# 使用ISE 3.3配置Linux VPN安全評估

目錄

<u>必要條件</u>
<u>採用元件</u>
<u>設定</u>
網路圖表
FMC/FTD上的組態
<u>ISE上的配置</u>
<u>Ubuntu上的配置</u>
<u>驗證</u>
<u>疑難排解</u>
相關資訊

簡介

本文檔介紹如何使用身份服務引擎(ISE)和Firepower威脅防禦(FTD)配置Linux VPN狀態。

必要條件

需求

思科建議您瞭解以下主題:

- 思科安全使用者端
- Firepower威脅防禦(FTD)上的遠端訪問VPN
- 身分識別服務引擎 (ISE)

採用元件

本檔案中的資訊是根據以下軟體版本:

- 烏班圖22.04
- 思科安全使用者端5.1.3.62
- Cisco Firepower威脅防禦(FTD) 7.4.1
- 思科Firepower管理中心(FMC) 7.4.1
- 思科身分辨識服務引擎(ISE) 3.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設) )的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

# 設定

# 網路圖表



拓撲

# FMC/FTD上的組態

步驟 1.已成功配置客戶端、FTD、FMC和ISE之間的連線。因為enroll.cisco.com用於進行重定向探 查的終端(有關詳細資訊,請參閱終端安全評估流程CCO 文檔<u>進階版和進階版2.2的ISE終端安全評</u> <u>估樣式比較</u>)。確定已正確設定FTD上至enroll.cisco.com的流量路由。

步驟 2.從<u>Cisco軟體下載</u>cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg下載軟體套件名稱,並確認下載檔案的md5校驗 和與Cisco軟體下載頁相同,以確保下載後檔案完好。

步驟 3. 導航到Objects > Object Management > VPN > Secure Client File。點選Add Secure Client File,提供名稱,瀏覽File Name以選擇 cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg,選擇File Type下拉選單中的Secure Client Image。然後按一下Save。

Firewall Managemen Objects / Object Management	t Center Overview Analysis Policie	is Devices Objects Integration		Deploy	९ 💕 🌣 🔕 admin 🗸	tine SECURE
> Distinguished Name DNS Server Group	Secure Client File			Add Secure	Client File Q, Filter	
> External Attributes	File objects represent files used for remote access V	/PN policy configurations. They can contain Secure Client profile and image files.				
File List > FlexConfig Geolocation		Add Secure Client File	0			
Interface Key Chain Network	Name client_image	Name:*		n-5.1.3.62-webdeploy-k9.pkg	Type Secure Client Image	±/¥
> РКІ Policy List	Default-External-Browser-package hostscan5_1_3_62	linux_5_1_3_62		36-webdeploy-k9.zip 1-5.1.3.62-k9.pkg	Secure Client External Browser Pa HostScan Package	± 9 11 ± 1 11
Port > Prefix List	linux_image	File Name:*		ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	±/1
Route Map Security Intelligence		Cisco-secure-client-linux64-5.1.3.62-W				
Sinkhole SLA Monitor		Secure Client Image				
Time Range Time Zone Tunnel Zone		Description:				
URL Variable Set						
VLAN Tag ~ VPN						
Certificate Map						
Group Policy IKEy1 IPsec Proposal		Cancel	Save			
IKEV1 Policy IKEV2 IPsec Proposal						
IKEv2 Policy						
Secure Client File				Displ	aying 1 = 4 of 4 rows. IC < Page 1	of 1 > > C

FMC\_Upload\_Secure\_Client\_Image

## 步驟 4. 導航到Objects > Object Management > Network。

# 步驟 4.1.建立DNS伺服器的物件。按一下Add Object,提供名稱和可用的DNS IP地址。按一下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 addresse	s. Network objects are used in various places, including acces	s control policies, network variables, intru	Add Network	Add Object      Add Object      Import Dispect      orts, and so on.
FlexConfig Geolocation Interface	Name	New Network Object	0	Value 0.0.0.0/0	Type Overside
Key Chain Network	any-ipv4	Name		0.0.0.0/0	Network Par Q = #
		Description			
		Network Host C Range Network			
		Allow Overrides			
			Cancel Save		

FMC\_Add\_Object\_DNS



**注意**:此處配置的DNS伺服器將用於VPN使用者。

步驟 4.2.為ISE PSN建立對象。按一下Add Object,提供名稱和可用的ISE PSN IP地址。按一下Save。

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects Integration		Deploy	Q. 🚱 🌣 🔕 🛛 admin 🗸 🔤 disde SEC	CURE
Distinguished Name     DNS Server Group     External Attributes     File List	Network A network object represents one or more IP addresse	s. Network objects are used in various places, including access	s control policies, network variables, intrusi	Add Network Add Network on rules, identity rules, network discovery rule Import Add Gr	Q. Filter     Show Unused Objects     orts, and so on.	
> FlexConfig Geolocation	Name	New Network Object	0	Value	Type Override	
Interface	any	New Network Object	v	0.0.0/0	Group 🖥 Q 🗑 🛤	
Key Chain Network	any-ipv4	Nama		0.0.0/0	Network 월 Q 🗑 🛤	
		ISE_PSN_ Description Network Host Range Network Allow Overrides	) FQDN			
			Cancel Save			

#### $FMC\_Add\_Object\_ISE$

步驟 5.導航到Objects > Object Management > VPN > Group Policy。按一下Add Group Policy。按一下DNS/WINS,在Primary DNS Server中選擇DNS伺服器的對象。然後按一下Save。

Citiects / Object Management	t Center Overview Anal	ysis Policies De	vices Objects	Integration			Deploy Q	° •	admin ~	dada SECURE
Distinguished Name     DNS Server Group     External Attributes     File List	Group Policy A Group Policy is a set of attribute an	nd value pairs, stored in a	group policy object, that	, t define the remote access VPN experience.TI	te RADIUS authorization server assig	ins the group policy or it is obtained fi	Add Group Polici	Q. Filter	le.	
> FlexConfig Geolocation	Name									
Interface Key Chain	DftGrpPolicy		Add Group Polic	y.						Zi.
Network Network PKI Policy List Port Policy List Route Map Scacurity Intelligence Sinkhole SLA Monitor Time Zone TumeI Zone URL Variable Set VLAN Tag V VPN Certificate Map Custom Attribute Group Policy IKEVI Pasc Proposal IKEVI Pasc Proposal IKEV2 PASC PASC PASC PASC PASC PASC PASC PASC			Name:* posture_gp Description: General Secur VPN Protocols IP Address Pools Banner DNS/WIVS Split Tunneling	e Client Advanced  Primary DNS Server: DNS = • • • Secondary DNS Server: • • Primary WINS Server: • • DHCP Network Scope: • • DHCP Network scope: • • DHCP Network scope: • •	+ + + + + et (0c 16.72.3.5)					/#
Secure Client File					Cancel Save		Displaying 1 - 2	of 2 rows	< Page 1	of 1 > >  C

FMC\_Add\_Group\_Policy



注意:確保VPN組策略中使用的DNS伺服器可以解析ISE客戶端調配門戶FQDN和enroll.cisco.com。

步驟 6. 導航到Objects > Object Management > Access List > Extended。按一下Add Extended Access List。

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🕢 admin ~ 🗄 🚓 SECURE
<ul> <li>AAA Server</li> <li>RADIUS Server Group</li> </ul>	Extended	Add Extended Access List Q, Filter
Single Sign-on Server Access List Extended	An access sit doject, also known as an access control inst (ACL), selects the trame to which a service will apply. Standard-identities trame based on destination address only, identities trame based addresses. You use these objects when configuring particular features, such as route maps.	Override

FMC\_Add\_Redirect\_ACL

步驟 6.1.提供重定向ACL的名稱。此名稱必須與ISE授權配置檔案中的名稱相同。按一下Add。

#### New Extended Access List Object

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

#### Allow Overrides

		Cancel Save
FMC Add Redirect ACL Part 1		

# 步驟 6.2. 阻止DNS流量、到ISE PSN IP地址的流量和補救伺服器將其排除在重定向之外。允許其餘的流量。這會觸發重新導向。按一下Save。

Add Extended Access List Entry		0
Action: Block		
Logging:		
Default 🔻		
Log Level:		
Informational <b>v</b>		
Log Interval:		
300 Sec.		
Network Port <b>()</b> Application <b>()</b> Users <b>()</b>	Security Group Tag	
Available Networks C +	Source Networks (0)	Destination Networks (1)
Q Search by name or value	any	ISE_PSN
IPv4-Private-192.168.0.0-16	to Source	J
IPv4-Private-All-RFC1918 Ad	to Destination	
IPv6-IPv4-Mapped		
IPv6-Link-Local		
IPv6-Private-Unique-Local-Addresses		
IPv6-to-IPv4-Relay-Anycast		
ISE_PSN_		
rtp_ise	Enter an IP address	dd 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	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	11

Cancel Save

 $FMC\_Add\_Redirect\_ACL\_Part\_3$ 



步驟 7. 導航到Objects > Object Management > RADIUS Server Group。按一下Add RADIUS Server Group。

Firewall Management Objects / Object Management	Center Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	6
AAA Server     RADIUS Server Group     Single Sign-on Server     Access List	RADIUS Server (	Group	or more referen	ces to RADI	JS Servers. Ti	ese AAA servers are used to authenticate users logging in through Remote Access VPN conne	ections.	Add RADIUS Se	ver Gro	up
Extended	Name						Value			

 $FMC\_Add\_New\_Radius\_Server\_Group$ 

步驟 7.1.提供名稱、檢查Enable authorize only、檢查Enable interim account update、檢查Enable dynamic authorization。

Add RADIUS Server Group	0
Name:*	1
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

# 步驟 7.2.按一下Plus 圖示增加新的RADIUS伺服器。提供ISE PSNIP Address/Hostname, Key。選擇specific interface進行連線。選擇 Redirect ACL。然後按一下Save儲存新的RADIUS伺服器。然後再次按一下Save,儲存新的RADIUS伺服器組。

Add RADIUS Server Group	0	New RADIUS Server	0
Enable authorize only		IP Address/Hostname:*	
Carlos Enable interim account update Interval:* (1-120) hours 24		Configure DNs at Tineat Detense Platform Settings to resolve Authentication Port:* (1-65535) [1812 Kau*	i nostname
Carlos Construction  Port:* (1024-65535)  1700  Merge Downloadable ACL with Cisco AV Pair ACL  After Cisco AV Pair ACL  Before Cisco AV Pair ACL  Carlos Construction		Confirm Kay:*	
RADIUS Servers (Maximum 16 servers)	+	Timeout: (1-300) Seconds	
IP Address/Hostname No records to display		Connect using: Routing O Specific Interface Inside_zone Redirect ACL: redirect Interface Inside_routing Insi	
[	Cancel Save		Cancel

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

步驟 8. 導航到Objects > Object Management > Address Pools > IPv4 Pools。按一下Add IPv4 Pools並提供Name, IPv4 Address Range和 Mask。然後按一下Save。

Firewall Managem Objects / Object Managem	tent Center Overview Analysis Policies Devices Objects Integration		Deploy Q 💕	o o fangni v	cisco SECURE
> AAA Server > Access List > Address Pools	IPv4 Pools IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.		Add IPv4 Pools	Q, Filter	
Pork Rook     Pork Rook     Pork Rook     Pork Rook     Application Filters     AS Path     BFD Template     Cipher Suite List     Community List     DetCP Prof Root     Distinguished Name     DNS Server Group     External Attributes     File List     Pers.Config     Geolocation     Interface     Key Chain     Network     Port     Port List     Roote Map     Societry Intelligence     Sistable     SLA Monitor     Time Range	Name       Add IPv4 Pool         posture_pool_97.0       Name*         posture_pool_97.0       Posture_pool         Posture_pool       Posture_pool         Description       Posture_pool         Posture_pool       Posture_pool	(Particular Save		Override ©	/1
Tunnel Zone URL Variable Set			Displaying 1 - 2 of 2	rows IC C Page 1	of 1 > >1 C

 $FMC\_Add\_New\_Pool$ 

Enrollment Type中選擇Self Signed Certificate。按一下Certificate Parameters頁籤,然後提供Common Name和Country Code。然後按一下 Save。

Firewall Managemen Objects / Object Managemen	nt Center Overview Analysis Policies Devi	Objects Integration		Deploy Q 💞 🐼 🕢 fangni 🗸 📩
AAA Server     Access List     Address Pools     Application Filters	Cert Enrollment A certificate enrollment object contains the Certification Authorit your Private Key Infrastructure (PKI).	(CA) server information and enrollment parameter	rs that are required for creating Certificate Signing Requests (CSRs) and obtain	Add Cert Enrollment Q. Filter
AS Path	Name			Type Override
BFD Template	Add Cert Enrollment	ø	Add Cert Enrollment	⊕ teni / ₩
Copher Suite List Community List DHCP IPv6 Pool Distinguished Name	Name* demo_vpn Description		Name* demo_vpn Description	>eri
DNS Server Group > External Attributes File List	CA Information Certificate Parameters Key Revo	cation	CA Information Certificate Parameters Key Revocat	ion
<ul> <li>FlexConfig</li> <li>Geolocation</li> <li>Interface</li> <li>Key Chain</li> <li>Network</li> </ul>	Errollment Type: Self Signed Certificate  Common Name (CN) is mandatory for self-signed certificate VPN. To configure CN, please navigate to 'Certificate Param Validation Usage: V Piece Client V SSL Client S	that is used in Remote Access eters' tab. IL Server	Include FQDN: Don't use FQDN in certificate Include Device's IP Address: Common Name (CR): demo.example.com Organization Unit (CU):	
PKI     Cert Enrollment     External Cert Groups     External Certs     Internal Certs			Organization (O):           Locality (L):           State (ST):           Country Code (C):	
Internal CAS Internal CAS Internal Cert Groups Internal Certs			Email (E): Include Device's Serial Number	
Trusted CAs Policy List	Allow Overrides		Allow Overrides	
> Prefix List		Cancel Save		Cancel Save
Route Map				Displaying 1 - 3 of 3 rows I < < Page 1 of 1 > > I C

FMC\_Add\_New\_Cert\_Enroll

步驟 10. 導航到Devices > Certificates。點選Add,在Device下選擇FTD名稱,在Cert Enrollment下選擇以前配置的註冊。按一下Add。

Firewall Management C Devices / Certificates	enter Overview Analysis	Policies Devices Objects	Integration		Deploy Q 🚱 🌣 🙆 f	angni ~ dede SECURE
Filter All Certificates						Add
Name Dom	nain Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
Add New Certifica	te		0			A
						1000
Add a new certificate to	the device using cert enro	ollment object which is used to		BOA GLD		1 1 C 1
generate CA and identif	fy certificate.					
Device*:				O CA LD		±₽°с∎
Posture-FTD-CML27	•					
Cert Enrollment*:						
demo_vpn	• +					
Cert Enrollment Details:						
Name:	demo_vpn					
Enrollment Type:	Self-Signed					
Enroliment URL:	N/A					
		Cancel				

 $FMC\_Add\_New\_Cert\_To\_FTD$ 

步驟 11. 導航到Devices > VPN > Remote Access。按一下Add。

步驟 11.1.提供名稱, 並新增FTD至Selected Devices。按一下Next。

Firewall Management Center Overview Devices / VPN / Secup Wizard	Analysis Policies Devices Objects Integration		Deploy Q 💕 🌣 🔕 edmin 🗸 🕬 SECURE
Connection Profile	• Secure Client • Access & Certificate   • Secure Client • Access & Certificate   • Secure Client • Access & Certificate   • Secure Client • Secure Client   • Secure Client • Secure Client	Before You Start     Before you start, ensure the following configuration elements to be in place to complete Remote Access VMP Volicy, Authentication Server Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients. Scure Client Package Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Clico codentiate to download it during the wizard. Device Interface Interface should be already configured on targeted for interface group to enable VPN access.	
			Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_1

# 步驟 11.2.在Authentication Server, Authorization Server, Accounting Server中選擇先前配置的radius伺服器組。向下捲動頁面。

Elizevall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🔕 admin V 🔤 tude SECURE
Remote Access VPN Policy Wizard         1 Pelicy Assignment         2 Connection Profile         3 Secure Client         4 Access & Certificate         5 Summary	
Remote Secure Client Cutside VPN Inside Corporate 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 group policies. Connection Profile Name**	
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:*	
Authorization Server: Trpise  (Reality of MAULOD)	
Accounting Server: Itskid + Client Address Assignment:	
Plane IP addeese ann ha teolanad fann AAA sonne PMPN samme and IP addeese annis. When mediate antines an	Cancel Back Not

FMC\_New\_RAVPN\_Wizard\_2

步驟 11.3.在IPv4 Address Pools中選擇以前配置的池名稱。在Group Policy中選擇以前配置的組策略。按一下Next。

Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 🚱 🌣 🚱 admin 🗸 👶 SECURE
Remote Access VPN Policy Wizard      Policy Assignment	(4) Access & Certificate (5) Summary	
	(Realm or BADUS) Accounting Server: (RADUS) (RADUS) +	
	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 PLOF Servers. Use 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:*	



FMC\_New\_RAVPN\_Wizard\_3

### 步驟 11.4.選中Linux映像的覈取方塊。按一下Next。

Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 🔮 🌣 🔕 admin ~ 🔤
Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 Secure Client	(4) Access & Certificate (5) Summary	
Remote User	Secure Client	
Secure 0	e Client Image	
The VPN (	N gateway can automatically download the latest Secure Client package to the client device when the VPN tion is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.	
Download	ad Secure Client packages from Cisco Software Download Center.	
	Show Re-order buttons +	
C Secu	iecure Client File Object Name Secure Client Package Name Operating System	
Clen	slent_image cisco-secure-client-win-5.1.3.62-webdepio Windows *	
🕑 linux	inux_5_1_3_62 cisco-secure-client-linux64-5.1.3.62-webd Linux 🔻	

Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_4

步驟 11.5.選擇VPN介面的介面。選取在步驟9中註冊FTD的憑證註冊。按一下Next。



Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_5

#### 步驟 11.6.在摘要頁面上重複確認相關資訊。如果一切正常,請按一下Finish。如果需要修改任何內容,請按一下Back。



FMC\_New\_RAVPN\_Wizard\_6

#### 步驟 12.將新組態部署到FTD以完成遠端存取VPN組態。

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy 2, 💞 🌣 🕢 admin	n ~ cisco SECURE
posture_vpn			Q Advanced Deploy 🔺 Ignore warnings	Deploy
			Posture-FTD-CML27 Ready for Deployment	sents.(1)
Connection Profile Access Interfaces Advanced				sy: None
				+
Name	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authonization: None Accounting: None	E DfttGrpPolicy		
posture_vpn	Authentication: riplee (RADIUS) Authonization: riplee (RADIUS) Accounting: riplee (RADIUS)	E posture_gp	1 selected   👩 1 pending	20

FMC\_Deploy\_FTD

#### ISE上的配置

步驟 13. 導航到Work Centers > Posture > Network Devices。按一下Add。

=	dentity Services E	Engine					Work Centers	/ Posture					Q	۵	0	٥	A
н	Bookmarks	Overview	Network De	evices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
	Dashboard	Not															
цġ	Context Visibility Network Devices												0				
*	Operations	Ø Edit	+ Add (	) Duplicate	🕁 Import 🖞 Export	✓ 👌 Generate PAC	🛛 Delete 🖂										V
U L	Administration	0	Name ^	IP/Mask	Profile Name	Location	Type		Description								
1	Work Centers	0	FTD-CML2	1000	🔍 🏥 Cisco 🕕	All Locations	Firewall										
		0	FTD-CML2	- Course	L m Cisco ()	All Locations	Firewall										
?	Interactive Help	0	8 at 1	-	# Cisco 🕕	All Locations	Firewall										

ISE\_增加\_新裝置

步驟 13.1.提供Name, IP Address並向下滾動頁面。

≡ ::	Identity Serv	vices Engine				w	ork Centers / I	Posture		
Щ	Overview Ne	twork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
5	Network Device	s List > New Network D	evice							
14	Network D	evices								
*	Name	posture-FTD		_						
U.	Description									
	IP Ac	idress 🗸 * IP :	······		0					
?										
	Device Prof	ile 就 Cisco	~	0						
	Model Nam	e	~	_						
	Software Ve	ersion	~	_						
	Network De	vice Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Devic	e	~	Set To Default					

ISE\_增加\_新裝置\_1

步驟 13.2. 選中RADIUS Authentication Settings覈取方塊。提供Shared Secret。按一下Submit。

≡	dentity Services	Engine					۷	Vork Centers / P	osture			۵ ۵	0 Q   A
н	Bookmarks	Overview	Network Devices	<b>Client Provisioning</b>	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings			
	Dashboard		~ RADIUS Authent	tication Settings									
-13	Context Visibility	-	RADIUS UDP Setting	5									
×	Operations		Protocol RA	DIUS									
1	Administration		Shared Secret		Show								
al.	Work Centers		Use Second Shared	I Secret 🕕									
			Secret			Show							
٢	Interactive Help		CoA Port 1	700	Set To Defa	uit .							
			RADIUS DTLS Setting	gs 🕕									
			DTLS Required ()	Sur Arts									
			Cot Part at		Set To Defe								
			Issuer CA of ISE										
			Certificates for CoA	velect ir required (opsonal)	- 0								
			General Settings										
			Key Encryption Key		Show								
			Message										
			Key		Show								
			ASCII HEXA	DECIMAL									
			V TACACS Authen	ntication Settings									
			<ul> <li>Advanced Trusts</li> </ul>	Sec Settings									
												Submit	Cancel

ISE\_增加\_新裝置\_2

步驟 14. 從<u>Cisco軟體下載</u>下載軟體套件名稱cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg,並確認下載檔案的 md5校驗和與Cisco軟體下載頁相同,從而確保檔案完好。已在步驟1中成功下載包名稱cisco-secure-client-linux64-5.1.3.62-webdeploy-

#### k9.pkg。

=	alight Identity Services Engine			Wo	rk Centers /	Posture			
Щ	Overview Network Devices	Client Pro	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
	Client Provisioning Policy Resources Client Provisioning Portal	Reso	ources					Selec	ted 0 Total 16 🕃
*		🖉 Edit	+ Add 🔿 📋 Duplicate 🍵 D	Pelete					AII V 🛛 🖓
0			Agent resources from Cisco site		T	ype ~	Version	Last Update	Description
<b>a</b> o			Agent resources from local disk		v	VinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Prov
-file			Native Supplicant Profile		N	lative Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
			Agent Configuration		N	lative Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?			Agent Posture Profile		N	MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Prov
			AMP Enabler Profile	5.1.3.062	c	SiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure C
			CiscoSecureClientDesktopLinux 5.	.1.3.062	c	SiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C
			CiscoSecureClientComplianceMod	duleWindows 4.3.4015.819	92 0	SiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
			CiscoSecureClientComplianceMod	duleLinux 4.3.3139.0	c	SiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure C
			CiscoAgentlessWindows 5.0.0306	1	c	iscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
			CiscoAgentlessOSX 5.0.03061		c	SiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
			CiscoTemporalAgentWindows 5.0.	.03061	c	SiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
			CiscoTemporalAgentOSX 5.0.0306	51	c	iscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

步驟 15. 導航到Work Centers > Posture > Client Provisioning > Resources。按一下Add。選擇Agent resources from local disk。

ISE\_Upload\_Resource

## 步驟 15.1.選擇Cisco Provided Package。點選Choose File上傳cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg。按一下Submit。

≡	dentity Services E	ngine		Work Cente	rs / Posture			Q	۵	0	Q	8
月 田 同 火	Bookmarks Dashboard Context Visibility Operations	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local Agent Resources Fro	Disk > Agent Resources From Local D om Local Disk	sk							
0 Ao Ali	Policy Administration Work Centers		Category	Cisco Provided Package	epłoy-k9.pkg							
•	Interactive Help		Submit	Agent Uploaded Resour     Name     CiscoSecureClientDesktopLi Cancel	C0S Type CiscoSecureClientDe	Version 5.1.3.62	Description Cisco Secure Client for II					

ISE\_Upload\_Resources\_1



註:重複步驟14上傳cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg。

步驟 16. 導航到Work Centers > Posture > Client Provisioning > Resources。按一下Add。選擇Agent Posture Profile。

= :	diale Identity Services Engine				Work Cent	ers / Posture			
щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Settings	1	
E A	Client Provisioning Policy Resources	Resources							
×	Client Provisioning Portal							Selected 0 Total 16	S C
0		🖉 Edit 🛛 🕂 Add 🔿	Duplicate 🍵 De	elete				$_{\rm AII}\sim$	$\nabla$
		Agent res	sources from Cisco site	,	Version	Last Update	Description		
40		Agent res	sources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		
-fil		Native Su	pplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		
		Agent Co	nfiguration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		
?		Agent Por	sture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			
		AMP Enal	bler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE\_Add\_Agent\_Posture\_Profile

#### 步驟 16.1.提供Name, Server name rules(並將其余的保留為預設值)。按一下Save。

# 名稱:linux\_agent\_profile

### 伺服器名稱規則:\*.example.com

≡ :8	sco Identity	Services Engine			Wa	ork Centers /	Posture			
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ 	Client Provis Resources Client Provis	ioning Policy	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	e						
(?)			Agent Behavior Parameter Enable debug log		Value No V	D	escription nables the debug log	on the agent		

ISE\_Add\_Agent\_Posture\_Profile\_1

≡ ::	Identity Services Engine			Work Centers / I	Posture		
щ	Overview Network Devices	s Client Provisioning Policy I	Elements Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provisioning Policy Resources	Posture Protocol					
×	Client Provisioning Portal	Parameter	Value		Description		
0		PRA retransmission time	120 secs		This is the age communication	nt retry period n failure	if there is a Passive Reassessment
a.		Retransmission Delay ()	60 secs		Time (in secon	ids) to wait bef	ore retrying.
ส์เ		Retransmission Limit ①	4		Number of retr	ies allowed for	r a message.
?		Discovery host ()			Enter any IP ad detects and re portal.	ddress or FQDM directs that htt	I that is routed through a NAD. The NAD p traffic to the Client Provisioning
		Discovery Backup Server List	Choose		By default, An PSNs sequenti as the backup discovery prob	yConnect send ally if the PSN list and restric ses.	s discovery probes to all the Cisco ISE is unreachable. Choose specific PSNs t the nodes to which AnyConnect sends
		Server name rules * ①	•.example.com		A list of wildca servers that th	irded, 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	prines the all the Policy service nodes tect to if the PSN that authenticated the some reason.
		Back-off Timer ()	30 secs		Agent will con targets and pr packets till this	tinuously try to eviously conne s max time limi	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
							Cancel Save

ISE\_Add\_Agent\_Posture\_Profile\_2

### 步驟 17. 導航到Work Centers > Posture > Client Provisioning > Resources。按一下Add。選擇Agent Configuration。

≡ :	listo Identity Services Engine				Work Cent	ers / Posture				
щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy S	Sets Troubleshoo	ot Reports S	Settings		
10	Client Provisioning Policy Resources	Resources	;							
×	Client Provisioning Portal							Se	lected 0 Total 16	Ø
0		🖉 Edit 🕂 Add 🔿	🗋 Duplicate 🏾 🍵 De	lete					ali $\sim$	V
8.		Agent r	esources from Cisco site	,	Version	Last Update	Description			
		Agent r	esources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client	for li		
-file		Native S	upplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nati	ve 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增加代理配置

#### 步驟 17.2.配置詳細資訊:

- 選取代理程式套件: CiscoSecureClientDesktopLinux 5.1.3.062
- 名稱: linux\_agent\_config
- 合規性模組:CiscoSecureClientComplianceModuleLinux 4.3.3139.0
- 核取核取方塊 VPN, Diagnostic and Reporting Tool
- 配置檔案選擇ISE終端安全評估:linux\_agent\_profile

### 按一下Submit。

≡ %	dentity	Services Engine					Work Cent	ers / Postu	re
Щ	Overview	Network Devices	<b>Client Provisioning</b>	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provis	ioning Policy					1		
14	Resources		* Select Agent Package:	Cit	scoSecureClientDesktopLin	nux 5.1.3.062 🗸 🗸			
*	Client Provis	ioning Portal	* Configuration Name:						
U			linux_agent_config						
80			Description:						
สเ				<i>i</i>					
			Description Value N	otes					
			* Compliance Module CiscoSecu	reClientComplianceModulel	Linux 4.3.∽				
			Cisco Secure Client	Module Selection					
			ISE Posture 🔽						
			Secure Firewall						
			Network Disibility						
			Diagnostic and Reporting 🗹 Tool						
			Profile Selection						
			* ISE Posture linux_ager	t_profile	~			Su	ubmit Canc

ISE\_Add\_Agent\_Configuration\_1

步驟 18. 導航到Work Centers > Posture > Client Provisioning > Client Provisioning Policy。在任何規則名稱的末尾按一下Edit 。選擇 Insert new policy below。

= -	diale Identity	Services	Engine									Wo	ork Ce	enters / Postu	e					
щ	Overview	Network	Devices	Clie	ent Provi	sioning	Policy Elemen	its	Posture Policy	,	Policy Sets	Trouble	eshoot	Reports	Settings					
111 131 141 141 141 141 141 141 141 141	Client Provi Resources Client Provi	isioning Policy	]	C Defi For For Intel For Mac If you	lient Agent Cor Native Suy dows Age 1 architect Windows 2 ARM64 p bu configui nout an AR	Provision figuration: v pplicant Con nt, Mac Age ures. Mac pu Agent ARM6 iolicies require an ARM64 conditi	ioning Policy to deter ersion of agent, as figuration: wizard p nt, Mac Temporal a blicies run the sam 4 policies, configu e no Other Condil c client provisioning n. This is because	miningent profi	cy e what users will recc profile, agent compli le and/or wizard. Dra Mac Agentiess policie cxage for both archit ession: OS-Architect a 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 ag drop rules to chan port ARM64. Wini 39. 2UALS arm64 in ti the ARM64 policy entially with the po	session in ent custor age the orn tows polic to Other C is at the b licies liste	nitiation mizatior der. ies run condition op of th d in this	: package. separate packages ns column. ie conditions list, al s window.	for ARM4 and read of policies					
				$\sim$																
?						Rule Name	•		Identity Groups		Operating Syste	ms		Other Conditions			Resul	ts		
				8		IOS		H	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-	ISE-NSP	Edit 🗸	
				8		Android		If	Any	and	Android		and	Condition(s)		then	Cisco-	ISE-NSP	Editis	
																	1	Duplicate above Duplicate below Insert new policy ab	low	

#### 步驟 18.1. 配置詳細資訊:

規則名稱:Linux

作業系統:Linux All

#### 結果:linux\_agent\_config

#### 按一下Done 和Save。

=	dentity Services Engine			Work C	enters / Posture		
Ц	Overview Network Devices	Client Provisioning Policy Elemen	ts Posture Policy	Policy Sets Troubleshoe	ot Reports Settings		
田  10  火  10  10  10  10	Client Provisioning Policy Resources Client Provisioning Portal	Client Provisioning Policy to deter For Agent Configuration: version of agent, ag For Native Supplicant Configuration: wizard p Windows Agent, Mac Agent, Mac Temporal a Intel architectures. Mac Agent, Mac Temporal a For Windows Agent ARM64 policies : configur Mac ARM64 policies require no Other Condit If you configure an ARM64 client provisioning without an ARM64 condition. This is because	mine what users will receive ent profile, agent complianc rofile and/or wizard. Drag ar and Mac Agentless policies si a package for both architecture ions arm64 configurations. p policy for an 0%, ensure th an endpoint is matched seq	upon login and user session initiatio ie module, and/or agent customizatio nd drop rules to change the order. iupport ARM64. Windows policies ru ures. EQUALS arm64 in the Other Conditi at the ARM64 policy is at the top of quentially with the policies listed in ti	on: on package. n separate packages for ARM4 and ons column. the conditions list, ahead of policies his window.		
?		Rule Name II 2 IOS II 2 Android II 2 Linux	Identity Groups           Id         Any         and           Id         Any         and           Id         Any         and	Operating Systems d Apple IOS All and d Android and d Linux All and	Other Conditions Condition(s) Condition(s) Condition(s)	Results then Cisco-ISE-NSP then Cisco-ISE-NSP then linux_agent_config	Edit ~ Edit ~ Edit ~

ISE\_Add\_New\_Provising\_Policy\_1

### 步驟 19. 導航到Work Centers > Posture > Policy Elements > Conditions > File。按一下Add。

=	dentity Services Engine	Work Centers / Posture	
щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
三 同 火	Conditions V Anti-Malware Anti-Spyware Anti-Virus	Q View 2 Edi + Add Duplicate Collection	Selected 0 Total 385 💋 🔕
	Compound	Name Description File name Condition Type	
40	Dictionary Compound	pc_XP64_X812797052_M513 Cisco Predefined Check: SYSTEM_PROGRAMS\C Cisco-Defined	1
mil	Dictionary Simple	pc_W8_64_XB3124275_MS Clsco Predefined Check: SYSTEM_ROOT\sysnativ Clsco-Defined	
	External DataSource	pc_Vista_K02093294_MS13 Cisco Predefined Check: SYSTEM_32\Imagehlp.dll Cisco-Defined	
?	File	pc_W81_64_K83032889_M Clsco Predefined Check: SYSTEM_ROOT\sysnativ Clsco-Defined	
	Firewall	pc_Vista64_X8925902_MS0 Cisco Predefined Check: SYSTEM_ROOT\winsxs\a Cisco-Defined	
	Hardware Attributes	pc_W10_64_1709_K845803 Clsco Predefined Check: SYSTEM_ROOT\sysnativ Clsco-Defined	
	Registry	pc_XP_K52653956_M512-0 Cisco Predefined Check: SYSTEM_32(Wintrust.dll Cisco-Defined	
	Script	pc_WIL_XB28P2074_MS13 Cisco Predefined Check: SYSTEM_32(Scrun.dll Cisco-Defined	
	Service	pc_W10_64_1909_K850139 Cisco Predefined Check: SYSTEM_ROOT\SysWO Cisco-Defined	
	U58	pc_W7_K82681578_M512 Cisco Predefined Check: SYSTEM_32(Win32k.sys Cisco-Defined	
	Remediations >	pc_W10_K83081436_MS15 Cisco Predefined Check: SYSTEM_321Edgehtml.dll Cisco-Defined	
	Regularments	pc_Will_64_Killo042553_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Allowed Protocols	pc_W8_64_X82727528_M5 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Authorization Profiles	pc_W8_64_X82992611_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Downloadable ACLs	pc_W7_K83078601_M515 Cisco Predefined Check: SYSTEM_321Win32k.sys Cisco-Defined	

 $ISE\_Add\_New\_File\_Condition$ 

步驟 19.1. 配置詳細資訊:

名稱:linux\_demo\_file\_exist

作業系統:Linux All

檔案型別:檔案存在

檔案路徑:home, Desktop/test.txt

檔案運算子:存在

按一下Submit。

≡	dentity Services Engine					Work Cen	ters / Post	ure		
н	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
	Cenditions V Anti-Malvare Anti-Spyvare Anti-Vius Application Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall Hardware Attributes Patich Management Registry Script Service	File Conditions List > New F File Condition Name * Description * Operating System Compliance Module A * File Type * File Path * File Operator	ile Condition	   	test.txt	]			Submit	Cancel
	Remediations > Requirements Allowed Protocols Authorization Profiles Downloadsble ACLs									

ISE\_Add\_New\_File\_Condition\_1

步驟 20. 導航到Work Centers > Posture > Policy Elements > Requirements。在任何規則名稱的末尾按一下Edit 。選擇Insert new Requirement。

=	dender Identity Services E	Engine							Work	Centers / P	osture					
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	Elements	Posture	Policy Policy Sets	Tro	oubleshoot	Reports	Settings				
5 1	Dashboard Context Visibility	Conditions Anti-Malw	÷									Guide Me				
$\times$	Operations	Anti-Spyw	rare	Requirements												
0	Policy	Anti-Virus Applicatio	n	Name		Operating Sys	tem	Compliance Module		Posture Type	•	Conditions		Remediations Actions		
<b>a</b>	Administration	Compound		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 🖂	
	Hack Contern	Dictionary	Compound	Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_def	then	AnyAVDefRemediationWin	Edit	Duplicat
mili	WORK Centers	Dictionary Dick Force	Simple	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 n
		External D	ataSource	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_ss_win_def	then	AnyASDefRemediationWin	Edit	Delete
(2)	interactive Help	File		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 😔	T
		Firewall		Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit 🤟	
		Hardware	Attributes	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 🤟	
		Patch Mar	agement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 🛩	
		Script		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 🛩	
		Service		Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_def	then	AnyAMDefRemediationWin	Edit 🤟	
		US8		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 👻	1
		Remediation	• >	Any_AM_Installation_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_inst	then	Select Remediations	Edit 😔	
		Requirements		Any_AM_Definition_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_def	then	Select Remediations	Edit 😔	
		Allowed Prot	ocols	US0_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 🤟	
		Authorization Downloadabl	Profiles e ACLs	Default_AppVis_Requiren ent_Win	for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Win	then	Select Remediations	Edit 🤟	
				Default_AppVis_Requiren ent_Mac	n for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Mac	then	Select Remediations	Edit 🔗	
				Default_Hardware_Attribu es_Requirement_Win	it for	Windows All	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟	
				Default_Hardware_Attributes_Requirement_Mac	it for	Mac OSX	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟	

ISE\_Add\_New\_Posture\_Requirement

#### 步驟 20.1. 配置詳細資訊:

名稱:Test\_exist\_linux

作業系統:Linux All

合規性模組:4.x或更高版本

狀態型別:代理

條件:linux\_demo\_file\_exist

按一下Done 和Save。

≡ ;	Indentity Services Engine			Work Centers / Posture		
	Overview Network Devices	Client Provisioning Policy Elem	ments Posture Policy Policy Sets Tr	oubleshoot Reports Sett	tings	
<u> </u>						
	Conditions ~					~ 0
11	Anti-Malware			Guide Me		
*	Anti-Spyware	Requirements				
	Anti-Virus	Name Ope	erating System Compliance Module	Posture Type 0	Conditions Remediations Action	
•	Application		• •			
a.	Compound Dictionary Compound	Test_exist_linux for Linux	xx All using 4.x or later using	Agent met if	inux_demo_file_ex then Select Remediations ist	Edit 🗸
-51	Dictionary Simple	Any_AV_Installation_Win for Wind	dows All using 3.x or earlier using	Agent met if J	ANY_av_win_inst then Message Text Only	Edit 🛩
	Disk Encryption	Any_AV_Definition_Win for Wind	dows All using 3.x or earlier using	Agent met if /	ANY_av_win_def then AnyAVDefRemediationWi	Edit 🛩
0	External DataSource	Any_AS_Installation_Win for Wind	dows All using 3.x or earlier using	Agent met if /	ANY_as_win_inst then Message Text Only	Edit 🛩
	File	Any_AS_Definition_Win for Wind	dows All using 3.x or earlier using	Agent met if A	ANY_as_win_def then AnyASDefRemediationWi	Edit 🗸
	Firewall	Any_AV_Installation_Mac for Mac	OSX using 3.x or earlier using	Agent met if A	ANY_av_mac_inst then Message Text Only	Edit ~
	Patch Management	Any_AV_Definition_Mac for Mac	COSX using 3.x or earlier using	Agent met if J	ANY_av_mac_def then AnyAVDefRemediationMa	e Edit ~
	Registry	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 👻
	Script	Any_AS_Definition_Mac for Mac	: OSX using 3.x or earlier using	Agent met if J	ANY_as_mac_def then AnyASDefRemediationMa	c Edit ↔
	Service	Any_AM_Installation_Win for Wind	dows All using 4.x or later using	Agent met if /	ANY_am_win_inst then Message Text Only	Edit v
	USB	Any AM Definition Win for Wind	dows All using 4.x or later using	Agent met if A	ANY am win def then AnyAMDefRemediationW	n Edit v
		Any AM Installation Mac for Mac	OSX using 4.x or later using	Agent met if A	ANY am mac inst then Message Text Only	Edit v
	Remediations	Any AM Definition Mac for Mac	DSX using 4.x or later using	Agent met if J	ANY am mac def then AnyAMDefRemediationM	
	Requirements	101 Jun 2001 101 101	and and the second	- Alexandre - A	an partane and representation of the	Eur v
	Allowed Protocols	Note:				
	Authorization Profiles	Remediation Action is filtered based on the op Remediation Actions are not applicable for App	perating system and stealth mode selection. oplication Conditions (configured using the Provision By Category	or Provision By Everything options), Hardwa	re Conditions, and External Data source conditions.	
	COMPROBIDIE PLOCS	Remediations Actions are not applicable for Ag	Agentiess Posture type.			
						Cause Daset
						Save

ISE\_Add\_New\_Posture\_Requirement\_1



**注意**:到目前為止,Linux代理程式僅支援Shell命令檔作為修正。

步驟 21. 導航到Work Centers > Posture > Policy Elements > Authorization Profiles。按一下Add。

步驟 21.1. 配置詳細資訊:

名稱: unknown\_redirect

核取核取方塊 Web Redirection(CWA,MDM,NSP,CPP)

選取 Client Provisioning(Posture)

ACL:重定向

### 值:使用者端布建入口網站(預設)

≡ :	dentity Services Engine	Work Centers / Posture
н.	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
■ は ※ ● ■ 。	Conditions Anti-Malware Anti-Spyware Anti-Virus Application Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall Hardware Attributes	Authorization Profile   * Name   unknown_redirect   Description   * Access Type   ACCESS_ACCEPT   Network Device Profile   # Cisco   Service Template   Track Movement   ①   Agentless Posture   ①   Passive Identity Tracking
	Patch Management Patch Management Registry Script Service USB Remediations Requirements Allowed Protocols Authorization Profiles Downloadable ACLs	<ul> <li>Common Tasks</li> <li>Voice Domain Permission</li> <li>Web Redirection (CWA, MDM, NSP, CPP</li> <li>Client Provisioning (Posture)</li> <li>ACL</li> <li>redirect</li> <li>Value</li> <li>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



附註:此ACL名稱重新導向必須與FTD上設定的對應ACL名稱相符。

步驟 21.2.重複Add 以建立另兩個授權配置檔案,為不相容和相容的終端提供詳細資訊。

名稱:non\_compliant\_profile

DACL名稱:DENY\_ALL\_IPv4\_TRAFFIC

名稱:compliant\_profile

DACL名稱: PERMIT\_ALL\_IPv4\_TRAFFIC



註:需要根據實際需求配置合規端點和不合規端點的DACL。

步驟 22. 導航到Work Centers > Posture > Posture Policy。在任何規則的末尾按一下Edit 。選擇Insert new policy。

- Advision Accession	- Franks							- 1		-						<b>•</b> •	~	0 1 0
<ul> <li>Casco Identity Service</li> </ul>	s Engine							l	Work Centers /	Pos	ture					ч <b>ф</b>	<u>ں</u>	ΨIX
Bookmarks	Overview	w Ne	etwork Devices	Client Provisioning	Policy Elements	Postu	re Policy Policy	Sets	Troubleshoot	R	teports Settings							
E Dashboard		_																
Context Visibility		Post	ure Policy	Guide Me														
% Operations		Define th	e Posture Policy by c	onfiguring rules based on open	ating system and/or of	her cond	itions.									9		Q,
Policy		~																
Administration		Status	Policy Options	Rule Name	Identity Groups		Operating Systems		Compliance Module		Posture Type	Other Conditions		Requirements				
Work Centers			Policy Options	Default_AntiMalware_Policy_Ma c	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Ma c	Edit প			- 1
			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	044	Any_AM_installation_Ma c_temporal	Edg Insert new policy			
③ Interactive Help			Policy Options	Default_AntiMalware_Policy_Win	ii Any	and	Windows All	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Win	Edit Oran			
			Policy Options	Default_AntiMalware_Policy_Win_temporal	ii Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Any_AM_Installation_Win_temporal	Edit +			
			Policy Options	Default_AppVIs_Policy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Default_AppVis_Require ment_Mac	Edit v			
			Policy Options	Default_AppVIs_Policy_Mac_te mporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Mac_temporal	Edit y			
			Policy Optiona	Default_AppVIs_Policy_Win	i' Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_AppVis_Require ment_Win	Edit v			
			Policy Options	Default_AppVis_Policy_Win_te mporal	i' Any	and .	Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Win_temporal	Edit +			
			Policy Options	Default_Firewalt_Policy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then.	Default_Firewall_Require ment_Mac	Edit v			
			Policy Options	Default_Firewall_Policy_Mac_temporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Mac_temporal	Edit +			
			Policy Optiona	Default_Firewall_Policy_Win	ii 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	II Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Win_temporal	Edit v			
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Mac	Edit v			
			Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	if Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edt v			
			Policy Options	Default_Hardware_Attributes_P olicy_Win	ii Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Win	Edit v			
		-	A	-			· · · · · · · · · · · · · · · · · · ·		* *- *-*		*							

ISE\_Add\_New\_Posture\_Policy

#### 步驟 22.1. 配置詳細資訊:

規則名稱:Demo\_test\_exist\_linux

身份組:任意

作業系統:Linux All

合規性模組:4.x或更高版本

狀態型別:代理

需求:Test\_exist\_linux

按一下Done 和Save。

Post		Guide Me	ting s	system and/or	r other cone	ditions.										2	×
×																	
	Policy Options	Default_Firewall_Policy_Mac	ii.	Atry	and	Mac OSX	an	d 4.)	x or later		nd	Agent	and	the	en.	Default_Firewall_Require ment_Mac	Edit 🗸
	Policy Options	Default_Firewall_Policy_Mac_te mporal	i.	Any	and	Mac OSX	an	d 4.)	x or later	- à	nd	Temporal Agent	and	th	65	Default_Firewall_Require ment_Mac_temporal	Edit 🗸
	Policy Options	Default_Firewall_Policy_Win	H.	Any	and	Windows All	an	d 4.3	x or later		nd	Agent	and	th	en.	Default_Firewall_Require ment_Win	Edit v
	Policy Options	Default_Firewall_Policy_Win_te mporal	H.	Any	and	Windows All	an	d 4.3	x or later	- 1	nd	Temporal Agent	and	the	en	Default_Firewall_Require ment_Win_temporal	Edit v
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	1	Any	and	Mac OSX	an	d 4.	x or later	-	nd	Agent	and	th	en	Default_Hardware_Attrib utes_Requirement_Mac	Edit 🗸
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	1	Any	and	Mac OSX	an	d 4.3	x or later	-	nd	Temporal Agent	and	th	en	Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Win	ii.	Any	and	Windows All	an	4 4.	x or later		nd	Agent	and	th	en.	Default_Hardware_Attrib utes_Requirement_Win	Edit 🗸
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	R.	Any	and	Windows All	an	d 4.3	x or later	-	nd	Temporal Agent	and	the	65	Default_Hardware_Attrib utes_Requirement_Win_t emporal	Edit v
	Policy Options	Default_US8_Block_Policy_Win	W.	Any	and	Windows All	an	d 4.3	x or later		nd	Agent	and	th	en.	USB_Block	Edit 😔
	Policy Options	Default_USB_Block_Policy_Win	1	Any	and	Windows All	an	d 4.3	x or later		nd	Temporal Agent	and	th	en.	USB_Block_temporal	Edit 😔

ISE\_Add\_New\_Posture\_Policy\_1

# 步驟 23. 導航到Work Centers > Posture > Policy Sets。按一下以Insert new row above。

$\equiv \frac{-de-de}{case}$ Identity Services	Engine	Work Centers / Posture	C & O Q   A
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy	y Sets Troubleshoot Reports Sett	ttings
El Dashboard	Policy Sets		Reset Policyset Hitcounts Save
* Operations	Status Policy Set Name Description Conditions		Allowed Protocols / Server Sequence Hits Actions View
Policy     Administration	Q. Search		
K Work Centers	Default Default policy set		Default Network Access 🥒 + 🔹 🚳 🕨
① Interactive Help			linger new row above
			2000 - 2000

ISE\_Add\_New\_Policy\_Set

步驟 23.1. 配置詳細資訊:

策略集名稱:防火牆狀態

#### 條件:網路訪問裝置IP地址等於[FTD IP地址]

按一下 Save。

≡ dentity Services	ingine Work Centers / Posture		c	4	۲	<b>0</b>	۹
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings						
10 Dashboard	Policy Sets	Reset	Policyset H	toounts		Save	
% Operations	Status Policy Set Name Description Conditions	Allowed Protocols / Server	Sequence	Hits	Actions	View	
E Policy	Q Search						
1. Administration	Firewall Posture     Postant Posture     Postant Access Davice IP Address EQUILS	Default Network Access	2+	,	٨	>	
📲 Work Centers	Default Default policy set	Default Network Access	2+	+	0	>	
① Interactive Help				Reset		Save	

ISE\_Add\_New\_Policy\_Set\_1

#### 步驟 23.2.按一下>以輸入策略集。 為狀態相容、不相容和未知狀態建立新的授權規則。按一下Save。

#### 與compliant\_profile相容

#### 與non\_compliant\_profile不相容

#### 未知與unknown\_redirect

dealer Identity	y Service	es Engine					Work Cent	ters / Postu	ire				- 1-0		
Overview	Netwo	ork Devices Cl	lient Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
	٥	Firewall Posture		🖳 Nete	vork Access-Device IP Add	ress EQUALS :						Default Network Ad	cess	1	+ •
∽Aut	hentication	Policy(1)													
۲	Status	Rule Name	Conditions								Use			Hits	Actions
	Q Search														
							+								
											All_User_ID_	Stores	0		
	0	Default									> Options			48	(3)
> Aut	horization	Policy - Local Excepti	ons												
> Aut	horization I	Policy - Global Except	tions												
∨Aut	horization	Policy(4)													
									Results						
۲	Status	Rule Name	Conditions						Profiles		Security Group	ps		Hits	Actions
	Q Search														
	۲	Compliant	t: Session	PostureStatus EQUALS Cor	mpliant				compliant_profile	0+	Select from I	st	0+	15	<u>ئ</u>
	٥	Non_Compliant	b Session	PostureStatus EQUALS Nor	Compliant				non_compliant_profile	0+	Select from li	ist	0 +	5	(2)
	0	Unknown	E Session	PostureStatus EQUALS Unk	nown				unknown_redirect	1 +	Select from li	ist	0 +	47	(2)
	Overview ✓Aut →Aut →Aut	Overview Network Overv	Overview     Network Devices     Ci       Overview     Network Devices     Ci       Image: Status     Filewell Posture     Image: Status       Image: Status     Rule Name       Image: Status     Rule Name       Image: Status     Rule Name       Image: Status     Rule Name       Image: Authorization Policy - Local Except       Image: Authorization Policy - Local Except       Image: Authorization Policy - Global Except       Image: Authorization Policy(4)       Image: Status       Image: Status </td <td>Overview       Network Devices       Client Provisioning         Complexity       Prevail Posture         Authentication Policy(1)         Status       Rule Name         Conditions         Authorization Policy - Local Exceptions         Authorization Policy(4)</td> <th>Overview       Network Devices       Client Provisioning       Policy Elements            <ul> <li>Prevail Pasture</li> <li>Authentication Policy(1)</li> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Search</li> </ul> <ul> <li>Default</li> <li>Authorization Policy - Local Exceptions</li> <li>Authorization Policy - Global Exceptions</li> <li>Authorization Policy(4)</li> </ul> <ul> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Search</li> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Conditions</li> <li>Conditions</li> <li>Search</li> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Conditions</li> <li>Search</li> <li>Searc</li></ul></th> <td>Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy         Image: Status       Prevail Pasture       Image: Network Access Device IP Add         Image: Authentication Policy(1)       Image: Network Access Device IP Add         Image: Status       Rule Name       Conditions         Image: Status       Rule Name       Conditions         Image: Default       Image: Status       Network Access Device IP Add         Image: Authorization Policy(1)       Image: Status       Network Access Device IP Add         Image: Default       Image: Status       Conditions         Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status Clukter Add       Network Access Device IP Add         Image: Default       Image: Default       Image: Status Clukter Add       Network Access Device IP Add         Image: Default       Image: Status Clukter Add       Image: Status Clukter Add       Network Access Dev</td> <td>Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy       Policy Sets         Image: Status       Prevent Policy       Image: Status       Image: Status</td> <td>Work Cont       Overview       Network Devices       Client Provisioning       Policy Elements       Policy Sets       Troubleshoot         Image: Set Set Set Set Set Set Set Set Set Set</td> <td>dettitity Services Engine     Work Centers / Postur       Overview     Network Devices     Client Provisioning     Policy Elements     Posture Policy     Policy Sets     Troubleshoot     Reports       Image: Set of the set of the</td> <td>Utentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Posture Policy         Policy Sets         Troubleshoot         Reports         Settings</td> <td>Udentity Services Engine Work Centers / Posture     Overview Network Devices     Client Provisioning Policy Elements     Prevel     Prevel     V-Authorization Policy(1)          Status Rule Hame     Conditions           V-Authorization Policy(2)          Authorization Policy - Lecel Exceptions               V-Authorization Policy(2)  <td>Udentity Services Engine Vork Centers / Posture     Overview Network Devices     Centers     Prevail Pathine     Prevail Pa</td><td>Clanticity Services Engine Vork 2 Anter / Posture     Overview Network Davices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Image: Client Provisioning Policy Elements     Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements Image: Client Provisioning     Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements     Constant Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements     Constant Constant Constant Constant Constant Constant Constant     Constant   Constant Constant Constant Constant Constant Constant Constant             Constant   Constant Constant Constant Constant Constant      Constant Constant Constant Constant Constant         Co</td><td>Addression Policy - Local Exceptions Conditions Equilation Results   &gt; Authorization Policy - Local Exceptions &gt; Conditions &gt; Conditions   &gt; Authorization Policy - Local Exceptions &gt; Conditions &gt; Conditions   &gt; Status Rate Name Conditions &gt; Conditions   &gt; Conditions Conditions &gt; Conditions &gt; Conditions   &gt; Authorization Policy - Cocal Exceptions &gt; Conditions &gt; Conditions   &gt; Authorization Policy - Cocal Exceptions &gt; Conditions &gt; Conditions   &gt; Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Authorization Policy - Cocal Exceptions &gt; Conditions &gt; Conditions   &gt; Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Conditions Conditions Conditions Policy Exceptions   &gt; Conditions Conditions Conditions Conditions Policy Exceptions <td< td=""><td>Market Iddentify Services Engine Work Centers / Potture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Patient         &lt;</td></td<></td></td>	Overview       Network Devices       Client Provisioning         Complexity       Prevail Posture         Authentication Policy(1)         Status       Rule Name         Conditions         Authorization Policy - Local Exceptions         Authorization Policy(4)	Overview       Network Devices       Client Provisioning       Policy Elements <ul> <li>Prevail Pasture</li> <li>Authentication Policy(1)</li> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Search</li> </ul> <ul> <li>Default</li> <li>Authorization Policy - Local Exceptions</li> <li>Authorization Policy - Global Exceptions</li> <li>Authorization Policy(4)</li> </ul> <ul> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Search</li> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Conditions</li> <li>Conditions</li> <li>Search</li> <li>Status</li> <li>Rule Name</li> <li>Conditions</li> <li>Conditions</li> <li>Search</li> <li>Searc</li></ul>	Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy         Image: Status       Prevail Pasture       Image: Network Access Device IP Add         Image: Authentication Policy(1)       Image: Network Access Device IP Add         Image: Status       Rule Name       Conditions         Image: Status       Rule Name       Conditions         Image: Default       Image: Status       Network Access Device IP Add         Image: Authorization Policy(1)       Image: Status       Network Access Device IP Add         Image: Default       Image: Status       Conditions         Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status       Network Access Device IP Add         Image: Default       Image: Default       Image: Status Clukter Add       Network Access Device IP Add         Image: Default       Image: Default       Image: Status Clukter Add       Network Access Device IP Add         Image: Default       Image: Status Clukter Add       Image: Status Clukter Add       Network Access Dev	Overview       Network Devices       Client Provisioning       Policy Elements       Posture Policy       Policy Sets         Image: Status       Prevent Policy       Image: Status       Image: Status	Work Cont       Overview       Network Devices       Client Provisioning       Policy Elements       Policy Sets       Troubleshoot         Image: Set	dettitity Services Engine     Work Centers / Postur       Overview     Network Devices     Client Provisioning     Policy Elements     Posture Policy     Policy Sets     Troubleshoot     Reports       Image: Set of the	Utentity Services Engine         Work Centers / Posture           Overview         Network Devices         Client Provisioning         Policy Elements         Posture Policy         Policy Sets         Troubleshoot         Reports         Settings	Udentity Services Engine Work Centers / Posture     Overview Network Devices     Client Provisioning Policy Elements     Prevel     Prevel     V-Authorization Policy(1)          Status Rule Hame     Conditions           V-Authorization Policy(2)          Authorization Policy - Lecel Exceptions               V-Authorization Policy(2) <td>Udentity Services Engine Vork Centers / Posture     Overview Network Devices     Centers     Prevail Pathine     Prevail Pa</td> <td>Clanticity Services Engine Vork 2 Anter / Posture     Overview Network Davices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Image: Client Provisioning Policy Elements     Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements Image: Client Provisioning     Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements     Constant Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements     Constant Constant Constant Constant Constant Constant Constant     Constant   Constant Constant Constant Constant Constant Constant Constant             Constant   Constant Constant Constant Constant Constant      Constant Constant Constant Constant Constant         Co</td> <td>Addression Policy - Local Exceptions Conditions Equilation Results   &gt; Authorization Policy - Local Exceptions &gt; Conditions &gt; Conditions   &gt; Authorization Policy - Local Exceptions &gt; Conditions &gt; Conditions   &gt; Status Rate Name Conditions &gt; Conditions   &gt; Conditions Conditions &gt; Conditions &gt; Conditions   &gt; Authorization Policy - Cocal Exceptions &gt; Conditions &gt; Conditions   &gt; Authorization Policy - Cocal Exceptions &gt; Conditions &gt; Conditions   &gt; Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Authorization Policy - Cocal Exceptions &gt; Conditions &gt; Conditions   &gt; Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Conditions Conditions Policy Exceptions &gt; Conditions   &gt; Conditions Conditions Conditions Conditions Conditions Policy Exceptions   &gt; Conditions Conditions Conditions Conditions Policy Exceptions <td< td=""><td>Market Iddentify Services Engine Work Centers / Potture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Patient         &lt;</td></td<></td>	Udentity Services Engine Vork Centers / Posture     Overview Network Devices     Centers     Prevail Pathine     Prevail Pa	Clanticity Services Engine Vork 2 Anter / Posture     Overview Network Davices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings     Constant Image: Client Provisioning Policy Elements Policy Sets Image: Client Provisioning Policy Elements     Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements Image: Client Provisioning     Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements     Constant Constant Image: Client Provisioning Policy Elements Image: Client Provisioning Policy Elements     Constant Constant Constant Constant Constant Constant Constant     Constant   Constant Constant Constant Constant Constant Constant Constant             Constant   Constant Constant Constant Constant Constant      Constant Constant Constant Constant Constant         Co	Addression Policy - Local Exceptions Conditions Equilation Results   > Authorization Policy - Local Exceptions > Conditions > Conditions   > Authorization Policy - Local Exceptions > Conditions > Conditions   > Status Rate Name Conditions > Conditions   > Conditions Conditions > Conditions > Conditions   > Authorization Policy - Cocal Exceptions > Conditions > Conditions   > Authorization Policy - Cocal Exceptions > Conditions > Conditions   > Conditions Conditions Policy Exceptions > Conditions   > Authorization Policy - Cocal Exceptions > Conditions > Conditions   > Conditions Conditions Policy Exceptions > Conditions   > Conditions Conditions Policy Exceptions > Conditions   > Conditions Conditions Conditions Conditions Policy Exceptions > Conditions   > Conditions Conditions Conditions Conditions Policy Exceptions > Conditions   > Conditions Conditions Conditions Conditions Conditions Policy Exceptions   > Conditions Conditions Conditions Conditions Policy Exceptions <td< td=""><td>Market Iddentify Services Engine Work Centers / Potture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Patient         &lt;</td></td<>	Market Iddentify Services Engine Work Centers / Potture     Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings       Press Patient         <

ISE\_Add\_New\_Policy\_Set\_2

#### Ubuntu上的配置

步驟 24.透過GUI登入到Ubuntu客戶端。打開瀏覽器以登入VPN門戶。在本示例中,它是demo.example.com。

demo.ex	xam	nple.com/+CS	COEX	+			-	đ	×
$\leftarrow \rightarrow$	è	С	0 🗛	https://demo.example.com/	CSCOE+/logon.html#form_title_text	ដ	$\bigtriangledown$	$\mathbf{F}$	≡

Logon
Group posture_vpn v Username
Logon

Ubuntu\_Browser\_VPN\_Login

步驟 25.按一下Download for Linux。

Cisco Secure Client Installatio	+				- 6	×
$\leftarrow \rightarrow $ C (0	https://demo. <b>example.com</b> /CACHE/stc/2/index.html	E 80	% <b>公</b>	(C	) 🕹	≡
Secure Clie	t					
	Cisco Secure Client Download					4
	Download & Install					
	Download Cisco Secure Client and install it on your computer. Download for Linux	0	nstructior	IS		

Ubuntu\_Browser\_VPN\_Download\_1

下載的檔名為cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh。



Ubuntu\_Browser\_VPN\_Download\_2

步驟 26.透過瀏覽器下載VPN證書並將檔案重新命名為<certificate>.crt。以下是使用firefox下載憑證的範例。

-	demo.example.	com/+CSCOE× +	$\sim$		ē	×
$\leftarrow$	$\rightarrow$ C	Ttps://demo. <b>example.com</b> /+CSCOE+/logon.html#form_title_text	${igsidential}$	۲	பி	≡

Page Info — https://demo.	example.com/+CSC	DE+/logon.html#fo	orm_title_text _ D
General Media Permissions S	ecurity		
Website Identity Website: demo.example.com Owner: This website does not s Verified by: C=CN,CN=demo.examp	ipply ownership info e.com	rmation.	<u>V</u> iew Certificate
Privacy & History Have I visited this website prior to to	lay?	No	
Is this website storing information or	my computer?	Yes, cookies	<u>C</u> lear Cookies and Site Data
Have I saved any passwords for this w	ebsite?	No	Vie <u>w</u> Saved Passwords
Technical Details Connection Encrypted (TLS_AES_128 The page you are viewing was encryp Encryption makes it difficult for unau therefore unlikely that anyone read t	_GCM_SHA256, 128 b ted before being tran thorized people to vi his page as it traveled	bit keys, TLS 1.3) Insmitted over the In Tew information trav d across the network	ternet. eling between computers. It i c. Help

Ubuntu\_Browser\_VPN\_Cert\_Download

步驟 27.打開Ubuntu客戶端上的終端。導航到path home/user/Downloads/安裝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 ./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\$

步驟 28.信任Ubuntu客戶端上的VPN門戶證書。

<#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

步驟 29.在Ubuntu客戶端上打開Cisco Secure Client,然後成功將VPN連線到demo.example.com。

		Cisco Secure	Client		•		×
AnyConnect VPN     A Statistics     About							
		יו ויו cisc	11 0				
Connect to:	demo.exa	ample.com			~		\$
Group:	posture_v	pn				~	
Username:	isetest						
Password:	******						



 $Ubuntu\_Secure\_Client\_Connected$ 

步驟 30.打開瀏覽器以訪問觸發重定向至ISE CPP門戶的任何網站。從ISE CPP門戶下載證書並將檔案重新命名為<certificate>.crt。 以 下是使用Firefox進行下載的範例。



```
Ubuntu_Browser_CPP_Cert_Download
```

#### 步驟 30.1.信任Ubuntu客戶端上的ISE CPP門戶證書。

#### <#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.
```

步驟 31.在ISE CPP門戶上點選Start。

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

Ubuntu\_Browser\_CPP\_Start

### 步驟32. Click here to download and install Agent。

Device Security C	:heck × +	- @ ×						
$\leftarrow \   \rightarrow \   G$	https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL 🏠	$\boxtimes$						
🚺 You must log in	to this network before you can access the Internet.	×						
cisco.	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								
0	+ Remind me what to do next							

Ubuntu\_Browser\_CPP\_Download\_Posture

步驟 33.打開Ubuntu客戶端上的終端。導航到安裝終端安全評估模組的路徑home/user/Downloads/。

## <#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\_0NcLgcMURfyZmR6HoI

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.

步驟 34.在Ubuntu客戶端UI上,退出Cisco Secure Client並重新打開它。ISE終端安全評估模組安裝並成功運行。



Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed

步驟 35.打開Ubuntu客戶端上的終端。導航到路徑home/user/Desktop(這是您尋找快取缺失可以使用的隱藏命令),然後建立一個 test.txt檔案以滿足ISE上配置的檔案條件。

## <#root>

user@ubuntu22-desktop:~\$

#### cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

#### 驗證

使用本節內容,確認您的組態是否正常運作。

步驟 1.將VPN連線到Ubuntu客戶端上的demo.example.com。

	- • ×								
AnyCor	nnect VPN	🖊 Statist	ics	🍥 ISE Posture	About				
cisco									
Connect to: demo.example.com									
Group: posture_vpn									
Username:	isetest								
Password:	*******								

	🇞 Di	isconnect
Connected to demo.example.c	om.	

驗證\_Ubuntu\_安全\_客戶端\_已連線

步驟 2.檢查Ubuntu客戶端上的ISE終端安全評估狀態。



Verify\_Ubuntu\_Secure\_Client\_Compliance

#### 步驟 3.檢查ISE上的Radius Live Log。導航到Operations > RADIUS Live Log。

=	dentity Services Engine			Opera	ations / RADIUS			
Ц	Live Logs Live Sessions							
::								
ы о	Misconfigured Supplicants 🕕	Miscor	figured Network Dev	ices 🕕	RADIUS Drops		Client Stopped Responding ①	Repeat Counter ①
*	0		0		0		0	0
U							Refresh Show	Within
a.							Never v Latest 20 re	cords 🗸 Last 24 hours 🗸
đ	💭 🖕 Reset Repeat Counts ්	🗅 Export To 🗸						Filter 🗸 🐵
	Time	Status Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	Authorization Policy
?		~	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
	May 29, 2024 09:08:48.798 PM	۵	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default F	irewall Posture >> Compliant
	May 29, 2024 09:08:48.798 PM			52:54:00:17:6B:FA		Compliant	Firewall Posture	irewall Posture >> Compliant
	May 29, 2024 09:08:13.570 PM		isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default F	irewall Posture >> Unknown

驗證\_ISE\_LiveLog

步驟 4.透過SSH或主控台導覽至FTD CLI。

#### <#root>

>

>

```
system support diagnostic-cli
```

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

ftdv741>

enable

Password: ftdv741# ftdv741#

show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
```

```
Username : isetest Index : 33
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 51596 Bytes Rx : 17606
Pkts Tx : 107 Pkts Rx : 136
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : posture_gp Tunnel Group : posture_vpn
Login Time : 14:02:25 UTC Fri May 31 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb007182000210006659d871
Security Grp : none Tunnel Zone : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 33.1
Public IP : 192.168.10.13
Encryption : none Hashing : none
TCP Src Port : 59180 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : linux-64
Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)
```

Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 6364 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 33.2 Assigned IP :192.168.6.30 Public IP : 192.168.10.13 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS\_AES\_128\_GCM\_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 59182 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Linux\_64 Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 6364 Bytes Rx : 498 Pkts Tx : 1 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3 DTLS-Tunnel: Tunnel ID : 33.3 Assigned IP :192.168.6.30 Public IP : 192.168.10.13 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56078 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Linux\_64 Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 38868 Bytes Rx : 17108 Pkts Tx : 105 Pkts Rx : 130 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

#### 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

對於終端安全評估流程和思科安全客戶端和ISE故障排除,請檢查CCO<u>文檔ISE終端安全評估樣式比較2.2之前和之後的比較</u>以及 <u>ISE會話管理和終端安全評估故障排除</u>。

相關資訊

- <u>思科身份服務引擎管理員指南3.3版</u>
- <u>思科技術支援與下載</u>

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。