



Cisco ISE Posture para VPN de Acceso Remoto con Cisco Secure Client

Comunidad de Cisco

Adrián Lira – Team Captain

Javier Acevedo – Technical Consulting Engineer

Jueves 7 de noviembre de 2024



Conecte, Interactúe, ¡Colabore!

Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.

Aceptar como solución

Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!

👍 0 Útil

Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los premios Spotlight Awards se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de [Mayo-Julio 2024](#)

¡Ahora también puedes nominar a un candidato! [Haga clic aquí](#)



Nuestros expertos

Adrián Lira



Team Captain

Es Ingeniero egresado del Instituto Politécnico Nacional bajo la especialidad en Comunicaciones y Electrónica impartida en ESIME.

Se unió a Cisco en 2019 al equipo de AAA como TAC Engineer certificado en CCNA y DEVNET ayudando a la resolución de casos de la plataforma ISE (Identity Services Engine) y sus diversas integraciones.

Actualmente se desempeña como capitán del equipo atendiendo casos complejos, escalaciones y documentando artículos de configuración y troubleshooting.

Nuestros expertos

Javier Acevedo



Technical Consulting Engineer

Es Ingeniero en Comunicaciones y Electrónica, egresado del Instituto Politécnico Nacional. Anteriormente trabajó como Ingeniero de soporte en Megacable (MCM Telecom) dentro del Centro de Control de la red.

En 2022 se unió a Cisco como Technical Consulting Engineer, obtuvo las certificaciones de CCNA y DEVNET. A continuación, comenzó a trabajar en el equipo de VPN convirtiéndose en experto en las tecnologías como AnyConnect, DMVPN, GETVPN, FlexVPN, etc.

Actualmente se encuentra trabajando, dando soporte a clientes con problemas en estas tecnologías específicas y apoya a la creación de contenido de calidad para nuestros clientes.

slido

Join at
slido.com
#2535 244



Cisco ISE Posture para VPN de Acceso Remoto con Cisco Secure Client

En este webinar...

Exploraremos cómo integrar Cisco Identity Services Engine (ISE) con Cisco Secure Client para planificar y asegurar el cumplimiento de dispositivos mediante un enfoque de postura en conexiones VPN de acceso remoto.

Aprenderán cómo Cisco ISE puede mejorar la seguridad evaluando el estado de los dispositivos que se conectan a la red, asegurando que solo aquellos que cumplan con las políticas establecidas puedan acceder.

También abordaremos técnicas de solución de problemas para optimizar la integración.



Agenda



1. Introducción a Cisco ISE y Cisco Secure Client
2. Descripción y funcionamiento de Posture
3. Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
4. Configuración básica
 - ISE: Políticas de provisionamiento y autorización
 - VPN: Acceso Remoto con Cisco Secure Client
5. Demo
6. Comprobación: Monitoreo y Reportes
7. Mejores Prácticas y Troubleshooting



Introducción a Cisco ISE y Cisco Secure Client

- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
- Configuración básica: ISE y VPN
- Demo
- Comprobación: Monitoreo y Reportes
- Mejores Prácticas y Troubleshooting



Introducción a Cisco ISE

Cisco Identity Services Engine (ISE) es una Plataforma centralizada de seguridad diseñada para la implementación de políticas de acceso. Las bases de Cisco ISE son la Autenticación, Autorización y Accounting (AAA).

Entre otras características se tienen:

- Evaluación del estado de Posture
- Segmentación de Red (TrustSec, SGTs)
- Visibilidad y Control (Context Visibility, Profiling)
- Diversidad de integraciones Active Directory, Pxgrid, Passive ID, etc.



Introducción a Cisco Secure Client VPN Acceso Remoto



Cisco Secure Client, antes Cisco AnyConnect, es una solución basada en módulos cuya función principal es garantizar acceso seguro a redes empresariales remotamente con el módulo principal VPN core, o localmente con el módulo NAM (Network Access Manager).

Entre otras características se tienen:

- Evaluación de Posture
- Inclusión de módulos para visibilidad (Secure Endpoint, AMP)
- Autenticación Multifactor

Descripción y funcionamiento de Posture

- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture**
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
- Configuración básica: ISE y VPN
- Demo
- Comprobación: Monitoreo y Reportes
- Mejores Prácticas y Troubleshooting



Join at
slido.com
#2535 244

¿Cuál es el rol principal de Cisco ISE en un entorno de acceso remoto por VPN?

a) Gestionar conexiones VPN

0%

b) Evaluar la postura de los dispositivos y hacer cumplir las políticas de red

0%

c) Proteger los dispositivos finales mediante firewalls

0%

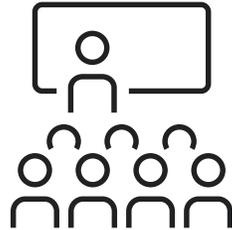
d) Proporcionar autenticación multifactor para los usuarios de VPN

0%

Descripción y funcionamiento de ISE Posture

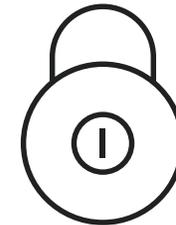
ISE Posture

La "postura" en Cisco ISE se refiere a la evaluación y verificación del estado de seguridad de los dispositivos antes y durante su acceso a la red

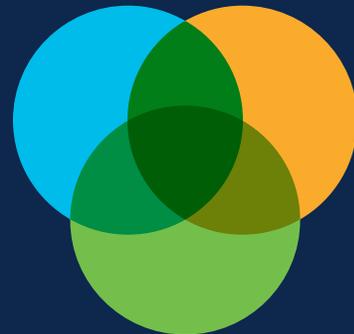


Asegurar acceso

Es una funcionalidad para asegurar que solo dispositivos que cumplen con las políticas de seguridad de la organización puedan acceder a los recursos de la red corporativa



Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment



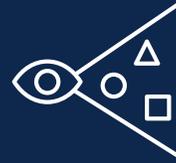
- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment**
- Configuración básica: ISE y VPN
- Demo
- Comprobación: Monitoreo y Reportes
- Mejores Prácticas y Troubleshooting

Interacción entre Cisco ISE y Secure Client

Cisco ISE y Secure Client se pueden implementar para la evaluación de Posture, garantizando así:



Conexión remota segura



Escaneo y cumplimiento
de políticas de Posture



Acceso a la Red de
acuerdo con el estado
de Posture

ISE Posture VS Secure Firewall Posture (Hostscan)

Alcance

ISE Posture: Es más amplio y centralizado, puede aplicarse a diferentes tipos de acceso a la red (cableado, inalámbrico, VPN).

Secure Firewall Posture: Está específicamente diseñado para evaluar la postura de dispositivos en conexiones VPN.



Funcionalidad de Remediación

ISE Posture: Capacidades amplias de remediación y puede integrarse con soluciones de gestión de parches y actualizaciones de una amplia variedad de productos.

Secure Firewall Posture: Enfocado en permitir o denegar el acceso basado en la evaluación de postura, con opciones limitadas de remediación.



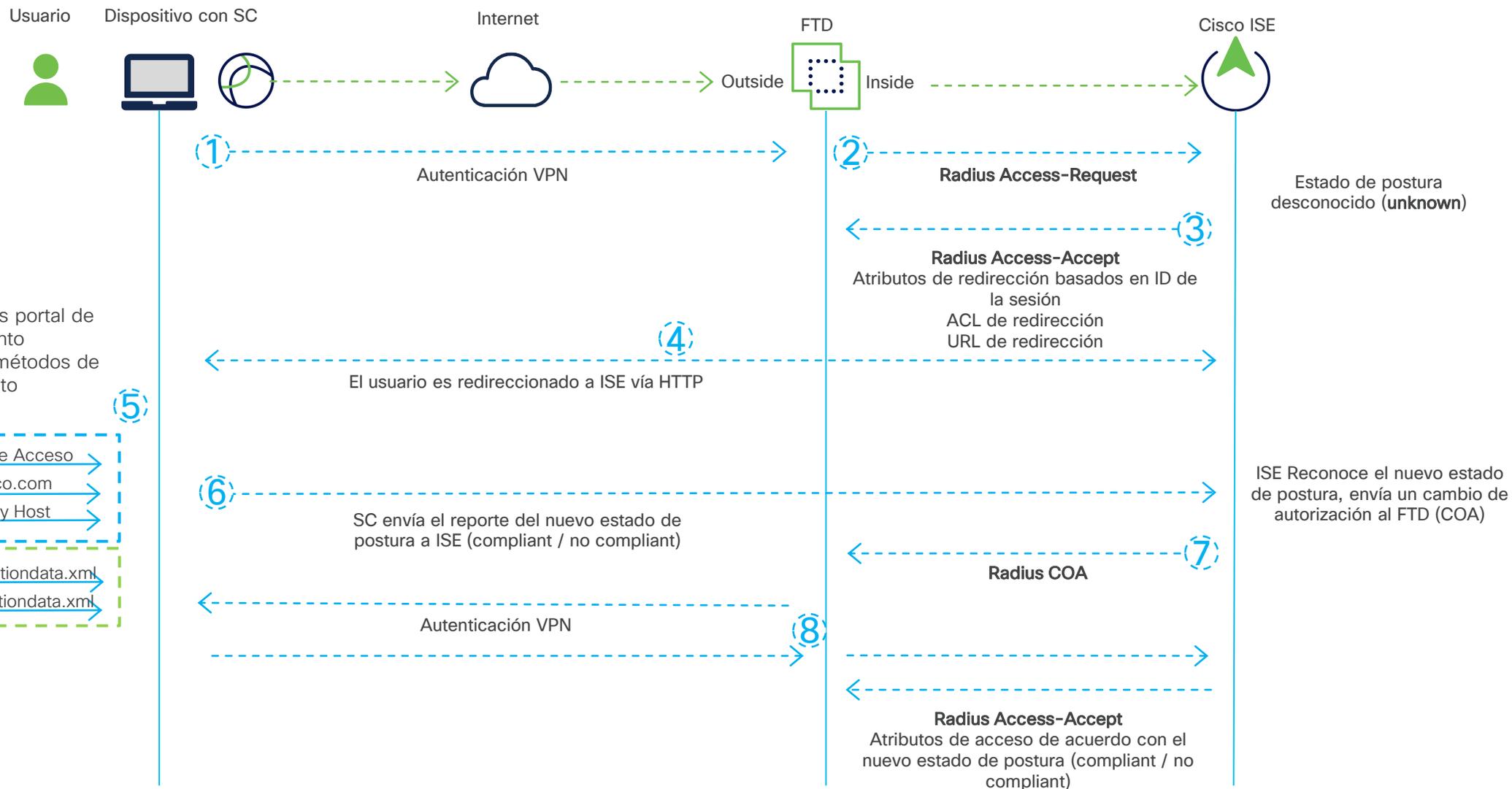
Catálogo

ISE Posture: Incluye una amplia variedad de condiciones de postura como, cifrado de disco, manejo de parches, backup, etc.

Secure Firewall Posture: Tiene condiciones de postura limitadas, antimalware, firewall, ip, certificados.



Flujo de Posture ISE-Secure Client con Redirección





¿Qué acción se toma si un usuario no cumple con los requisitos de postura en Cisco ISE durante el acceso a la red?

a) Se bloquea el acceso a la red completamente

0%

b) Se aplica una acción de remediación configurada

0%

c) Se le asigna una nueva dirección IP

0%

d) Se le permite el acceso limitado solo a servicios críticos

0%

Join at
slido.com
#2535 244

Configuración básica: ISE y VPN

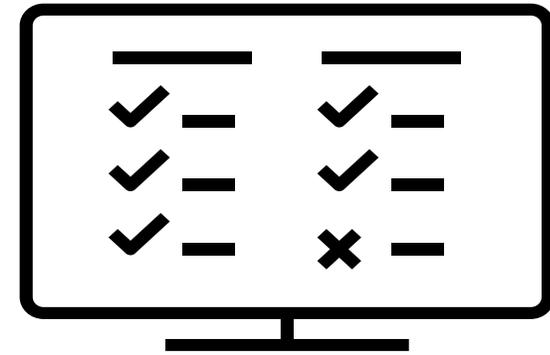
- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
- Configuración básica: ISE y VPN**
- Demo
- Comprobación: Monitoreo y Reportes
- Mejores Prácticas y Troubleshooting



Configuración Cisco ISE



Configuraciones Iniciales de Posture



Configuración Inicial de Posture

Paso 1: Actualización de Base de datos de Posture

Administration > System > Settings > Posture > Updates.



Posture Updates

Web Offline

* Update Feed
URL

<https://www.cisco.com/web/>

Set to Default

Proxy Address



Proxy Port

Automatically check for updates starting from initial delay

HH

23

MM

47

SS

39

every 2

hours

Save

Update Now

Reset

<https://www.cisco.com/web/secure/spa/posture-offline.html>

Configuración Inicial de Posture

Paso 2: Ajustes Generales

Administration > System > Settings > Posture > General Settings



Posture General Settings

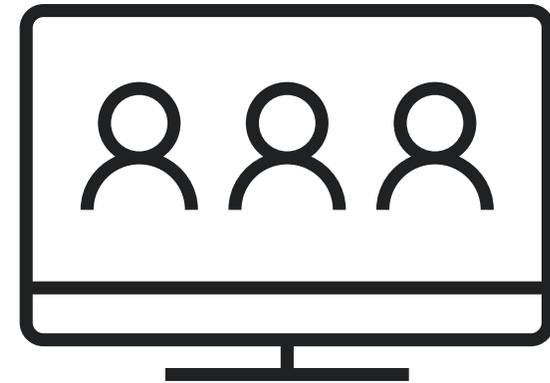
These settings will be used if there is no profile under client provisioning policy.

Remediation Timer	10	Minutes	?
Network Transition Delay	3	Seconds	?
Acceptable Use Policy in Stealth Mode	Block		?
Default Posture Status	NonCompliant		?
<input type="checkbox"/> Automatically Close Login Success Screen After	0	Seconds	?
<input checked="" type="checkbox"/> Continuous Monitoring Interval	15	Minutes	?

Posture Lease

<input checked="" type="radio"/> Perform posture assessment every time a user connects to the network			
<input type="radio"/> Perform posture assessment every	1	Days	?
<input type="checkbox"/> Cache Last Known Posture Compliant Status			
Last Known Posture Compliant State	0	Minutes	?

Provisionamiento: Recursos y políticas



Configuración Básica ISE: Provisionamiento

Paso 1: Descargar módulo de Cumplimiento (CM)

Policy > Policy Elements > Results > Client Provisioning > Resources

Add > Agent Resources From Cisco Site

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3320.0	Cisco Secure Client Linux Compliance Module 4.3.3320.0
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3357.0	Cisco Secure Client Linux Compliance Module 4.3.3357.0
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3698.6400	Cisco Secure Client OSX Compliance Module 4.3.3698.6400
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3735.6400	Cisco Secure Client OSX Compliance Module 4.3.3735.6400
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.4214.8192	Cisco Secure Client Windows Compliance Module 4.3.4214.8192
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.4248.8192	Cisco Secure Client Windows Compliance Module 4.3.4248.8192
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.4214...	Cisco Secure Client WindowsARM64 Compliance Module 4.3.4214...
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.4248...	Cisco Secure Client WindowsARM64 Compliance Module 4.3.4248...
<input type="checkbox"/>	AnyConnectComplianceOSX 4.3.3698.6400	Cisco Secure Client for OSX With CM 4.3.3698.6400

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Configuración Básica ISE: Provisionamiento

Paso 2: Descargar y subir Imagen de Cisco Secure Client

[https://software.cisco.com/download/Policy > Policy Elements > Results > Client Provisioning Add > Agent Resources From Local Disk](https://software.cisco.com/download/Policy%20>%20Policy%20Elements%20>%20Results%20>%20Client%20Provisioning%20Add%20>%20Agent%20Resources%20From%20Local%20Disk)

Cisco Secure Client Headend Deployment Package (Windows) 24-Sep-2024 145.00 MB   

[cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg](#)

[Advisories](#) 

[Agent Resources From Local Disk](#) > [Agent Resources From Local Disk](#)

Agent Resources From Local Disk

Category Cisco Provided Package  

cisco-secure-...eploy-k9.pkg

Agent Uploaded Resources

Name	Type	Version	Description
CiscoSecureClientDesktopW...	CiscoSecureClientDe...	5.1.6.103	Cisco Secure Client for ...



[Cancel](#)

Configuración Básica ISE: Provisionamiento

Paso 3: Configuración del perfil de posture para Secure Client (Agente)

Policy > Policy Elements > Results > Client Provisioning

Add > Agent Configuration

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ	1.2.3.4	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.

Configuración Básica ISE: Provisionamiento

Paso 4: Configuración del perfil del Agente SC

Policy > Client Provisioning > Resources

> Agent Configuration > New agent configuration

The screenshot shows the Cisco ISE Client Provisioning configuration page. The navigation tabs at the top are Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, and Troubleshoot. The left sidebar shows Client Provisioning Policy, Resources (selected), and Client Provisioning Portal. The main content area is titled 'New agent configuration' and contains several fields:

- Select Agent Package:** CiscoSecureClientDesktopWindows 5.1.6.103
- Configuration Name:** CSC Agent Configuration
- Description:** (empty text area)
- Description Value Notes:** (empty text area)
- Compliance Module:** CiscoSecureClientComplianceModuleWindows
- Cisco Secure Client Module Selection:**
 - ISE Posture
 - VPN
 - Zero Trust Access
 - Network Access Manager
 - Secure Firewall Posture
 - Network Visibility
 - Umbrella
 - Start Before Logon
 - Diagnostics and Reporting Tool
- Profile Selection:** ISE Posture CSC Agent Posture Profile

Configuración Básica ISE: Provisionamiento

Paso 5: Configuración de política de provisionamiento de cliente

Policy > Client Provisioning
Edit > Insert Rule Above

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

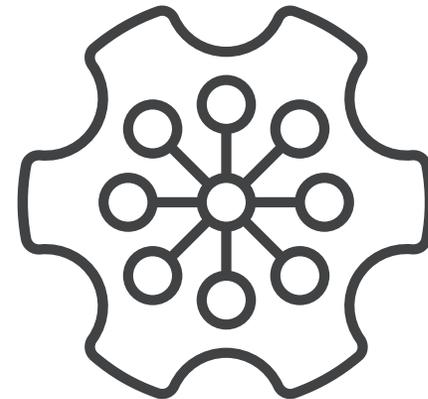
Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> Cisco Secure Client 5	If Any	and Windows All	and Cisco-VPN3000:CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_Posture	then CSC Agent Configuration Edit
<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP Edit
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit

Condiciones, Remediación, Requerimientos y Políticas.



Configuración Básica ISE: Condiciones

Paso 1: Configuración de reglas de Posture para evaluar los clientes, caso de uso, Instalación AM Cisco Secure Endpoint.

Work Centers > Policy Elements > Conditions > Posture > Anti-Malware > Add

The screenshot shows the Cisco ISE configuration interface for creating a new Anti-Malware Condition. The navigation path is: Work Centers > Policy Elements > Conditions > Posture > Anti-Malware > Add. The interface is divided into a left sidebar and a main configuration area.

Left Sidebar (Conditions):

- Conditions (dropdown arrow)
- Anti-Malware (highlighted with a red box)
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall

Main Configuration Area (Anti-Malware Condition):

Anti-Malware Conditions List > New Anti-Malware Condition

Anti-Malware Condition

* Name: AM-Cisco-SecureEp-Con (highlighted with a red box)

Description: _____

Compliance Module: 4.x or later ⓘ

* Operating System: Windows All (dropdown menu, highlighted with a red box)

Vendor: Cisco Systems, Inc. (dropdown menu, highlighted with a red box)

Check Type: Installation Definition (highlighted with a red box)

Bottom Summary Row:

<input checked="" type="checkbox"/>	Cisco Secure Endpoint	7.x (dropdown arrow)	8.x	4.3.3726.6145
-------------------------------------	-----------------------	----------------------	-----	---------------

Configuración Básica ISE: Remediación

Paso 2: Configuración de acciones de remediación.

Work Centers > Policy Elements > Remediations > Posture > Anti-Malware > Add

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports

Conditions >

Remediations >

- Application
- Anti-Malware**
- Anti-Spyware
- Anti-Virus
- File
- Firewall
- Launch Program
- Link
- Patch Management
- Script
- USB
- Windows Server Update Servi...
- Windows Update

Anti-Malware Remediations List > New Anti-Malware Remediation

Anti-Malware Remediation

* Name	AM-Cisco-SecureEp-R
Description	
Operating System	<input checked="" type="radio"/> Windows <input type="radio"/> Mac
Compliance Module	4.x or later
Remediation Type	Manual
* Interval	0 (in secs) (Valid Range 0 to 9999)
* Retry Count	0 (Valid Range 0 to 99)
* Anti-Malware Vendor Name	ANY

Configuración Básica ISE: Requerimientos

Paso 3: Configuración de requisitos de Posture para el estado de cumplimiento (Compliant) de usuarios.

Policy > Policy Elements > Results > Posture > Requirements

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
_temporal					
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations Edit ▾
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations Edit ▾
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations Edit ▾
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations Edit ▾
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win Edit ▾
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac Edit ▾
AM-Cisco-SecureEp-Req	for Windows All	using 4.x or later	using Agent	met if AM-Cisco-SecureEp-Con	then AM-Cisco-SecureEp-Rem Edit ▾
AM-Posture-Req	for Windows All	using 4.x or later	using Agent	met if AM-Posture-Win	then AM-Posture-WinRem Edit ▾

Los requisitos se evaluarán para todos los usuarios que cumplan con las condiciones configuradas, en caso de no cumplir con los requisitos solicitados se les aplicará la acción de remediación correspondiente.

Configuración Básica ISE: Política de Posture

Paso 4: Configuración y activación de la política de Posture.

Work Centers > Posture > Posture Policy

Overview Network Devices Client Provisioning Policy Elements **Posture Policy** Policy Sets Troubleshoot Reports Settings

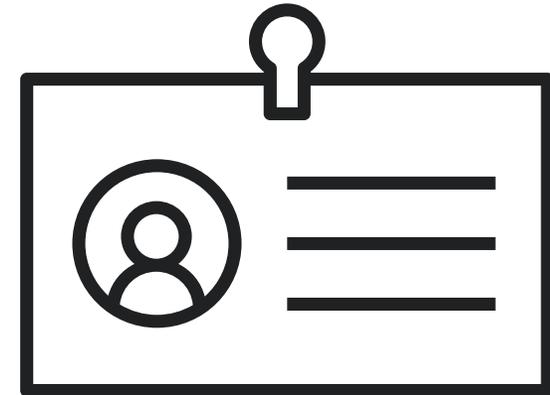
Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

∨

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	AM-Cisco-SecureEP-Pol	If Any	and Windows All	and 4.x or later	and Agent	and	then AM-Cisco-SecureEp-Req
<input checked="" type="checkbox"/>	Policy Options	AM-Posture-Policy	If Any	and Windows All	and 4.x or later	and Agent	and	then AM-Posture-Req
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Any_AM_Installation_Mac
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Mac_temporal
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Any_AM_Installation_Win

Políticas de Autenticación y Autorización





¿Cuál es el propósito principal de las DACL (Listas de Control de Acceso Dinámicas) en la configuración de Cisco ISE para usuarios de VPN de acceso remoto?

- a) Restringir el acceso a la red según el estado de cumplimiento de la postura
 0%
- b) Proporcionar acceso completo a todos los usuarios
 0%
- c) Asignar direcciones IP estáticas a los usuarios
 0%
- d) Monitorear el tráfico de red en tiempo real
 0%

Join at
slido.com
#2535 244

Configuración Básica ISE: Políticas de Autorización

Paso 1: Configuración de políticas de autorización de acuerdo con el estado de Posture: Compliant

Policy > Policy Elements > Results > Authorization > Downloadable ACLS
Policy > Policy Elements > Results > Authorization > Authorization Profiles

Downloadable ACL

* Name **PostureCompliant**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
...	

Results

Authorization Profiles > Posture-Compliant

Authorization Profile

* Name **Posture-Compliant**

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

Cisco

Service Template

Track Movement

 ⓘ

Agentless Posture

 ⓘ

Passive Identity Tracking

 ⓘ

Common Tasks

DACL Name ⓘ

PostureCompliant

Configuración Básica ISE: Políticas de Autorización

Configuración de políticas de autorización de acuerdo con el estado de Posture: Non-Compliant

Policy > Policy Elements > Results > Authorization > Downloadable ACLS
Policy > Policy Elements > Results > Authorization > Authorization Profiles

Downloadable ACL

* Name **PostureNonCompliant**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	deny ip any 10.0.0.0 255.0.0.0
8910111	deny ip any 17.16.0.0 255.240.0.0
2131415	deny ip any 192.168.0.0 255.255.0.0
1617181	permit ip any any
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

Results

Authorization Profiles > Posture-Non-Compliant

Authorization Profile

* Name **Posture-Non-Compliant**

Description

* Access Type **ACCESS_ACCEPT** ▾

Network Device Profile  Cisco ▾ ⊕

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name ⓘ **PostureNonCompliant** ▾

Configuración Básica ISE: Políticas de Autorización

Configuración de políticas de autorización de acuerdo con el estado de Posture: Desconocido / Unknown

Policy > Policy Elements > Results > Authorization > Downloadable ACLS
Policy > Policy Elements > Results > Authorization > Authorization Profiles

Downloadable ACL

* Name **PostureUnknown**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit udp any any eq domain
8910111	permit ip any host
2131415	permit tcp any any eq 80
1617181	permit tcp any any eq 443
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
.....	

Results

Authorization Profiles > Posture-Redirect-Unknown

Authorization Profile

* Name **Posture-Redirect-Unknown**

Description

Type **ACCESS_ACCEPT**

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name ⓘ **PostureUnknown**

Configuración Básica ISE: Políticas de Autorización

Configuración de políticas de autorización de acuerdo con el estado de Posture: Desconocido / Unknown

Atributos de redirección

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ▾

ACL

PostureRedirectACL ▾

Value Client Provisioning Portal (def: ▾

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Attributes Details

Access Type = ACCESS_ACCEPT

DACL = PostureUnknown

cisco-av-pair = url-redirect-acl=PostureRedirectACL

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=ee39fd08-7180-4995-8aa2-9fb282645a8f&action=cpp

Configuración Básica ISE: Políticas de Autorización

Paso 2: Configuración de un nuevo set de políticas de autenticación y autorización acorde al estado de Posture: Compliant, Non-Compliant, Unknown

Policy > Policy Sets

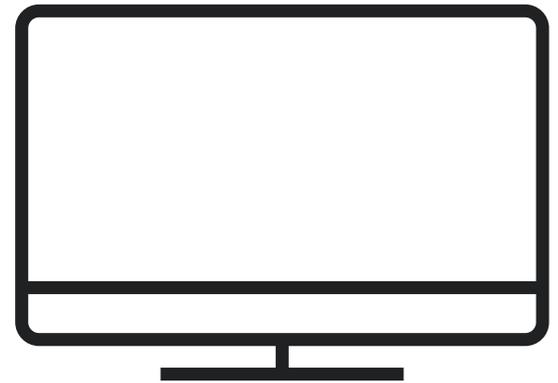
Identity Services Engine Policy / Policy Sets

Reset Reset Policyset Hitcounts Save

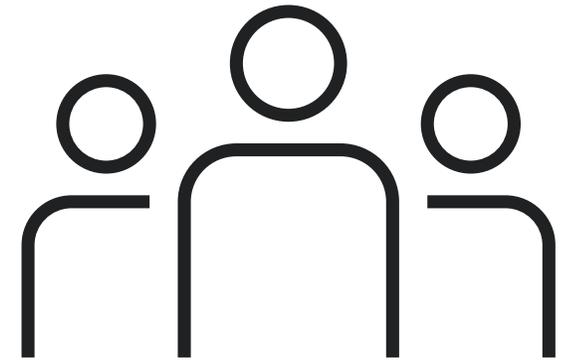
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	ISE_Posture_VPN_RA		AND Network Access-NetworkDeviceName EQUALS FTD1_Lab Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_Posture	Default Network Access	0		

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Posture_Redirect_Unknown	AND Session-PostureStatus EQUALS Unknown Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_POSTURE	Posture-Redirect-Unknown	Select from list	89	
✓	Posture_Non_Compliant	AND Session-PostureStatus EQUALS NonCompliant Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_POSTURE	Posture-Non-Compliant	Select from list	0	
✓	Posture_Compliant	AND Session-PostureStatus EQUALS Compliant Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_POSTURE	Posture-Compliant	Select from list	22	

Configuración Básica FMC: Túnel, Servidores de ISE, Listas y perfil de acceso



Servidores de ISE y Listas de acceso



Configuración Básica FMC: Servidores de ISE

Paso 1: Configuración de objeto de red con la IP del ISE

Objects > Object management > Network > Add object

Edit Network Object ?

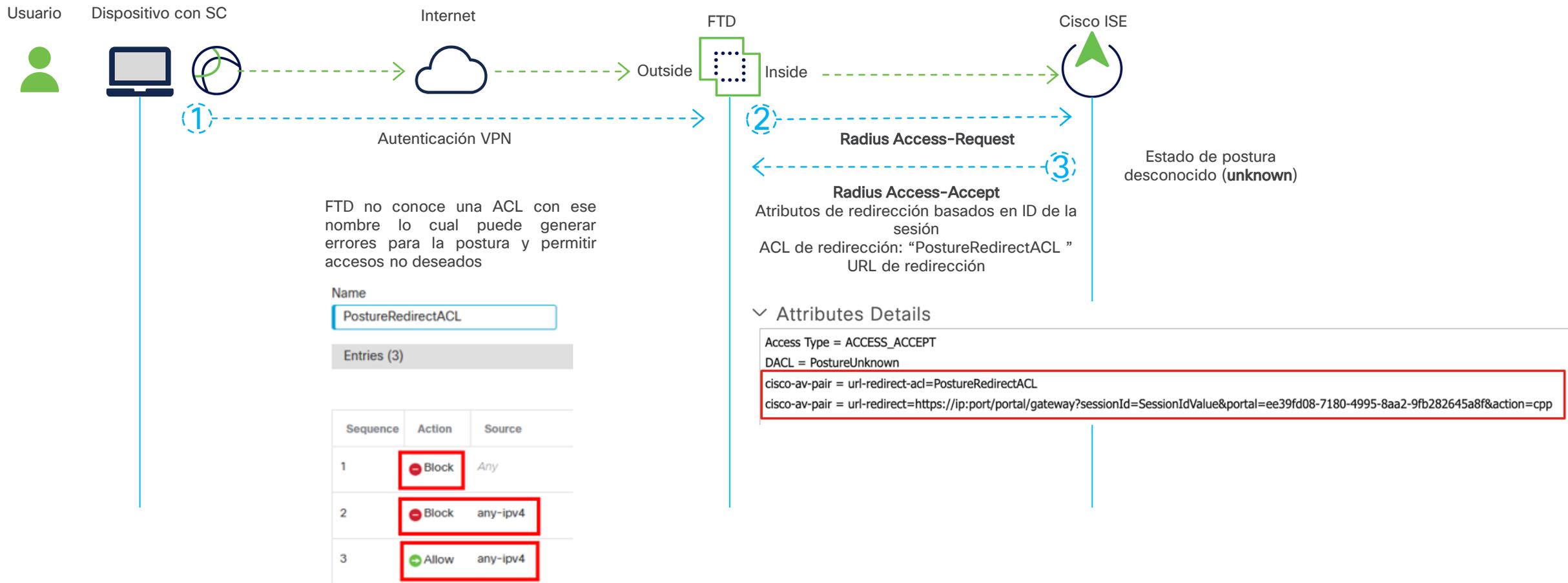
Name

Description

Network
 Host Range Network FQDN

Allow Overrides

Atención al nombre de la ACL de redirección



Configuración Básica FMC: Lista de acceso de redirección

Paso 2: Configurar una ACL de redirección

Allow significará que ese tráfico será redirigido, Deny significará que el tráfico no será redirigido.

Objects > Object management > Access List > Extended > Add Extended Access List

Name

Entries (3) [Add](#)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	Any	Any	Any	DNS_over_UDP	Any	Any	Any	 
2	Block	any-ipv4	Any	ISE_PSN	Any	Any	Any	Any	 
3	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	 

Allow Overrides

[Cancel](#) [Save](#)

Configuración Básica FMC: Grupo de servidores RADIUS

Paso 3: Configurar un grupo de servidores RADIUS para poder agregar nuestro servidor ISE

Edit RADIUS Server Group ?

Name:*

Description:

Group Accounting Mode:

Retry Interval:* (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

Objects > Object management > AAA Server >
RADIUS Server Group > Add RADIUS Server Group

Configuración Básica FMC: Servidores de ISE

Paso 3: Configuración de los servidores individuales de ISE dentro del grupo (autenticación y autorización)

Edit RADIUS Server / Add RADIUS Server

Edit RADIUS Server ?

IP Address/Hostname:*
192.168.12.30
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)
1812

Key:*
••••••••

Confirm Key:*
••••••••

Accounting Port: (1-65535)
1813

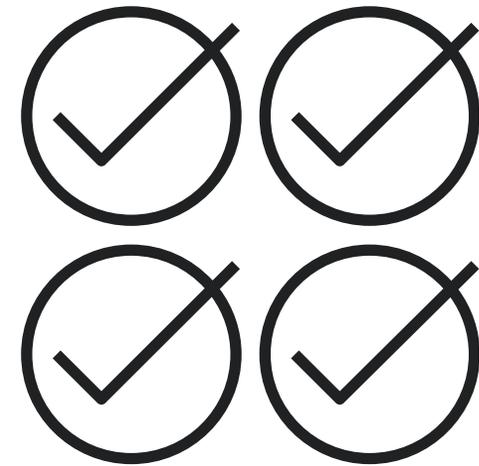
Timeout: (1-300) Seconds
10

Connect using:
 Routing Specific Interface ⓘ
outside-ftd1 +

Redirect ACL:
PostureRedirectACL +

Cancel Save

Configuración VPN de acceso remoto (RAVPN)



Configuración Básica FMC: RAVPN

Paso 4: Configuración del Tunnel Group, asegurarnos que el FTD otorgue IPs a los usuarios remotos
Devices > VPN > Remote Access > Edit Policy > Edit Connection profile

Edit Connection Profile ?

Connection Profile:*

Group Policy:* +
[Edit Group Policy](#)

Client Address Assignment AAA Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
Pool_Split_FTD1	192.168.21.10-192.168.21.100	 

DHCP Servers: +

Name	DHCP Server IP Address	

Configuración Básica FMC: RAVPN

Paso 5: Configuración de métodos de autenticación y autorización

Devices > VPN > Remote Access > Edit Policy > Edit Connection profile > AAA

Edit Connection Profile ?

Connection Profile:* ISE_POSTURE

Group Policy:* FTD1_Split +
[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: ISE (RADIUS)

Fallback to LOCAL Authentication

Use secondary authentication

Authorization

Authorization Server: ISE (RADIUS)

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

► Advanced Settings

Cancel Save

Configuración Básica FMC: Group policy

Paso 6: Configuración del Group Policy: Perfil

Devices > VPN > Remote Access > Edit Policy > Edit Connection Profile > Edit Group policy > Secure client

Edit Group Policy ?

Name:*

Description:

General **Secure Client** Advanced

Profile

- Management Profile
- Client Modules
- SSL Settings
- Connection Settings
- Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:
 +

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

Configuración Básica FMC: Group policy

Paso 7: Configuración del “split tunnel”

Devices > VPN > Remote Access > Edit Policy > Edit Connection profile > Edit Group policy > General > Split Tunneling

Edit Standard Access List Object

Name:

▼ Entries (3)

Sequence No	Action	Network	
1	→ Allow	FTD1_LAN_192.168.1.0_24	
2	→ Allow	72.163.1.80	
3	→ Allow	ISE_PSN	

Allow Overrides

Edit Group Policy

Name:

Description:

General | Secure Client | Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:

IPv6 Split Tunneling:

Split Tunnel Network List Type:
 Standard Access List Extended Access List

Standard Access List:

DNS Request Split Tunneling
DNS Requests:

Domain List:

Configuración Básica FMC: Interfaz

Paso 8: Configuración de la interfaz

Devices > VPN > Remote Access > Edit Policy > Access Interfaces

Connection Profile **Access Interfaces** Advanced

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL
outside-ftd1		+	+

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:*

DTLS Port Number:*

SSL Global Identity Certificate: +

Note: Ensure the port used in VPN configuration is not used in other services

IPsec-IKEv2 Settings

IKEv2 Identity Certificate: +

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Demo

- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
- Configuración básica: ISE y VPN
- Demo**
- Comprobación: Monitoreo y Reportes
- Mejores Prácticas y Troubleshooting

Comprobación: Monitoreo y Reportes

- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
- Configuración básica: ISE y VPN
- Demo
- Comprobación: Monitoreo y Reportes**
- Mejores Prácticas y Troubleshooting

ISE Live Logs y Reportes de posture



Monitoreo y Reportes: ISE Live Logs

Flujo de posture en caso de uso Cisco Secure Endpoint

Operations > Radius > Live Logs

Reset Repeat Counts Export To

Filter

Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	
			Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	
✓			#ACSACL#-IP-PostureCompliant...						
🌐		0	3	Usuario_Posture	00:50:56:B3:75:CE	Windows10-Workstation	ISE_Posture_VPN_RA >> Default	ISE_Posture_VPN_RA >> Posture_Compliant	Posture-Compliant
✓			2		00:50:56:B3:75:CE		ISE_Posture_VPN_RA	ISE_Posture_VPN_RA >> Posture_Compliant	Posture-Compliant
✓			#ACSACL#-IP-PostureUnknown-...						
✓			1	Usuario_Posture	00:50:56:B3:75:CE		ISE_Posture_VPN_RA >> Default	ISE_Posture_VPN_RA >> Posture_Redirect_Unknown	Posture-Redirect-Unknown

Reset Repeat Counts Export To

Authorization Profiles	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server	Mdm Ser...	Session ID
Authorization Profiles	IP Address	Network Devi	Device Port	Identity Group	Posture Status	Server	Mdm Serve	Session ID
		FTD1_Lab				ISE-Vedo		0c046229000d2000672abb12
Posture-Compliant					Compliant	ISE-Vedo		0c046229000d2000672abb12
Posture-Compliant		FTD1_Lab			Compliant	ISE-Vedo		0c046229000d2000672abb12
		FTD1_Lab				ISE-Vedo		0c046229000d2000672abb12
Posture-Redirect-Unknown		FTD1_Lab		User Identity Group	Pending	ISE-Vedo		0c046229000d2000672abb12



Monitoreo y Reportes: Reportes de Posture

Reportes de provisionamiento: Lista clientes que han descargado SC y perfiles vía portal de provisionamiento

Operations > Reports > Reports > Endpoints and Users > Client Provisioning

Client Provisioning ⓘ

From 2024-10-30 00:00:00.0 To 2024-10-30 03:45:09.0

Reports exported in last 7 days 0

Click here to do visibility setup [Do not show this again.](#)

Filter ▾

Refresh ↻



Logged At	Server	Event	Identity ⓘ	Endpoint ID ⓘ	IP Address	Client Provisioning ...	Failure Reason
× Today ▾ ×			Identity	Endpoint ID			
2024-10-30 03:40:00.7...	ISE-Vedo	Client provisioning succeeded	Usuario_Posture	00:50:56:B3:75:CE		Cisco Secure Client 5	

Monitoreo y Reportes: Reportes de Posture

Reportes de cumplimiento por dispositivo: Lista y detalles de clientes que han pasado por el proceso de posture, condiciones, requerimientos, programas, etc.

Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint

Posture Assessment by Endpoint ⓘ

[Add to My Reports](#) [Export To](#) ▼ [Schedule](#)

From 2024-11-06 00:00:00.0 To 2024-11-06 00:53:05.0

Reports exported in last 7 days 0

[Filter](#) ▼ [Refresh](#) 

Status	Details	Identity ⓘ	Endpoint ID ⓘ	IP Address	Endpoint OS	Agent	Message	PRA Action
	▼	Identity	Endpoint ID		Endpoint OS			
		Usuario_Posture	00:50:56:B3:75:CE		Windows 10 Enterprise 64-bit	Posture Agent for Windows 5.1.6.103	Received a posture report from an endpoint	N/A
	Click Here for Detail Report	Usuario_Posture	00:50:56:B3:75:CE		Windows 10 Enterprise 64-bit	Posture Agent for Windows 5.1.6.103	Received a posture report from an endpoint	N/A
		Usuario_Posture	00:50:56:B3:75:CE		Windows 10 Enterprise 64-bit	Posture Agent for Windows 5.1.6.103	Received a posture report from an endpoint	N/A

Posture Report

Posture Status

NonCompliant

Logged At

2024-11-06 00:49:46.352

Monitoreo y Reportes: Reportes de Posture

Detalles del reporte

Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint

AM Installed

Windows Defender;4.18.24090.11;;

Posture Policy Details

Policy	Name	Enforcement Type	Status	Passed Conditions	Failed Conditions	Skipped Conditions
AM-Cisco-SecureEP-Pol	AM-Cisco-SecureEp-Req	Mandatory	Failed		am_inst_v4_CiscoSecureEndpoint_7_x,am_inst_v4_CiscoSe...	
AM-Posture-Policy	AM-Posture-Req	Mandatory	Passed	am_inst_v4_WindowsDefender_4_x		,am_inst_v4_WindowsDefender_6_x

Secure Client: Módulos VPN y ISE Posture



Monitoreo y Reportes: Módulo de VPN

Detalles de la conexión remota de VPN
Secure Client > AnyConnect VPN > Statistics

Cisco Secure Client



Secure Client

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Connection Information

State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:18:37
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information

Client (IPv4):	192.168.21.10
Client (IPv6):	Not Available
Server:	

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Received: 4966

Client Management

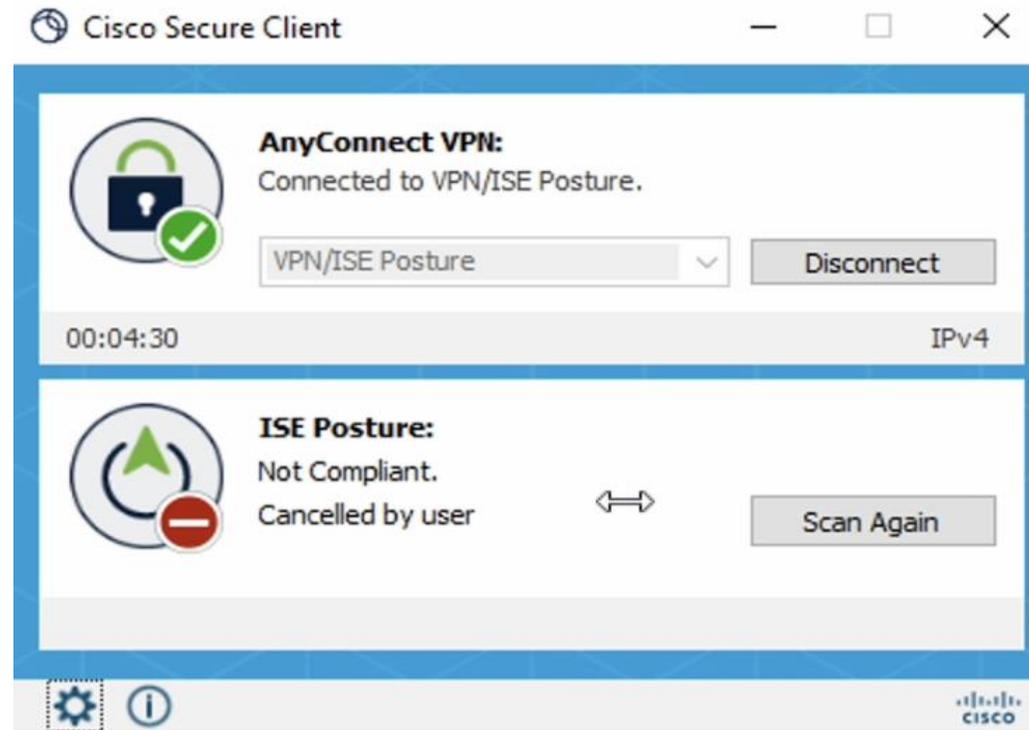
Administrative Domain:	Undefined
Profile Name:	allowRemoteUsersFTD1.xml



Monitoreo y Reportes: Módulo de ISE Posture

Detalles del estado de posture.

Interfaz de usuario



Monitoreo y Reportes: Módulo de ISE Posture

Detalles del estado de posture.

Secure Client > ISE Posture > Statistics / Security Products

Cisco Secure Client



General

Status Overview

AnyConnect VPN

ISE Posture

ISE Posture

Preferences Statistics **Security Products** Scan Summary Message History

Compliance Information

Current Status: Not Compliant

Acceptable Use Policy: Unknown

Latest Scan Start Time: Tue Oct 29 22:40:38 2024

Missing Requirements: 1

Remaining Optional Updates: None

Compliance Module Version: 4.3.4248.8192

Connection Information

Policy Server: ISE-Vedo.cisco.com

ISE Posture

Preferences Statistics **Security Products** Scan Summary Message History

Product Name	Product Type	Product Version	Defir
Windows Defender	AM	4.18.24090.11	
BitLocker Drive Encryption	DE	10.0.19041.1	
Windows Firewall	FW	10.0.19041.4291	
Windows Update Agent	PM	10.0.19041.4717	



Monitoreo y Reportes: Módulo de ISE Posture

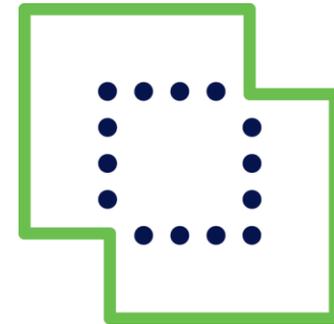
Detalles del estado de posture.

Secure Client > ISE Posture > Scan Summary

The screenshot shows the Cisco Secure Client interface. On the left is a navigation menu with the following items: General, Status Overview, AnyConnect VPN, and ISE Posture (which is selected and has a right-pointing arrow). The main content area is titled 'ISE Posture' and contains several tabs: Preferences, Statistics, Security Products, Scan Summary (which is active), and Message History. Below the tabs is a table with columns for 'Updates' and 'Status'. A sub-section titled 'Required' is visible. The table contains two rows, both of which are highlighted with a red border:

	Updates	Status
1	AM-Cisco-SecureEp-Req	Required (Manual)
2	AM-Posture-Req	Done

FTD: Detalles de la sesión y atributos aplicados



Monitoreo y Reportes: FTD detalles de la sesión

Detalles de la sesión y atributos aplicados

Conexión ssh al FTD > show vpn-sessiondb detail anyconnect (opcional + filter name <nombre del usuario>)

```
> show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : Usuario_Posture      Index      : 182
Assigned IP   : 192.168.21.10        Public IP  : ██████████
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      : 15558                Bytes Rx   : 6093
Pkts Tx       : 2                    Pkts Rx    : 15
Pkts Tx Drop  : 0                    Pkts Rx Drop : 0
Group Policy  : FTD1 Split            Tunnel Group : ISE POSTURE
Login Time    : 03:37:48 UTC Wed Oct 30 2024
Duration      : 0h:00m:59s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN       : none
Audt Sess ID  : 0c046229000b60006721aa0c
Security Grp  : none                  Tunnel Zone : 0
```

Monitoreo y Reportes: FTD detalles de la sesión

Detalles de los atributos de redirección

Conexión ssh al FTD > show vpn-sessiondb detail anyconnect (opcional + filter name <nombre del usuario>)

ISE Posture:

Redirect URL : <https://ISE-Vedo.cisco.com:8443/portal/gateway?sessionId=0c046229000b60006721aa0c&portal=ee39fd08-7180...>

Redirect ACL : PostureRedirectACL

Monitoreo y Reportes: FTD detalles de la sesión

Detalles de los atributos del estado de postura ejemplo, non-compliant

Conexión ssh al FTD > show vpn-sessiondb detail anyconnect (opcional + filter name <nombre del usuario>)

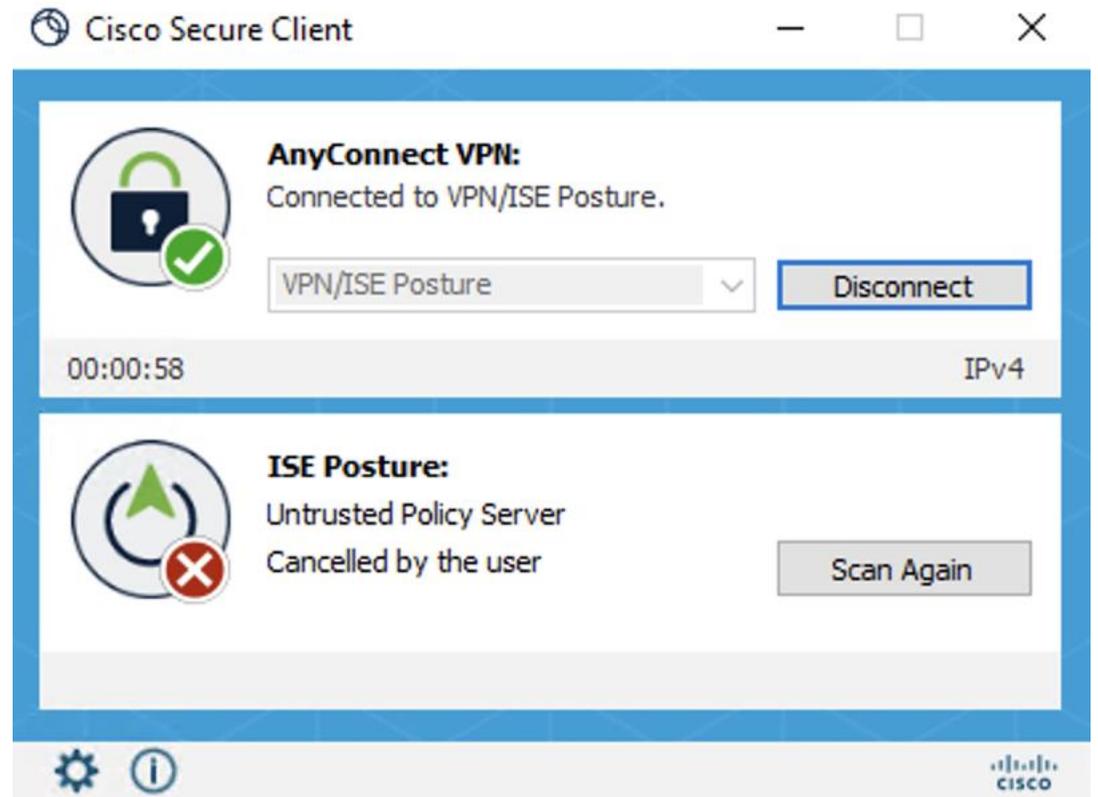
```
SSL-Tunnel:
Tunnel ID      : 182.2
Assigned IP    : 192.168.21.10      Public IP      : ██████████
Encryption     : AES-GCM-128       Hashing        : SHA256
Ciphersuite    : TLS_AES_128_GCM_SHA256
Encapsulation  : TLSv1.3           TCP Src Port   : 50070
TCP Dst Port   : 443              Auth Mode      : userPassword
Idle Time Out  : 30 Minutes        Idle T0 Left   : 23 Minutes
Client OS      : Windows
Client Type    : SSL VPN Client
Client Ver     : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx       : 7779              Bytes Rx       : 6093
Pkts Tx        : 1                Pkts Rx       : 15
Pkts Tx Drop   : 0                Pkts Rx Drop  : 0
Filter Name    : #ACSACL#-IP-PostureNonCompliant-66f8b3f9

DTLS-Tunnel:
Tunnel ID      : 182.3
Assigned IP    : 192.168.21.10      Public IP      : ██████████
Encryption     : AES-GCM-256       Hashing        : SHA384
Ciphersuite    : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation  : DTLSv1.2         UDP Src Port   : 58694
UDP Dst Port   : 443              Auth Mode      : userPassword
Idle Time Out  : 30 Minutes        Idle T0 Left   : 25 Minutes
Client OS      : Windows
Client Type    : DTLS VPN Client
Client Ver     : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx       : 455              Bytes Rx       : 574
Pkts Tx        : 4                Pkts Rx       : 6
Pkts Tx Drop   : 0                Pkts Rx Drop  : 0
Filter Name    : #ACSACL#-IP-PostureNonCompliant-66f8b3f9
```

Mejores Prácticas y Troubleshooting

- Introducción a Cisco ISE y Cisco Secure Client
- Descripción y funcionamiento de Posture
- Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
- Configuración básica: ISE y VPN
- Demo
- Comprobación: Monitoreo y Reportes
- Mejores Prácticas y Troubleshooting**

Secure Client: conexión a un servidor no reconocido

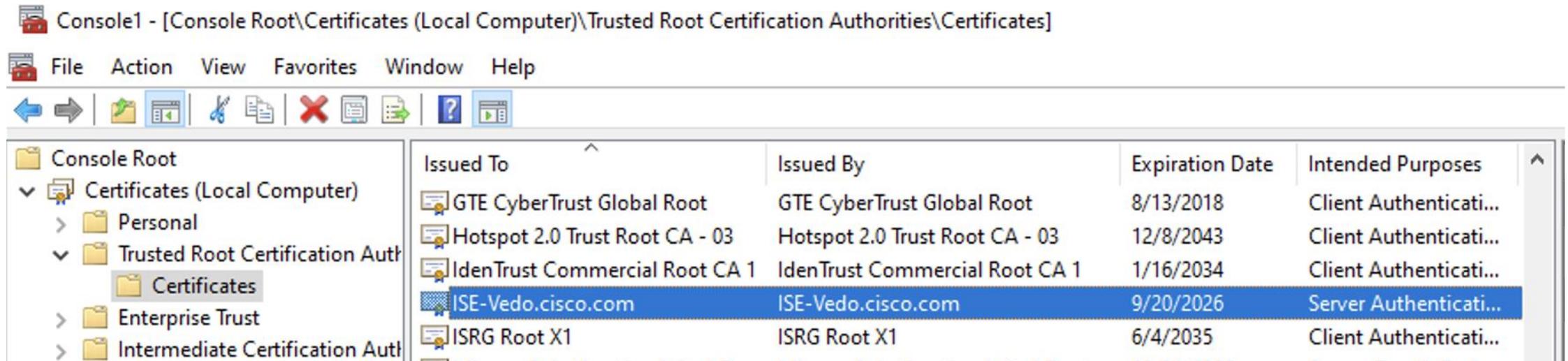


Secure Client: Untrusted Server Connection

Ocurre cuando el equipo no puede verificar el certificado Admin y Portal del servidor en que se está haciendo posture.

¿Qué verificar?

1) Instalación de certificados

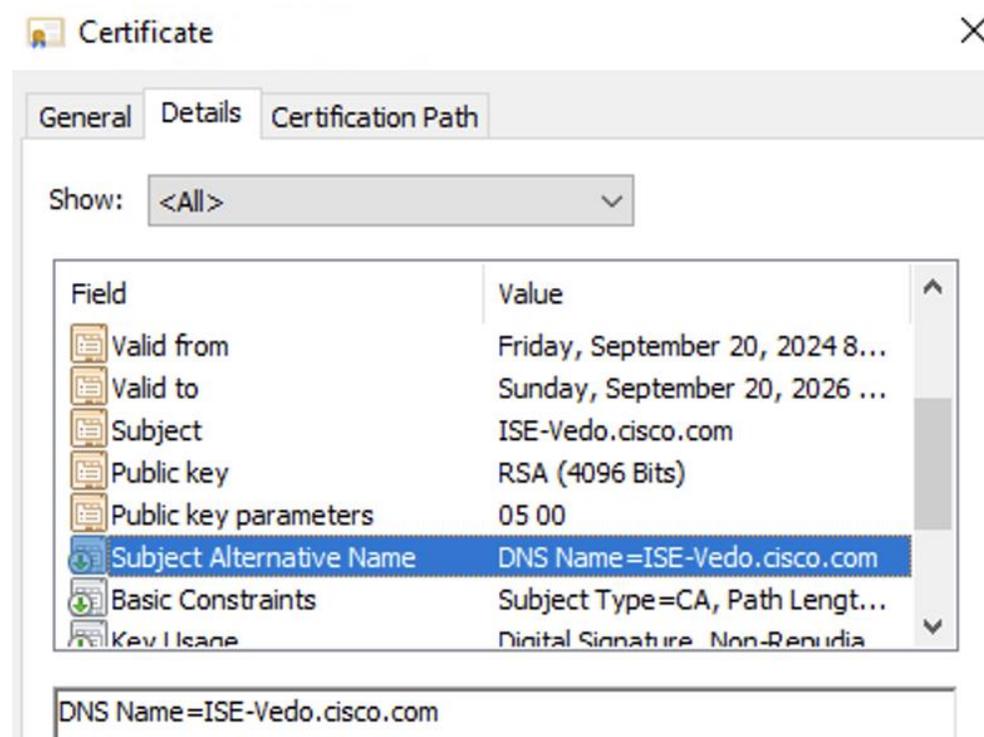


Secure Client: Untrusted Server Connection

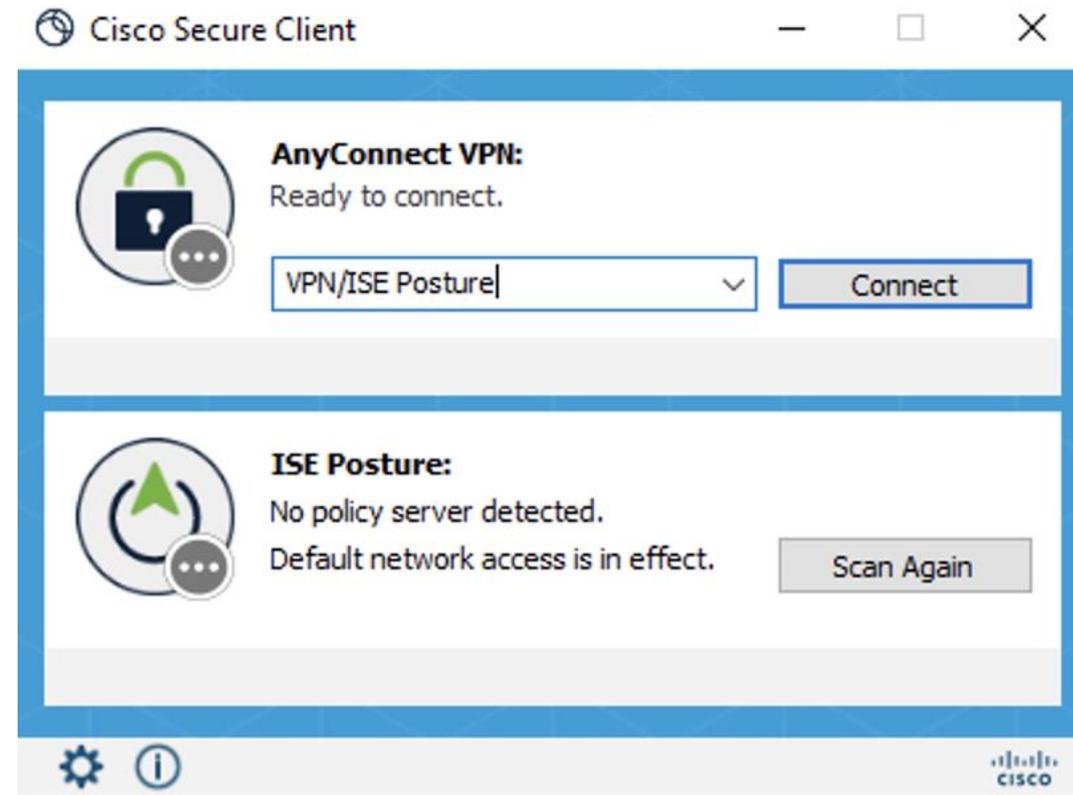
Ocurre cuando el equipo no puede verificar el certificado Admin y Portal del servidor en que se está haciendo posture.

¿Qué verificar?

2) Campos del certificado



Secure Client: Servidor no encontrado



Secure Client: No Policy Server Detected

SC (dispositivo) no puede comunicarse y / o encontrar los servidores ISE, generalmente porque los métodos de descubrimiento fallan.

¿Qué Verificar?

1) Lista de Acceso de Redirección

Name
PostureRedirectACL

Entries (3) Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	Any	Any	Any	DNS_over_UDP	Any	Any	Any	 
2	Block	any-ipv4	Any	ISE_PSN	Any	Any	Any	Any	 
3	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	 

Allow Overrides

Cancel Save

Secure Client: No Policy Server Detected

SC (dispositivo) no puede comunicarse y / o encontrar los servidores ISE, generalmente porque los métodos de descubrimiento fallan.

¿Qué Verificar?

2) La Lista de Acceso del Túnel

Edit Standard Access List Object ?

Name
FTD1_Split_Tunnel_ACL

▼ Entries (3) Add

Sequence No	Action	Network	
1	→ Allow	FTD1_LAN_10.191.51.192-28	 
2	→ Allow	72.163.1.80	 
3	→ Allow	ISE_PSN	 

Allow Overrides

Cancel Save

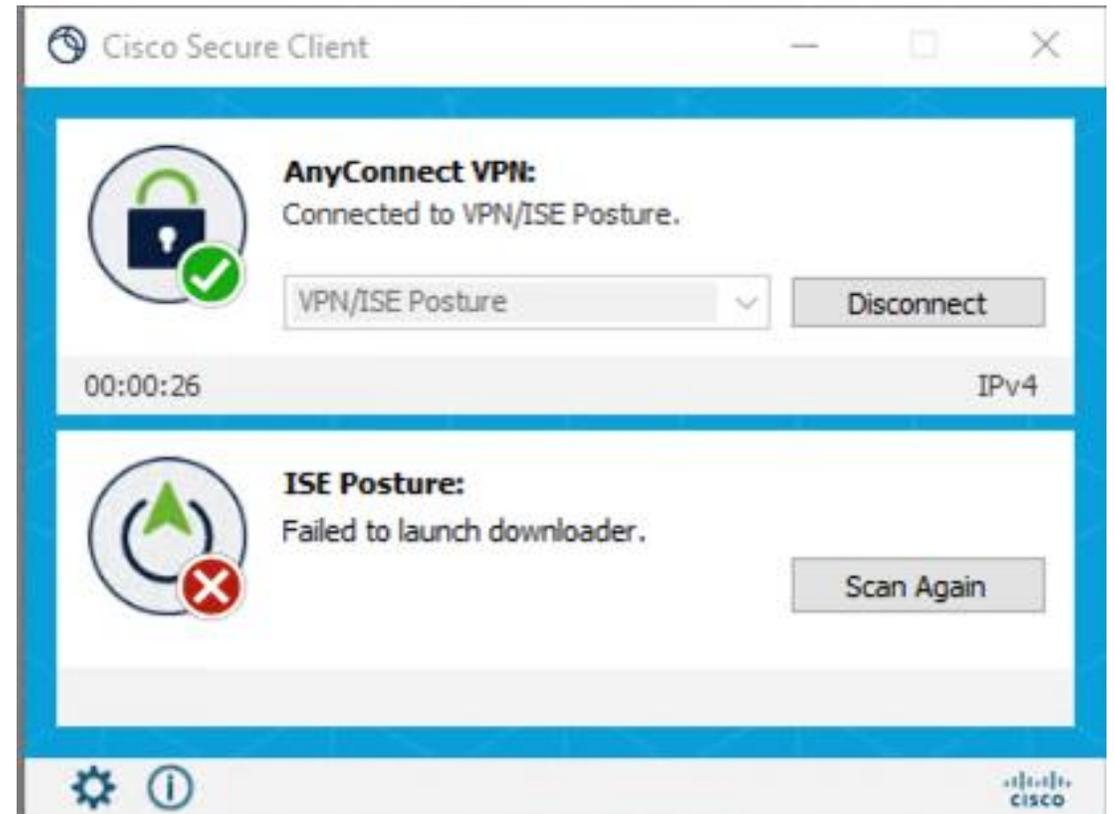
Secure Client: No Policy Server Detected

SC (dispositivo) no puede comunicarse y / o encontrar los servidores ISE, generalmente porque los métodos de descubrimiento fallan.

¿Qué Verificar?

3) En escenarios con FW, que el tráfico http y tcp puerto 8443 está siendo permitido entre el dispositivo y los servidores ISE

Secure Client: Falla al descargar los módulos



Secure Client: Failed to Launch Downloader

Generalmente ocurre por problemas de provisionamiento, Secure Client o Compliance Module

¿Qué Verificar?

1) Reglas de provisionamiento



Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> Cisco Secure Client 5	If Any	and Windows All	and Cisco-VPN3000:CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_Posture	then CSC Agent Configuration Edit
<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 5.0.03061 And WinSPWizard 3.2.0.1 And Cisco-ISE-NSP Edit

Secure Client: Failed to Launch Downloader

Generalmente ocurre por problemas de provisionamiento, Secure Client o Compliance Module

¿Qué Verificar?

2) Provisionamiento ISE y FTD/FMC.

[Agent Configuration](#) > CSC Agent Configuration

* Select Agent Package:

* Configuration Name:

Description:

Description Value Notes

* Compliance Module

Secure Client Images

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup t

Download Secure Client packages from [Cisco Software Download Center](#).

Secure Client File Object Name	Secure Client Package Name
cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg	cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg

Secure Client: Errores en el servidor ISE

Secure Client: Internal Server Error

Generalmente ocurre por problemas en el nodo PSN de ISE.

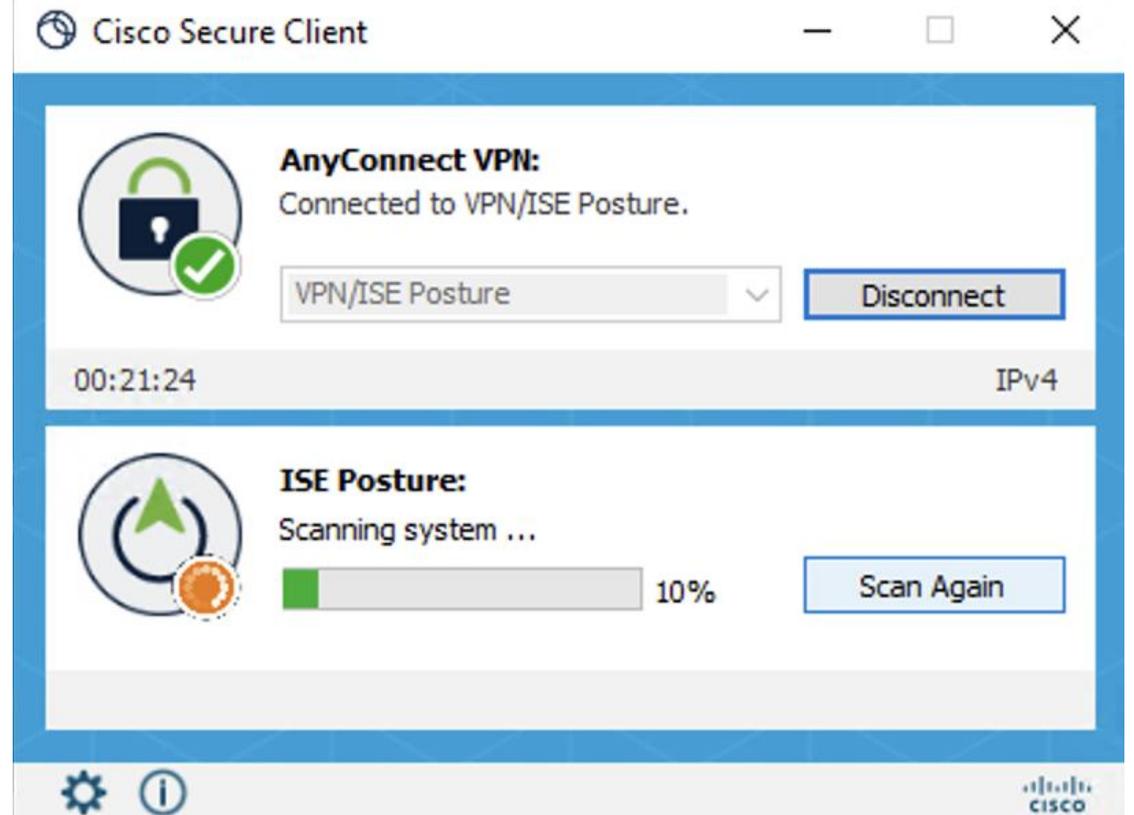
¿Qué Verificar?

1) Licenciamiento en los servidores de ISE para Posture

✓ Enable ✗ Disable ↻ Refresh

	License	Status	Compliance	Consumption	Days Out of Compliance
▼ Tier					
<input type="checkbox"/>	Essential	Enabled	Released Entitlement ⓘ	0	-
<input type="checkbox"/>	Advantage	Enabled	Released Entitlement ⓘ	0	-
<input type="checkbox"/>	Premier	Enabled	Released Entitlement ⓘ	1	-

Secure Client: Scan atascado.



Secure Client: Scan detenido en cierto porcentaje

Generalmente ocurre por problemas en Secure Client o en el dispositivo.

¿Qué Verificar?

1) Módulo de Cumplimiento adecuado

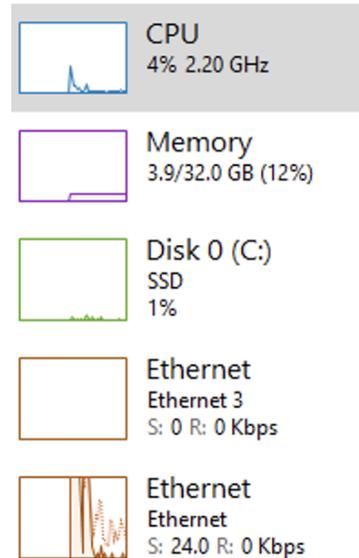
<input checked="" type="checkbox"/>	Cisco Secure Endpoint	<u>7.x</u> ▼	8.x	4.3.3726.6145
-------------------------------------	-----------------------	--------------	-----	---------------

Secure Client: Scan detenido en cierto porcentaje

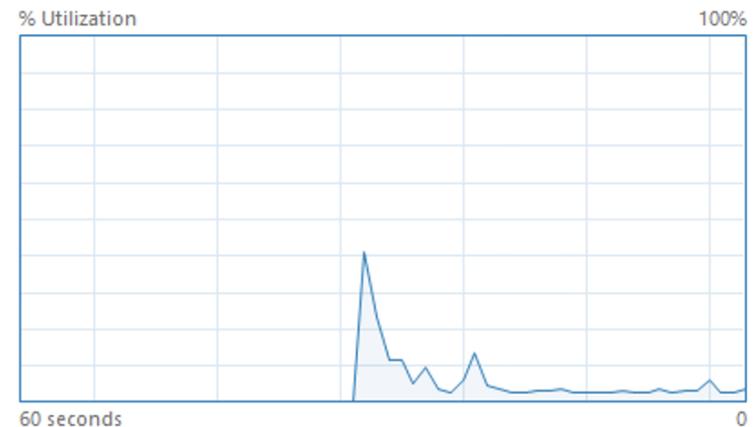
Generalmente ocurre por problemas en Secure Client o en el dispositivo.

¿Qué Verificar?

2) Rendimiento en el dispositivo



CPU Intel(R) Xeon(R) Platinum 8276 CPU @ 2.20GHz



Utilization	Speed	Base speed:	2.20 GHz
4%	2.20 GHz	Sockets:	4
Processes	Threads	Handles	Virtual processors: 4
179	1994	70193	Virtual machine: Yes
			L1 cache: N/A

Up time
1:01:57:47

Secure Client: Scan detenido en cierto porcentaje

Generalmente ocurre por problemas en Secure Client o en el dispositivo.

¿Qué Verificar?

3) Secure Client ISE posture este en la lista de programas permitidos por AV/AM

Q&A





¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar

¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) y ¡mande sus dudas antes del viernes de la próxima semana!



Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.



Nuestras Redes Sociales

LinkedIn
[Cisco Community](#)

Twitter
[@CiscoCommunity](#)

YouTube
[CiscoCommunity](#)

Facebook
[CiscoCommunity](#)



© 2024 Cisco and/or its affiliates. All rights reserved.

