

# 通過RADIUS授權為AnyConnect使用者配置靜態IP地址分配

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[通過FMC使用AAA/RADIUS身份驗證配置遠端訪問VPN](#)

[在ISE上配置授權策略 \( RADIUS伺服器 \)](#)

[驗證](#)

[疑難排解](#)

## 簡介

本文說明如何使用身分識別服務引擎(ISE)伺服器設定RADIUS授權，以便其透過RADIUS屬性8 Framed-IP-Address將同一IP位址轉送到特定Cisco AnyConnect安全行動化使用者端的Firepower威脅防禦(FTD)。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- FTD
- Firepower Management Center (FMC)
- ISE
- Cisco AnyConnect Security Mobility Solution — 遠端存取
- RADIUS通訊協定

### 採用元件

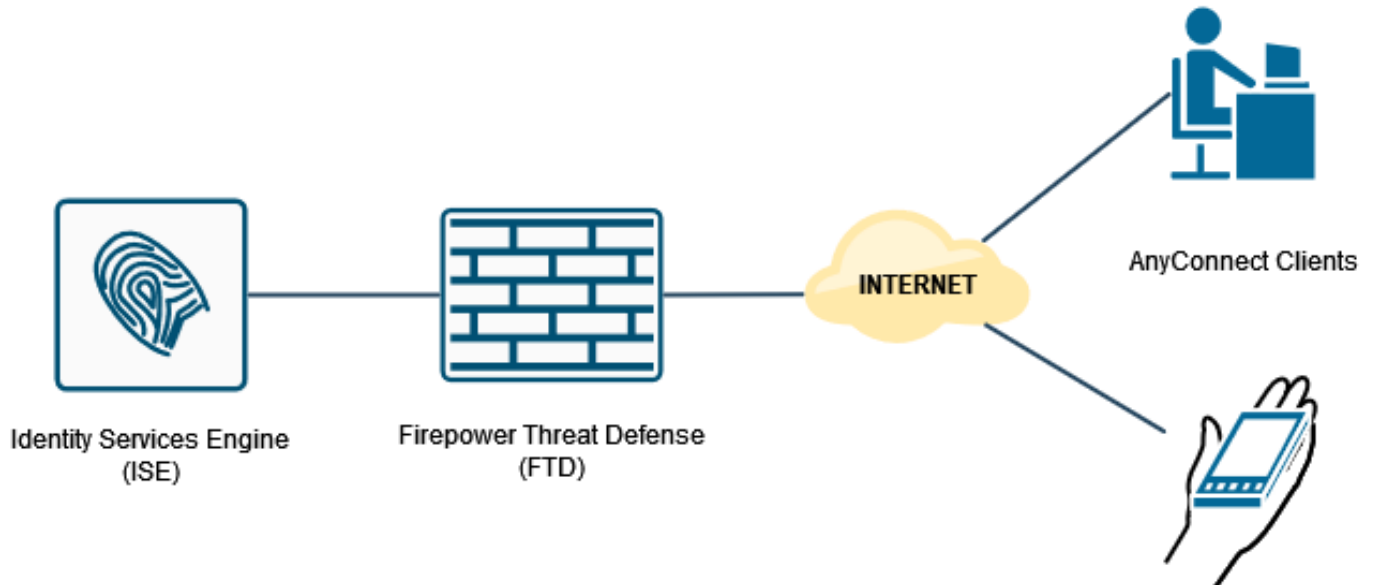
本檔案中的資訊是根據以下軟體版本：

- FMCv - 7.0.0 ( 內部版本94 )
- FTDv - 7.0.0 ( 內部版本94 )
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086
- Windows 10 Pro

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

### 網路圖表



### 通過FMC使用AAA/RADIUS身份驗證配置遠端訪問VPN

如需逐步程式，請參閱本檔案及以下影片：

- [FTD上的AnyConnect遠端存取VPN組態](#)
- [FMC管理的FTD的初始AnyConnect配置](#)

FTD CLI上的遠端存取VPN組態為：

```
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
```

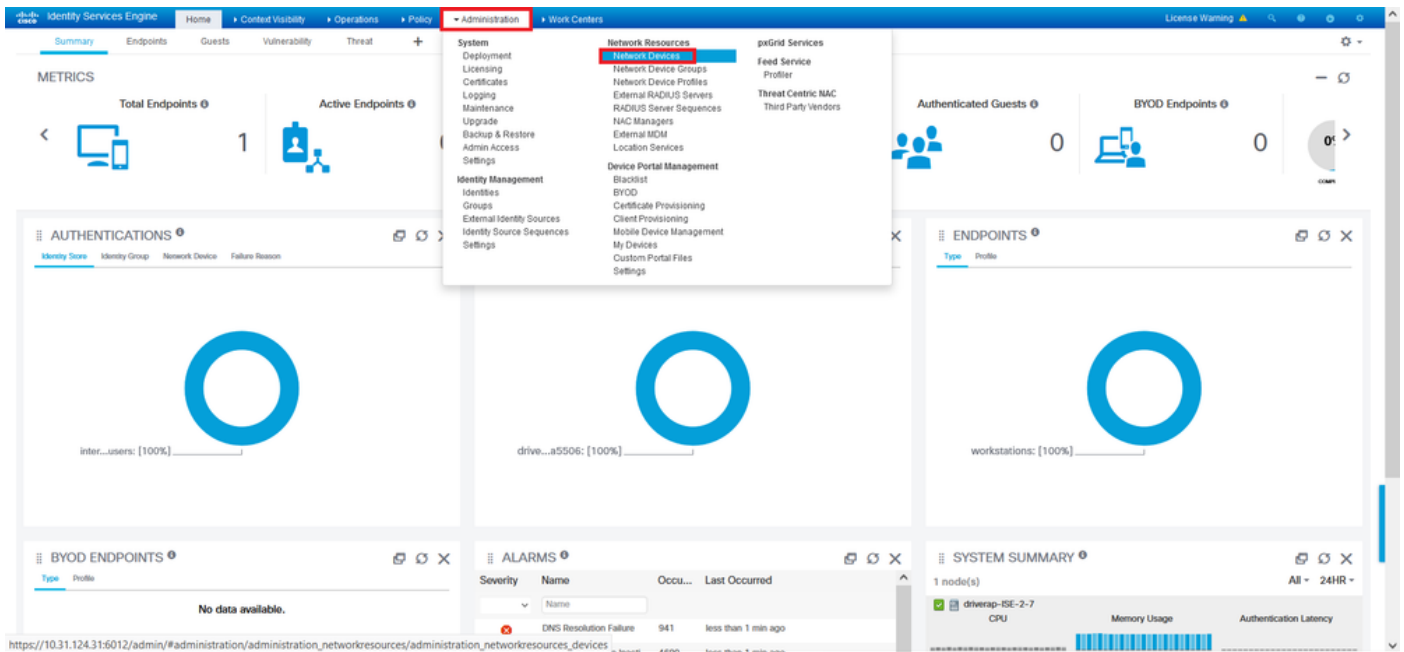
```
webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list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

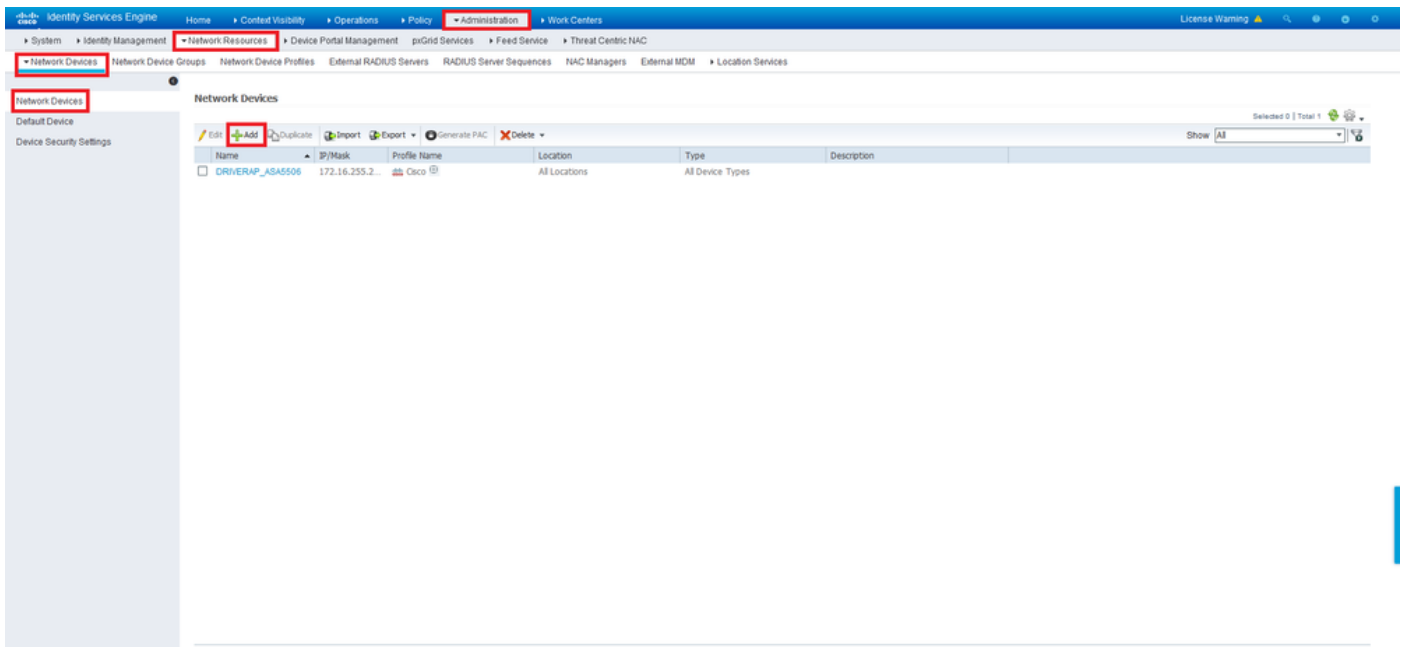
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

## 在ISE上配置授權策略 ( RADIUS伺服器 )

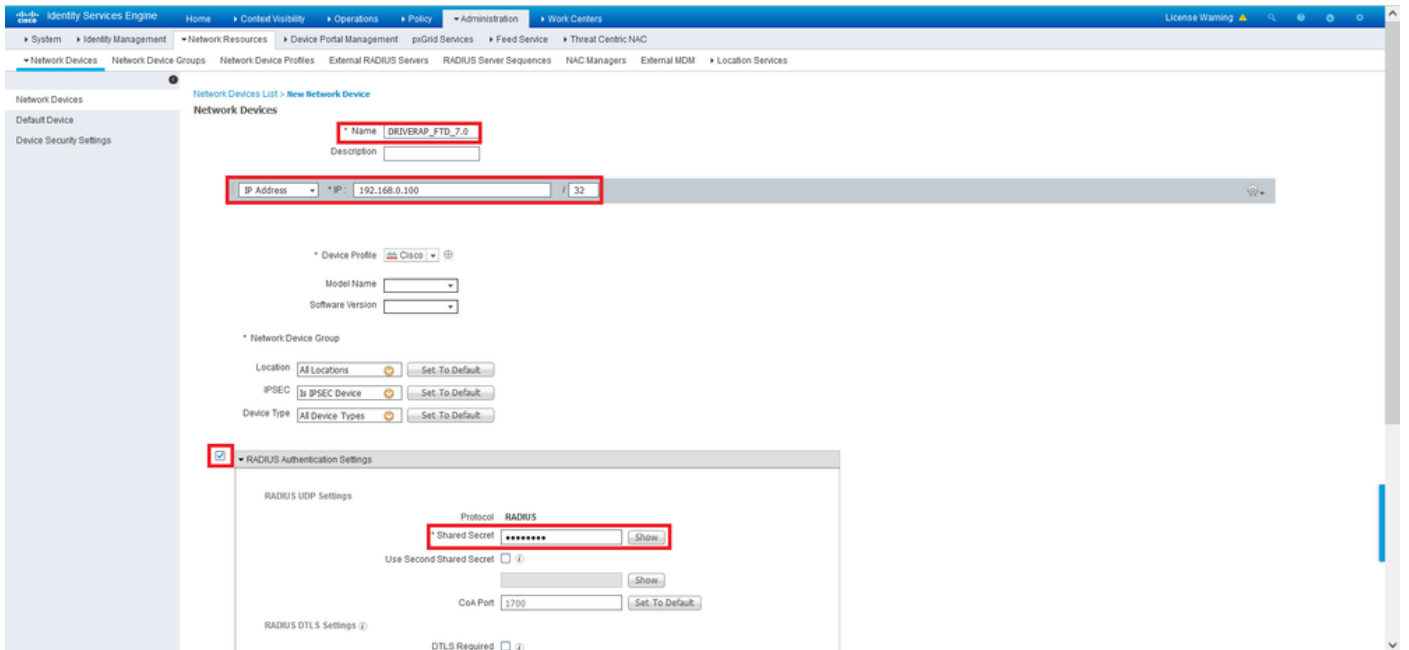
步驟1.登入到ISE伺服器並導航到**管理>網路資源>網路裝置**。



步驟2. 在「網路裝置」區段中，按一下Add，以便ISE可以處理來自FTD的RADIUS存取要求。

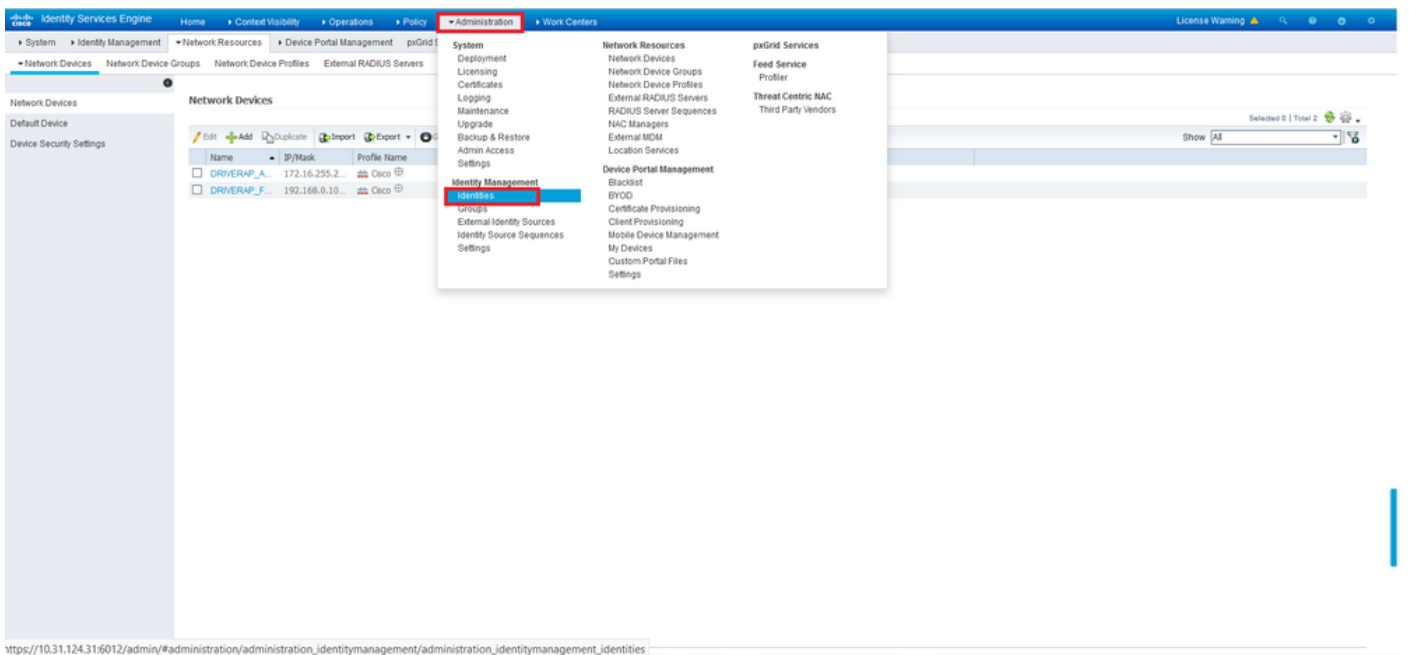


輸入網路裝置名稱和IP地址欄位，然後選中RADIUS身份驗證設定框。Shared Secret的值必須與建立FMC上的RADIUS伺服器對象時使用的值相同。

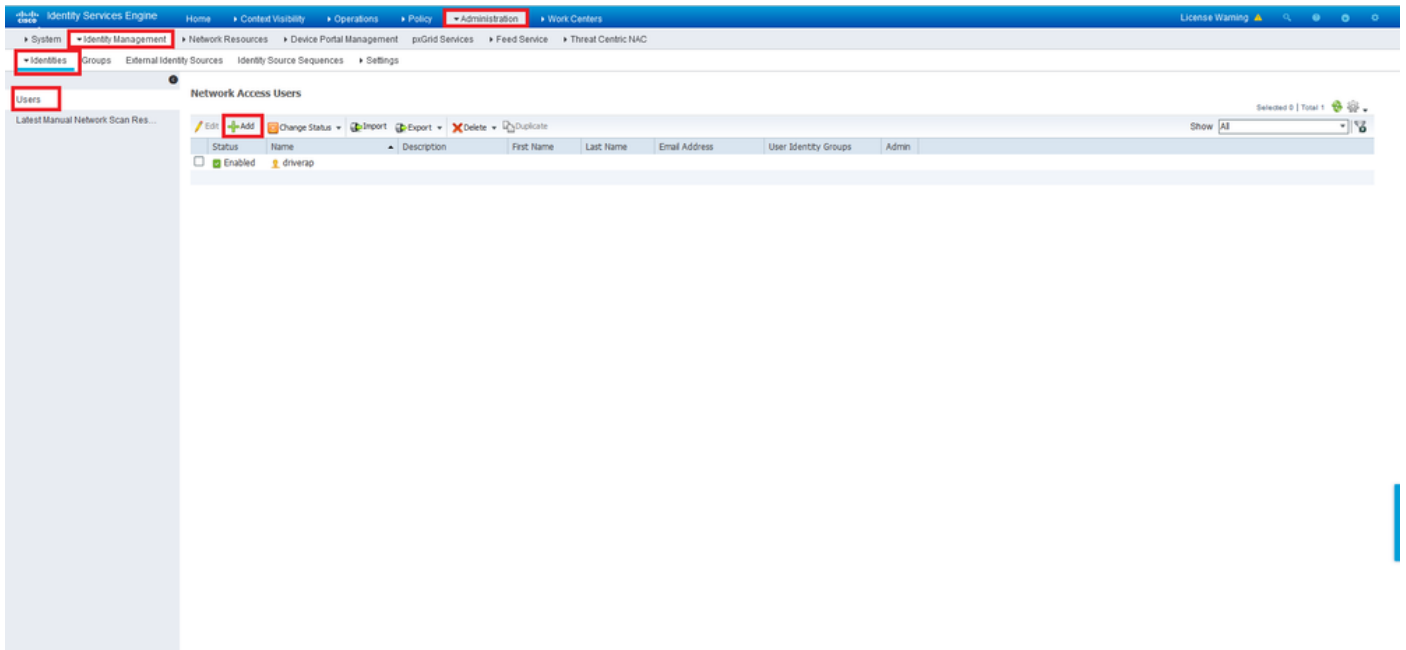


使用此頁面結尾的按鈕儲存。

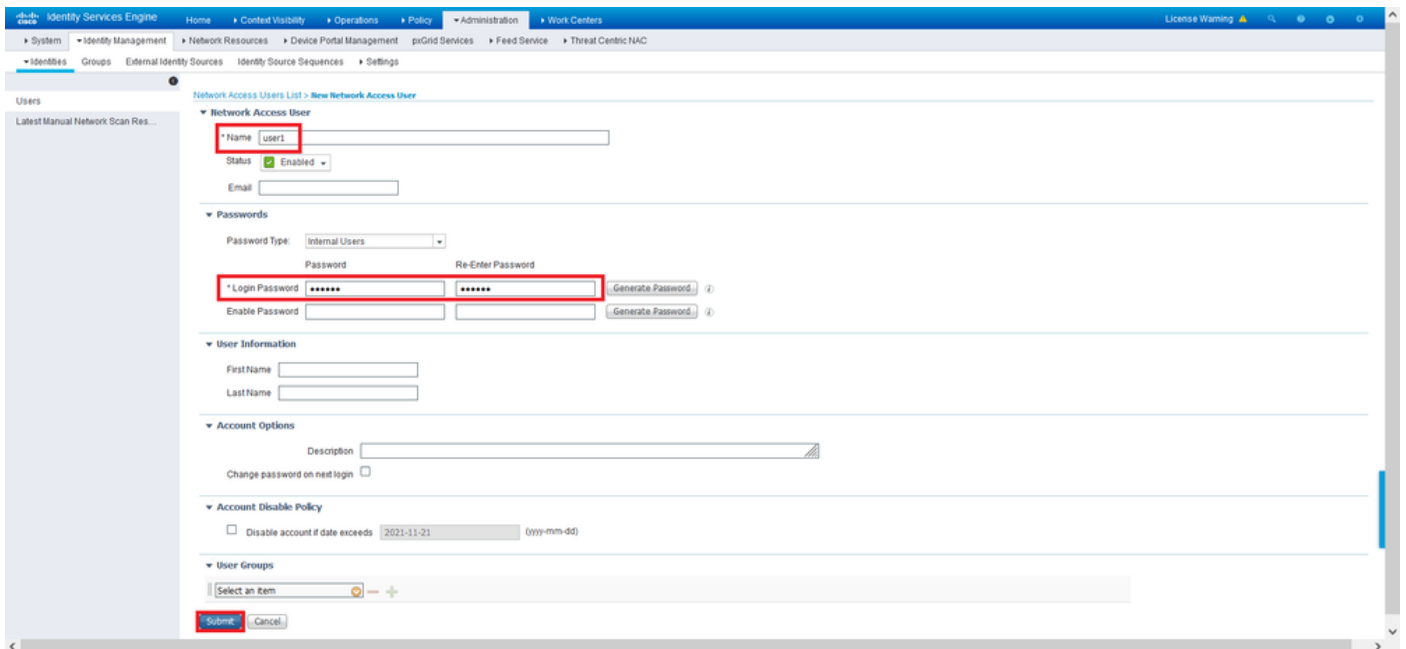
步驟3. 導航到管理>身份管理>身份。



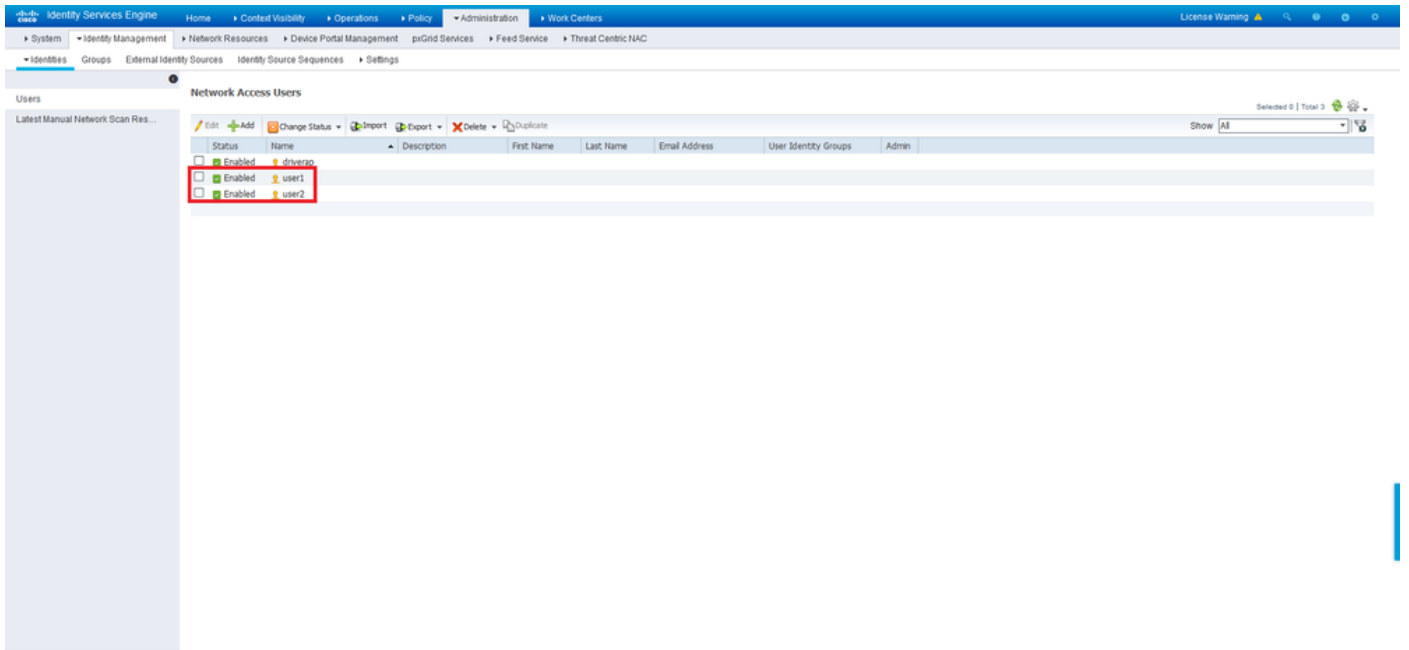
步驟4. 在Network Access Users部分，按一下Add以便在ISE的本地資料庫中建立user1。



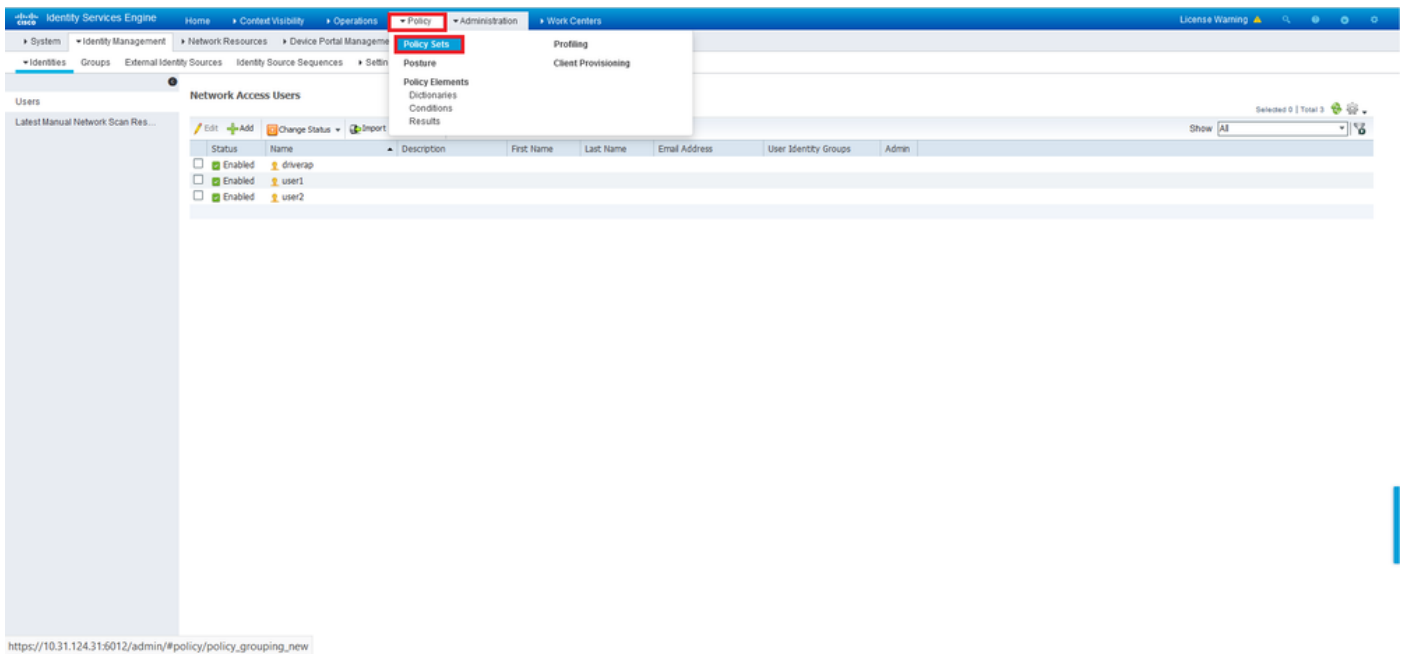
在Name和Login Password欄位中輸入使用者名稱和密碼，然後按一下Submit。



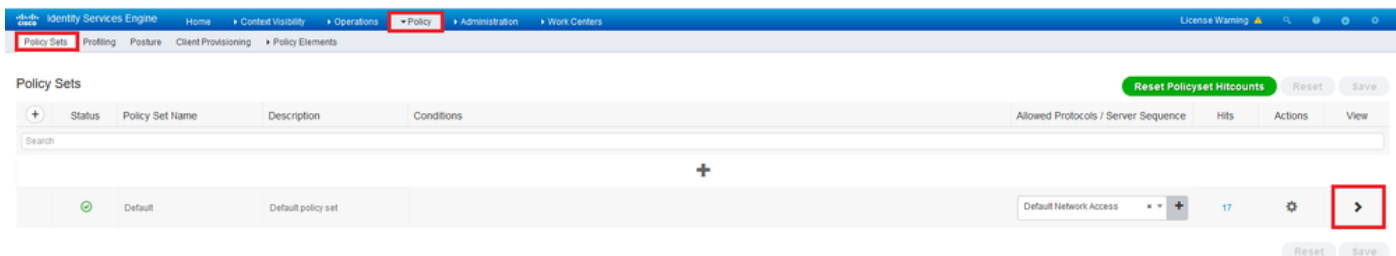
步驟5.重複上述步驟以建立user2。



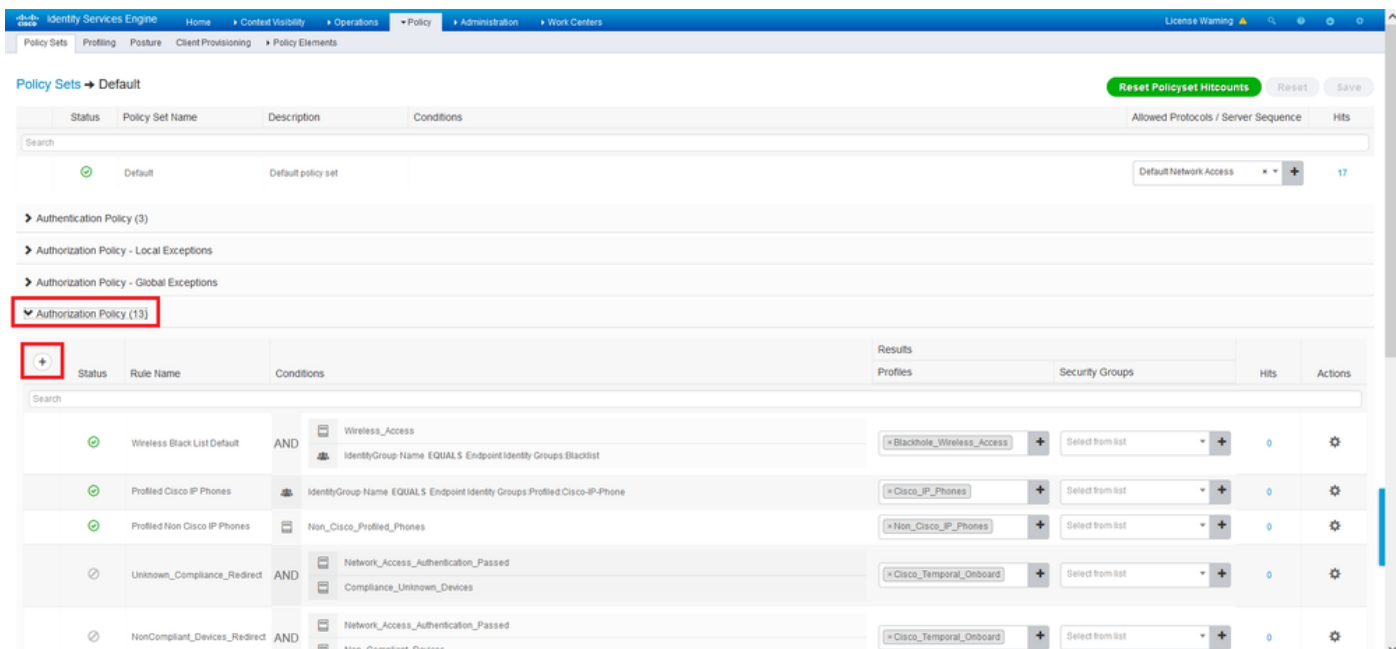
步驟6.導覽至Policy > Policy Sets。



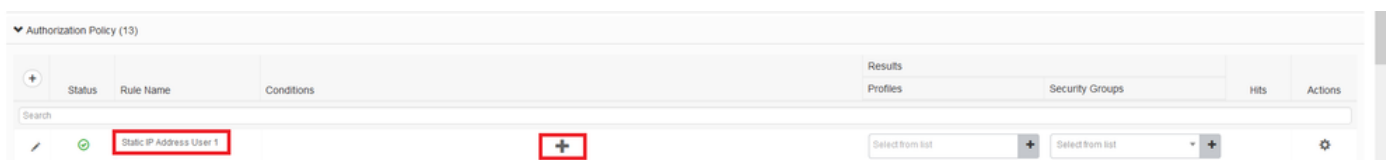
步驟7.按一下屏幕右側的箭頭>。



步驟8. 按一下 **Authorization Policy** 旁邊的箭頭> 將其展開。現在，按一下 + 符號以新增新規則。



為規則提供名稱，並在條件列下選擇 + 符號。



在「屬性編輯器」(Attribute Editor) 文本框中按一下，然後按一下「主題」(Subject) 圖示。向下滾動，直到找到 **RADIUS User-Name** 屬性並選擇它。



Conditions Studio

Library

Search by Name

Editor

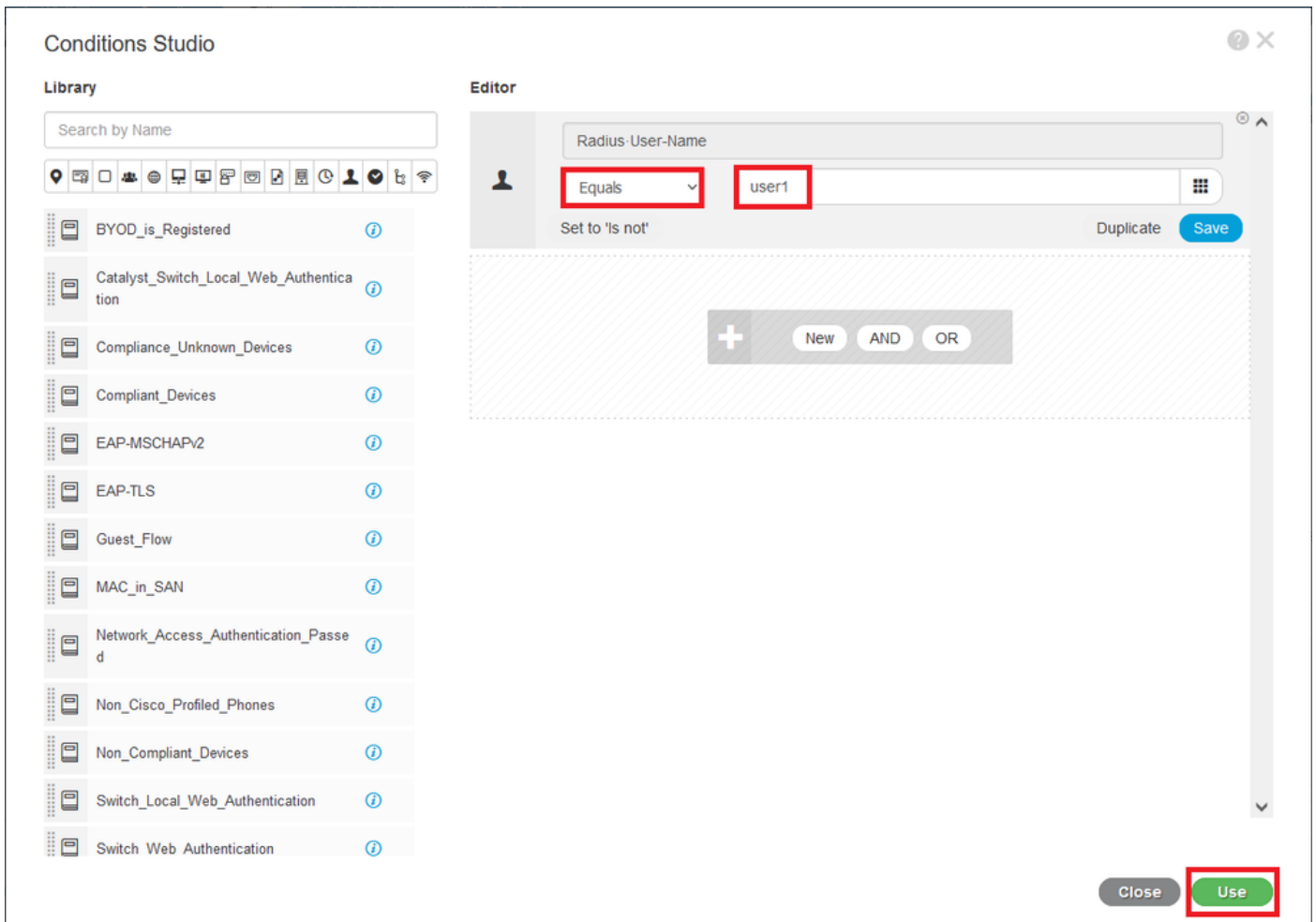
Click to add an attribute

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>

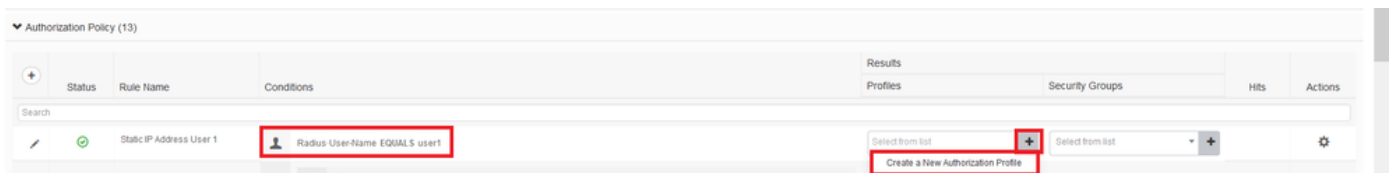
Close Use

保留Equals作為運算子，並在其旁邊的文本框中輸入user1。按一下「Use」以儲存屬性。

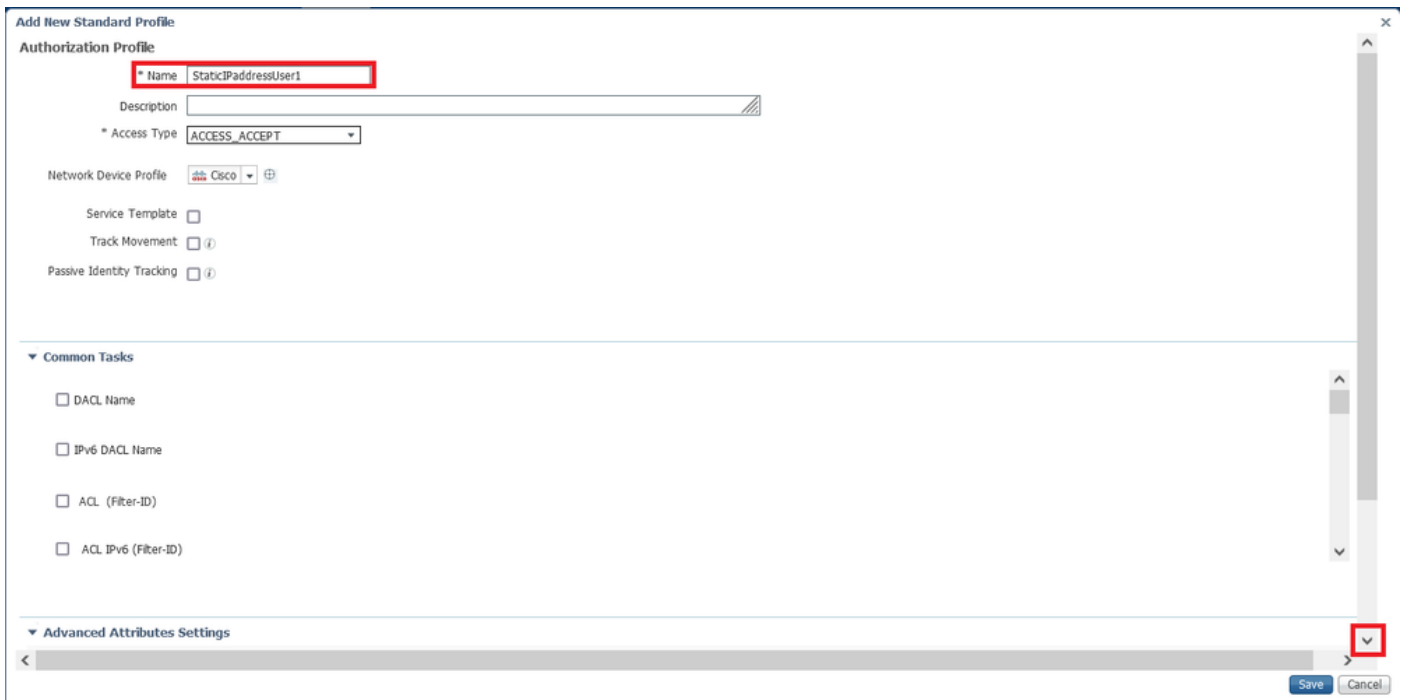


現在已設定此規則的條件。

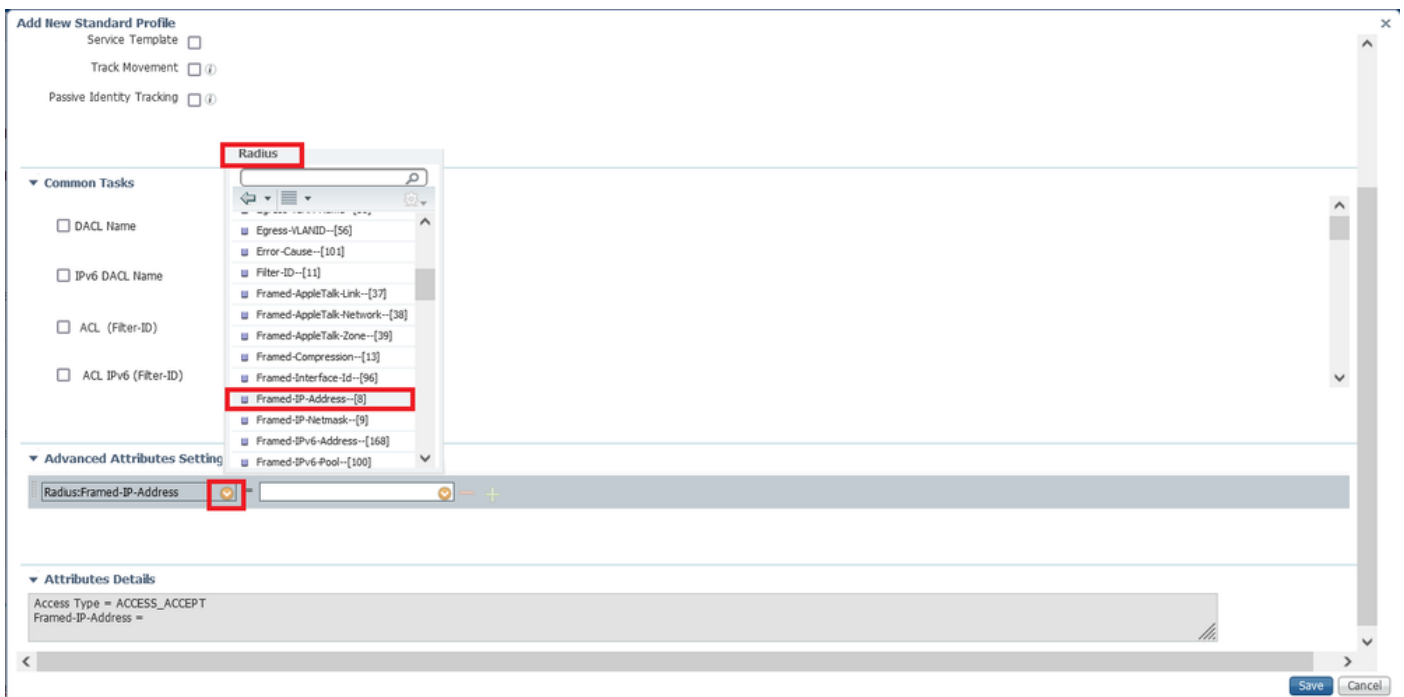
步驟9.在Results/Profiles列中，按一下+號並選擇Create a New Authorization Profile。



為其指定名稱，並保留ACCESS\_ACCEPT作為存取型別。向下滾動至高級屬性設定部分。



按一下橙色箭頭並選擇Radius > Framed-IP-Address - [8]。



鍵入要始終為此使用者靜態分配的IP地址，然後按一下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

步驟10.現在，選擇新建立的授權配置檔案。

**Authorization Policy (13)**

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✓	Static IP Address User 1	Radius-User-Name EQUALS user1	Select from list	Static_IP_address	Select from list	0	⚙️
✓	Wireless Black List Default	AND Wireless_Access IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	DenyAccess	Select from list	Select from list	0	⚙️
✓	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled-Cisco-IP-Phone	NSP_Onboard	Select from list	Select from list	0	⚙️
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	StaticIPaddressUser1	Select from list	Select from list	0	⚙️

現在已設定授權規則。按一下「**Save**」。

**Policy Sets → Default**

Reset Policyset Hitcounts Reset **Save**

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

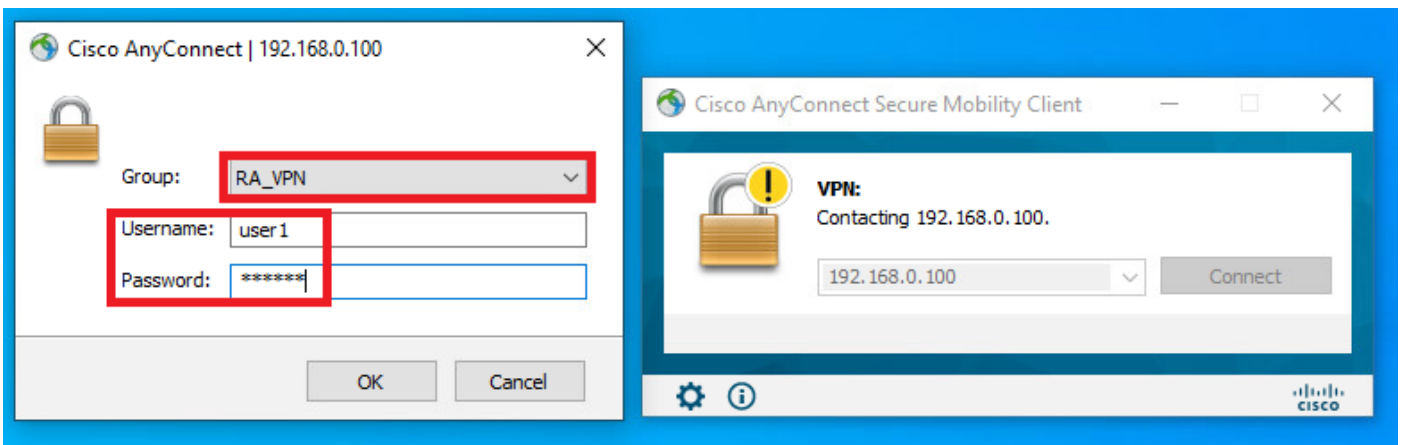
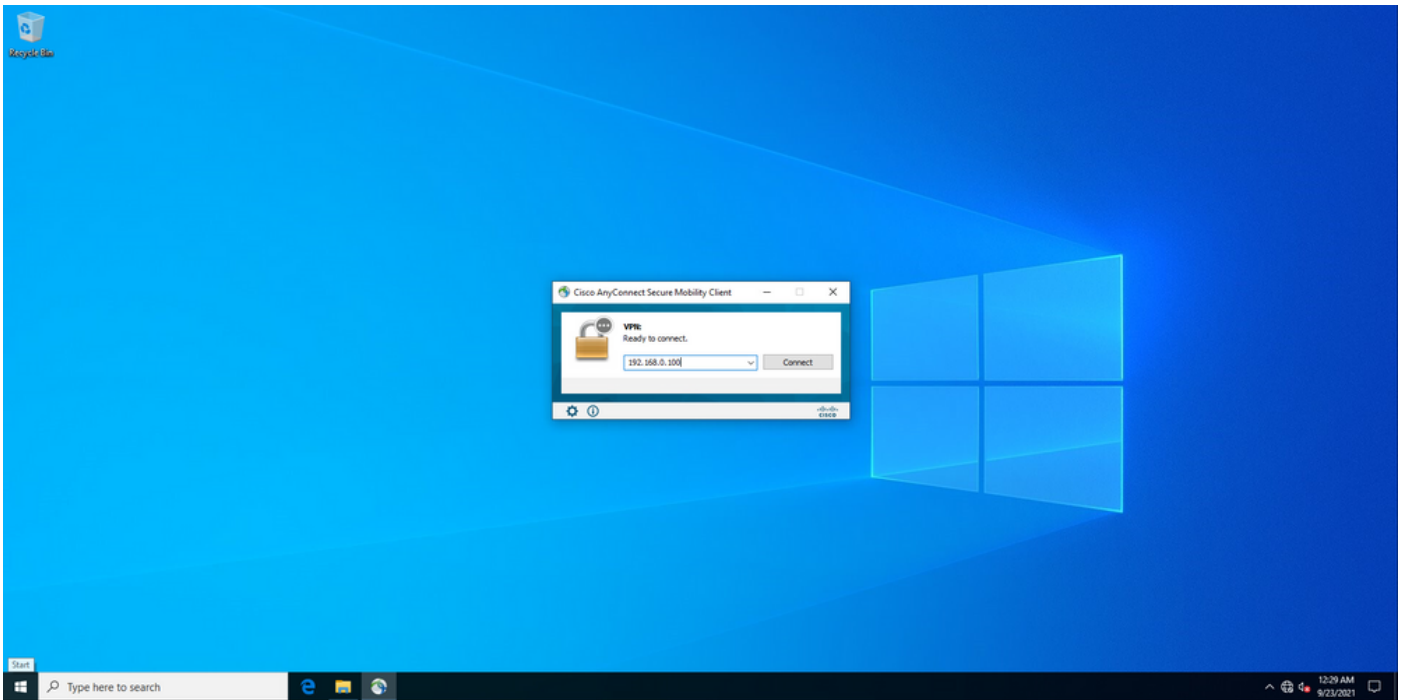
---

**Authorization Policy (13)**

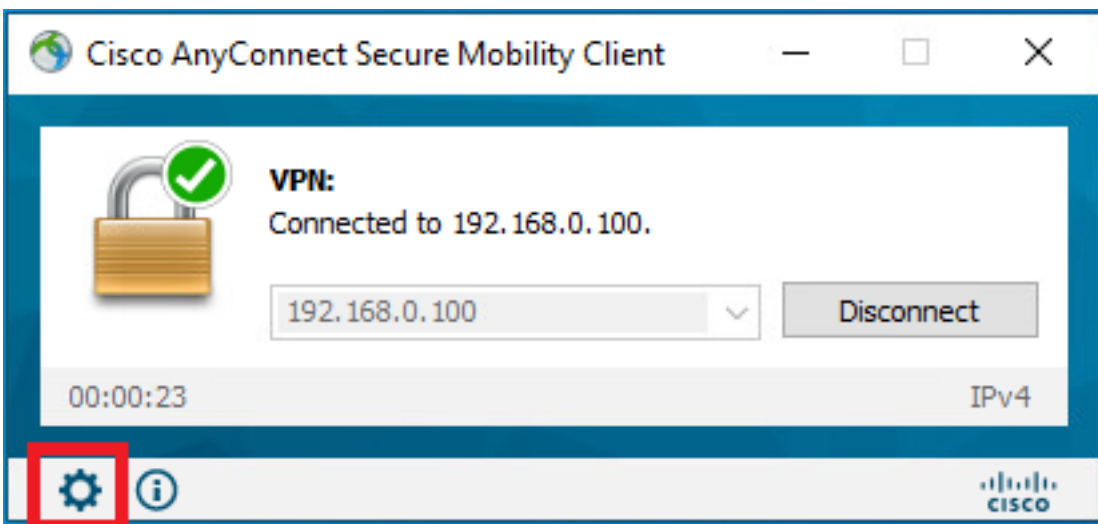
Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✓	Static IP Address User 1	Radius-User-Name EQUALS user1	StaticIPaddressUser1	Static_IP_address	Select from list	0	⚙️

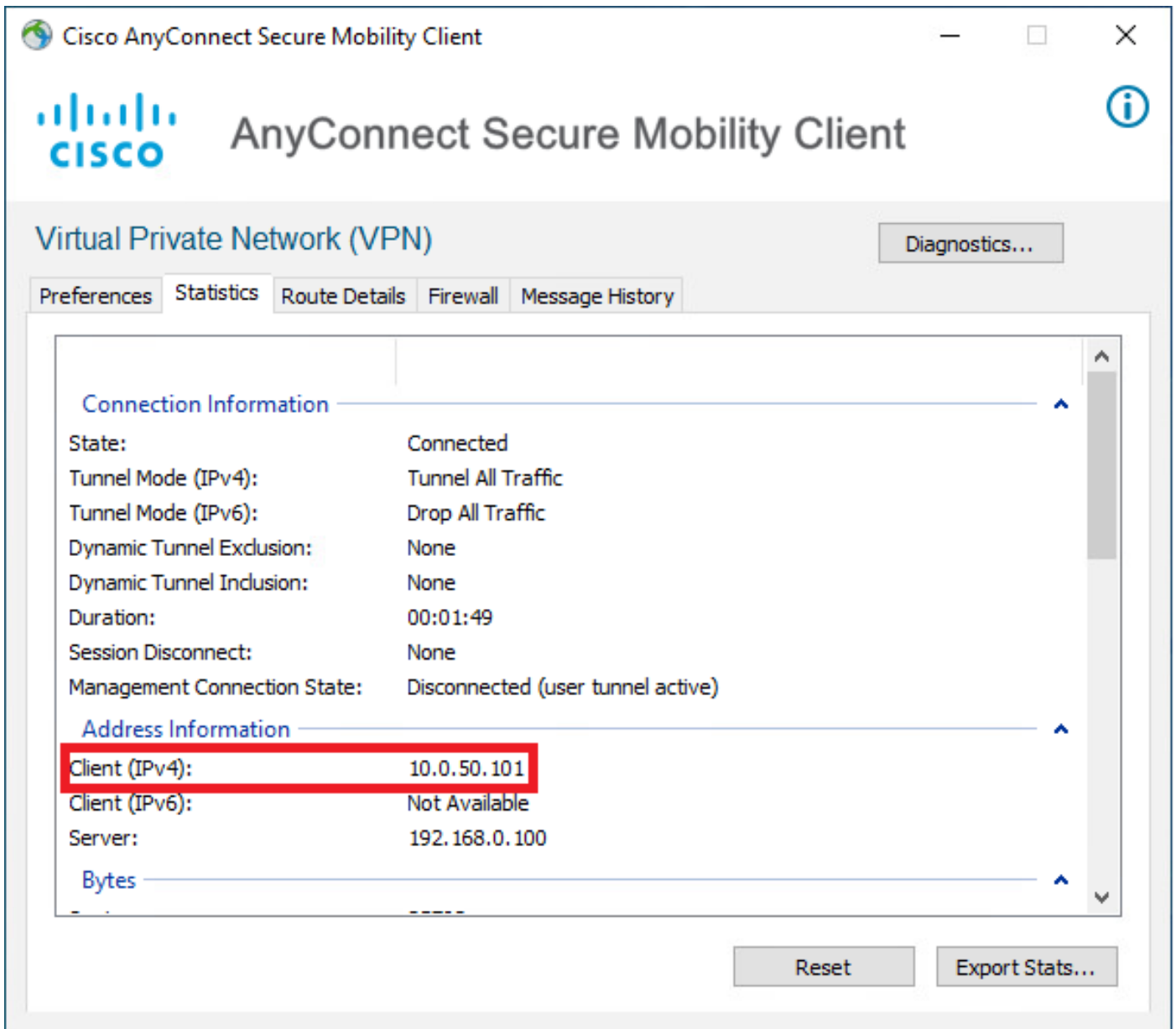
## 驗證

步驟1.導航到安裝了Cisco AnyConnect Security Mobility客戶端的客戶端電腦。連線到FTD頭端（此處使用Windows機器），並輸入user1憑證。



按一下齒輪圖示（左下角）並導航到**Statistics**頁籤。在**Address Information**部分中確認分配的IP地址確實是為該使用者在ISE授權策略中配置的地址。





FTD上的debug radius all命令輸出顯示：

```
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 記錄顯示 :**

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 Live日誌顯示：



Identity Services Engine

### Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:00:56:45:0f: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	00:00:56:45:0f:0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	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
15040 Queried PIP - Normalised Radius Radius/lowType (4 times)
22072 Selected identity source sequence - All_User_IDStore
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
15030 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-2-71417494978/23
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_Ad_Join_Points
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
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

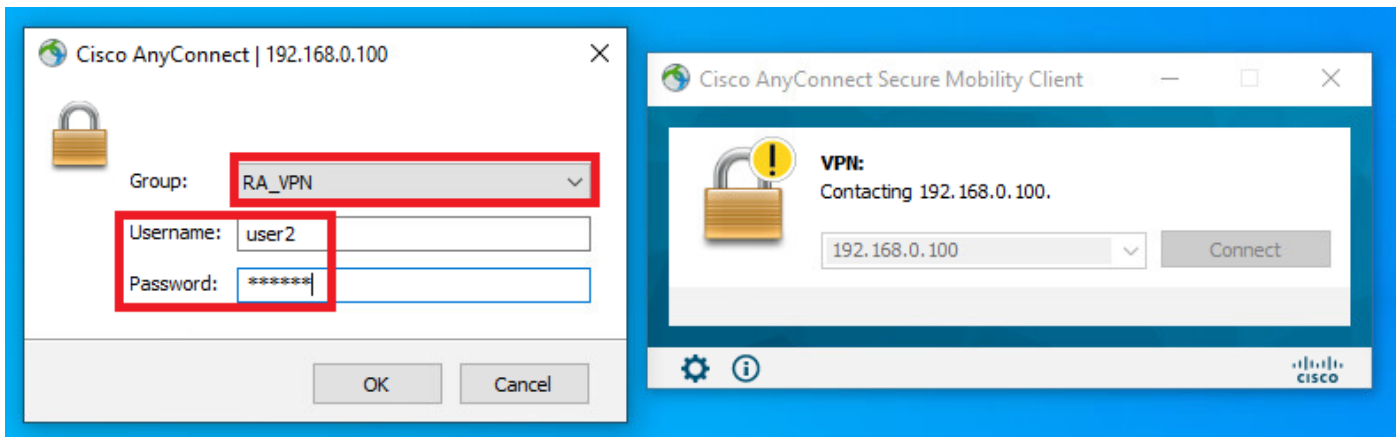
IPSEC	IPSECCalc IPSEC Device#0
EnabledFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM SessionID	d8a800540000d00014bc1d0
Called-Station-ID	192.168.0.100
CiscoAVPair	mdu-dmdevice-platform, mdu-dmdevice-man00:00:56:45:0f:01, mdu-dmdevice-platform-version=10.0.13352, mdu-dmdevice-publicman00:00:56:45:0f:01, mdu-dmdevice-agent=AnyConnect Windows 4 10.02086, mdu-dmdevice-type=VMware, Inc VMware Virtual Platform, mdu-dmdevice-uid, glbaem158788E0CF62F3F2CDE241409F4BA2AE2C583, mdu-dmdevice-uid=3C38427071F90782F810F124621184A08598C717E370388CC030F9443C880244, audit-session-id=d8a800540000d00014bc1d0, ip-source-ip=192.168.0.101, oca-push=true

### Result

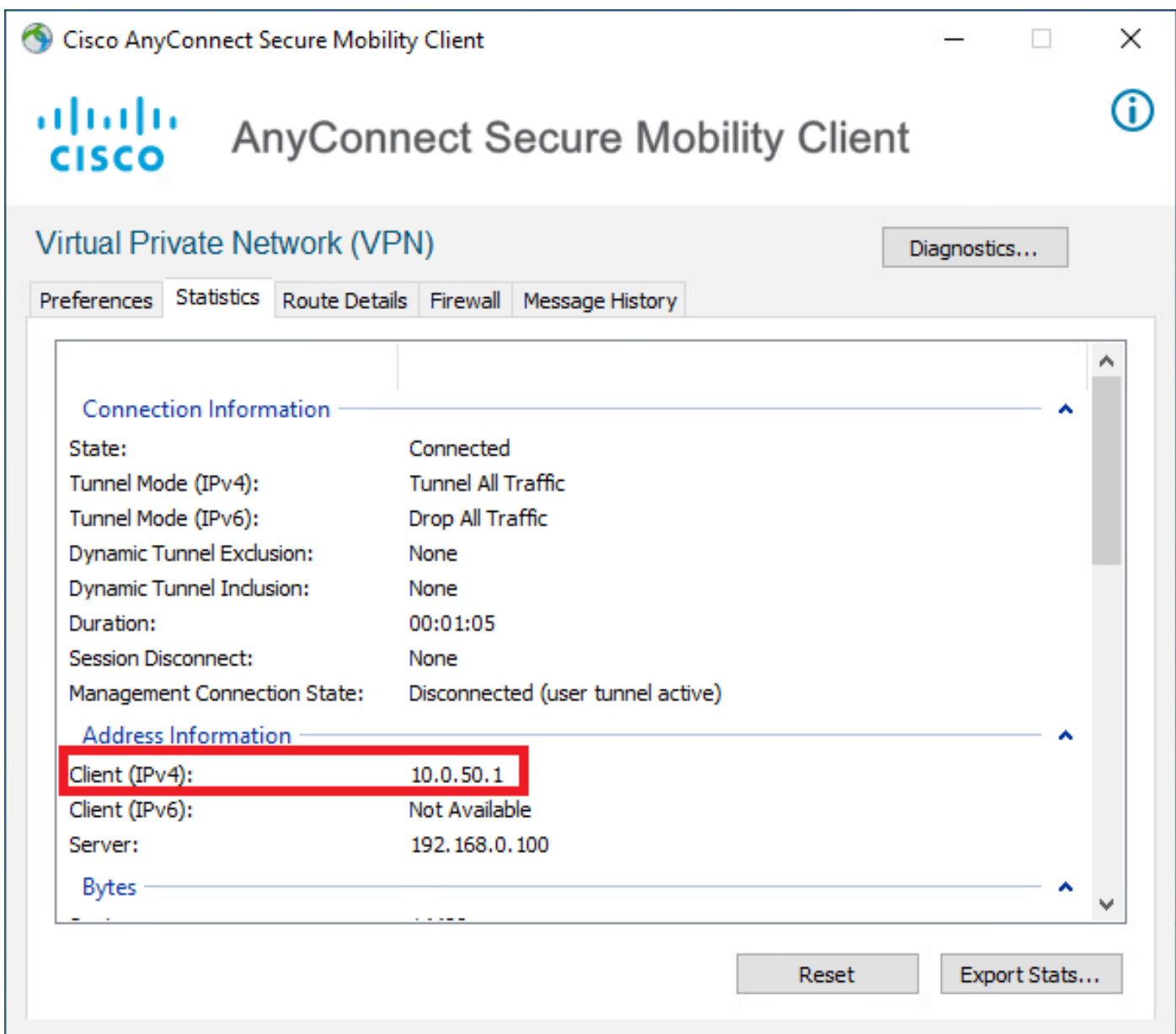
Framed IP Address	10.0.0.101
Class	CACS-d8a800540000d00014bc1d0 driverap-ISE-2-71417494978/23
cisco-av-pair	profile-name=Windows10-Workstation
License Types	Base license consumed

### Session Events

步驟2.連線到FTD頭端 ( 此處使用Windows電腦 ) 並輸入user2憑證。



Address Information部分顯示，分配的IP地址實際上是通過FMC配置的IPv4本地池中的第一個IP地址。



FTD上的debug radius all命令輸出顯示：

```
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 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 記錄顯示 :

<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: **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**

# ISE上的RADIUS Live日誌顯示：

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	da800540000d00014bc087
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
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15043 Queried PIP - Normalised Radius RadiusForType (4 times)
- 20272 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
- 22037 Authentication Passed
- 24714 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
- 15016 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
CVPR3000ASAPR7x-Tunnel-Group-Name	RA_VPN
OriginalUsername	user2
NetworkDeviceProfileId	b0099005-3150-4210-a80e-67534545f05c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPR7x-Client-Type	2
Acx SessionID	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

Identity Services Engine

IPSEC	IPSECv6v5 IPSEC Device#No
Name	Endpoint Identity Groups Profiled Workstation
EnabledFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPM SessionID	da800540000d00014bc087
Called Station ID	192.168.0.100
CiscoAVPair	mdm-dm-device-platform:mim-dm-device-macos-00-50-56-96-45-6f-0;mdm-dm-device-platform-reqtype:0,0,18362;mdm-dm-device-publicmap:00-50-56-96-45-6f;mdm-dm-device-appkey:Connect;Windows,4,10,22086;mdm-dm-device-type:VMware,Inc. VMware Virtual Platform;mdm-dm-device-uid:globa@158f88e00f52f3f2c0e243459f48aa2ae2c083;mdm-dm-device-uid-3c38427071f80782f816f124621184406596c717e370388cc030f94402885244;audit-session-0da800540000d00014bc087;ip-source-ip=192.168.0.101;os=publicv6

### Result

Class	CACS-da800540000d00014bc087-driverap-ISE-2-71417494978-24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

**附註：**您必須在FTD IP本地池和ISE授權策略上對IP地址分配使用不同的IP地址範圍，以避免您的AnyConnectClients之間的重複IP地址衝突。在此組態範例中，FTD設定為從10.0.50.1 到10.0.50.100的IPv4本機池，而ISE伺服器指派靜態IP位址10.0.50.101。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在FTD上：

- **debug radius all**

在ISE上：

- **RADIUS即時日誌**