

Konfiguration des Linux VPN-Status mit ISE 3.3

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen auf FMC/FTD](#)

[Konfigurationen auf der ISE](#)

[Konfigurationen unter Ubuntu](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration des Linux VPN-Status mit Identity Services Engine (ISE) und Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Secure Client
- Remote Access VPN mit Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

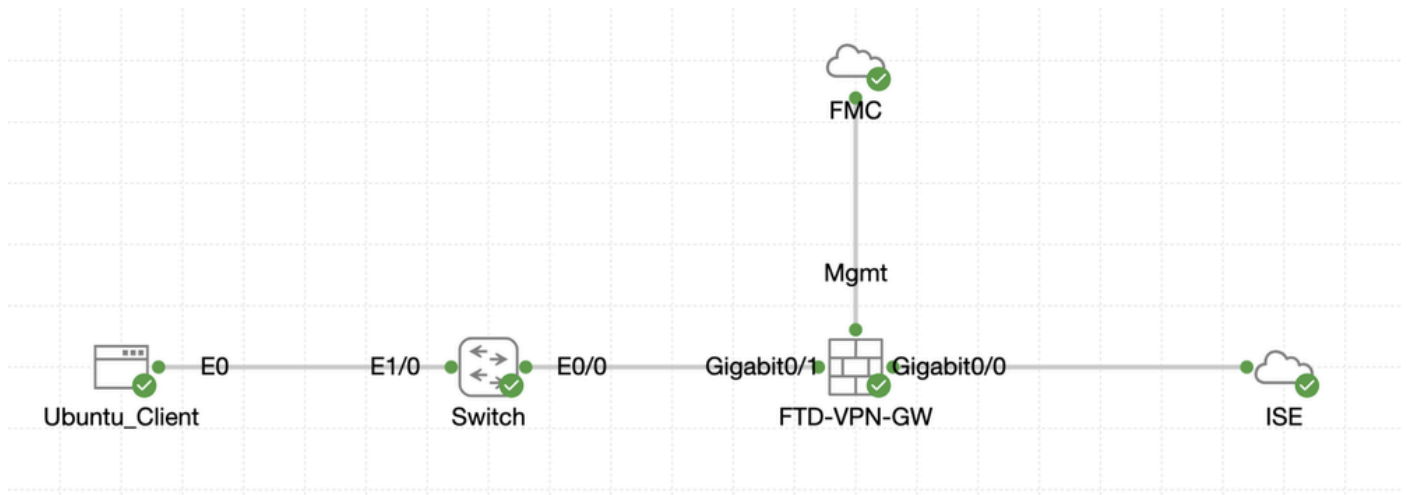
- Ubuntu 22,04
- Cisco Secure Client 5.1.3.62
- Cisco Firepower Threat Defense (FTD) 7.4.1
- Cisco FirePOWER Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

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



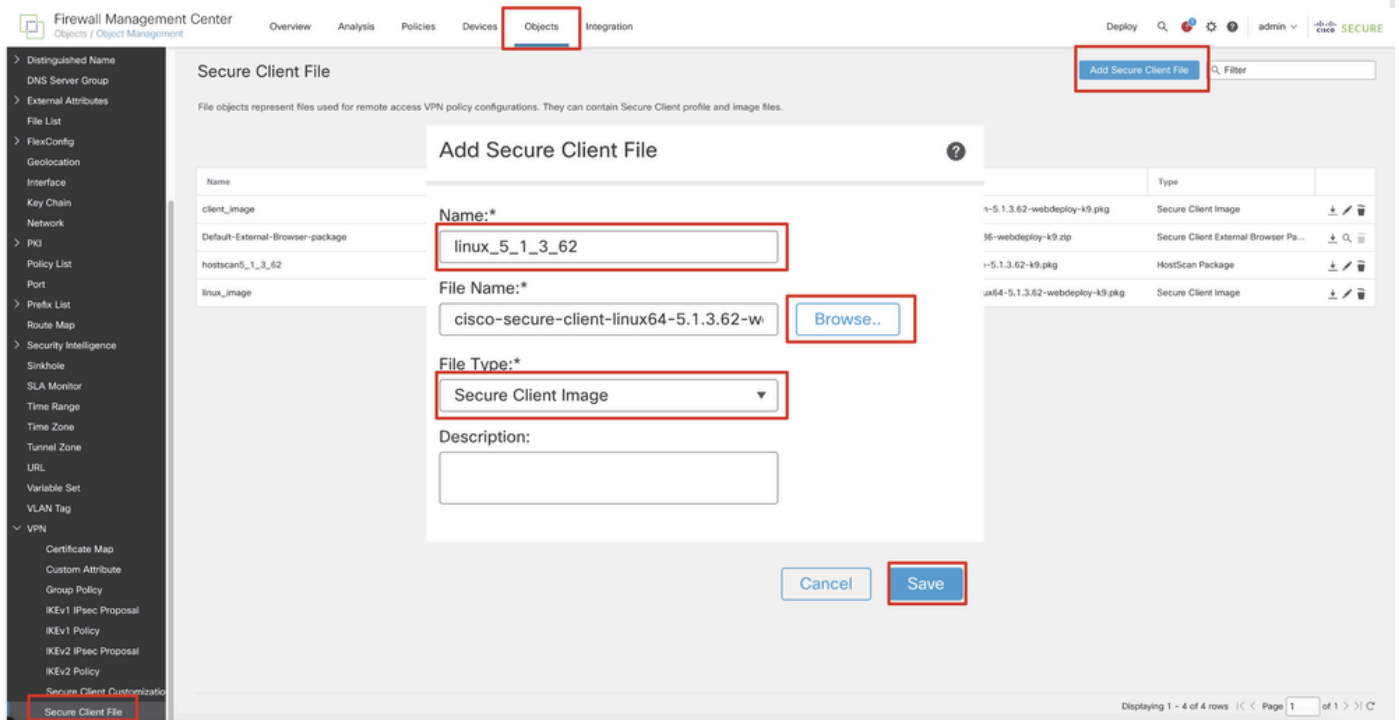
Topologie

Konfigurationen auf FMC/FTD

Schritt 1: Die Verbindung zwischen dem Client, FTD, FMC und ISE wurde erfolgreich konfiguriert. Da enroll.cisco.com für Endpunkte verwendet wird, die eine Überprüfung der Umleitung durchführen (weitere Informationen finden Sie in den CCO-[Dokumenten zum Statusablauf ISE Posture Style Comparison for Pre and Post 2.2](#)). Stellen Sie sicher, dass die Route für den Datenverkehr zu enroll.cisco.com auf FTD richtig konfiguriert ist.

Schritt 2: Laden Sie den Paketnamen `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg` von [Cisco Software Download herunter](#), und vergewissern Sie sich, dass die Datei nach dem Download korrekt ist. Bestätigen Sie, dass die MD5-Prüfsumme der heruntergeladenen Datei mit der Cisco Software Download-Seite übereinstimmt.

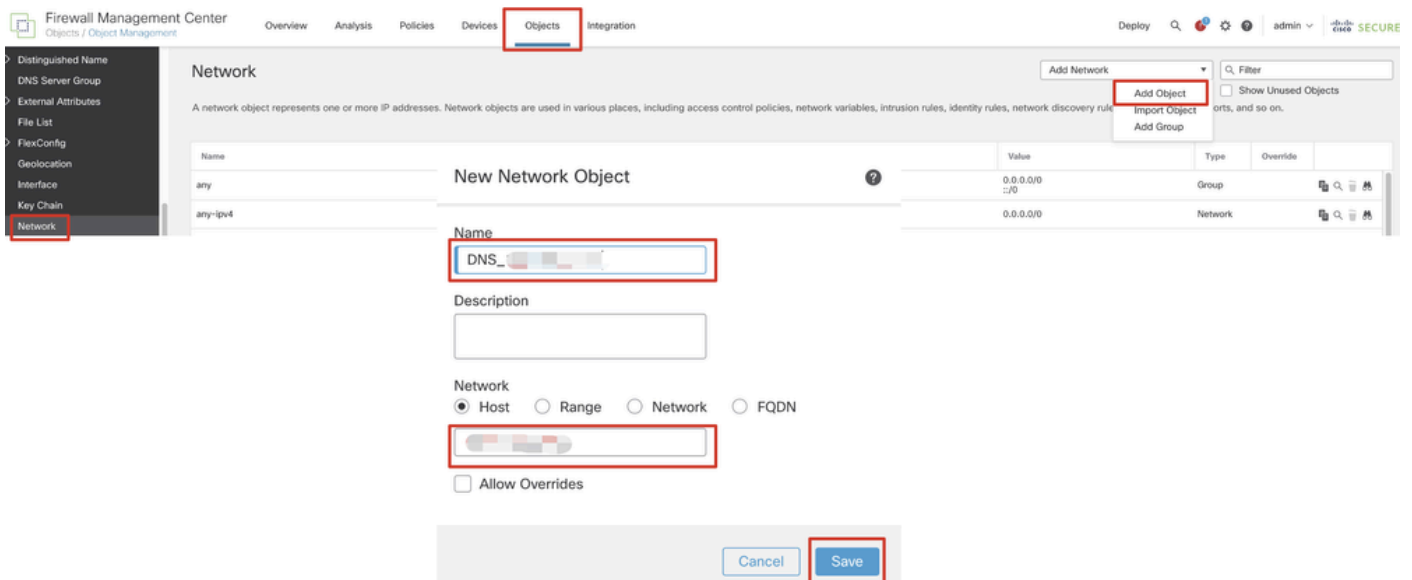
Schritt 3: Navigieren Sie zu Objects > Object Management > VPN > Secure Client File. Klicken Sie auf Add Secure Client File, geben Sie den Namen ein, File Name wählen Sie aus, `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg` und wählen Sie Secure Client Image in der Dropdown-Liste aus File Type. Klicken Sie dann auf Save.



FMC_Upload_Secure_Client_Image

Schritt 4: Navigieren Sie zu Objects > Object Management > Network.

Schritt 4.1: Erstellen eines Objekts für den DNS-Server Klicken Sie auf Add Object, geben Sie den Namen und die verfügbare DNS-IP-Adresse an. Klicken Sie auf .Save

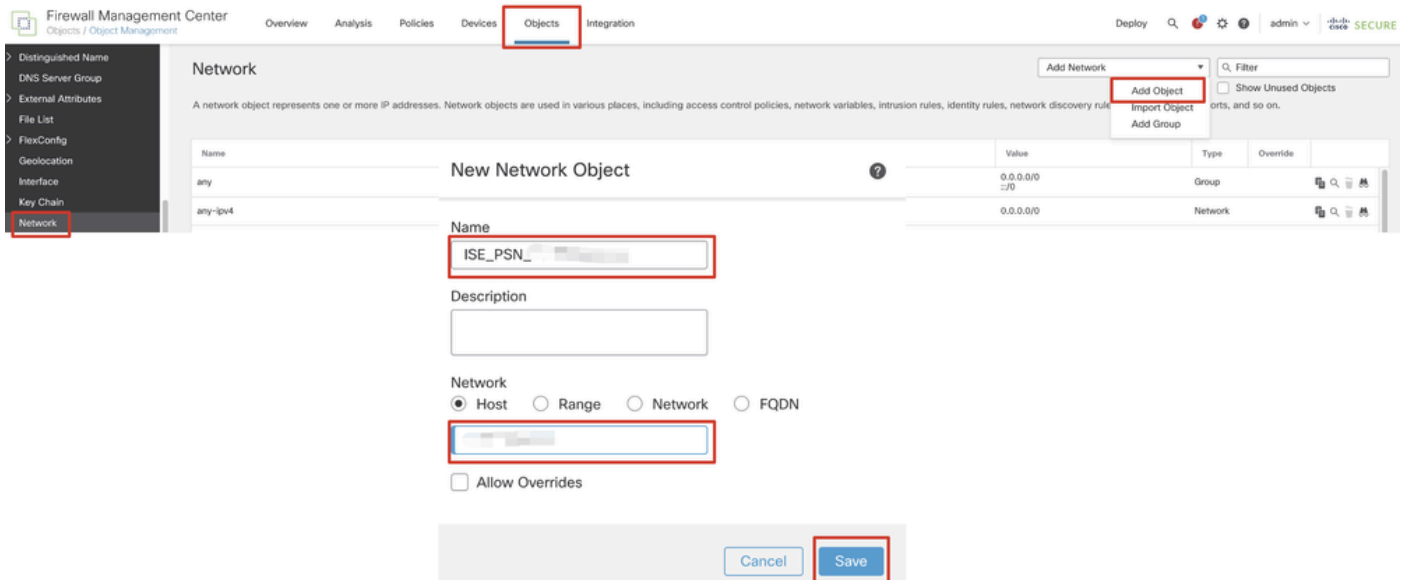


FMC_Add_Object_DNS



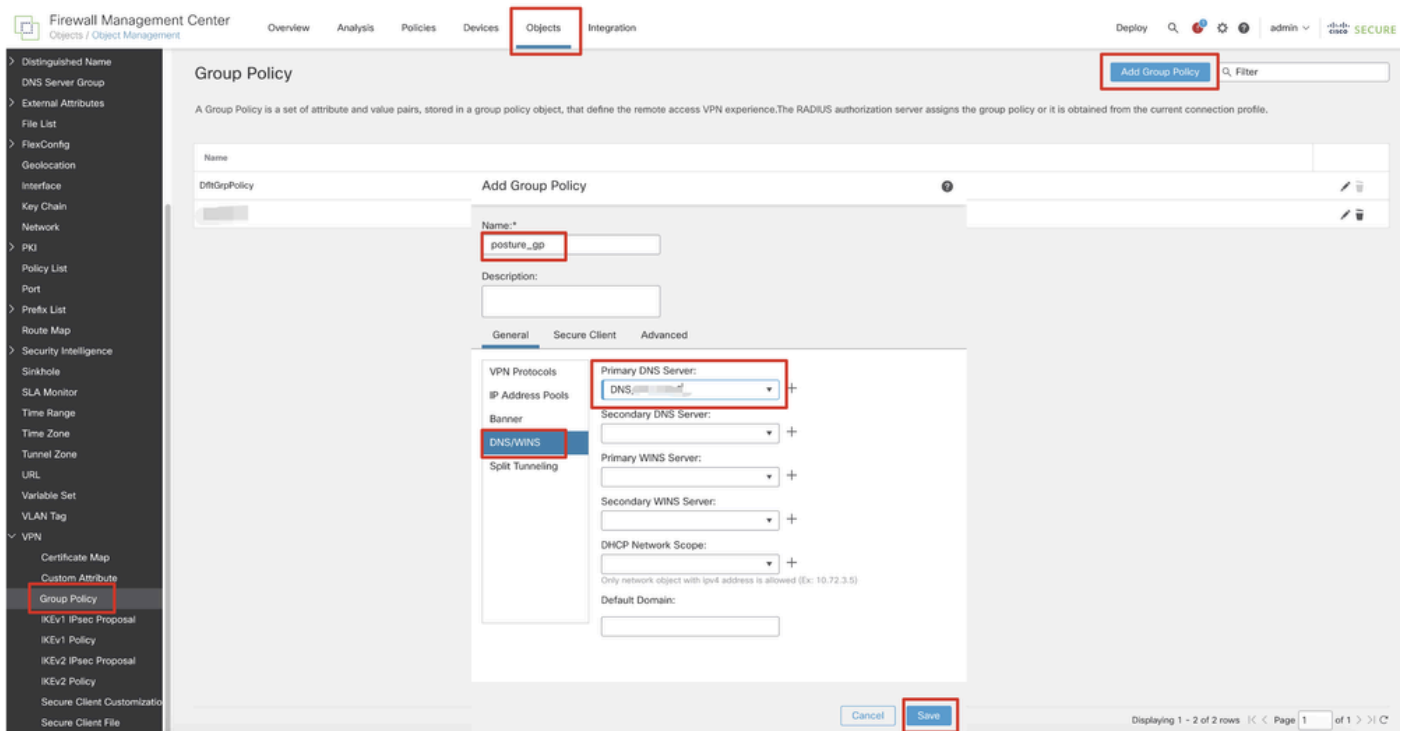
Hinweis: Der hier konfigurierte DNS-Server muss für VPN-Benutzer verwendet werden.

Schritt 4.2: Erstellen eines Objekts für ISE PSN Klicken Sie auf Add Object, geben Sie den Namen und die verfügbare ISE PSN-IP-Adresse an. Klicken Sie auf .Save



FMC_Add_Object_ISE

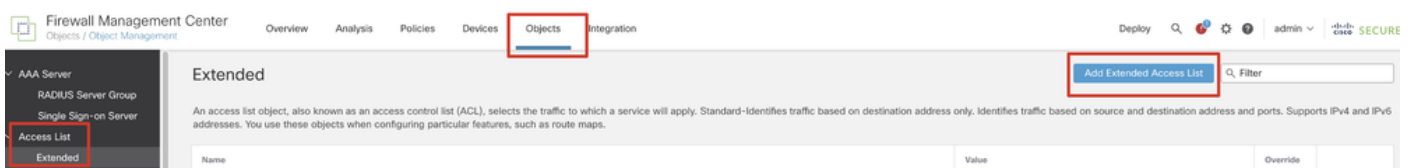
Schritt 5: Navigieren Sie zu Objects > Object Management > VPN > Group Policy. Klicken Sie auf .Add Group Policy Klicken Sie aufDNS/WINS, und wählen Sie das Objekt des DNS-Servers in ausPrimary DNS Server. Klicken Sie dann auf Save.



FMC_Add_Group_Policy

Hinweis: Stellen Sie sicher, dass der in der VPN-Gruppenrichtlinie verwendete DNS-Server den ISE-Clientbereitstellungsportal-FQDN und enroll.cisco.com auflösen kann.

Schritt 6: Navigieren Sie zu Objects > Object Management > Access List > Extended. Klicken Sie auf .Add Extended Access List



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

AAA Server
RADIUS Server Group
Single Sign-on Server
Access List
Extended

Extended

[Add Extended Access List](#) 🔍 Filter

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Name	Value	Override
------	-------	----------

FMC_Add_Redirect_ACL

Schritt 6.1: Geben Sie den Namen der Umleitungszugriffskontrollliste an. Dieser Name muss mit dem im ISE-Autorisierungsprofil

übereinstimmen. Klicken Sie auf .Add

New Extended Access List Object

Name
redirect

Entries (0)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

Allow Overrides

Cancel Save

FMC_Add_Redirect_ACL_Teil_1

Schritt 6.2: Blockieren Sie DNS-Datenverkehr, Datenverkehr zur ISE PSN-IP-Adresse und zu den Wiederherstellungsservern, um diese von der Umleitung auszuschließen. Den restlichen Verkehr zulassen. Dies löst eine Umleitung aus. Klicken Sie auf .Save

Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network Port Application Users Security Group Tag

Available Networks

- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- ISE_PSN_...
- rtp_ise

Source Networks (0)

Destination Networks (1)

ISE_PSN_...

Enter an IP address Add









Cancel Add

FMC_Add_Redirect_ACL_Teil_2

Name
redirect

Entries (4)

Add

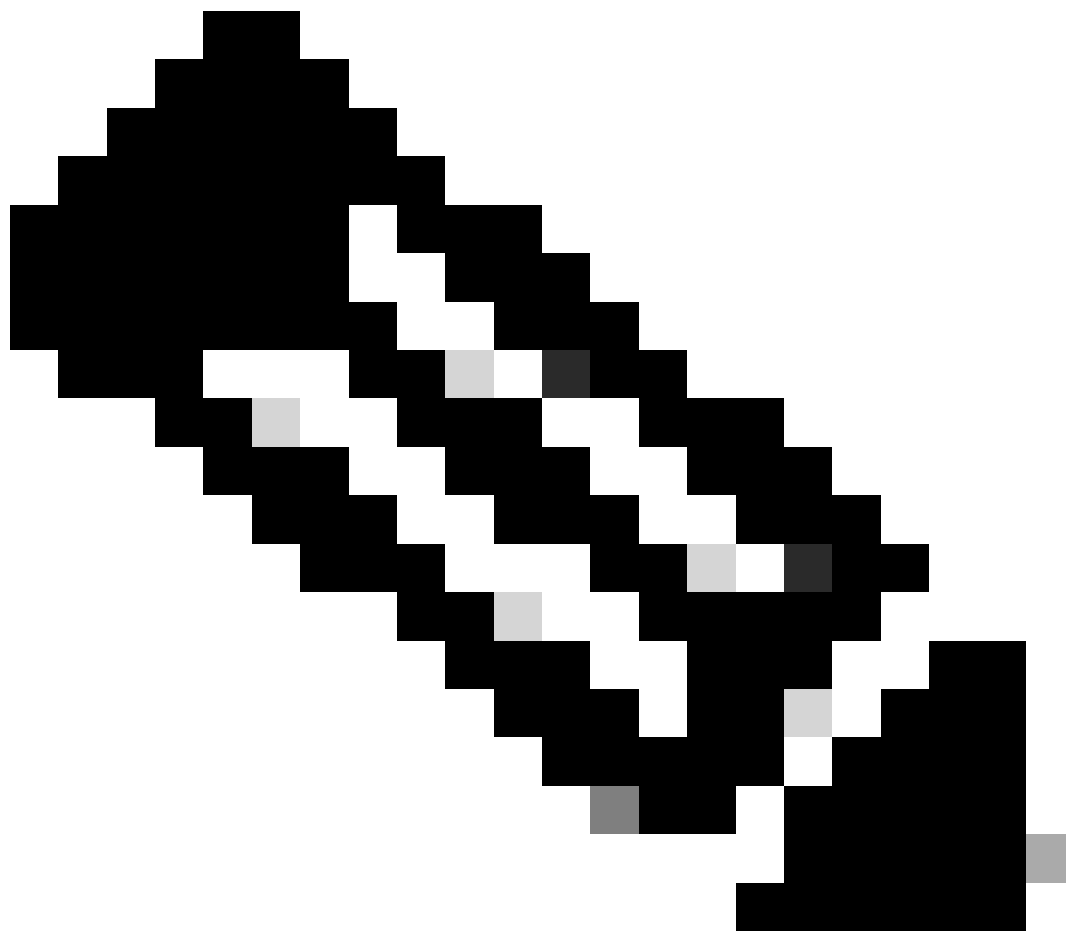
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN_...	Any	Any	Any	Any	 
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	 
3	Block	Any	Any	FTP_...	Any	Any	Any	Any	 
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	 

Allow Overrides

Cancel

Save

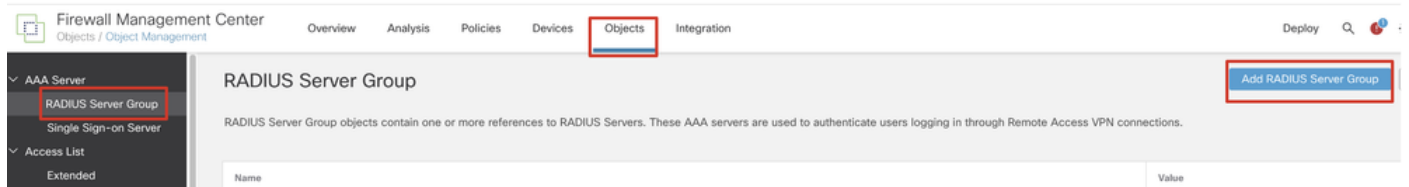
FMC_Add_Redirect_ACL_Teil_3



Hinweis: In diesem Beispiel für die Umleitungszugriffskontrollliste wird das Ziel-FTP als Beispiel für den Wiederherstellungsserver

verwendet.

Schritt 7. Navigieren Sie zu Objects > Object Management > RADIUS Server Group. Klicken Sie auf .Add RADIUS Server Group



FMC_Add_New_Radius_Server_Gruppe

Schritt 7.1: Geben Sie einen Namen ein, prüfen Sie Enable authorize only, prüfen Sie Enable interim account update, prüfen Sie Enable dynamic authorization.

Add RADIUS Server Group



Name:*

rtpise

Description:

Group Accounting Mode:

Single



Retry Interval:* (1-10) Seconds

10

Realms:



Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

Cancel

Save

FMC_Add_New_Radius_Server_Gruppe_Teil_1

Schritt 7.2: Klicken Sie auf das Plus Symbol, um einen neuen Radius-Server hinzuzufügen. Geben Sie die ISE PSN IP Address/Hostname, Key an. Wählen Sie die specific interface Option zum Herstellen der Verbindung aus. Wählen Sie den Redirect ACL. Klicken Sie dann Save auf, um den neuen Radius-Server zu speichern. Klicken Sie dann erneut auf Save, um die neue Radius-Server-Gruppe zu speichern.

Add RADIUS Server Group

Enable authorize only
 Enable interim account update
Interval:* (1-120) hours
24
 Enable dynamic authorization
Port:* (1024-65535)
1700
 Merge Downloadable ACL with Cisco AV Pair ACL
 After Cisco AV Pair ACL Before Cisco AV Pair ACL

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

New RADIUS Server

IP Address/Hostname:*
.....
Configure DNS at Threat Defense Platform Settings to resolve hostname
Authentication Port:* (1-65535)
1812
Key:*
.....
Confirm Key:*
.....
Accounting Port: (1-65535)
1813
Timeout: (1-300) Seconds
10

Connect using:
 Routing Specific Interface
inside_zone
+
Redirect ACL:
redirect
+

FMC_Add_New_Radius_Server_Gruppe_Teil_2

Schritt 8: Navigieren Sie zu Objects > Object Management > Address Pools > IPv4 Pools. Klicken Sie auf Add IPv4 Pools, und geben Sie das Name, IPv4 Address Range und Mask an. Klicken Sie dann auf Save.

Firewall Management Center
Overview Analysis Policies Devices **Objects** Integration

Deploy Search Settings fangni **SECURE**

IPv4 Pools

IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

Filter

Name	Override
posture_pool_97_0	<input type="checkbox"/>

Add IPv4 Pool

Name*
posture_pool

Description

IPv4 Address Range*
192.168.6.30-192.168.6.100
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*
255.255.255.0

Allow Overrides

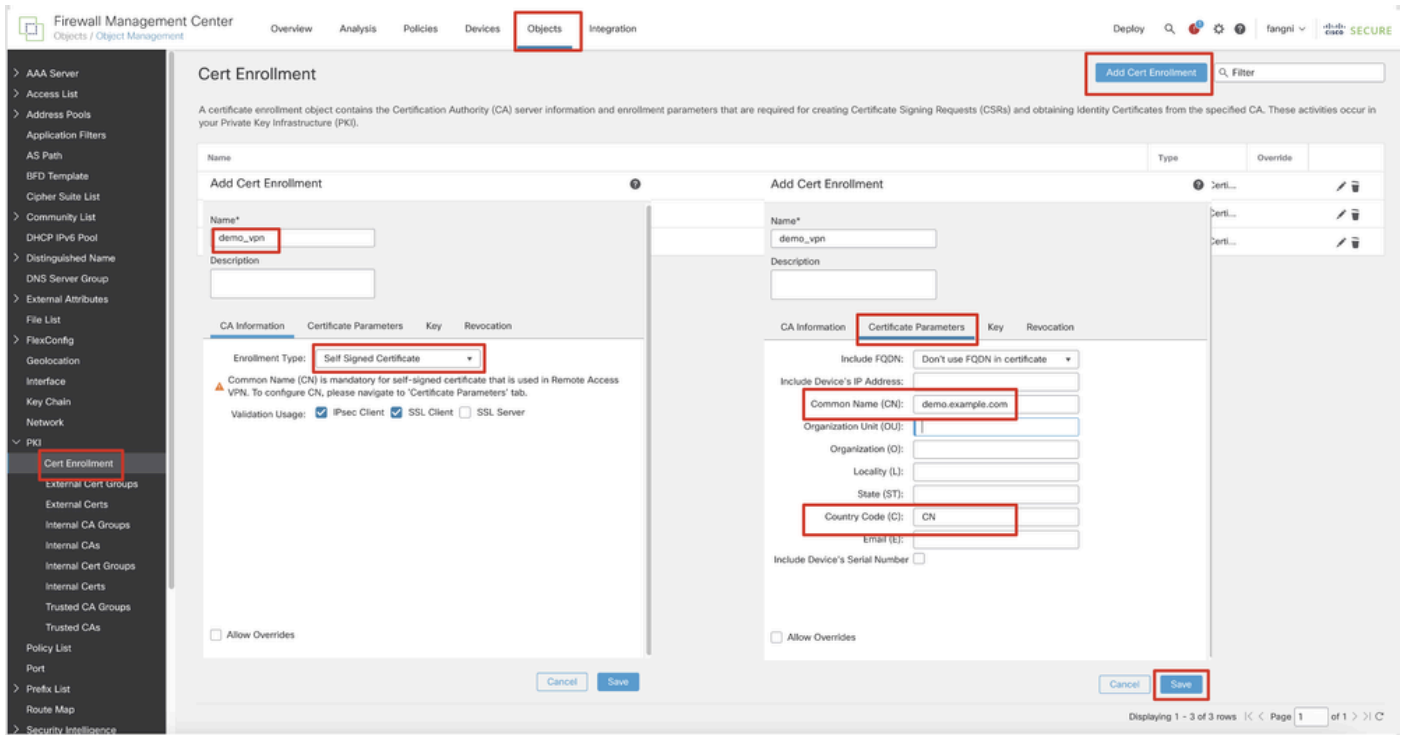
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

Displaying 1 - 2 of 2 rows Page 1 of 1

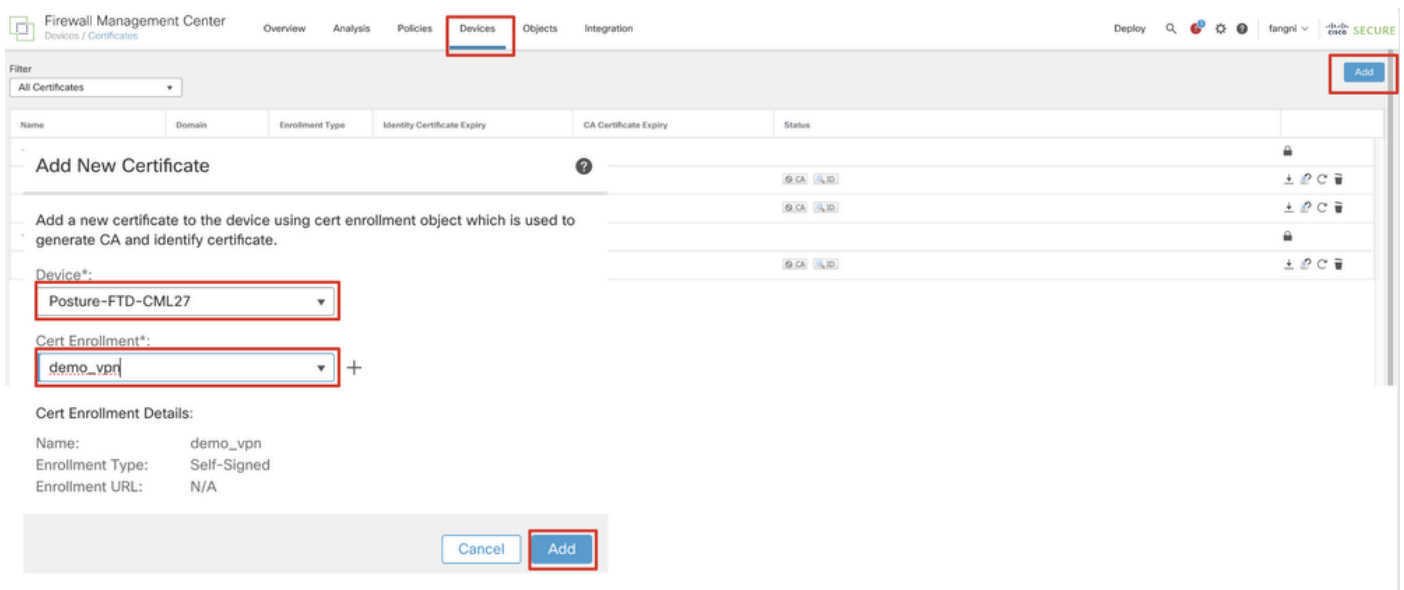
FMC_Add_New_Pool

Schritt 9. Navigieren Sie zu Certificate Objects > Object Management > PKI > Cert Enrollment. Klicken Sie Add Cert Enrollment auf, geben Sie einen Namen an, und wählen Sie Self Signed Certificate as Enrollment Type. Klicken Sie auf die Certificate Parameters Registerkarte, und geben Sie Common Name und Country Code an. Klicken Sie dann auf Save.



FMC_Add_New_Cert_Enrollment

Schritt 10. Navigieren Sie zu Devices > Certificates. Klicken Sie auf Add, wählen Sie den FTD-Namen unter Device, und wählen Sie die zuvor konfigurierte Registrierung unter Cert Enrollment aus. Klicken Sie auf .Add



FMC_Add_New_CERT_TO_FTD

Schritt 11. Navigieren Sie zu Devices > VPN > Remote Access. Klicken Sie auf .Add

Schritt 11.1: Geben Sie den Namen an, und fügen Sie die FTD zu Selected Devices hinzu. Klicken Sie auf .Next

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name: posture_vpn

Description:

VPN Protocols:

- SSL
- IPsec-IKEv2

Targeted Devices:

Available Devices

Search

Posture-FTD-CML27

VPN-FTD-Posture-CML

Add

Selected Devices

Posture-FTD-CML27

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Cancel Back **Next**

FMC_New_RAVPN_Assistent_1

Schritt 11.2: Wählen Sie die zuvor konfigurierte Servergruppe für den Radius im Authentication Server, Authorization Server, Accounting Server. Blättern Sie auf der Seite nach unten.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 **Connection Profile** — 3 Secure Client — 4 Access & Certificate — 5 Summary

Remote User — Secure Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: posture_vpn

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server: rtptise

Authorization Server: rtptise

Accounting Server: rtptise

Client Address Assignment:

Client IP address can be assigned from AAA server, FQDN server and IP address pool. When multiple servers are...

Cancel Back **Next**

FMC_New_RAVPN_Assistent_2

Schritt 11.3: Wählen Sie den zuvor konfigurierten Poolnamen in IPv4 Address Pools. Wählen Sie die zuvor konfigurierte Gruppenrichtlinie in Group Policyaus. Klicken Sie auf Next.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

(Realm or RADIUS)
Accounting Server: +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: ✎
 IPv6 Address Pools: ✎

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy*: +
 Edit Group Policy

Cancel Back **Next**

FMC_New_RAVPN_Wizard_3

Schritt 11.4: Aktivieren Sie das Kontrollkästchen des Linux-Abbilds. Klicken Sie auf .Next

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Secure Client File Object Name	Secure Client Package Name	Operating System
<input type="checkbox"/> client_image	cisco-secure-client-win-5.1.3.62-webdepl...	Windows
<input checked="" type="checkbox"/> linux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd...	Linux

Cancel Back **Next**

FMC_New_RAVPN_Assistent_4

Schritt 11.5: Wählen Sie die Schnittstelle der VPN-Schnittstelle aus. Wählen Sie die Zertifizierung aus, die in Schritt 9 bei FTD registriert wurde. Klicken Sie auf .Next

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin v **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 Secure Client 4 **Access & Certificate** 5 Summary

Network Interface for Incoming VPN Access
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:

Enable DTLS on member interfaces

⚠️ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

Cancel Back **Next**

FMC_New_RAVPN_Assistent_5

Schritt 11.6: Bestätigen Sie die verwandten Informationen auf der Zusammenfassungsseite. Wenn alles in Ordnung ist, klicken Sie auf Finish. Wenn Sie Änderungen vornehmen möchten, klicken Sie auf Back.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin v **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 Secure Client 4 Access & Certificate 5 **Summary**

Remote Access VPN Policy Configuration
Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	posture_vpn
Device Targets:	Posture-FTD-CM27
Connection Profile:	posture_vpn
Connection Alias:	posture_vpn
AAA:	
Authentication Method:	AAA Only
Authentication Server:	rtplse (RADIUS)
Authorization Server:	rtplse
Accounting Server:	rtplse
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	posture_pool
Address Pools (IPv6):	-
Group Policy:	posture_gp
Secure Client Images:	linux_5_1_3_62
Interface Objects:	outside_zone
Device Certificates:	demo_vpn

Device Identity Certificate Enrollment
Certificate enrollment object 'demo_vpn' is not installed on one or more targeted

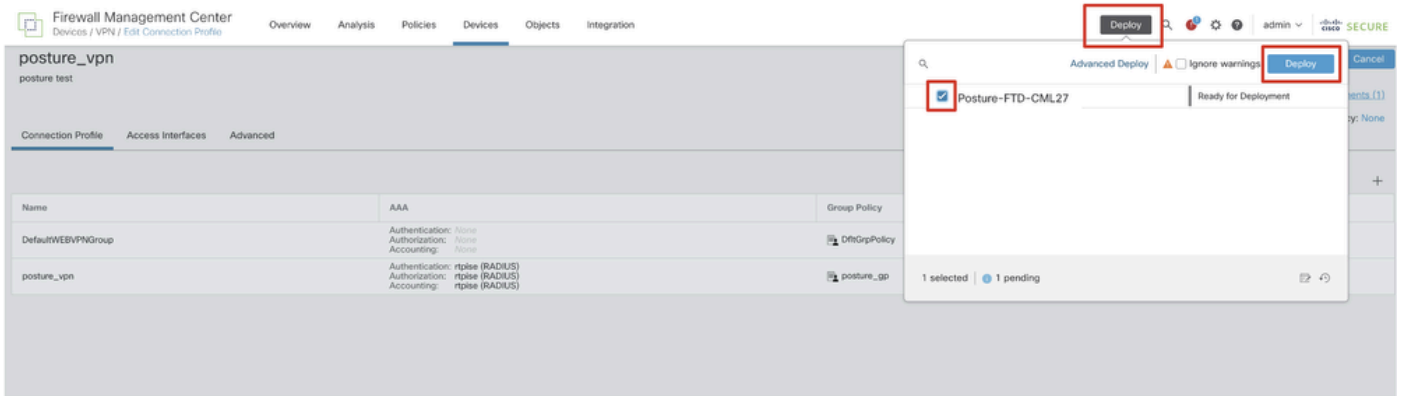
Additional Configuration Requirements
After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.
- Network Interface Configuration**

Cancel Back **Finish**

FMC_New_RAVPN_Assistent_6

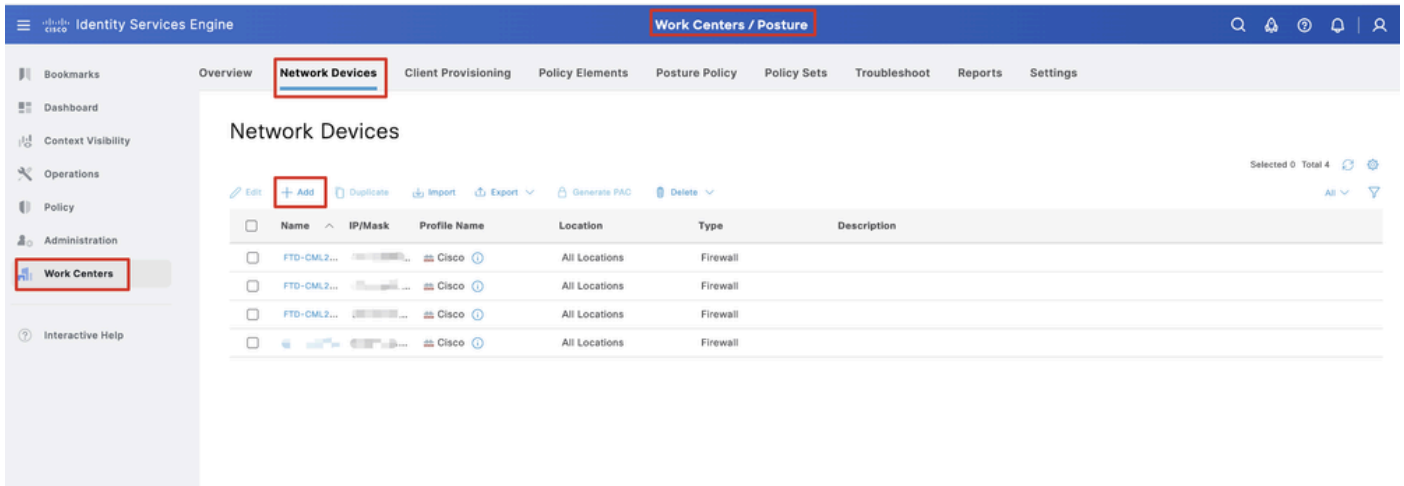
Schritt 12: Stellen Sie die neue Konfiguration in FTD bereit, um die Remote Access-VPN-Konfiguration abzuschließen.



FMC_Bereitstellung_FTD

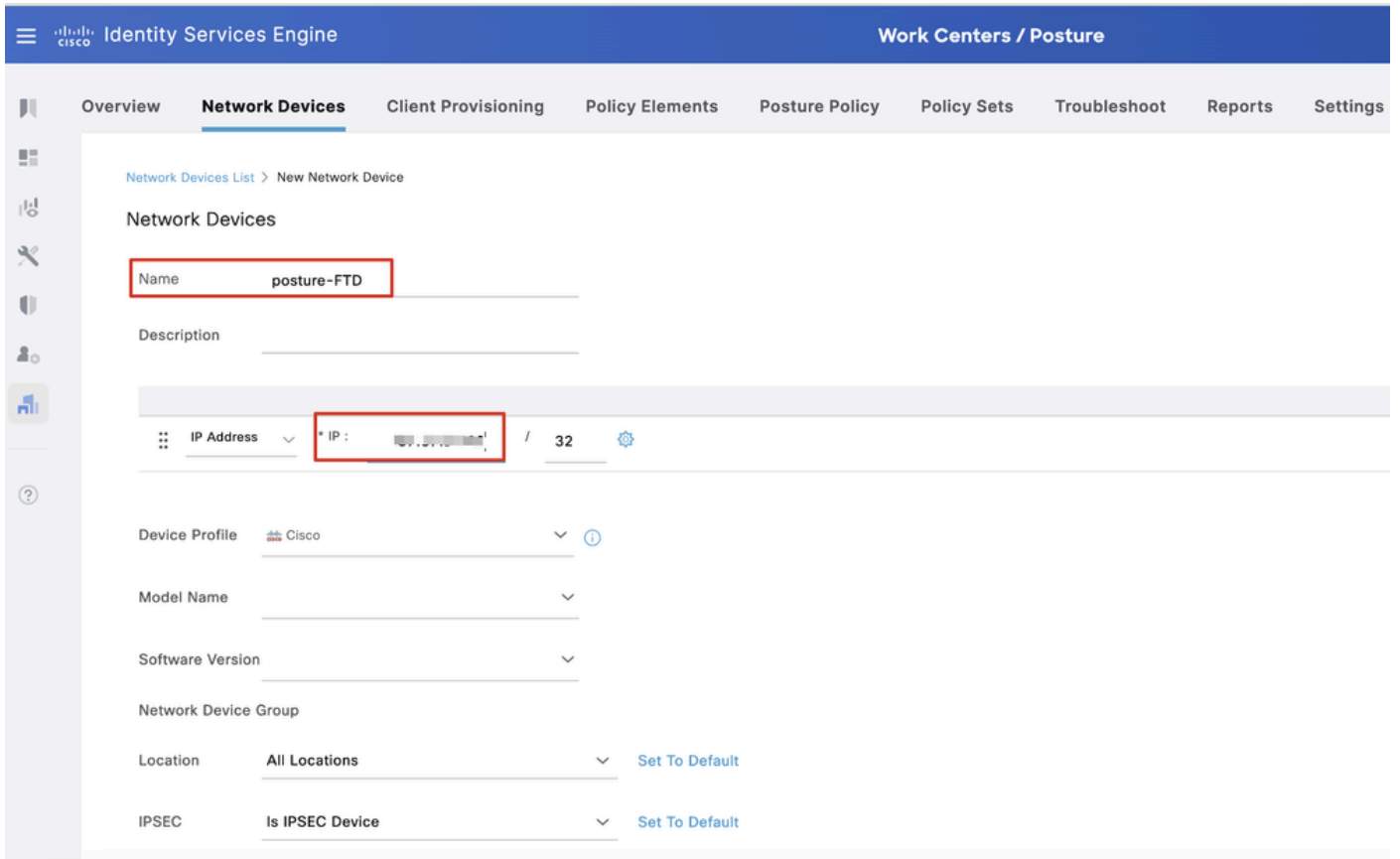
Konfigurationen auf der ISE

Schritt 13: Navigieren Sie zu Work Centers > Posture > Network Devices. Klicken Sie auf .Add



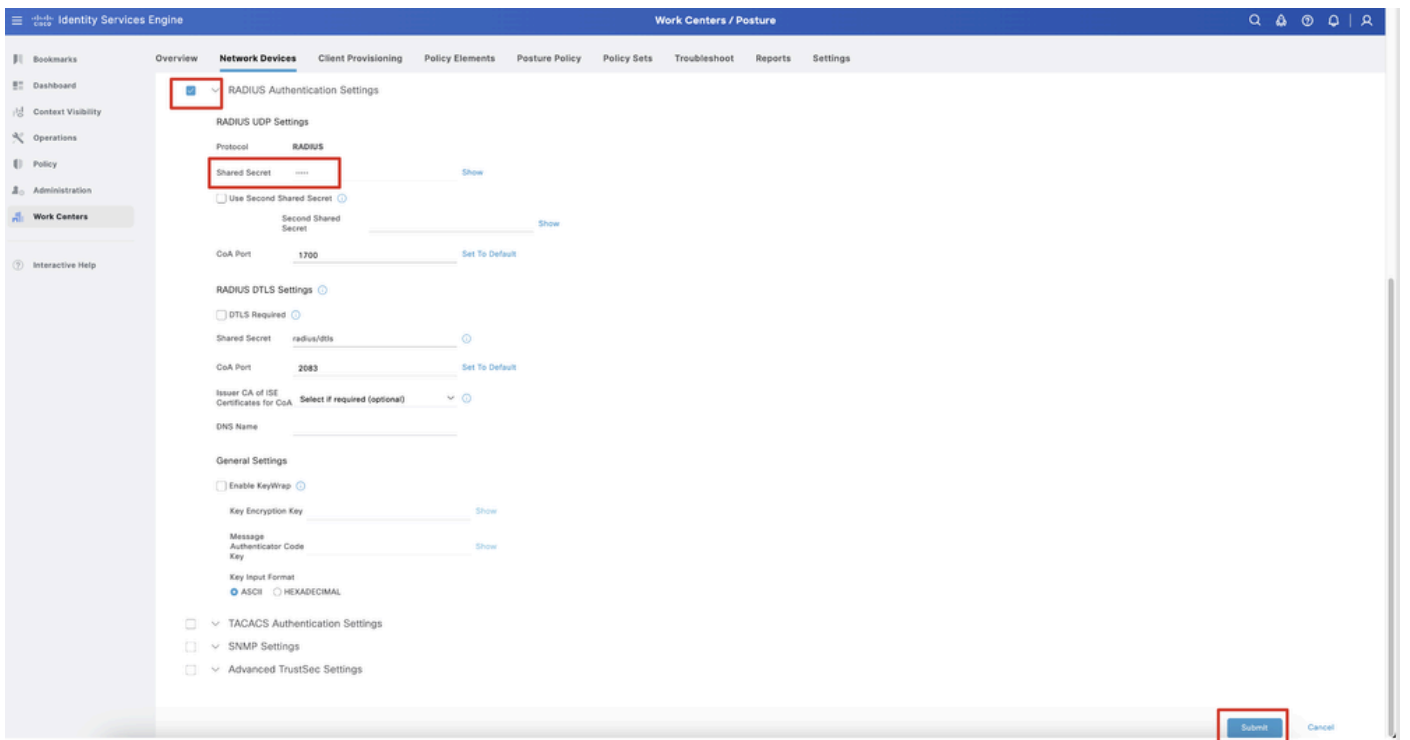
ISE_Hinzufügen_Neue_Geräte

Schritt 13.1: Stellen Sie das bereit, Name, IP Address und blättern Sie auf der Seite nach unten.



ISE_Hinzufügen_Neue_Geräte_1

Schritt 13.2: Aktivieren Sie das Kontrollkästchen von RADIUS Authentication Settings. Stellen Sie die Shared Secret bereit. Klicken Sie auf .Submit



ISE_Hinzufügen_Neue_Geräte_2

Schritt 14: Laden Sie den Paketnamen cisco-secure-client-linux64-4.3.139.0-isecompliance-webdeploy-k9.pkg von [Cisco Software Download](#)

[herunter](#), und vergewissern Sie sich, dass die Datei korrekt ist, indem Sie bestätigen, dass die MD5-Prüfsumme der heruntergeladenen Datei mit der Cisco Software Download-Seite übereinstimmt. Der Paketname cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg wurde in Schritt 1 erfolgreich heruntergeladen.

Schritt 15: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Resources. Klicken Sie auf .Add Auswählen Agent resources from local disk.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The main navigation menu has 'Client Provisioning' selected. The left sidebar shows 'Resources' under 'Client Provisioning Policy'. The main content area is titled 'Resources' and shows a table of agent resources. A dropdown menu is open under the '+ Add' button, with 'Agent resources from local disk' selected. The table below lists various agent resources with columns for Type, Version, Last Update, and Description.

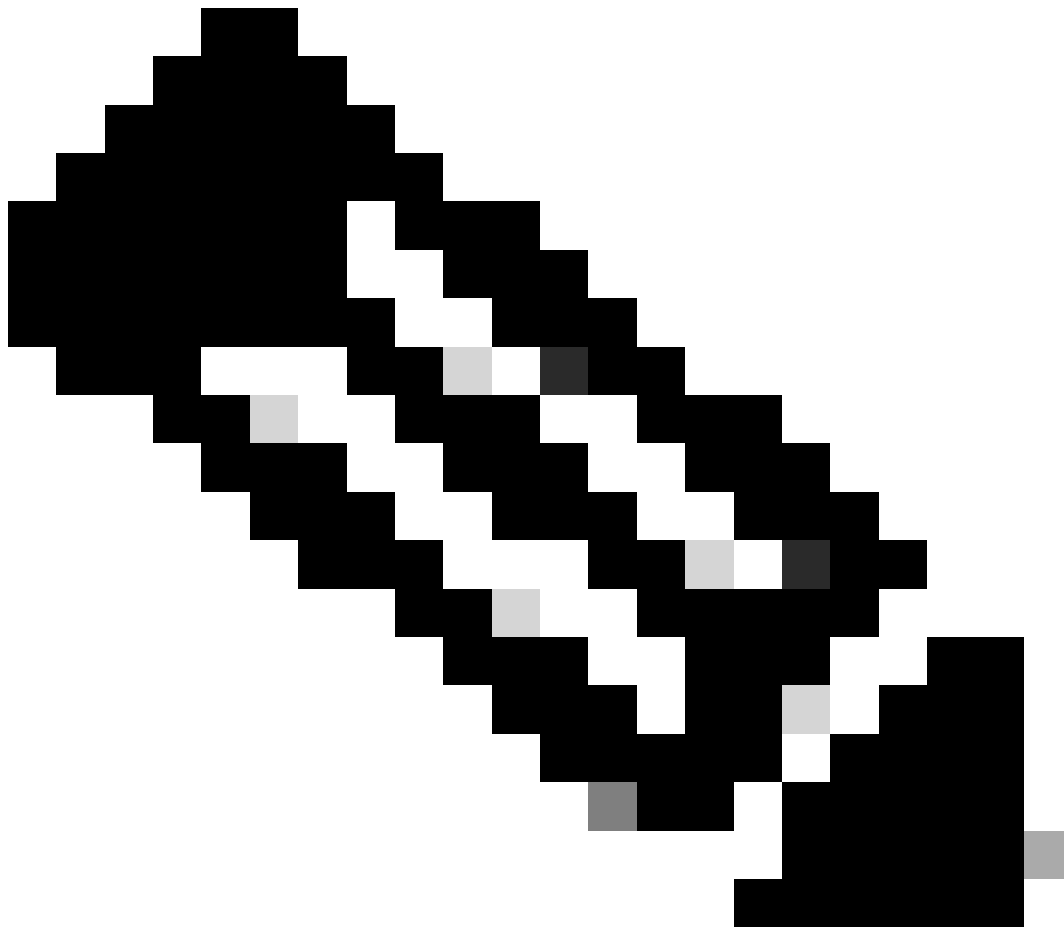
Type	Version	Last Update	Description
WinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Pro...
Native Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured
Native Supplicant Pro...	Not Applic...	2023/07/04 07:55:16	Pre-configured
MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro...
CiscoSecureClientDe...	5.1.3.62	2024/05/08 10:20:06	Cisco Secure C...
CiscoSecureClientDesktopLinux 5.1.3.062	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C...
CiscoSecureClientComplianceModuleWindows 4.3.4015.8192	4.3.4015....	2024/05/08 10:26:57	Cisco Secure C...
CiscoSecureClientComplianceModuleLinux 4.3.3139.0	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure C...
CiscoAgentlessWindows 5.0.03061	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
CiscoAgentlessOSX 5.0.03061	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
CiscoTemporalAgentWindows 5.0.03061	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
CiscoTemporalAgentOSX 5.0.03061	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE_Upload_Resource

Schritt 15.1: Auswählen Cisco Provided Package. Klicken Sie hier Choose File, um cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg hochzuladen. Klicken Sie auf .Submit

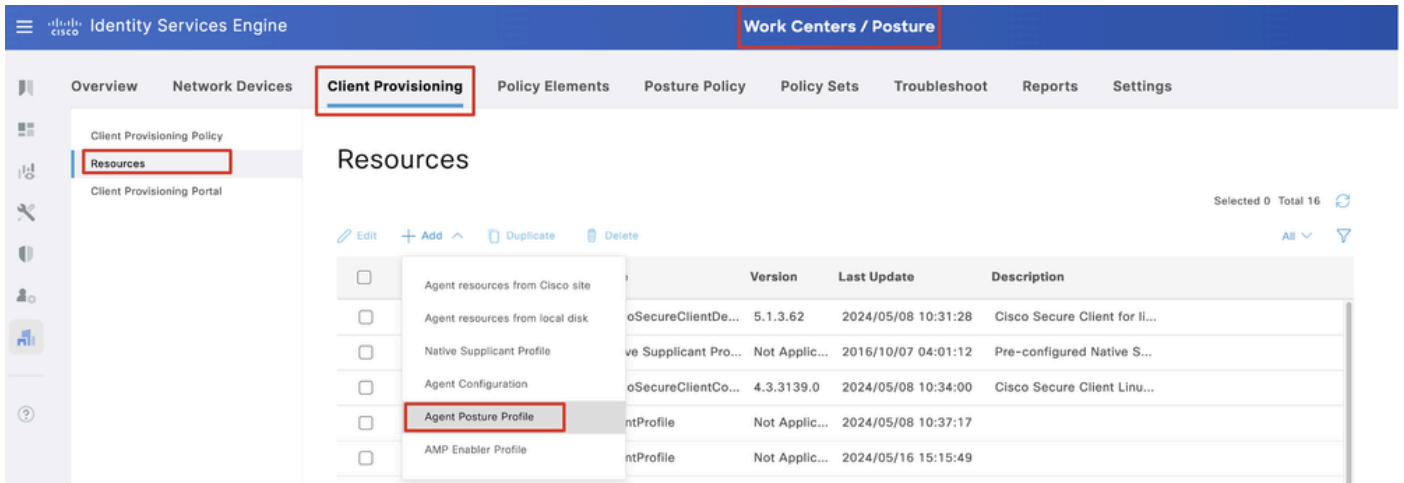
The screenshot shows the Cisco Identity Services Engine (ISE) interface for uploading an agent resource. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The main navigation menu has 'Work Centers' selected. The left sidebar shows 'Work Centers' under 'Administration'. The main content area is titled 'Agent Resources From Local Disk' and shows a form for uploading a file. The 'Category' dropdown is set to 'Cisco Provided Package'. The 'Choose File' button is highlighted, and the file name 'cisco-secure-...eploy-k9.pkg' is visible. Below the form, there is a table of 'Agent Uploaded Resources' with columns for Name, Type, Version, and Description. The 'Submit' button is highlighted.

Name	Type	Version	Description
CiscoSecureClientDesktopLI...	CiscoSecureClientDe...	5.1.3.62	Cisco Secure Client for li...



Hinweis: Wiederholen Sie Schritt 14, um hochzuladen `cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg`.

Schritt 16: Navigieren Sie zu `Work Centers > Posture > Client Provisioning > Resources`. Klicken Sie auf `.Add` Auswählen Agent Posture Profile.

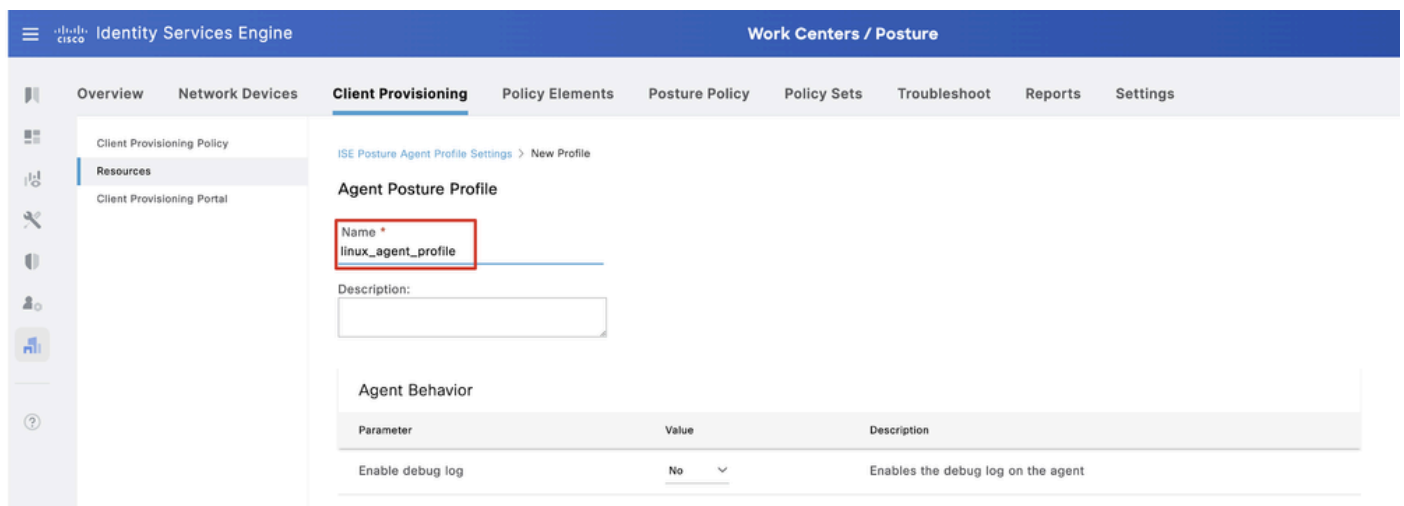


ISE_Add_Agent_Status_Profil

Schritt 16.1: Geben Sie die Name, Server name rules an, und behalten Sie den Rest als Standard bei. Klicken Sie auf .Save

Name: linux_agent_profile

Servernamen-Regeln: *.example.com



ISE_Add_Agent_Posture_Profile_1

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy
Resources
Client Provisioning Portal

Posture Protocol

Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*.example.com	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Cancel Save

ISE_Add_Agent_Posture_Profile_2

Schritt 17: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Resources. Klicken Sie auf .Add Auswählen Agent Configuration.

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy
Resources
Client Provisioning Portal

Resources

Selected 0 Total 16

Edit + Add Duplicate Delete

	Version	Last Update	Description
<input type="checkbox"/> Agent resources from Cisco site			
<input type="checkbox"/> Agent resources from local disk	oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28
<input type="checkbox"/> Native Supplicant Profile	ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12
<input type="checkbox"/> Agent Configuration	oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00
<input type="checkbox"/> Agent Posture Profile	ntProfile	Not Applic...	2024/05/08 10:37:17
<input type="checkbox"/> AMP Enabler Profile	ntProfile	Not Applic...	2024/05/16 15:15:49

ISE_Add_Agent_Konfiguration

Schritt 17.2: Konfigurieren Sie die Details:

Agent-Paket auswählen: CiscoSecureClientDesktopLinux 5.1.3.062

Name: linux_agent_config

Compliance-Modul: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Aktivieren Sie das Kontrollkästchen von VPN, Diagnostic and Reporting Tool

Profilauswahl ISE-Status: linux_agent_profile

Klicken Sie auf .Submit

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

* Select Agent Package: CiscoSecureClientDesktopLinux 5.1.3.062

* Configuration Name: linux_agent_config

Description:

Description Value Notes

* Compliance Module: CiscoSecureClientComplianceModuleLinux 4.3

Cisco Secure Client Module Selection

ISE Posture

VPN

Secure Firewall Posture

Network Visibility

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: linux_agent_profile

Submit Cancel

ISE_Add_Agent_Konfiguration_1

Schritt 18: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Klicken Sie Edit auf das Ende eines beliebigen Regelnamens. Auswählen Insert new policy below.

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP

Duplicate above

Duplicate below

Insert new policy above

Insert new policy below

Delete

ISE_Add_New_Provisioning_Policy

Schritt 18.1: Konfigurieren Sie die Details:

Regelname: Linux

Betriebssysteme: Linux Alle

Ergebnisse: linux_agent_config

Klicken Sie auf Done und Save.

The screenshot shows the 'Client Provisioning Policy' configuration page in Cisco ISE. The 'Linux' rule is highlighted with a red box. The rule details are as follows:

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Linux	If Any	and Linux All	and Condition(s)	then linux_agent_config

ISE_Hinzufügen_Neu_Bereitstellung_Richtlinie_1

Schritt 19: Navigieren Sie zu Work Centers > Posture > Policy Elements > Conditions > File. Klicken Sie auf .Add

The screenshot shows the 'File Conditions' configuration page in Cisco ISE. The '+ Add' button is highlighted with a red box. The page displays a list of predefined file conditions.

Name	Description	File name	Condition Type
pc_xp64_kb2797052_ms13...	Cisco Predefined Check...	SYSTEM_PROGRAMS\C...	Cisco-Defined
pc_w8_64_kb3124275_ms...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_vista_kb2893294_ms13...	Cisco Predefined Check...	SYSTEM_32\imagehlp.dll	Cisco-Defined
pc_w81_64_kb3033889_m...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_vista64_kb925902_ms0...	Cisco Predefined Check...	SYSTEM_ROOT\winsxs\l...	Cisco-Defined
pc_w10_64_1709_kb45803...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_xp_kb2653956_ms12-0...	Cisco Predefined Check...	SYSTEM_32\Wintrust.dll	Cisco-Defined
pc_w8_kb2892074_ms13-...	Cisco Predefined Check...	SYSTEM_32\Scrren.dll	Cisco-Defined
pc_w10_64_1909_kb50139...	Cisco Predefined Check...	SYSTEM_ROOT\SysWO...	Cisco-Defined
pc_w7_kb2681578_ms12-...	Cisco Predefined Check...	SYSTEM_32\Win32k.sys	Cisco-Defined
pc_w10_kb3081436_ms15...	Cisco Predefined Check...	SYSTEM_32\Edgehtml.dll	Cisco-Defined
pc_w81_64_kb3042553_m...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_w8_64_kb2727526_ms...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_w8_64_kb292611_ms...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_w7_kb3078601_ms15-...	Cisco Predefined Check...	SYSTEM_32\Win32k.sys	Cisco-Defined

ISE_Add_New_File_Condition

Schritt 19.1: Konfigurieren Sie die Details:

Name: linux_demo_file_exist

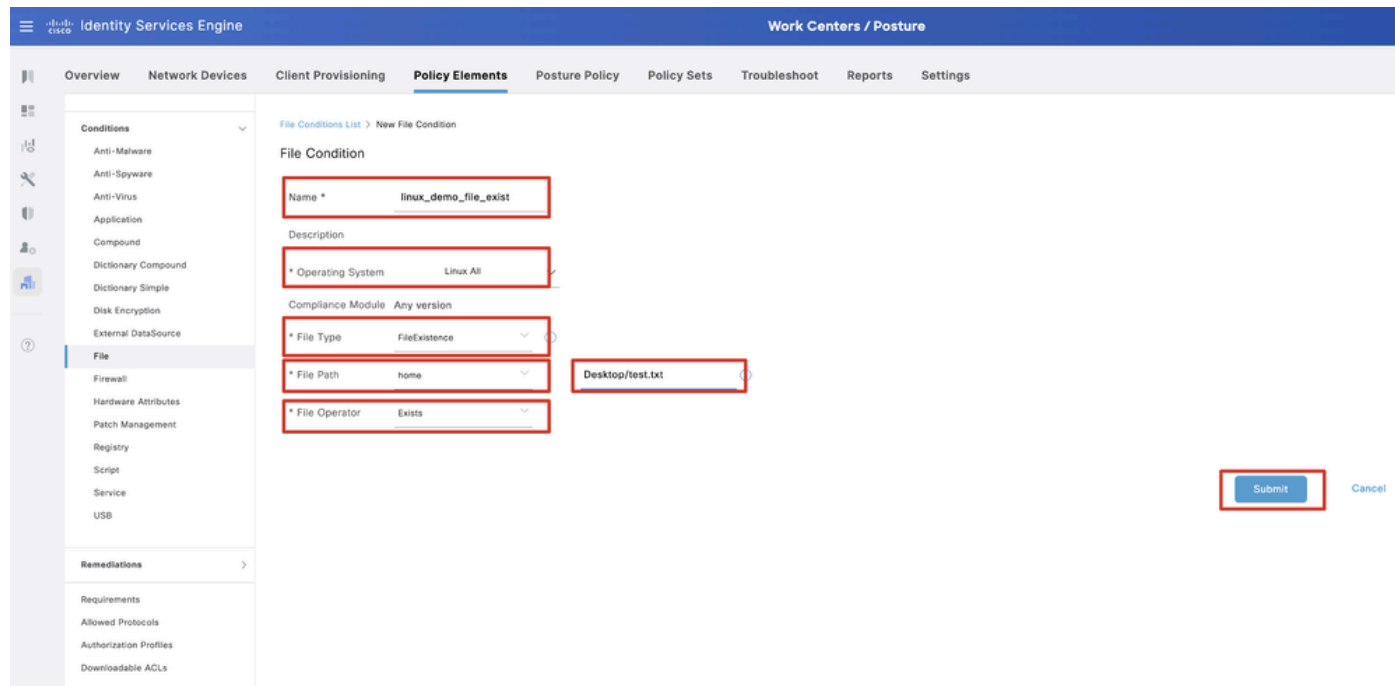
Betriebssysteme: Linux Alle

Dateityp: FileExistence

Dateipfad: home, Desktop/test.txt

Dateioperator: existiert

Klicken Sie auf .Submit



ISE_Hinzufügen_Neue_Datei_Bedingung_1

Schritt 20: Navigieren Sie zu Work Centers > Posture > Policy Elements > Requirements. Klicken Sie Edit auf das Ende eines beliebigen Regelnamens. Auswählen Insert new Requirement.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration **Work Centers** Interactive Help

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs
- Requirements**

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_inst then	Message Text Only	Edit
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_def then	AnyAVDefRemediationWin	Edit Duplicate
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_inst then	Message Text Only	Edit Insert new Requirement
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_def then	AnyASDefRemediationWin	Edit Delete
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_inst then	Message Text Only	Edit
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_def then	AnyAVDefRemediationMac	Edit
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_inst then	Message Text Only	Edit
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_def then	AnyASDefRemediationMac	Edit
Any_AM_Installation_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_inst then	Message Text Only	Edit
Any_AM_Definition_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_def then	AnyAMDefRemediationWin	Edit
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_inst then	Message Text Only	Edit
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_def then	AnyAMDefRemediationMac	Edit
Any_AM_Installation_Lin	for Linux All	using 4.x or later	using Agent	met if ANY_am_lin_inst then	Select Remediations	Edit
Any_AM_Definition_Lin	for Linux All	using 4.x or later	using Agent	met if ANY_am_lin_def then	Select Remediations	Edit
USB_Block	for Windows All	using 4.x or later	using Agent	met if USB_Check then	USB_Block	Edit
Default_AppVia_Requirement_Win	for Windows All	using 4.x or later	using Agent	met if Default_AppVia_Condition_Win then	Select Remediations	Edit
Default_AppVia_Requirement_Mac	for Mac OSX	using 4.x or later	using Agent	met if Default_AppVia_Condition_Mac then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Win	for Windows All	using 4.x or later	using Agent	met if Hardware_Attributes_Check then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using Agent	met if Hardware_Attributes_Check then	Select Remediations	Edit

Note:
Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.

ISE_Hinzufügen_Neu_Status_Anforderung

Schritt 20.1: Konfigurieren Sie die Details:

Name: Test_exist_linux

Betriebssysteme: Linux Alle

Compliance-Modul: 4.x oder spätere Version

Statustyp: Agent

Bedingungen: linux_demo_file_exist

Klicken Sie auf Done und Save.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Required Protocols
- Authorization Profiles
- Downloadable ACLs

Guide Me

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Test_exist_linux	for Linux All	using 4.x or later	using Agent	met if linux_demo_file_exist	then Select Remediations
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_inst	then Message Text Only
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_def	then AnyAVDefRemediationWin
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_inst	then Message Text Only
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_def	then AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_inst	then Message Text Only
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_def	then AnyAMDefRemediationMac

Note:
Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.

Save Reset

ISE_Hinzufügen_Neu_Status_Anforderung_1



Hinweis: Ab sofort werden nur Shell-Skripts für Linux-Agenten als Problembehebung unterstützt.

Schritt 21: Navigieren Sie zu Work Centers > Posture > Policy Elements > Authorization Profiles. Klicken Sie auf .Add

Schritt 21.1: Konfigurieren Sie die Details:

Name: unknown_redirect

Aktivieren Sie das Kontrollkästchen von Web Redirection(CWA,MDM,NSP,CPP)

Auswählen Client Provisioning(Posture)

ACL: umleiten

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, the navigation bar includes 'Work Centers / Posture'. The main navigation menu has 'Policy Elements' selected. The left sidebar lists various categories, with 'Authorization Profiles' highlighted. The main content area is titled 'Authorization Profile' and shows the configuration for a profile named 'unknown_redirect'. The 'Name' field is 'unknown_redirect', and the 'Access Type' is 'ACCESS_ACCEPT'. Under 'Common Tasks', the 'Web Redirection (CWA, MDM, NSP, CPP)' checkbox is checked, and the 'ACL' dropdown is set to 'redirect'. The 'Value' dropdown is set to 'Client Provisioning Portal (defi...)'.

ISE_Add_New_Authorization_Profile_Redirect_1



Hinweis: Diese ACL-Namensweiterleitung muss mit dem entsprechenden, für FTD konfigurierten ACL-Namen übereinstimmen.

Schritt 21.2: Wiederholen Sie den Schritt, Add um weitere zwei Autorisierungsprofile für nicht konforme und konforme Endpunkte mit den Details zu erstellen.

Name: nicht_konformes_Profil

DACL-Name: DENY_ALL_IPv4_TRAFFIC

Name: compliant_profile

DACL-Name: PERMIT_ALL_IPv4_TRAFFIC



Hinweis: Die DACL für kompatible oder nicht kompatible Endgeräte muss entsprechend den tatsächlichen Anforderungen konfiguriert werden.

Schritt 22: Navigieren Sie zu Work Centers > Posture > Posture Policy. Klicken Sie Edit am Ende einer Regel auf. Auswählen Insert new policy.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning Policy Elements **Posture Policy** Policy Sets Troubleshoot Reports Settings

Posture Policy Guide Me

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements	
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Any_AM_Installation_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Any_AM_Installation_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win	Any	Windows All	4.x or later	Agent		Any_AM_Installation_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Any_AM_Installation_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Default_AppViz_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Default_AppViz_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win	Any	Windows All	4.x or later	Agent		Default_AppViz_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_AppViz_Requirement_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Default_Firewall_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Default_Firewall_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win	Any	Windows All	4.x or later	Agent		Default_Firewall_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Firewall_Requirement_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Default_Hardware_Attributes_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Win	Any	Windows All	4.x or later	Agent		Default_Hardware_Attributes_Requirement_Win	Edit - Duplicate

ISE_Hinzufügen_Neuer_Status_Richtlinie

Schritt 22.1: Konfigurieren Sie die Details:

Regelname: Demo_test_exist_linux

Identitätsgruppen: Alle

Betriebssysteme: Linux Alle

Compliance-Modul: 4.x oder spätere Version

Statustyp: Agent

Voraussetzungen: Test_exist_linux

Klicken Sie auf Done und Save.

Identity Services Engine Work Centers / Posture

Posture Policy Guide Me

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Mac	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Mac	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Win	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Win_temporal	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Hardware_Attributes_Requirement_Mac	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Mac_temporal	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Hardware_Attributes_Requirement_Win	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Win_temporal	Edit
<input type="checkbox"/>	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then USB_Block	Edit
<input type="checkbox"/>	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then USB_Block_temporal	Edit
<input checked="" type="checkbox"/>	Demo_test_exist_linux	If Any	and Linux All	and 4.x or later	and Agent	and	then Test_exist_linux	Edit

ISE_Hinzufügen_Neu_Status_Richtlinie_1

Schritt 23: Navigieren Sie zu Work Centers > Posture > Policy Sets. Klicken Sie auf Insert new row above.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning Policy Elements Posture Policy **Policy Sets** Troubleshoot Reports Settings

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Default	Default policy set		Default Network Access		+ o ⚙️	▶

Insert new row above Reset Save

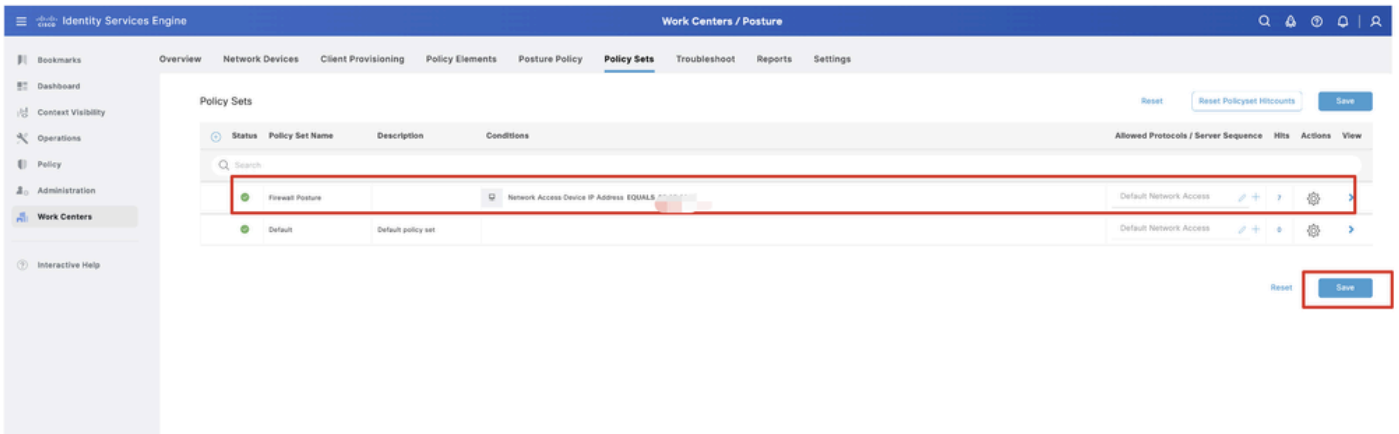
ISE_Hinzufügen_Neu_Policy_Set

Schritt 23.1: Konfigurieren Sie die Details:

Richtliniensatzname: Firewall-Status

Bedingungen: IP-Adresse des Netzwerkzugriffsgeräts ENTSPRICHT [FTD-IP-Adresse]

Klicken Sie auf Save



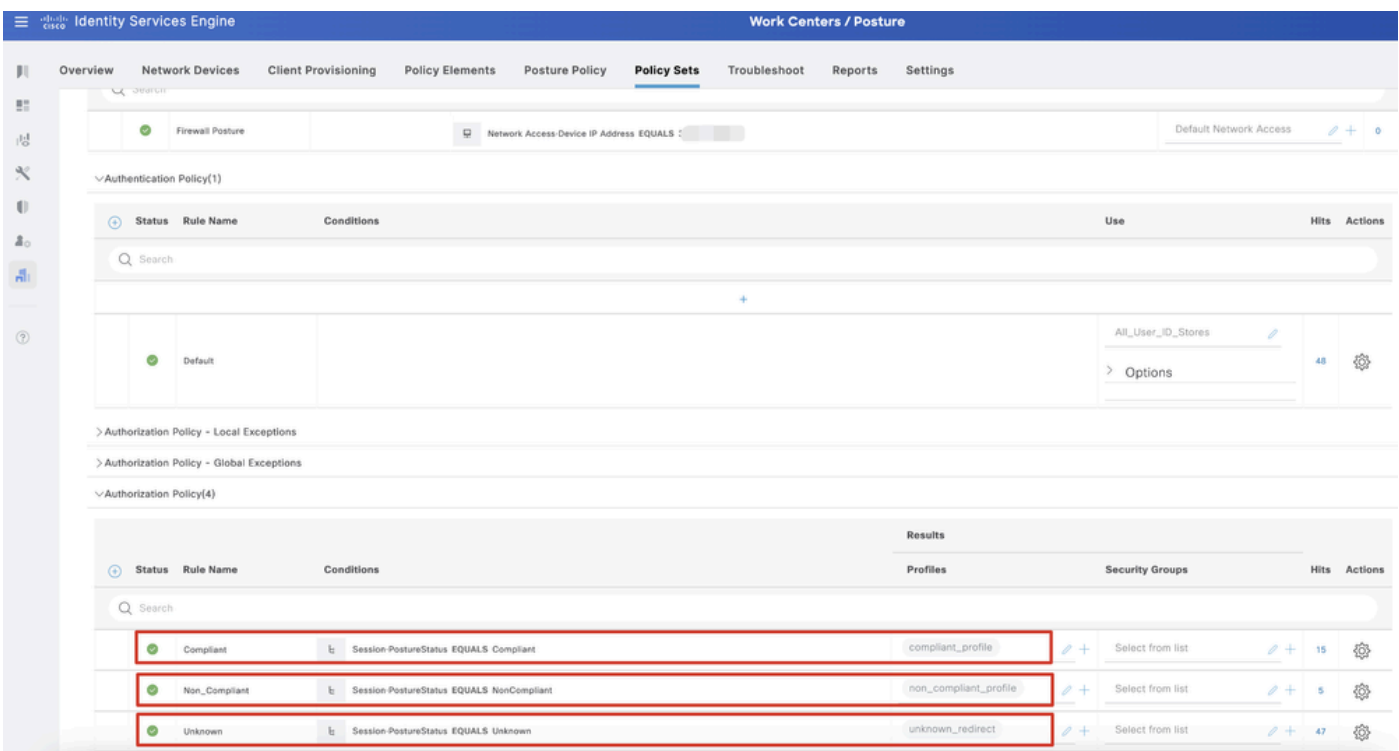
ISE_Hinzufügen_Neue_Richtlinie_Festlegen_1

Schritt 23.2: Klicken Sie >, um den Richtlinienatz einzugeben. Erstellen Sie neue Autorisierungsregeln für den Status "Compliance", "Compliance nicht" und "Unbekannt". Klicken Sie auf .Save

Konformität mit compliance_profile

Nicht konform mit nicht konformem Profil

Unbekannt mit unknown_redirect



ISE_Hinzufügen_Neue_Richtlinie_Festlegen_2

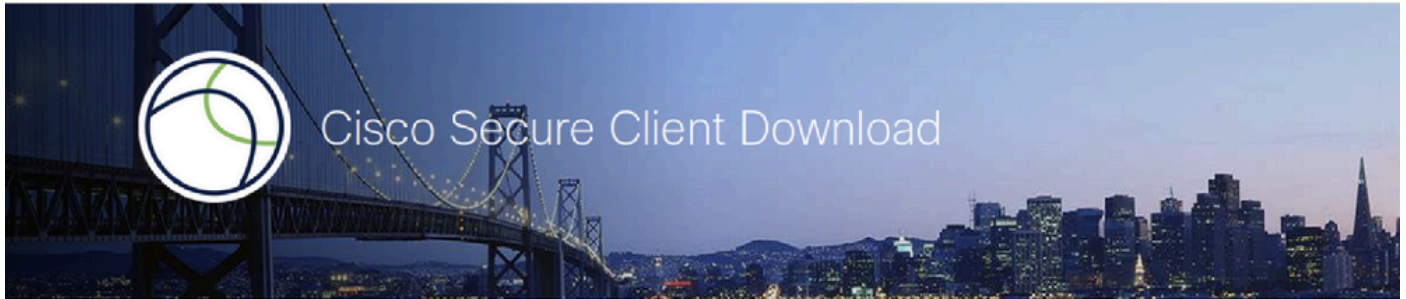
Konfigurationen unter Ubuntu

Schritt 24: Melden Sie sich über die Benutzeroberfläche beim Ubuntu-Client an. Öffnen Sie den Browser, um sich beim VPN-Portal anzumelden. In diesem Beispiel ist dies demo.example.com.

A screenshot of a 'Logon' dialog box. The dialog has a title bar with a key icon and the text 'Logon'. Inside the dialog, there are three input fields: a dropdown menu for 'Group' with 'posture_vpn' selected, a text box for 'Username', and a text box for 'Password'. Below these fields is a button labeled 'Logon'.

Ubuntu-Browser_VPN_Anmeldung

Schritt 25: Klicken Sie auf `.Download for Linux`



Download & Install

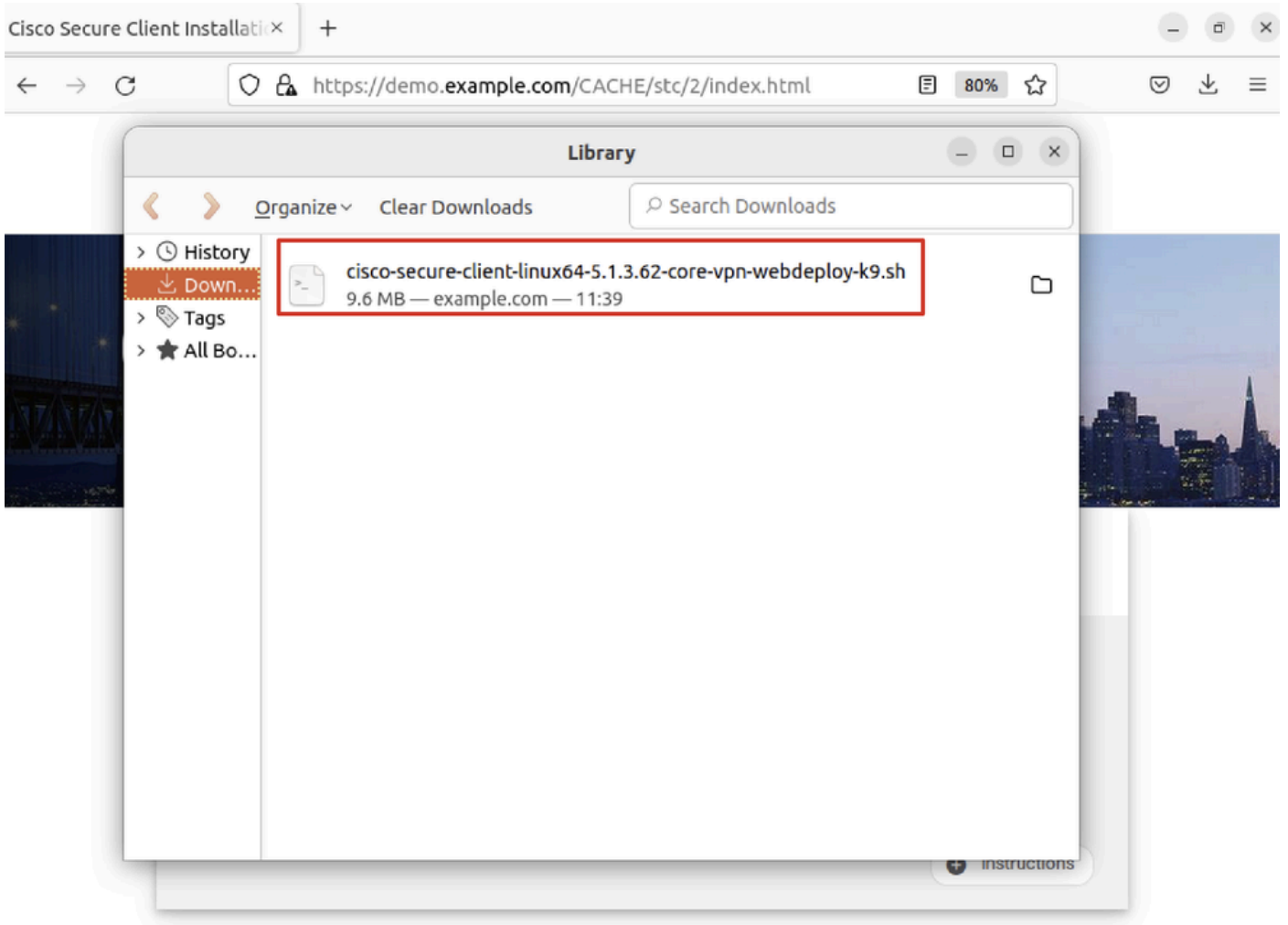
Download Cisco Secure Client and install it on your computer.

[Download for Linux](#)

[+ Instructions](#)

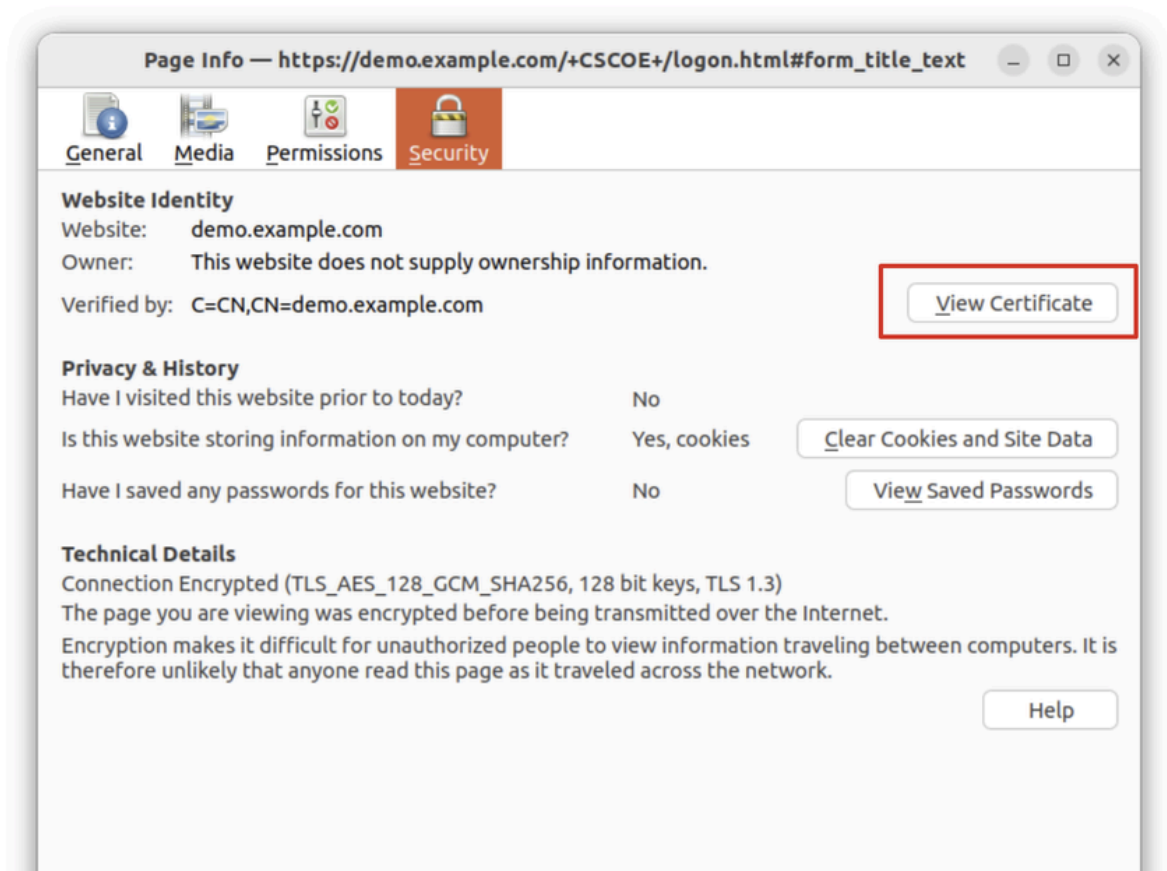
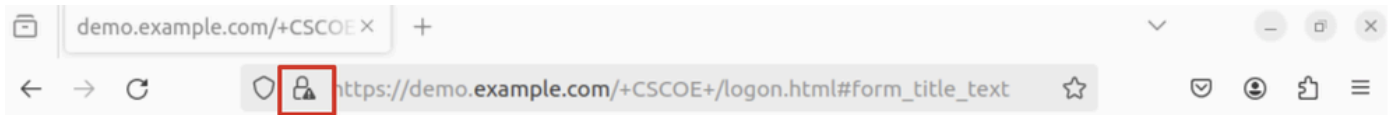
Ubuntu-Browser_VPN_Download_1

Der Name der heruntergeladenen Datei lautet cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu-Browser, VPN, Download 2

Schritt 26: Laden Sie das VPN-Zertifikat über den Browser herunter, und benennen Sie die Datei um in <Zertifikat>.crt. Dies ist das Beispiel, in dem Firefox zum Herunterladen des Zertifikats verwendet wird.



Ubuntu-Browser_VPN_Zertifikat_Herunterladen

Schritt 27: Öffnen Sie das Terminal auf dem Ubuntu-Client. Navigieren Sie zu `path home/user/Downloads/` um Cisco Secure Client zu installieren.

```
<#root>
```

```
user@ubuntu22-desktop:~$
```

```
cd Downloads/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
ls
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
demo-example-com.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo ./cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
[sudo] password for user:
```

```
Installing Cisco Secure Client...
```

```
Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory
```

```
Extracting installation files to /tmp/vpn.zaeAZd/vpninst959732303.tgz...
```

```
Unarchiving installation files to /tmp/vpn.zaeAZd...
```

```
Starting Cisco Secure Client Agent...
```

```
Done!
```

```
Exiting now.
```

```
user@ubuntu22-desktop:~/Downloads$
```

Schritt 28: Vertrauen Sie dem VPN-Portalzertifikat auf dem Ubuntu-Client.

```
<#root>
```

```
user@ubuntu22-desktop:~$
```

```
cd Downloads/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
ls
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
demo-example-com.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
openssl verify demo-example-com.crt
```

```
CN = demo.example.com, C = CN
```

```
error 18 at 0 depth lookup: self-signed certificate
```

```
Error demo-example-com.crt:
```

```
verification failed
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo cp demo-example-com.crt /usr/local/share/ca-certificates/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
```

```
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

```
1 added
```

```
, 0 removed; done.
```

```
Running hooks in /etc/ca-certificates/update.d...
```

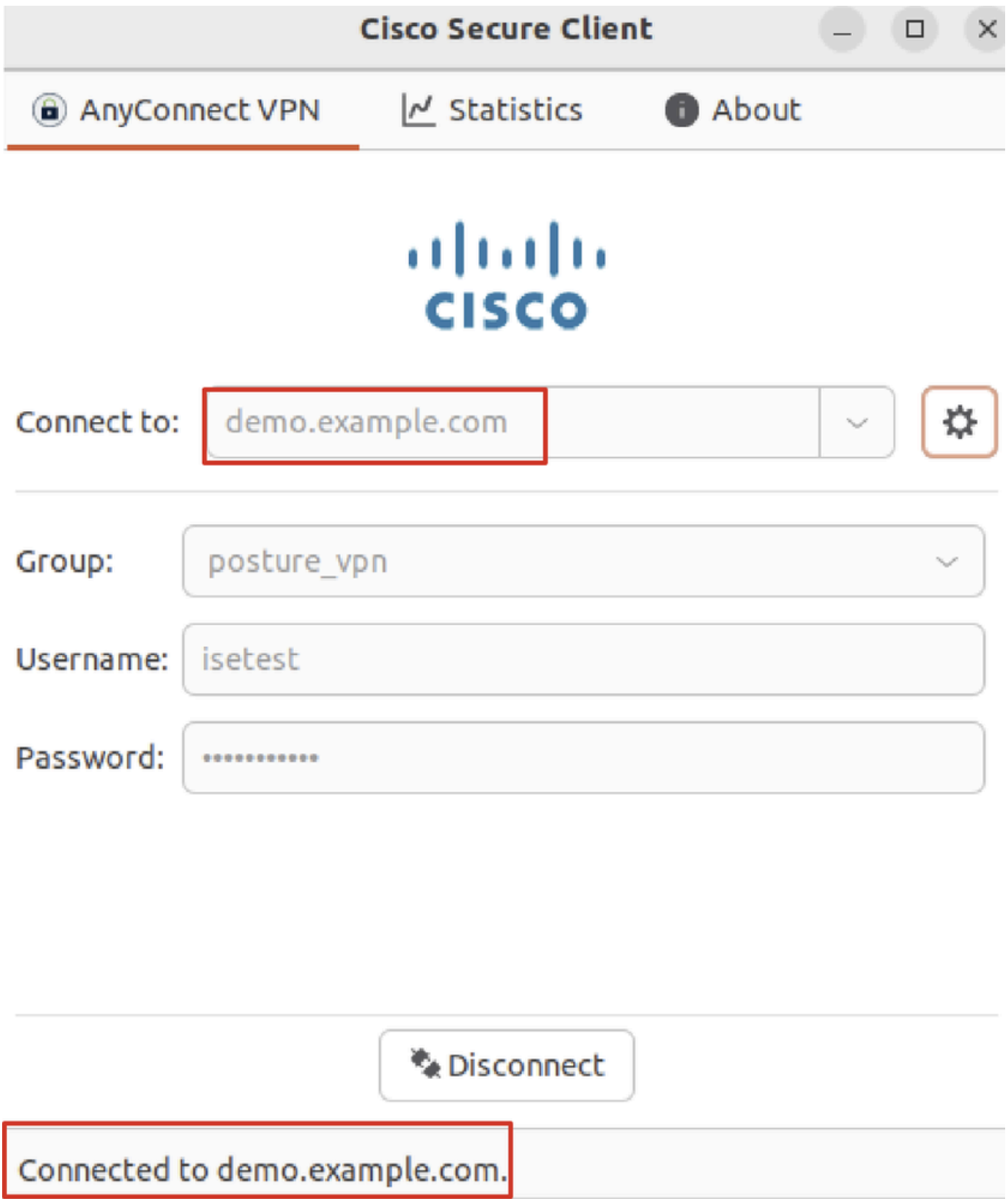
done.

```
user@ubuntu22-desktop:~/Downloads$
```

```
openssl verify demo-example-com.crt
```

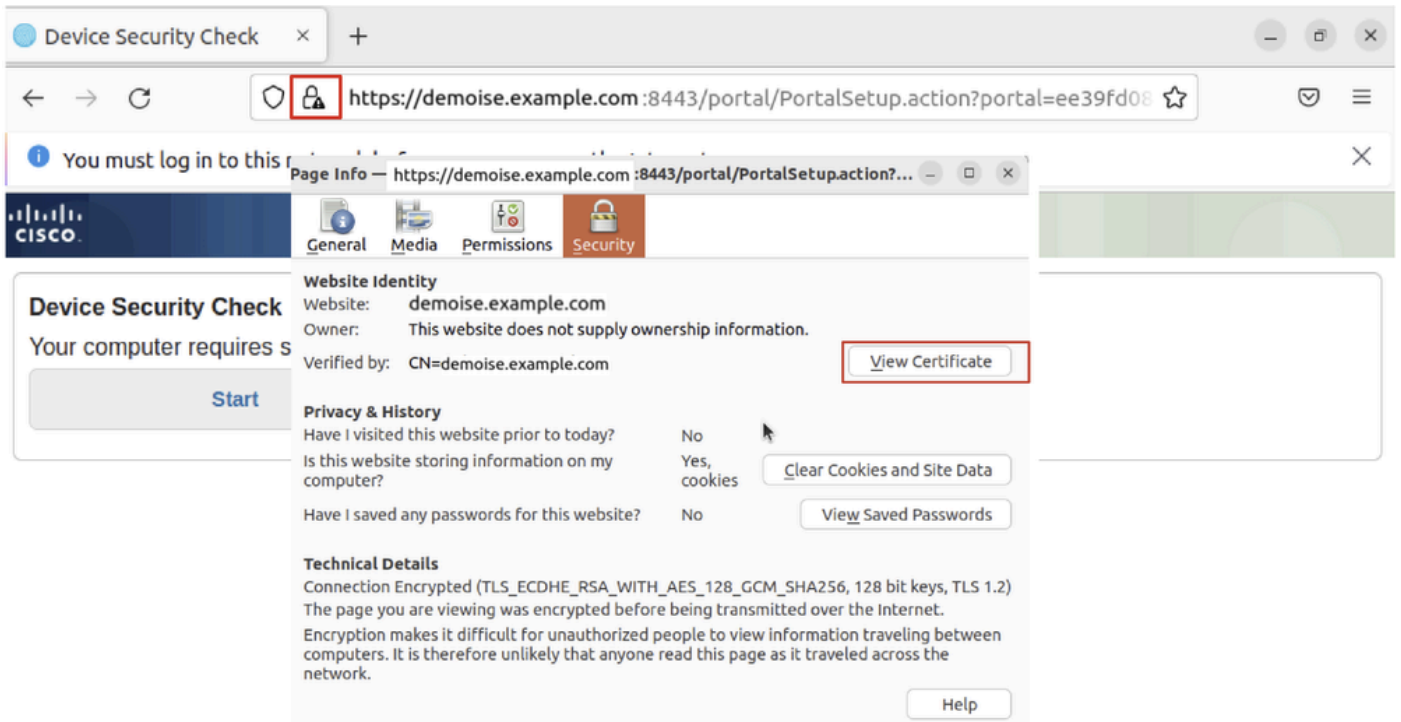
```
demo-example-com.crt: OK
```

Schritt 29: Öffnen Sie Cisco Secure Client auf dem Ubuntu-Client, und stellen Sie eine Verbindung zwischen VPN und demo.example.com her.



Ubuntu_Secure_Client_Verbunden

Schritt 30: Öffnen Sie den Browser, um auf eine Website zuzugreifen, die die Umleitung zum ISE CPP-Portal auslöst. Laden Sie das Zertifikat vom ISE CPP-Portal herunter, und benennen Sie die Datei um in <Zertifikat>.crt. Dies ist ein Beispiel für die Verwendung von Firefox zum Herunterladen.



Ubuntu-Browser_CPP_Zertifizierung_Herunterladen

Schritt 30.1: Vertrauen Sie dem ISE CPP-Portalzertifikat auf dem Ubuntu-Client.

<#root>

```
user@ubuntu22-desktop:~/Downloads$ ls
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
```

```
ise-cert.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo cp ise-cert.crt /usr/local/share/ca-certificates/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
```

```
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

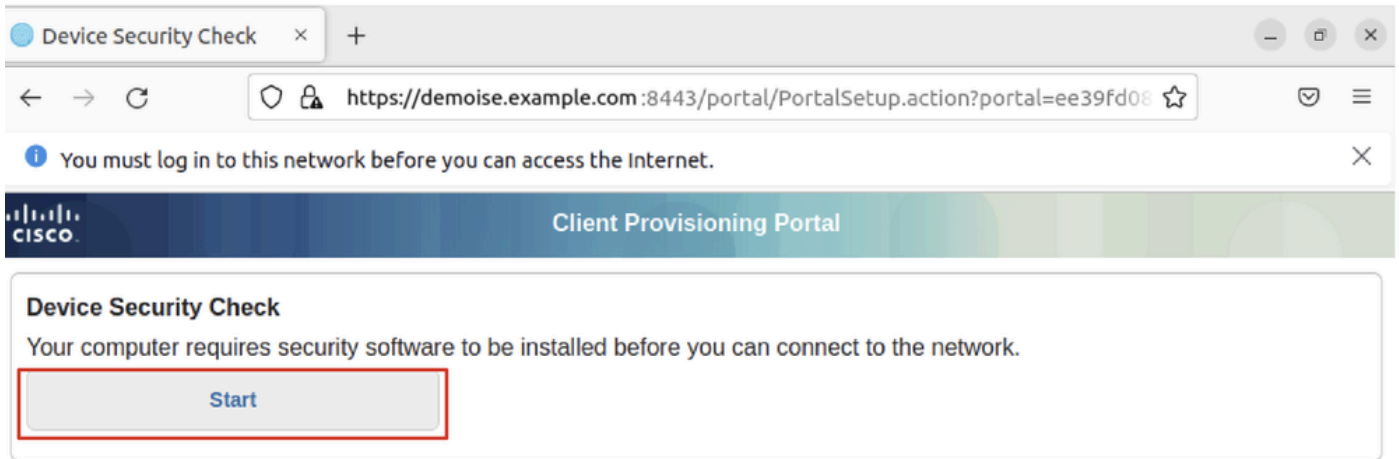
```
1 added
```

```
, 0 removed; done.
```

```
Running hooks in /etc/ca-certificates/update.d...
```

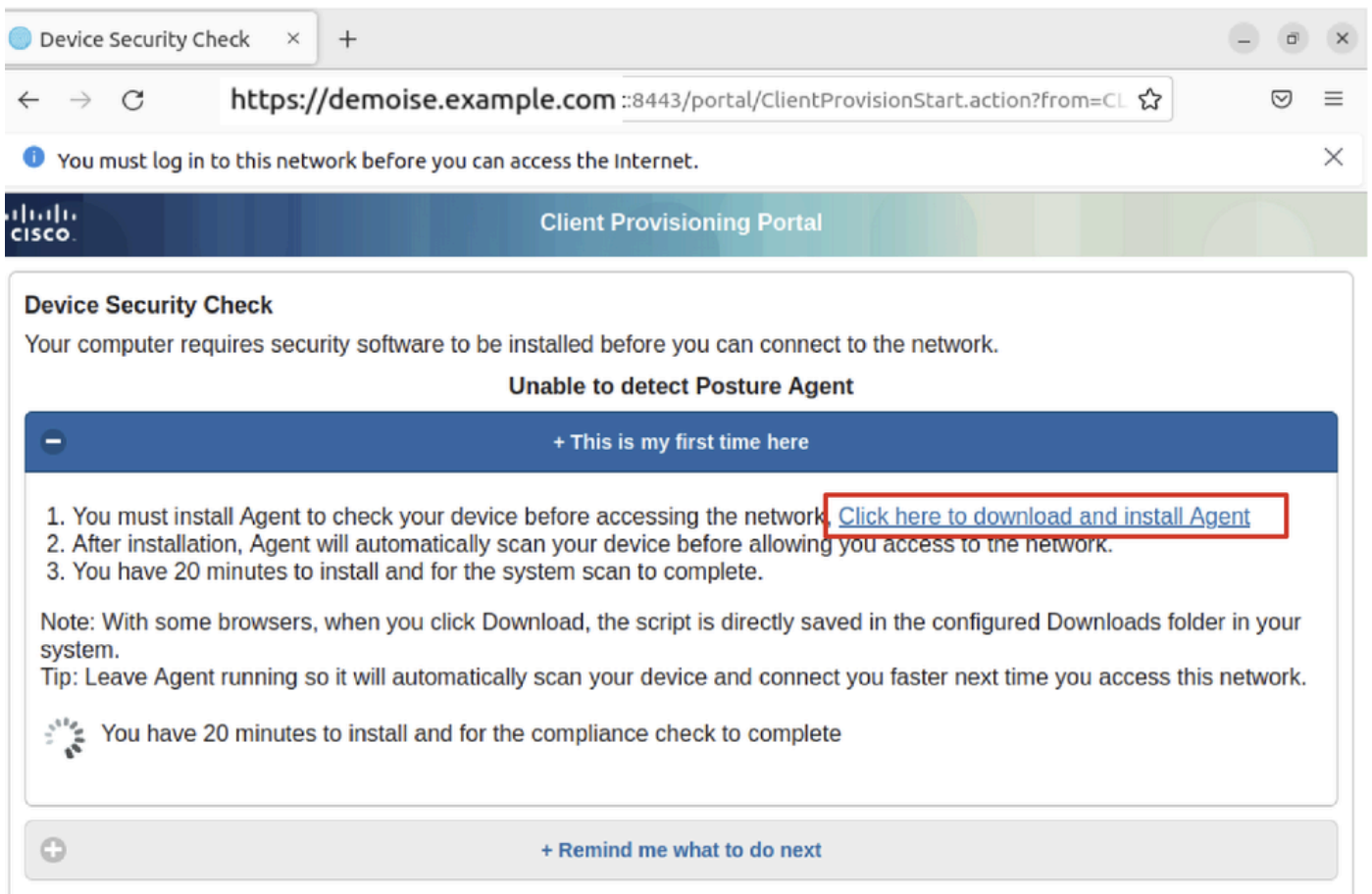
```
done.
```

Schritt 31: Klicken Sie Start auf das ISE CPP-Portal.



Ubuntu-Browser_CPP_Start

Schritt 32. Click here to download and install Agent.



Ubuntu-Browser_CPP_Download_Status

Schritt 33: Öffnen Sie das Terminal auf dem Ubuntu-Client. Navigieren Sie zum Pfadhome/user/Downloads/, um das Statusmodul zu installieren.

```
<#root>
```

```
user@ubuntu22-desktop:~/Downloads$ ls
```

```
cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6HoLmL
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
ise-cert.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6H0
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
./cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6H0
```

Cisco Network Setup Assistant

(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks

Cisco ISE Network Setup Assistant started. Version - 5.1.3.62

Trusted and Secure Connection

You are connected to

demoise.example.com

whose identity has been certified. Your connection to this website is encrypted.

Downloading Cisco Secure Client...

Downloading remote package...

Running Cisco Secure Client - Downloader...

Installation is completed.

Schritt 34: Beenden Sie auf der Benutzeroberfläche des Ubuntu-Clients den Cisco Secure Client, und öffnen Sie ihn erneut. Das ISE-Statusmodul wurde installiert und erfolgreich ausgeführt.



Ubuntu_Secure_Client_ISE_Posture_Installed

Schritt 35: Öffnen Sie das Terminal auf dem Ubuntu-Client. Navigieren Sie zu Pfad `home/user/Desktop` , und erstellen Sie eine Datei, um die auf der ISE konfigurierte Dateibedingung zu erfüllen `test.txt`.

```
<#root>
```

```
user@ubuntu22-desktop:~$
```

```
cd Desktop/
```

```
user@ubuntu22-desktop:~/Desktop$
```

echo test > test.txt

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Verbinden Sie VPN mit demo.example.com auf dem Ubuntu-Client.



The screenshot shows the Cisco Secure Client application window. The title bar reads "Cisco Secure Client". The main menu includes "AnyConnect VPN", "Statistics", "ISE Posture", and "About". The "ISE Posture" section is active, displaying the Cisco logo and a "Connect to:" field with the value "demo.example.com". Below this are fields for "Group" (posture_vpn), "Username" (isetest), and "Password" (masked with dots). A "Disconnect" button is visible at the bottom. A status bar at the bottom of the window displays "Connected to demo.example.com."

Verify_Ubuntu_Secure_Client_Connected

Schritt 2: Überprüfen Sie den Status des ISE-Status auf dem Ubuntu-Client.



Network access allowed.



Verify_Ubuntu_Secure_Client_Compliant

Schritt 3: Aktivieren Sie Radius Live Log auf ISE. Navigieren Sie zu Operations > RADIUS Live Log.

Identity Services Engine | Operations / RADIUS

Live Logs | Live Sessions

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

Refresh: Never | Show: Latest 20 records | Within: Last 24 hours

Reset Repeat Counts | Export To

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
			Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
May 29, 2024 09:08:48.798 PM	●		isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default	Firewall Posture >> Compliant
May 29, 2024 09:08:48.798 PM	✔			52:54:00:17:6B:FA		Compliant	Firewall Posture	Firewall Posture >> Compliant
May 29, 2024 09:08:13.570 PM	✔		isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default	Firewall Posture >> Unknown

Schritt 4: Navigieren Sie über SSH oder Konsole zu FTD CLI.

```
<#root>
```

```
>  
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
ftdv741>
```

```
enable
```

```
Password:
```

```
ftdv741#
```

```
ftdv741#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : isetest Index : 33
```

```
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx : 51596 Bytes Rx : 17606
```

```
Pkts Tx : 107 Pkts Rx : 136
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
Group Policy : posture_gp Tunnel Group : posture_vpn
```

```
Login Time : 14:02:25 UTC Fri May 31 2024
```

```
Duration : 0h:00m:55s
```

```
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
```

```
Audt Sess ID : cb007182000210006659d871
```

```
Security Grp : none Tunnel Zone : 0
```

```
AnyConnect-Parent Tunnels: 1
```

```
SSL-Tunnel Tunnels: 1
```

```
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
```

```
Tunnel ID : 33.1
```

```
Public IP : 192.168.10.13
```

```
Encryption : none Hashing : none
```

```
TCP Src Port : 59180 TCP Dst Port : 443
```

```
Auth Mode : userPassword
```

```
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
```

```
Client OS : linux-64
```

```
Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)
```

Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62

Bytes Tx : 6364 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 33.2
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 59182
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 6364 Bytes Rx : 498
Pkts Tx : 1 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:

Tunnel ID : 33.3
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56078
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 38868 Bytes Rx : 17108
Pkts Tx : 105 Pkts Rx : 130
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Informationen zum Statusablauf und zur Fehlerbehebung bei Cisco Secure Client und der ISE finden Sie in den CCO-[DokumentenISE-Statusstilvergleich für Vor- und Nachbereitung 2.2](#) und [Fehlerbehebung bei ISE-Sitzungsmanagement und -status](#).

Zugehörige Informationen

- [Kompatibilität der Cisco Identity Services Engine mit Netzwerkkomponenten, Version 3.3](#)

- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3](#)
- [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.