Configurare la postura della VPN Linux con ISE 3.3

Sommario
Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione
Esempio di rete
Configurazioni su FMC/FTD
Configurazioni su ISE
Configurazioni su Ubuntu
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

Questo documento descrive come configurare la postura della VPN Linux con Identity Services Engine (ISE) e Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Client
- VPN ad accesso remoto su Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- 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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione



Esempio di rete

Topologia

Configurazioni su FMC/FTD

Passaggio 1. Configurazione della connettività tra client, FTD, FMC e ISE completata. Come enroll.cisco.com si usa per gli endpoint che eseguono la sonda per il reindirizzamento (per i dettagli, fare riferimento ai <u>documenti</u> CCO del flusso di postura <u>e al confronto degli stili di postura</u> <u>ISE per le versioni precedenti e successive</u> alla <u>2.2</u>). Verificare che il percorso del traffico verso enroll.cisco.com su FTD sia configurato correttamente.

Passaggio 2. Scaricare il nome del pacchetto cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg da <u>Cisco Software</u> <u>Download</u> e assicurarsi che il file sia valido dopo il download confermando che il checksum md5 del file scaricato è lo stesso della pagina di download del software Cisco.

Passaggio 3. Passare a Objects > Object Management > VPN > Secure Client File. Fare clic suAdd Secure Client File, fornire il nome, sfogliare File Name per selezionare cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, selezionare Secure Client Image in elenco a discesaFile Type. Quindi fate clic su Save.

Firewall Management	t Center Overview Analysis Policie	as Devices Objects Integration		Deploy	९ 🗳 🌣 🔕 admin v	ence SECURE
> Distinguished Name DNS Server Group	Secure Client File			Add Secure	Client File Q, Filter	
> External Attributes File List	File objects represent files used for remote access V	/PN policy configurations. They can contain Secure Client profile and image files.				
> FlexConfig Geolocation		Add Secure Client File	0			
Interface	Name				Туре	
Key Chain Network	client_image	Name:*		n-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	1/1
> ркі	Default-External-Browser-package	linux_5_1_3_62		36-webdeploy-k9.zip	Secure Client External Browser Pa	± 9, ≣
Policy List	hostscan5_1_3_62			1-5.1.3.62-k9.pkg	HostScan Package	1/1
Port > Prediv 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 Brow	vse			
> Security Intelligence						
Sinkhole		File Type:*				
SLA Monitor		Secure Client Image				
Time Range						
Turnel Zone		Description:				
URL						
Variable Set						
VLAN Tag						
V VPN						
Certificate Map						
Custom Attribute		Cance	Save			
Group Policy		Canoo				
KEV1 Polev						
IKEv2 IPsec Proposal						
IKEv2 Policy						
Secure Client Customizatio				Displa	aying 1 - 4 of 4 rows IC C Page 1	of 1 > > I C

Immagine_client_caricamento_protetto_FMC

Passaggio 4. Passare a Objects > Object Management > Network.

Passaggio 4.1. Creare un oggetto per il server DNS. Fare clic su Add Object, specificare il nome e l'indirizzo IP DNS disponibile. Fare clic su .Save

more IP addresses. Network objects are used in various places, including acces New Network Object Name	sss control policies, network variables, intrusion rules, identity rule	Add Network Add Object Import Object Add Group Value Value 200 0.0 0/0	C, Filter Show Unused C orts, and so on. Type Override	Xbjects
New Network Object	0	Value 0.0.0.0/0 ::/0	Type Override	
New Network Object	0	0.0.0.0/0 ::/0		
Name			Group	¶. Q ⊕ M
Name		0.0.0/0	Network	¶. q. ⊕. M.
Description Network Host Range Network				
	Allow Overrides	Allow Overrides	Allow Overrides	Cancel Save

FMC_Aggiungi_Oggetto_DNS



Nota: il server DNS configurato qui deve essere utilizzato per gli utenti VPN.

Passaggio 4.2. Crea un oggetto per ISE PSN. Fare clic su Add Object, fornire il nome e l'indirizzo IP PSN ISE disponibile. Fare clic su .Save

Firewall Management	t Center Overview Analysis Polic	ies Devices Objects Integration		Deploy	९ 💕 🌣 😰 🛛 admin	osce SECURE
Distinguished Name DNS Server Group External Attributes	Network			Add Network Add Ob	Q. Filter	Objects
File List > FlexConfig	A network object represents one or more IP addre	sses. Network objects are used in various places, including acce	ss control policies, network variables, intrusi	on rules, identity rules, network discovery rule Add Gn	Object orts, and so on. oup	
Geolocation	Name	New Network Object	0	Value	Type Override	
Interface	any	New Network Object		0.0.0.0/0 ::/0	Group	¶a. ≣ &
Key Chain	any-ipv4	News		0.0.0.0/0	Network	¶g Q ⊕ 85
		Name	1			
		Description				
		Network				
		Host Range Network	O FQDN			
]			
		Allow Overrides	-			
			Cancel Save			

FMC_Add_Object_ISE

Passaggio 5. Passare a Objects > Object Management > VPN > Group Policy. Fare clic su .Add Group Policy Fare clic su DNS/WINS, selezionare l'oggetto del server DNS in Primary DNS Server. Quindi fate clic su Save.

Firewall Management Objects / Object Management	t Center Overview Analysis Policies	Devices Objects Integration		Deploy Q 🥩 🌣 🕢 admin 🗸 📩
Distinguished Name DNS Server Group External Attributes File List	Group Policy A Group Policy is a set of attribute and value pairs, st	pred in a group policy object, that define the remote access VP	N experience. The RADIUS authorization server assigns the group policy or it is of	Add Group Policy Q, Filter
> FlexConfig Geolocation	Name			
Key Chain Network > PKI Policy List Port > Prefix List Route Map > Security Intelligence Sinkhole SLA Monitor Time Zone Time Zone TumeI Zone URL Variable Set VLAN Tag > VPN Certificate Map Custom Attribute Group Policy IKEy1 IPsec Proposal		Name:" posture_gp Description: General Secure Client Advanced VPN Protocols Primary DNS Server: DNS/WINS Split Tunneling Primary WINS Server: DHCP Network Scipe: DHCP Network Scipe: DHCP Network Scipe: Default Domain:		/1
IKEv1 Policy IKEv2 IPsec Proposal IKEv2 Policy Secure Client Customizatio Secure Client File			Cancel	Displaying 1 - 2 of 2 rows $ < < Page 1 of 1 > C$

FMC_Add_Group_Policy



Nota: verificare che il server DNS utilizzato in Criteri di gruppo VPN sia in grado di risolvere il nome di dominio completo del portale di provisioning dei client ISE e enroll.cisco.com.

Passaggio 6. Passare a Objects > Object Management > Access List > Extended. Fare clic su .Add Extended Access List

Firewall Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🚱 admin V 付 SECURE
 AAA Server RADIUS Server Group 	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
Single Sign-on Server Access List Extended	An access as object, nor shown as an access constraint (object, since a net owners) a stress in a ppg, climitation for many owners and the constraint of the	Override

FMC_Add_Redirect_ACL

Passaggio 6.1. Specificare il nome dell'ACL di reindirizzamento. Questo nome deve essere uguale a quello specificato nel profilo di

autorizzazione ISE. Fare clic su .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 Ov	errides								

FMC_Add_Redirect_ACL_Part_1

Passaggio 6.2. Blocca il traffico DNS, il traffico verso l'indirizzo IP PSN ISE e i server di correzione per escluderli dal reindirizzamento. Consentire il resto del traffico. Questo attiva il reindirizzamento. Fare clic su .Save

Add Extended Access List Entry			0
Action: Block Logging: Default			
Log Level:			
Informational v			
Log Interval: 300 Sec.			
Network Port 0 Application 1 Users 0 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			
IPv4-Private-All-RFC1918 Add to Destination			
IPv6-Link-Local			
IPv6-Private-Unique-Local-Addresses			
IPv6-to-IPv4-Relay-Anycast			
rtp_ise	Enter an IP address Add	Enter an IP address	Add

FMC_Add_Redirect_ACL_Part_2

Cancel Save

Cancel

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 On	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	/1

Cancel Save

 $FMC_Add_Redirect_ACL_Part_3$



Nota: come esempio del server di monitoraggio e aggiornamento viene utilizzato l'FTP di destinazione in questo esempio di ACL di

Firewall Management Center Ph Q 🚱 Overview Analysis Policies Devices Objects Integration **RADIUS Server Group** AAA S RADIUS Server Gro ntain one or more references to RADIUS Servers. These AAA se cess VPN conne ale Si Name Value

Passaggio 7. Passare a Objects > Object Management > RADIUS Server Group. Fare clic su .Add RADIUS Server Group

FMC_Add_New_Radius_Server_Group

Passaggio 7.1. Fornire nome, controlloEnable authorize only, controllo Enable interim account update, controllo Enable dynamic authorization.

Name:*	_		
rtpise			
Description:			
Group Accounting Mode:			
Single	•		
Retry Interval:* (1-10) Seconds			
10			
Realms:			
	•		
Enable authorize only			
Enable interim account update			
Interval:* (1-120) hours			
24			
Enable dynamic authorization			
Port:* (1024-65535)			
		Cancel	Save
		Cancer	Save

 $FMC_Add_New_Radius_Server_Group_Part$

Passaggio 7.2. Fare clic sull'Plus icona per aggiungere un nuovo server RADIUS. Fornire il numero di serie del servizio (PSN)IP Address/Hostname, Key per l'ISE. Selezionare il nome per la specific interface connessione. Selezionare la Redirect ACLvoce. Quindi fare clic su Saveper salvare il nuovo server radius. Quindi fare nuovamente clicSave su per salvare il nuovo gruppo di server radius.

?

IP Address/Hostname I Address/Hostname I P Address/Hostname	Add RADIUS Server Group	0	New RADIUS Server	0
Configure DAS at Threat Defense Platform Settings to resolve hostname Interval:* (1-120) hours 24 [1812 © Enable dynamic authorization Port:* (1024-65535) 1700 Omerge Downloadable ACL with Cisco AV Pair ACL © After Cisco AV Pair ACL © After Cisco AV Pair ACL Before Cisco AV Pair ACL (1-65535) (1-65535) 1700 Dranker IP Address/Hostname No records to display Headings to display Address./Lostname	Enable authorize only		IP Address/Hostname:*	
Instable dynamic authorization Port:* (1024-65535) 1700 Merge Downloadable ACL with Clisco AV Pair ACL Image Downloadable ACL with Clisco AV Pair ACL	Enable interim account update Interval:* (1-120) hours 24		Configure DNS at Threat Defense Platform Settings to resolve hostname Authentication Port:* (1-65535) 1812 Kev:*	
	Enable dynamic authorization Port:* (1024-65535) 1700 Merge Downloadable ACL with Cisco AV Pair ACL		Confirm Keyr* Accounting Port: (1-65535)	
IP Address/Hostname Connect using: No records to display No records to display Redirect ACL:	After Cisco AV Pair ACL Before Cisco AV Pair ACL RADIUS Servers (Maximum 16 servers)	+	1813 Timeout: (1-300) Seconds 10	
	IP Address/Hostname No records to display		Connect using: Routing Specific Interface Inside_zone Redirect ACL:	
Cancel Save		Cancel Save	redirect • +	Save

FMC_Add_New_Radius_Server_Group_Part

Passaggio 8. Passare a Objects > Object Management > Address Pools > IPv4 Pools. Fare clic su Add IPv4 Pools e specificare **Name, IPv4** Address **Range**e Mask. Quindi fate clic su Save.

Firewall Managen Objects / Object Managen	nent Center Overview Analysis Policies Devices	Objects Integration	Deploy Q 💕 🌣 🔕 fangni "Indo SECUI
> AAA Server > Access List > Address Pools	IPv4 Pools	nostic interface with clustering, or for VPN remote access profiles.	Add IPv4 Pools Q, Filter
I'NG Pools Application Fiters AS Path BFD Template Cipher State List DHOP IPA6 Pool Distinguished Name DNS Serviced Roup DNS Serviced Roup DNS Serviced Name DNS Serviced Name Pool Distribution Pool Distribution Pool Distribution Route Map	Norme of posture_pool_97_0	Add IPv4 Pool Name* posture_pool Description IPv4 Address Range* 192.168.6.300-192.168.6.100 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150 Mask* 255.255.255.0 C Allow Overrides C Onfigure device overrides in the address pool object to avoid IP address conflicts in case of object to shared devices C Override (0)	Overdas Image: Control of the second seco
> Security Intelligence SinAMonitor Time Range Time Zone Tunnel Zone URL URL Variable Set		Cancel	Save Displaying 1 - 2 of 2 rows. IC < Page 1 of 1 > 31 C

FMC_Add_New_Pool

Passaggio 9. Passare a Certificate Objects > Object Management > PKI > Cert Enrollment. Fare clic suAdd Cert Enrollment, fornire un nome e selezionare Self Signed Certificatein Enrollment Type. Fare clic sulla Certificate Parameters scheda e specificare Common Name e Country Code. Quindi fate clic su Save.

Firewall Management Objects / Object Management	t Center Overview Analysis Policies Devic	es Objects Integration		Deploy Q 🚱 🗘 🕢 fangni
AAA Server Access List Address Pools Angleation Filters	Cert Enrollment A certificate enrollment object contains the Certification Authority your Private Key Infrastructure (PKI).	(CA) server information and enrollment parameters	that are required for creating Certificate Signing Requests (CSRs) and obtaining	Add Cert Enrollment Q, Filter
AS Path BFD Template	Name			Type Override
Cipher Suite List > Community List DHCP IPv6 Pool > Distinguished Name DNS Server Group > External Attributes File List > FlaxConfig Geolocation Interface Key Chain Network > PKI Cert Enrollment External Cert Groups Internal CA Groups Internal CAS Internal CAS	Name* @emo_spn Description CA Information Certificate Parameters Key Revoc Enrollment Type: Salt Signed Certificate VPN: To compare CA, Inservingte to "Certificate Parameters Validation Usage: Validation Usage: © Psec Client: SSI Client	ation	PLOU VEIT EITHOMITTERN Name* demo_vpin Description CA Information Certificate Parameters Key Revocation Include PQDN: Don't use PQDN in certificate Include PqUNca's IP Address: Common Name (CM): Common Name (CM): Common Name (CM): State (ST): Country Code (C): CN Email (L): Include Device's Serial Number	m m m
Trusted CAs Policy List	Allow Overrides		Allow Overrides	
Port Prefix List Route Map Security Intelligence		Cancel Save		Cancel Seve Displaying 1 - 3 of 3 rows I < < Page 1 of 1 >> I C

FMC_Add_New_Cert_Enroll

Passaggio 10. Passare a Devices > Certificates. Fare clic suAdd, selezionare il nome FTD in Device, selezionare l'iscrizione configurata in precedenza in Cert Enrollment. Fare clic su Add

Firewall Managem Devices / Certificates	ent Center	Overview Analysis	Policies Devices	Objects	Integration		Deplo	y Q 💰	00	fangni v diada SECU
Filter All Certificates	٠									Add
Name	Domain	Enrollment Type	Identity Certificate Expiry		CA Certificate Expiry	Status				
Add New Cert	ificate			6						•
Add New Och	incuto					G CA LD				± ₽ C ∎
Add a new certific	ate to the devic	e using cert enr	ollment object which	is used to		G CA LD				± ₽ C ∎
generate CA and i	dentify certifica	te.								-
Device*:						O CA LD				± @ C ∎
Posture-FTD-Cf	VL27	*								
Cost Forella cott										
demo und		- +								
denio_vpr		• +								
Cert Enrollment De	etails:									
Name:	demo_vpn									
Enrollment Type:	Self-Signe	d								
Enrollment URL:	N/A									
			Cancel	Add						

FMC_Add_New_Cert_To_FTD

Passaggio 11. Passare a Devices > VPN > Remote Access. Fare clic su .Add

Passaggio 11.1. Fornire il nome e aggiungere l'FTD a Selected Devices. Fare clic su .Next

Firewall Management Center Overview	Analysis Policies Devices Objects Integration		Deploy Q 🧬 🌣 🔕 admin 🗸 📫 SECURE
Firewall Management Center Devices / VEW / Senze Woard Memote Access VPN Policy Wizard Policy Assignment 2 Connection Profile	Analysis Policies Devices Objects integration 3 Secure Client 4 Access & Certificate 6 Summary Targeted Devices and Protocols This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile. Name::	Before You Start Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy. Authentication Server Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN Client download it during the wizard. Device Interface	Deploy Q
	 Sst. Piser-KEv2 Targeted Devices Q. Search Posture-FTD-CML27 VPN-FTD-Posture-CML: 	Interface that they can be used as a security zone or interface Interface build will well with the security zone or interface build be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.	
			Cancel Back Next

FMC_New_RAVPN_Wizard_1

Passaggio 11.2. Selezionare il gruppo di server radius configurato in precedenza in Authentication Server, Authorization Server, Accounting Server. Scorrere la pagina verso il basso.

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 😡 admin v 👘 SECURE
Remote Access VPN Policy Wizard	
1) Policy Assignment Connection Profile Secure Client Access & Certificate Summary	
Secure Clerit Understand Secure Clerit Understand Connection Profile Connection Profiles Connection Profile is specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itset, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* 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:* Tipise UCUAL or Health or HAUNUS) Failback to LOCAL Authentication	
Authorization Server: replace +	
Accounting Server:	
Client Address Assignment:	
	Cancel Back Next

$FMC_New_RAVPN_Wizard_2$

Passaggio 11.3. Selezionare il nome del pool configurato in precedenza in IPv4 Address Pools. Selezionare Criteri di gruppo configurati in precedenza in Group Policy. Fare clic su Next.

Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 💞 🌣 🔕 admin 🗸 🖏 SECU
Remote Access VPN Policy Wizard		
Policy Assignment (2) Connection Profile (3) Secure Client	Access & Certificate (5) Summary	
•	(Realm or RADIUS)	
	Accounting Server: ripsie (0AOUS)	
	Client Address Assignment:	
	Clent IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.	
	Use AAA Server (Realm or RADIUS only)	
	Use DHCP Servers	
	Use IP Address Pools	
	IPv4 Address Pools: 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:* postere_ap +	
	Edit Group Policy	

Cancel Back Next

FMC_New_RAVPN_Wizard_3

Passaggio 11.4. Selezionare la casella di controllo dell'immagine Linux. Fare clic su .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 Cl	ent 4 Access & Certificate _	5 Summary		
	Remote User Client	Internet Outside VPM	e Inside Corporate Resources	
	Secure Client Image			
	The VPN gateway can automatically di connection is initiated. Minimize connect	ownload the latest Secure Client package to t ion setup time by choosing the appropriate OS fo	the client device when the VPN in the selected package.	
	Download Secure Client packages from	Cisco Software Download Center.		
			Show Re-order buttons +	
	Secure Client File Object Name	Secure Client Package Name	Operating System	
	client_image	cisco-secure-client-win-5.1.3.62-webdeplo	Windows *	
	Enux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux 👻	

Cancel Back Next

 $FMC_New_RAVPN_Wizard_4$

Passaggio 11.5. Selezionare l'interfaccia dell'interfaccia VPN. Selezionare l'iscrizione certificato registrata in FTD nel passaggio 9. Fare clic su .Next



Cancel Back Next

FMC_New_RAVPN_Wizard_5

Passaggio 11.6. Confermare le informazioni correlate nella pagina di riepilogo. Se tutto funziona, fare clic su Finish. Se è necessario apportare modifiche, fare clic su Back.





Passaggio 12. Distribuire la nuova configurazione in FTD per completare la configurazione della VPN di accesso remoto.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy 🔍 💞 🌣 🕲	admin ~ dode SECURE
posture_vpn			Q Advanced Deploy A Ignore warm	tings Deploy Cancel
hoarna rear			Posture-FTD-CML27 Ready for	Deployment vents.(1)
Connection Profile Access Interfaces Advanced				ty: None
				+
Namo	АЛА	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	Dft:GrpPolicy		
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	E posture_gp	1 selected @ 1 pending	20

FMC_Deploy_FTD

Configurazioni su ISE

Passaggio 13. Passare a Work Centers > Posture > Network Devices. Fare clic su .Add

=	diale Identity Services I	Engine					Work Centers	Posture				Q	۵	0	Q	۹
н	Bookmarks	Overview	Network Devi	ces	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
-	Dashboard															
명	Context Visibility	Net	work Dev	ices												
×	Operations											s	elected 0	Total 4	Ø	٥
0	Policy	Ø Edit	+ Add () 0	uplicate	🕁 Import 🛛 🖞 Export 🖻	C Generate PAC	0 Delete 🗸							1	a Y	V
8.	Administration		Name ^ IP	P/Mask	Profile Name	Location	Type		Description							
	Work Contors	0	FTD-CML2		🟥 Cisco 🕕	All Locations	Firewall									
-	HOIR CONTON	0	FTD-CML2	-	🟥 Cisco 🕕	All Locations	Firewall									
		0	FTD+CML2 (🟥 Cisco 🕕	All Locations	Firewall									
0	Interactive Help		8,000,0		🟥 Cisco 🕠	All Locations	Firewall									

ISE_Add_New_Devices

Passaggio 13.1. Fornire le informazioni Name, IP Addresse scorrere la pagina verso il basso.

≡ du	dentity Service	es Engine				w	ork Centers / I	Posture		
н	Overview Netwo	ork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Ⅲ 回 火 ●	Network Devices Lis Network Devic Name Description	> New Network D es posture-FTD	evice	_						
20 Al	IP Addres	s 🗸 * IP :	/ 32	2	¢					
?	Device Profile	👬 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

Passaggio 13.2. Selezionare la casella di spunta di RADIUS Authentication Settings. Fornire il Shared Secret. Fare clic su .Submit

$\equiv \frac{-d_{\rm bolds}}{c_{ m orce}}$ Identity Ser	rvices Engine					•	Vork Centers / P	osture			۵ ۵	0 Q A
JI Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings			
E Dashboard		~ RADIUS Authent	lication Settings									
Pd Context Visibility	_	RADIUS UDP Setting	5									
Operations		Protocol RA	DIUS									
 Administration 		Shared Secret		Show								
J Work Centers		Use Second Shared	Secret ()									
		Secre			Show							
③ Interactive Help		CoA Port 12	700	Set To Defa	an a							
		RADIUS DTLS Setting	ps 🕕									
		DTLS Required										
		Shared Secret rad	lius/dtls									
		CoA Port 21	083	Set To Defa	a							
		Certificates for CoA S	elect if required (optional)	~ <u>o</u>								
		DNS Name										
		General Settings										
		🗌 Enable KeyWrap 💿										
		Key Encryption Key		Show								
		Message Authenticator Code Key		Show								
		Key Input Format ASCII O HEXA	DECIMAL									
		V TACACS Authen	tication Settings									
		 Advanced Trusts 	Sec Settings									
											Submit	Cancel

ISE_Add_New_Devices_2

Passaggio 14. Scaricare il nome del pacchetto cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg da <u>Cisco Software</u> <u>Download</u> e accertarsi che il file sia valido confermando che il checksum md5 del file scaricato è lo stesso della pagina di download del software Cisco. Download del nomecisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg del pacchetto completato nel passaggio 1.

Passaggio 15. Passare a Work Centers > Posture > Client Provisioning > Resources. Fare clic su .Add Selezionare Agent resources from local disk.

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings Image: Client Provisioning Policy Client Provisioning Policy Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
Client Provisioning Policy	
Resources Resources Select	ted 0 Total 16 📿 All 🗸 🛛 🏹
Agent resources from Cisco site Type Version Last Update	Description
Agent resources from local disk WinSPWizard 3.2.0.1 2023/07/04 06:54:02	Supplicant Prov
Native Supplicant Profile Native Supplicant Pro Not Applic 2016/10/07 04:01:12	Pre-configurec
Agent Configuration Native Supplicant Pro Not Applic 2023/07/04 07:55:16	Pre-configurec
Pagent Posture Profile MacOsXSPWizard 2.7.0.1 2023/07/04 06:54:02	Supplicant Prov
AMP Enabler Profile 5.1.3.062 CiscoSecureClientDe 5.1.3.62 2024/05/08 10:20:06	Cisco Secure C
CiscoSecureClientDesktopLinux 5.1.3.062 CiscoSecureClientDe 5.1.3.62 2024/05/08 10:31:28	Cisco Secure C
CiscoSecureClientComplianceModuleWindows 4.3.4015.8192 CiscoSecureClientCo 4.3.4015 2024/05/08 10:26:57	Cisco Secure C
CiscoSecureClientComplianceModuleLinux 4.3.3139.0 CiscoSecureClientCo 4.3.3139.0 2024/05/08 10:34:00	Cisco Secure C
CiscoAgentlessWindows 5.0.03061 CiscoAgentlessWind 5.0.3061.0 2023/07/04 06:54:10	With CM: 4.3.3
CiscoAgentlessOSX 5.0.03061 CiscoAgentlessOSX 5.0.3061.0 2023/07/04 06:54:14	With CM: 4.3.3
CiscoTemporalAgentWindows 5.0.03061 CiscoTemporalAgent 5.0.3061.0 2023/07/04 06:54:03	With CM: 4.3.3
CiscoTemporalAgentOSX 5.0.03061 CiscoTemporalAgent 5.0.3061.0 2023/07/04 06:54:07	With CM: 4.3.3

 $ISE_Upload_Resource$

Passaggio 15.1. Selezionare Cisco Provided Package. Fare clicChoose File per caricare cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Fare clic su .Submit

=	dentity Services E	ngine		Work Centers / Posture	Q	426	0	\$	A
三 川 三 小 三 一 三 一 三 一 三 一 三 一 三 一 三 一 三 一 二 二 一 二 二 二 二	Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local D Agent Resources Fro Category	Work Centers / Posture Disk > Agent Resources Frem Local Disk: um Local Disk Cisco Provided Package Cisco Provided Package Choose File Cisco-secureeploy-k9.pkg Choose File Cisco-secureeploy-k9.pkg Agent Uploaded Resources Name Type Version Description	Q			4	
			Submit	ancel					

ISE_Upload_Resources_1



Nota: ripetere il passo 14. per caricare cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

Passaggio 16. Passare a Work Centers > Posture > Client Provisioning > Resources. Fare clic su .Add Selezionare Agent Posture Profile.

≡ :	listo Identity Services Engine				Work Cent	ers / Posture				
Щ.	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy S	Sets Troubleshoo	t Reports Se	ettings		
10 10	Client Provisioning Policy Resources Client Provisioning Portal	Resources								
×	Cilent Provisioning Portai								Selected 0 Total 16	Ø
		🖉 Edit 🛛 🕂 Add 🔿	🚺 Duplicate 🛛 📋 De	lete					$_{\rm All}\sim$	∇
ж		Agent re:	sources from Cisco site	,	Version	Last Update	Description			
		Agent res	ources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client fo	or li		
-file		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 Li	nu		
?		Agent Po	sture Profile	ntProfile	Not Applic	2024/05/08 10:37:17				
		AMP Ena	bler Profile	ntProfile	Not Applic	2024/05/16 15:15:49				

ISE_Add_Agent_Posture_Profile

Passaggio 16.1. Fornire il Name, Server name rules e mantenere il resto come valore predefinito. Fare clic su .Save

Nome: linux_agent_profile

Regole nome server: *.example.com

≡ :#	dentity	Services Engine			W	ork Centers /	Posture			
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ ⅠⅠ ※ ● ▲₀	Client Provis Resources Client Provis	ioning Policy Ioning Portal	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	e						
٢			Agent Behavior Parameter Enable debug log		Value No V	D	escription	on the agent		

ISE_Add_Agent_Posture_Profile_1

≡ :	sco Identity	Services Engine			w	ork Centers / F	Posture		
FI.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provis Resources	ioning Policy	Posture Protocol						
×	Client Provis	ioning Portal	Parameter	Value			Description		
0			PRA retransmission ti	me 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	ds) to wait bef	lore retrying.
ส์เ			Retransmission Limit	① <u>4</u>			Number of retr	ies allowed for	r a message.
?			Discovery host ()				Enter any IP ac detects and re portal.	Idress or FQDN directs that htt	N that is routed through a NAD. The NAD p traffic to the Client Provisioning
			Discovery Backup Ser	ver List Choose	9		By default, An PSNs sequenti as the backup discovery prob	Connect sends ally if the PSN list and restrict es.	s discovery probes to all the Cisco ISE is unreachable. Choose specific PSNs t the nodes to which AnyConnect sends
			Server name rules * () •.examp	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 tect to if the PSN that authenticated the some reason.
			Back-off Timer ①	30	secs		Agent will cont targets and pro packets till this	tinuously try to eviously connects max time limit	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
									Cancel

ISE_Add_Agent_Posture_Profile_2

Passaggio 17. Passare a Work Centers > Posture > Client Provisioning > Resources. Fare clic su .Add Selezionare Agent Configuration.

= :	lister Identity S	ervices Engine				Work Cent	ers / Posture				
щ	Overview	Network Devices	Client Prov	visioning Policy Elements	Posture Policy	/ Policy	Sets Troublesho	ot Reports	Settings		
	Client Provisio Resources	ning Policy	Reso	urces							
×	Client Provisio	ning Portal								Selected 0 Total 16	Ø
			🖉 Edit -	+ Add 🔨 📋 Duplicate 🛛 👔 (Delete					All 😒	∇
U.				Anant 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	t for li		Т
-fit				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nat	ive S.		-1
				Agent Configuration	oSecureClientCo	4 3 3139 0	2024/05/08 10:34:00	Cisco Secure Client	Linu		-1
(?)				Agent Posture Profile		Not Applie	2024/05/00 10:04:00	01300 000010 011011			-1
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/08 10:37:17				-1
				cont canada riollite	ntProfile	Not Applic	2024/05/16 15:15:49				_

ISE_Add_Agent_Configuration

Passaggio 17.2. Configurare i dettagli:

Seleziona pacchetto agente: CiscoSecureClientDesktopLinux 5.1.3.062

Nome: linux_agent_config

Modulo conformità: Cisco Secure Client Compliance Module Linux 4.3.3139.0

Selezionare la casella di controllo VPN, Diagnostic and Reporting Tool

Selezione profilo ISE Posture: linux_agent_profile

Fare clic su .Submit

≡ :	inde Identity	Services Engine					Work Cent	ters / Postu	re
Щ.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provis	ioning Policy					1		
14	Resources		* Select Agent Package:	Ci	scoSecureClientDesktopLin	nux 5.1.3.062 🗸 🗸			
×	Client Provis	ioning Portal	* Configuration Name:						
0			linux_agent_config						
80			Description:						
កា				le					
(?)			Description Value N	otes					
			* Compliance Module CiscoSecu	reClientComplianceModule	Linux 4.3. ~				
			Cisco Secure Client	Module Selection					
			ISE Posture 🛛 VPN 🗹						
			Secure Firewall Dosture						
			Network Disibility						
			Diagnostic and Reporting 🔽 Tool						
			Profile Selection						
			* ISE Posture linux_agen	at_profile	Ý			S	ubmit Cance

ISE_Add_Agent_Configuration_1

Passaggio 18. Passare a Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Fare clic Edit alla fine del nome di una regola. Selezionare Insert new policy below.

≡ ::	isco Identity	Services E	ingine									w	ork C	enters / Postur	e				
щ	Overview	Network I	Devices	Clie	nt Provis	sioning	Policy Elemen	nts	Posture Polic	V	Policy Sets	Troubl	eshoo	t Reports	Settings				
11日 1日 火 日 品。	Client Provis Resources Client Provis	ioning Policy		CI Defir For A For N Wind Intel For M Mac If you with	ient f Agent Coni Vative Sup Jows Agen architectu Windows A ARM64 pr u configur out an ARI	Provision figuration: v plicant Con Mt, Mac Agei rres. Mac po Agent ARM6 policies requi e an ARM64	ioning Policy to deter ersion of agent, ar figuration: wizard p nt, Mac Temporal a blicles run the sam 4 policies, configu e no Other Condi c client provisionin n. This is because	min gent profi and e pa re S tion: g pc e an	e what users will recu profile, agent compl le and/or wizard. Dra Mac Agentless polici ackage for both architi ession: OS-Architect a arm64 configuration licy for an OS, ensur endpoint is matched	eive u g and g and secture cure E0 is, e that seque	pon login and use module, and/or ay drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 policy entially with the policy	r session i gent custo nge the or dows polit he Other O r is at the i plicies liste	initiation mization rder. cies run Conditio top of ti ed in thi	n n package. separate packages ins column. he conditions list, at s window.	for ARM4 and read of policies				
				\sim															
?						Rule Name	,		Identity Groups		Operating Syst	ems		Other Conditions			Result	ts	
						IOS		H	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-I	ISE-NSP	Edit 😔
				8		Android		Ħ	Any	and	Android		and	Condition(s)		then	Cisco-	ISE-NSP	Edit
																	(Duplicate above Duplicate below Insert new policy at Insert new policy be	slow

Passaggio 18.1. Configurare i dettagli:

Nome regola: Linux

Sistemi operativi: Linux All

Risultati: linux_agent_config

Fare clic su Done e su Save.

= :	lindin Identity	Services Engine							Wo	ork C	enters / Postu	ire				
Щ	Overview	Network Devices	Client Pro	visioning	Policy Elements	Post	ture Policy	Policy Se	ts Trouble	eshoo	t Reports	Settings				
11日 1日 火 日 よ。	Client Provisioning Policy Resources Client Provisioning Portal		Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order. Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures. For Windows Agent AMA64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column. Mac ARM64 policies require no Other Conditions arm64 configurations. If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policies is ist, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.													
0				Rule Nam IOS Android Linux	e it it	Identity Any Any Any	Groups and and and	Operating Apple IOS A Android Linux All	Systems	and and and	Other Conditions Condition(s) Condition(s) Condition(s)	1	then then then	Results Cisco-ISE-NSP Cisco-ISE-NSP linux_agent_config	E	dit v dit v dit v

ISE_Add_New_Provisioning_Policy_1

≡	diale Identity Services Engine	Work Centers / Posture	
н	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
三 正 火	Cenditions V Anti-Malvare Anti-Spyware Anti-Virus	Q. Very 2 Eds + Add C Duplicate C Deleter	Selected 0 Total 385 🔗 🔕
	Application	Name Description File name Condition Type	
40 	Dictionary Compound	pc_XP64_x812797052_M517 Cisco Predefined Check: SYSTEM_PROGRAMS\C Cisco-Defined	1
mil	Dictionary Simple	pc_W8_64_KB3124275_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	External DataSource	pc_Vista_K82893294_MS13 Cisco Predefined Check: SYSTEM_32\/magehlp.dll Cisco-Defined	
(?)	File	pc_W81_64_K83033889_M Clsco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Firewall	pc_Vista64_x8925902_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_KB2653956_MS12-0 Cisco Predefined Check: SYSTEM_32(Wintrust.dll Cisco-Defined	
	Script	pc_W8_K82892074_MS13 Cisco Predefined Check: SYSTEM_32\Scrun.dll Cisco-Defined	
	Service	pc_W10_64_1909_K850139 Clsco Predefined Check: SYSTEM_ROOT\SysWO Clsco-Defined	
	038	pc_W7_K82681578_M512 Cisco Predefined Check: SYSTEM_32(Win32k.sys Cisco-Defined	
	Remediations >	pc_W10_KB3081436_MS15 Cisco Predefined Check: SYSTEM_321Edgehtml.dll Cisco-Defined	
	Bequirements	pc_W81_64_K83042553_M Cisce Predefined Check: SYSTEM_ROOT(sysnativ Cisco-Defined	
	Allowed Protocols	pc_W8_64_K82727528_MS Cisco Predefined Check: SYSTEM_ROOT(sysnativ Cisco-Defined	
	Authorization Profiles	pc_W8_64_K82992611_M5 Clsco Predefined Check: SYSTEM_ROOT(sysnativ Clsco-Defined	
	Downloadable ACLs	pc_W7_K83078601_MS15 Cisco Predefined Check SYSTEM_32\Win32k.sys Cisco-Defined	

Passaggio 19. Passare a Work Centers > Posture > Policy Elements > Conditions > File. Fare clic su .Add

Passaggio 19.1. Configurare i dettagli:

Nome: linux_demo_file_exist

ISE_Add_New_File_Condition

Sistemi operativi: Linux All

Tipo di file: FileExistence

Percorso file: home, Desktop/test.txt

Operatore file: esistente

Fare clic su .Submit

=	dentity Service	es Engine					Work Cer	iters / Post	ure		
н	Overview Netwo	ork Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
11日 1日 火 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日	Conditions Anti-Maiware Anti-Spyvare Aptilication Compound Dictionary Simple Disk Encryption External DataSource File Firemall Horizon Athrobas Patch Management Registry Script Service USB	d	File Conditions List > New File Condition Name * Description * Operating System Compliance Module & * File Type * File Path * File Operator	File Condition Ilinux_demo_file_exist Linux All Nny version FileExistence Exists	Uesktop/	tost. txt	_}			Submit	Cancel
	Remediations Requirements Allowed Protocols Authorization Profiles Downloadable ACLs	>									

ISE_Add_New_File_Condition_1

Passaggio 20. Passare a Work Centers > Posture > Policy Elements > Requirements. Fare clic Edit alla fine del nome di una regola. Selezionare Insert new Requirement.

=	deader Identity Services E	ingine							Work	Centers / Po	sture								
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	/ Elements	Posture	Policy Policy Sets	Tro	ubleshoot	Reports \$	ettings							
10 1-1	Dashboard Context Visibility	Conditions Anti-Malw	~									Guide Me							
\times	Operations	Anti-Spyw	are	Requirements															
0	Policy	Anti-Virus Apolicatio		Name		Operating Sys	tem	Compliance Module		Posture Type		Conditions		Remediations Actions					
1.	Administration	Compound	1	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 🛩				
		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	Duplica			
nili	Work Centers	Dictionary	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 r			
		External D	ataSource	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit	Delete			
(?)	Interactive Help	File File Firewall Hardware Attributes		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.			
			Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit 🤟					
			Any_AS_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_inst	then	Message Text Only	Edit 🤟					
		Patch Mar	Patch Management Registry Script	Patch Management Registry Script	Patch Management Registry	Registry	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_Max	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 🤟				
		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	USØ_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 🐱				
		Anowed Protocols Authorization Profiles Downloadable ACLs	Authorization Profiles Downloadable ACLs	Authorization Profiles Downloadable ACLs	Default_AppVis_Requiren ent_Win	tor	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 9				
				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

Passaggio 20.1. Configurare i dettagli:

Nome: Test_exist_linux

Sistemi operativi: Linux All

Modulo conformità: 4.x o versioni successive

Tipo di postura: agente

Condizioni: linux_demo_file_exist

Fare clic su Done e su 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



Nota: al momento, solo gli script shell sono supportati per gli agenti Linux come correzione.

Passaggio 21. Passare a Work Centers > Posture > Policy Elements > Authorization Profiles. Fare clic su .Add

Passaggio 21.1. Configurare i dettagli:

Nome: known_redirect

Selezionare la casella di controllo Web Redirection(CWA,MDM,NSP,CPP)

Seleziona Client Provisioning(Posture)

ACL: reindirizzamento

Valore: Portale di provisioning client (predefinito)

≡ ;;	lister Identity Services Engine	Work Centers / Posture
Щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
III	Conditions Anti-Malware Anti-Spyware Anti-Virus Application Compound Dictionary 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 Registry Script Service USB Remediations Requirements Allowed Protocols Authorization Profiles Downloadable ACLs	Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) Client Provisioning (Posture) ACL redirect Static IP/Host name/FQDN Suppress Profiler CoA for endpoints in Logical Profile

ISE_Add_New_Authorization_Profile_Redirect_1



Nota: questo reindirizzamento del nome ACL deve corrispondere al nome ACL corrispondente configurato su FTD.

Passaggio 21.2. Ripetere l'operazione Add per creare altri due profili di autorizzazione per gli endpoint non conformi e conformi con i dettagli.

Nome: non_compliant_profile

Nome DACL: DENY_ALL_IPv4_TRAFFIC

Nome: compliant_profile

Nome DACL: PERMIT_ALL_IPv4_TRAFFIC



Nota: il DACL per gli endpoint conformi o non conformi deve essere configurato in base ai requisiti effettivi.

Passaggio 22. Passare a Work Centers > Posture > Posture Policy. Fare clic Edit alla fine di qualsiasi regola. Selezionare Insert new policy.

						8-8		Г										~		_		_
Identity Services	Engine							L	Work Centers /	Pos	ture							Q	4	0	φ	L.
J Bookmarks	Overview	r Ne	twork Devices	Client Provisioning P	olicy Elements	Posture Poli	cy Policy S	Sets	Troubleshoot	R	teports Settings											
E Dashboard		_			L																	
10 Context Visibility		Post	ure Policy	Guide Me																		
% Operations		Define the	e Posture Policy by c	onfiguring rules based on operat	ting system and/or othe	conditions.													~			-
Policy		~																				
L_ Administration		Status	Policy Options	Rule Name	Identity Groups	Operat	ing Systems	(Compliance Module		Posture Type		Other Conditions	Re	quirements	_	-					
			Policy Options	Default_AntiMalware_Policy_Ma c	If Any	and Mac 05	×	and 4	k.x. or later	and	Agent	and	then	e An	_AM_Installation_Ma	Edit v						
			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ii Any	and Mac 05	×	and a	Lx or later	and	Temporal Agent	and	the	An 6_1	_AM_installation_Ma emporal	Edit	Duptcate Insert new policy					
③ Interactive Help			Policy Options	Default_AntiMalware_Policy_Win	ii Any	and Window	s All	ind 4	Lx or later	and	Agent	and	the	- An	AM_Installation_Wi	Edi	04419					
			Policy Options	Default_AntiMalware_Policy_Win_temporal	ii Any	and Window	s Al	and 4	La. or later	and	Temporal Agent	and	then	. An	, AM_Installation_Wi emporal	Edit						
			Policy Options	Default_AppVis_Policy_Mac	ii Any	and Mac OS	×	and 4	Lx or later	and	Agent	and	then	Def	auit_AppVis_Require rt_Mac	Edt -						
			Policy Options	Default_AppVis_Policy_Mac_temporal	II Any	and Mac OS	×	ind a	La or later	and	Temporal Agent	and	then	Def	ault_AppVis_Require nt_Mac_temporal	Edt y						
			Policy Options	Default_AppVis_Policy_Win	ii Any	and Window	a All	and 4	i.x.or later	and	Agent	and	then	Def	ault_AppVIs_Require nt_Win	Edit 9						
			Policy Options	Default_AppVIs_Policy_Win_te mporal	ii Any	and Window	s Al	ind 4	La or later	and	Temporal Agent	and	the	Def	ault_AppVis_Require nt_Win_temporal	Edit -						
			Policy Options	Default_Firewall_Policy_Mac	ii Any	and Mac OS	x	and 4	Lx or later	and	Agent	and	Det	Del me	ault_Firewalt_Require rt_Mac	Edit y						
			Policy Options	Default_Firewall_Policy_Mac_te mporal	ii Any	and Mac OS	×	and 4	Lx or later	and	Temporal Agent	and	the	Def	ault_Firewall_Require nt_Mac_temporal	Edt -						
			Policy Options	Default_Firewall_Policy_Win	IF Any	and Window	s Al	and 4	i.x or later	and	Agent	and	then	Def	auit_Firewall_Require nt_Win	Edit 9						
			Pulicy Options	Default_Firewall_Policy_Win_te mporal	ir Any	and Window	s Alt	and 4	La or later	and	Temporal Agent	and	the	Def	ault_Firewall_Require nt_Win_temporal	Edt v						
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	II Any	and Med 05	×	and 4	Lx or later	and	Agent	and	the	Def ute	auit_Hardware_Attrib s_Requirement_Mac	Edt v						
			Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	ii Any	and Mac OS	x .	and 4	k.x. or later	and	Temporal Agent	and	then	Def ute	ault_Hardware_Attrib s_Requirement_Mac_ poral	Edit v						
			Policy Options	Default_Hardware_Attributes_P olicy_Win	II Any	and Window	s Al	and 4	Lx or later	and	Agent	and	then	Def	ault_Hardware_Attrib s_Requirement_Win	Edt -						
		-	·····	-					- ii tali		*				and the second second							

ISE_Add_New_Posture_Policy

Passaggio 22.1. Configurare i dettagli:

Nome regola: Demo_test_exist_linux

Gruppi di identità: qualsiasi

Sistemi operativi: Linux All

Modulo conformità: 4.x o versioni successive

Tipo di postura: agente

Requisiti: Test_exist_linux

Fare clic su Done e su Save.

Post	ture Policy	Guide Me	iting :	system and/o	r other con	ditions.							2	~
~														
	Policy Options	Default_Firewall_Policy_Mac	H.	Any	and	Mac OSX	an	4.x or later	and	Agent	and	the	 Default_Firewall_Require ment_Mac 	Edit 👻
	Policy Options	Default_Firewall_Policy_Mac_te mporal	1	Any	and	Mac OSX	an	4.x or later	and	Temporal Agent	and	the	n Default_Firewall_Require ment_Mac_temporal	Edit 🤟
	Policy Options	Default_Firewall_Policy_Win	H	Any	and	Windows All	an	4.x or later	and	Agent	and	the	n Default_Firewall_Require ment_Win	Edit ~
	Policy Options	Default_Firewall_Policy_Win_temporal	H	Any	and	Windows All	an	4.x or later	and	Temporal Agent	and	the	n Default_Firewall_Require ment_Win_temporal	Edit 🤟
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	H	Any	and	Mac OSX	an	4.x or later	and	Agent	and	the	n Default_Hardware_Attrib utes_Requirement_Mac	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	1	Any	and	Mac OSX	an	4.x or later	and	Temporal Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Mac_ temporal 	Edit 🐱
	Policy Options	Default_Hardware_Attributes_P olicy_Win	H.	Any	and	Windows All	an	4.x or later	and	Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Win 	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	18	Any	and	Windows All	ani	4.x or later	and	Temporal Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Win_t emporal 	Edit 😔
	Policy Options	Default_US8_Block_Policy_Win	if.	Any	and	Windows All	ani	4.x or later	and	Agent	and	the	n USB_Block	Edit 😔
-	Policy Options	Default_USB_Block_Policy_Win	11	Any	and	Windows All	an	4.x or later	80	Temporal Agent	and	the	n USB_Block_temporal	Edit 🗸

ISE_Add_New_Posture_Policy_1

Passaggio 23. Passare a Work Centers > Posture > Policy Sets. Fare clic per Insert new row above.

Q A) د	۵ ۵	¢									osture	rs / P	rk Center	We												ingine	ices E	ty Serv	Identit		≡
											ettings	 Report	pot	froublesho	ets	Policy S	ure Policy	Pot	Elements	Policy	visioning	Client Pro	vices (ork Dev	Netwo	ew	Overvie			marks	Book	н
Save	15	rt Hitcounts	eset Policyset H	Reset	leset	Res									_									ts.	xlicy Sets	Poli			lity	board ext Visibili	Dash Cont	81 73
ns View	Act	ce Hits	rver Sequence	is / Server	d Protocols	Allowed Pr												nditions	Cor	ion	Descript	me	dicy Set Nar	tus Po	 Statu 					ations	Oper	×
																								arch	Q Sea					y	Polic	U
>	ŝ	+ •	n /+	Access	t Network /	Default N														licy set	Default po		ner.	Def	•					Centers	Work	4. 41
1	above	t new row a	Insert n																										lp.	active Help	Inter	٢
Save	ţ.	Reset																														
	l	Reset	Linsert re																										lp	sctive Helj	Inter	٢

ISE_Add_New_Policy_Set

Passaggio 23.1. Configurare i dettagli:

Nome set di criteri: postura firewall

Condizioni: Indirizzo IP del dispositivo di accesso alla rete EQUALs [Indirizzo IP FTD]

Fare clic su . Save

=	dentity Services	Engine		=:					Work Centers /	Posture					c	۵ ۱	0	۹	۹
J.	Bookmarks	Overview	Networl	k Devices	Client Provisionin	g Policy Elemen	ts Posture Policy	Policy Sets	Troubleshoot	Reports	Settings								
80 10	Dashboard Context Visibility	P	olicy Sets										Reset	Reset P	olicyset H	icounts		Save	
*	Operations		🕑 Status	Policy Set N	Name Desc	ription	Conditions						Allowed Protoco	ols / Server S	lequence	Hits	Actions	View	
0	Policy		Q. Searc	A															
8.	Administration		0	Firewall Postu	29 C		Network Access Device I	P Address EQUALS					Default Network	k Access	2+	,	0	>	
-1	Work Centers		•	Default	Defau	It policy set							Default Network	k Access	2+		◈	>	
٢	Interactive Help																_		
																Reset		Save	
																	_		

ISE_Add_New_Policy_Set_1

Passaggio 23.2. Fare clic> per immettere il set di criteri. Creare nuove regole di autorizzazione per lo stato conforme alla postura, non conforme e sconosciuto. Fare clic su .Save

Conforme con compliant_profile

Non conforme con non_compliant_profile

Sconosciuto con known_redirect

=	disco Identity	Service	es Engine					Work Cent	ters / Postu	re					
н	Overview	Netwo	ork Devices Clie	nt Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
同		0	Firewall Posture		D Netw	ork Access-Device IP Add	ress EQUALS :						Default Network Access		e + •
*	~Authr	Intication	Policy(1)												
0	۲	Status	Rule Name	Conditions								Use		Hits	Actions
#0	0	Search													
-								+							
?			Default									All_User_ID_	Stores 🦉	48	念
		-										> Options			123
	> Autho	orization	Policy - Local Exception	15											
	> Autho	orization I	Policy - Global Exception	ins											
	~Autho	orization	Policy(4)												
										Results					
	۲	Status	Rule Name	Conditions						Profiles		Security Group	os	Hits	Actions
	9	Search													
		٥	Compliant	E Session-P	ostureStatus EQUALS Con	npliant				compliant_profile	1 +	Select from li	ist 🥒 +	15	
		۲	Non_Compliant	b Session P	ostureStatus EQUALS Non	Compliant				non_compliant_profile	0+	Select from li	ist 🥒 +	5	(2)
		٥	Unknown	E Session-P	ostureStatus EQUALS Unk	nown				unknown_redirect	<i>e</i> +	Select from I	ist 🖉 +	47	(i)

ISE_Add_New_Policy_Set_2

Configurazioni su Ubuntu

Passaggio 24. Accedere al client Ubuntu tramite la GUI. Aprire il browser per accedere al portale VPN. Nell'esempio, questo valore è demo.example.com.

demo	.exar	mple.com/+C	SCOEX	+			-	ø	×
\leftarrow	\rightarrow	С	0 8	https://demo.example.com/	-CSCOE+/logon.html#form_title_text	ជ	${igsidential}$	\mathbf{F}	≡

Logon
Group posture_vpn v Username
Password
Logon

Accesso Ubuntu_Browser_VPN

Passaggio 25. Fare clic su .Download for Linux

Cisco	Secu	re Client Insta	allati	<	+					-	ē	×
\leftarrow	\rightarrow	C	0 8	A	https://demo. example.com /CACHE/stc/2/index.html	Ē	80%	ជ		${igvarsim}$	⊻	≡
		Secure	re Client	nt								
		C			Disco Secure Client Download							A
					Download & Install							
					Download Cisco Secure Client and install it on your computer. Download for Linux							
						0	🕀 Inst	ructio	าร			

Ubuntu_Browser_VPN_Download_1

Il nome del file scaricato è cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_Browser_VPN_Download_2

Passaggio 26. Scaricare il certificato VPN tramite il browser e rinominare il file in <certificato>.crt. Questo è l'esempio di come utilizzare firefox per scaricare il certificato.

-	demo.example	.com/+CSCOE× +		\sim		D.	×
\leftarrow	\rightarrow G	Dttps://demo.example.com/+CSCOE+/logon.html#form_title_text	ŝ	${igsidential}$	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	e Internet. raveling between computers. It rork. Help

Ubuntu_Browser_VPN_Cert_Download

Passaggio 27. Aprire il terminale sul client Ubuntu. Passarepath home/user/Downloads/ a per installare 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\$

Passaggio 28. Considera attendibile il certificato del portale VPN nel client Ubuntu.

```
<#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

Passaggio 29. Aprire Cisco Secure Client sul client Ubuntu e connettere la VPN a demo.example.com.

		Cisco Secure	Client		-	×
AnyCon	nect VPN	🖊 Statist	ics	About		
		ıı ııı cısc	11 0			
Connect to:	demo.exa	ample.com			~	₽
Group:	posture_v	pn				~)
Username:	isetest					
Password:	******					



 $Ubuntu_Secure_Client_Connected$

Passaggio 30. Aprire il browser per accedere a tutti i siti Web da cui viene attivato il reindirizzamento al portale CCP ISE. Scaricare il certificato dal portale ISE CPP e rinominare il file in <certificato>.crt. Questo è un esempio di come usare Firefox per scaricare.



Ubuntu_Browser_CPP_Cert_Download

Passaggio 30.1. Considerare attendibile il certificato del portale CPP ISE sul client Ubuntu.

<#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.
```

Passaggio 31. Fare clic su Start sul portale ISE CPP.

Device Security Check × +	-	đ	×							
← → 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.										

Ubuntu_Browser_CPP_Start

Passaggio 32. Click here to download and install Agent.

Device Security Che	eck × +	- • ×						
$\leftarrow \ \rightarrow \ G$	https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL 🏠	\odot						
You must log in to	o this network before you can access the Internet.	\times						
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							
 You must install Agent to check your device before accessing the network. <u>Click here to download and install Agent</u> After installation, Agent will automatically scan your device before allowing you access to the network. You have 20 minutes to install and for the system scan to complete. 								
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	0 minutes to install and for the compliance check to complete							
Φ	+ Remind me what to do next							

Ubuntu_Browser_CPP_Download_Posture

Passaggio 33. Aprire il terminale sul client Ubuntu. Passare al percorso home/user/Downloads/ per installare il modulo di postura.

<#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.
```

Passaggio 34. Nell'interfaccia utente del client Ubuntu, uscire da Cisco Secure Client e riaprirlo. Il modulo ISE Posture è stato installato ed eseguito correttamente.



Ubuntu_Secure_Client_ISE_Posture_Installed

Passaggio 35. Aprire il terminale sul client Ubuntu. Passare a pathhome/user/Desktop, creare un test.txt file che soddisfi la condizione configurata in ISE.

<#root>

user@ubuntu22-desktop:~\$

cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passaggio 1. Connettere la VPN a demo.example.com sul client Ubuntu.



* Disconnect							
Connected to demo.example.com.							

 $Verify_Ubuntu_Secure_Client_Connected$

Passaggio 2. Controllare lo stato di ISE Posture sul client Ubuntu.



Verify_Ubuntu_Secure_Client_Compliant

Passaggio 3. Controllare Radius Live Log su ISE. Passare a Operations > RADIUS Live Log.

=	dentity Services Engine			Operations / RADIUS			Q & @ Q A		
Щ	Live Logs Live Sessions								
ы	Misconfigured Supplicants 🕕	Miscor	nfigured Network Devices 🕕	RADIUS Drops		Client Stopped Responding ①	Repeat Counter ①		
*	0		0	0		0	0		
U						Refresh Show	Within		
80						Never v Latest 20 re	ecords v Last 24 hours v		
di.	ට් 🖯 Reset Repeat Counts ර	🗅 Export To 🗸					Filter 🗸 🐵		
	Time	Status Details	Identity Endpoin	t ID Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy		
?		V Identity		Endpoint ID Endpoint Profile P		Authentication Policy	Authorization Policy		
	May 29, 2024 09:08:48.798 PM	ف ا	isetest 52:54:00:	17:6B:FA Ubuntu-Workstation	Compliant	Firewall Posture >> Default	Firewall Posture >> Compliant		
	May 29, 2024 09:08:48.798 PM		52:54:00:	17:6B:FA	Compliant	Firewall Posture F	Firewall Posture >> Compliant		
	May 29, 2024 09:08:13.570 PM		isetest 52:54:00:	17:6B:FA Ubuntu-Workstation	Pending	Firewall Posture >> Default	Firewall Posture >> Unknown		

Verifica_ISE_LiveLog

Passaggio 4. Passare alla CLI FTD tramite SSH o 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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per il flusso della postura e la risoluzione dei problemi di Cisco Secure Client e ISE, consultare i <u>documenti</u> CCO<u>Confronto tra stili di</u> postura ISE per versioni precedenti e successive alla 2.2 e <u>Risoluzione dei problemi di gestione e postura delle sessioni ISE</u>.

Informazioni correlate

<u>Compatibilità dei componenti di rete Cisco Identity Services Engine, versione 3.3</u>

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).