

Configure a Static IP Address on an AnyConnect Remote Access VPN with ISE and AD

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Background Information](#)
- [Configure](#)
- [AD Configuration](#)
- [ISE Configuration](#)
- [ASA Configuration](#)
- [Verify](#)
- [For Users without Static IP Addresses on AD](#)
- [Troubleshoot](#)

Introduction

This document describes how to configure a Static IP Address on Cisco AnyConnect Remote Access VPN with Identity Services Engine (ISE) and Active Directory (AD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco ISE Versions 3.0
- Configuration of Cisco Adaptive Security Appliance (ASA)/Firepower Threat Defense (FTD)
- VPN Authentication flow

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 3.0
- Cisco ASA
- Windows 2016
- Windows 10
- Cisco AnyConnect Client

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

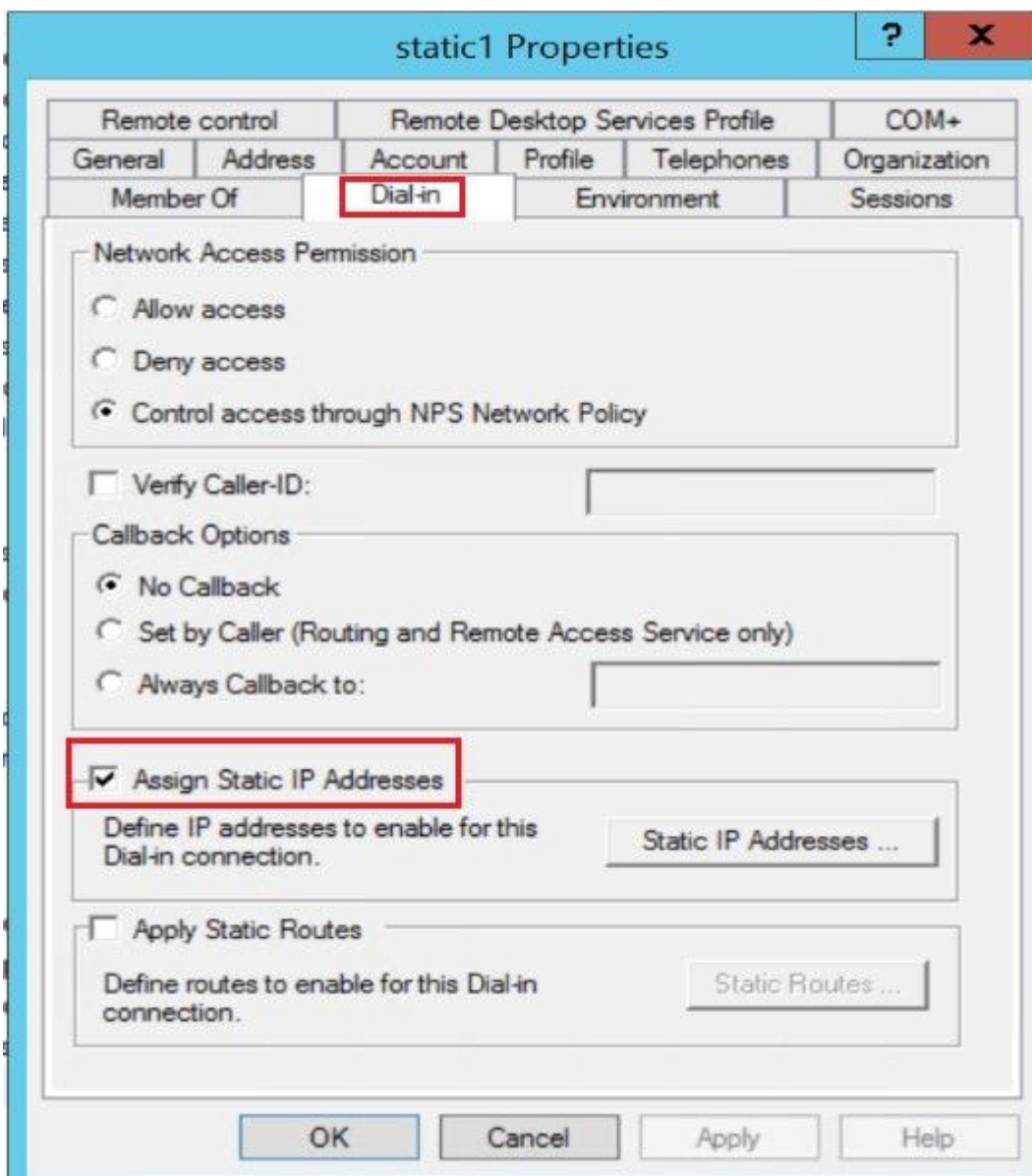
When users perform VPN authentication with a Cisco ASA with the AnyConnect VPN Client software, in some instances it is useful to assign the same static IP address to a client. Here, you can configure a static IP address per user account in AD and use this IP address whenever the user connects to the VPN. ISE can be configured with the attribute `msRADIUSFramedIPAddress` to query AD to fetch the IP address from AD and assign it to the client whenever they connect.

This document only describes how to configure a static IP address on a Cisco AnyConnect Remote Access VPN.

Configure

AD Configuration

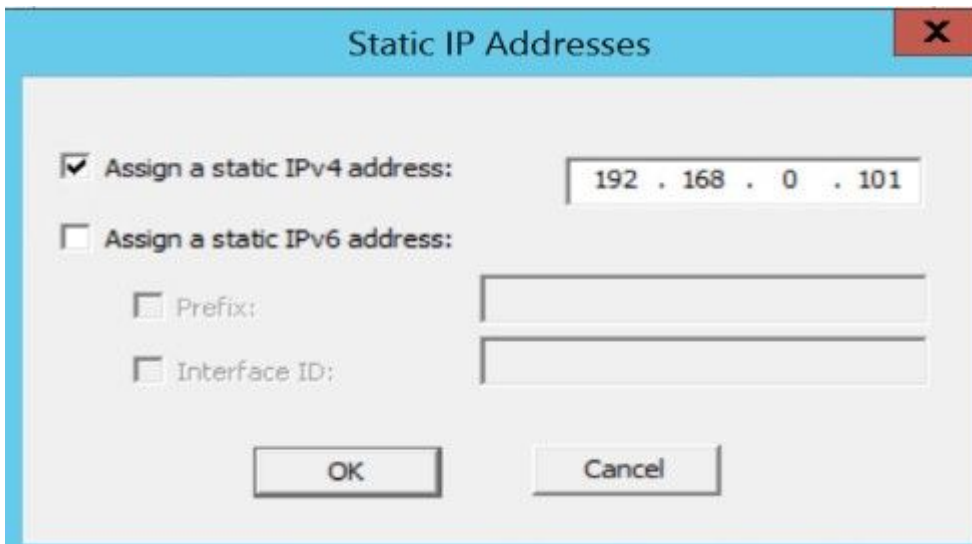
Step 1. Select a test account within AD. Modify the Properties of the test account; select the Dial-in tab as shown in the image.



Step 2. Tick the Assign Static IP Address box.

Step 3. Click the Static IP Addresses button.

Step 4. Tick the Assign a static IPv4 address box and enter an IP Address.



Static IP Addresses

Assign a static IPv4 address: 192 . 168 . 0 . 101

Assign a static IPv6 address:

Prefix:

Interface ID:

OK Cancel

Note: The assigned IP address must not be utilized or included in the DHCP pool.

Step 5. Click OK to complete the configuration.

ISE Configuration

Step 1. Add network Device on ISE and configure RADIUS and shared key. Navigate to ISE > Administration > Network Devices > Add Network Device.

Step 2. Integrate ISE with AD. Navigate to ISE > Administration > External Identity Sources > Active Directory > Join ISE to Domain .

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

External Identity Sources

Certificate Authentication F

Active Directory

AD

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

REST (ROPC)

Connection

Allowed Domains

PassiveID

Groups

Attributes

Advanced Sett

* Join Point Name AD ⓘ

* Active Directory Domain sumans.local ⓘ

+ Join + Leave Test User Diagnostic Tool Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller
<input type="checkbox"/>	ise30-1.sumans.local	PRIMARY	<input checked="" type="checkbox"/> Operational	WIN-VH9RF25V0LD.s
<input type="checkbox"/>	ise30-2.sumans.local	SECONDARY	<input checked="" type="checkbox"/> Operational	server-16.sumans.lo

Step 3. Add AD Attribute msRADIUSFramedIPAddress. Navigate to ISE > Administration > External Identity Sources > Active Directory and then select the Joint Point name created. Click on Edit. Then, click the Attributes tab. And, click Add > Select Attributes from Directory.

Enter the name of the test user present on AD to which the Static IP address is assigned and select Retrieve Attributes.

Ensure you tick the box msRADIUSFramedIPAddress and click OK .

Directory Attributes

Only attributes selected below will be available for use as policy conditions in policy rules.

* Sample User or Machine

Account

static1



Retrieve Attributes...

<input type="checkbox"/>	Name	Type	Example Value
<input type="checkbox"/>	displayName	STRING	static1
<input type="checkbox"/>	distinguishedName	STRING	CN=static1,CN=Users,DC=sumans,DC=local
<input type="checkbox"/>	givenName	STRING	static1
<input type="checkbox"/>	instanceType	STRING	4
<input type="checkbox"/>	lastLogon	STRING	132660621872151004
<input type="checkbox"/>	lastLogonTimestamp	STRING	132678496044504702
<input type="checkbox"/>	logonCount	STRING	10
<input checked="" type="checkbox"/>	msRADIUSFramedIPAddress	STRING	-1062731675
<input type="checkbox"/>	msRASSavedFramedIPAddress	STRING	-1062731675
<input type="checkbox"/>	name	STRING	static1
<input type="checkbox"/>	objectCategory	STRING	CN=Person,CN=Schema,CN=Configuration,D
<input type="checkbox"/>	objectClass	STRING	top

Cancel

Edit the attribute msRADIUSFramedIPAddress and change the Type value from STRING to IP and click Save.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- > Certificate Authentication F
- ▼ Active Directory
 - AD
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - > SAML Id Providers
 - Social Login
 - REST (ROPC)

Connection Allowed Domains PassiveID Groups **Attributes** Ad

[Edit](#) [+ Add](#) [Delete Attribute](#)

<input type="checkbox"/>	Name	Type	Default
<input type="checkbox"/>	msRADIUSFramedIPAddress	IP	

INT

STRING

IP

OCTET_STRING

BOOLEAN

Step 4. Create an Authorization Profile. Navigate to ISE > Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.

In the Advanced Attributes Settings, add a new value for Radius: Framed-IP-Address and equals the msRADIUSFramedIPAddress value previously selected under AD Attributes (in Step 3.).

Navigation tabs: Dictionaries, Conditions, **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
 - Authorization Profiles
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

- Agentless Posture ⓘ
- Passive Identity Tracking ⓘ
- > Common Tasks
- ▾ **Advanced Attributes Settings**
 - ⋮ Radius:Framed-IP-Address ▾ = AD:msRADIUS
- ▾ **Attributes Details**
 - Access Type = ACCESS_ACCEPT**
 - DAACL = VPN_DACI
 - Framed-IP-Address = AD:msRADIUSFramedIPAddress**

Step 5. Create Policy Set. Navigate to ISE > Policy > Policy Sets. Create a Policy Set and Save. Create an Authentication Policy and select the identity source as Active Directory (joined in Step 2.). Create an Authorization Policy and select the result with the Authorization Profile created (created in Step 4.).

Status	Policy Set Name	Description	Conditions
✔	VPN Policy Set		Radius-NAS-IP-Address EQUALS 10.127.197.229

Authentication Policy (2)

Status	Rule Name	Conditions	Us
✔	Authentication Rule	Radius-NAS-Port-Type EQUALS Virtual	>
✔	Default		>

Authorization Policy (2)

Status	Rule Name	Conditions	Results	Profiles
✔	Authorization Rule	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS TG-2	VPN_Profile.x	+
✔	Default		DenyAccess.x	+

ASA Configuration

Enable WebVPN on the OUTSIDE interface and enable AnyConnect image.

```
webvpn
```

```
enable OUTSIDE
```

```
anyconnect image disk0:/anyconnect-win-4.10.00093-webdeploy-k9.pkg 1
```

```
anyconnect enable
```

```
tunnel-group-list enable
```

Define AAA Server Group and Server:


```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.127.197.230
key *****
authentication-port 1812
accounting-port 1813
radius-common-pw *****
authorize-only
interim-accounting-update periodic 24
dynamic-authorization
```

VPN Pool:

```
ip local pool VPN_POOL 192.168.1.1-192.168.1.50 mask 255.255.255.0
```

Group Policy:

```
group-policy GP-1 internal
group-policy GP-1 attributes
  dns-server value 10.127.197.254
  vpn-tunnel-protocol ssl-client
  address-pools value VPN_POOL
```

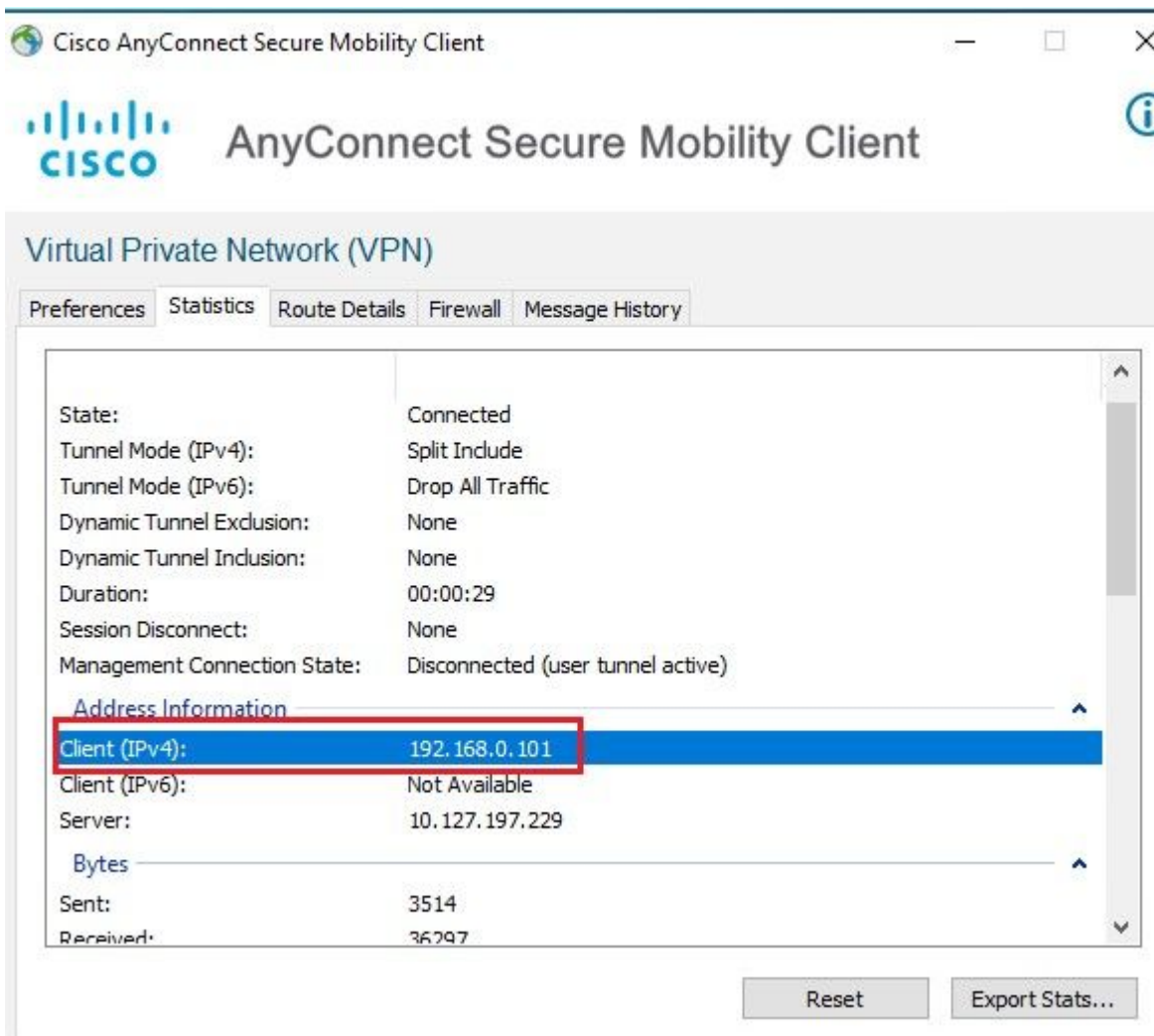
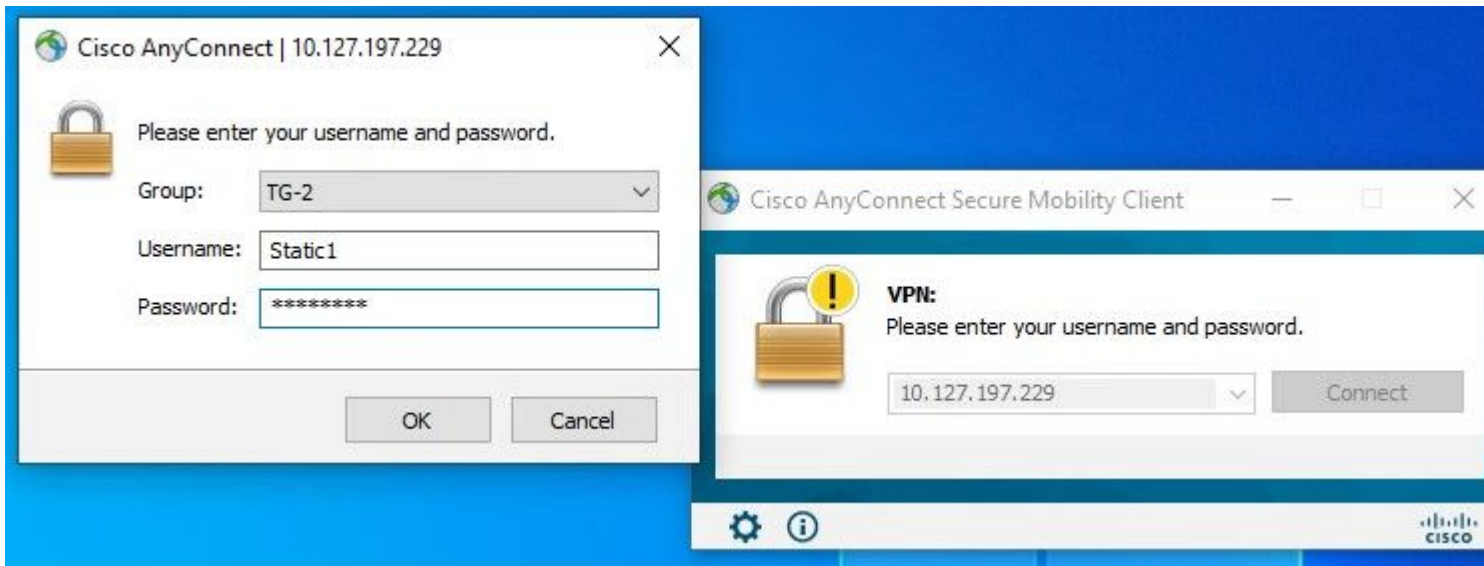
Tunnel Group:

```
tunnel-group TG-2 type remote-access
tunnel-group TG-2 general-attributes
  authentication-server-group ISE
  default-group-policy GP-1
tunnel-group TG-2 webvpn-attributes
  group-alias TG-2 enable
```

Verify

Use this section in order to confirm that your configuration works properly.

If you have static IP assigned on AD:



ISE Live logs:

Overview	
Event	5200 Authentication succeeded
Username	Static1
Endpoint Id	00:50:56:8B:2D:5D ⊕
Endpoint Profile	Windows10-Workstation
Authentication Policy	VPN Policy Set >> Authentication Rule
Authorization Policy	VPN Policy Set >> Authorization Rule
Authorization Result	VPN_Profile

Other Attributes: Here, you can see the attribute `msRADIUSFramedIPAddress` with an IP address assigned for this user on AD.

Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
msRADIUSFramedIPAddress	192.168.0.101
RADIUS Username	Static1
Device IP Address	10.127.197.229
CPMSessionID	0a7fc5e50002800060c4709e
Called-Station-ID	10.127.197.229
CiscoAVPair	mdm-tlv=device-platform=win, mdm-tlv=device-mac=00-50-56-8b-2d-5d, mdm-tlv=device-platform-version=10.0.19041 , mdm-tlv=device-public-mac=00-50-56-8b-2d-5d, mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.00093, mdm-tlv=device-type=VMware, Inc. VMware Virtual Platform, mdm-tlv=device-uid- global=C46D16F0DFA72C40FEB6F8D27FD299519B59EBC8, mdm-tlv=device- uid=769856F734054A9C3356302EE9EB8AD45262FCB86BC 53DF5852C702938DCE8FB, audit-session-id=0a7fc5e50002800060c4709e, ip:source-ip=10.106.32.72, coa-push=true

Results: IP Address sent from ISE to ASA.

Result

Framed-IP-Address	192.168.0.101
Class	CACS:0a7fc5e50002800060c4709e:ise30-1/407833752/82168
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-VPN_DACI-60c45eda
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Essential license consumed.

Output from ASA:

Command: show vpn-sessiondb anyconnect

```
Username       : Static1           Index           : 40
Assigned IP    : 192.168.0.101       Public IP       : 10.106.32
Protocol       : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-
unnel: (1)AES-GCM-256
Hashing        : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA3
: (1)SHA384
Bytes Tx       : 15860             Bytes Rx        : 3979
Group Policy   : GP-1             Tunnel Group    : TG-2
Login Time     : 08:30:22 UTC Sat Jun 12 2021
Duration       : 0h:13m:18s
Inactivity     : 0h:00m:00s
VLAN Mapping   : N/A             VLAN            : none
Audt Sess ID   : 0a7fc5e50002800060c4709e
Security Grp   : none
```

For Users without Static IP Addresses on AD

If the users do not have an IP address assigned on AD, they are assigned with the IP address assigned from local VPN_Pool or DHCP (if configured). Here, the local pool defined on ASA is used.

Cisco AnyConnect | 10.127.197.229

Please enter your username and password.

Group: TG-2

Username: userA

Password: *****

OK Cancel

Cisco AnyConnect Secure Mobility Client

VPN: Please enter your username and password.

10.127.197.229

Connect

Cisco AnyConnect Secure Mobility Client

AnyConnect Secure Mobility Client

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:55
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)
Address Information	
Client (IPv4):	192.168.1.2
Client (IPv6):	Not Available
Server:	10.127.197.229
Bytes	
Sent:	5225
Received:	36295
Frames	

Reset Export Stats...

ISE Live logs:

Overview

Event	5200 Authentication succeeded
Username	userA
Endpoint Id	00:50:56:8B:2D:5D ⊕
Endpoint Profile	Windows10-Workstation
Authentication Policy	VPN Policy Set >> Authentication Rule
Authorization Policy	VPN Policy Set >> Authorization Rule
Authorization Result	VPN_Profile

IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	userA
Device IP Address	10.127.197.229
CPMSessionID	0a7fc5e50002900060c4759f
Called-Station-ID	10.127.197.229
CiscoAVPair	mdm-tlv=device-platform=win, mdm-tlv=device-mac=00-50-56-8b-2d-5d, mdm-tlv=device-platform-version=10.0.19041 , mdm-tlv=device-public-mac=00-50-56-8b-2d-5d, mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.00093, mdm-tlv=device-type=VMware, Inc. VMware Virtual Platform, mdm-tlv=device-uid- global=C46D16F0DFA72C40FEB6F8D27FD299519B59EBC8, mdm-tlv=device- uid=769856F734054A9C3356302EE9EB8AD45262FCB86BC 53DF5852C702938DCE8FB, audit-session-id=0a7fc5e50002900060c4759f, ip:source-ip=10.106.32.72, coa-push=true

Result

Class	CACS:0a7fc5e50002900060c4759f:ise30-1/407833752/82292
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-VPN_DACI-60c45eda
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Essential license consumed.

Output from ASA:

Command: show vpn-sessiondb anyconnect

```
Username       : userA                Index           : 41
Assigned IP    : 192.168.1.2          Public IP       : 10.106.32.72
Protocol       : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing        : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx       : 15856                Bytes Rx        : 4856
Group Policy   : GP-1                 Tunnel Group    : TG-2
Login Time     : 08:51:43 UTC Sat Jun 12 2021
Duration       : 0h:00m:29s
Inactivity     : 0h:00m:00s
VLAN Mapping   : N/A                  VLAN            : none
Audt Sess ID   : 0a7fc5e50002900060c4759f
Security Grp   : none
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.