Konfigurieren der statischen IP-Adresszuweisung zu AnyConnect-Benutzern über RADIUS-Autorisierung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die RADIUS-Autorisierung mit einem Identity Services Engine (ISE)-Server konfigurieren, sodass dieser immer dieselbe IP-Adresse über das RADIUS-Attribut 8 Framed-IP-Adresse an die Firepower Threat Defense (FTD) für einen bestimmten Benutzer des Cisco AnyConnect Secure Mobility Client weiterleitet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FTD
- Firepower Management Center (FMC)
- ISE
- Cisco AnyConnect Secure Mobility Client
- RADIUS-Protokoll

Verwendete Komponenten

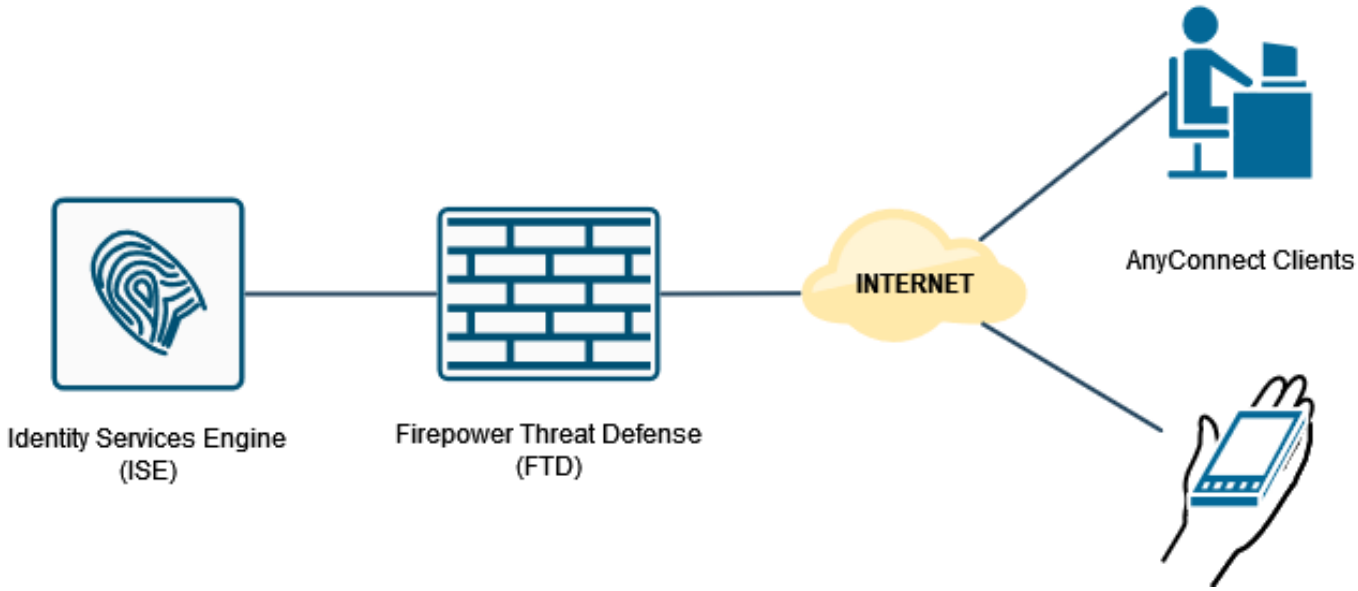
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- FMCv - 7.0.0 (Build 94)
- FTDv - 7.0.0 (Build 94)
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086
- Windows 10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Konfiguration eines Remote Access-VPN mit AAA/RADIUS-Authentifizierung über FMC

Eine schrittweise Anleitung finden Sie in diesem Dokument und in diesem Video:

- AnyConnect Remote Access VPN-Konfiguration auf FTD
- Erste AnyConnect-Konfiguration für FTD von FMC verwaltet

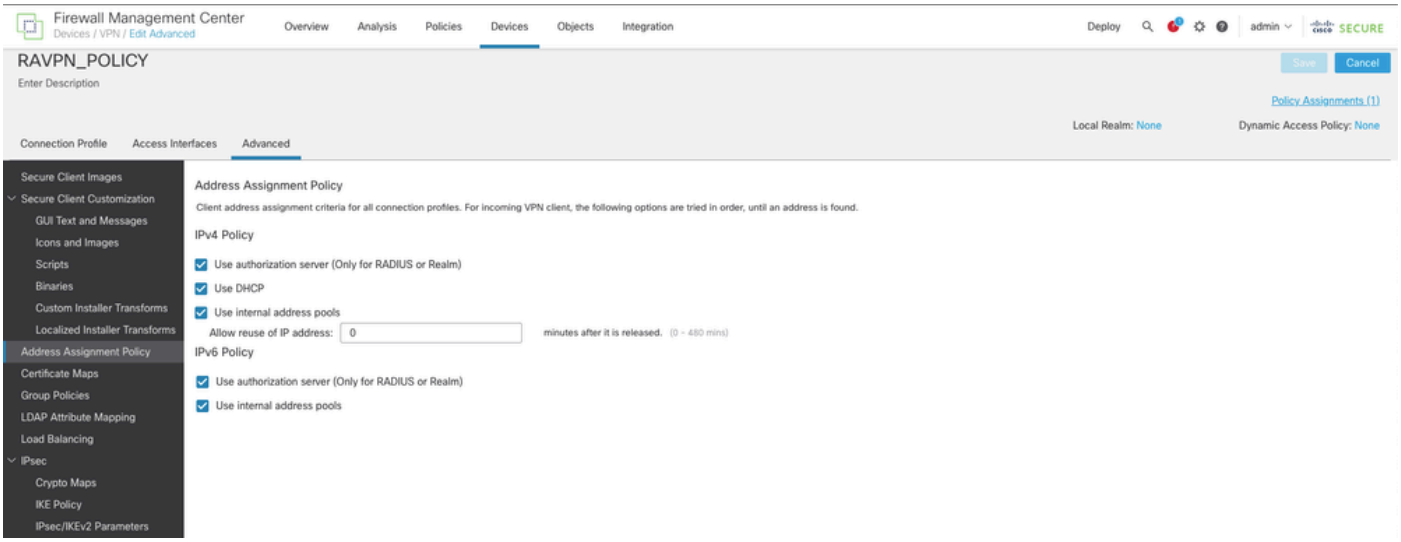
Die VPN-Konfiguration für den Remote-Zugriff auf der FTD-CLI lautet wie folgt:

```
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
```

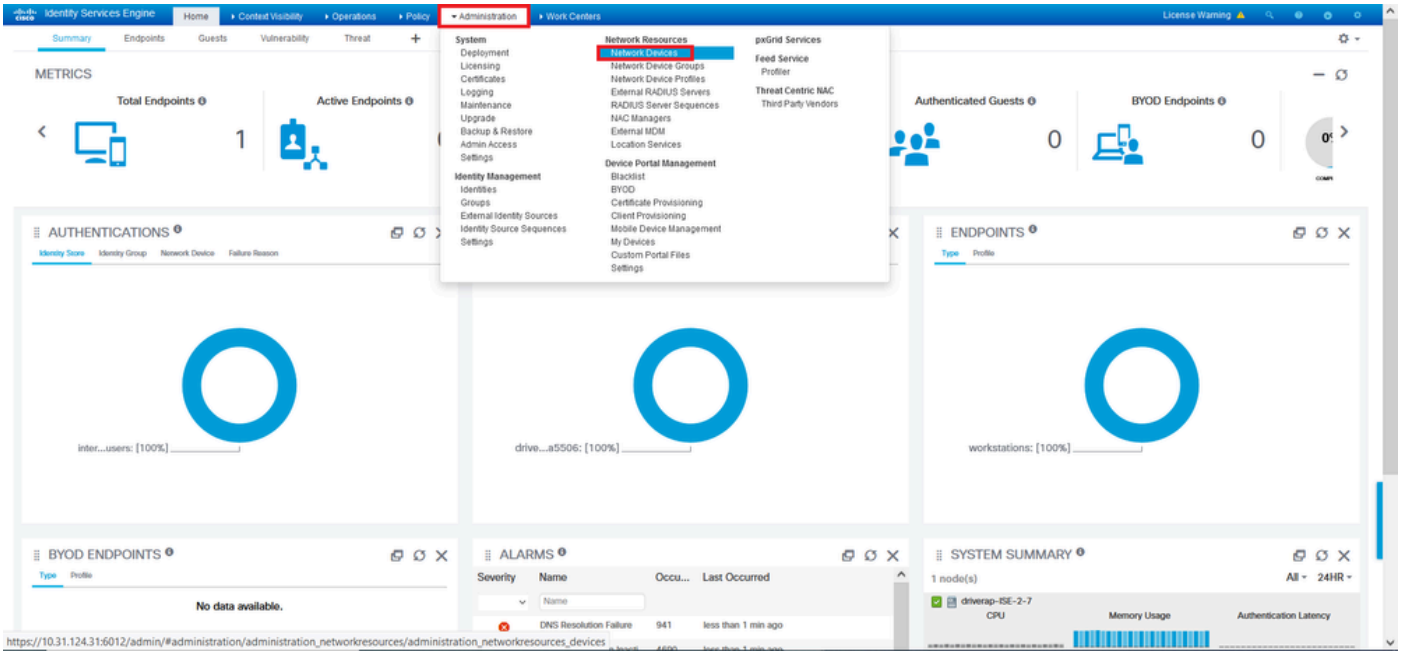
Konfigurieren der Verwendung des Autorisierungsservers auf dem FMC

Navigieren Sie zu Devices (Geräte) > Remote Access (Remote-Zugriff), und wählen Sie die gewünschte Remote Access-VPN-Richtlinie aus. Navigieren Sie zu Erweitert > Adresszuweisungsrichtlinie, und stellen Sie sicher, dass die Option Autorisierungsserver verwenden (nur für RADIUS oder Bereich) aktiviert ist.

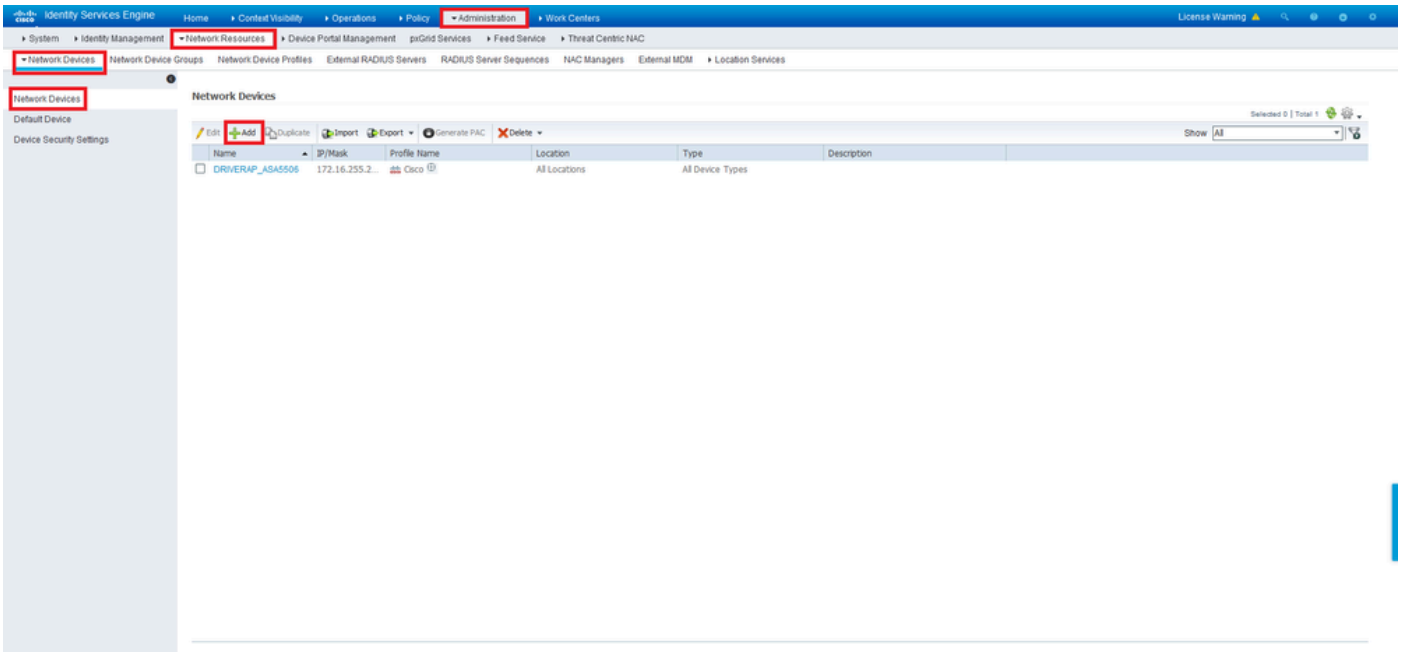


Autorisierungsrichtlinie auf ISE (RADIUS-Server) konfigurieren

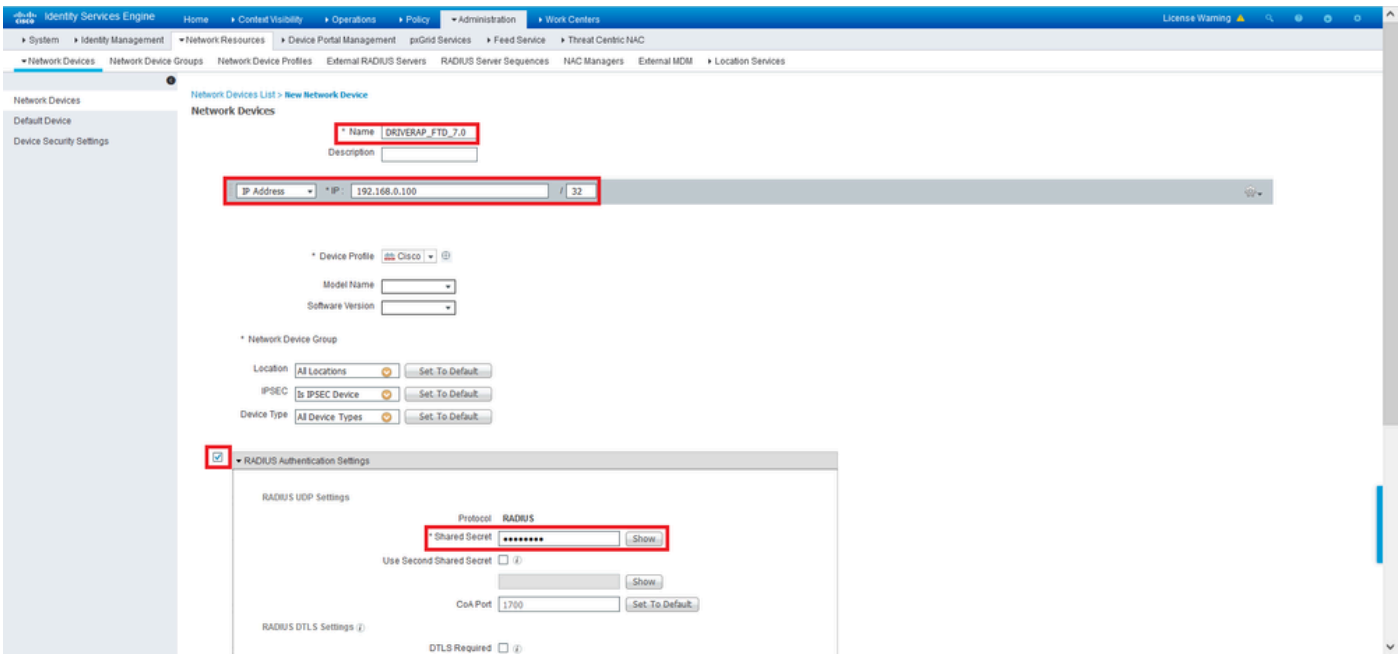
Schritt 1: Melden Sie sich beim ISE-Server an, und navigieren Sie zu Administration > Network Resources > Network Devices.



Schritt 2: Klicken Sie im Abschnitt "Netzwerkgeräte" auf Hinzufügen, damit die ISE RADIUS-Zugriffsanforderungen aus dem FTD verarbeiten kann.

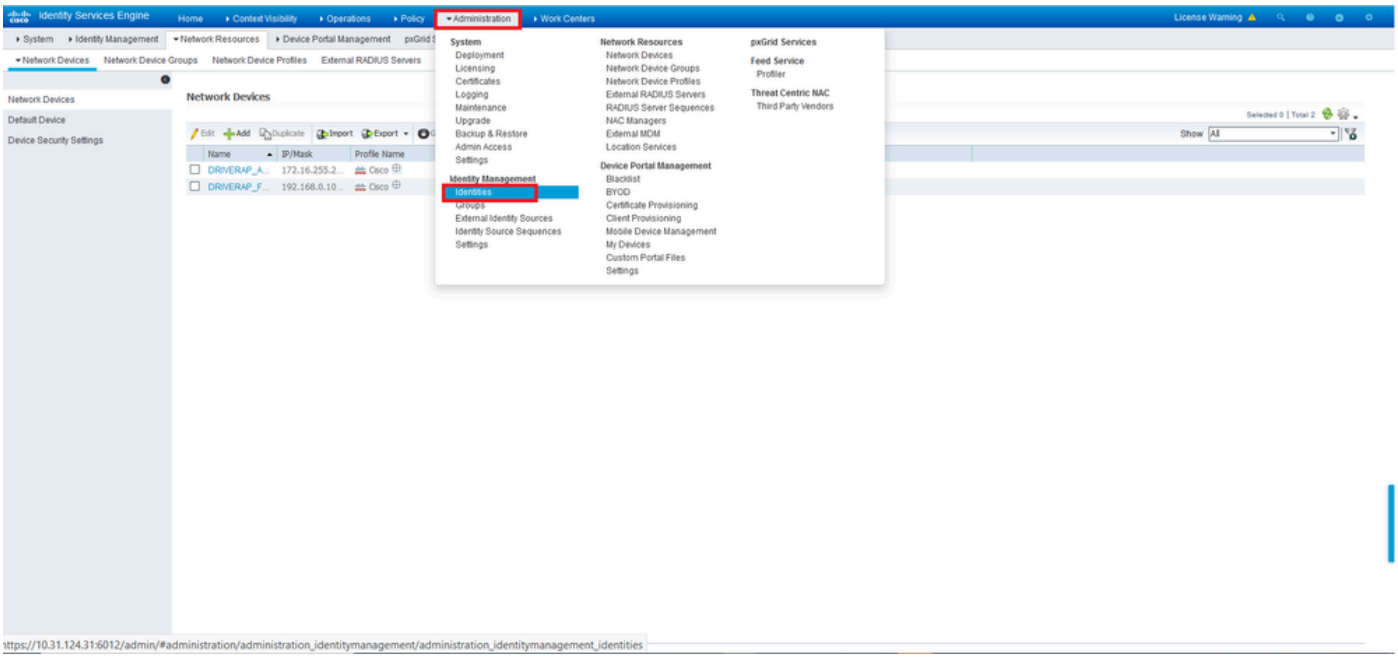


Geben Sie die Felder für den Netzwerkgerätenamen und die IP-Adresse ein, und aktivieren Sie das Kontrollkästchen RADIUS Authentication Settings (RADIUS-Authentifizierungseinstellungen). Der gemeinsame geheime Schlüssel muss derselbe Wert sein, der beim Erstellen des RADIUS-Serverobjekts auf dem FMC verwendet wurde.

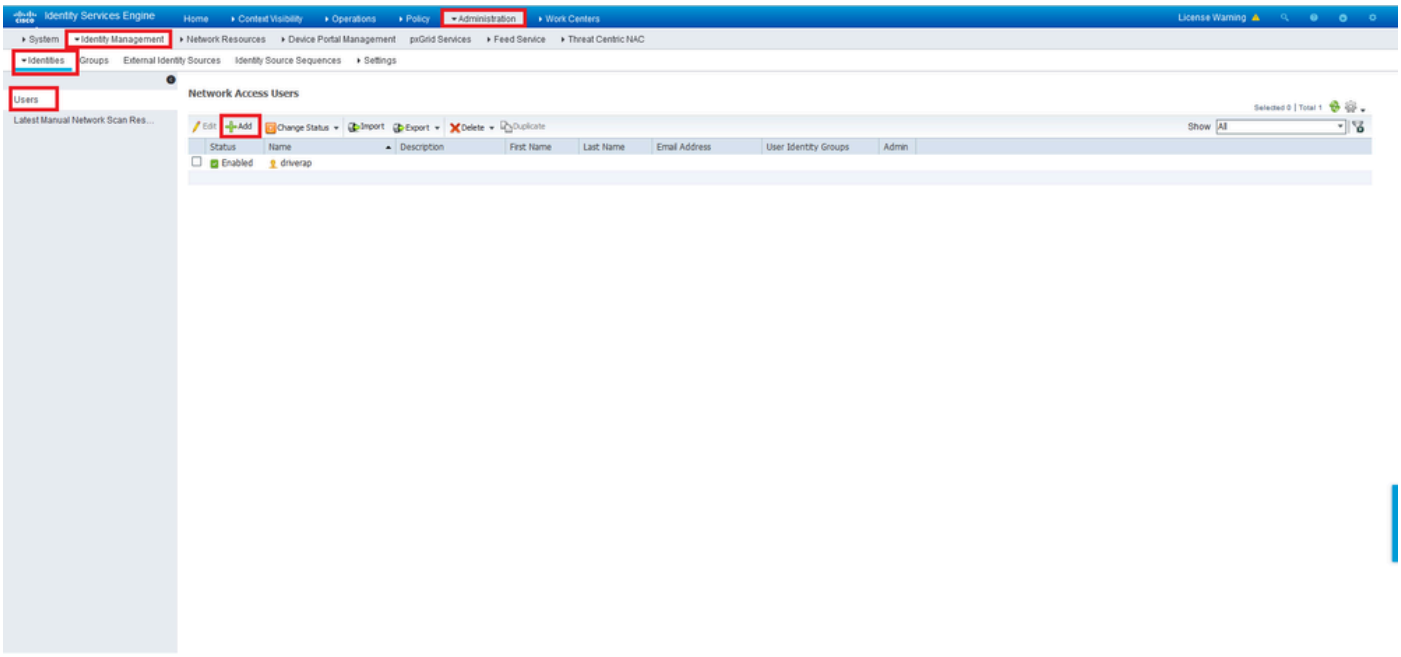


Speichern Sie es mit der Schaltfläche am Ende dieser Seite.

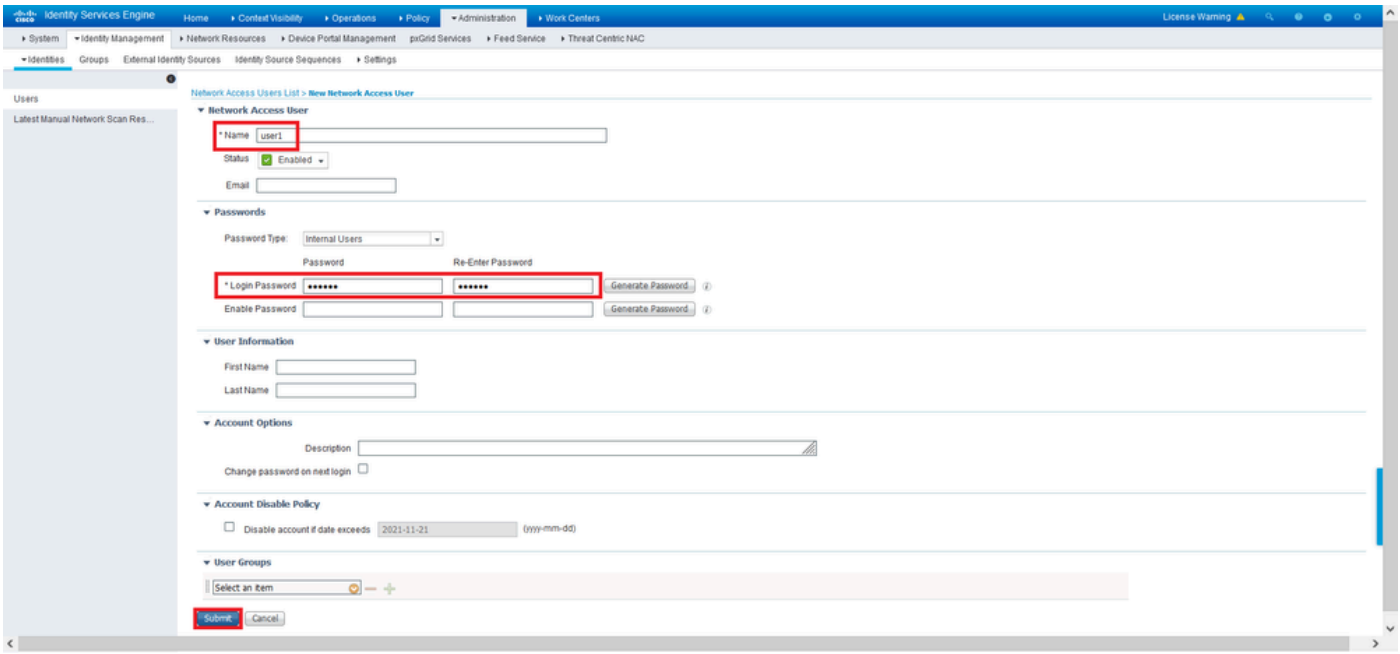
Schritt 3: Navigieren Sie zu Administration > Identity Management > Identities.



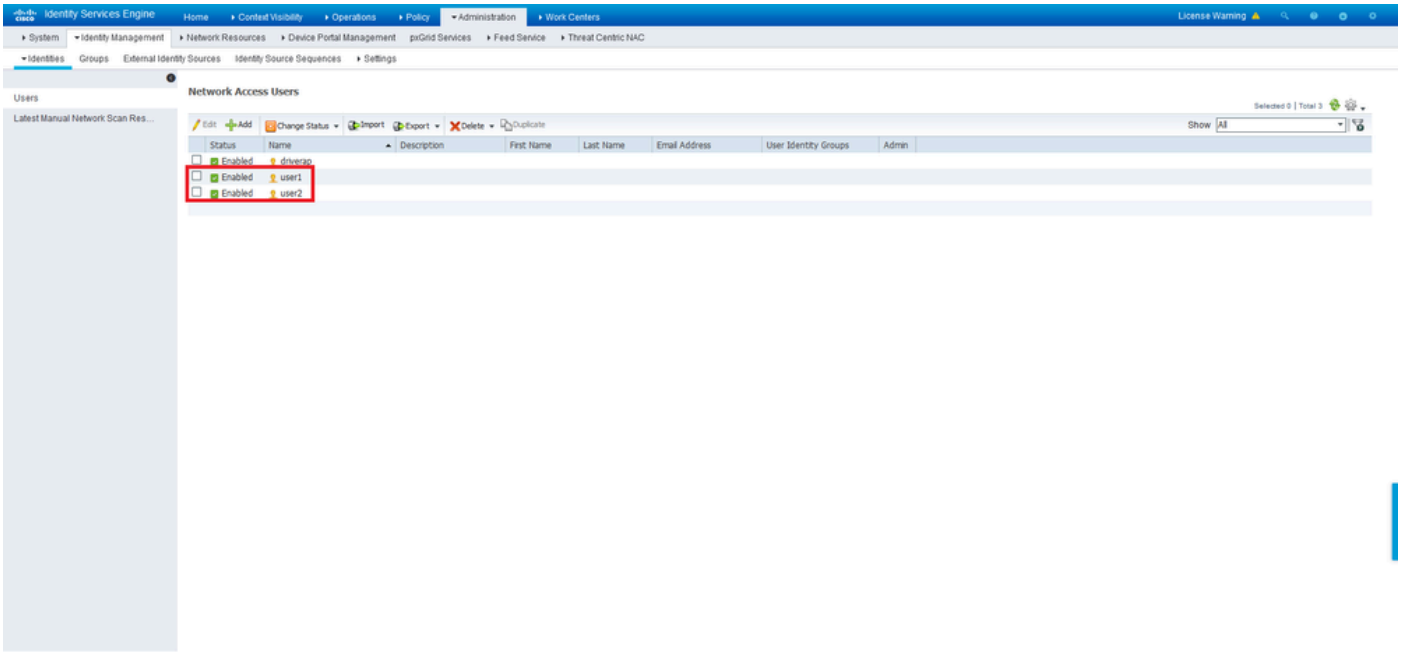
Schritt 4: Klicken Sie im Abschnitt "Netzwerkzugriffsbenutzer" auf Hinzufügen, um user1 in der lokalen ISE-Datenbank zu erstellen.



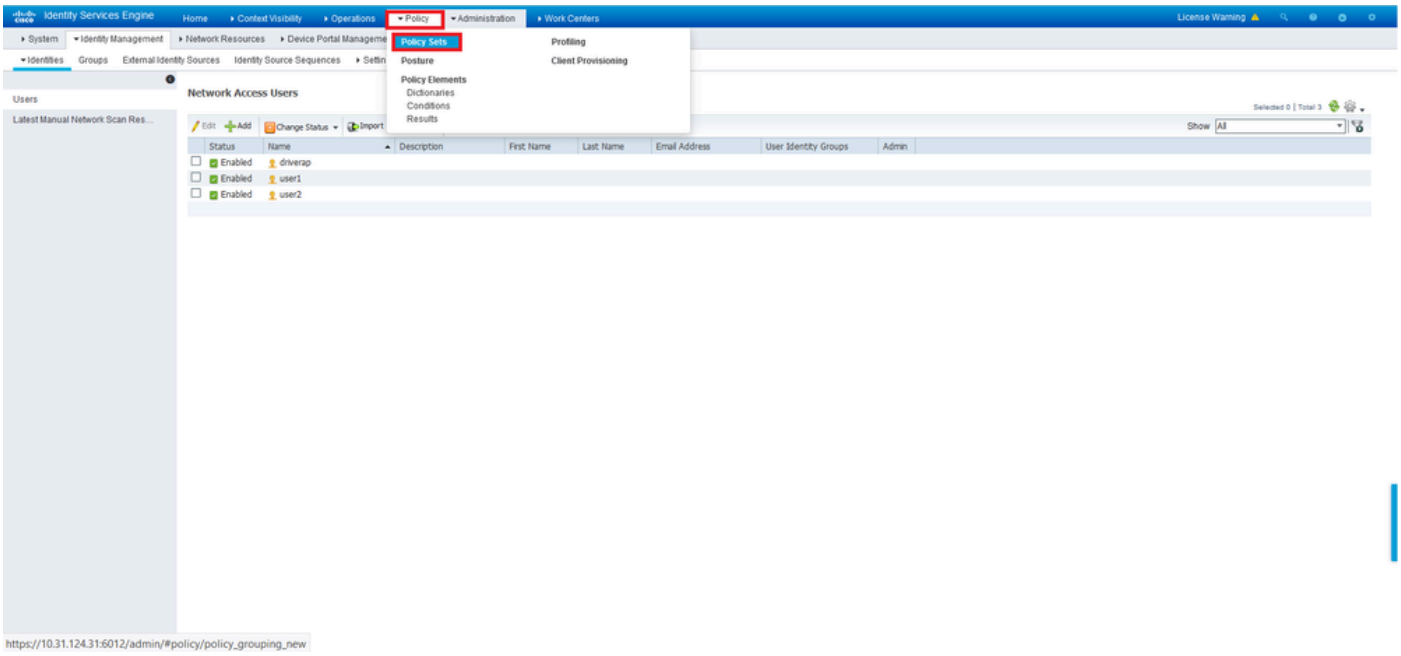
Geben Sie in den Feldern Name und Anmeldekennwort Benutzername und Kennwort ein, und klicken Sie dann auf Senden.



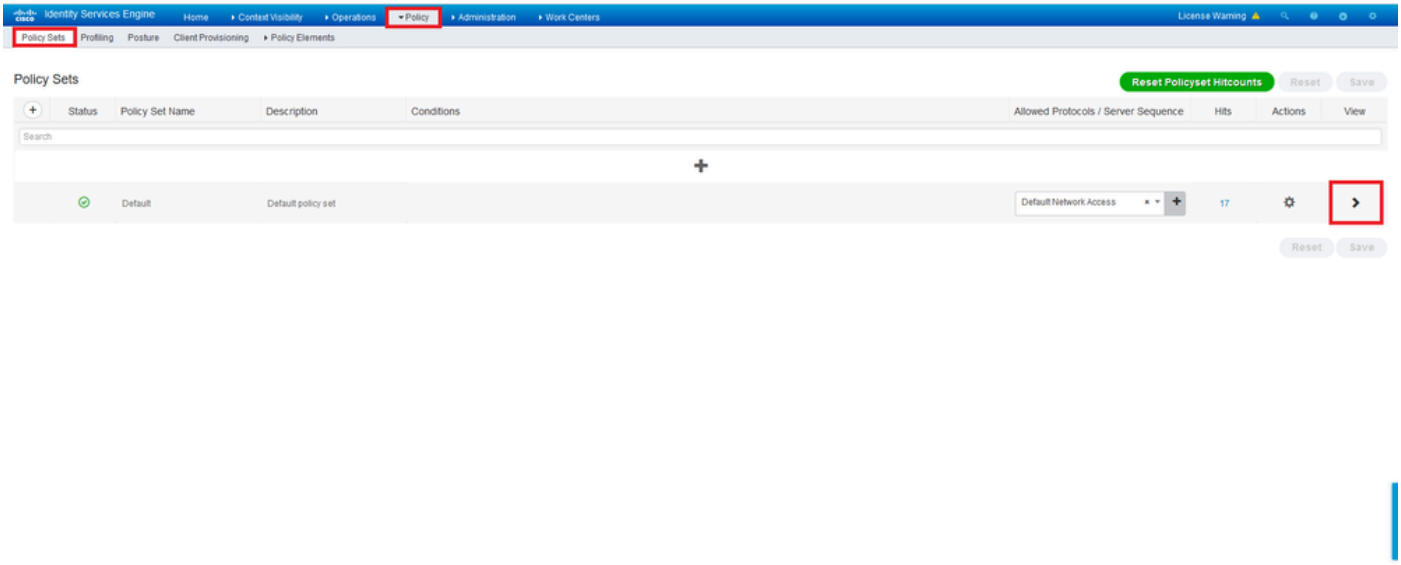
Schritt 5: Wiederholen Sie die vorherigen Schritte, um user2 zu erstellen.



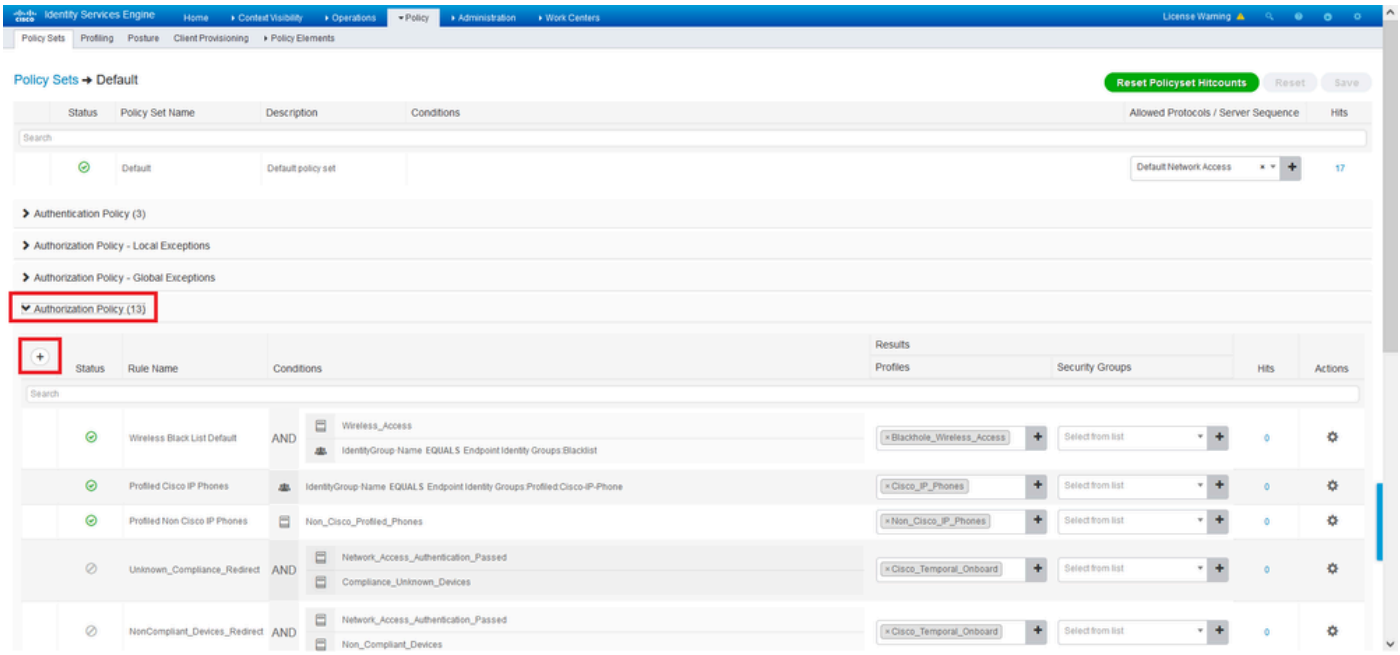
Schritt 6: Navigieren Sie zu Policy > Policy Sets.



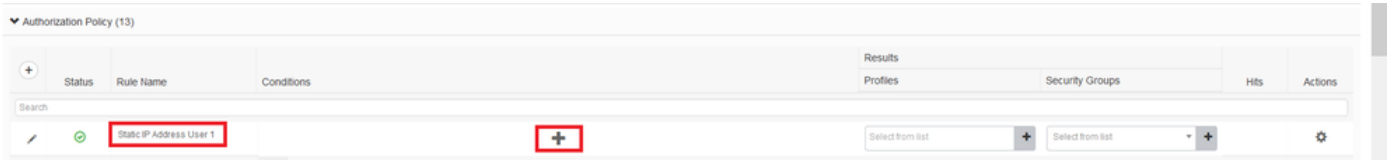
Schritt 7. Klicken Sie auf den Pfeil > auf der rechten Seite des Bildschirms.



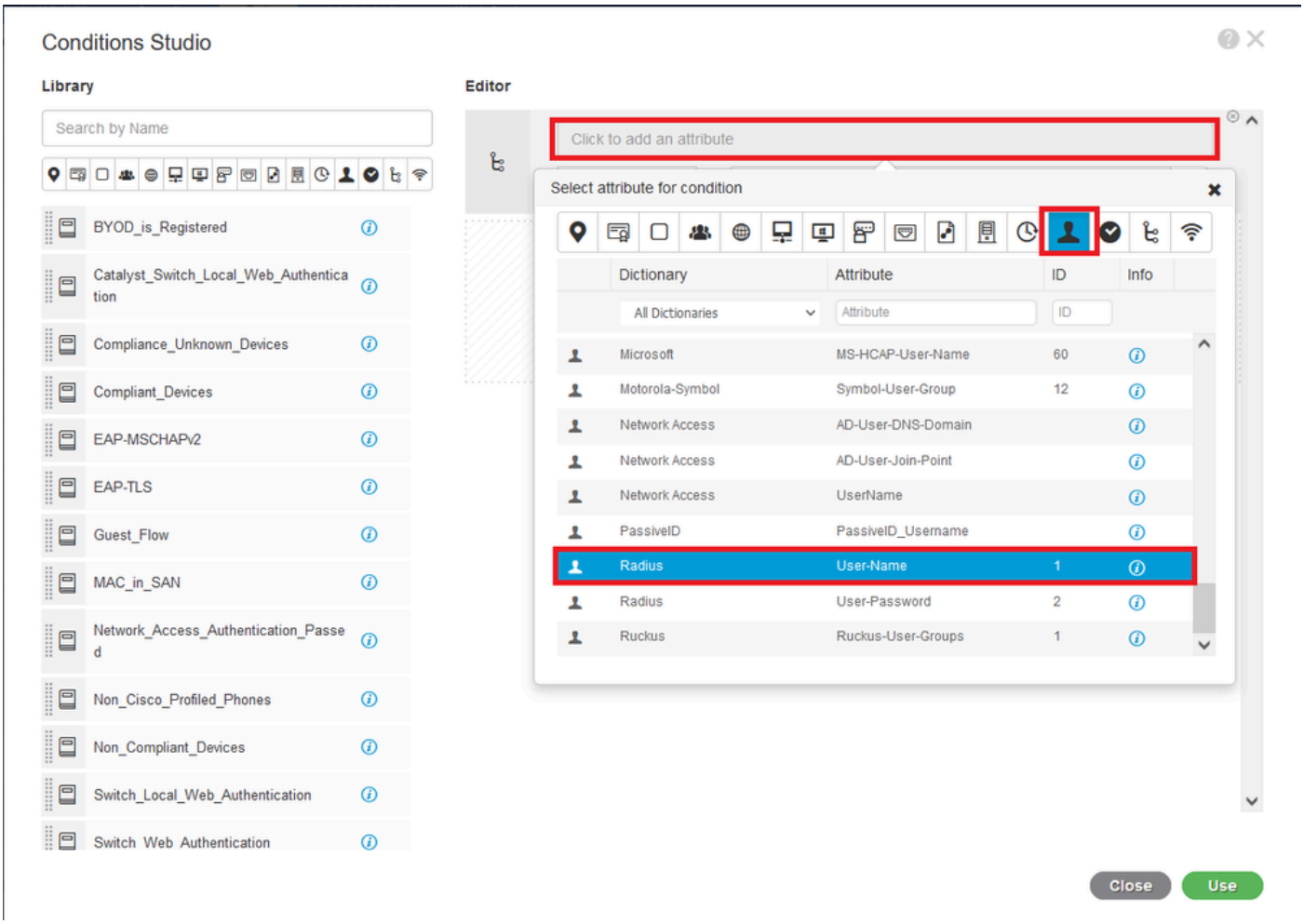
Schritt 8: Klicken Sie auf den Pfeil > neben Autorisierungsrichtlinie, um sie zu erweitern. Klicken Sie nun auf das + Symbol, um eine neue Regel hinzuzufügen.



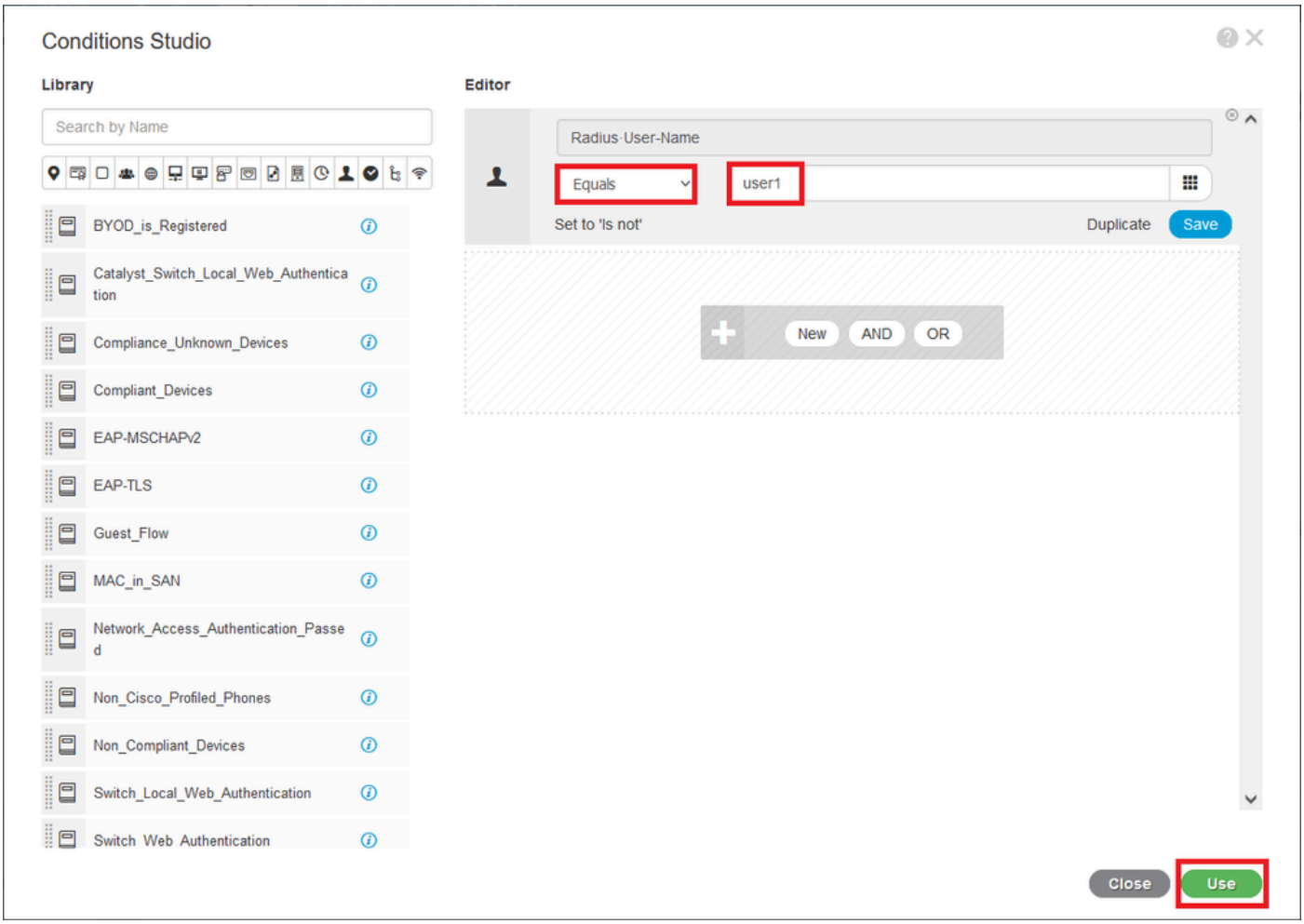
Geben Sie einen Namen für die Regel ein, und wählen Sie in der Spalte Bedingungen das Symbol + aus.



Klicken Sie in das Textfeld Attribute-Editor, und klicken Sie auf das Symbol Betreff. Blättern Sie nach unten, bis Sie das Attribut RADIUS User-Name finden und auswählen.

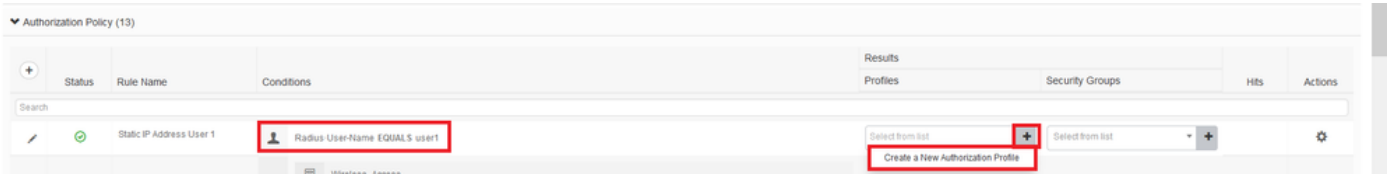


Behalten Sie Equals als Operator bei, und geben Sie user1 in das Textfeld daneben ein. Klicken Sie auf Verwenden, um das Attribut zu speichern.

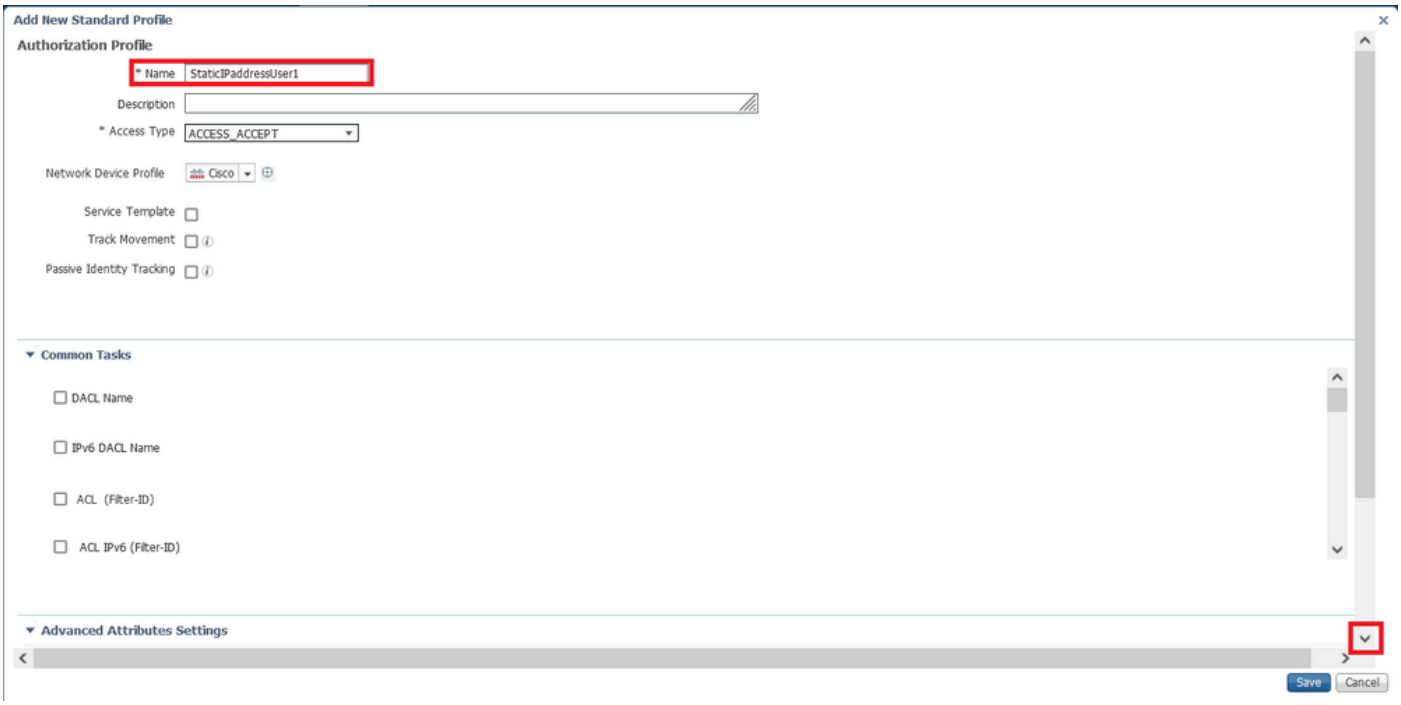


Die Bedingung für diese Regel ist jetzt festgelegt.

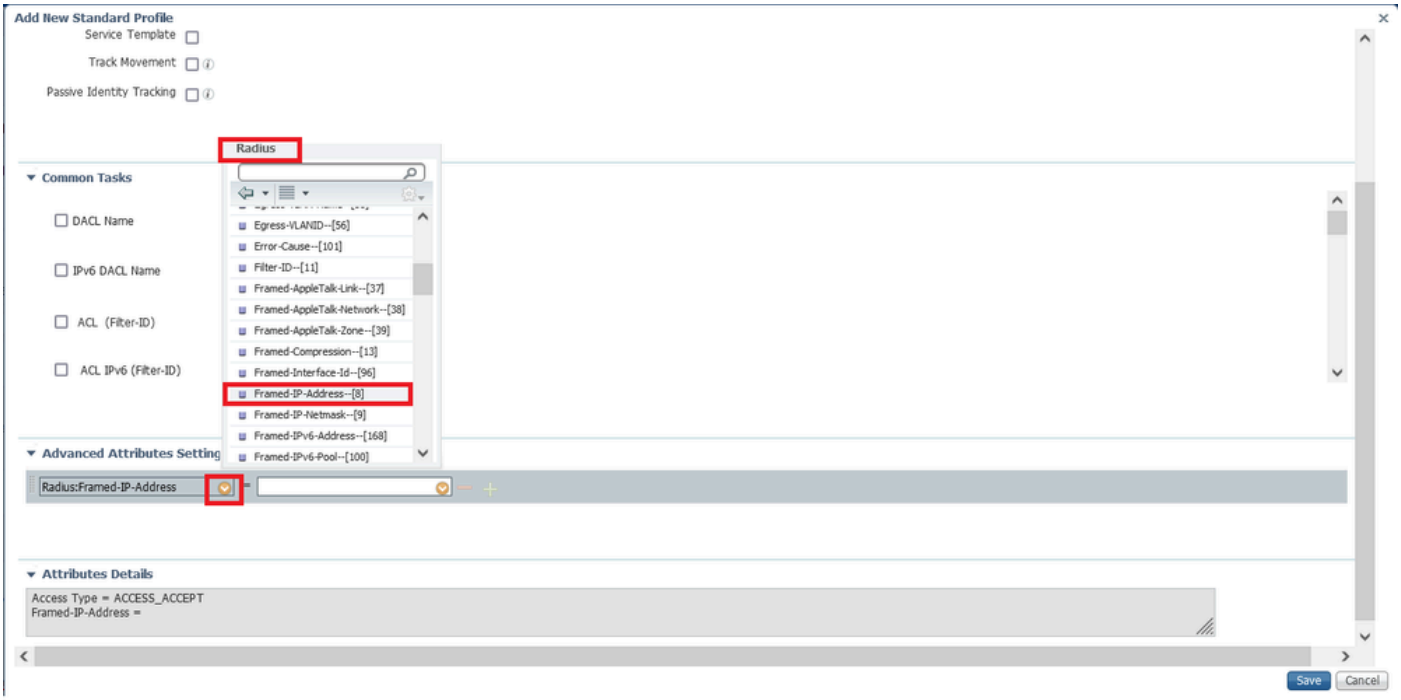
Schritt 9: Klicken Sie in der Spalte Ergebnisse/Profile auf das Symbol +, und wählen Sie Create a New Authorization Profile (Neues Autorisierungsprofil erstellen).



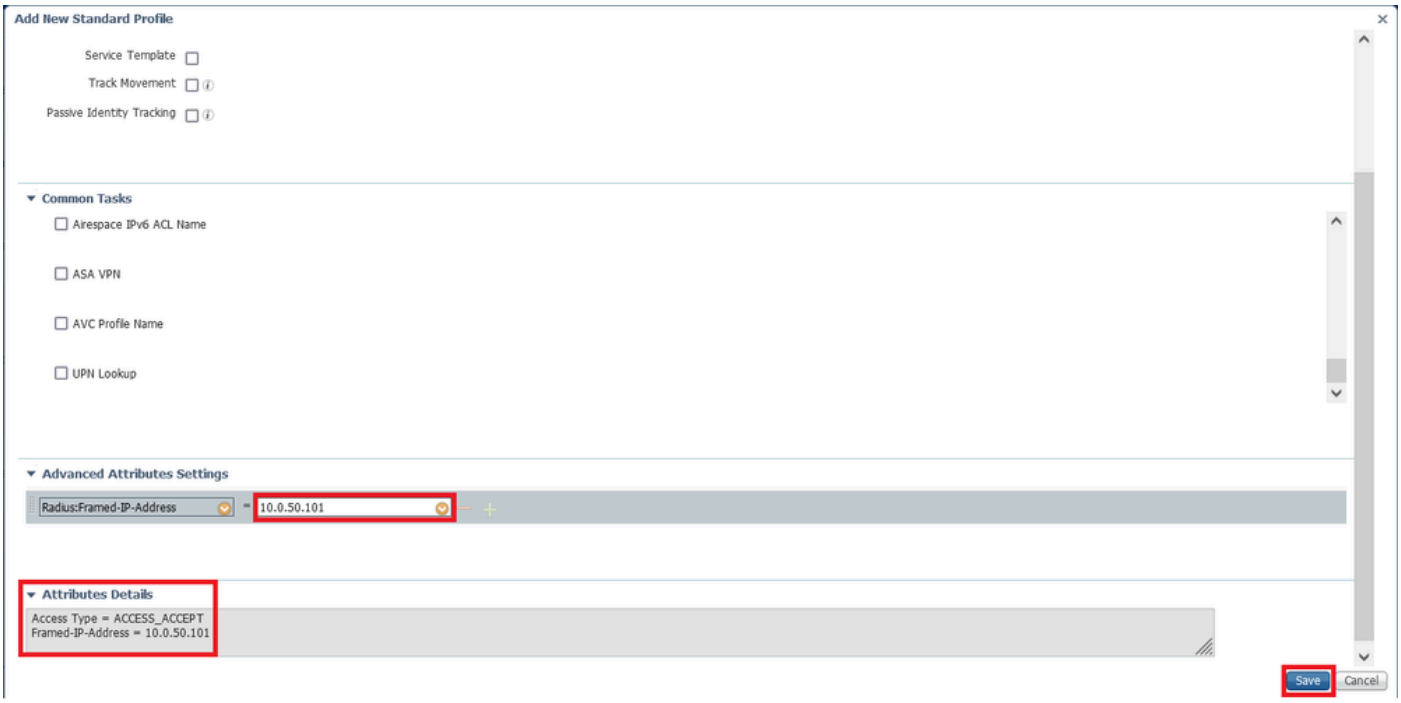
Geben Sie ihm einen Namen, und behalten Sie ACCESS_ACCEPT als Zugriffstyp bei. Blättern Sie nach unten zum Abschnitt Erweiterte Attributeinstellungen.



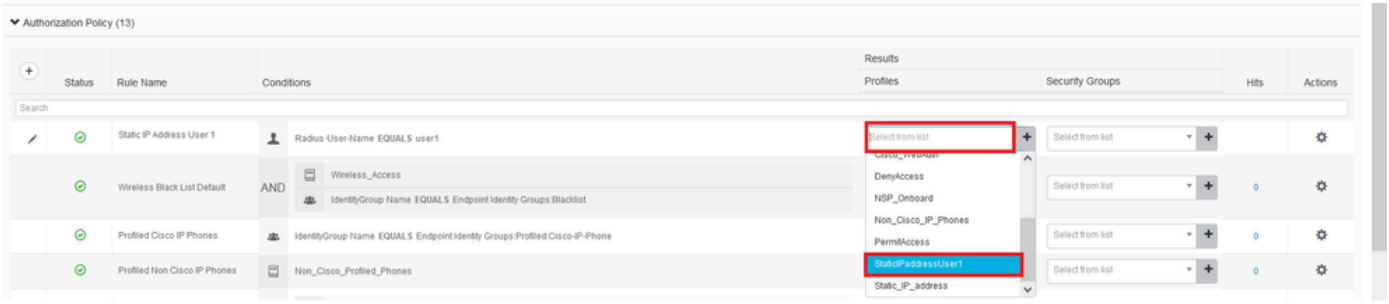
Klicken Sie auf den orangefarbenen Pfeil, und wählen Sie Radius > Framed-IP-Address—[8].



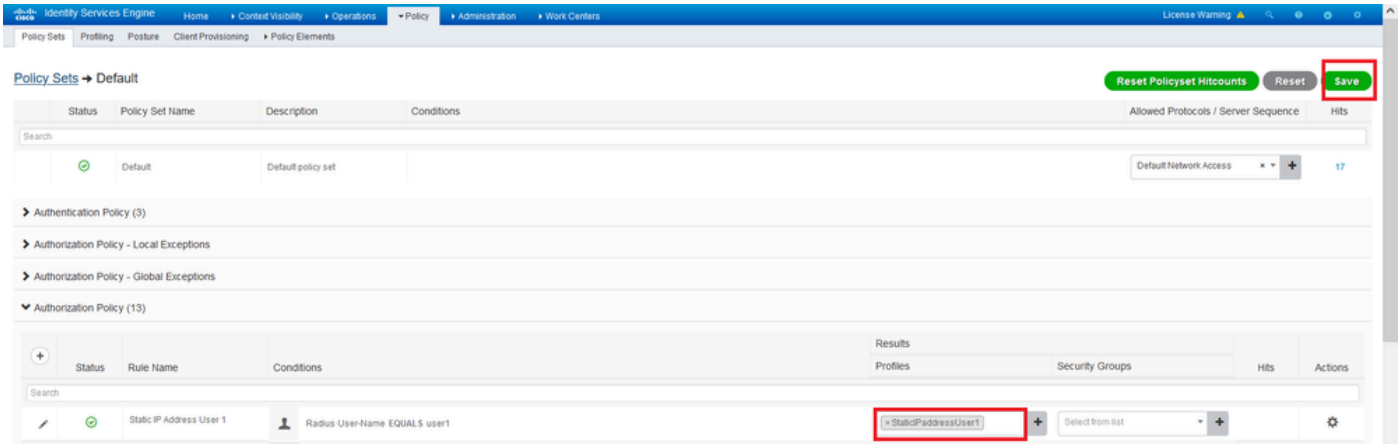
Geben Sie die IP-Adresse ein, die Sie diesem Benutzer statisch immer zuweisen möchten, und klicken Sie auf Speichern.



Schritt 10: Wählen Sie nun das neu erstellte Autorisierungsprofil.

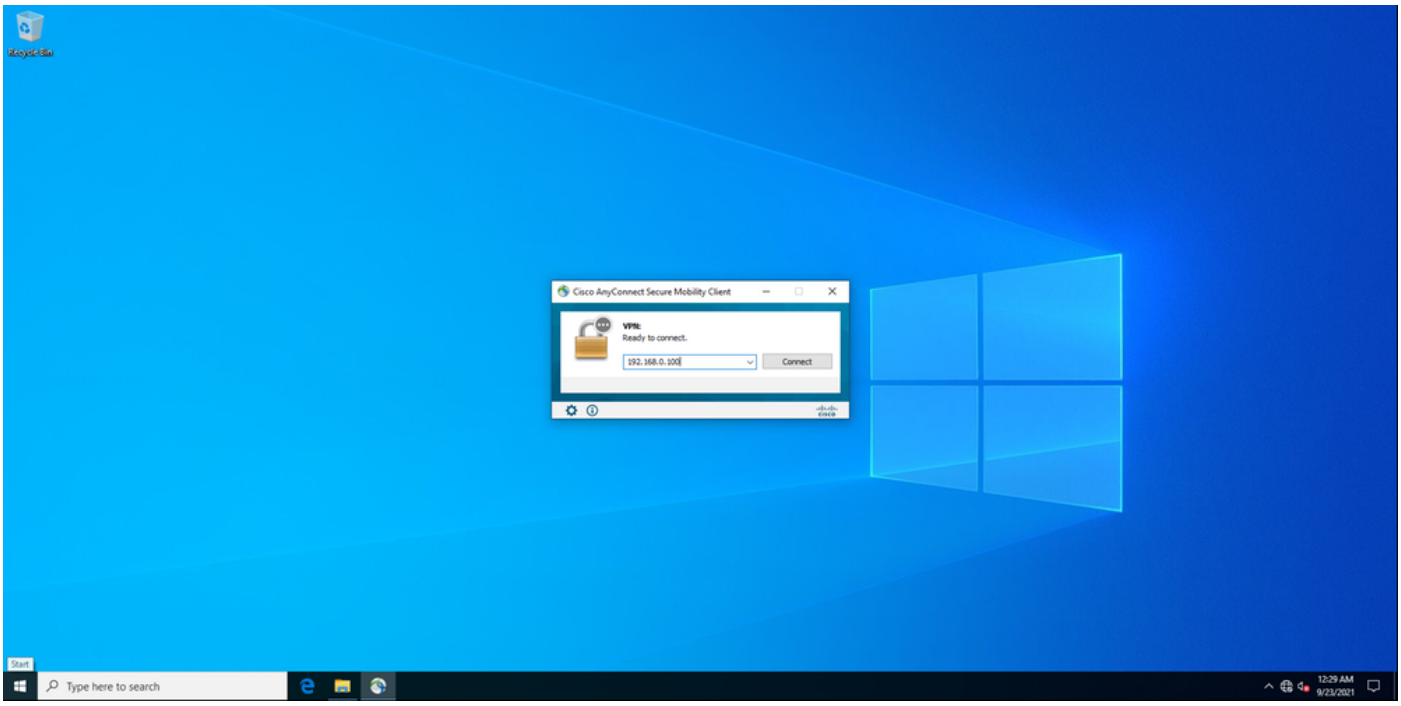


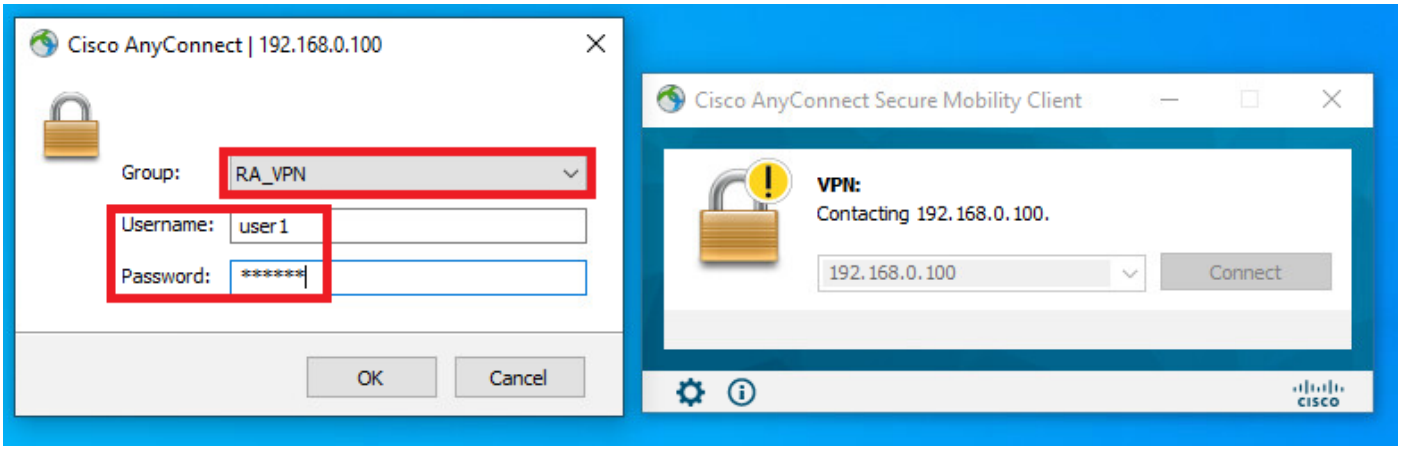
Die Autorisierungsregel ist jetzt festgelegt. Klicken Sie auf Speichern.



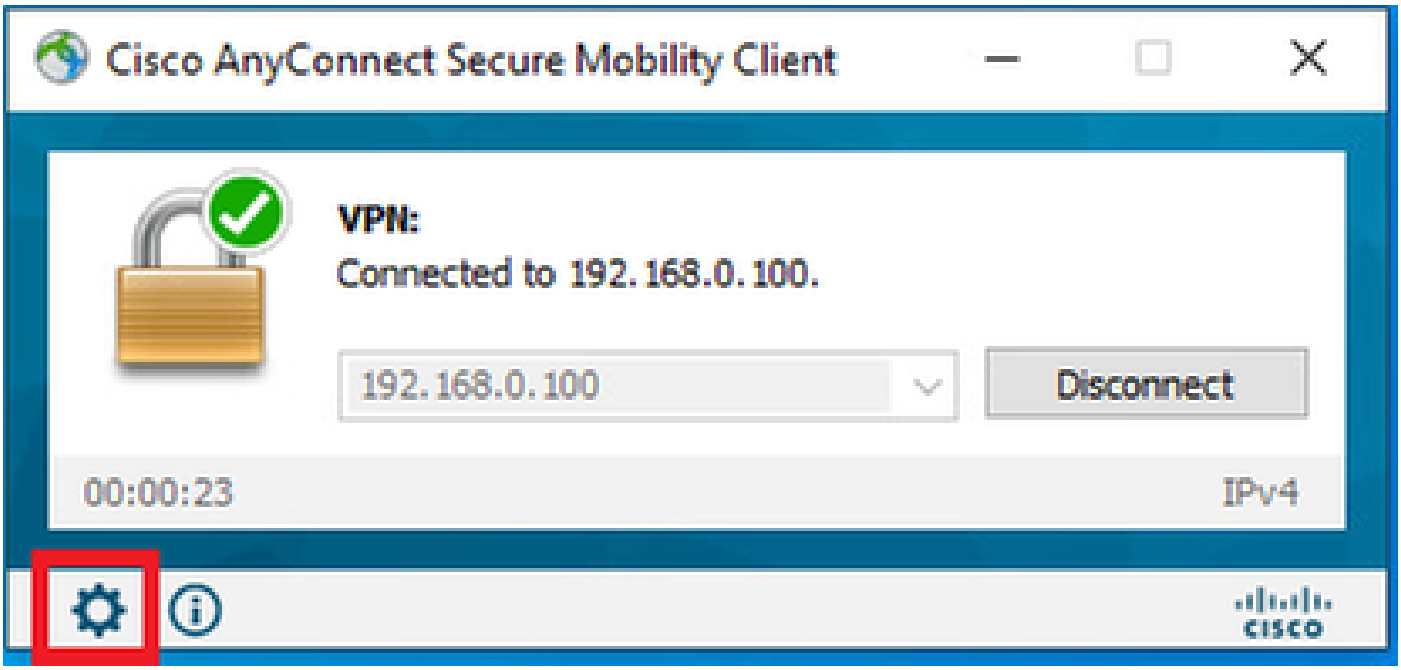
Überprüfung

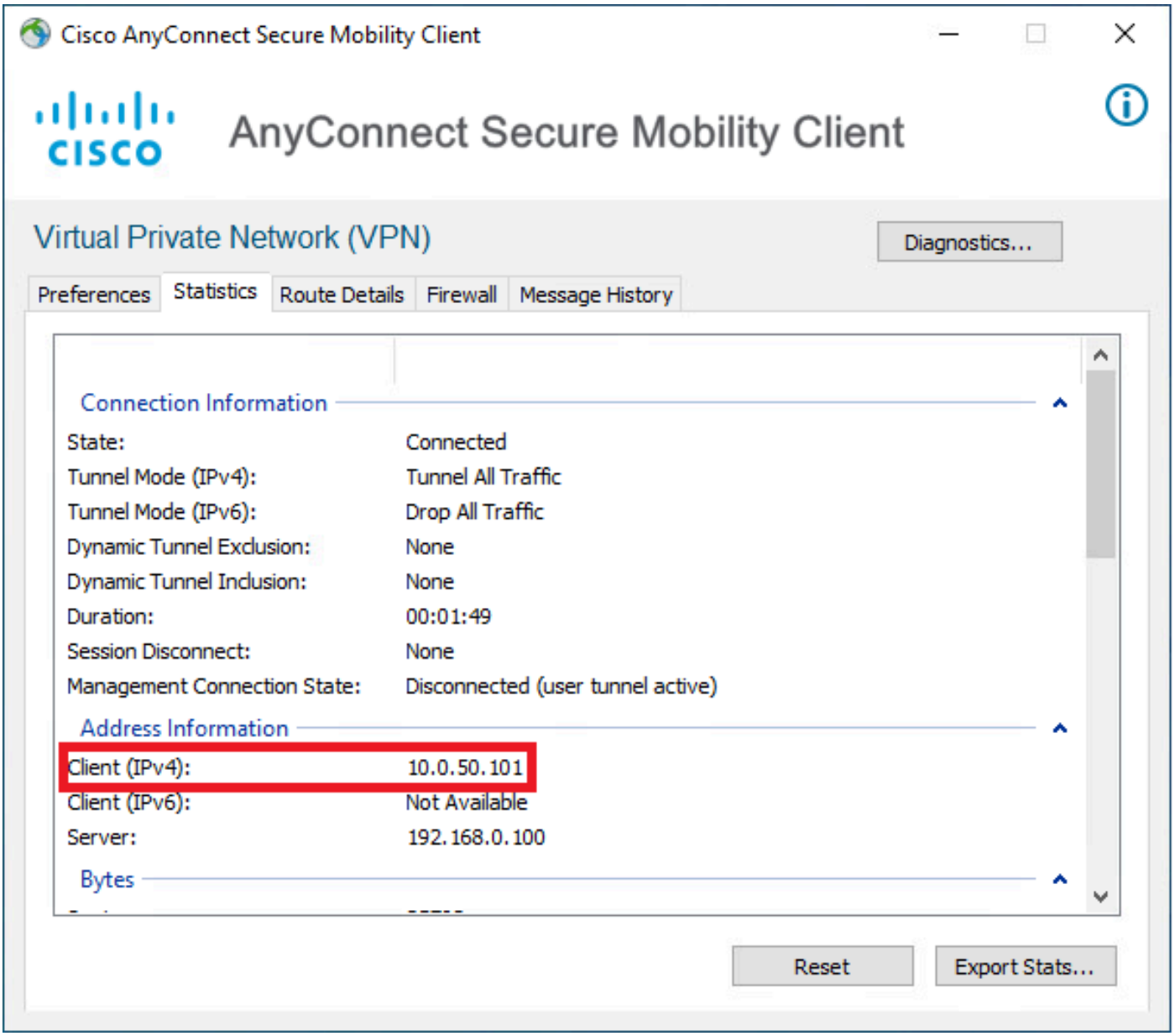
Schritt 1: Navigieren Sie zu dem Client-Computer, auf dem der Cisco AnyConnect Secure Mobility Client installiert ist. Stellen Sie eine Verbindung zu Ihrem FTD-Headend her (hier wird ein Windows-Computer verwendet), und geben Sie die Anmeldeinformationen user1 ein.





Klicken Sie auf das Zahnradsymbol (linke untere Ecke), und navigieren Sie zur Registerkarte "Statistik". Bestätigen Sie im Abschnitt "Adressinformationen", dass die zugewiesene IP-Adresse tatsächlich die in der ISE-Autorisierungsrichtlinie für diesen Benutzer konfigurierte IP-Adresse ist.


Cisco AnyConnect Secure Mobility Client
VPN:
Connected to 192.168.0.100.
192.168.0.100
Disconnect
00:00:23
IPv4
cisco


Cisco AnyConnect Secure Mobility Client
cisco
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Tunnel All Traffic
Tunnel Mode (IPv6): Drop All Traffic
Dynamic Tunnel Exclusion: None
Dynamic Tunnel Inclusion: None
Duration: 00:01:49
Session Disconnect: None
Management Connection State: Disconnected (user tunnel active)
Address Information
Client (IPv4): 10.0.50.101
Client (IPv6): Not Available
Server: 192.168.0.100
Bytes
Reset
Export Stats...

Der Debugradius aller Befehle in FTD zeigt Folgendes an:

<#root>

```
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
```

Die FTD-Protokolle zeigen Folgendes:

<#root>

```
firepower#
<omitted output>
Sep 22 2021 23:52:40: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.1
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 =
Sep 22 2021 23:52:48: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user
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[
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.radius[
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.radius[
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.g
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.u
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.u
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.t
Sep 22 2021 23:52:48: %FTD-6-734001: DAP: User user1, Addr 192.168.0.101, Connection AnyConnect: The fo
Sep 22 2021 23:52:48: %FTD-6-113039: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> AnyConnect p
<omitted output>
Sep 22 2021 23:53:17: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.1
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
Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: callback failed during IPv
Sep 22 2021 23:53:17: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User <user1> IP <
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 SV
Sep 22 2021 23:53:17: %FTD-6-722022: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> TCP SVC conn
Sep 22 2021 23:53:17: %FTD-7-746012:
```

user-identity: Add IP-User mapping 10.0.50.101 - LOCAL\user1 Succeeded - VPN user

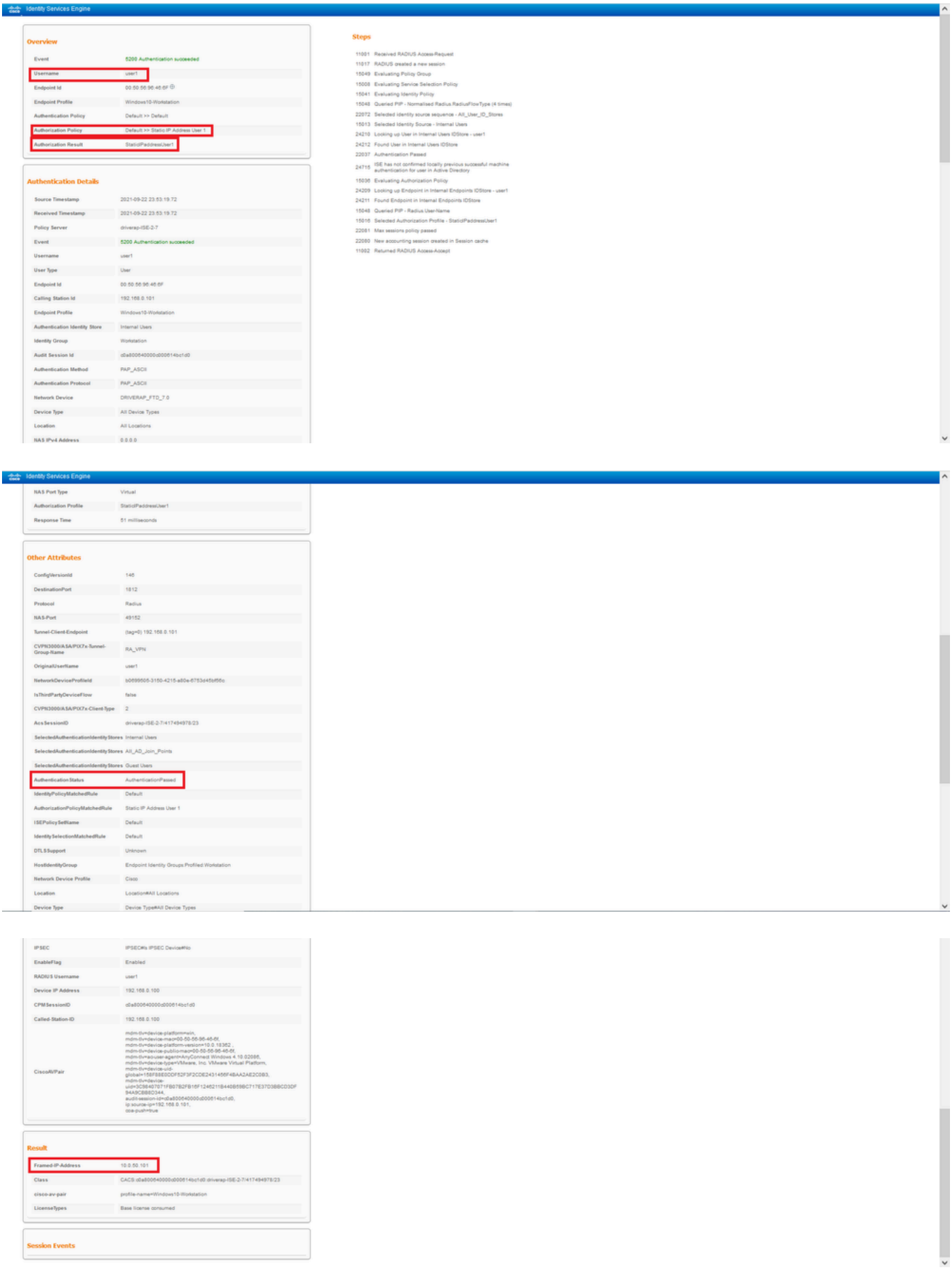
```
Sep 22 2021 23:53:17: %FTD-6-722055: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> Client Type:
Sep 22 2021 23:53:17: %FTD-4-722051:
```

Group

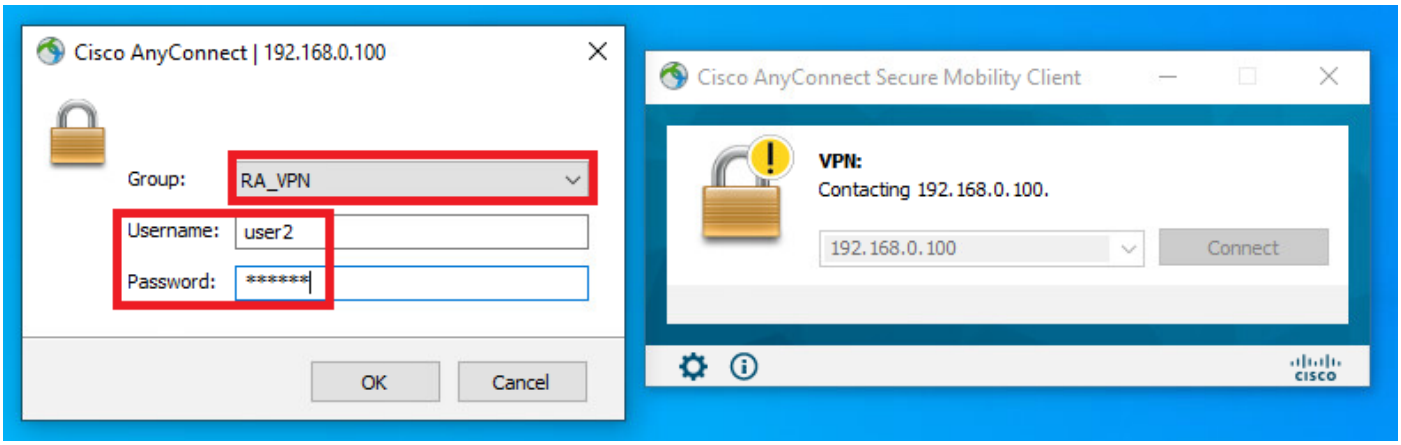
User

IP <192.168.0.101> IPv4 Address <10.0.50.101> IPv6 address <::> assigned to session

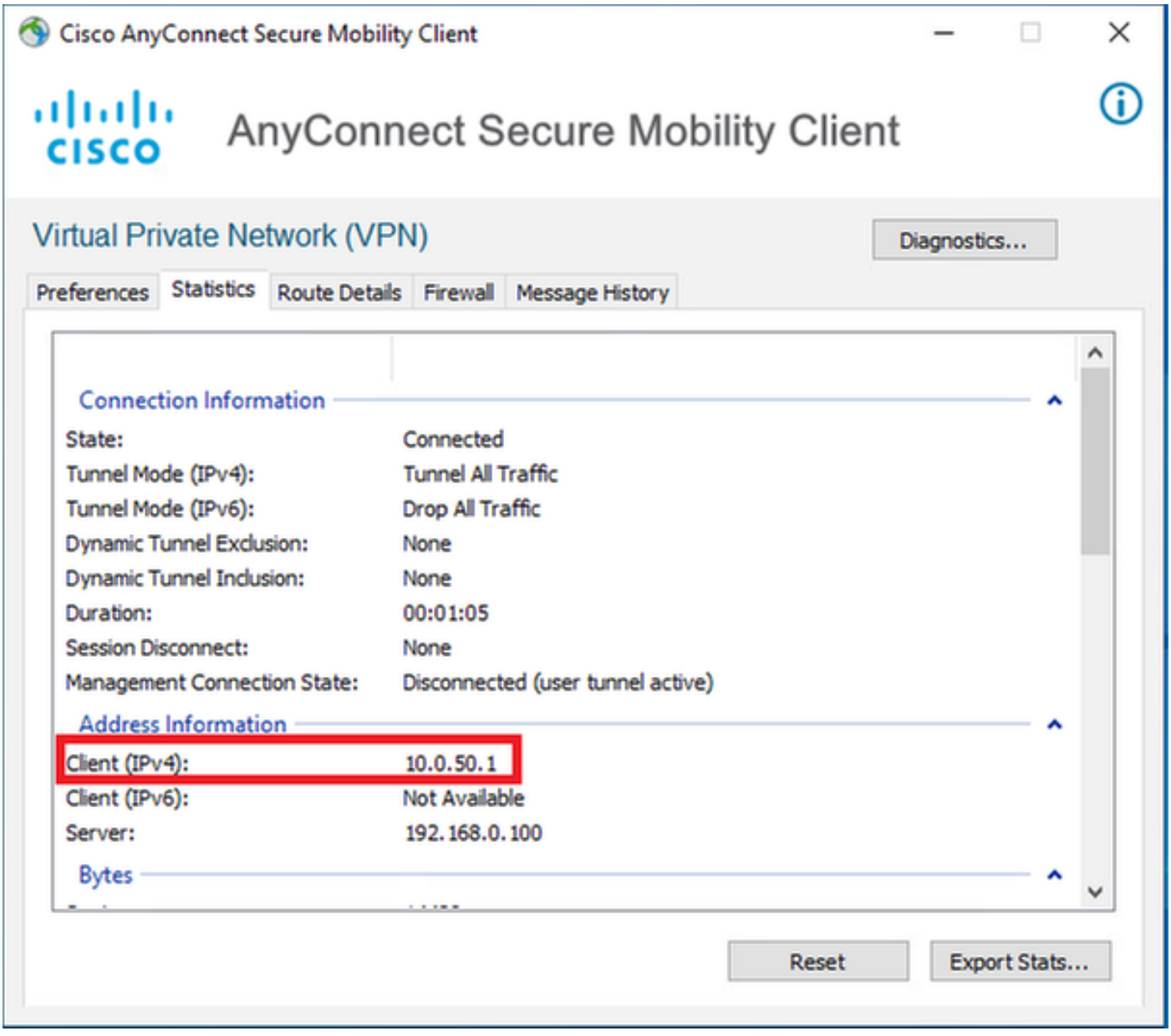
Die RADIUS Live-Protokolle auf der ISE zeigen Folgendes:



Schritt 2: Stellen Sie eine Verbindung zu Ihrem FTD-Headend her (hier wird ein Windows-Computer verwendet), und geben Sie die Anmeldeinformationen user2 ein.



Im Abschnitt Address Information (Adressinformationen) wird angezeigt, dass die zugewiesene IP-Adresse tatsächlich die erste verfügbare IP-Adresse im lokalen IPv4-Pool ist, der über FMC konfiguriert wurde.



Der Debugradius aller Befehle in FTD zeigt Folgendes an:

<#root>

```
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 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
```

Die FTD-Protokolle zeigen Folgendes:

<#root>

```
<omitted output>
Sep 22 2021 23:59:26: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.1
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 =
Sep 22 2021 23:59:35: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user
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[
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.radius[
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.g
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.u
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.u
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.t
Sep 22 2021 23:59:35: %FTD-6-734001: DAP: User user2, Addr 192.168.0.101, Connection AnyConnect: The fo
Sep 22 2021 23:59:35: %FTD-6-113039: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> AnyConnect p
<omitted output>
Sep 22 2021 23:59:52: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.1
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
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:
```

VPNFIP: 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
Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: callback failed during IPv
Sep 22 2021 23:59:52: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User <user2> IP <
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 SV
Sep 22 2021 23:59:52: %FTD-6-722022: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> TCP SVC conn
Sep 22 2021 23:59:52: %FTD-7-746012:

user-identity: Add IP-User mapping 10.0.50.1 - LOCAL\user2 Succeeded - VPN user

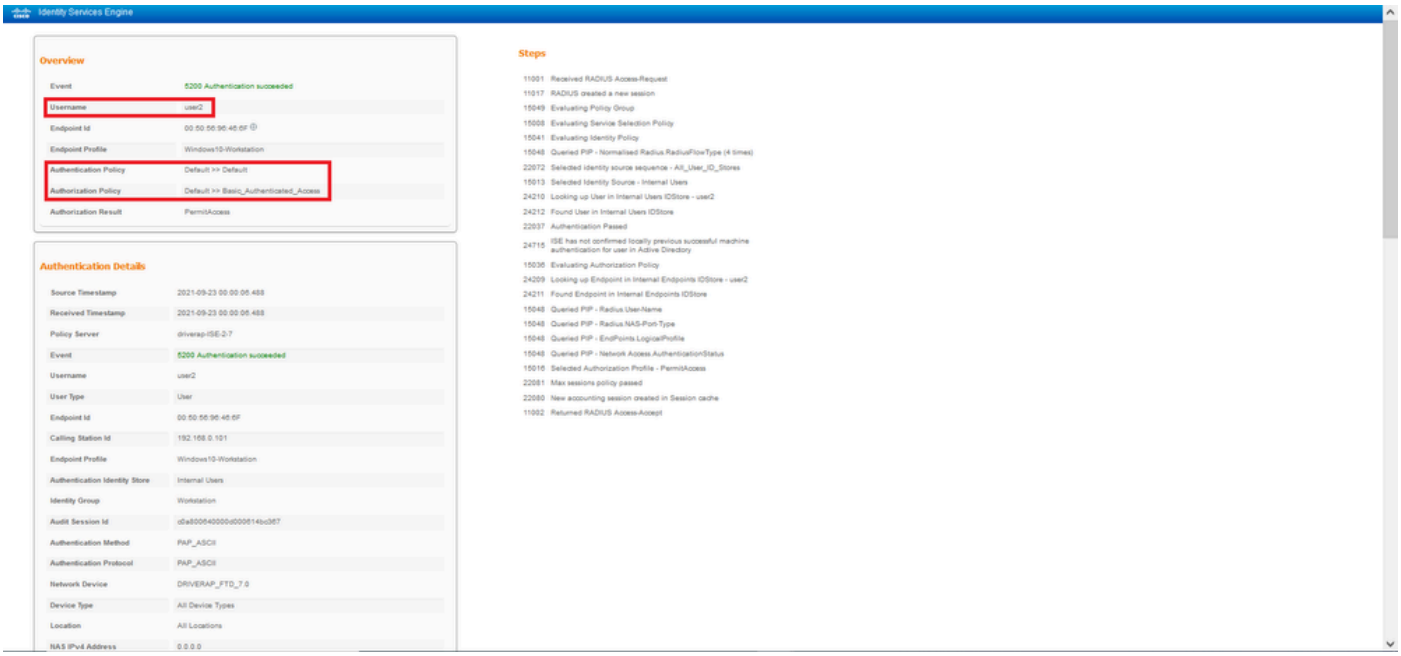
Sep 22 2021 23:59:52: %FTD-6-722055: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> Client Type:
Sep 22 2021 23:59:52: %FTD-4-722051:

Group

User

IP <192.168.0.101> IPv4 Address <10.0.50.1> IPv6 address <::> assigned to session

Die RADIUS Live-Protokolle auf der ISE zeigen Folgendes:



Anmerkung: Sie müssen unterschiedliche IP-Adressbereiche für die Zuweisung von IP-

Adressen sowohl für den lokalen FTD-IP-Pool als auch für die ISE-Autorisierungsrichtlinien verwenden, um doppelte IP-Adresskonflikte zwischen Ihren AnyConnect-Clients zu vermeiden. In diesem Konfigurationsbeispiel wurde FTD mit einem lokalen IPv4-Pool von 10.0.50.1 bis 10.0.50.100 konfiguriert, und der ISE-Server weist die statische IP-Adresse 10.0.50.101 zu.

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Auf FTD:

- debug radius all

Auf der ISE:

- RADIUS-Live-Protokolle

Informationen zu dieser Übersetzung

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