# Configure Split Exclude for AnyConnect FlexVPN Using ISE

## Contents



## Introduction

This document describes the procedure to configure split-exclude using ISE for IKEv2 AnyConnect connection to a Cisco IOS® XE router.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Experience with AnyConnect IPsec configuration on a router
- Cisco Identity Services Engine (ISE) configuration
- Cisco Secure Client (CSC)
- RADIUS protocol

### Components Used

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

- Cisco Catalyst 8000V (C8000V) - 17.12.04
- Cisco Secure Client - 5.0.02075
- Cisco ISE - 3.2.0
- Windows 10

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.

# Configure

## Network Diagram


*Network Diagram*

## Configurations

In order to complete the configuration, take into consideration these sections.

### Router Configuration

1. Configure a RADIUS server for authentication and local authorization on the device:

```
radius server ISE
 address ipv4 10.127.197.105 auth-port 1812 acct-port 1813
 timeout 120
 key cisco123

aaa new-model
aaa group server radius FlexVPN_auth_server
 server name ISE

aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network a-eap-author-grp local
```

2. Configure a trustpoint to install the router certificate. Since the local authentication of the router is type RSA, the device requires that the server authenticates itself using a certificate. You can refer to Certificate Enrollment for a PKI -1 and Certificate Enrollment for a PKI -2 for more details on the certificate creation:

```
crypto pki trustpoint flex
 enrollment terminal
 ip-address none
 subject-name CN=flexserver.cisco.com
 revocation-check none
 rsakeypair flex1
 hash sha256
```

3. Define an IP local pool to assign addresses to AnyConnect VPN clients upon successful AnyConnect connection:

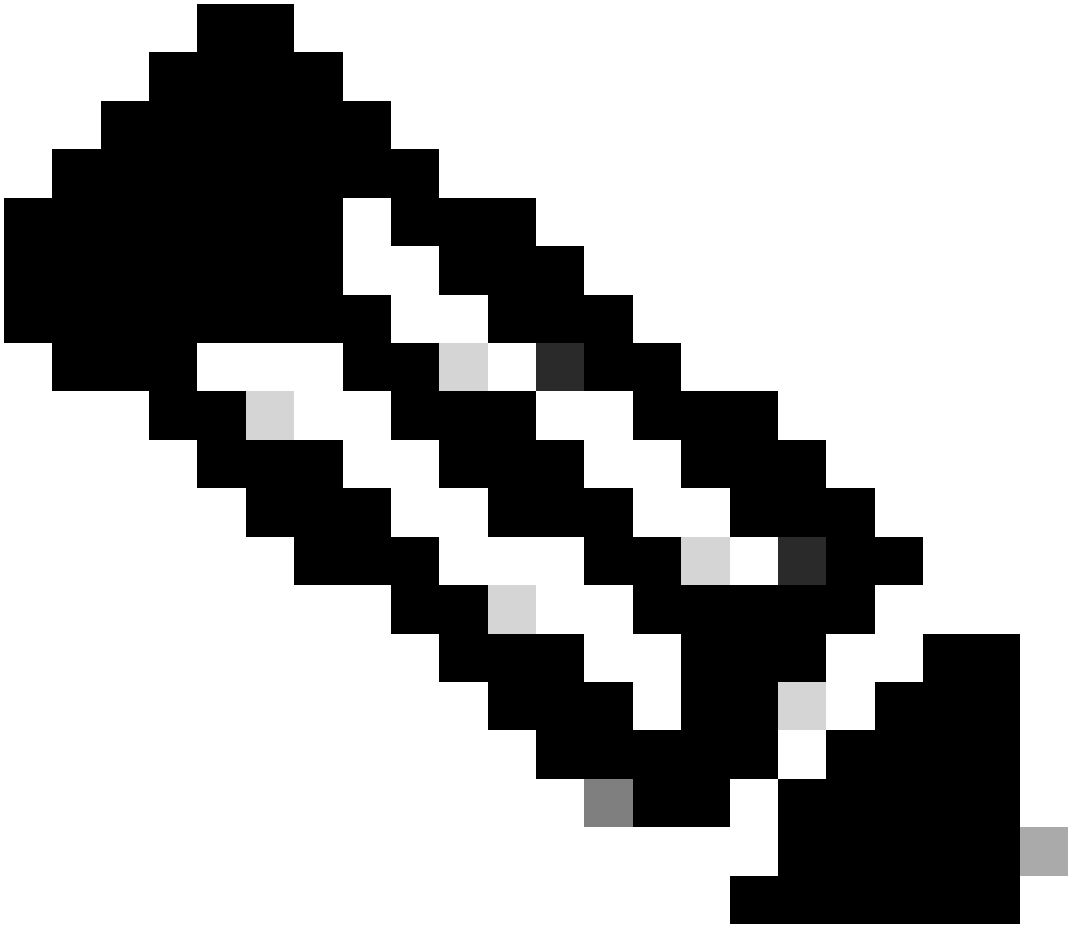
```
ip local pool ACPOOL 172.16.10.5 172.16.10.30
```

4. Create an IKEv2 local authorization policy:

The attributes defined in this policy along with the attributes pushed from Radius Server are applied to the users

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 dns 8.8.8.8
```

---



**Note**: If the custom IKEv2 authorization policy is not configured, the default authorization policy called **default** is used for authorization. The attributes specified under the IKEv2 authorization policy can also be pushed via the RADIUS server. You need to push the split-exclude attribute from the RADIUS server.

---

5 (Optional). Create an IKEv2 proposal and policy (if not configured, smart defaults are used):

```
crypto ikev2 proposal IKEv2-prop1
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop1
```

6 (Optional). Configure the transform-set (if not configured, smart defaults are used):

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
```

7. Configure a loopback interface with some dummy IP address. The Virtual-Access interfaces borrow the IP address from it:

```
interface Loopback100
 ip address 10.0.0.1 255.255.255.255
```

8. Configure a Virtual template from which the virtual-access interfaces are cloned:

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
```

9. Upload the AnyConnect client profile to the bootflash of the router and define the profile as given:

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

10. Configure an IKEv2 profile that contains all the connection-related information:

```
crypto ikev2 profile prof1
 match identity remote key-id *$AnyConnectClient$*
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint flex
 aaa authentication eap FlexVPN_auth
 aaa authorization group eap list a-eap-author-grp ikev2-auth-policy
```

```
 aaa authorization user eap cached
 virtual-template 100
 anyconnect profile acvpn
```

These are used in the IKEv2 profile:

- **match identity remote key-id *$AnyConnectClient$*** - Refers to the identity of the client. AnyConnect uses ***$AnyConnectClient$*** as its default IKE identity of type **key-id.** However, this identity can be manually changed in the AnyConnect profile to match deployment needs.
- **authentication remote** - Mentions that EAP protocol must be used for client authentication.
- **authentication local -** Mentions that certificates must be used for local authentication.
- **aaa authentication eap** - During EAP authentication, the RADIUS server **FlexVPN_auth** is used.
- **aaa authorization group eap list** - During the authorization, the network list **a-eap-author-grp** used with the authorization policy **ikev2-auth-policy.**
- **aaa authorization user eap cached-** Enables implicit user authorization.
- **virtual-template 100** - Defines which virtual template to clone.
- **anyconnect profile acvpn** - The client profile defined in Step 9. is applied here to this IKEv2 profile.

11. Configure the IPsec profile:

```
crypto ipsec profile AnyConnect-EAP
 set transform-set TS
 set ikev2-profile prof1
```

12. Add the IPsec profile to the virtual template:

```
interface Virtual-Template100 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

13. Disable the HTTP-URL based certificate lookup and HTTP server on the router:

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

14. Configure the SSL policy and specify the WAN IP of the router as the local address for downloading the profile:

```
crypto ssl policy ssl-server
 pki trustpoint flex sign
 ip address local 10.106.67.33 port 443

crypto ssl profile ssl_prof
 match policy ssl-server
```

Snippet of the AnyConnect Client Profile (XML Profile):

Prior to Cisco IOS XE 16.9.1, automatic profile downloads from the headend is not available. Post 16.9.1, it is possible to download the profile from the headend.

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>

<HostName>

Flex

</HostName>
<HostAddress>

flexserver.cisco.com

</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
```

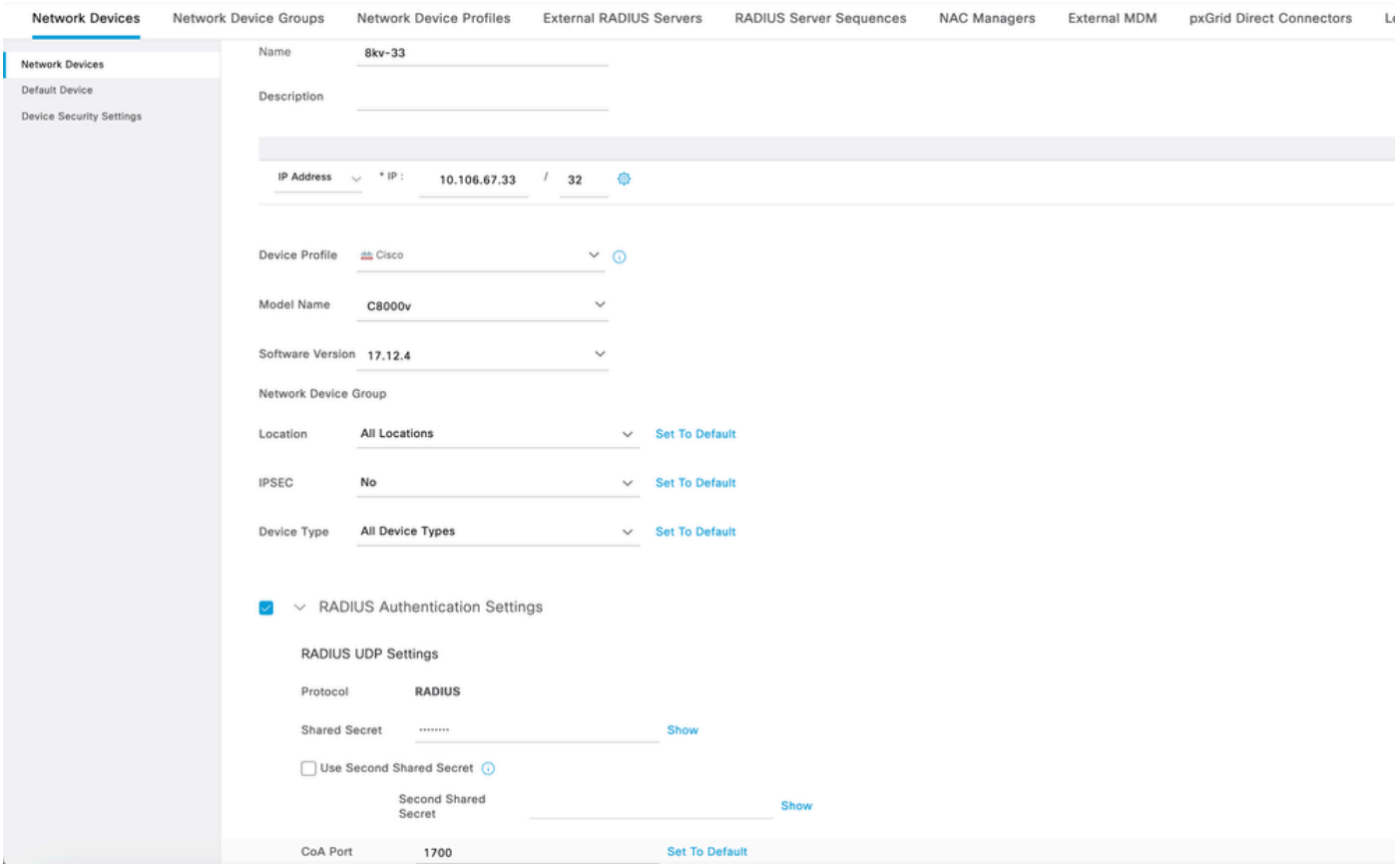
```
<AuthMethodDuringIKENegotiation>
```

**EAP-MD5**

```
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

## Identity Services Engine (ISE) Configuration

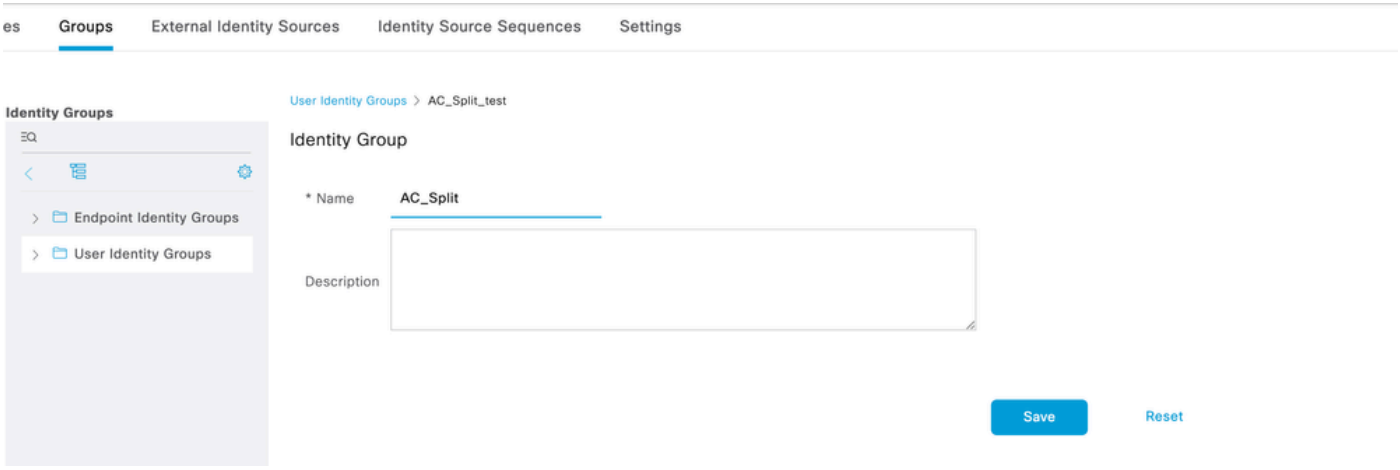
1. Register the router as a valid network device on ISE and configure the shared secret key for RADIUS. For this, navigate to **Administration > Network Resources > Network Devices**. Click **Add** to configure the router as a AAA client:




*Add Network Device*

2. Create identity groups:

Define identity groups to associate users with similar characteristics and who share similar permissions. These are used in the next steps. Navigate to **Administration > Identity Management > Groups > User Identity Groups**, then click **Add**:




*Create Identity Group*

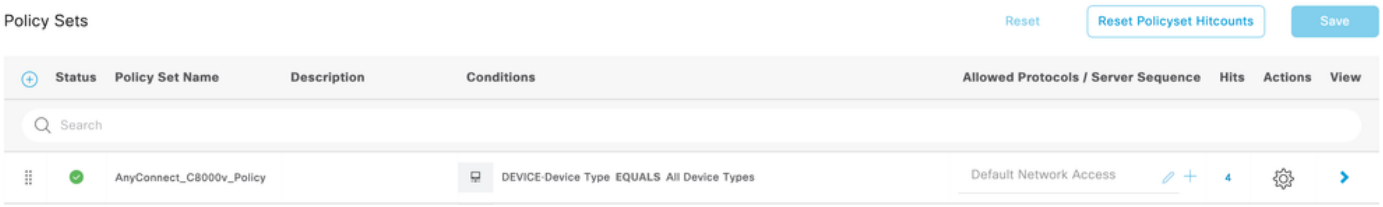
3. Associate users to identity groups:

Associate users to the right identity group. Navigate to **Administration > Identity Management > Identities > Users**.


*Add User to Identity Group*

4. Create Policy Set:

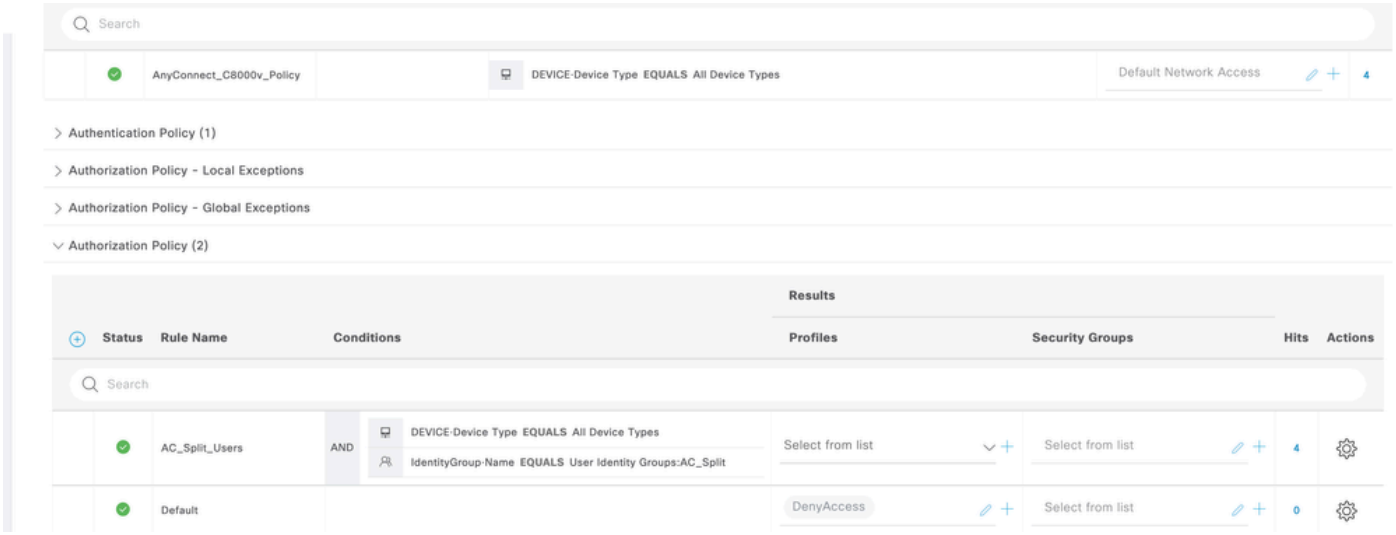
Define a new policy set and define the conditions that match the policy. In this example, all device types are allowed under the conditions. To do this, navigate to **Policy>Policy sets**:



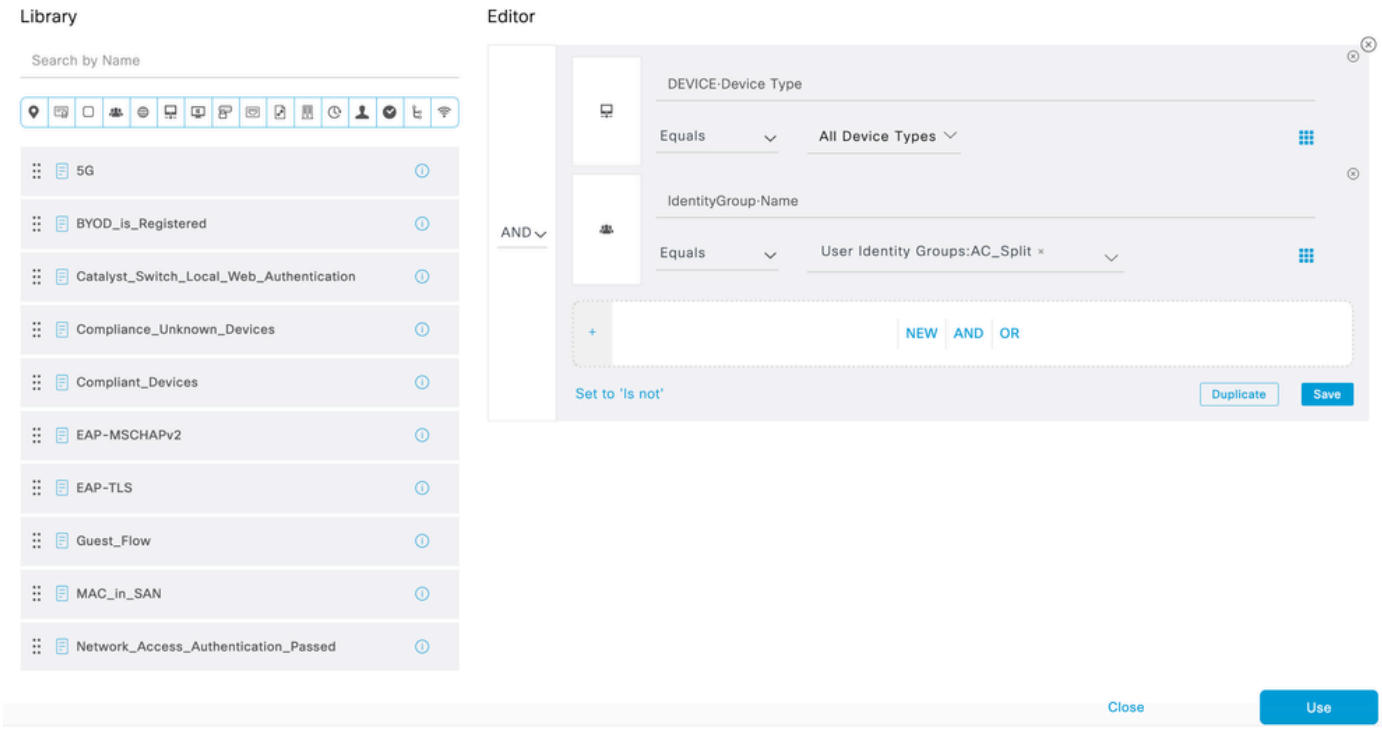

*Create Policy Set*

5. Create an Authorization Policy:

Define a new Authorization Policy with the required conditions to match the policy. Ensure to include the identity groups created in step 2 as a condition.




*Create Authorization Policy*

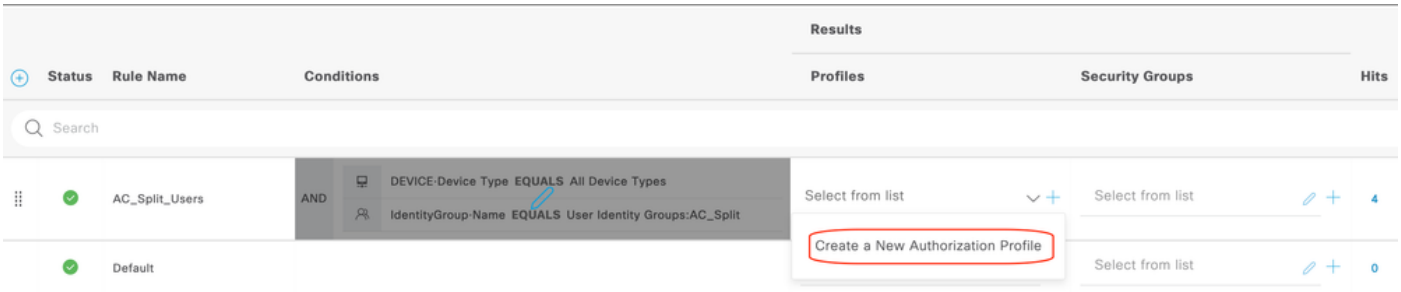



*Choose Conditions in Authorization Policy*

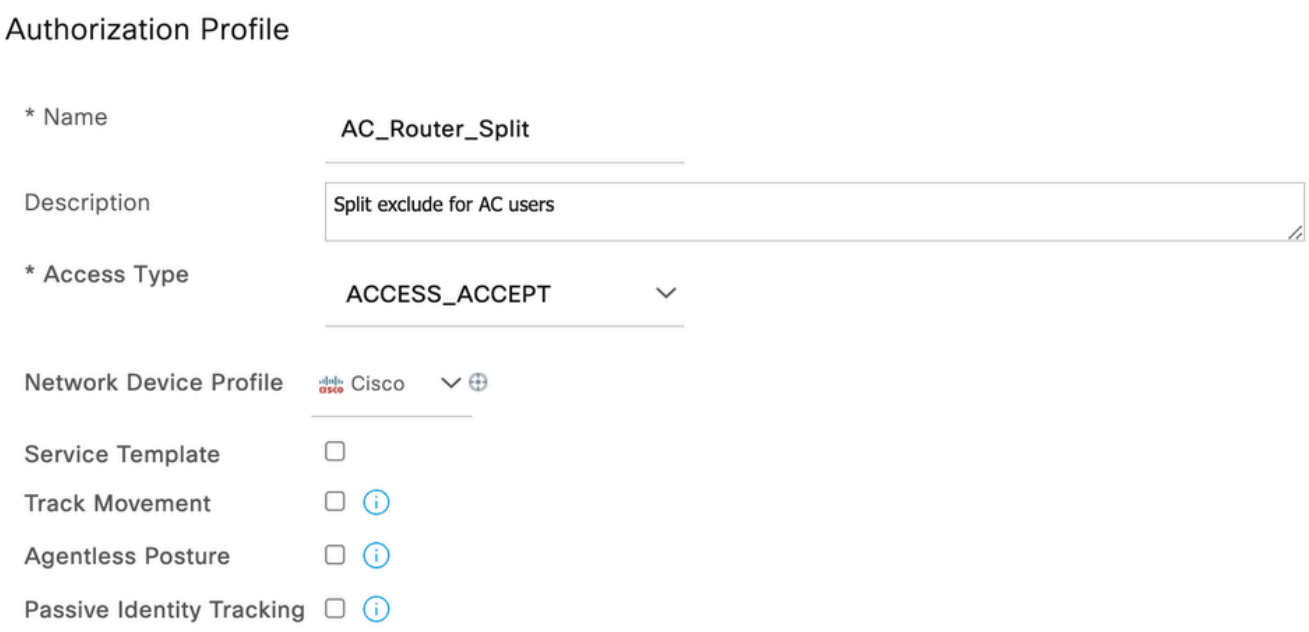
6. Create an Authorization Profile:

The authorization profile includes the actions that are taken when the authorization policy is matched. Create a new Authorization Profile that includes the next attributes:

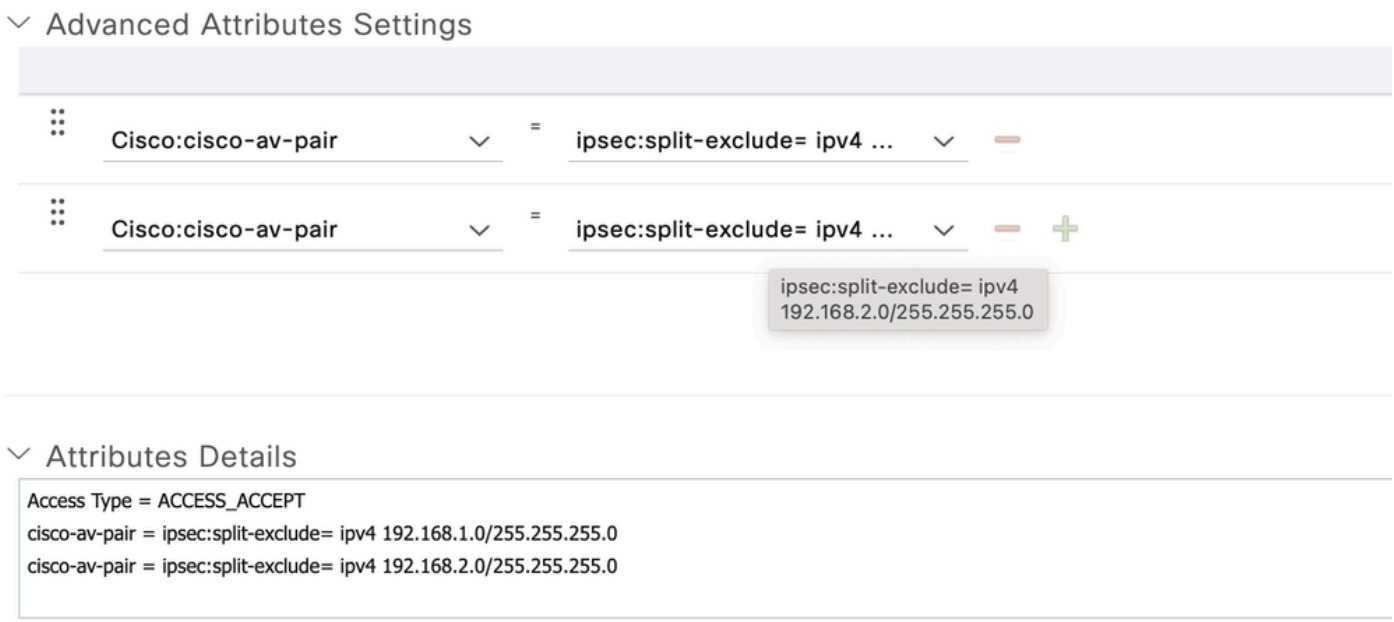
Access Type = ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <ip_network>/<subnet_mask>




*Create New Authorization Profile*

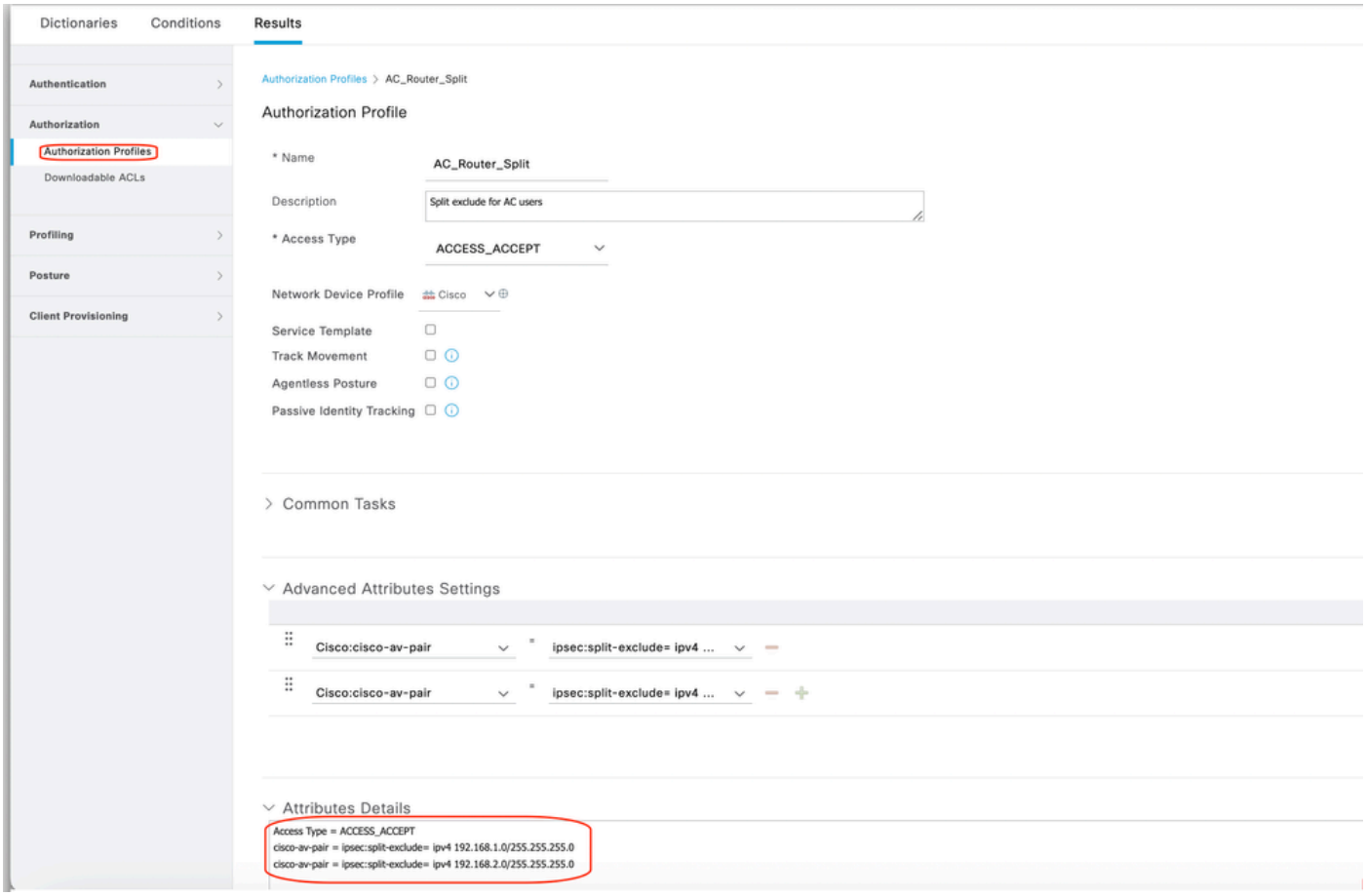



*Authorization Profile Config*



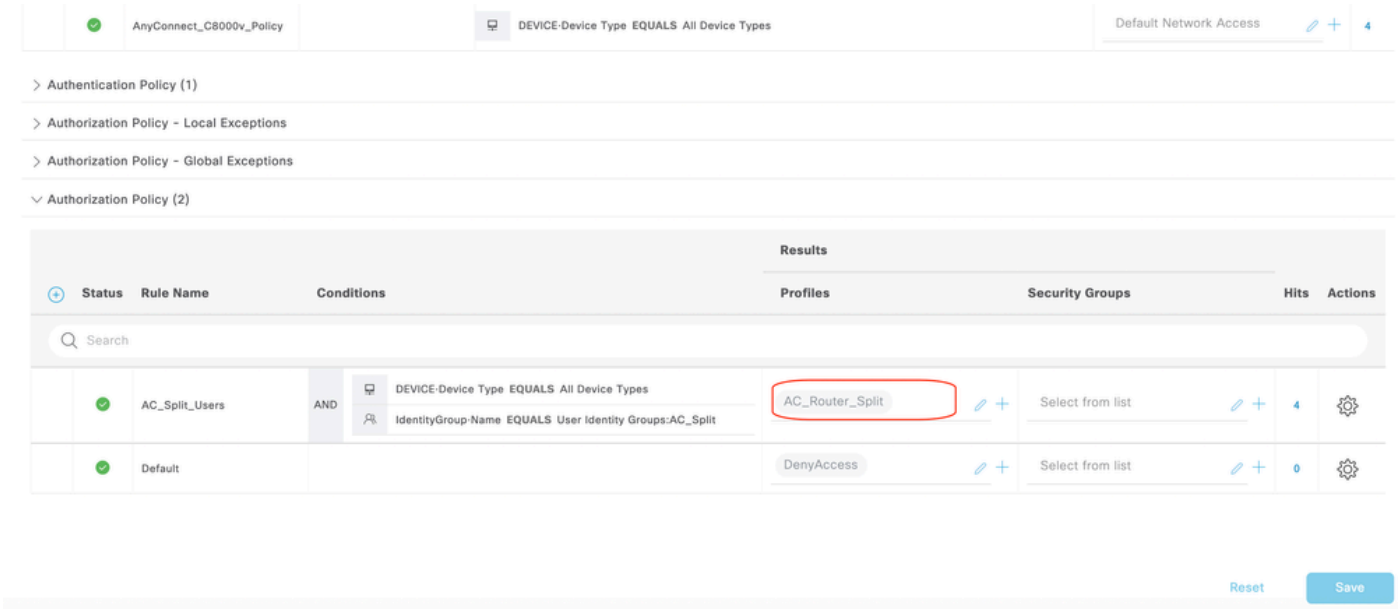

*Configure Attributes in Authorization Profile*

7. Review the Authorization Profile configuration.



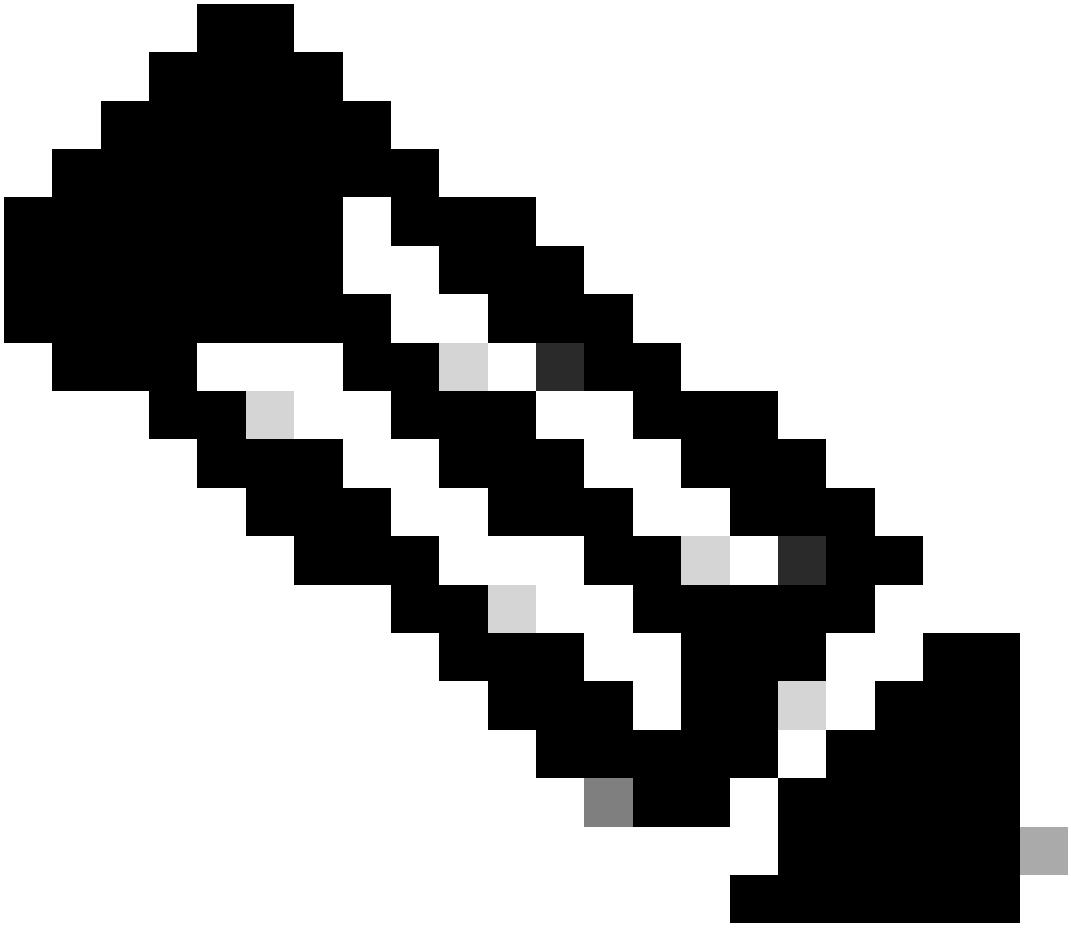

*Review the Authorization Profile Config*

8. This is the Authorization policy in Policy Set configuration after selecting required profiles:




***Final Authorization Policy Config***

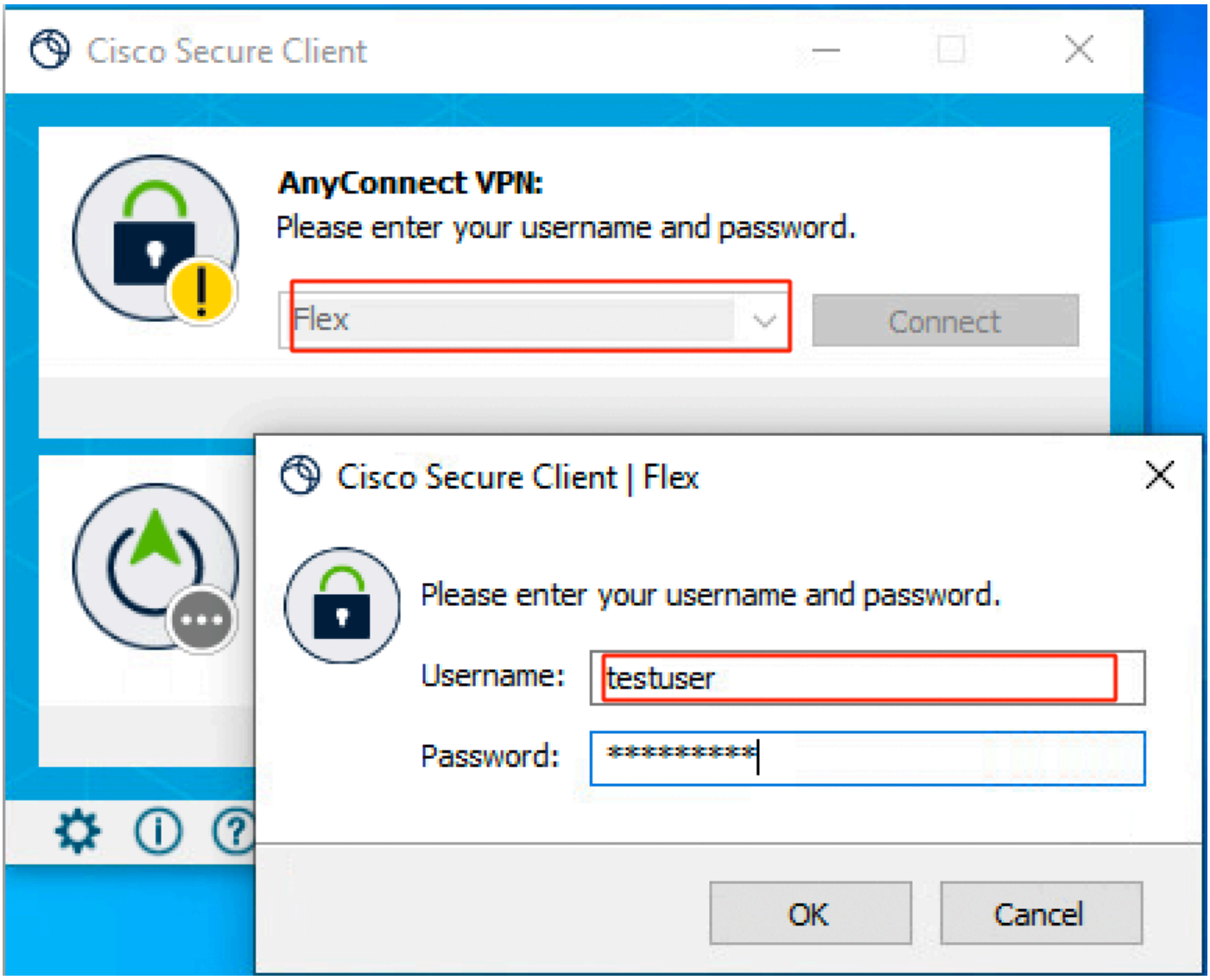
With this configuration example, you can exclude networks from passing through VPN through ISE configuration based on the identity group the user belongs to.



**Note**: Only one split-exclude subnet can be pushed to client PC when using Cisco IOS XE headend for a RA VPN connection. This has been addressed by Cisco bug ID CSCwj38106 and multiple split-exclude subnets can be pushed from 17.12.4. Refer to the bug for more details on Fixed versions.

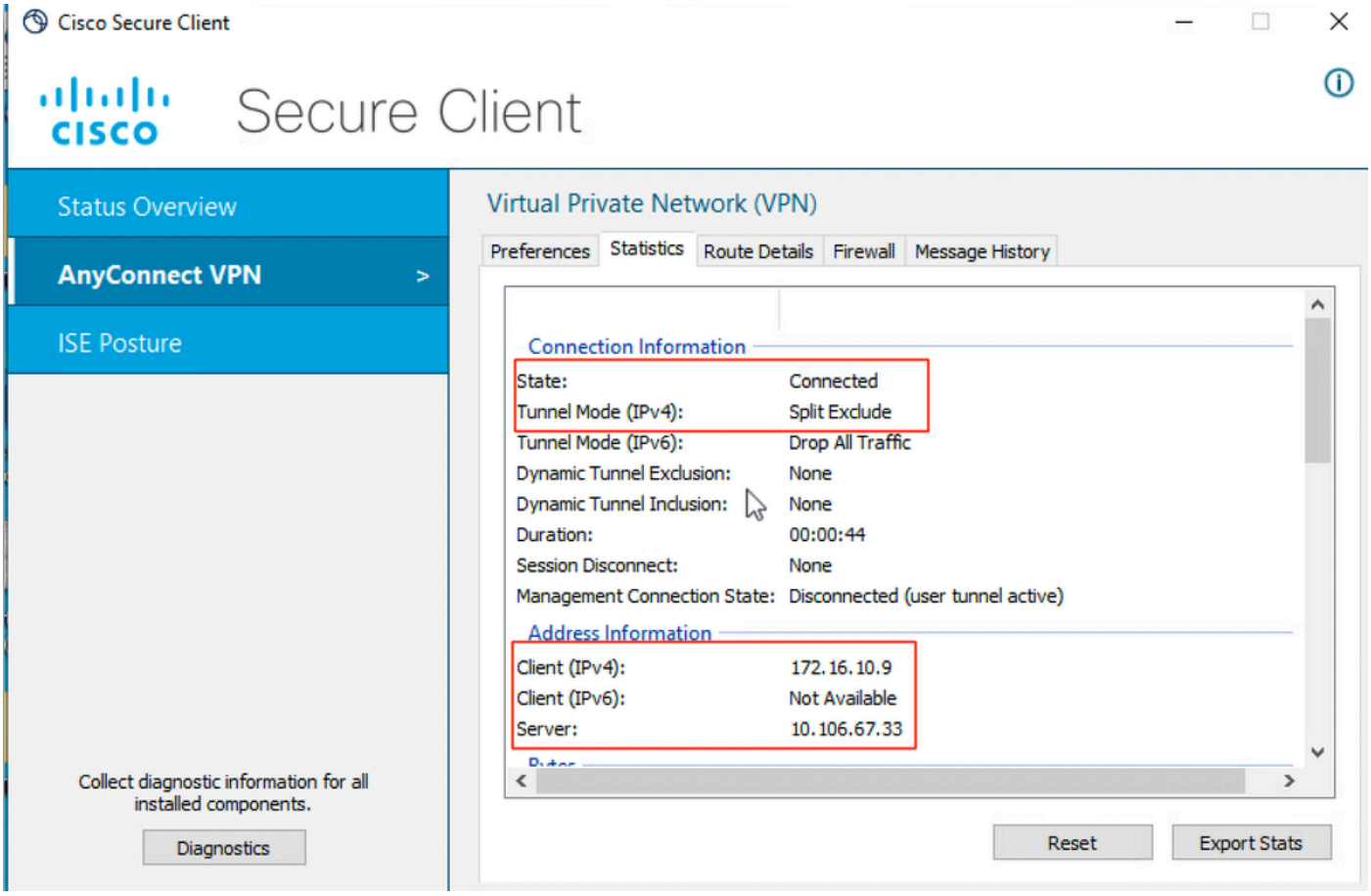
# Verify

1. In order to test the authentication, **connect** to the C8000V from the PC of the user through AnyConnect and **enter** the credentials.



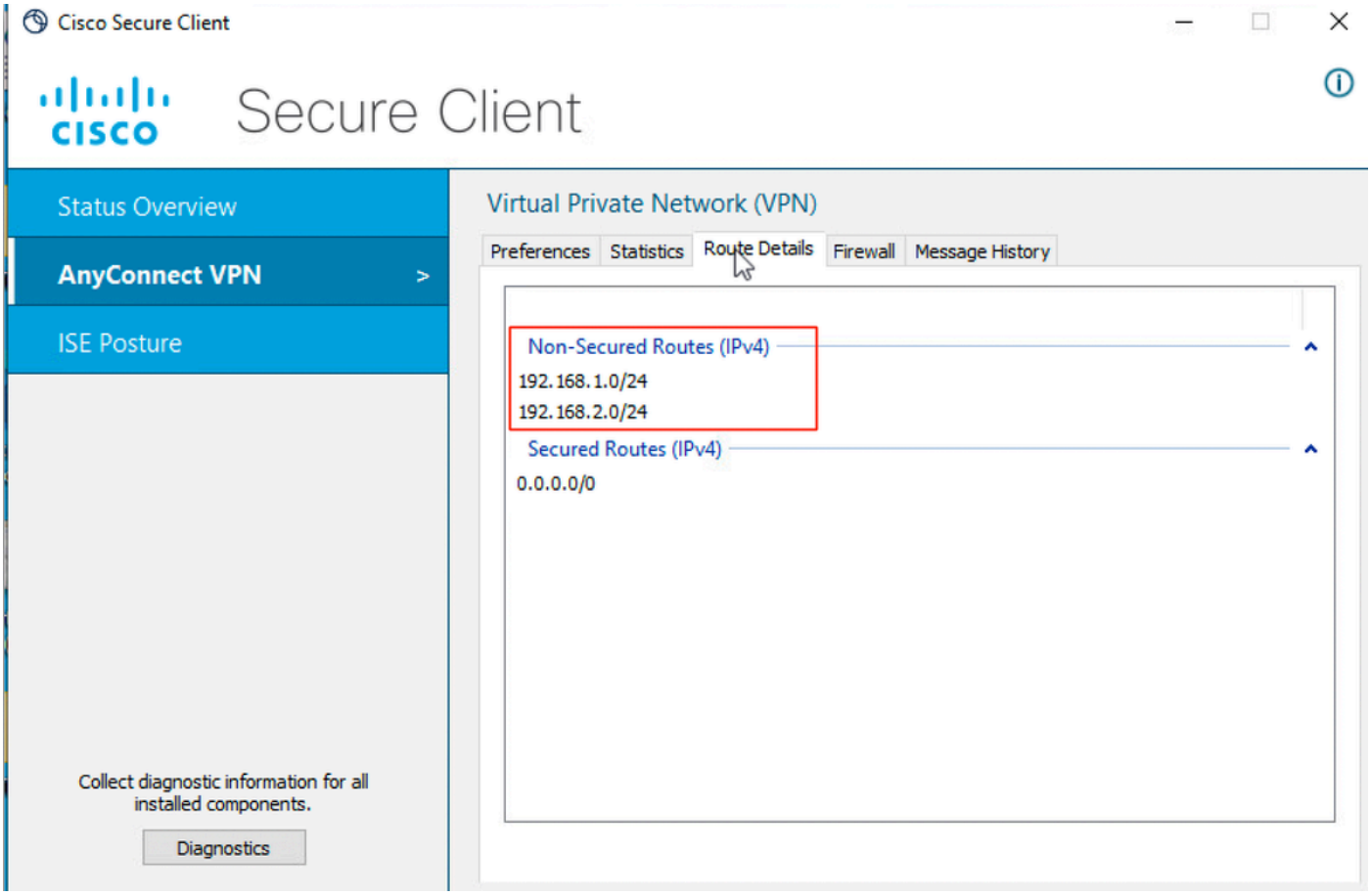

*Log in to AnyConnect*

2. Once the connection is established, **click** the **gear icon** (lower left corner) and navigate to **AnyConnect VPN > Statistics**. Confirm the Tunnel Mode to be Split Exclude.




*Validate the Statistics*

Navigate to **AnyConnect VPN > Route details** and confirm the information displayed corresponds to the secure routes and non-secure routes.




*Validate the Route Details*

You can also verify the connection details on the VPN headend:

1. IKEv2 parameters

<#root>

8kv#

**show crypto ikev2 sa detail**

**IPv4 Crypto IKEv2 SA**

**Tunnel-id Local Remote fvrf/ivrf Status**

**1 10.106.67.33/4500 10.106.50.91/55811 none/none READY**

**Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth verify: EAP**

**Life/Active Time: 86400/22 sec**

**CE id: 1012, Session-id: 6**

**Local spi: E8C6C5EEF0F0EF72 Remote spi: 7827644A7CA8F1A5**

**Status Description: Negotiation done**

**Local id: 10.106.67.33**

**Remote id: *$AnyConnectClient$***

**Remote EAP id: testuser**

**Local req msg id: 0 Remote req msg id: 6**

**Local next msg id: 0 Remote next msg id: 6**

**Local req queued: 0 Remote req queued: 6**

**Local window: 5 Remote window: 1**

**DPD configured for 0 seconds, retry 0**

**Fragmentation not configured.**

**Dynamic Route Update: disabled**

**Extended Authentication configured.**

**NAT-T is detected outside**

**Cisco Trust Security SGT is disabled**

**Assigned host addr: 172.16.10.10**

**Initiator of SA : No**

**Post NATed Address : 10.106.67.33**

**PEER TYPE: Other**

**IPv6 Crypto IKEv2 SA**

2.This is the crypto session detail for the VPN session:

<#root>

8kv#

**show crypto session detail**

**Crypto session current status**

**Code: C - IKE Configuration mode, D - Dead Peer Detection**

**K - Keepalives, N - NAT-traversal, T - cTCP encapsulation**

**X - IKE Extended Authentication, F - IKE Fragmentation**

**R - IKE Auto Reconnect, U - IKE Dynamic Route Update**

**S - SIP VPN**

**Interface: Virtual-Access1**

**Profile: prof1**

**Uptime: 00:00:44**

**Session status: UP-ACTIVE**

**Peer: 10.106.50.91 port 55811 fvrf: (none) ivrf: (none)**

```
Phase1_id: *$AnyConnectClient$*

Desc: (none)

Session ID: 16

IKEv2 SA: local 10.106.67.33/4500 remote 10.106.50.91/55811 Active

Capabilities:NX connid:1 lifetime:23:59:16

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.10.10

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 114 drop 0 life (KB/Sec) 4607987/3556

Outbound: #pkts enc'ed 96 drop 0 life (KB/Sec) 4608000/3556
```

3. Verify on ISE live logs.

# Troubleshoot

On Cisco Router:

1. Use the IKEv2 and IPsec debugs to verify the negotiation between the headend and the client.

```
debug crypto condition peer ipv4 <public_ip>
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. Use AAA debugs to verify the assignment of local and/or remote attributes.

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

On ISE:

Use the RADIUS live logs by navigating to **Operations > Live logs**.

**Working Scenario**

This is the debug of the successful connection:

<#root>

```
*Oct 13 10:01:25.928: RADIUS/ENCODE(0000012D):Orig. component type = VPN IPSEC
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): dropping service type, "radius-server attribute 6 on-for
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IP: 0.0.0.0
*Oct 13 10:01:25.929: vrfid: [65535] ipv6 tableid : [0]
*Oct 13 10:01:25.929: idb is NULL
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IPv6: ::
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): acct_session_id: 4291
*Oct 13 10:01:25.929: RADIUS(0000012D): sending
*Oct 13 10:01:25.929: RADIUS/ENCODE: Best Local IP-Address 10.106.67.33 for Radius-Server 10.127.197.10
*Oct 13 10:01:25.929: RADIUS: Message Authenticator encoded
*Oct 13 10:01:25.929: RADIUS(0000012D): Send Access-Request to 10.127.197.105:1812 id 1645/24, len 344
RADIUS: authenticator 85 AC BF 77 BF 42 0B C7 - DE 85 A3 9A AF 40 E5 DC
*Oct 13 10:01:25.929: RADIUS: Service-Type [6] 6 Login [1]
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 26
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 45
```

***Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 39 "isakmp-phase1-id=*$AnyConnectClient$*"**

```
*Oct 13 10:01:25.929: RADIUS: Calling-Station-Id [31] 14 "10.106.50.91"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 64
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L40A6A4321ZO2L40A6A325BZH1194CC58
*Oct 13 10:01:25.929: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 21
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
*Oct 13 10:01:25.929: RADIUS: EAP-Message [79] 24
RADIUS: 02 8E 00 16 04 10 8A 09 BB 0D 4B A9 D6 2B 59 1C C8 FE 1C 90 56 F5 [ K+YV]
*Oct 13 10:01:25.929: RADIUS: Message-Authenticato[80] 18
RADIUS: 54 85 1B AC BE A8 DA EF 24 AE 4D 28 46 32 8C 48 [ T$M(F2H]
*Oct 13 10:01:25.929: RADIUS: State [24] 90
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 30 41 36 41 34 33 32 31 5A 4F 32 4C 34 [2L40A6A4321ZO2L4]
RADIUS: 30 41 36 41 33 32 35 42 5A 48 31 31 39 34 43 43 [0A6A325BZH1194CC]
RADIUS: 35 38 5A 4E 31 32 3B 33 30 53 65 73 73 69 6F 6E [58ZN12;30Session]
RADIUS: 49 44 3D 69 73 65 2D 70 73 6E 2F 35 31 37 31 33 [ID=ise-psn/51713]
RADIUS: 35 39 30 30 2F 33 38 3B [ 5900/38;]
*Oct 13 10:01:25.929: RADIUS: NAS-IP-Address [4] 6 10.106.67.33
*Oct 13 10:01:25.929: RADIUS(0000012D): Sending a IPv4 Radius Packet
*Oct 13 10:01:25.929: RADIUS(0000012D): Started 120 sec timeout
```

***Oct 13 10:01:25.998: RADIUS: Received from id 1645/24 10.127.197.105:1812, Access-Accept, len 239**

```
RADIUS: authenticator BC 19 F2 EE 10 67 80 C5 - 9F D9 30 9A EA 7E 5E D3
*Oct 13 10:01:25.998: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.998: RADIUS: Class [25] 67
RADIUS: 43 41 43 53 3A 4C 32 4C 34 30 41 36 41 34 33 32 [CACS:L2L40A6A432]
RADIUS: 31 5A 4F 32 4C 34 30 41 36 41 33 32 35 42 5A 48 [1ZO2L40A6A325BZH]
RADIUS: 31 31 39 34 43 43 35 38 5A 4E 31 32 3A 69 73 65 [1194CC58ZN12:ise]
RADIUS: 2D 70 73 6E 2F 35 31 37 31 33 35 39 30 30 2F 33 [-psn/517135900/3]
```

```
RADIUS: 38 [ 8]
*Oct 13 10:01:25.998: RADIUS: EAP-Message [79] 6
RADIUS: 03 8E 00 04
*Oct 13 10:01:25.998: RADIUS: Message-Authenticato[80] 18
RADIUS: F9 61 C1 FD 6D 26 31 A2 89 04 72 BC DD 32 A9 29 [ am&1r2)]
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0"

*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0"

*Oct 13 10:01:25.998: RADIUS(0000012D): Received from id 1645/24
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
8kv#
```

# References

- Configure FlexVPN Headend for IKEv2 Remote Access Using Local User Database
- Configure AnyConnect Flexvpn with EAP and DUO Authentication
- Configure AnyConnect IKEv2 Remote Access with EAP-MD5