RADIUS認証によるAnyConnectユーザへのスタティックIPアドレス割り当ての設定

内容

概要

このドキュメントでは、Identity Services Engine(ISE)サーバを使用してRADIUS認可を設定し、RADIUS属性8 Framed-IP-Addressを使用して、特定のCisco AnyConnectセキュアモビリティクライアントユーザのFirepower Threat Defense(FTD)に常に転送する方法についてを説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FTD
- Firepower Management Center（FMC）
- ISE
- Cisco AnyConnect セキュア モビリティ クライアント
- RADIUS プロトコル

使用するコンポーネント

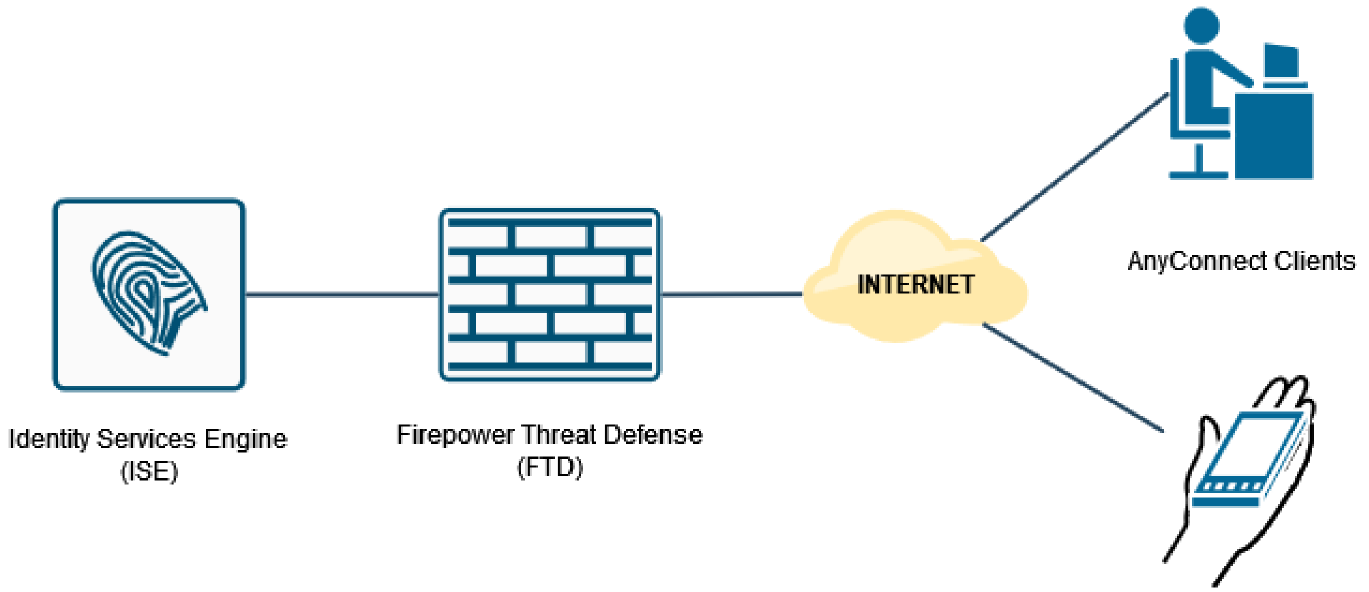
このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCv - 7.0.0（ビルド94）
- FTDv - 7.0.0（ビルド94）
- ISE:2.7.0.356
- AnyConnect - 4.10.02086
- Windows 10 Pro

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



FMCによるAAA/RADIUS認証を使用したリモートアクセスVPNの設定

手順については、次のドキュメントとビデオを参照してください。

- FTD での AnyConnect Remote Access VPN の設定
- FMCによって管理されるFTDの初期AnyConnect設定

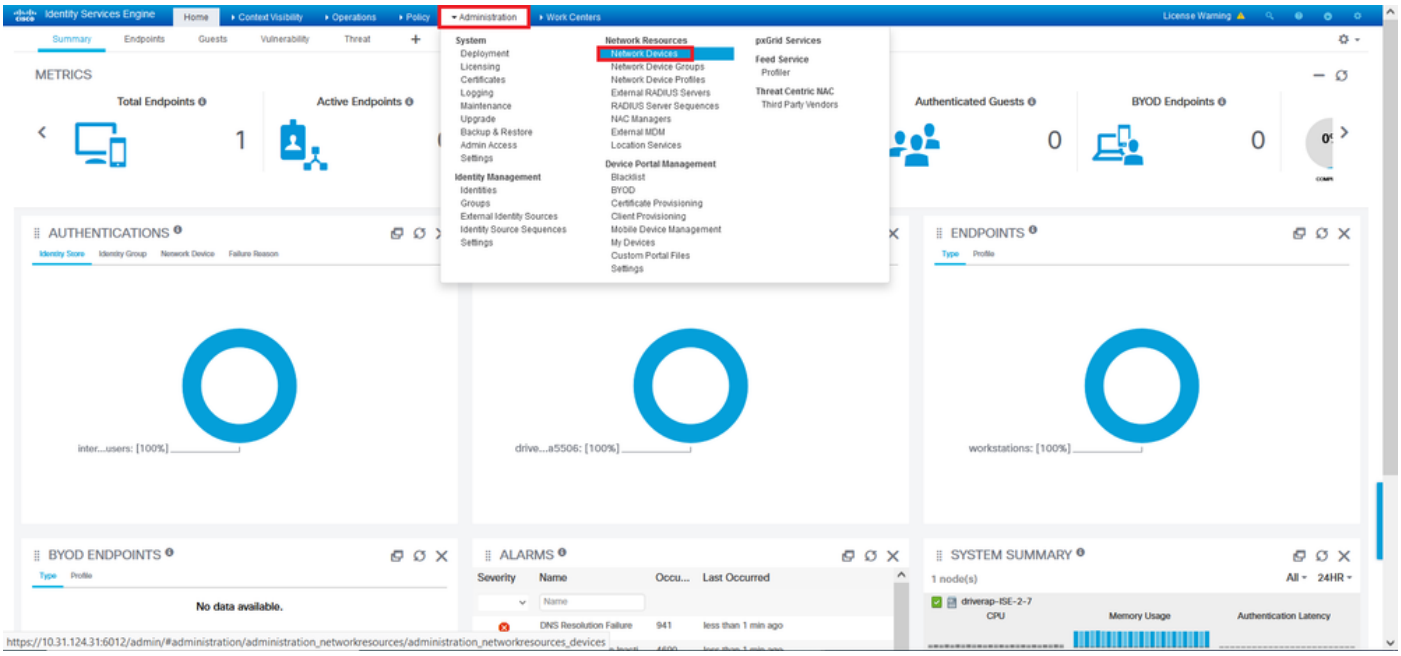
FTD CLIでのリモート・アクセスVPNの構成：

```
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
```

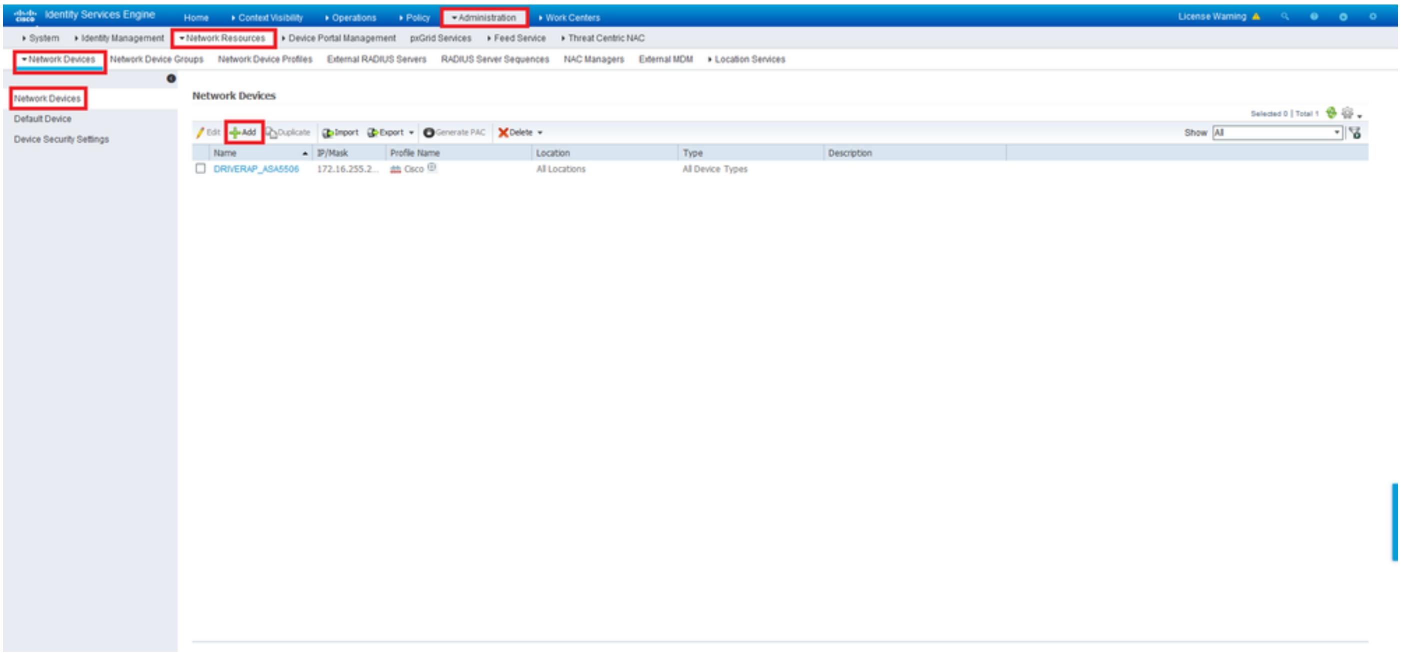
```
ssl trust-point RAVPN_Self-Signed_Cert

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
```

ISE（RADIUSサーバ）での認可ポリシーの設定

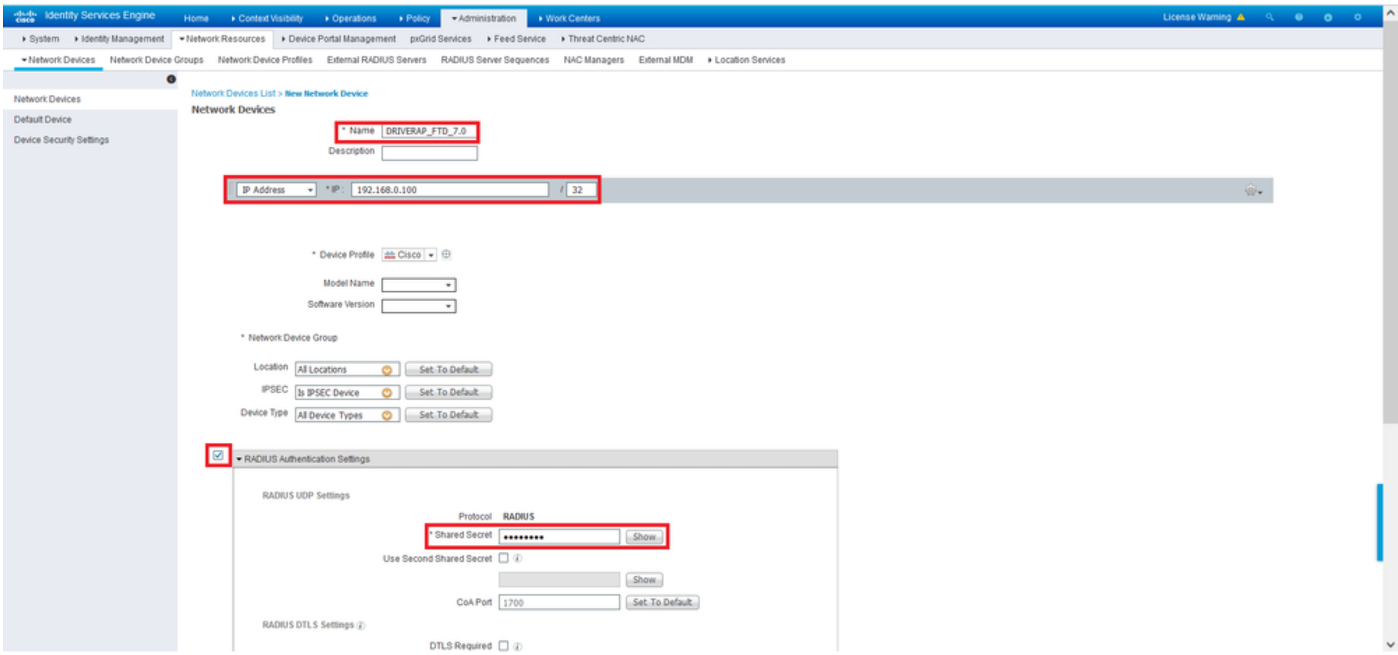
ステップ1:ISEサーバにログインし、[**Administration**] > [**Network Resources**] > [**Network Devices]に移動します。**



ステップ2:[Network Devices]セクションで[**Add**]をクリックし、ISEがFTDからのRADIUSアクセス要求を処理できるようにします。



ネットワークデバイスの[**名前**]フィールド**と[IPアドレ**ス]フィールドを入力し、[**RADIUS Authentication Settings]ボックスをオンに**します。[Shared Secret]**は、**FMC上のRADIUSサーバオブジェクトの作成時に使用された値と同じである必要があります。



* Name: DRIVERAP_FTD_7.0

Description:

IP Address ▾ * IP : 192.168.0.100 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

☑ RADIUS Authentication Settings

Protocol: RADIUS

* Shared Secret: ••••••••

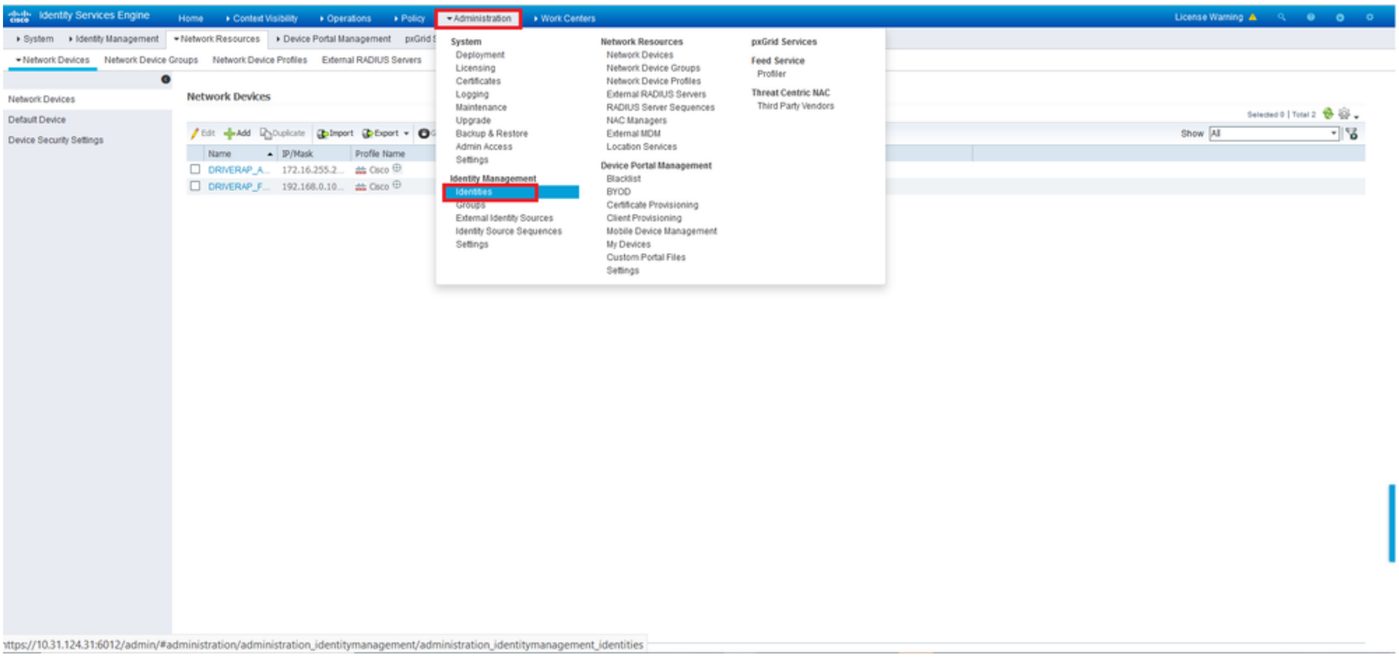
Use Second Shared Secret ☐

CoA Port: 1700

DTLS Required ☐

このページの最後にあるボタンで保存します。

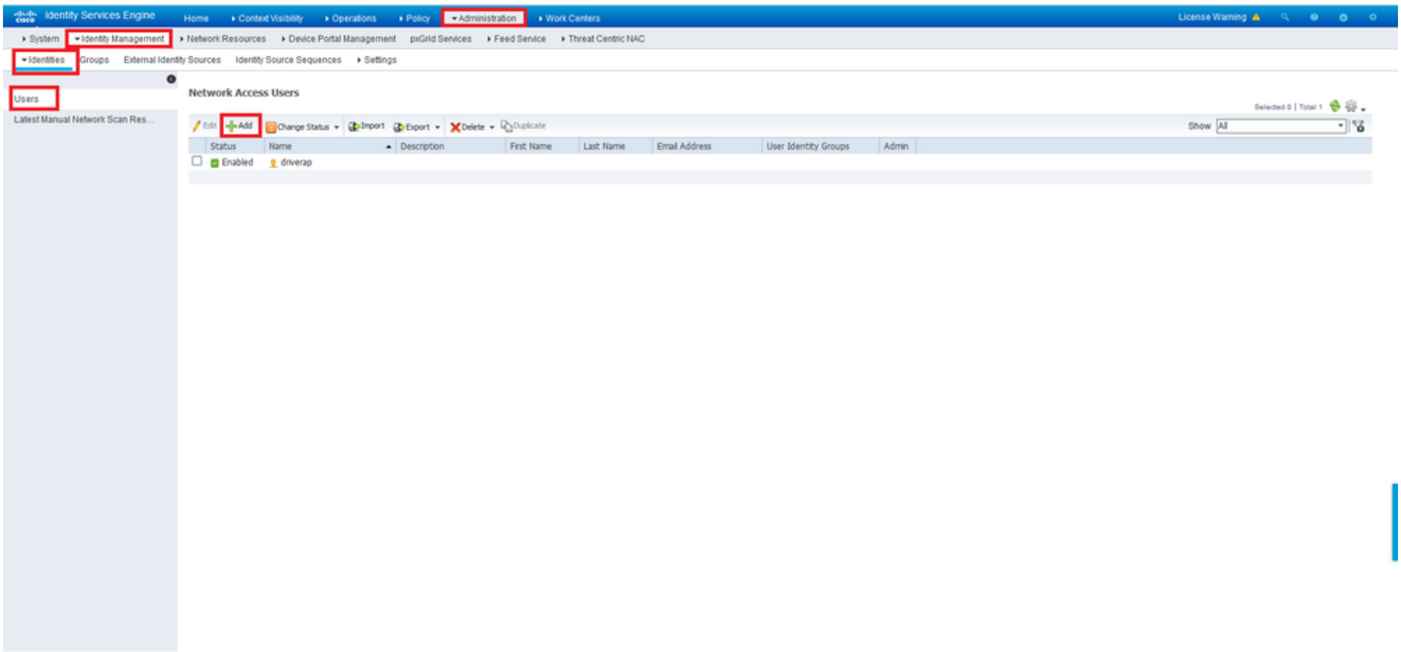
ステップ3:[Administration] > **[Identity Management] > [Identities]に移動します。**



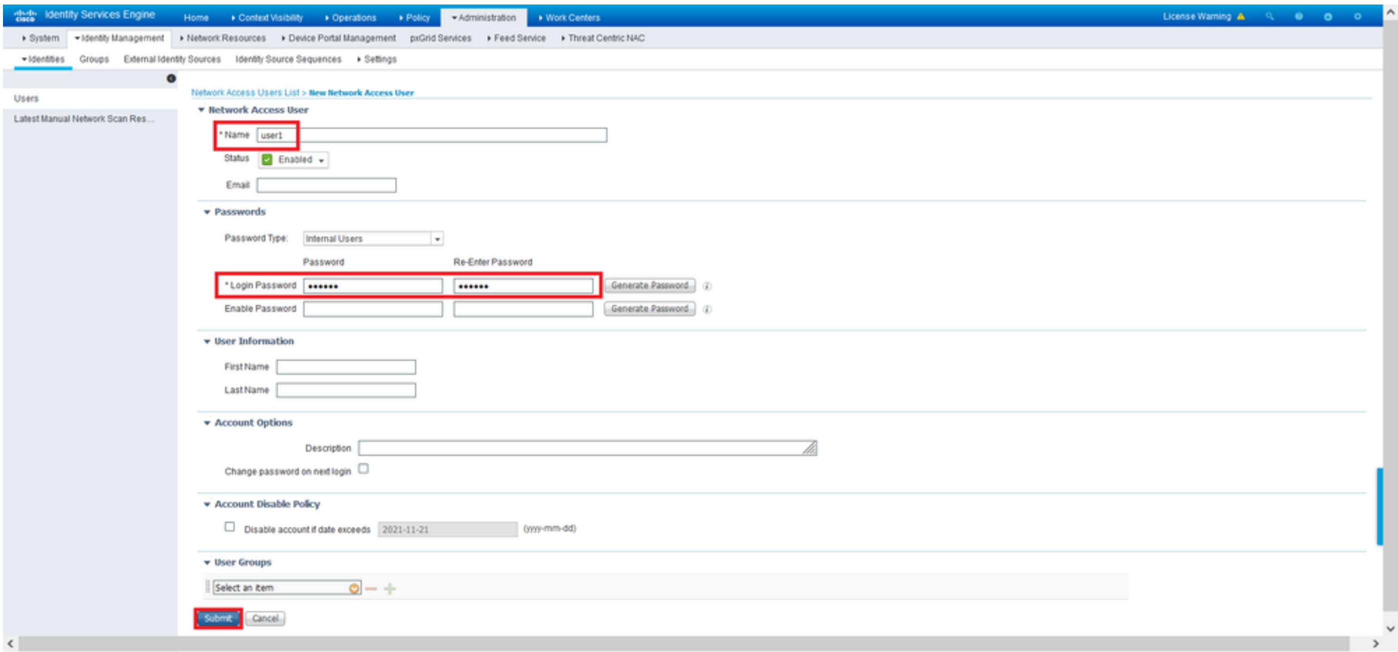
Name	IP/Mask	Profile Name
☐ DRIVERAP_A...	172.16.255.2...	Cisco
☐ DRIVERAP_F...	192.168.0.10...	Cisco

https://10.31.124.31:6012/admin/#administration/administration_identitymanagement/administration_identitymanagement_identities

ステップ4:[Network Access Users]セクションで、[*Add*]をクリックしてISEのローカルデータベースに*user1*を作成します。



[名前]フィールドと[ログインパスワー**ド]フィールド**にユーザ名と**パスワード**を入力し、[送信]をクリック**します**。



Network Access User

- * Name: user1
- Status: Enabled
- Email:

Passwords

- Password Type: Internal Users
- * Login Password: •••••• / ••••••

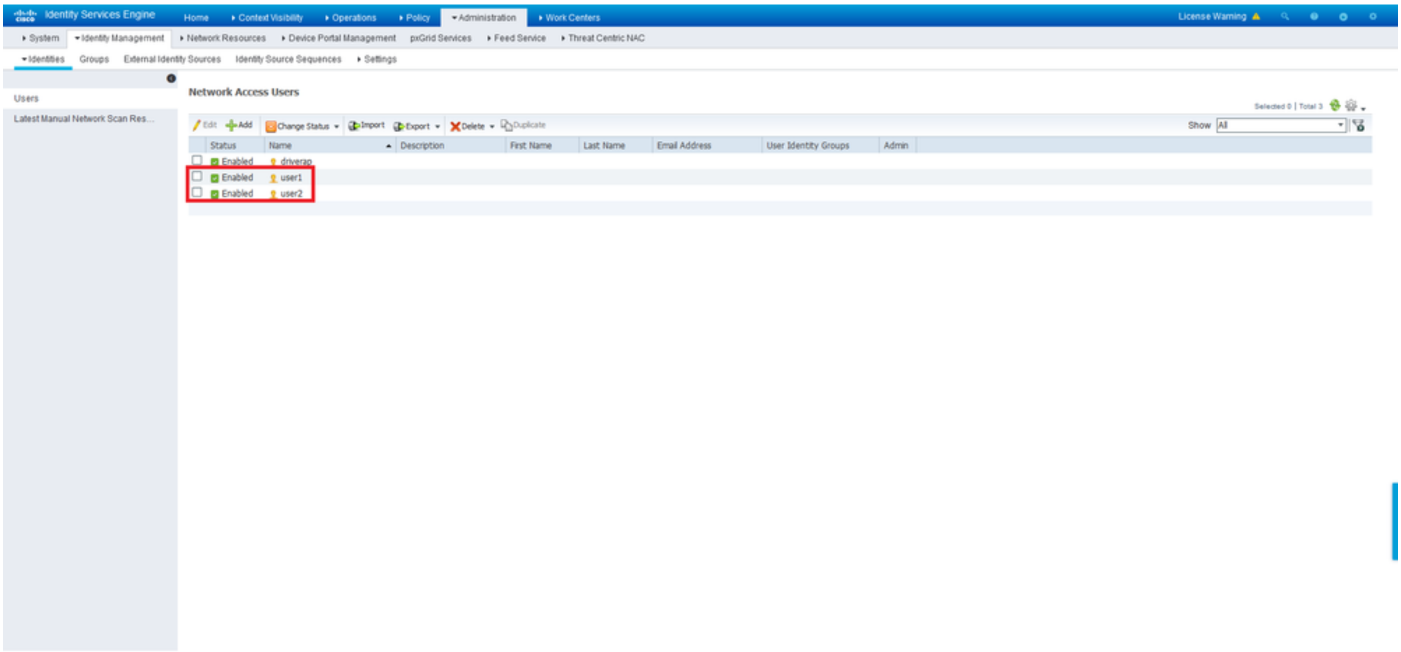
Account Options

- Change password on next login □

Account Disable Policy

- □ Disable account if date exceeds 2021-11-21 (yyyy-mm-dd)

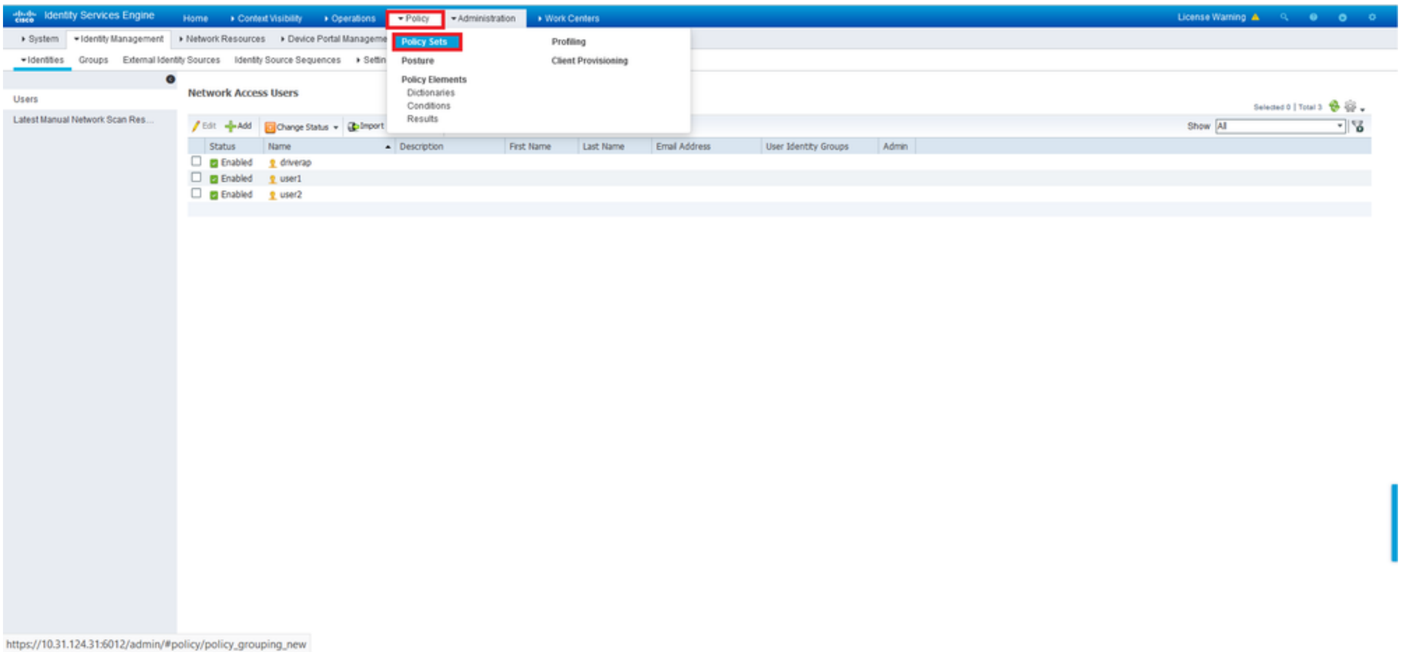
ステップ5：前のステップを繰り返して、*user2*を作成します。



Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□ Enabled	driverap						
□ Enabled	user1						
□ Enabled	user2						

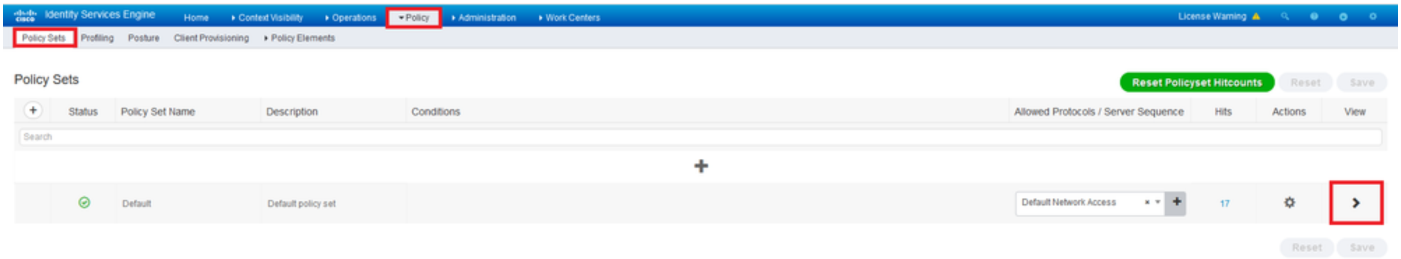
ステップ6:[Policy] > **[Policy Sets]に移動します。**



Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□ Enabled	driverap						
□ Enabled	user1						
□ Enabled	user2						

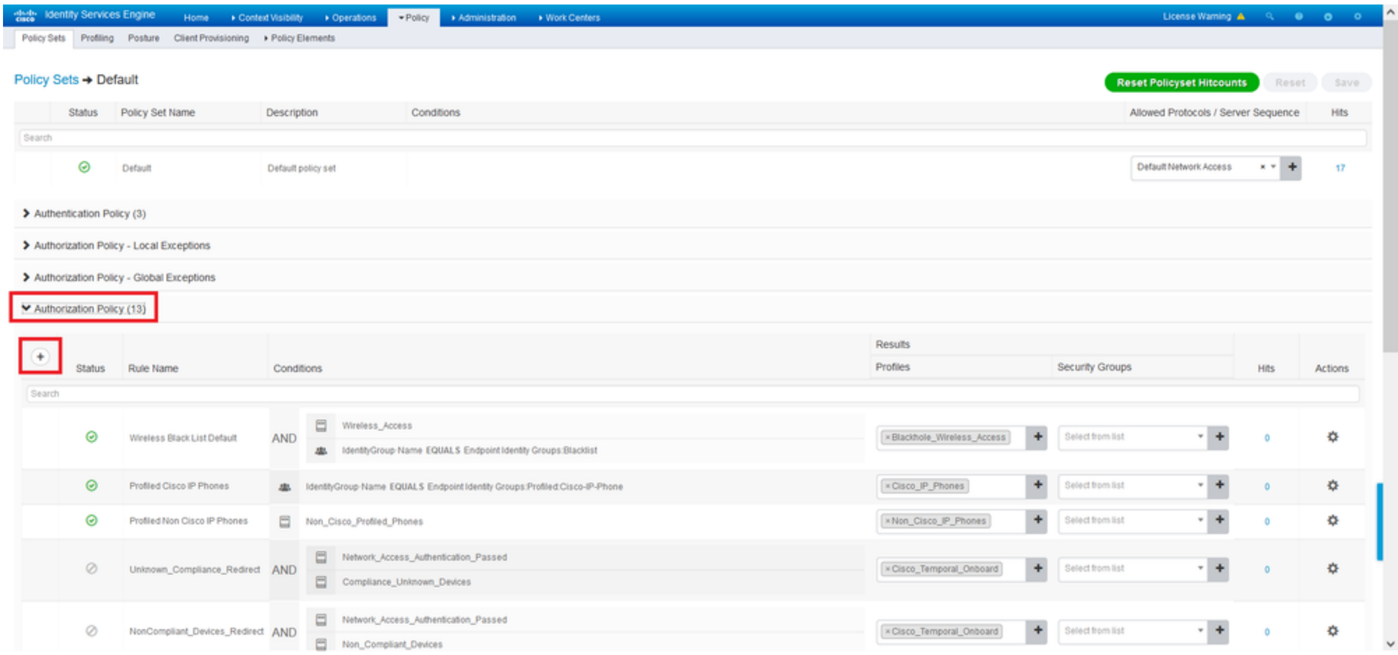
ステップ7：画面の右側にある矢印をクリックします。



Policy Sets

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

ステップ8:[Authorization Policy]の横にある矢印>をクリックして、**[Authorization Policy]**を展開します。次に、+記号をクリックして新しい規則を追加します。



Policy Sets → Default

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

> Authentication Policy (3)

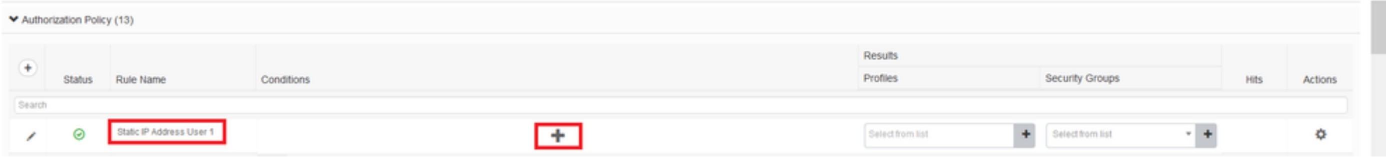
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (13)

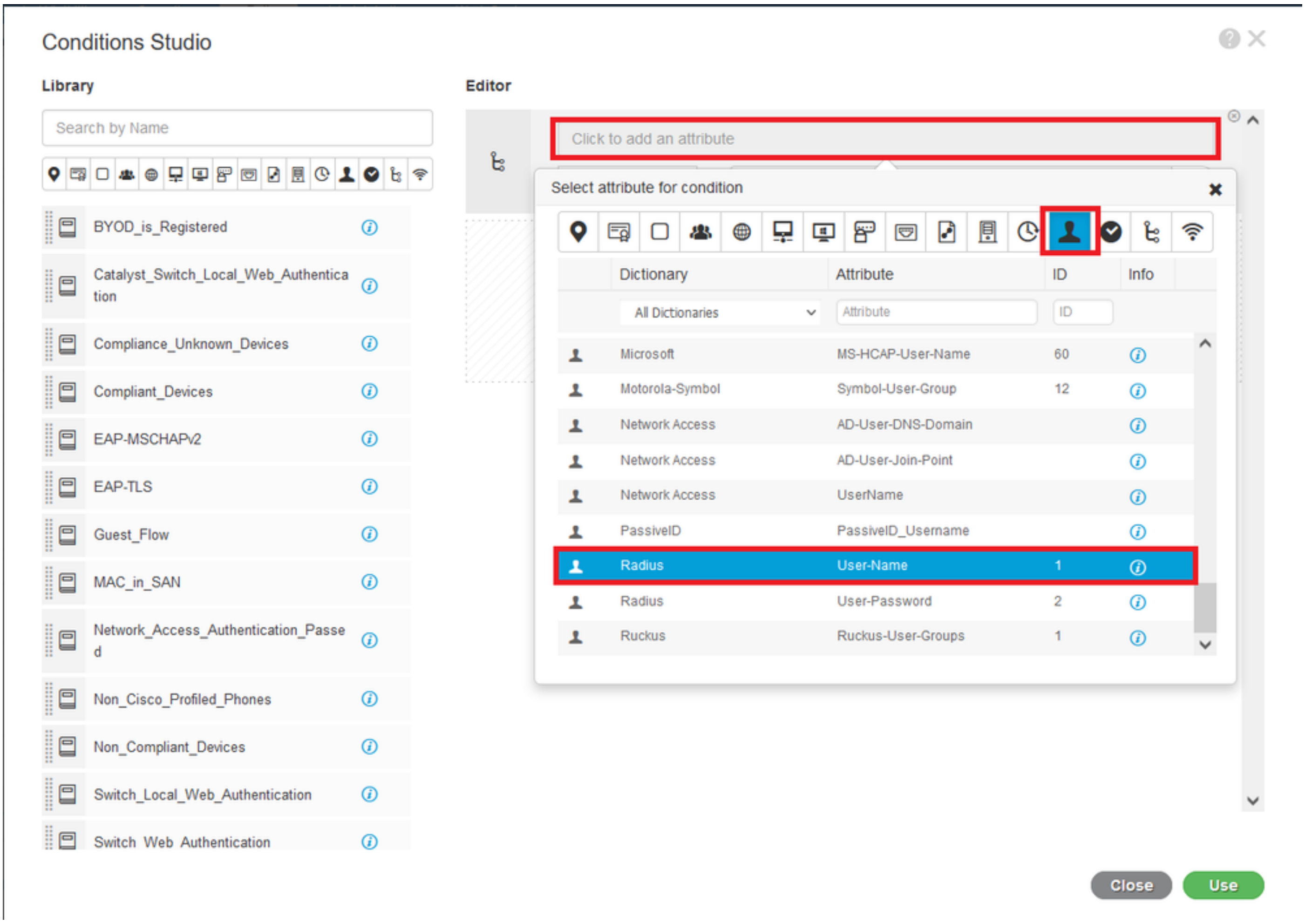
				Results			
Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
✓	Wireless Black List Default	AND	Wireless_Access IdentityGroup·Name EQUALS Endpoint Identity Groups:Blacklist	Blackhole_Wireless_Access	Select from list	0	⚙
✓	Profiled Cisco IP Phones		IdentityGroup·Name EQUALS Endpoint Identity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

ルールに名前を付け、[条件]列の*下の+記号*を選択します。


Authorization Policy (13)

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

[Attribute Editor]テキストボックスをクリックし、[Subject]アイコンを**クリック**します。[*RADIUS User-Name*]属性が見つかるまで下にスクロールし、それを選択します。



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_Passed
- Non_Cisco_Profiled_Phones
- Non_Compliant_Devices
- Switch_Local_Web_Authentication
- Switch_Web_Authentication

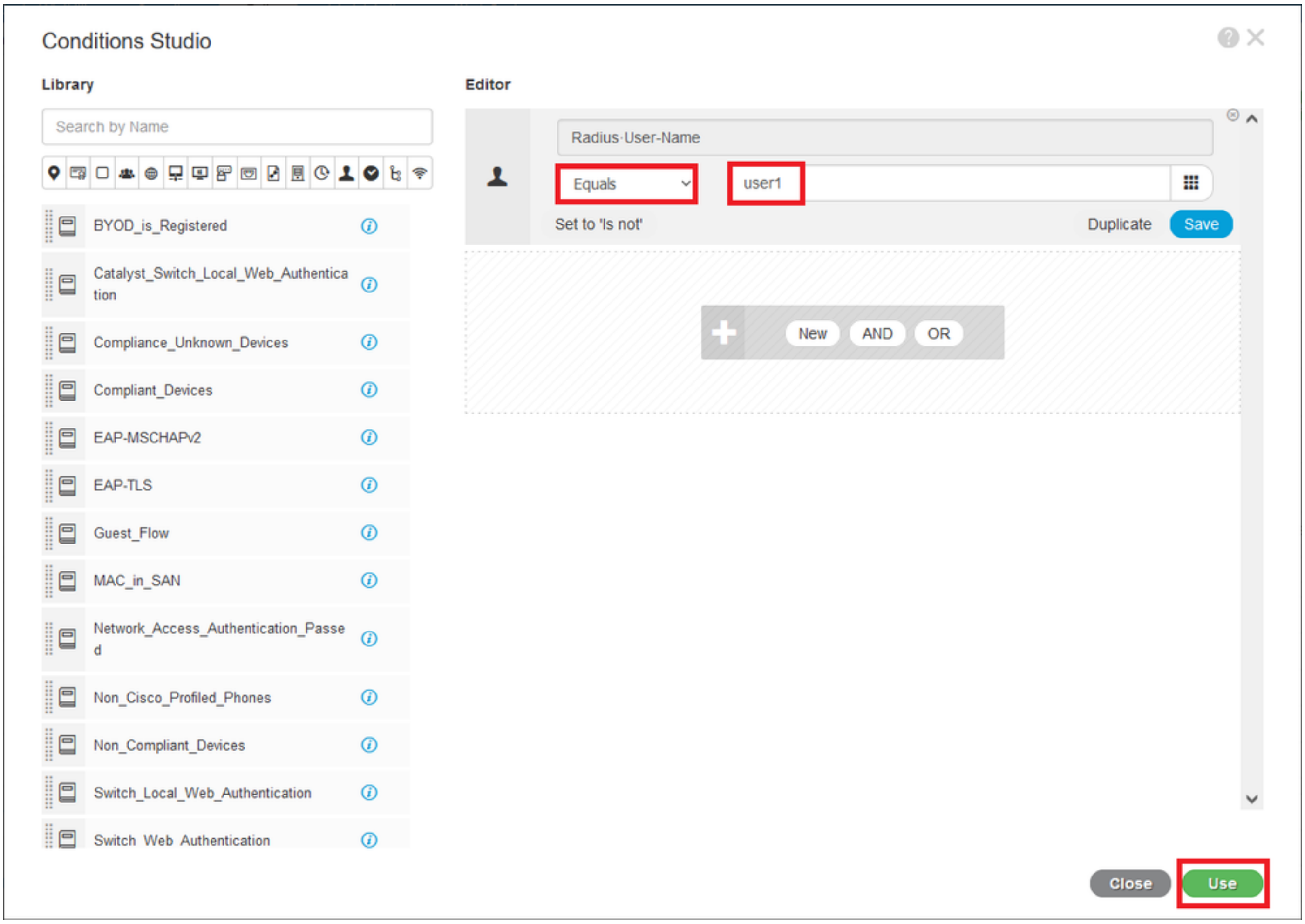
Editor

Click to add an attribute

Select attribute for condition

	Dictionary	Attribute	ID	Info
	All Dictionaries	Attribute	ID	
👤	Microsoft	MS-HCAP-User-Name	60	ⓘ
👤	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	ⓘ

演算子として[等しい]を選択し、その横のテキストボックスにuser1と入力します。[Use]をクリックし、属性を保存します。



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_Passed
- Non_Cisco_Profiled_Phones
- Non_Compliant_Devices
- Switch_Local_Web_Authentication
- Switch_Web_Authentication

Editor

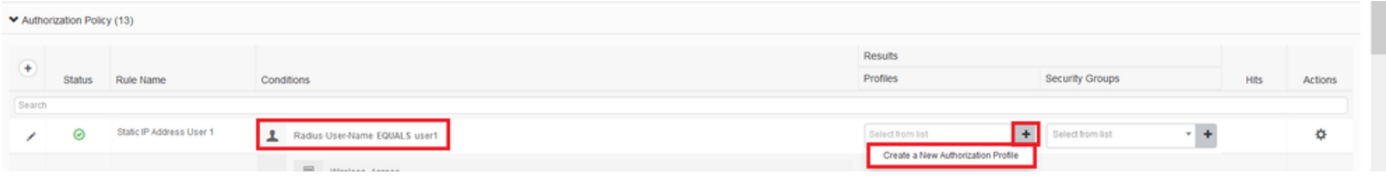
Radius·User-Name

Equals

user1

これで、このルールの条件が設定されました。

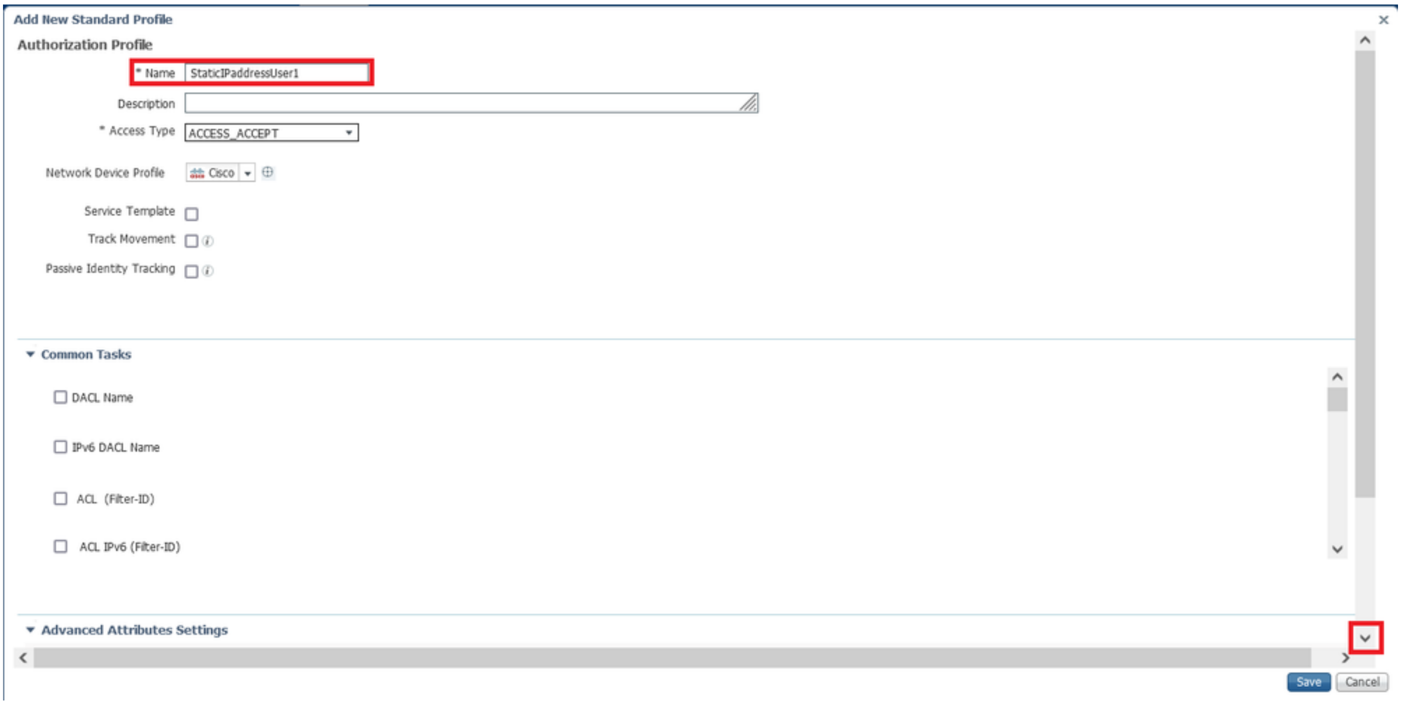
ステップ9:**[Results/Profiles]**列で、+記号をクリックし、**[Create a New Authorization Profile]を選択します。**



Authorization Policy (13)

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

名前を指定**し、***ACCESS*_ACCEPTを*アクセスタイプ*として保**持します**。[Advance Attributes Settings]セクションまで**スクロールダウン**します。



Add New Standard Profile

Authorization Profile

* Name StaticIPaddressUser1

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

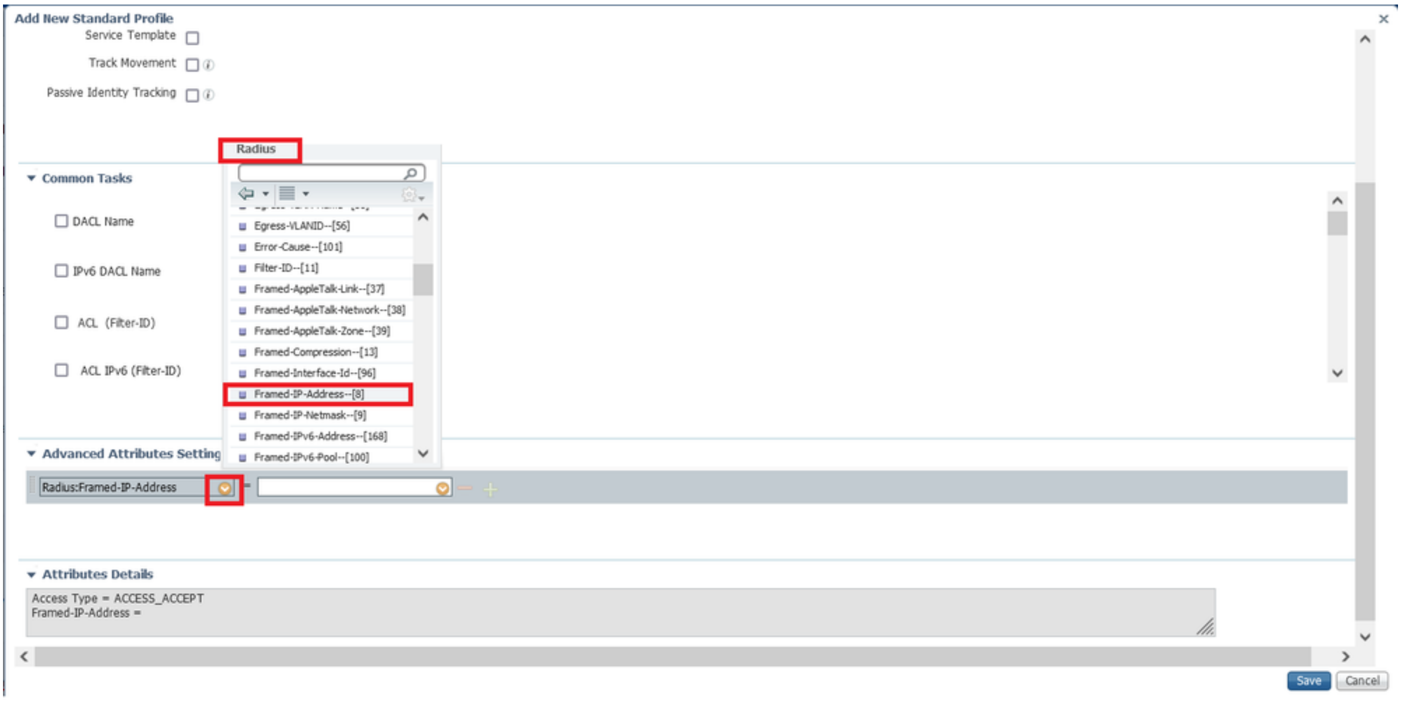
□ IPv6 DACL Name

□ ACL (Filter-ID)

□ ACL IPv6 (Filter-ID)

Advanced Attributes Settings

オレンジ色の矢印をクリックし、[Radius] > [Framed-IP-Address—[8]を選択します。



Add New Standard Profile

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ IPv6 DACL Name

□ ACL (Filter-ID)

□ ACL IPv6 (Filter-ID)

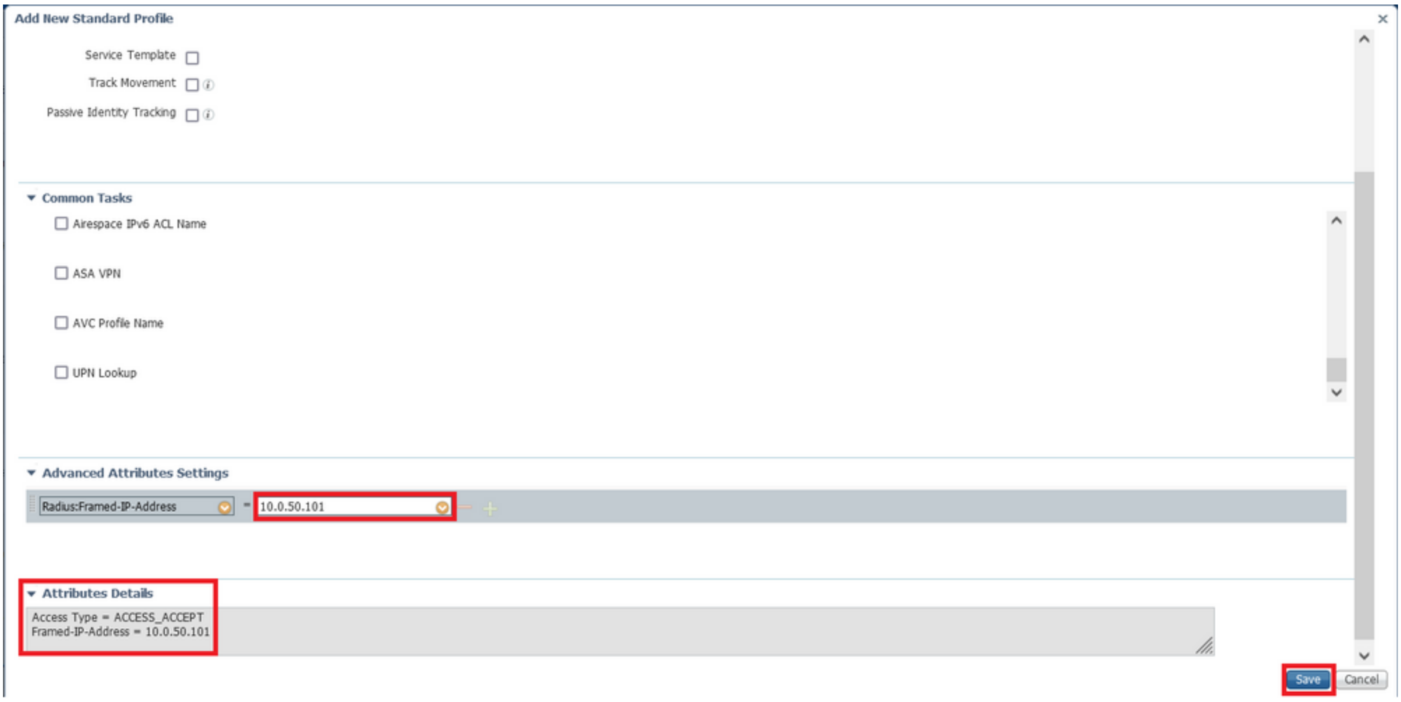
Advanced Attributes Settings

Radius:Framed-IP-Address =

Attributes Details

Access Type = ACCESS_ACCEPT
Framed-IP-Address =

このユーザーに常に静的に割り当てるIPアドレスを入力し、[保存]をクリックします。



Add New Standard Profile

Service Template □

Track Movement □

Passive Identity Tracking □

▾ Common Tasks

□ Airespace IPv6 ACL Name

□ ASA VPN

□ AVC Profile Name

□ UPN Lookup

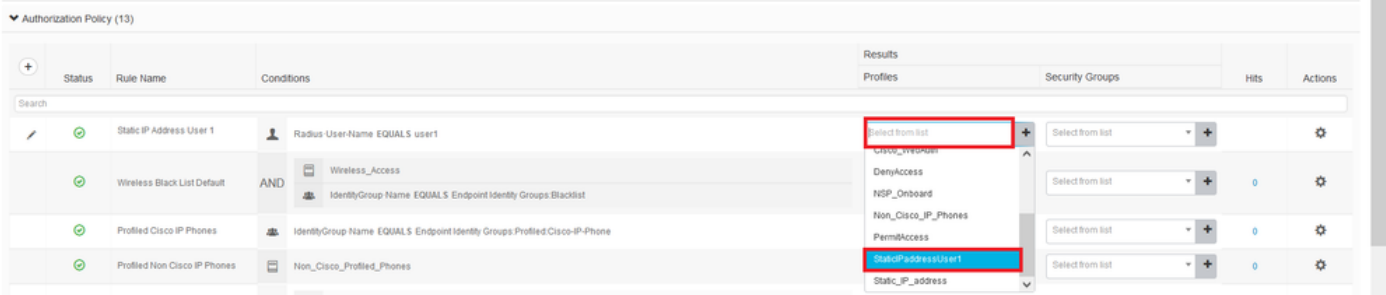
▾ Advanced Attributes Settings

Radius:Framed-IP-Address = 10.0.50.101

▾ Attributes Details

```
Access Type = ACCESS_ACCEPT
Framed-IP-Address = 10.0.50.101
```

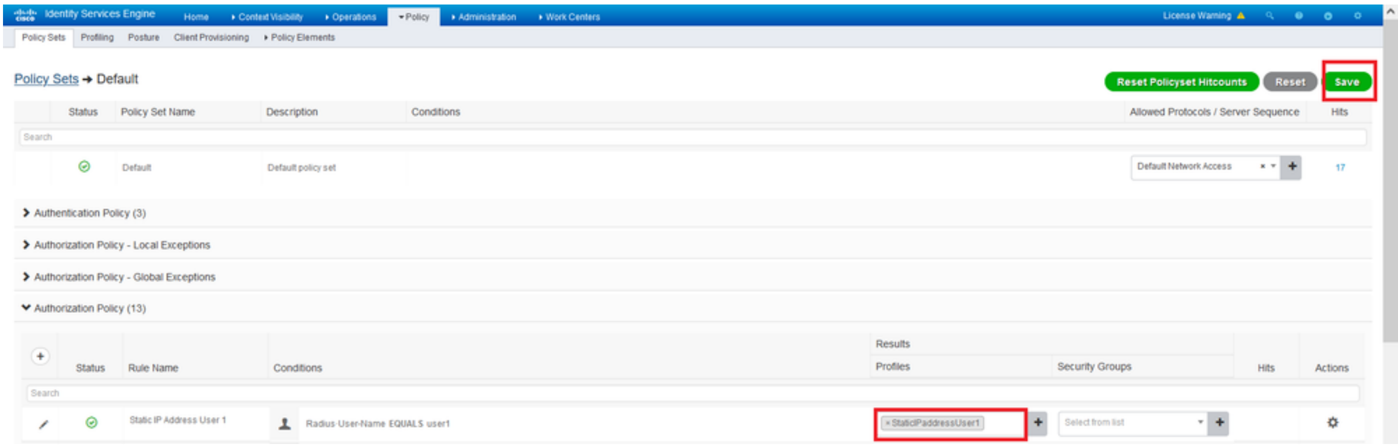
ステップ10：ここで、新しく作成した認可プロファイルを選択します。



Authorization Policy (13)

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

これで、認可ルールがすべて設定されました。[Save] をクリックします。



Policy Sets → Default

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

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

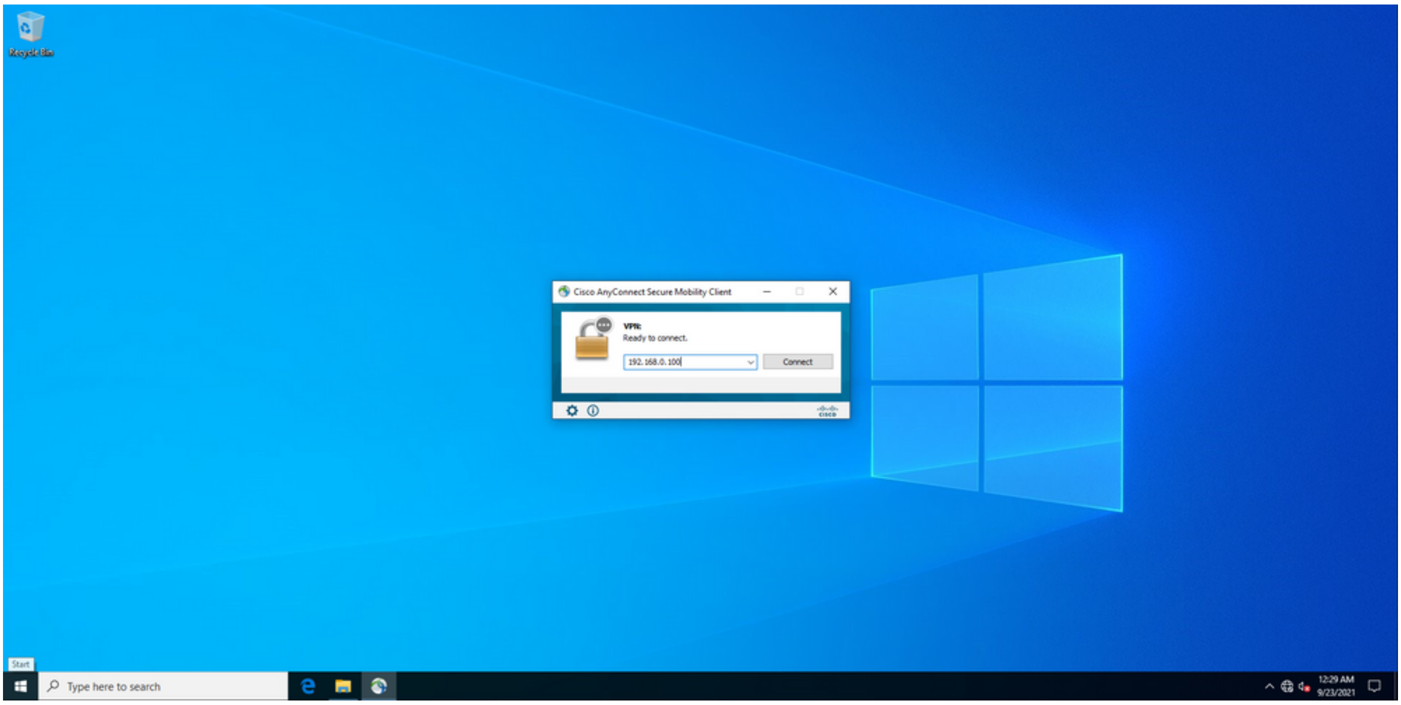
> Authorization Policy - Global Exceptions

⌄ Authorization Policy (13)

	Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
Search							
	✓	Static IP Address User 1	Radius·User-Name EQUALS user1	× StaticIPaddressUser1	Select from list		⚙

確認

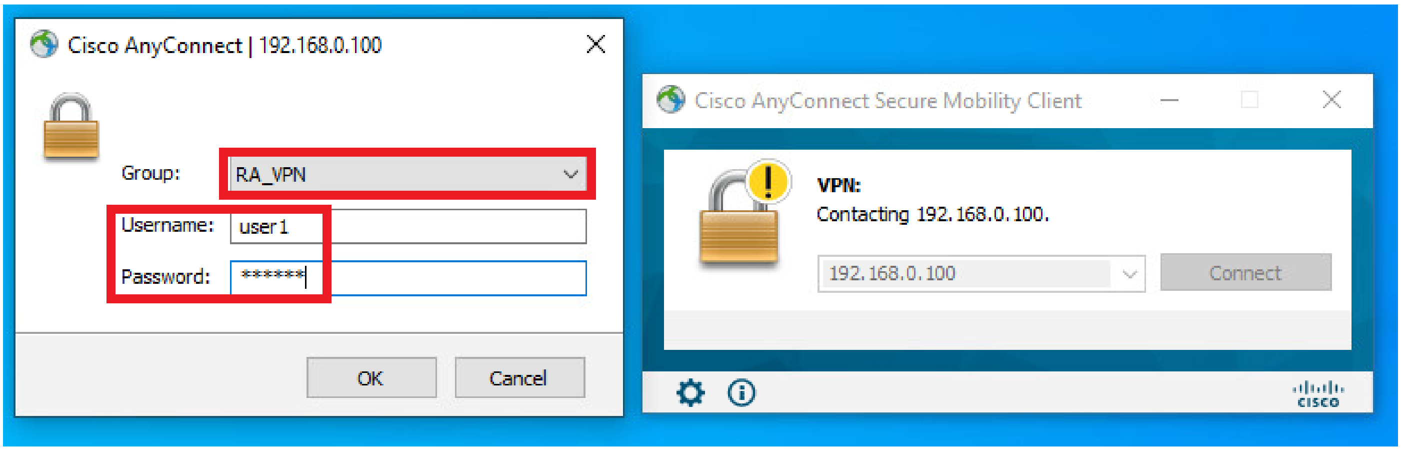
ステップ1:Cisco AnyConnectセキュアモビリティクライアントがインストールされているクライアントマシンに移動します。FTDへッドエンド（ここではWindowsマシンを使用）に接続し、*user1*クレデンシャルを入力します。



Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

192.168.0.100



Cisco AnyConnect | 192.168.0.100

Group: RA_VPN

Username: user1

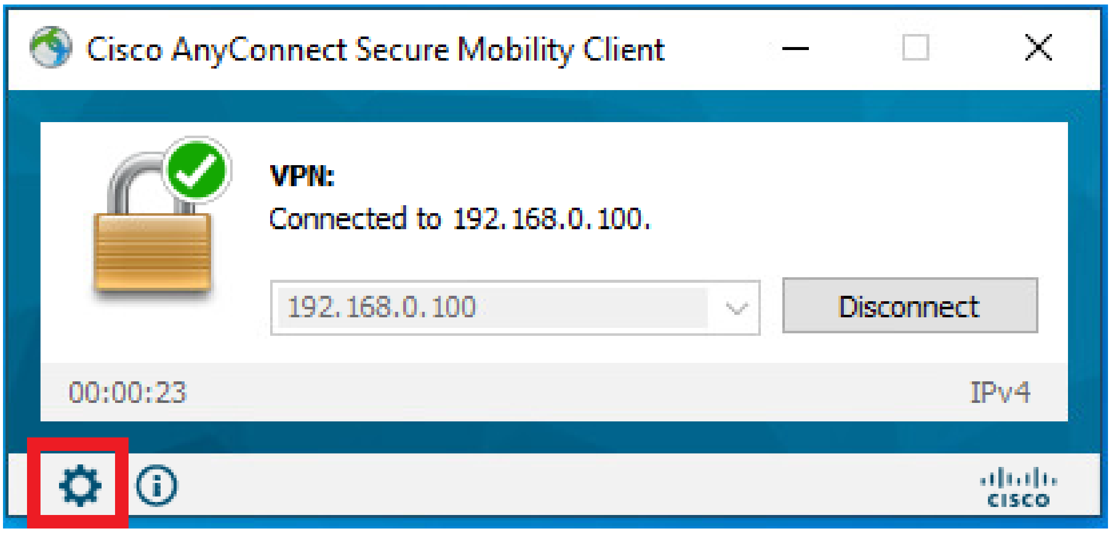
Password: ******

Cisco AnyConnect Secure Mobility Client

VPN:
Contacting 192.168.0.100.

192.168.0.100

歯車のアイコン（左下の角）をクリックして、[Statistics] タブに移動します。[Address Information]セクションで、割り当てられたIPアドレスが、このユーザのISE認証ポリシーで設定されているIPアドレスであることを確認します。

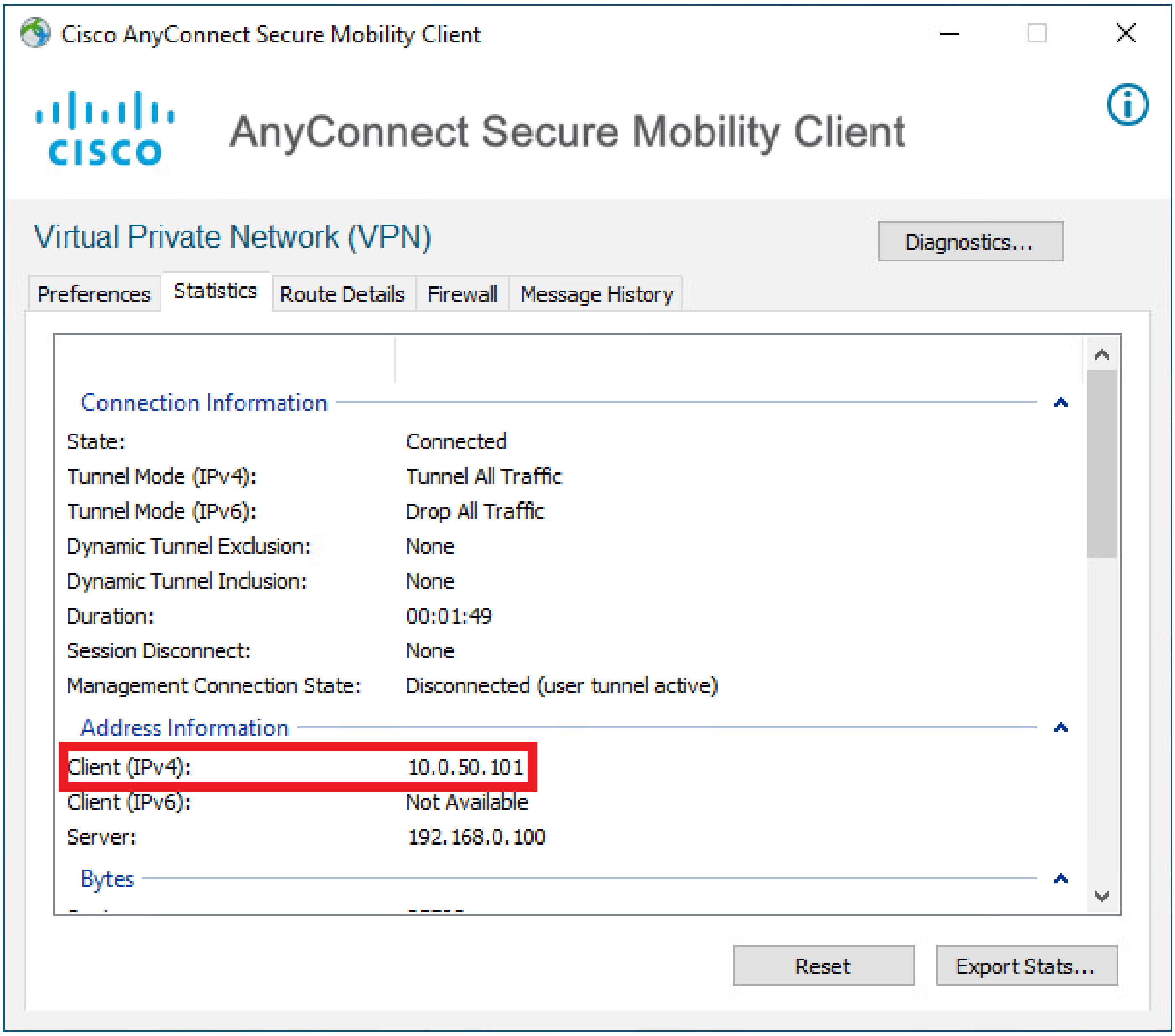


Cisco AnyConnect Secure Mobility Client

VPN:
Connected to 192.168.0.100.

192.168.0.100

00:00:23 IPv4


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Reset
Export Stats...

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

FTDでのdebug radius allコマンドの出力は次のとおりです。

```
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).....
```

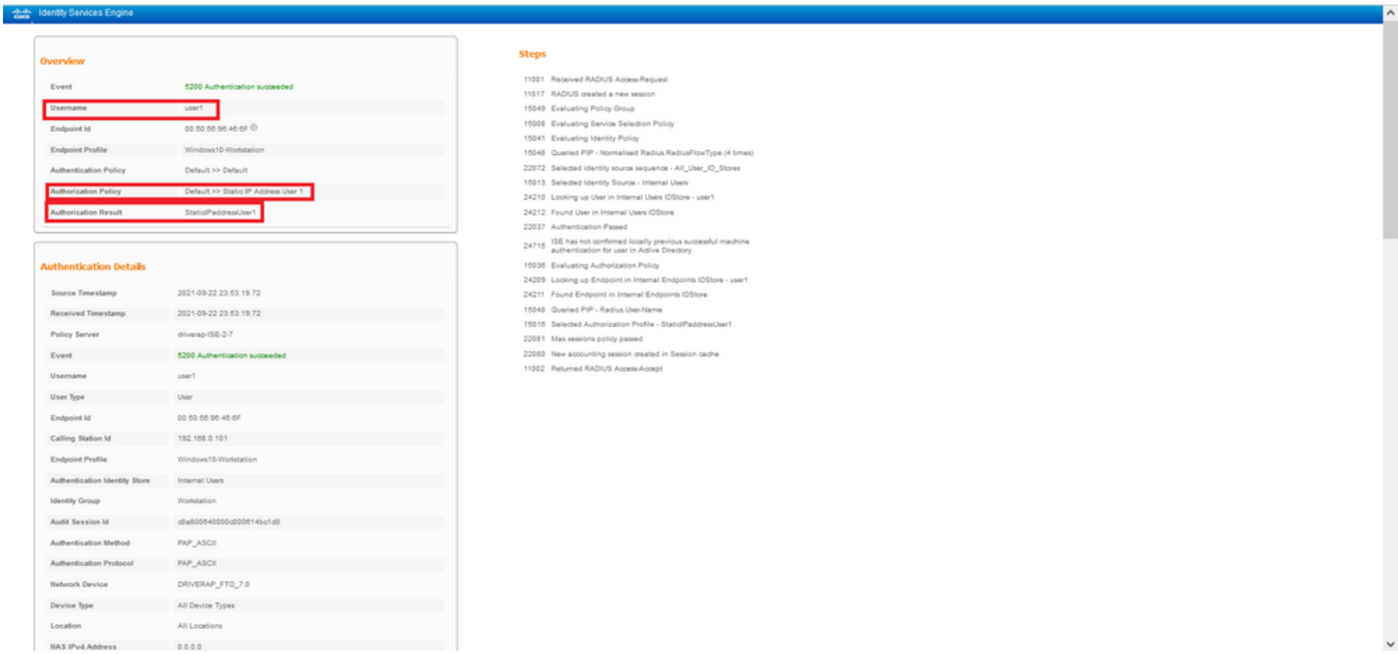
```
02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 | .......AK..X...1
7d aa 38 1e 01 07 75 73 65 72 31 08 06 0a 00 32 | }.8...user1....2
65 19 3d 43 41 43 53 3a 63 30 61 38 30 30 36 34 | e.=CACS:c0a80064
30 30 30 30 61 30 30 30 36 31 34 62 63 30 32 64 | 0000a000614bc02d
3a 64 72 69 76 65 72 61 70 2d 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
```

FTD のログは次のとおりです。

```
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:c0a800640000c000614bc1d0: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
```

ISEのRADIUS Liveログには次のように表示されます。



Identity Services Engine

Overview

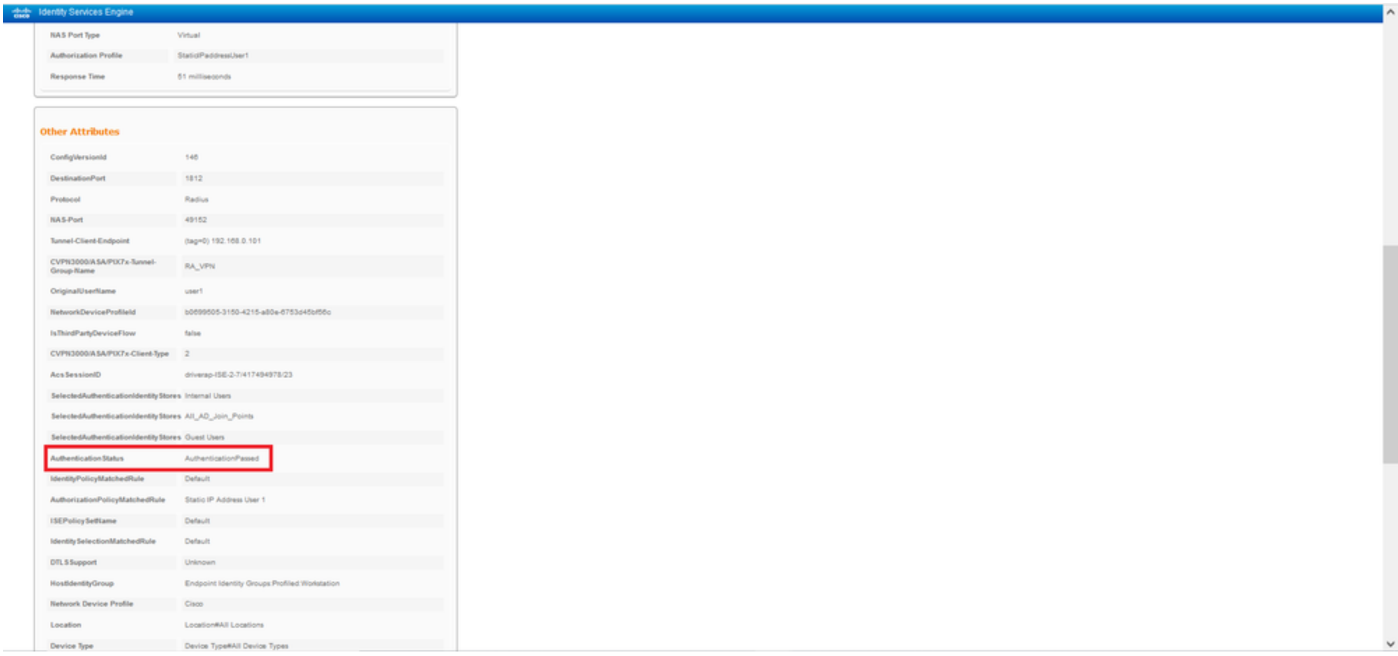
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:50:56:96:46:6F
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPaddressUser1

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	00:50:56:96:46:6F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	c0a800640000c000614bc1d0
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
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 Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	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 - user1
24212	Found User in Internal Users IDStore
22037	Authentication Passed
24715	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 Access-Accept

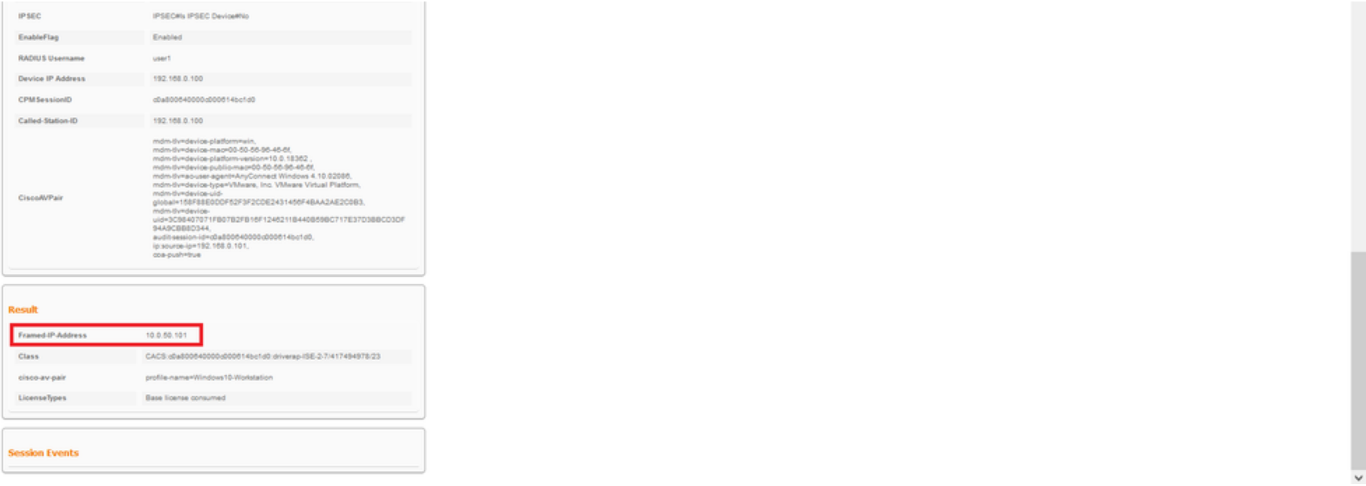


Identity Services Engine

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
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	RA_VPN
OriginalUserName	user1
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/23
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled:Workstation
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types



IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPMSessionID	c0a800640000c000614bc1d0
Called-Station-ID	192.168.0.100

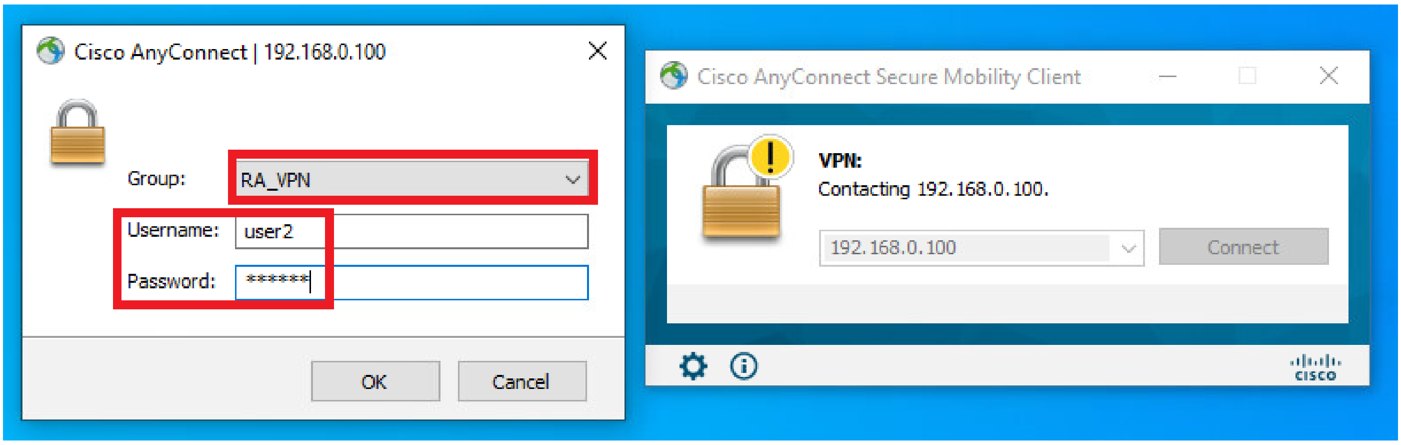
CiscoAVPair	mdm-tlv=device-platform=win,
	mdm-tlv=device-mac=00-50-56-96-46-6f,
	mdm-tlv=device-platform-version=10.0.18362 ,
	mdm-tlv=device-public-mac=00-50-56-96-46-6f,
	mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.02086,
	mdm-tlv=device-type=VMware, Inc. VMware Virtual Platform,
	mdm-tlv=device-uid-global=158F88E0DDF62F3F2CDE2431456F4BAA2AE2C0B3,
	mdm-tlv=device-uid=3C98407071FB07B2FB16F1246211B440B59BC717E37D3BBCD3DF94A9CBB8D344,
	audit-session-id=c0a800640000c000614bc1d0,
	ip:source-ip=192.168.0.101,
	coa-push=true

Result

Framed-IP-Address	10.0.50.101
Class	CACS:c0a800640000c000614bc1d0:driverap-ISE-2-7/417494978/23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Session Events

ステップ2:FTDヘッドエンド（ここではWindowsマシンを使用）に接続し、*user2*のクレデンシャルを入力します。



Cisco AnyConnect | 192.168.0.100

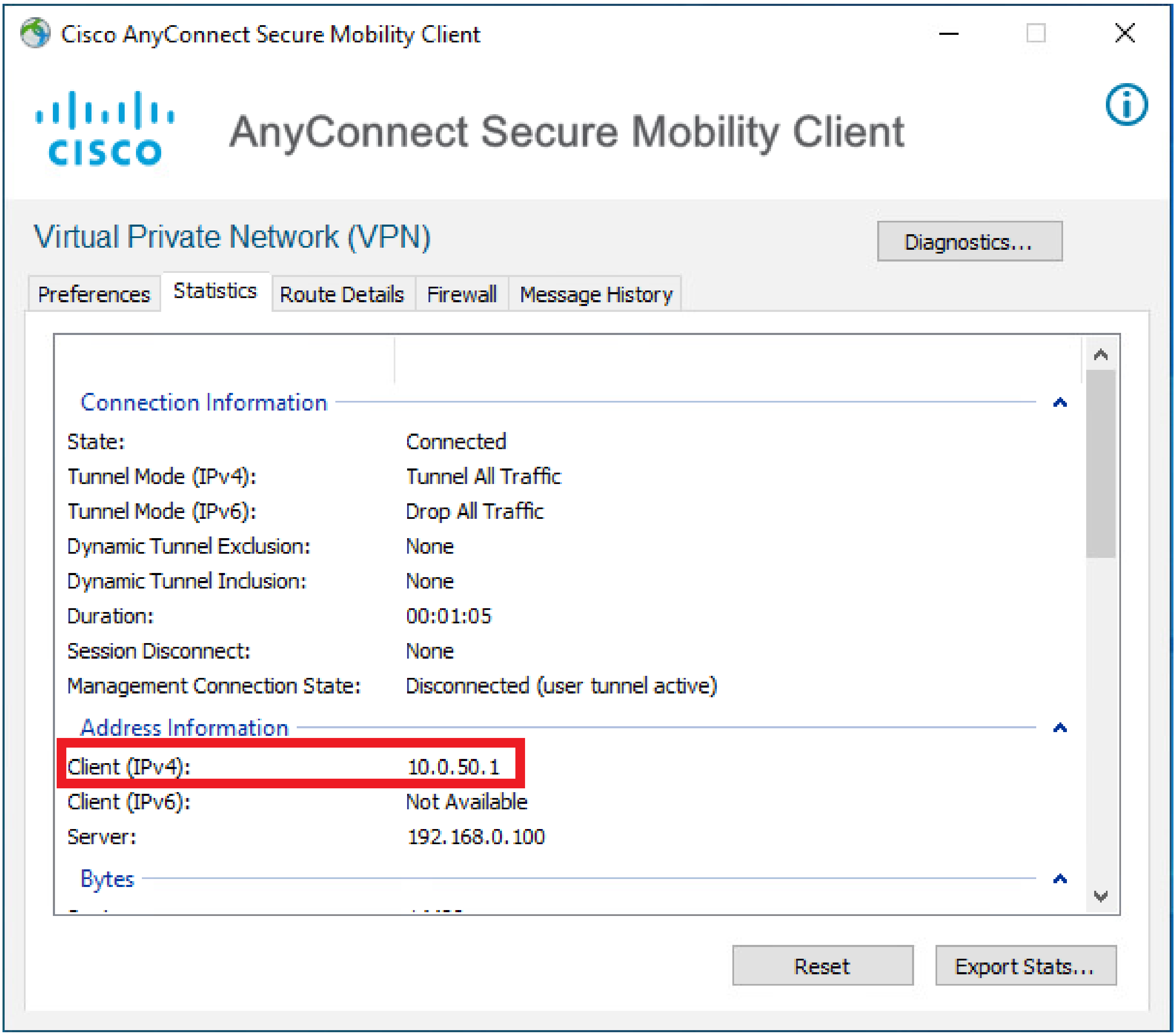
Group: RA_VPN

Username: user2

Password: ******

VPN:
Contacting 192.168.0.100.

[Address Information] セクションでは、割り当てられたIPアドレスが、FMCを介して設定されたIPv4ローカルプールで使用可能な最初のIPアドレスであることが示されています。



Cisco AnyConnect Secure Mobility Client
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: 00:01:05
Session Disconnect: None
Management Connection State: Disconnected (user tunnel active)

Address Information

Client (IPv4): 10.0.50.1
Client (IPv6): Not Available
Server: 192.168.0.100

Bytes

FTDでの**debug radius all**コマンドの出力は次のとおりです。

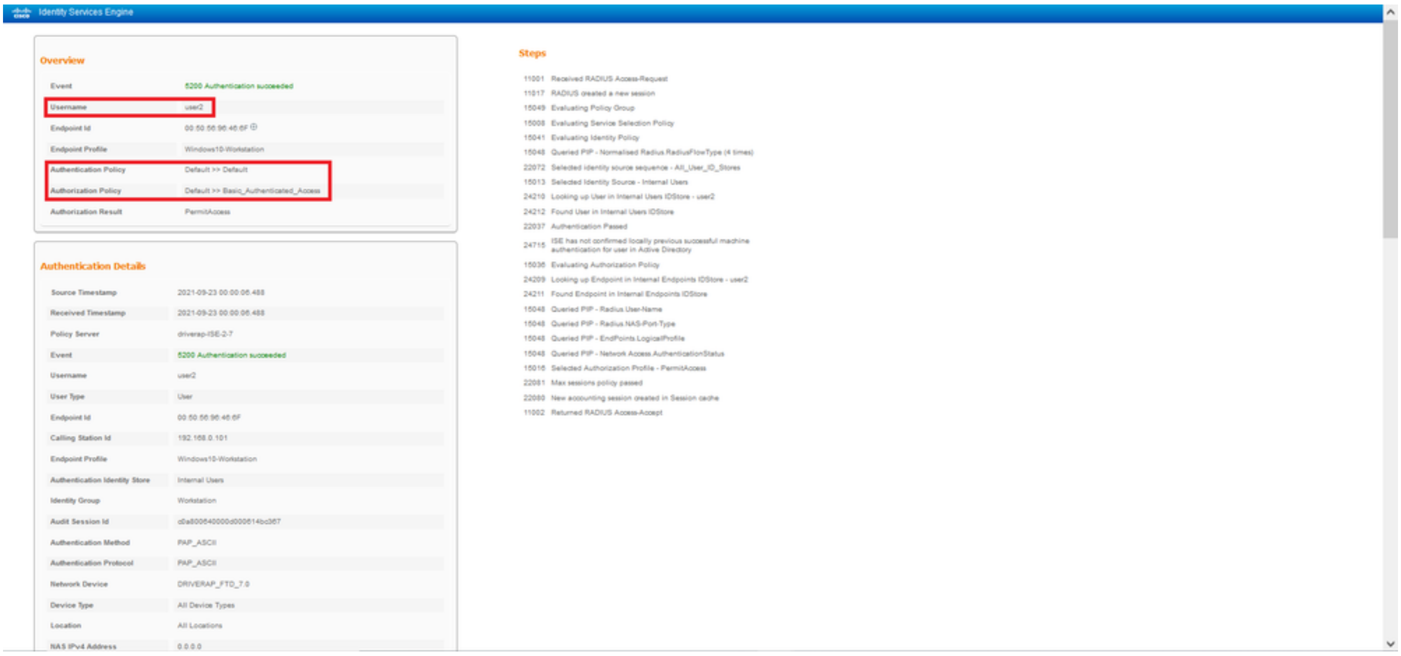
```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
```

```
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
```

FTD のログは次のとおりです。

```
<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: 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 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
```

ISEのRADIUS Liveログには次のように表示されます。



Overview

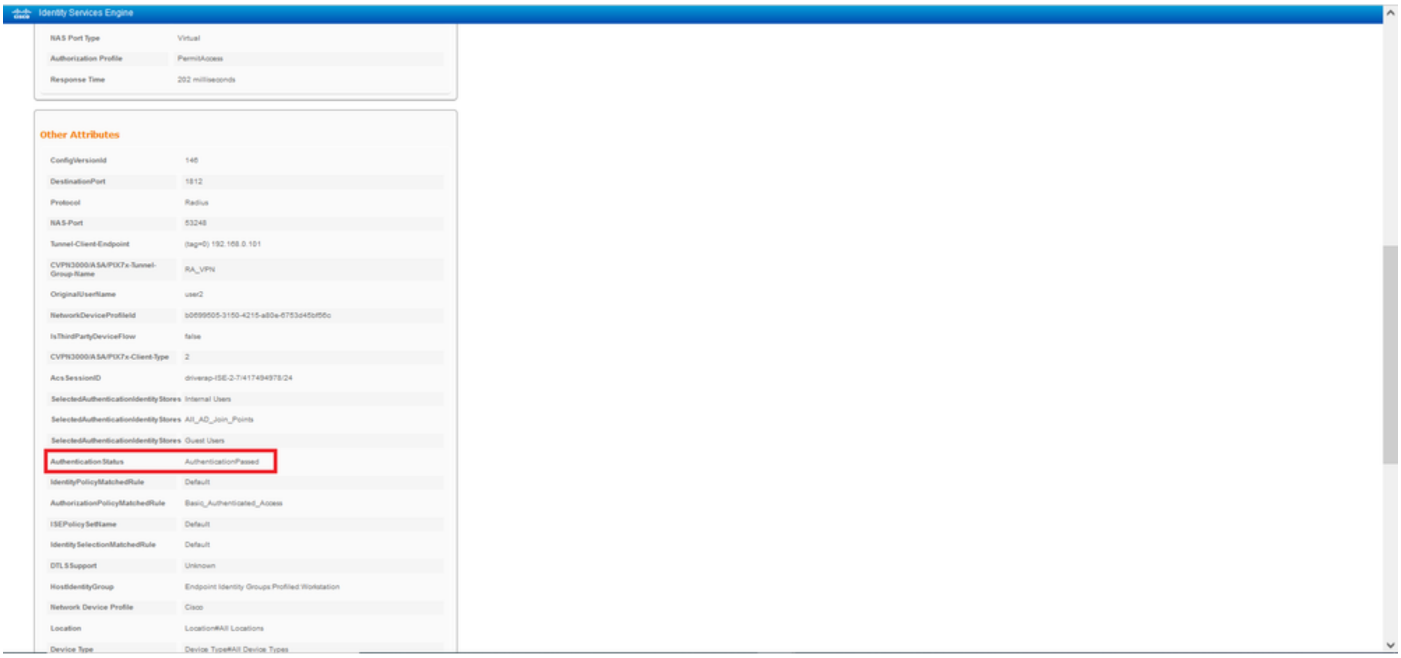
Event	5200 Authentication succeeded
Username	user2
Endpoint Id	00:50:56:96:46:6F
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2021-09-23 00:00:06.488
Received Timestamp	2021-09-23 00:00:06.488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	00:50:56:96:46:6F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	c0a800640000d000614bc367
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	DRIVERAP_FTD_7.0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

Steps

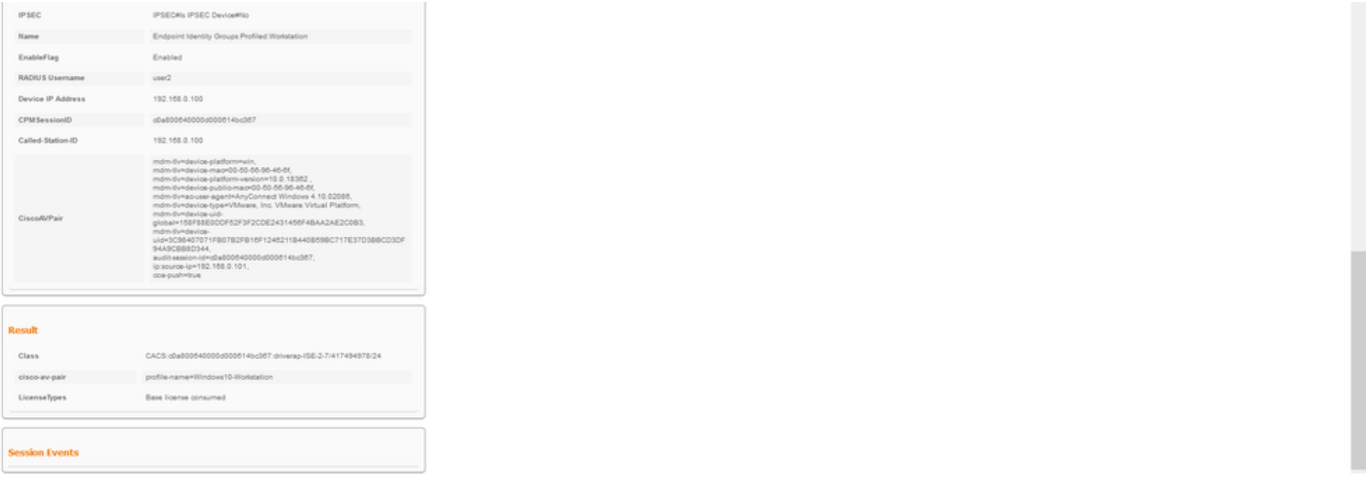
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType (4 times)
22072	Selected identity source sequence - All_User_ID_Stores
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
24715	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.LogicalProfile
15048	Queried PIP - Network Access.AuthenticationStatus
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11002	Returned RADIUS Access-Accept



NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	202 milliseconds

Other Attributes

ConfigVersionId	146
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	RA_VPN
OriginalUserName	user2
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/24
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled:Workstation
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types



IPSEC	IPSEC#Is IPSEC Device#No
Name	Endpoint Identity Groups:Profiled:Workstation
EnableFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPMSessionID	c0a800640000d000614bc367
Called-Station-ID	192.168.0.100

CiscoAVPair	mdm-tlv=device-platform=win,
	mdm-tlv=device-mac=00-50-56-96-46-6f,
	mdm-tlv=device-platform-version=10.0.18362 ,
	mdm-tlv=device-public-mac=00-50-56-96-46-6f,
	mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.02086,
	mdm-tlv=device-type=VMware, Inc. VMware Virtual Platform,
	mdm-tlv=device-uid-global=158F88E0DDF52F3F2CDE2431456F4BAA2AE2C0B3,
	mdm-tlv=device-uid=3C98407071FB07B2FB16F1246211B4408598C717E37D3BBCD3DF94A9CBB8D344,
	audit-session-id=c0a800640000d000614bc367,
	ip:source-ip=192.168.0.101,
	coa-push=true

Result

Class	CACS:c0a800640000d000614bc367:driverap-ISE-2-7/417494978/24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Session Events

注：AnyConnectクライアント間で重複するIPアドレスの競合を避けるには、FTD ipローカルプールとISE認可ポリシーの両方でIPアドレス割り当てに異なるIPアドレス範囲を使用する必要があす。この設定例では、10.0.50.1から10.0.50.100までのIPv4ローカルプールを使用してFTDが設定され、ISEサーバは10.0.50.101の静的IPアドレスを割り当てます。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

FTD：

- **debug radius all**

ISE:

- RADIUS ライブ ログ