Konfigurieren von Secure Client IKEv2/ASA im ASDM mit AAA & Zertifizierungsauthentifizierung

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration eines sicheren Clients über IKEv2 auf ASA mit ASDM mit AAA und Zertifikatsauthentifizierung beschrieben.

Voraussetzungen

Anforderungen

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

- Konfiguration der Cisco Identity Services Engine (ISE)
- Konfiguration der Cisco Adaptive Security Virtual Appliance (ASAv)
- Konfiguration des Cisco Adaptive Security Device Manager (ASDM)
- VPN-Authentifizierungsablauf

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

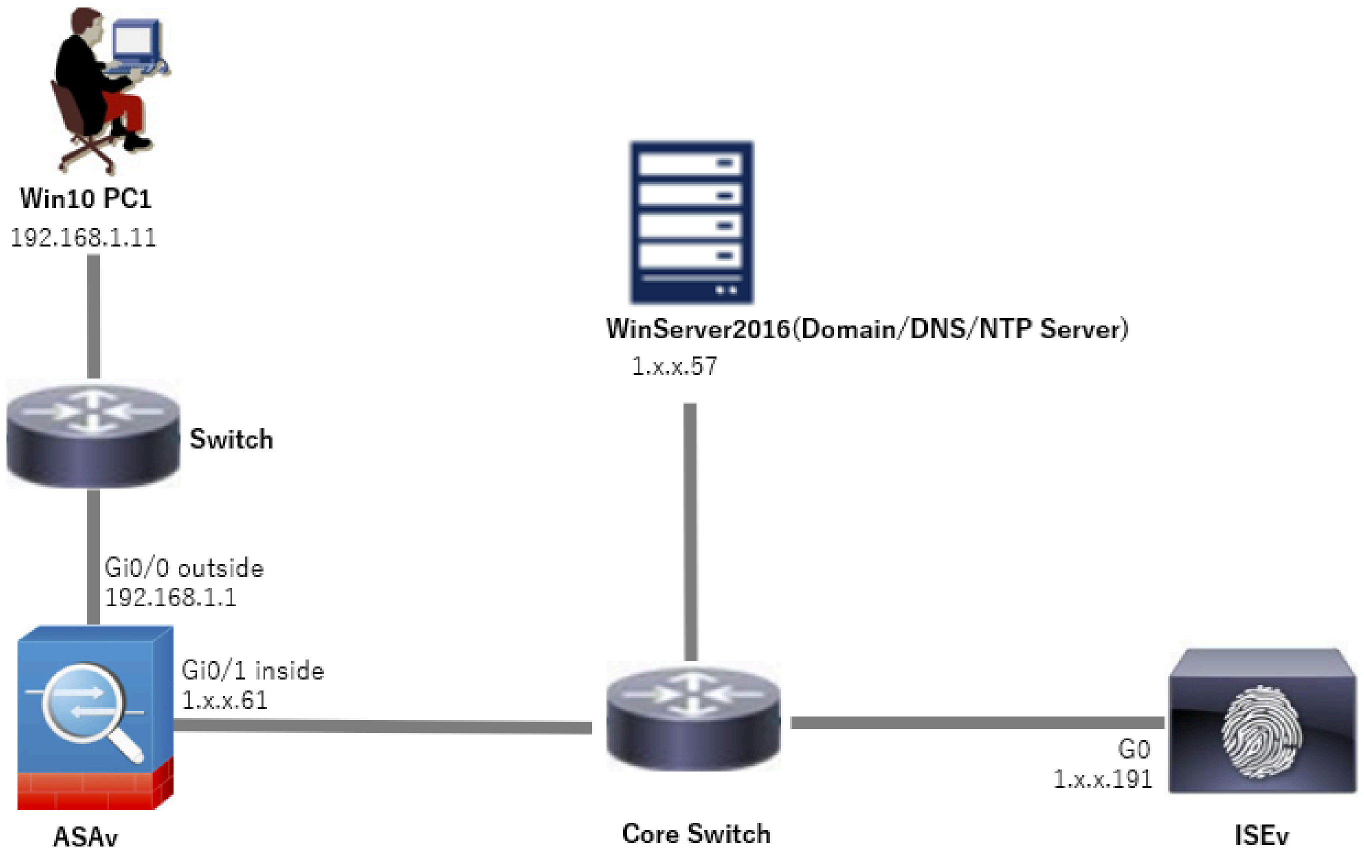
- Identity Services Engine Virtual 3.3 Patch 1
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

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.

Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.

Der unter Windows Server 2016 konfigurierte Domänenname ist ad.rem-system.com. Dies wird in diesem Dokument als Beispiel verwendet.



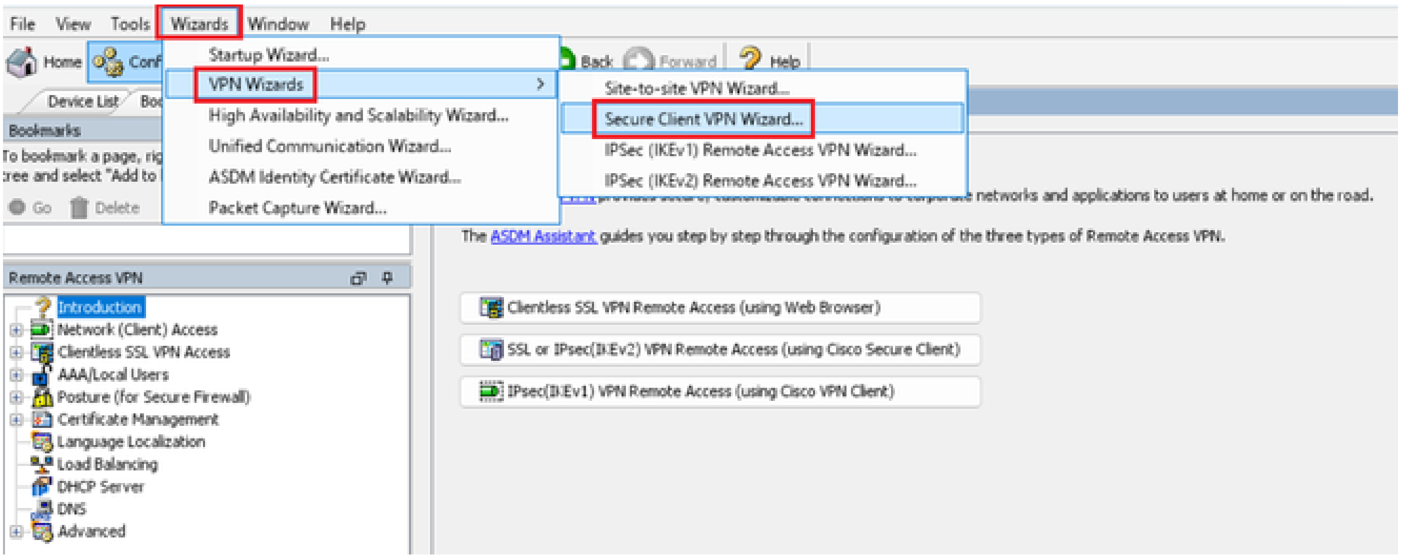
Netzwerkdiagramm

Konfigurationen

Konfiguration in ASDM

Schritt 1: Offene VPN-Assistenten

Navigieren Sie zu Wizards > VPN Wizards, und klicken Sie auf Secure Client VPN Wizard.

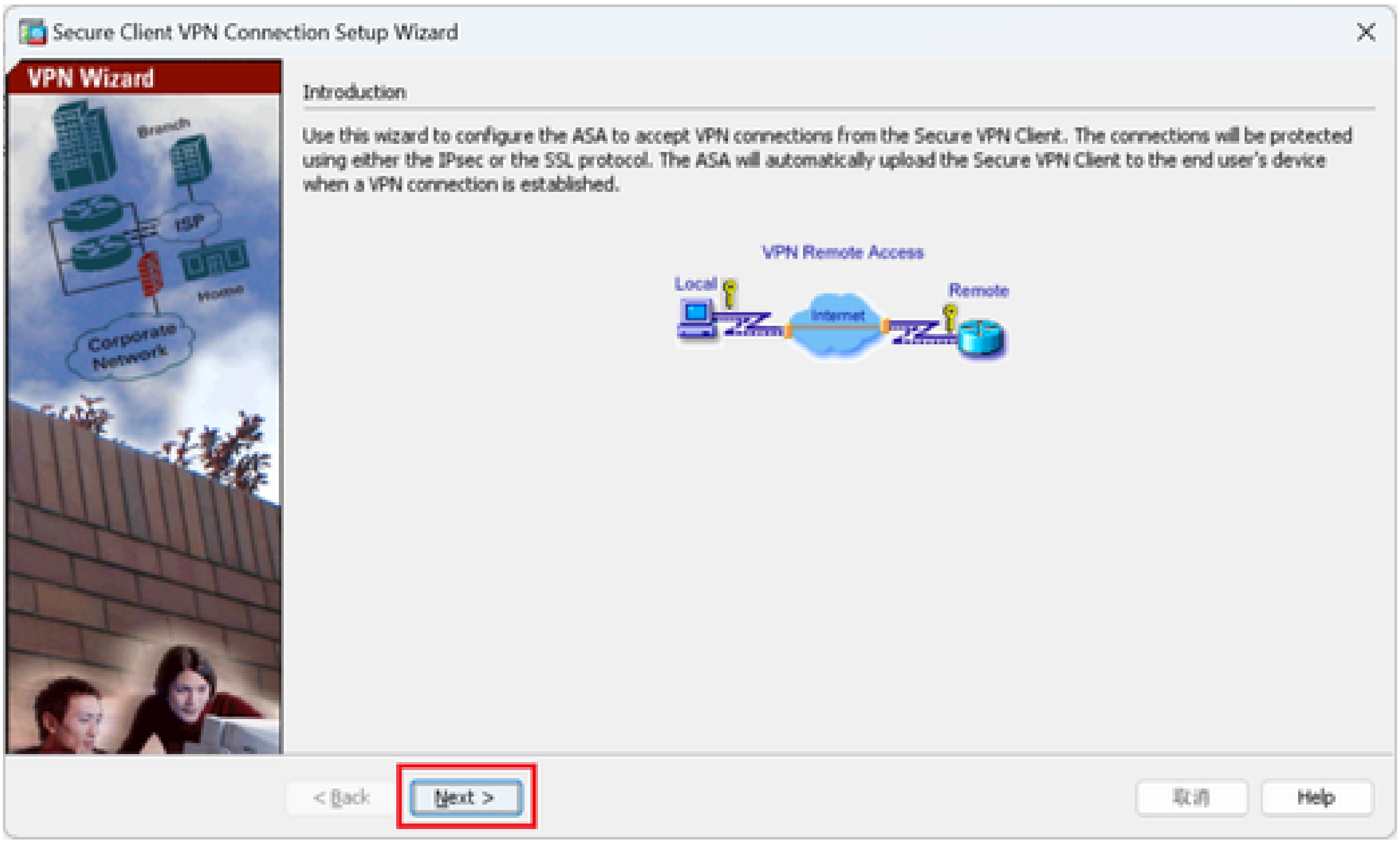

File View Tools Wizards Window Help
Home Conf
Back Forward Help
Device List Boo
Bookmarks
To bookmark a page, rig
tree and select "Add to
Go Delete
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
ASDM Identity Certificate Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
Secure Client VPN Wizard...
IPSec (IKEv1) Remote Access VPN Wizard...
IPSec (IKEv2) Remote Access VPN Wizard...
Remote Access VPN
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Posture (for Secure Firewall)
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Clientless SSL VPN Remote Access (using Web Browser)
SSL or IPsec(IKEv2) VPN Remote Access (using Cisco Secure Client)
IPsec(IKEv1) VPN Remote Access (using Cisco VPN Client)

networks and applications to users at home or on the road.

The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN.

Offene VPN-Assistenten

Klicken Sie auf Next (Weiter).



Secure Client VPN Connection Setup Wizard

VPN Wizard

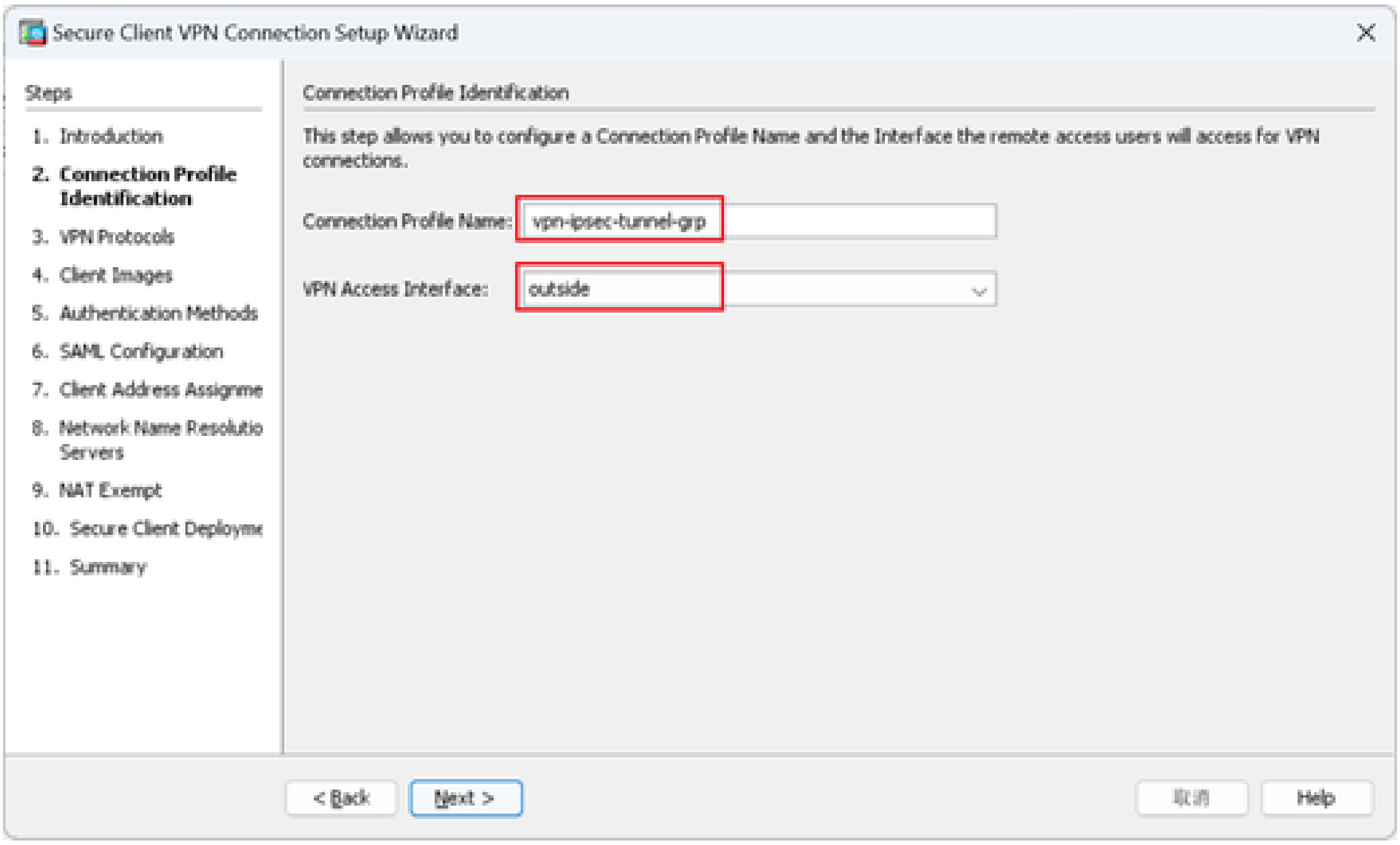
Introduction

Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the Secure VPN Client to the end user's device when a VPN connection is established.

Klicken Sie auf Weiter

Schritt 2: Verbindungsprofilidentifizierung

Eingabeinformationen für das Verbindungsprofil.
Name des Verbindungsprofils: vpn-ipsec-tunnel-grp
VPN-Zugriffsschnittstelle: außen



Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
< Back
Next >
取消
Help

Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

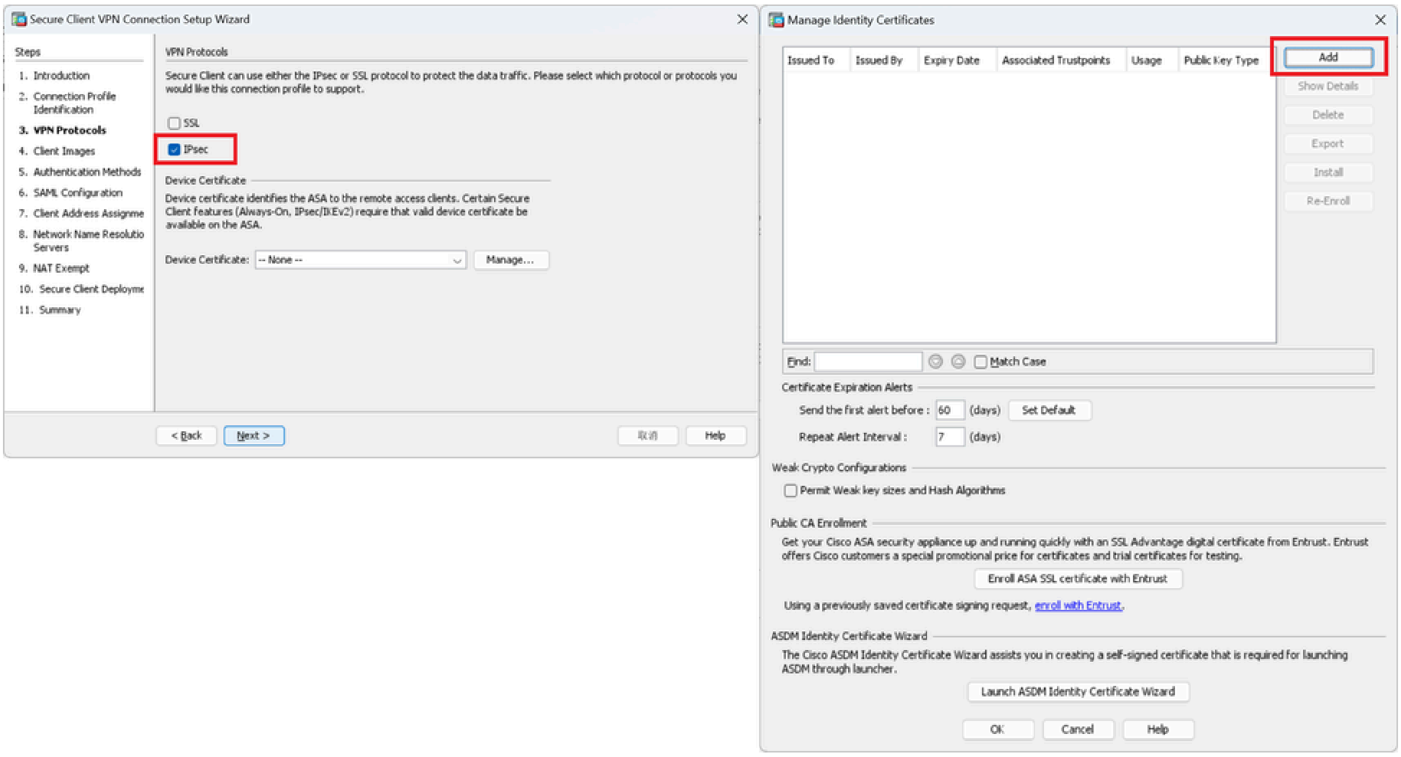
Connection Profile Name: vpn-ipsec-tunnel-grp

VPN Access Interface: outside

Verbindungsprofilidentifizierung

Schritt 3: VPN-Protokolle

Wählen Sie IPsec aus, und klicken Sie auf Hinzufügen, um ein neues selbstsigniertes Zertifikat hinzuzufügen.



Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
Manage...
< Back
Next >
取消
Help
Manage Identity Certificates
Add
Show Details
Delete
Export
Install
Re-Enroll
Find:
Set Default
Enroll ASA SSL certificate with Entrust
Launch ASDM Identity Certificate Wizard
OK
Cancel
Help

VPN Protocols

Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

□ SSL

☑ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: -- None --

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

□ Match Case

Certificate Expiration Alerts

Send the first alert before : 60 (days)

Repeat Alert Interval : 7 (days)

Weak Crypto Configurations

□ Permit Weak key sizes and Hash Algorithms

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certificate signing request, enroll with Entrust.

ASDM Identity Certificate Wizard

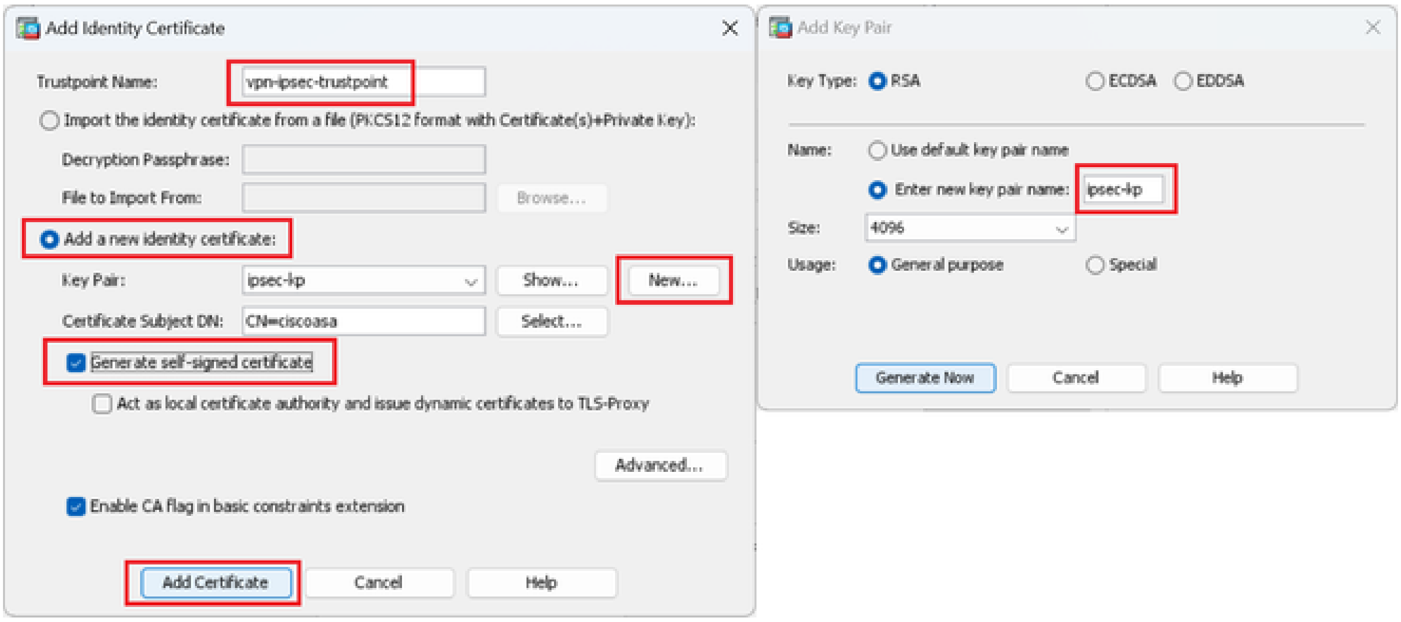
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

VPN-Protokolle

Eingabeinformationen für selbstsigniertes Zertifikat.

Vertrauenspunktname: vpn-ipsec-trustpoint

Schlüsselpaar: ipsec-kp



Add Identity Certificate

Trustpoint Name: vpn-ipsec-trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From: Browse...

● Add a new identity certificate:

Key Pair: ipsec-kp Show... New...

Certificate Subject DN: CN=ciscoasa Select...

☑ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced...

☑ Enable CA flag in basic constraints extension

Add Certificate Cancel Help

Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

● Enter new key pair name: ipsec-kp

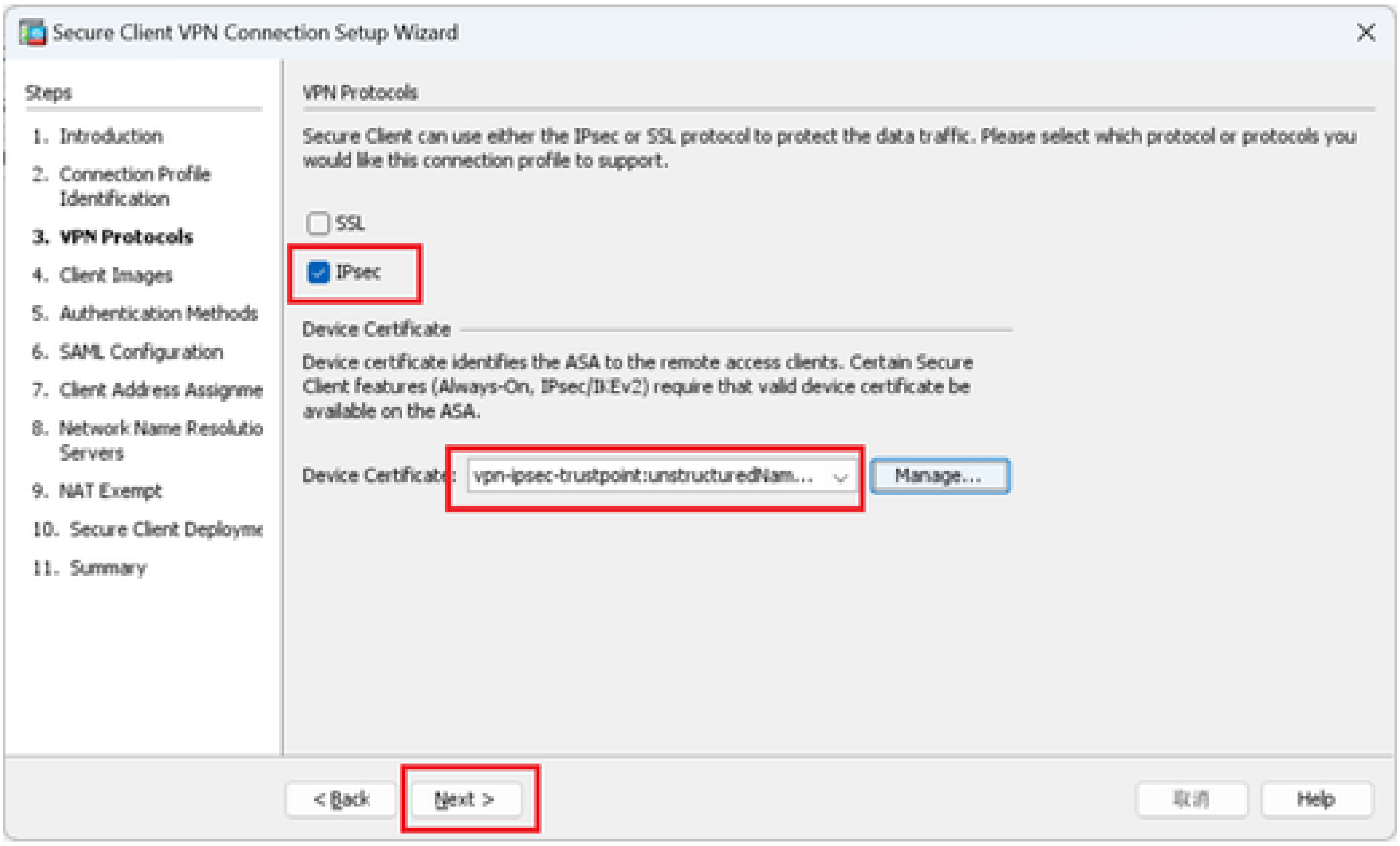
Size: 4096

Usage: ● General purpose ○ Special

Generate Now Cancel Help

Detail des selbstsignierten Zertifikats

Bestätigen Sie die Einstellungen der VPN-Protokolle, und klicken Sie auf die Schaltfläche Weiter.



Secure Client VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. **VPN Protocols**
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

VPN Protocols

Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

□ SSL

☑ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

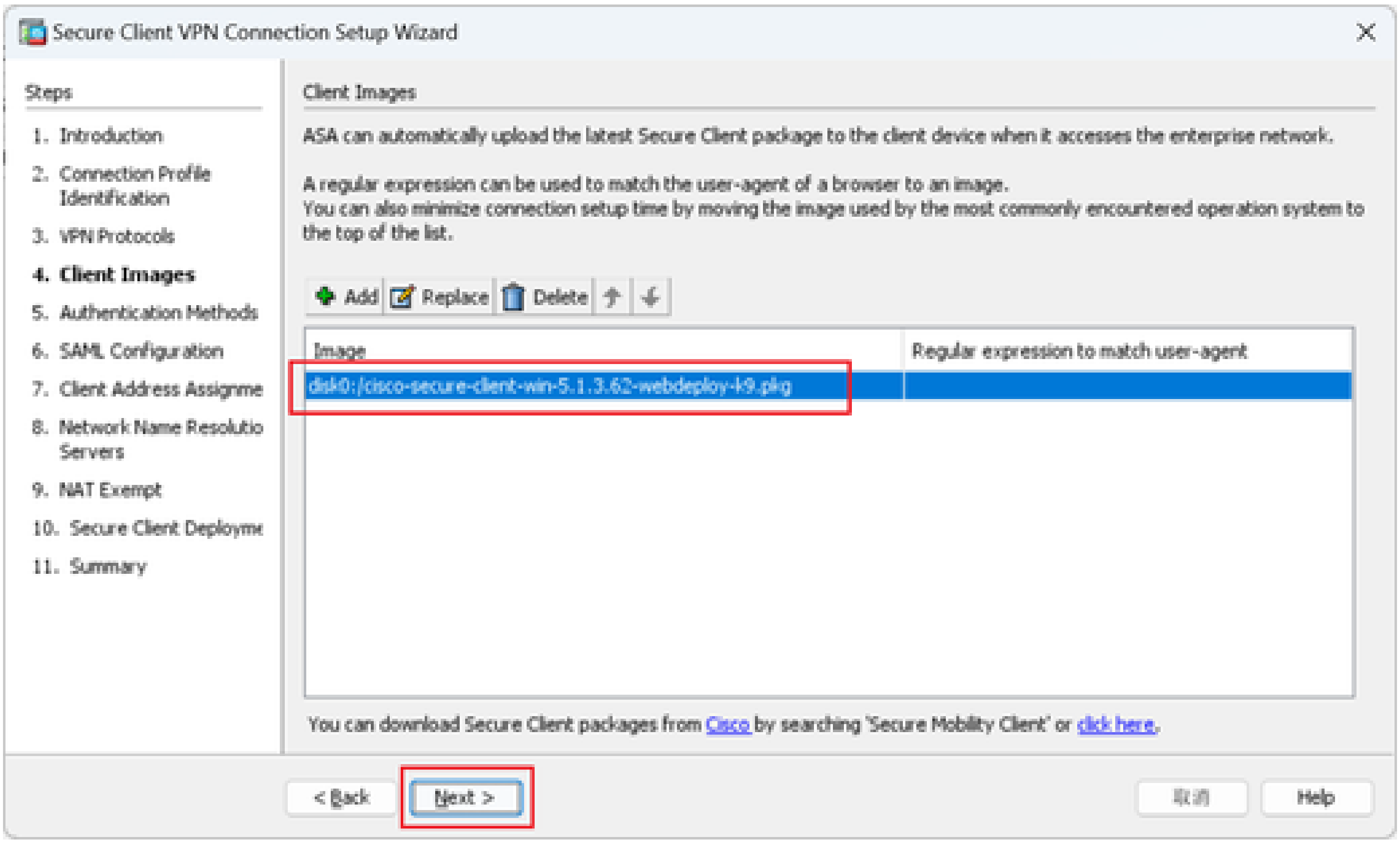
Device Certificate: vpn-ipsec-trustpoint:unstructuredNam... Manage...

< Back Next > 取消 Help

Einstellungen des VPN-Protokolls bestätigen

Schritt 4: Client-Images

Klicken Sie auf die Schaltfläche Hinzufügen, um ein sicheres Client-Image hinzuzufügen, und klicken Sie auf die Schaltfläche Weiter.


Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
Add
Replace
Delete
< Back
Next >
取消
Help

Client Images

ASA can automatically upload the latest Secure Client package to the client device when it accesses the enterprise network.

A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg	

You can download Secure Client packages from Cisco by searching 'Secure Mobility Client' or click here.

Client-Images

Schritt 5: Authentifizierungsmethoden

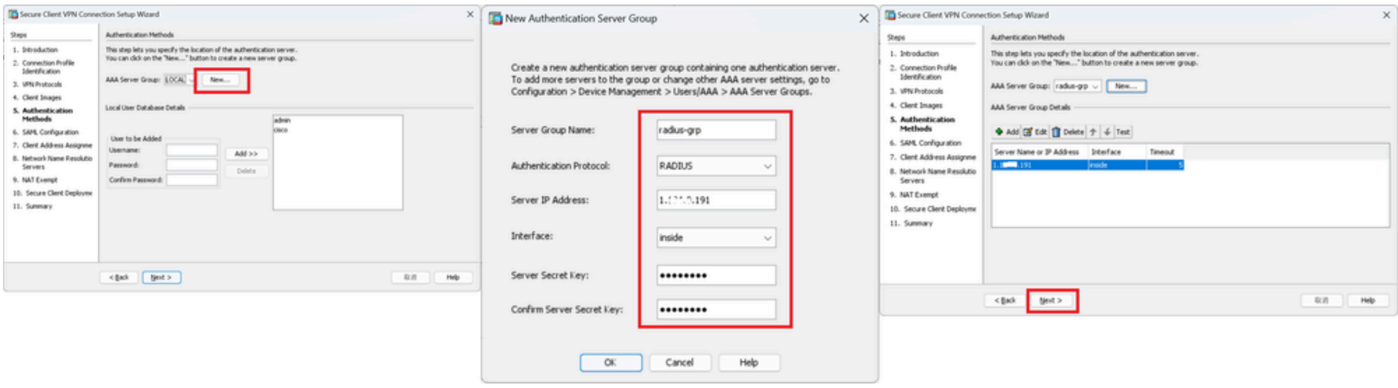
Klicken Sie auf die Schaltfläche Neu, um einen neuen AAA-Server hinzuzufügen, und klicken Sie auf die Schaltfläche Weiter.

Server-Gruppenname: radius-grp

Authentifizierungsprotokoll: RADIUS

Server-IP-Adresse: 1.x.x.191

Schnittstelle : innen



Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

AAA Server Group: LOCAL

Local User Database Details

User to be Added
Username:
Password:
Confirm Password:

admin
cisco

New Authentication Server Group

Create a new authentication server group containing one authentication server.
To add more servers to the group or change other AAA server settings, go to
Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: radius-grp
Authentication Protocol: RADIUS
Server IP Address: 1.[redacted].191
Interface: inside
Server Secret Key: ••••••••
Confirm Server Secret Key: ••••••••

AAA Server Group: radius-grp

AAA Server Group Details

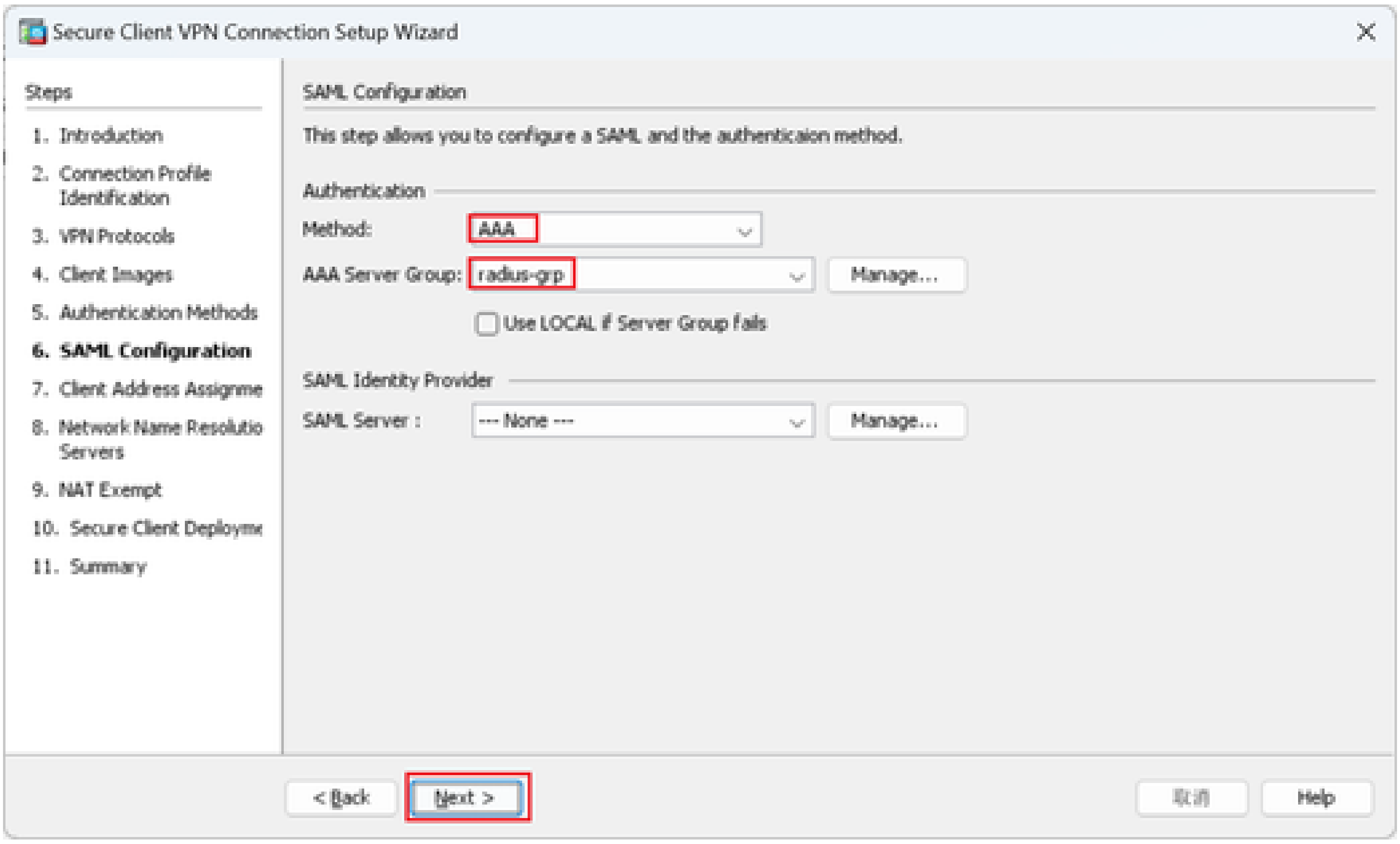
Server Name or IP Address	Interface	Timeout
1.[redacted].191	inside	5

Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
New...
Add >>
Delete
Add
Edit
Delete
Test
OK
Cancel
Help
< Back
Next >
取消
Help

Authentifizierungsmethoden

Schritt 6: SAML-Konfiguration

Klicken Sie auf die Schaltfläche Weiter.



SAML Configuration

This step allows you to configure a SAML and the authenticaion method.

Authentication

Method: AAA

AAA Server Group: radius-grp

☐ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : --- None ---

Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
Manage...
Manage...
< Back
Next >
取消
Help

SAML-Konfiguration

Schritt 7. Client-Adressenzuweisung

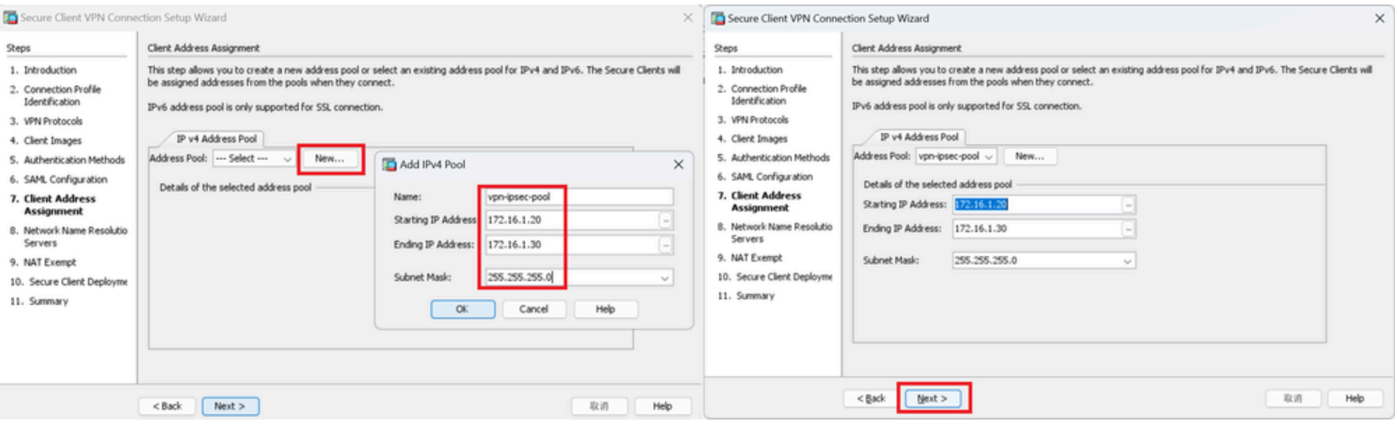
Klicken Sie auf die Schaltfläche Neu, um einen neuen IPv4-Pool hinzuzufügen, und klicken Sie auf die Schaltfläche Weiter.

Name: vpn-ipsec-pool

Start-IP-Adresse: 172.16.1.20

End-IP-Adresse: 172.16.1.30

Subnetzmaske: 255.255.255.0



Secure Client VPN Connection Setup Wizard

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The Secure Clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

IP v4 Address Pool

Address Pool: --- Select ---

Add IPv4 Pool

Name: vpn-ipsec-pool

Starting IP Address: 172.16.1.20

Ending IP Address: 172.16.1.30

Subnet Mask: 255.255.255.0

Address Pool: vpn-ipsec-pool

Details of the selected address pool

Starting IP Address: 172.16.1.20

Ending IP Address: 172.16.1.30

Subnet Mask: 255.255.255.0

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignment
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
New...
OK
Cancel
Help
< Back
Next >
取消
Help

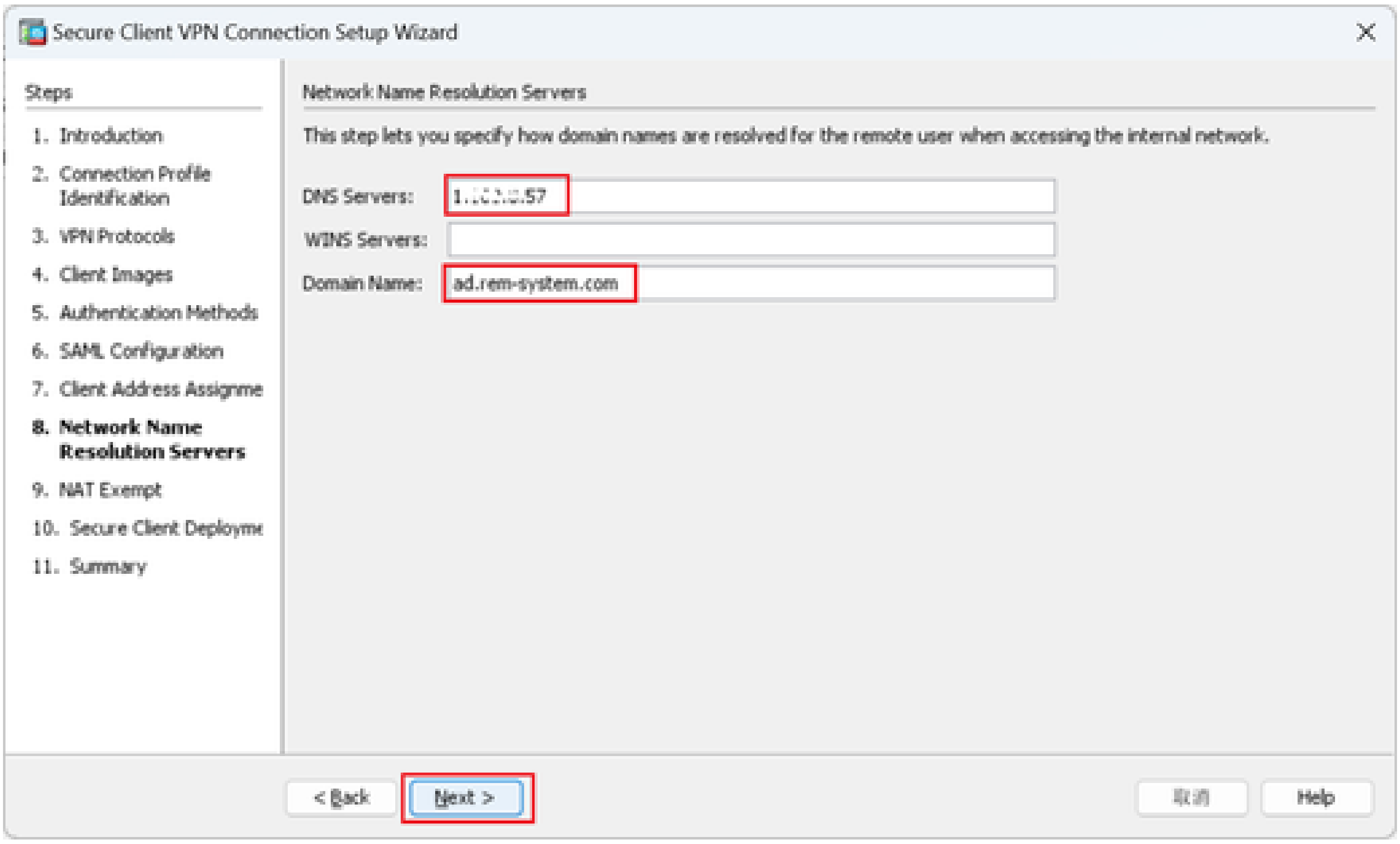
Client-Adresse zuweisen

Schritt 8: Server für die Netzwerknamensauflösung

Geben Sie Informationen für DNS und Domäne ein, und klicken Sie auf die Schaltfläche Weiter.

DNS-Server: 1.x.x.57

Domänenname: ad.rem-system.com



Secure Client VPN Connection Setup Wizard

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 1.[redacted].57

WINS Servers:

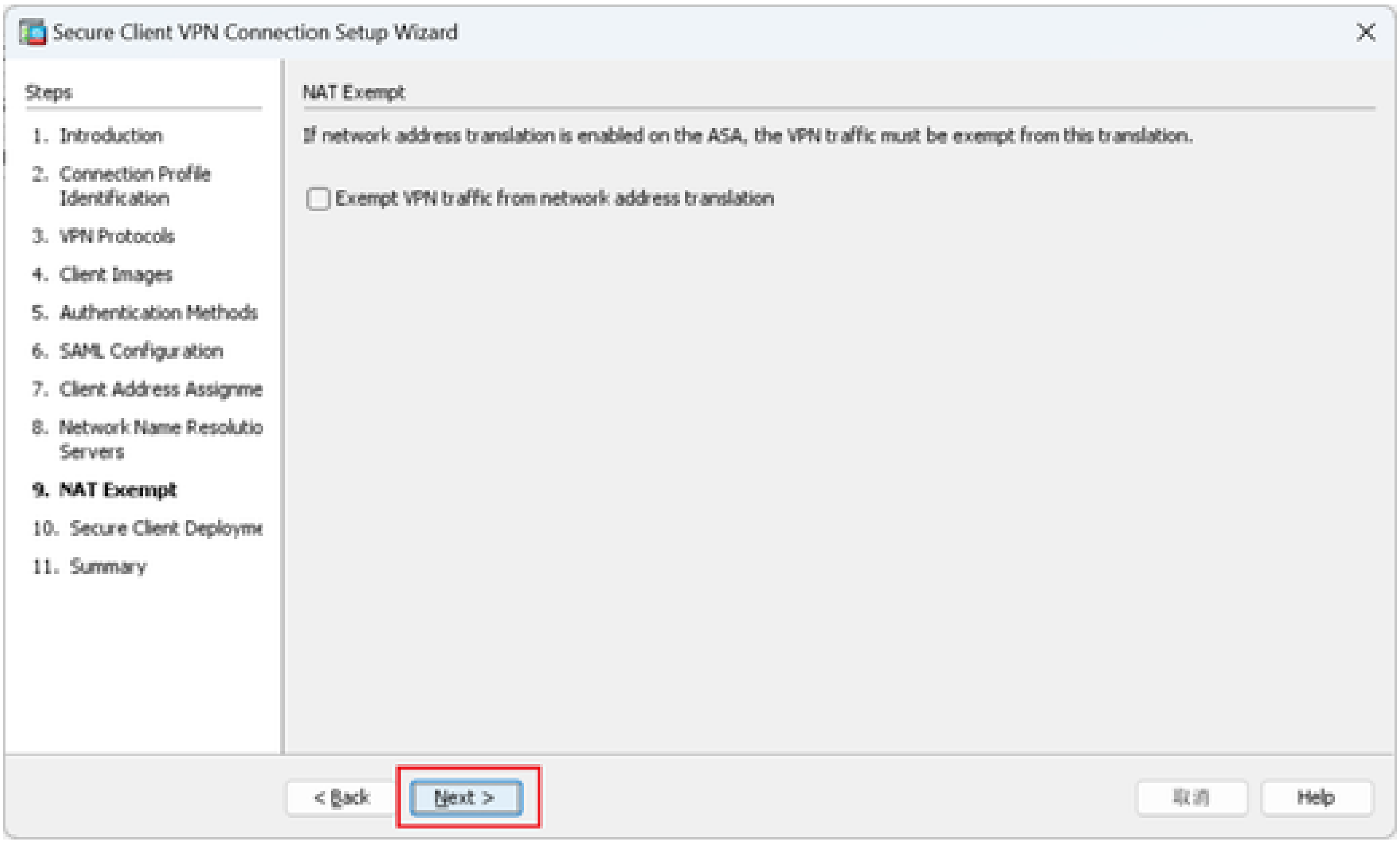
Domain Name: ad.rem-system.com

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolution Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
< Back
Next >
取消
Help

Server für die Netzwerknamensauflösung

Schritt 9. NAT-Ausnahme

Klicken Sie auf die Schaltfläche Weiter.


Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
< Back
Next >
取消
Help

NAT Exempt

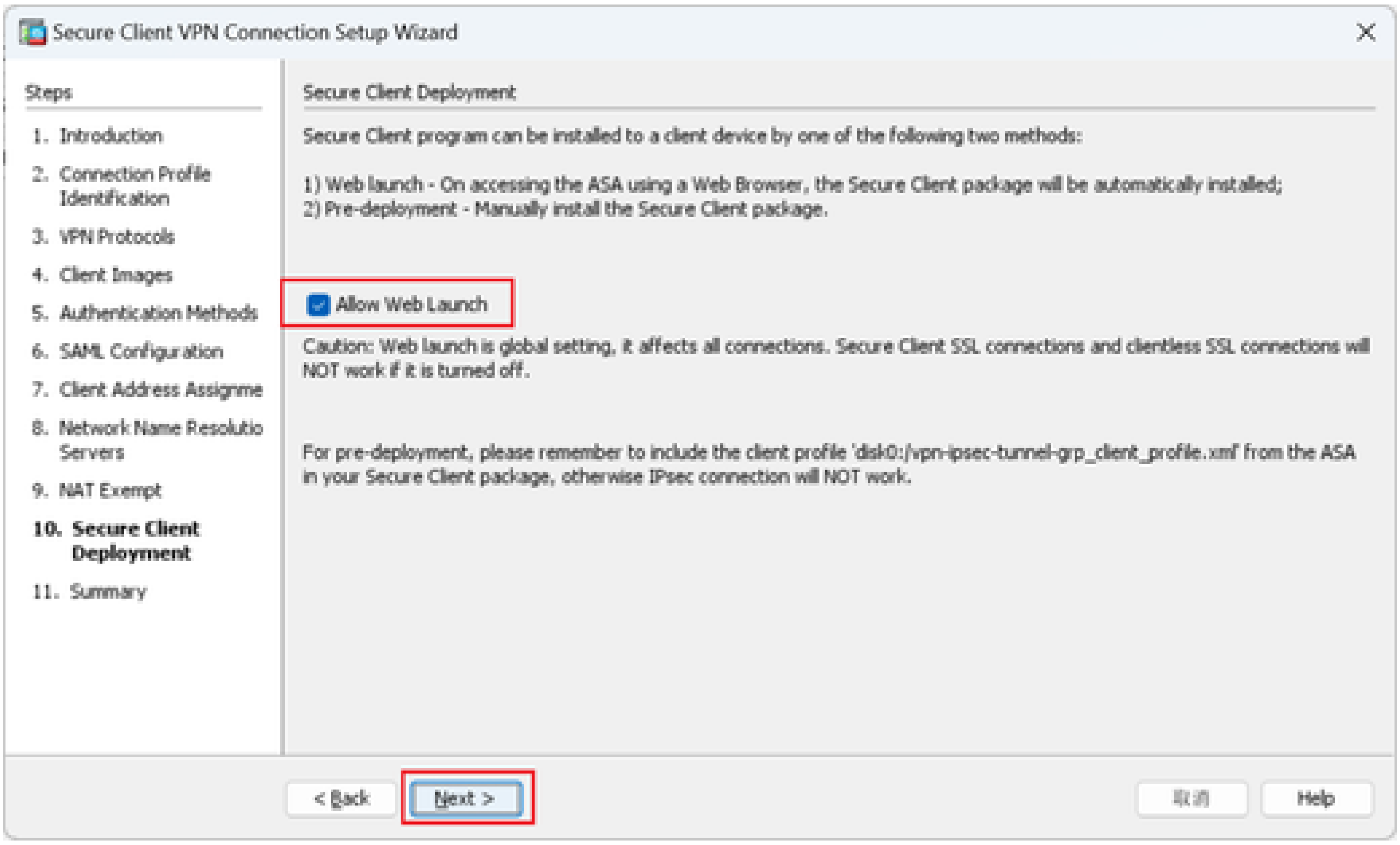
If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

□ Exempt VPN traffic from network address translation

NAT-Ausnahme

Schritt 10. Sichere Client-Bereitstellung

Wählen Sie Web-Start zulassen aus, und klicken Sie auf die Schaltfläche Weiter.


Secure Client VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployment
11. Summary
< Back
Next >
取消
Help

Secure Client Deployment

Secure Client program can be installed to a client device by one of the following two methods:

1) Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed;
2) Pre-deployment - Manually install the Secure Client package.

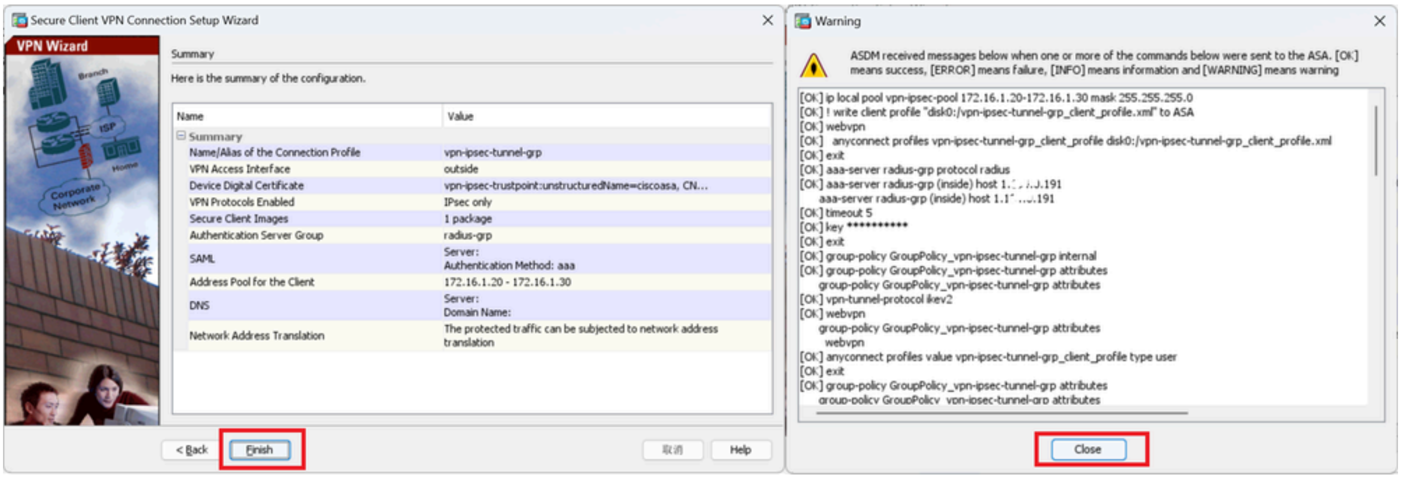
☑ Allow Web Launch

Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will NOT work if it is turned off.

For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA in your Secure Client package, otherwise IPsec connection will NOT work.

Schritt 11. Einstellungen speichern

Klicken Sie auf Fertig stellen, und speichern Sie die Einstellungen.



Summary

Here is the summary of the configuration.

Name	Value
Summary	
Name/Alias of the Connection Profile	vpn-ipsec-tunnel-grp
VPN Access Interface	outside
Device Digital Certificate	vpn-ipsec-trustpoint:unstructuredName=ciscoasa, CN...
VPN Protocols Enabled	IPsec only
Secure Client Images	1 package
Authentication Server Group	radius-grp
SAML	Server: Authentication Method: aaa
Address Pool for the Client	172.16.1.20 - 172.16.1.30
DNS	Server: Domain Name:
Network Address Translation	The protected traffic can be subjected to network address translation

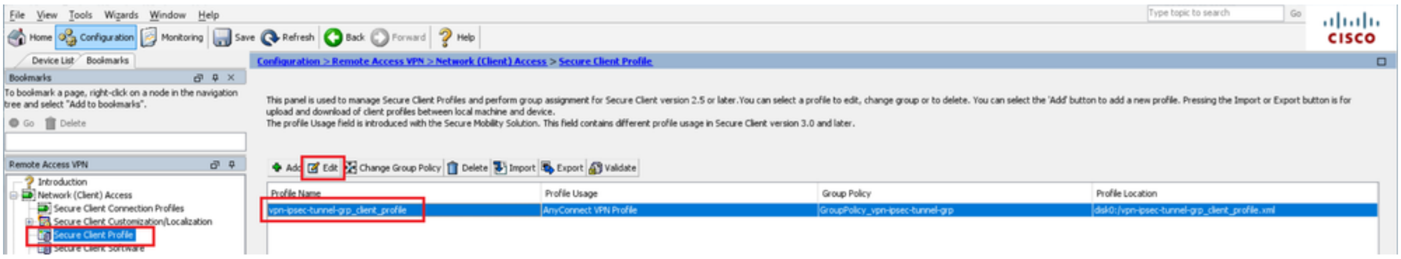
ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

```
[OK] ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0
[OK] ! write client profile "disk0:/vpn-ipsec-tunnel-grp_client_profile.xml" to ASA
[OK] webvpn
[OK]   anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
[OK] exit
[OK] aaa-server radius-grp protocol radius
[OK] aaa-server radius-grp (inside) host 1.[illegible].191
     aaa-server radius-grp (inside) host 1.1[illegible].191
[OK] timeout 5
[OK] key **********
[OK] exit
[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal
[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
     group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
[OK] vpn-tunnel-protocol ikev2
[OK] webvpn
     group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
      webvpn
[OK] anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user
[OK] exit
[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
     group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
```

Einstellungen speichern

Schritt 12: Sicheres Clientprofil bestätigen und exportieren

Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile, und klicken Sie auf die Schaltfläche Edit.



Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile

Bookmarks

To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

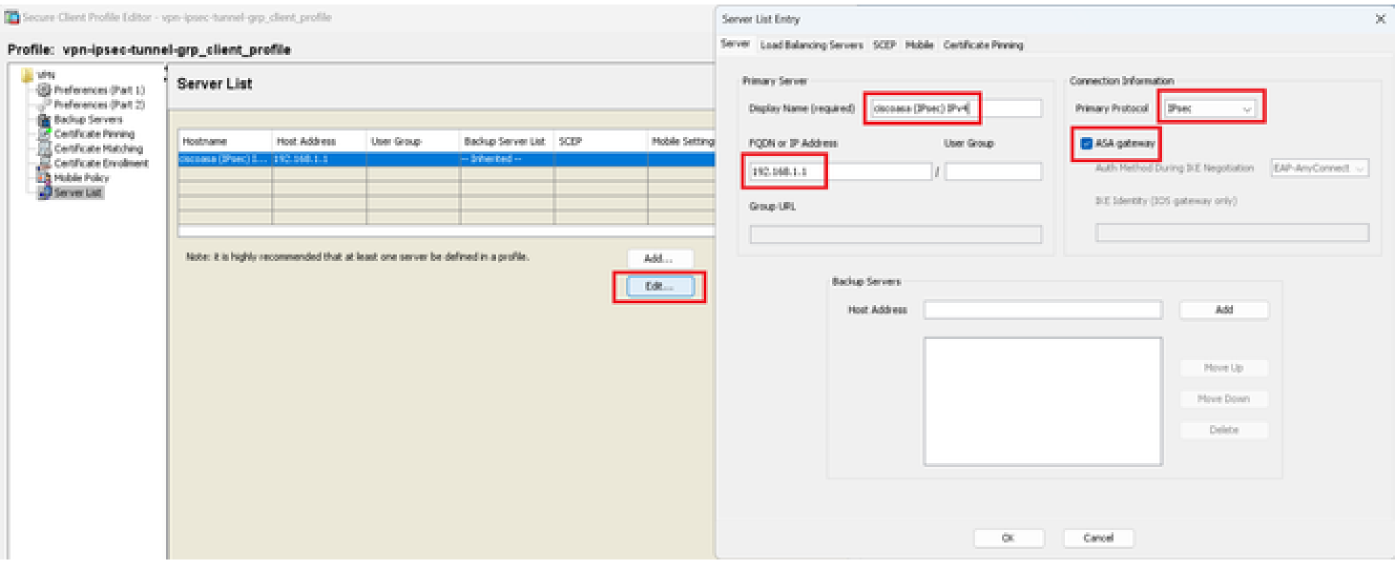
This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in Secure Client version 3.0 and later.

Profile Name	Profile Usage	Group Policy	Profile Location
vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml

Sicheres Clientprofil bearbeiten

Bestätigen Sie die Profildetails.

- Anzeigename (erforderlich): Cisco ASA (IPsec) IPv4
- FQDN oder IP-Adresse: 192.168.1.1
- Primäres Protokoll: IPsec



Profile: vpn-ipsec-tunnel-grp_client_profile

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Setting
ciscoasa (IPsec) I...	192.168.1.1		-- Inherited --		

Note: it is highly recommended that at least one server be defined in a profile.

Server List Entry

Primary Server

Display Name (required): ciscoasa (IPsec) IPv4

FQDN or IP Address: 192.168.1.1

Connection Information

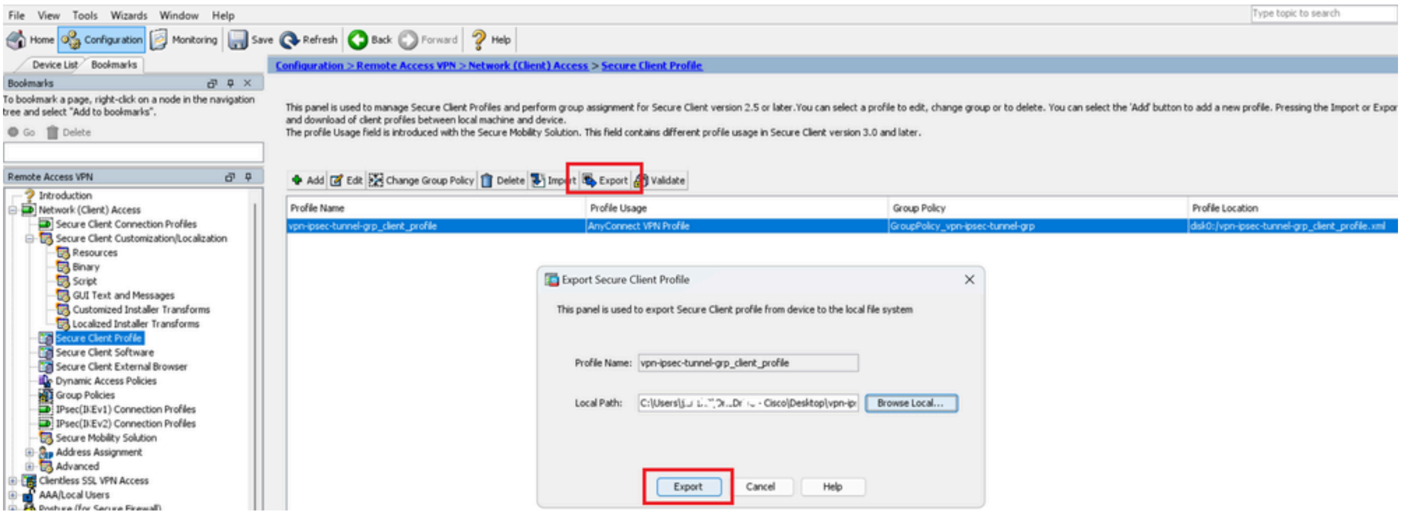
Primary Protocol: IPsec

☑ ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

Sicheres Clientprofil bestätigen

Klicken Sie auf die Schaltfläche Exportieren, um das Profil auf den lokalen PC zu exportieren.



Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile

This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Expor and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in Secure Client version 3.0 and later.

Profile Name	Profile Usage	Group Policy	Profile Location
vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml

Export Secure Client Profile

This panel is used to export Secure Client profile from device to the local file system

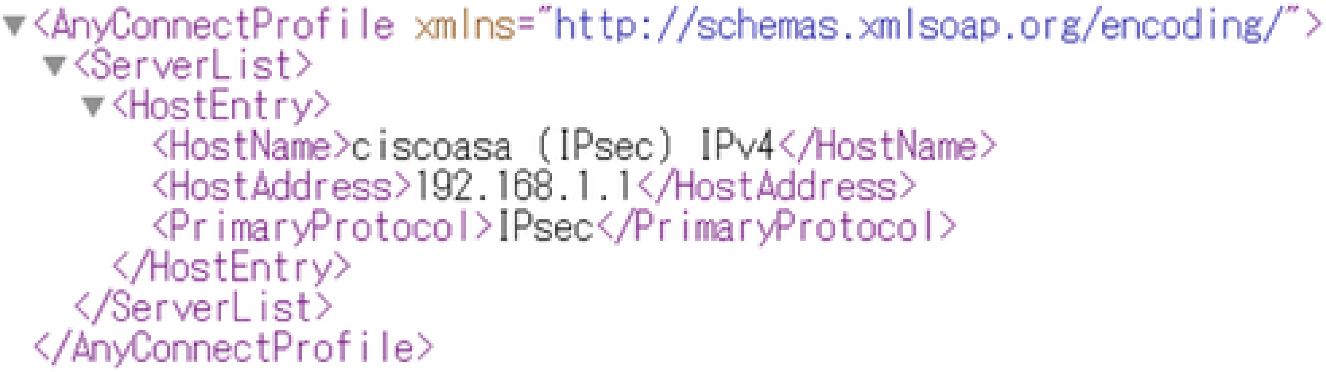
Profile Name: vpn-ipsec-tunnel-grp_client_profile

Local Path: C:\Users\...\Cisco\Desktop\vpn-ip

Sicheres Clientprofil exportieren

Schritt 13: Details des sicheren Clientprofils bestätigen

Öffnen Sie Secure Client Profile by browser, und stellen Sie sicher, dass das primäre Protokoll für den Host IPsec ist.



```
▼<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">
  ▼<ServerList>
    ▼<HostEntry>
        <HostName>ciscoasa (IPsec) IPv4</HostName>
        <HostAddress>192.168.1.1</HostAddress>
        <PrimaryProtocol>IPsec</PrimaryProtocol>
      </HostEntry>
    </ServerList>
  </AnyConnectProfile>
```

Details zum sicheren Clientprofil

Schritt 14: Bestätigen der Einstellungen in der ASA CLI

Bestätigen Sie die von ASDM in der ASA CLI erstellten IPsec-Einstellungen.

```
// Defines a pool of addresses
ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0

// Defines radius server
aaa-server radius-grp protocol radius
aaa-server radius-grp (inside) host 1.x.x.191
timeout 5

// Define the transform sets that IKEv2 can use
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1

// Configures the crypto map to use the IKEv2 transform-sets
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside

// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
crl configure

// Defines self-signed certificate
crypto ca certificate chain vpn-ipsec-trustpoint
certificate 6651a2a2
308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b
......
ac76f984 efd41d13 073d0be6 f923a9c6 7b
quit

// IKEv2 Policies
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 10
```

```
encryption aes-192
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 40
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400

// Enabling client-services on the outside interface
crypto ikev2 enable outside client-services port 443

// Specifiies the certificate the ASA uses for IKEv2
crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint

// Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
enable
anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1
anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
anyconnect enable
tunnel-group-list enable

// Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile
group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal
group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
wins-server none
dns-server value 1.x.x.57
vpn-tunnel-protocol ikev2
default-domain value ad.rem-system.com
webvpn
anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user

// Ties the pool of addressess to the vpn connection
tunnel-group vpn-ipsec-tunnel-grp type remote-access
tunnel-group vpn-ipsec-tunnel-grp general-attributes
address-pool vpn-ipsec-pool
authentication-server-group radius-grp
default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp
tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes
group-alias vpn-ipsec-tunnel-grp enable
```

Schritt 15: Verschlüsselungsalgorithmus hinzufügen

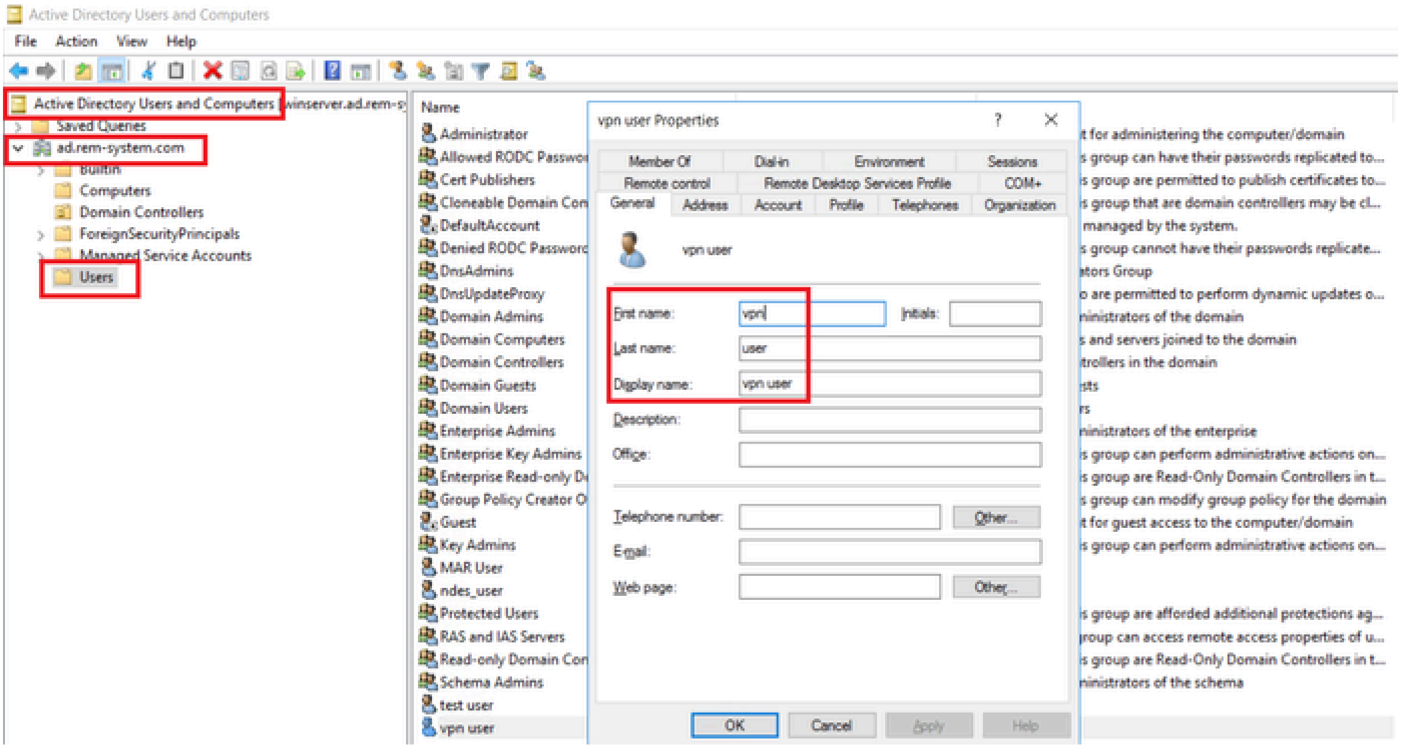
Fügen Sie in der ASA CLI Gruppe 19 zur IKEv2-Richtlinie hinzu.

Hinweis: Für IKEv2/IPsec-Verbindungen unterstützt der Cisco Secure Client seit Version 4.9.00086 nicht mehr die Diffie-Hellman (DH)-Gruppen 2, 5, 14 und 24. Diese Änderung kann aufgrund von nicht übereinstimmenden kryptografischen Algorithmen zu Verbindungsfehlern führen.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#
```

Konfiguration in Windows Server

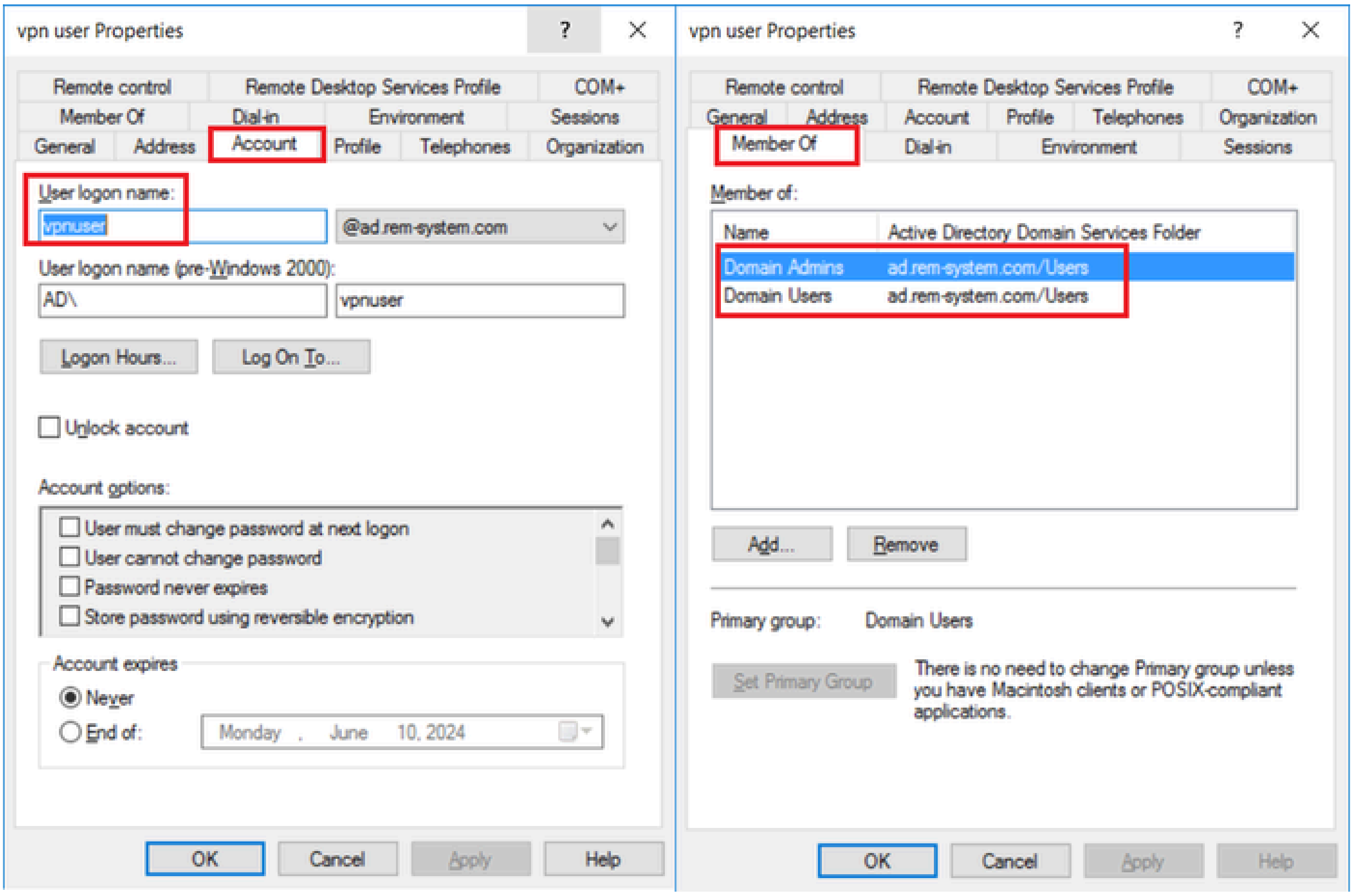
Sie müssen einen Domänenbenutzer für die VPN-Verbindung hinzufügen. Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Benutzer. Fügen Sie vpnuser als Domänenbenutzer hinzu.



First name: vpn
Initials:
Last name: user
Display name: vpn user
Description:
Office:

Domänenbenutzer hinzufügen

Fügen Sie den Domänenbenutzer einem Mitglied von Domänenadministratoren und Domänenbenutzern hinzu.



User logon name: vpnuser @ad.rem-system.com

User logon name (pre-Windows 2000): AD\ vpnuser

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Monday , June 10, 2024

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	ad.rem-system.com/Users
Domain Users	ad.rem-system.com/Users

Primary group: Domain Users

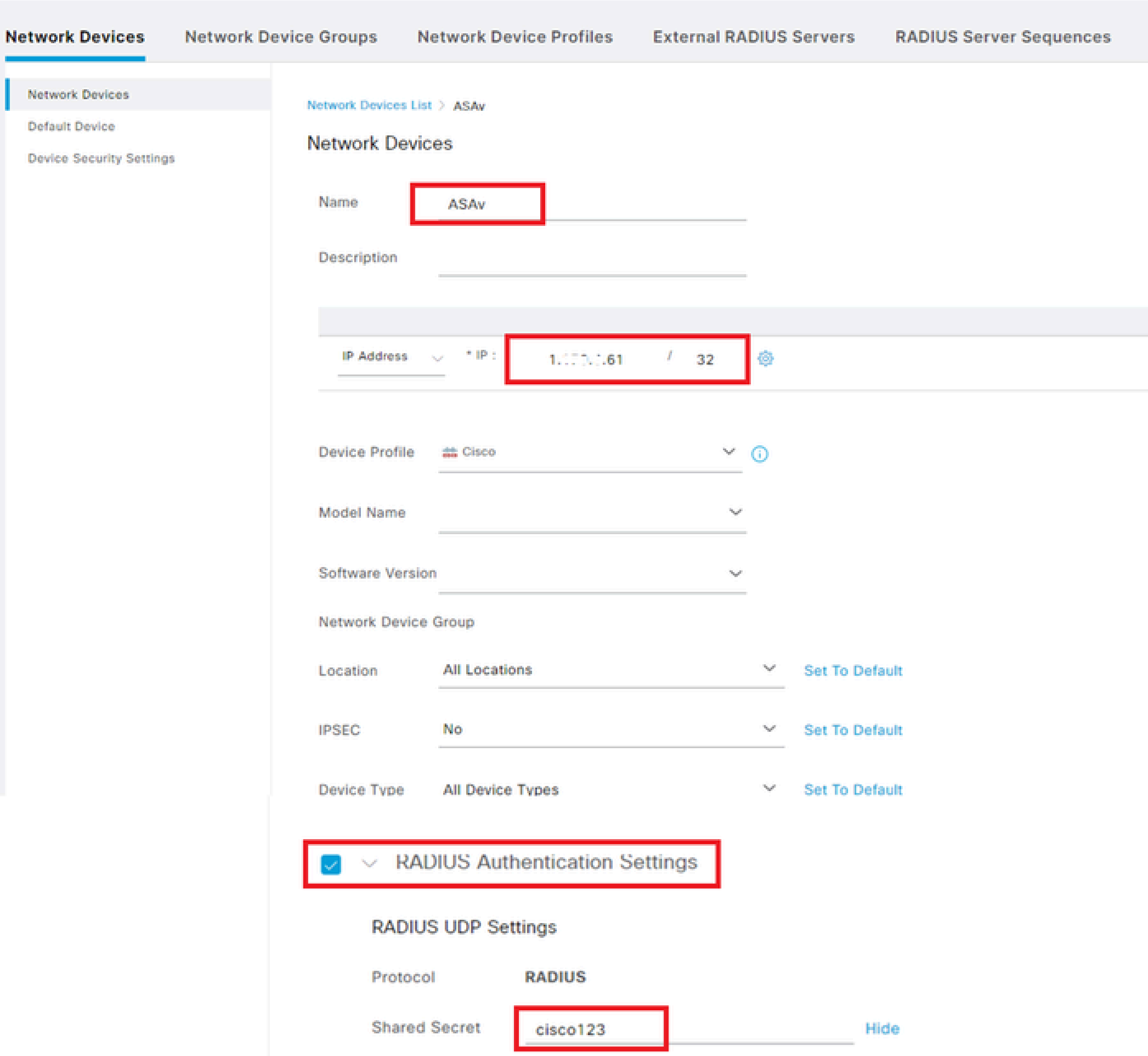
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Domänenadministratoren und Domänenbenutzer

Konfiguration in der ISE

Schritt 1: Gerät hinzufügen

Navigieren Sie zu Administration > Network Devices, und klicken Sie auf Add (Hinzufügen), um ein ASAv-Gerät hinzuzufügen.



Name: ASAv

Description:

IP Address * IP : 1.[redacted].61 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

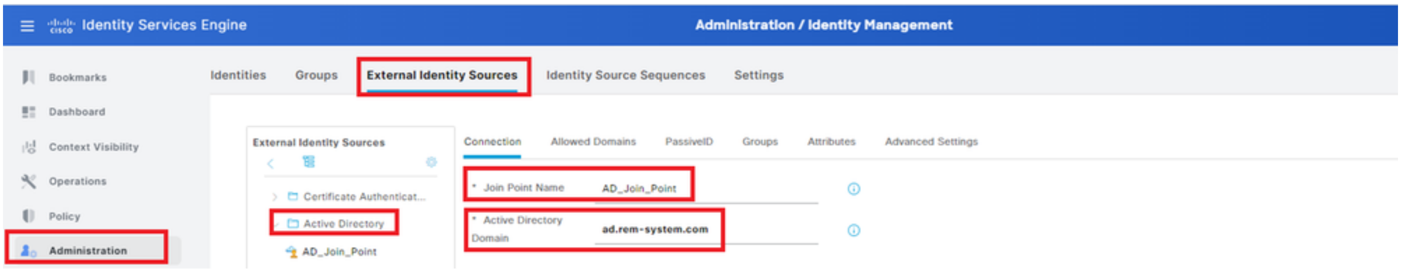
Shared Secret: cisco123 — Hide

Gerät hinzufügen

Schritt 2: Active Directory hinzufügen

Navigieren Sie zu Administration > External Identity Sources > Active Directory, klicken Sie aufRegisterkarte Connection, und fügen Sie Active Directory zur ISE hinzu.

- Verknüpfungspunkt-Name: AD_Join_Point
- Active Directory-Domäne: ad.rem-system.com

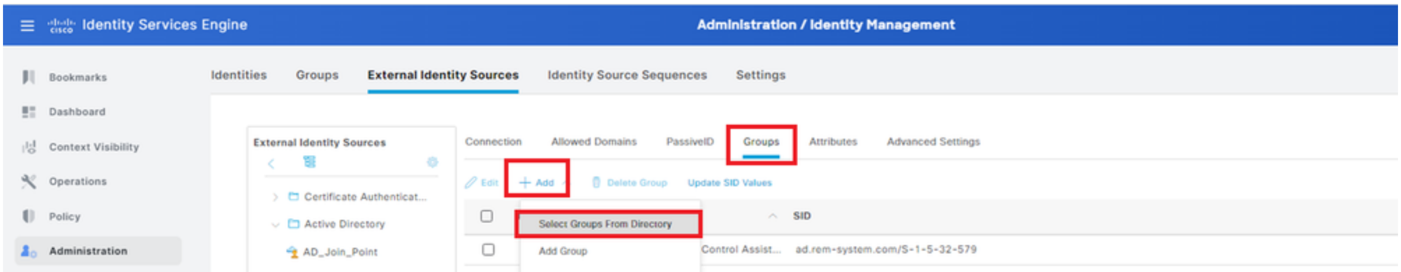


* Join Point Name: AD_Join_Point

* Active Directory Domain: ad.rem-system.com

Active Directory hinzufügen

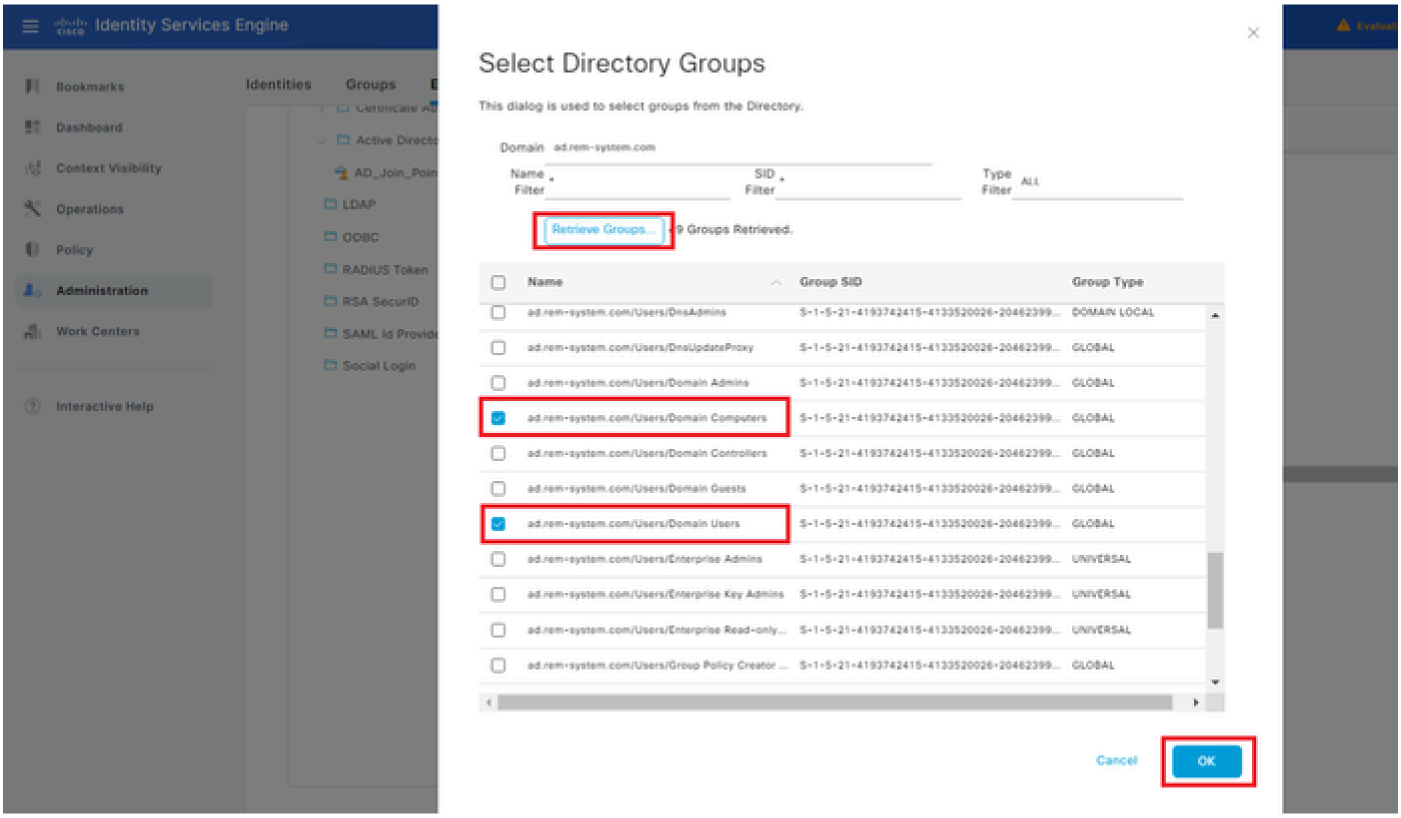
Navigieren Sie zur Registerkarte Gruppen, und wählen SieGruppe auswählen aus Verzeichnis aus Dropdown-Liste.



Name	SID
Control Assist...	ad.rem-system.com/S-1-5-32-579

Gruppe auswählen aus Verzeichnis

Klicken Sie auf Gruppen aus der Dropdown-Liste abrufen. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Benutzer und klicken auf OK.



This dialog is used to select groups from the Directory.

Domain: ad.rem-system.com

Name Filter: * SID Filter: * Type Filter: ALL

9 Groups Retrieved.

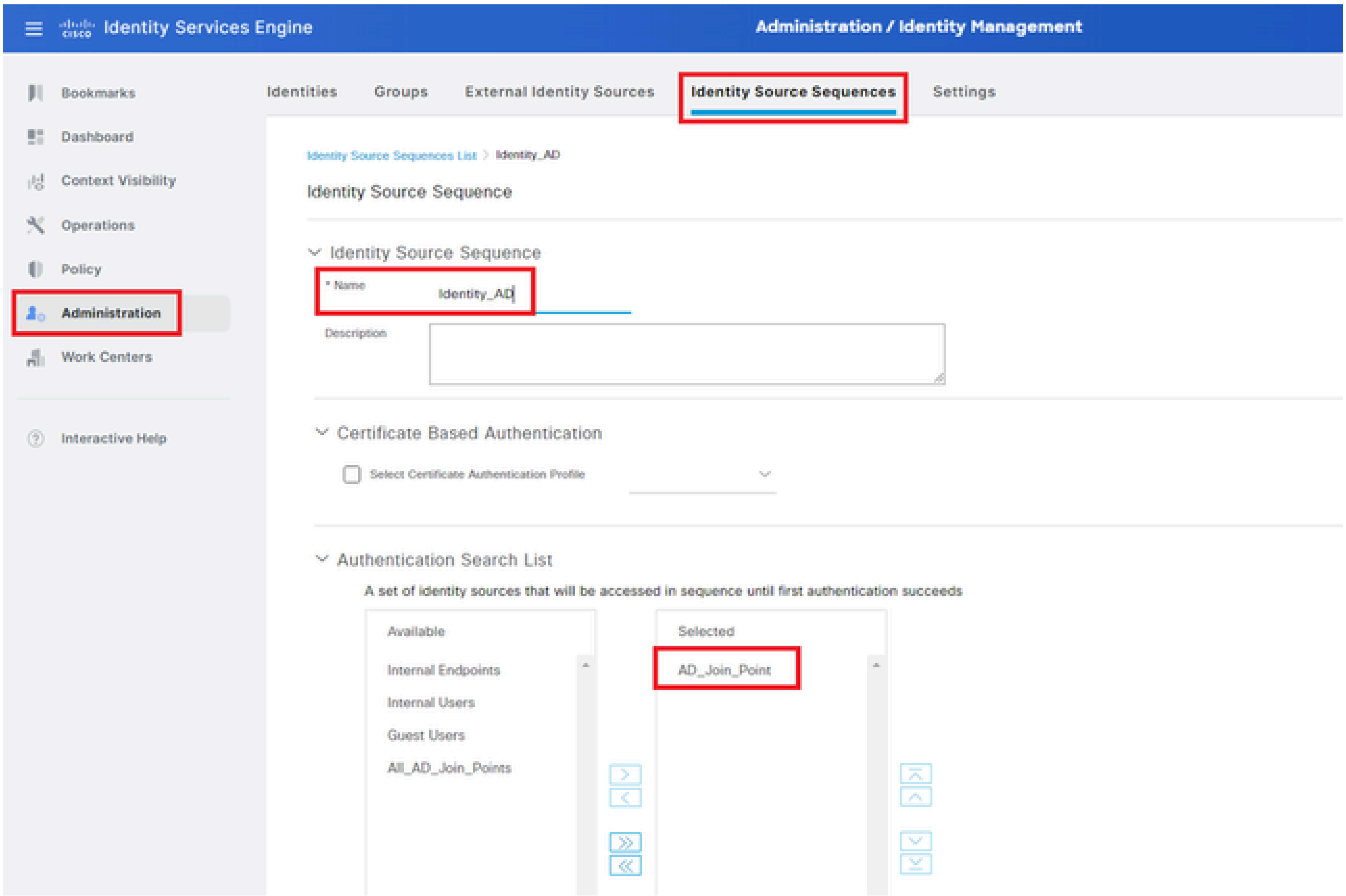
☐	Name	Group SID	Group Type
☐	ad.rem-system.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☐	ad.rem-system.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-system.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Domain Guests	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-system.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Enterprise Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-system.com/Users/Enterprise Key Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-system.com/Users/Enterprise Read-only...	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-system.com/Users/Group Policy Creator ...	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

Domänencomputer und -benutzer hinzufügen

Schritt 3: Identitätsquelltext hinzufügen

Navigieren Sie zu Administration > Identity Source Sequences, und fügen Sie eine Identity Source Sequence hinzu.

- Name: Identity_AD
- Authentifizierungs-Suchliste: AD_Join_Point



Identity Source Sequence

Identity Source Sequence

* Name: Identity_AD

Description:

Certificate Based Authentication

□ Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Internal Endpoints, Internal Users, Guest Users, All_AD_Join_Points

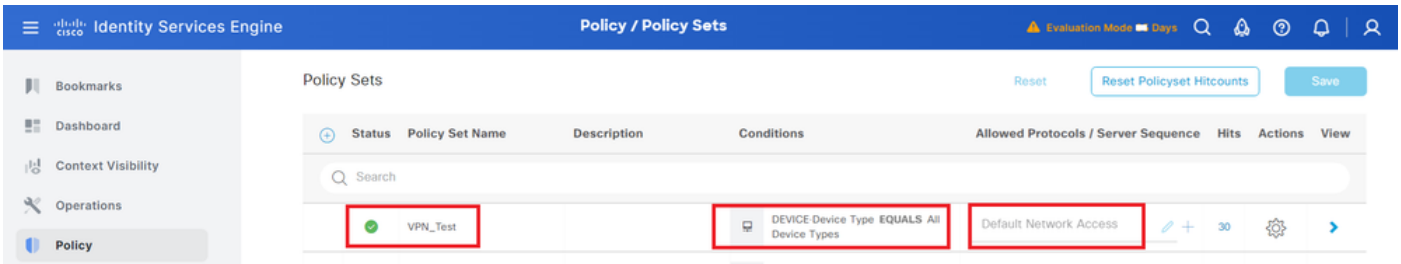
Selected: AD_Join_Point

Identitätsquellensequenzen hinzufügen

Schritt 4: Policy Set hinzufügen

Navigieren Sie zu Policy > Policy Sets, und klicken Sie auf +, um einen Policy Set hinzuzufügen.

- Richtliniensatzname: VPN_Test
- Bedingungen : GERÄTETYP ENTSPRICHT ALLEN GERÄTETYPEN
- Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff



Policy Sets

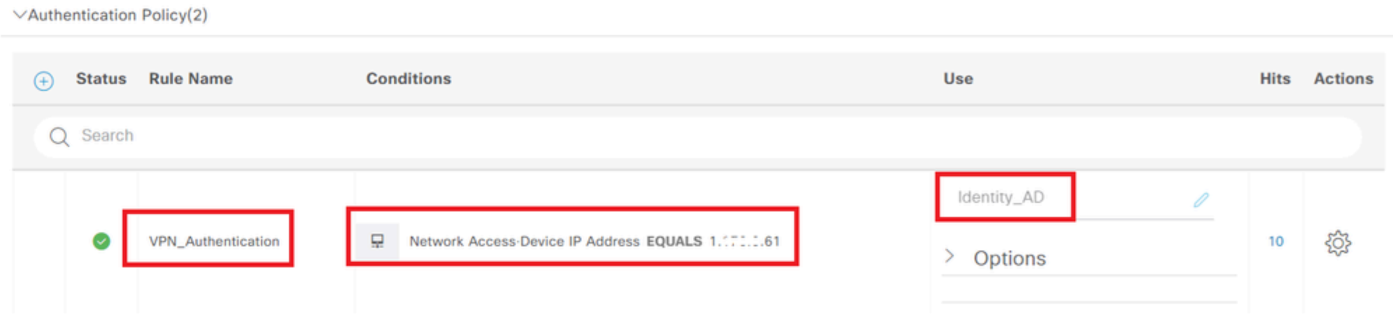
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	VPN_Test		DEVICE·Device Type EQUALS All Device Types	Default Network Access	30	⚙	›

Policy Set hinzufügen

Schritt 5: Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf VPN_Test, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: VPN_Authentication
- Bedingungen: IP-Adresse des Netzwerkzugriffsgeräts ENTSPRICHT 1.x.x.61
- Verwenden: Identity_AD



Authentication Policy(2)

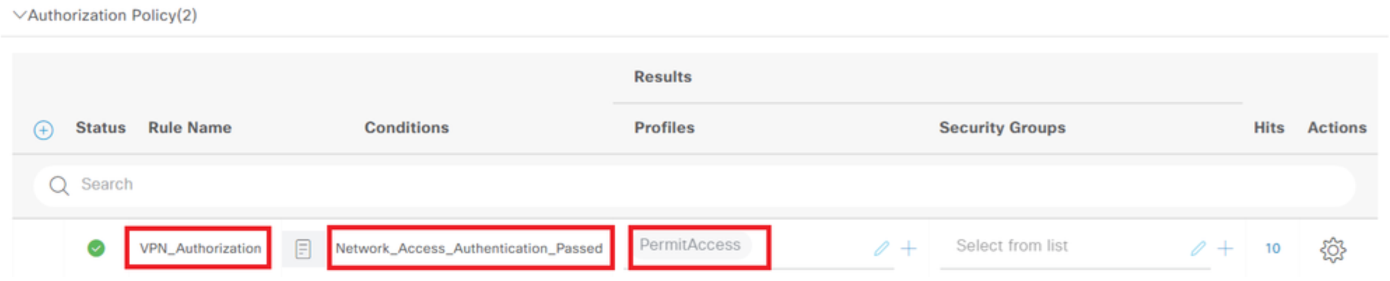
Status	Rule Name	Conditions	Use	Hits	Actions
✓	VPN_Authentication	Network Access·Device IP Address EQUALS 1.[redacted].61	Identity_AD Options	10	⚙

Authentifizierungsrichtlinie hinzufügen

Schritt 6: Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf VPN_Test, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: VPN_Authorization
- Bedingungen: Network_Access_Authentication_Passed
- Ergebnisse : PermitAccess



Authorization Policy(2)

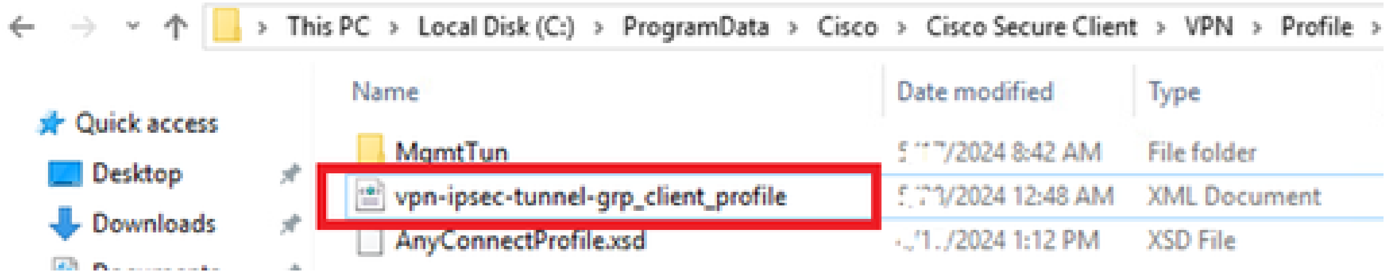
			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	10	⚙

Autorisierungsrichtlinie hinzufügen

Überprüfung

Schritt 1: Kopieren des sicheren Clientprofils auf Win10 PC1

Kopieren Sie das sichere Clientprofil in das Verzeichnis C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



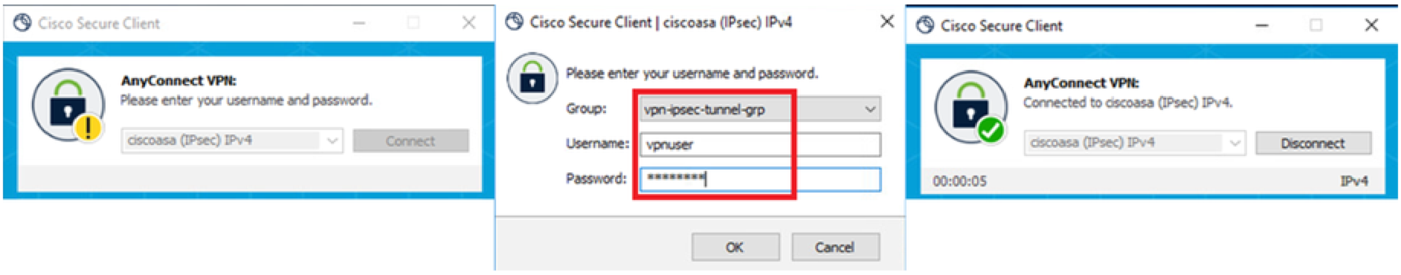
This PC › Local Disk (C:) › ProgramData › Cisco › Cisco Secure Client › VPN › Profile ›

Name	Date modified	Type
MgmtTun	[redacted]/2024 8:42 AM	File folder
vpn-ipsec-tunnel-grp_client_profile	[redacted]/2024 12:48 AM	XML Document
AnyConnectProfile.xsd	[redacted]/2024 1:12 PM	XSD File

Profil auf PC kopieren

Schritt 2: VPN-Verbindung initiieren

Führen Sie auf dem Endgerät den Cisco Secure Client aus, geben Sie den Benutzernamen und das Kennwort ein, und bestätigen Sie dann, dass die Verbindung mit dem Cisco Secure Client erfolgreich hergestellt wurde.



Cisco Secure Client

AnyConnect VPN:
Please enter your username and password.

ciscoasa (IPsec) IPv4

Cisco Secure Client | ciscoasa (IPsec) IPv4

Please enter your username and password.

Group: vpn-ipsec-tunnel-grp
Username: vpnuser
Password: ********

Cisco Secure Client

AnyConnect VPN:
Connected to ciscoasa (IPsec) IPv4.

ciscoasa (IPsec) IPv4

00:00:05 IPv4

Verbindung erfolgreich

Schritt 3: Syslog auf ASA bestätigen

Überprüfen Sie im Syslog, ob die IKEv2-Verbindung erfolgreich war.

<#root>

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser 

New Connection Established


May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser 
```

Schritt 4: IPsec-Sitzung auf ASA bestätigen

Führen Sie einen Befehl ausshow vpn-sessiondb detail anyconnect, um die IKEv2/IPsec-Sitzung auf der ASA zu bestätigen.

<#root>

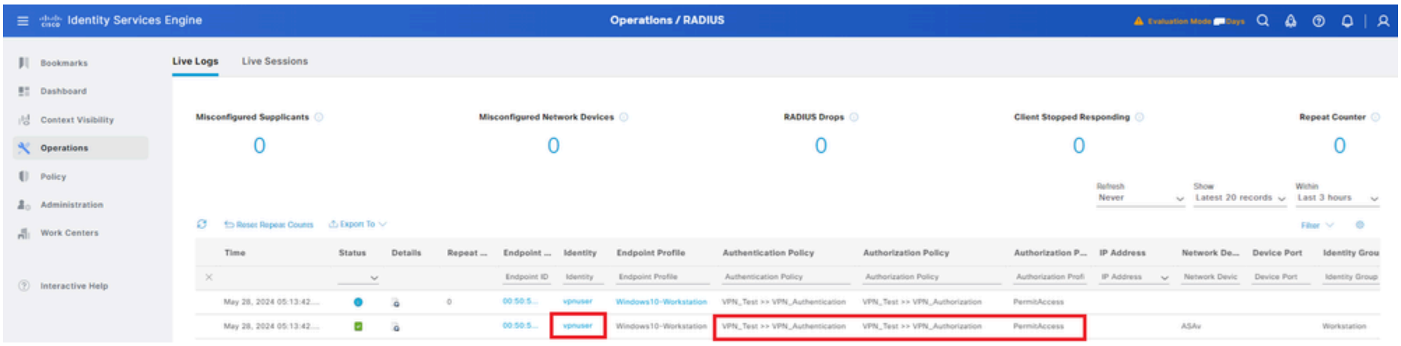
```
ciscoasa#

show vpn-sessiondb detail anyconnect



Session Type: AnyConnect Detailed

Username : vpnuser Index : 23
Assigned IP : 172.16.1.20 Public IP : 192.168.1.11
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none
Bytes Tx : 840 Bytes Rx : 52408
```

```
Pkts Tx : 21 Pkts Rx : 307
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp
Tunnel Group : vpn-ipsec-tunnel-grp
Login Time : 08:13:20 UTC Tue May 28 2024
Duration : 0h:10m:10s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 01aa003d0001700066559220
Security Grp : none


IKEv2 Tunnels: 1



IPsecOverNatT Tunnels: 1



AnyConnect-Parent Tunnels: 1




AnyConnect-Parent:
Tunnel ID : 23.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : 5.1.3.62

IKEv2:
Tunnel ID : 23.2
UDP Src Port : 50982 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds
PRF : SHA256 D/H Group : 19
Filter Name :
Client OS : Windows Client Type : AnyConnect

IPsecOverNatT:
Tunnel ID : 23.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.1.20/255.255.255.255/0/0
Encryption : AES256 Hashing : SHA256
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307
```

Schritt 5: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live**-Protokolle) in der ISE-GUI, und bestätigen Sie das Live-

Protokoll für die VPN-Authentifizierung.



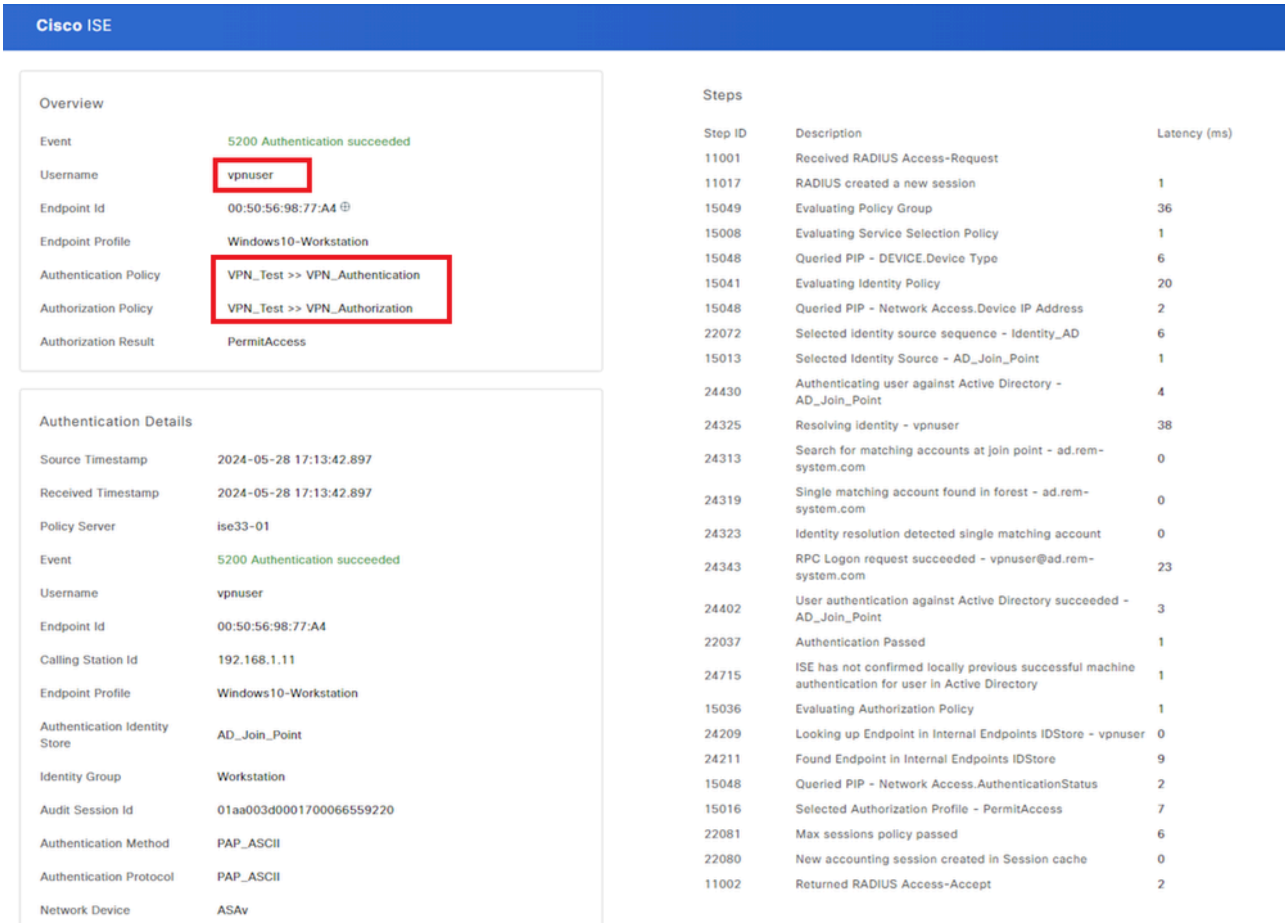
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never
Show: Latest 20 records
Within: Last 3 hours

Time	Status	Details	Repeat ...	Endpoint ...	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...	Device Port	Identity Grou
				Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	Network Devic	Device Port	Identity Group
May 28, 2024 05:13:42....	●		0	00:50:5...	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess				
May 28, 2024 05:13:42....	✓			00:50:5...	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Workstation

Radius-Live-Protokoll

Klicken Sie auf Status, um die Details des Live-Protokolls zu bestätigen.



Overview

Event	5200 Authentication succeeded
Username	vpnuser
Endpoint Id	00:50:56:98:77:A4
Endpoint Profile	Windows10-Workstation
Authentication Policy	VPN_Test >> VPN_Authentication
Authorization Policy	VPN_Test >> VPN_Authorization
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-28 17:13:42.897
Received Timestamp	2024-05-28 17:13:42.897
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	vpnuser
Endpoint Id	00:50:56:98:77:A4
Calling Station Id	192.168.1.11
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	AD_Join_Point
Identity Group	Workstation
Audit Session Id	01aa003d0001700066559220
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	ASAv

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	1
15049	Evaluating Policy Group	36
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	6
15041	Evaluating Identity Policy	20
15048	Queried PIP - Network Access.Device IP Address	2
22072	Selected identity source sequence - Identity_AD	6
15013	Selected Identity Source - AD_Join_Point	1
24430	Authenticating user against Active Directory - AD_Join_Point	4
24325	Resolving identity - vpnuser	38
24313	Search for matching accounts at join point - ad.rem-system.com	0
24319	Single matching account found in forest - ad.rem-system.com	0
24323	Identity resolution detected single matching account	0
24343	RPC Logon request succeeded - vpnuser@ad.rem-system.com	23
24402	User authentication against Active Directory succeeded - AD_Join_Point	3
22037	Authentication Passed	1
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
15036	Evaluating Authorization Policy	1
24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
24211	Found Endpoint in Internal Endpoints IDStore	9
15048	Queried PIP - Network Access.AuthenticationStatus	2
15016	Selected Authorization Profile - PermitAccess	7
22081	Max sessions policy passed	6
22080	New accounting session created in Session cache	0
11002	Returned RADIUS Access-Accept	2

Details zum Live-Protokoll

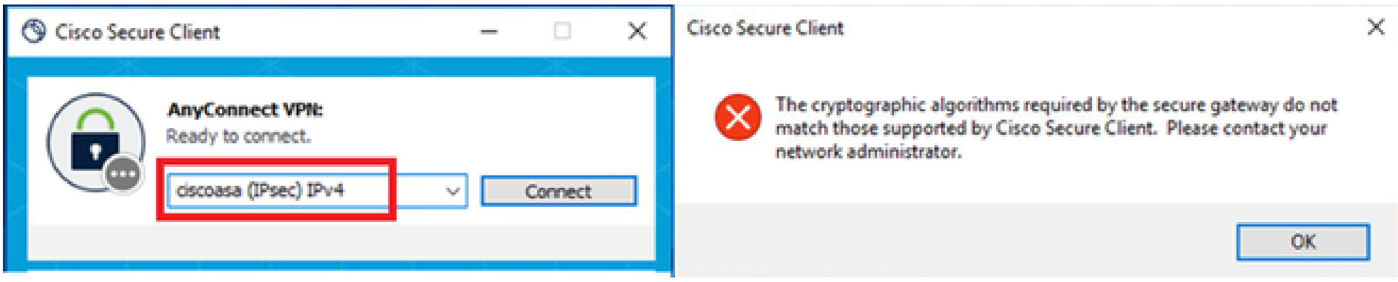
Fehlerbehebung

Die Nichtübereinstimmung der kryptografischen Algorithmen kann zu Verbindungsfehlern führen. Dies ist ein Beispiel dafür, wenn ein Problem mit einer Nichtübereinstimmung der Algorithmen auftritt. Durch Ausführen von Schritt 15 des Abschnitts "Konfiguration" in ASDM kann das Problem behoben werden.

Schritt 1: VPN-Verbindung initiieren

Führen Sie auf dem Endgerät den Cisco Secure Client aus, und vergewissern Sie sich, dass die Verbindung aufgrund einer nicht übereinstimmenden kryptografischen Algorithmen fehlgeschlagen ist.

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.Please contact your network administrator.



The cryptographic algorithms required by the secure gateway do not match those supported by Cisco Secure Client. Please contact your network administrator.

Verbindung fehlgeschlagen

Schritt 2: Syslog in CLI bestätigen

Bestätigen Sie im Syslog, dass die IKEv2-Aushandlung fehlgeschlagen ist.

<#root>

```
May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE_INIT_SA requ
May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ERI

Failed to find a matching policy
```

Referenz

[AnyConnect über IKEv2 zu ASA mit AAA und Authentifizierung von Zertifikaten]