# ISE 3.3에서 Linux VPN Posture 구성

## 목차

<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
사용되는 구성 요소
<u>구성</u>
<u>네트워크 다이어그램</u>
FMC/FTD의 컨피그레이션
<u>ISE의 컨피그레이션</u>
<u>Ubuntu 구성</u>
<u>다음을 확인합니다.</u>
<u>문제 해결</u>
<u>관련 정보</u>

## 소개

이 문서에서는 ISE(Identity Services Engine) 및 FTD(Firepower Threat Defense)를 사용하여 Linux VPN Posture를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 클라이언트
- FTD(Firepower 위협 방어)의 원격 액세스 VPN
- Identity Services Engine(ISE)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Ubuntu 22.04
- Cisco Secure Client 5.1.3.62
- Cisco FTD(Firepower Threat Defense) 7.4.1
- Cisco FMC(Firepower Management Center) 7.4.1
- Cisco ISE(Identity Services Engine) 3.3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

### 네트워크 다이어그램



토폴로지

### FMC/FTD의 컨피그레이션

1단계. 클라이언트, FTD, FMC 및 ISE 간의 연결이 성공적으로 구성되었습니다. enroll.cisco.com는 리디렉션을 위해 프로브를 수행하는 엔드포인트에 사용됩니다(자세한 내용은 포스처 플로우 CCO 문서ISE Posture Style Comparison for Pre and Post 2.2 참조). FTD에서 enroll.cisco.com으로 이동 하는 트래픽에 대한 경로가 올바르게 구성되었는지 확인합니다.

2단계. <u>Cisco Software Download</u>cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg에서 패키지 이름을 다운로드하고 다 운로드한 파일의 md5 체크섬이 Cisco Software Download 페이지와 동일한지 확인하여 다운로드 후 파일이 정상인지 확인합니다.

3단계. 로 Objects > Object Management > VPN > Secure Client File 이동합니다. 클릭Add Secure Client File, 이름 입력, 선택File Name, cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg드롭다운 목록에서 선택Secure Client Image File Type. 그런 다음 을 클릭합니다 Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policie	s Devices Objects Integration		Deploy	९ 💕 🌣 🔕 admin ~	circo 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	Name:*		n-5.1.3.62-webdeploy-k9.pkg	Type Secure Client Image	1/1
> РКI Policy List	Default-External-Browser-package hostscan5_1_3_62	linux_5_1_3_62		36-webdeploy-k9.zip -5.1.3.62-k9.pkg	Secure Client External Browser Pa HostScan Package	±011 ±/11
Port Prefix List	linux_image	File Name:*	WSP	ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	1/1
Route Map     Security Intelligence     Sinkhole		File Type:*				
SLA Monitor Time Range		Secure Client Image				
Time Zone Tunnel Zone		Description:				
URL Variable Set VLAN Tag						
~ VPN						
Certificate Map Custom Attribute Group Policy IKEv1 IPsec Proposal IKEv1 Policy		Cance	Save			
IKEv2 IPsec Proposal IKEv2 Policy Secure Client Customizatio Secure Client File				Disple	nying 1 - 4 of 4 rows. I< < Page 1	of 1 > > ⊂

FMC\_Upload\_Secure\_Client\_Image

4단계. 로 Objects > Object Management > Network 이동합니다.

4.1단계. DNS 서버용 개체를 만듭니다. 을 Add Object 클릭하고 이름과 사용 가능한 DNS IP 주소를 입력합니다. 를 Save 클릭합니다.

Firewall Management	t Center Overview Analysis Polic	ies Devices Objects Integration		Deploy	Q 🔮 🌣 🔕 admin	* circo SECURE
Distinguished Name     DNS Server Group     External Attributes     File List     FlexConfig     Geolocation	Network A network object represents one or more IP addres	ses. Network objects are used in various places, including acces	is control policies, network variables, intrusion	Add Network	C, Filter     Object     orts, and so on.	Dbjects
	Name			Value	Type Override	
Interface	any	New Network Object	Ø	0.0.0.0/0 ::/0	Group	¶a.≑#
Key Chain Network	any-ipv4			0.0.0.0/0	Network	¶aq ⊕ #
		Description	O FQDN			
			Cancel			

FMC\_Add\_Object\_DNS



**참고**: 여기에 구성된 DNS 서버는 VPN 사용자를 위해 사용됩니다.

4.2단계. ISE PSN에 대한 개체를 만듭니다. 을 Add Object 클릭하고 이름 및 사용 가능한 ISE PSN IP 주소를 입력합니다. 를 Save 클릭 합니다.

Firewall Management	Center Overview Analysis Policie	s Devices Objects Integration		Deploy	역 🚱 🌣 🙆 🛛 admin 🗸 讨 dista SECURE
Distinguished Name     DNS Server Group     External Attributes     File List     File List     Geolocation     Interface     Key Chain     Network	Network A network object represents one or more IP address	es. Network objects are used in various places, including acces	s control policies, network variables, intrusi	Add Network Add Obj on rules, identity rules, network discovery rule Import Add Gro	P. Filter     Objects     Object     orts, and so on.
	Name	New Network Object	Ø	Value 0.0.0.0/0 =/0	Type Override Group 🗛 🗑 &
	any-ipu4	Name ISE_PSN_ Description Network Host Range Network Allow Overrides	O FQDN	0.0.0/9	Network <table-cell> 🛱 Q, 🗑 🤼</table-cell>
			Cancel Save		

FMC\_Add\_Object\_ISE

5단계. 로 Objects > Object Management > VPN > Group Policy 이동합니다. 를 Add Group Policy 클릭합니다. 를 DNS/WINS 클릭하고 의 DNS 서버 개체를 선택합니다Primary DNS Server. 그런 다음 을 클릭합니다Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects	Integration	Deploy Q 💞 🌣 🛛 admin V 👘 SECURI
<ul> <li>Distinguished Name</li> <li>DNS Server Group</li> </ul>	Group Policy			Add Group Policy Q, Filter
> External Attributes File List	A Group Policy is a set of attribute and value pairs, stored in	a group policy object, that	t define the remote access VPN experience. The RADIUS authorization server assign	s the group policy or it is obtained from the current connection profile.
Geolocation	Name			
Interface	DftGrpPolicy	Add Group Polic	y @	/i
Network		Name:* posture_gp		/1
Policy List Port		Description:		
> Prefix List Route Map		General Secu	e Client Advanced	
> Security Intelligence Sinkhole		VPN Protocols	Primary DNS Server:	
SLA Monitor		IP Address Pools	DNS,	
Time Range Time Zone		Banner DNS/WINS	Secondary DNS Server:	
Tunnel Zone URL		Split Tunneling	Primary WINS Server:	
Variable Set VLAN Tag			Secondary WINS Server:	
V VPN			DHCP Network Scope:	
Custom Attribute			Crity network object with ipv4 address is allowed (Ec: 10.72.3.5)	
Group Policy IKEv1 IPsec Proposal			Default Domain:	
IKEv1 Policy IKEv2 IPsec Proposal				
IKEv2 Policy Secure Client Customizatio				
Secure Client File			Cancel Save	Displaying 1 - 2 of 2 rows I < < Page 1 of 1 > >I ℃

FMC\_Add\_Group\_Policy



**참고**: VPN 그룹 정책에 사용된 DNS 서버가 ISE 클라이언트 프로비저닝 포털 FQDN 및 enroll.cisco.com을 확인할 수 있는 지 확인하십시오.

6단계. 로 Objects > Object Management > Access List > Extended 이동합니다. 를 Add Extended Access List 클릭합니다.

Cipects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🕢 admin 🗸 divin SECURE
<ul> <li>AAA Server</li> <li>RADIUS Server Group</li> </ul>	Extended	Add Extended Access List Q, Filter
Single Sign-on Server	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 on addresses. You use these objects when configuring particular features, such as route maps.	by, identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6
Extended	Name	Value Override

FMC\_Add\_Redirect\_ACL

#### 단계. 리디렉션 ACL의 이름을 제공합니다. 이 이름은 ISE 권한 부여 프로파일과 동일해야 합니다. 를 Add 클릭합니다.

New Exte	nded Aco	cess List Object							0
Name redirect									
Entries (0)									
									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
No record	s to display								
Allow Ov	errides								
								Cancel	Save

 $FMC\_Add\_Redirect\_ACL\_Part\_l$ 

6.2단계. 리디렉션에서 제외할 DNS 트래픽, ISE PSN IP 주소에 대한 트래픽 및 리미디에이션 서버를 차단합니다. 나머지 트래픽을 허 용합니다. 리디렉션이 트리거됩니다. 를 Save 클릭합니다.

				Ø
Action: Block				
Logging: Default				
Log Level: Informational				
Log Interval: 300 Sec.				
Network Port (1) Application (1) Users	Security Group Tag			
Available Networks C +		Source Networks (0)	Destination Networks (1)	
O Creat have a second as				
Q Search by name or value		any	ISE_PSN	
IPv4-Private-192.168.0.0-16	Add to Source	any	ISE_PSN	
IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918	Add to Source	any	ISE_PSN	Ì
IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped	Add to Source	any	ISE_PSN	Ĩ
IPv4-Private-192.168.0.0-16       IPv4-Private-All-RFC1918       IPv6-IPv4-Mapped       IPv6-Link-Local	Add to Source	any	ISE_PSN	
V Search by name or value         IPv4-Private-192.168.0.0-16         IPv4-Private-All-RFC1918         IPv6-IPv4-Mapped         IPv6-Link-Local         IPv6-Private-Unique-Local-Addresses	Add to Source	any	ISE_PSN	
Q Search by name or value         IPv4-Private-192.168.0.0-16         IPv4-Private-All-RFC1918         IPv6-IPv4-Mapped         IPv6-Link-Local         IPv6-Private-Unique-Local-Addresses         IPv6-to-IPv4-Relay-Anycast	Add to Source Add to Destination	any	ISE_PSN	W
IPv4-Private-192.168.0.0-16         IPv4-Private-All-RFC1918         IPv6-IPv4-Mapped         IPv6-Link-Local         IPv6-Private-Unique-Local-Addresses         IPv6-to-IPv4-Relay-Anycast	Add to Source Add to Destination	any	ISE_PSN	
IPv4-Private-192.168.0.0-16         IPv4-Private-All-RFC1918         IPv6-IPv4-Mapped         IPv6-Link-Local         IPv6-Private-Unique-Local-Addresses         IPv6-to-IPv4-Relay-Anycast         ISE_PSN	Add to Source	any Enter an IP address Add	ISE_PSN Enter an IP address	đd
IPv4-Private-192.168.0.0-16         IPv4-Private-All-RFC1918         IPv6-IPv4-Mapped         IPv6-Link-Local         IPv6-Private-Unique-Local-Addresses         IPv6-to-IPv4-Relay-Anycast         ISE_PSN	Add to Source Add to Destination	any Enter an IP address Add	ISE_PSN	đd

Cancel

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	/1
4 Allow Or	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	/1

Cancel Save

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



**참고**: 이 리디렉션 ACL 예의 대상 FTP는 리미디에이션 서버 예제로 사용됩니다.

7단계. 로 Objects > Object Management > RADIUS Server Group 이동합니다. 를 Add RADIUS Server Group 클릭합니다.

Firewall Management Objects / Object Management	Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	69
<ul> <li>✓ AAA Server</li> <li>RADIUS Server Group</li> <li>Single Sign-on Server</li> <li>✓ Access List</li> </ul>	RADIUS S	Gerver G	roup	or more refere	nces to RADI	US Servers. Ti	ese AAA servers are used to authenticate users logging in through Remote Access VPN conn	ections.	Add RADIUS Set	ver Gro	up
Extended	Name							Value			

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

7.1단계. 이름, 확인Enable authorize only, 확인Enable interim account update, 확인Enable dynamic authorization을 입력합니다.

Name:*   rtpise   Description:   Group Accounting Mode:   Single   Retry Interval:*   (1-10) Seconds   10   Realms:   Image: Interval:*   Interval:*   (1-120) hours   24   Interval:*   Interval:*   (10) Labele dynamic authorization   Port:*	Add RADIUS Server Group	?
rtpise Description: Group Accounting Mode: Single Retry Interval:* (1-10) Seconds 10 Realms: C Enable authorize only Enable interim account update Interval:* (1-120) hours 24 C Enable dynamic authorization Port:* (1024-65535)	Name:*	
Description: Group Accounting Mode: Single Retry Interval:* (1-10) Seconds 10 Realms: Price Enable authorize only Enable interim account update Interval:* (1-120) hours 24 Enable dynamic authorization Port:* (1024-65535)	rtpise	
Group Accounting Mode: Single  Retry Interval:* (1-10) Seconds 10  Realms:  C Enable authorize only Enable interim account update Interval:* (1-120) hours 24  Enable dynamic authorization Port:* (1024-65535)	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)		
Single   Retry Interval:*   10   Realms:   ✓   Enable authorize only   ✓   Enable interim account update   Interval:*   (1-120) hours   24   ✓   Enable dynamic authorization   Port:*   (1024-65535)	Group Accounting Mode:	
Retry Interval:* (1-10) Seconds 10 Realms: Carterian account update Interval:* (1-120) hours 24 Carterian Enable dynamic authorization Port:* (1024-65535)	Single	
10         Realms:         ✓         Enable authorize only         ✓         Enable interim account update         Interval:*         (1-120) hours         24         ✓         Enable dynamic authorization         Port:*         (1024-65535)	Retry Interval:* (1-10) Seconds	
Realms:	10	
<ul> <li>Enable authorize only</li> <li>Enable interim account update</li> <li>Interval:* (1-120) hours</li> <li>24</li> <li>Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> </ul>	Realms:	
<ul> <li>Enable authorize only</li> <li>Enable interim account update</li> <li>Interval:* (1-120) hours</li> <li>24</li> <li>Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> </ul>	▼	
<ul> <li>Enable Interim account update</li> <li>Interval:* (1-120) hours</li> <li>24</li> <li>✓ Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> </ul>	Enable authorize only	
Interval:*       (1-120) hours         24       ✓         ✓       Enable dynamic authorization         Port:*       (1024-65535)		
<ul> <li>Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> </ul>	Interval:* (1-120) hours	
Enable dynamic authorization       Port:*     (1024-65535)	24	
Port:* (1024-65535)	Enable dynamic authorization	
	Port:* (1024-65535)	
	I I	

Cancel

7.2단계. 아이콘을 Plus 클릭하여 새 RADIUS 서버를 추가합니다. ISE PSN을 제공합니다. IP Address/Hostname, Key연결할 를 specific interface 선택합니다. 을 Redirect ACL선택합니다. 그런 다음 새 SaveRADIUS 서버를 저장하려면 클릭합니다. 그런 다음 다시 클릭하 여Save 새 RADIUS 서버 그룹을 저장합니다.

Add RADIUS Server Group	0	New RADIUS Server	0
Enable authorize only		IP Address/Hostname:*	
Enable interim account update Interval:* (1-120) hours 24		Configure DNS at Threat Defense Platform Settings to resolve hostname Authentication Port:* (1-65535) 1812	
Enable dynamic authorization   Port:* (1024-65535)   1700     Merge Downloadable ACL with Cisco AV Pair ACL    After Cisco AV Pair ACL		Kev:*  Confirm Key:*  Accounting Port: (1-65535)  [1813 Timeent: (1-200) Seconds	
RADIUS Servers (Maximum 16 servers) IP Address/Hostname No records to display	+	10         Connect using:         Routing	
	Cancel Save	Cancel	Save

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

8단계. 로 Objects > Object Management > Address Pools > IPv4 Pools 이동합니다. 을 Add IPv4 Pools 클릭하고 및 을 **Name, IPv4 Address Range**제공합니다Mask. 그런 다음 을 클릭합니다Save.

Firewall Managem Objects / Object Manager	Inter Center Overview Analysis Policies Devices Objects Integration De	Deploy Q 💕 🕻	angni v	cisco SECURE
> AAA Server > Access List > Address Pools IPv4 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	
IPA4 Pools PA4 Pools Application Filters AS Path BFD Template Cipther Suite List > Centinuity List DHCP IPA6 Pool > Distinguished Name DHCP IPA6 Pool > Distinguished Name DHCP IPA6 Pool > Distinguished Name DHCP IPA6 Pool > Distinguished Name DHCP IPA6 Pool > External Attitudes File List > PiecContig Geolocation Interface Kay Chain Network > Pool Policy List Port > Prot List Route Map > Security Intelligence Sitabole SLA Monitor Time Range	Name     od     posture_pool_97,0     Name*     Description     PV4 Address Range*     192.168.6.30-192.168.6.100        Pormat: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150     Mask*   252.255.255.0        Image: Configure device overrides in the address pool object to avoid P address conflicts in case of object is shared across avoid P address conflicts in case of object to shared across avoid		Deeride O	/¥ /¥
Time Zone Tunnel Zone URL Variable Set		Displaying 1 - 2 of 2 r	ows IC < Page 1	of 1 > >1 C

9단계. 로 Certificate Objects > Object Management > PKI > Cert Enrollment 이동합니다. 을 Add Cert Enrollment 클릭하고 이름을 입력한 다음 Self Signed Certificatein을 Enrollment Type 선택합니다. 탭을 Certificate Parameters 클릭하고 및 를Common Name 제공합니다 Country Code. 그런 다음 을 클릭합니다Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices	s Objects Integration		Deploy Q 🚱 🌣 😡 fangni -	disce SECURE
> AAA Server > Access List > Address Pools	Cert Enrollment A certificate enrolment object contains the Certification Authority ( your Private Key Infrastructure (PK).	CA) server information and enrollment parameter	s that are required for creating Certificate Signing Requests (CSRs) and obtaining Ide	Add Cert Enrollment Q, Filter	tivities occur in
Application Filters AS Path BFD Template Cipher Suite List	Name Add Cert Enrollment	٥	Add Cert Enrollment	Type Override	/1
Community List     DHCP IPv6 Pool     Distinguished Name	Name*		Name" demo_xpn	Derti Serti	/1
DNS Server Group     External Attributes	Vescription		Lescription		
File List > FlexConfig Geolocation Interface Key Chain Network > PKI Cert Enrollment External Cert Groups External Cert Groups Internal CA Groups Internal CA Groups	CA Information Certificate Parameters Key Revocat Enrollment Type: Self Signed Certificate  ↓ Common Name (CN) is mandatory for self-signed certificate it VPN. To configure CN, please navigate to Certificate Paramete Validation Usage: Piece Client SSL Client SSL U	ion is used in Remote Access is 'tab. Server	CA Information Certificate Parameters Key Revocation Include FQDN: Don't use FQDN in certificate   Include FQDN: Don't use FQDN in certificate  Include Device's IP Address: Common Name (CN): demo.example.com Crganization Unit (UU): [ Organization (0): Locatly (L): State (CT): Country Code (C): CN Limat (L):		
Internal Cert Groups Internal Certs Trusted CA Groups Trusted CAs Policy List	Allow Overrides		Include Device's Seriel Number		
Port Prefix List Route Map Security Intelligence		Cancel Save		Cancel Save Displaying 1 - 3 of 3 rows 14 4 Page 1	of $1 > > C$

FMC\_Add\_New\_Cert\_Enroll

10단계. 로 Devices > Certificates 이동합니다. 을 Add 클릭하고 아래에서 FTD 이름을 Device 선택한 다음 아래에서 이전 구성된 등록 을 선택합니다Cert Enrollment. 를 Add 클릭합니다.

Firewall Managem Devices / Certificates	ent Center	Overview Analysis	s Policies Devices	Objects Integ	ration		Deploy	۹ (	P © 6	a fangni	<ul> <li>diada SECU</li> </ul>	ŧE
Filter											Add	1
All Certificates	*											۲
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Ce	intificate Expiry	Status						l
Add New Cert	ificate			0						<b>a</b>		l
Add New Och	incuto			•		G CA LD				*	2 C	l
Add a new certific	ate to the devic	e using cert enr	ollment object which	is used to		G CA LD				*	2CT	l
generate CA and i	dentify certifica	te.								<b>a</b>		l
Device*:						() CA				+	₽C ∎	l
Posture-FTD-CI	VL27	<b>*</b>										l
Cost Forelles està:												l
demo vod		- L										l
denio_vpi		• +										ł
Cert Enrollment De	etails:											
Name:	demo_vpn											
Enrollment Type:	Self-Signe	d										
Enrollment URL:	N/A											
			Cancel	Add								

FMC\_Add\_New\_Cert\_To\_FTD

11단계. 로 Devices > VPN > Remote Access 이동합니다. 를 Add 클릭합니다.

11.1단계. 이름을 입력하고 FTD를 추가합니다Selected Devices. 를 Next 클릭합니다.

Firewall Management Center Overview	Analysis Policies Devices Objects Integration		Deploy Q 🚱 🌣 🕢 admin 🗸 👯 SECURE
Connection Profile	<ul> <li>Secure Client <ul> <li>Access &amp; Certificate <ul> <li>Summary</li> </ul> </li> </ul> </li> <li> Cargeted Devices and Protocols <ul> <li>takes and will guide you through the required minimal steps to configure the flemote access VPU poly with a new user-defined connection protein.</li> </ul> </li> <li> Ven Protocols: <ul> <li>Secure Client</li> <li>Prote-KEV2</li> </ul> </li> <li> Cargeted Devices <ul> <li>Secure Client</li> <li>Secure Client</li></ul></li></ul>	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 Readm or RADRUS Server Group or SSO to authenciate VPN Policients. Secure Client Package Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Clico credentiats to download it during the witard. Device Interface Interface should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.	
			Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_1

11.2단계. 에서 이전에 구성한 RADIUS 서버 그룹을 Authentication Server, Authorization Server, Accounting Server 선택합니다. 페이지 를 아래로 스크롤합니다.

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🗳 🌣 🕢 admin 🗸 🗤 ECURE
Remote Access VPN Policy Wizard	
🕐 Policy Assignment 🔞 Connection Profile	
• Paicy Assignment   • Paicy Assignment • Secure Client • Surmay     • Paicy Connection Profile     Connection Profile   Connection Profiles specify the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection. These policies perfait to creating the tunnel group policies for a VPN connection to the VPN gateway.  Connection Public Mathematication (AAA, creating case or both), and the AAA servers that will be used for VPN connection. The policy to method of authematication (AAA, creating case or topologic).  Culter indication Method:   A Conv •   Undertication Server: • <td></td>	
Client Address Assignment:	
Plines ID addesse are he areland from AAA server PMPD server and ID addesse areas When multiple antiper are	
	Cancel Back Next

 $FMC\_New\_RAVPN\_Wizard\_2$ 

11.3단계. 에서 이전에 구성된 풀 이름을 IPv4 Address Pools 선택합니다. 에서 이전에 구성된 그룹 정책을 Group Policy 선택합니다. 을 Next 누릅니다.

Firewall Management Center Overview Analysis Polici	cies Devices Objects Integration	Deploy Q 🧬 🌣 🔕 admin 🗸 🔥 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 Secure Client -	4 Access & Certificate 5 Summary	
	(Realm or RADUG) Accounting Server:	
	Client Address Assignment:	
	Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.	
	Use AAA Server (Realm or RADIUS only)	
	Use DHCP Servers	
	Vse IP Address Pools	
	IPv4 Address Pools: posture_pool	
	IPv6 Address Pools:	
	Group Policy:	
	A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.	
	Group Policy:* posture_ap +	
	Edit Group Policy	



 $FMC\_New\_RAVPN\_Wizard\_3$ 

#### 11.4단계. Linux 이미지의 확인란을 선택합니다. 를 Next 클릭합니다.

Firewall Management Center Overview Analysis Devices / VPN / Setup Wizard	Policies Devices Objects In	tegration		Deploy Q 🚱 🌣 🔕 admin ~ 🔤
Remote Access VPN Policy Wizard				
1 Policy Assignment 2 Connection Profile 8 Secure Cli	ient 4 Access & Certificate	5 Summary		
	Remote Secure Client	Outside VPP	Inside Corporate Pressures	
	The VPN gateway can automatically de connection is initiated. Minimize connecti	ownload the latest Secure Client package to t ion setup time by choosing the appropriate OS fo	he client device when the VPN r 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 *	
	Minux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd	Linux	

Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_4

11.5단계. VPN 인터페이스의 인터페이스를 선택합니다. 9단계에서 FTD에 등록한 인증서 등록을 선택합니다. 를 Next 클릭합니다.

Firewall Management Center Overview Devices / VPN / Servp Wizard	r Analysis Policies I	evices Objects Integration	Deploy Q 💞 🌣 🛛 admin 🗸 📩 SECURE
Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile	3 Secure Client	Access & Certificate      S Summary	
	Remote User	Secure Clerk Internet Cutside Ven Indernet Composite Resources	
		Network Interface for Incoming VPN Access	
		Select or create an interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.	
		Interface group/Security Zone:* outside_zone +	
		Enable DTLS on member interfaces	
		All the devices must have interfaces as part of the Interface Group/Security Zone selected.	
		Device Certificates	
		Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.	
		Certificate Enrollment:* demo_vpn +	
		Enroll the selected certificate object on the target devices	
		Access Control for VPN Traffic	
		All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.	
		Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)	

Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_5

11.6단계. 요약 페이지에서 관련 정보를 다시 확인합니다. 모든 것이 좋으면 클릭하십시오Finish. 수정해야 할 사항이 있으면 을 클릭 합니다Back.



 $FMC\_New\_RAVPN\_Wizard\_6$ 

12단계. FTD에 새 컨피그레이션을 구축하여 원격 액세스 VPN 컨피그레이션을 완료합니다.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy Q	🚱 🕸 🕢 admin 🗸 🐝 SECURE
posture_vpn			Q. Advanced Deploy	] Ignore warnings Deploy Cancel
			Posture-FTD-CML27	Ready for Deployment ents.(1)
Connection Profile Access Interfaces Advanced				ty: None
				+
Name	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfttGrpPolicy		
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	E posture_gp	1 selected   👩 1 pending	20

FMC\_Deploy\_FTD

#### ISE의 컨피그레이션

13단계. 로 Work Centers > Posture > Network Devices 이동합니다. 를 Add 클릭합니다.

=	dentity Services	Engine					Work Centers	/ Posture				Q	۵	0	Q	<u>م</u>
Ц	Bookmarks	Overview	Network De	evices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
5	Dashboard															
15	Context Visibility	Net	work De	evices												
*	Operations												Selected 0	Total 4	Ø	ø
0	Policy	Ø Edit	+ Add	) Duplicate	🕁 Import 🏠 Export	Generate PAC	0 Delete 🗸							^	• ¥	7
2.	Administration		Name $\land$	IP/Mask	Profile Name	Location	Туре		Description							
■ 他 用 Bo 用 Di R Co 平 Pe 和 W ② Int	Work Centers	0	FTD-CML2		🛄 🛲 Cisco 🕕	All Locations	Firewall									
		0	FTD-CML2	1.00	m Cisco 🕕	All Locations	Firewall									
0	Interactive Help	0	FTD+CML2		🟥 Cisco 🕡	All Locations	Firewall									
■ 目 目 目 日 次 0 あ 。 一 の の つ つ	interactive netp	0	8.005	100.0	🟥 Cisco 🕧	All Locations	Firewall									

ISE\_Add\_New\_Device

13.1단계. 를 Name, IP Address입력하고 페이지를 아래로 스크롤합니다.

≡ :	dentity Service	s Engine				w	ork Centers / I	Posture		
Щ	Overview Netwo	rk Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Ⅲ ◎ ペ ●	Network Devices List Network Devic Name Description	> New Network D es posture-FTD	evice	_						
20 A	IP Addres	s ∨ * IP ;	······		¢					
?	Device Profile	👬 Cisco	~	0						
	Model Name Software Versio	n	``````````````````````````````````````							
	Network Device	Group								
	IPSEC	All Locations	0	~	Set To Default Set To Default					

ISE\_Add\_New\_Devices\_1

13.2단계. 의 확인란을 RADIUS Authentication Settings 선택합니다. 를 Shared Secret 제공합니다. 를 Submit 클릭합니다.

=	dealer Identity Services	Engine					v	Vork Centers / P	osture			۵ ۵	© Q   A	
щ	Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings				
	Dashboard		~ RADIUS Authen	tication Settings										
명	Context Visibility	·	RADIUS UDP Setting	15										
*	Operations		Protocol RA	DIUS										
0	Policy		Shared Secret		Show									
10	Administration		Use Second Shared	f Secret 🕕										
ส์เ	Work Centers		Seco Secre	nd Shared		Show								
1	Interactive Help		CoA Port	700	Set To Defa	ult								
			RADIUS DTLS Settin	gs ()										1
			DTLS Required											
			Shared Secret ra	diws/dtls										
			CoA Port 2	083	Set To Defa	uit								
			Issuer CA of ISE Certificates for CoA	Select if required (optional)	¥ ()									
			DNS Name											
			General Settings											
			🗌 Enable KeyWrap 🤅											
			Key Encryption Key		Show									
			Message Authenticator Code		Show									
			Key Inout Ecomat											
			ASCII O HEX	ADECIMAL										
			V TACACS Auther	ntication Settings										
			<ul> <li>SNMP Settings</li> </ul>											
			<ul> <li>Advanced Trust</li> </ul>	Sec Settings										
												Submit	Cancel	

ISE\_Add\_New\_Devices\_2

14단계. <u>Cisco Software Download</u>cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg에서 패키지 이름을 다운로드하 고 다운로드한 파일의 md5 체크섬이 Cisco Software Download 페이지와 동일한지 확인하여 파일이 정상인지 확인합니다. 패키지 이름 cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg이 1단계에서 성공적으로 다운로드되었습니다.

15단계. 로 Work Centers > Posture > Client Provisioning > Resources 이동합니다. 를 Add 클릭합니다. 를 Agent resources from local disk 선택합니다.

≡	duals Identity Services Engine			Wo	ork Centers /	Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
। । । ।	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 🌒 De	ieto				Sele	cted 0 Total 16 😅
Ψ.		Agent rese	ources from Cisco site		Ту	rpe ~	Version	Last Update	Description
-0		Agent res	ources from local disk		w	/inSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Prov
-file		Native Sup	oplicant Profile		N	ative Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agent Cor	figuration		N	ative Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agent Pos	ture Profile		м	acOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Prov
		AMP Enab	ler Profile	5.1.3.062	С	iscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure C
		CiscoSecure	ClientDesktopLinux 5.1	.3.062	C	iscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C
		CiscoSecure	ClientComplianceModu	leWindows 4.3.4015.819	92 C	iscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure C
		CiscoSecure	ClientComplianceModu	leLinux 4.3.3139.0	C	iscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure C
		CiscoAgenti	essWindows 5.0.03061		C	iscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgentl	essOSX 5.0.03061		C	iscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	oralAgentWindows 5.0.0	3061	C	iscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTempo	ralAgentOSX 5.0.03061		C	iscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE\_Upload\_Resource

15.1단계. 를 Cisco Provided Package선택합니다. cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg를 업로드하려면 클릭합니다 Choose File. 를 Submit 클릭합니다.

=	dentity Services E	ngine		Work Centers / Posture	۹	۵	0	Q	<u>୍</u>
Щ	Bookmarks								
-	Dashboard	Client Provisioning Policy	Agent Resources From Local	Disk > Agent Resources From Local Disk					
15	Context Visibility	Resources	Agent Resources Fr	m Local Disk					
*	Operations	Client Provisioning Portal							
.0	Policy								
80	Administration		Category	Cisco Provided Package V					
đ	Work Centers			Choose File cisco-secureeploy-k9 pkg					
(?)	Interactive Help			<ul> <li>Agent Uploaded Resources</li> </ul>					
				Name ^ Type Version Description					
				CiscoSecureClientDesktopLi CiscoSecureClientDe 5.1.3.62 Cisco Secure Client for II					
			Submit	ancel					



참고: 14단계를 반복하여 를 업로드합니다cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

16단계. 로 Work Centers > Posture > Client Provisioning > Resources 이동합니다. 를 Add 클릭합니다. 를 Agent Posture Profile선택합니다

=	dentity Services Engine				Work Cent	ers / Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Setting	S	
- <u>-</u>	Client Provisioning Policy Resources	Resources	6						
×								Selected 0 Total 16	Ø
0		C Edit + Add	Duplicate 📋 De	elete				$_{\rm All}\sim$	$\nabla$
*		Agent	resources from Cisco site	,	Version	Last Update	Description		
		Agent A	resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		
កា		Native	Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		
		Agent Agent	Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		
?		Agent I	Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			
		AMP E	habler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE\_Add\_Agent\_Posture\_Profile

#### 16.1단계. 를 Name, Server name rules 제공하고 나머지는 기본값으로 유지합니다. 를 Save 클릭합니다.

#### 이름: linux\_agent\_profile

#### 서버 이름 규칙: \*.example.com

≡ :#	dentity	Services Engine			Wa	ork Centers / I	Posture			
щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ 因 火 ● ▲0	Client Provis	lioning Policy	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	tings > New Profile						
?			Agent Behavior Parameter Enable debug log		Value No Y	D	escription nables the debug log	on the agent		

ISE\_Add\_Agent\_Posture\_Profile\_1

≡ :#	dentity	Services Engine			w	ork Centers / F	Posture		
FI.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
<b>同</b>	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
<b>a</b>			Retransmission Delay	() 60	secs		Time (in secon	ds) to wait bef	fore retrying.
Al.			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 up traffic to the Client Provisioning
			Discovery Backup Ser	ver List Choose	8		By default, Any PSNs sequenti as the backup discovery prob	Connect send ally if the PSN list and restrict es.	is 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 onnect to. E.g. " *.cisco.com"
			Call Home List 🕕				A list of IP add that the agent endpoint does	resses, that de will try to conn n't respond for	fines the all the Policy service nodes sect 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 connect max time limit	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
									Cancel Save

ISE\_Add\_Agent\_Posture\_Profile\_2

17단계. 로 Work Centers > Posture > Client Provisioning > Resources 이동합니다. 를 Add 클릭합니다. 를 Agent Configuration 선택합니다.

≡ :	see Identity	Services Engine				Work Cent	ers / Posture				
Щ	Overview	Network Devices	Client Prov	visioning Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports S	Settings		
	Client Provis Resources	ioning Policy	Reso	urces							
×	Client Provis	ioning Portal								Selected 0 Total 16	S
			🖉 Edit -	+ Add 🔿 📋 Duplicate 🛛 🔮 D	elete					$_{\rm All}\sim$	$\nabla$
U L				Agent resources from Cisco site	2	Version	Last Update	Description			
				Agent resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client	for li		
-file				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nativ	ve S		
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client	Linu		
?				Agent Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17				
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49				

ISE\_Add\_Agent\_Configuration

#### 17.2단계. 세부 정보를 구성합니다.

에이전트 패키지 선택: CiscoSecureClientDesktopLinux 5.1.3.062

- 이름: linux\_agent\_config
- 규정 준수 모듈: CiscoSecureClientComplianceModuleLinux 4.3.3139.0
- 의 확인란을 선택합니다. VPN, Diagnostic and Reporting Tool
- 프로파일 선택 ISE 상태: linux\_agent\_profile

#### 를 Submit 클릭합니다.

≡ ::	identity	Services Engine					Work Cent	ers / Postu	re
JI.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provis	sioning Policy	* Select Agent Package:	Cir	scoSecureClientDesktopLir	nux 5.1.3.062 V	1		
19	Client Provis	sioning Portal	* Configuration				J		
*			Name:						
0			linux_agent_config						
<b>a</b> 0			Description:						
				R.					
			Description Value N	otes					
			* Compliance Module	reClientComplianceModulel	Linux 4.3.~				
			Cisco Secure Client	Module Selection					
			ISE Posture						
			Network Visibility Diagnostic and Reporting						
			Profile Selection						
			* ISE Posture linux_agen	t_profile	Ý			S	ubmit Cance

ISE\_Add\_Agent\_Configuration\_1

18단계. 로 Work Centers > Posture > Client Provisioning > Client Provisioning Policy 이동합니다. 규칙 이름Edit 의 끝에서 을 클릭합니다 . 를 Insert new policy below선택합니다.

= :	diale Identity	Services	Engine									w	ork Ce	enters / Postu	re				
щ	Overview	Network	Devices	Clie	nt Provis	sioning	Policy Elemen	its	Posture Policy	<i>,</i>	Policy Sets	Troubl	eshoo	t Reports	Settings				
王 ら、火 し む	Client Provis Resources Client Provis	sioning Policy	]	CI Defii For / For I Wind Intel For I Mac If yo with	ient I Agent Con Native Sup dows Ager I architectu Windows A ARM64 po to configur Iout an ARI	Provis ent Provision figuration: v plicant Con nt, Mac Age ures. Mac pro- Agent ARM6 olicies requi e an ARM64 M64 condition	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	min gent profi ind e pa ions j po e an	e what users will recc profile, agent compil le and/or wizard. Dra Mac Agentless policié kckage for both archit ession: OS-Architect a arm64 configuratic for an OS, ensure endpoint is matched	eive up ance i g and es sup ecture ure E0 is. e that seque	pon login and use module, and/or ay drop rules to cha uport ARM64, Win 35. 2UALS arm64 in t the ARM64 policy antially with the policy	session i lent custo nge the or dows polid me Other ( lis at the f licies liste	initiation mization rder. cles run Conditio top of th ed in thi	1: n package. separate packaget ns column. he conditions list, a s window.	i for ARM4 and head of policies				
				$\sim$															
?						Rule Name			Identity Groups		Operating System	ems		Other Conditions			Result	ts	
				8		10S		H	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-I	ISE-NSP	Edit 🐱
				8		Android		If	Any	and	Android		and	Condition(s)		then	Cisco-I	ISE-NSP	Edit
																	(	Duplicate above Duplicate below Insert new policy at Insert new policy b	bove

#### 18.1단계. 세부 정보를 구성합니다.

규칙 이름: Linux

운영 체제: Linux All

결과: linux\_agent\_config

andDone 를 Save클릭합니다.

=	dentity	Services Engine					t				Wor	k C	enters / Postu	re				
Щ	Overview	Network Devices	Clie	nt Provisi	oning	Policy Element	s	Posture Policy	,	Policy Sets	Troubles	hoo	t Reports	Settings				
日代の代表	Client Provis Resources Client Provis	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 ARM64 policies, configurations. For Windows Agent ARM64 policies, configurations. Hy ou configure an ARM64 colicies, configurations. Hy ou configure an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.														
?			-		Rule Name IOS Android Linux		H i	Identity Groups Any Any Any	and and and	Operating Syste Apple IOS All Android Linux All	ems	and and and	Other Conditions Condition(s) Condition(s)		then then then	Results Cisco-ISE-NSP Cisco-ISE-NSP linux_agent_config	1	Edit ~ Edit ~ Edit ~

ISE\_Add\_New\_Provisioning\_Policy\_1

	dealer Identity Services Engine	Work Centers / Posture	
щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
ः ह	Conditions ~ Anti-Malware Anti-Spyware	File Conditions	Selected 0 Total 385 🧔 🔕
0	Anti-Virus Application	Q. Vew     Vew     0 Depleters     0 Depleters       Name     Description     File name     Condition Type	an V 🛛 🖓
# ,fi	Dictionary Compound Dictionary Simple	pc_XP64_X82797002_MS13 Cisce Predefined Check: SYSTEM_PROGRAMS\C Cisco-Defined     ws_44_K8134275_MSCisce Predefined Check:SYSTEM_PDOTNstrontlyCisco-Defined	8
(?)	Disk Encryption External DataSource	pr	
	File Firewall Hardware Attributes	pr_mt_cs_csudder_m. Cisco Predefined Check 3131Em_NOOTIspaniatv Cisco-Defined     pr_Vista64_X8925902_M50 Cisco Predefined Check SYSTEM_ROOTIwinsxsla Cisco-Defined	
	Patch Management Registry	pc_W10_64_1709_C845803 Cisco Predefined Check: STSTEM_KOOTIsyshattiv Cisco-Defined     pc_X0_k1265356_MS12-6 Cisco Predefined Check: SYSTEM_32(Wintrust.dll Cisco-Defined	
	Script Service USB	pc_VWB_KR2895074_V\$13 Cisco Predefined Check: SYSTEM_322Scrun.dll Cisco-Defined     pc_VWB_64_1909_K850139 Cisco Predefined Check: SYSTEM_ROOT\SysWO Cisco-Defined	
	Remediations >	pc_W7_K82681578_UX512         Cisco Predefined Check:         SYSTEM_32/Win32k.sys         Cisco-Defined           pc_W10_K83081436_M515         Cisco Predefined Check:         SYSTEM_32/LEdgehtml.dll         Cisco-Defined	
	Requirements Allowed Protocols	pc_W81_64_K83042553_M Cisce Predefined Check: SYSTEM_ROOT(sysnativ Cisco-Defined     pc_W8_64_K82727558_M5 Cisco Predefined Check: SYSTEM_ROOT(sysnativ Cisco-Defined	
	Authorization Profiles Downloadable ACLs	pc_W8_64_X8292611_M5       Cisco Predefined Check:       SYSTEM_ROOT(sysnativ       Cisco-Defined         pc_W7_K13078601_MS15       Cisco Predefined Check:       SYSTEM_32(Win32x.sys       Cisco-Defined	

ISE\_Add\_New\_File\_Condition

#### 19.1단계. 세부 정보를 구성합니다.

이름: linux\_demo\_file\_exist

운영 체제: Linux All

파일 유형: FileExistence

파일 경로: 홈, Desktop/test.txt

파일 연산자: 있음

를 Submit 클릭합니다.

≡	dentity Ser	rvices Engine					Work Cen	ters / Post	ure		
н	Overview N	letwork Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
	Conditions Anti-Malware Anti-Spyware Anti-Spyware Anti-Spyware Compound Dictionary Dictionary Disk Encryption External DataS File Firewall Herkoware Attri Patch Manager Registry Script Service USB	mpound pple n lource budes ment	File Conditions List > New I File Condition Name * Description * Operating System Compliance Module A * File Type * File Path * File Operator	File Condition	 ∠ ∠   _	lost.txt	]			Submit	Cancel
	Remediations Requirements Allowed Protocols Authorization Prot	s rites 2Ls									

 $ISE\_Add\_New\_File\_Condition\_1$ 

20단계. 로 Work Centers > Posture > Policy Elements > Requirements 이동합니다. 규칙 이름Edit 의 끝에서 을 클릭합니다. 를 Insert new Requirement 선택합니다.

									Work	Centers / Post	ture					
JЦ В	ookmarks	Overview	Network Devices	Client Provisioning	Policy	Elements	Posture P	Policy Policy Sets	Tro	ubleshoot R	leports \$	ettings				
III D	sshboard ontext Visibility	Conditions Anti-Malw	÷									Guide Me				
* •	perations	Anti-Spyw	are	Requirements												
() Р	licy	Anti-Virus Apolicatio		Name		Operating Syst	em	Compliance Module		Posture Type		Conditions		Remediations Actions		
8. 4	impletration	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 🖂	
#0 N		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	Juplicat
a w	ork 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	nsert ne
		Disk Encry	ption	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit	helete
(?) In	teractive 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 🗵	1
		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	gnieu	Agent	met if	ANY_as_mac_inst	then	Message Text Only	Edit 🤟	
		Patch Man	agement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 🛩	
		Registry		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 👻	
		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 👻	Ĩ.,
		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 Proto	scols	US0_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 🤟	
		Authorization Downloadable	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	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	t for	Windows All	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟	
				Default_Hardware_Attribues_Requirement_Mac	t 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

#### 20.1단계. 세부 정보를 구성합니다.

이름: Test\_exist\_linux

운영 체제: Linux All

Compliance Module: 4.x 이상

#### 포스처 유형: 에이전트

조건: linux\_demo\_file\_exist

andDone 를 Save클릭합니다.

≡ ;	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 Darest
						Save

ISE\_Add\_New\_Posture\_Requirement\_1



**참고**: 현재로서는 Linux 에이전트에 대한 셸 스크립트만 교정으로 지원됩니다.

21단계. 로 Work Centers > Posture > Policy Elements > Authorization Profiles 이동합니다. 를 Add 클릭합니다.

21.1단계. 세부 정보를 구성합니다.

이름: unknown\_redirect

의 확인란을 선택합니다. Web Redirection(CWA,MDM,NSP,CPP)

선택 Client Provisioning(Posture)

ACL: 리디렉션

#### 값: Client Provisioning Portal(기본값)

≡ :	dentity Services Engine	Work Centers / Posture
щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
11 13 10 10 10 10 10 10 10 10 10 10 10 10 10	Conditions     >       Anti-Maiware       Anti-Spyware       Anti-Virus       Application       Compound       Dictionary Compound       Dictionary Simple       Disk Encryption       External DataSource       File       Firewall       Hardware Attributes       Patch Management	Authorization Profile   * Name   unknown_redirect   Description   * Access Type   ACCESS_ACCEPT   Network Device Profile   mclisco   Service Template   Image: Track Movement   Image: Im
	Registry Script Service USB Remediations Requirements Allowed Protocols Authorization Profiles Deschartable ACI s	<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 redirect</li> <li>Value Client Provisioning Portal (def: ~</li> <li>Static IP/Host name/FQDN</li> <li>Suppress Profiler CoA for endpoints in Logical Profile</li> </ul>

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



**참고**: 이 ACL 이름 리디렉션은 FTD에 구성된 해당 ACL 이름과 일치해야 합니다.

21.2단계. 를 반복하여 Add 세부사항과 함께 규정준수 위반 및 규정준수 엔드포인트에 대한 또 다른 두 개의 권한 부여 프로파일을 생성합니다.

이름: non\_compliant\_profile

DACL 이름: DENY\_ALL\_IPv4\_TRAFFIC

이름: compliant\_profile

DACL 이름: PERMIT\_ALL\_IPv4\_TRAFFIC



**참고**: 규정 준수 또는 비준수 엔드포인트에 대한 DACL은 실제 요구 사항에 따라 구성해야 합니다.

22단계. 로 Work Centers > Posture > Posture Policy 이동합니다. 규칙Edit 의 끝에 있는 을 클릭합니다. 를 Insert new policy선택합니다.

							_								~		-	~ 1	h
The Identity Services	Engine						_	Work Centers /	Pos	ture					Q	4	0	<b>Q</b>	
Bookmarks	Overview	v Ne	work Devices	Client Provisioning Po	olicy Elements	Posture Policy Poli	cy Set	s Troubleshoot	5	teports Settings									
Dashboard		_	_		Ľ														
Context Visibility		Post	ure Policy	Guide Me															
Operations		Define the	Posture Policy by o	onfiguring rules based on operat	ing system and/or othe	conditions.										<i></i>			
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 05X	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Ma c	Edit 🤟					
			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ir Any	and Mac 05X	and	4.x or later	and	Temporal Agent	and	the	Any_AM_Installation_Ma c_temporal	Edit Insert new policy					
D Interactive Help			Policy Options	Default_AntiMalware_Policy_Win	ii Any	and Windows All	and	4.x or later	and	Agent	and	the	Any_AM_Installation_Win	Edit Celete					
			Policy Options	Default_AntiMalware_Policy_Win_temporal	if Any	and Windows All	and	4.x or later	and	Temporal Agent	and	then	Any_AM_installation_Win_temporal	Edt -					
			Policy Options	Default_AppVis_Policy_Mac	r Any	and Mac OSX	and	4.x or later	and	Agent	and	the	Default_AppVis_Require ment_Mac	Edit v					
			Policy Options	Default_AppVis_Policy_Mac_temporal	ir Any	and Mac 05X	and	4.x or later	and	Temporal Agent	and	044	Default_AppVis_Require ment_Mac_temporal	Edit 🤟					
			Policy Options	Default_AppVis_Policy_Win	i' Any	and Windows All	and	4.x or later	and	Agent	and	then	Default_AppVIs_Require ment_Win	Edit 9					
			Policy Options	Default_AppVIs_Policy_Win_te mporal	i' Any	and Windows All	and	4.x or later	and	Temporal Agent	and	their	Default_AppVis_Require ment_Win_temporal	Edit +					
			Pulicy Options	Default_Firewall_Policy_Mac	i' Any	and Mac 05X	and	4.x or later	and	Agent	and	the s	Default_Firewalt_Require ment_Mac	Edt y					
			Policy Options	Default_Firewall_Policy_Mac_te mporal	r Any	and Mac OSX	and	4.x or later	and	Temporal Agent	and	ther	Default_Firewall_Require ment_Mac_temporal	Edit +					
			Policy Options	Default_Firewall_Policy_Win	ir Any	and Windows All	and	4.x or later	and	Agent	and	then	Default_Firewall_Require ment_Win	Edit v					
			Policy Options	Default_Firewall_Policy_Win_te mporal	i' Any	and Windows At	and	4.x or later	and	Temporal Agent	and	the	Default_Firewalt_Require ment_Win_temporal	Edt y					
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	i' Any	and Mac 05X	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Mac	Edt					
			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	т Алу	and Windows All	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Win	Edt ×					
		-	·····	-				* - 11 Mali		*			-						

ISE\_Add\_New\_Posture\_Policy

#### 22.1단계. 세부 정보를 구성합니다.

규칙 이름: Demo\_test\_exist\_linux

ID 그룹: 모두

운영 체제: Linux All

Compliance Module: 4.x 이상

포스처 유형: 에이전트

요구 사항: Test\_exist\_linux

andDone 를 Save클릭합니다.

Post	ture Policy	Guide Me configuring rules based on opera	ting syste	m and/or other co	nditi	ons.									~
~															
	Policy Options	Default_Firewall_Policy_Mac	II Any	80	d A	lac OSX	and	4.x or later	- an	d A	pent	and	the	<ul> <li>Default_Firewall_Require ment_Mac</li> </ul>	Edit 🗸
	Policy Options	Default_Firewall_Policy_Mac_te mporal	II Any	an	d A	Aac OSX	and	4.x or later	-24	d Te	imporal Agent	and	the	n Default_Firewall_Require ment_Mac_temporal	Edit 😔
	Policy Options	Default_Firewall_Policy_Win	If Any	an	d N	Nindows All	and	4.x or later	an.	d A	pent	and	the	<ul> <li>Default_Firewall_Require ment_Win</li> </ul>	Edit 😔
	Policy Options	Default_Firewall_Policy_Win_temporal	If Any	an	d V	Windows All	and	4.x or later	- 80	d Te	Imporal Agent	and	the	<ul> <li>Default_Firewall_Require ment_Win_temporal</li> </ul>	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	II Any	an	d N	/ac OSX	and	4.x or later	20	d A	pent	and	the	Default_Hardware_Attrib utes_Requirement_Mac	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	ii Any	an	d N	lac OSX	and	4.x or later	20	d Te	emporal Agent	and	the	<ul> <li>Default_Hardware_Attrib utes_Requirement_Mac_ temporal</li> </ul>	Edit 🐱
	Policy Options	Default_Hardware_Attributes_P olicy_Win	II Any	an	d N	Nindows All	and	4.x or later	- 20	d A	pent	and	the	Default_Hardware_Attrib utes_Requirement_Win	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	II Any	an	d V	Mindows All	and	4.x or later	an	d Te	emporal Agent	and	the	Default_Hardware_Attrib utes_Requirement_Win_t emporal	Edit 😔
	Policy Options	Default_US8_Block_Policy_Win	II Any	an	d V	Windows All	and	4.x or later	an	d A	gent	and	the	US8_Block	Edit 😔
	Policy Options	Default_USB_Block_Policy_Win	If Any	an	d V	Windows All	and	4.x or later	20	d Te	emporal Agent	and	the	USB_Block_temporal	Edit 😔

ISE\_Add\_New\_Posture\_Policy\_1

#### 23단계. 로 Work Centers > Posture > Policy Sets 이동합니다. 클릭하여 다음을 Insert new row above 수행합니다.

=	dentity Services E	Engine					Work Centers /	Posture			۵ ۵	0	٥	<u>م</u> ا
F	Bookmarks	Overview	Network Devices	Client Provisionin	ng Policy Elements	Posture Policy Policy	Sets Troubleshoot	Reports	Settings					
81 13	Dashboard Context Visibility	5	Policy Sets							Reset Policys	et Hitcounts		Save	
*	Operations		<ul> <li>Status Policy Set</li> </ul>	t Name Desc	cription Con	ditions				Allowed Protocols / Server Seque	tce Hits	Action	s Viev	
U	Policy		Q Search											
3. 4	Administration Work Centers		O Default	Defaul	ult policy set					Default Network Access	+ 0	\$	>	
٢	Interactive Help									Ince	rt new row a Reset	bove	Save	

ISE\_Add\_New\_Policy\_Set

23.1단계. 세부 정보를 구성합니다.

정책 집합 이름: 방화벽 상태

조건: 네트워크 액세스 장치 IP 주소 EQUALs [FTD IP 주소]

를 클릭합니다 Save .

=	dealer Identity Services	Engine								Work Centers /	Posture						۹	۵	۲	<b>0</b>	۹
F.	Bookmarks	Overview	Network	Devices	Client Provisi	ioning I	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings									
11  13	Dashboard Context Visibility	р	olicy Sets											Res	et J	aset Polic	yset Hitc	cunts		Save	
*	Operations		🕣 Status	Policy Set N	iame I	Description	Con	ditions						Allowed Pr	rotocols / Se	rver Sequ	ence	Hits /	Actions	View	
Ð	Policy		Q. Search																		
8.	Administration		۰	Firewall Postu	•		0	Network Access Device	IP Address EQUALS					Default N	etwork Acce	н 2	2 +	,	٨	,	
ส์เ	Work Centers		0	Default		Default policy a	urt							Default N	etwork Acce	0 J	/ +	•	Ø	>	
٢	Interactive Help																	Reset		Save	

ISE\_Add\_New\_Policy\_Set\_1

23.2단계. 정책 집합을 입력하려면 클릭하십시오>. 포스처 호환, 비호환, 알 수 없음 상태에 대한 새 권한 부여 규칙을 생성합니다. 를 Save 클릭합니다.

compliant\_profile 준수

Non\_compliant\_profile 준수 안 됨

알 수 없음(unknown\_redirect)

= -	disco Identi	ity Se	rvice	s Engine				Work Cen	ters / Postu	ire						
ц	Overview	v I Q 20	Netwo	rk Devices Client F	Provisioning Policy E	Elements Posture Pol	icy Policy Sets	Troubleshoot	Reports	Settings						
15		•		irewall Posture		P Network Access-Device	IP Address EQUALS :						Default Networ	k Access	1	+ 0
*	~A/	wthent	ication	Policy(1)												
0		+ S	tatus	Rule Name	Conditions							Use			Hits	Actions
#0 		Q 8	earch													
								+								
•				Default								All_User_ID	_Stores	0	48	念
												> Options				121
	> A/	uthoriz	ation P	olicy - Local Exceptions												
	> A/	uthoriz	ation P	olicy - Global Exceptions												
	∼A	uthoriz	ation P	olicy(4)												
										Results						
		⊕ S <sup>1</sup>	tatus	Rule Name	Conditions					Profiles		Security Gro	ups		Hits	Actions
		Q 5	earch													
			0	Compliant	と Session-PostureStatus	EQUALS Compliant				compliant_profile	<i>i</i> +	Select from	list	/ +	15	¢۶
		[	0	Non_Compliant	E Session PostureStatus	EQUALS NonCompliant				non_compliant_profile	<i>ø</i> +	Select from	list	/ +	5	(2)
			0	Unknown	E Session-PostureStatus	EQUALS Unknown				unknown_redirect	0 +	Select from	list	1 +	47	(2)

ISE\_Add\_New\_Policy\_Set\_2

#### Ubuntu 구성

24단계. GUI를 통해 Ubuntu 클라이언트에 로그인합니다. VPN 포털에 로그인하려면 브라우저를 엽니다. 이 예에서는 demo.example.com입니다.

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

Logon
Group posture_vpn v Username
Password
Logon

Ubuntu\_Browser\_VPN\_Log

25단계. 를 Download for Linux 클릭합니다.

Cisco	Secu	re Client Inst	allati	:	+															e	ē	×
$\leftarrow$	$\rightarrow$	C	0 &		https:	//dem	o.exa	mple	.com	n/CAC	CHE/	/stc/2	/inde	ex.htm	l	F	80%	ជ	•	$\bigtriangledown$	$\checkmark$	≡
		secure	re Client	t																		
		C		C	Cisc	0 5	Sec X	ure	e C	Clie	en	t D	)ov	vnlc	oad							A
								D	ow	nlo	ad	8	Inst	tall								
							Downlo	ad Cisc	co Sec	cure Cli Downl	lient a	and inst	all it on NUX	i your coi	mputer.							
																	🔁 Ins	structi	ons			

 $Ubuntu\_Browser\_VPN\_Download\_1$ 

다운로드한 파일 이름은 입니다cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu\_Browser\_VPN\_Download\_2

26단계. 브라우저를 통해 VPN 인증서를 다운로드하고 파일 이름을 <certificate>로 변경합니다.crt. Firefox를 사용하여 인증서를 다운 로드하는 예입니다.

-	demo.example.	com/+CSCOE× +		$\sim$	-	ē	×
$\leftarrow$	$\rightarrow$ C	O 🔓 https://demo.ex	ample.com/+CSCOE+/logon.html#form_title_text	${igardown}$	۲	பி	≡

General M Website Iden Website: Dwner:	tedia <u>P</u> ermissions ntity demo.example.com	Security					
<b>Website Ide</b> Website: Owner:	ntity demo.example.com						
Website: Owner:	demo.example.com						
Owner:	This website does a	at supply averaghin in	Formation				
Verified by:	C=CN,CN=demo.exa	mple.com	rormation.	<u>V</u> iew Certificate			
Privacy & His Have I visited	<b>story</b> I this website prior to	o today?	No				
s this websit	e storing informatio	n 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			
<b>Fechnical De</b> Connection E The page you Encryption m :herefore un	etails Encrypted (TLS_AES_ a are viewing was en bakes it difficult for u likely that anyone re	128_GCM_SHA256, 12 crypted before being t inauthorized people to ad this page as it trave	8 bit keys, TLS 1.3) ransmitted over the view information tr led across the netwo	Internet. aveling between computers. It ork. Help			

Untu\_Browser\_VPN\_Cert\_Download

27단계. Ubuntu 클라이언트에서 터미널을 엽니다. Cisco Secure Clientpath home/user/Downloads/를 설치하려면 로 이동합니다.

```
<#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\$

28단계. Ubuntu 클라이언트에서 VPN 포털 인증서를 신뢰합니다.

#### <#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

29단계. Ubuntu 클라이언트에서 Cisco Secure Client를 열고 VPN을 demo.example.com에 연결했습니다.

		Cisco Secure	Client		•		×
AnyConnect VPN / Statistics About							
		ייןיי כוsc	11 0				
Connect to:	demo.exa	ample.com			~	3	\$
Group:	posture_v	pn				~	- )
Username:	isetest						
Password:	*****						



*Ubuntu\_Secure\_Client\_*연결됨

30단계. 브라우저를 열어 ISE CPP 포털로의 리디렉션을 트리거하는 웹 사이트에 액세스합니다. ISE CPP 포털에서 인증서를 다운로 드하고 파일 이름을 <certificate>.crt로 바꿉니다. 이는 Firefox를 사용하여 다운로드하는 예입니다.



*Ubuntu\_Browser\_CPP\_Cert\_*다운로드

30.1단계. Ubuntu 클라이언트에서 ISE CPP 포털 인증서를 신뢰합니다.

#### <#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.
```

31단계. ISE Start CPP 포털을 클릭합니다.

O Device Security Check × +		ō	×					
← → C () A https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08 ☆	6	Ð	≡					
1 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. Start Ubuntu_Browser_CPP_시작 32단계. Click here to download and install Agent.								
Device Security Check × +		ē	×					
$\leftarrow \rightarrow C \qquad https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL \cond the conduction is the conductive of the cond$	2	Ð	≡					
You must log in to this network before you can access the Internet.			×					

**Client Provisioning Portal** 

#### **Device Security Check**

uluilu cisco.

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.
+ Remind me what to do next



33단계. Ubuntu 클라이언트에서 터미널을 엽니다. Posture 모듈을 home/user/Downloads/ 설치하기 위한 경로로 이동합니다.

#### <#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.

34단계. Ubuntu 클라이언트 UI에서 Cisco Secure Client를 종료하고 다시 엽니다. ISE Posture 모듈이 설치되고 성공적으로 실행됩니다.



Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed

35단계. Ubuntu 클라이언트에서 터미널을 엽니다. 경로home/user/Desktop로 이동하여 ISE에test.txt 구성된 파일 조건을 충족하도록 파 일을 생성합니다.

#### <#root>

user@ubuntu22-desktop:~\$

#### cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. Ubuntu 클라이언트에서 VPN을 demo.example.com에 연결합니다.

	- • ×									
AnyConnect VPN	✓ Statistics	🛞 ISE Posture	About							
cisco										
Connect to: demo.example.com 🗸										
Group: posture_vpn ~										
Username: isetest										
Password:										

× D	Disconnect
Connected to demo.example.com.	

 $Verify\_Ubuntu\_Secure\_Client\_Connected$ 

2단계. Ubuntu 클라이언트에서 ISE Posture 상태를 확인합니다.



Verify\_Ubuntu\_Secure\_Client\_Compliance

#### 3단계. ISE에서 Radius Live Log(RADIUS 라이브 로그)를 선택합니다. 로 Operations > RADIUS Live Log 이동합니다.

≡	dentity Services Engine			Oper	ations / RADIUS			
Щ	Live Logs Live Sessions							
::								
10	Misconfigured Supplicants 🕕	Miscor	figured Network Devi	ces 🕕	RADIUS Drops		Client Stopped Responding ①	Repeat Counter ①
*	0		0		0		0	0
U							Refresh Show	Within
80							Never v Latest 20 re	cords 🗸 Last 24 hours 🗸
di.	💭 🖕 Reset Repeat Counts ර	🗅 Export To 🗸						Filter 🗸 🐵
	Time	Status Details	Identity I	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 5	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default F	irewall Posture >> Compliant
	May 29, 2024 09:08:48.798 PM	2 .		52:54:00:17:6B:FA		Compliant	Firewall Posture	irewall Posture >> Compliant
	May 29, 2024 09:08:13.570 PM	2	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default F	irewall Posture >> Unknown

Verify\_ISE\_LiveLog

4단계. SSH 또는 콘솔을 통해 FTD CLI로 이동합니다.

#### <#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

#### 문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

Cisco Secure Client 및 ISE의 상태 흐름 및 문제 해결에 대해서는 CCO 문서ISE Posture Style Comparison for Pre and Post 2.2 and Troubleshoot ISE Session Management and Posture를 참조하십시오.

관련 정보

<u>Cisco Identity Services Engine 네트워크 구성 요소 호환성, 릴리스 3.3</u>

- <u>Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3</u>
- <u>Cisco 기술 지원 및 다운로드</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.