Configurazione dell'assegnazione dell'indirizzo IP statico agli utenti AnyConnect tramite l'autorizzazione RADIUS

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione della VPN ad accesso remoto con autenticazione AAA/RADIUS tramite FMC](#)
[Configura criterio di autorizzazione su ISE (server RADIUS)](#)
[Verifica](#)
[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare l'autorizzazione RADIUS con un server Identity Services Engine (ISE) in modo che inoltri sempre lo stesso indirizzo IP a Firepower Threat Defense (FTD) per un utente Cisco AnyConnect Secure Mobility Client tramite l'indirizzo IP-Frame dell'attributo RADIUS 8.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

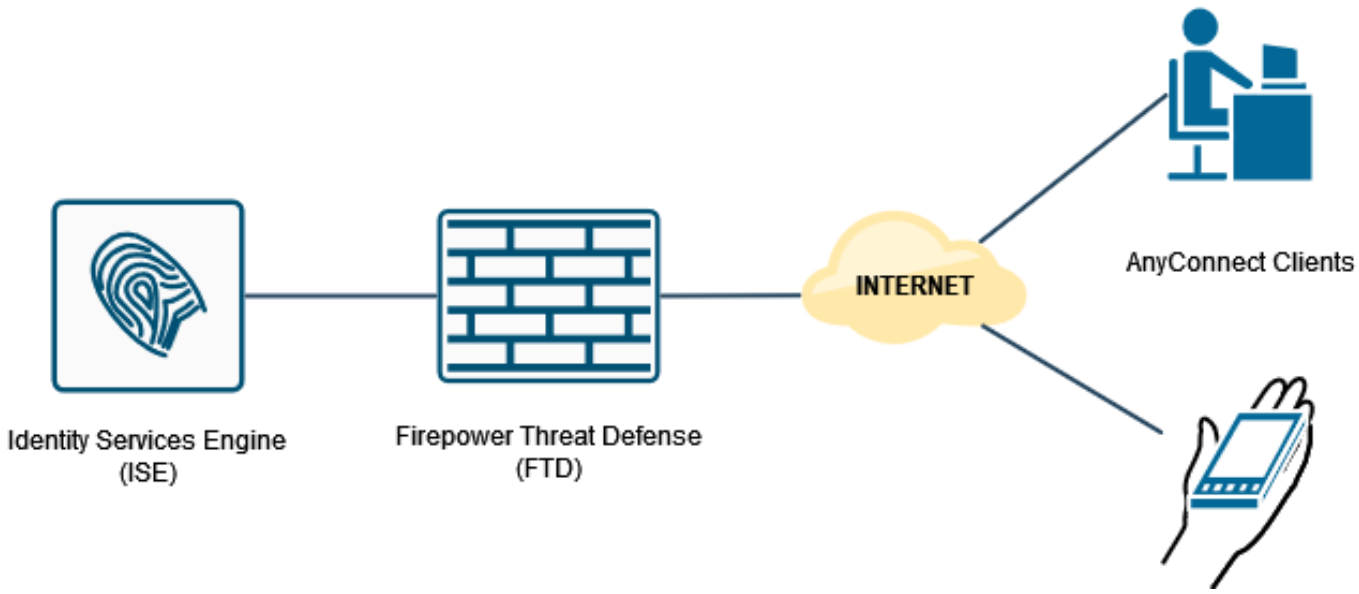
- FMCv - 7.0.0 (build 94)
- FTDv - 7.0.0 (Build 94)
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086

- Windows 10 Pro

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazione della VPN ad accesso remoto con autenticazione AAA/RADIUS tramite FMC

Per una procedura dettagliata, fare riferimento a questo documento e a questo video:

- Configurazione VPN ad accesso remoto AnyConnect su FTD
- Configurazione iniziale di AnyConnect per FTD gestito da FMC

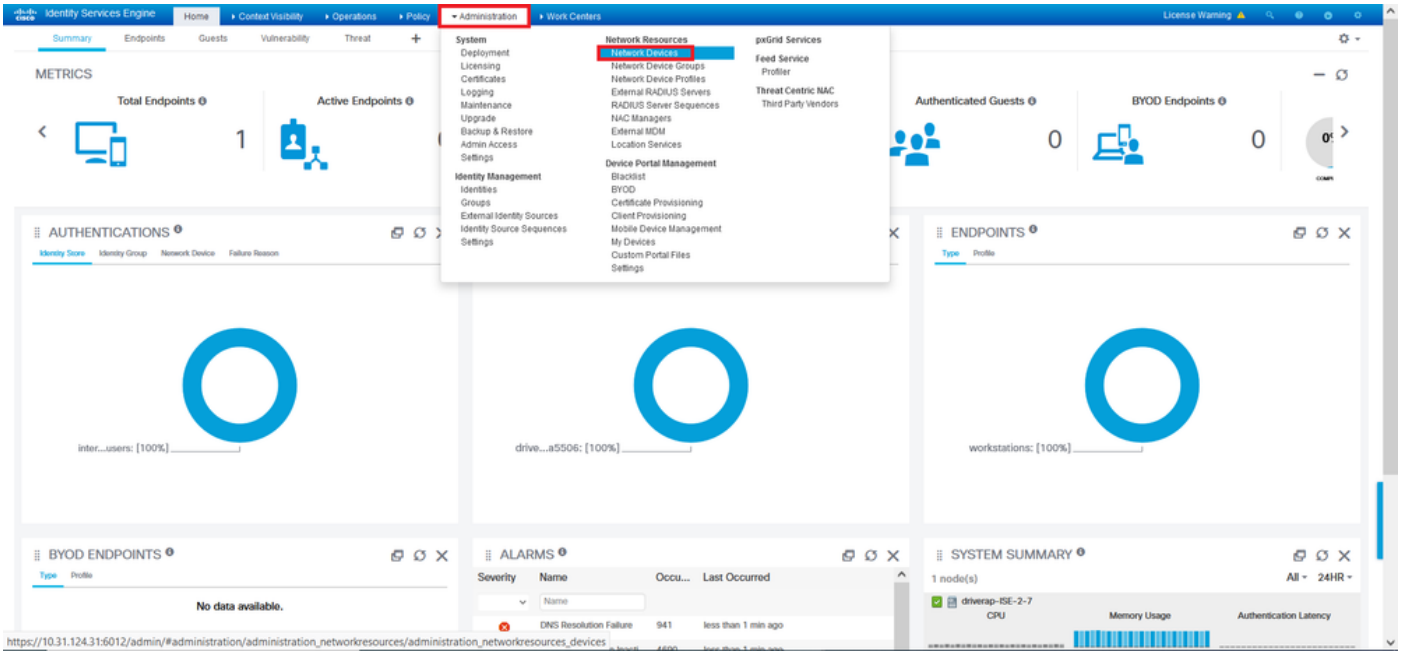
La configurazione VPN ad accesso remoto nella CLI del FTD è:

```
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
```

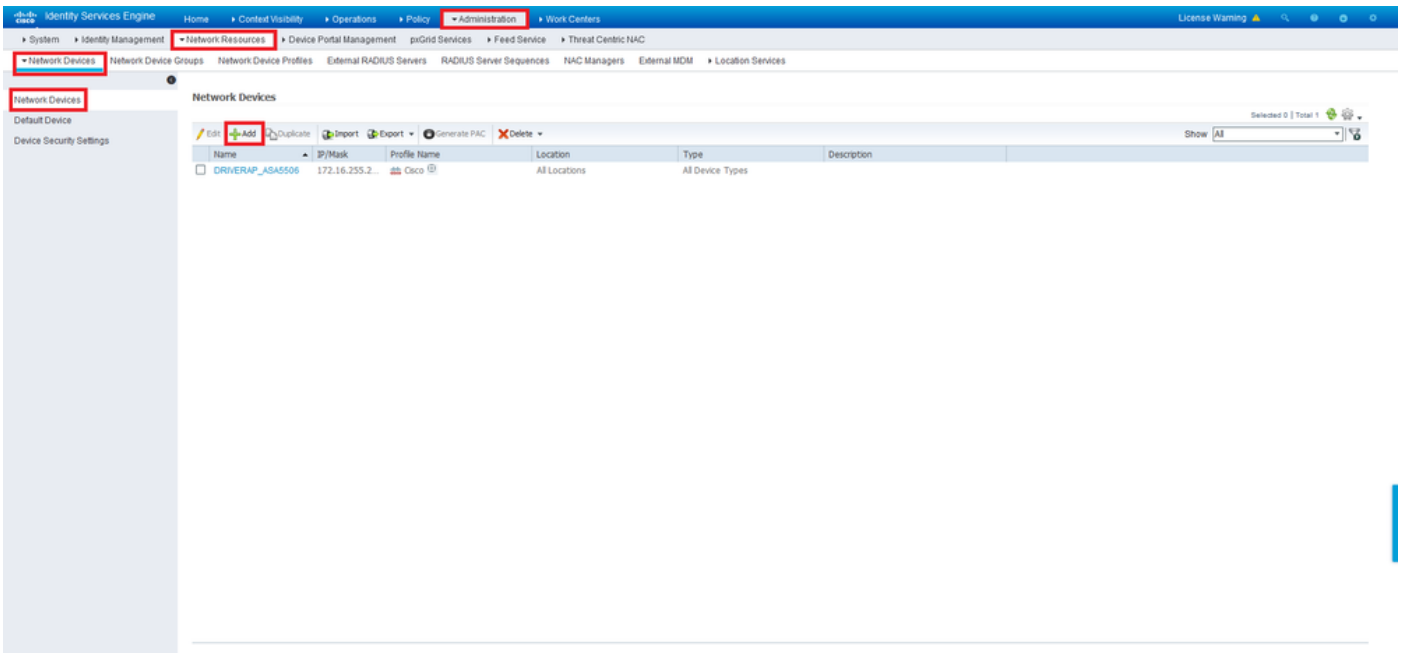
```
fqdn none
subject-name CN=192.168.0.100
keypair <Default-RSA-Key>
crl configure

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
```

Configura criterio di autorizzazione su ISE (server RADIUS)

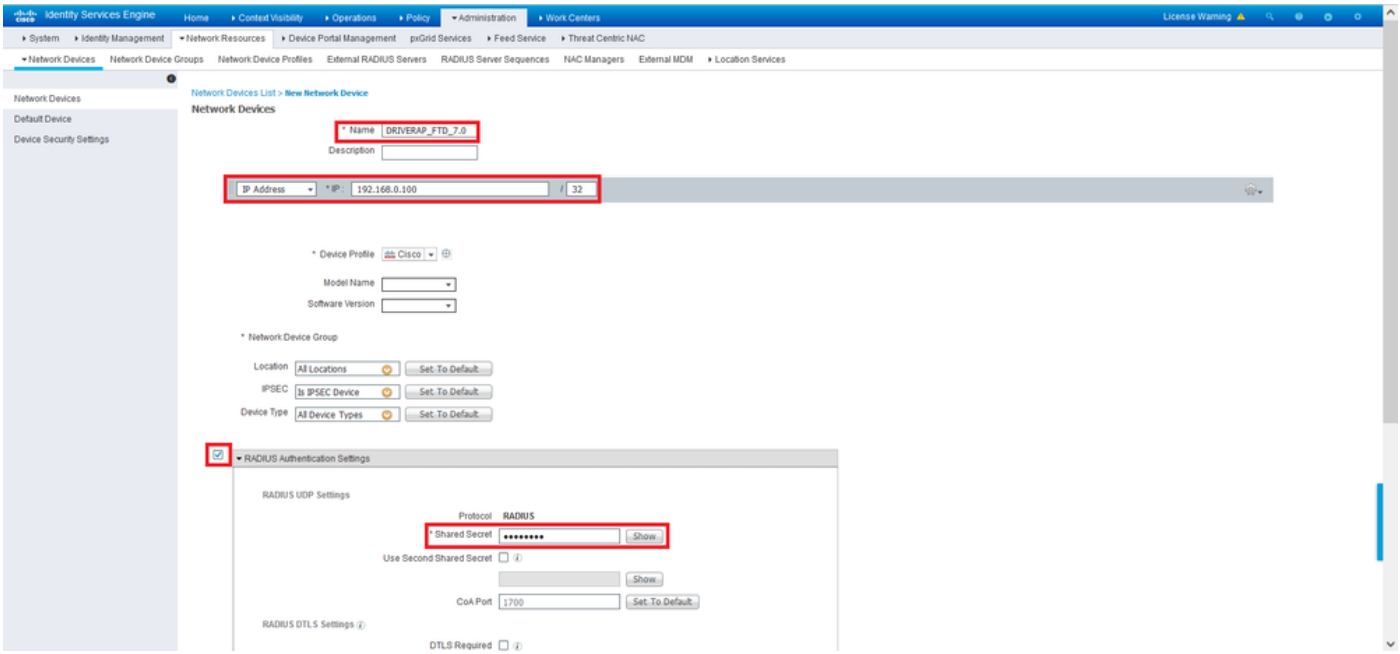
Passaggio 1. Accedere al server ISE e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**.



Passaggio 2. Nella sezione Dispositivi di rete, fare clic su **Add** per elaborare le richieste di accesso RADIUS dall'FTD.

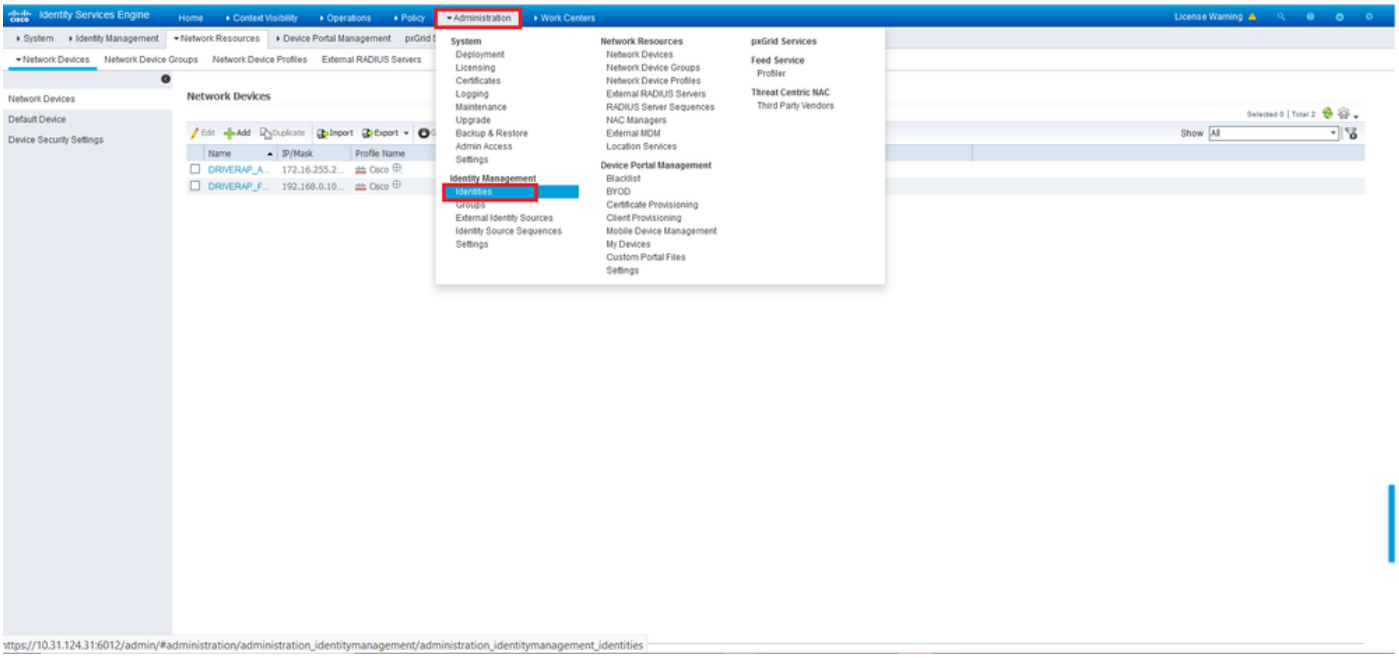


Immettere i campi **Nome** dispositivo di rete e **Indirizzo IP**, quindi selezionare la casella **Impostazioni autenticazione RADIUS**. Il **segreto condiviso** deve essere lo stesso valore utilizzato al momento della creazione dell'oggetto server RADIUS in FMC.

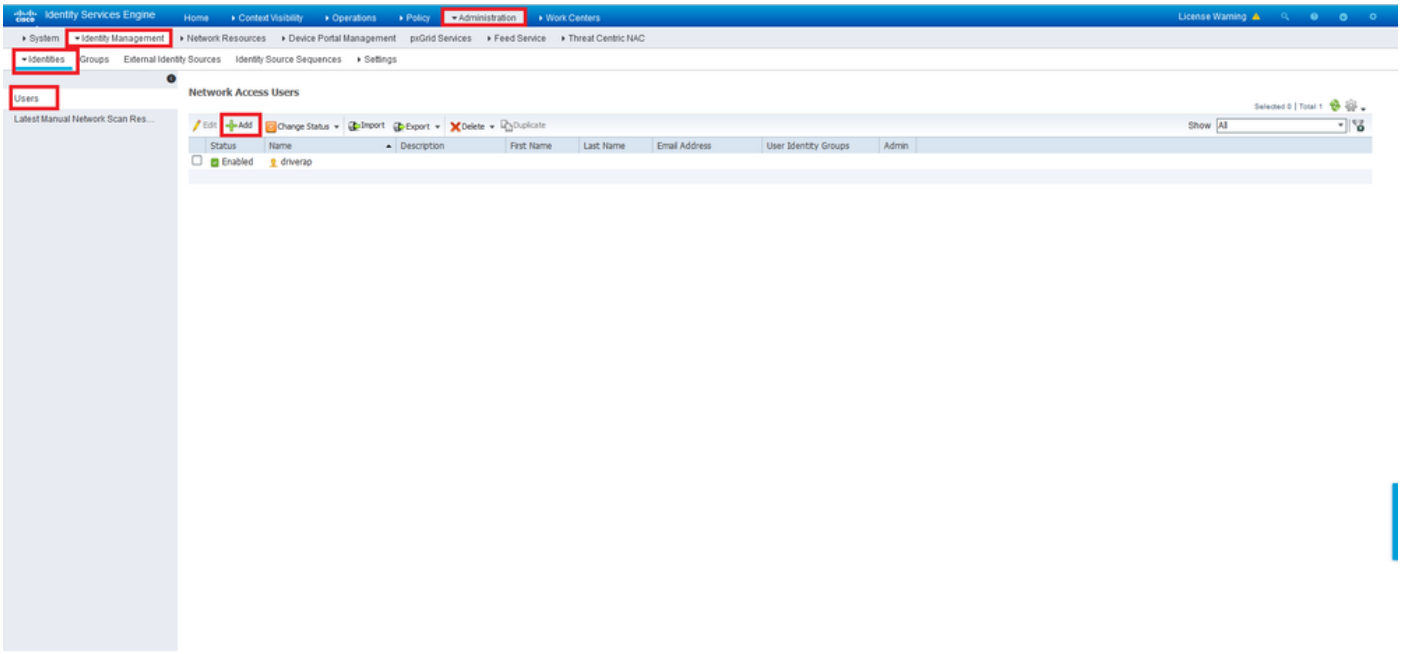


Salvarlo con il pulsante alla fine della pagina.

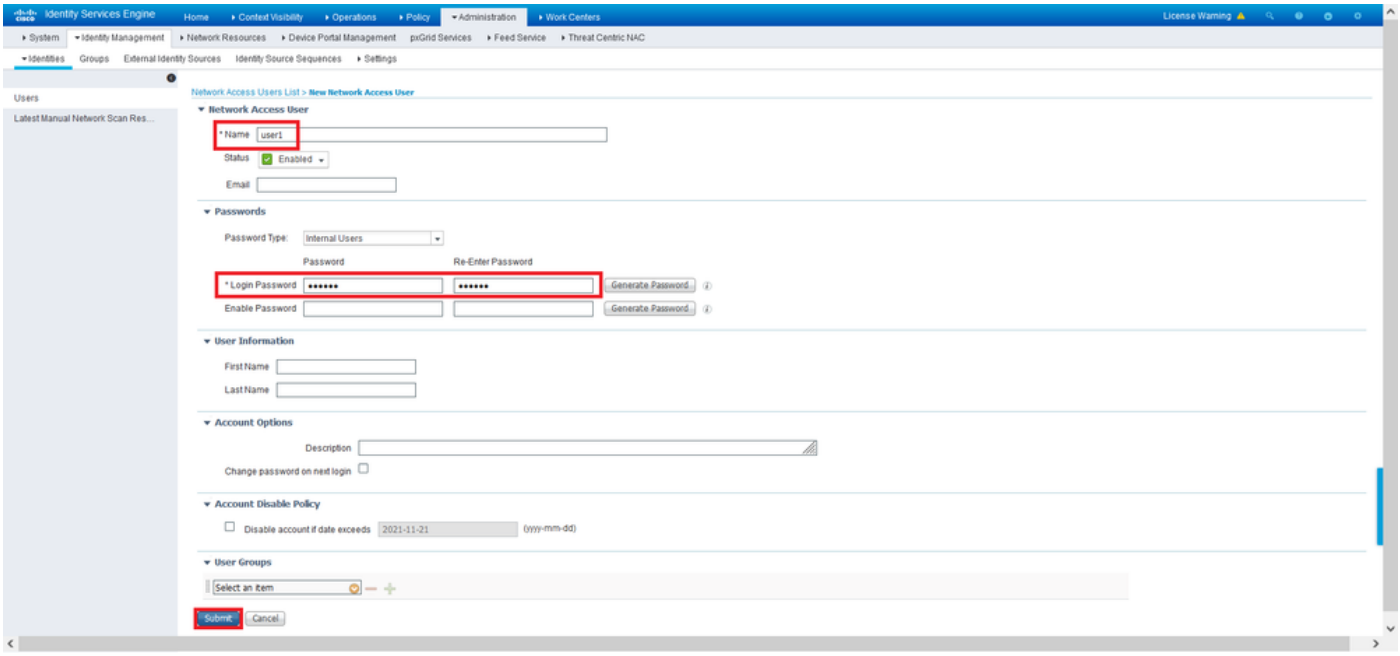
Passaggio 3. Passare a **Amministrazione > Gestione delle identità > Identità**.



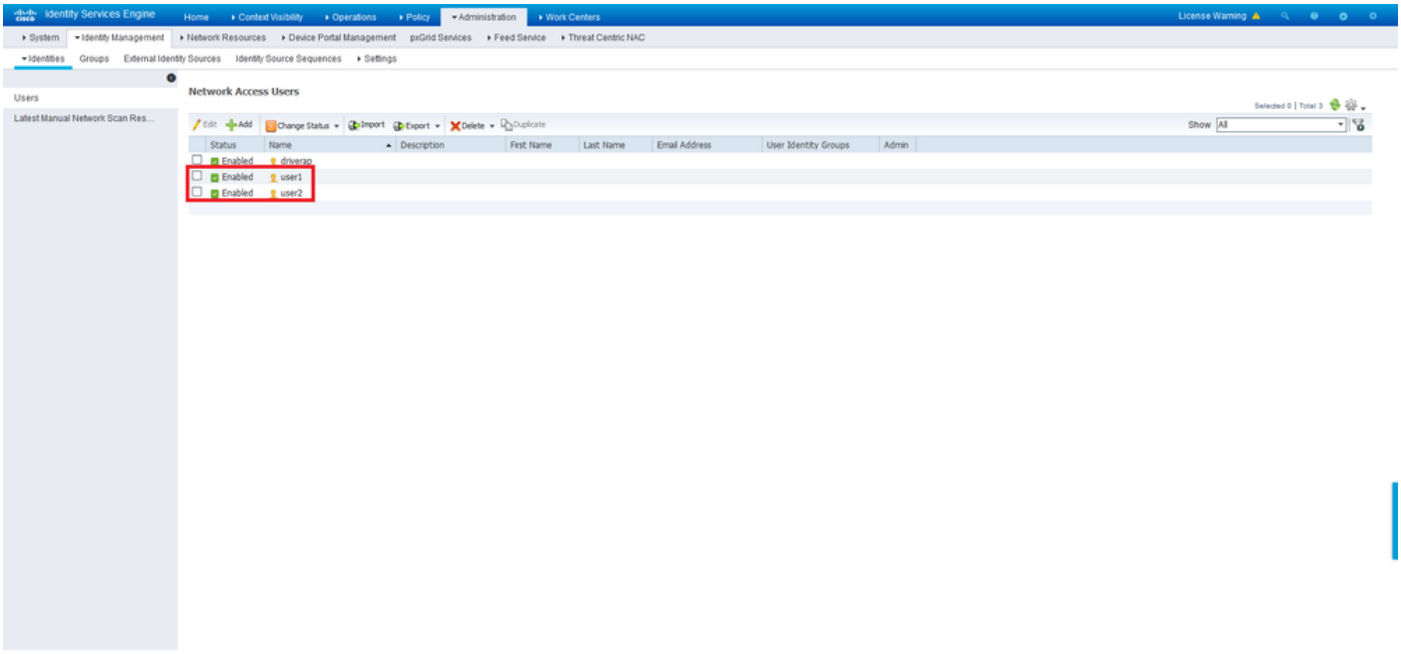
Passaggio 4. Nella sezione Network Access Users, fare clic su **Add** per creare *user1* nel database locale di ISE.



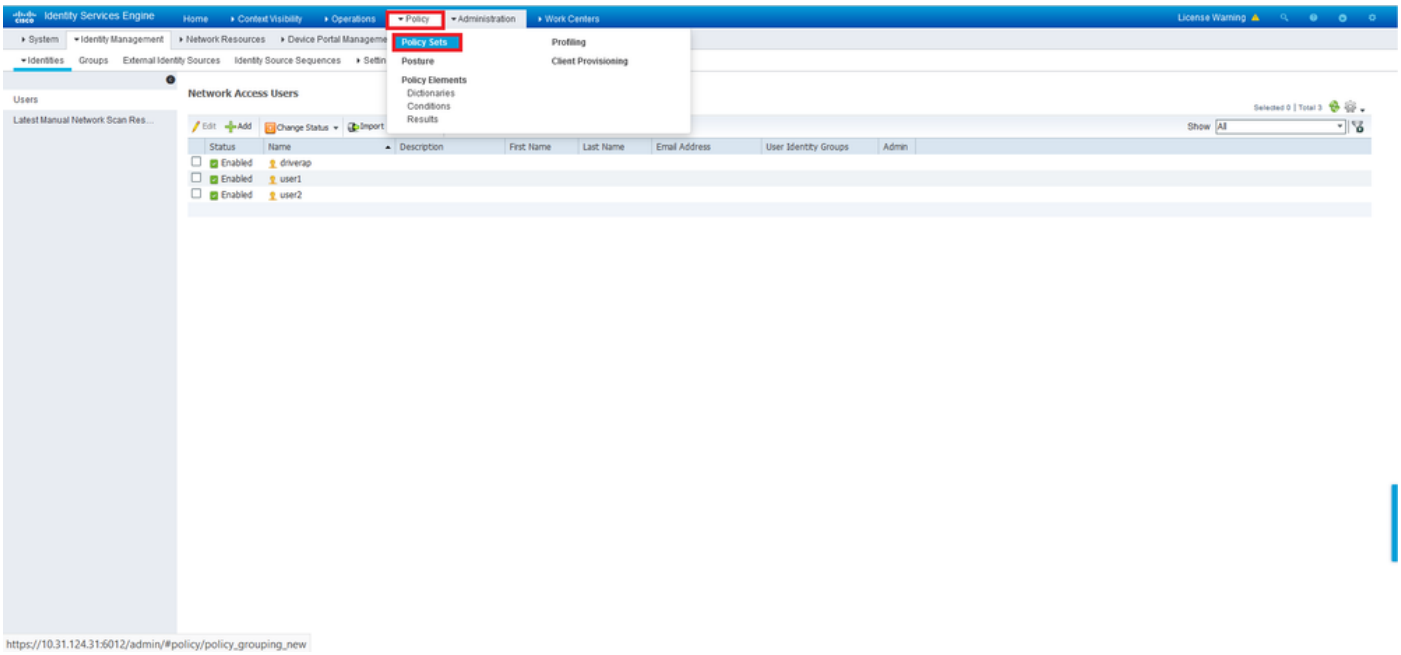
Immettere nome utente e password nei campi **Nome** e **Password di accesso** e quindi fare clic su **Invia**.



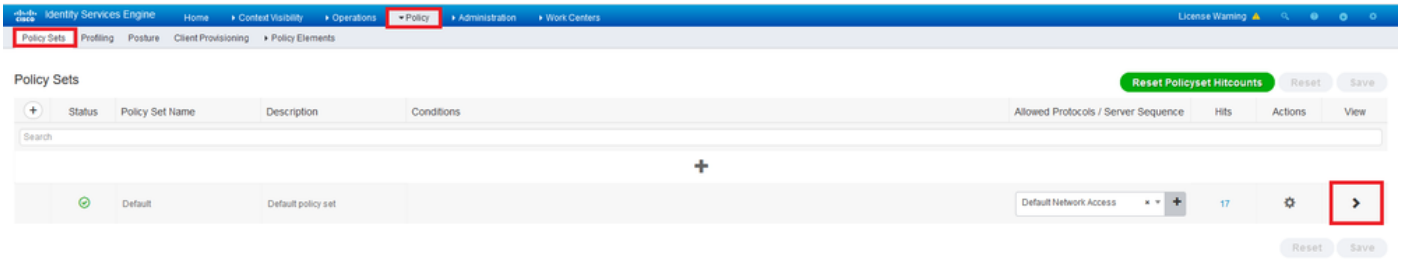
Passaggio 5. Ripetere i passaggi precedenti per creare *user2*.



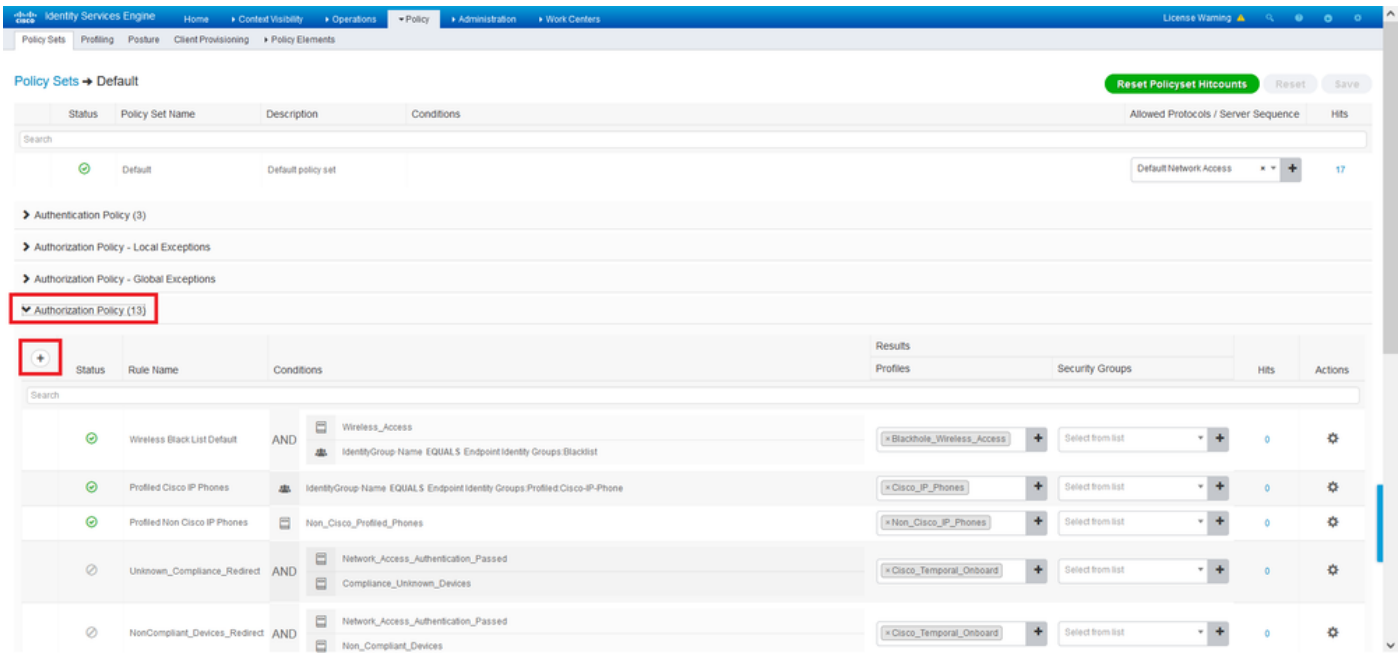
Passaggio 6. Andare a **Policy > Policy Sets (Policy > Set di policy).**



Passaggio 7. Fare clic sulla freccia > sul lato destro della schermata.

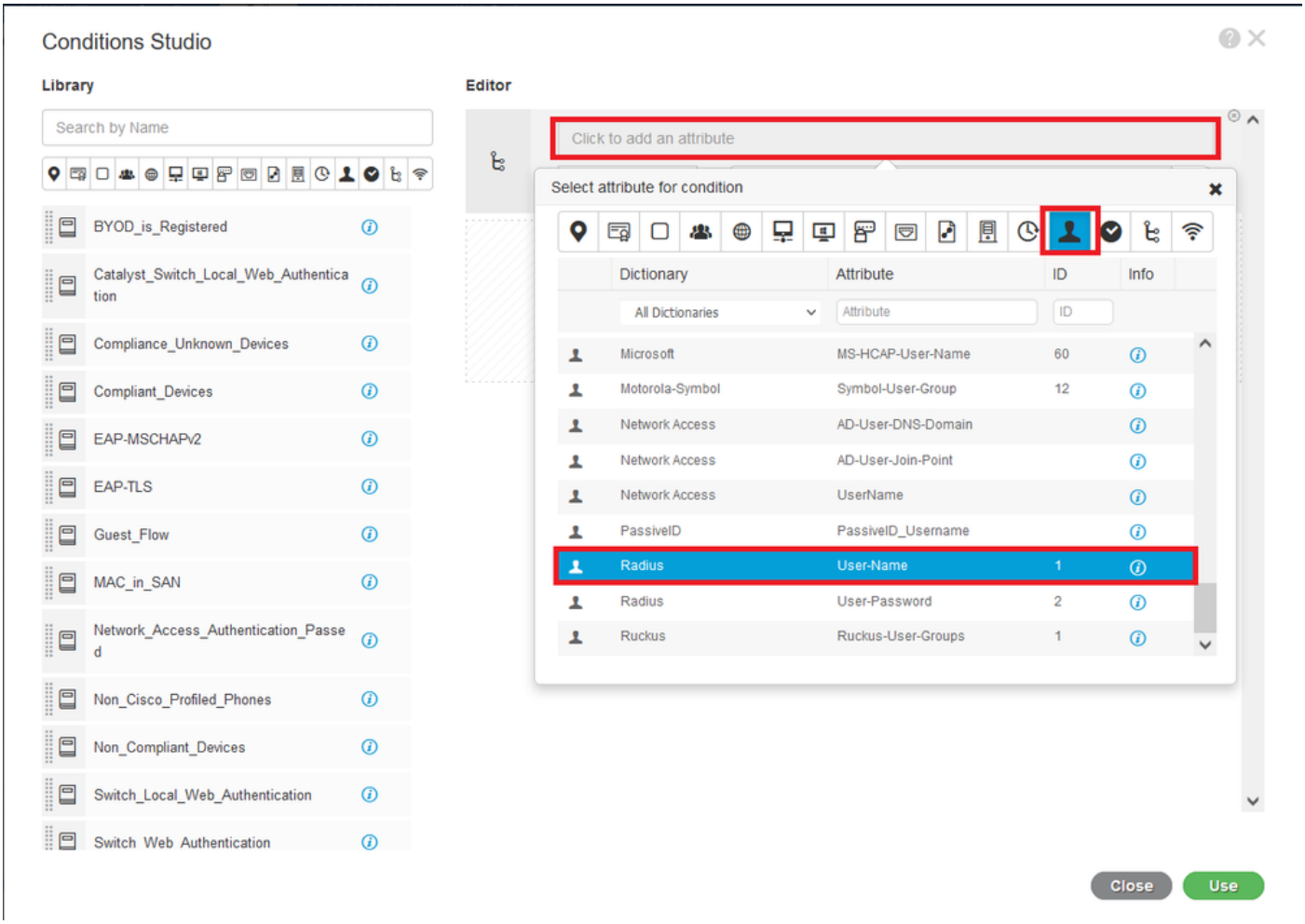


Passaggio 8. Fare clic sulla freccia **>** accanto a **Criteri di autorizzazione** per espanderlo. A questo punto, fare clic sul simbolo *+* per aggiungere una nuova regola.

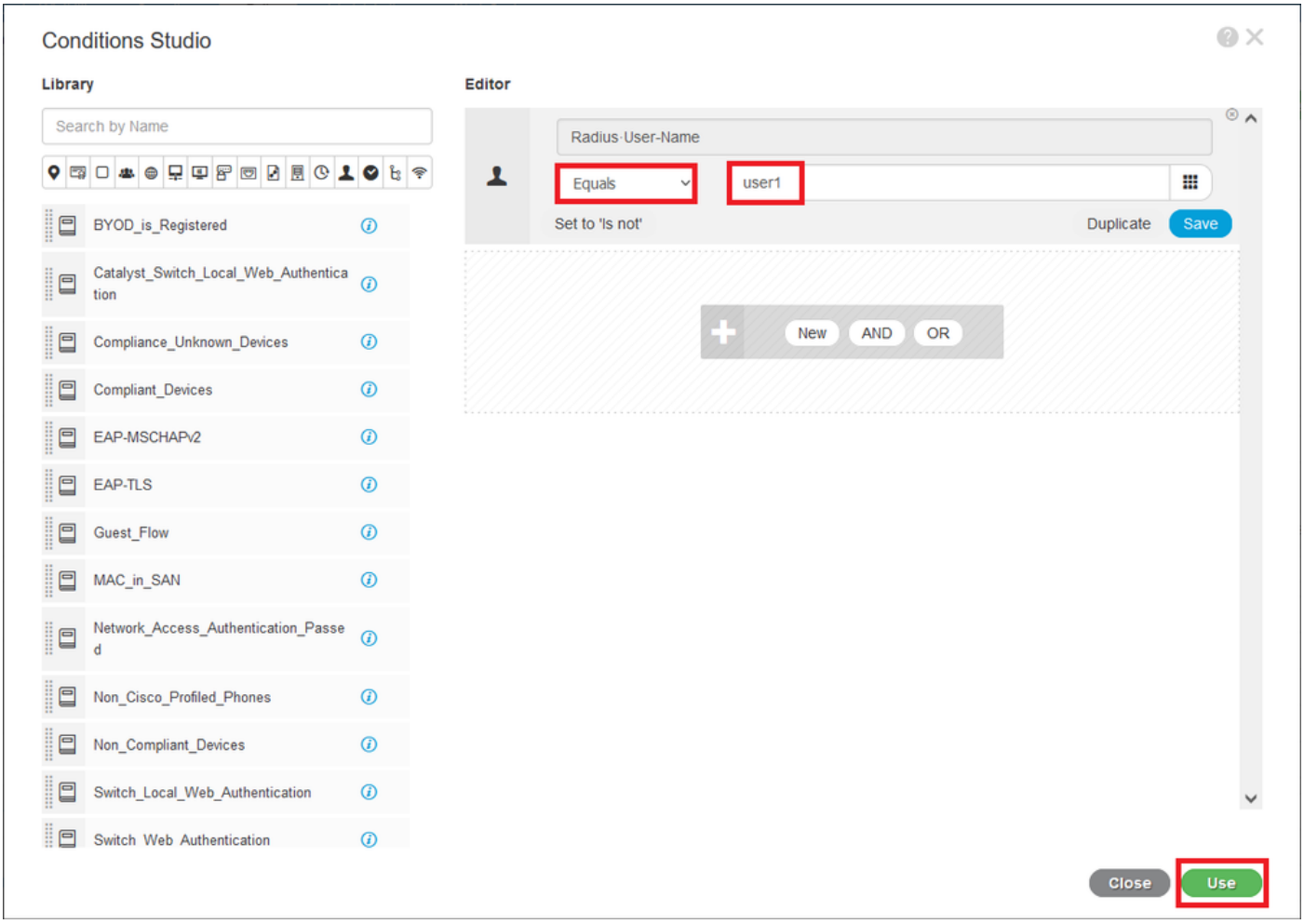


Fornite un nome alla regola e selezionate il simbolo *+* nella colonna **Condizioni (Conditions)**.

Fare clic nella casella di testo Editor attributi e fare clic sull'icona **Oggetto**. Scorrere verso il basso fino a individuare l'attributo *Nome utente RADIUS* e selezionarlo.

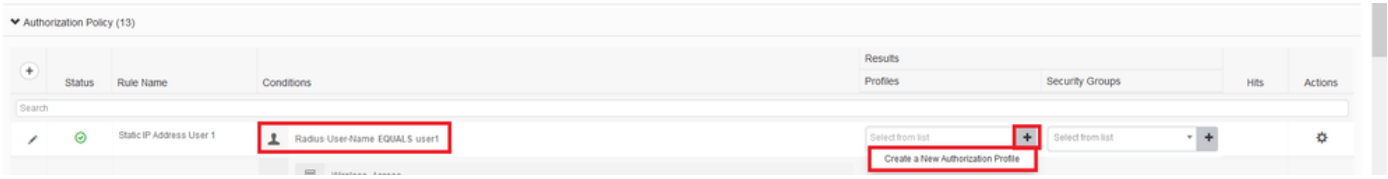


Mantieni **uguale** come operatore e immettere *user1* nella casella di testo accanto ad esso. Per salvare l'attributo, fare clic su **Use** (Usa).

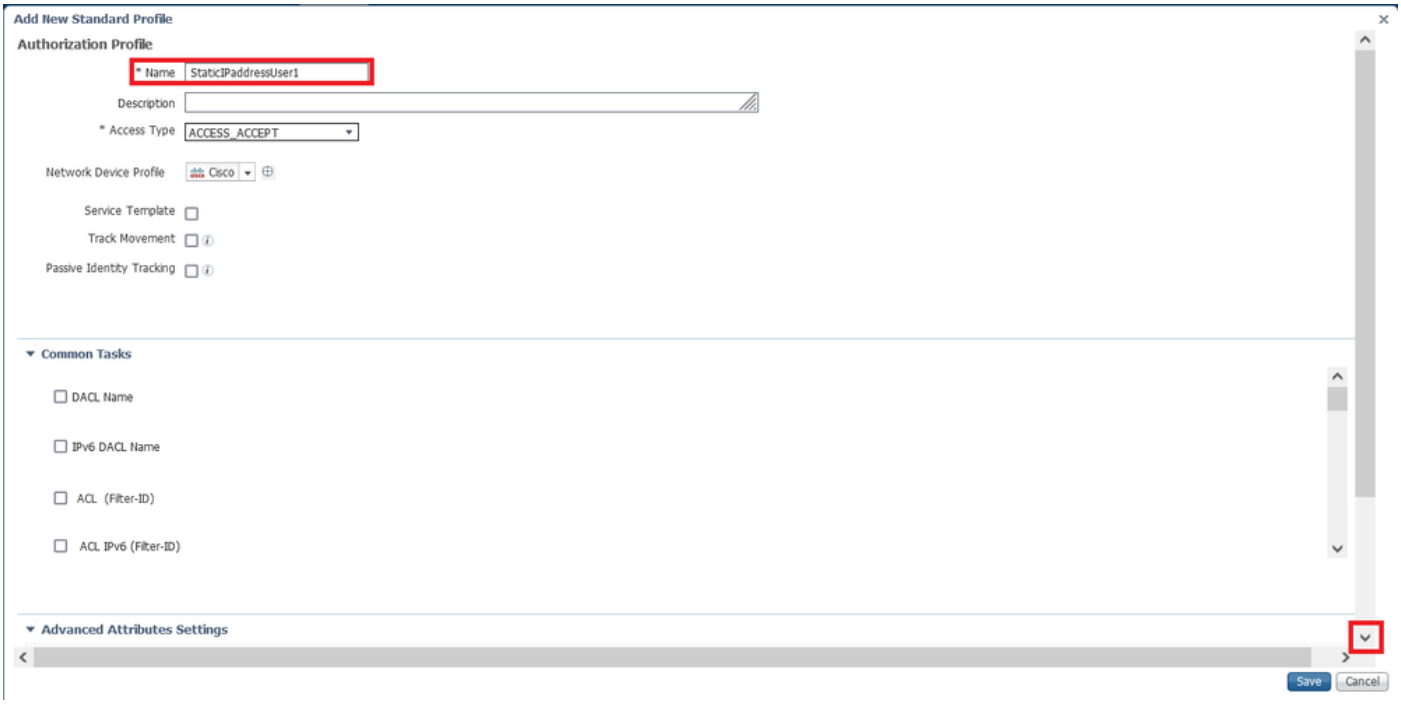


La condizione per questa regola è ora impostata.

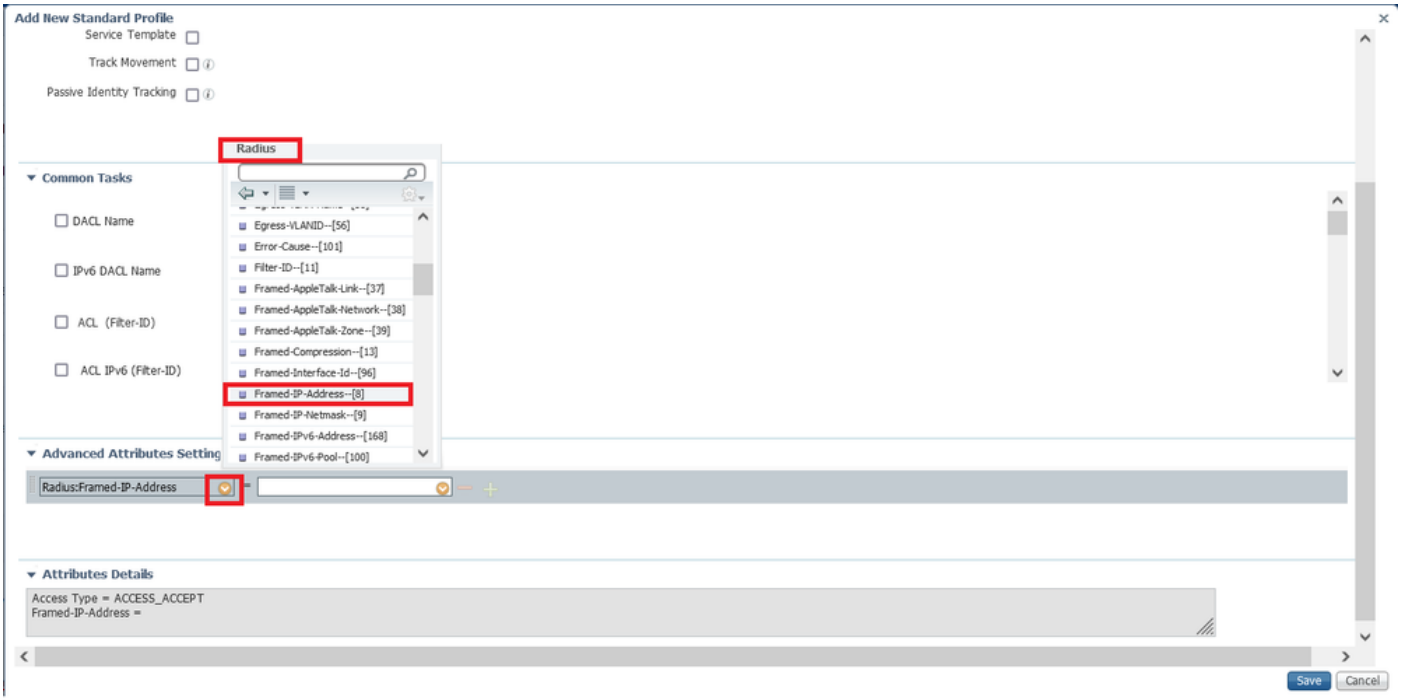
Passaggio 9. Nella colonna **Risultati/Profili**, fare clic sul simbolo + e scegliere **Crea nuovo profilo di autorizzazione**.



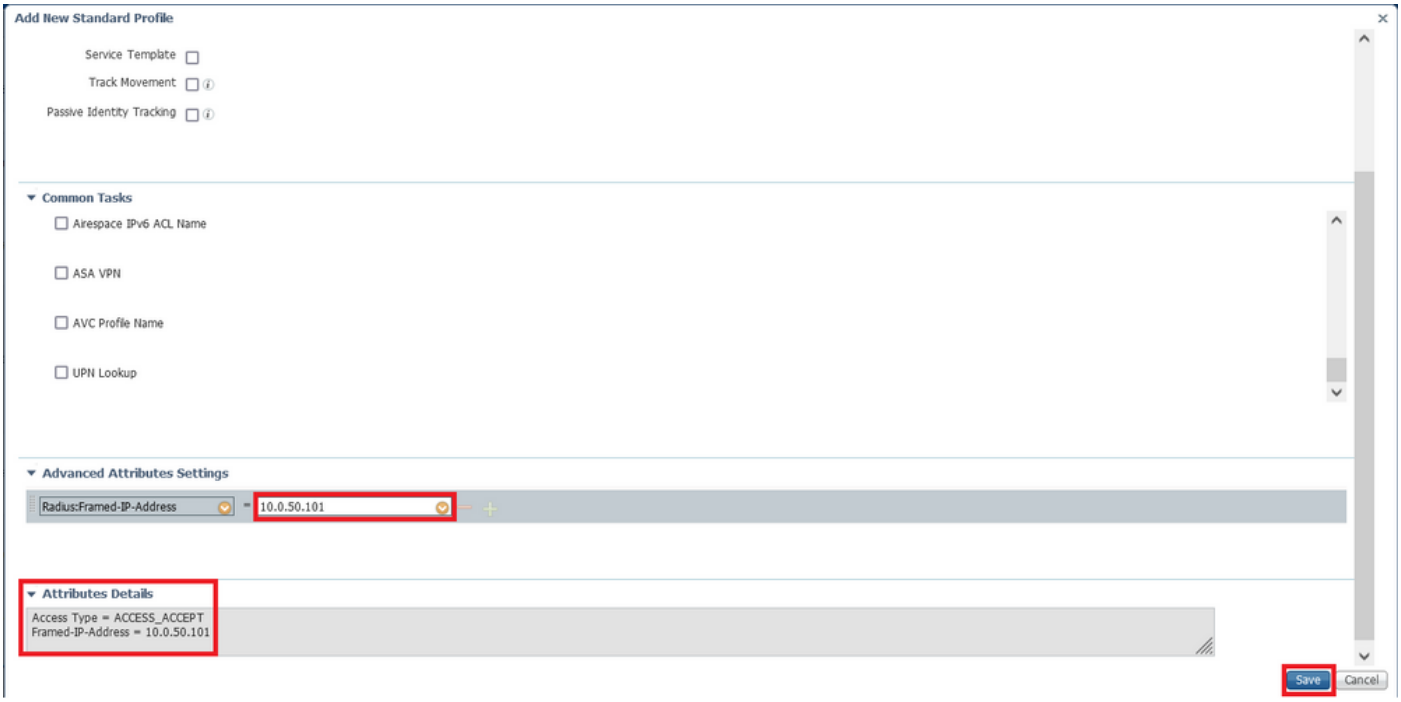
Assegnare un **nome** al file e mantenere *ACCESS_ACCEPT* come **Tipo di accesso**. Scorrere fino alla sezione **Impostazioni avanzate attributi**.



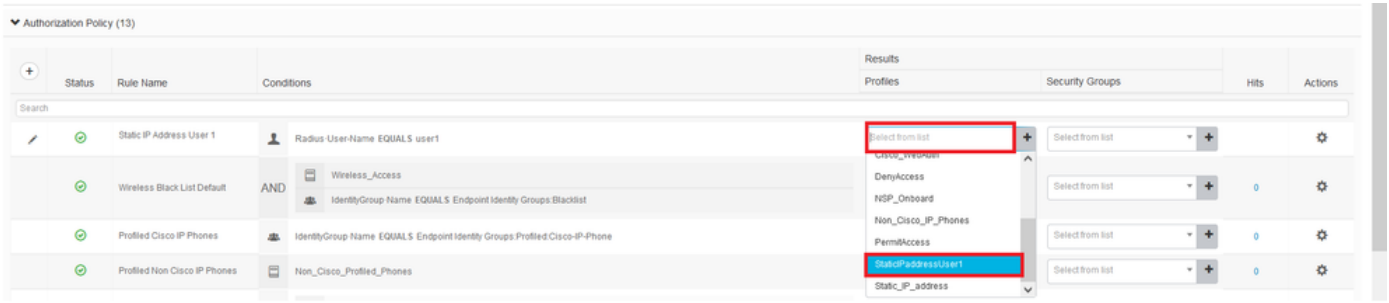
Fate clic sulla freccia arancione e scegliete **Raggio (Radius) > Indirizzo-IP-Frame-[8]**.



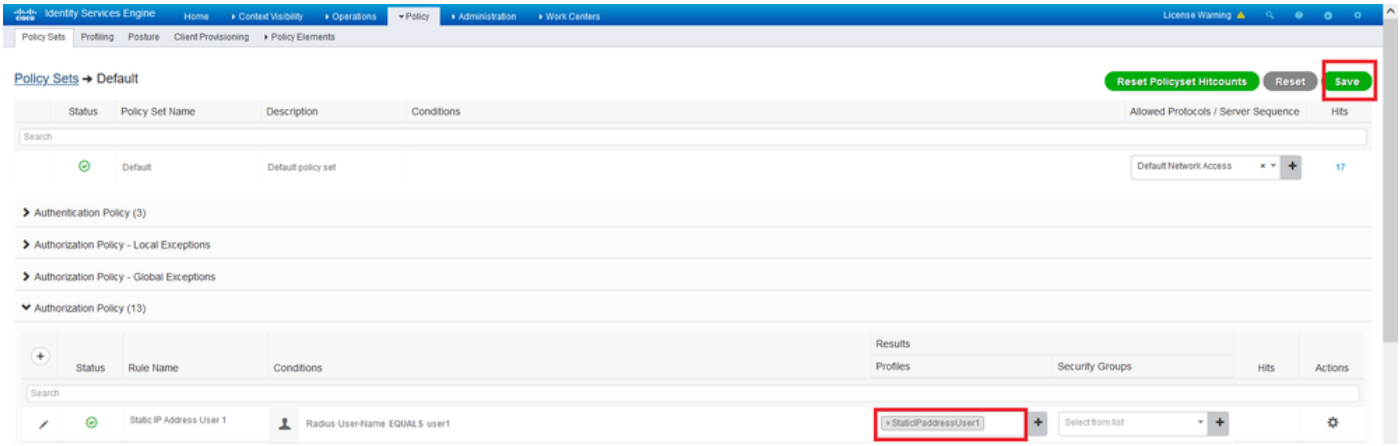
Digitare l'indirizzo IP che si desidera assegnare in modo statico sempre a questo utente e fare clic su **Salva**.



Passaggio 10. Scegliere il profilo di autorizzazione appena creato.

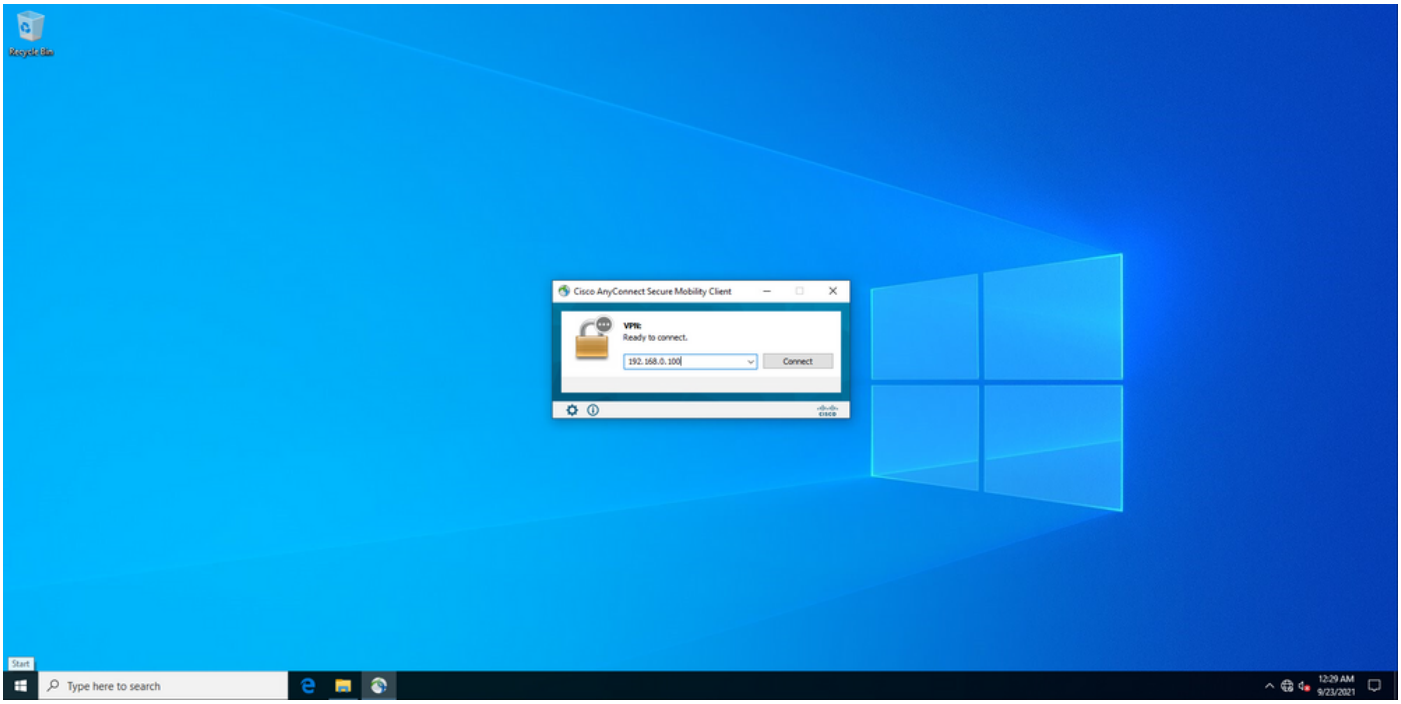


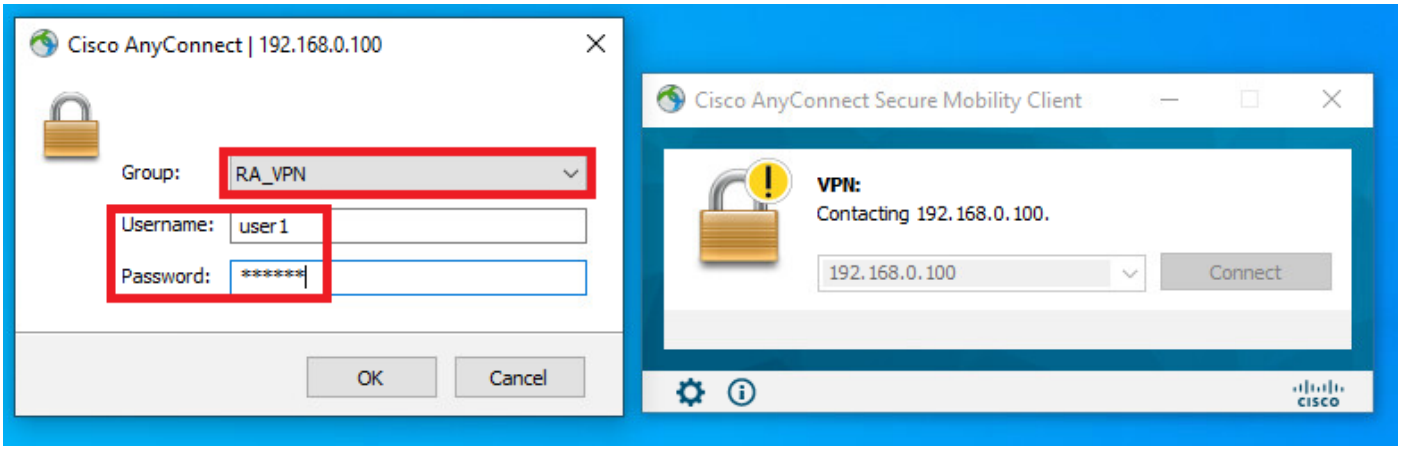
La regola di autorizzazione è ora impostata. Fare clic su **Salva**.



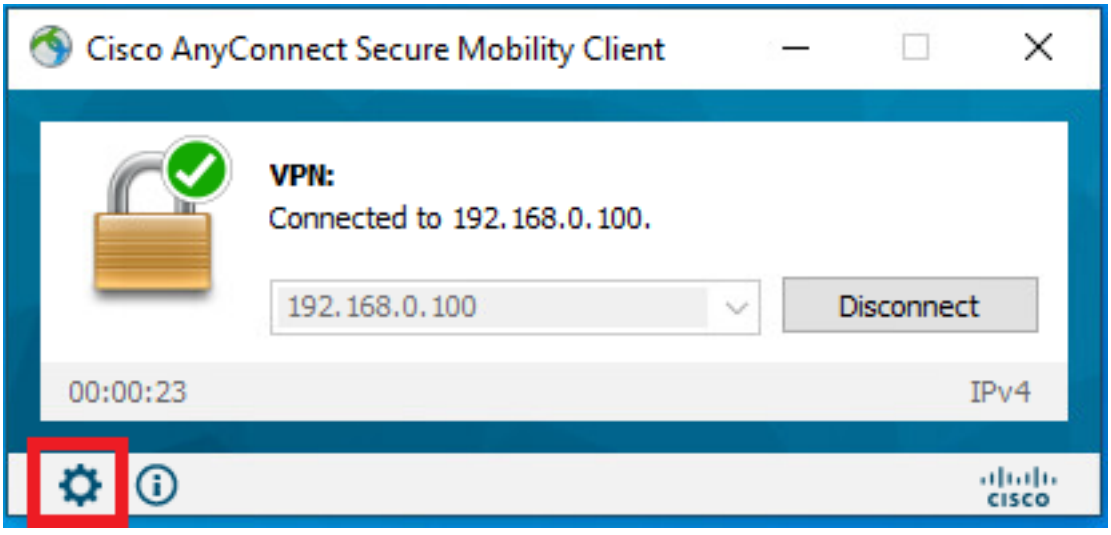
Verifica

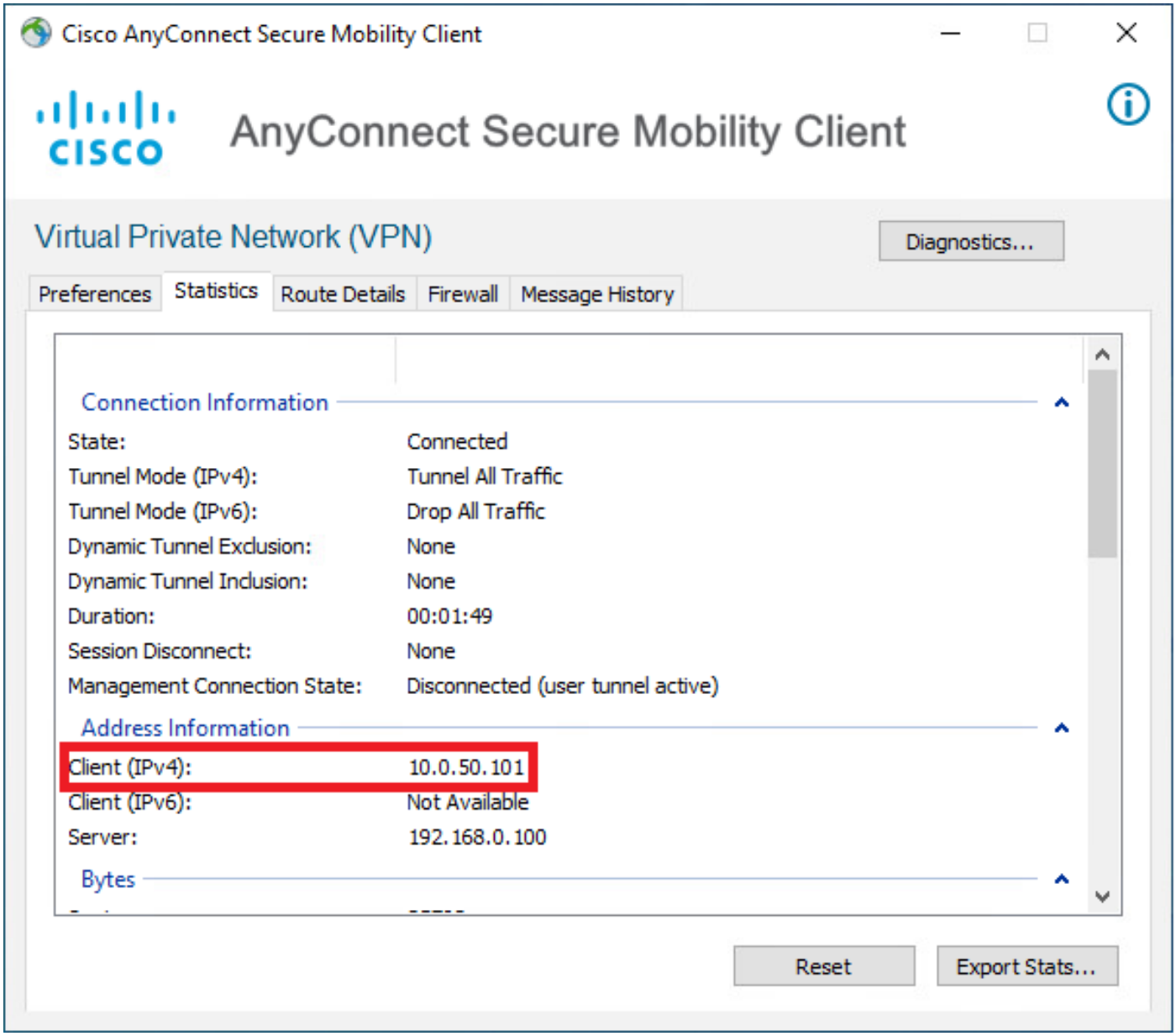
Passaggio 1. Passare al computer client in cui è installato il client Cisco AnyConnect Secure Mobility. Connettersi all'headend FTD (qui viene utilizzato un computer Windows) e immettere le credenziali *utente1*.





Fare clic sull'icona dell'ingranaggio (nell'angolo in basso a sinistra) e selezionare la scheda **Statistiche**. Confermare nella sezione **Informazioni indirizzo** che l'indirizzo IP assegnato è effettivamente quello configurato nel criterio di autorizzazione ISE per questo utente.





L'output del comando **debug radius all** sull'FTD visualizza:

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

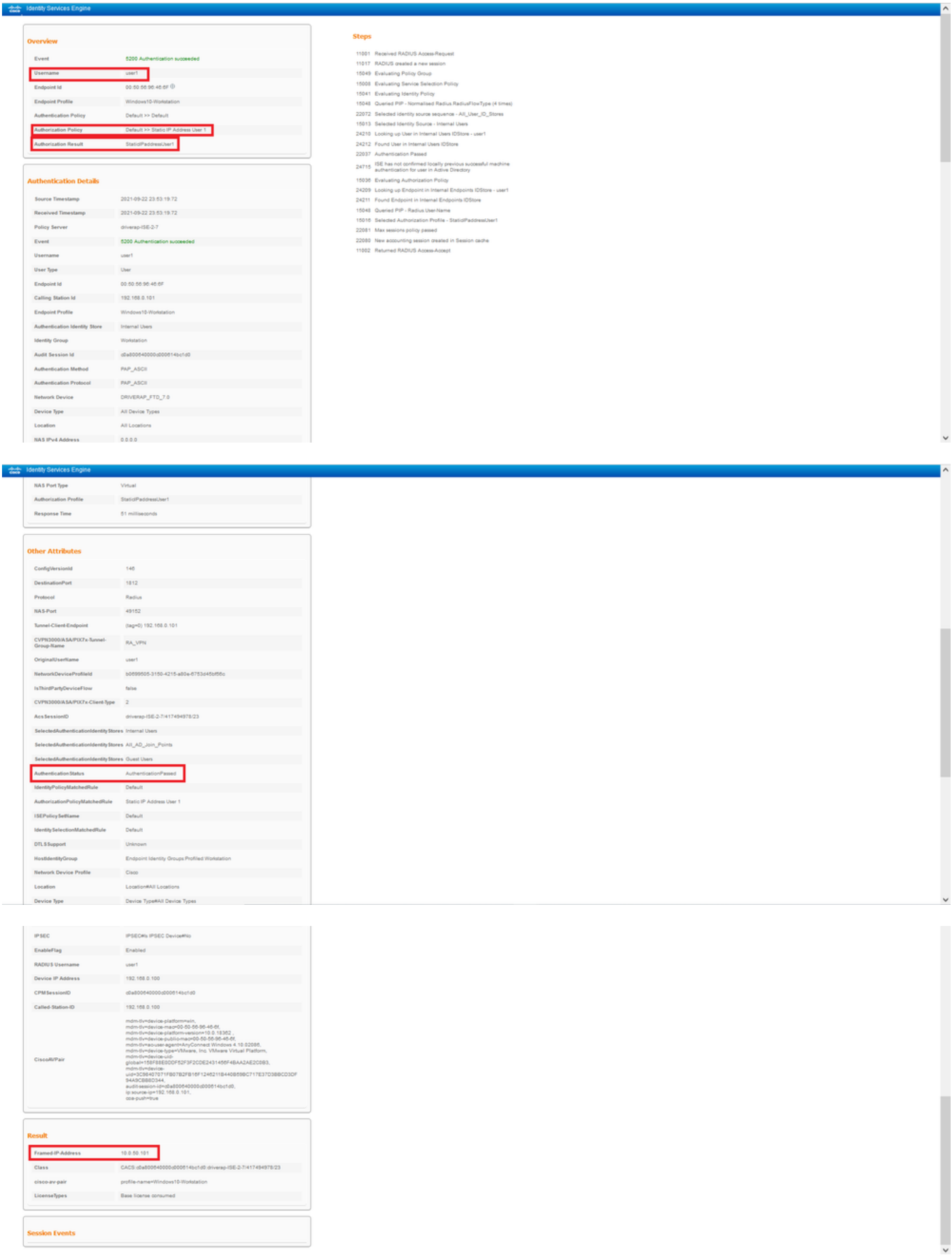
```
02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 | .......AK..X...1
7d aa 38 1e 01 07 75 73 65 72 31 08 06 0a 00 32 | }.8...user1....2
65 19 3d 43 41 43 53 3a 63 30 61 38 30 30 36 34 | e.=CACS:c0a80064
30 30 30 30 61 30 30 30 36 31 34 62 63 30 32 64 | 0000a000614bc02d
3a 64 72 69 76 65 72 61 70 2d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

I log FTD mostrano:

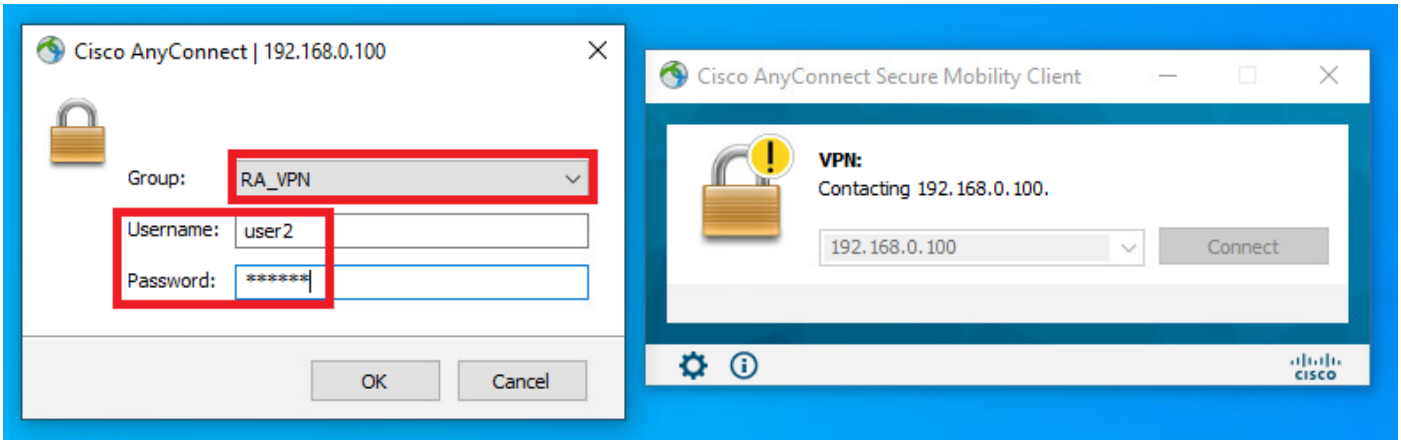
```
firepower#
<omitted output>
Sep 22 2021 23:52:40: %FTD-6-725002: Device completed SSL handshake with client
Outside_Int:192.168.0.101/60405 to 192.168.0.100/443 for TLSv1.2 session
Sep 22 2021 23:52:48: %FTD-7-609001: Built local-host Outside_Int:172.16.0.8
Sep 22 2021 23:52:48: %FTD-6-113004: AAA 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**

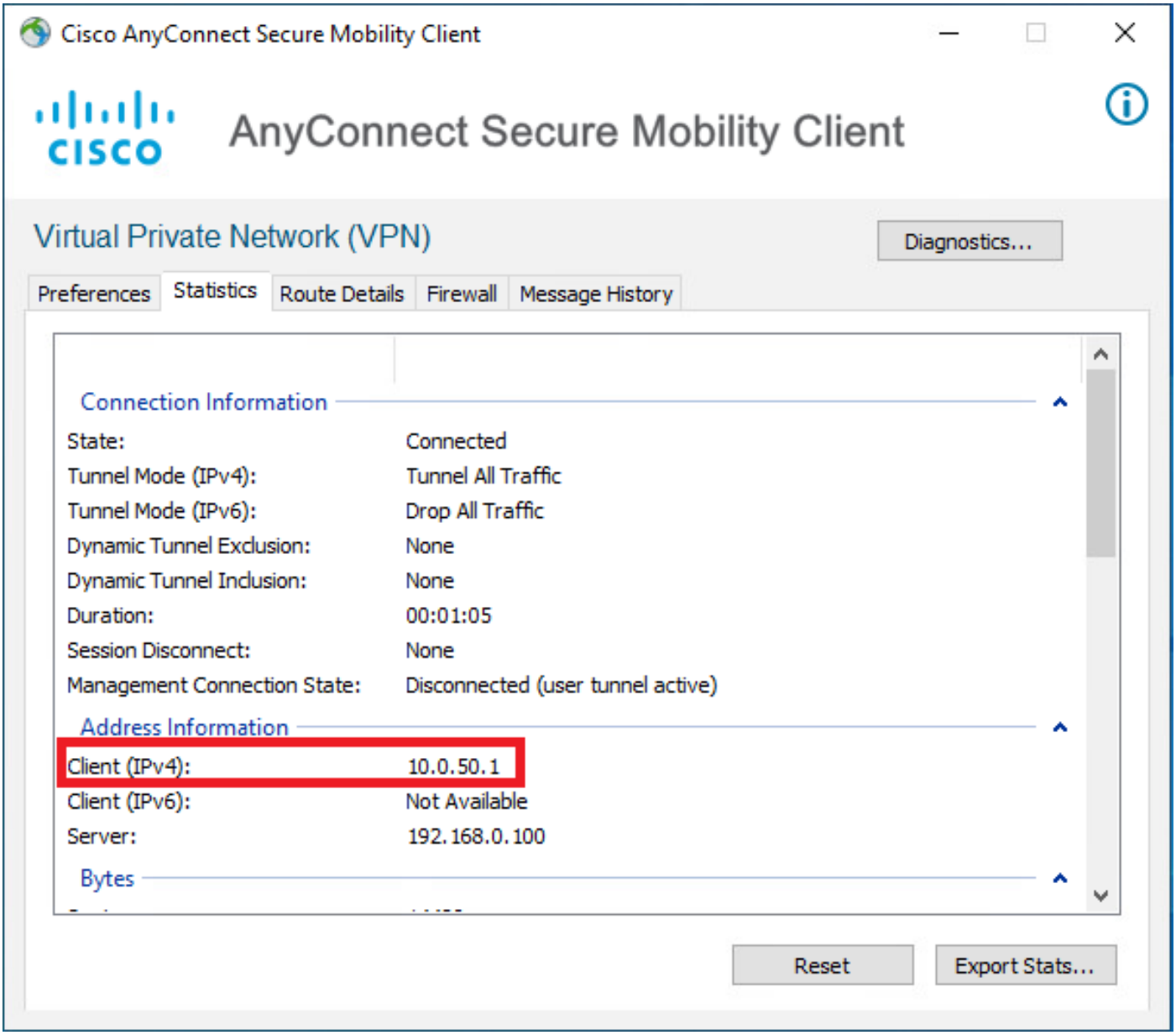
I log di RADIUS Live su ISE mostrano:



Passaggio 2. Connettersi all'headend FTD (qui viene utilizzato un computer Windows) e immettere le credenziali *utente2*.



La sezione **Address Information** mostra che l'indirizzo IP assegnato è effettivamente il primo indirizzo IP disponibile nel pool locale IPv4 configurato tramite FMC.



L'output del comando **debug radius all** sull'FTD visualizza:

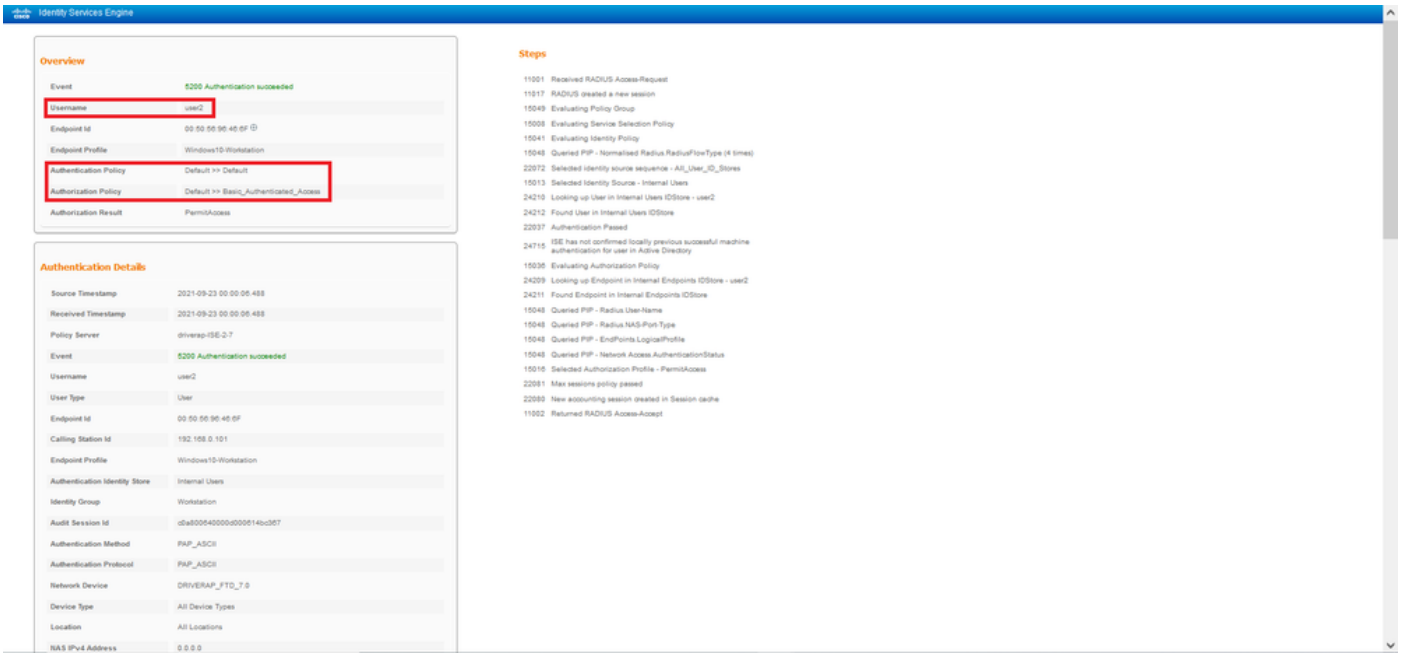
```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
```

```
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
```

I log FTD mostrano:

<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**

I log di RADIUS Live su ISE mostrano:



Nota: Per evitare conflitti di indirizzi IP duplicati tra i tuoi client AnyConnect, è necessario utilizzare intervalli di indirizzi IP diversi per l'assegnazione degli indirizzi IP sia sul pool locale IP FTD che sui criteri di autorizzazione ISE. Nell'esempio di configurazione, il protocollo FTD è stato configurato con un pool locale IPv4 compreso tra 10.0.50.1 e 10.0.50.100, quindi il server ISE assegna un indirizzo IP statico pari a 10.0.50.101.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Su FTD:

- **debug radius all**

ISE:

- Registri attivi RADIUS