

FlexVPNリモートユーザのためのRADIUS属性マッピングの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ルータの設定](#)

[Identity Services Engine \(ISE\) の設定](#)

[クライアントの設定](#)

[確認](#)

[トラブルシューティング](#)

[デバッグとログ](#)

[正常動作シナリオ](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)を使用してIDを確認し、属性グループマッピングを実行するようにFlexVPNを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CLIを介したCisco IOS® XEルータ上でのIKEV2/IPsec設定によるリモートアクセス仮想プライベートネットワーク(RAVPN)
- Cisco Identity Services Engine(ISE)の設定
- Cisco Secure Client(CSC)
- RADIUS プロトコル

使用するコンポーネント

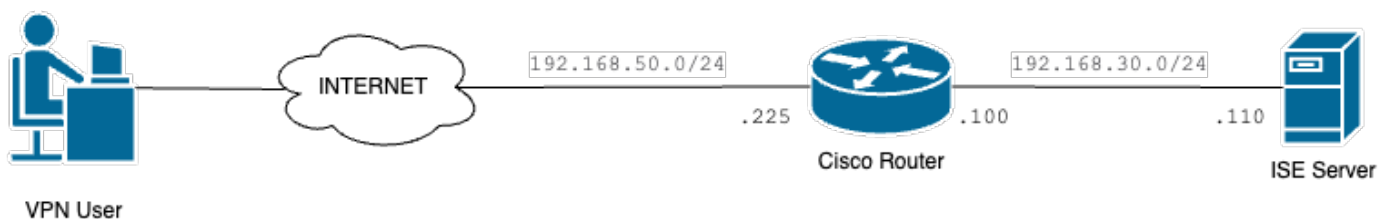
このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco CSR1000V(VXE) : バージョン17.03.04a
- Cisco Identity Services Engine(ISE) - 3.1
- Cisco Secure Client(CSC) : バージョン5.0.05040
- Windows 11

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



基本的なネットワーク図

コンフィギュレーション

ルータの設定

ステップ 1 : デバイスで認証およびローカル認可を行うようにRADIUSサーバを設定します。

```
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
```

aaa authentication login <list_name> (オプション) コマンドは、認証、許可、アカウントイング (AAA)グループ (RADIUSサーバを定義する) を参照します。

aaa authorization network <list_name> localコマンドは、ローカルに定義されたユーザ/グループを使用する必要があることを明示します。

手順2:ルータ証明書を保存するトラストポイントを設定する。ルータのローカル認証のタイプはRSAであるため、デバイスではサーバが証明書を使用して自身を認証する必要があります。

```
crypto pki trustpoint FlexVPN-TP
```

```
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
revocation-check none
rsakeypair FlexVPN_KEY
```

ステップ 3 : 異なるユーザグループごとにIPローカルプールを定義します。

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

ステップ 4 : ローカル認可ポリシーを設定します。

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

ユーザが属するグループに基づいて関連する値 (DNS、プール、保護ルートなど) を送信する責任を認証サーバが負うため、認証ポリシーの設定は必要ありません。ただし、ローカル認証データベースでユーザ名を定義するように設定する必要があります。

ステップ 5 (オプション) : IKEv2プロポーザルとポリシーを作成します (設定されていない場合は、スマートデフォルトが使用されます) 。

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

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

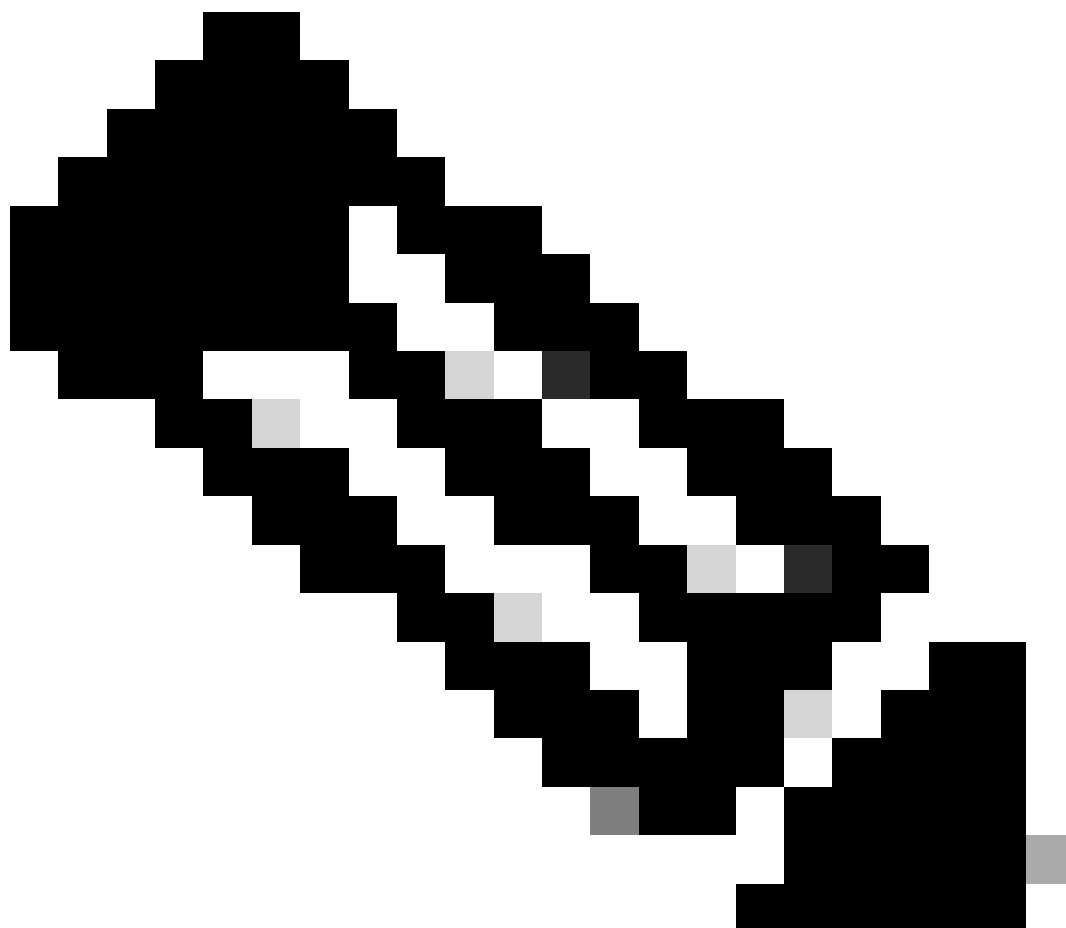
ステップ 6 (オプション) : トランスフォームセットを設定します (設定しない場合は、スマートデフォルトが使用されます) 。

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

手順 7 : 適切なローカルおよびリモートID、認証方式 (ローカルおよびリモート) 、トラストポイント、AAA、および接続に使用される仮想プレートインターフェイスを使用して、IKEv2プロファイルを設定します。

```
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
```

aaa authorization user eap cached コマンドは、EAP認証中に受信した属性をキャッシュする必要があることを指定します。このコマンドがないと認証サーバから送信されたデータが使用されず、接続が失敗するため、このコマンドは設定に不可欠です。



注：リモートキーIDは、XMLファイルのキーID値と一致する必要があります。XMLファイルで変更されていない場合は、デフォルト値(*\$AnyConnectClient\$)が使用され、IKEv2プロファイルで設定する必要があります。

ステップ 8 : IPsecプロファイルを設定し、トランスフォームセットとIKEv2プロファイルを割り当てます。

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

ステップ 9 : ループバックインターフェイスを設定します。バーチャルアクセスインターフェイスは、そこからIPアドレスを借ります。

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

ステップ 10 : さまざまなバーチャルアクセスインターフェイスの作成に使用するバーチャルテンプレートを作成し、手順8で作成したIPSecプロファイルをリンクします。

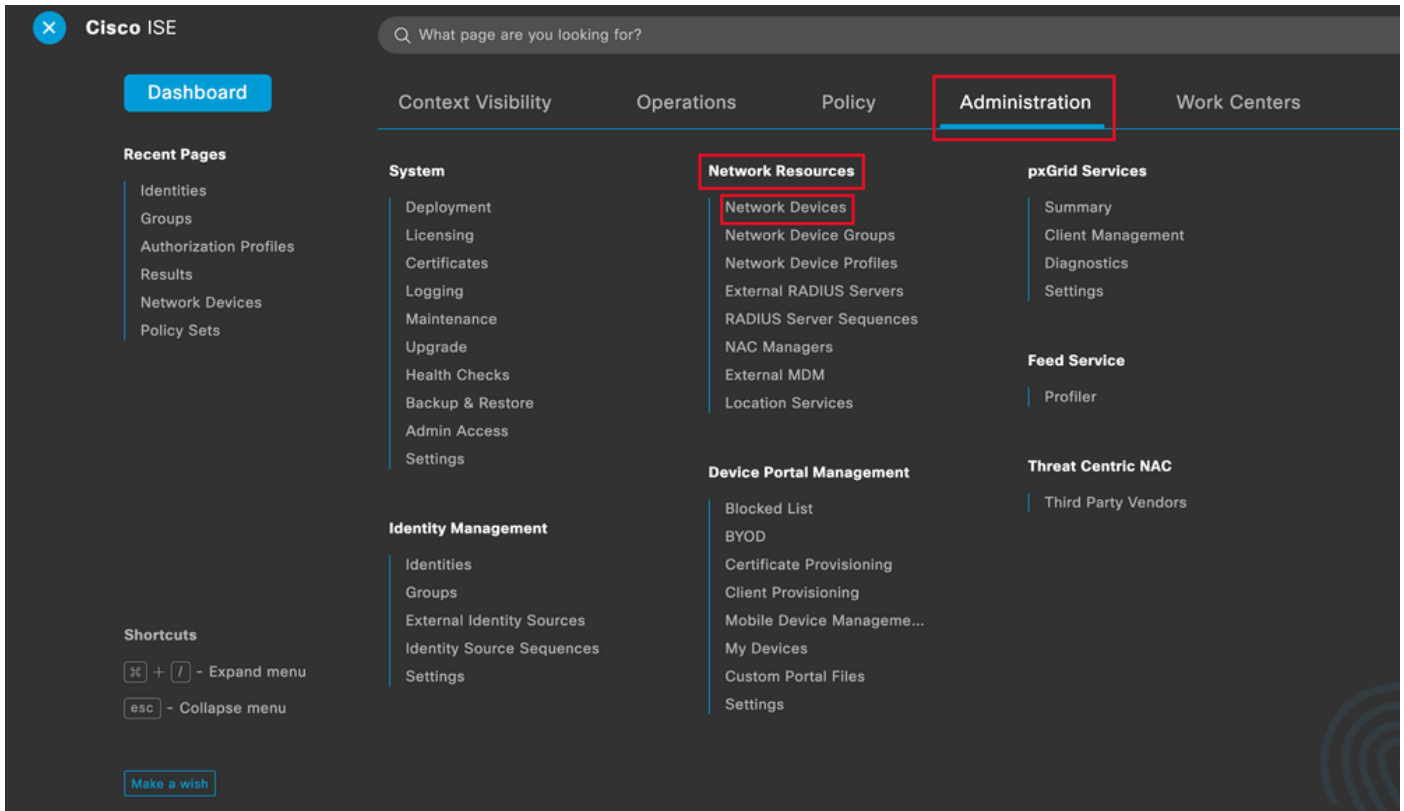
```
interface Virtual-Template100 type tunnel
ip unnumbered Loopback100
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

ステップ 11ルータでHTTP-URLベースの証明書検索とHTTPサーバを無効にします。

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

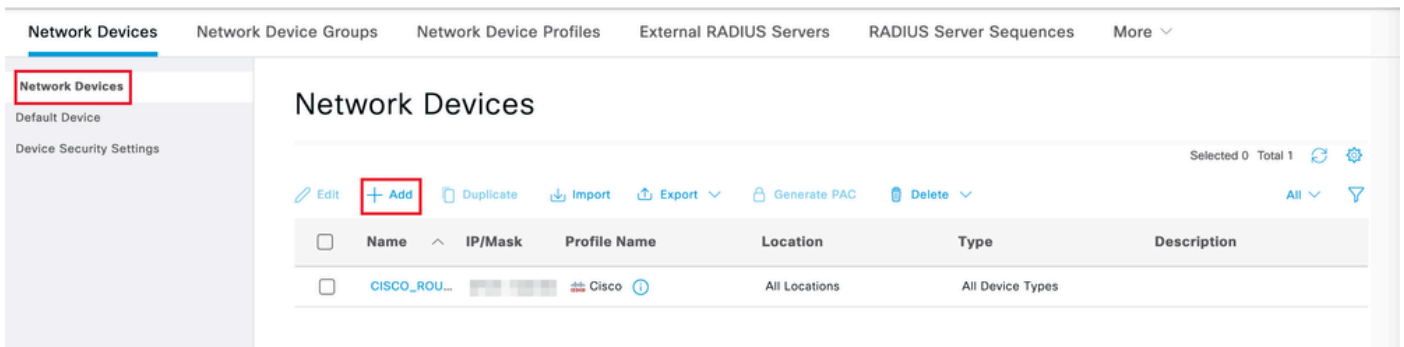
Identity Services Engine (ISE) の設定

ステップ 1 : ISEサーバにログインし、Administration > Network Resources > Network Devicesの順に移動します。



ISE一般メニュー

ステップ 2 : Addをクリックして、ルータをAAAクライアントとして設定します。



新しいネットワークデバイスの追加

ネットワークデバイスのNameフィールドとIP Addressフィールドを入力し、RADIUS Authentication Settingsボックスにチェックマークを入れて、Shared Secretを追加します。この値は、ルータ上にRADIUSサーバオブジェクトを作成したときに使用した値と同じである必要があります。

Network Devices

Name	CISCO_ROUTER
------	--------------

Description	
-------------	--

IP Address	IP : 192.168.30.110 / 32	
------------	--------------------------	--

名前とIPアドレス

<input checked="" type="checkbox"/>	▼ RADIUS Authentication Settings
-------------------------------------	----------------------------------

RADIUS UDP Settings

Protocol RADIUS

Shared Secret	Show
---------------	-------	------

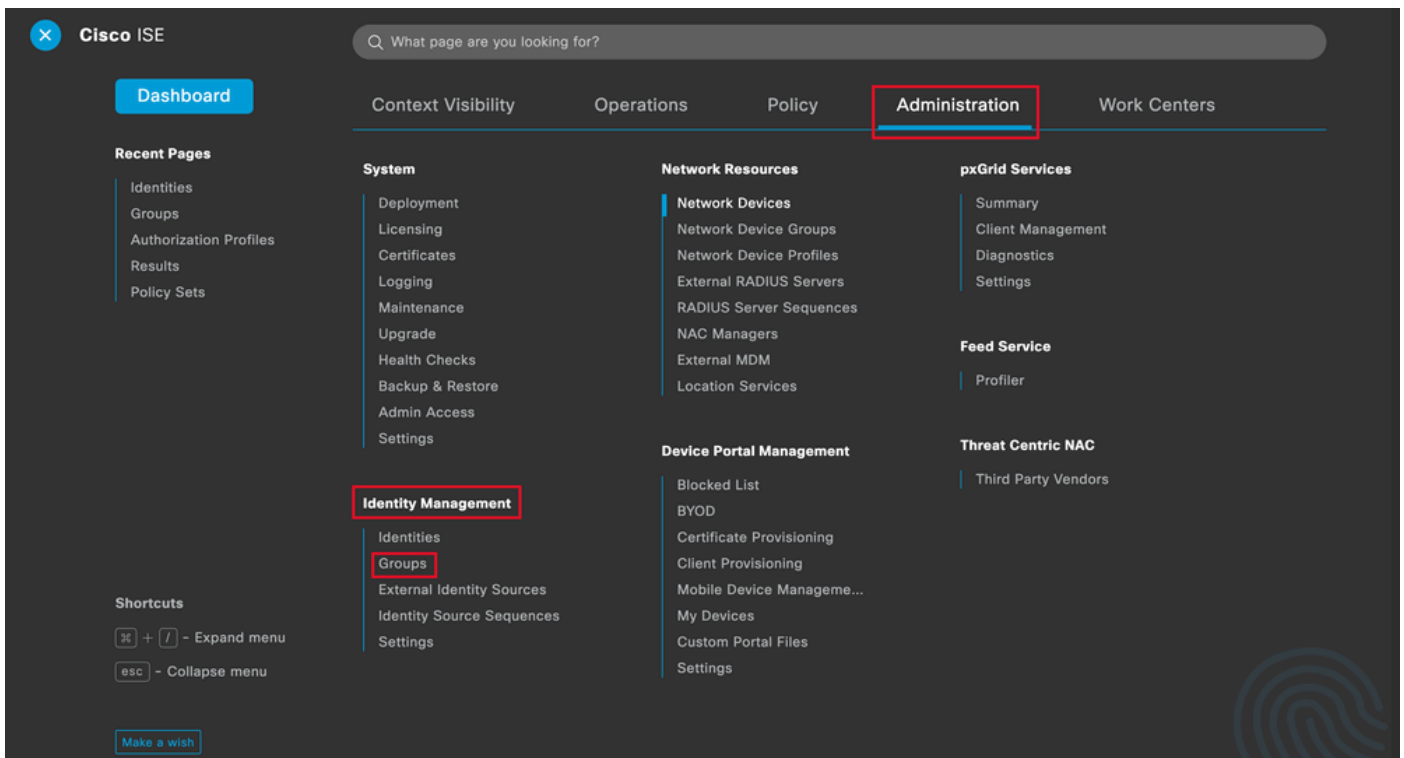
<input type="checkbox"/>	Use Second Shared Secret
--------------------------	--------------------------

networkDevices.secondSharedSecret [Show](#)

Radiusパスワード

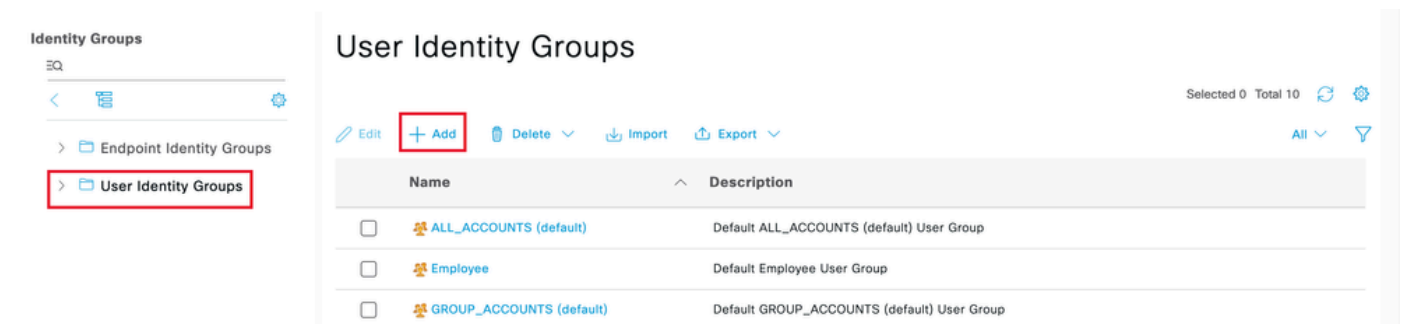
[Save] をクリックします。

ステップ 3 : Administration > Identity Management > Groupsの順に移動します。



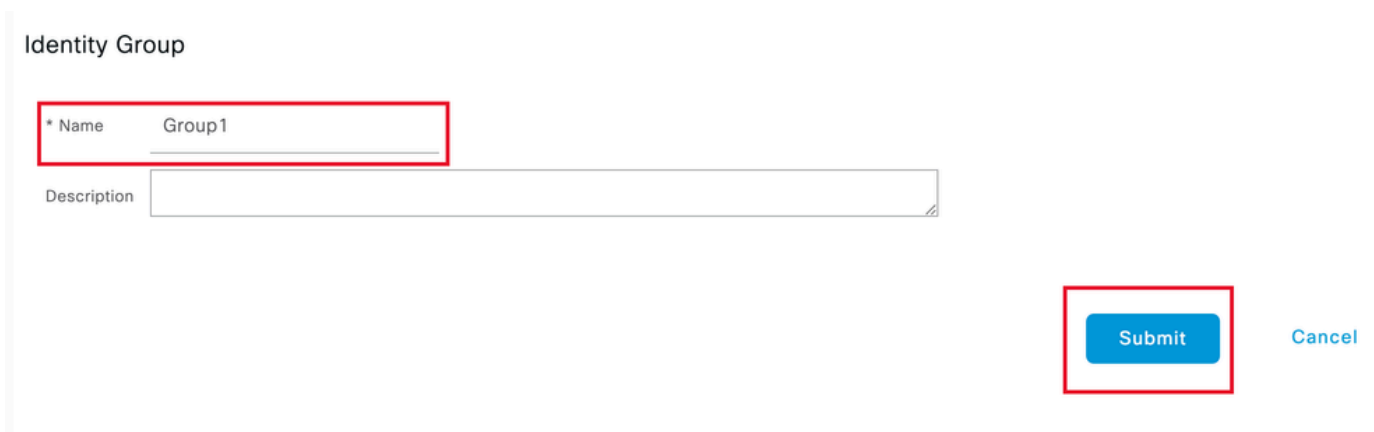
ISE一般メニュー

ステップ 4 : User Identity Groupsをクリックし、次にAddをクリックします。

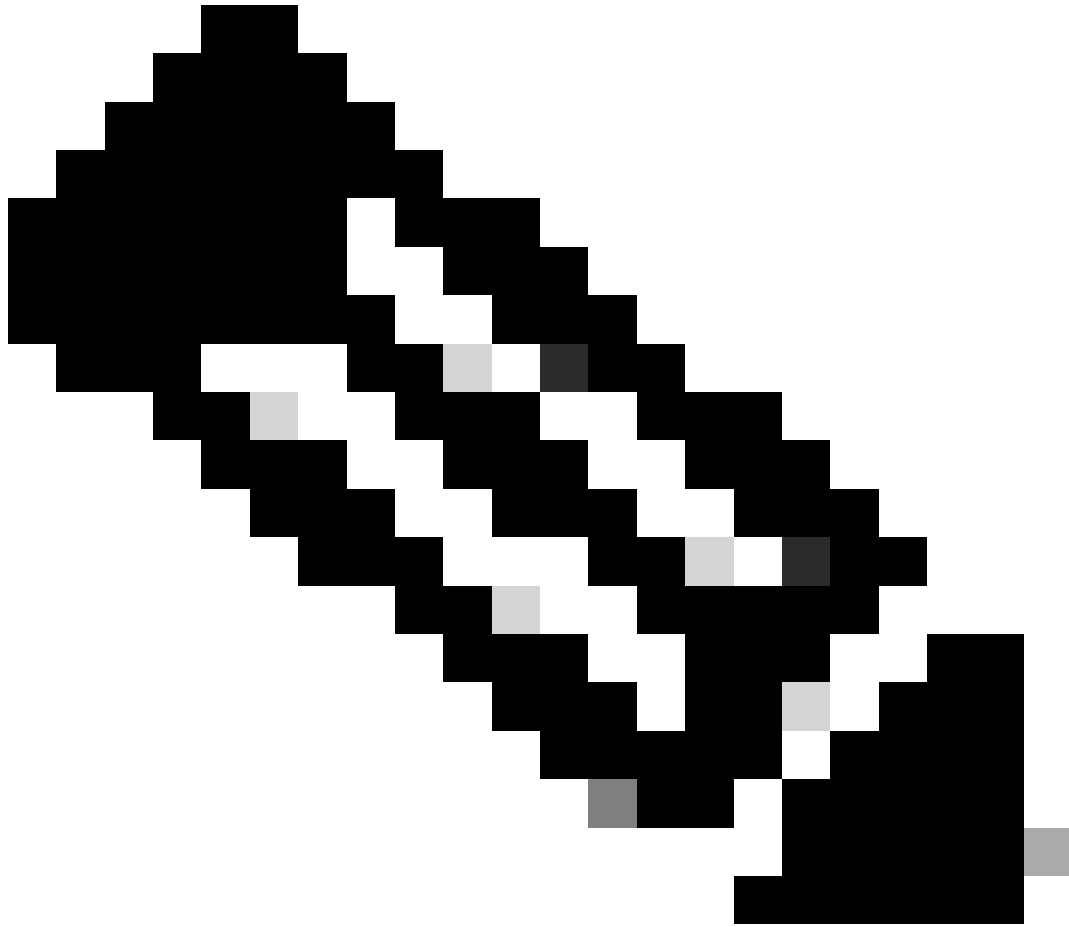


新しいグループの追加

グループNameを入力し、Submitをクリックします。

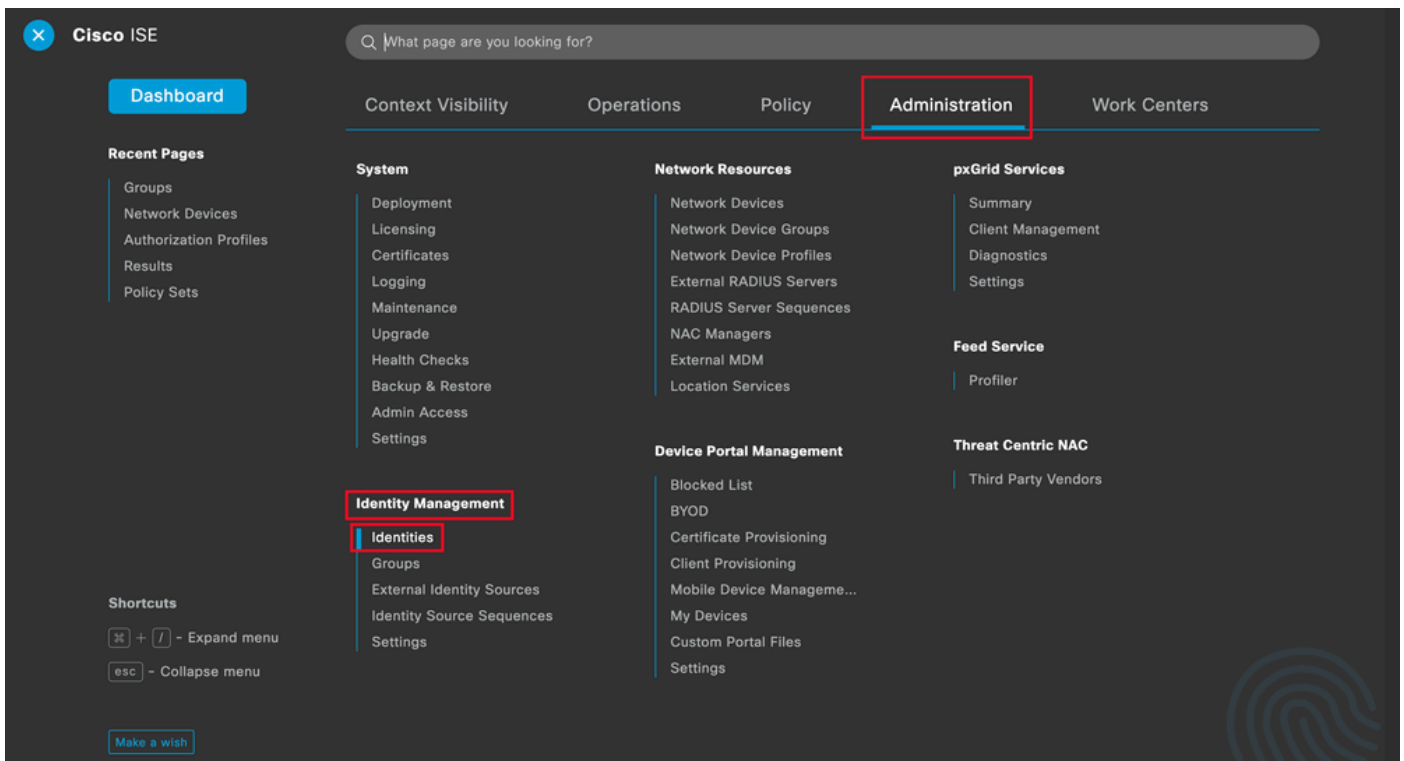


グループ情報



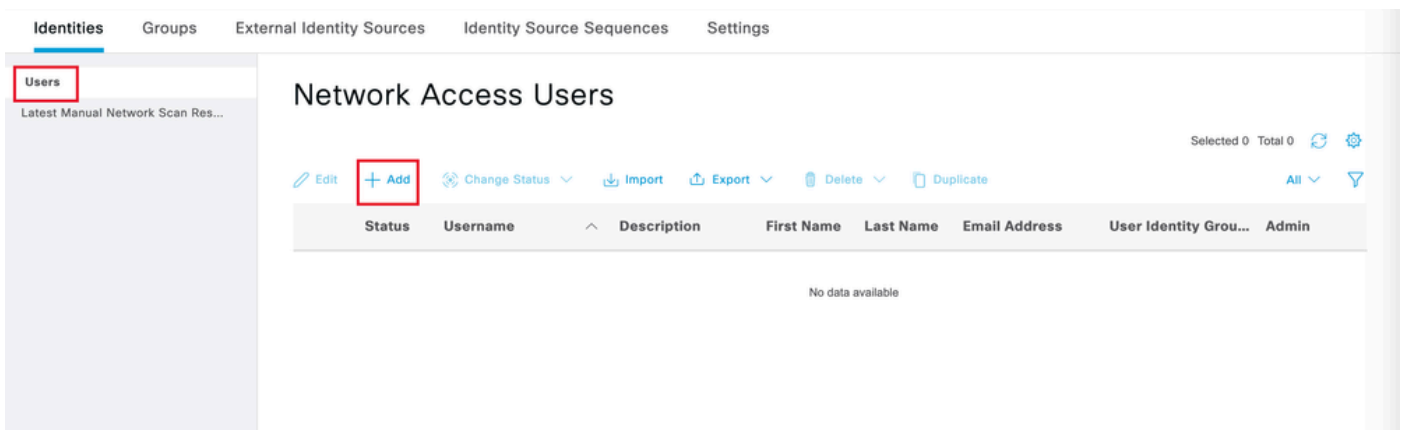
注：必要な数のグループを作成するには、手順3と4を繰り返します。

ステップ 5： Administration > Identity Management > Identitiesの順に移動します。



ISE一般メニュー

手順 6 : Addをクリックして、サーバローカルデータベースに新しいユーザを作成します。



ユーザの追加

ユーザ名とログインパスワードを入力します。次に、このページの最後に移動し、ユーザグループを選択します。

Network Access User

* Username

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

[Generate Password](#) ⓘ
[Generate Password](#) ⓘ

Enable Password

ユーザ名とパスワード

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 20

User Groups

User Groups

EQ

< [List Icon] [Settings Icon]

- ALL_ACCOUNTS (default)
- Employee
- Group1**
- Group2
- GROUP_ACCOUNTS (default)

⋮

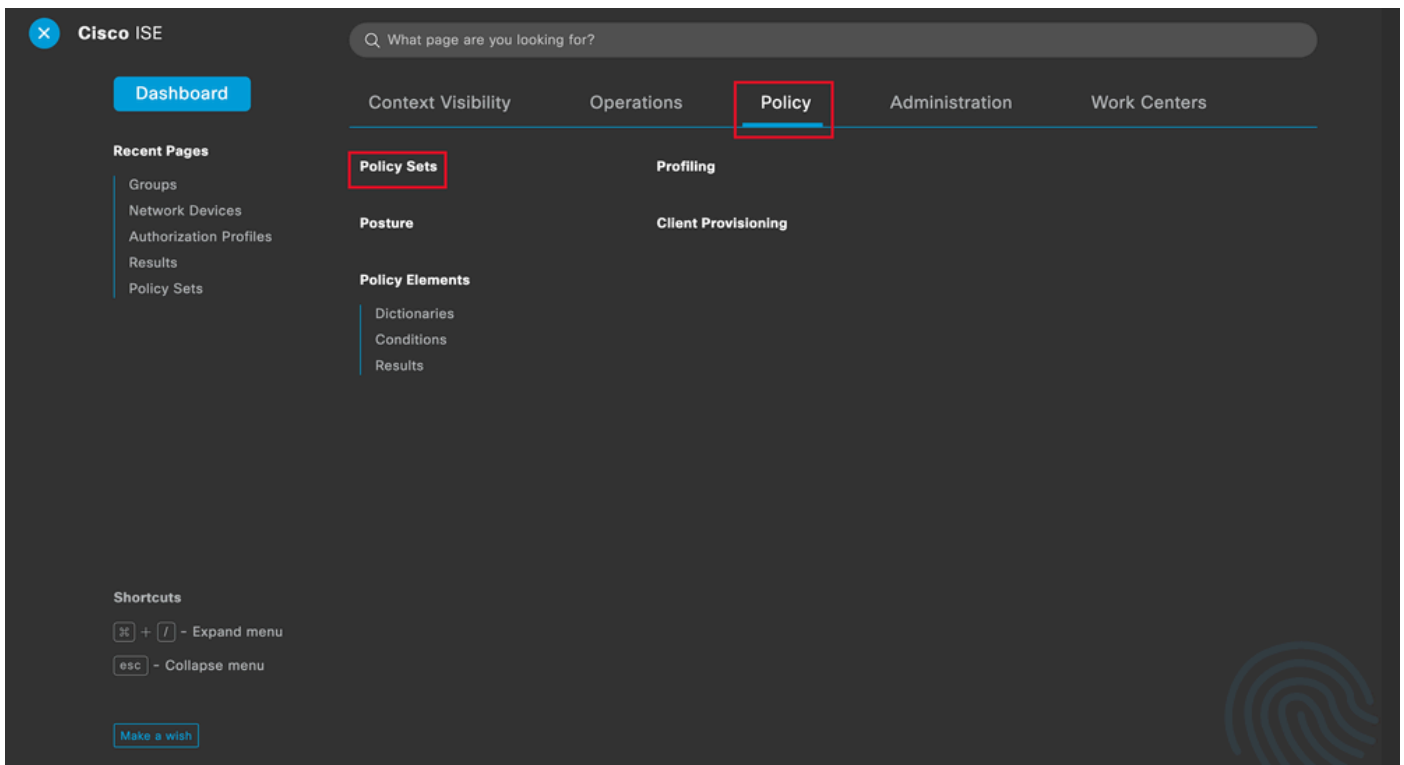
ユーザへの正しいグループの割り当て

[Save] をクリックします。



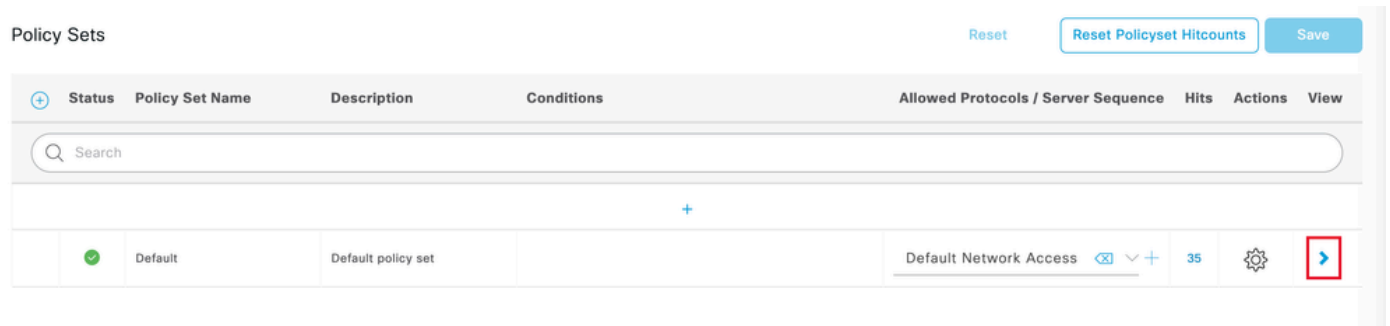
注：手順5と6を繰り返して、必要なユーザを作成し、対応するグループに割り当てます。

ステップ7:Policy > Policy Setsの順に移動します。



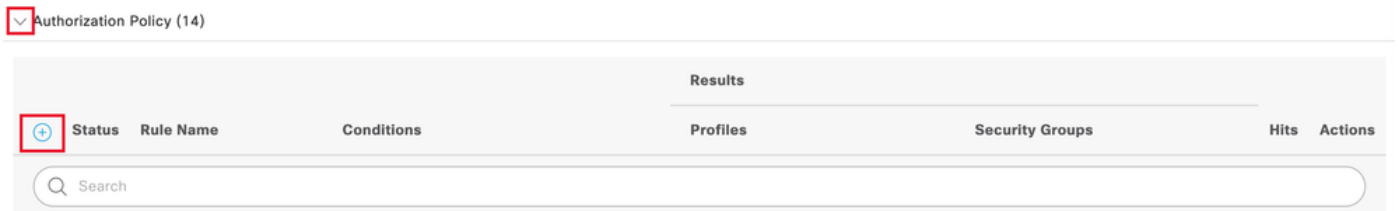
ISE一般メニュー

画面の右側にある矢印をクリックして、デフォルトの許可ポリシーを選択します。



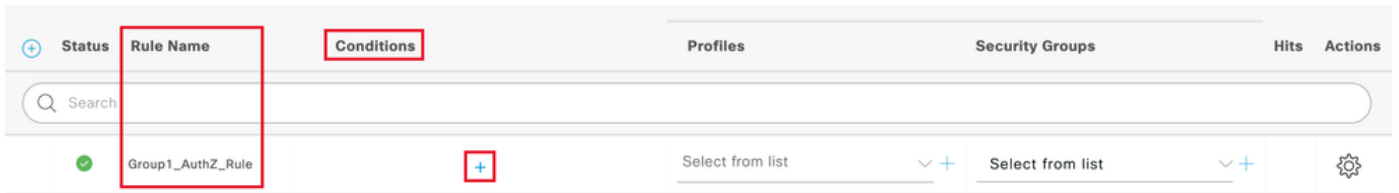
許可ポリシーの選択

ステップ 8 : Authorization Policyの横にあるドロップダウンメニューの矢印をクリックして展開します。次に、add (+)アイコンをクリックして新しいルールを追加します。



新しい許可ルールの追加

ルールの名前を入力し、Conditions列の下のadd (+)アイコンを選択します。



条件の追加

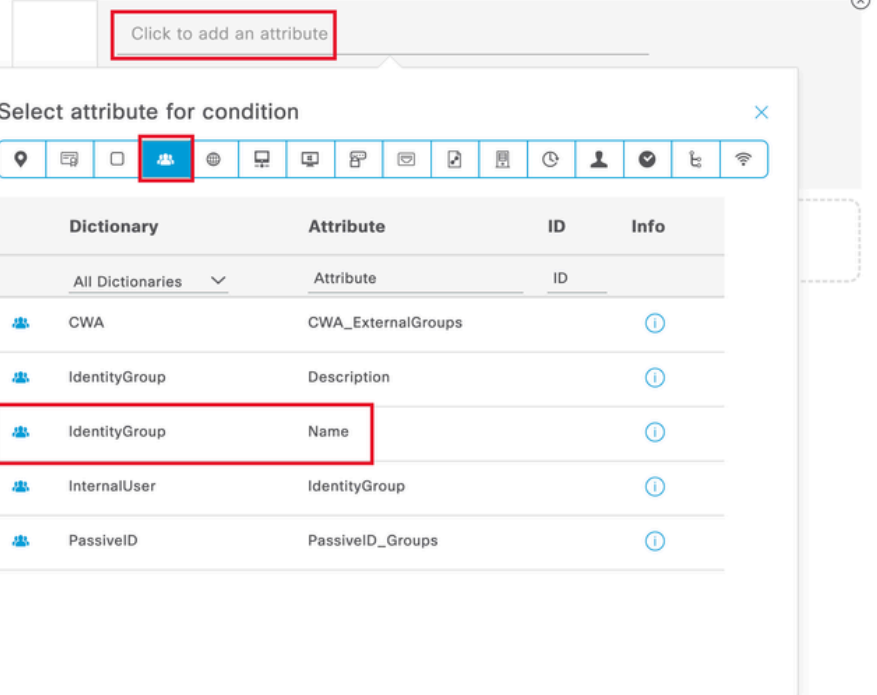
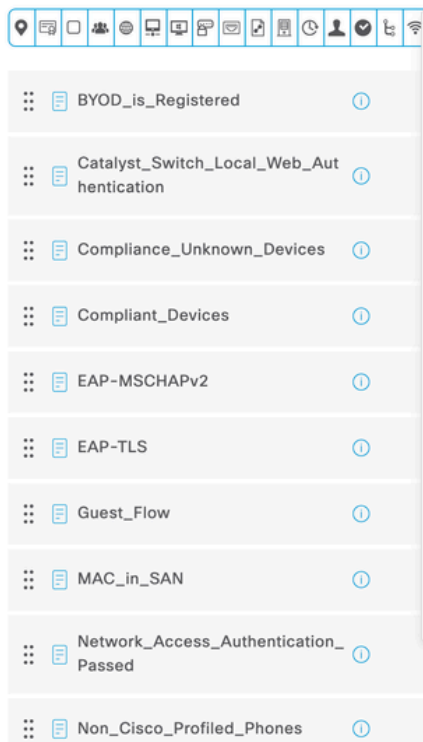
ステップ 9: アトリビュートエディタのテキストボックスをクリックし、Identityグループアイコンをクリックします。Identity group - Name 属性を選択します。

Conditions Studio

Library

Editor

Search by Name



条件の選択

次に、演算子としてEqualasを選択し、ドロップダウンメニューの矢印をクリックして使用可能なオプションを表示し、User Identity Groups:<GROUP_NAME>を選択します。

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

グループの選択

[Save] をクリックします。

ステップ10:Profiles列でadd (+)アイコンをクリックし、Create a New Authorization Profileを選択します。

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	Wireless_Access AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	Create a New Authorization Profile	Select from list	0	⚙️

許可プロファイルの作成

プロファイル名を入力します

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

プロフィール情報

このページの最後に移動してAdvanced Attribute Settingsに移動し、ドロップダウンメニュー矢印をクリックします。Ciscoをクリックして、cisco-av-pair--[1]を選択します。

Advanced Attributes Settings

Select an item

- 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

「属性タイプ」を選択

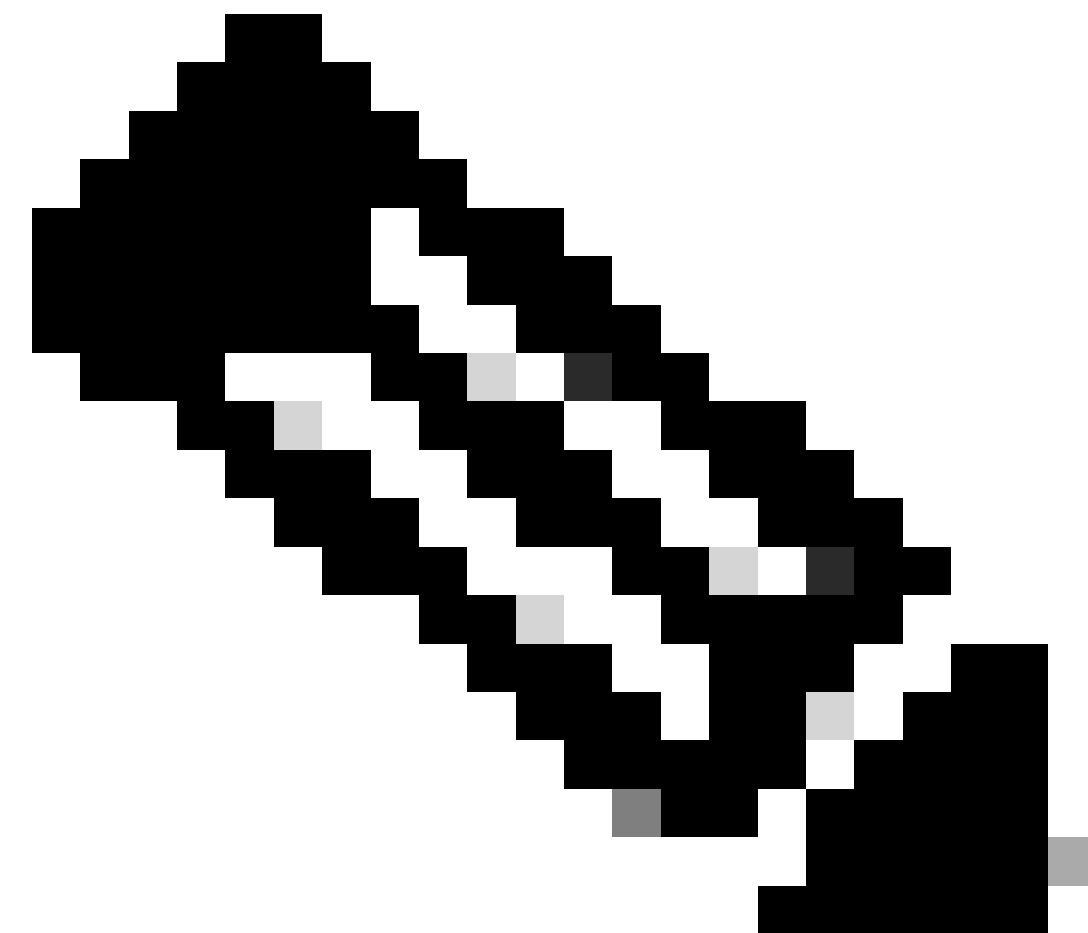
します。

設定するcisco-av-pair属性を追加し、追加(+)アイコンをクリックして別の属性を追加します。

Advanced Attributes Settings

☰ Cisco:cisco-av-pair ▼ = ipsec:dns-servers=10.0.50.10 ▼ - +

属性の設定



注：属性の仕様（名前、構文、説明、例など）については、FlexVPN RADIUS属性設定ガイドを参照してください。

[FlexVPNおよびインターネットキーエクスチェンジ\(IKE\)バージョン2コンフィギュレーションガイド、Cisco IOS XE Fuji 16.9.x：サポートされるRADIUS属性](#)



注：必要な属性を作成するには、前の手順を繰り返します。

[Save] をクリックします。

次に来る属性は各グループに割り当てられました。

- グループ1属性：

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

Group1属性

- グループ2属性 :

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

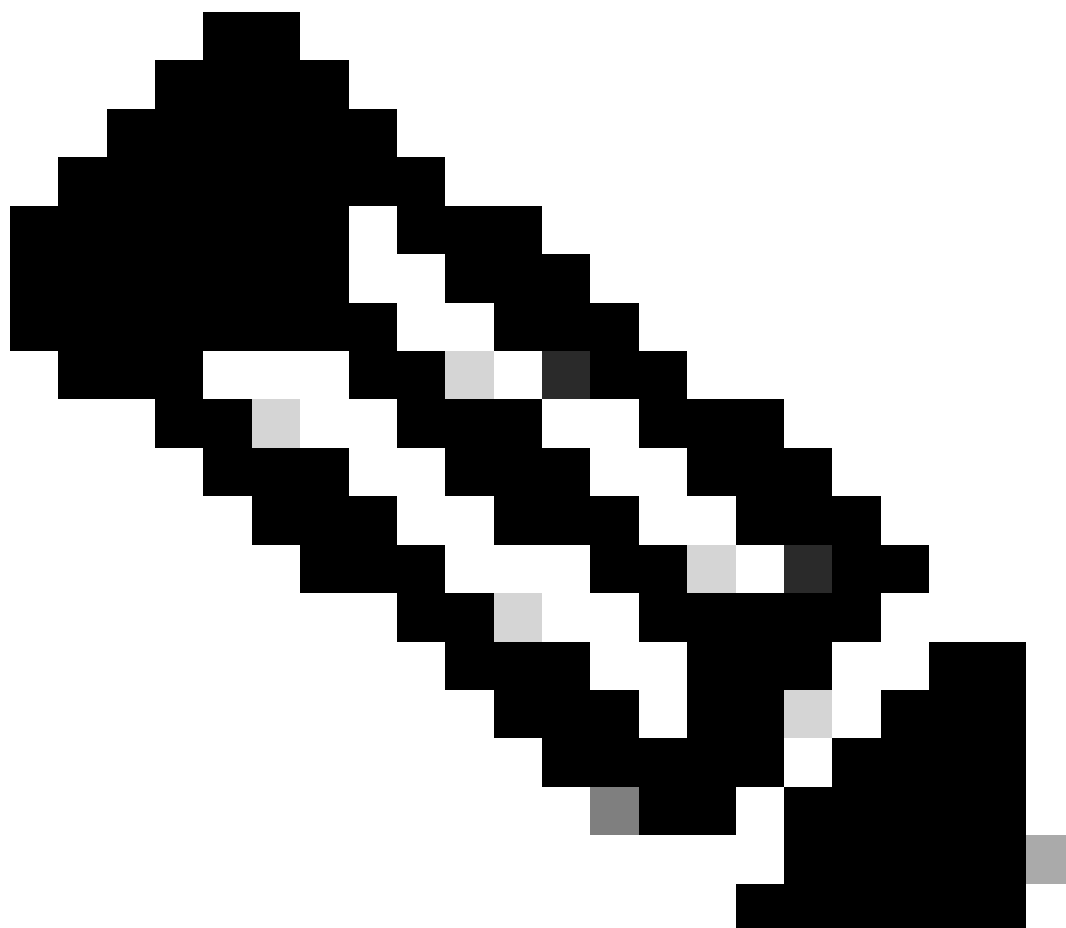
Group2属性

ステップ11 : ドロップダウンメニューの矢印をクリックし、ステップ10で作成した許可プロファイルを選択します。

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 Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	DenyAccess NSP_Onboard Non_Cisco_IP_Phones PermitAccess 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	⚙️

許可プロファイルの割り当て

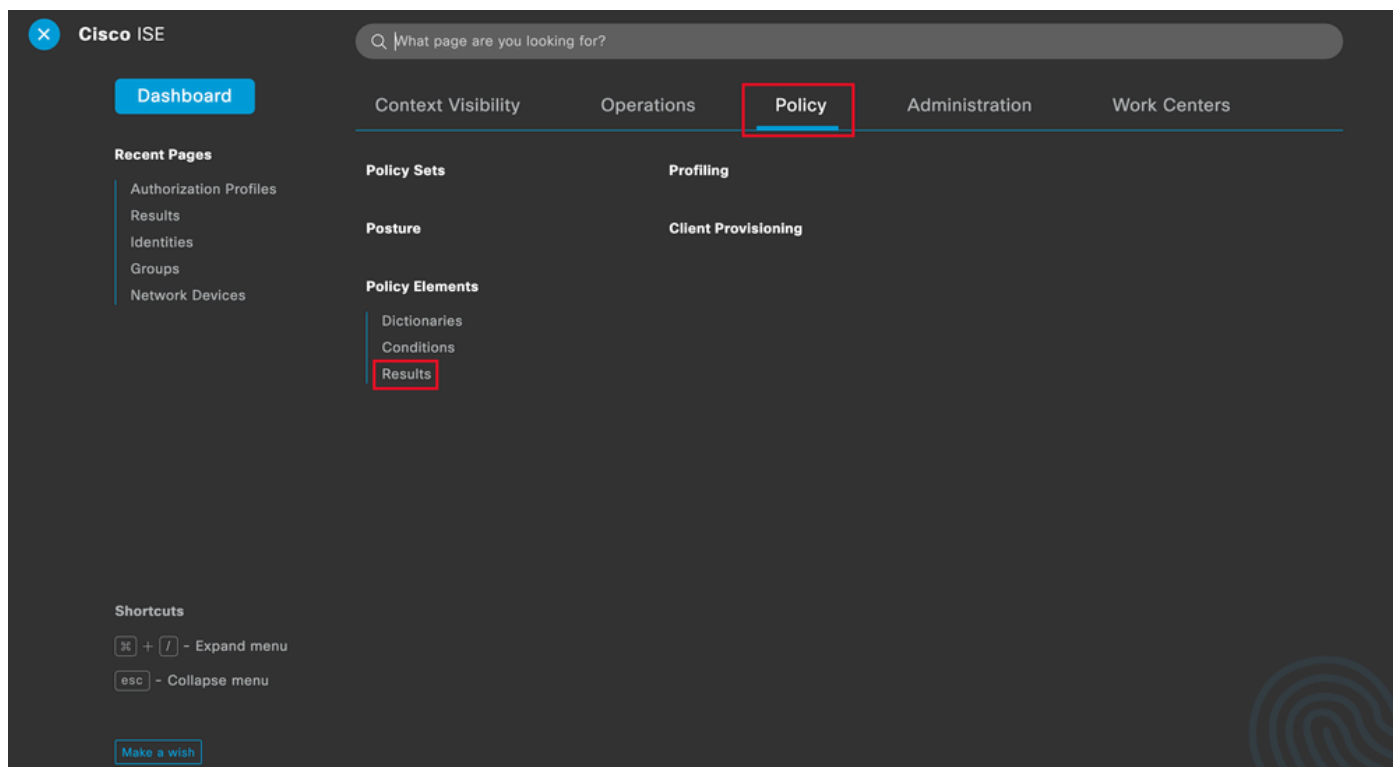
[Save] をクリックします。



注：ステップ8～11を繰り返して、各グループに必要な認可ルールを作成します。

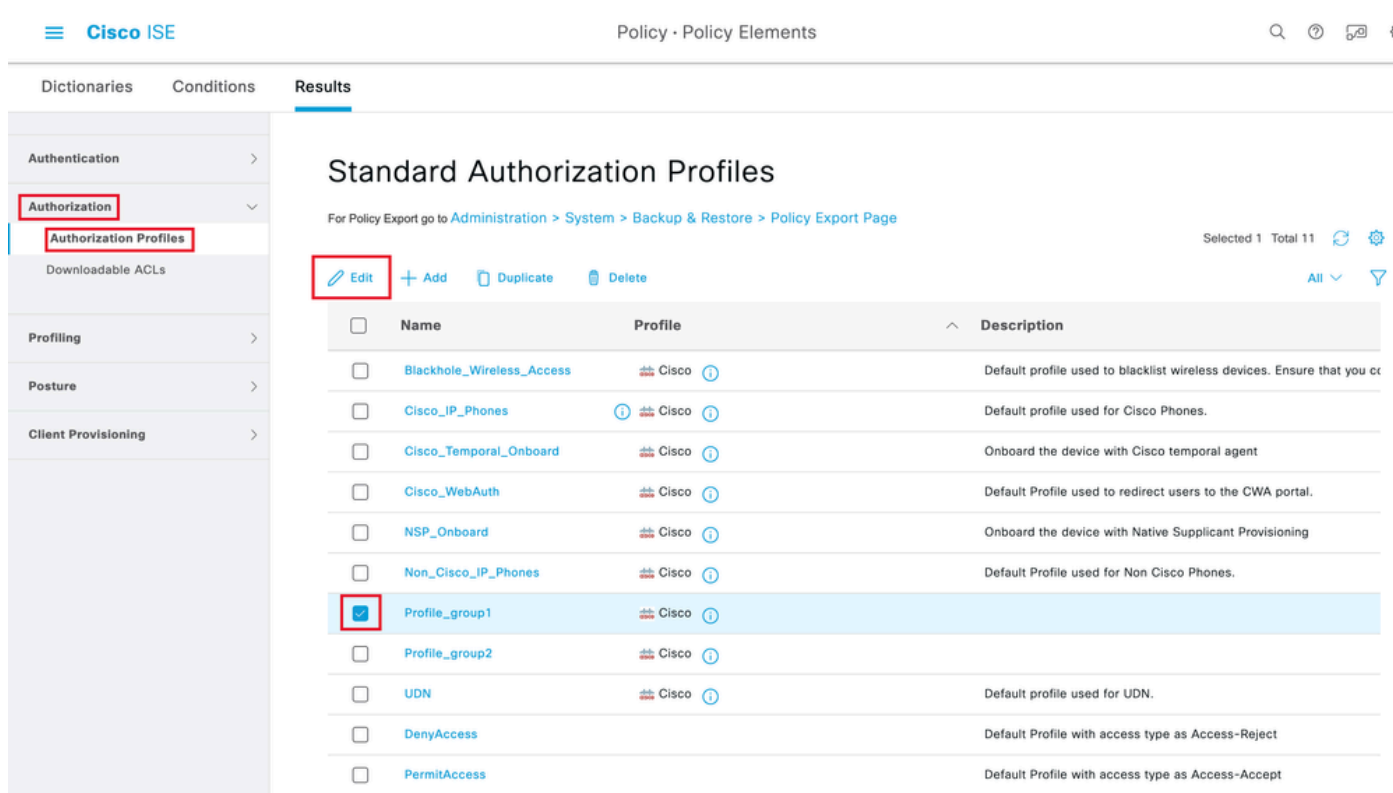
ステップ 12 (オプション)： 認可プロファイルを編集する必要がある場合は、Policy >

Resultsの順に移動します。



ISE一般メニュー

Authorization > Authorization Profilesの順に移動します。変更するプロファイルのチェックボックスをクリックして、Editをクリックします。



許可プロファイルの編集

クライアントの設定

ステップ 1: XMLプロファイルエディタを使用してXMLプロファイルを作成します。次の例は、このドキュメントの作成に使用した例です。

```
<#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>
```

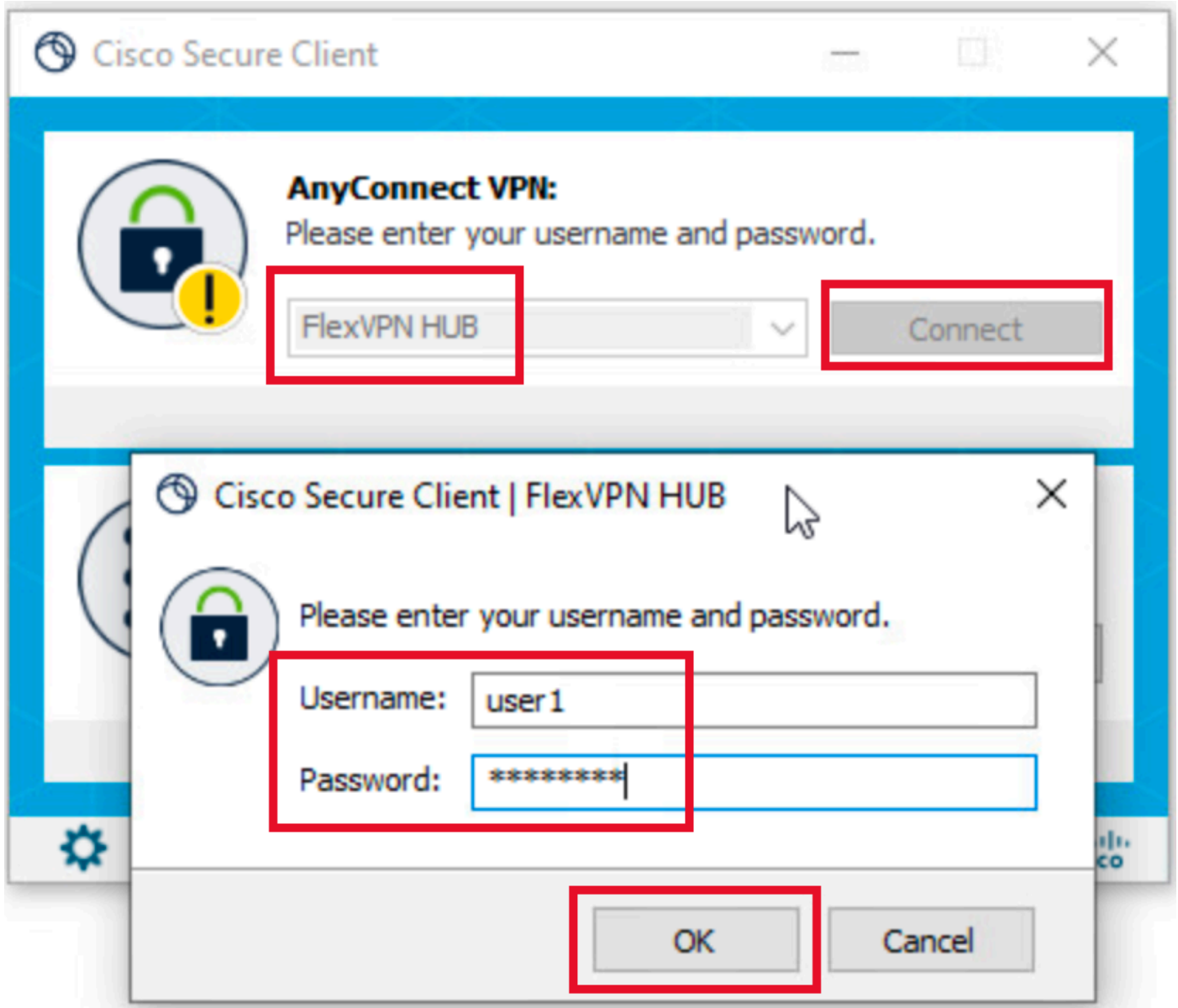
cisco.example

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

- <HostName> : ホスト、IPアドレス、または完全修飾ドメイン名(FQDN)を参照するために使用されるエイリアス。これはCSCボックスに表示されます。
- <HostAddress>:FlexVPNハブのIPアドレスまたはFQDN。
- <PrimaryProtocol> : クライアントがSSLの代わりにIKEv2/IPsecを使用するように、IPsecを設定する必要があります。
- <AuthMethodDuringIKENegotiation>:EAP内でEAP-MD5を使用するように設定する必要があります。これは、ISEサーバに対する認証に必要です。
- <IKEIdentity> : この文字列は、ID_GROUPタイプのIDペイロードとしてクライアントによって送信されます。これは、クライアントをハブ上の特定のIKEv2プロファイルと照合するために使用できます。

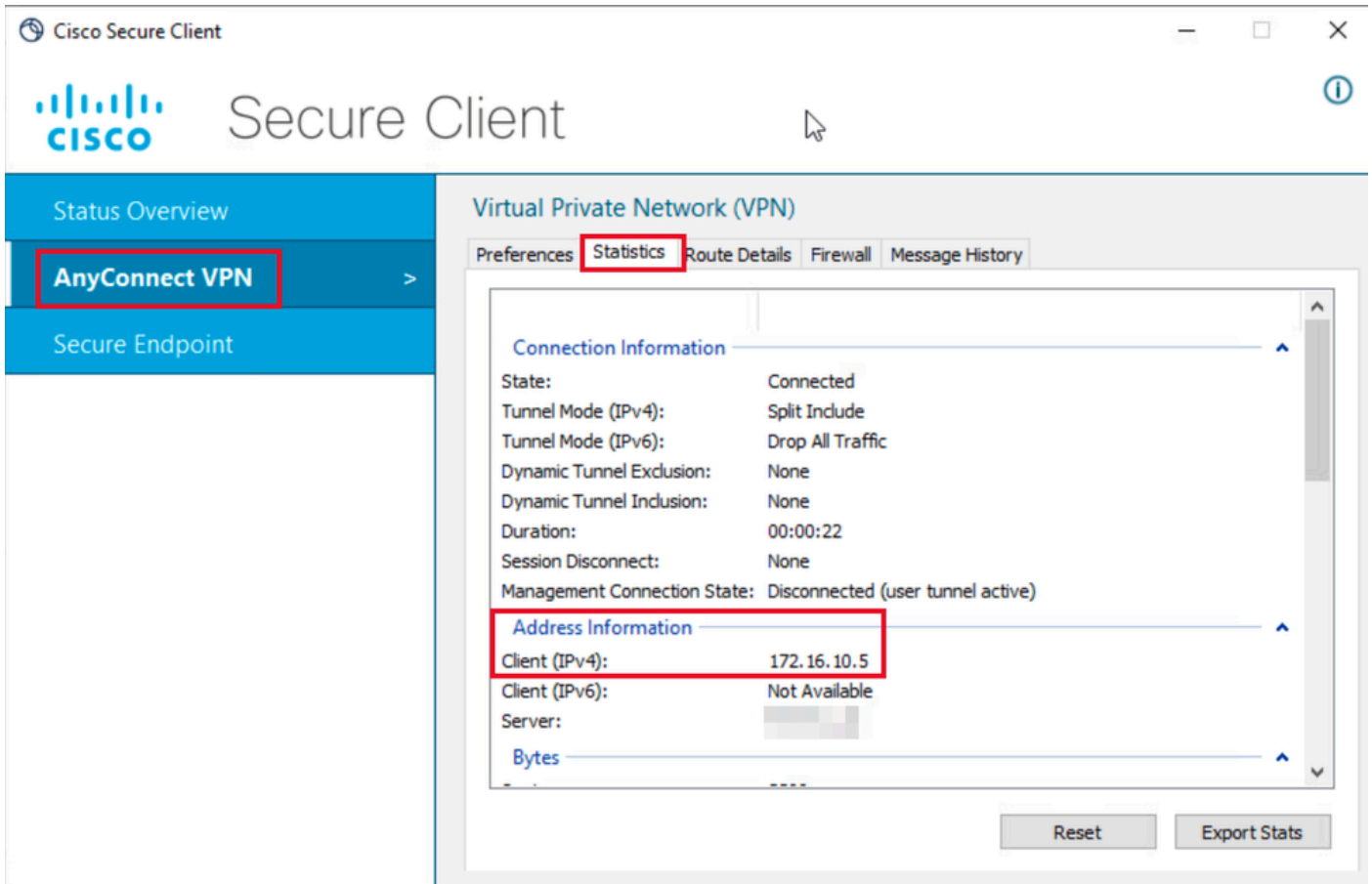
確認

ステップ 1 : CSCがインストールされているクライアントマシンに移動します。FlexVPNハブに接続し、user1クレデンシャルを入力します。



ユーザ1のクレデンシャル

ステップ 2：接続が確立されたら、歯車アイコン（左下隅）をクリックして、AnyConnectVPN > Statisticsに移動します。Address Informationセクションで、割り当てられたIPアドレスが、group1に設定されたプールに属していることを確認します。



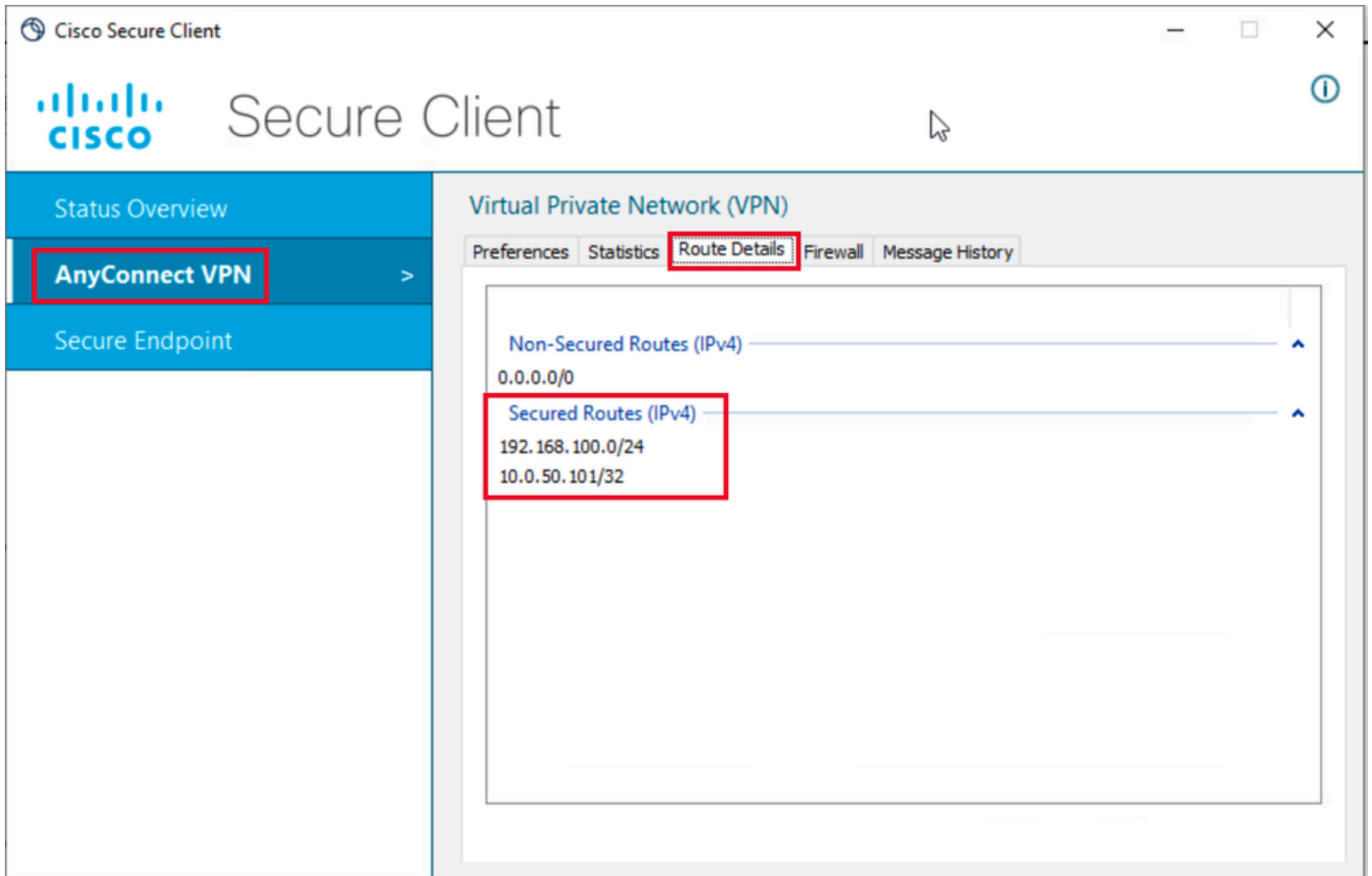
The screenshot shows the Cisco Secure Client interface. On the left, a navigation pane includes 'Status Overview', 'AnyConnect VPN' (highlighted with a red box), and 'Secure Endpoint'. The main area is titled 'Virtual Private Network (VPN)' and has tabs for 'Preferences', 'Statistics' (highlighted with a red box), 'Route Details', 'Firewall', and 'Message History'. Under the 'Statistics' tab, there are two expandable sections: 'Connection Information' and 'Address Information' (highlighted with a red box). The 'Address Information' section shows 'Client (IPv4): 172.16.10.5' and 'Client (IPv6): Not Available'. At the bottom right, there are 'Reset' and 'Export Stats' buttons.

Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:22
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information	
Client (IPv4):	172.16.10.5
Client (IPv6):	Not Available
Server:	

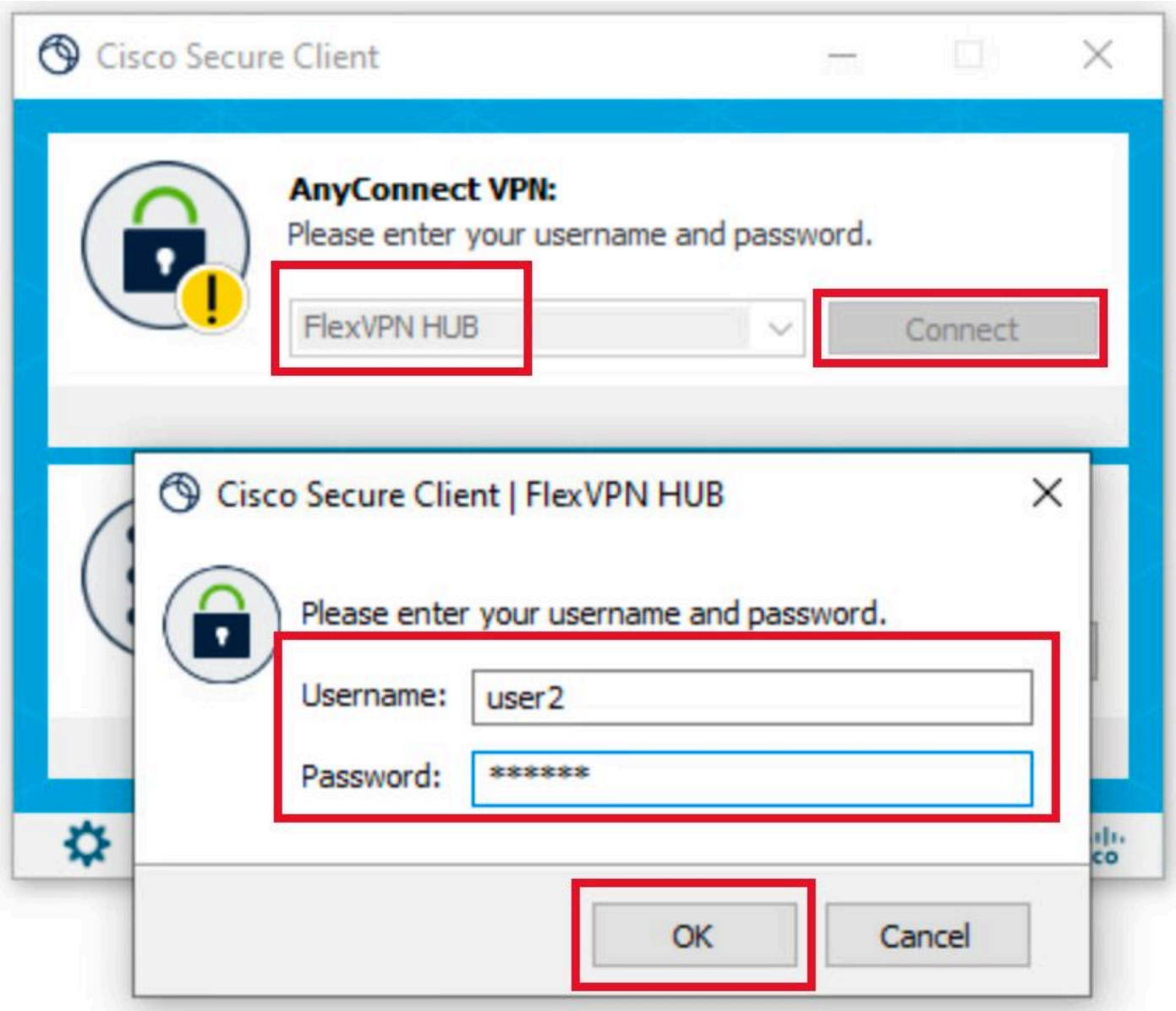
ユーザ1の統計情報

AnyConnectVPN > Route detailsに移動し、表示される情報がgroup1に設定されたセキュアルートとDNSに対応していることを確認します。

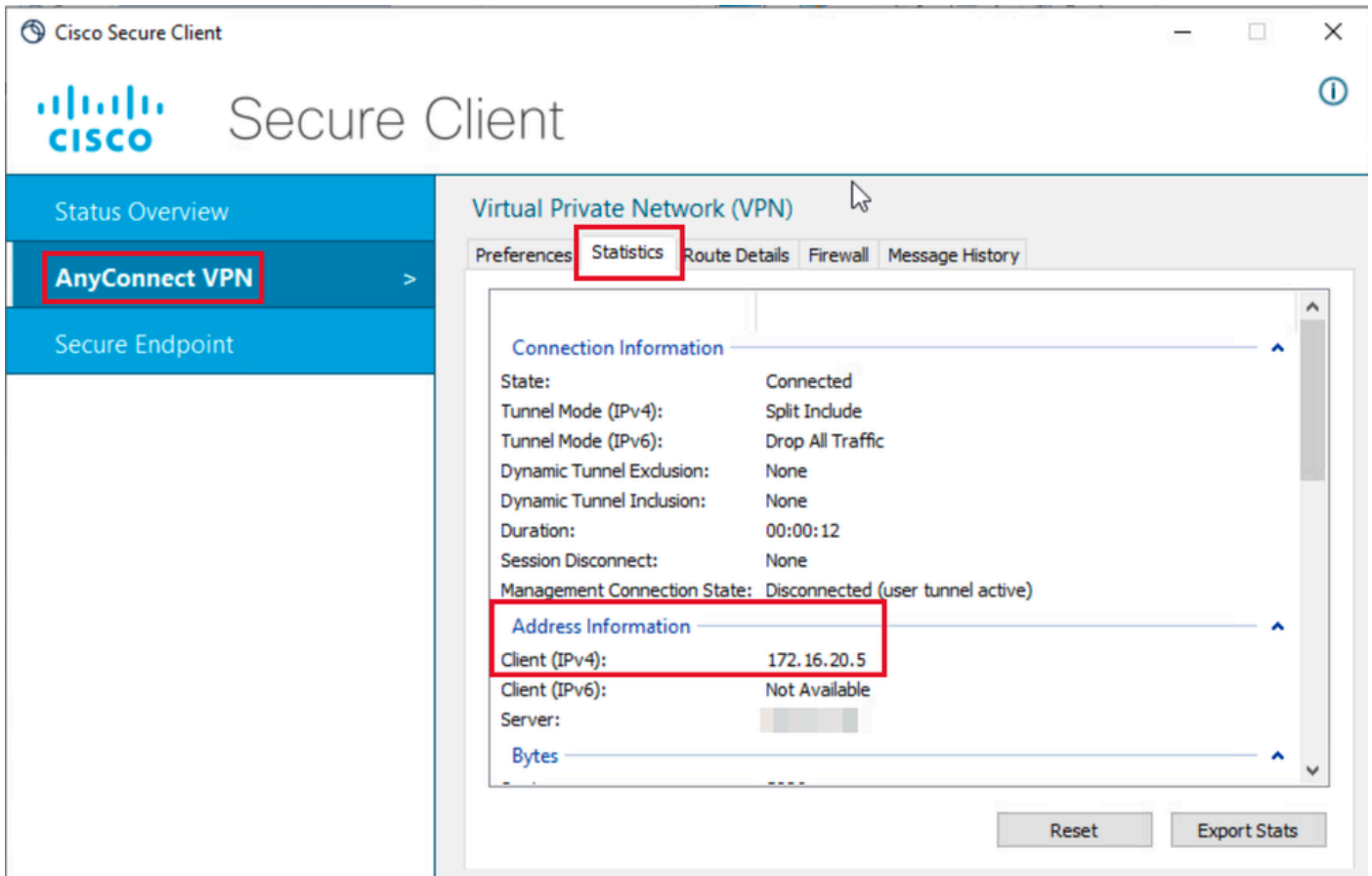


User1ルートの詳細

ステップ 3 : user2クレデンシャルを使用してステップ1と2を繰り返す、情報がこのグループのISE認可ポリシーで設定された値と一致することを確認します。



ユーザ2のクレデンシャル



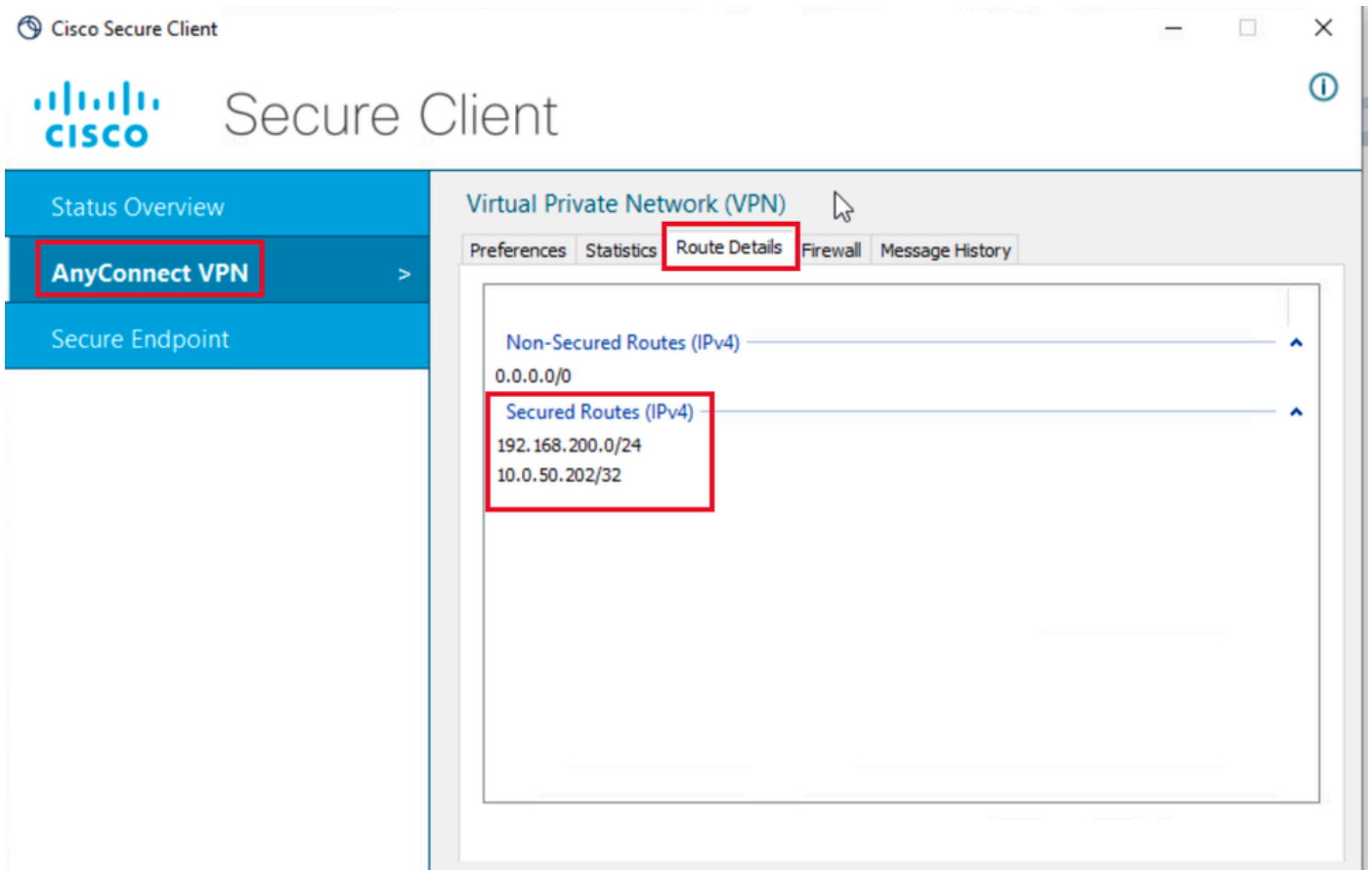
The screenshot shows the Cisco Secure Client interface. The left sidebar contains 'Status Overview', 'AnyConnect VPN', and 'Secure Endpoint'. The main window is titled 'Virtual Private Network (VPN)' and has tabs for 'Preferences', 'Statistics', 'Route Details', 'Firewall', and 'Message History'. The 'Statistics' tab is active and displays the following information:

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:	[Redacted]

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

ユーザ2の統計情報



The screenshot shows the Cisco Secure Client interface with the 'Route Details' tab selected. The main window displays the following route information:

Non-Secured Routes (IPv4)	
0.0.0.0/0	

Secured Routes (IPv4)	
192.168.200.0/24	
10.0.50.202/32	

ユーザ2のルートの詳細

トラブルシューティング

デバッグとログ

Ciscoルータの場合:

1. IKEv2およびIPSecデバッグを使用して、ヘッドエンドとクライアント間のネゴシエーションを確認します。

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

2. AAAデバッグを使用して、ローカル属性やリモート属性の割り当てを確認します。

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

ISEで次を実行します。

- RADIUS ライブ ログ

正常動作シナリオ

次の出力は、正常な接続の例です。

- User1のデバッグ出力 :

<#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
```

• User2のデバッグ出力 :

```
<#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-phrase1-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

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。