

# Configuración de la asignación de atributos RADIUS para usuarios remotos de FlexVPN

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del router](#)

[Configuración de Identity Services Engine \(ISE\)](#)

[Configuración del Cliente](#)

[Verificación](#)

[Troubleshoot](#)

[Depuraciones y registros](#)

[Escenario de trabajo](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar FlexVPN mediante Cisco Identity Services Engine (ISE) para verificar identidades y realizar la asignación de grupos de atributos.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red privada virtual de acceso remoto (RAVPN) con configuración IKEV2/IPsec en un router Cisco IOS® XE mediante CLI
- Configuración de Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocolo RADIUS

### Componentes Utilizados

Este documento se basa en las siguientes versiones de software y hardware:

- Cisco CSR1000V (VXE), versión 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1
- Cisco Secure Client (CSC), versión 5.0.05040
- Windows 11

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

### Diagrama de la red

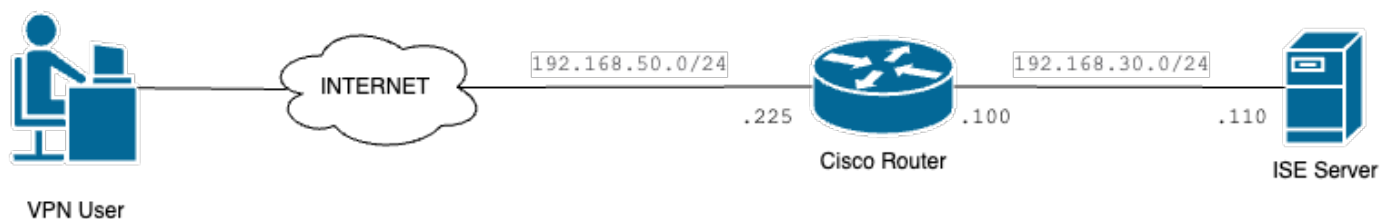


Diagrama de red básico

## Configuraciones

### Configuración del router

Paso 1. Configure un servidor RADIUS para la autenticación y autorización local en el dispositivo:

```
aaa new-model
aaa group server radius FlexVPN-Authentication-Server
server-private 192.168.30.110 key Cisco123
aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server
aaa authorization network FlexVPN-Authorization-List local
```

El comando `aaa authentication login <list_name>` hace referencia al grupo de autenticación, autorización y contabilización (AAA) (que define el servidor RADIUS).

El comando `aaa authorization network <list_name> local` indica que se deben utilizar los usuarios/grupos definidos localmente.

Paso 2. Configure un punto de confianza para almacenar el certificado del router. Dado que la autenticación local del router es de tipo RSA, el dispositivo requiere que el servidor se autentique utilizando un certificado:

```
crypto pki trustpoint FlexVPN-TP
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
revocation-check none
rsa-keypair FlexVPN_KEY
```

Paso 3. Defina un conjunto local de IP para cada grupo de usuarios diferente:

```
ip local pool group1 172.16.10.1 172.16.10.50
ip local pool group2 172.16.20.1 172.16.20.50
```

Paso 4. Configure la política de autorización local:

```
crypto ikev2 authorization policy FlexVPN-Local-Policy
```

No se requiere ninguna configuración en la directiva de autorización, ya que el servidor de autenticación es responsable de enviar los valores relevantes (DNS, agrupación, rutas protegidas, etc.) en función del grupo al que pertenece el usuario. Sin embargo, debe configurarse para definir el nombre de usuario en nuestra base de datos de autorización local.

Paso 5 (opcional). Cree una propuesta y una política IKEv2 (si no se configura, se utilizan los valores predeterminados inteligentes):

```
crypto ikev2 proposal IKEv2-prop
  encryption aes-cbc-256
  integrity sha256
  group 14
```

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

Paso 6 (opcional). Configure el conjunto de transformación (si no se configura, se utilizan los valores predeterminados inteligentes):

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

Paso 7. Configure un perfil IKEv2 con las identidades locales y remotas adecuadas, los métodos

de autenticación (local y remota), el punto de confianza, AAA y la interfaz de plantilla virtual utilizada para las conexiones:

```
crypto ikev2 profile FlexVPN-IKEv2-Profile
match identity remote key-id cisco.example
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FlexVPN-TP
aaa authentication eap FlexVPN-Authentication-List
aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy
aaa authorization user eap cached
virtual-template 100
```

El comando `aaa authorization user eap cached` especifica que los atributos recibidos durante la autenticación EAP deben almacenarse en caché. Este comando es esencial para la configuración porque sin él, los datos enviados por el servidor de autenticación no se utilizan, lo que lleva a una conexión fallida.



Nota: La ID de clave remota debe coincidir con el valor de ID de clave del archivo XML. Si no se modifica en el archivo XML, se utiliza el valor predeterminado (\*\$AnyConnectClient\$\*) y se debe configurar en el perfil IKEv2.

---

Paso 8. Configure un perfil IPsec y asigne el conjunto de transformación y el perfil IKEv2:

```
crypto ipsec profile FlexVPN-IPsec-Profile
set transform-set TS
set ikev2-profile FlexVPN-IKEv2-Profile
```

Paso 9. Configure una interfaz de loopback. Las interfaces de acceso virtual toman prestada la dirección IP de la misma:

```
interface Loopback100
```

```
ip address 10.0.0.1 255.255.255.255
```

Paso 10. Cree la plantilla virtual que se va a utilizar para crear las distintas interfaces de acceso virtual y enlace el perfil IPsec creado en el paso 8:

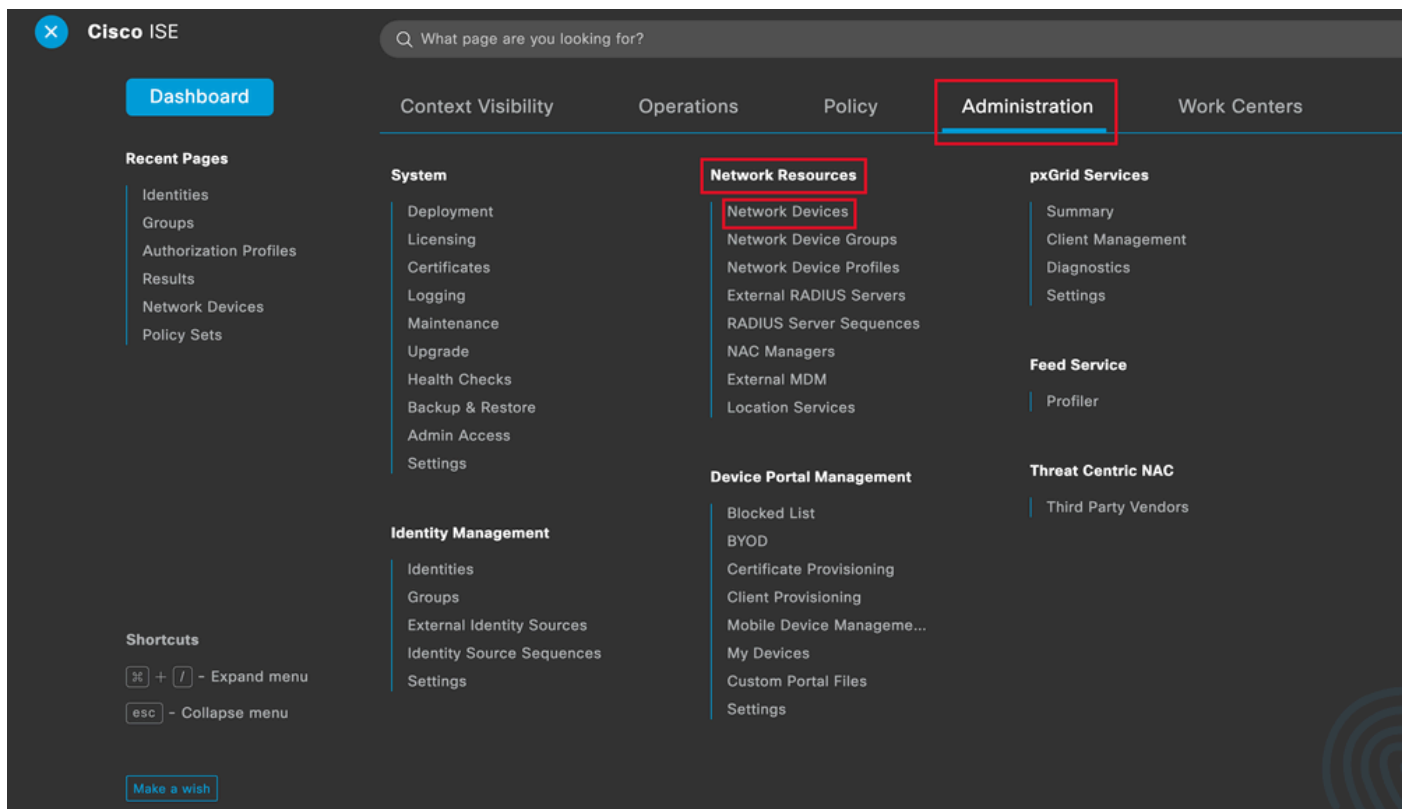
```
interface Virtual-Template100 type tunnel
ip unnumbered Loopback100
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

Paso 11. Inhabilite la búsqueda de certificados basada en HTTP-URL y el servidor HTTP en el router:

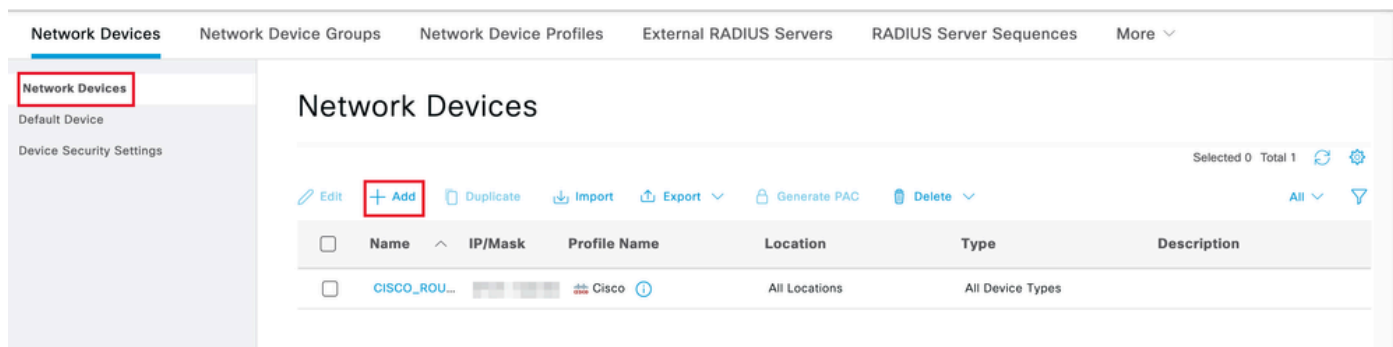
```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

## Configuración de Identity Services Engine (ISE)

Paso 1. Inicie sesión en el servidor ISE y navegue hasta Administration > Network Resources > Network Devices:



## Paso 2. Haga clic en Agregar para configurar el router como un cliente AAA:



Adición de un nuevo dispositivo de red

Ingrese los campos Network Device Name y IP Address y luego marque la casilla RADIUS Authentication Settings y agregue el secreto compartido; este valor debe ser el mismo que se utilizó cuando se creó el objeto de servidor RADIUS en el router.

## Network Devices

Name

Description

IP Address

Nombre y dirección IP



## ✓ RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

\*\*\*\*\*

Show

Use Second Shared Secret ⓘ

networkDevices.secondSharedSecret

Show

Contraseña de RADIUS

Click Save.

Paso 3. Vaya a Administration > Identity Management > Groups:

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. The left sidebar has 'Recent Pages' (Identities, Groups, Authorization Profiles, Results, Policy Sets) and 'Shortcuts' (Expand menu, Collapse menu). The main content area is divided into sections: 'System' (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), 'Network Resources' (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), 'Device Portal Management' (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Manageme..., My Devices, Custom Portal Files, Settings), 'pxGrid Services' (Summary, Client Management, Diagnostics, Settings), 'Feed Service' (Profiler), and 'Threat Centric NAC' (Third Party Vendors). In the 'System' section, 'Identity Management' and 'Groups' are highlighted with red boxes.

Menú general de ISE

Paso 4. Haga clic en User Identity Groups y luego haga clic en Add:



## Identity Groups

EQ



> Endpoint Identity Groups

> User Identity Groups

## User Identity Groups

Selected 0 Total 10

Edit **+ Add** Delete Import Export

All

| Name  | Description                                 |
|---|---|
| <input type="checkbox"/> ALL_ACCOUNTS (default)   | Default ALL_ACCOUNTS (default) User Group   |
| <input type="checkbox"/> Employee                 | Default Employee User Group                 |
| <input type="checkbox"/> GROUP_ACCOUNTS (default) | Default GROUP_ACCOUNTS (default) User Group |

Agregar un nuevo grupo

Introduzca el nombre del grupo y haga clic en Enviar.

### Identity Group

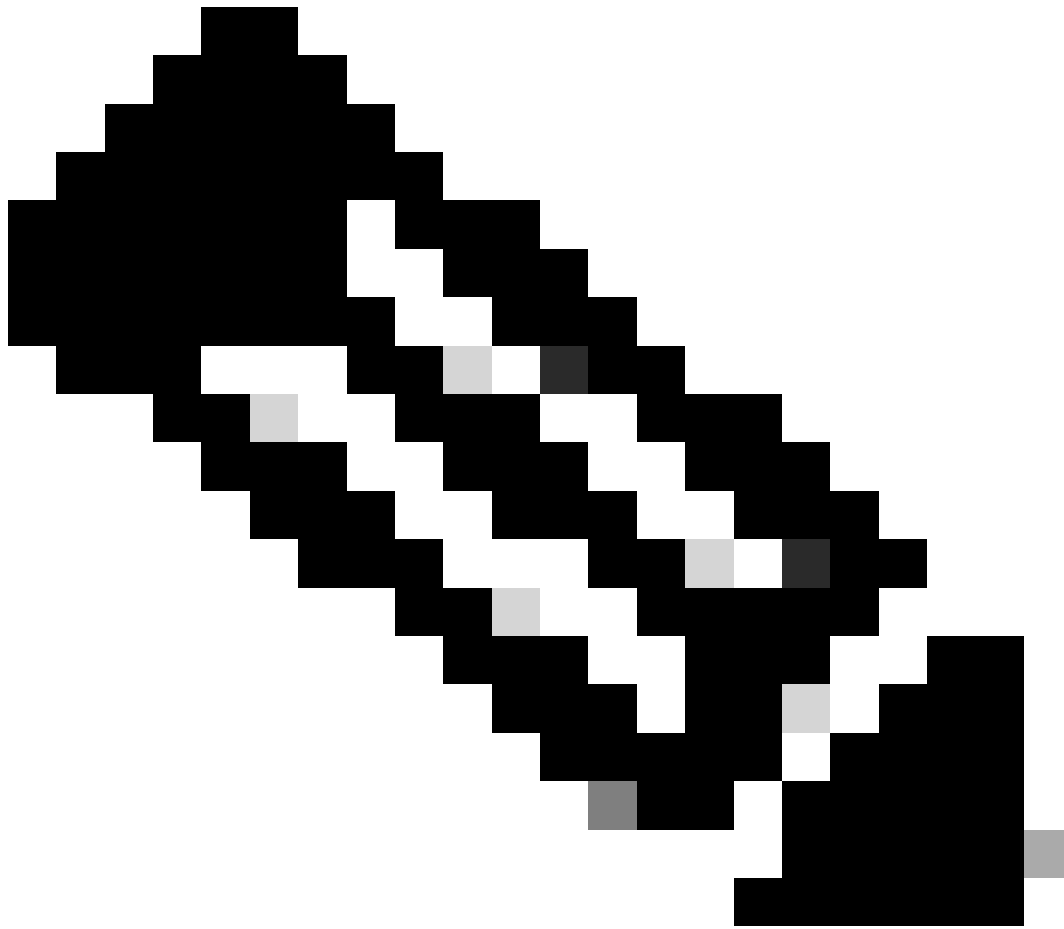
\* Name Group1

Description

Submit

Cancel

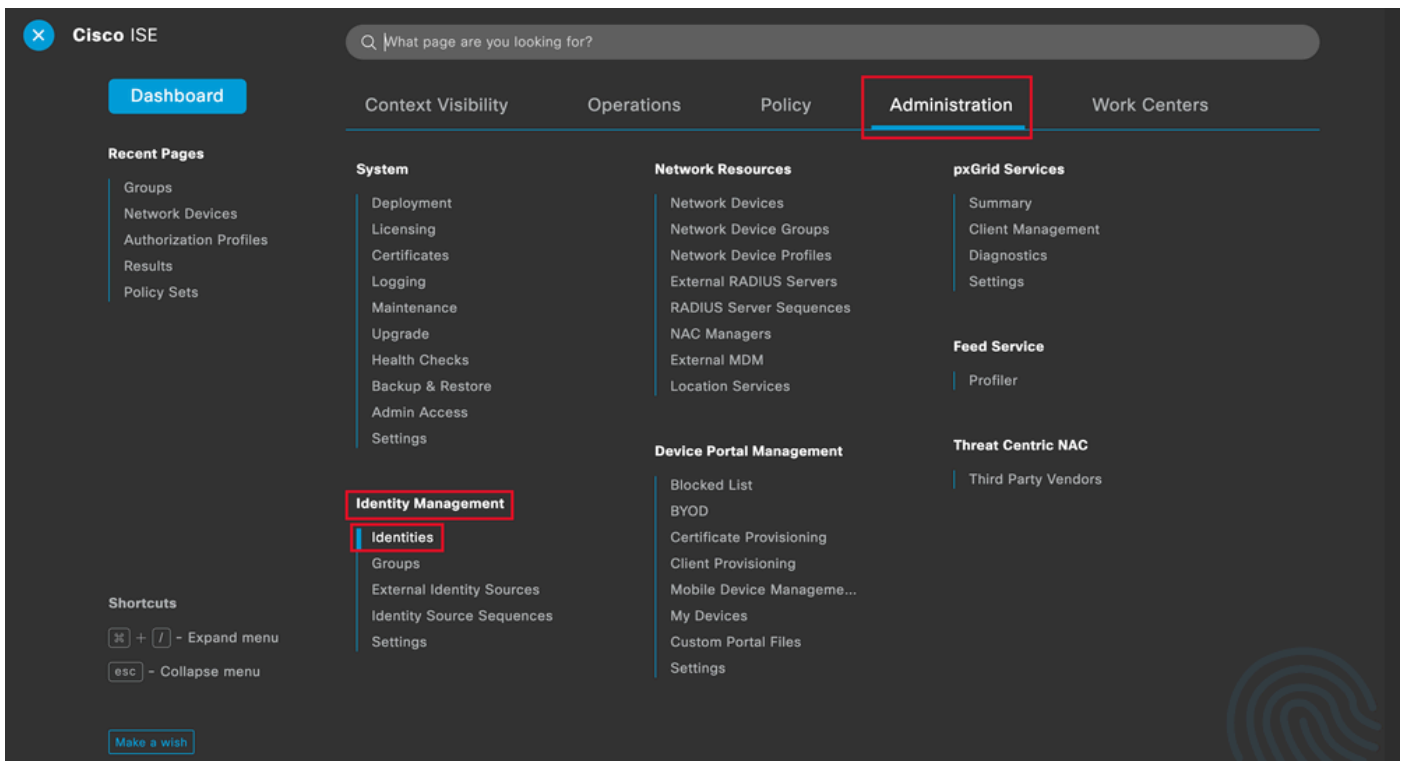
Información de grupo



Nota: Repita los pasos 3 y 4 para crear tantos grupos como sea necesario.

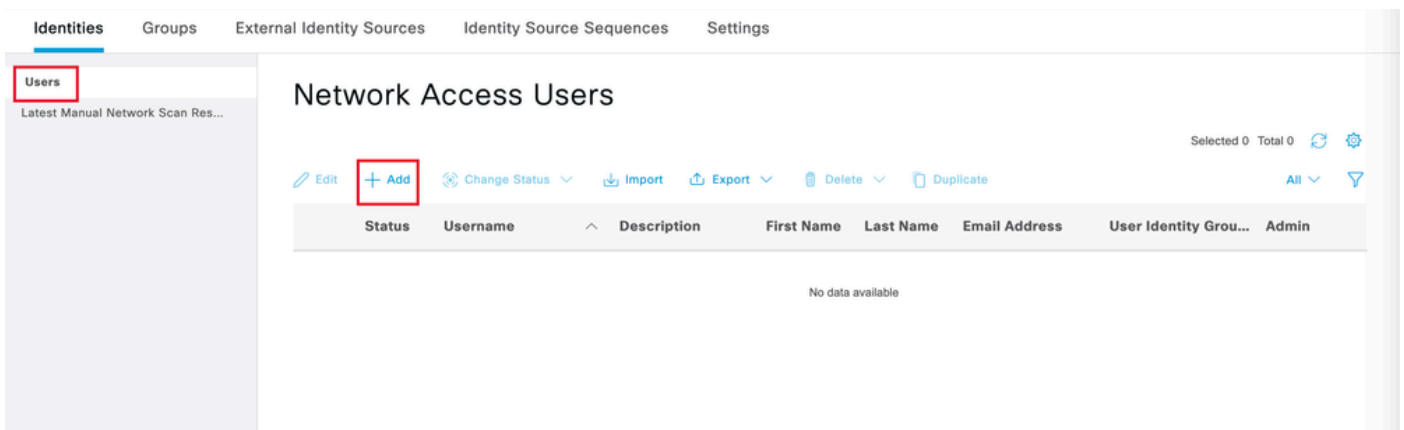
---

Paso 5. Vaya a Administration > Identity Management > Identities:



Menú general de ISE

Paso 6. Haga clic en Agregar para crear un nuevo usuario en la base de datos local del servidor:



Agregar un usuario

Introduzca el nombre de usuario y la contraseña de inicio de sesión. A continuación, desplácese hasta el final de esta página y seleccione el Grupo de usuarios:

Network Access User

\* Username user1

Status  Enabled

Email

Passwords

Password Type: Internal Users

Password \* Login Password ..... Re-Enter Password .....

Generate Password ⓘ

Generate Password ⓘ

Enable Password

Nombre de usuario y contraseña

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 20

User Groups

User Groups

SEARCH

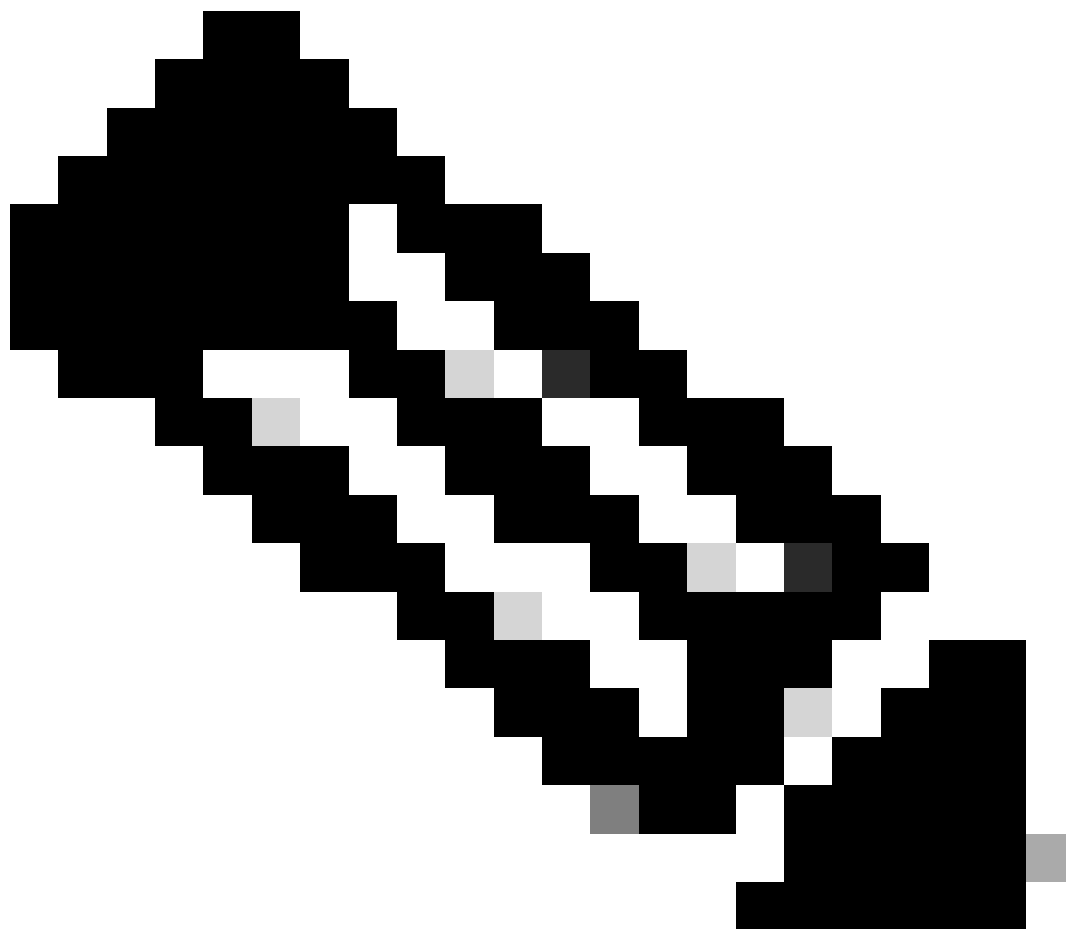
< [icon] [gear]

- ALL\_ACCOUNTS (default)
- Employee
- Group1**
- Group2
- GROUP\_ACCOUNTS (default)

Select an item

Asignar el grupo correcto al usuario

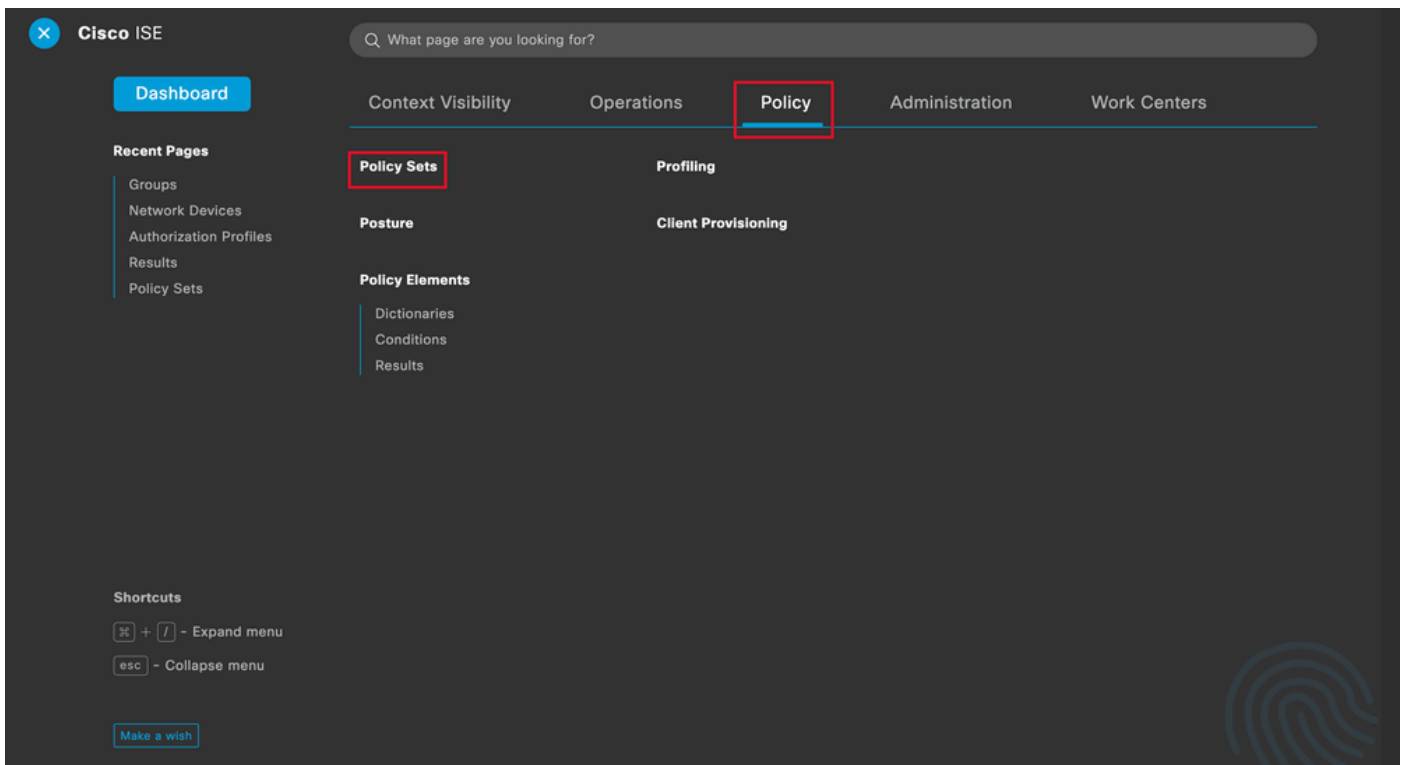
Click Save.



Nota: Repita los pasos 5 y 6 para crear los usuarios que necesite y asignarlos al grupo correspondiente.

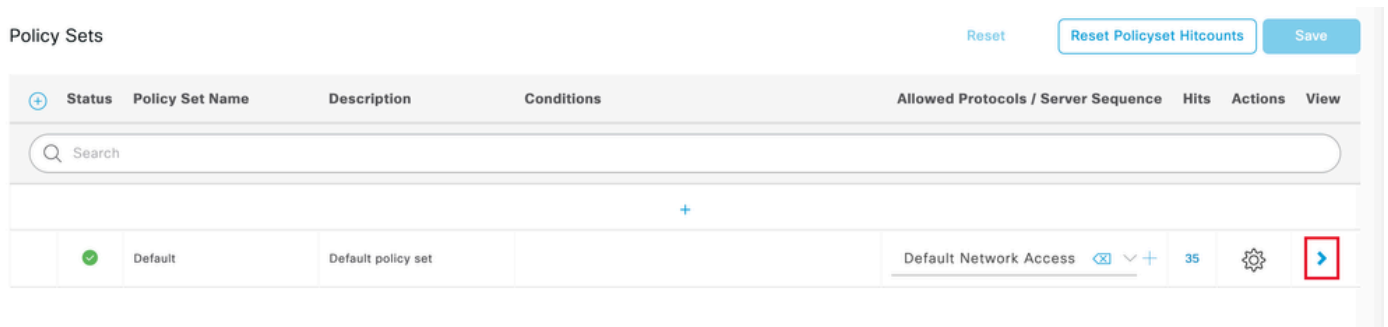
---

Paso 7. Navegue hasta Política > Juegos de Políticas:



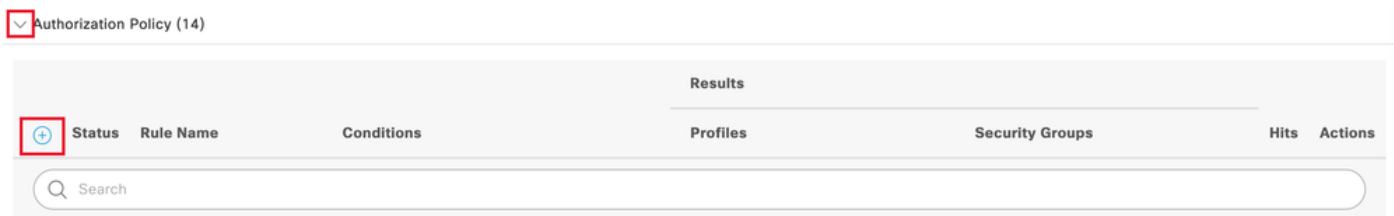
Menú general de ISE

Seleccione la política de autorización predeterminada haciendo clic en la flecha situada a la derecha de la pantalla:



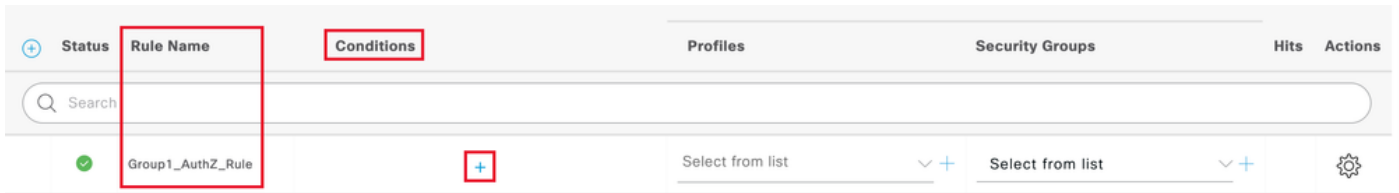
Seleccione la política de autorización

Paso 8. Haga clic en la flecha del menú desplegable junto a Directiva de autorización para expandirla. Luego, haga clic en el icono add (+) para agregar una nueva regla:



Agregar una nueva regla de autorización

Introduzca el nombre de la regla y seleccione el icono add (+) en la columna Conditions:



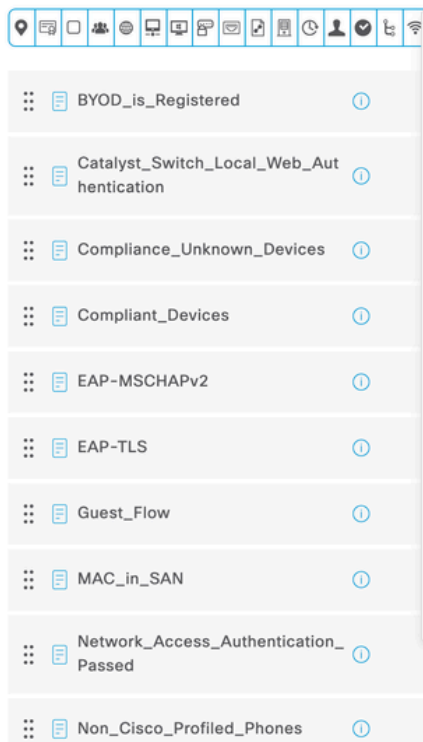
Agregar una condición

Paso 9. Haga clic en el cuadro de texto Editor de atributos y haga clic en el grupo Identidad. Seleccione el atributo Identity group - Name:

## Conditions Studio

### Library

Search by Name



### Editor

Click to add an attribute

#### Select attribute for condition

| Dictionary       | Attribute          | ID | Info |
|------------------|--------------------|----|------|
| All Dictionaries | Attribute          | ID |      |
| CWA              | CWA_ExternalGroups |    |      |
| IdentityGroup    | Description        |    |      |
| IdentityGroup    | Name               |    |      |
| InternalUser     | IdentityGroup      |    |      |
| PassiveID        | PassiveID_Groups   |    |      |

Seleccione la condición

Select(Seleccionar) Igual que el operador; a continuación, haga clic en la flecha del menú desplegable para mostrar las opciones disponibles y seleccione User Identity Groups:<GROUP\_NAME>.

## Editor

IdentityGroup-Name

Equals

Choose from list or type

Set to 'Is not'

User Identity Groups:GROUP\_ACCOUNTS (default)

**User Identity Groups:Group1**

User Identity Groups:Group2

User Identity Groups:GuestType\_Contractor (default)

User Identity Groups:GuestType\_Daily (default)

Save

Seleccione el grupo

Click Save.

Paso 10. En la columna Profiles, haga clic en el icono add (+) y elija Create a New Authorization Profile:

| Status | Rule Name                   | Conditions   | Profiles                                  | Security Groups  | Hits | Actions |
|--------|-----------------------------|--|---|------------------|------|---------|
| ✓      | Group1_AuthZ_Rule           | IdentityGroup-Name EQUALS User Identity Groups:Group1                            | Select from list <b>+</b>                 | Select from list | 10   | ⚙️      |
| ✓      | Wireless Black List Default | Wireless_Access AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist | <b>Create a New Authorization Profile</b> | Select from list | 0    | ⚙️      |

Crear el perfil de autorización

Introduzca el nombre del perfil




# Add New Standard Profile

## Authorization Profile


\* Name Profile\_group1


Description


\* Access Type ACCESS\_ACCEPT

Network Device Profile  Cisco

Service Template

Track Movement  


Agentless Posture  

Passive Identity Tracking  

Información de perfil

Desplácese hasta el final de esta página hasta Advanced Attribute Settings (Parámetros de atributos avanzados) y haga clic en la flecha del menú desplegable. A continuación, haga clic en Cisco y seleccione cisco-av-pair--[1]:

Advanced Attributes Settings

Select an item  =

**Cisco**

- cisco-abort-cause--[21]
- cisco-account-info--[250]
- cisco-assign-ip-pool--[218]
- cisco-av-pair--[1]**
- cisco-call-filter--[243]
- cisco-call-id--[141]

Attributes Details

Access Type = ACCESS\_ACCEPT

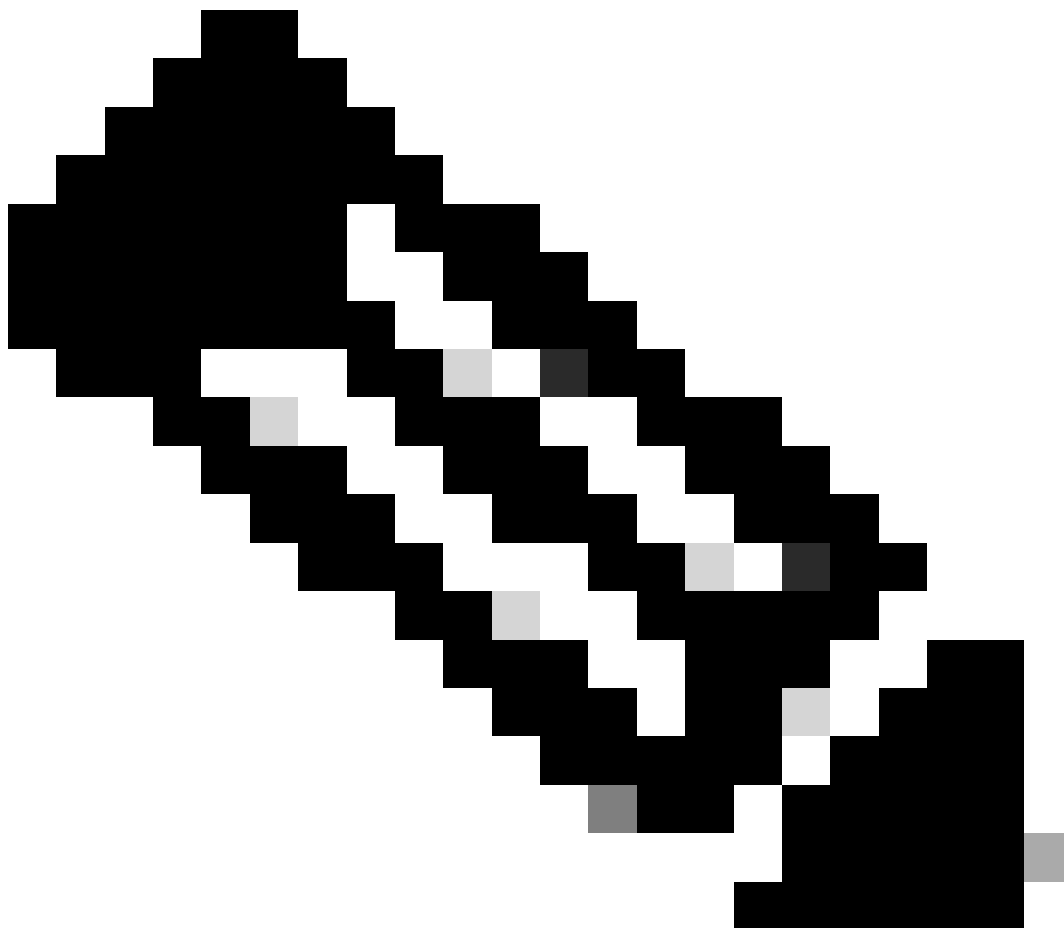
Seleccione el tipo de atributo

Agregue el atributo cisco-av-pair que desee configurar y haga clic en el icono add (+) para agregar otro atributo:

### Advanced Attributes Settings

 Cisco:cisco-av-pair  

Configuración del atributo



Nota: Para obtener información sobre las especificaciones de atributos (nombre, sintaxis, descripción, ejemplo, etc.), consulte la guía de configuración de atributos RADIUS de

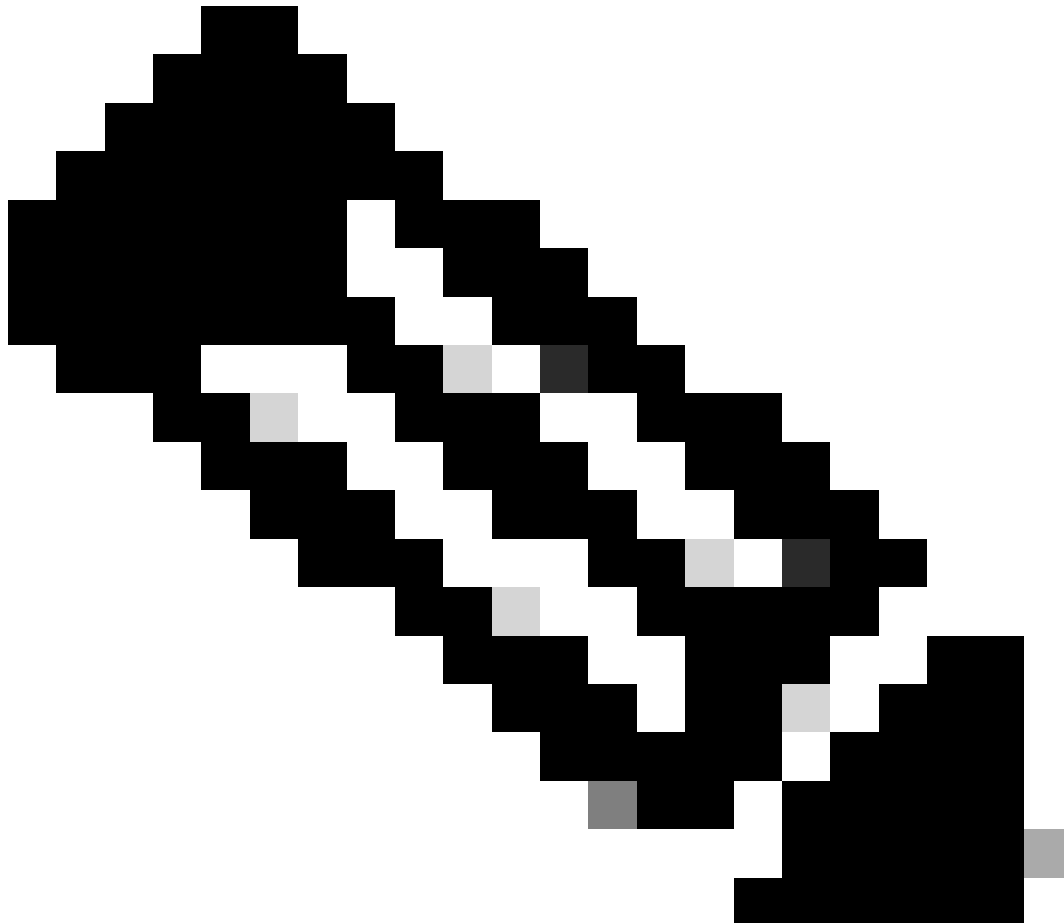
---

FlexVPN:

[Guía de configuración de FlexVPN e Intercambio de claves de Internet versión 2, Cisco IOS XE Fuji 16.9.x - Atributos RADIUS admitidos](#)

---

---



Nota: Repita el paso anterior para crear los atributos necesarios.

---

Click Save.

Los atributos que vienen a continuación se asignaron a cada grupo:

- Atributos del grupo 1:

Advanced Attributes Settings

|   |                     |   |   |   |   |     |
|---|---------------------|---|---|---|---|-----|
| ⋮ | Cisco:cisco-av-pair | ▼ | = | ipsec:dns-servers=10.0.50.10            | ▼ | —   |
| ⋮ | Cisco:cisco-av-pair | ▼ | = | ipsec:route-set=prefix 192.168.100.0/24 | ▼ | —   |
| ⋮ | Cisco:cisco-av-pair | ▼ | = | ipsec:addr-pool=group1                  | ▼ | — + |

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = ipsec:dns-servers=10.0.50.101  
cisco-av-pair = ipsec:route-set=prefix 192.168.100.0/24  
cisco-av-pair = ipsec:addr-pool=group1

Atributo Group1

- Atributos del grupo 2:

Advanced Attributes Settings

|   |                     |   |   |   |   |     |
|---|---------------------|---|---|---|---|-----|
| ⋮ | Cisco:cisco-av-pair | ▼ | = | ipsec:dns-servers=10.0.50.20            | ▼ | —   |
| ⋮ | Cisco:cisco-av-pair | ▼ | = | ipsec:route-set=prefix 192.168.200.0/24 | ▼ | —   |
| ⋮ | Cisco:cisco-av-pair | ▼ | = | ipsec:addr-pool=group2                  | ▼ | — + |

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = ipsec:dns-servers=10.0.50.202  
cisco-av-pair = ipsec:route-set=prefix 192.168.200.0/24  
cisco-av-pair = ipsec:addr-pool=group2

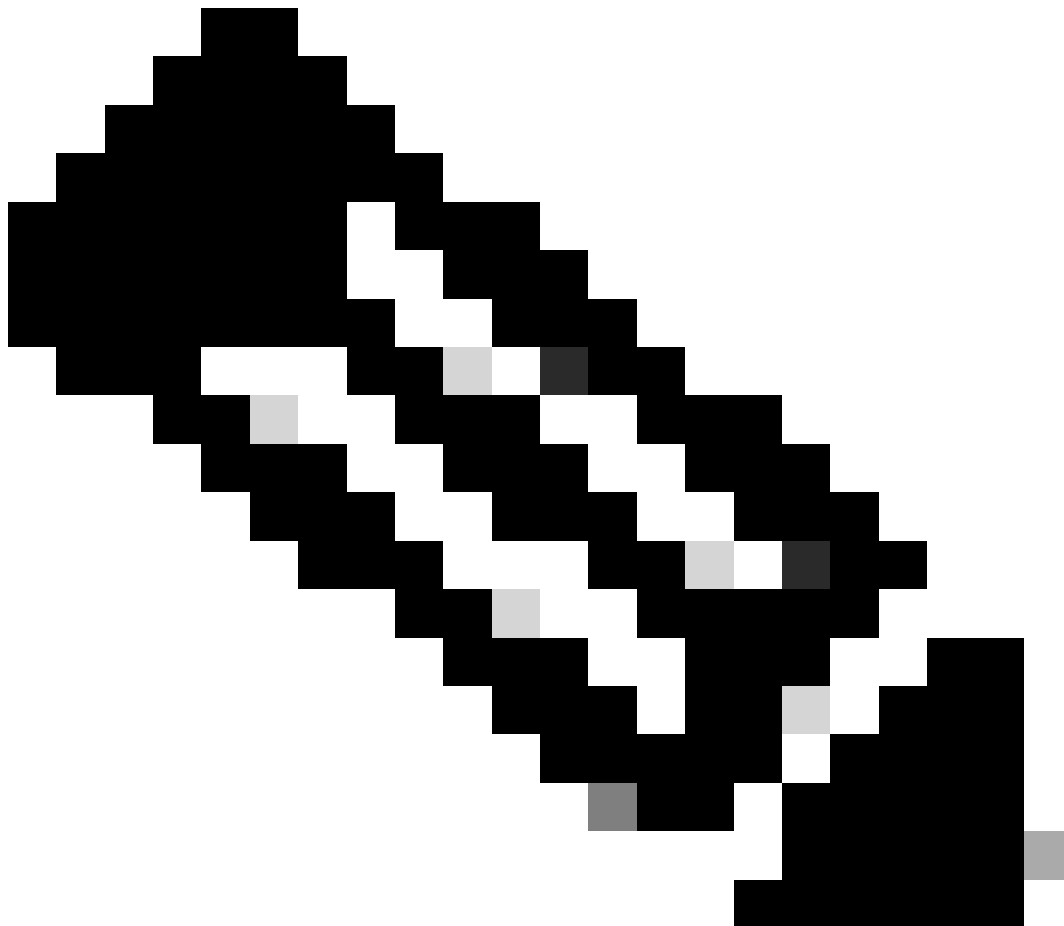
Atributos de Group2

Paso 11. Haga clic en la flecha del menú desplegable y seleccione el perfil de autorización creado en el paso 10:

| Status | Rule Name                    | Conditions   | Profiles   | Security Groups  | Hits | Actions |
|--------|------------------------------|--|--|------------------|------|---------|
| ✓      | Group1_AuthZ_Rule            | IdentityGroup-Name EQUALS User Identity Groups:Group1                                  | Select from list   | Select from list | 10   | ⚙️      |
| ✓      | Wireless Black List Default  | AND<br>Wireless_Access<br>IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist | DenyAccess<br>NSP_Onboard<br>Non_Cisco_IP_Phones<br>PermitAccess<br>Profile_group1 | 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  | Non_Cisco_IP_Phones  | Select from list | 0    | ⚙️      |

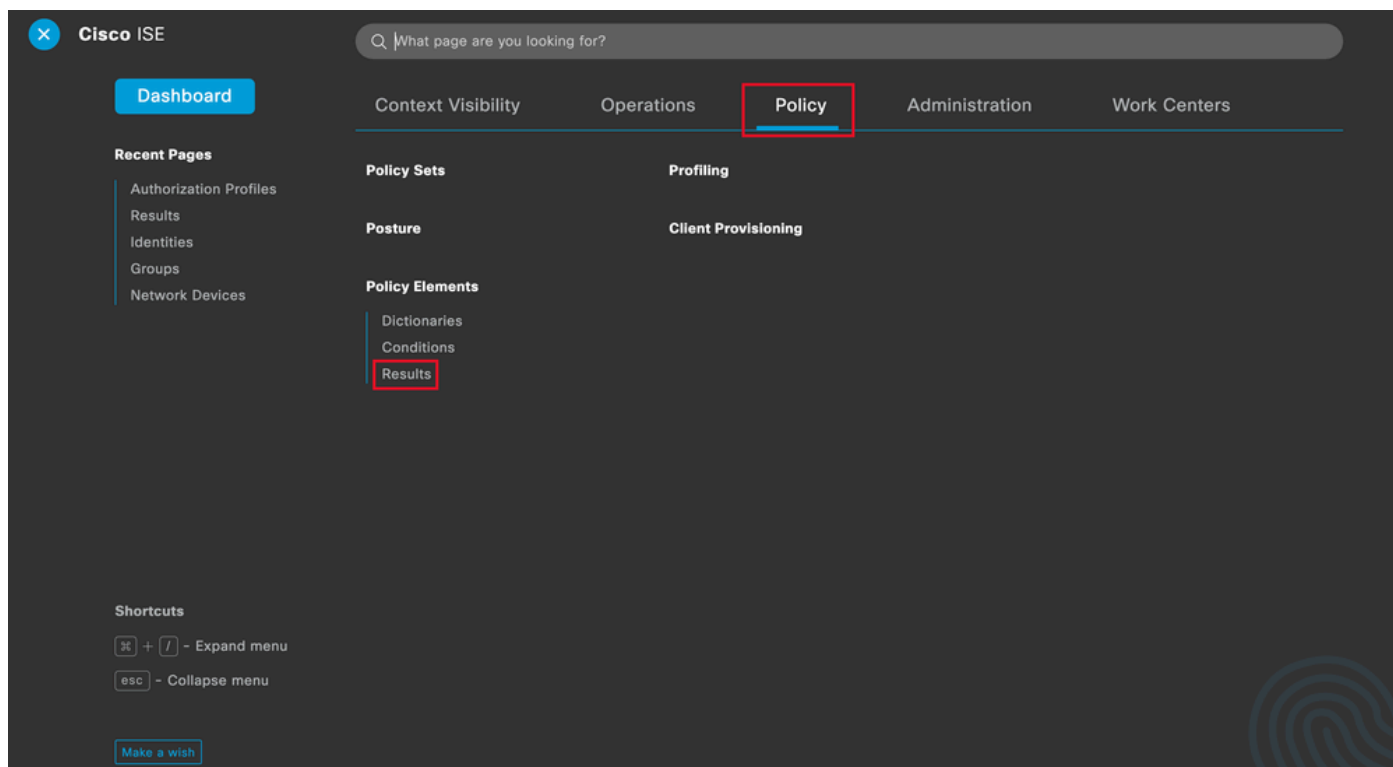
Asignar perfil de autorización

Click Save.



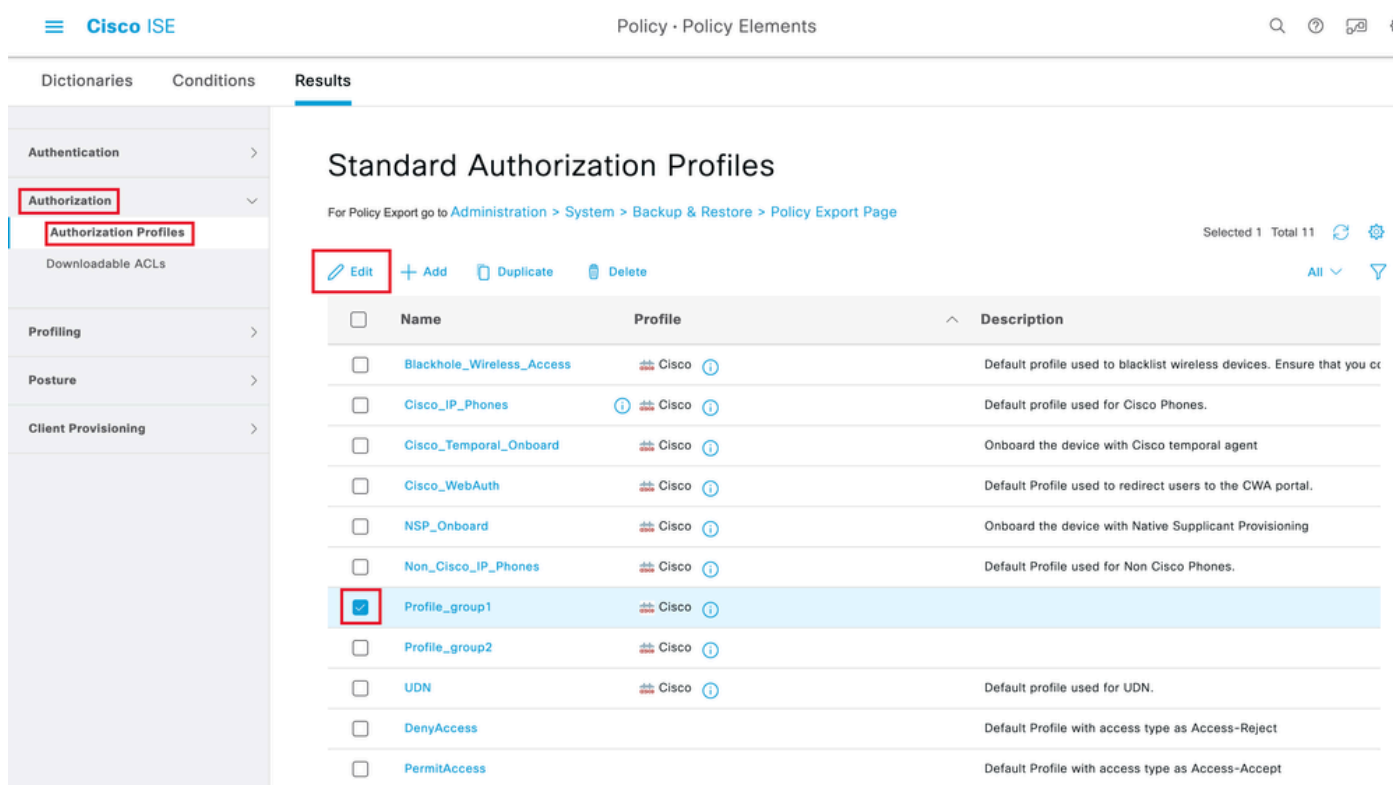
Nota: Repita los pasos del 8 al 11 para crear las reglas de autorización necesarias para cada grupo.

Paso 12 (opcional). Si necesita editar el perfil de autorización, navegue hasta Política > Resultados:



Menú general de ISE

Vaya a Autorización > Perfiles de autorización. Haga clic en la casilla de verificación del perfil que desea modificar y, a continuación, haga clic en Editar:



Editar el perfil de autorización

## Configuración del Cliente

Paso 1. Cree un perfil XML mediante el editor de perfiles XML. Este ejemplo es el utilizado para la creación de este documento:

```
<#root>
```

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreLinux>All</CertificateStoreLinux>
    <CertificateStoreOverride>true</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4, IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">
      true
    </AutoReconnect>
    <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
    <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEExclusion UserControllable="false">
      Disable
    </PPPEExclusion>
    <PPPEExclusionServerIP UserControllable="false"/>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">
      false
    </EnableAutomaticServerSelection>
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    <RetainVpnOnLogoff>false </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>true</AllowManualHostInput>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>
FlexVPN HUB
      </HostName>
      <HostAddress>
```

192.168.50.225

```
</HostAddress>  
<PrimaryProtocol>
```

**IPsec**

```
<StandardAuthenticationOnly>  
true  
<AuthMethodDuringIKENegotiation>
```

**EAP-MD5**

```
</AuthMethodDuringIKENegotiation>  
<IKEIdentity>
```

**cisco.example**

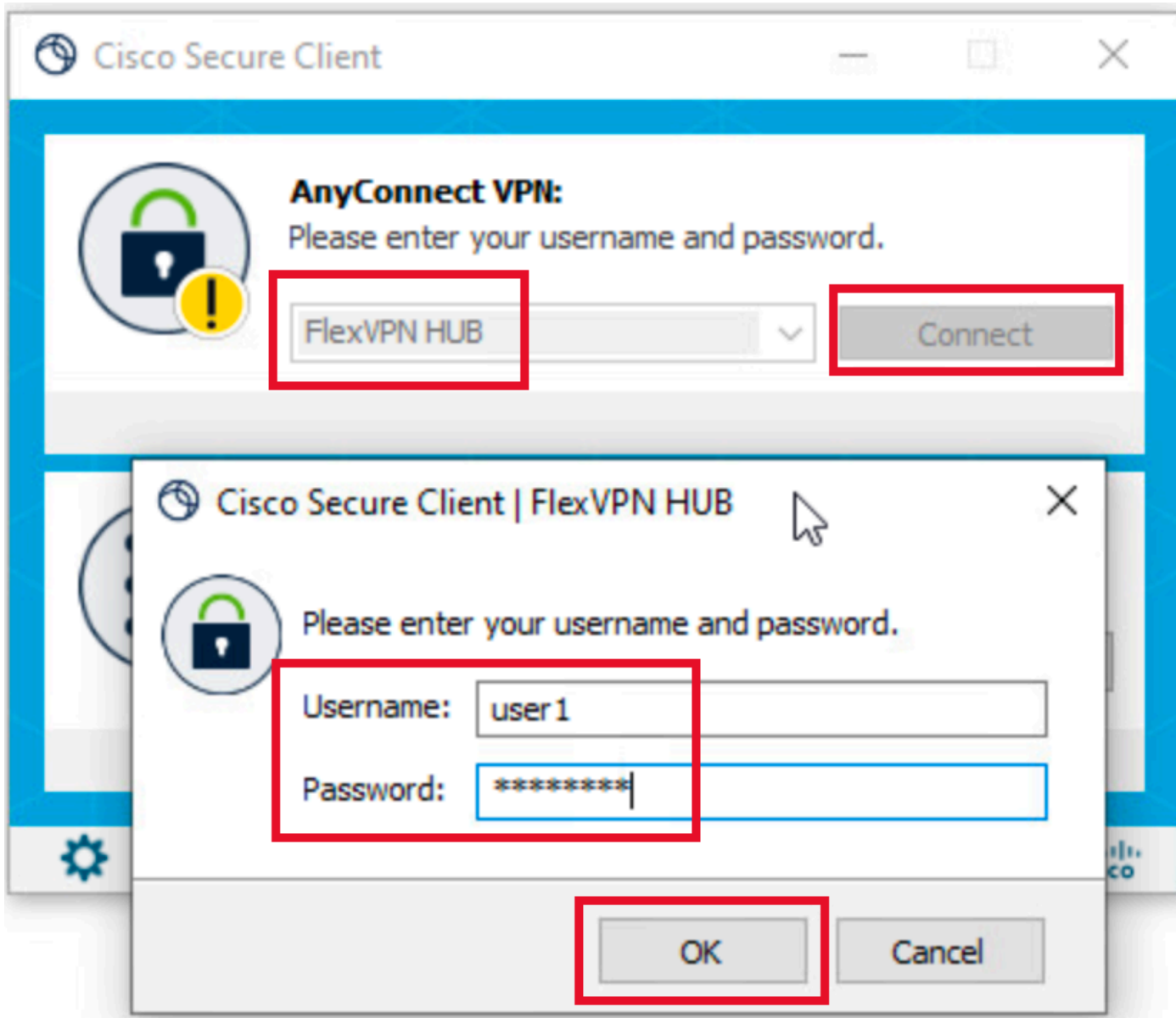
```
</IKEIdentity>  
</StandardAuthenticationOnly>  
</PrimaryProtocol>  
</HostEntry>  
</ServerList>  
</AnyConnectProfile>
```

- **<HostName>**: alias utilizado para hacer referencia al host, la dirección IP o el nombre de dominio completo (FQDN). Se muestra en el cuadro CSC.
- **<HostAddress>**: dirección IP o FQDN del hub FlexVPN.
- **<PrimaryProtocol>** - Se debe establecer en IPsec para forzar al cliente a utilizar IKEv2/IPsec en lugar de SSL.
- **<AuthMethodDuringIKENegotiation>** - Se debe establecer para utilizar EAP-MD5 en EAP. Esto es necesario para la autenticación en el servidor ISE.
- **<IKEIdentity>** - Esta cadena es enviada por el cliente como la carga útil de ID de tipo ID\_GROUP. Esto se puede utilizar para hacer coincidir el cliente con un perfil IKEv2 específico en el hub.

## Verificación

Paso 1. Vaya al equipo cliente donde está instalado CSC. Conéctese al hub FlexVPN e introduzca las credenciales user1:





Credenciales de usuario1

Paso 2. Una vez establecida la conexión, haga clic en el icono del engranaje (esquina inferior izquierda) y navegue hasta AnyConnectVPN > Statistics. Confirme en la sección Información de Dirección que la dirección IP asignada pertenece al conjunto configurado para el grupo 1:

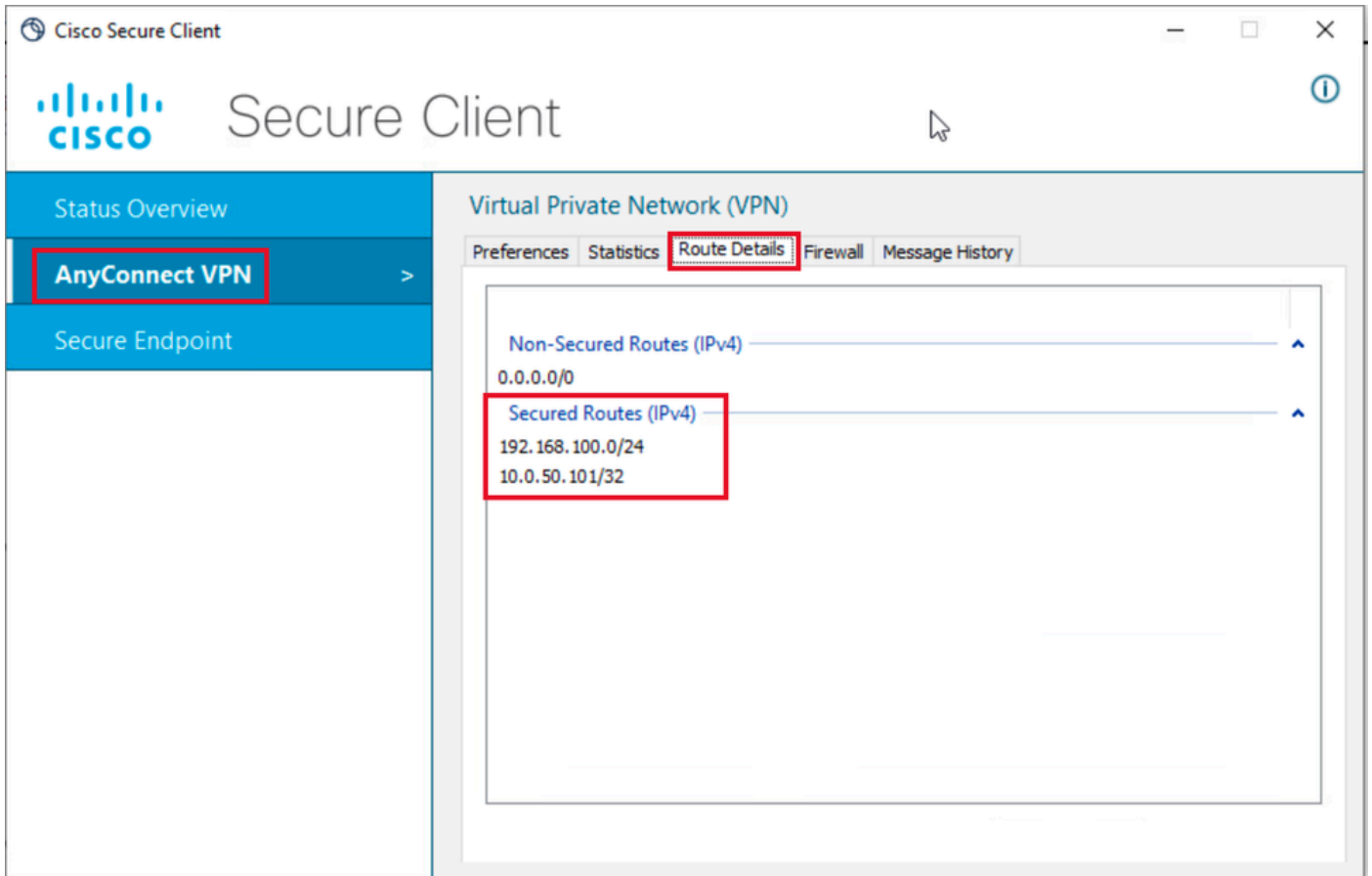
The screenshot shows the Cisco Secure Client interface. On the left, a navigation pane includes 'Status Overview', 'AnyConnect VPN' (highlighted with a red box), and 'Secure Endpoint'. The main window is titled 'Virtual Private Network (VPN)' and has tabs for 'Preferences', 'Statistics' (highlighted with a red box), 'Route Details', 'Firewall', and 'Message History'. The 'Statistics' tab is active, showing 'Connection Information' and 'Address Information' sections. The 'Address Information' section is also highlighted with a red box and contains the following data:

| Address Information |               |
|---------------------|---------------|
| Client (IPv4):      | 172.16.10.5   |
| Client (IPv6):      | Not Available |
| Server:             | [Redacted]    |

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

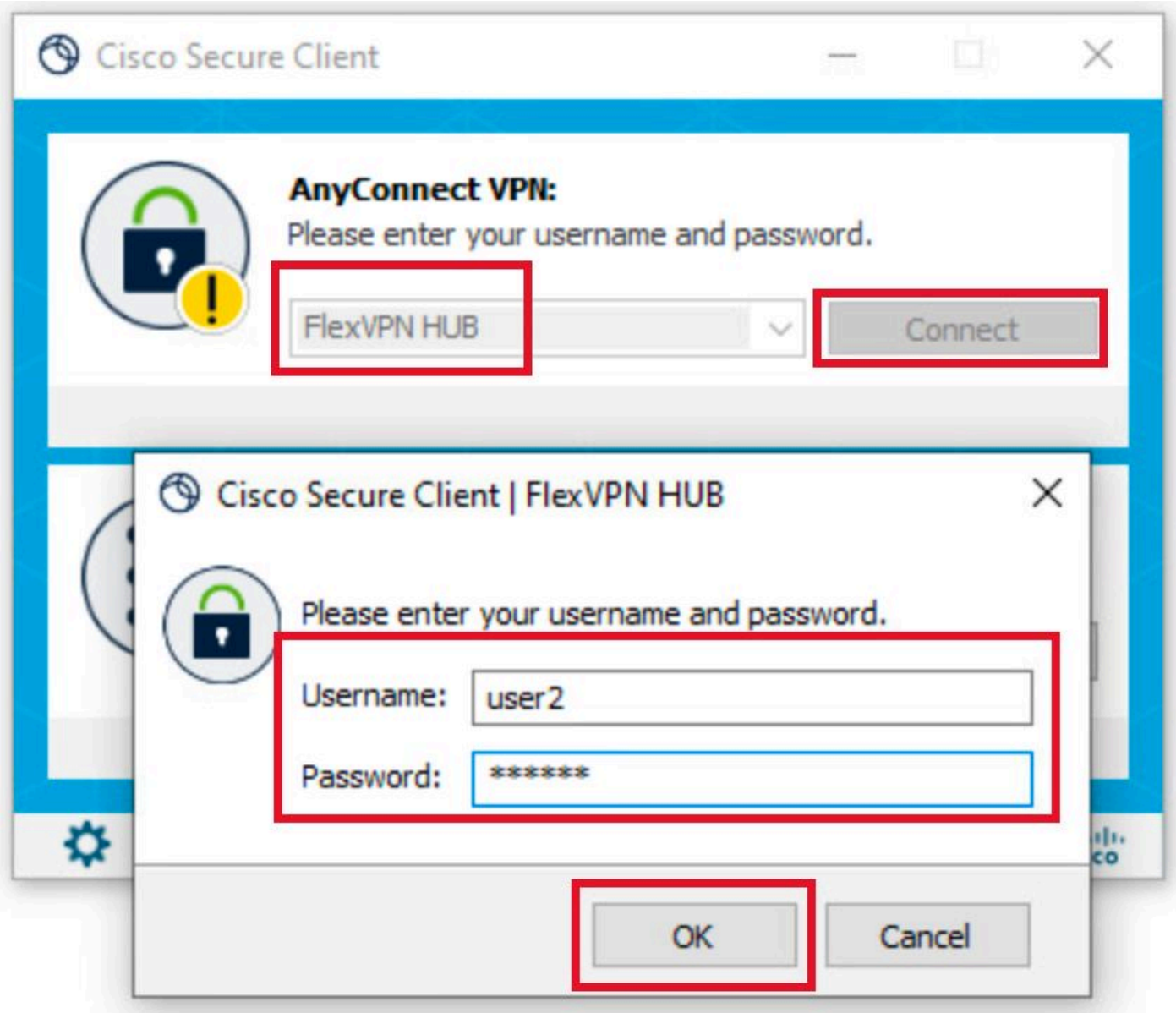
Estadísticas de usuario1

Navigate to AnyConnectVPN > Route details and confirm that the information displayed corresponds to the secure routes and the DNS configured for group 1:



Detalles de la ruta Usuario1

Paso 3. Repita los pasos 1 y 2 con las credenciales del usuario 2 para comprobar que la información coincide con los valores configurados en la política de autorización de ISE para este grupo:



Credenciales de usuario 2

Cisco Secure Client

# Secure Client

Status Overview

**AnyConnect VPN**

Secure Endpoint

## Virtual Private Network (VPN)

Preferences **Statistics** Route Details Firewall Message History

**Connection Information**

|                              |                                   |
|------------------------------|-----------------------------------|
| State:                       | Connected                         |
| Tunnel Mode (IPv4):          | Split Include                     |
| Tunnel Mode (IPv6):          | Drop All Traffic                  |
| Dynamic Tunnel Exclusion:    | None                              |
| Dynamic Tunnel Inclusion:    | None                              |
| Duration:                    | 00:00:12                          |
| Session Disconnect:          | None                              |
| Management Connection State: | Disconnected (user tunnel active) |

**Address Information**

|                |               |
|----------------|---------------|
| Client (IPv4): | 172.16.20.5   |
| Client (IPv6): | Not Available |
| Server:        |               |

Bytes

Reset Export Stats

Estadísticas de usuario2

Cisco Secure Client

# Secure Client

Status Overview

**AnyConnect VPN**

Secure Endpoint

## Virtual Private Network (VPN)

Preferences Statistics **Route Details** Firewall Message History

**Non-Secured Routes (IPv4)**

0.0.0.0/0

**Secured Routes (IPv4)**

|                  |
|------------------|
| 192.168.200.0/24 |
| 10.0.50.202/32   |

Detalles de la ruta Usuario2

# Troubleshoot

## Depuraciones y registros

En el router de Cisco:

1. Utilice las depuraciones de IKEv2 e IPsec para verificar la negociación entre la cabecera y el cliente:

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. Utilice los debugs AAA para verificar la asignación de atributos locales y/o remotos:

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

En ISE:

- Registros en directo de RADIUS

## Escenario de trabajo

Los siguientes resultados son ejemplos de conexiones exitosas:

- Salida de depuración de User1:

<#root>

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
```

```
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
```

```
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
```

```
Jan 30 02:57:21.088: vrfid: [65535] ipv6 tableid : [0]
```

```
Jan 30 02:57:21.088: idb is NULL
```

```
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IPv6: ::
```

Jan 30 02:57:21.089: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.089: RADIUS(000000FF): sending  
Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.089: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229

RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34  
Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.089: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12  
RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1]  
Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18  
RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II\*?0"  
Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.089: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.090: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.094: RADIUS:

Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5  
Jan 30 02:57:21.094: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8  
RADIUS: 01 52 00 06 0D 20 [ R ]  
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18  
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@0XH6]  
Jan 30 02:57:21.094: RADIUS(000000FF): Received from id 1645/85  
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes  
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (000000FF):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC  
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0  
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 02:57:21.097: idb is NULL

Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::  
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.097: RADIUS(000000FF): sending  
Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.097: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC

Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.098: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8  
RADIUS: 02 52 00 06 03 04 [ R]  
Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18  
RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g\$D&d]  
Jan 30 02:57:21.098: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.101: RADIUS:

Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1

Jan 30 02:57:21.101: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32  
RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC 0F B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai  
Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18  
RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL!]  
Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86  
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes  
Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):



Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC  
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 02:57:21.103: RADIUS(000000FF): Config NAS IP: 0.0.0.0  
Jan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 02:57:21.104: idb is NULL  
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::  
Jan 30 02:57:21.104: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.104: RADIUS(000000FF): sending  
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.104: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332

RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46  
Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.104: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24  
RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/]  
Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18  
RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>Tv]  
Jan 30 02:57:21.104: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.170: RADIUS:

Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233

RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6  
Jan 30 02:57:21.170: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.170: RADIUS: Class [25] 68  
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]

```
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]
RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams()]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31
```

```
"ipsec:dns-servers=10.0.50.101"
```

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41
```

```
"ipsec:route-set=prefix 192.168.100.0/24"
```

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24
```

```
"ipsec:addr-pool=group1"
```

```
Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f
Jan 30 02:57:21.175: AAA/AUTHOR (0x100):
```

```
Pick method list 'FlexVPN-Authorization-List'
```

```
Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
Jan 30 02:57:21.192: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:
```

```
Line protocol on Interface Virtual-Access1, changed state to up
```

- Resultado de depuración de usuario 2:

```
<#root>
```

```
Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f
Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.103: RADIUS(00000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229

RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64

Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]

Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26

Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"

Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36

Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"

Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64

Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"

Jan 30 03:28:58.104: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21

Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"

Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12

RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]

Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18

RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]

Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100

Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet

Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout

Jan 30 03:28:58.109: RADIUS:

Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43

Jan 30 03:28:58.109: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8

RADIUS: 01 35 00 06 0D 20 [ 5 ]

Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18

RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]

Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88

RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes

Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC

Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-

Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0

Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]

Jan 30 03:28:58.113: idb is NULL

Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: ::

Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct\_session\_id: 4249

Jan 30 03:28:58.113: RADIUS(00000103): sending

Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1

Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded

Jan 30 03:28:58.113: RADIUS(00000103):

Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316

RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C

Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30

"isakmp-phrase1-id=cisco.example"

Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"

Jan 30 03:28:58.113: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"

Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8

RADIUS: 02 35 00 06 03 04 [ 5]

Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18

RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]

Jan 30 03:28:58.113: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100

Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet

Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout

Jan 30 03:28:58.116: RADIUS:

Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02

Jan 30 03:28:58.116: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32

RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM]

Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18

RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]

Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89

RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes

Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-

Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0

Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0]

Jan 30 03:28:58.118: idb is NULL  
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: ::  
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct\_session\_id: 4249  
Jan 30 03:28:58.118: RADIUS(00000103): sending  
Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded  
Jan 30 03:28:58.119: RADIUS(00000103):

Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332

RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE  
Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"  
Jan 30 03:28:58.119: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24  
RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w]  
Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18  
RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo]  
Jan 30 03:28:58.119: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]  
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]  
Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet  
Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout  
Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233  
RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD  
Jan 30 03:28:58.186: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.186: RADIUS: Class [25] 68  
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]  
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]  
RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE]  
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]  
RADIUS: 33 30 [ 30]  
Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6  
RADIUS: 03 36 00 04 [ 6]  
Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18  
RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S]  
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37  
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31

"ipsec:dns-servers=10.0.50.202"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47

Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.200.0/24"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30

Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group2"

Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90

RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes

Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f

Jan 30 03:28:58.190: AAA/AUTHOR (0x104):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to

Jan 30 03:28:58.209: %SYS-5-CONFIG\_P: Configured programmatically by process Crypto INT from console as

Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access2, changed state to up

## Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).