# **Configure Linux VPN Posture with ISE 3.3**

# Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Network Diagram
Configurations on FMC/FTD
Configurations on ISE
Configurations on Ubuntu
Verify
Troubleshoot
Related Information

# Introduction

This document describes how to configure Linux VPN posture with Identity Services Engine (ISE) and Firepower Threat Defense (FTD).

# Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

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

### **Components Used**

The information in this document is based on these software versions:

- 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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configure

### **Network Diagram**



Topology

### **Configurations on FMC/FTD**

Step 1. Connectivity among the client, FTD, FMC, and ISE has been successfully configured. As enroll.cisco.com is used for endpoints doing probe for redirection (refer to posture flow CCO documents<u>ISE</u> <u>Posture Style Comparison for Pre and Post 2.2</u> for details). Ensure the route for traffic to enroll.cisco.com on FTD is configured correctly.

Step 2. Download the package name cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg from <u>Cisco Software</u> <u>Download</u> and ensure the file is good after download by confirming md5 checksum of the downloaded file is the same as the Cisco Software Download page.

Step 3. Navigate to Objects > Object Management > VPN > Secure Client File. Click Add Secure Client File, provide the name, browse File Name to select cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, select Secure Client Image in File Type drop-down list. Then click Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policie	as Devices Objects Integration		Deploy	९ 💕 🌣 🔕 admin ~	ence SECURE
Distinguished Name     DNS Server Group     External Attributes	Secure Client File			Add Secure	Client File Q. Filter	
File List	File objects represent files used for remote access v	VPN policy configurations. They can contain Secure Client profile and image files.				
> FlexConfig Geolocation		Add Secure Client File	0			
Interface	Name				Туре	
Key Chain	client_image	Name:*		n-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	1/1
Network	Default-External-Browser-package	linux 5 1 2 62		36-webdeploy-k9.zip	Secure Client External Browser Pa	± q ≣
Policy List	hostscan5_1_3_62	Linux_5_1_5_62		1-5.1.3.62-k9.pkg	HostScan Package	1/1
Port Prefix List	linux_image	File Name:*	_	ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	1/1
Route Map		cisco-secure-client-linux64-5.1.3.62-w Browse				
> Security Intelligence						
Sinkhole		File Type:*				
SLA Monitor		Secure Client Image				
Time Range		coolie chent intege				
Time Zone		Description:				
Tunnel Zone						
Uni Variable Set						
VLAN Tao						
✓ VPN						
Certificate Map						
Custom Attribute			0			
Group Policy		Cancel	Save			
IKEv1 IPsec Proposal						
IKEv1 Policy						
IKEv2 IPsec Proposal						
Secure Client Customizatio						
Secure Client File				Displ	aying 1 - 4 of 4 rows IC < Page 1	of 1 >> I C

FMC\_Upload\_Secure\_Client\_Image

 $Step \ 4. \ Navigate \ to \ \ Objects > Object \ Management > Network.$ 

Step 4.1. Create an object for the DNS server. Click Add Object, provide the name and available DNS IP address. Click Save.

Firewall Managemen	t Center Overview Analysis Policies	Devices Objects Integration		Deploy	Q 💕 🌣 😨 🛛 admin	* cisco SECURE
Distinguished Name     DNS Server Group     External Attributes     File List	Network A network object represents one or more IP addresses	. Network objects are used in various places, including access co	ntrol policies, network variables, intrusion rules,	Add Network identity rules, network discovery rule Import Add Gr	Q, Filter     C, Filter     Show Unused of     orts, and so on.	Dbjects
> FlexConfig Geolocation	Name			Value	Type Override	
Interface	any	New Network Object	0	0.0.0.0/0 ::/0	Group	¶a q ≣ #
Key Chain Network	any-ipv4			0.0.0.0/0	Network	$\eta_{0} \circ_{i} \equiv \mathfrak{K}$
		Discription  Network Host Range Network  Allow Overrides	FQDN			
			Cancel			

FMC\_Add\_Object\_DNS



Note: DNS server configured here is to be used for VPN users.

Step 4.2. Create an object for ISE PSN. Click Add Object, provide the name and available ISE PSN IP address. Click Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects Integration		Deploy Q	🚱 🌣 🔕 admin 🗸 🔤 secure
Distinguished Name     DNS Server Group     External Attributes     File List	Network A network object represents one or more IP addresses	. Network objects are used in various places, including access	control policies, network variables, intrusio	Add Network Add Object Import Obj Add Group	Q, Filter     Show Unused Objects     orts, and so on.
> FlexConfig Geolocation	Name	New Network Object		Value	Type Override
Interface	any	New Network Object	0	0.0.0/0 ::/0	Group 🖬 Q 🗑 🛤
Key Chain	any-ipv4	<b>N</b>		0.0.0.0/0	Network 🗓 Q 🗑 🛤
		Description Network Host Range Network Allow Overrides	O FQDN		
			Cancel Save		

FMC\_Add\_Object\_ISE

Step 5. Navigate to Objects > Object Management > VPN > Group Policy. Click Add Group Policy. Click DNS/WINS, select the object of the DNS server in Primary DNS Server. Then click Save.

Firewall Managemen	nt Center Overview Analysis Policies	Devices Objects	integration		Deploy Q 🧬 🌣 🕢 admin 🗸 📩
> Distinguished Name DNS Server Group	Group Policy				Add Group Policy Q, Filter
bestinguished Name     DNS Server Group     External Attributes     File List     FilesConfig     Geolocation     interface     Key Chain     Network     Policy List     Port     Prot     Prot     Stat Monitor     Time Eange     Time Zone     Turnel Zone     URL     Variable Set	Group Policy is a set of attribute and value pairs, stor	ed in a group policy object, that of Add Group Policy Name:* posture_gp Description: General Secure VPN Protocols BP Address Pools Banner DSSWINS Split Tunneling	lefine the remote access VPN experience. The RADIUS author for the remote access VPN experience. The RADIUS author for the remote access VPN experience. The RADIUS author for the remote access VPN experience. The remote access velocity VPN Server:	ization server assigns the group policy or	Add Group Pullcy     Q. Filter   t is obtained from the current connection profile.
VLAN Tag VIPN Certificate Map Custom Attribute Group Policy KEV1 (Psec Proposal KEV2 Paciloy KEV2 Paciloy Secure Client Customizatio Secure Client File			the second	uncel Seve	Displaying 1 - 2 of 2 rows $ \langle \langle Page   1 \rangle \rangle  C$

FMC\_Add\_Group\_Policy



**Note**: Ensure the DNS server used in the VPN group policy can resolve ISE client provisioning portal FQDN and enroll.cisco.com.

Step 6. Navigate to Objects > Object Management > Access List > Extended. Click Add Extended Access List.

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🔕 admin v 👘 see SECURE
<ul> <li>AAA Server</li> <li>RADIUS Server Group</li> <li>Single Single Server Group</li> </ul>	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	Add Extended Access List Q. Filter
Access List Extended	addresses. You use these objects when configuring particular features, such as route maps. Name Value	Override

 $FMC\_Add\_Redirect\_ACL$ 

Step 6.1. Provide the name of the redirect ACL. This name must be the same as in the ISE authorization profile. Click Add.

New Ex	tended	Access	List	Object
--------	--------	--------	------	--------

Name redirect									
Entries (0)									
									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
No record	s to display								

Cancel	Save

FMC\_Add\_Redirect\_ACL\_Part\_1

Allow Overrides

Step 6.2. Block DNS traffic, traffic to ISE PSN IP address, and the remediation servers to exclude them from redirection. Allow the rest of the traffic. This triggers redirection. Click Save.

Add Extended Access List Entry				0
Action: Block				
Logging: Default				
Log Level: Informational				
Log Interval: 300 Sec.				
Network Port <b>()</b> Application <b>()</b> Users	Security Group Tag			
Available Networks C +		Source Networks (0)	Destination Networks (1)	
Q Search by name or value		any	ISE_PSN	Ĩ
IPv4-Private-192.168.0.0-16	Add to Source			
IPv4-Private-All-RFC1918				
IPv6-IPv4-Mapped				
IPv6-Link-Local				
IPv6-Private-Unique-Local-Addresses				
IPv6-to-IPv4-Relay-Anycast				
ISE_PSN_		Enter an IP address	Enter an IP address	Add

FMC\_Add\_Redirect\_ACL\_Part\_2

Cancel

Add

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	1
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	11
3	Block	Any	Any	FTP	Any	Any	Any	Any	11
4 Allow O	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	/1

Can

FMC\_Add\_Redirect\_ACL\_Part\_3



Note: Destination FTP in this redirect ACL example is used as the remediation server example.

Step 7. Navigate to Objects > Object Management > RADIUS Server Group. Click Add RADIUS Server Group.



?

FMC\_Add\_New\_Radius\_Server\_Group

Step 7.1. Provide name, check Enable authorize only, check Enable interim account update, check Enable dynamic authorization.

### Add RADIUS Server Group

Step 7.2. Click the iconPlus to add a new radius server. Provide the ISE PSN IP Address/Hostname, Key. Select the specific interface for connecting. Select the Redirect ACL. Then click Saveto save the new radius server. Then click Save again to save the new radius server group.

FMC\_Add\_New\_Radius\_Server\_Group\_Part\_1

Add RADIUS Server Group	0	New RADIUS Server	0
<ul> <li>Enable authorize only</li> <li>Enable interim account update</li> <li>Interval:* (1-120) hours</li> <li>24</li> <li>Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> <li>1700</li> <li>Merge Downloadable ACL with Cisco AV Pair ACL</li> <li>After Cisco AV Pair ACL</li> <li>After Cisco AV Pair ACL</li> <li>After Cisco AV Pair ACL</li> </ul>		IP Address/Hostname:* Configure DNS at Threat Defense Platform Settings to resolve M Authentication Port: (1-65535) 1812 Key:*  Confirm Key:*  Accounting Port: (1-65535) 1813 Timeout: (1-300) Seconds	iostname
IP Address/Hostname No records to display		10 Connect using: Routing Specific Interface • inside_zone • Redirect ACL: redirect •	
	Cancel Save		Cancel

FMC\_Add\_New\_Radius\_Server\_Group\_Part\_2

Step 8. Navigate to Objects > Object Management > Address Pools > IPv4 Pools. Click Add IPv4 Pools and provide the Name, IPv4 Address Rangeand Mask. Then click Save.

Firewall Managem Objects / Object Managem	nent Center Overview Analysis Policies De	vices Objects Integration		Deploy Q 💕 🐇	angni v	enco SECURE
> AAA Server > Access List > Address Pools IPv4 Pools	IPv4 Pools IPv4 pool contains list of IPv4 addresses, it is used for manage	ment/diagnostic interface with clustering, or for VPN remote access profiles.		Add IPv4 Pools	Q, Filter	
Prof Roois     Prof Pools     Application Filters     AS Path     BFD Template     Cipher Suite List     DHCP IPv6 Pool     Distinguished Name     DHS Server Group     External Attibutes     File List     PlacConfig     Geslocation     Interface     Key Chain     Network     Pool     Pools     Pools     Pools     Pools     Suite List     Poot     Security Intelligence     Sinkhole     SLA Monitor     Time Range	Name of posture_pool_97_0	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         I Allow Overrides         Maddress conflicts in case of object to swoid P address conflicts in case of object is shared across multiple devices         • Override (0)	Cancel		Override ©	/1
Time Zone Tunnel Zone URL Variable Set				Displaying 1 - 2 of 2 r	ows IC < Page 1	of 1 > >1 C

FMC\_Add\_New\_Pool

Step 9. Navigate to Certificate Objects > Object Management > PKI > Cert Enrollment. Click Add Cert Enrollment, provide a name, and select Self Signed Certificatein Enrollment Type. Click the Certificate Parameters tab and provide Common Name and Country Code. Then click Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects Integration		Deploy Q, 💕 🌣 🕲 fangni 🛤	SECURE
AAA Server     Access List     Address Pools     Application Filters	Cert Enrollment A certificate enrollment object contains the Certification A your Private Key Infrastructure (PKI).	uthority (CA) server information and enrollment parameter	rs that are required for creating Certificate Signing Requests (CSRs) and obtainin	Add Cert Enrollment Q. Filter	occur in
AS Path BFD Template Circher Suite List	Name Add Cert Enrollment	0	Add Cert Enrollment	Type Override	/1
Sommunity List     DHCP IPv6 Pool     Community List     DHCP IPv6 Pool     DIstinguished Name     DhS Server Group     External Attributes     File List     Server Group     External Can Compa     External Can Compa     External Can Compa     External Can Compa     Internal CA     Internal CA     Internal CA     Internal CA     Internal CA     Internal Can Groups     Internal CA     Internal CA	Name*         demo_vpn         Description         CA Information       Certificate Parameters         Key         Enrollment Type:       Self Signed Certificate         VPN, To configure ON, please navigate to "Certificate         Validation Usage:       Image: Please Client Image: SSL Client	Revocation  Ifficate that is used in Remote Access Parameters' tab.  SSL Server	Name*         demo, spin         Description         CA Information       Certificate Parameters         Key       Revocation         Include FQDN:       Don't use FQON in certificate         Include Device's PA Address:       Common Name (CA):         Organization Unit (04):       Coganization (01):         Locatify (L):       State (ST):         County Code (C):       CN         Enal (L):       Include Device's Setial Number	n n n n n n n n n n n n n n	/1
Policy List	Allow Overrides		Allow Overrides		
Port Prefix List Route Map Security Intelligence		Cancel Save		Cancel Save Displaying 1 - 3 of 3 rows 1 < < Page 1 of	f1 > >1 C

FMC\_Add\_New\_Cert\_Enroll

Step 10. Navigate to Devices > Certificates. Click Add, select the FTD name under Device, select previous configured enrollment under Cert Enrollment. Click Add.

Firewall Manager Devices / Certificates	ment Center	Overview Analysis	Policies Devices Obje	cts Integration		Deploy	९ 🧬 🌣 🔕 fangni 🗸 ंतिर्देष SECURE
Filter All Certificates	*						Add
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
Add New Cer	tificate			0	e ca 🔍 ID		
Add a new certifi	cate to the devic	e using cert enro	ollment object which is use	ed to	@ CA ( 10)		± D C T
generate CA and Device*: Posture-FTD-C Cert Enroliment*: demo_vpn	identify certifica	• • • • • • • • • • • • • • • • • • •			9.04 LD		1 1 2 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Cert Enrollment D Name: Enrollment Type: Enrollment URL:	etails: demo_vpr Self-Signe N/A	i d					
			Cancel	Add			

FMC\_Add\_New\_Cert\_To\_FTD

Step 11. Navigate to Devices > VPN > Remote Access. Click Add.

Step 11.1. Provide the name, and add the FTD to Selected Devices. Click Next.

Firewall Management Center Overview Devices / VPN / Sexup Wizard	Analysis Policies Devices Objects Integration		Deploy Q 💞 🌣 🛛 admin 🗸 🖏 SECURE
Firewall Management Center     Devices / VFW / Sence Wexed      Access VPN Policy Wizard      Policy Assignment     C Connection Profile	Analysis Policies     Objects tetegration     Secure Client <ul> <li>Access &amp; Certificate</li> <li>Summary</li> </ul> Targeted Devices and Protocols   Targeted Devices and Protocols <ul> <li>Secure View View Option with one we user-defined connection profile.</li> </ul> Description:   Description:      Post-refuto   Secure Client   Secure Client   Secure Client   Output   Description:   Description:   Secure Client   Secure Client Secur	O 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 RADUS Server Group or SNO to authenticate VPN clients. Secure Client Package Mate sure you have Secure Client package for VPN Client downloaded it during the witzard. 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.	Deploy Q.
			Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_1

Step 11.2. Select previously configured radius server group in the Authentication Server, Authorization Server, Accounting Server. Scroll down the page.

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🔕 admin V 🖓 SECURE
Remote Access VPN Policy Wizard         1 Policy Assignment	
Renote Secure Client Liternet Outside Ven Isside Coporate Resources	
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 orrang 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	
Authentication Method:  AAA Only	
ULCUCL of Hasting of HACUDS	
Authorization Server: tp39 v + Vealth or RAUNUs Accounting Server: tp34	
Client Address Assignment:	
	Course Course Starts

 $FMC\_New\_RAVPN\_Wizard\_2$ 

Step 11.3. Select the previously configured pool name in IPv4 Address Pools. Select previously configured group policy in Group Policy. Click Next.

Firewall Management Center Overview Analysis Policies	s Devices Objects Integration	Deploy	۹	¢ 🗘	0	dmin ~	diste SECURE
Remote Access VPN Policy Wizard							
Policy Assignment (2) Connection Profile (3) Secure Client	Access & Certificate S Summary						
	(Realm or RADIUS)						
	Accounting Server: Tplie  (04/005)						
	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						
	Vise IP Address Pools						
	IPv4 Address Pools: posture_pool						
	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:* posture_ap +						
	Edit Group Policy						

Cancel Back Next

Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_3

### Step 11.4. Check the checkbox of Linux image. Click Next.

Firewall Management Center Overview Analysis Devices / VPN / Setup Wizard	Policies Devices Objects In	tegration		Deploy Q	🔮 🌣 📵 admin 🗸 👘 🐯 SECURE
Remote Access VPN Policy Wizard					
1 Policy Assignment 2 Connection Profile 8 Secure Clin	ent 4 Access & Certificate	5 Summary			
	Remote User Socure Client	outside vyp Internet	Inside Corpor Resource	100 100 100	
		AAA			
	Secure Client Image				
	The VPN gateway can automatically de connection is initiated. Minimize connecti	ownload the latest Secure Client package to t on setup time by choosing the appropriate OS fo	he client device when the VPN the selected package.		
	Download Secure Client packages from (	Disco Software Download Center.			
			Show Re-order buttons +		
	Secure Client File Object Name	Secure Client Package Name	Operating System		
	C attest lesses	cisco, socuro, client, wie, 5 1 3 62, webdario	Windows *		
	Cient_mage	elses-secore-ellent-will-strates-weddeplott			
	☑ linux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	1	
	☑ Linux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	]	
	Cienc_mage ☑ linux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	]	
	○ Cont_mays ○ Inux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	]	
	inur_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	]	
	inux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	]	
	<ul> <li>Cent_mays</li> <li>inuc_5_1_3_62</li> </ul>	cisco-secure-clent-linux64-5.1.3.62-webd	Linux	]	

FMC\_New\_RAVPN\_Wizard\_4

Step 11.5. Select the interface of VPN interface. Select the cert enrollment that enrolled on FTD in step 9. Click Next.

Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 💕 🌣 🚳 admin 🗸 🔥 SECURE
Remote Access VPN Policy Wizard		
Policy Assignment ② Connection Profile ③ Secure Client	- 3 Access & Certificate 5 Summary	
	<image/>	
		Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_5

Step 11.6. Double confirm the related information on summary page. If everything is good, click Finish. If anything needs to be modified, click Back.

Firewall Management Center Overview Analysis Policies Device	es Objects Integration		Deploy Q 🚱 🌣 😡 admin 🗸 😡 SECURE
Remote Access VPN Policy Wizard    Policy Assignment  Connection Profile  Connection P	Access & Certificate (3) Summary		
Remot	e Secure Client Ident	VPN Inside Corporate Resources	
Remote Accer Frevail Manager Name: Device Targets: Connection Polit Connection A AAA: Authenti Authenti Authenti Address DINCP S Address Group Policy Secure Client Ime Interface Objects: Device Centificate	ss VPN Policy Configuration ment Center will configure an RA VPN Policy with the following settings posture-TTD-CAL27 ei posture-TTD-CAL27 ei posture_yon clation dented: AAA Orly clation Server: rplike (RADUS) clation	Additional Configuration Requirements After the wizard completes, the following confront all device targets: • Access Control Policy Update Access Control Policy Update Access Control Policy Update With target on all targeted devices. • WAT 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 policy on the targeted devices. • Port Configuration SSL will be enabled on port 443. SSL will be enabled on port 643. SSL will be enabled on	
Device Identity C Certificate enrollm	Certificate Enrollment nent object 'demo_vpn' is not installed on one or more targeted	NAT Policy or other services before deploying the configuration.	
de de			Cancel Back Finish



Step 12. Deploy the new configuration to FTD to complete the remote access VPN configuration.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration			eploy 🔍 🚱 🗘 😨 🛛 admin 🗸 🚓 SECUS
posture_vpn			Q. Advanced	Deploy A Ignore warnings Deploy Cance
			Posture-FTD-CML27	Ready for Deployment
Connection Profile Access Interfaces Advanced				sy: wor
				-
Name	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfttGrpPolicy		
posture_vpn	Authentication: rtpise (RADIUS) Authonization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp	1 selected   O 1 pending	₽ 0

FMC\_Deploy\_FTD

## **Configurations on ISE**

Step 13. Navigate to Work Centers > Posture > Network Devices. Click Add.

=	diale Identity Services I	Engine				Work Centers / Posture					۹	۵	<u>ی</u> و	0 I	۹		
н	Bookmarks	Overview	Network D	evices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
-	Dashboard																
pd of	Context Visibility	Net	Network Devices														
×	Operations												s	elected 0	Total 4	Ø	ø
0	Policy	Ø Edit	+ Add	) Duplicate	🕁 Import 🔥 Export	Generate PAC	0 Delete 🗸								AI	× .	7
8.	Administration		Name ^	IP/Mask	Profile Name	Location	Туре		Description								
	Work Centers	0	FTD-CML2		L. 🗰 Cisco 🕕	All Locations	Firewall										
		0	FTD-CML2	-	🟥 Cisco 🕕	All Locations	Firewall										
			FTD-CML2	-	🗯 Cisco 🕡	All Locations	Firewall										
0	Interactive Help		8.00	100.0	🗯 Cisco 🕡	All Locations	Firewall										

ISE\_Add\_New\_Devices

Step 13.1. Provide the Name, IP Addressand scroll down the page.

≡ :	line Identity Service	s Engine				w	ork Centers / I	Posture		
Щ	Overview Netwo	ork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Ⅲ ◎ ※	Network Devices List Network Device Name	> New Network D es posture-FTD	evice	_						
20 AI	Description	s 🗸 * IP ;	······ / 32	-	¢					
?	Device Profile	at Cisco	~	0						
	Model Name		、 、	_						
	Software Versio	n	``							
	Network Device	Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Device	8	~	Set To Default					

ISE\_Add\_New\_Devices\_1

Step 13.2. Check the checkbox of RADIUS Authentication Settings. Provide the Shared Secret. Click Submit.

$\equiv \frac{1}{1000}$ Identity Service	s Engine					۷	Vork Centers / P	osture				2 <b>4</b> 0 0	A
JI Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings				
El Dashboard		~ RADIUS Authent	lication Settings										
Ho Context Visibility		RADIUS UDP Settings	5										
× Operations		Protocol RA	DIUS										
Policy		Shared Secret		Show									
Administration		Use Second Shared	Secret ()										
Work Centers		Secon Secret	d Shared		Show								
(?) Interactive Help		CoA Port 17	700	Set To Defa	uit								
		RADIUS DTLS Setting	ps ()										
		DTLS Required											
		Shared Secret rad	lius/dtls										
		CoA Port 20	083	Set To Defa	uit								
		Issuer CA of ISE Certificates for CoA	elect if required (optional)	× 0									
		DNS Name											
		General Settings											
		🗌 Enable KeyWrap 🕕											
		Key Encryption Key		Show									
		Message Authenticator Code		Show									
		Key Input Format											
		O ASCII 🔿 HEXA	DECIMAL										
		V TACACS Authen	tication Settings										
		<ul> <li>SNMP Settings</li> </ul>											
		<ul> <li>Advanced Trusts</li> </ul>	Sec Settings										
											Su	wit Cancel	

ISE\_Add\_New\_Devices\_2

Step 14. Download the package name cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg from <u>Cisco</u> <u>Software Download</u> and ensure the file is good by confirming md5 checksum of downloaded file is the same as Cisco Software Download page. Package name cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg has been downloaded successfully in Step 1.

Step 15. Navigate to Work Centers > Posture > Client Provisioning > Resources. Click Add. Select Agent resources from local disk.

≡	dentity Services Engine			Wo	rk Centers /	/ Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 🏾 🏮 De	leto				Sele	cted 0 Total 16 () All ~ 文
		Agent rese	ources from Cisco site		т	'ype 🗸	Version	Last Update	Description
#0		Agent rese	ources from local disk		1	WinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Prov
nii.		Native Sup	plicant Profile		1	Native Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agent Cor	figuration		1	Native Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agent Pos	ture Profile		,	MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Prov
		AMP Enab	ler Profile	5.1.3.062	(	CiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure C
		CiscoSecure	ClientDesktopLinux 5.1	.3.062	(	CiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C
		CiscoSecure	ClientComplianceModu	leWindows 4.3.4015.819	92 (	CiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSecure	ClientComplianceModu	leLinux 4.3.3139.0	(	CiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAgentl	essWindows 5.0.03061		(	CiscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgenti	essOSX 5.0.03061		(	CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	ralAgentWindows 5.0.0	3061	(	CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTempo	ralAgentOSX 5.0.03061		(	CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE\_Upload\_Resource

Step 15.1. Select Cisco Provided Package. Click Choose File to upload cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Click Submit.

≡	dentity Services E	ngine		Work Centers / Posture		Q 🕼	<u>ଡ</u> ୦   ୧
н	Bookmarks						
11 13 火	Dashboard Context Visibility Operations	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local Disk > A Agent Resources From Loc	gent Resources From Local Disk al Disk			
0 3.0	Policy Administration		Category	co Provided Package			
<b>ก</b>	Interactive Help		V Age	nt Uploaded Resources	Version Description		
			CiscoS	ecureClientDesktopLi CiscoSecureClientDe	5.1.3.62 Cisco Secure Client for	B	
			Submit				

ISE\_Upload\_Resources\_1



Note: Repeat the Step 14. to upload cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

	Step 16. Naviga	te to Work Centers > Posture > Client Provisioning > Resour	ces. Click Add. Select	Agent Posture Pro
--	-----------------	---	------------------------	-------------------

≡ :8	ldentity Services Engine				Work Cent	ers / Posture			
н.	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Setting	S	
15 15	Client Provisioning Policy Resources	Resources							
×	Client Provisioning Portal		🗋 Duplicate 📑 De	lete				Selected 0 Total 16	ß ▼
0		Agent re	sources from Cisco site	,	Version	Last Update	Description		
		Agent re	sources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		
-ili		Native S	upplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		
		Agent C	onfiguration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		
?		Agent P	osture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			
		AMP En	abler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE\_Add\_Agent\_Posture\_Profile

Step 16.1. Provide the Name, Server name rules and keep the rest as default. Click Save.

#### Name: linux\_agent\_profile

### Server name rules: \*.example.com

≡ :	liste Identity Services Engine		Woi	rk Centers / Postu	re	
Щ	Overview Network Devices	Client Provisioning Policy Elements	Posture Policy	Policy Sets Tro	ubleshoot Reports	Settings
11日 1日 火 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	Cilent Provisioning Policy Resources Cilent Provisioning Portal	ISE Posture Agent Profile Settings > New Profile Agent Posture Profile Name * Linux_agent_profile Description:				
?		Agent Behavior Parameter	Value	Descriptio	'n	
		Enable debug log	No V	Enables	the debug log on the agent	

ISE\_Add\_Agent\_Posture\_Profile\_1

dentity	Services Engine			w	ork Centers / I	Posture		
Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provis Resources	sioning Policy	Posture Protocol						
Client Provis	sioning Portal	Parameter	Value			Description	nt retry period	if there is a Passive Reassessment
		PRA retransmission tir	me <u>120</u>	secs		communication	n failure	
		Retransmission Delay	() <u>60</u>	secs		Number of retr	ids) to wait bef	r a message.
		Discovery host ①				Enter any IP ac detects and re portal.	Idress or FQDN directs that htt	i that is routed through a NAD. The NAD p traffic to the Client Provisioning
		Discovery Backup Ser	ver List Choose	8		By default, Any PSNs sequenti as the backup discovery prob	Connect send ally if the PSN list and restric es.	s discovery probes to all the Cisco ISE is unreachable. Choose specific PSNs t the nodes to which AnyConnect sends
		Server name rules * (	.exam	ple.com		A list of wildca servers that th	rded, comma- e agent can co	separated names that defines the nnect to. E.g. "*.cisco.com"
		Call Home List 🕕				A list of IP add that the agent endpoint does	iresses, that de will try to conn n't respond for	fines the all the Policy service nodes lect to if the PSN that authenticated the some reason.
		Back-off Timer 🕕	30	secs		Agent will cont targets and pro packets till this	tinuously try to aviously conne a max time limi	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
								Cancel Save



Step 17. Navigate to Work Centers > Posture > Client Provisioning > Resources. Click Add. Select Agent Configuration.

= -	dentity	Services Engine				Work Cent	ers / Posture		
щ	Overview	Network Devices	Client Prov	visioning Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Set	ttings
10 10	Client Provis Resources	ioning Policy	Reso	urces					
×	Client Provis	ioning Portal							Selected 0 Total 16 🦪
			0 Edit	+ Add 🔿 📋 Duplicate 🏾 📋 D	Pelete				all $\sim$ $\gamma$
U.				Agent resources from Cisco site	,	Version	Last Update	Description	
80				Agent resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for	r II
สีเ				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native	S
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Lin	nu
?				Agent Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17		
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49		

 $ISE\_Add\_Agent\_Configuration$ 

Step 17.2. Configure the details:

Select Agent Package: CiscoSecureClientDesktopLinux 5.1.3.062

Name: linux\_agent\_config

Compliance module: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Check the checkbox of VPN, Diagnostic and Reporting Tool

Profile Selection ISE Posture: linux\_agent\_profile

Click Submit.

$\equiv \frac{\mathrm{dealer}}{\mathrm{cisco}}$ Identity S	Services Engine					Work Cent	ers / Postu	'e
Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provisio	oning Policy					1		
Resources		* Select Agent Package:	Ci	scoSecureClientDesktopLin	ux 5.1.3.062 🗸 🗸			
Client Provisio	oning Portal	* Configuration Name:						
0		linux_agent_config						
<b>a</b>		Description:						
កា			k					
3		Description Value Na Compliance Module CiscoSecure Client Cisco Secure Client ISE Posture VPN Secure Firewall Posture Network Visibility Diagnostic and Reporting Tool Profile Selection * ISE Posture Iinux_agen	otes reClientComplianceModule Module Selection	Linux 4.3.			Su	bmit Cance

ISE\_Add\_Agent\_Configuration\_1

Step 18. Navigate to Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Click Edit at the end of any rule name. Select Insert new policy below.

≡	🖞 Identity	Services I	Engine									W	ork C	enters	/ Postur	e				
н	Overview	Network	Devices	Clie	ent Provi	sioning	Policy Elemen	ts	Posture Policy	,	Policy Sets	Troubl	eshoo	t R	eports	Settings				
태 18 왕 민 유 종	Client Provis Resources Client Provis	sioning Policy	]	Defi For For Intel For Mac If you	lient Agent Co Native Su dows Age I architect Windows c ARM64 p ou configu nout an AF	Provis ent Provision figuration: v pplicant Con int, Mac Age ures. Mac pu ves.	ioning Policy to deterr rersion of agent, ag figuration: wizard p nt, Mac Temporal a blicies run the samu 4 policies, configur re no Other Condit t client provisioning on. This is because	mine ent rofil nd N pare Si jons pol	cy e what users will rece profile, agent compil le and/or wizard. Dray Mac Agentless policie cxage for both archite ession: OS-Architect arm64 configuration licy for an OS, ensure endpoint is matched	eive up ance g and ecture ure E0 s. e that seque	pon login and use module, and/or a drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 policy entially with the po	session i ent custo ige the or fows polk ne Other ( is at the plicies liste	initiation mizatio rder. cies run Conditio top of ti ed in thi	n: n packaj n separat ons colur he cond is windo	ge. e packages nn. itions list, al w.	for ARM4 and read of policies				
0				~																
						Rule Name	)		Identity Groups		Operating Syste	ms		Other (	Conditions			Result	ts	
				_		IOS		H	Any	and	Apple IOS All		and	Conditio	n(s)		then	Cisco-I	ISE-NSP	Edit 🗸
					: 🖬	Android			Any	ano	Android		and	Conditio	n(s)		then	(1500-1	Duplicate above Duplicate below Insert new policy a Insert new policy b Delete	bove



#### Step 18.1. Configure the details:

#### Rule Name: Linux

#### Operating Systems: Linux All

### Results: linux\_agent\_config

#### Click Done and Save.

≡ :#	sco Identity	Identity Services Engine         Work Centers / Posture           rerview         Network Devices         Client Provisioning         Policy Elements         Posture Policy         Policy Sets         Troubleshoot         Reports         Settings           Client Provisioning Policy         Client Provisioning Policy         Policy Sets         Troubleshoot         Reports         Settings           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 Haim Shumpleset Configuration: version of agent, agent profile, agent configuration package.         Reference and drop user and drop usere and drop user and drop user and drop user and drop user and d																
н	Overview	Network Devices	Clier	nt Provis	ioning	Policy Elemen	nts	Posture Poli	су	Policy Sets	Troubles	hoo	t Reports	Settings				
王 同 火 し む	Client Provis Resources Client Provis	ioning Policy	Cli Defin For A For N Wind Intel : For V Mac J If you	e the Clie igent Con lative Sup ows Ager architectu Vindows A ARM64 po	Provison figuration: vi plicant Conf t, Mac Ager res. Mac poo gent ARM6- blicles require a an ARM64	ioning Policy to detei ersion of agent, a liguration: wizard ti, Mac Temporal : dicles run the sam 4 policies, configa re no Other Condi cilient provisionin	oli rmine gent profil and I ie pa ire S itions	cy e what users will re profile, agent comp le and/or wizard. Dr Mac Agentless polit ckage for both arch ession: OS-Archite arm64 configuratik (loy for an OS, ensu	ceive u bliance rag and cies sup litectur cture E bns. ire that	pon login and use module, and/or a l drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 policy	r session init gent customi nge the orde dows policie: he Other Cor r is at the top	iation zation r. s run nditio	n: n package. I separate packages ons column. he conditions list, al	for ARM4 and				
<b>?</b>			witho	v v	Rule Name IOS Android Linux	n. This is because	if If	Identity Groups Any Any Any	and and and	Operating Syst Operating Syst Apple IOS All Android Linux All	ems	and and and	Other Conditions Condition(s) Condition(s) Condition(s)		then then then	Results Cisco-ISE-NSP Cisco-ISE-NSP linux_egent_config	]	Edit ~ Edit ~ Edit ~

ISE\_Add\_New\_Provisioning\_Policy\_1

Step 19. Navigate to Work Centers > Posture > Policy Elements > Conditions > File. Click Add.

≡	dentity Services Engine	Work Centers / Posture	
н	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
11 13 <b>X</b>	Conditions V Anti-Malware Anti-Spyware Anti-Virus	Q. View / Edit + Add Displicate Caleboard	Selected 0 Total 385 🔗 🔕
	Application	Name Description File name Condition Type	
3. 	Dictionary Compound	pc_XP64_x82797002_M513 Cisco Predefined Check SYSTEM_PROGRAMS\C Cisco-Defined	8
-	Dictionary Simple Disk Encryption	pc_W8_64_KB3124275_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	External DataSource	pc_Vista_K82893294_MS13 Clsco Predefined Check: SYSTEM_32\Imagehlp.dll Cisco-Defined	
3	File	pc_W81_64_K83033889_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Firewall	pc_Vista64_K8925902_MS0 Cisco Predefined Check: SYSTEM_ROOT/winsxs\a Cisco-Defined	
	Hardware Attributes	pc_W10_64_1709_K845803 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry	pc_XP_K02653956_MS12+0 Clsco Predefined Check: SYSTEM_32\Wintrust.dll Cisco-Defined	
	Script	pc_W8_K82892074_MS13 Clsco Predefined Check: SYSTEM_32\Scrrun.dll Cisco-Defined	
	Service	pc_W10_64_1909_K850139 Cisco Predefined Check: SYSTEM_ROOT\SysWO Cisco-Defined	
	USB	pc_W7_K82681578_MS12 Clsce Predefined Check: SYSTEM_32\Win32k.sys Clsco-Defined	
	Remediations >	pc_W10_K83081435_MS15 Cisco Predefined Check SYSTEM_32\Edgehtml.dll Cisco-Defined	
	Requirements	pc_W81_64_K82042553_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Allowed Protocols	pc_W8_64_K02727528_M5 Cisco Predefined Check SYSTEM_ROOT\sysnativ Cisco-Defined	
	Authorization Profiles	pc_W8_64_K82992611_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Downloadable ACLs	pc_W7_K83078401_MS15 Cisco Predefined Check SYSTEM_32(Win32k.sys Cisco-Defined	

 $ISE\_Add\_New\_File\_Condition$ 

Step 19.1. Configure the details: Name: linux\_demo\_file\_exist Operating Systems: Linux All File Type: FileExistence

#### File Path: home, Desktop/test.txt

#### File Operator: Exists

Click Submit.



ISE\_Add\_New\_File\_Condition\_1

Step 20. Navigate to Work Centers > Policy Elements > Requirements. Click Edit at the end of any rule name. Select Insert new Requirement.

=	dentity Services I	Engine							Work	Centers / Po	osture					
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	Elements	Posture P	Policy Policy Sets	Tro	ubleshoot	Reports	Settings				
11 .14	Dashboard	Conditions	· ~ ·									Guide Me				
×	Operations	Anti-Male Anti-Spyv Anti-Vieus	ware Nare	Requirements												
.0	Policy	Applicatio	an .	Name		Operating Sys	tem	Compliance Module		Posture Type		Conditions		Remediations Actions		
<b>a</b> .,	Administration	Compoun	d	Any_AV_Installation_W	n for	Windows All	using	3.x or earlier	using	Agent	ne	t if ANY_av_win_inst	then	Message Text Only	Edit 🗠	
	West Centers	Dictionary	y Compound	Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	me	t if ANY_av_win_def	then	AnyAVDefRemediation/Win	Edit	Duplicate
rill	Work Centers	Dictionary Simple Disk Encryption		Any_AS_Installation_W	n for	Windows All	using	3.x or earlier	using	Agent	74	t if ANY_as_win_inst	then	Message Text Only	Edit	Insert new Requir
		External D	DataSource	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent		t if ANY_as_win_def	then	AnyASDefRemediationWin	Edit	Delete
0	Interactive Help	File		Any_AV_Installation_M	ic for	Mac OSX	using	3.x or earlier	using	Agent	ne	t if ANY_av_mac_inst	then	Message Text Only	Edit 👻	
		Firewall		Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent		t if ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit 🤟	
		Hardware	Attributes	Any_AS_Installation_M	ic for	Mac OSX	using	3.x or earlier	using	Agent	ne	t if ANY_as_mac_inst	then	Message Text Only	Edit 👻	
		Patch Mar	nagement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	THE OFFICE	t if ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 🛩	
		Script		Any_AM_Installation_W	in for	Windows All	using	4.x or later	using	Agent	ne	t if ANY_am_win_inst	then	Message Text Only	Edit 🗵	
		Service		Any_AM_Definition_Wir	for	Windows All	using	4.x or later	using	Agent	me	t if ANY_am_win_def	then	AnyAMDefRemediationWin	Edit 👻	
		USB		Any_AM_Installation_M	ac for	Mac OSX	using	4.x or later	using	Agent	ne	t if ANY_am_mac_inst	then	Message Text Only	Edit 🗸	
				Any_AM_Definition_Ma	o for	Mac OSX	using	4.x or later	using	Agent		t if ANY_am_mac_def	then	AnyAMDefRemediationMac	Edit 🗵	
		Remediation	•	Any_AM_Installation_Li	n for	Linux All	using	4.x or later	using	Agent	7.4	t if ANY_am_lin_inst	then	Select Remediations	Edit 🗵	
		Requirement	15	Any_AM_Definition_Lin	for	Linux All	using	4.x or later	using	Agent	me	t if ANY_am_lin_def	then	Select Remediations	Edit 9	
		Allowed Prot	tocols	USB_Block	for	Windows All	using	4.x or later	using	Agent	14	t If USB_Check	then	USB_Block	Edit 🗵	
		Authorization	e ACLs	Default_AppVis_Requin ent_Win	m for	Windows All	using	4.x or later	using	Agent	me	t if Default_AppVis_Co ndition_Win	then	Select Remediations	Edit 🤟	
				Default_AppVis_Require ent_Mac	im for	Mac OSX	using	4.x or later	using	Agent	me	t if Default_AppVis_Co ndition_Mac	then	Select Remediations	Edit 👻	
				Default_Hardware_Attri es_Requirement_Win	but for	Windows All	using	4.x or later	using	Agent		t if Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟	
				Default_Hardware_Attri es_Requirement_Mac	but for	Mac OSX	using	4.x or later	using	Agent		t if Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟	
				Note:												

Remediation Actions are not applicable for Application Conditions [configured using the P Remediations Actions are not applicable for Agentless Posture type. By Ca

ns, and External Data so

ISE\_Add\_New\_Posture\_Requirement

Step 20.1. Configure the details:

Name: Test\_exist\_linux

Operating Systems: Linux All

Compliance Module: 4.x or later

Posture Type: Agent

### Conditions: linux\_demo\_file\_exist

#### Click Done and Save.

= 1	deater Identity Services Engine					Work Centers / P	osture							
щ	Overview Network Devices	Client Provisioning	olicy Elements	Posture Policy	Policy Sets T	roubleshoot Repor	ts S	ettings						
目 王 同 光 日 よ。 予	Vereview     Active Markere       Active Markere     Active Markere       Active Antivere     Active Markere       Active Antivere     Active Markere       Active Antivere     Active Markere       Active Antivere     Active Markere       Dictionary Compound     Dictionary Simple       Diak Encryption     External DataSource       File     Prevail       Markere Attributes     Path Management       Registry     Script       Script     Script       Script     Script       Script     Script	Client Provisioning Pe Requirements Name Test_exist_inux Any_AV_Installation_Win Any_AV_Installation_Win Any_AS_Installation_Win Any_AS_Definition_Mac Any_AS_Definition_Mac Any_AS_Definition_Mac Any_AS_Definition_Mac Any_AS_Definition_Mac Any_AS_Definition_Mac Any_AS_Definition_Mac Any_AM_Definition_Win Any_AM_Installation_Win Any_AM_Definition_Mac	Operating Syri Operating Syri Const All Orier All Or	Posture Policy           tem         Control           using         4.x           using         3.x           using         4.x           using         4.x           using         4.x           using         4.x	r Policy Sets 7	roubleshot Repor	ts S	Conditions     Conditions     Inox_demo_file_ex     ist     ANY_av_win_inst     ANY_av_win_inst     ANY_av_win_def     ANY_as_win_def     ANY_as_win_def     ANY_as_mec_inst     ANY_as_mec_inst	then then then then then then then then	Remediations Actions Select Remediations Actions Select Remediations Message Text Only AnyAVDefRemediationNam Message Text Only AnyAVDefRemediationNam Message Text Only AnyAVDefRemediationNam AnyANDefRemediationNam Message Text Only AnyANDefRemediationNam Message Text Only AnyANDefRemediationNam	Edit v Edit v	<u> </u>		Q
	Allowed Protocols Authorization Profiles Downloadable ACLs	Note: Remediation Action is filtered base Remediations Actions are not appli Remediations Actions are not appli	ed on the operating syst cable for Application Co licable for Agentless Por	em and stealth mode nditions (configured ture type.	selection. using the Provision By Catego	ry or Provision By Everything op	tions), Harc	tware Conditions, and E	xternal	Data source conditions.		Save	Reset	t

ISE\_Add\_New\_Posture\_Requirement\_1



Note: As of now, only shell scripts are supported for Linux agents as remediation.

 $Step \ 21. \ Navigate \ to \ \ Work \ Centers > \ Policy \ Elements > \ Authorization \ Profiles. \ Click \ \ Add.$ 

Step 21.1. Configure the details:

Name: unknown\_redirect

Check the checkbox of Web Redirection(CWA,MDM,NSP,CPP)

Select Client Provisioning(Posture)

ACL: redirect

Value: Client Provisioning Portal(default)

≡ :	Index Identity Services Engine	Work Centers / Posture	
н.	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
11日   内   ペ   日   和   ⑦	Conditions ~ Anti-Malware Anti-Spyware Anti-Virus Application Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall	Authorization Profile         * Name       uuknown_redirect         Description         * Access Type       ACCESS_ACCEPT         Network Device Profile       Cisco         Service Template	
	Patch Management Registry Script Service USB Remediations Requirements Allowed Protocols Luthorization Profiles Downloadable ACLs	<ul> <li>Common Tasks</li> <li>Voice Domain Permission</li> <li>Web Redirection (GWA, MDM, NSP, CPP)</li> <li>Client Provisioning (Posture)</li> <li>ACL redirect</li> <li>Value Client Provisioning Portal (def: ~</li> <li>Static IP/Host name/FQDN</li> <li>Suppress Profiler CoA for endpoints in Logical Profile</li> </ul>	

ISE\_Add\_New\_Authorization\_Profile\_Redirect\_1



Note: This ACL name redirect must match the corresponding ACL name configured on FTD.

Step 21.2. Repeat the Add to create another two authorization profiles for non-compliant and compliant endpoints with the details.

Name: non\_compliant\_profile

DACL Name: DENY\_ALL\_IPv4\_TRAFFIC

Name: compliant\_profile

DACL Name: PERMIT\_ALL\_IPv4\_TRAFFIC



**Note**: The DACL for compliant or non-compliant endpoints needs to be configured according to the actual requirements.

Step 22. Navigate to Work Centers > Posture > Posture Policy. Click Edit at the end of any rules. Select Insert new policy.

the identity Servic	es Engine						Work	Centers / Po	sture				Q	۵	0	٥
															-	Ť
Bookmarks	Overview	v Ne	twork Devices	Client Provisioning P	olicy Elements	Posture Policy Polic	y Sets Tr	subleshoot	Reports Settin	gs						
Dashboard		Doct	uro Doliou													
Context Visibility		POSI	ure Policy	Guide Me												
Operations		Define the	Posture Policy by c	onfiguring rules based on operat	ting system and/or othe	r conditions.							×			
Policy		~														
Administration		Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compli	nce Module	Posture Type	Other Conditions	Requirements	_				
First Castors			Policy Options	Default_AntiMalware_Policy_Ma c	if Any	and Mac OSK	and 4.x or lat	er int	Agent	and	then Any_AM_Installation_Ma	Edit প				
and a second s			Policy Options	Default_AntiMalware_Policy_Ma	ir Any	and Mad OSX	and America	er and	Temporal Agent	and	then Any_AM_installation_Ma	Duplicate				
		_		e_temporal							c_temporal	Insert new policy				
Interactive Help			Policy Options	n	i Any	and Windows All	and Alk or lat		Agent	and	n n	Edit Celete				
			Policy Options	Default_AntiMalware_Policy_Win_temporal	ii Any	and Windows All	and 4.x or lat	er ind	Temporal Agent	and	then Any_AM_Installation_Wi n_temporal	Edt -				
			Policy Options	Default_AppVIs_Policy_Mac	r Any	and Mac OSX	and 4 x or lat	er and	Agent	and	then Default_AppVis_Require ment_Mac	Edt »				
			Policy Options	Default_AppVis_Policy_Mac_te mporal	II Any	and Mac OSX	and Axorlar	e	Temporal Agent	and	then Default_AppVis_Require ment_Mac_temporal	Edt y				
			Policy Options	Default_AppVis_Policy_Win	ii Any	and Windows All	and 4.x or lat	e in	Agent	and	then Default_AppVis_Require ment_Wis	Edt 9				
			Policy Options	Default_AppVis_Policy_Win_te mporal	ii Any	and Windows All	and Alk or lat	P 313	Temporal Agent	and	then Default_AppVis_Require ment_Wis_temporal	Edit +				
			Policy Options	Default_Firewalt_Policy_Mac	π Any	and Mac OSX	and Axorla	er and	Agent	and	then Default_Firewalt_Require ment_Mac	Edit v				
			Policy Options	Default_Firewall_Policy_Mac_te mporal	ii Any	and Mac OSX	and 4.x or lat	e and	Temporal Agent	and	then Default_Firewall_Require ment_Mac_temporal	Edt +				
			Policy Options	Default_Firewall_Policy_Win	ii Any	and Windows All	and 4.x or lat	r 10	Agent	and	then Default_Firewall_Require ment_Win	Edt +				
			Policy Options	Default_Firewall_Policy_Win_te mporal	II Any	and Windows All	and Alsorial	н 30	Temporal Agent	and	then Default_Firewalt_Require ment_Win_temporal	Edit v				
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	ii Any	and Med OSX	and 4.x or lat	e	Agent	and	then Default_Hardware_Attrib utes_Requirement_Mac	Edt v				
			Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	ii Any	and Mac OSX	and 4.x or lat	r ===	Temporal Agent	and	then Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edt 🤟				
			Policy Options	Default_Hardware_Attributes_P olicy_Win	i Any	and Windows All	and Axorlat	e	Agent	and	then Default_Hardware_Attrib utes_Requirement_Win	Edit				
		-	<b>M</b> 1.11.1. <b>M</b> 1.11.1.1	*			int to its		*							

ISE\_Add\_New\_Posture\_Policy

### Step 22.1. Configure the details:

Rule Name: Demo\_test\_exist\_linux

Identity Groups: Any

Operating Systems: Linux All

Compliance Module: 4.x or later

Posture Type: Agent

Requirements: Test\_exist\_linux

Click Done and Save.

ientity	Services Engin	e			in the second	vork Centers / Posture			
Post	ture Policy	Guide Me	ting 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_Require ment_Mac	Edit 🤟
	Policy Options	Default_Firewall_Policy_Mac_te mporal	II Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Require ment_Mac_temporal	Edit 👻
	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Firewall_Require ment_Win	Edit 🛩
	Policy Options	Default_Firewall_Policy_Win_te mporal	if Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Require ment_Win_temporal	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Hardware_Attrib utes_Requirement_Mac	Edit 🤟
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	II Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Hardware_Attrib utes_Requirement_Win	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	II Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attrib utes_Requirement_Win_t emporal	Edit 😔
	Policy Options	Default_US8_Block_Policy_Win	II Any	and Windows All	and 4.x or later	and Agent	and	then USB_Block	Edit 🗸
	Policy Options	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 😔
	Policy Options	Demo_test_exist_linux	If Any	and Linux All	and 4.x or later	and Agent	and	then Test_exist_linux	Edit 🐱

Step 23. Navigate to Work Centers > Posture > Policy Sets. Click to Insert new row above.

=	dealer Identity Services 8	Engine						Work Centers / P	osture					۵.	0	۹ ۱	۹
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings							
81 /d	Dashboard Context Visibility	F	Policy Sets					1				Reset	Reset Policys	et Hitcounts		Save	
*	Operations		<ul> <li>Status Policy Set</li> </ul>	Name Descrip	tion Cond	litions						Allowed Protocols	/ Server Seque	nce Hits	Actions	View	
U	Policy		Q. Search														
1. A	Administration Work Centers		O Default	Default p	olicy set							Default Network A	ccess 🧳	+ •	@-	,	
٢	Interactive Help												Inse	ert new row a	bove		
														Reset		Save	

ISE\_Add\_New\_Policy\_Set

Step 23.1. Configure the details:

Policy Set Name: Firewall Posture

Conditions: Network Access Device IP Address EQUALs [FTD IP Address]

#### Click Save.

addate Identity Services	s Engine						Vork Centers / F	Posture					۹	۵	<u>ه</u> (	8 I 8
Bookmarks	Overview	Network	Devices Client P	rovisioning Policy Elen	ents Posture Policy	Policy Sets	Troubleshoot	Reports	Settings							
문 Dashboard		Policy Sets									Reset	Reset Poli	cyset Hitco	ounts	S	eve
N Operations		🕙 Status	Policy Set Name	Description	Conditions						Allowed Protocols /	Server Seq	tneuce b	Hits Ad	ctions	View
E Policy		Q Search	1													
2. Administration		•	Firewall Posture		Network Access Device	P Address EQUALS					Default Network Acc	1055	2+	, .	¢	>
K Work Centers		•	Default	Default policy set							Default Network Acc	1055	2+	• •	¢	>
① Interactive Melp													R	leset	S	nve

ISE\_Add\_New\_Policy\_Set\_1

Step 23.2. Click > to enter the policy set. Create new authorization rules for posture compliant, non-compliant, and unknown status. Click Save.

Compliant with compliant\_profile

NonCompliant with non\_compliant\_profile

Unknown with unknown\_redirect

= :	diade Identit	y Ser	vice	s Engine						Work Cen	ters / Postu	ire						
н	Overview	N L Star	etwo	k Devices Client F	Provisioning	Policy E	lements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
15		0	F	irewall Posture			D Netwo	ork Access-Device IP Addr	ress EQUALS :						Default Netw	ork Access	0	+ •
*	~Au	thentic	ation #	Policy(1)														
0	€	Sta	tus	Rule Name	Condition									Use			Hits	Actions
#0		Q Se	arch															
- All										+								
?														All_Use	_ID_Stores	0		
		•		Default										> Optio	ons		48	¢
	> Au	thorizat	tion Po	olicy - Local Exceptions														
	> Aut	thorizat	tion Po	blicy - Global Exceptions														
	\~Au	thorizat	tion Po	olicy(4)														
												Results						
	C	Sta	tus	Rule Name	Condition	•						Profiles		Security (	iroups		Hits	Actions
		Q Se	arch															
		•	2	Compliant	는 Sessi	on PostureStatus	EQUALS Com	plant				compliant_profile	1 +	Select fr	om list	0 +	15	ŵ
		•	>	Non_Compliant	b Sessi	on PostureStatus	EQUALS Non	Compliant				non_compliant_profile	0+	Select fr	om list	/ +	5	(2)
		•	2	Unknown	h Sessi	on PostureStatus	EQUALS Unkr	nown				unknown_redirect	0 +	Select fr	om list	<u>0</u> +	47	٨

ISE\_Add\_New\_Policy\_Set\_2

### **Configurations on Ubuntu**

Step 24. Login to Ubuntu client via GUI. Open the browser to login the VPN portal. In this example, it is demo.example.com.

demo	.exar	nple.com/+CS	COEX	+			-	٥	×
$\leftarrow$	$\rightarrow$	C	0 🕰	https://demo. <b>example.com</b> /	-CSCOE+/logon.html#form_title_text	☆	$\bigtriangledown$	$ \pm $	≡

Logon	
Group posture_vpn v Username Password	
Logon	

### Step 25. Click Download for Linux.

Cisco	Secu	re Client Insta	allatic×	:	+					-	ē	×
÷	$\rightarrow$	C	0 8	2	https://demo. <b>example.com</b> /CACHE/stc/2/index.html	F	80%	ជ		${igsidential}$	$ \pm $	≡
		Secure	<mark>re</mark> Client	t								
					Cisco Secure Client Download							4
					Download & Install							
					Download Cisco Secure Client and install it on your computer.							
					Download for Linux							
							Inst	ructio	ns			

Ubuntu\_Browser\_VPN\_Download\_1

The downloaded file name is cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu\_Browser\_VPN\_Download\_2

Step 26. Download VPN certificate through the browser and rename the file to <certificate>.crt. This is the example of using firefox to download the certificate.

-	demo.e	example.c	com/+CSCOE×	+		$\sim$		ō	×
$\leftarrow$	→ C	;		//demo. <b>example.com</b> /+CSCOE+/logon.html#form_title_text	☆	$\bigtriangledown$	۲	ර	≡

General Media Permissions Security				
Website Identity         Website:       demo.example.com         Owner:       This website does not supply ownership in         Verified by:       C=CN,CN=demo.example.com	formation.	<u>V</u> iew Certificate		
Privacy & History Have I visited this website prior to today?	No			
Is this website storing information on my computer?	Yes, cookies	<u>C</u> lear Cookies and Site Data		
Have I saved any passwords for this website?	No	Vie <u>w</u> Saved Passwords		
Technical Details Connection Encrypted (TLS_AES_128_GCM_SHA256, 12 The page you are viewing was encrypted before being t Encryption makes it difficult for unauthorized people to therefore unlikely that anyone read this page as it trave	8 bit keys, TLS 1.3) ransmitted over the view information t led across the netw	Internet. raveling between computers. It ork. Help		

Ubuntu\_Browser\_VPN\_Cert\_Download

Step 27. Open the terminal on the Ubuntu client. Navigate to path home/user/Downloads/ to install Cisco Secure 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$
chmod +x 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\$

Step 28. Trust the VPN portal certificate on the 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

, O 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

Step 29. Open Cisco Secure Client on Ubuntu client, and connect VPN to demo.example.com successfully.

		Cisco Secure Clie	nt	-		×			
AnyCon	nect VPN	✓ Statistics	About						
		ıılıılı cısco							
Connect to:	demo.exa	ample.com		~		₽			
Group:	posture_v	pn				~			
Username:	isetest								
Password:	*******								
		* Disconnect							
Connected	o demo eva		)						
connected to demo.example.com.									

 $Ubuntu\_Secure\_Client\_Connected$ 

Step 30. Open the browser to access any website triggering the redirection to the ISE CPP portal. Download the certificate from the ISE CPP portal and rename the file to <certificate>.crt. This is an example of using Firefox for downloading.



Ubuntu\_Browser\_CPP\_Cert\_Download

#### Step 30.1. Trust the ISE CPP portal certificate on the 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

```
, O removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

Step 31. Click Start on the ISE CPP portal.

Oevice Security Check × +		ø	×						
← → C () A https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08 ☆		$\bigtriangledown$	≡						
You must log in to this network before you can access the Internet.									
Client Provisioning Portal									
Device Security Check Your computer requires security software to be installed before you can connect to the network.									

#### Step 32. Click here to download and install Agent.

Device Security Check × +	- 0 ×									
← → C https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL &	≣ ₪									
You must log in to this network before you can access the Internet.	×									
Client Provisioning Portal										
Device Security Check Your computer requires security software to be installed before you can connect to the network. Unable to detect Posture Agent										
+ This is my first time here										
<ol> <li>You must install Agent to check your device before accessing the network. <u>Click here to download and install Agent</u></li> <li>After installation, Agent will automatically scan your device before allowing you access to the network.</li> <li>You have 20 minutes to install and for the system scan to complete.</li> </ol>										
Note: With some browsers, when you click Download, the script is directly saved in the configured Downloads folder in your system. Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.										
You have 20 minutes to install and for the compliance check to complete										
+ Remind me what to do next										

 $Ubuntu\_Browser\_CPP\_Download\_Posture$ 

Step 33. Open the terminal on the Ubuntu client. Navigate to path home/user/Downloads/ to install the posture module.

<#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_0NcLgcMURfy
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_0NcLgcMURfyZmR6Hol
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.
```

Step 34. On Ubuntu client UI, quit the Cisco Secure Client and reopen it. The ISE Posture module is installed and run successfully.



Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed

Step 35. Open the terminal on the Ubuntu client. Navigate to path home/user/Desktop, create a test.txt file to meet the file condition configured on ISE.

<#root> user@ubuntu22-desktop:~\$ cd Desktop/ user@ubuntu22-desktop:~/Desktop\$

echo test > test.txt

# Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Connect VPN to demo.example.com on Ubuntu client.



Step 2. Check the ISE Posture status on the Ubuntu client.



Verify\_Ubuntu\_Secure\_Client\_Compliant

#### Step 3. Check Radius Live Log on ISE. Navigate to Operations > RADIUS Live Log.

≡	diada Identity Services Engine			Opera	tions / RADIUS			Q & @ &   A
Щ	Live Logs Live Sessions							
55								
01	Misconfigured Supplicants 🕕	Misc	onfigured Network D	evices 🕕	RADIUS Drops		Client Stopped Responding ①	Repeat Counter ①
*	0		0		0		0	0
0							Refresh Show	Within
a.							Never v Latest 20 rec	cords 🗸 Last 24 hours 🗸
di.	Ø ⊆ Reset Repeat Counts (	🕆 Export To 🗸						Filter 🗸 🛞
	Time	Status Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy Au	uthorization Policy
?		~	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	uthorization Policy
	May 29, 2024 09:08:48.798 PM	۵	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default Fir	rewall Posture >> Compliant
	May 29, 2024 09:08:48.798 PM			52:54:00:17:6B:FA		Compliant	Firewall Posture Fir	rewall Posture >> Compliant
	May 29, 2024 09:08:13.570 PM	a a	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default Fir	rewall Posture >> Unknown

Verify\_ISE\_LiveLog

Step 4. Navigate to FTD CLI via SSH or console.

<#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

# Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

For posture flow and troubleshooting Cisco Secure Client and ISE, check the CCO documents **ISE Posture Style Comparison for Pre and Post 2.2** and **Troubleshoot ISE Session Management and Posture.** 

# **Related Information**

- Cisco Identity Services Engine Network Component Compatibility, Release 3.3
- Cisco Identity Services Engine Administrator Guide, Release 3.3
- <u>Cisco Technical Support & Downloads</u>