

# Configure Static IP Address Assignment to AnyConnect Users via RADIUS Authorization

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configure Remote Access VPN with AAA/RADIUS Authentication via FMC](#)

[Configure Authorization Policy on ISE \(RADIUS Server\)](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes how to configure RADIUS Authorization with an Identity Services Engine (ISE) server so it always forwards the same IP address to the Firepower Threat Defense (FTD) for a specific Cisco AnyConnect Secure Mobility Client user via the RADIUS Attribute 8 Framed-IP-Address.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

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

### Components Used

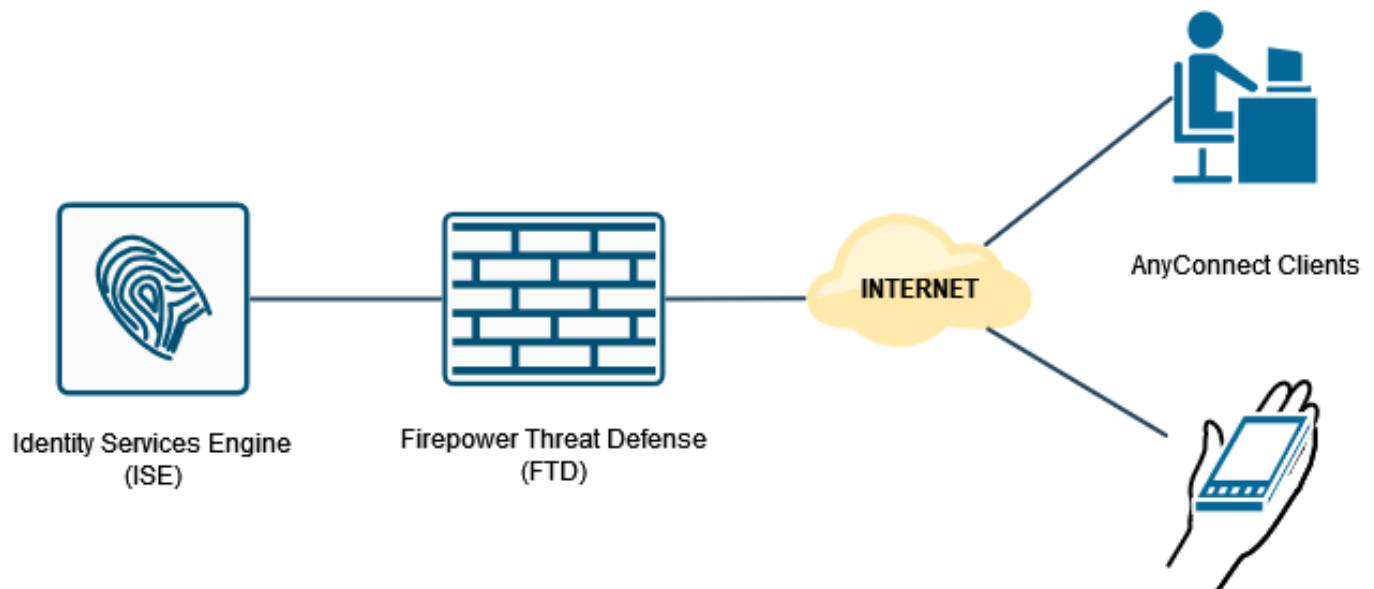
The information in this document is based on these software versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

### Network Diagram



### Configure Remote Access VPN with AAA/RADIUS Authentication via FMC

For a step-by-step procedure, refer to this document and this video:

- [AnyConnect Remote Access VPN Configuration on FTD](#)
- [Initial AnyConnect Configuration for FTD Managed by FMC](#)

Remote Access VPN configuration on the 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

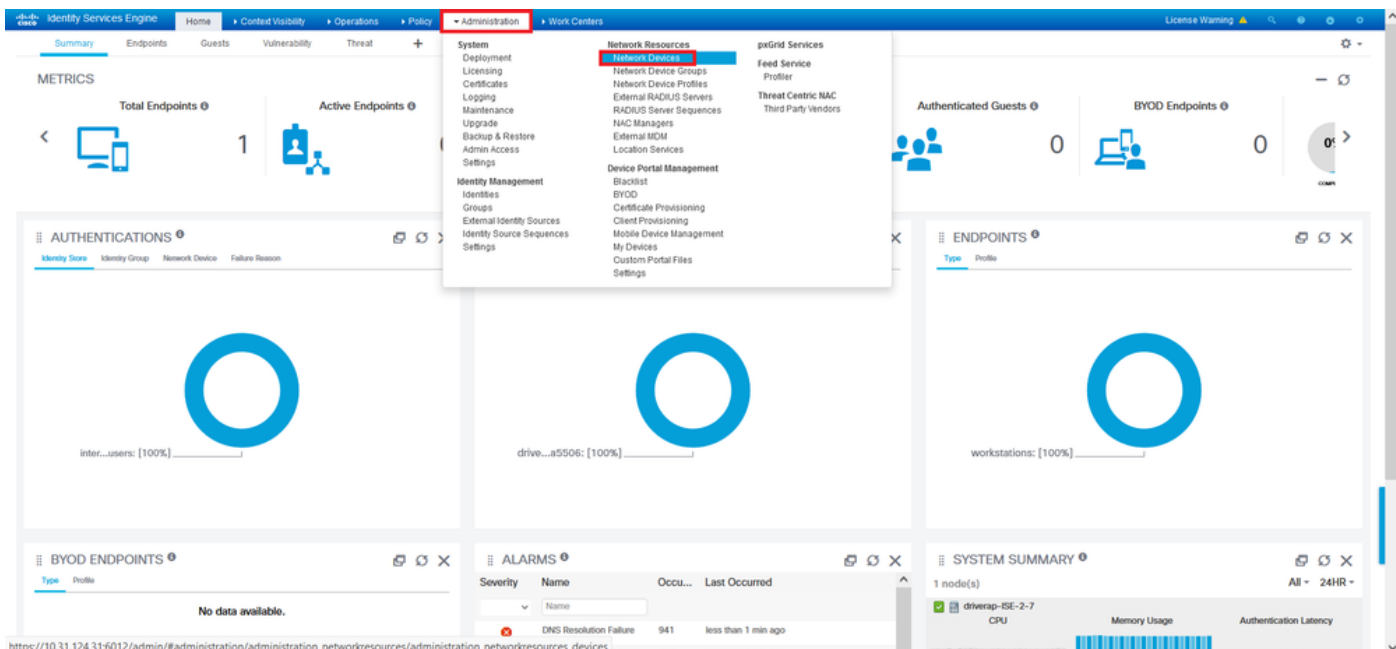
webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list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

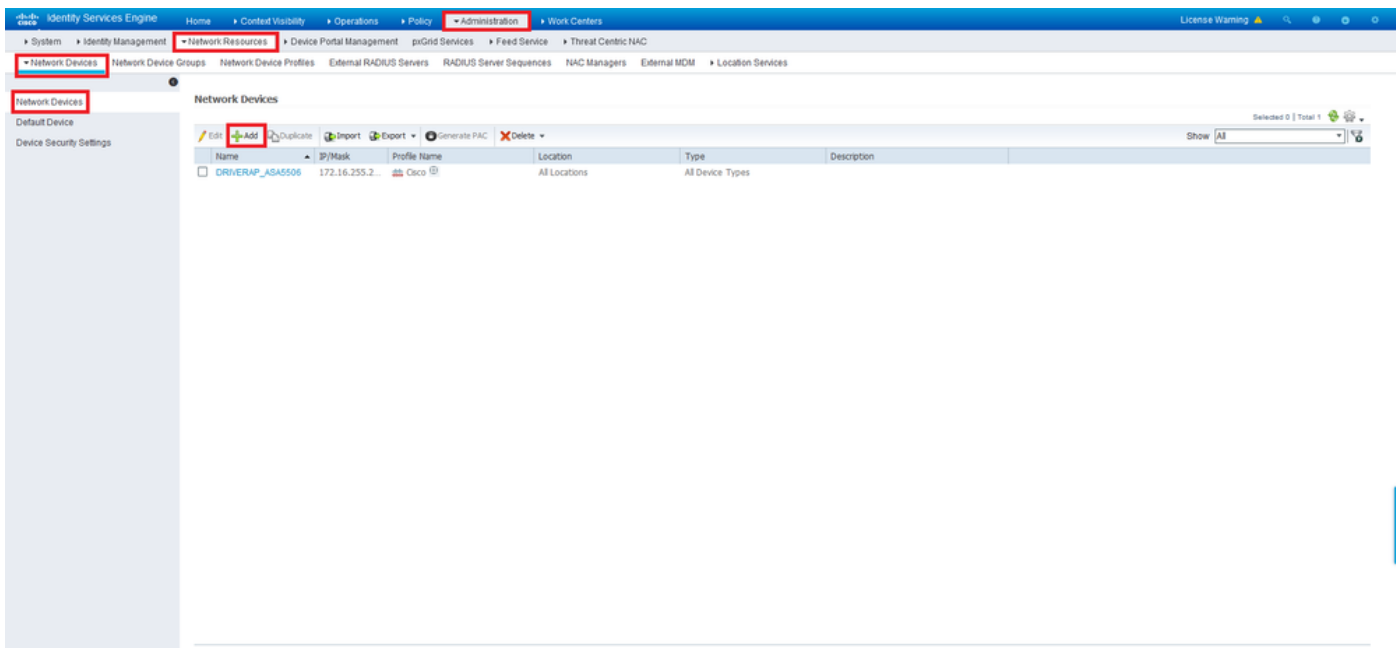
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

## **Configure Authorization Policy on ISE (RADIUS Server)**

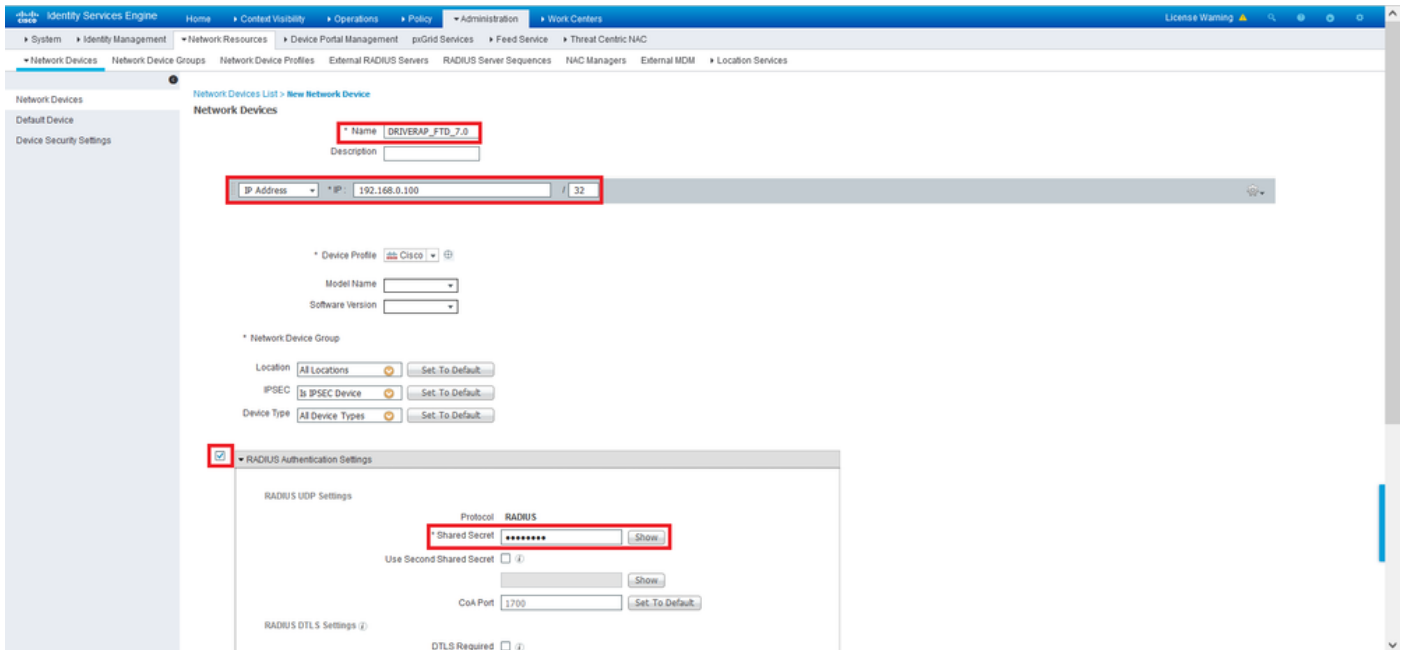
Step 1. Log in to the ISE server and navigate to **Administration > Network Resources > Network Devices**.



Step 2. In the Network Devices section, click **Add** so ISE can process RADIUS Access Requests from the FTD.

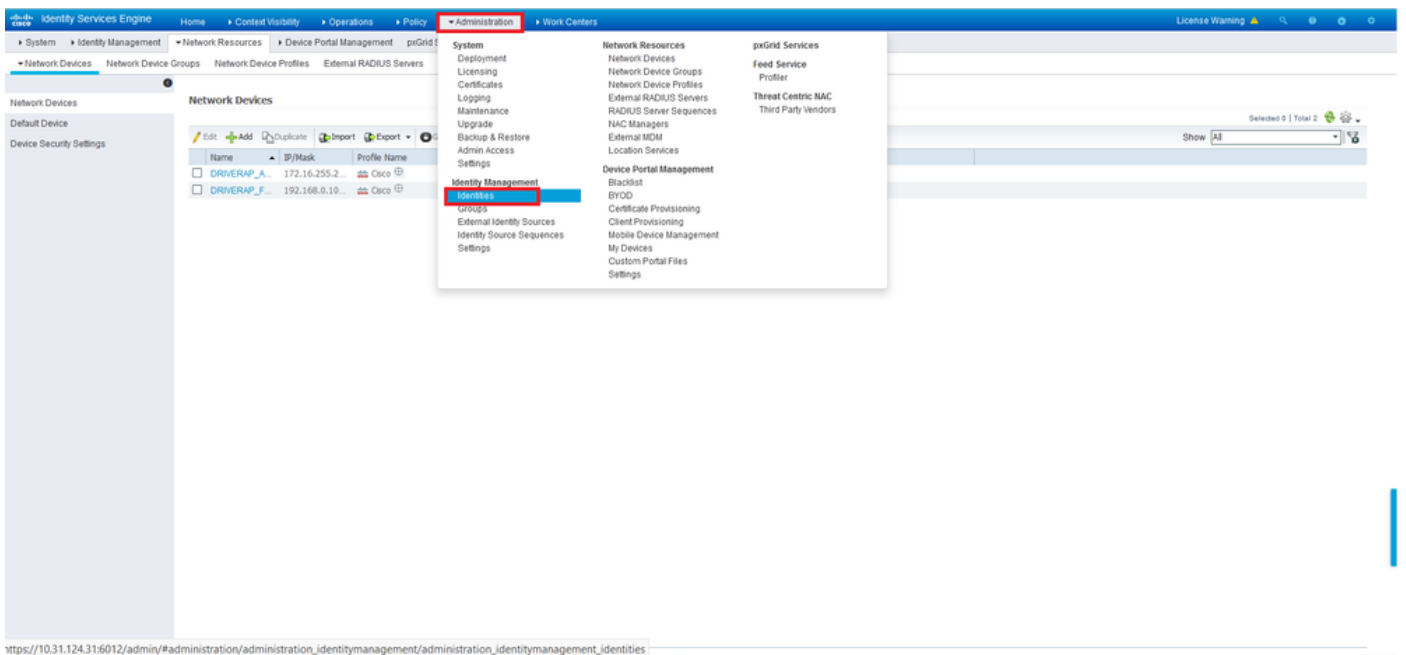


Enter the network device **Name** and **IP Address** fields and then check **RADIUS Authentication Settings** box. The **Shared Secret** must be the same value that was used when the RADIUS Server object on FMC was created.

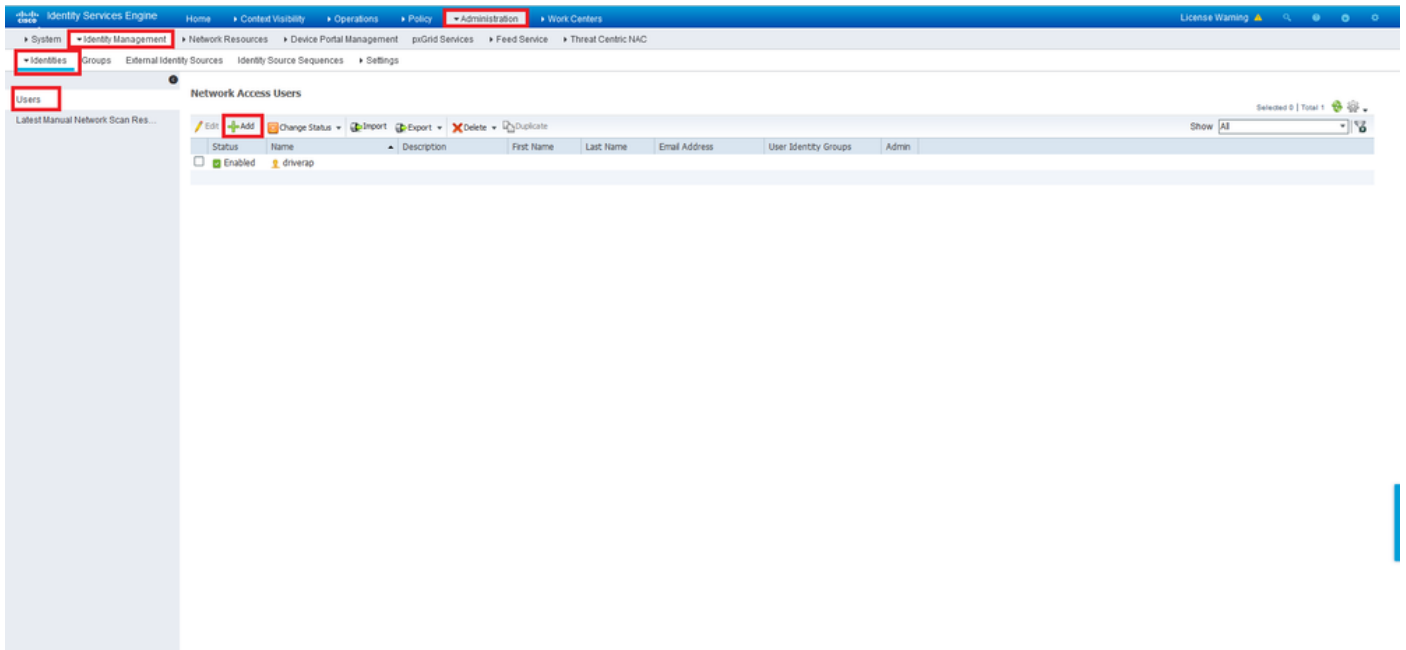


Save it with the button at the end of this page.

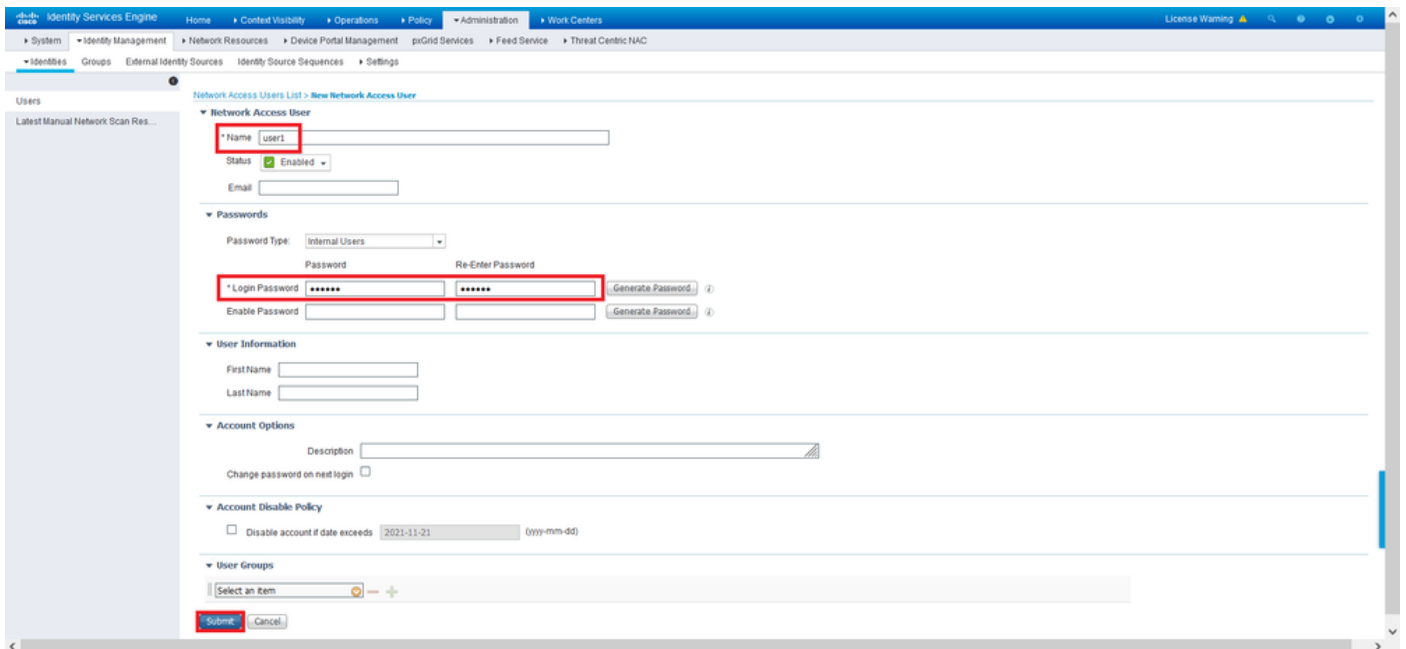
Step 3. Navigate to **Administration > Identity Management > Identities**.



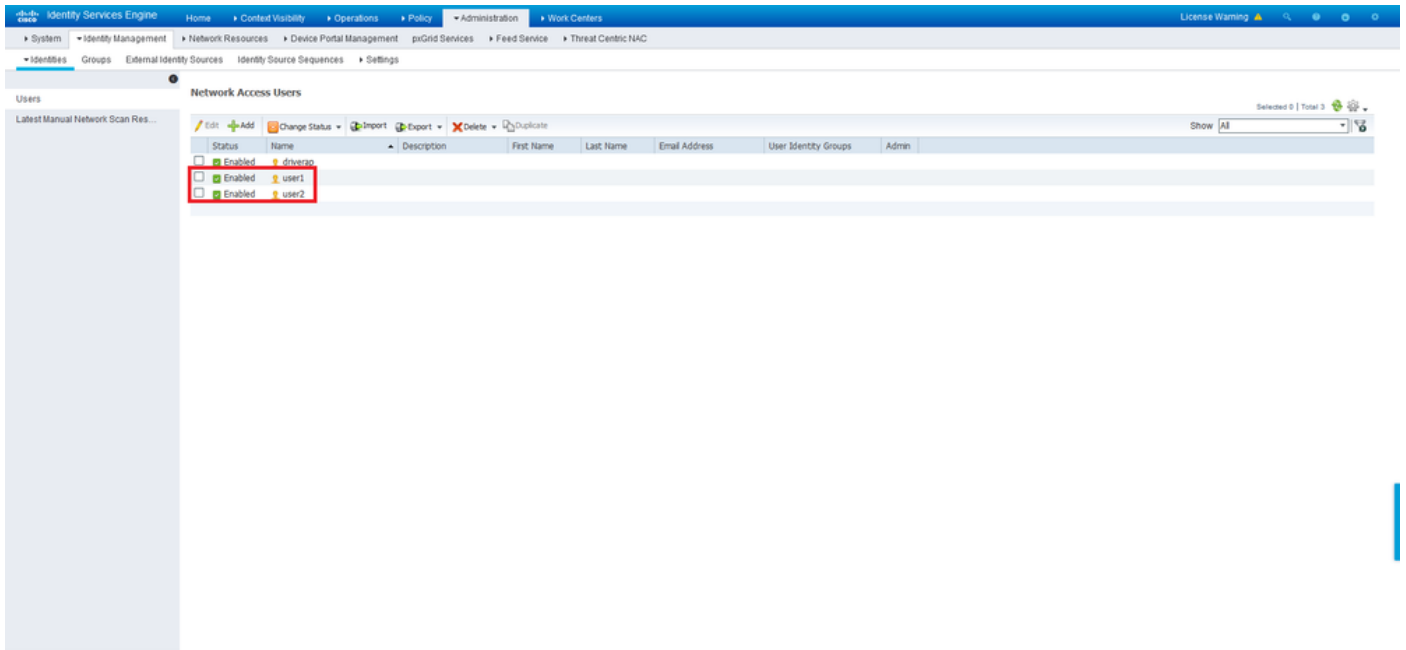
Step 4. In the Network Access Users section, click **Add** in order to create *user1* in ISE's local database.



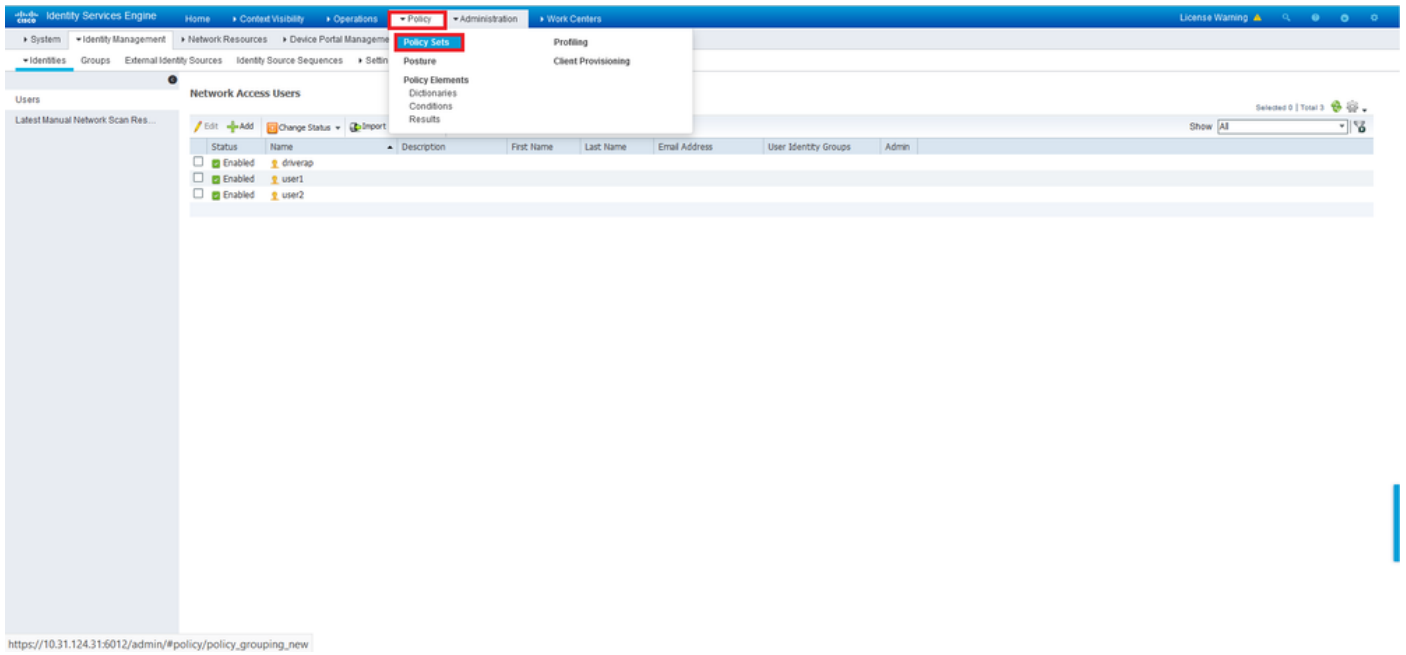
Enter username and password in the **Name** and **Login Password** fields, and then click **Submit**.



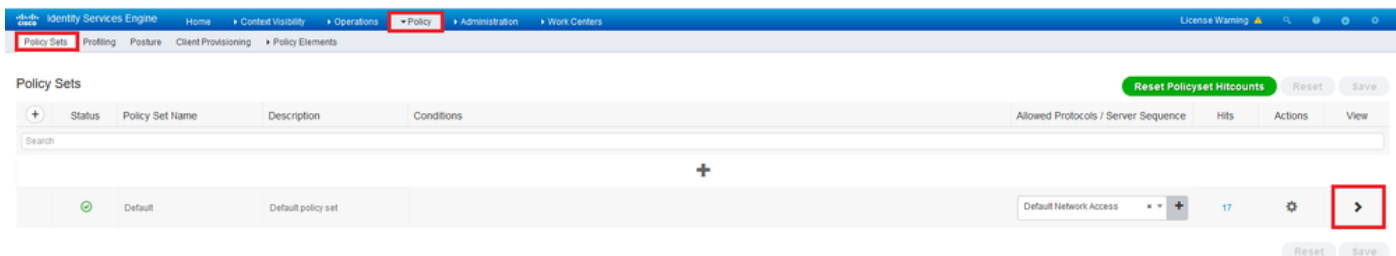
Step 5. Repeat the previous steps in order to create *user2*.



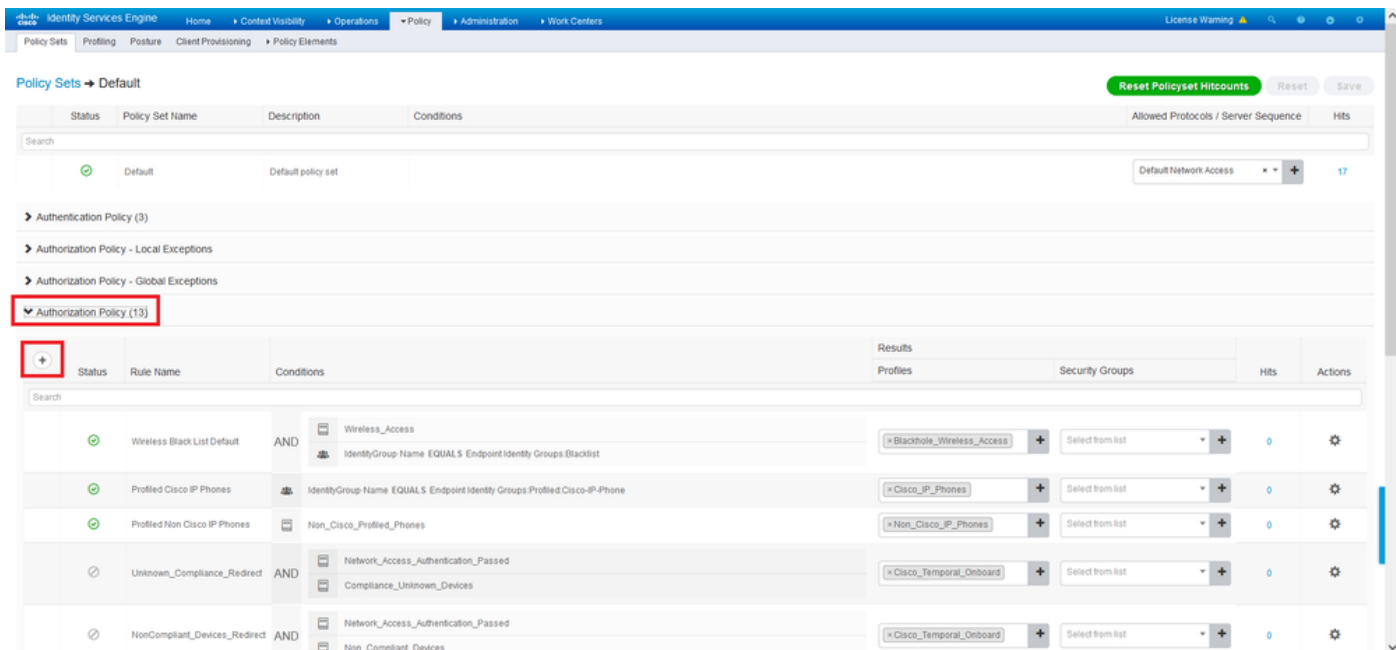
Step 6. Navigate to **Policy > Policy Sets**.



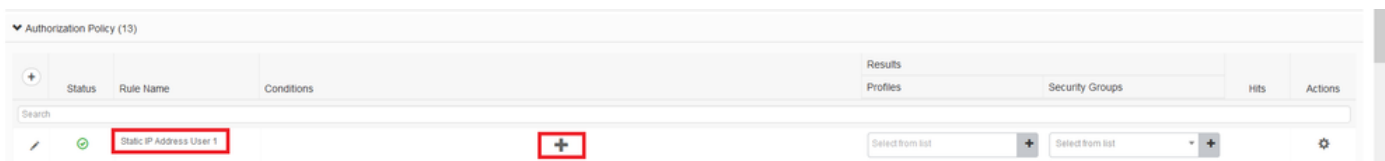
Step 7. Click the arrow > on the right side of the screen.



Step 8. Click the arrow > next to **Authorization Policy** to expand it. Now, Click the + symbol in order to add a new rule.



Provide a name to the rule and select the + symbol under **Conditions** column.



Click in the Attribute Editor textbox and click the **Subject** icon. Scroll down until you find *RADIUS User-Name* attribute and choose it.



Conditions Studio

Library

Search by Name

Editor

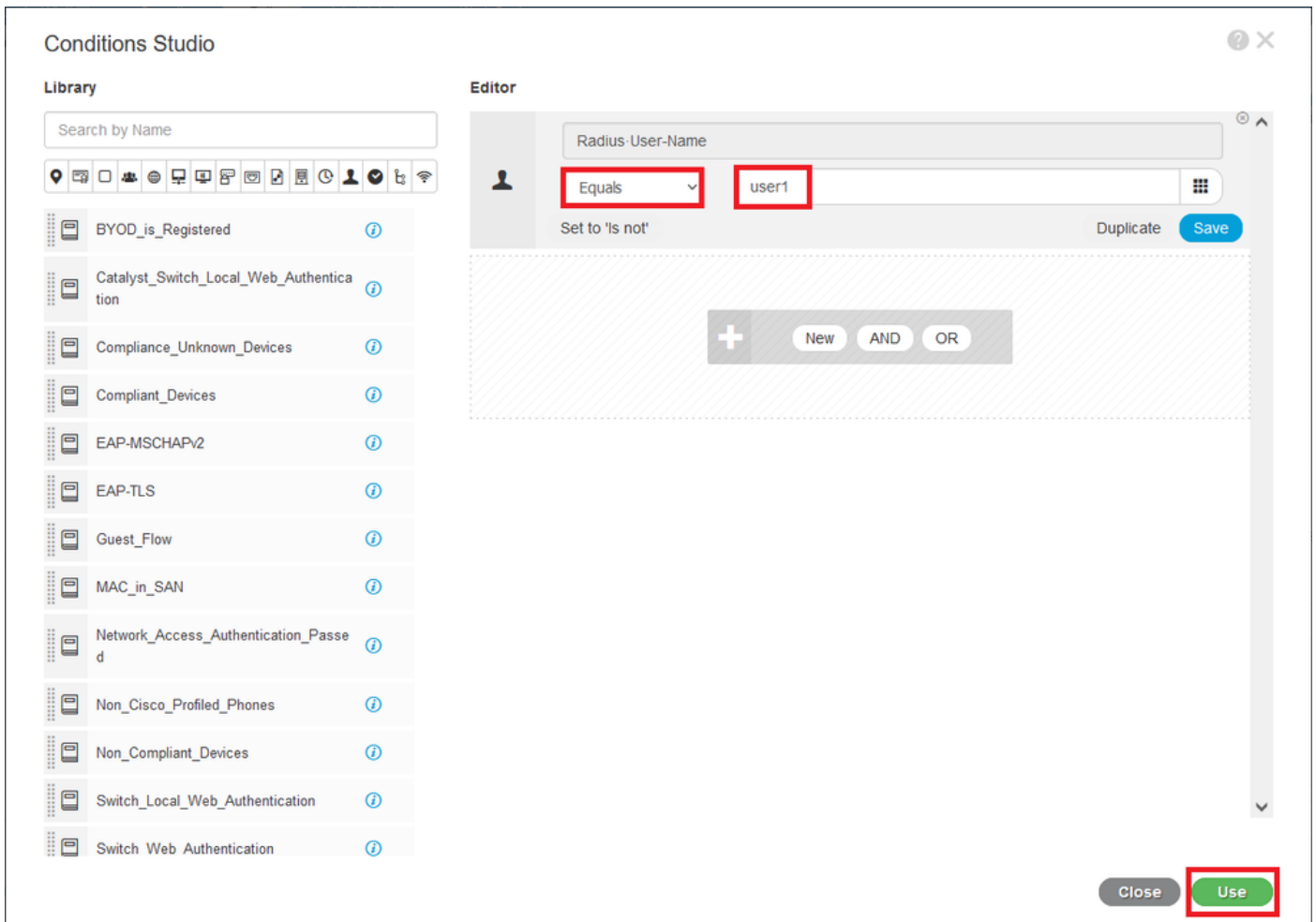
Click to add an attribute

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>

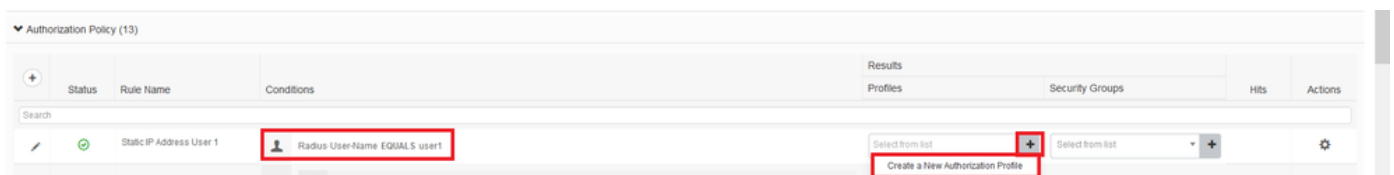
Close Use

Keep **Equals** as the operator and enter *user1* in the text box next to it. Click **Use** in order to save the attribute.



The condition for this rule is now set.

Step 9. In the **Results/Profiles** column, click the + symbol and choose **Create a New Authorization Profile**.



Give it a **Name** and keep **ACCESS\_ACCEPT** as the **Access Type**. Scroll down to the **Advance Attributes Settings** section.

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

Click the orange arrow and choose **Radius > 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

Type the IP address that you want to statically assign always to this user and click **Save**.

**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

Step 10. Now, choose the newly created Authorization Profile.

**Authorization Policy (13)**

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

The Authorization rule is now all set. Click **Save**.

**Policy Sets → Default**

**Reset Policyset Hitcounts** **Reset** **Save**

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	17

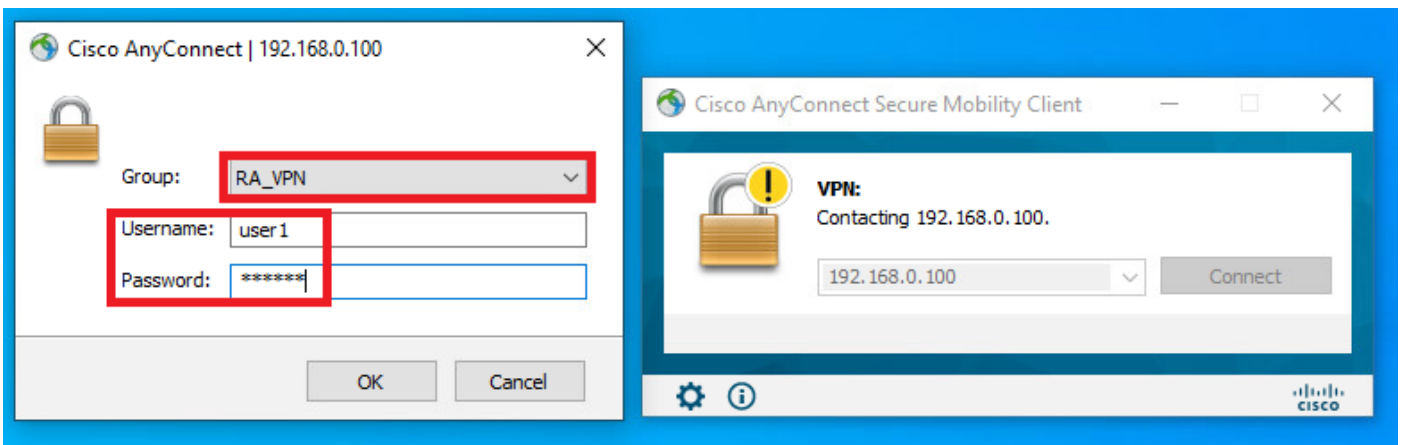
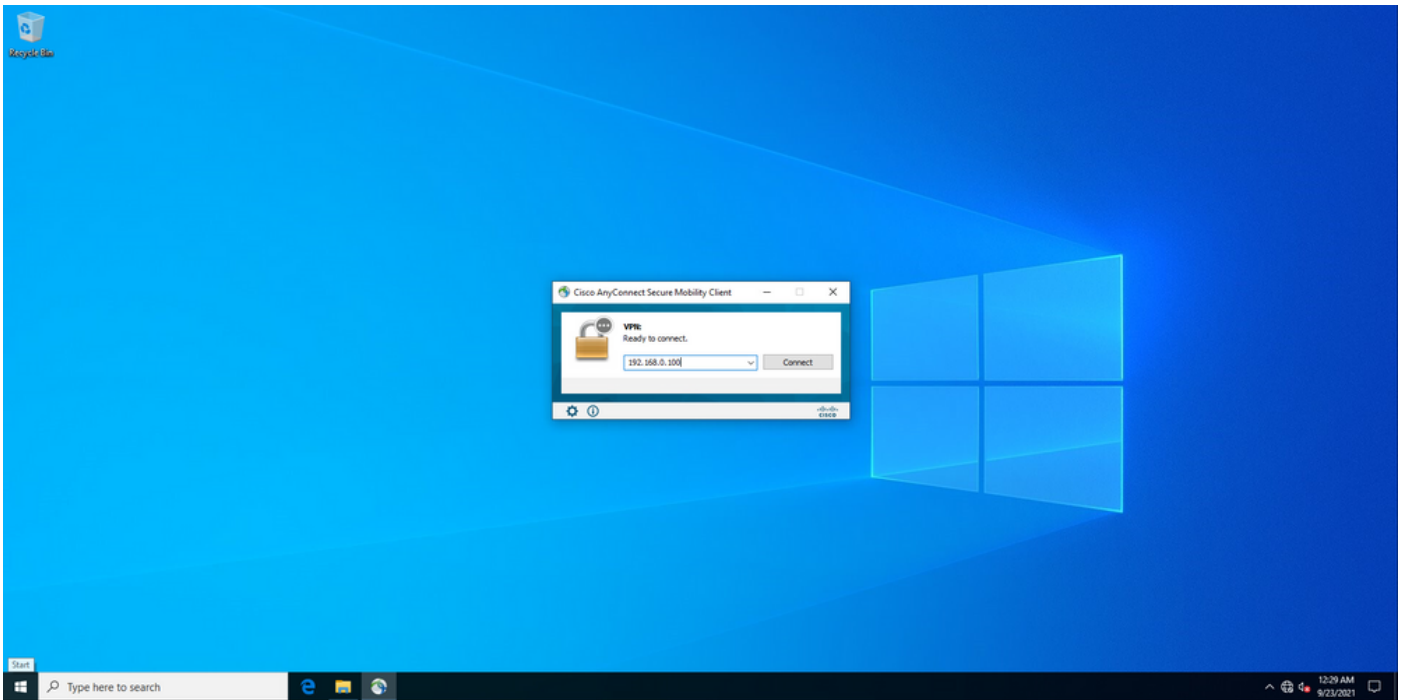
---

**Authorization Policy (13)**

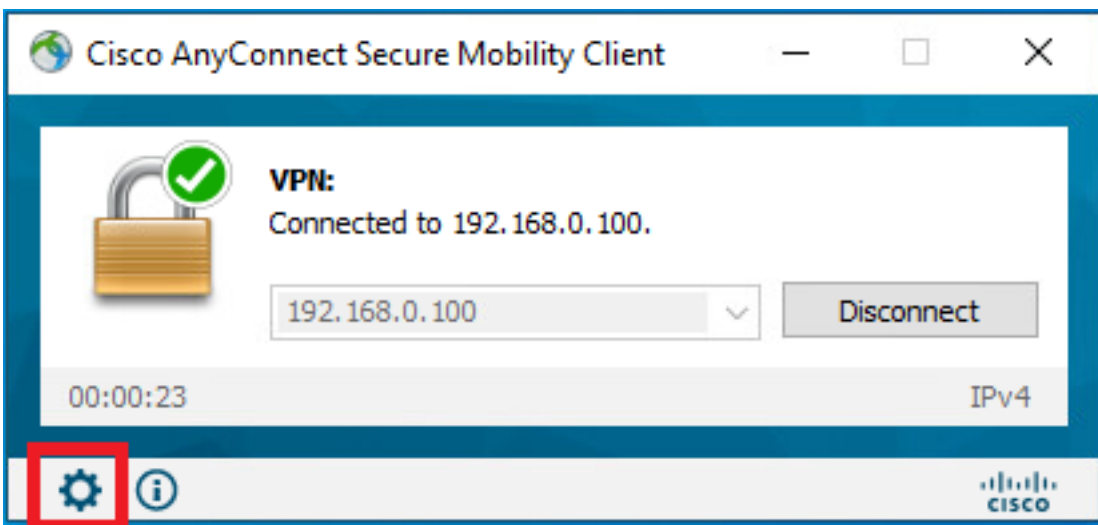
Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
<input checked="" type="checkbox"/>	Static IP Address User 1	Radius-User-Name EQUALS user1	StaticIPAddressUser1	Select from list		

## Verify

Step 1. Navigate to your client machine where the Cisco AnyConnect Secure Mobility client is installed. Connect to your FTD headend (a Windows machine is used here) and enter the *user1* credentials.



Click the gear icon (lower left corner) and navigate to the **Statistics** tab. Confirm in the **Address Information** section that the IP address assigned is indeed the one configured on ISE Authorization policy for this user.



The screenshot shows the Cisco AnyConnect Secure Mobility Client interface. The title bar reads "Cisco AnyConnect Secure Mobility Client". Below the title bar is the Cisco logo and the text "AnyConnect Secure Mobility Client". The main window is titled "Virtual Private Network (VPN)" and contains several tabs: "Preferences", "Statistics", "Route Details", "Firewall", and "Message History". A "Diagnostics..." button is located in the top right corner. The "Statistics" tab is active, displaying connection information and address information. The "Connection Information" section shows: 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, and Management Connection State: Disconnected (user tunnel active). The "Address Information" section shows: Client (IPv4): 10.0.50.101 (highlighted with a red box), Client (IPv6): Not Available, and Server: 192.168.0.100. At the bottom of the window are "Reset" and "Export Stats..." buttons.

The **debug radius all** command output on FTD shows:

```
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)
<omitted output>

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

The FTD logs show:

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 <DfltGrpPolicy> User <user1> IP <192.168.0.101> IPv4
Address <10.0.50.101> IPv6 address <::> assigned to session

```

The RADIUS Live logs on ISE show:



Identity Services Engine

### Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:00:56:96:46:0F (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	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00:00:56:96:46:0F
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
15046 Queried PIP - Normalized Radius Radius/lowType (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
15036 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-2-7141749378/23
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

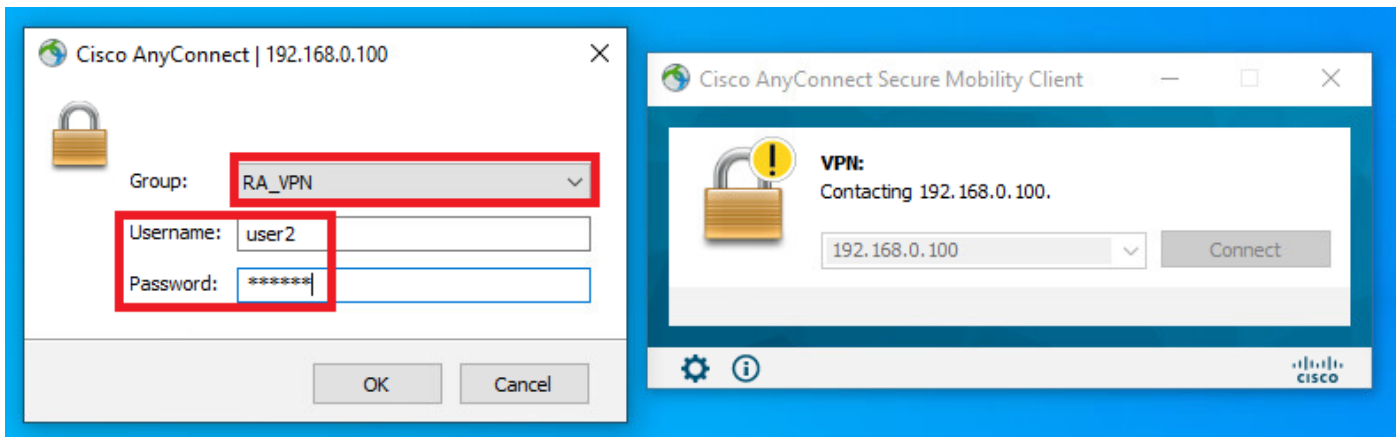
IPSEC	IPSECOnly IPSEC Device#0
EnabledFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM SessionID	d8a800540000d00014bc1d0
Called-Station-ID	192.168.0.100
CiscoAVPair	mdm-dmdevice-platform; mdm-dmdevice-manid=00:00:56:96:46:0f; mdm-dmdevice-platform-version=10.0.13352; mdm-dmdevice-public-manid=00:00:56:96:46:0f; mdm-dmdevice-agent=AnyConnect Windows 4 10.02086; mdm-dmdevice-type=VMware, Inc VMware Virtual Platform; mdm-dmdevice-uid=glbactm158788E0CF62F3F2CDE241409F4BA2AE2C583; mdm-dmdevice-uid=3C38427071F907B2F810F124621184A08596C717E370386CC03F845C0880244; audit-session-id=d8a800540000d00014bc1d0; ip-source-ip=192.168.0.101; oca-push=true

### Result

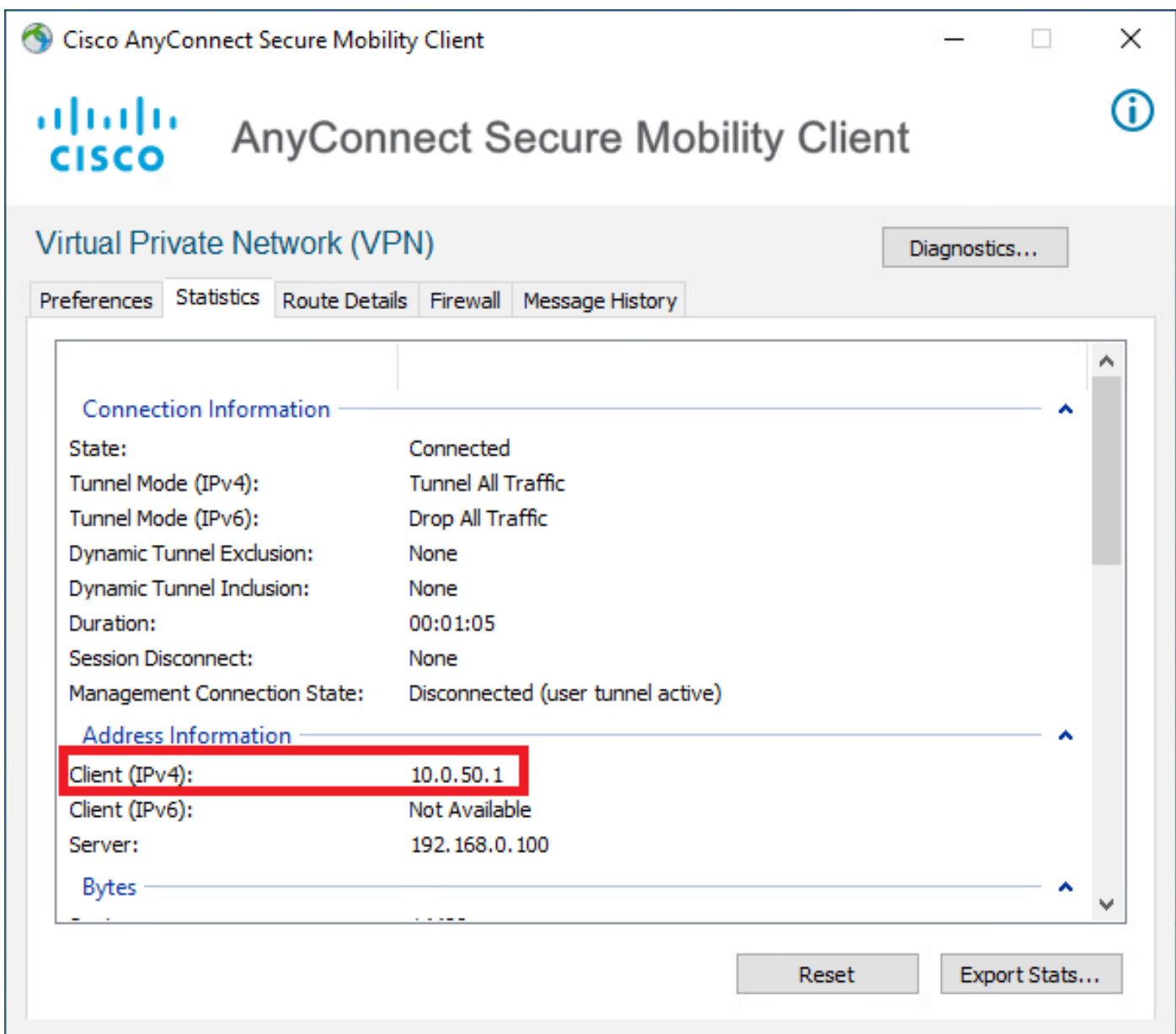
Framed IP Address	10.0.0.101
Class	CACS-d8a800540000d00014bc1d0 driverap-ISE-2-7141749378/23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

Step 2. Connect to your FTD headend (a Windows machine is used here) and enter the *user2* credentials.



The **Address Information** section shows that the IP address assigned is indeed the first IP address available in the IPv4 local pool configured via FMC.



The **debug radius all** command output on FTD shows:

```
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)
<omitted output>
```

#### **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 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
```

The FTD logs show:

<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 <DfltGrpPolicy> User <user2> IP <192.168.0.101> IPv4  
Address <10.0.50.1> IPv6 address <::> assigned to session**

# The RADIUS Live logs on ISE show:

Identity Services Engine

### Overview

Event	5200 Authentication succeeded
Username	user2
Endpoint Id	00 00 56 96 46 6F 0D
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	drivrap-ISE-2.7
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	00 00 56 96 46 6F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	cb8000400004000014bc307
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 Access-Request
11017 RADIUS created a new session
10049 Evaluating Policy Group
10050 Evaluating Service Selection Policy
10041 Evaluating Identity Policy
10048 Queried PIP - Normalized Radius RadiusFlowType (4 times)
22012 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 - user2
22037 Authentication Passed
24714 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
10036 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user2
24211 Found Endpoint in Internal Endpoints IDStore
10048 Queried PIP - Radius User-Name
10048 Queried PIP - Radius NAS-Port Type
10048 Queried PIP - EndPoints LogicalProfile
10048 Queried PIP - Network Access AuthenticationStatus
10010 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	202 milliseconds

### Other Attributes

ConfigVersionId	148
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPR3000ASAPROX-Tunnel-Group-Name	RA_VPN
OriginalUserName	user2
NetworkDeviceProfileId	b0099005-3150-4215-a80a-d753445d550c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPROX-Client-Type	2
Acx-Session-ID	drivrap-ISE-2-71417494978/24
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_join_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTL-Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Class
Location	LocationAll Locations
Device Type	Device TypeAll Device Types

IPSEC

IPSECs IPSEC Device#No	
Name	Endpoint Identity Groups Profiled Workstation
EnabledFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPM Session ID	cb8000400004000014bc307
Called-Station-ID	192.168.0.100
CiscoAVPair	mdm-device-platform=main,mdm-device-os=ios-96-46-41,mdm-device-platform-version=10.0.13362,mdm-device-public-name=00:00:56:96:46:6F,mdm-device-user-agent=AnyCommand Windows 4.10.22088,mdm-device-type=VMware, Inc VMware Virtual Platform,mdm-device-uid=global=159f88e20cf52f32c0e2431409f4baa2ae2c083,mdm-device-uid=3c38427071f90782f810f124621184408698c717e370388cc030f8440c880344,audit-session-id=cb8000400004000014bc307,ip-source-ip=192.168.0.101,coa-push=true

### Result

Class	CACS:cb8000400004000014bc307:drivrap-ISE-2-71417494978/24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

**Note:** You must use different IP address ranges for IP address assignment on both FTD ip local pool and ISE Authorization policies in order to avoid duplicate IP address conflicts

among your AnyConnect Clients. In this configuration example, FTD was configured with an IPv4 local pool from 10.0.50.1 through 10.0.50.100 and ISE server assigns static IP address of 10.0.50.101.

## Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

On FTD:

- **debug radius all**

On ISE:

- RADIUS live logs