

# 通过RADIUS授权配置静态IP地址分配给AnyConnect用户

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[通过FMC配置使用AAA/RADIUS身份验证的远程访问VPN](#)

[在ISE \( RADIUS服务器 \) 上配置授权策略](#)

[验证](#)

[故障排除](#)

## 简介

本文档介绍如何使用身份服务引擎(ISE)服务器配置RADIUS授权，以便它始终通过RADIUS属性8 Framed-IP-Address将同一IP地址转发到特定Cisco AnyConnect安全移动客户端用户的Firepower威胁防御(FTD)。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- FTD
- Firepower管理中心(FMC)
- ISE
- Cisco AnyConnect 安全移动客户端
- RADIUS协议

### 使用的组件

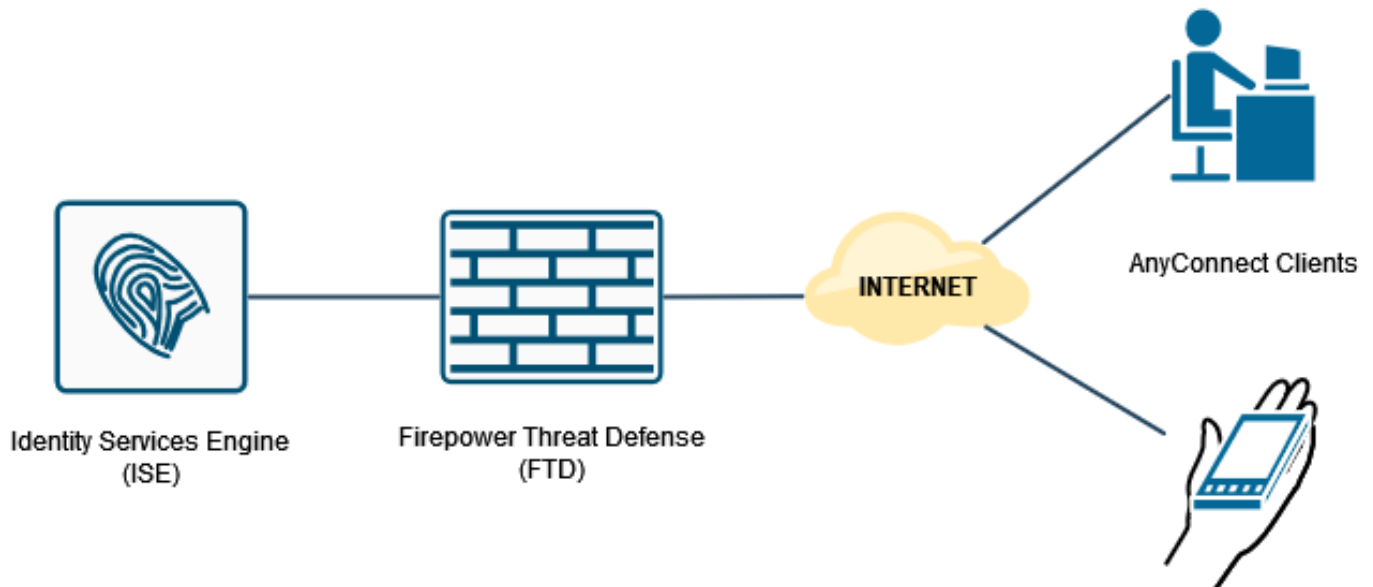
本文档中的信息基于以下软件版本：

- FMCv - 7.0.0 ( 内部版本94 )
- FTDv - 7.0.0 ( 内部版本94 )
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086
- Windows 10专业版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

### 网络图



### 通过FMC配置使用AAA/RADIUS身份验证的远程访问VPN

有关分步过程，请参阅本文档和此视频：

- [FTD上的AnyConnect远程访问VPN配置](#)
- [FTD的初始AnyConnect配置，由FMC管理](#)

FTD CLI上的远程访问VPN配置为：

```
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
```

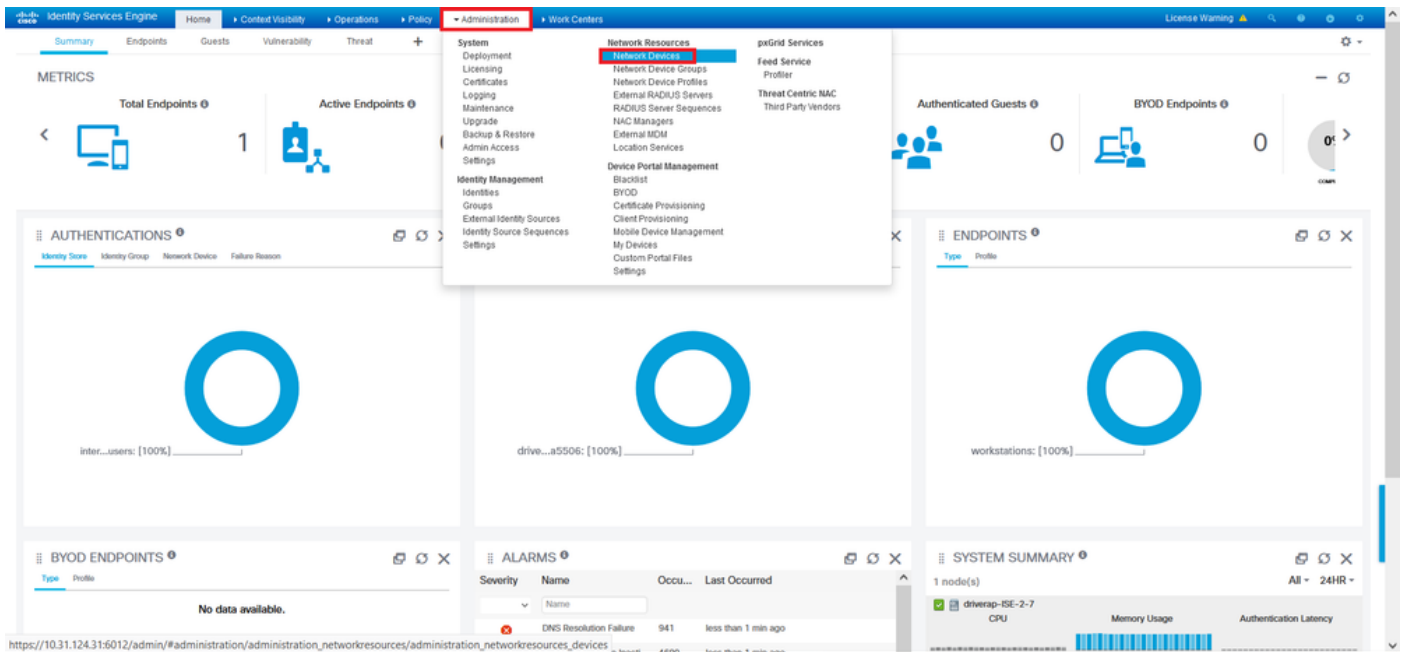
```
webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list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

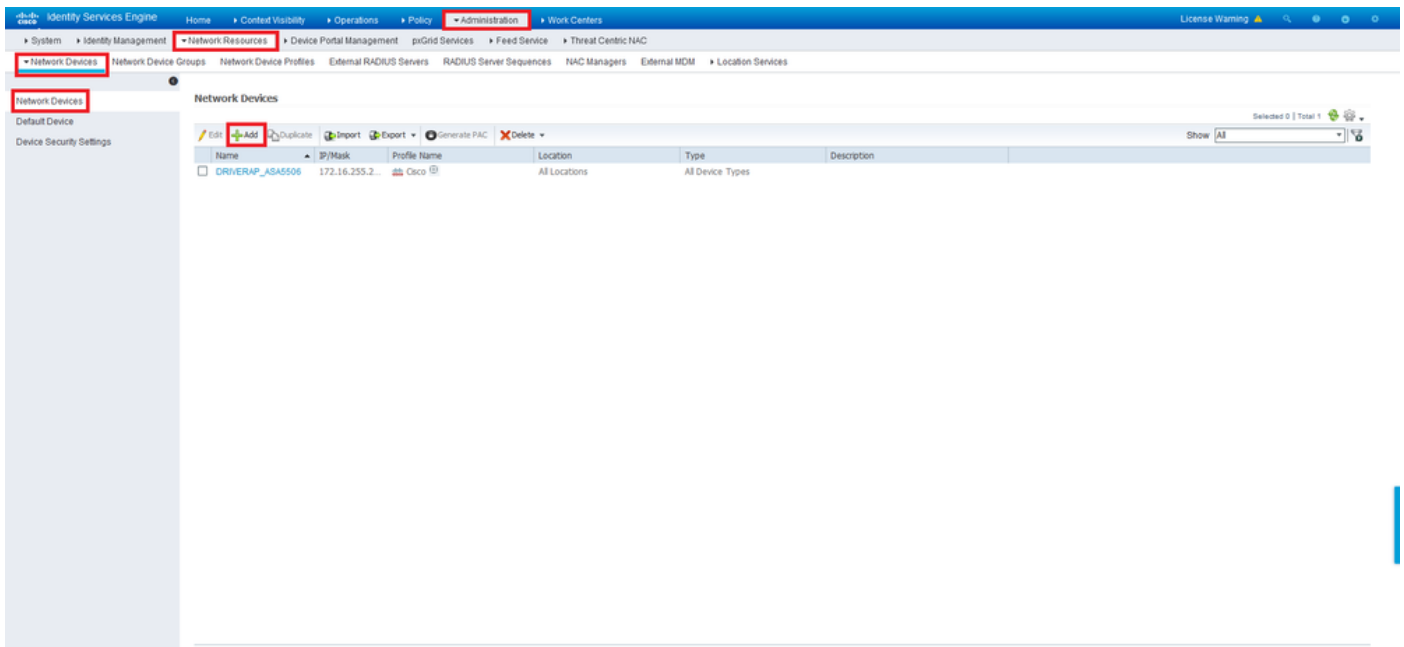
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

## 在ISE ( RADIUS服务器 ) 上配置授权策略

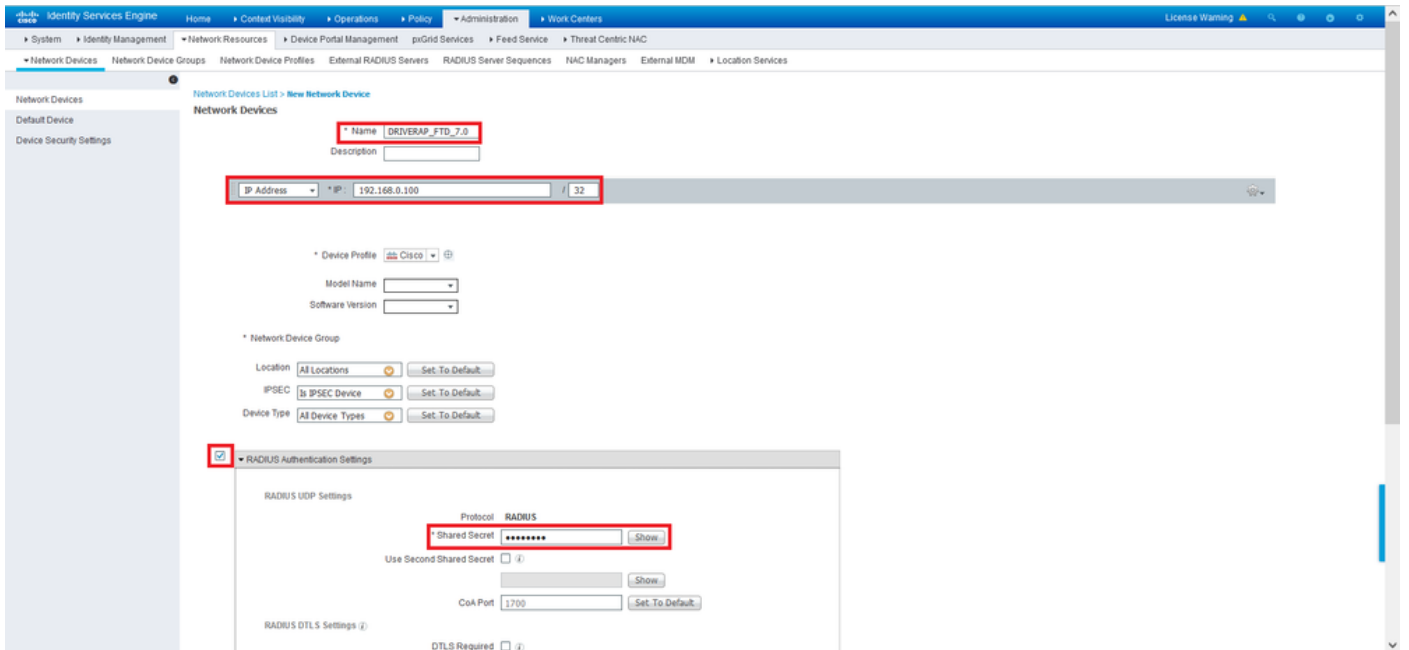
步骤1.登录ISE服务器并导航至Administration > Network Resources > Network Devices。



步骤2.在“网络设备”部分，单击添加，以便ISE可以处理来自FTD的RADIUS访问请求。

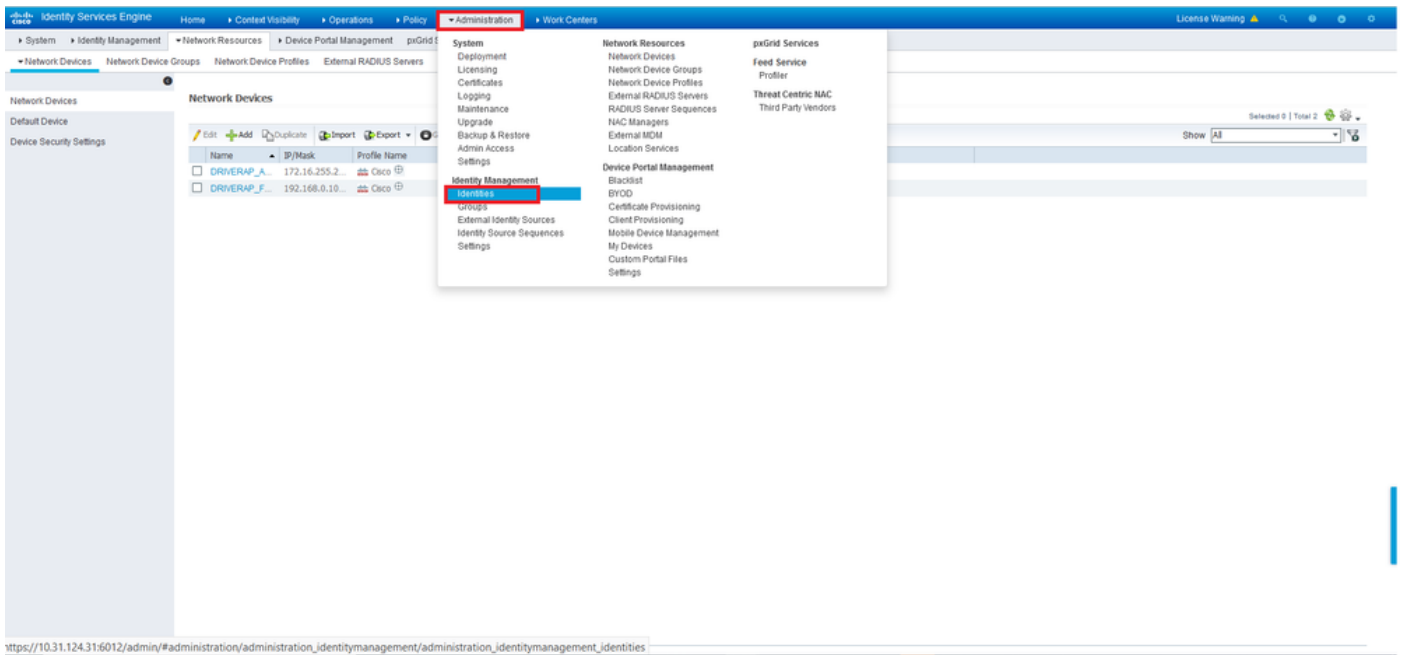


输入网络设备名称和IP地址字段，然后选中RADIUS Authentication Settings框。共享密钥必须与在FMC上创建RADIUS服务器对象时使用的值相同。

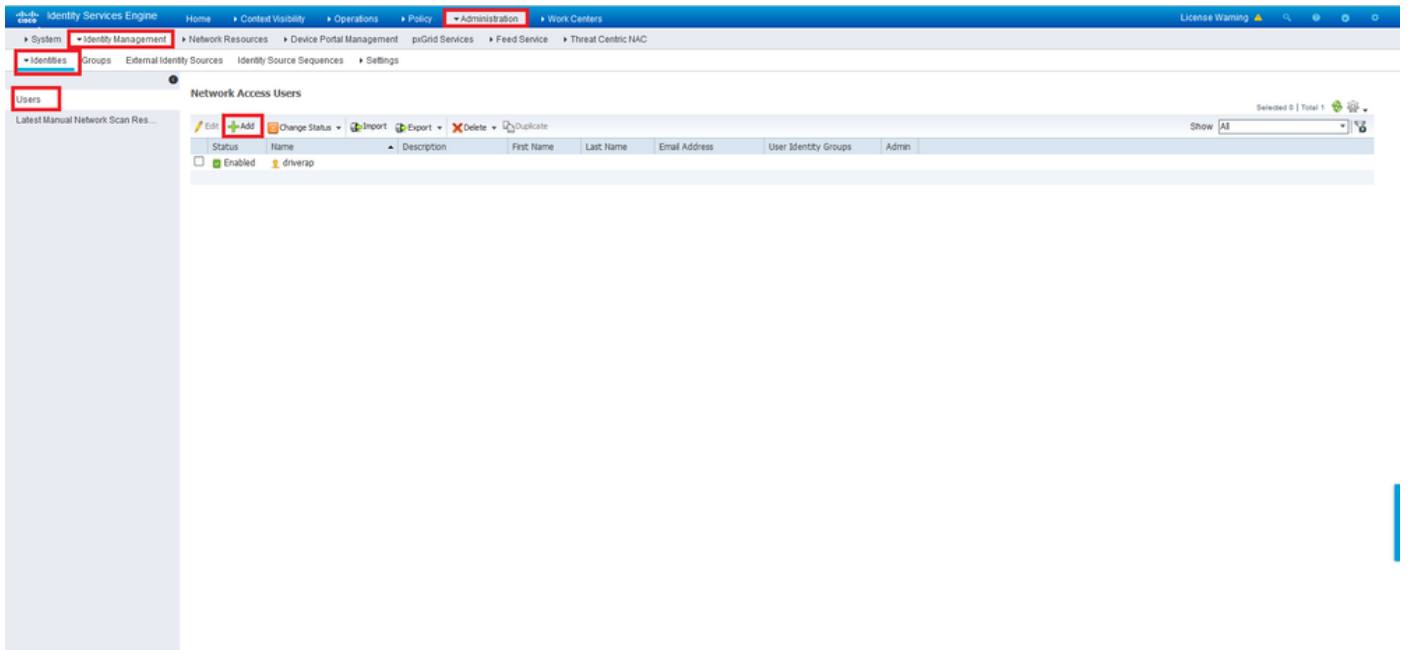


用此页末的按钮保存。

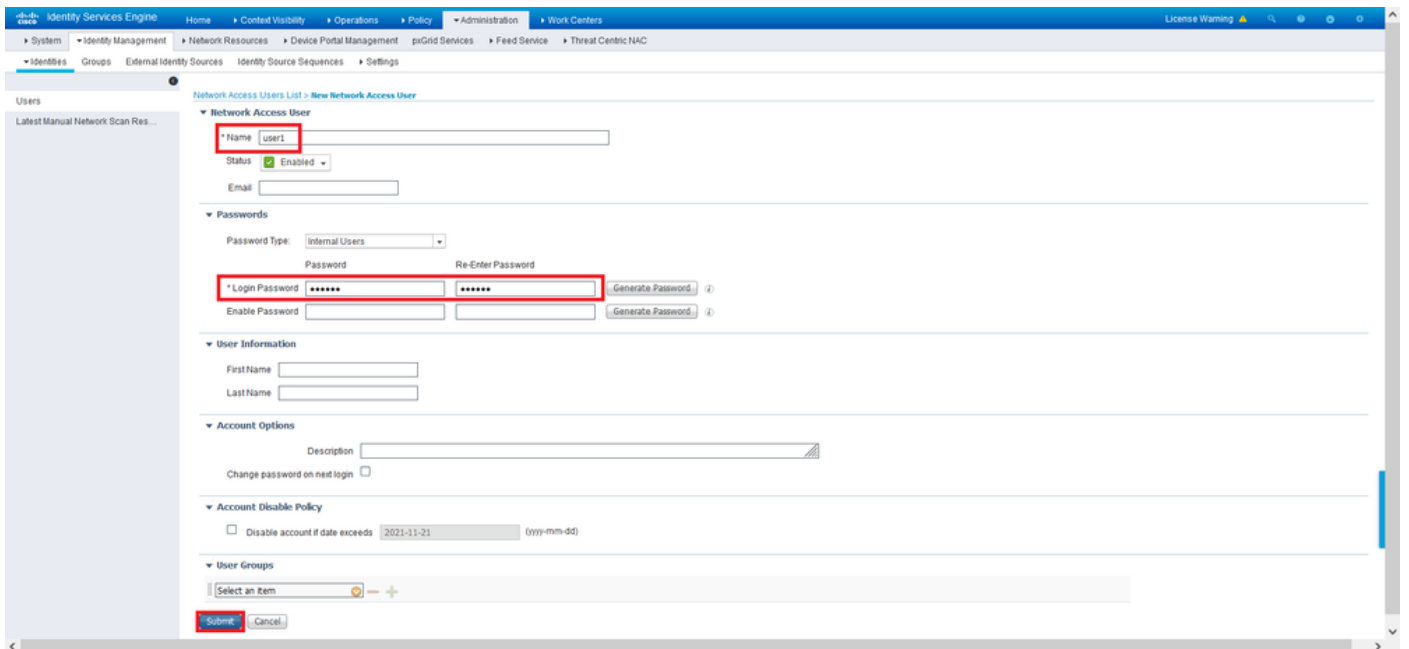
步骤3. 导航至Administration > Identity Management > Identities。



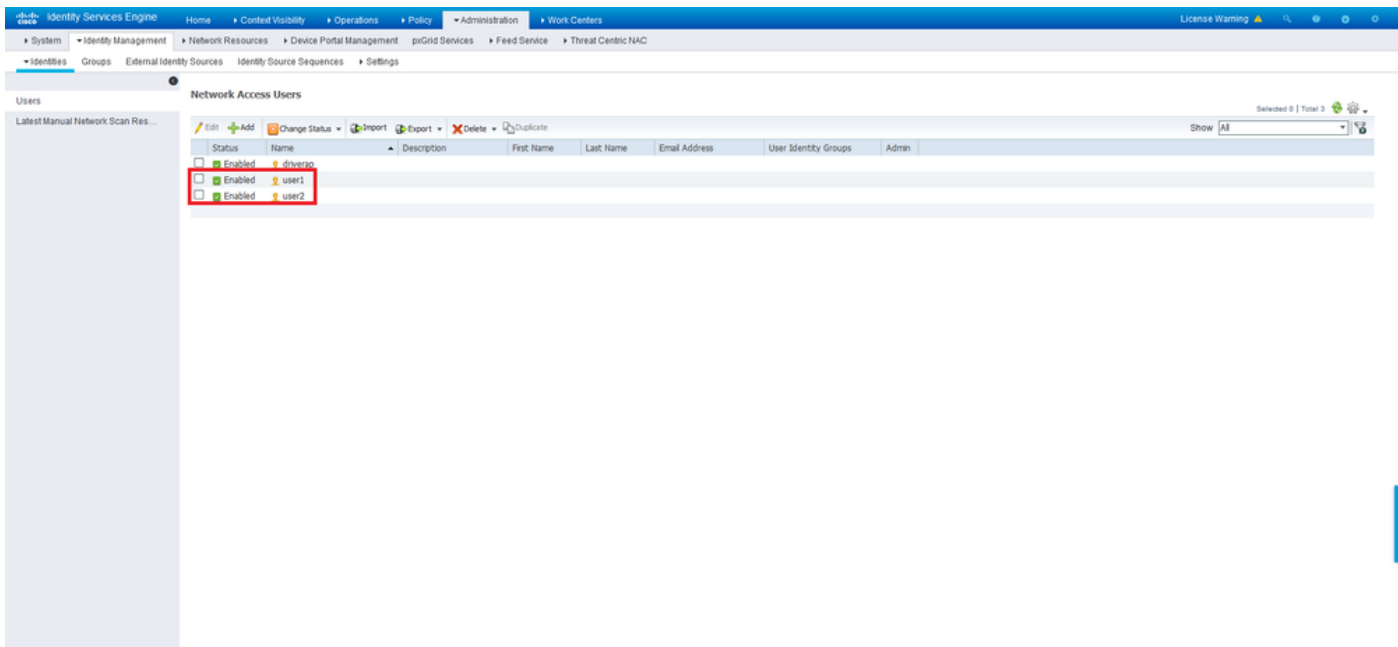
步骤4. 在Network Access Users部分中，单击Add以在ISE的本地数据库中创建user1。



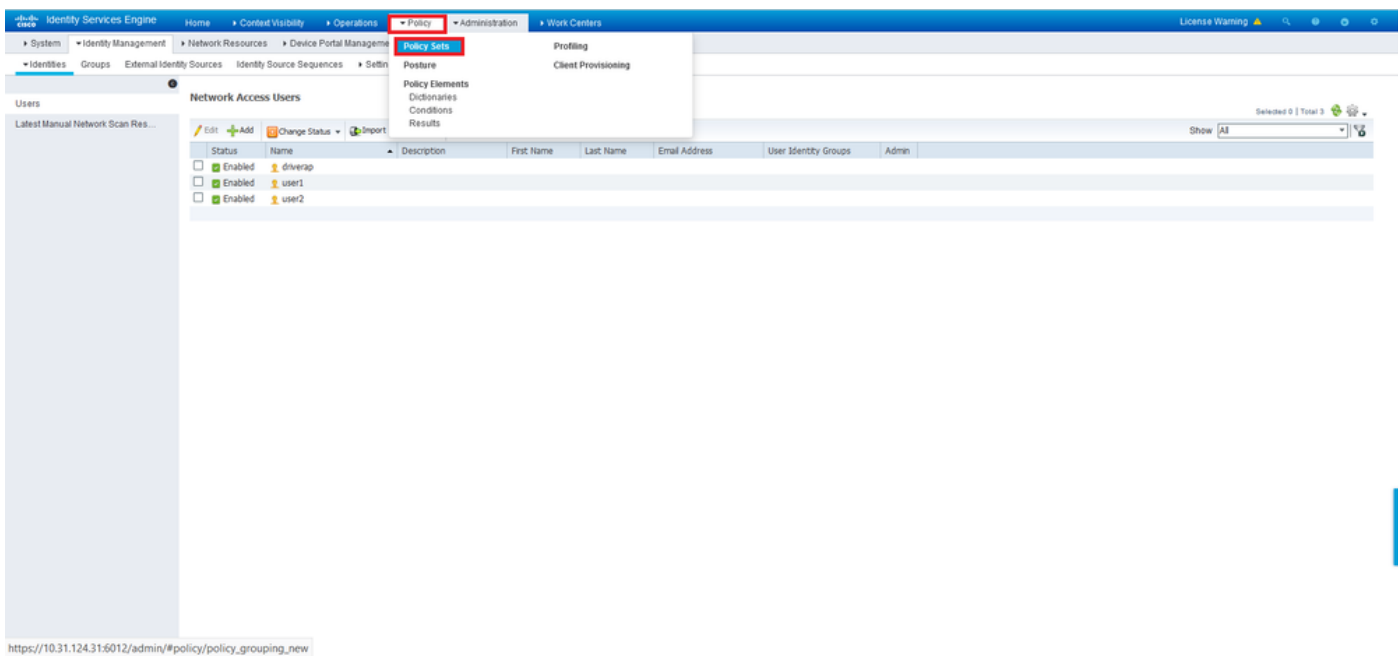
在“名称”和“登录密码”字段中输入用户名和密码，然后单击提交。



步骤5.重复上述步骤以创建user2。

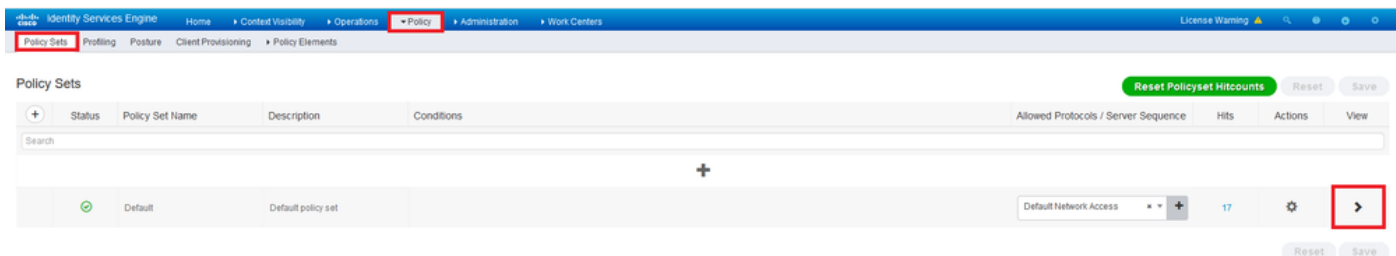


步骤6. 导航至 Policy > Policy Sets。

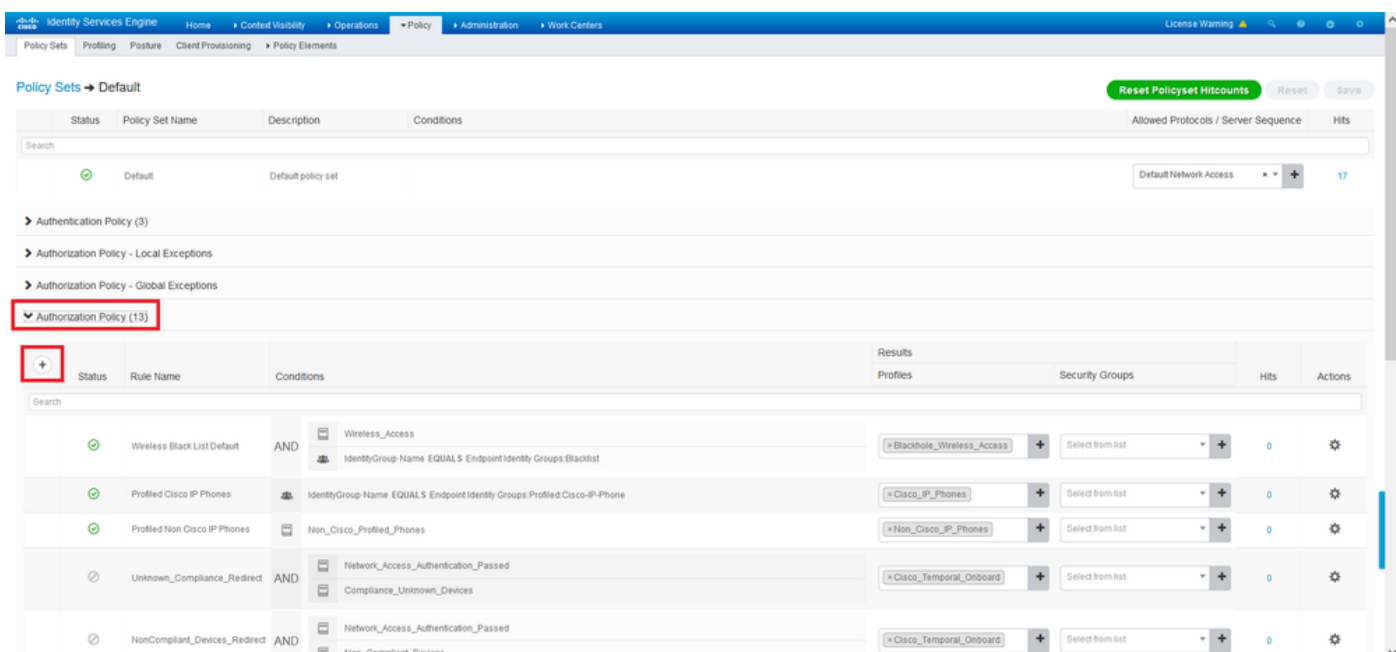


[https://10.31.124.31:6012/admin/#policy/policy\\_grouping\\_new](https://10.31.124.31:6012/admin/#policy/policy_grouping_new)

步骤7. 单击屏幕右侧的箭头>。



步骤8.单击Authorization Policy(授权策略)旁边的箭头>展开它。现在，单击+符号以添加新规则。

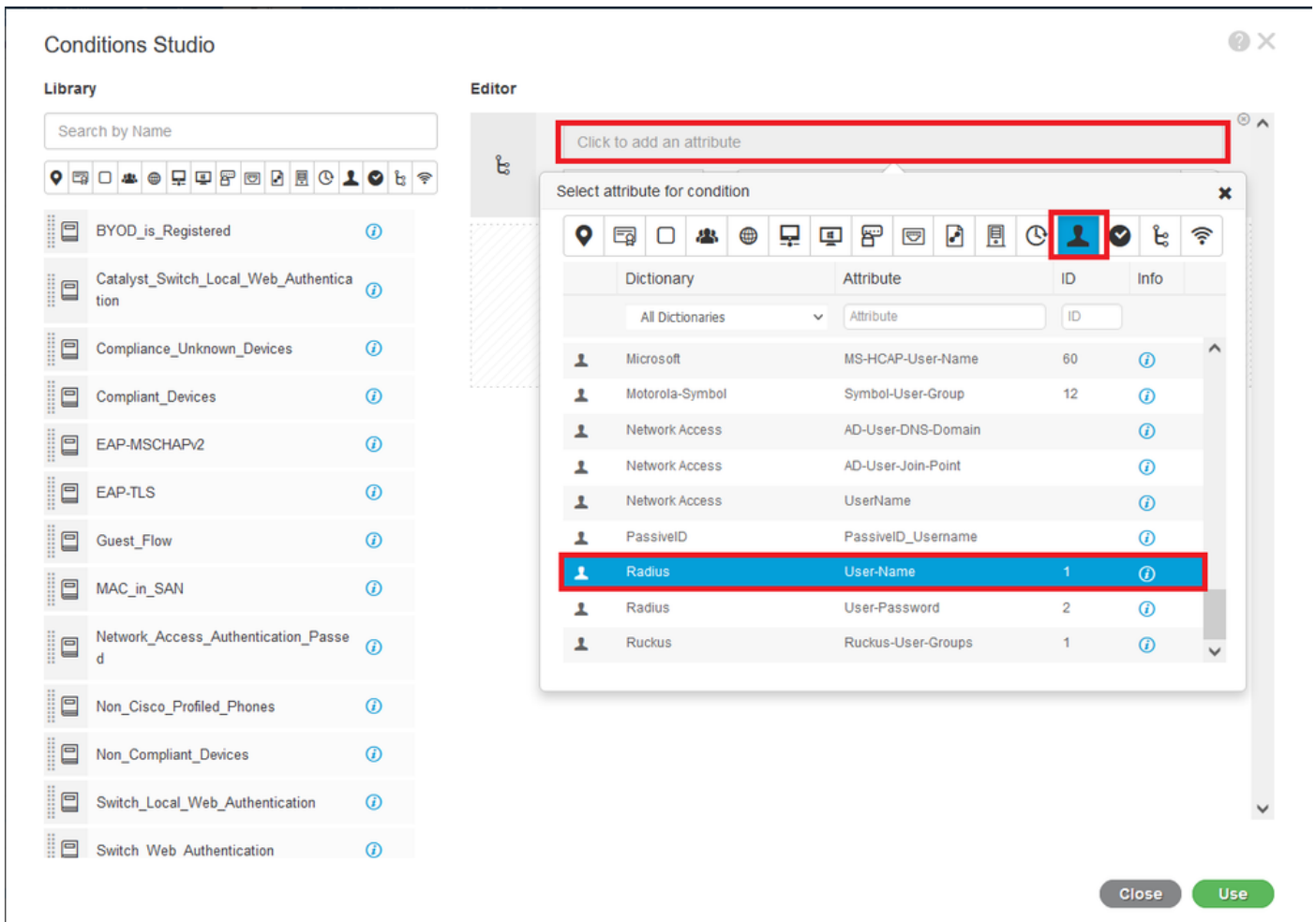


为规则提供名称，然后在“条件”列下选择+符号。

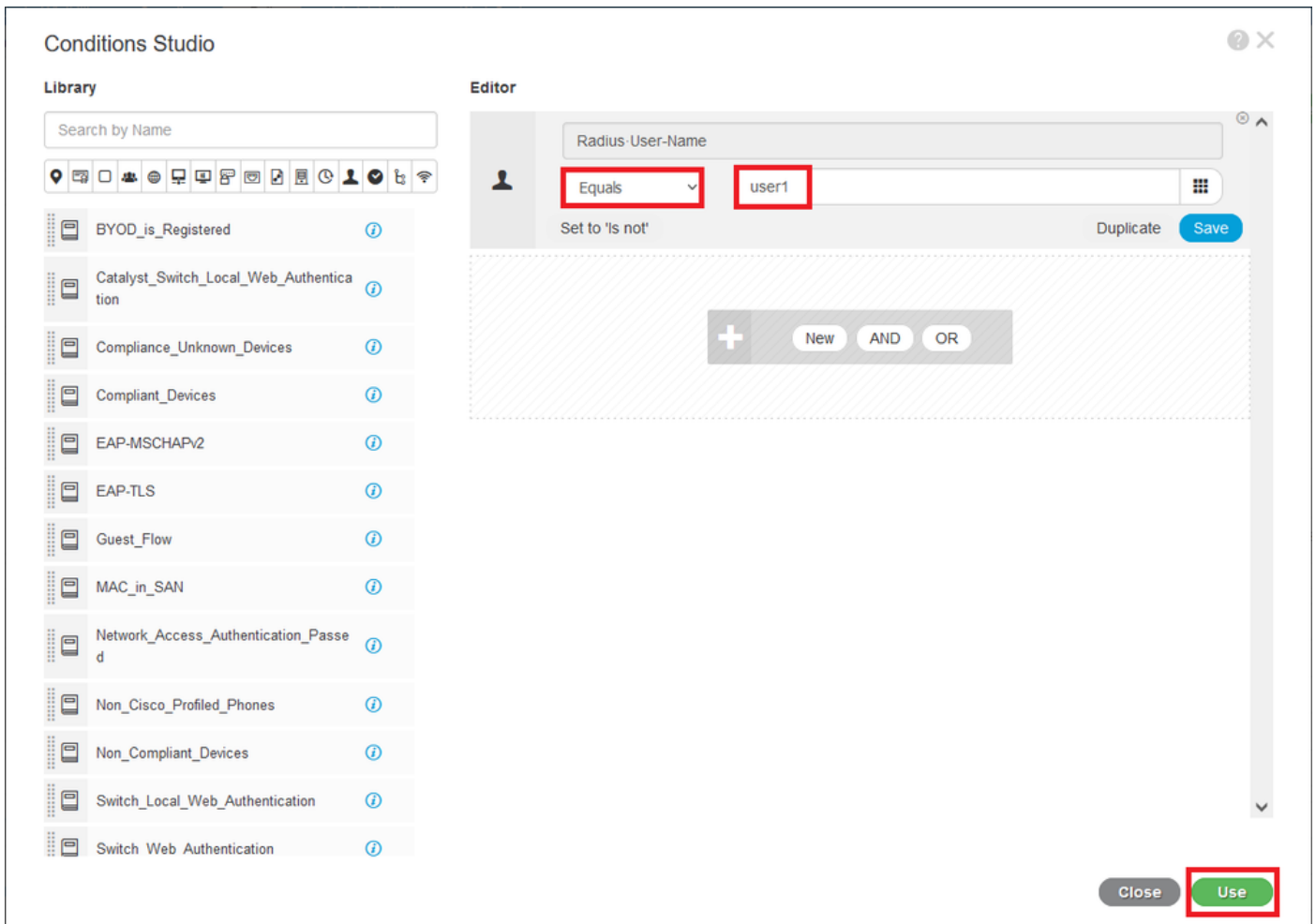


单击“属性编辑器”(Attribute Editor)文本框，然后单击“主题”(Subject)图标。向下滚动，直到您找到RADIUS User-Name属性并选择它。



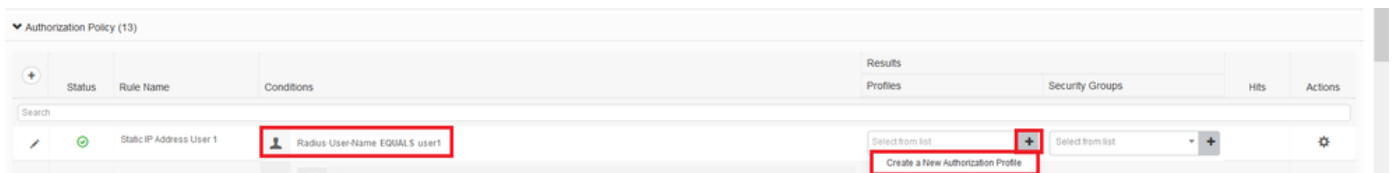


将**Equals**保留为运算符，并在其旁边的文本框中输入user1。单击**Use**以保存属性。

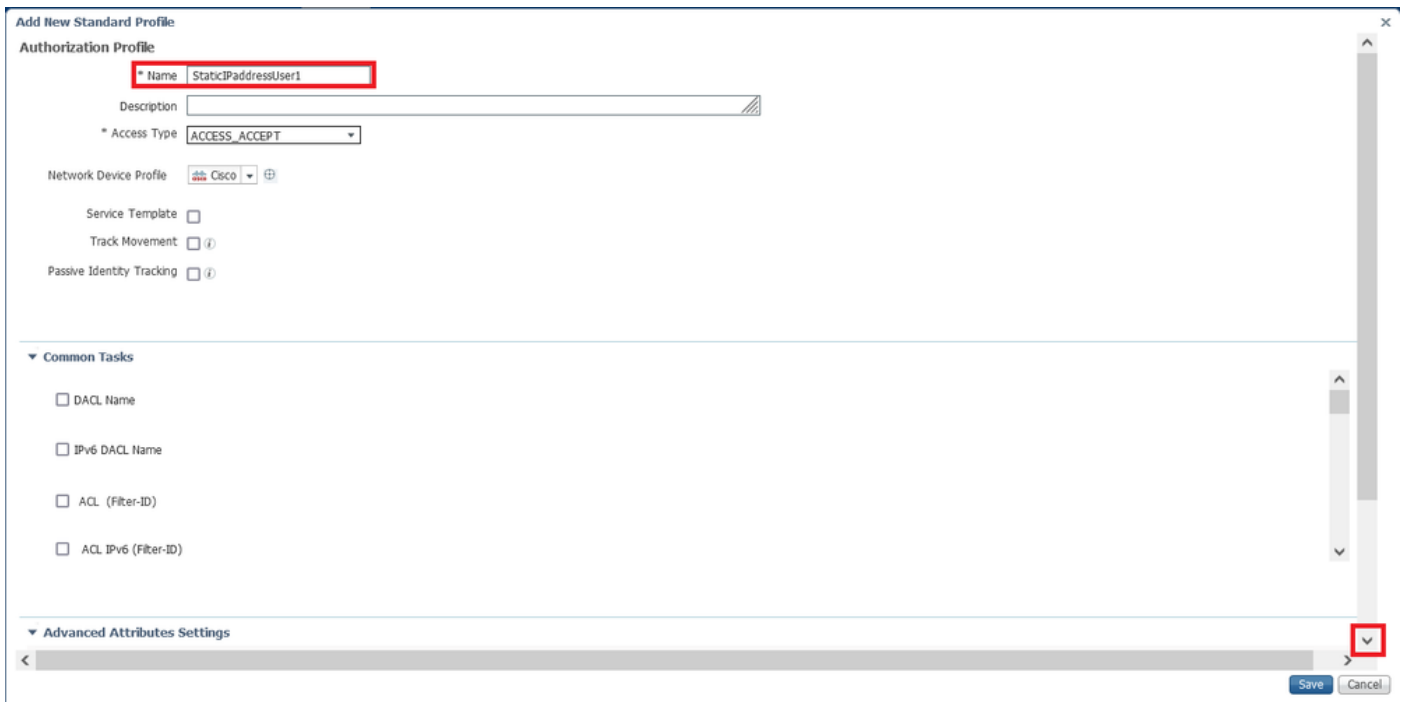


此规则的条件现已设置。

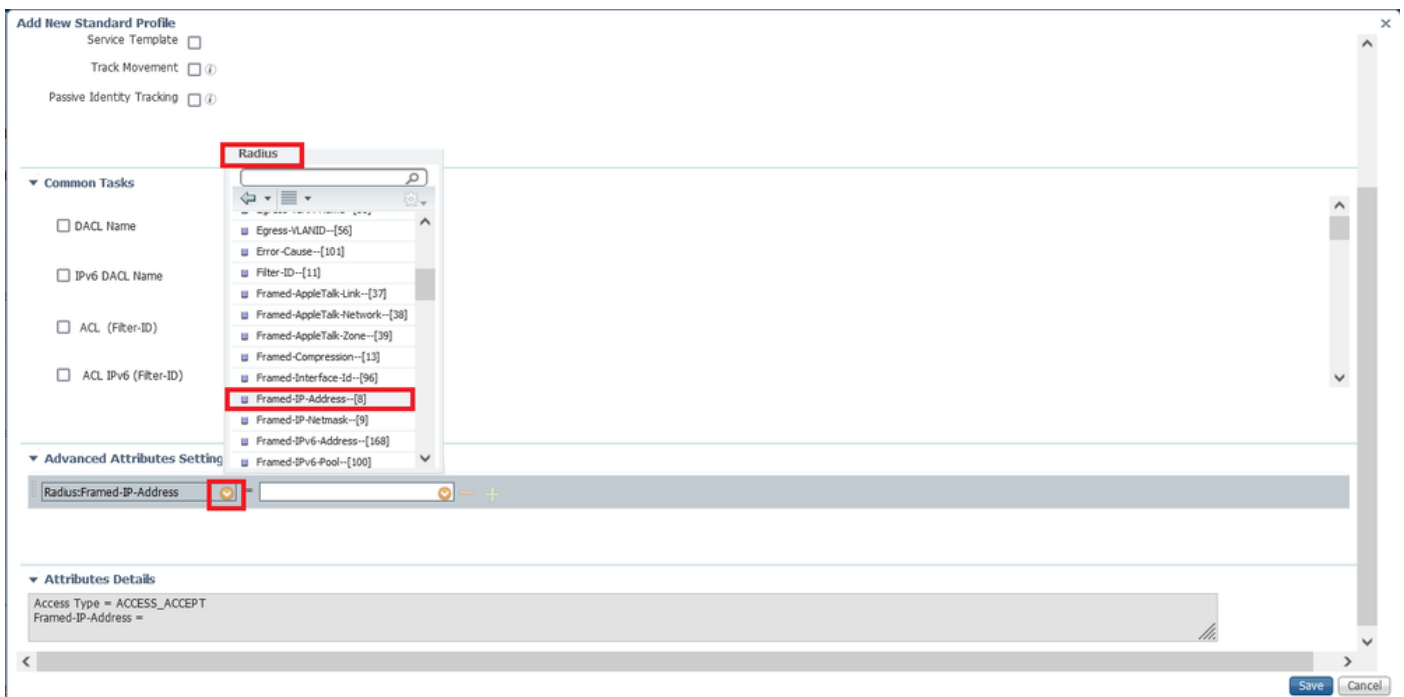
步骤9.在“结果/配置文件”列中，单击+号并选择“创建新授权配置文件”。



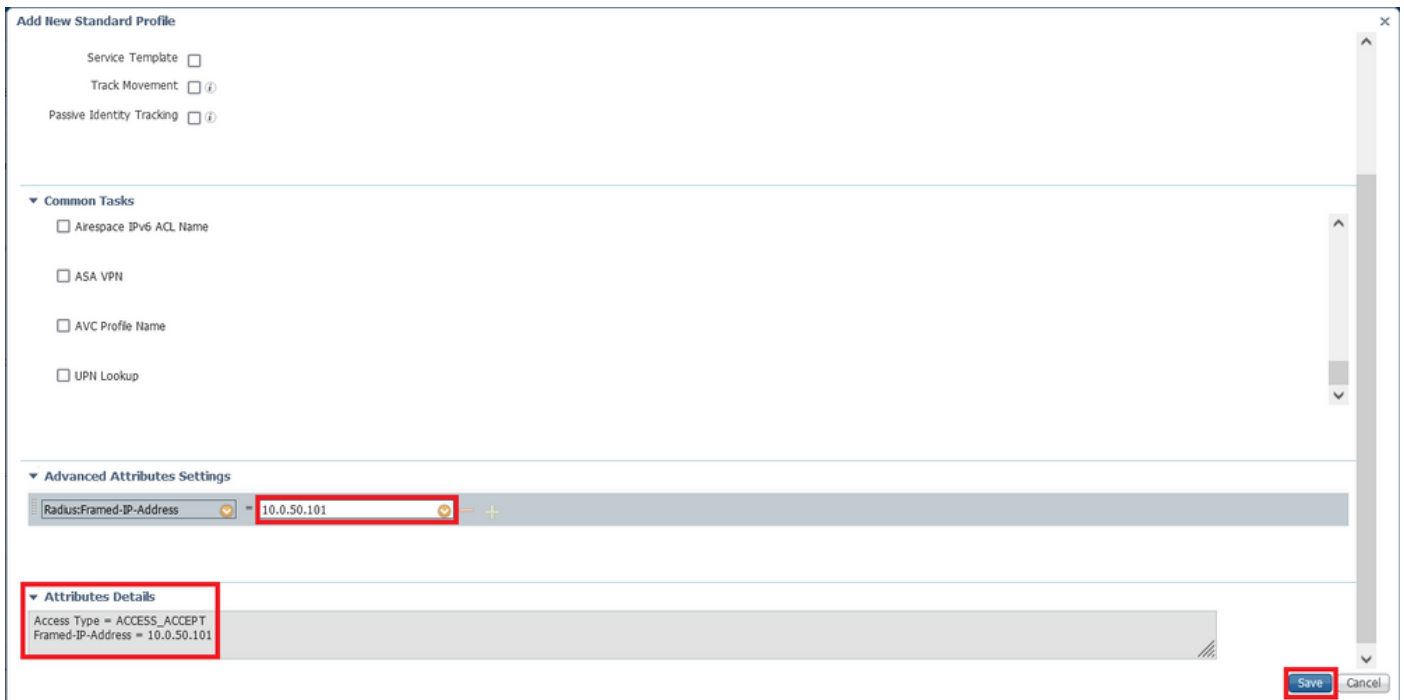
为其指定名称，并将ACCESS\_ACCEPT保留为访问类型。向下滚动到“高级属性设置”部分。



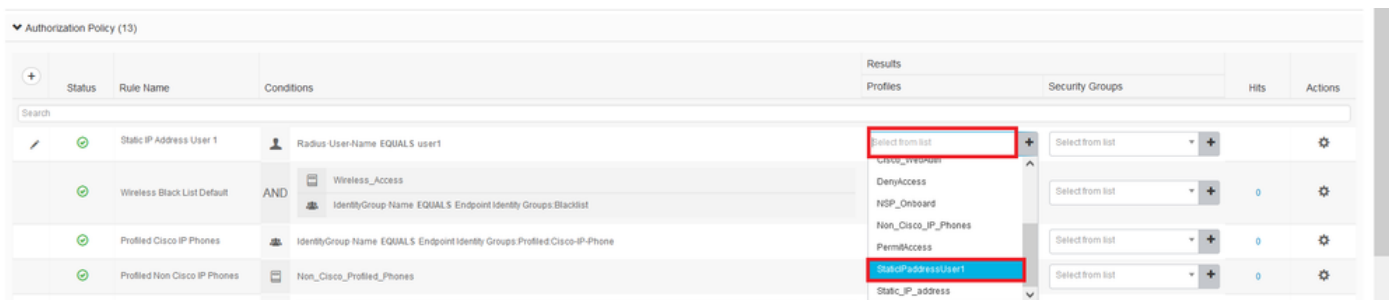
单击橙色箭头并选择Radius > Framed-IP-Address—[8]。



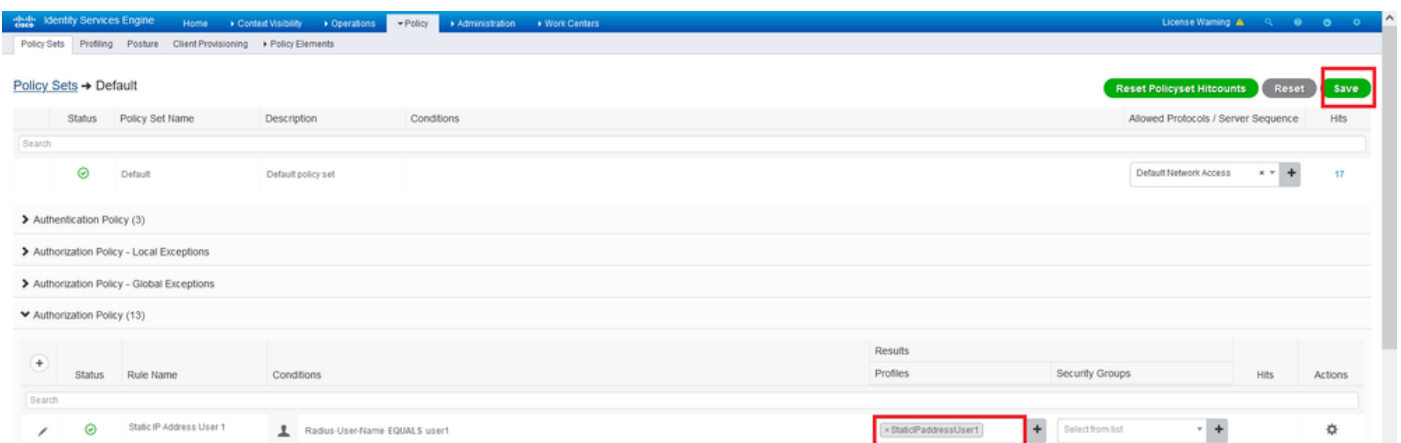
键入要始终静态分配给此用户的IP地址，然后单击Save。



步骤10.现在，选择新创建的授权配置文件。

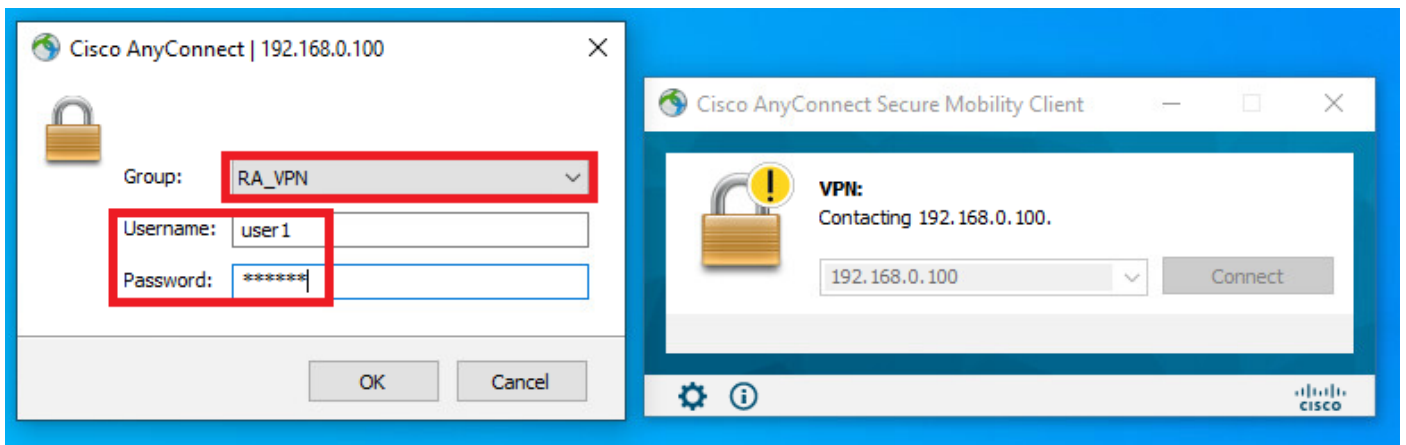
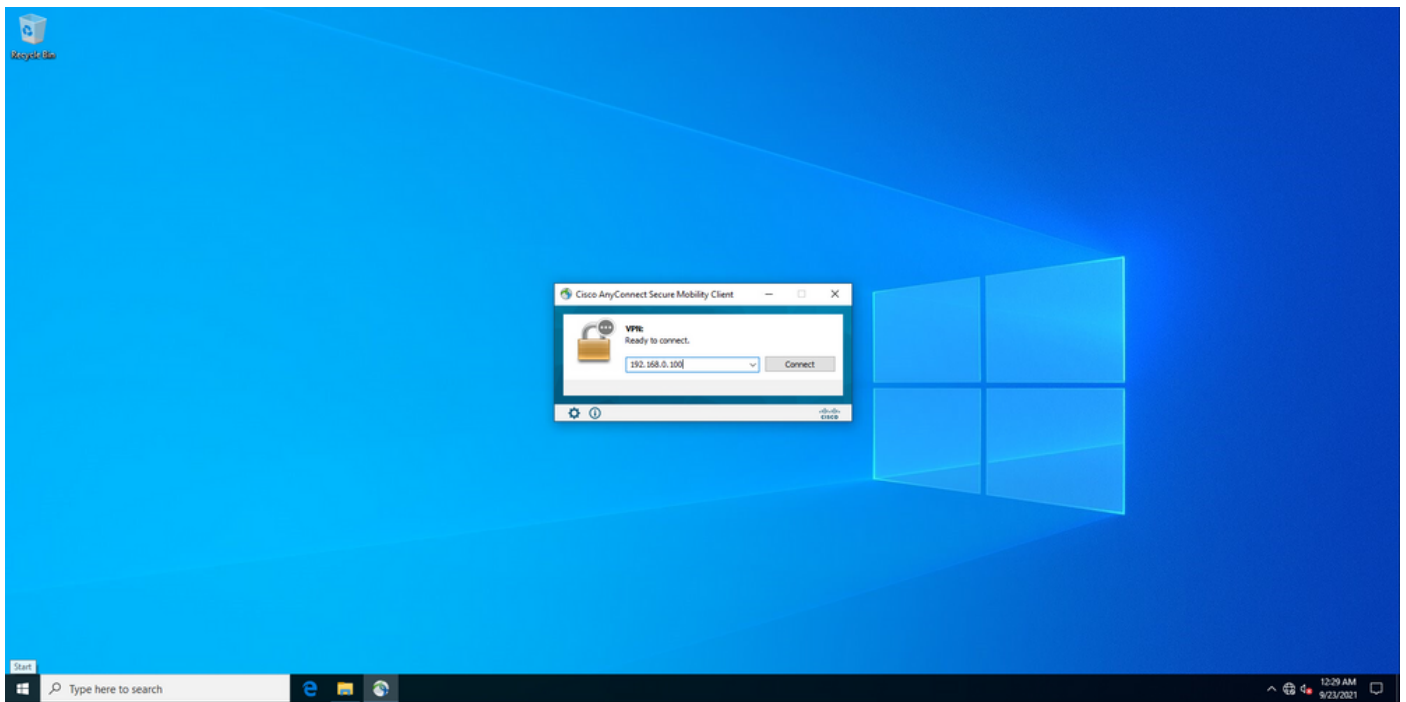


“授权”(Authorization)规则现在已全部设置。Click **Save**.

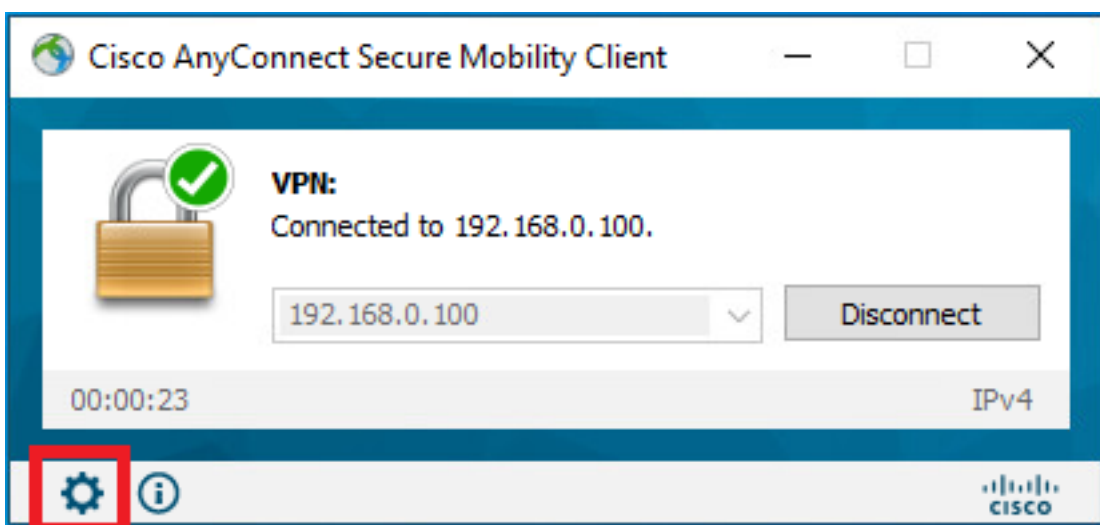


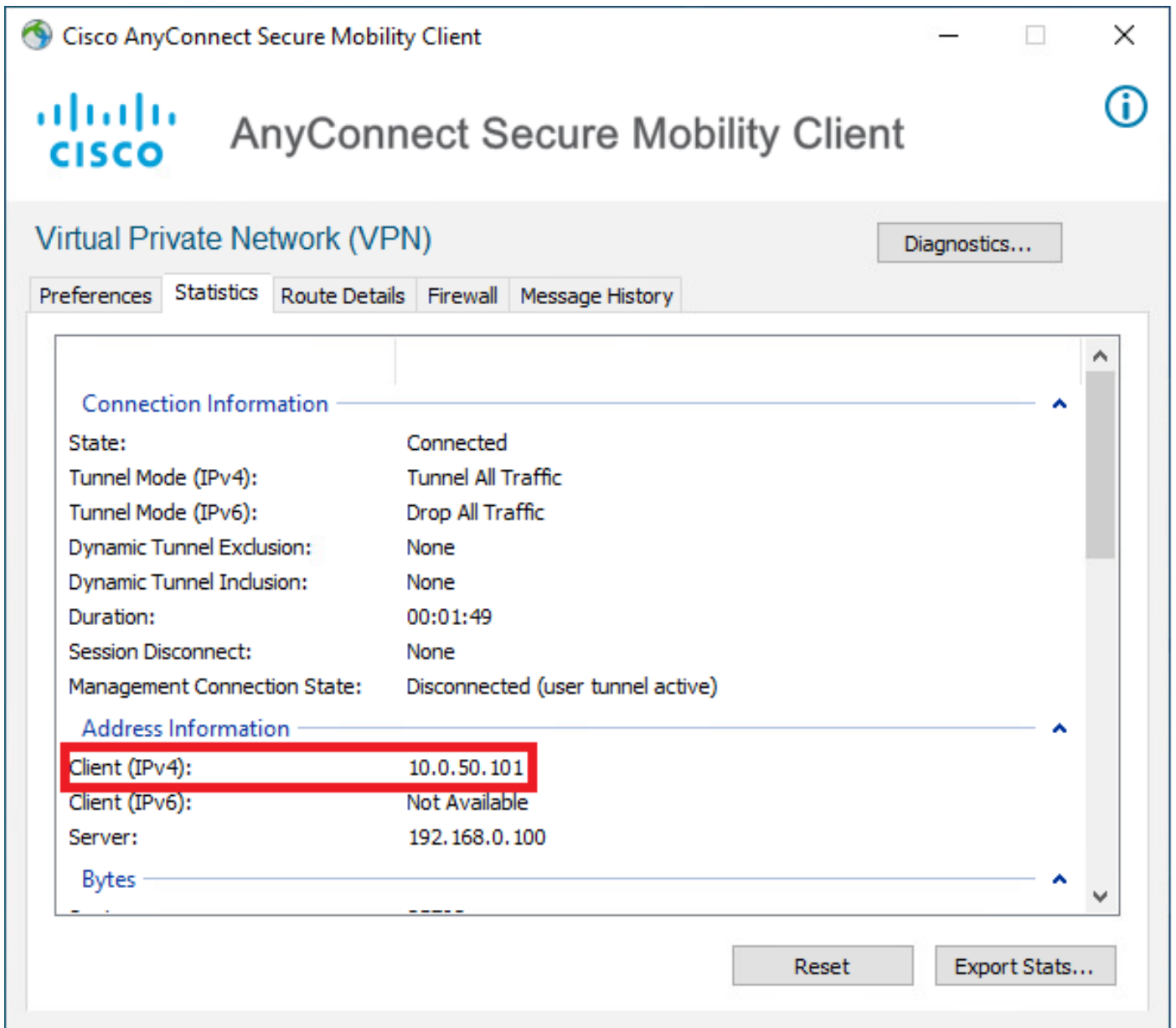
## 验证

步骤1.导航至安装Cisco AnyConnect安全移动客户端的客户端计算机。连接到FTD头端（此处使用Windows计算机）并输入user1凭据。



单击齿轮图标（左下角）并导航至**统计**选项卡。在**地址信息**部分确认分配的IP地址确实是在此用户的ISE授权策略上配置的IP地址。





FTD上的debug radius all命令输出显示：

```
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日志显示 :**

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
```

ISE上的RADIUS实时日志显示：



Identity Services Engine

### Overview

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

### Steps

```

11001 Returned RADIUS AccessRequest
11017 RADIUS created a new session
15049 Evaluating Policy Group
15058 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15046 Queried PIP - Normalised Radius Radius/TokenType (4 times)
22072 Selected identity source sequence - All_User_IDStores
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-6753440f850c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPPOX-Client-Type	2
Acx-SessionID	driverap-ISE-2-71417494978-23
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_Ad_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLS-Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	LocationAll Locations
Device Type	Device TypeAll Device Types

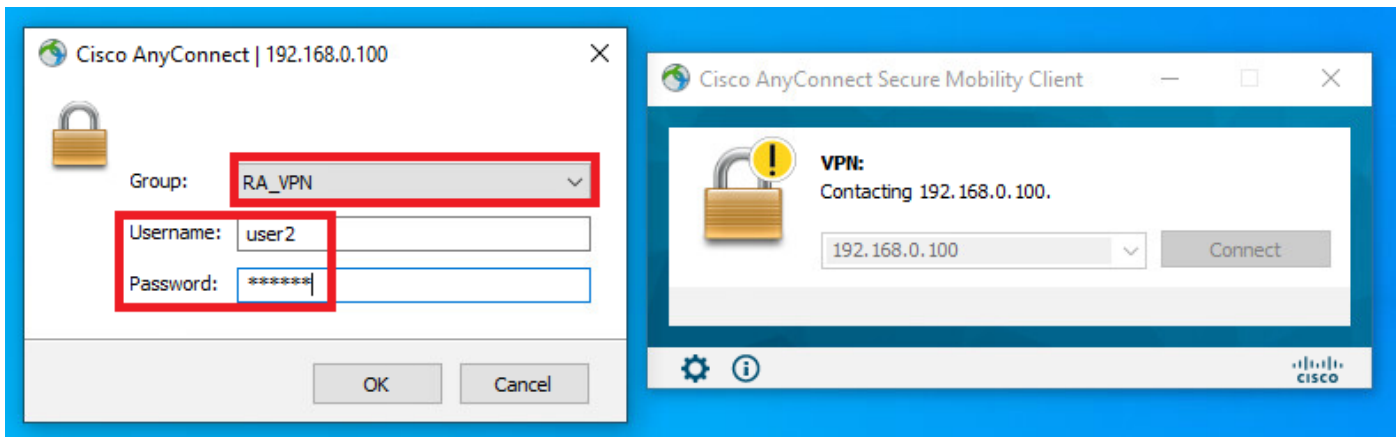
IPSEC	IPSECOnly IPSEC Device#0
EnabledFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM SessionID	d8a800540000d00014bc1d0
Called-Station-ID	192.168.0.100
CiscoAVPair	mdu-dmdevice-platform=win, mdu-dmdevice-manid=00:00:56:96:45:0f, mdu-dmdevice-platform-version=10.0.13352, mdu-dmdevice-publicmanid=00:00:56:96:45:0f, mdu-dmdevice-agent=AnyConnect Windows 4 10.02086, mdu-dmdevice-type=VMware, Inc VMware Virtual Platform, mdu-dmdevice-uid=glbactm158f88e30cf629f2c0e2431409f4bAAGAE20583, mdu-dmdevice-uid=3C38427071F90782F810F124621184A08596C717E370386CC030F945C8880344, audit-session-id=d8a800540000d00014bc1d0, ip-source-ip=192.168.0.101, oca-push=true

### Result

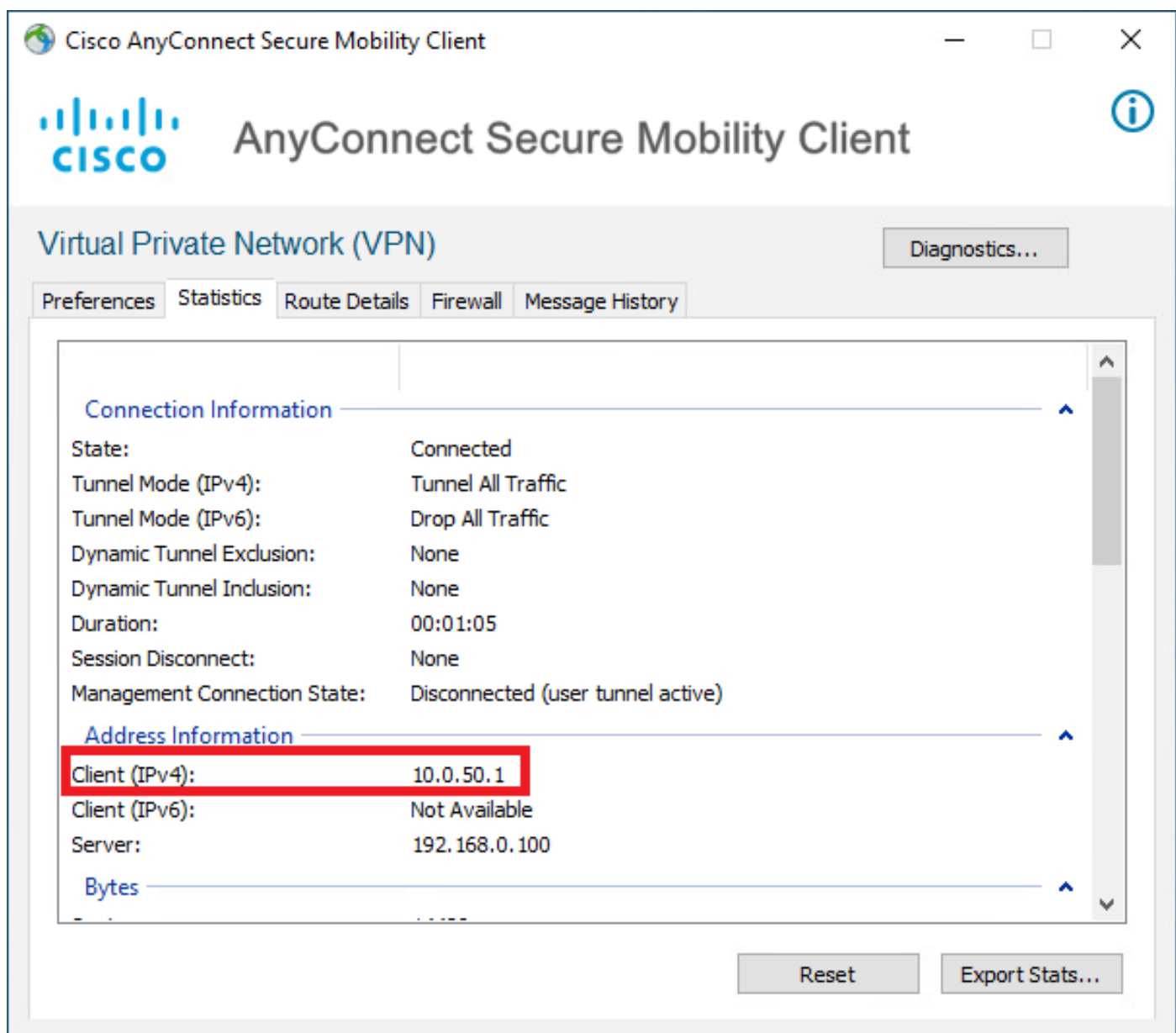
Framed-IP-Address	10.0.0.101
Class	CACS-d8a800540000d00014bc1d0 driverap-ISE-2-71417494978-23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

步骤2. 连接到FTD头端 ( 此处使用Windows计算机 ) 并输入用户2凭据。



地址信息部分显示，分配的IP地址确实是通过FMC配置的IPv4本地池中的第一个可用IP地址。



FTD上的debug radius all命令输出显示：

```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)
```

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

RADIUS packet decode (authentication request)
```

### **RADIUS packet decode (response)**

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

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

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

**FTD日志显示：**

<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上的RADIUS实时日志显示：

Identity Services Engine

### Overview

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

### Authentication Details

Source Timestamp	2021-09-23 00:00:06:488
Received Timestamp	2021-09-23 00:00:06:488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	00:50:56:96:45:6F:0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	cb800040000d00014bc0b7
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	DRIVERAP_FT0_7-0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

### Steps

- 11001 Received RADIUS AccessRequest
- 11017 RADIUS created a new session
- 15043 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15045 Queried PIP - Normalised Radius RadiusForType (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
- 15030 Evaluating Authorization Policy
- 24209 Looking up Endpoint in Internal Endpoints IDStore - user2
- 24211 Found Endpoint in Internal Endpoints IDStore
- 15048 Queried PIP - Radius User Name
- 15048 Queried PIP - Radius NAS-Port Type
- 15048 Queried PIP - EndPoints LogicalProfile
- 15048 Queried PIP - Network Access AuthenticationStatus
- 15010 Selected Authorization Profile - PermitAccess
- 22081 Max sessions policy passed
- 22083 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

Identity Services Engine

NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	202 milliseconds

### Other Attributes

ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53243
Tunnel Client Endpoint	{tag=0} 192.168.0.101
CVPR3000ASAPRFX-Tunnel-Group-Name	RA_VPN
OriginalUsername	user2
NetworkDeviceProfileId	b0009005-3150-4210-a80a-675345b050c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPRFX-Client-Type	2
AccSessionID	driverap-ISE-2-71417494978-24
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_join_Points
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
ISEPolicySetName	Default
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	LocationAll Locations
Device Type	Device TypeAll Device Types

IPSEC	IPSECOnly IPSEC Device#No
Name	Endpoint Identity Groups Profiled Workstation
EnableFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPM Session ID	cb800040000d00014bc0b7
Called Station ID	192.168.0.100
CiscoAvPair	mdm-dm-device-platform=ms-00-50-56-96-45-6f-0; mdm-dm-device-platform=espip10.0.18362; mdm-dm-device-publicmap=00-50-56-96-45-6f-0; mdm-dm-device-user-agent=anyConnect; Windows 4.10; 02088; mdm-dm-device-type=VMware, Inc. VMware Virtual Platform; mdm-dm-device-uid=global+19f88e3d0f52f3f2c0e2431459f48aa2ae2c0b3; mdm-dm-device-uid=3c38427071f80782f816f124621184406596c717e370388cc030f94402885244; audit-session-ip=cb800040000d00014bc0b7; ip-source-ip=192.168.0.101; os=pubintv4

### Result

Class	CACS-cb800040000d00014bc0b7-driverap-ISE-2-71417494978-24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

**注意：**您必须在FTD IP本地池和ISE授权策略上使用不同的IP地址范围来分配IP地址，以避免AnyConnect 客户端之间出现重复的IP地址冲突。在此配置示例中，FTD配置了IPv4本地池，该池从10.0.50.1到10.0.50.100,ISE服务器分配了静态IP地址10.0.50.101。

## 故障排除

本节提供可用于排除配置故障的信息。

在FTD上：

- **debug radius all**

在ISE上：

- **RADIUS实时日志**