

# ي مدختسمل تباثلا IP ناووع نييغت نيوكت RADIUS ضيوقت ربع AnyConnect

## تاوتحمل

[عمدقمل](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسمل تانوكمل](#)

[نيوكتلا](#)

[ةكبش ل ل يطيطختلا مسرلا](#)

[FMC ربع AAA/RADIUS ةقداصم مادختساب دعب نع لوصولل VPN ةكبش نيوكت](#)

[\(RADIUS مداخ\) ISE لعل ليوختلا جهن نيوكت](#)

[ةحصلا نم ققحتلا](#)

[اهجالص او عااطخألا فاشكتسا](#)

## عمدقمل

ةيوهلا تامدخ كرحم مداخ مادختساب RADIUS ضيوقت نيوكت ةيفيكت دننتسمل اذه فصبي  
(FTD) FirePOWER ديدهت نع عافدلا ل هسفن IP ناووع هيچوت ةداعإ امئاد موقبي كلذل (ISE)  
يتلا 8 RADIUS ةمس ربع Cisco AnyConnect Secure Mobility Client نم صاخ مدختسمل  
رطوؤمل IP ناووع نمضتت.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلالاتل عيضاوملاب ةفرعم كيديل نوكت ناب Cisco ي صوت:

- Firepower Threat Defense (FTD) ماظن
- Firepower (FMC) ةرادإ زكرم
- (ISE) ةيوهلا فشك تامدخ كرحم
- Cisco AnyConnect Secure Mobility Client
- RADIUS لوكوتورب

### عمدختسمل تانوكمل

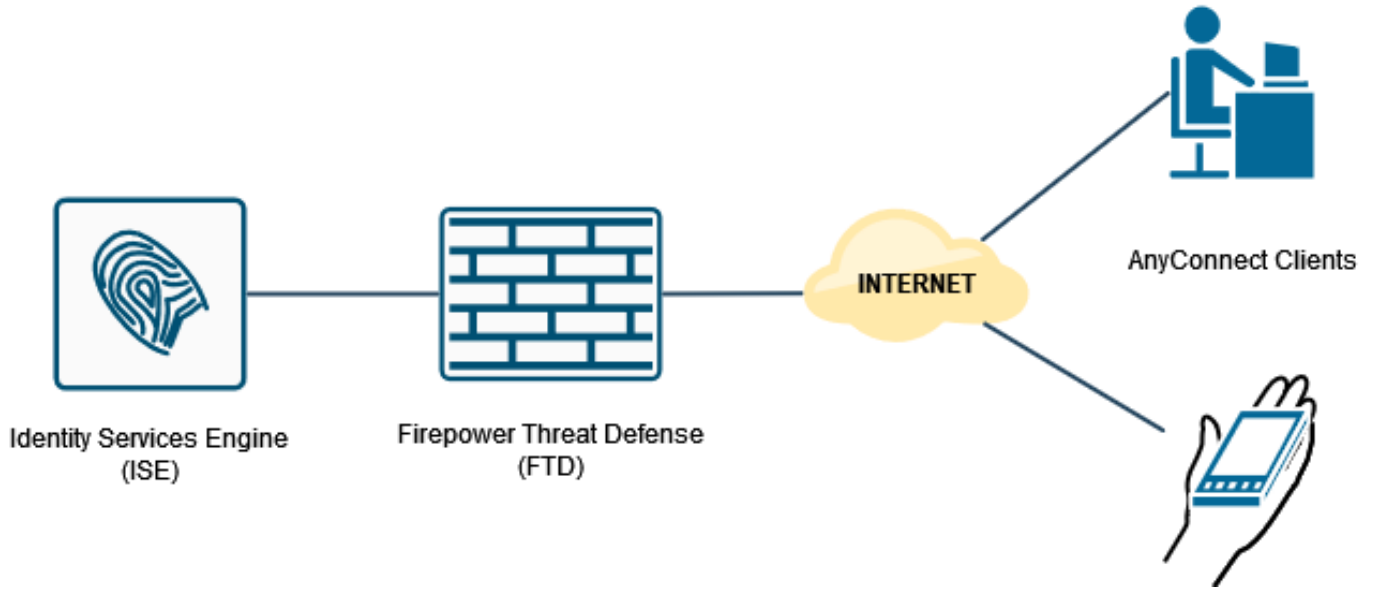
ةيلالاتل جماربال تارادصإ ل دننتسمل اذه يف ةدراولا تامولعمل دننتست:

- FMCv - 7.0.0 (ةينب) 94
- FTDv - 7.0.0 (ةينبلا) 94
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086
- Windows 10 Pro ليغشتلا ماظن

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراولما تامولعملما عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالا عيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكأتف ،ليغشتلا دي ق ك تكبش

## نيوكتلا

### ةكبش ل ل يطي طختلا مسرلا



### ر ب ع AAA/RADIUS ةقداصم مادختساب دع ب نع لوصولل VPN ةكبش نيوكت FMC

ويديفالا اذهو دنتسملا اذه ي ل ع ج را ،ةوطخب ةوطخ لصفم ءارجا يلع لوصولل

- [FTD يلع AnyConnect Remote Access VPN نيوكت](#)
- [FMC ةطساوب رادمل ل ي ل وائل AnyConnect نيوكت](#)

FTD ل (CLI) رم اوائل رطس ةهجاو يلع دع ب نع لوصولل VPN نيوكت:

```
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

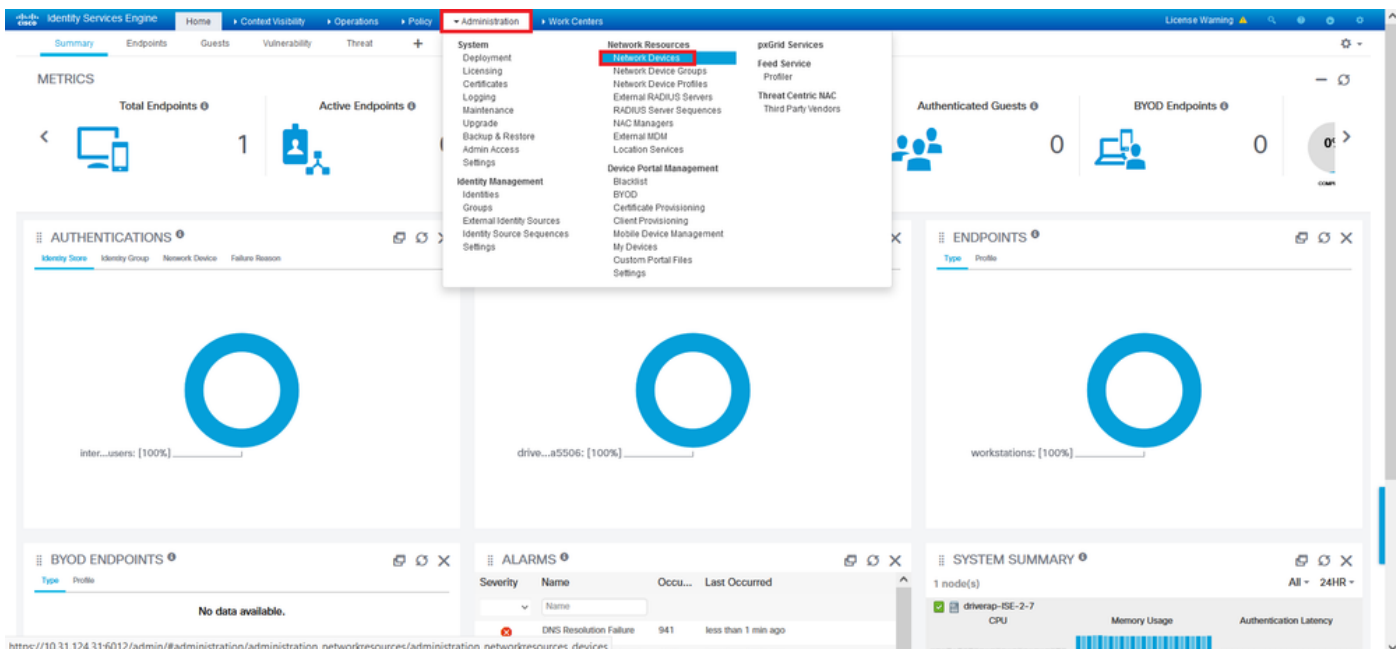
webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list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

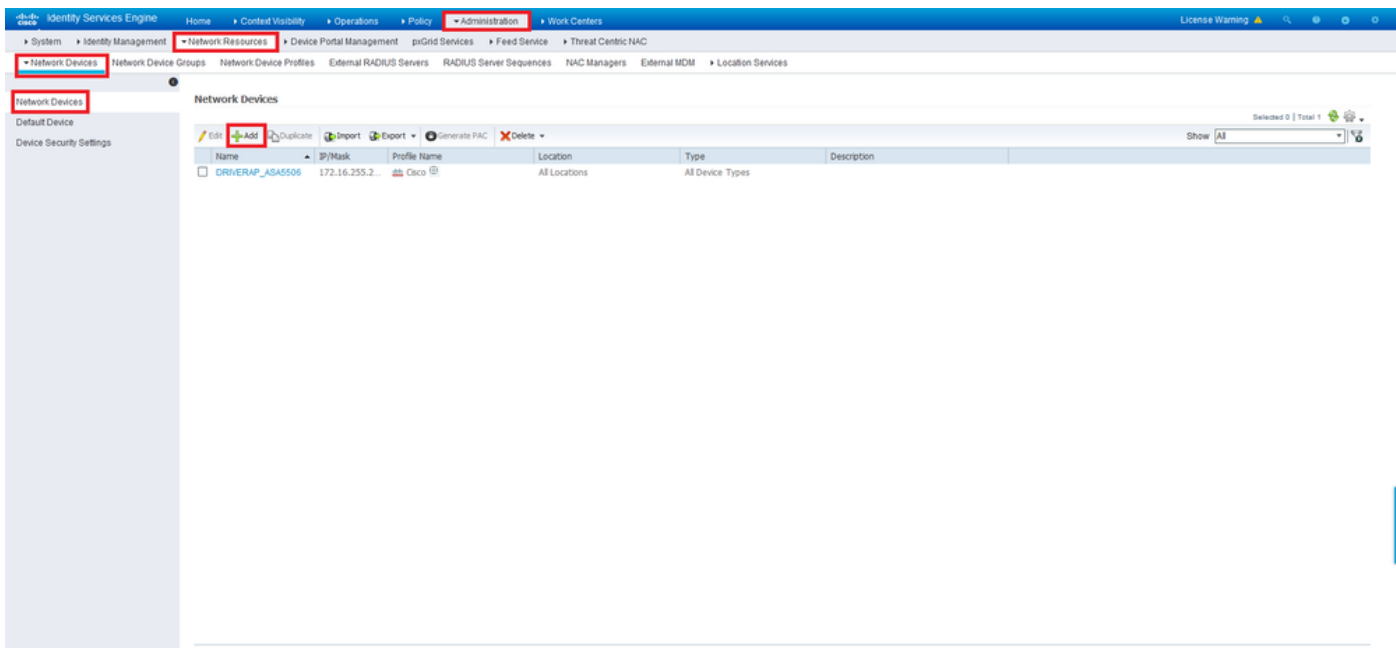
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

## ISE (RADIUS مداخل) لى لىوختلا جهن نيوكت

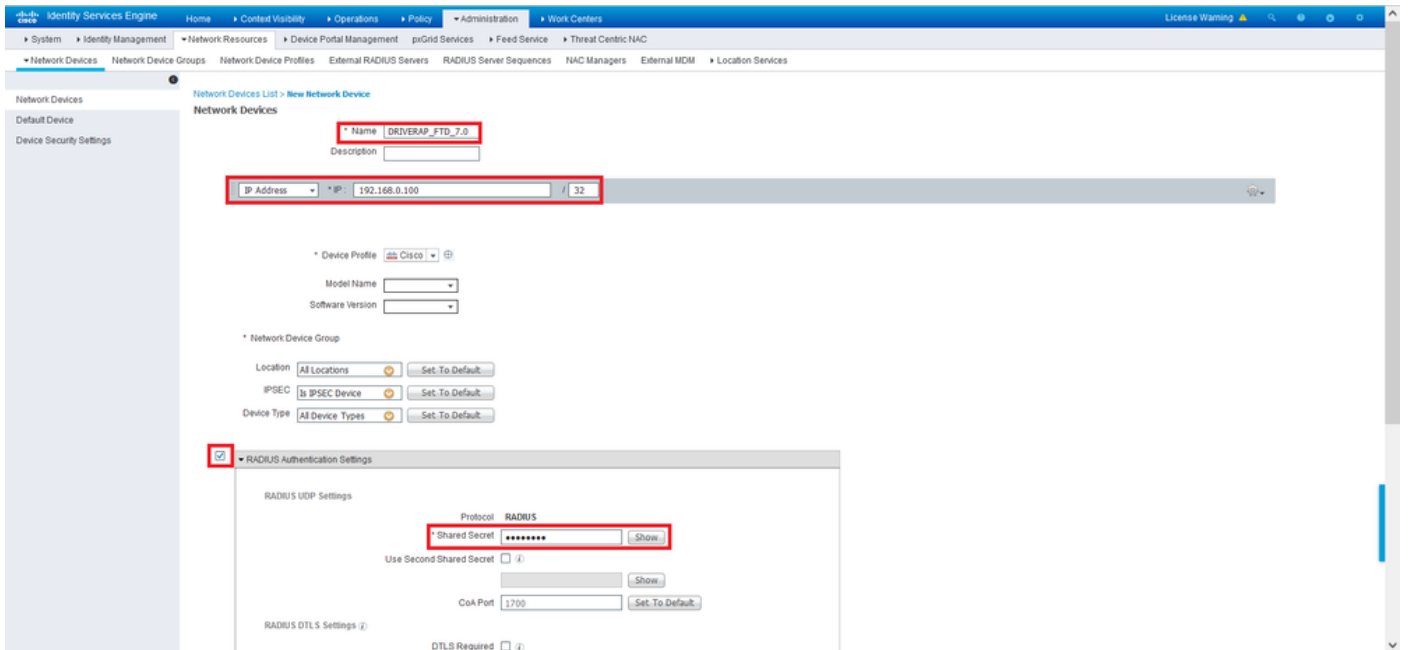
ةكبشلا ةزهجأ > ةكبشلا دراوم > ةرادا لى لى لىوختناو ISE مداخل لى لى لوخدلا لىس 1. ةوطخلا



تابلط ءءلاءم نم ISE نكم تي ءءء ءافاضا لىل ءقنا ،ءكبشلا ءزهءا مسق يف 2. ءوطلال ءم RADIUS لىل ءووللا

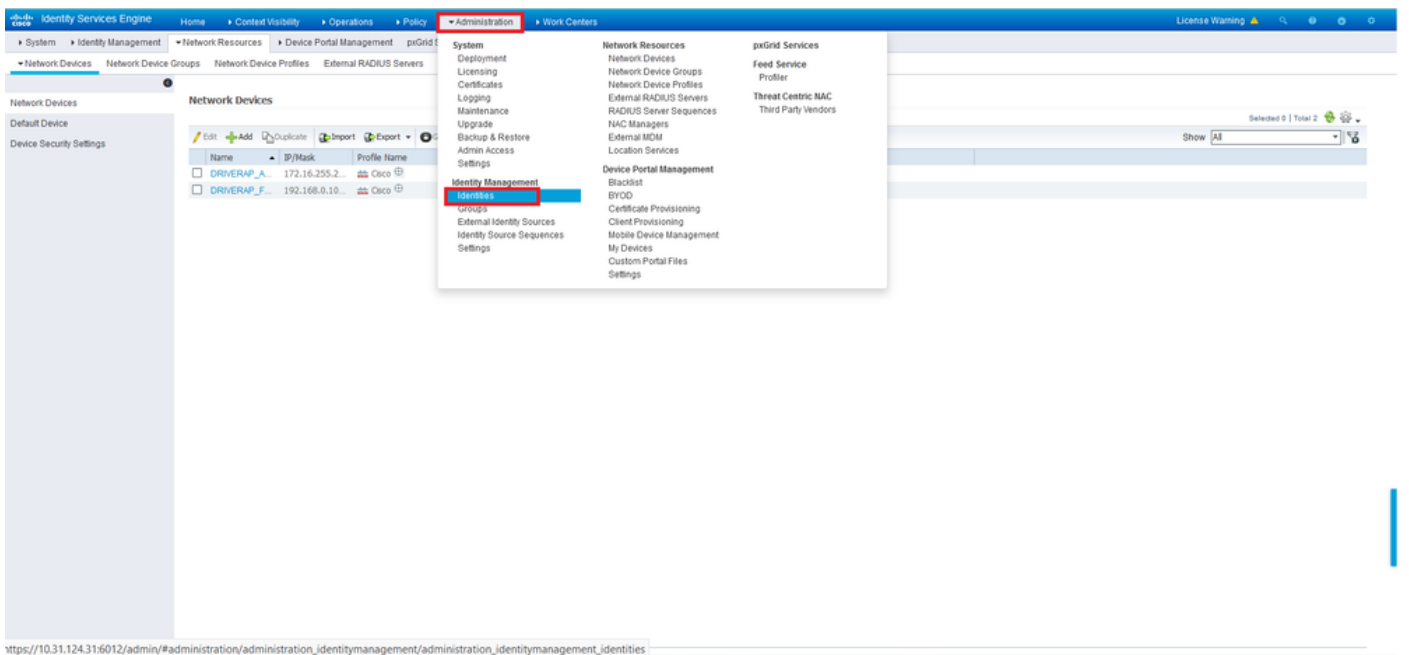


نوكي نأ بجي .RADIUS ءقءاصم ءاءاءءا ءبرم ءءء مء IP ناوئءو ءكبشلا زاھ مسال لىل ءءءا ءم FMC لىل RADIUS مءءا نءءا ءاشن ءءء ءمءءءءا ءمءل ءرءءءمءل

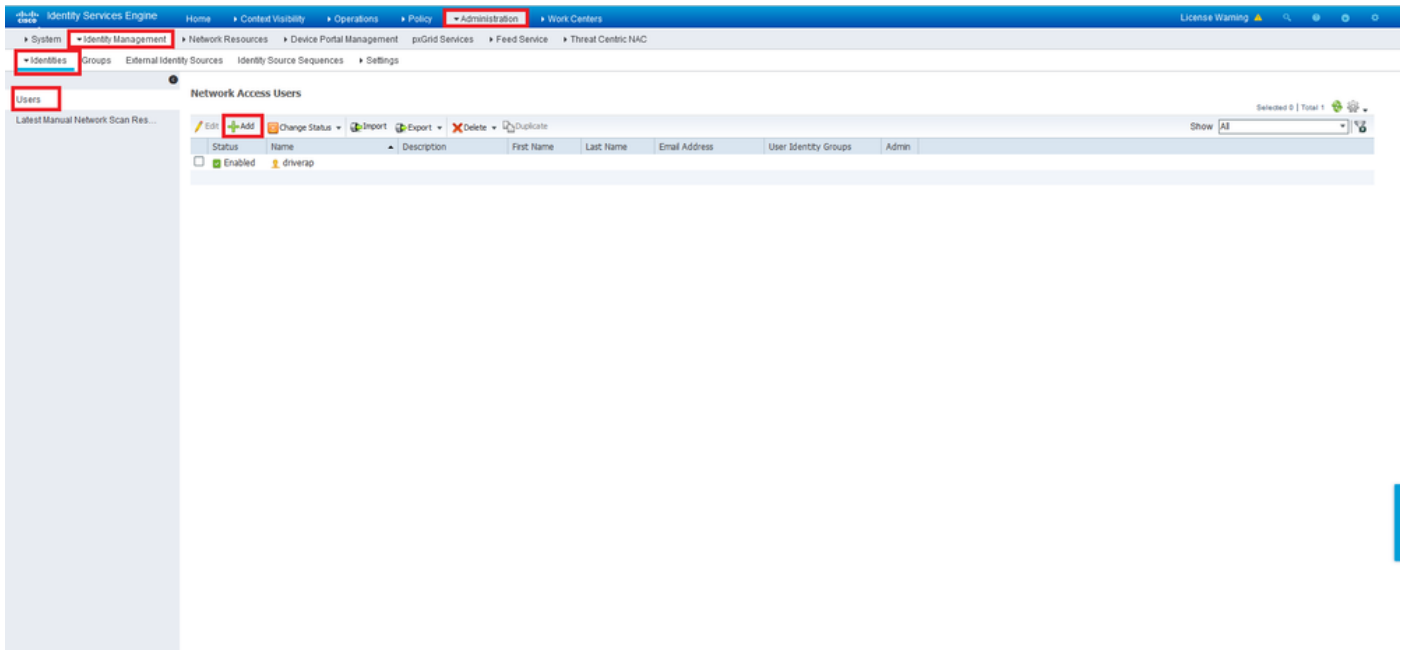


ةحفصل هذه ةياهن يف دوجوملا رزلاب هوظفاح.

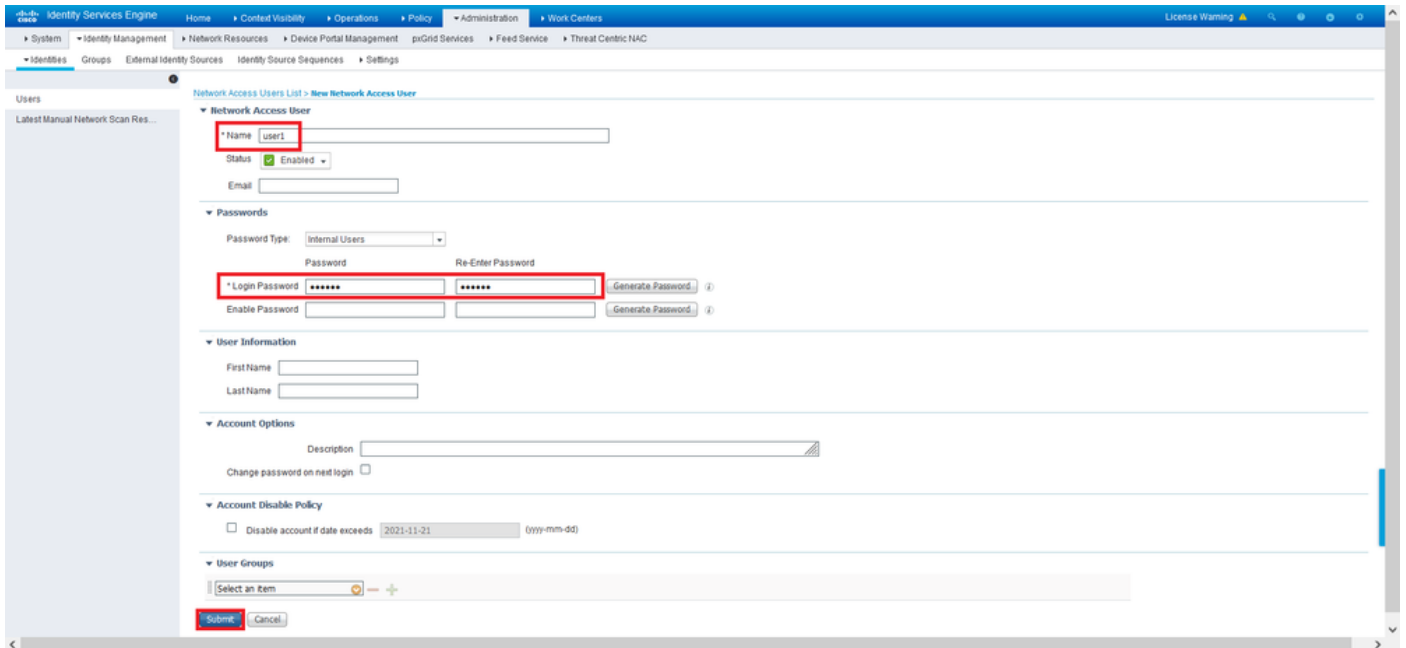
تايوهلا > ةيوهلا ةرادا > ةرادا ىلإ لقتنا. 3 ةوطخلال



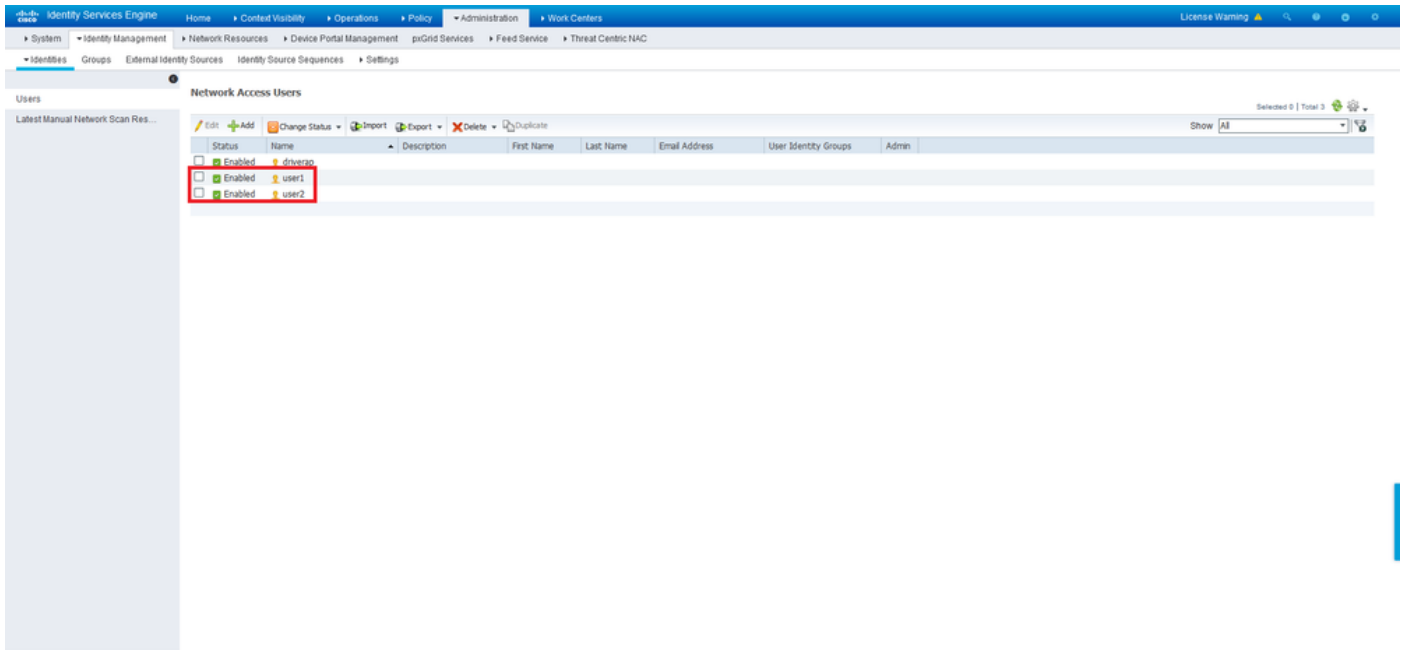
يف 1مدختسم عاشنإل ةفاضل قوف رقنا، Network Access يف مدختسم مسق يف 4. ةوطخلال ةيحلحمل ISE تانايب ةدعاق.



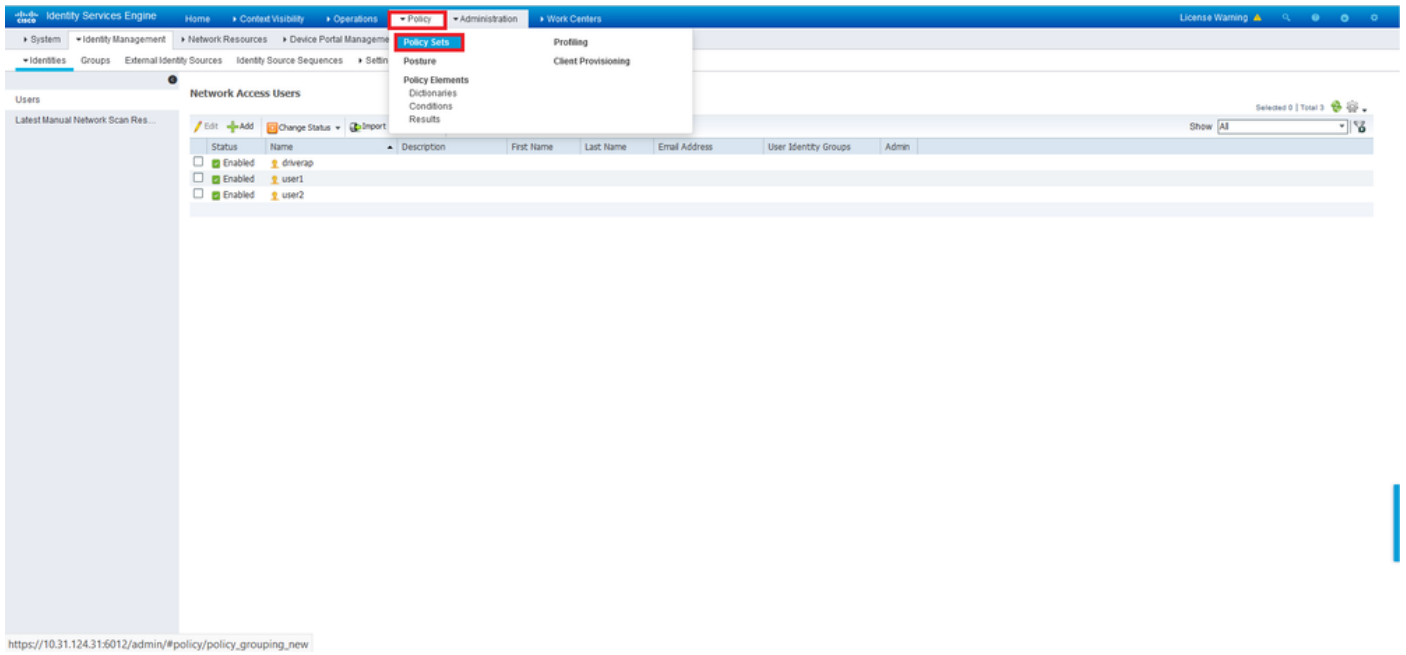
يلع رقنا مٲ ، لوخدلا ليجست رورم ةمك و مسالا يلقح يف رورملا ةمك و مدختس مل مسا لخدأ لاسلا.



2. مدختس م عاشنإل ةقباسلا تاوطخال ررك 5. ةوطخال.

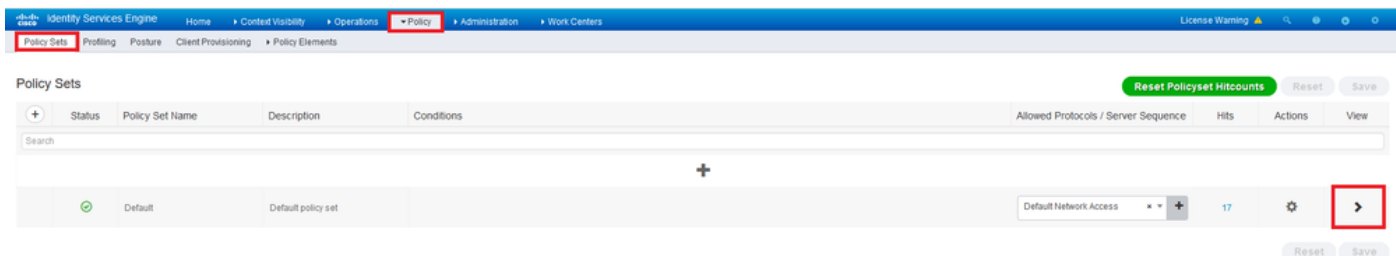


تاسايسال تاعومجم > ةسايسال ال لقتنا 6. ةوطخال

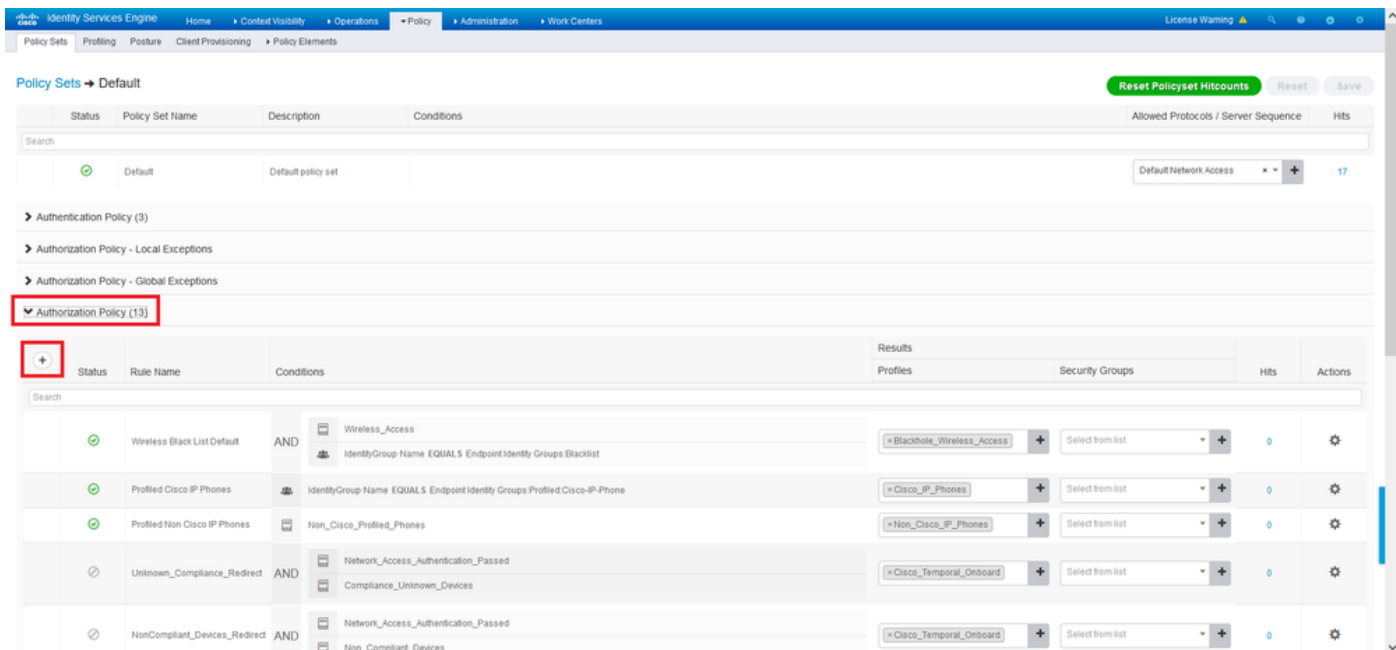


[https://10.31.124.31:6012/admin/#policy/policy\\_grouping\\_new](https://10.31.124.31:6012/admin/#policy/policy_grouping_new)

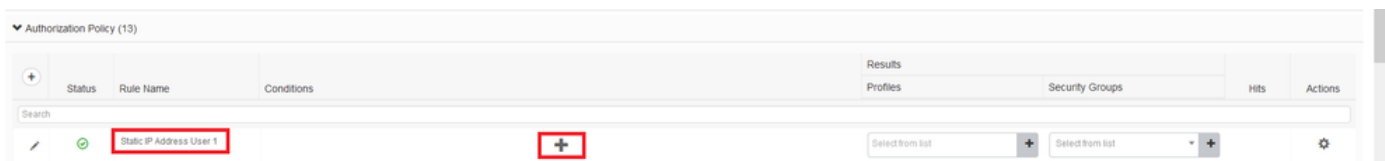
ةشاشال نم نميال بناجال يف > مهسال قوف رقنا 7. ةوطخال



ةفاضال زمرلا + قوف رقنا ،نآلا .هيدمتل ليوختلا جهن راوجب > مهسلا قوف رقنا .8 ةوطخلا ةديج ةدعاق



طورشلا دومع تحت زمرلا + ددحو ري طستلل مساري فوتب مق



يتح لفسأل ري رمتلاب مق .عوضوملا ةنوقيأ قوف رقناو تامسلا ررحم صن ع برم ي ف رقنا ك.لذ راتختو RADIUS مدختسم مسا ةمس دجت



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\_Passwd

Non\_Cisco\_Profiled\_Phones

Non\_Compliant\_Devices

Switch\_Local\_Web\_Authentication

Switch\_Web\_Authentication

Editor

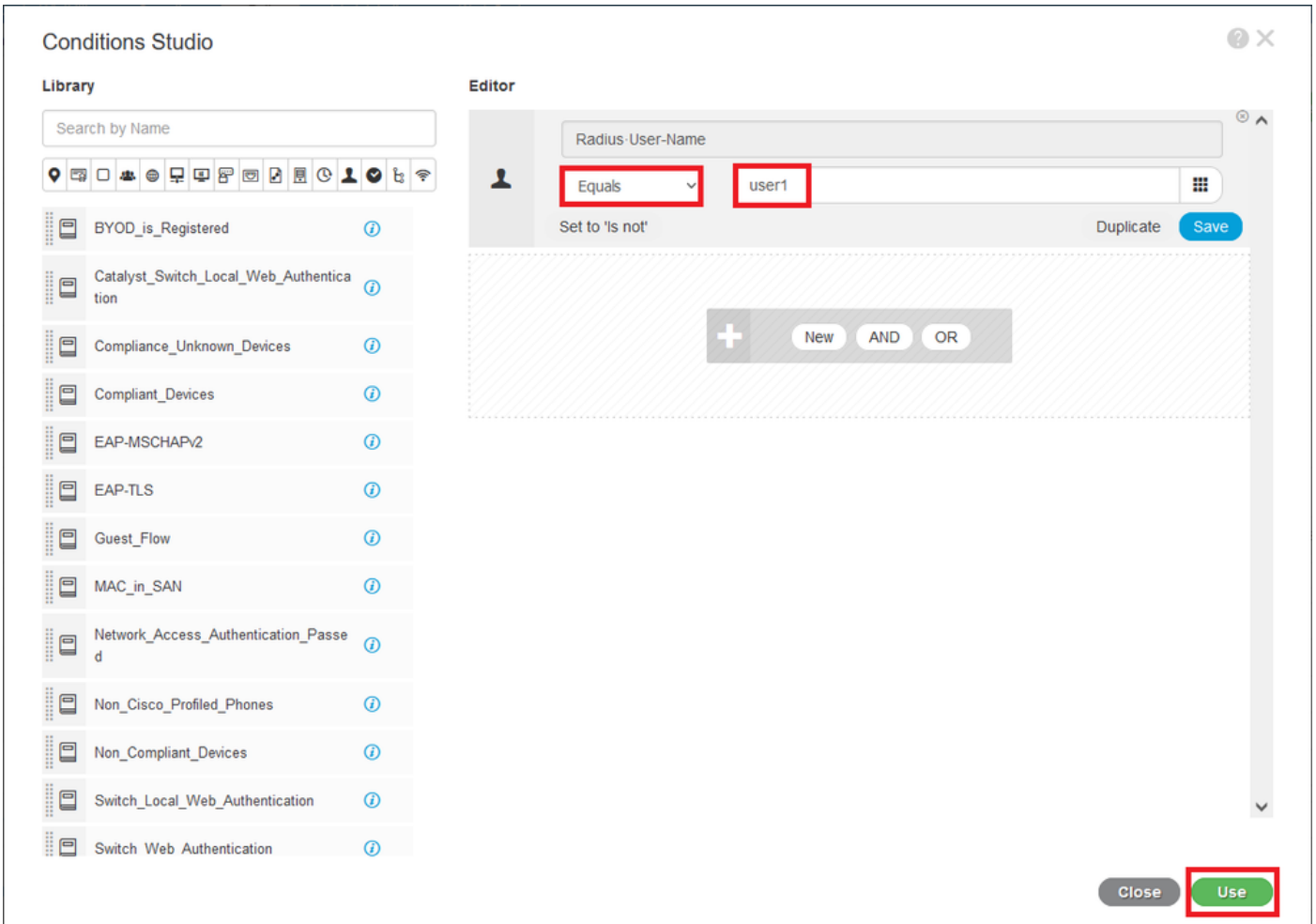
Click to add an attribute

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	

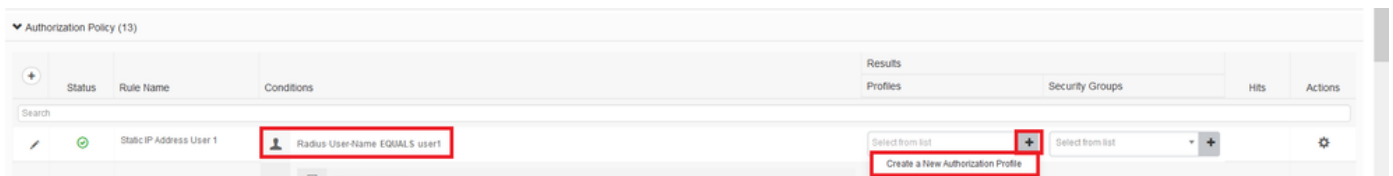
Close Use

مادختسا قوف رقنا .هل رواجملا صنلا عبرم في user1 لخدأو لغشمك يواس تلاب ظف تحا ةمسلال ظف حل .

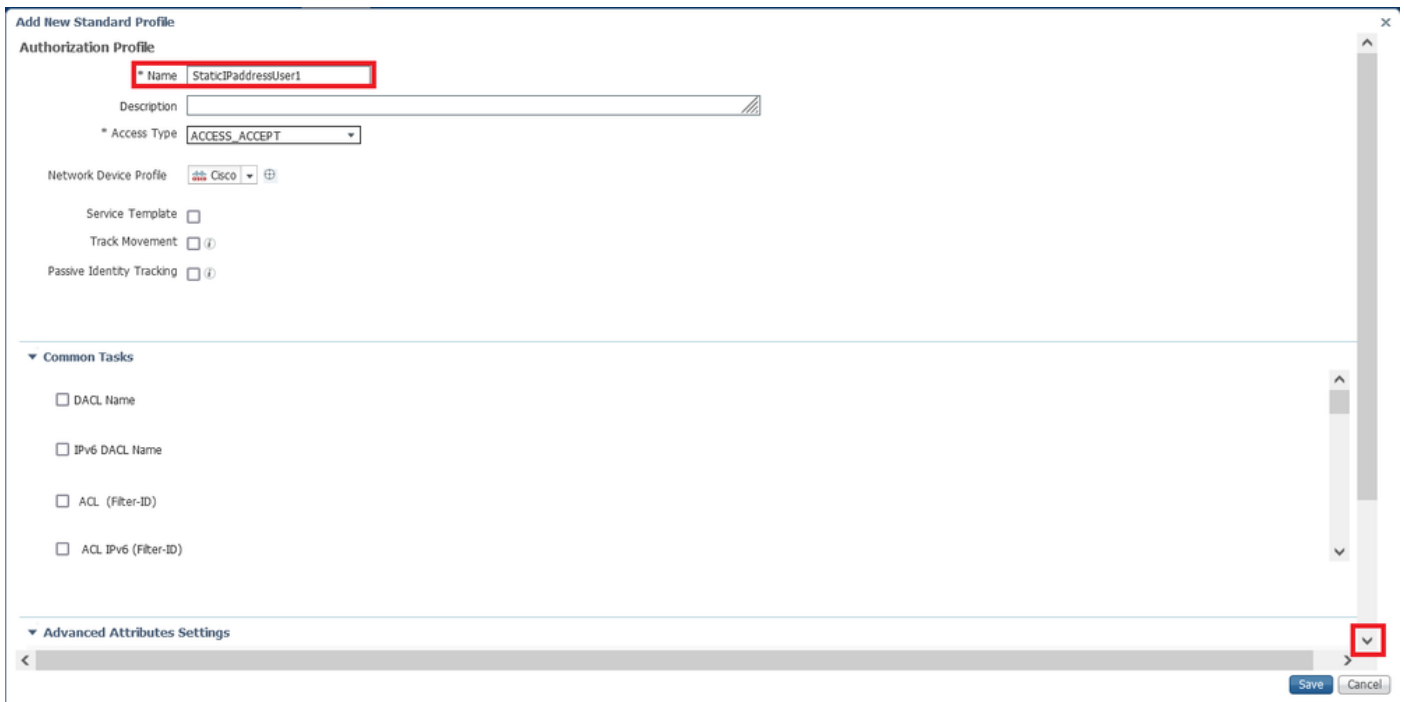


نآلآ ةدعاقلا هذهل طارشلا نبيعت مت

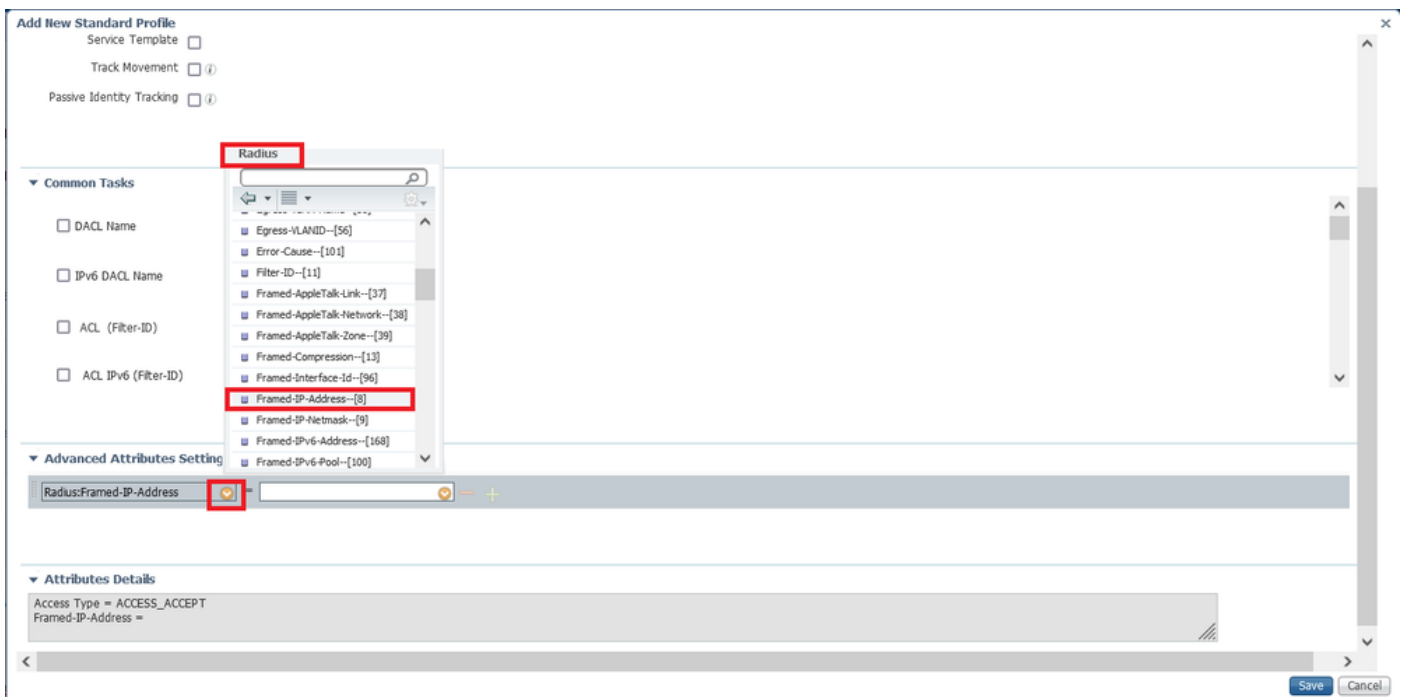
ليوخت في صوت عاشن | رتخاو + زمرلا يلع رقنا ، تافيصوتلا/جئاتنلا دوماع في 9 ةوطخال ديديج.



ىلآ لفسأل رييرمتلاب مق . Access عونك ACCESS\_ACCEPT ىلع طفاحتو امسا هئاطع اب مق ةمدقتمل صئاصخال تاداع | مسق .



راديوس > Framed-IP-Address—[8].



ظافح قوف رقناو مدختس مالا اذهل تباث لكش ب هني عت دي رت يذلا IP ناو نع بتكنا

**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

اثيردح هؤاشنإ مت يذلا ليوختلا فيرعت فلم نآلا رتخأ 10. ةوطخل

**Authorization Policy (13)**

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+	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	DenyAccess	Select from list	0	
+	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco IP-Phone	Non_Cisco_IP_Phones	Select from list	0	
+	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	StaticIPAddressUser1	Select from list	0	

ظفح ةقطقط .لمكلااب نآلا ليوختلا ةدعاق نييعت مت

Identity Services Engine

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 (3)**

**Authorization Policy - Local Exceptions**

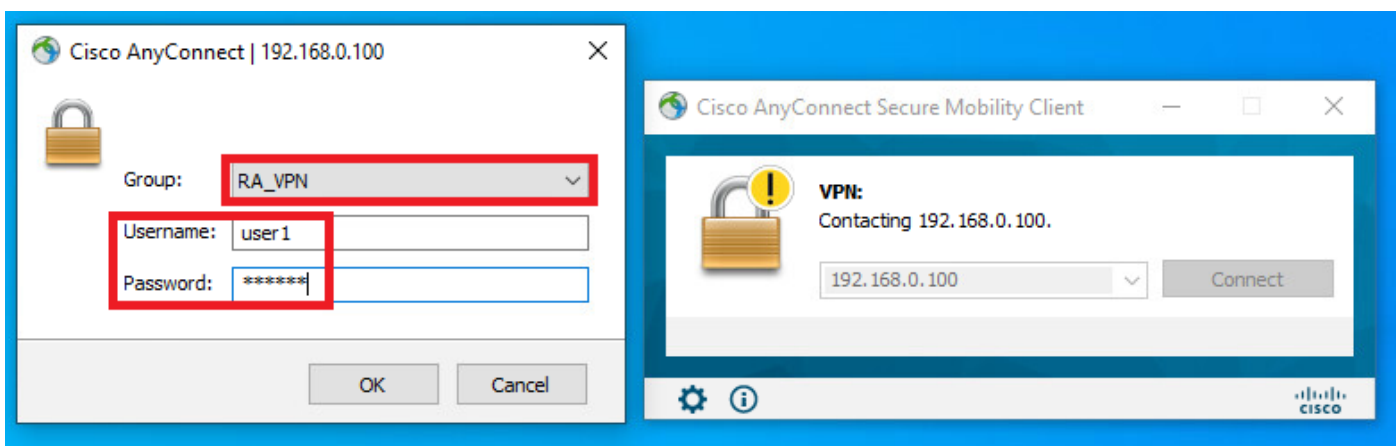
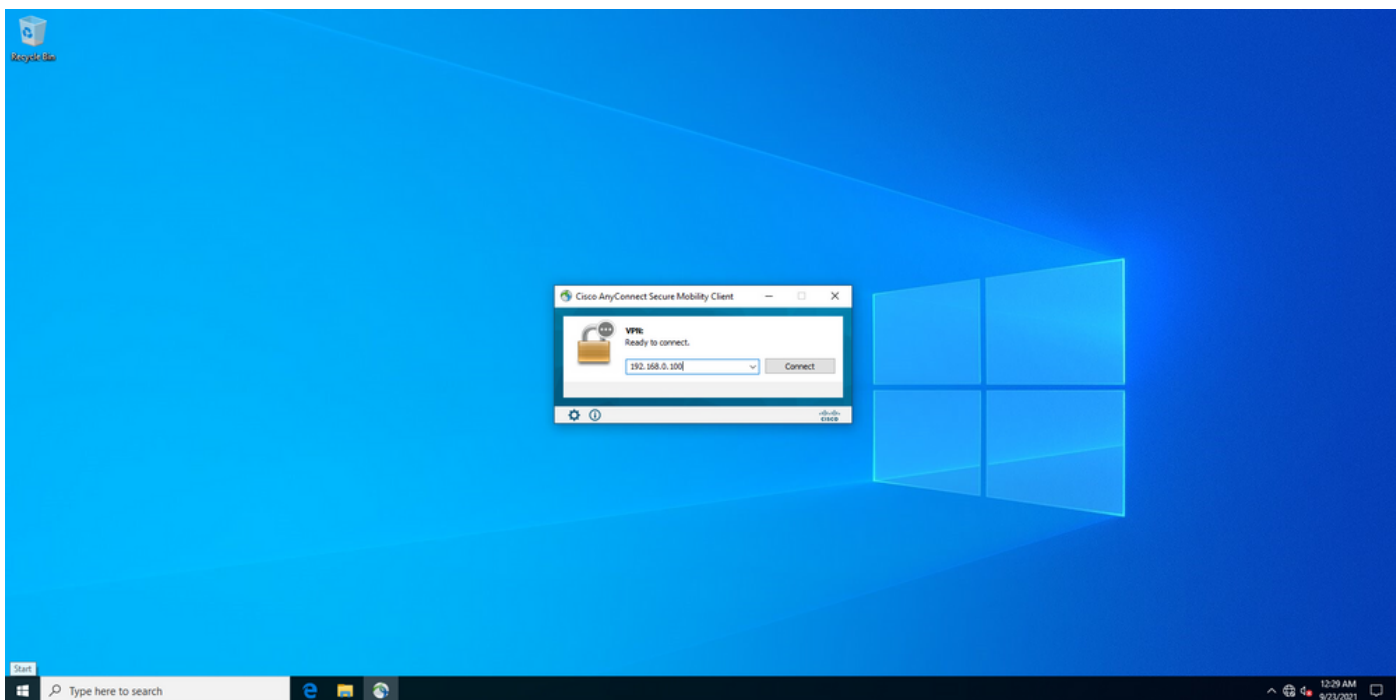
**Authorization Policy - Global Exceptions**

**Authorization Policy (13)**

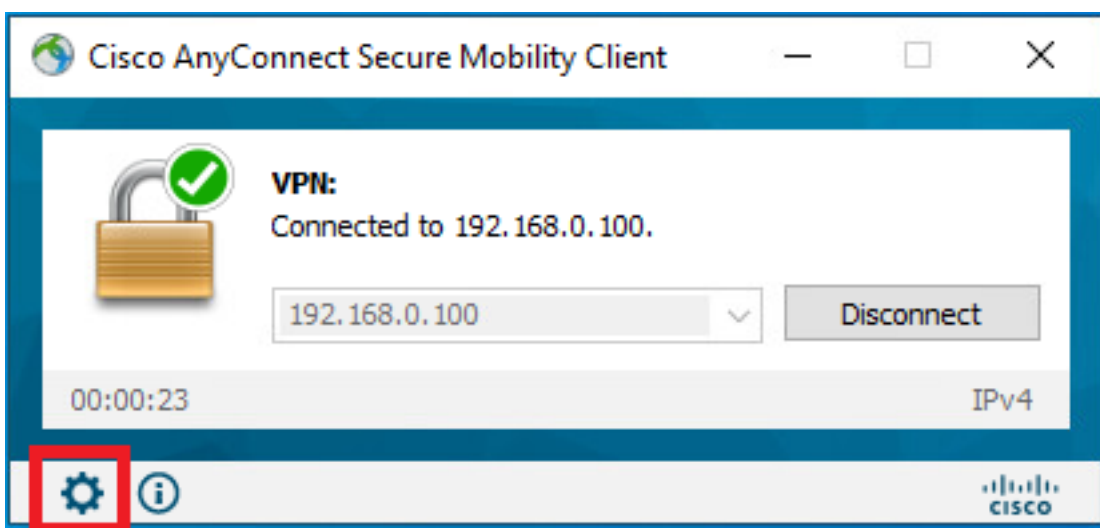
Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+	Static IP Address User 1	Radius-User-Name EQUALS user1	StaticIPAddressUser1	Select from list		

## ةحصللا نم ققحتلا

1. ةوطخل Cisco AnyConnect Secure Mobility Client تيبثت مت شيح ليمعلا زاهج لىل لقتنا . Windows زاهج مادختسإ متي) FTD جم انربب ةصاخلا ثبالو لابقستسالا ةدحوب لاصتالاب مق 1.مدختسمل/ دامتعا تانايب لخدأو (انه



دکأت .تایئاصح الال ءحفص الال ءحفصتو (للفسلال یرسلال ءلوازلال) سورتلال ءنوقلأل رقلنا  
مئل ذللا ناوئللال لءفلابل وه هلئلئل مئل ذللا IP ناوئل نا ناوئللال تامولعم مسقل ف  
مءءلسملا اءهل ISE ضلوفل ءهن ف هللوكل



The screenshot shows the Cisco AnyConnect Secure Mobility Client interface. The title bar reads "Cisco AnyConnect Secure Mobility Client". The main window title is "AnyConnect Secure Mobility Client". Below the title bar, there is a "Virtual Private Network (VPN)" section with a "Diagnostics..." button. The interface has several tabs: "Preferences", "Statistics", "Route Details", "Firewall", and "Message History". The "Statistics" tab is selected, showing connection information and address information.

**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

At the bottom of the window, there are "Reset" and "Export Stats..." buttons.

FTD: debug radius all رمل ا جا رخ رهظي

```
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: تالچس رهظت**

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: ضرع ىلع رADIUS Live لجس



**Identity Services Engine**

### Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:00:50:50:40:0f (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	00:00:50:50:40:0f
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	0ba800540000d00014bctd0
Authentication Method	PAP_ASCM
Authentication Protocol	PAP_ASCM
Network Device	DRIVERAP_JTD_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
15050 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15040 Queried PIP - Normalized Radius Radius/lowType (4 times)
22072 Selected identity source sequence - All_User_ID_Store
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	140
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	00099005:3150-4210-a80a-6753440f050c
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

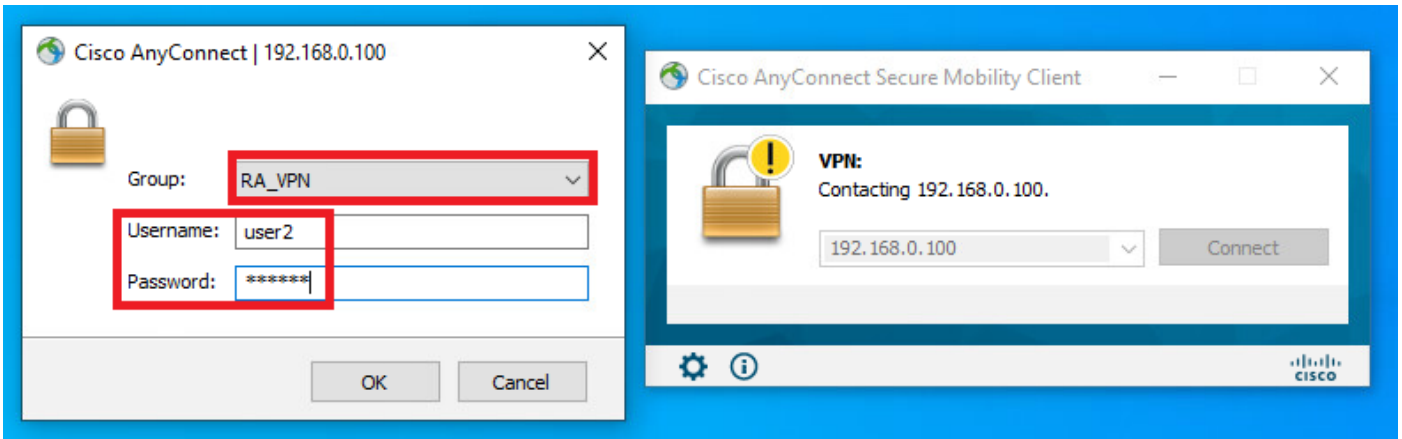
IPSEC	IPSECOnly IPSEC Device#0
EnabledFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM SessionID	0ba800540000d00014bctd0
Called-Station-ID	192.168.0.100
CiscoAVPair	mdm-dmdevice-platform=win, mdm-dmdevice-manufacturer=50:50:50:40:0f, mdm-dmdevice-platform-version=10.0.13522, mdm-dmdevice-publicname=00:00:50:50:40:0f, mdm-dmdevice-agent=AnyConnect Windows 4.10.02080, mdm-dmdevice-type=VMware, Inc VMware Virtual Platform, mdm-dmdevice-uid=glbactm158788E0CF62F3F2C0E241409F4BA2AE2C583, mdm-dmdevice-uid=3C38427071F90782F810F124021184A08598C717E370388CC030F8443C880344, audit-session-id=0ba800540000d00014bctd0, ip-source-ip=192.168.0.101, oca-push=true

### Result

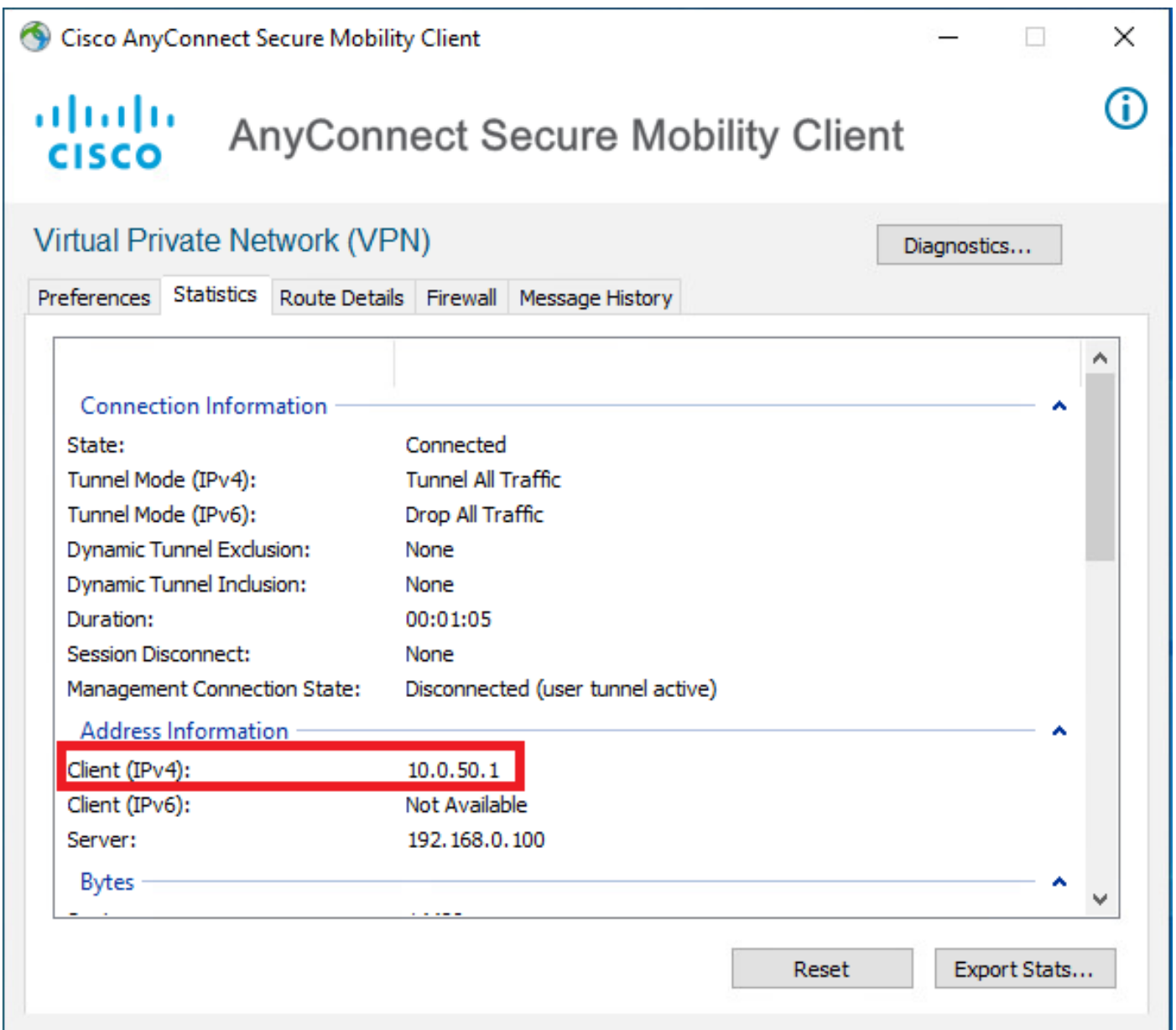
Framed IP Address	10.0.0.101
Class	CACS-0ba800540000d00014bctd0 driverap-ISE-2-71417494978/23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

زاهج مادختسا متي) FTD چمان رربب ةصاخلا ثبلاو لابقتسالا ةطحمب لاصتالاب مق 2. ةوطخلا User2 دامتعا تانايب لخدأو (انه Windows



في حالت IP ناووع لوالع فلاب وه هنيي عت مت يذال IP ناووع نا ناووعلا تامولعم مسق حضوي فم لال فم هنيوكت مت يذال IPv4 ليلحالم عمحتلال



FTD: `debug radius all` رمأل جارخ رهظي

```
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: تالچس رهظت

<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: عرض سجل RADIUS Live

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
CVPR3000ASAPRXTA-Tunnel-Group-Name	RA_VPN
OriginalUsername	user2
NetworkDeviceProfileId	b0099005-3150-4210-a80e-67534545b50c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPRXTA-Client-Type	2
Acq 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	IPSECv4v5 IPSEC Device#No
Name	Endpoint Identity Groups Profiled Workstation
EnableFlag	Enabled
RADIUS Username	user2
Device IP Address	192.168.0.100
CPM SessionID	da800540000d00014bc087
Called Station ID	192.168.0.100
CiscoAVPair	mdu-dm-device-platform:mdu-dm-device-platform-00-50-56-96-45-6f-01 mdu-dm-device-platform-reqip:10.0.18.362 mdu-dm-device-publicmap:00-50-56-96-45-6f-01 mdu-dm-user-agent:VLAN:Windows 4.10.22088 mdu-dm-device-type:VMware, Inc. VMware Virtual Platform mdu-dm-device-uid: globa:158f88e00f52f3f2c0e243459f48aa2ae208b3 mdu-dm-device- uid-3c38427071f8b782f816f124621184406596c717e370388cc030f 94402885244 audit session-ida800540000d00014bc087 ip source ip=192.168.0.101 os=pubintv4

### Result

Class	CACS-ida800540000d00014bc087-driverap-ISE-2-71417494978-24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

### Session Events

لك ىل ع IP نىوانع نىيىعتل ةفلتخلم ال IP نىوانع تاقاطن مادختس اىل ع بىي: ةظالم نىوانع تاضراعت بنجت ل ISE ضىيوقت تاساىسو FTD لوكوتوربل لىل حم ال IP عمجت نم مادختساب FTD نىيوقت مت ، اذه نىيوقتلا لاثم لىي ف AnyConnect. االمع نىي ب ةرركم ال IP نم تباثل ال IP ناونعل ISE م داخ نىيىعتو 10.0.50.100 لىل 10.0.50.1 نم لىل حم ال IPv4 عمجت 10.0.50.101.

## اهال صاوا عاطخا ل فاشكتسا

اهال صاوا نىيوقتلا عاطخا فاشكتسال اهمادختسا ل كنكم لىي تال تامولعمل مسقلا اذه رفوى

فى FTD:

- debug radius all

لىل ISE:

- ةرشابم ال RADIUS تال جس

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل