.168.0.101, oca-push=true

### Result

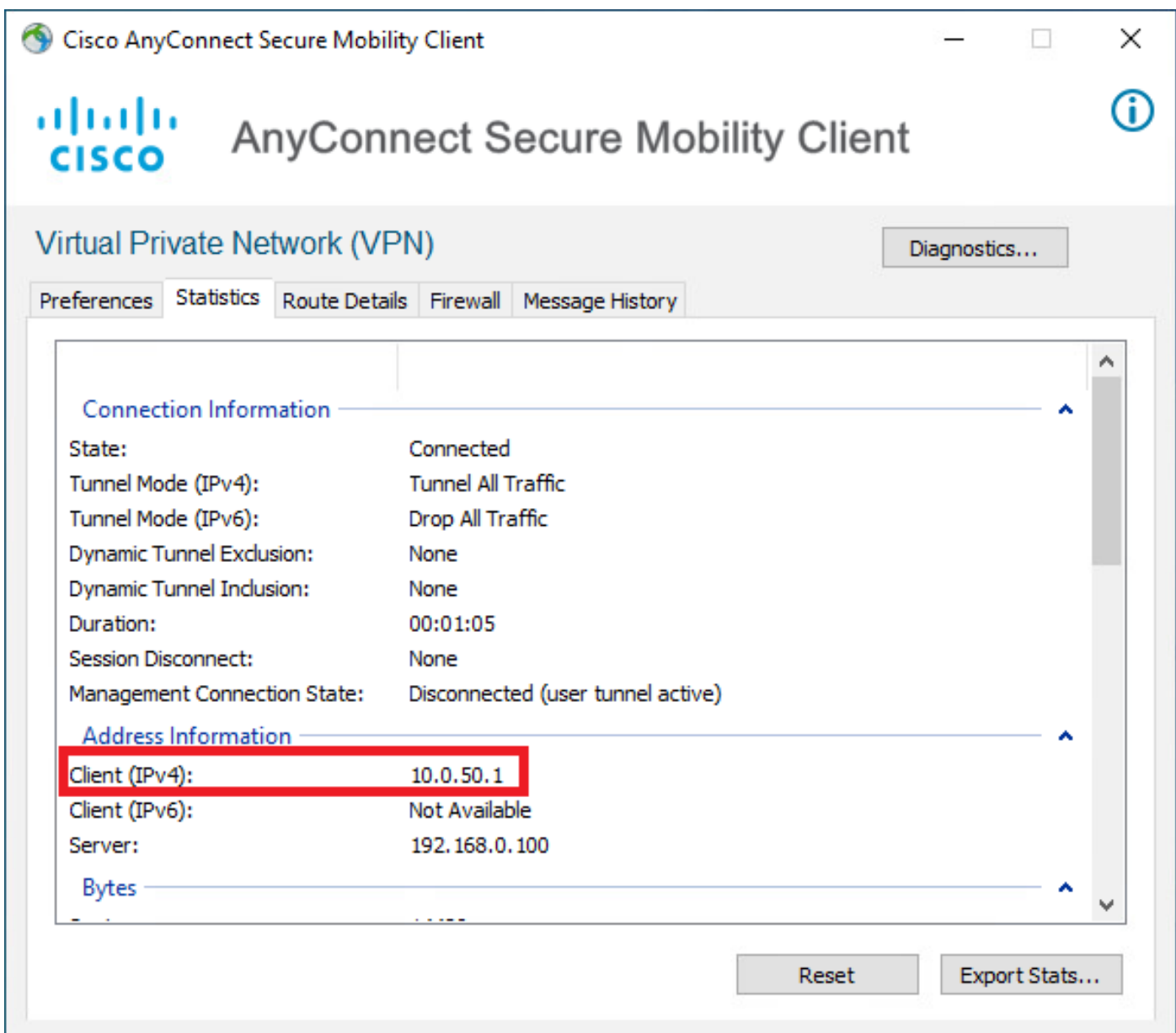
Framed IP Address	10.0.0.101
Class	CACS-d8a800540000d00014bc1d0-driverap-ISE-2-71417494978-23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

Stap 2. Sluit aan op uw FTD head-end (hier wordt een Windows-machine gebruikt) en voer de user2 aanmeldingsgegevens in.



Het gedeelte **Adres Informatie** laat zien dat het IP-adres dat is toegewezen inderdaad het eerste IP-adres is dat beschikbaar is in de IPv4-pool die via FMC is geconfigureerd.



De debug straal straalt alle opdrachtuitvoer op FTD toont:

```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
```

```
np_svc_destroy_session(0xA000)
radius mkreq: 0x15
alloc_rip 0x0000145d043b6460
new request 0x15 --> 4 (0x0000145d043b6460)
got user 'user2'
got password
add_req 0x0000145d043b6460 session 0x15 id 4
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.0.101

RADIUS packet decode (authentication request)
```

**RADIUS packet decode (response)**

```
-----
Raw packet data (length = 130).....
02 04 00 82 a6 67 35 9e 10 36 93 18 1f 1b 85 37 | .....g5..6.....7
b6 c3 18 4f 01 07 75 73 65 72 32 19 3d 43 41 43 | ...O..user2.=CAC
53 3a 63 30 61 38 30 30 36 34 30 30 30 30 62 30 | S:c0a800640000b0
30 30 36 31 34 62 63 30 61 33 3a 64 72 69 76 65 | 00614bc0a3:drive
72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 31 37 34 | rap-ISE-2-7/4174
39 34 39 37 38 2f 32 32 1a 2a 00 00 09 01 24 | 94978/22.*.....$
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win
64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati
6f 6e | on
```

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 4 (0x04)
Radius: Length = 130 (0x0082)
Radius: Vector: A667359E103693181F1B8537B6C3184F
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 32 | user2
Radius: Type = 25 (0x19) Class
Radius: Length = 61 (0x3D)
Radius: Value (String) =
43 41 43 53 3a 63 30 61 38 30 30 36 34 30 30 30 | CACS:c0a80064000
30 62 30 30 30 36 31 34 62 63 30 61 33 3a 64 72 | 0b000614bc0a3:dr
69 76 65 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 | iverap-ISE-2-7/4
31 37 34 39 34 39 37 38 2f 32 32 | 17494978/22
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 42 (0x2A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 36 (0x24)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win
64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati
6f 6e | on
```

```
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Windows10-Workstation
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x0000145d043b6460 session 0x15 id 4
free_rip 0x0000145d043b6460
radius: send queue empty
```

De FTD-logboeken tonen:

<omitted output>

Sep 22 2021 23:59:26: %FTD-6-725002: Device completed SSL handshake with client  
Outside\_Int:192.168.0.101/60459 to 192.168.0.100/443 for TLSv1.2 session  
Sep 22 2021 23:59:35: %FTD-7-609001: Built local-host Outside\_Int:172.16.0.8  
Sep 22 2021 23:59:35: %FTD-6-113004: AAA user authentication Successful : server = 172.16.0.8 :  
user = user2  
Sep 22 2021 23:59:35: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user  
= user2  
Sep 22 2021 23:59:35: %FTD-6-113008: AAA transaction status ACCEPT : user = user2  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute  
aaa.radius["1"]["1"] = user2  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute  
aaa.radius["25"]["1"] = CACS:c0a800640000d000614bc367:driverap-ISE-2-7/417494978/24  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute  
aaa.cisco.grouppolicy = DfltGrpPolicy  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: **Session Attribute  
aaa.cisco.username = user2**  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute  
aaa.cisco.username1 = user2  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute  
aaa.cisco.username2 =  
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute  
aaa.cisco.tunnelgroup = RA\_VPN  
Sep 22 2021 23:59:35: %FTD-6-734001: DAP: User user2, Addr 192.168.0.101, Connection AnyConnect:  
The following DAP records were selected for this connection: DfltAccessPolicy  
Sep 22 2021 23:59:35: %FTD-6-113039: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101>  
AnyConnect parent session started.

<omitted output>

Sep 22 2021 23:59:52: %FTD-6-725002: Device completed SSL handshake with client  
Outside\_Int:192.168.0.101/60470 to 192.168.0.100/443 for TLSv1.2 session  
Sep 22 2021 23:59:52: %FTD-7-737035: IPAA: Session=0x0000d000, 'IPv4 address request' message  
queued  
Sep 22 2021 23:59:52: %FTD-7-737035: IPAA: Session=0x0000d000, 'IPv6 address request' message  
queued  
Sep 22 2021 23:59:52: %FTD-7-737001: IPAA: Session=0x0000d000, Received message 'IPv4 address  
request'  
Sep 22 2021 23:59:52: %FTD-5-737003: IPAA: Session=0x0000d000, DHCP configured, no viable  
servers found for tunnel-group 'RA\_VPN'  
Sep 22 2021 23:59:52: %FTD-7-737400: **POOLIP: Pool=AC\_Pool, Allocated 10.0.50.1 from pool**  
Sep 22 2021 23:59:52: %FTD-7-737200: **VPNFIIP: Pool=AC\_Pool, Allocated 10.0.50.1 from pool**  
Sep 22 2021 23:59:52: %FTD-6-737026: **IPAA: Session=0x0000d000, Client assigned 10.0.50.1 from  
local pool AC\_Pool**  
Sep 22 2021 23:59:52: %FTD-6-737006: **IPAA: Session=0x0000d000, Local pool request succeeded for  
tunnel-group 'RA\_VPN'**  
Sep 22 2021 23:59:52: %FTD-7-737001: IPAA: Session=0x0000d000, Received message 'IPv6 address  
request'  
Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: no IPv6 address  
available from local pools  
Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: callback failed  
during IPv6 request  
Sep 22 2021 23:59:52: %FTD-4-722041: TunnelGroup <RA\_VPN> GroupPolicy <DfltGrpPolicy> User  
<user2> IP <192.168.0.101> No IPv6 address available for SVC connection  
Sep 22 2021 23:59:52: %FTD-7-609001: Built local-host Outside\_Int:10.0.50.1  
Sep 22 2021 23:59:52: %FTD-5-722033: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> First  
TCP SVC connection established for SVC session.  
Sep 22 2021 23:59:52: %FTD-6-722022: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> TCP  
SVC connection established without compression  
Sep 22 2021 23:59:52: %FTD-7-746012: **user-identity: Add IP-User mapping 10.0.50.1 - LOCAL\user2  
Succeeded - VPN user**  
Sep 22 2021 23:59:52: %FTD-6-722055: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101>  
Client Type: Cisco AnyConnect VPN Agent for Windows 4.10.02086  
Sep 22 2021 23:59:52: %FTD-4-722051: **Group**

# De RADIUS Live-logbestanden op ISE tonen:

Identity Services Engine

### Overview

Event	5200 Authentication succeeded
Username	user2
Endpoint Id	00:50:56:96:45:6F:0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

### Authentication Details

Source Timestamp	2021-09-23 00:00:06:488
Received Timestamp	2021-09-23 00:00:06:488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	00:50:56:96:45:6F:0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	da800540000d00014bc087
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	DRIVERAP_FT0_7-0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

### Steps

```

11001 Received RADIUS AccessRequest
11017 RADIUS created a new session
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15043 Queried PIP - Normalised Radius RadiusForType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
10013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user2
24212 Found User in Internal Users IDStore
22037 Authentication Passed
24716 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15030 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user2
24211 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - Radius User Name
15048 Queried PIP - Radius NAS-Port Type
15048 Queried PIP - EndPoints LogicalProfile
15048 Queried PIP - Network Access AuthenticationStatus
15016 Selected Authorization Profile - PermitAccess
22081 Max sessions policy passed
22083 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept
    
```

Identity Services Engine

NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	202 milliseconds

### Other Attributes

ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53243
Tunnel Client Endpoint	(tag=0) 192.168.0.101
CVPR3000ASAPRXTA-Tunnel-Group-Name	RA_VPN
OriginalUsername	user2
NetworkDeviceProfileId	b0099005-3150-4210-a80a-675345b0f06c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPRXTA-Client-Type	2
Acq SessionID	driverap-ISE-2-71417494978-24
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_join_Points
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
ISEPolicySetName	Default
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	LocationAll Locations
Device Type	Device TypeAll Device Types

Identity Services Engine

IPSEC	IPSECCalls IPSEC Device#No
Name	Endpoint Identity Groups Profiled Workstation
EnableFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPM SessionID	da800540000d00014bc087
Called Station ID	192.168.0.100
CiscoAVPair	<pre> mdu-mv-device-platform:mdu-mv-device-platform:00:50:56:96:45:6f:0 mdu-mv-device-platform:radius:192.0.18.352 mdu-mv-device-publicmap:00:50:56:96:45:6f:0 mdu-mv-device-appeal:Connect:Windows 4.10:02088 mdu-mv-device-type:VMware, Inc. VMware Virtual Platform mdu-mv-device-uid: globa@158f88e00f52f3f2c0e243459f48aa2ae2083 mdu-mv-device- uid=3C38427071F80782F816F124521184406596C71E370388CC03F 94402885244 audit session-ip=da800540000d00014bc087 ip source-ip=192.168.0.101 os=pub@ntwk     </pre>

### Result

Class	CACS-da800540000d00014bc087-driverap-ISE-2-71417494978-24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

**Opmerking:** U moet verschillende IP-adresbereik gebruiken voor IP-adrestoewijzing op zowel de lokale FTD-pool als het ISE-autorisatiebeleid om dubbele IP-adresconflicten tussen uw AnyConnect-clients te voorkomen. In dit configuratievoorbeeld werd FTD geconfigureerd met een IPv4 lokale pool van 10.0.50.1 tot 10.0.50.100 en de ISE server toegewezen een statisch IP-adres van 10.0.50.101.

## Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Op FTD:

- **Straal verwijderen**

Op ISE:

- RADIUS-live logbestanden