

ISE 3.3 عم Linux VPN ةيعضو نيوكت

تايوتحمل

[قمدملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[ةكبشليليطيختلا مسرلا](#)

[FMC/FTD يلعتاننيوكتلا](#)

[ISE يلعتاننيوكتلا](#)

[Ubuntu يف تاننيوكتلا](#)

[ةحصللا نم ققحتلا](#)

[اهجالص او عاخالألا فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

تامدخ كرحم مادختساب Linux نم VPN ةكبش ةيعضو نيوكت ةيفيكن دنتسملا اذه حضوي (FTD) ةيرانلا ةقاطلا ديدهت دض عافدلاو (ISE) ةيوهلا

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco ي صوت

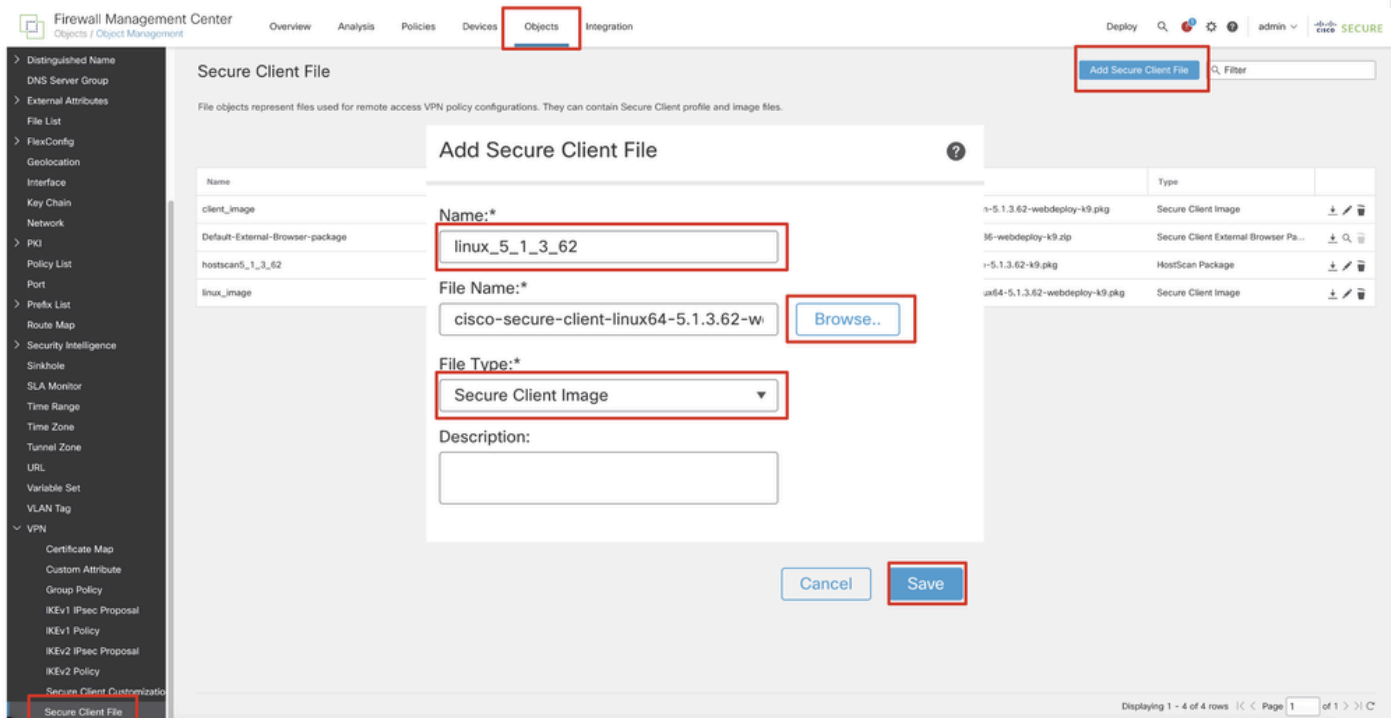
- Cisco Secure Client
- VPN ةكبش يلى دعب نع لوصولل FirePOWER (FTD) ديدهت نع عافدلا
- (ISE) ةيوهلا تامدخ كرحم

ةمدختسملا تانوكملا

ةيلاتلا جماربال تارادصا يلى دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Ubuntu، رادصإلا 22.04
- Cisco Secure Client 5.1.3.62
- Cisco 7.4.1 FirePOWER (FTD) ديدهت دض عافدلا جماربال
- Cisco Firepower (FMC) 7.4.1 ةرادا زكرم
- Cisco Identity Services Engine (ISE) 3.3

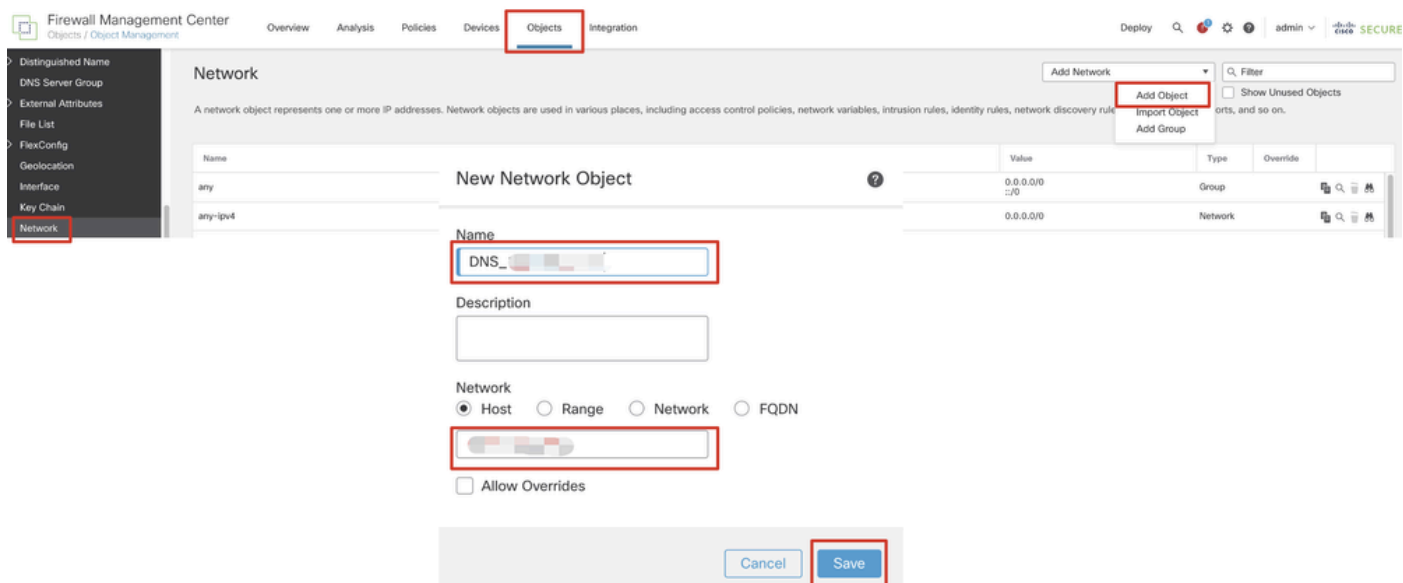
ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجالألا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت



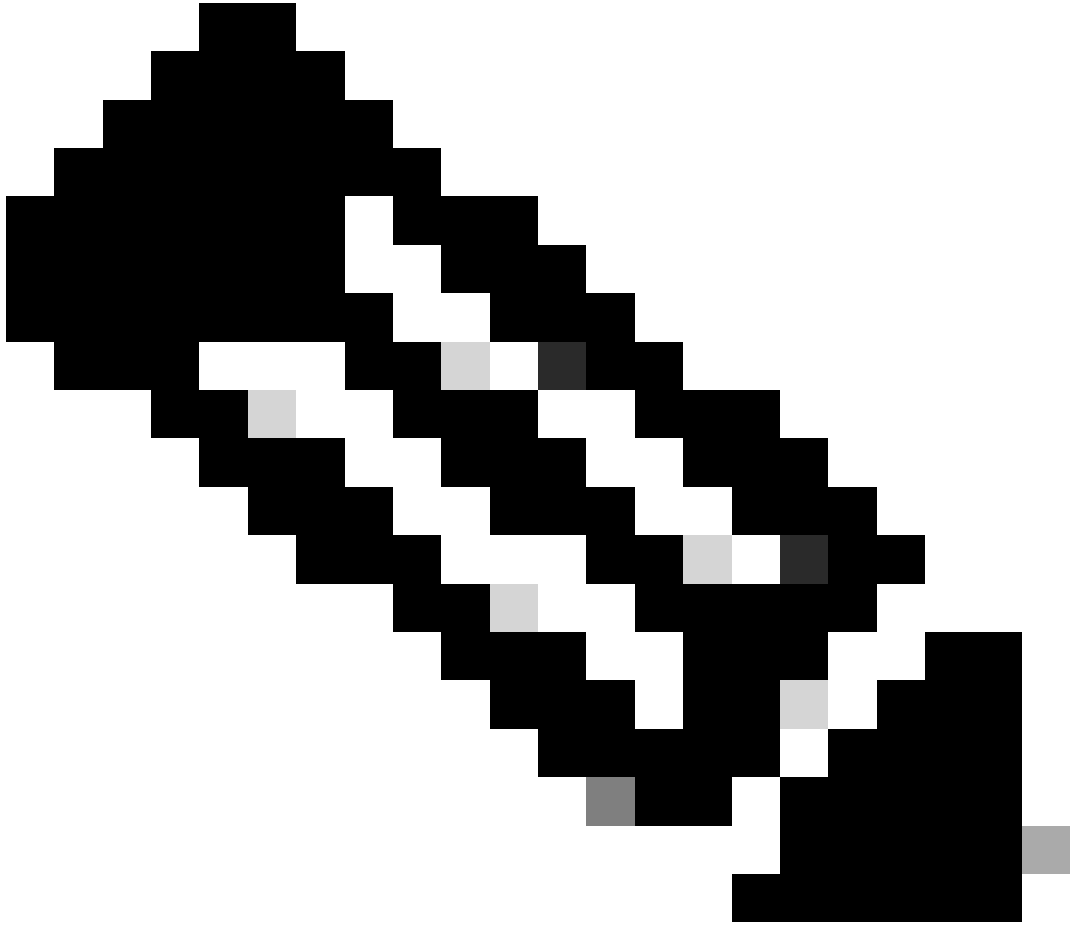
FMC_Upload_Secure_Client_Image

4. عوطخال Objects > Object Management > Network.

Save. رقنا DNS ل رفوتم ال IP نا ونعو مسالا ريفوتب مق ، Add Object، رقنا DNS مداخل نئاك عاشناب مق . 4.1 عوطخال

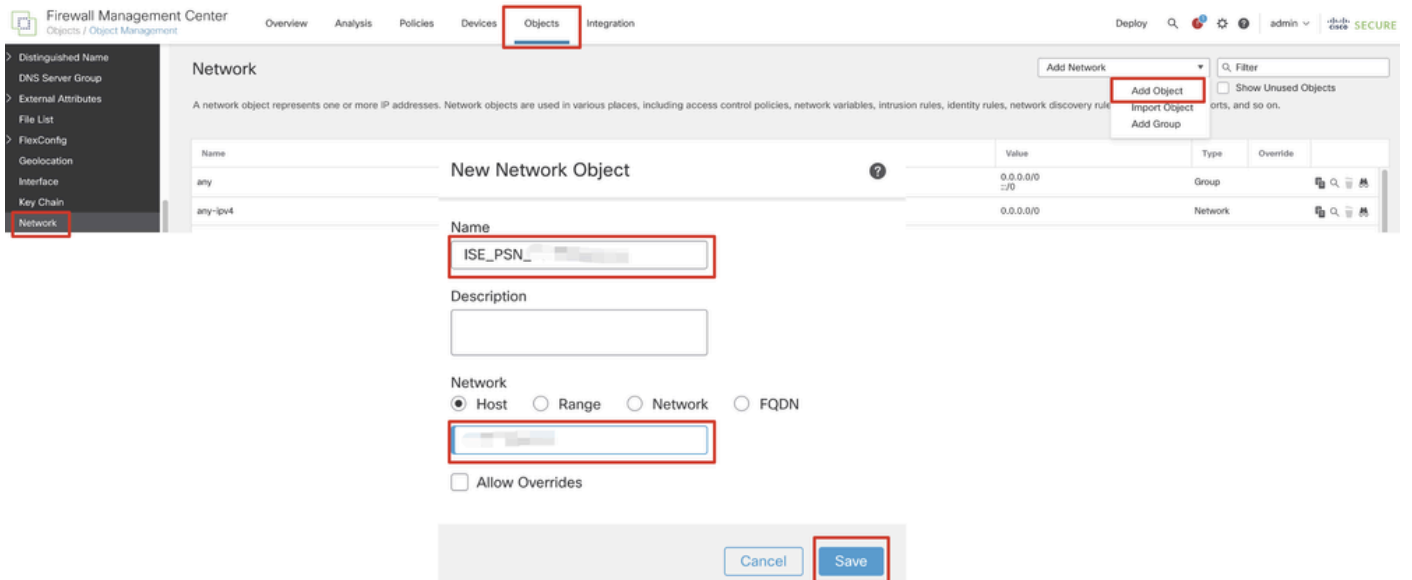


FMC_Add_Object_DNS



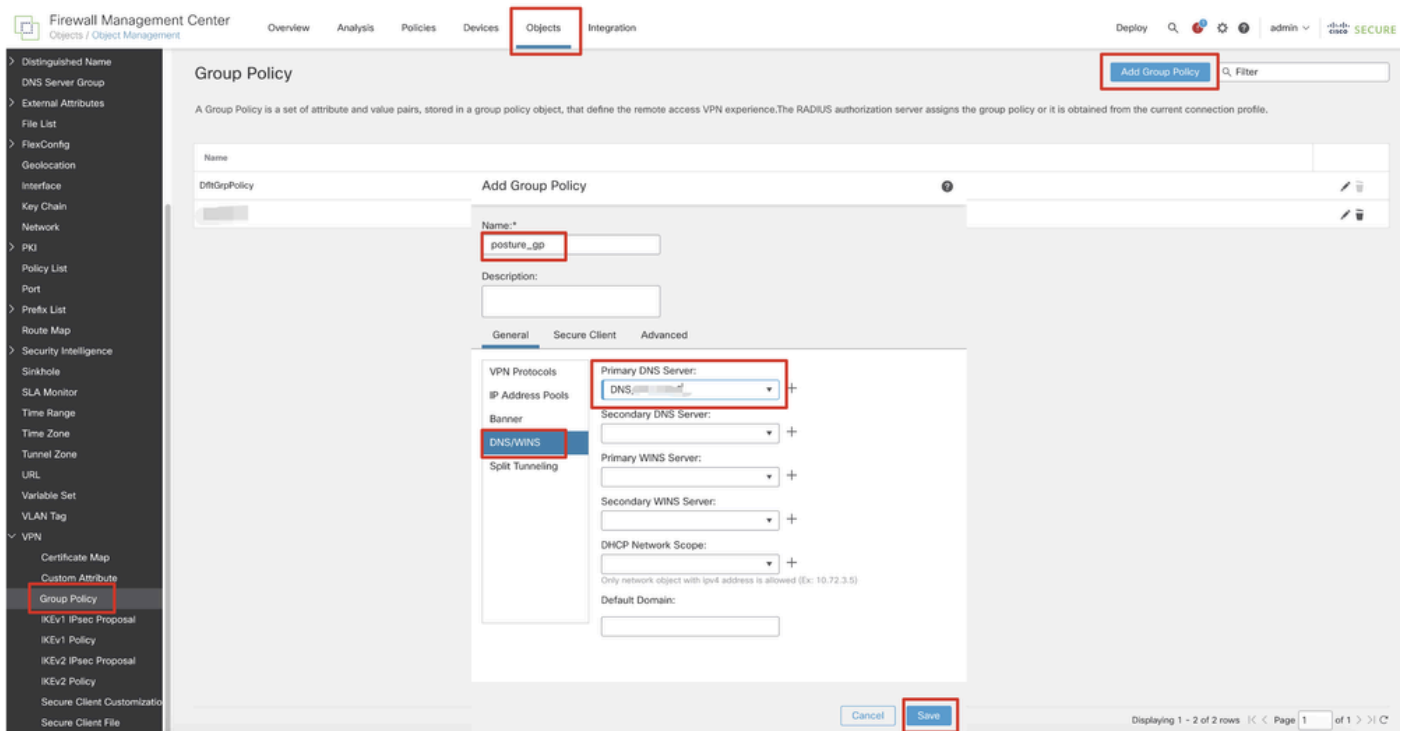
VPN يمدخ تسمل انه هنيوكت مت يذلا DNS م داخ م ادخ تس | بجي :نظحالم

Save.رقنا .حاتملا IP ISE PSN نا ونعو مسالا ريفوت ب مق ، Add Object رقنا ISE PSN ل نئاك عاشن | 4.2 ةوطخل



FMC_Add_Object_ISE

مداخ نئىك ددح، DNS/WINS رقنا Add Group Policy رقنا. Objects > Object Management > VPN > Group Policy. 5 ةوطخلال DNS Primary DNS Server في رقنا مث. Save.



FMC_Add_GROUP_POLICY

و enroll.cisco.com. FQDN Client Provisioning Portal ISE لحن كم VPN ةومجمن هون يف مدختسم ال DNS م داخ نأ نم دكأت: ؤظحالم

للقنا 6 ةوطخلل Add Extended Access List. رقنا. Objects > Object Management > Access List > Extended. للى لقتنا.

Fire Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy Filter

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

Extended

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
------	-------	----------

Add Extended Access List

FMC_Add_Redirect_ACL

يف دوجومال هسفن وه مسالا اذه نوكي نأ بجي. اههيجوت داعمال (ACL) لوصولا يف مكحتلال عمئاق مساري فوت. 6.1 ةوطخلال
لم. Add. رقنا. ISE ليوتخت فيرت فل

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_Part_1

هيجوتلال ةداع| نم مهءاعبتسال ةجالعالم مداوخو ISE PSN IP ناوع لىل رورمال ةكرحو DNS رورم ةكرح رطحب مق. 6.2 ةوطخلال
لم. Save. رقنا. هيجوتلال ةداع| لىل اذه يدؤي. رورمال ةكرح ةيقيب حامسال

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)

any

Destination Networks (1)

ISE_PSN_

Enter an IP address Add

Enter an IP address Add

Cancel Add

FMC_Add_Redirect_ACL_Part_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

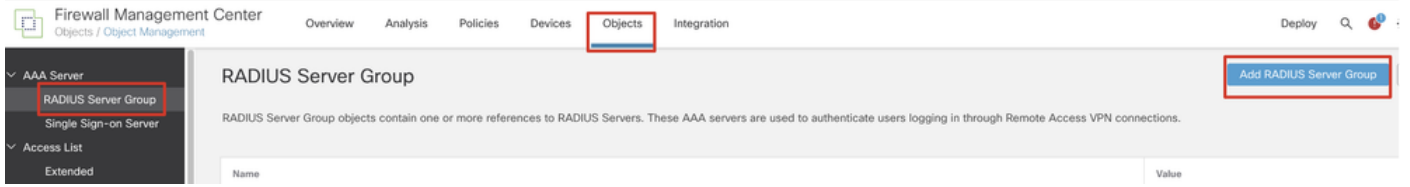
Save

FMC_Add_Redirect_ACL_Part_3

مداخل لثمك اذه ههيجوت داعملا (ACL) لوصولوا يف مكحتلا ةمئاق لاثم يف ةهوجلل FTP مادختسا متي: ةظحالم

حاصل الـ

7.1. Add RADIUS Server Group. ر ق ن ا . Objects > Object Management > RADIUS Server Group. ل ل ل ق ن ا . ة و ط خ ل ا



FMC_ADD_NEW_RADIUS_SERVER_GROUP

7.1. ة و ط خ ل ا . Enable dynamic authorization. ق ق ح ت ل ا . Enable interim account update. ق ق ح ت ل ا . Enable authorize only. ق ق ح ت ل ا ، م س ا ل ا ر ي ف و ت .

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_GROUP_PART_1

7.2. ةوطخلال Plus ICTO قوف رقنا. specific ددح ISE PSN IP Address/Hostname, Key. ريفوتب مق. ديدج RADIUS مداخ ةفاضل Redirec ACL. ددح. لاصلال interface مداوخ ةومجم ظفحل ىرخ ةرم Save رقنا م. ديدجل RADIUS مداخ ظفحل Save رقنا م. ةديدل RADIUS.

Add RADIUS Server Group

Enable authorize only
 Enable interim account update
 Interval:* (1-120) hours

 Enable dynamic authorization
 Port:* (1024-65535)

 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)

 Key:*

 Confirm Key:*

 Accounting Port: (1-65535)

 Timeout: (1-300) Seconds

 Connect using:
 Routing Specific Interface

 Redirect ACL:

FMC_ADD_NEW_RADIUS_SERVER_GROUP_PART_2

إلى لقتنا 8. ةوطخال Objects > Object Management > Address Pools > IPv4 Pools. Add IPv4 Pools Name, IPv4 Address Range ري فوتل Mask. وقنا مث Save.

Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Filter 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*

Description

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

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

إلى لقتنا 9. ةوطخال Certificate Objects > Object Management > PKI > Cert Enrollment. Add Cert Enrollment، م سا ري فوتل مق، Common Name Country Code بي وبتل ال ةمالع Certificate Parameters قوف رقتنا. Self Signed Certificate Enrollment Type ري فوتل ددو Save.

FMC_Add_NEW_CERT_LOGIN

هنيوكت مت يذلا قباسلا ليجستلا دحو، Device تحت FTD مس ا دح، Add رونا Devices > Certificates. لى لقتنا 10. ةوطخلا Cert Enrollment. رونا.Add

FMC_ADD_NEW_CERT_TO_FTD

Add رونا Devices > VPN > Remote Access. لى لقتنا 11. ةوطخلا

Next رونا Selected Devices لى لقتنا FTD ةفاض او مسالا ريفوتب مق 11.1. ةوطخلا

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_Wizard_1

11.2. ةوطخل Authentication Server, Authorization Server, Accounting Server ف اقبس م انه نوك م ت ال RADIUS مداوخ ةومج م دح. ةوفصل لفسأ ل ق لزنأ.

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: rtplse

Authorization Server: rtplse

Accounting Server: rtplse

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_Wizard_2

11.3. ةوطخل IPv4 Address Pools ف اقبس م انه نوك م ت ال ةومج م جهن دح. ةوفصل لفسأ ل ق لزنأ Group Policy.

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

Next. رونا. سكونيل ةروصل رايخالال ةناخ ددح 11.4 ةوطخال

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_Wizard_4

Next. رونا 9 ةوطخال في FTD في هليجست مت يذلا ةداهشال ليجست ددح VPN ةكبش ةهجاو ةهجاو ددح 11.5 ةوطخال

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

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: * **outside_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: * **demo_vpn**

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_Wizard_5

إذا Finish رِقنا ف، اديج عيش لك ناك اذا. صخلملما ةحفص يف ةلصلما تاذا تامولعملما يلع جودزملما ديكتألاب مق 11.6 ةوطخلما
Back رِقنا، ليدعتلما لىل جاتحي عيش ياً كانه ناك

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

Name:	posture_vpn
Device Targets:	Posture-FTD-CM127
Connection Profile:	posture_vpn
Connection Alias:	posture_vpn
AAA:	
Authentication Method:	AAA Only
Authentication Server:	radius (RADIUS)
Authorization Server:	radius
Accounting Server:	radius
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

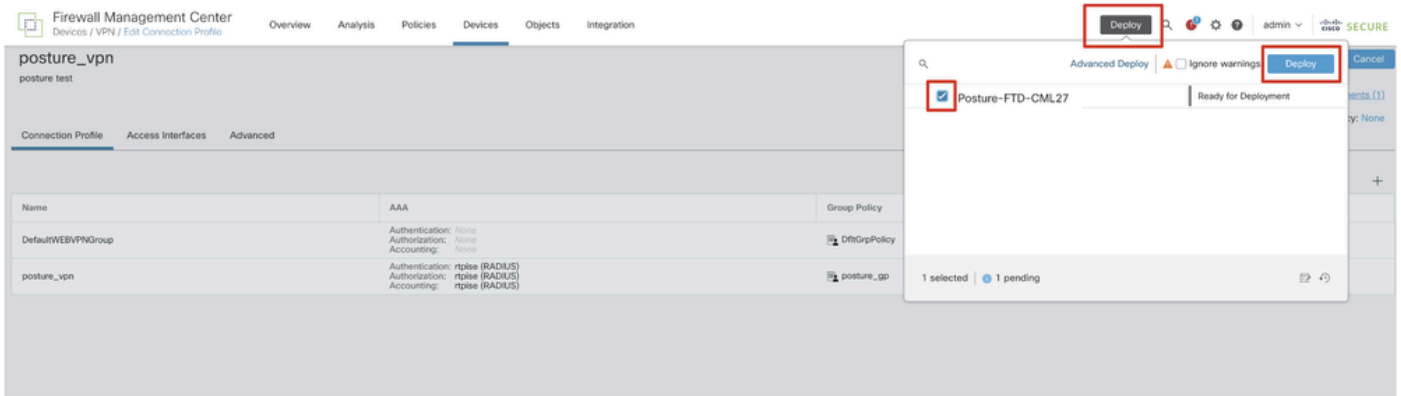
Additional Configuration Requirements
After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- 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_Wizard_6

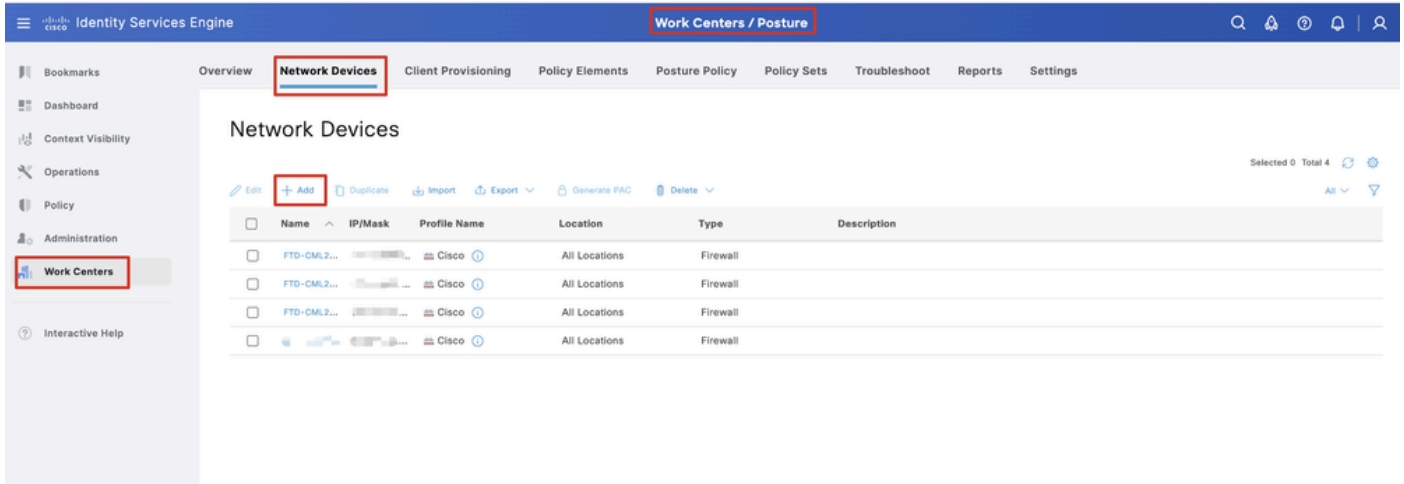
دعب نع لوصولل VPN نيوكت لامكإل FTD لىل ديدجلما نيوكتلا رشنب مق 12 ةوطخلما.



FMC_DEPLOY_FTD

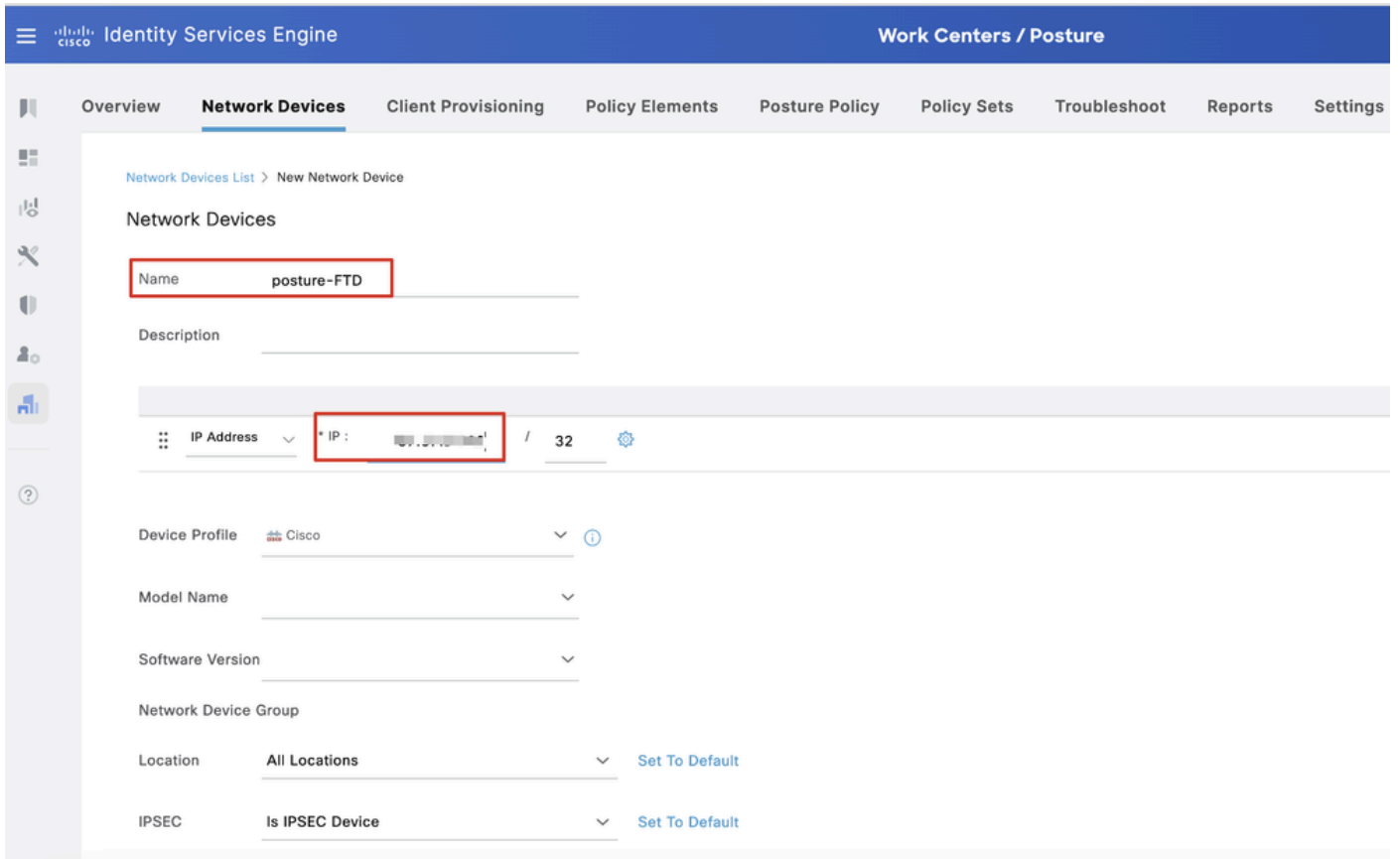
ISE على تاني وكالت

Add رقنا. Work Centers > Posture > Network Devices. لى لقتنا 13. ةوطخال



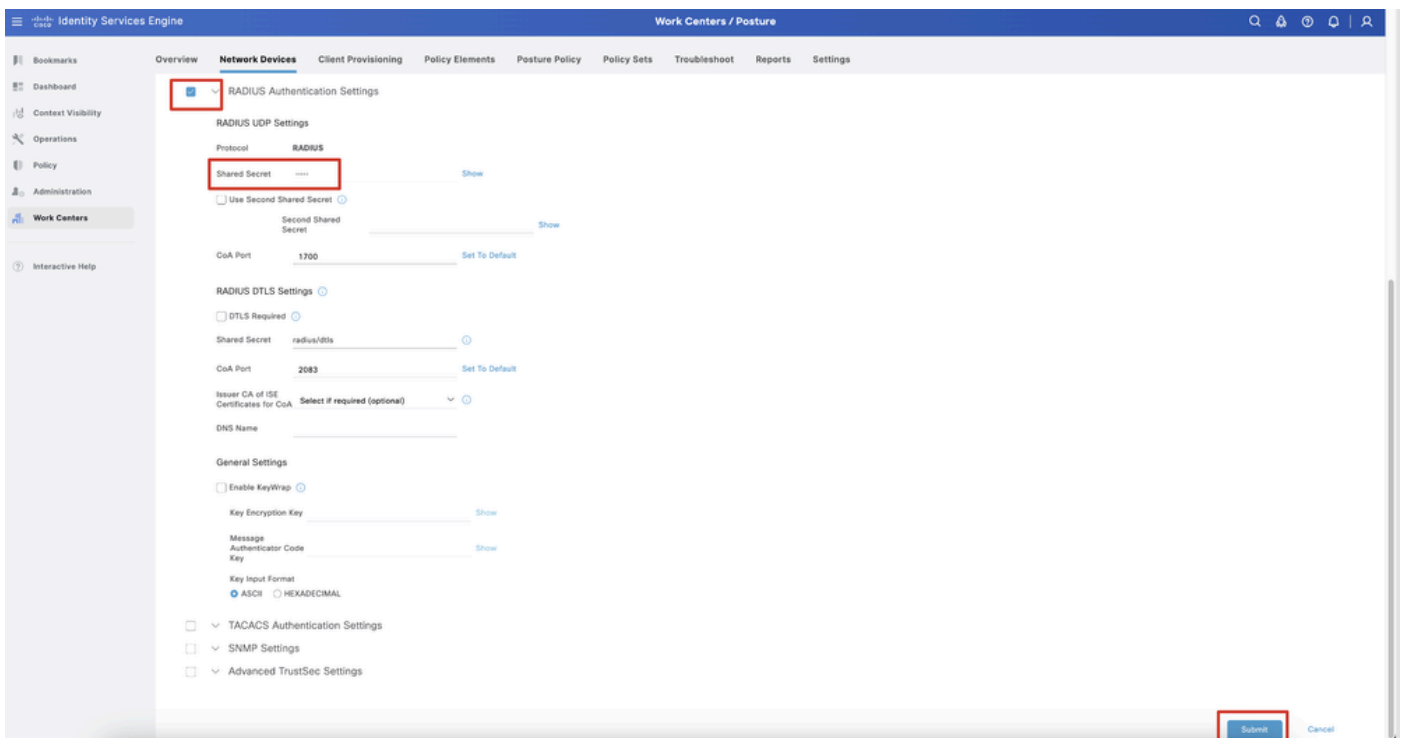
ISE_ADD_NEW_DEVICES

ةحفص الالف سأل لقتنا و IP Address، Name ريفوت ب مق 13.1. ةوطخال



ISE_ADD_NEW_DEVICES_1

Submit. رقنا Shared Secret ري فوت. RADIUS Authentication Settings ل راي تخال ا ءنا ددح 13.2 ءوطلال



ISE_ADD_NEW_DEVICES_2

Cisco [جمارب ليزنت](#) نم cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg ءمزلال مسا ليزنتب مق 14 ءوطلال جمارب ليزنت ءحفصل هسفن وه هليزنت مت يذلا فللمل MD5 يراب تخال ءومجملا ديكأ لال ءنم دي ءم فللمل نأ نم دكأ ءو

1. ةوطخلال ي ف حاجن ة مزحلل Cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg ل لزنن م Cisco.

15. ةوطخلال Work Centers > Posture > Client Provisioning > Resources. رقنا. Add دي دحت Agent resources from local disk.

The screenshot shows the 'Resources' page in the ISE Client Provisioning section. The 'Add' button is highlighted, and the dropdown menu is open, showing 'Agent resources from local disk' as the selected option. The table below lists various 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
CiscoSecureClientDesktoLinux 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

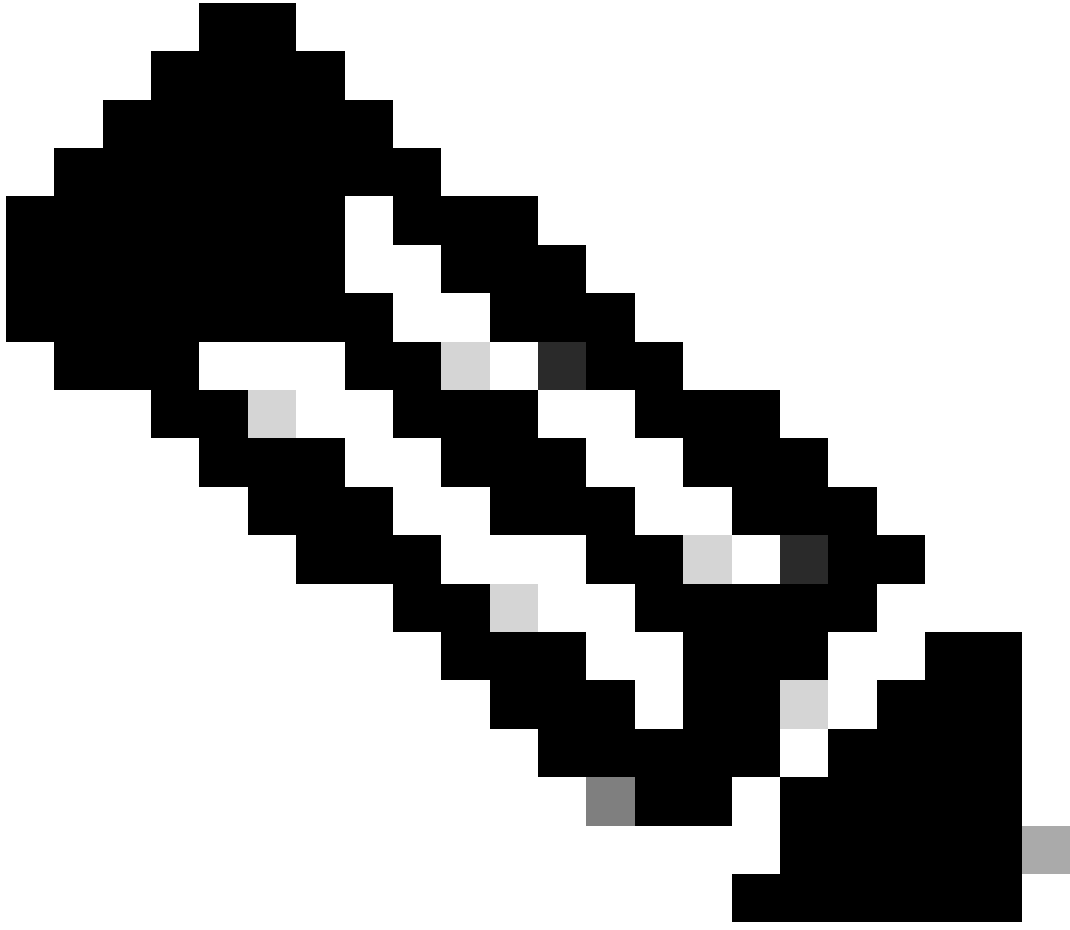
ISE_Upload_Resource

15.1. ةوطخلال Cisco Provided Package. رقنا Choose File ل ل مزحلل Cisco-secure-client-Linux64-5.1.3.62-webdeploy-k9.pkg. رقنا. Submit.

The screenshot shows the 'Agent Resources From Local Disk' page in the ISE Client Provisioning section. The 'Category' dropdown is set to 'Cisco Provided Package', and the 'Choose File' button is highlighted. The 'Submit' button is also highlighted. The table below shows the 'Agent Uploaded Resources'.

Name	Type	Version	Description
CiscoSecureClientDesktoL...	CiscoSecureClientDe...	5.1.3.62	Cisco Secure Client for ll...

ISE_Upload_RESOURCES_1



. cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg لى محتى ل 14 ة و ط خ ل ا ر ر ك : ة ظ ح ا ل م

Agent Posture Profile. Add ر ق ن ا . Work Centers > Posture > Client Provisioning > Resources. لى ل ل ق ت ن ا 16 ة و ط خ ل ا

Identity Services Engine Work Centers / Posture

Client Provisioning Policy Resources Client Provisioning Portal

Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

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	Cisco Secure Client for li...
<input type="checkbox"/> Native Supplicant Profile	ve Supplicant Pro...	Not Applic... 2016/10/07 04:01:12	Pre-configured Native S...
<input type="checkbox"/> Agent Configuration	oSecureClientCo...	4.3.3139.0 2024/05/08 10:34:00	Cisco Secure Client Linu...
<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_POSTURE_PROFILE

Save. رقتنا. يضا رتفاك هب ظافتحال او يقابل ال Name, Server name rules ريفوت 16.1 ةوطخال

مساال: linux_agent_profile

مدخال مسا دعواق: *.example.com

Identity Services Engine Work Centers / Posture

Client Provisioning Policy Resources Client Provisioning Portal

Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

ISE Posture Agent Profile Settings > New Profile

Agent Posture Profile

Name *
linux_agent_profile

Description:

Agent Behavior

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent

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

إضافة إعدادات العميل (Agent Configuration) رقمنا. Add Agent Configuration. Work Centers > Posture > Client Provisioning > Resources. 17.2. ةوطخال

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			
<input type="checkbox"/> Native Supplicant Profile			
<input type="checkbox"/> Agent Configuration	oSecureClientCo...	2024/05/08 10:34:00	Cisco Secure Client Linu...
<input type="checkbox"/> Agent Posture Profile	ntProfile	2024/05/08 10:37:17	
<input type="checkbox"/> AMP Enabler Profile	ntProfile	2024/05/16 15:15:49	

ISE_Add_AGENT_CONFIGURATION

إضافة ملف إعدادات العميل (Agent Configuration): 17.2. ةوطخال

إسم الملف: CiscoSecureClientDesktopLinux 5.1.3.062

إسم الملف: linux_agent_config

إسم الملف: Cisco SecureClientComplianceModuleLinux 4.3.3139.0

إسم الملف: VPN, Diagnostic and Reporting Tool

إسم الملف: Linux_agent_profile

رقننا.Submit

Identity Services Engine Work Centers / Posture

Client Provisioning

* 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_CONFIGURATION_1

ةدعاق مسأ يا ةي اهان يف Edit رقنا. Work Centers > Posture > Client Provisioning > Client Provisioning Policy. 18 ةوطخلا Insert new policy below. دي دحت

Identity Services Engine Work Centers / Posture

Client Provisioning Policy

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

لي صافات ال نيوك ت 18.1 ة و ط خ ل ا

دعا ق ل ا م س ا : Linux

ا ل س ك و ن ي ل : ل ي غ ش ت ل ا ة م ط ن ا

جئ ا ت ل ل ا : linux_agent_config

ق ط ق Done Save.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Client Provisioning Policy. The 'Client Provisioning Policy' is selected, and 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_Add_NEW_PROVISIONING_POLICY_1

ا د د ر ق ن ا . Add ر ق ن ا . File > Conditions > Policy Elements > Posture > Work Centers > ل ل ل ق ت ن ا 19 ة و ط خ ل ا

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Policy Elements. The 'Policy Elements' tab is selected, and the 'File' condition is highlighted with a red box. The 'File Conditions' table is visible, showing various predefined checks.

Name	Description	File name	Condition Type
pc_XP64_KB2797052_MS13...	Cisco Predefined Check:...	SYSTEM_PROGRAMS\IC...	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_WB1_64_KB3033869_M...	Cisco Predefined Check:...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_Vista64_KB295902_MS0...	Cisco Predefined Check:...	SYSTEM_ROOT\winsxsl...	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\Scrun.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_WB1_64_KB3042553_M...	Cisco Predefined Check:...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_WB_64_KB2727528_MS...	Cisco Predefined Check:...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_W8_64_KB2992611_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

لي صافات ال نيوك ت 19.1 ة و ط خ ل ا

م س ا ل ا : Linux_demo_file_existing

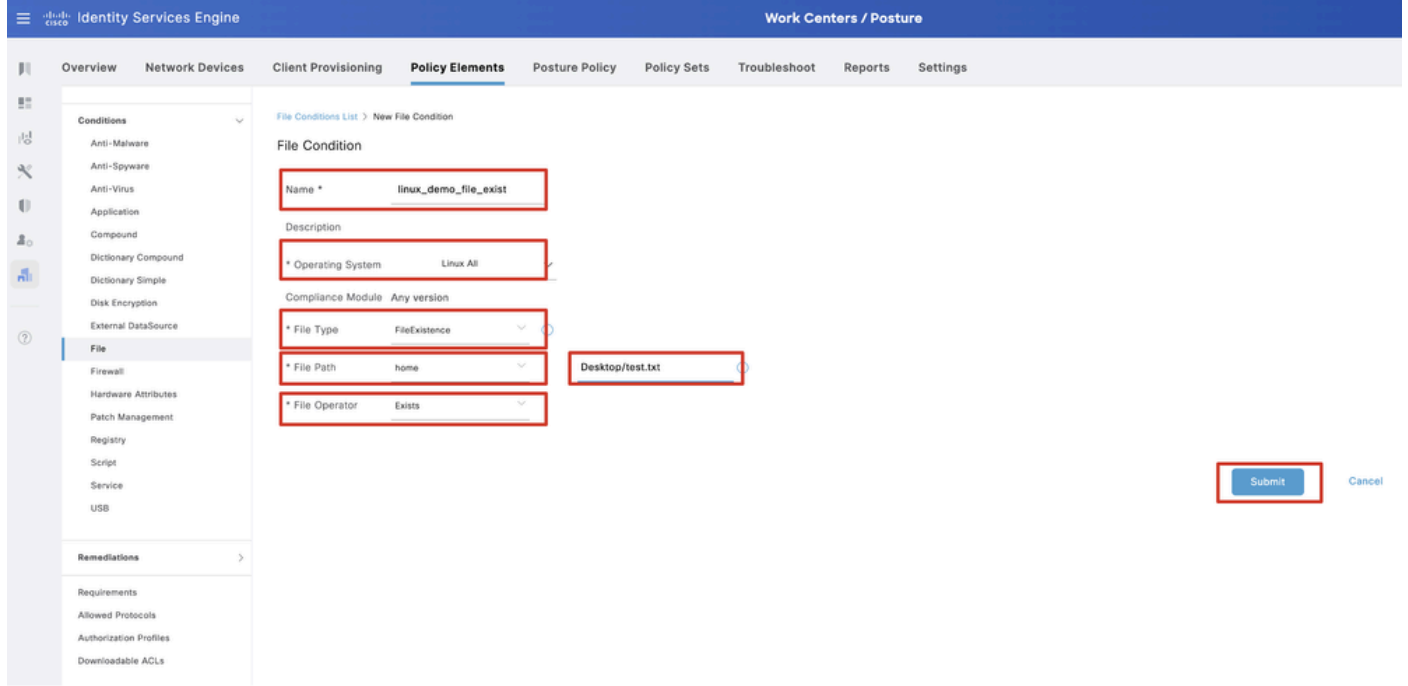
all سكوني ل: لي غشت الة مظنأ

FilePresence: فمل الة عون

Desktop/test.txt، ةسي ئر الة ح ف ص ال: فمل الة راسم

دوچوم: فمل الة لي غشت ل ماع

Submit. ر ق ن ا



ISE_ADD_NEW_FILE_CONDITION_1

Work Centers > Posture > Policy Elements > Requirements. Edit ر ق ن ا. ةدعاق م س ا ي ة ي ا ه ن ي ف ر ق ن ا. 20 ةوطخ الة Insert دي دحت. new Requirement.

Identity Services Engine Work Centers / Posture

Policy Elements

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_Add_NEW_POSTURE_REQUIREMENTS

لي صافات لني وك ت. 20.1 ة و ط خ ل ا

م س ا ل ا : test_exist_linux

ا ل ل س ك و ن ي ل : لي غ ش ت ل ا ة م ظ ن ا

ث د ح ا ر ا د ص ا و ا 4.x : ق ف ا و ت ل ا ة د و ح

ل ي ك و ل ا : ع ض و ل ا ع و ن

ط و ر ش ل ا د ج و ت : linux_demo_file_existing

Done Save ة ق ط ق ط

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_Add_NEW_POSTURE_REQUIREMENTS_1

جالعك سكونيل عالمعل ةريصق ةيصن جمارب يوس معد متي ال ،نآل ىتح :ةظحالم

Add رقنا . Work Centers > Posture > Policy Elements > Authorization Profiles | ل لقتنا 21 ةوطخال

:ل صافات ل نيوك ت 21.1 ةوطخال

م سالا : unknown_redirect

دح Web Redirection(CWA,MDM,NSP,CPP) ل رايخال ةناخ دح

ديحت Client Provisioning(Posture)

هيجوتل ةداع | (ACL) لوصول ي ف مكحتل ةمئاق

(يضا رت فالال) ليم عل ريفوت لخدم: ةم يق ل

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Work Centers / Posture'. The main navigation tabs are 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The left sidebar lists various configuration 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. The 'ACL' dropdown is set to 'redirect', and the 'Value' dropdown is set to 'Client Provisioning Portal (def)'. Other options like 'Voice Domain Permission', 'Static IP/Host name/FQDN', and 'Suppress Profiler CoA for endpoints in Logical Profile' are unchecked.

ISE_ADD_NEW_AUTHORIZATION_PROFILE_REDIRECT_1

لوصول في مكحلتا عمئاق مسا عم هذه (ACL) لوصول في مكحلتا عمئاق مسا هي جوت ءءاع قباطت نأ بجي: ءظءالم
FTD. لعل هن يوك مت يءلا ءقباطملا (ACL).

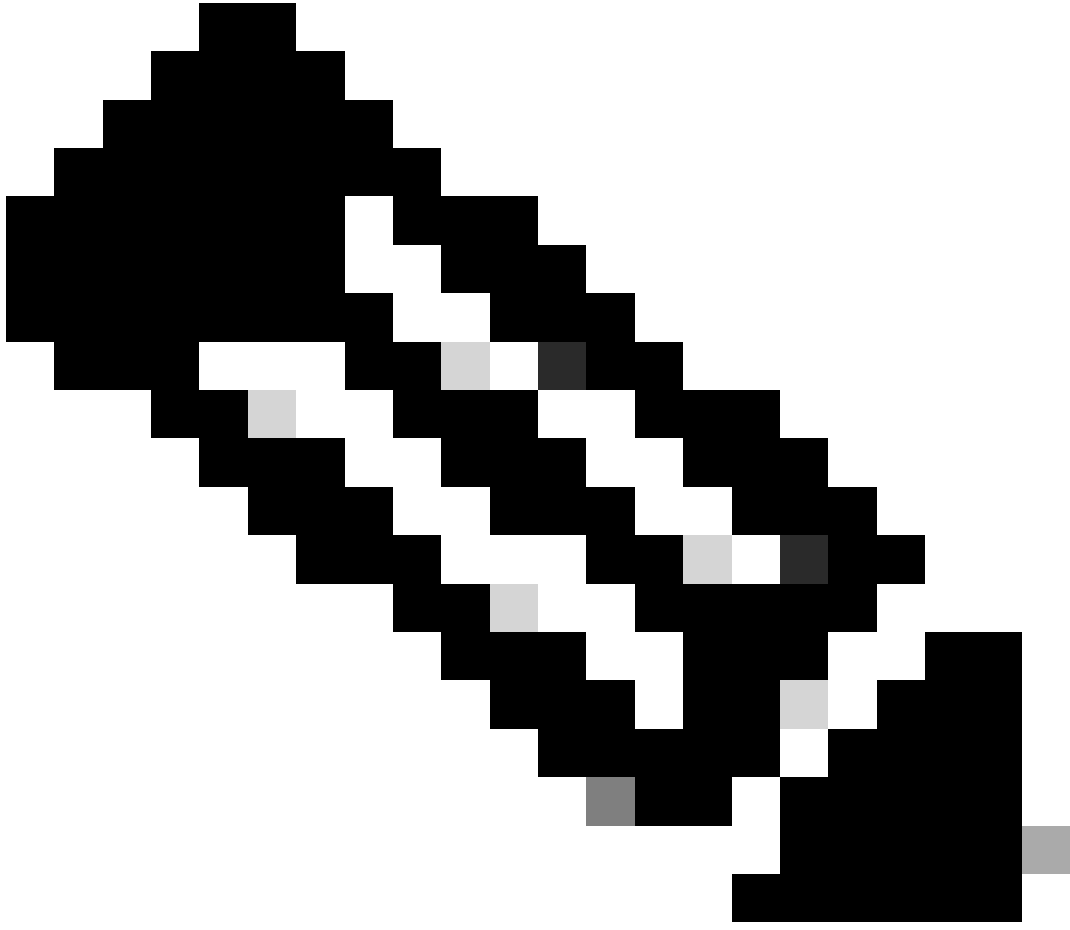
ل.لصافلا عم ءقفاوتملا و ءقفاوتملا ريغ ءياهنلا طاقنل ن يءرءا ءامءعا ي فيصوت ءاشن | Add ررك 21.2 ءوطءلا

مسا: non_compliant_profile

مسا DAACL: DENY_ALL_IPv4_TRAFFIC

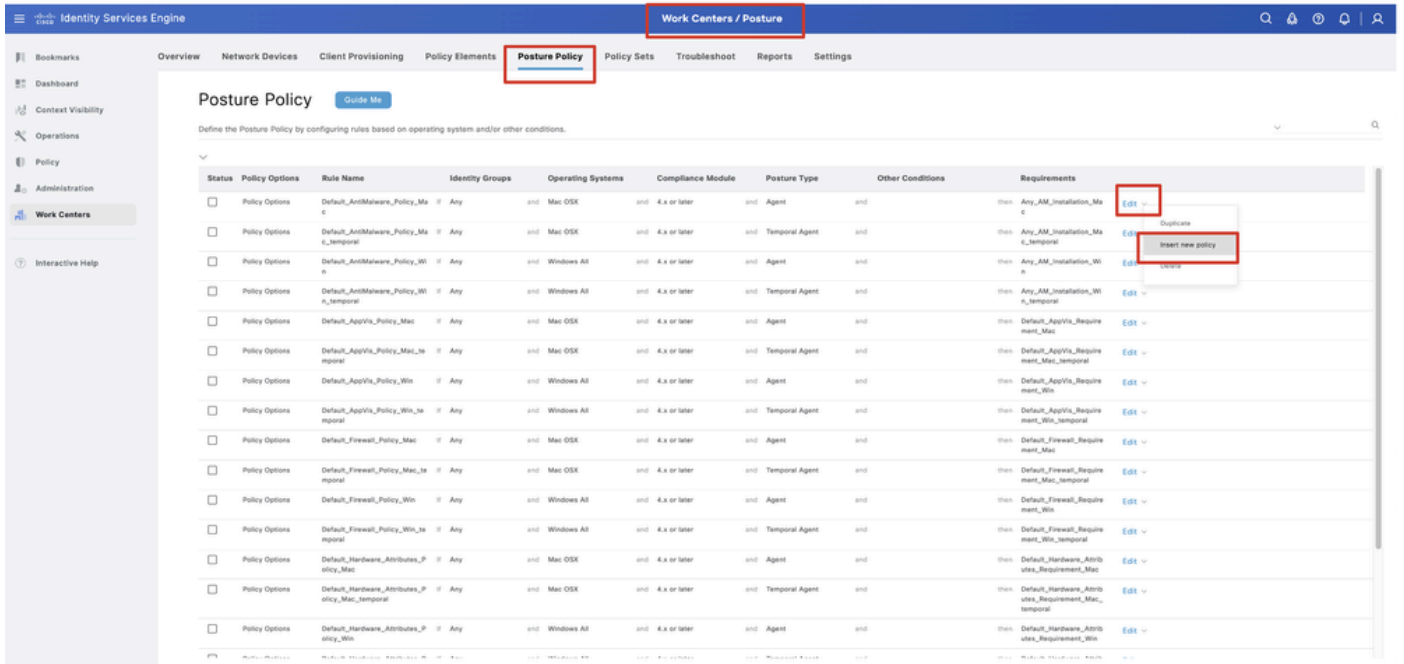
مسا: compliant_profile

مسا: allow_all_ipv4_traffic ءساسة نبللا لوصول في مكحلتا عمئاق مسا



ريغ وأقفاوتملا ةياهنلا طاقنل (DACL) ةيساسألا ةينبلل لوصولا يف مكحتلا ةمئاق نيوكت مزلي: ةظحالم
ةيلعفلابلطتملل اقفو ةقفاوتملا.

Insert new policy. ددح. دعاوق يأةهان يف Edit رقنا. Work Centers > Posture > Posture Policy. لىلقنا. 22 ةوطخل



ISE_Add_NEW_POSTURE_POLICY

لي صاف التا نيوكت 22.1 ة و ط خ ل :

ة د ع ا ق ل م س ا : demo_test_exist_linux

ي أ : ة ي و ه ل ا ت ا ع و م ج م

ا l l ة س ك و ن ي ل : ل ي غ ش ت ل ا ة م ظ ن أ

ت ح أ ر ا د ص ا و ا 4.x : ق ف ا و ت ل ا ة د ح و

ل ي ك و ل ا : ع ض و ل ا ع و ن

ا ت ا ب ل ط ت م ل : test_exist_linux

ط ق ط ق Done 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_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_Add_NEW_POSTURE_POLICY_1

إلى Insert new row above. Work Centers > Posture > Policy Sets. إلى لقتنا 23. ةوطخال

Identity Services Engine Work Centers / Posture

Work Centers / Posture

Policy Sets

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

[Insert new row above](#)

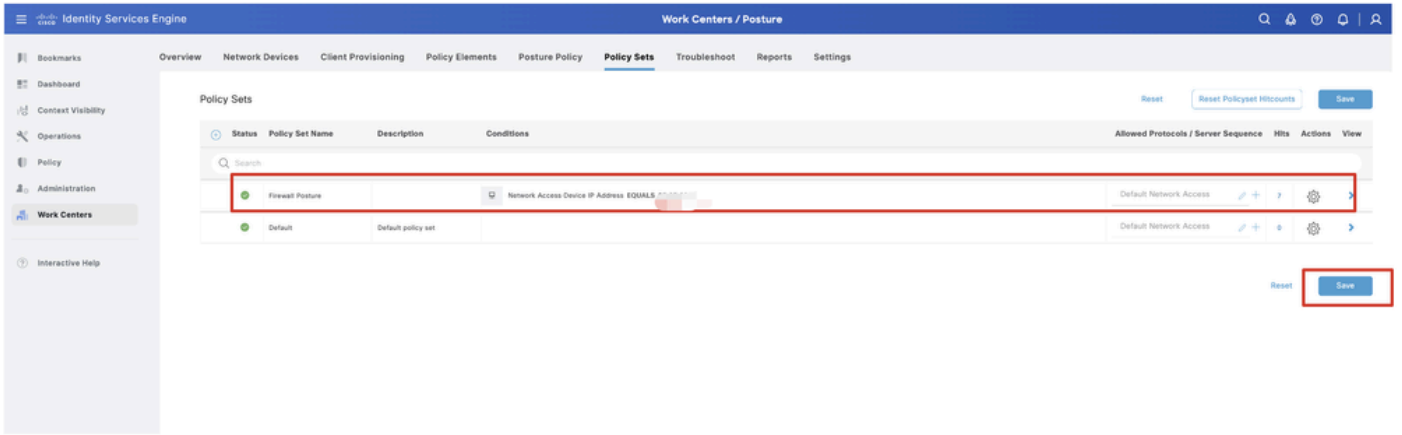
ISE_Add_NEW_POLICY_SET

إلى صافات ال نيوك ت. 23.1. ةوطخال

ةيامحل رادج عضو: جهن ال ةومجم مس

إلى لوصول زاهج ةصال ال IP نيوانع: طورشل ال [IP ل فTD ةكبش ال

رقنا. Save



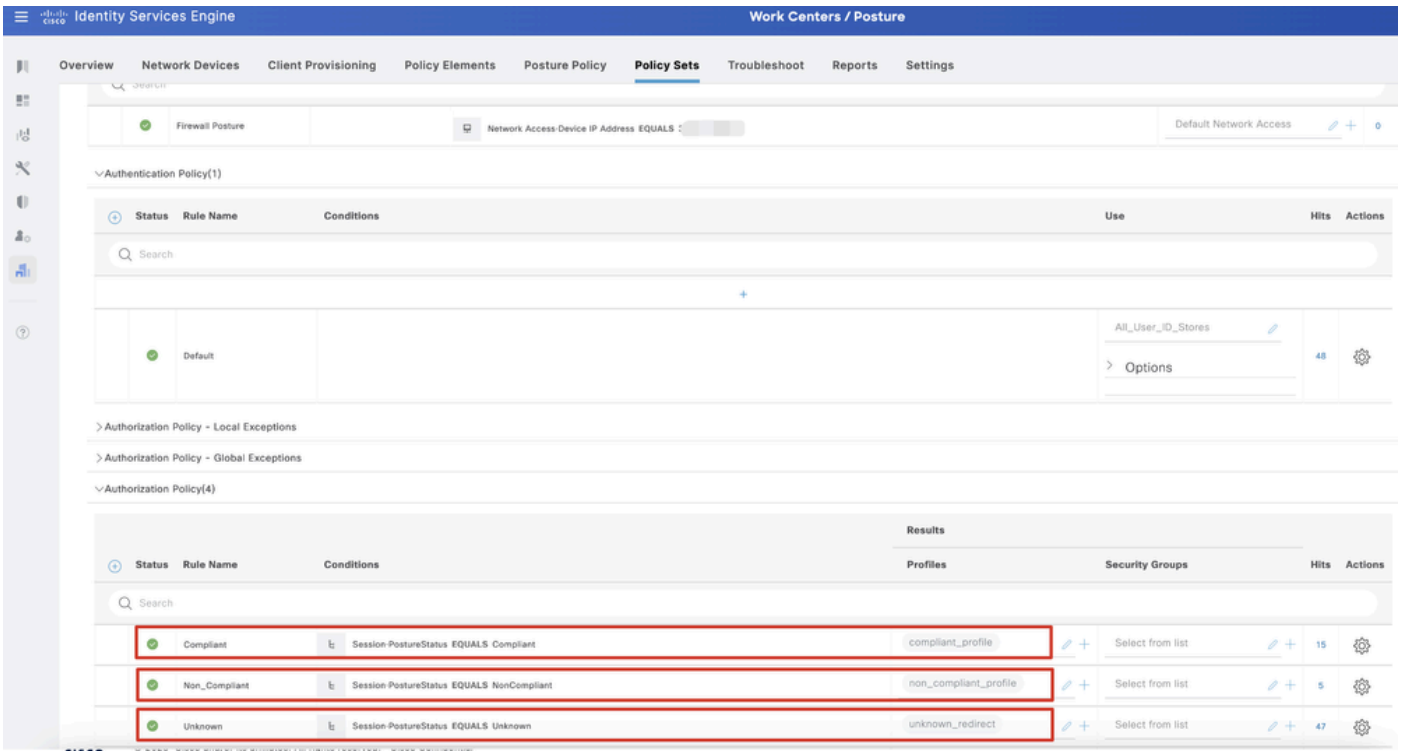
ISE_Add_NEW_POLICY_SET_1

ةقفاوتم ريغو وعضولا عم ةقفاوتم ريغ ةلاجل ةديج ليوخت دعاوق ءاشنا ب مق .جهنلا ةومجم لاخ دال > رقنا 23.2 ةوطخلال .Save رقنا

عم قفاوتم profile

عم قفاوتم ريغ non_compliant_profile

عم ريغ UNKNOWN_REDIRECT مادختساب فورعم ريغ



ISE_Add_NEW_POLICY_SET_2

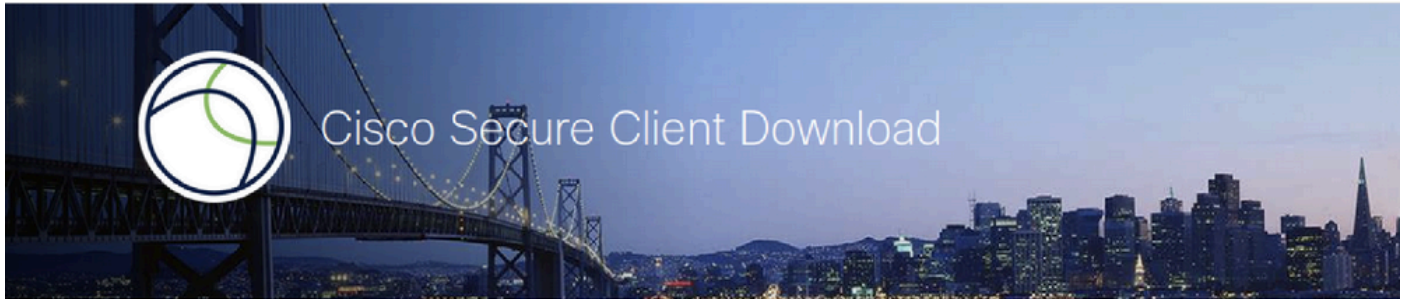
Ubuntu في تانيوكتال

ةباوب لى لا لوخدلا ليحستل ضرعتسمال حتفا .ةيموسرلا مدختسمال ةهجاو ربع Ubuntu ليم عم لى لا لوخدلا ليحست 24. ةوطخلال demo.example.com نوكتس ،لا ثمال اذه في .(VPN) ةيرهظلال ةصاخلال ةكبشلال

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

Ubuntu_browser_VPN_LOGIN

Download for Linux. رقمنا 25. ةوطخلال



Download & Install

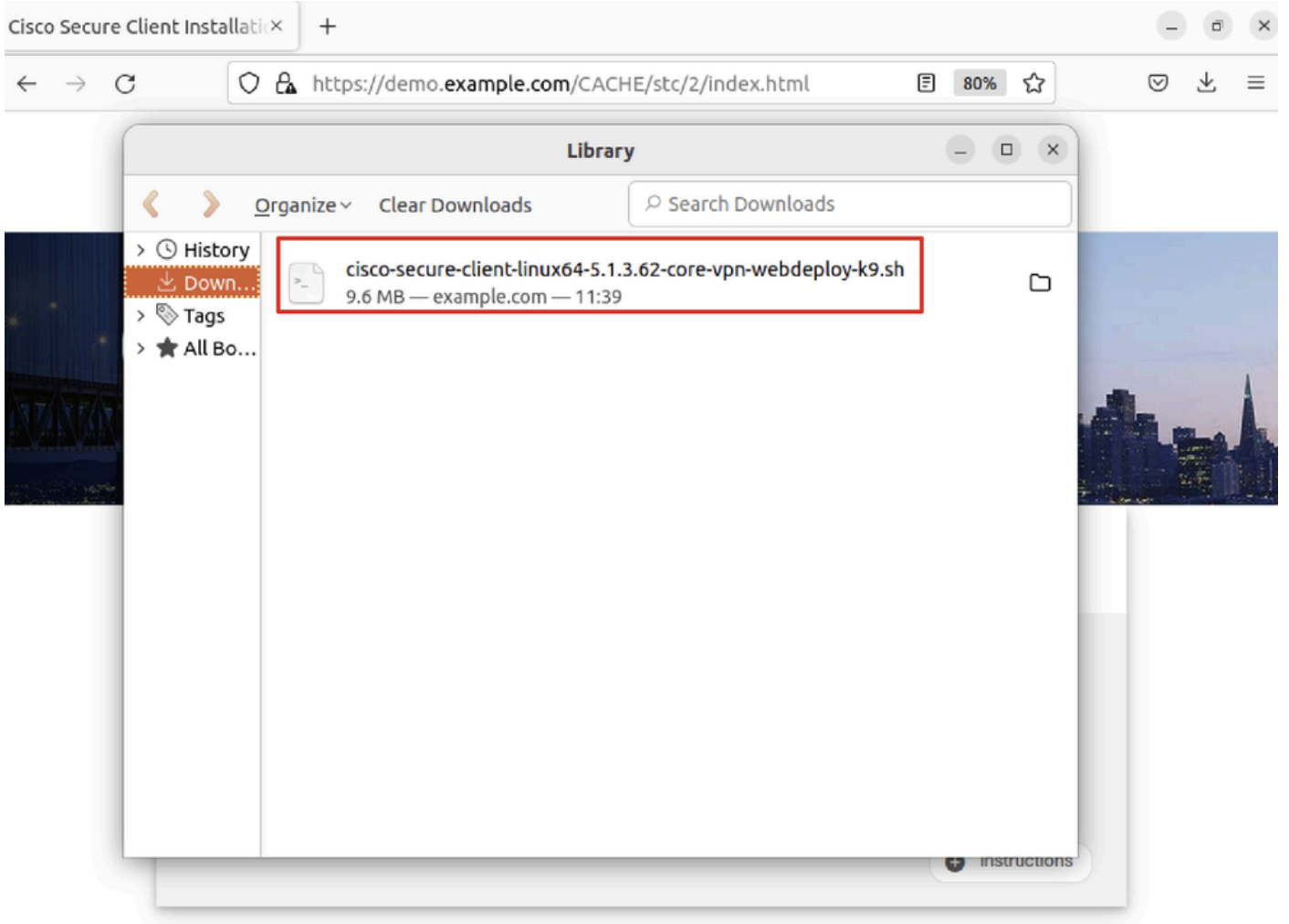
Download Cisco Secure Client and install it on your computer.

[Download for Linux](#)

[+ Instructions](#)

Ubuntu_browser_VPN_DOWNLOAD_1

وہ ہلےزنت مت یدلا فلملا مس ا cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_browser_VPN_DOWNLOAD_2

مادخت سال لاثم اذه <certificate>.crt حبصيل فللم لة يمست دعأو ضرعت سمل لال لال خ نم VPN ةداهش ليزنت ب مق. 26 ةوطخال ل ةداهش لال ليزنت ل س ك و ف ر ي ا ف .


```
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$
```

Ubuntu لڤي مع ىل ع VPN لخدم ةداهش يف ةقثلا. 28 ةوطخل

```
<#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...
```

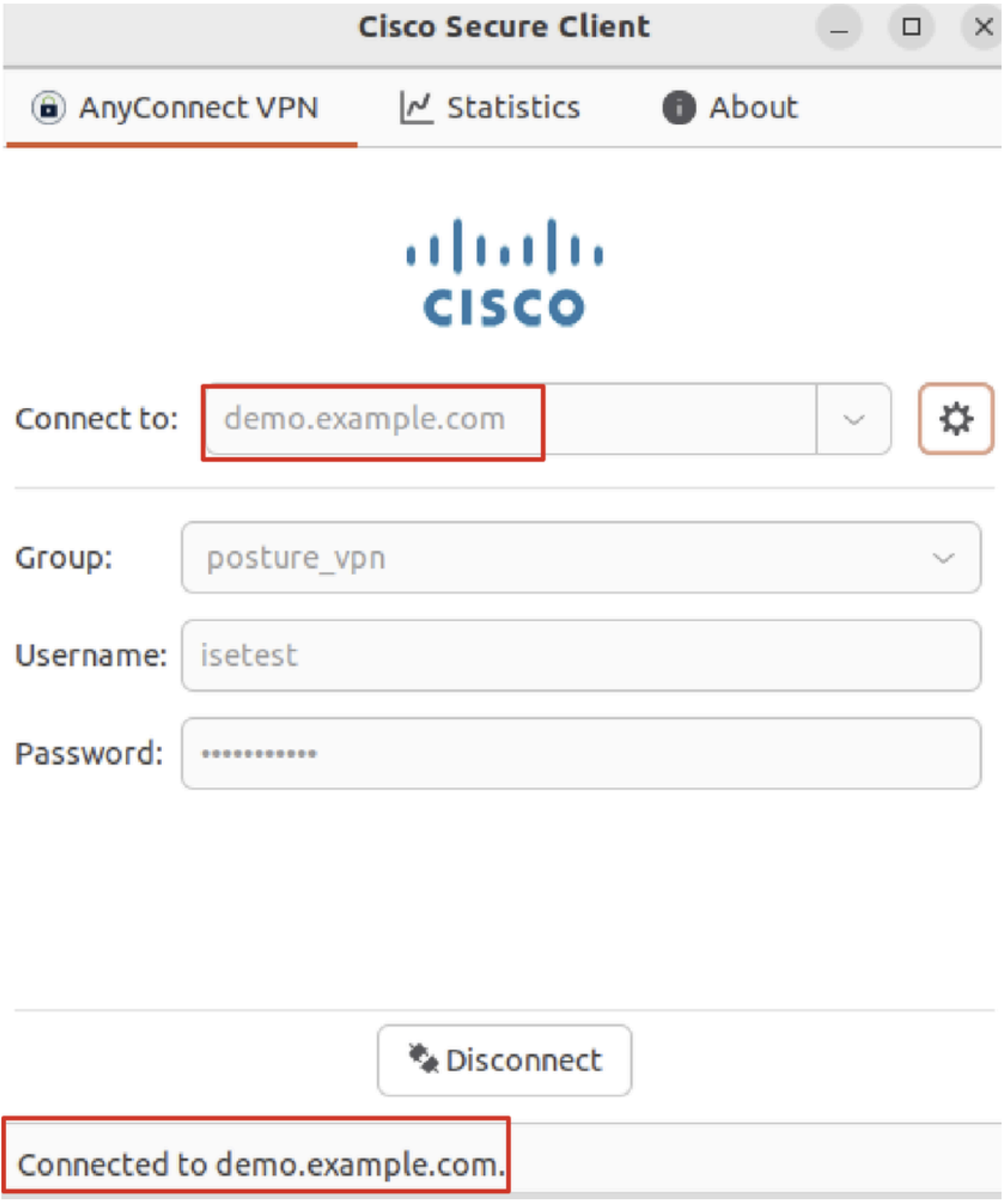
```
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

```
1 added
```

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

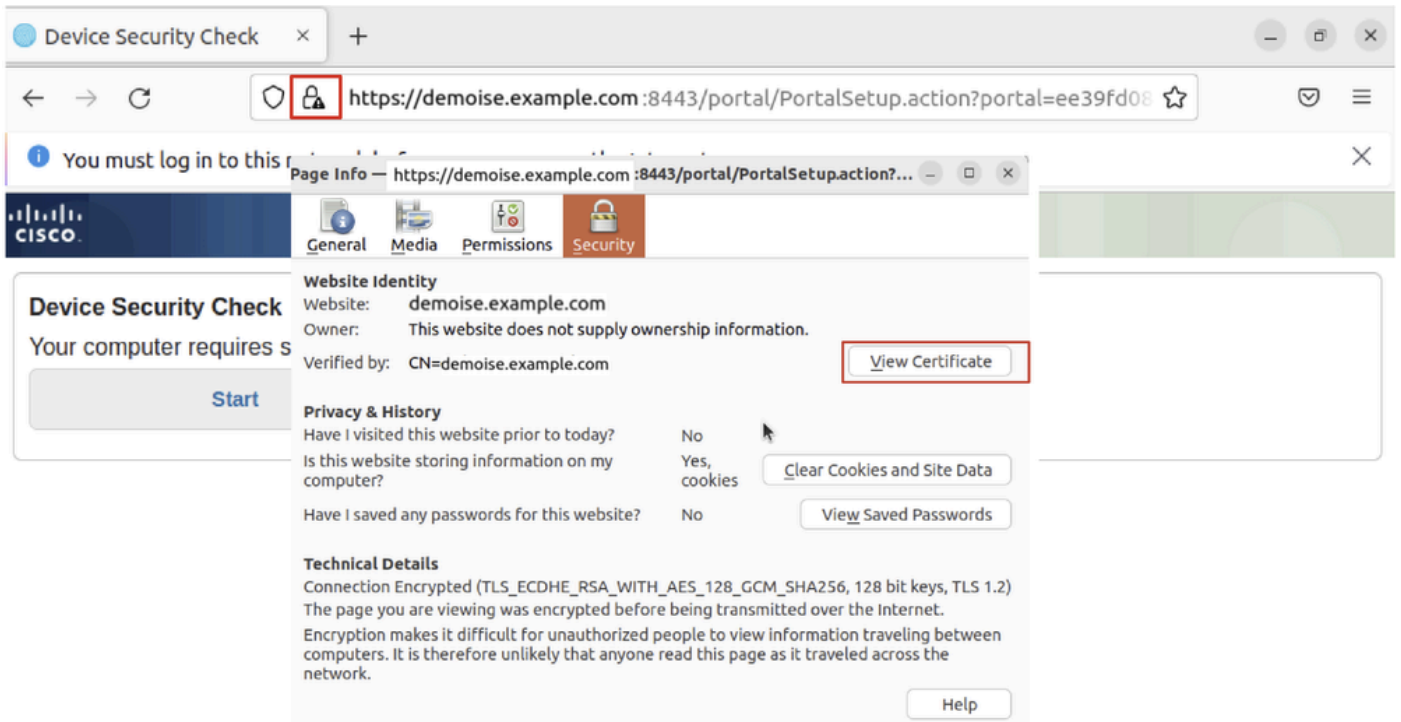
```
Running hooks in /etc/ca-certificates/update.d...
```

```
done.
```

Ubuntu_Secure_Client_Connected

مكتحة التاىوتسم ةباوب الى هيچوتال ةداع| ليغشتب موقبي بيوعقوم ي الى لوصولل ضرعتسمالحتفا 30 ةوطخال
Firefox مادختسالىل لاثم اذه <certificate>.crt الى فلمال ةيمست دعأو ISE CPP ةباوب نم ةداهشلاليزنتب مق ISE ل (CPP)
لليزنتلل.



Ubuntu_browser_CPP_CERT_DOWNLOAD

Ubuntu لى جمع لى ISE ب ةصاخال (CPP) م كحتال لى وتسم ةيامح ةبواب ةداهش لى ةقثال 30.1 ةوطخال

<#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.
```

Ubuntu لى جمع لى ISE CPP ةبواب لى Start رقنا 31 ةوطخال


```
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_0NcLgcMURfyZmR6Ho
```

```
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_0NcLgcMURfyZmR6Ho
```

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.

هي طمّن ال ISE Posture ودحو تي بثت مت. هحتف دعأو Cisco Secure Client ءاناب مق Ubuntu، لي مع مدختسم ةهجاو يف 34. ةوطخال
حاجنّب اهلي غشتو.



Ubuntu_Secure_Client_ISE_Posture_Install

يتم إعداد ملف test.txt مع اسم المستخدم home/user/Desktop ، راسم الما إلى لقتنا. Ubuntu لي مع على عة ف رطال ة دح وال حت فا. 35 ة و ط خ ل ا ح ل ا ح ISE. على ا ه ا ن ي و ك ت م ت ي ت ا ل ف ل م ل ة ل ا ح

<#root>

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

```
cd Desktop/
```

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

echo test > test.txt

ةحصلا نم ققحتلا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذم دختسا

Ubuntu لمع ىلع demo.example.com ب VPN ةكبش لىصوتب مق 1. ةوطخلا

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" option is highlighted with a red box. Below the menu is the Cisco logo. The "Connect to:" field contains "demo.example.com" and is highlighted with a red box. 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 shows "Connected to demo.example.com." highlighted with a red box.

Verify_Ubuntu_Secure_Client_Connected

Ubuntu لمع ىلع (ISE) ةيوهلا تامدخ كرحم ةيعضو ISE Posture ةلاح نم ققحت 2. ةوطخلا



Network access allowed.

verify_ubuntu_secure_client_compliant

Operations > RADIUS Live Log. ISE. Radius Live لوخد ليچست نم ققحت 3. ةوطخلال

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
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

مكتحلتا ةدحو وأ SSH لوكوتورب ربع FTD ب ةصاخ (CLI) رمأوأ رطس ةهجاو ىلا لقتنا 4. ةوطخلال

```
<#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

اهال ص او ااطخ ال فاشكت سا

اهال ص او نيوكت ال ااطخ فاشكت سا ال اهم ادخ تس ال كن كم ي تام ول عم مس ق ل اذه رفوي

اهال ص او ل [Pre and Post 2.2](#) CCO ل عضو [طعن فتراقم](#) نم ق قحت ، اهل ص او ISE و Cisco Secure Client ااطخ فاشكت سا و عضوا ق فدل
[اهال ص او اعضوو ISE قس ل ج قراا](#) ااطخ فاشكت سا و

قلص تاذا تام ول عم

- [3.3 رادص ال ، Cisco نم ق ي وول ا تام دخ كن جم قك بش نو كم ق فاوت](#)

- [3.3 رادص اليا Cisco نم ؤه ليا تامدخ كرحم لوؤس م لي ليد](#)
- [Cisco نم تال يزنتلا او ينفل م عدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا