

Konfigurieren der RADIUS-Attributzuordnung für FlexVPN-Remote-Benutzer

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Router-Konfiguration](#)

[Konfiguration der Identity Services Engine \(ISE\)](#)

[Client-Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Debugs und Protokolle](#)

[Arbeitsszenario](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie FlexVPN mithilfe der Cisco Identity Services Engine (ISE) konfiguriert wird, um Identitäten zu überprüfen und die Attributgruppenzuordnung durchzuführen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Remote Access Virtual Private Network (RAVPN) mit IKEV2/IPsec-Konfiguration auf einem Cisco IOS® XE-Router über CLI
- Konfiguration der Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- RADIUS-Protokoll

Verwendete Komponenten

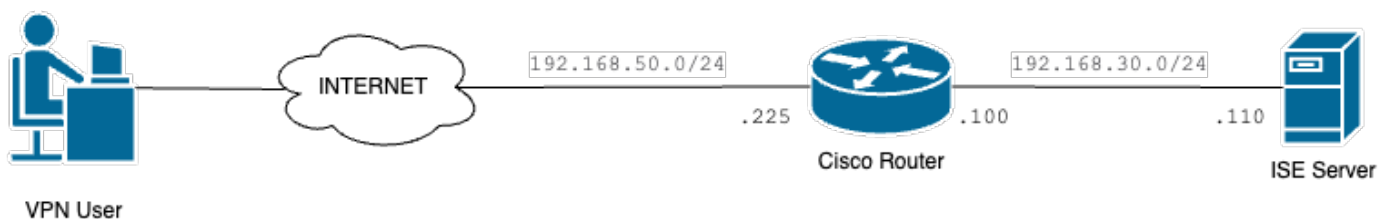
Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Grundlegendes Netzwerkdiagramm

Konfigurationen

Router-Konfiguration

Schritt 1: Konfigurieren Sie einen RADIUS-Server für die Authentifizierung und lokale Autorisierung auf dem Gerät:

```
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
```

Der Befehl `aaa authentication login <list_name>` bezieht sich auf die AAA-Gruppe (Authentication, Authorization, Accounting), die den RADIUS-Server definiert.

Der lokale Befehl `aaa Authorization Network <list_name>` gibt an, dass lokal definierte Benutzer/Gruppen verwendet werden sollen.

Schritt 2: Konfigurieren eines Vertrauenspunkts zum Speichern des Router-Zertifikats Da die lokale Authentifizierung des Routers vom Typ RSA ist, muss sich der Server mithilfe eines Zertifikats authentifizieren:

```
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
```

Schritt 3: Definieren Sie einen lokalen IP-Pool für jede Benutzergruppe:

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

Schritt 4: Konfigurieren Sie die lokale Autorisierungsrichtlinie:

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

In der Autorisierungsrichtlinie ist keine Konfiguration erforderlich, da der Authentifizierungsserver für das Senden der relevanten Werte (DNS, Pool, geschützte Routen usw.) auf Basis der Gruppe, der der Benutzer angehört, verantwortlich ist. Sie muss jedoch so konfiguriert werden, dass der Benutzername in unserer lokalen Autorisierungsdatenbank definiert wird.

Schritt 5 (optional). Erstellen Sie einen IKEv2-Vorschlag und eine IKEv2-Richtlinie (wenn diese nicht konfiguriert sind, werden intelligente Standardeinstellungen verwendet):

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

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

Schritt 6 (optional). Konfigurieren Sie den Transformationssatz (falls nicht konfiguriert, werden intelligente Standardeinstellungen verwendet):

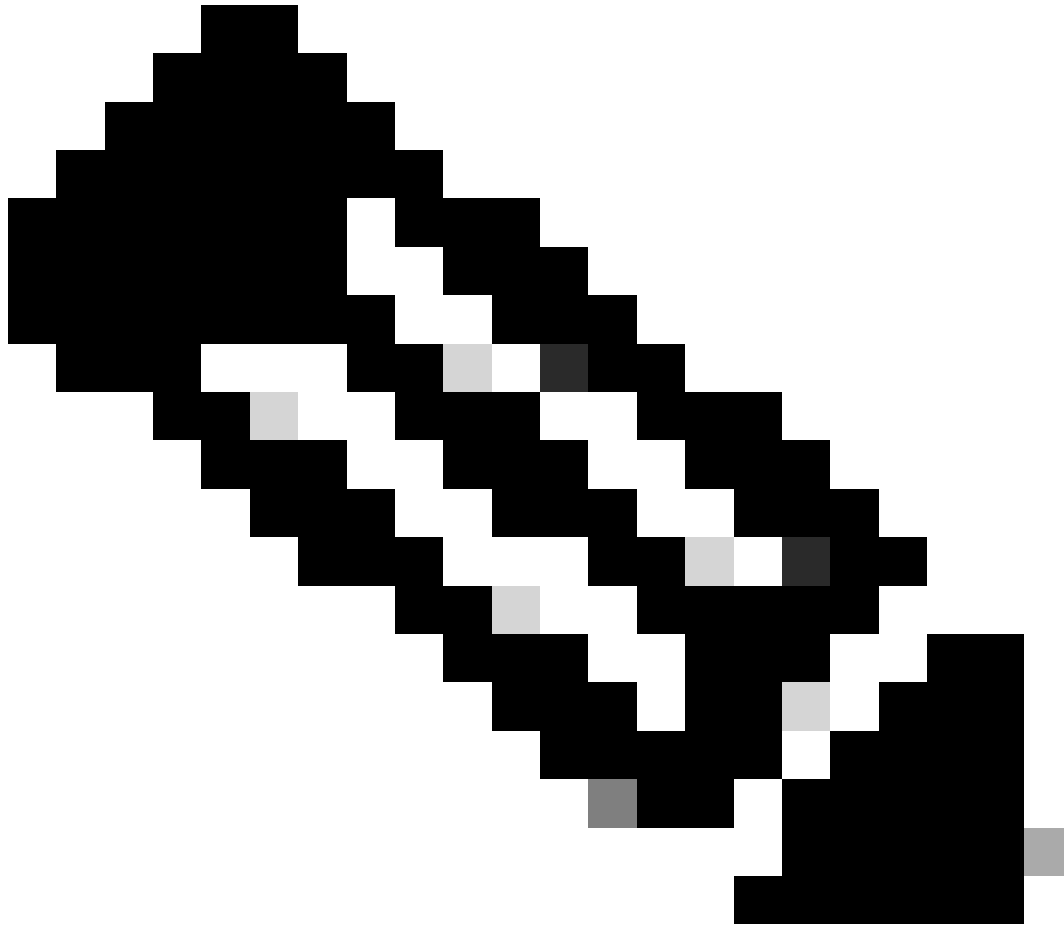
```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
  mode tunnel
```

Schritt 7. Konfigurieren Sie ein IKEv2-Profil mit den richtigen lokalen und Remote-Identitäten,

Authentifizierungsmethoden (lokal und remote), Trustpoint, AAA und der virtuellen Vorlagenschnittstelle, die für die Verbindungen verwendet wird:

```
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
```

Der Befehl `aaa authentication user eap cached` gibt an, dass die während der EAP-Authentifizierung empfangenen Attribute zwischengespeichert werden müssen. Dieser Befehl ist für die Konfiguration erforderlich, da ohne diesen Befehl die vom Authentifizierungsserver gesendeten Daten nicht verwendet werden. Dies führt zu einem Verbindungsfehler.



Hinweis: Die entfernte Schlüssel-ID muss mit dem Schlüssel-ID-Wert in der XML-Datei übereinstimmen. Wenn sie nicht in der XML-Datei geändert wird, wird der Standardwert (*\$AnyConnectClient\$*) verwendet, der im IKEv2-Profil konfiguriert werden muss.

Schritt 8: Konfigurieren Sie ein IPsec-Profil, und weisen Sie den Transformationssatz und das IKEv2-Profil zu:

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

Schritt 9. Konfigurieren einer Loopback-Schnittstelle Die Virtual-Access-Schnittstelle borgt sich die IP-Adresse daraus:

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

Schritt 10. Erstellen Sie die virtuelle Vorlage, die zum Erstellen der verschiedenen Schnittstellen für den virtuellen Zugriff verwendet wird, und verknüpfen Sie das in Schritt 8 erstellte IPSec-Profil:

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

Schritt 11. Deaktivieren Sie die HTTP-URL-basierte Zertifikatssuche und den HTTP-Server auf dem Router:

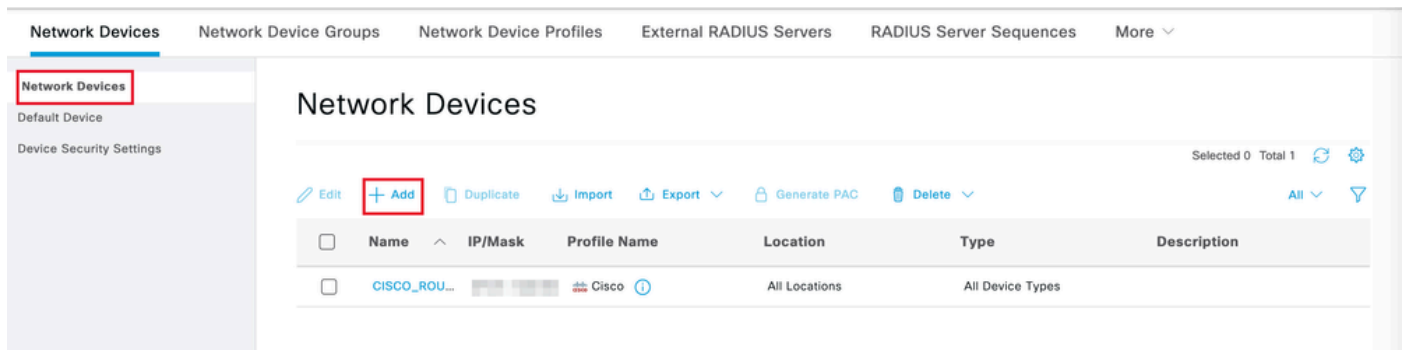
```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

Identity Services Engine (ISE)-Konfiguration

Schritt 1: Melden Sie sich beim ISE-Server an, und navigieren Sie zu Administration > Network Resources > Network Devices:

The screenshot displays the Cisco ISE Administration web interface. The top navigation bar includes 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. Below this, the 'Administration' section is expanded to show 'Network Resources' (highlighted with a red box), which contains 'Network Devices' (also highlighted with a red box). Other visible sections include 'System', 'Identity Management', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The left sidebar shows 'Recent Pages' with 'Network Devices' listed. The bottom left corner features a 'Shortcuts' section with keyboard shortcuts for expanding and collapsing the menu, and a 'Make a wish' button.

Schritt 2: Klicken Sie auf Hinzufügen, um den Router als AAA-Client zu konfigurieren:



Hinzufügen eines neuen Netzwerkgeräts

Geben Sie die Felder für den Netzwerkgerätenamen und die IP-Adresse ein, aktivieren Sie das Kontrollkästchen RADIUS Authentication Settings (RADIUS-Authentifizierungseinstellungen), und fügen Sie den freigegebenen Schlüssel hinzu. Dieser Wert muss mit dem identisch sein, der bei der Erstellung des RADIUS-Serverobjekts auf dem Router verwendet wurde.

Network Devices

Name

Description

IP Address

Name und IP-Adresse



✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

Show

Use Second Shared Secret ⓘ

networkDevices.secondSharedSecret

Show

Radius-Kennwort

Klicken Sie auf Speichern.

Schritt 3: Navigieren Sie zu 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). Under 'System', 'Identity Management' is highlighted with a red box, and 'Groups' is highlighted with a red box.

ISE - Allgemeines Menü

Schritt 4: Klicken Sie auf Benutzeridentitätsgruppen und dann auf Hinzufügen:

Identity Groups

EQ

< [Menu] [Settings]

> Endpoint Identity Groups

> **User Identity Groups**

User Identity Groups

Selected 0 Total 10 [Refresh] [Settings]

[Edit] **+ Add** [Delete] [Import] [Export]

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

Neue Gruppe hinzufügen

Geben Sie den Gruppennamen ein, und klicken Sie auf Senden.

Identity Group

* Name

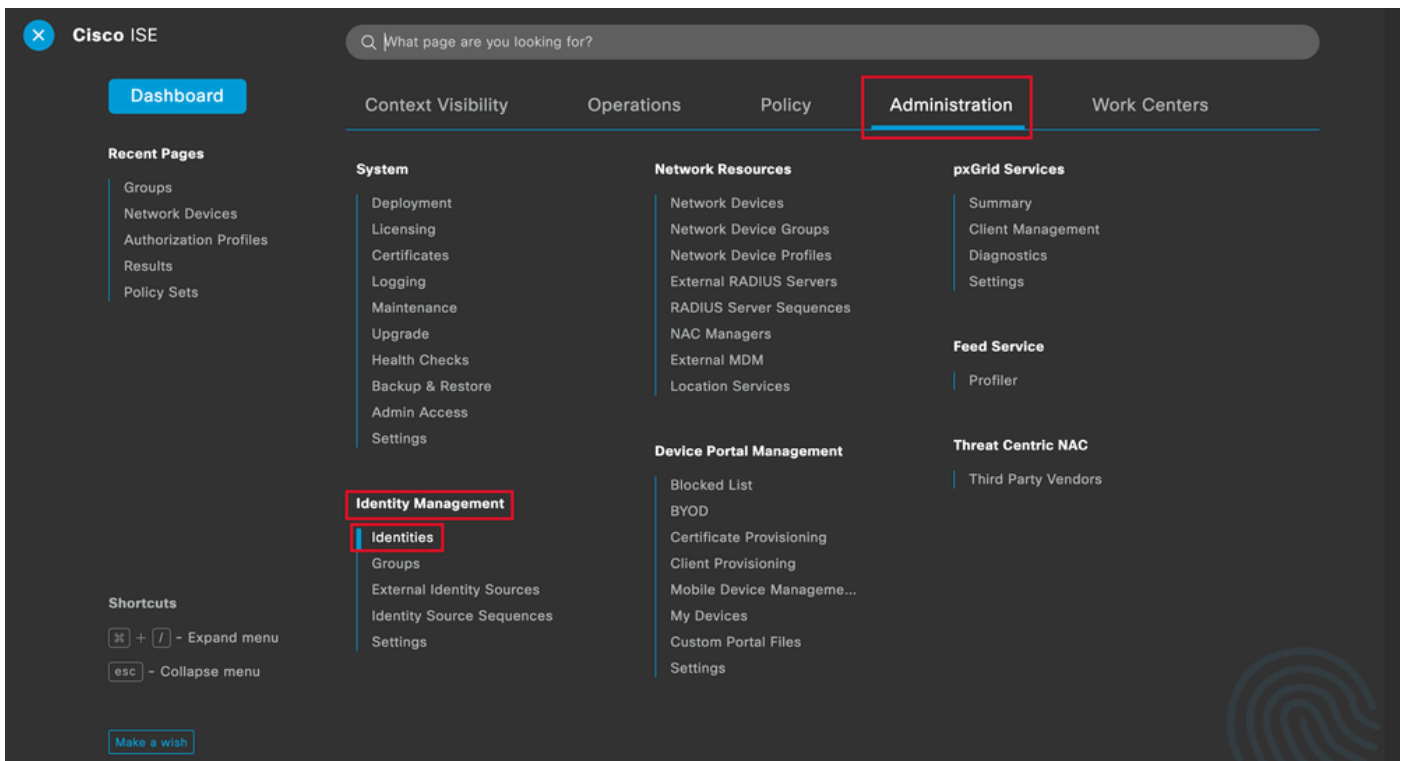
Description

Gruppeninformationen



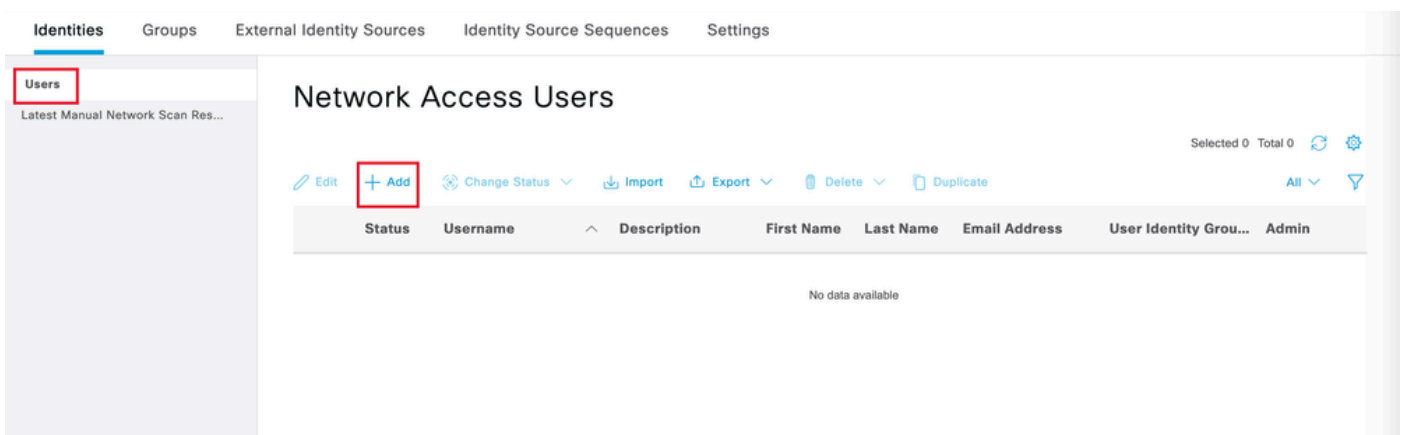
Hinweis: Wiederholen Sie die Schritte 3 und 4, um so viele Gruppen wie nötig zu erstellen.

Schritt 5: Navigieren Sie zu Administration > Identity Management > Identities:



ISE - Allgemeines Menü

Schritt 6: Klicken Sie auf Hinzufügen, um einen neuen Benutzer in der lokalen Serverdatenbank zu erstellen:



Benutzer hinzufügen

Geben Sie den Benutzernamen und das Anmeldekennwort ein. Navigieren Sie anschließend zum Ende dieser Seite, und wählen Sie die Benutzergruppe aus:

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

Benutzername und Passwort

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 20

User Groups

User Groups

EQ

< [icon] [gear]

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

Select an item

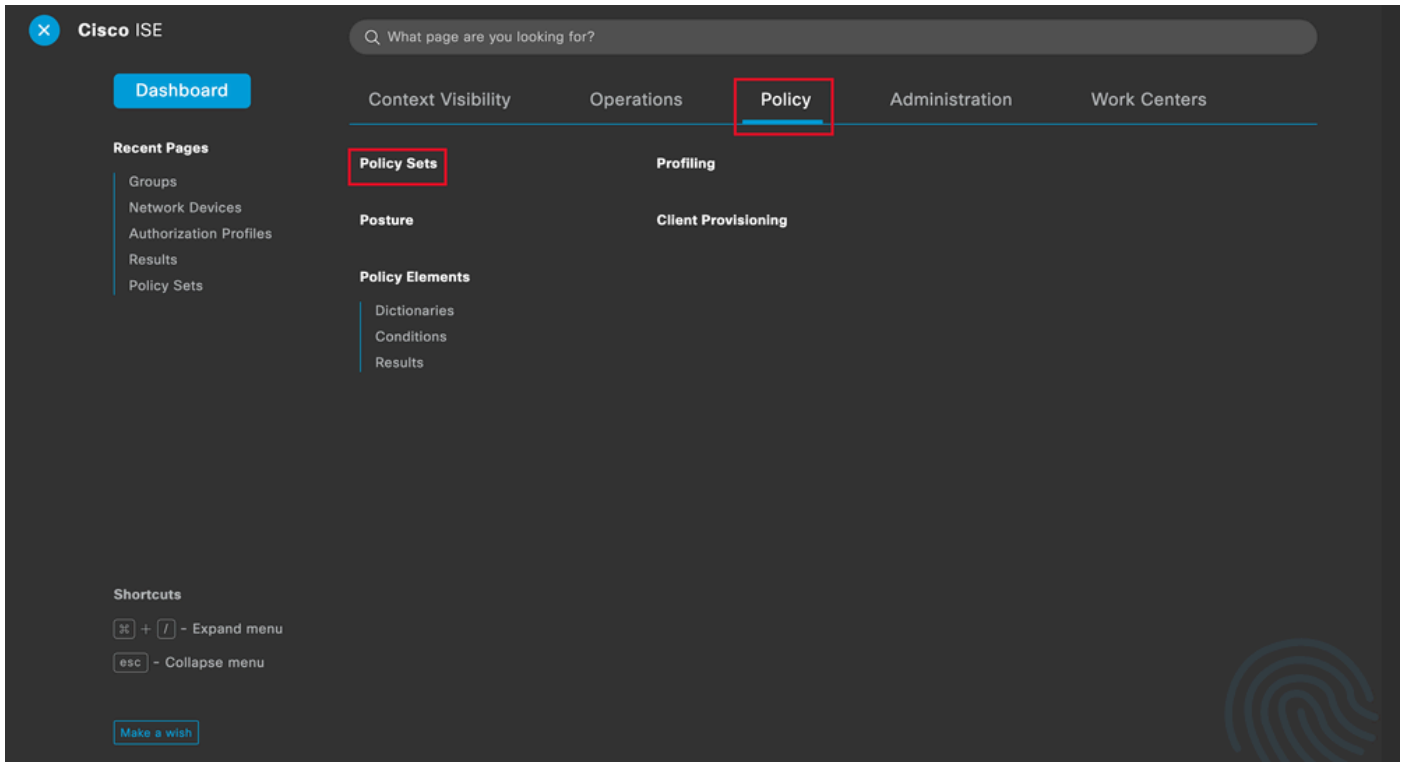
Zuweisen der richtigen Gruppe zum Benutzer

Klicken Sie auf Speichern.



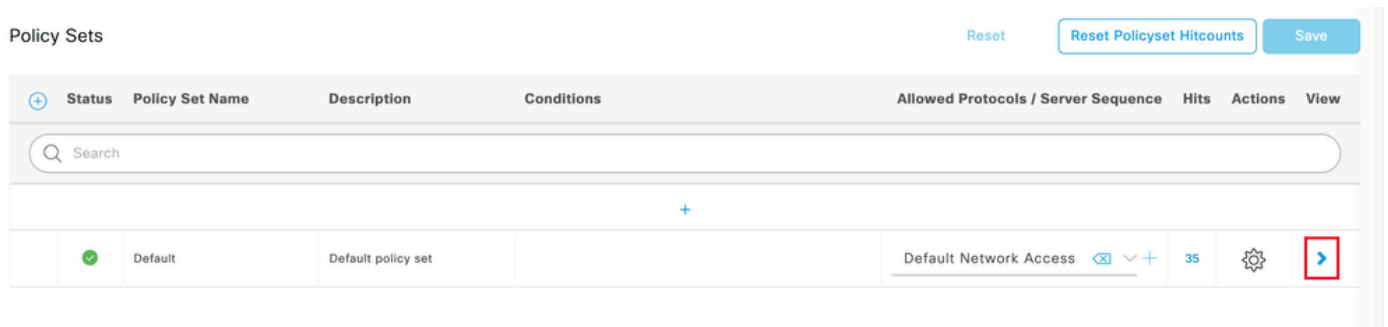
Hinweis: Wiederholen Sie die Schritte 5 und 6, um die benötigten Benutzer zu erstellen und der entsprechenden Gruppe zuzuweisen.

Schritt 7: Navigieren Sie zu Richtlinie > Richtlinienansätze:



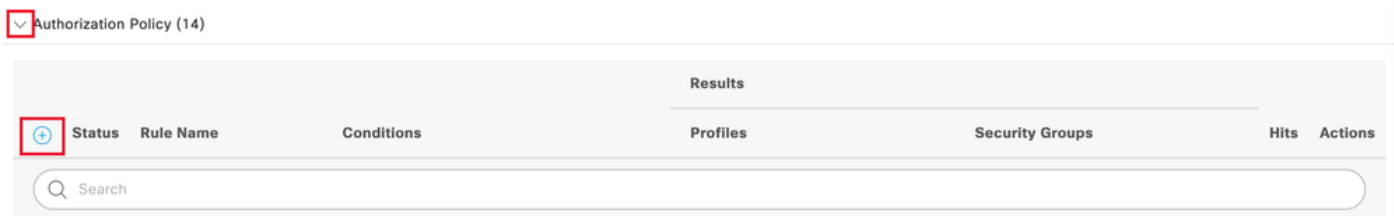
ISE - Allgemeines Menü

Wählen Sie die Standard-Autorisierungsrichtlinie aus, indem Sie auf den Pfeil rechts im Bildschirm klicken:



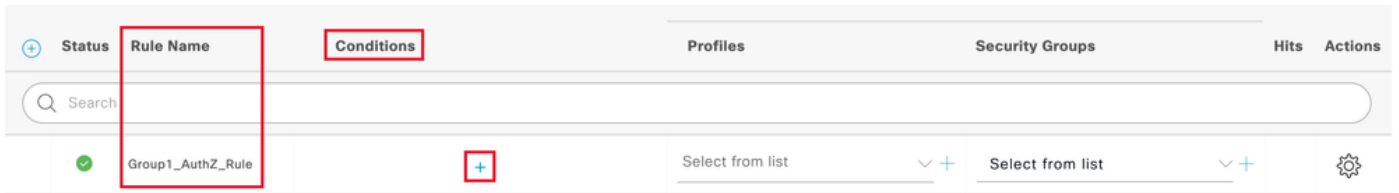
Autorisierungsrichtlinie auswählen

Schritt 8: Klicken Sie auf den Pfeil des Dropdown-Menüs neben Autorisierungsrichtlinie, um sie zu erweitern. Klicken Sie anschließend auf das Symbol add (+), um eine neue Regel hinzuzufügen:



Neue Autorisierungsregel hinzufügen

Geben Sie den Namen für die Regel ein, und wählen Sie in der Spalte "Bedingungen" das Symbol add (+) aus:



Bedingung hinzufügen

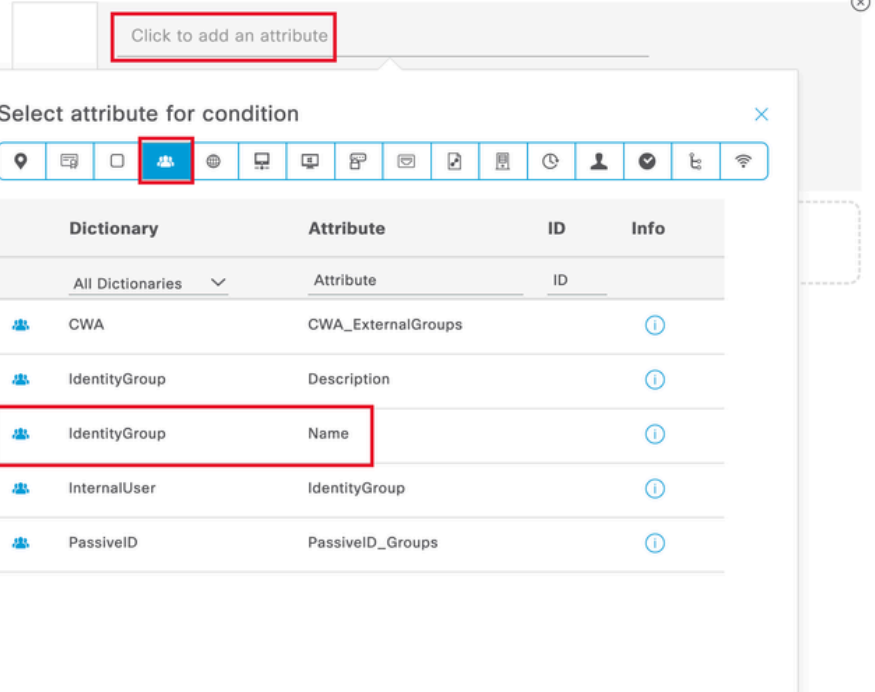
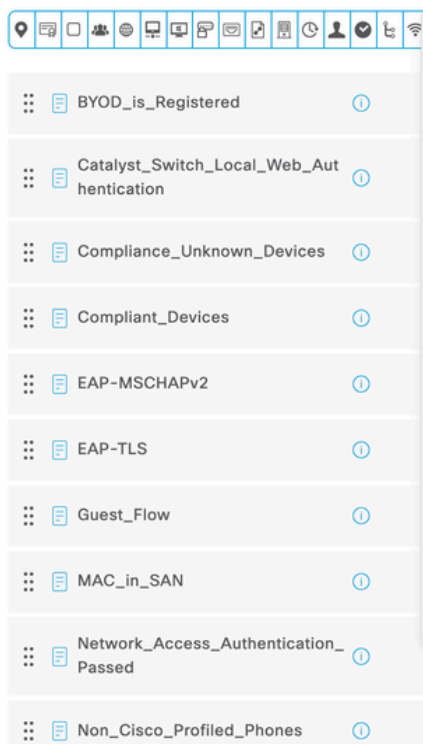
Schritt 9. Klicken Sie in das Textfeld Attribute-Editor, und klicken Sie auf das Symbol der Gruppidentität. Wählen Sie das Attribut Identity group - Name aus:

Conditions Studio

Library

Editor

Search by Name



Bedingung auswählen

Wählen Sie dann Gleich als Operator aus, klicken Sie auf den Pfeil des Dropdown-Menüs, um die verfügbaren Optionen anzuzeigen, und wählen Sie Benutzeridentitätsgruppen:<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

Gruppe auswählen

Klicken Sie auf Speichern.

Schritt 10. Klicken Sie in der Spalte Profile auf das Symbol add (+) und wählen Sie Create a New Authorization Profile (Neues Autorisierungsprofil erstellen):

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	⚙️

Autorisierungsprofil erstellen

Name des Profils eingeben

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Profilinformationen

Navigieren Sie zum Ende dieser Seite zu Erweiterte Attributeinstellungen, und klicken Sie auf den Pfeil des Dropdown-Menüs. Klicken Sie dann auf Cisco, und wählen Sie cisco-av-pair--[1]:

Advanced Attributes Settings

Select an item

Attributes Details

Access Type = ACCESS_ACCEPT

- 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]

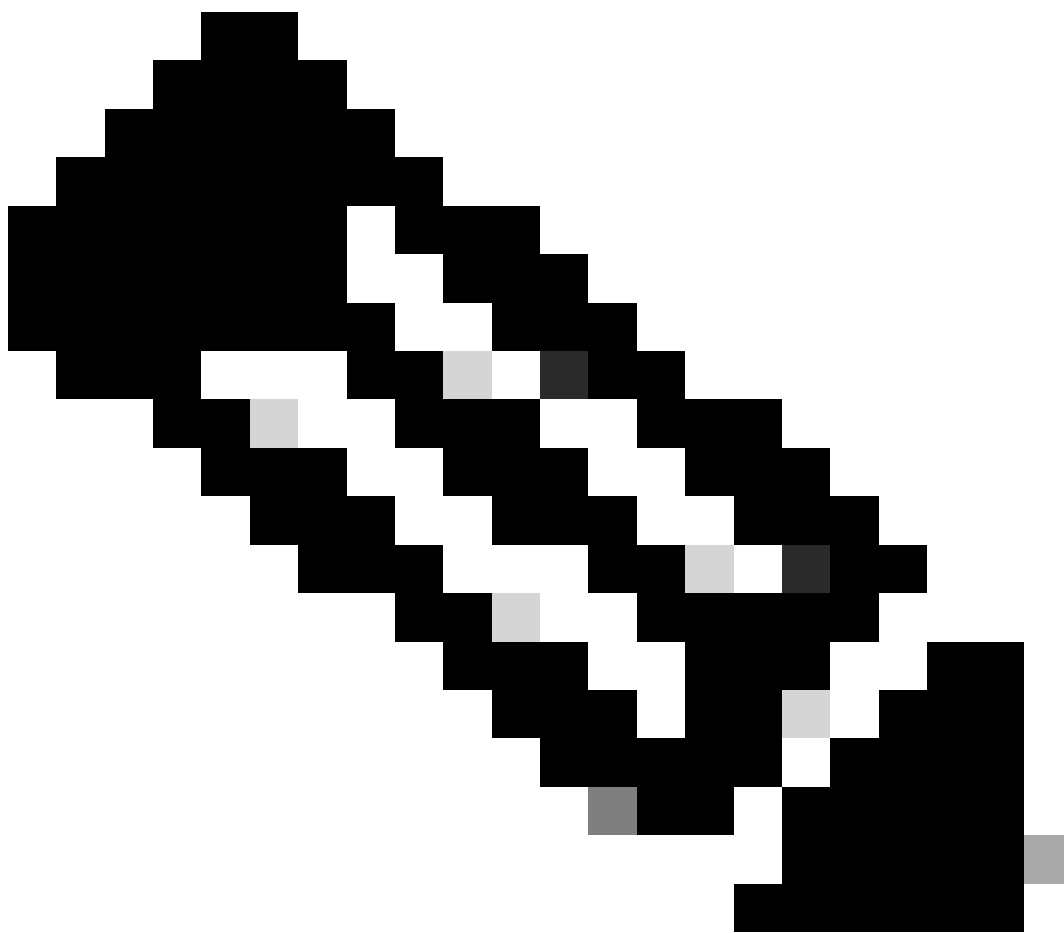
Wählen Sie den Attributtyp aus

Fügen Sie das cisco-av-pair-Attribut hinzu, das Sie konfigurieren möchten, und klicken Sie auf das Symbol add (+), um ein weiteres Attribut hinzuzufügen:

Advanced Attributes Settings

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

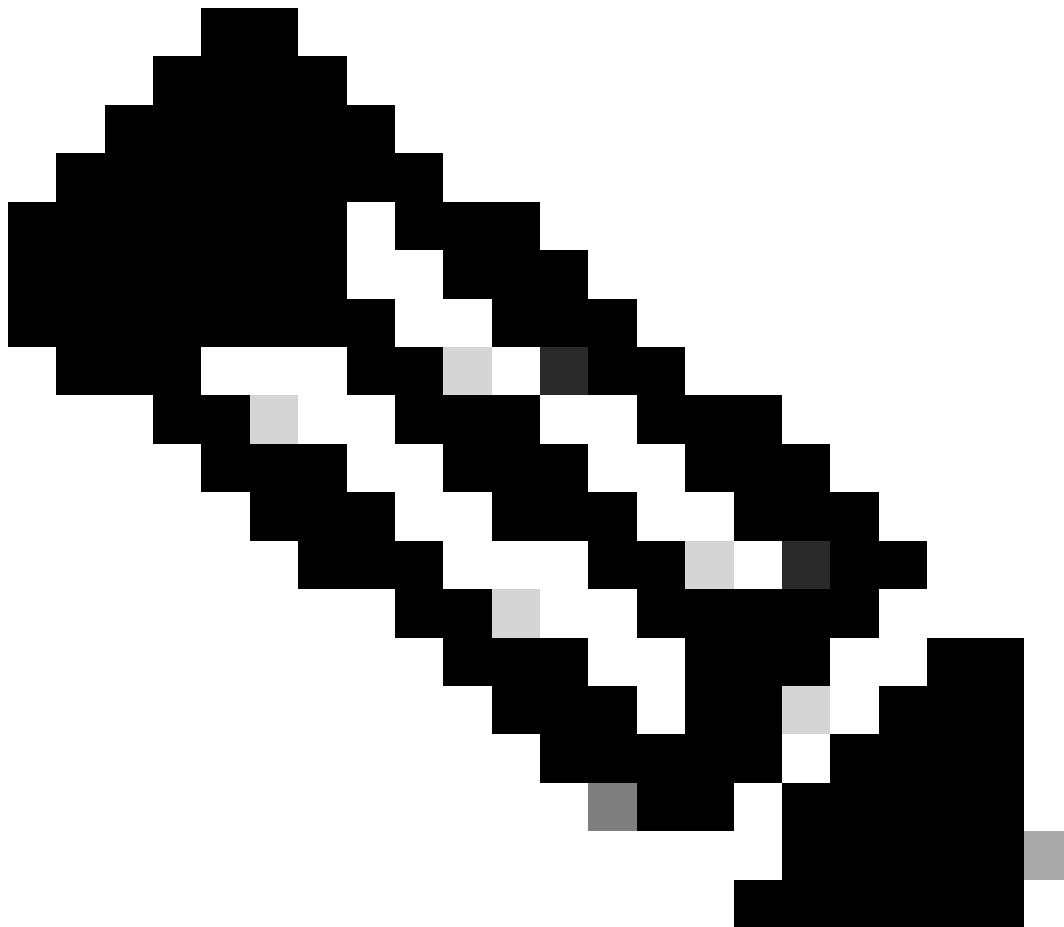
Konfigurieren des Attributs



Hinweis: Informationen zu Attributspezifikationen (Name, Syntax, Beschreibung, Beispiel usw.) finden Sie im Konfigurationsleitfaden für FlexVPN RADIUS-Attribute:

[FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE Fuji](#)

[16.9.x - Unterstützte RADIUS-Attribute](#)



Hinweis: Wiederholen Sie den vorherigen Schritt, um die erforderlichen Attribute zu erstellen.

Klicken Sie auf Speichern.

Die Attribute, die als Nächstes folgen, wurden jeder Gruppe zugewiesen:

- Attribute der Gruppe 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

Group1-Attribut

- Attribute der Gruppe 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

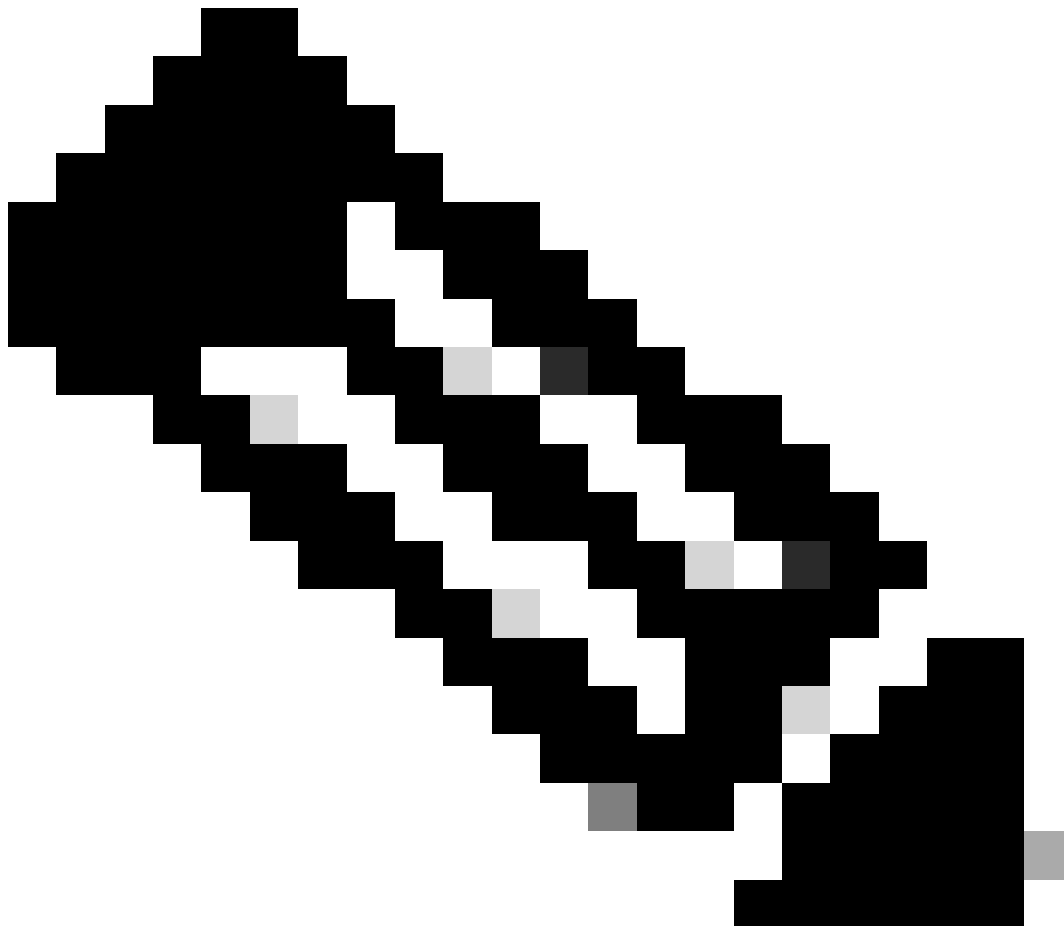
Group2-Attribute

Schritt 11: Klicken Sie auf den Dropdown-Menüpfel, und wählen Sie das in Schritt 10 erstellte Autorisierungsprofil aus:

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	⚙️

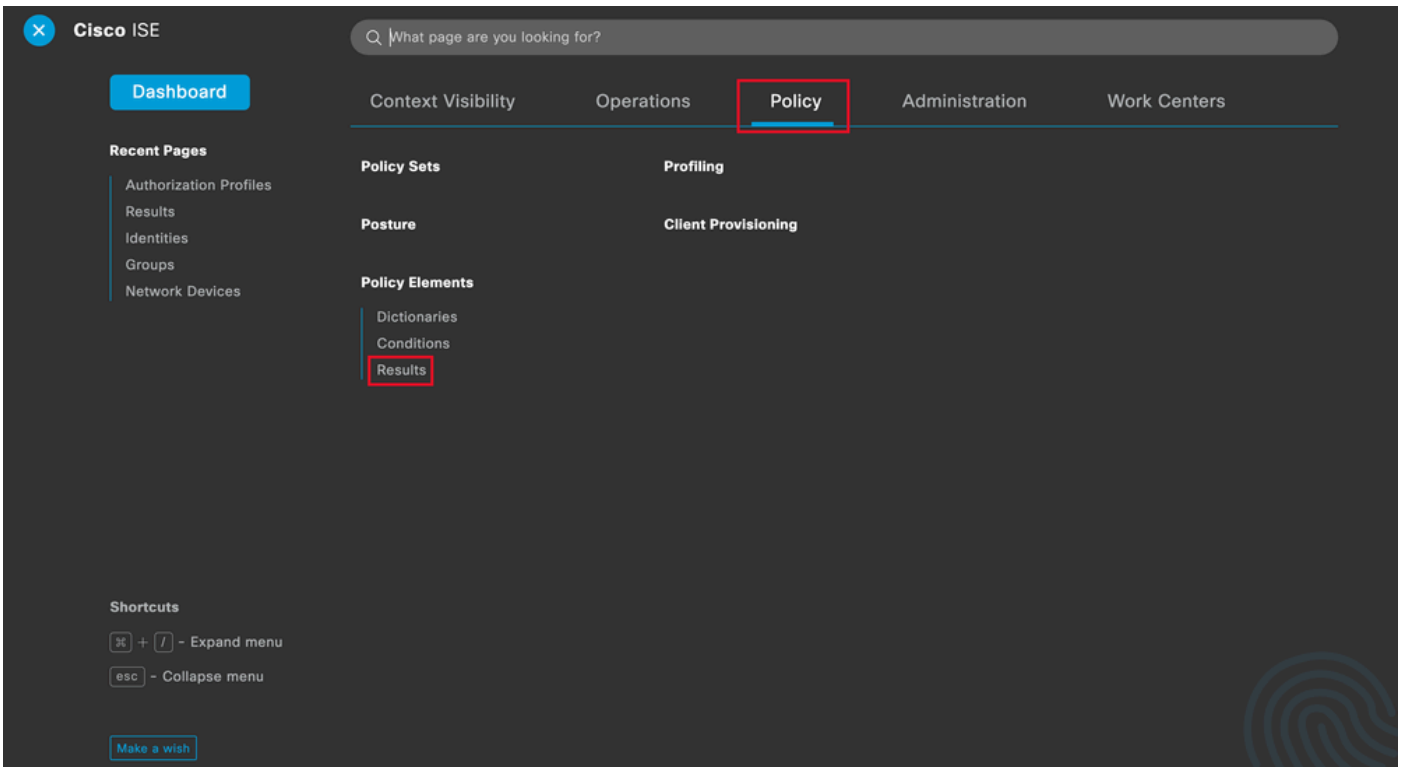
Autorisierungsprofil zuweisen

Klicken Sie auf Speichern.



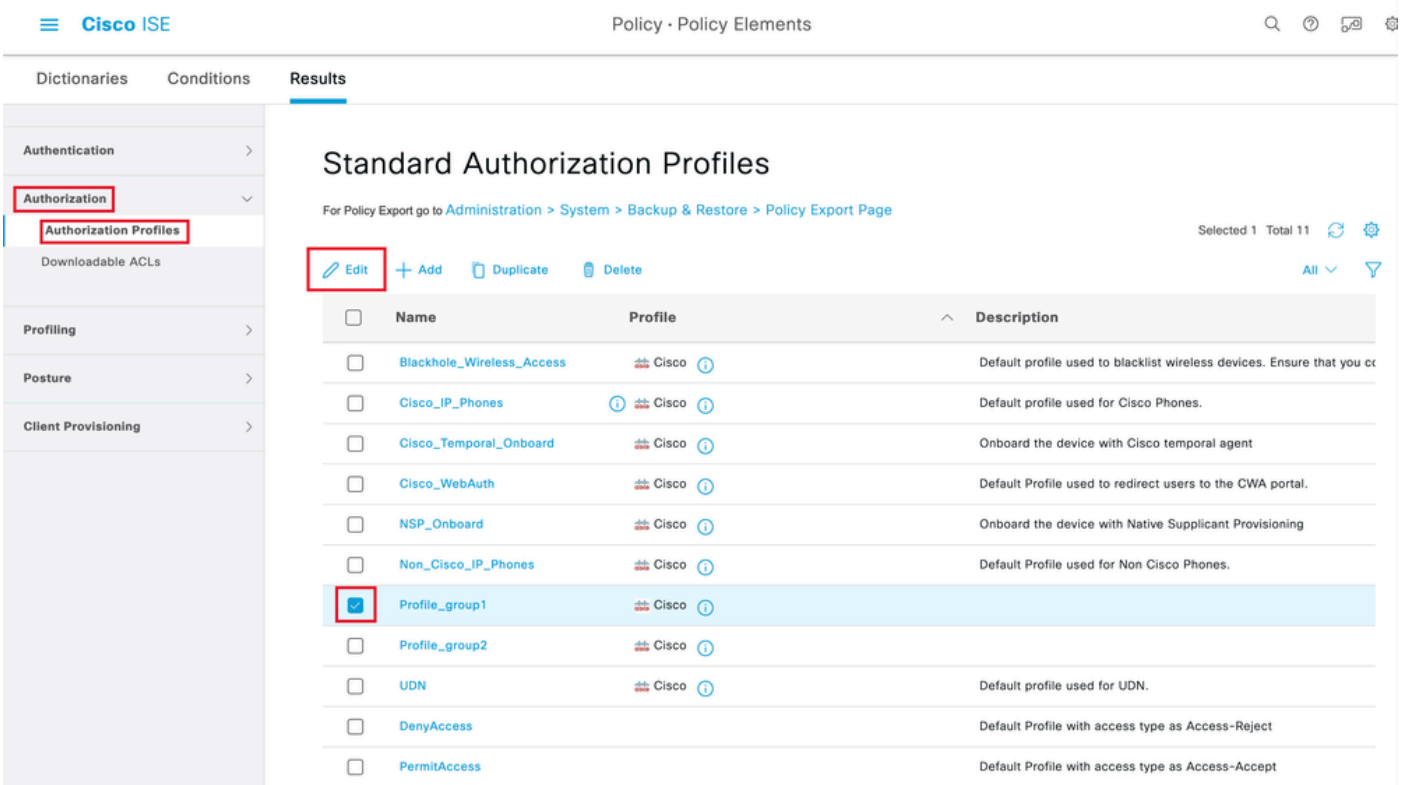
Hinweis: Wiederholen Sie die Schritte 8 bis 11, um die erforderlichen Autorisierungsregeln für jede Gruppe zu erstellen.

Schritt 12 (optional). Wenn Sie das Autorisierungsprofil bearbeiten müssen, navigieren Sie zu Richtlinie > Ergebnisse:



ISE - Allgemeines Menü

Navigieren Sie zu Autorisierung > Autorisierungsprofile. Aktivieren Sie das Kontrollkästchen des Profils, das Sie ändern möchten, und klicken Sie dann auf Bearbeiten:



Autorisierungsprofil bearbeiten

Client-Konfiguration

Schritt 1: Erstellen Sie ein XML-Profil mit dem XML-Profil-Editor. Dieses Beispiel wird für die Erstellung dieses Dokuments verwendet:

```
<#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
    <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
  </AutoReconnect>
    <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
    <PPPEExclusionServerIP UserControllable="false"/>
  </PPPEExclusion>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">
      false
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
  </EnableAutomaticServerSelection>
    <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>
```

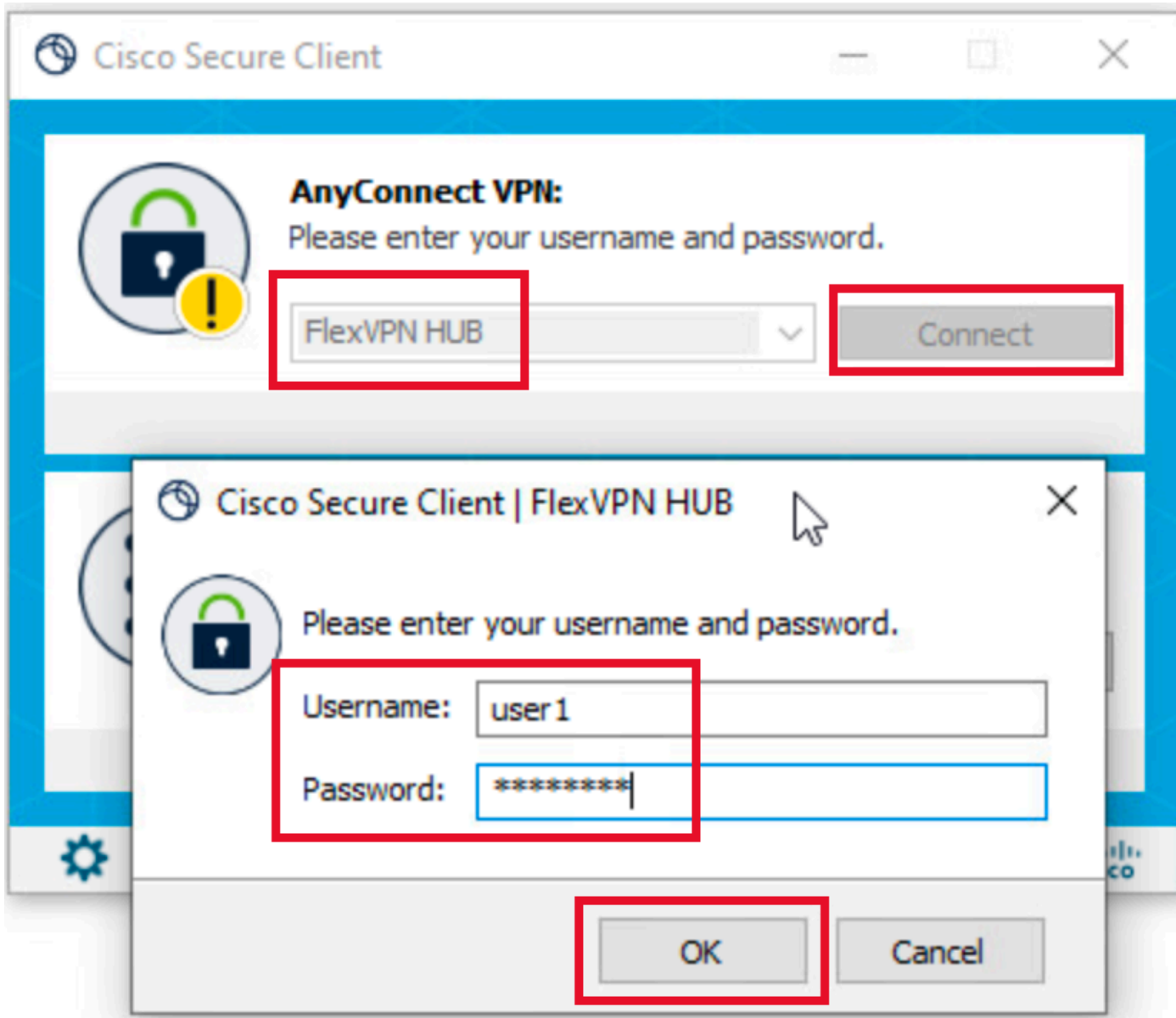
cisco.example

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

- **<Hostname>** - Der Alias, der für den Host, die IP-Adresse oder den vollqualifizierten Domännennamen (FQDN) verwendet wird. Dies wird im CSC-Feld angezeigt.
- **<HostAddress>** - IP-Adresse oder FQDN des FlexVPN-Hubs.
- **<PrimaryProtocol>** - Muss auf "IPsec" gesetzt werden, damit der Client IKEv2/IPsec anstelle von SSL verwenden kann.
- **<AuthMethodWhileIKENegotiation>** - Muss für die Verwendung von EAP-MD5 innerhalb von EAP festgelegt werden. Dies ist für die Authentifizierung gegenüber dem ISE-Server erforderlich.
- **<IKEIdentity>** - Diese Zeichenfolge wird vom Client als ID_GROUP-Typ-ID-Nutzlast gesendet. Damit kann der Client einem bestimmten IKEv2-Profil auf dem Hub zugeordnet werden.

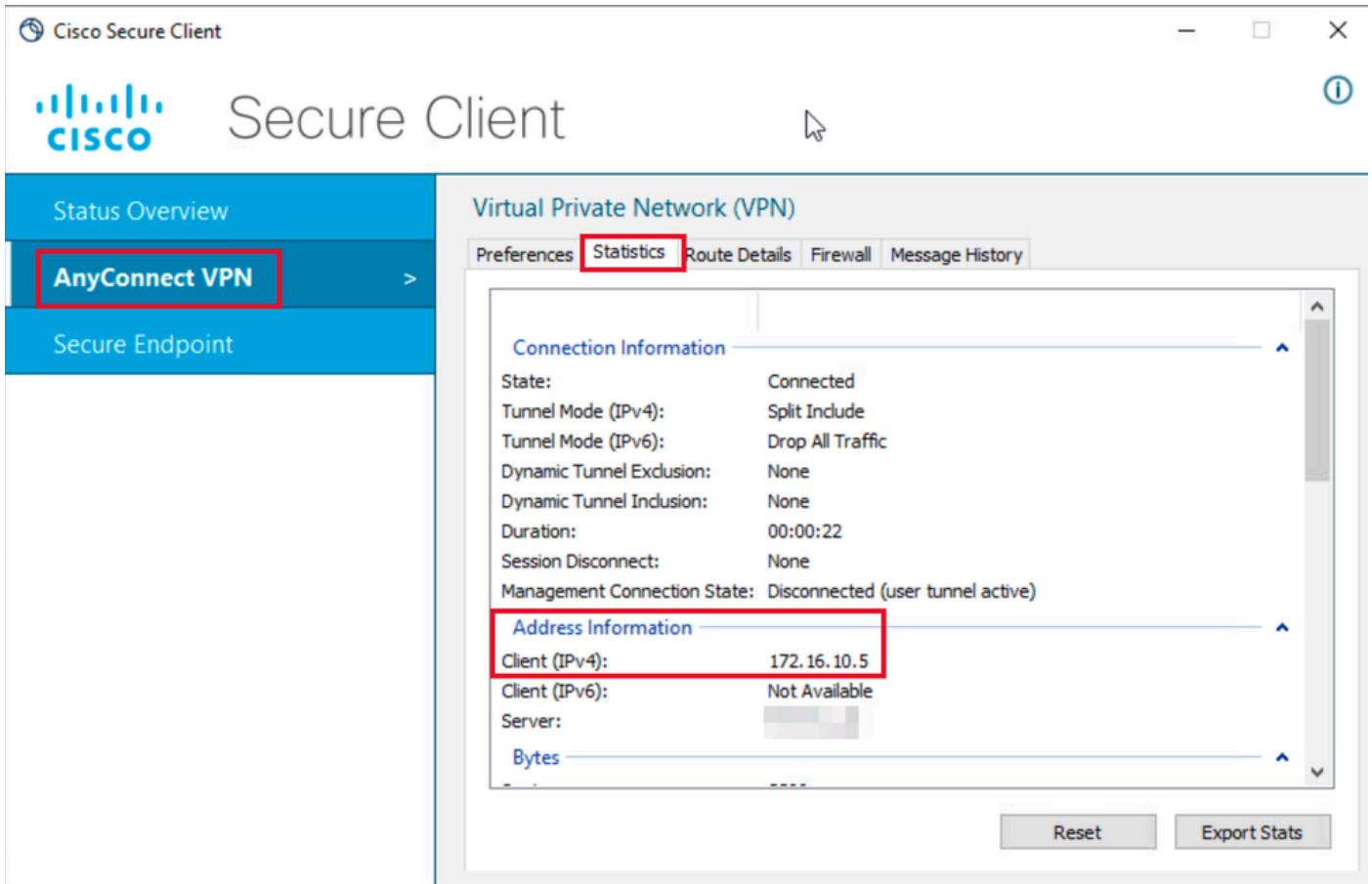
Überprüfung

Schritt 1: Navigieren Sie zu dem Client-Computer, auf dem CSC installiert ist. Stellen Sie eine Verbindung zum FlexVPN-Hub her, und geben Sie die Anmeldeinformationen user1 ein:



Benutzer1-Anmeldeinformationen

Schritt 2: Sobald die Verbindung hergestellt ist, klicken Sie auf das Zahnrad-Symbol (linke untere Ecke) und navigieren Sie zu AnyConnectVPN > Statistics. Bestätigen Sie im Abschnitt Address Information (Adressinformationen), dass die zugewiesene IP-Adresse zu dem für group1 konfigurierten Pool gehört:



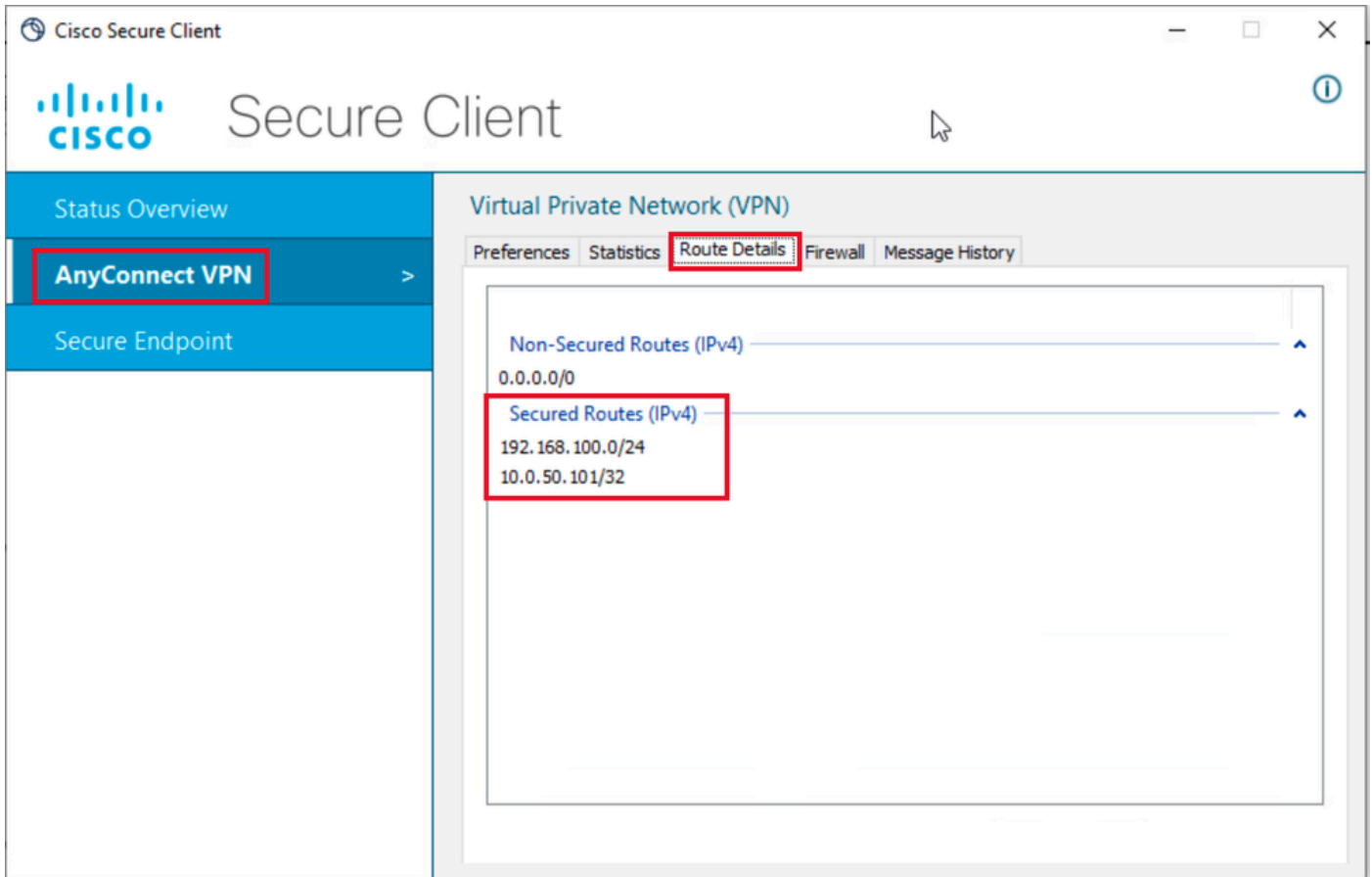
The screenshot shows the Cisco Secure Client interface. On the left, a navigation pane includes 'Status Overview', 'AnyConnect VPN' (highlighted with a red box), and 'Secure Endpoint'. The main window is titled 'Virtual Private Network (VPN)' and has tabs for 'Preferences', 'Statistics' (highlighted 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.

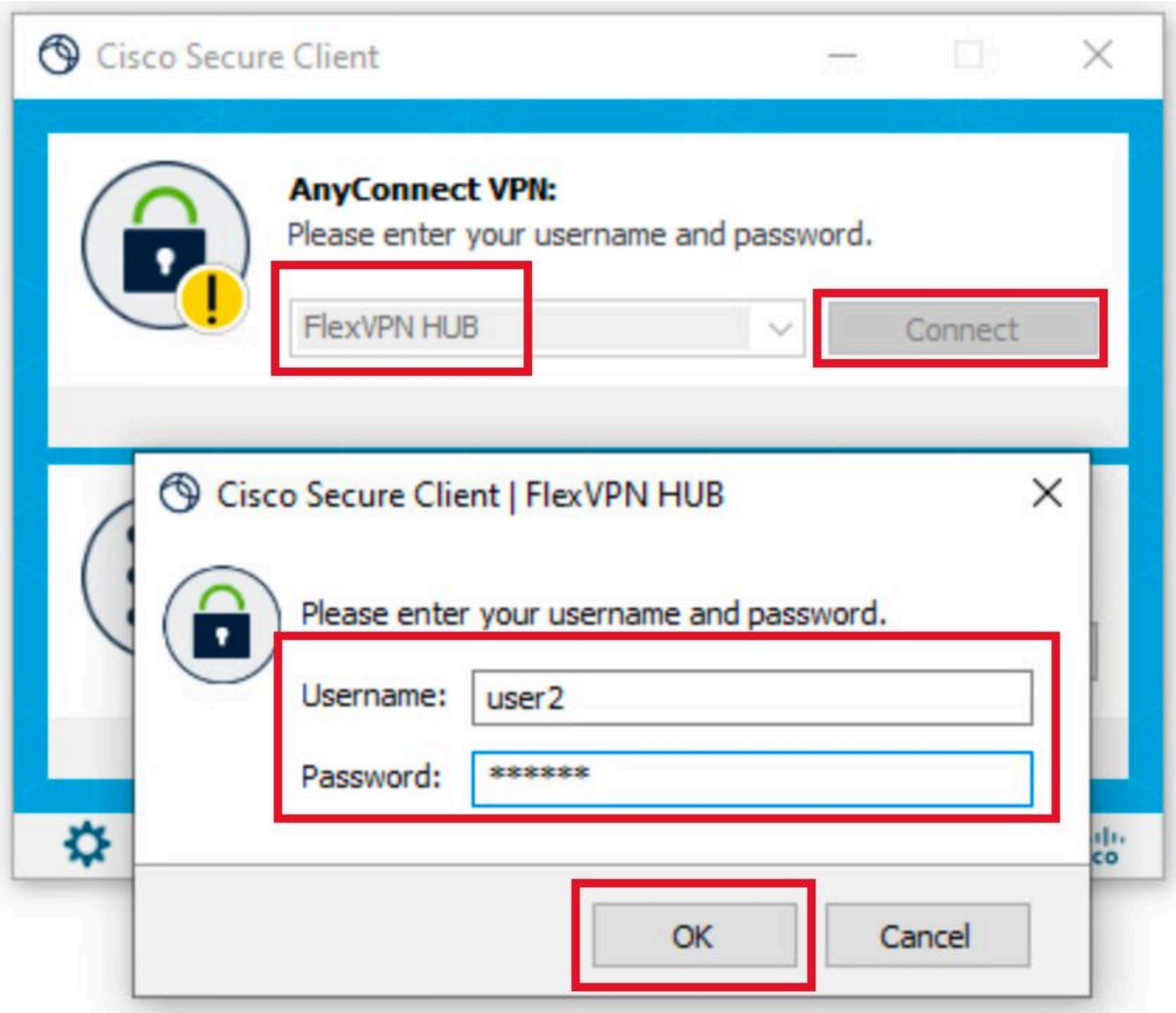
Benutzer1 Statistik

Navigieren Sie zu AnyConnectVPN > Route details, und stellen Sie sicher, dass die angezeigten Informationen den für Gruppe 1 konfigurierten sicheren Routen und DNS entsprechen:



Benutzer 1 - Routendetails

Schritt 3: Wiederholen Sie die Schritte 1 und 2 mit den Anmeldeinformationen user2, um zu überprüfen, ob die Informationen mit den Werten übereinstimmen, die in der ISE-Autorisierungsrichtlinie für diese Gruppe konfiguriert wurden:



Benutzer2-Anmeldeinformationen

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

Benutzer2-Statistik

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

Benutzer2 - Routendetails

Fehlerbehebung

Debugs und Protokolle

Auf dem Cisco Router:

1. Verwenden Sie das IKEv2- und IPSec-Debugging, um die Aushandlung zwischen dem Headend und dem Client zu überprüfen:

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

2. Verwenden Sie AAA-Debugging-Funktionen, um die Zuweisung von lokalen und/oder Remote-Attributen zu überprüfen:

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

Auf der ISE:

- RADIUS-Live-Protokolle

Arbeitsszenario

Die nächsten Ausgaben sind Beispiele für erfolgreiche Verbindungen:

- User1 Debug-Ausgabe:

<#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@OXH6]
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 Debug-Ausgabe:

```
<#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-phase1-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 down
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
```

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.