

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

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration eines Remote Access-VPN mit AAA/RADIUS-Authentifizierung über FMC](#)

[Konfigurieren der Verwendung des Autorisierungsservers auf dem FMC](#)

[Autorisierungsrichtlinie auf ISE \(RADIUS-Server\) konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

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

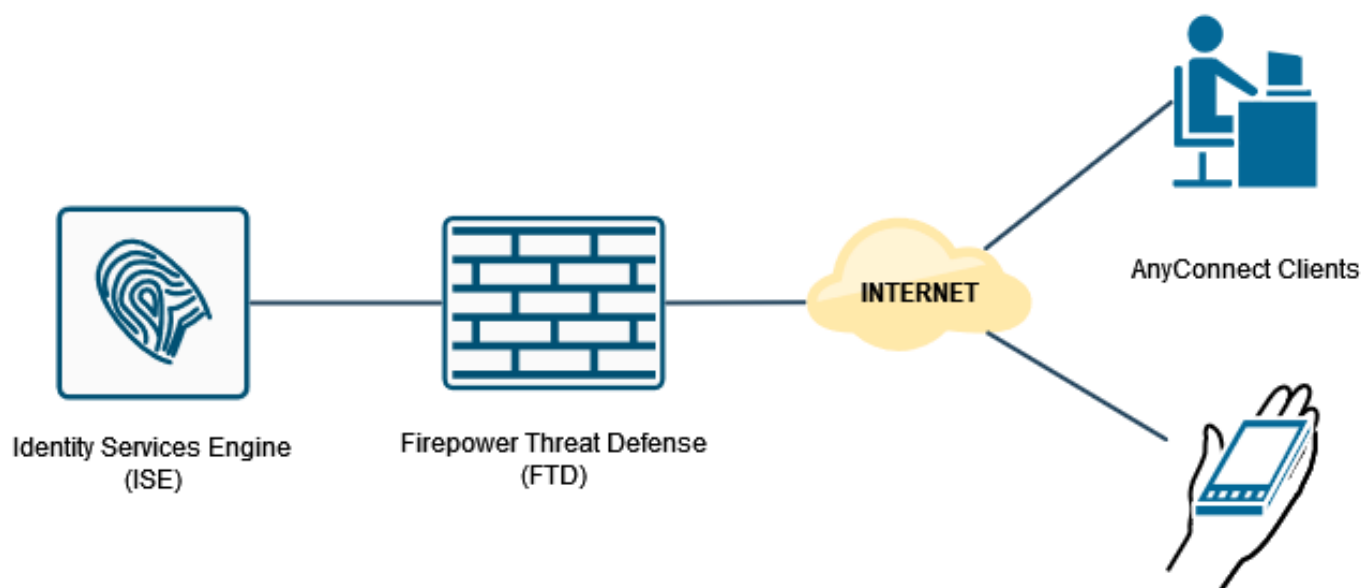
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- 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

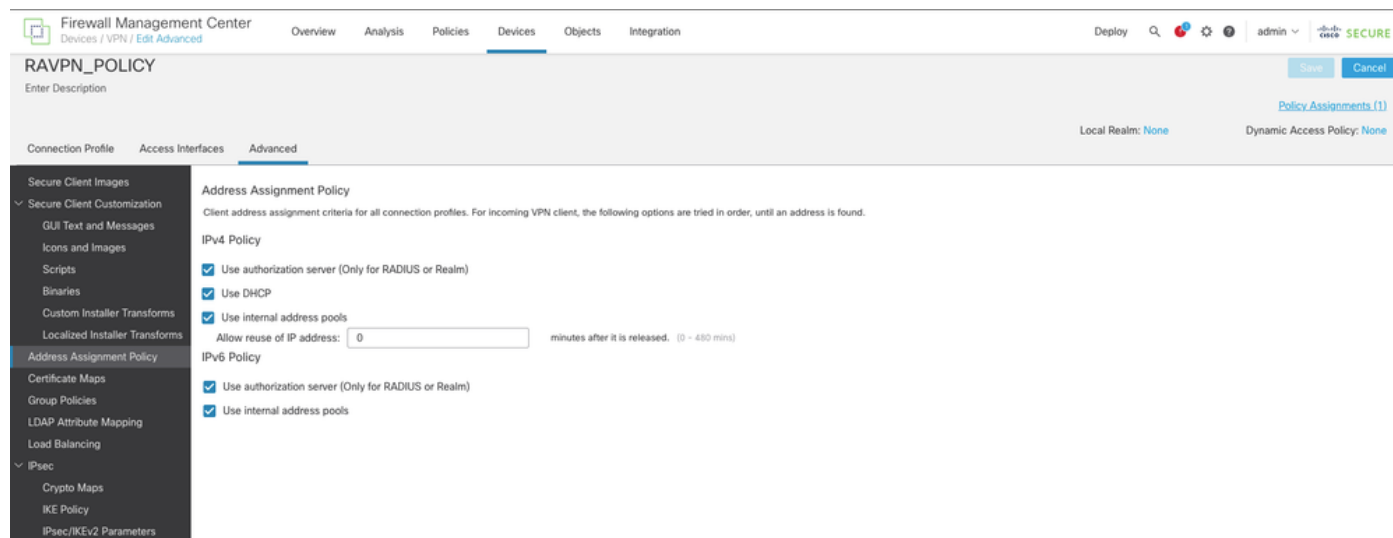
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev2 ssl-client
user-authentication-idle-timeout none
webvpn
anyconnect keep-installer none
anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry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

```

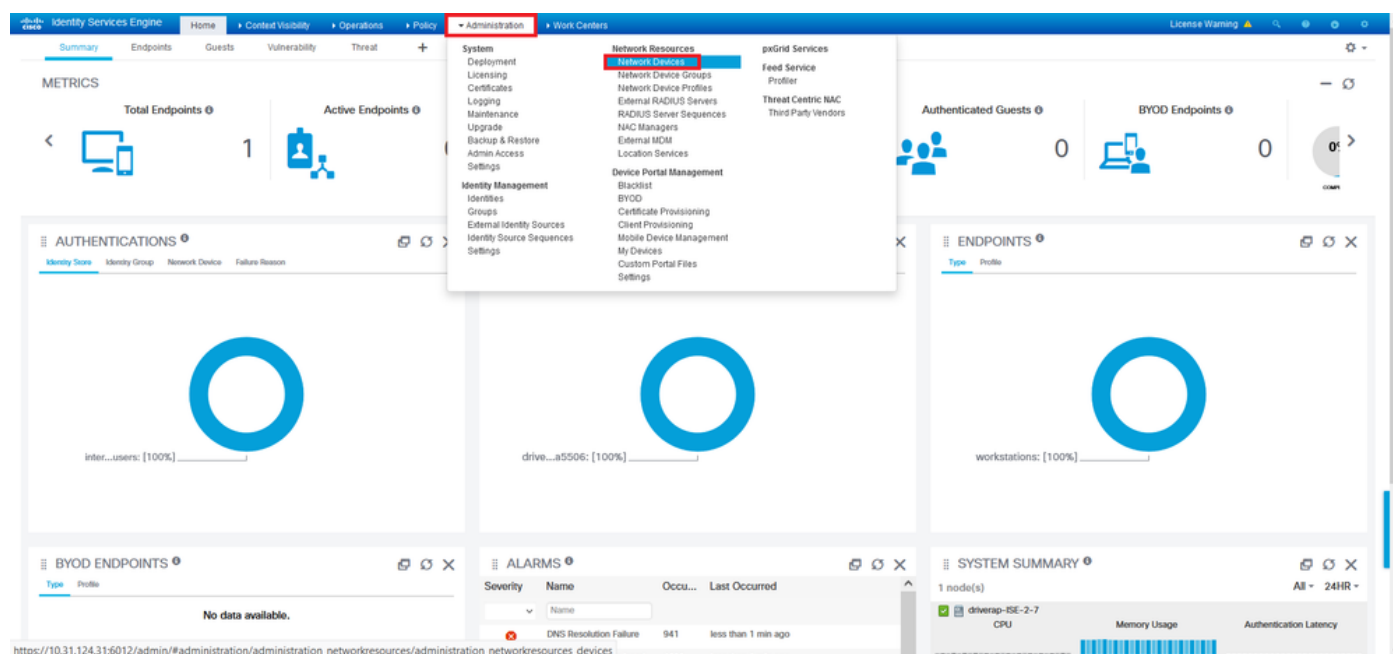
Konfigurieren der Verwendung des Autorisierungsservers auf dem FMC

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.

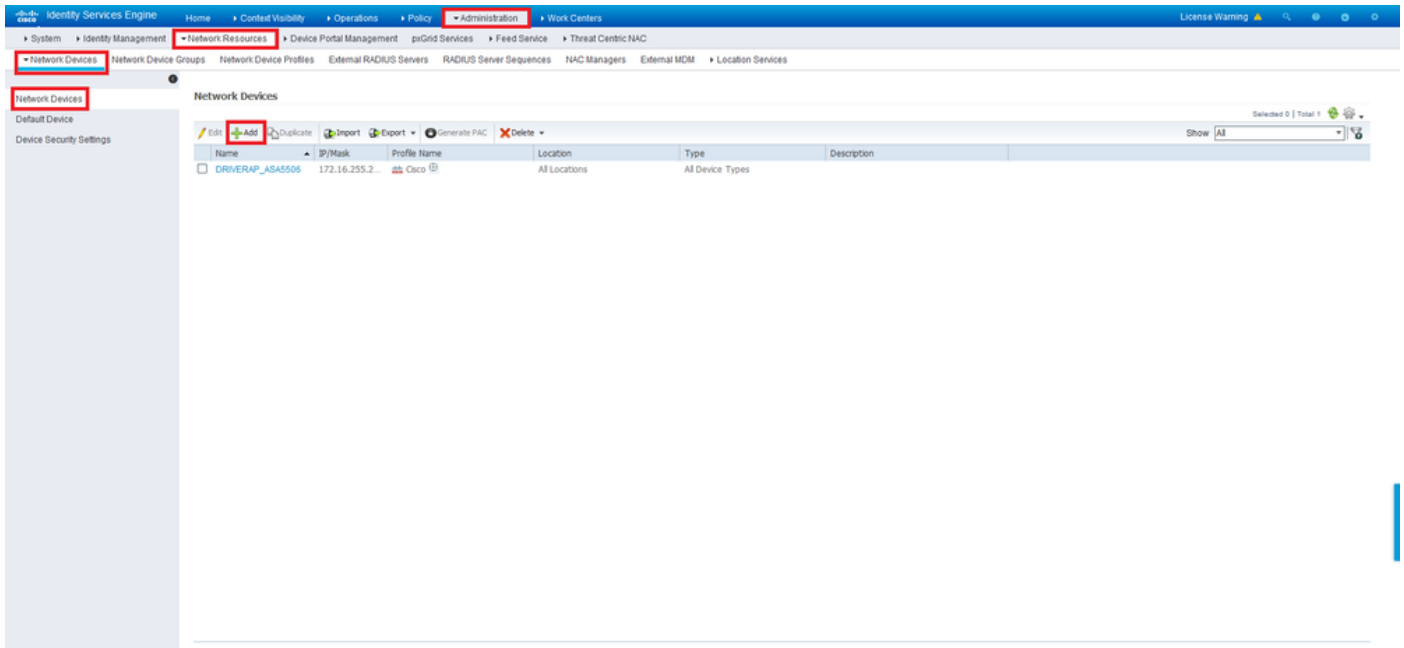


Autorisierungsrichtlinie auf ISE (RADIUS-Server) konfigurieren

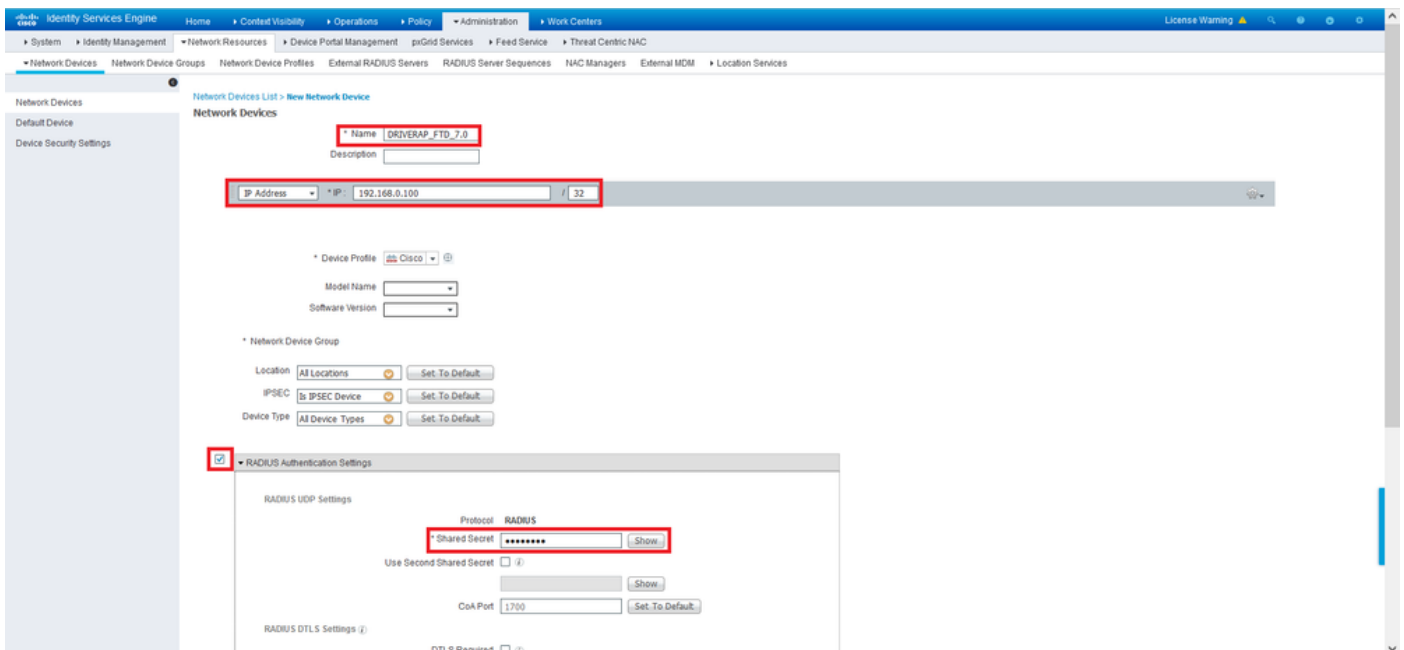
Schritt 1: Melden Sie sich beim ISE-Server an, und navigieren Sie zu Administration > Network Resources > Network Devices.



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

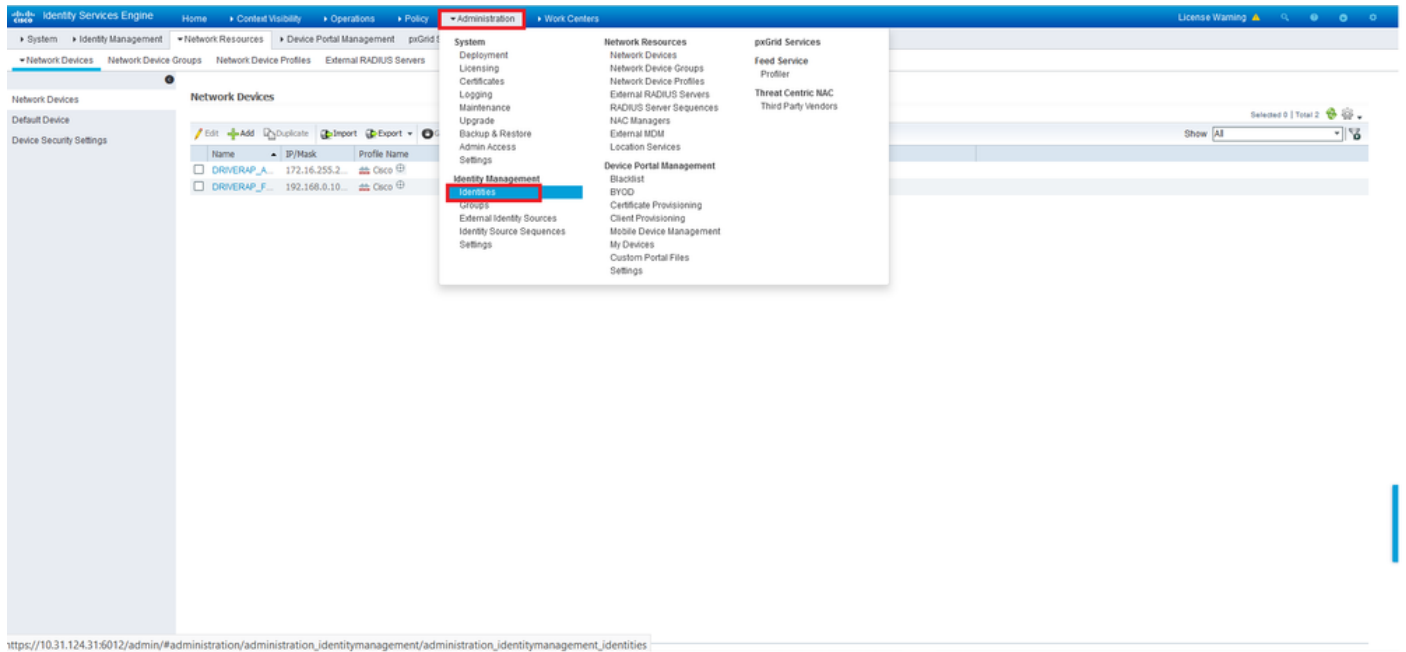


Geben Sie die Felder für den Netzwerkgerätenamen und die IP-Adresse ein, und aktivieren Sie das Kontrollkästchen RADIUS Authentication Settings (RADIUS-Authentifizierungseinstellungen). Der gemeinsame geheime Schlüssel muss derselbe Wert sein, der beim Erstellen des RADIUS-Serverobjekts auf dem FMC verwendet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

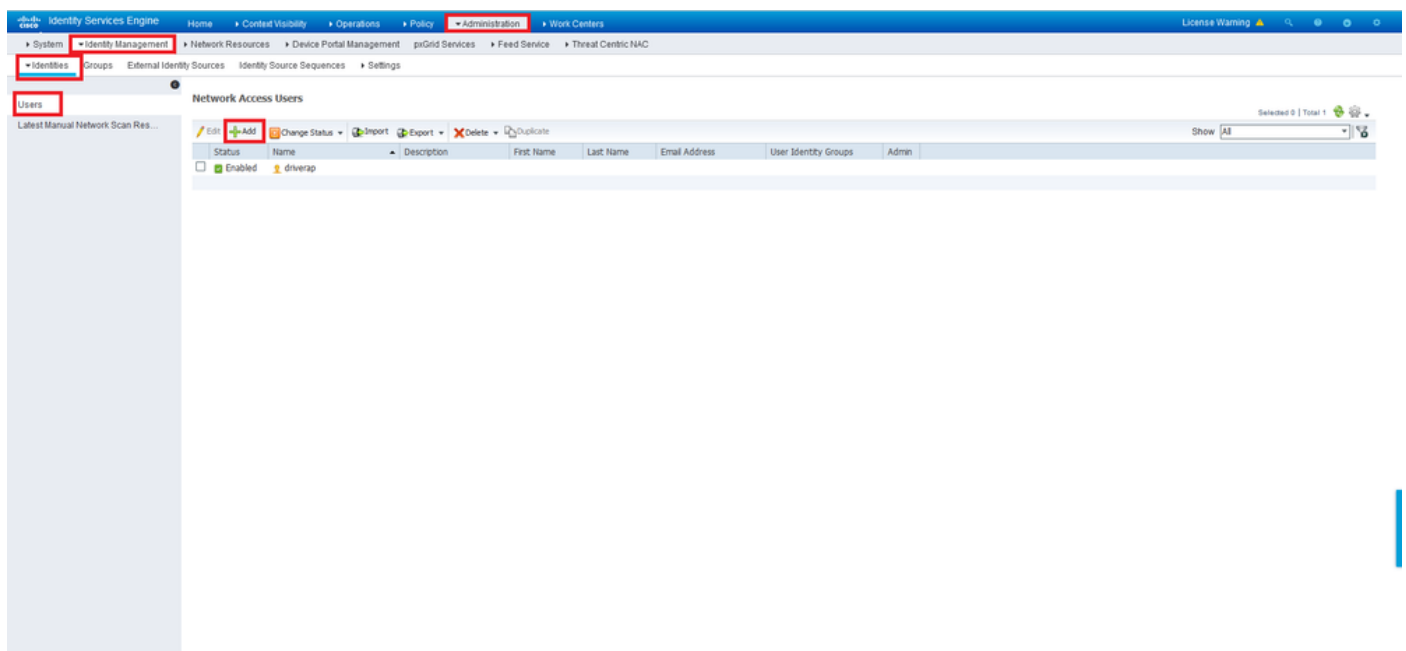


Speichern Sie es mit der Schaltfläche am Ende dieser Seite.

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.

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

Name:

Status: ☒ Enabled

Email:

Passwords

Password Type:

Password: Re-Enter Password:

Generate Password

Enable Password: Generate Password

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login: ☐

Account Disable Policy

Disable account if date exceeds: (yyy-mm-dd)

User Groups

Select an item

Submit Cancel

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

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

Users

Latest Manual Network Scan Res...

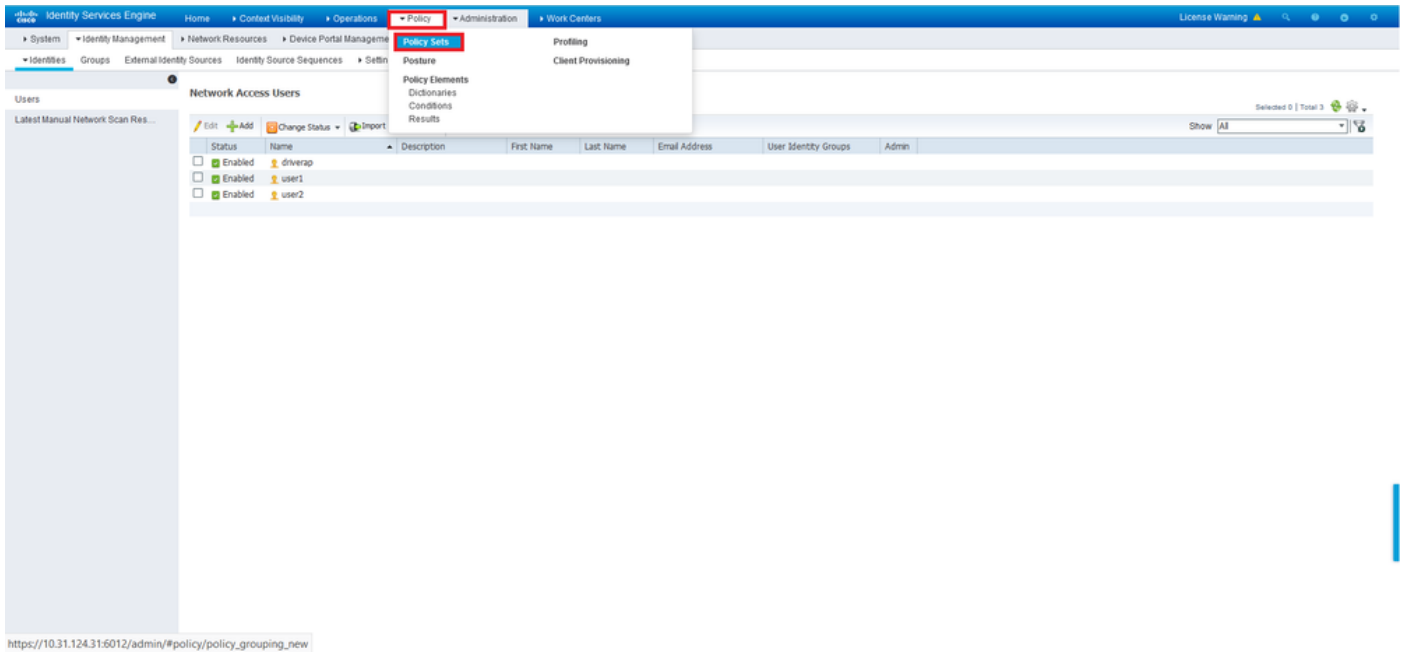
Network Access Users

Selected 0 | Total 3

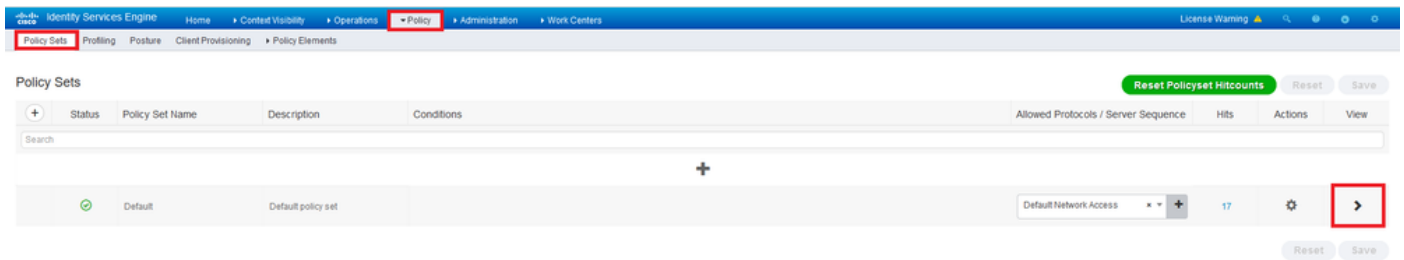
Show All

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
☒ Enabled	divergo						
☒ Enabled	user1						
☒ Enabled	user2						

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.

Identity Services Engine Home > Content Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Default

Reset Policyset Hitcounts Reset Save

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

Authentication Policy (3)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (13)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+						
✓	Wireless Black List Default	AND Wireless_Access IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	x Blackhole_Wireless_Access	Selected from list	0	⚙
✓	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco IP-Phone	x Cisco_IP_Phones	Selected from list	0	⚙
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	x Non_Cisco_IP_Phones	Selected from list	0	⚙
✓	Unknown_Compliance_Redirect	AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	x Cisco_Temporal_Onboard	Selected from list	0	⚙
✓	NonCompliant_Devices_Redirect	AND Network_Access_Authentication_Passed Non_Compliant_Devices	x Cisco_Temporal_Onboard	Selected from list	0	⚙

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

Authorization Policy (13)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+						
✓	Static IP Address User 1	+	Selected from list	Selected from list		⚙

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.

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_Profiling_Phones

Non_Compliant_Devices

Switch_Local_Web_Authentication

Switch_Web_Authentication

Editor

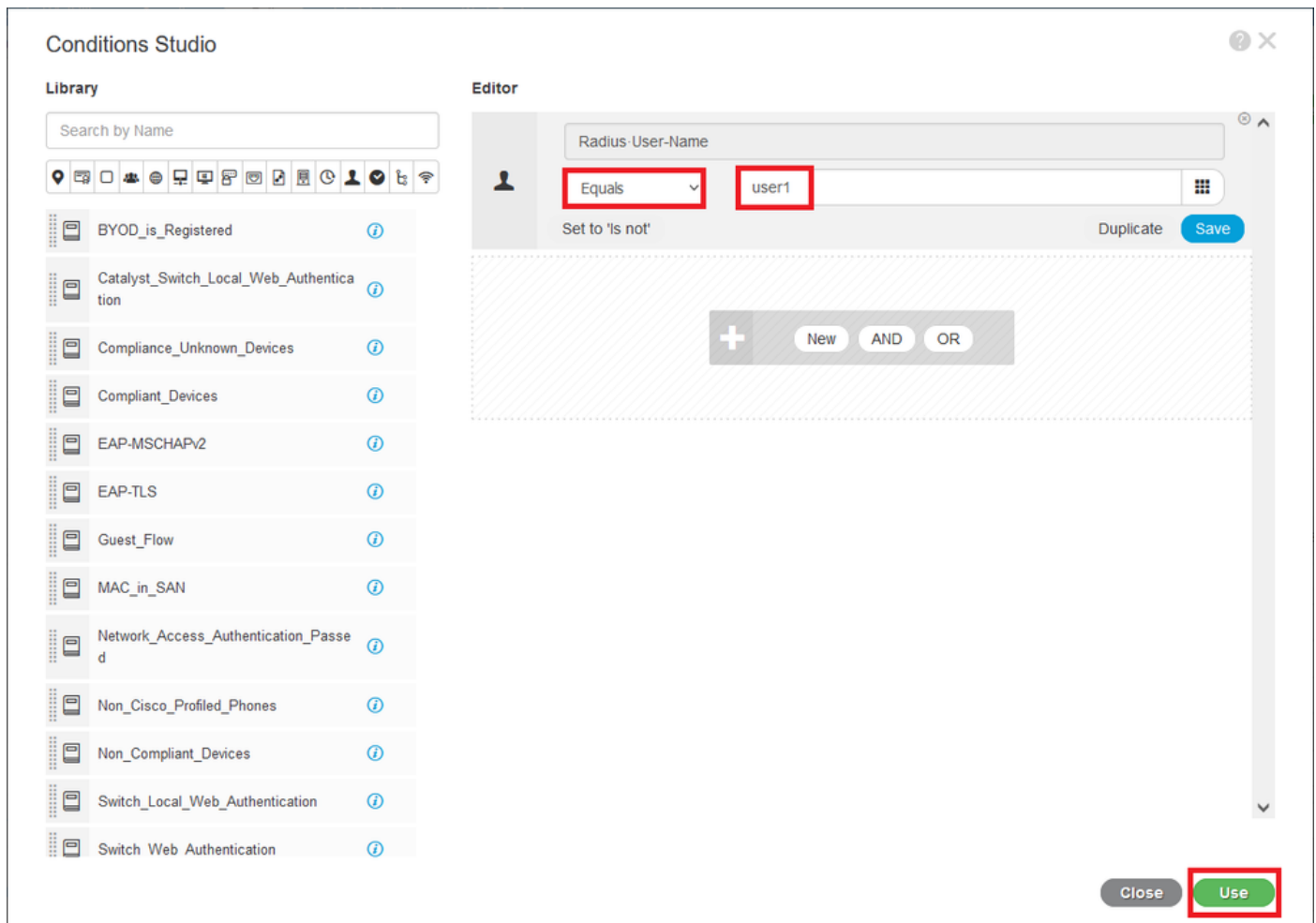
Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Microsoft	MS-HCAP-User-Name	60	
Motorola-Symbol	Symbol-User-Group	12	
Network Access	AD-User-DNS-Domain		
Network Access	AD-User-Join-Point		
Network Access	UserName		
PassiveID	PassiveID_Username		
Radius	User-Name	1	
Radius	User-Password	2	
Ruckus	Ruckus-User-Groups	1	

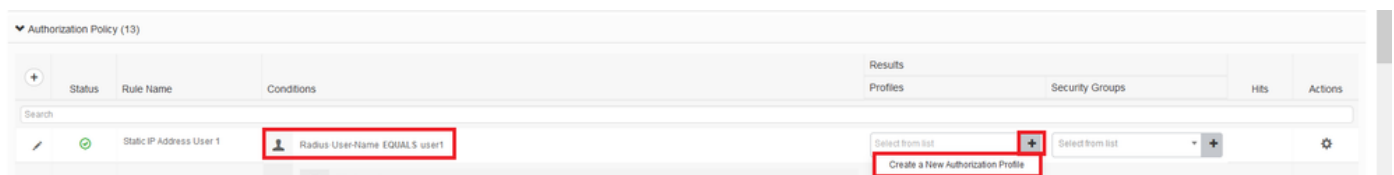
Close Use

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.

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

☐ DACL Name

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

Advanced Attributes Settings

< >

Save Cancel

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

Add New Standard Profile

Service Template: ☐

Track Movement: ☐ (i)

Passive Identity Tracking: ☐ (i)

Common Tasks

☐ DACL Name

☐ IPv6 DACL 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

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

Add New Standard Profile

Service Template ☐

Track Movement ☐ (i)

Passive Identity Tracking ☐ (i)

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**

Schritt 10: Wählen Sie nun das neu erstellte Autorisierungsprofil.

Authorization Policy (13)

	Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+	✓	Static IP Address User 1	Radius-User-Name EQUALS user1	Selected from list	Selected from list		⚙
+	✓	Wireless Black List Default	AND Wireless_Access IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	DenyAccess	Selected from list	0	⚙
+	✓	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled-Cisco-IP-Phone	NSP_Onboard	Selected from list	0	⚙
+	✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones PermitAccess	Selected from list	0	⚙
				StaticIPAddressUser1	Selected from list	0	⚙
				Static_IP_address			

Die Autorisierungsregel ist jetzt festgelegt. Klicken Sie auf Speichern.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

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

Authentication Policy (3)

Authorization Policy - Local Exceptions

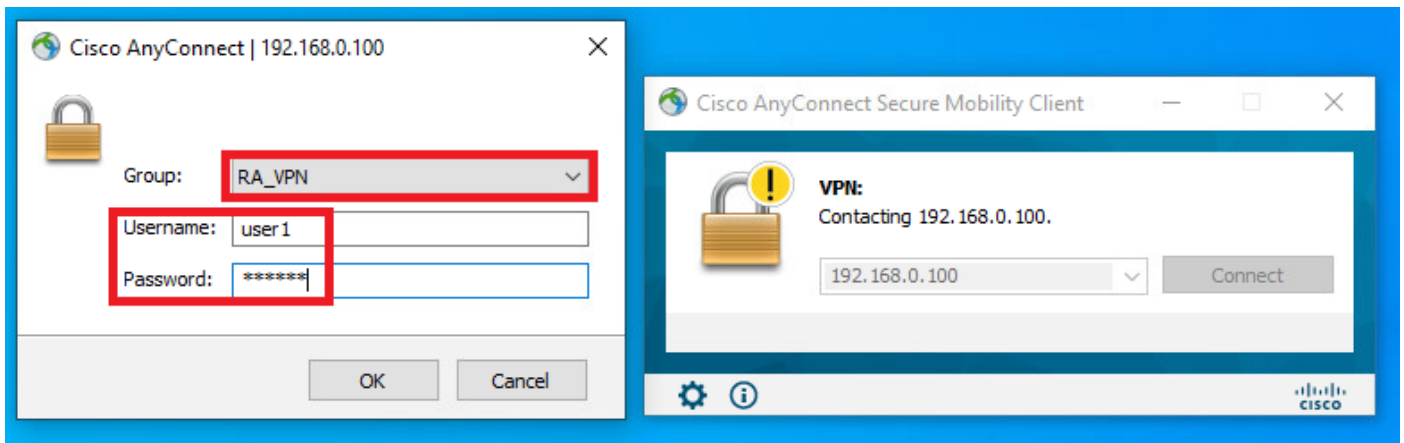
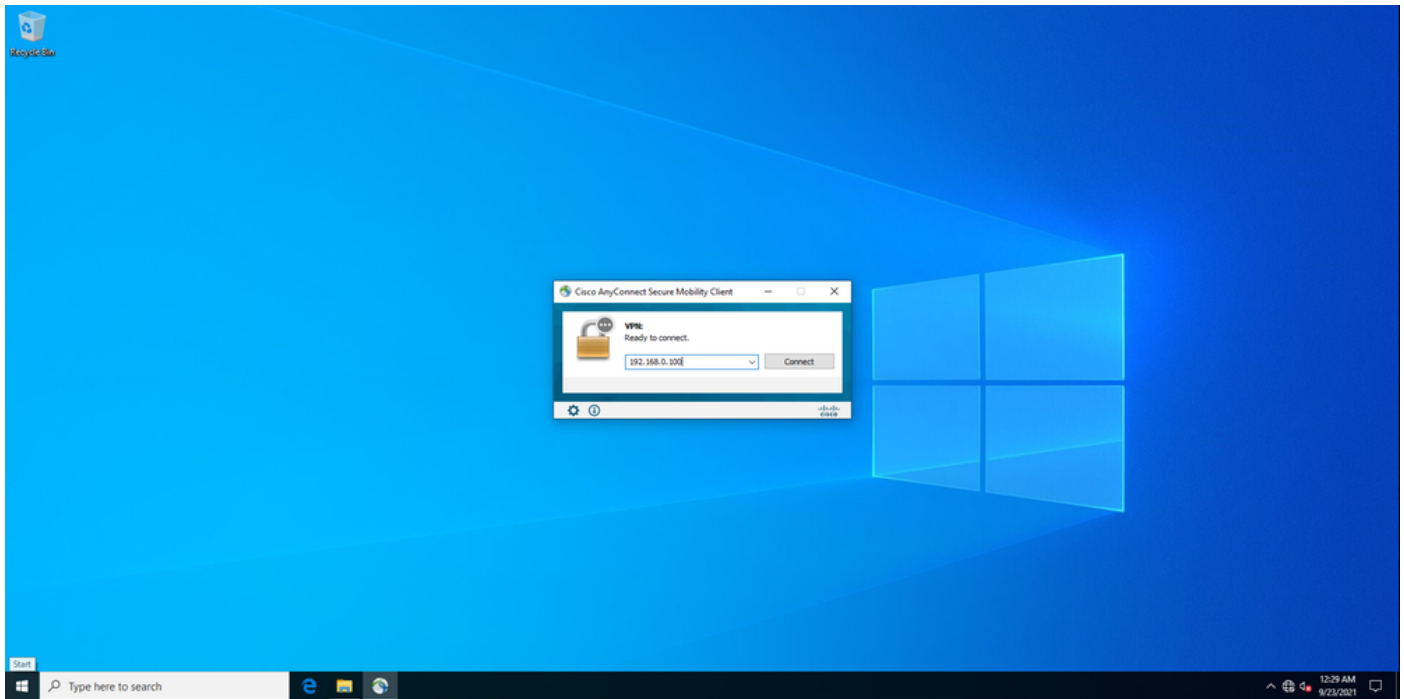
Authorization Policy - Global Exceptions

Authorization Policy (13)

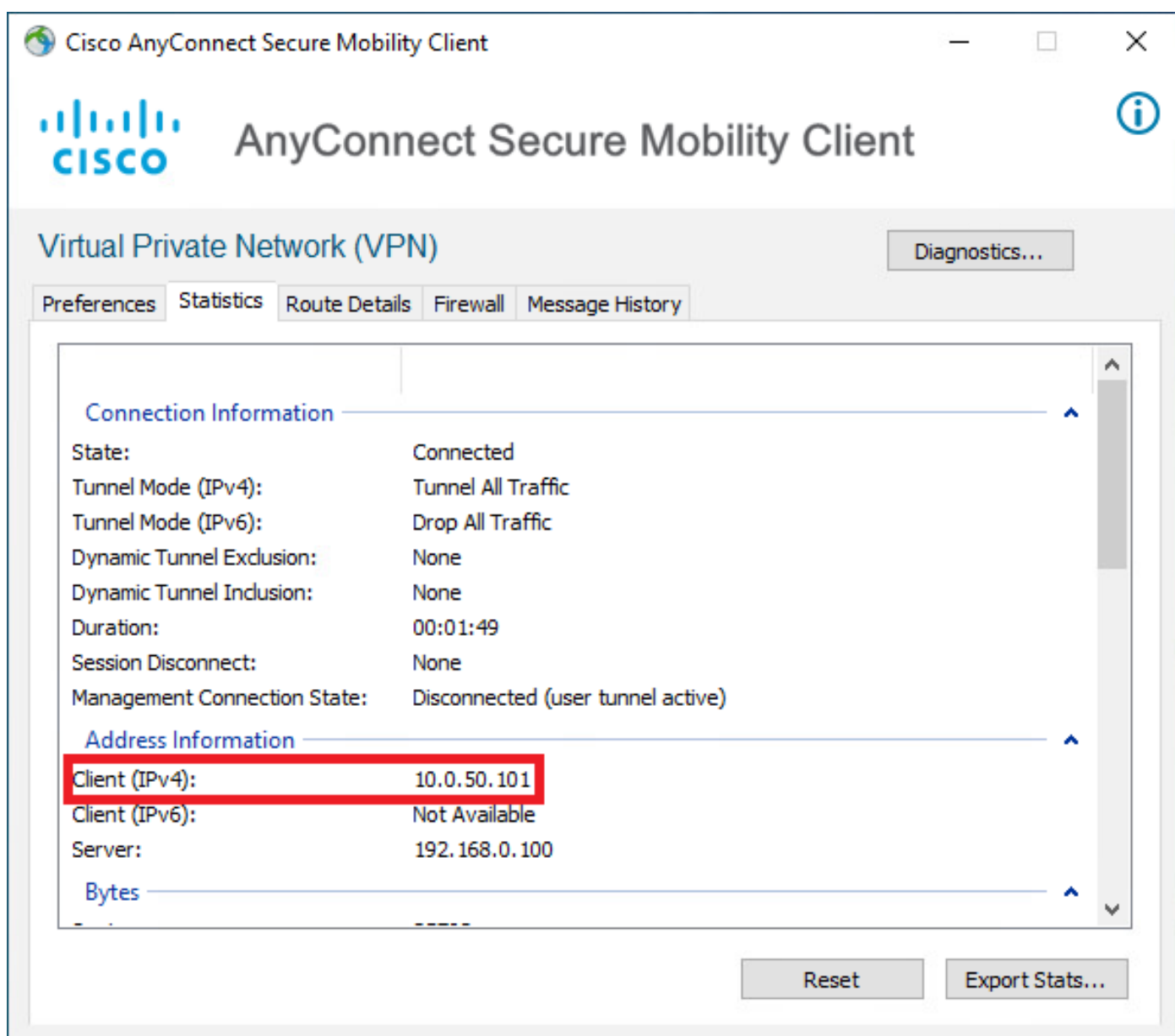
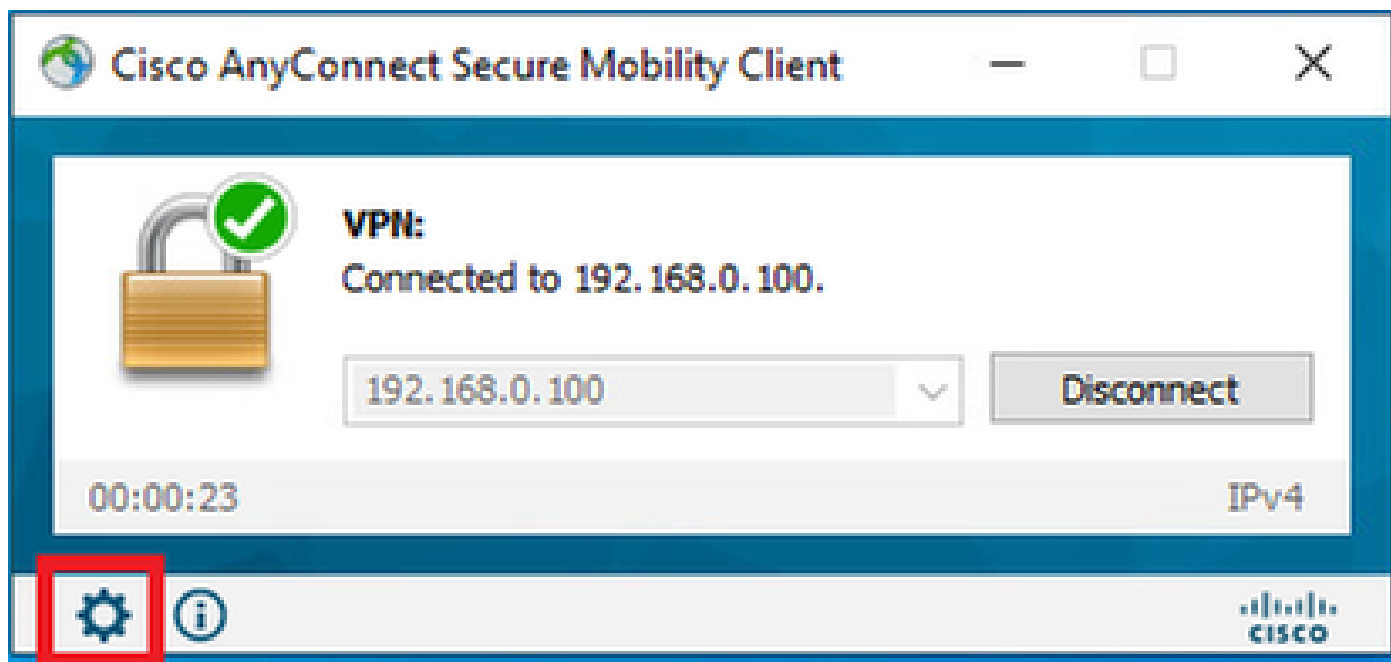
	Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+	✓	Static IP Address User 1	Radius-User-Name EQUALS user1	StaticIPAddressUser1	Selected from list		⚙

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.



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:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint ID	00:50:55:95:45:0F:0
Endpoint Profile	Windows10-Workstation
Authentication 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	drivewap-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint ID	00:50:55:95:45:0F:0
Calling Station ID	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session ID	d8a300540000d00014bctd0
Authentication Method	PAP_AKSC8
Authentication Protocol	PAP_AKSC8
Network Device	DRIVERAP_FTD_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
15050 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15040 Queried PIP - Normalised Radius RadiusFlowType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
15010 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
24719 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
24219 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - Radius UserName
15010 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	145
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel Client Endpoint	(lag=0) 192.168.0.101
CVPN3000ASA/POFX-Tunnel-Group-Name	RA_VPN
OriginalUsername	user1
NetworkDeviceProfileId	b0c09505-3150-4215-a80e-0753a45b5b0c
IsThirdPartyDeviceFlow	false
CVPN3000ASA/POFX-Client-Type	2
AccSessionID	drivewap-ISE-2-7-1417494978-23
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_join_Points
SelectedAuthenticationIdentity Stores	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

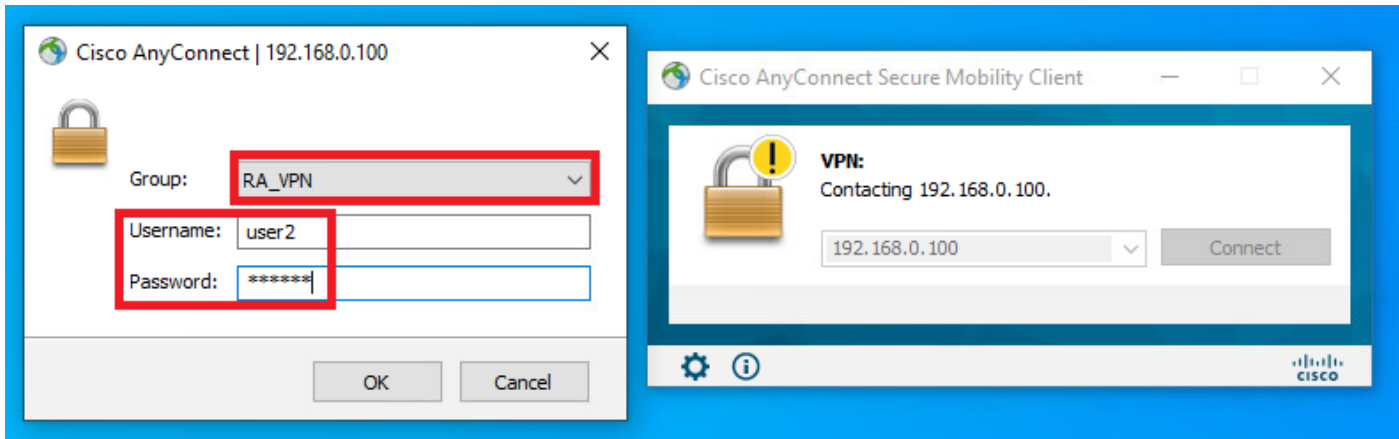
IPSEC	IPSECOnly IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM Session ID	d8a300540000d00014bctd0
Called Station ID	192.168.0.100
CiscoNPair	mdu-mdu-device-platform=main, mdu-mdu-device-manufacturer=00:50:55:95:45:0F:0, mdu-mdu-device-platform-version=10.0.18362, mdu-mdu-device-public-name=00:50:55:95:45:0F:0, mdu-mdu-device-user-agent=AnyConnect Windows 4.10.02086, mdu-mdu-device-type=VMware, Inc. VMware Virtual Platform, mdu-mdu-device-uid= global=153788E0C0F6273F2C0E2431456F4BA2A2E05B3, mdu-mdu-device- user=0C38407071F80782F810F1240211B440B596C717E370386C030F 94a3C0685C044, audit-session-id=d8a300540000d00014bctd0, ip-source-ip=192.168.0.101, ise-push=true

Result

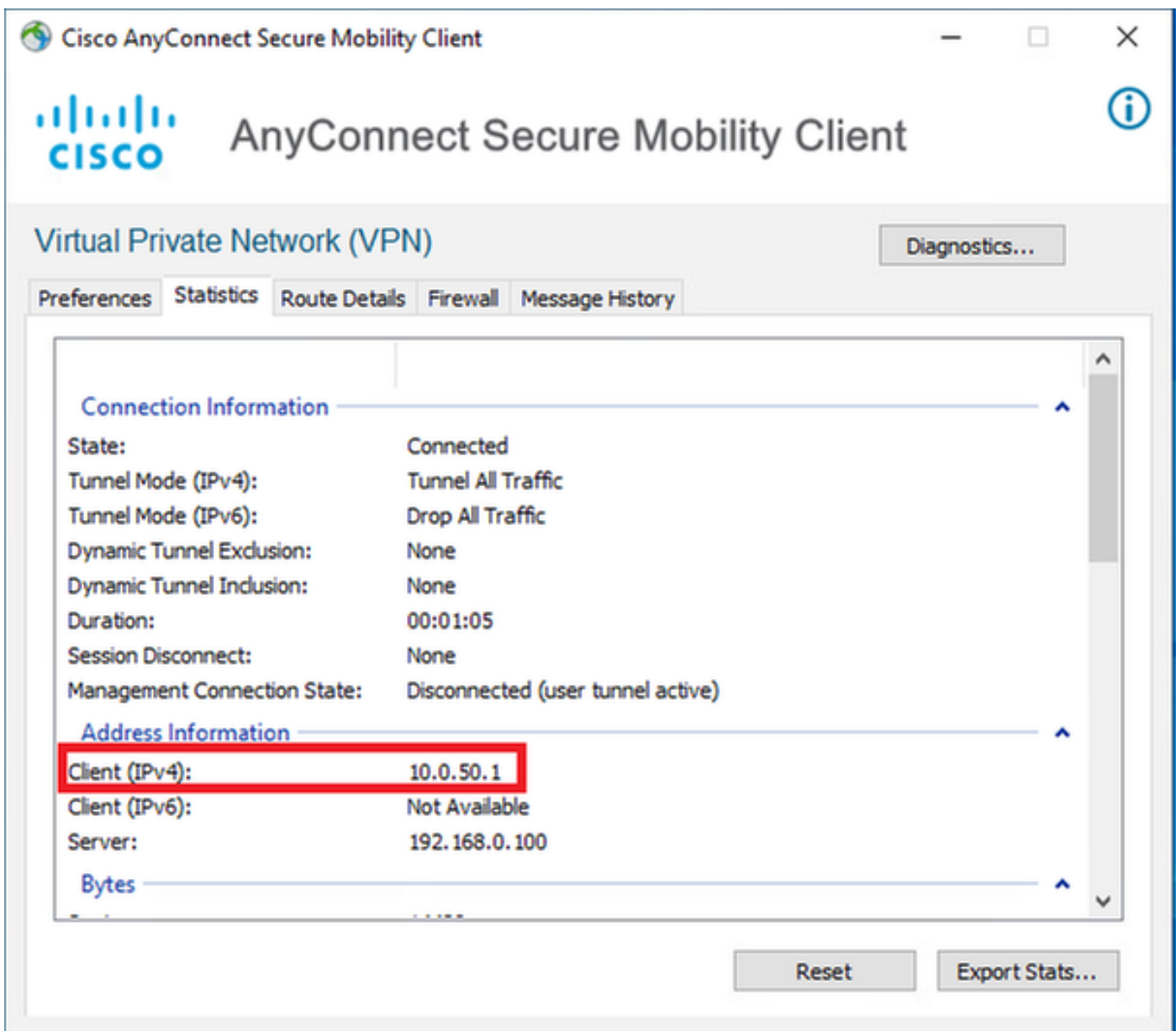
Framed IP Address	10.0.50.101
Class	CAC3-d8a300540000d00014bctd0-drivewap-ISE-2-7-1417494978-23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Session Events

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 | ...0..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 = 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[
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 IPv6

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:

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 00:00:05.488
Received Timestamp	2021-09-23 00:00:05.488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	00:50:56:96:45:6F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	ida00040000d00014bc367
Authentication Method	PAP_ACS
Authentication Protocol	PAP_ACS
Network Device	DRIVERAP_FTD_7.9
Device Type	All Device Types
Location	All Locations
NAS IP Address	0.0.0.0

Steps

11001 Received RADIUS Access-Request

11017 RADIUS created a new session

15049 Evaluating Policy Group

15058 Evaluating Service Selection Policy

15041 Evaluating Identity Policy

15048 Queried PIP - Normalised Radius RadiusFlowType (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 - user2

24212 Found User in Internal Users IDStore

22037 Authentication Passed

24719 ISE has not confirmed locally previous successful machine authentication for user in Active Directory

15036 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 Logical Profile

15048 Queried PIP - Network Access Authentication Status

15016 Selected Authorization Profile - PermitAccess

22081 Max sessions policy passed

22080 New accounting session created in Session cache

11002 Returned RADIUS Access-Accept

Identity Services Engine

NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	282 milliseconds

Other Attributes

ConfigVersionId	145
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel Client Endpoint	(lag=0) 192.168.0.101
CVRN3000/ASA/PIX/7+ Tunnel Group Name	RA_VPN
OriginalUsername	user2
NetworkDeviceProfileId	b0599505-3150-4215-a80e-6753e4b0f5bc
IsThirdPartyDeviceFlow	false
CVRN3000/ASA/PIX/7+ Client Type	2
Acx SessionId	driverap-ISE-2-7-1417494978-24
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_Ad_join_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
OTLS 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#No
Name	Endpoint Identity Groups Profiled Workstation
EnableFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPM SessionId	ida00040000d00014bc367
Called Station Id	192.168.0.100
CiscoAVPair	mfm:dv:device:platform:mfm:dv:device:mac:00:50:56:96:45:6f:mfm:dv:device:platform:version:15.0.18352:mfm:dv:device:public:map:00:50:56:96:45:6f:mfm:dv:device:agent:day:Connect:Windows 4 10 52088:mfm:dv:device:type:V/Mware, Inc. V/Mware Virtual Platform:mfm:dv:device:uid:globaem159f88e00cf32f2c0e2431456f48aa2ae2c083:mfm:dv:device:uid:3c38427071f807b2f816f124521184408596c717e370388cc03cf9445c882044:auth:session:ida00040000d00014bc367:(0) source-ip=192.168.0.101, (0) source-mac=

Result

Class	CACS ida00040000d00014bc367 driverap-ISE-2-7-1417494978-24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Session Events



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.