

Implemente la condición sin redirección de ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Connectiondata.xml](#)

[Lista de inicio de llamadas](#)

[Diseño](#)

[Configurar](#)

[Grupos de dispositivos de red \(opcional\)](#)

[Dispositivo de red](#)

[Aprovisionamiento de clientes](#)

[Aprovisionamiento manual \(previo a la implementación\)](#)

[Portal de aprovisionamiento de clientes \(Web Deploy\)](#)

[Política de aprovisionamiento de clientes](#)

[Autorización](#)

[Perfil de autorización](#)

[Política de autorización](#)

[Troubleshoot](#)

[Cumplimiento de Cisco Secure Client y estado No aplicable \(pendiente\) en ISE](#)

[Sesiones antiguas/fantasma](#)

[Identificar](#)

[Solución](#)

[Rendimiento](#)

[Identificar](#)

[Solución](#)

[Contabilidad](#)

[Información Relacionada](#)

Introducción

Este documento describe el uso y la configuración del flujo de estado sin redirección y las sugerencias para la resolución de problemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Flujo de estado en ISE
- Configuración de los componentes de estado en ISE
- Redirección a portales de ISE

Para una mejor comprensión de los conceptos descritos más adelante, se recomienda pasar por:

[Comparación del flujo de redirección de postura de ISE con el flujo sin redirección de postura de ISE](#)

[Solución de problemas de administración y estado de sesiones de ISE](#)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 3.3
- Cisco Secure Client 5.0.01242

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El flujo de estado de ISE consta de estos pasos:

0. Autenticación/Autorización. Generalmente se realiza justo antes de que se inicie el flujo de postura, pero se puede omitir para ciertos casos prácticos como la reevaluación de postura (PRA).

Como la autenticación en sí no activa el descubrimiento de la postura, esto no se considera esencial para cada flujo de postura.

1. Descubrimiento. Proceso realizado por el módulo de postura de ISE de Secure Client para encontrar el propietario de PSN de la sesión activa actual.
2. Aprovisionamiento de clientes. Proceso realizado por ISE para aprovisionar al cliente con el módulo de estado de ISE de Cisco Secure Client (anteriormente AnyConnect) y las versiones del módulo de conformidad correspondientes. En este paso, la copia local del perfil de estado contenido y firmado por el PSN concreto también se envía al cliente.
3. Análisis del sistema. El módulo de cumplimiento evalúa las políticas de estado configuradas en ISE.
4. Remediación (opcional). Se lleva a cabo en el caso de que alguna política de estado no sea conforme.
5. CoA. Es necesario volver a autorizar el acceso a la red final (conforme o no conforme).

Este documento se centra en el proceso de detección del flujo de estado de ISE.

Cisco recomienda utilizar la redirección para el proceso de detección; sin embargo, hay algunos casos en los que no es posible implementar la redirección, como el uso de dispositivos de red de terceros en los que no se admite la redirección. Este documento tiene como objetivo proporcionar una guía general y mejores prácticas para implementar y resolver problemas de postura sin redireccionamiento en tales entornos.

La descripción completa del flujo sin redirección se describe en [Comparar flujo de redirección de postura de ISE con flujo sin redirección de postura de ISE](#)

Existen dos tipos de sondeos de detección de estado que no utilizan la redirección:

1. Connectiondata.xml
2. Lista de inicio de llamadas

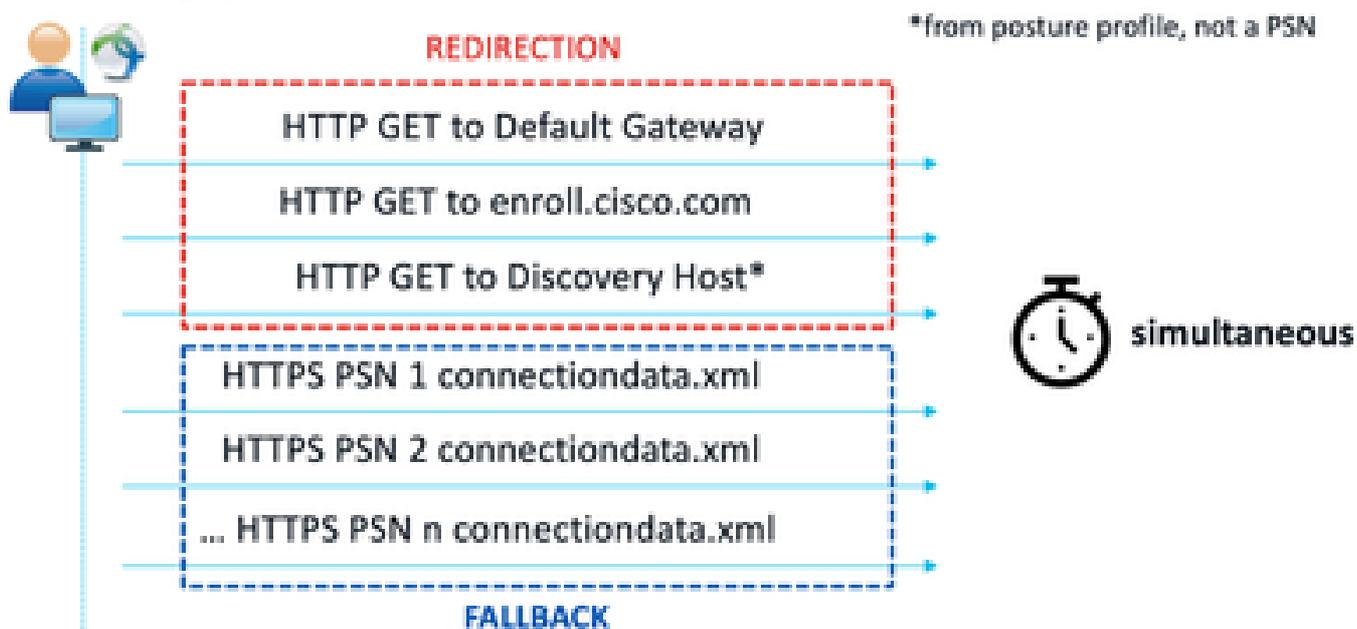
Connectiondata.xml

Connectiondata.xml es un archivo creado y mantenido automáticamente por Cisco Secure Client. Consta de una lista de PSN a los que el cliente se ha conectado previamente correctamente para el estado; por lo tanto, se trata solo de un archivo local y su contenido no es persistente en todos los terminales.

El objetivo principal de connectiondata.xml es funcionar como mecanismo de copia de seguridad para los sondeos de detección de las fases 1 y 2. En caso de que los sondeos de redirección o lista de inicio de llamada no puedan encontrar un PSN con una sesión activa, Cisco Secure Client envía una solicitud directa a cada uno de los servidores enumerados en connectiondata.xml.

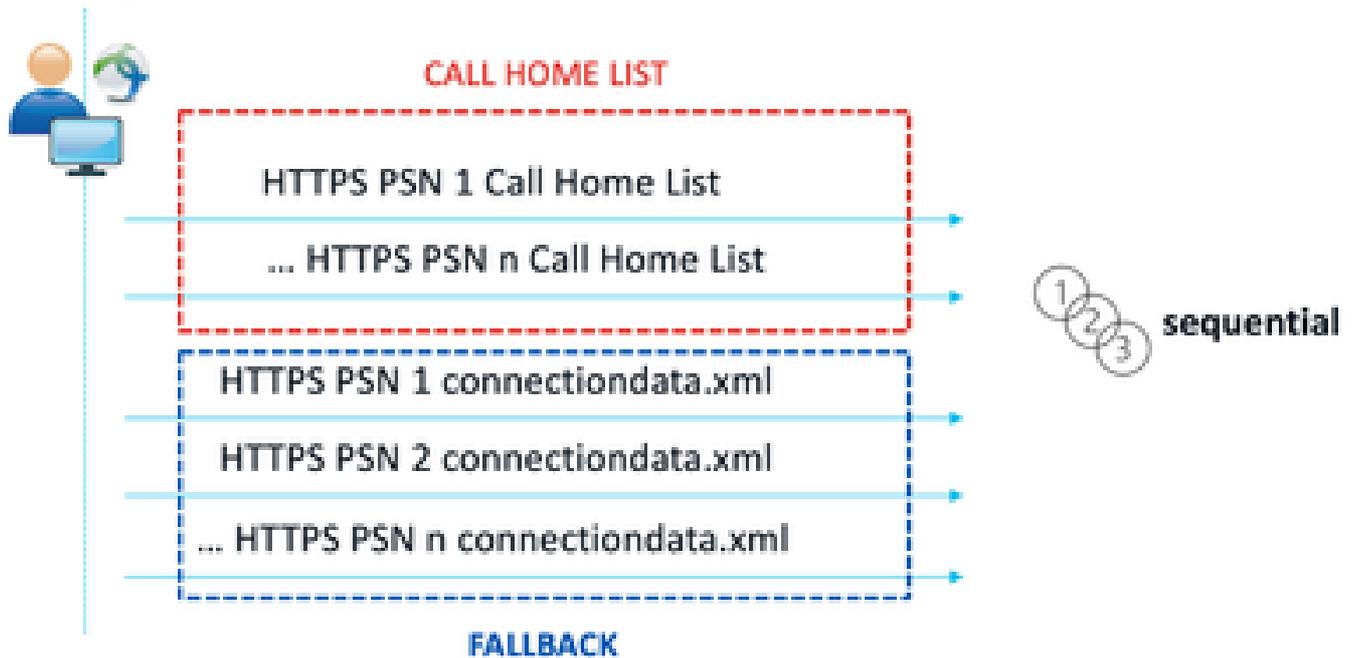
Stage 1 discovery probes

No-MnT stage probes



Stage 2 discovery probes

MnT stage probes



Sondas de detección de etapa 2

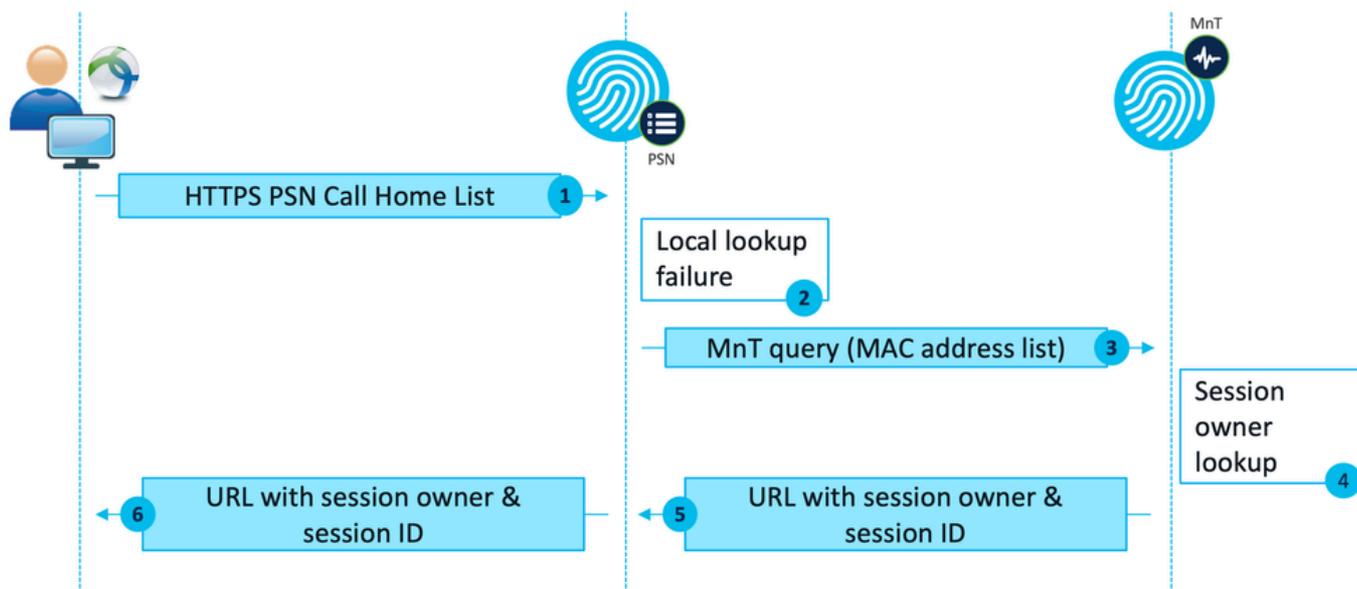
Un problema común causado por el uso de sondeos de connectiondata.xml es una sobrecarga de la implementación de ISE debido al gran número de solicitudes HTTPS enviadas por los terminales. Es importante tener en cuenta que, si bien connectiondata.xml es eficaz como mecanismo de copia de seguridad para evitar interrupciones completas de los mecanismos de estado tanto de redirección como de redirección, no es una solución sostenible para un entorno de estado; por lo tanto, es necesario diagnosticar y resolver los problemas de diseño y configuración que causan la falla de las sondas de detección principales y que dan lugar a problemas de detección.

Lista de inicio de llamadas

La lista de inicio de llamadas es una sección del perfil de estado en la que se especifica una lista de PSN que se utilizarán para el estado. A diferencia de connection.xml, lo crea y mantiene un administrador de ISE y puede requerir una fase de diseño para lograr una configuración óptima. La lista de PSN en la lista de inicio de llamada coincide con la lista de servidores de autenticación y cuentas que se configuró en el dispositivo de red o el equilibrador de carga para RADIUS.

Los sondeos de la lista de inicio de llamadas permiten el uso de una búsqueda de MnT durante la búsqueda de sesión activa en caso de que se produzca un error de búsqueda local en un PSN. La misma funcionalidad se extiende a los sondeos connection.data.xml sólo cuando se utilizan durante la detección de la etapa 2. Por este motivo, todos los sondeos de la etapa 2 también se denominan sondeos de nueva generación.

MnT lookup



Flujo de búsqueda de MnT

Diseño

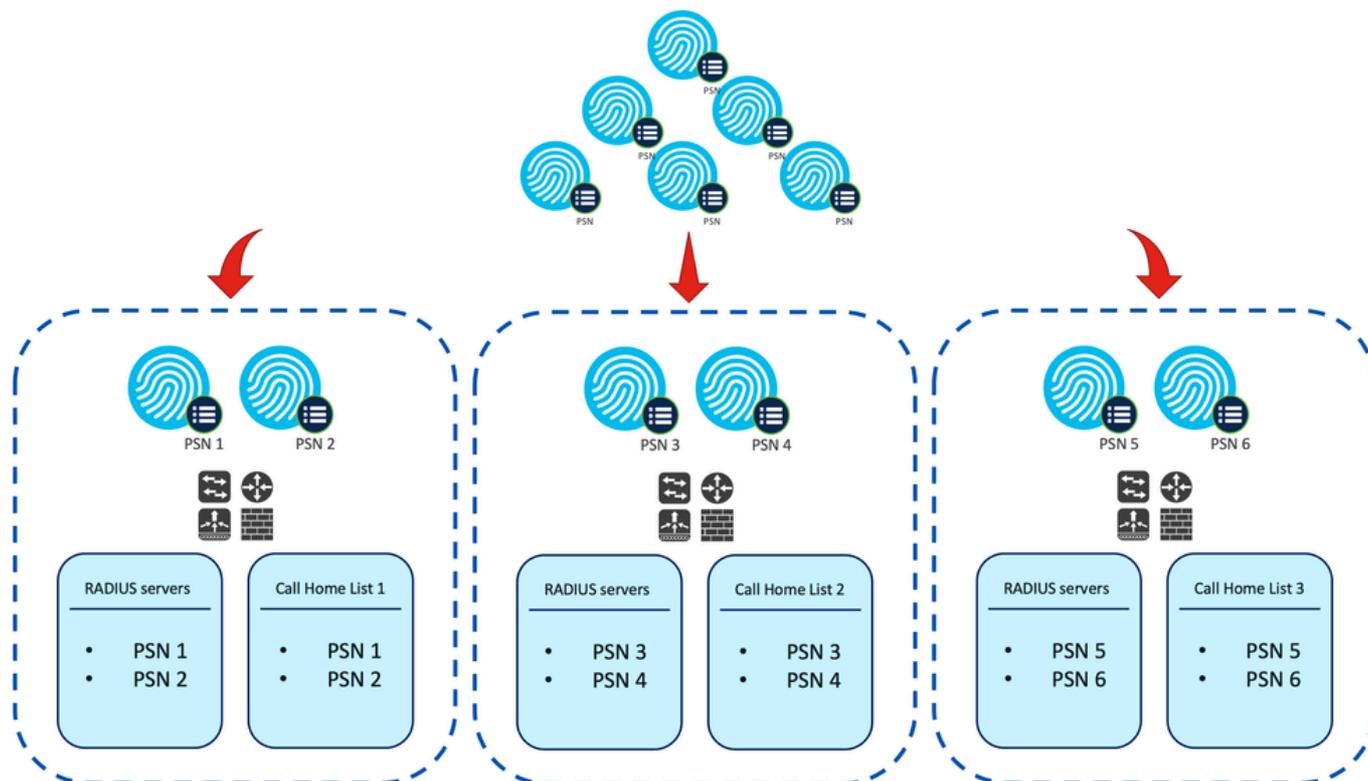
Dado que un proceso de detección sin redirección suele conllevar un flujo más complejo y una mayor cantidad de procesamiento en PSN y MnT en comparación con un flujo de redirección, existen dos retos comunes que pueden surgir durante la implementación:

1. Descubrimiento eficaz
2. Rendimiento de la implementación de ISE

Para hacer frente a estos retos, se recomienda diseñar la lista de inicio de llamadas para limitar el número de PSN que un terminal determinado puede utilizar para el estado. En el caso de implementaciones medianas y grandes, es necesario distribuir la implementación para crear varias listas de inicio de llamadas con un número reducido de PSN. Por consiguiente, la lista de PSN que se utilizan para la autenticación RADIUS de un dispositivo de red determinado se puede limitar del mismo modo para que coincida con la lista de inicio de llamadas correspondiente.

Estos aspectos se pueden tener en cuenta al desarrollar la estrategia de distribución de PSN para determinar el número máximo de PSN en cada lista de inicio de llamada:

- Número de PSN en la implementación
- Especificaciones de hardware de PSN y nodos MnT
- Número máximo de sesiones de estado simultáneas en la implementación
- Número de dispositivos de red
- Entornos híbridos (redirección simultánea e implementación de estado sin redirección)
- Número de adaptadores utilizados por los terminales
- Ubicación de los dispositivos de red y PSN
- Tipos de conexiones de red utilizados para el estado (por cable, inalámbricas, VPN)



Ejemplo: Distribución de PSN para estado sin redirección

 Consejo: Utilice [Network Device Groups](#) para clasificar los dispositivos de red según el diseño.

Configurar

Grupos de dispositivos de red (opcional)

Los grupos de dispositivos de red se pueden utilizar para identificar y hacer coincidir los dispositivos de red con su correspondiente lista de servidores RADIUS y lista de inicio de llamada. En el caso de los entornos híbridos, también se pueden utilizar para identificar dispositivos que admiten la redirección desde dispositivos que no la admiten.

Si la estrategia de distribución desarrollada durante la fase de diseño depende de los grupos de dispositivos de red, siga los siguientes pasos para configurarlos en ISE:

1. Vaya a Administration > Network Resources Network Resource Groups .
2. Haga clic en Agregar para agregar un nuevo grupo, proporcione un nombre y seleccione el grupo primario, si corresponde.
3. Repita el paso 2 para crear todos los grupos necesarios.

En los ejemplos utilizados en esta guía, el grupo de dispositivos de ubicación se utiliza para identificar la lista de servidores RADIUS y la lista de inicio de llamada, y un grupo de dispositivos de postura personalizado se utiliza para identificar la redirección desde dispositivos de postura sin

redirección.

Refresh + Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

<input type="checkbox"/> Name	Description	No. of Network Devices
<input type="checkbox"/> > All Device Types	All Device Types	--
<input type="checkbox"/> ▾ All Locations	All Locations	--
<input type="checkbox"/> ▾ US		0
<input type="checkbox"/> CENTRAL		0
<input type="checkbox"/> EST		1
<input type="checkbox"/> WEST		1
<input type="checkbox"/> > Is IPSEC Device	Is this a RADIUS over IPSEC Device	--
<input type="checkbox"/> ▾ Posture	Posture redirection or redirectionless group	--
<input type="checkbox"/> Redirection		0
<input type="checkbox"/> Redirectionless		1

Grupos de dispositivos de red

Dispositivo de red

1. El dispositivo de red se puede configurar para la autenticación, autorización y administración de cuentas RADIUS. Consulte la documentación de cada proveedor para conocer los pasos de configuración. Configure la lista de servidores RADIUS según la lista de inicio de llamada correspondiente.
2. En ISE, vaya a Administration > Network Resources > Network Devices y haga clic en Add. Configure los grupos de dispositivos de red según el diseño y habilite RADIUS Authentication Settings para configurar el secreto compartido.

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location WEST

[Set To Default](#)

IPSEC No

[Set To Default](#)

Device Type All Device Types

[Set To Default](#)

Posture Redirectionless

[Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret

[Show](#)

Configuración de dispositivos de red

Aprovisionamiento de clientes

Hay dos formas de proporcionar al cliente el software y el perfil adecuados para realizar el estado en un entorno sin redirección:

1. Aprovisionamiento manual (antes de la implementación)
2. Portal de aprovisionamiento de clientes (implementación web)

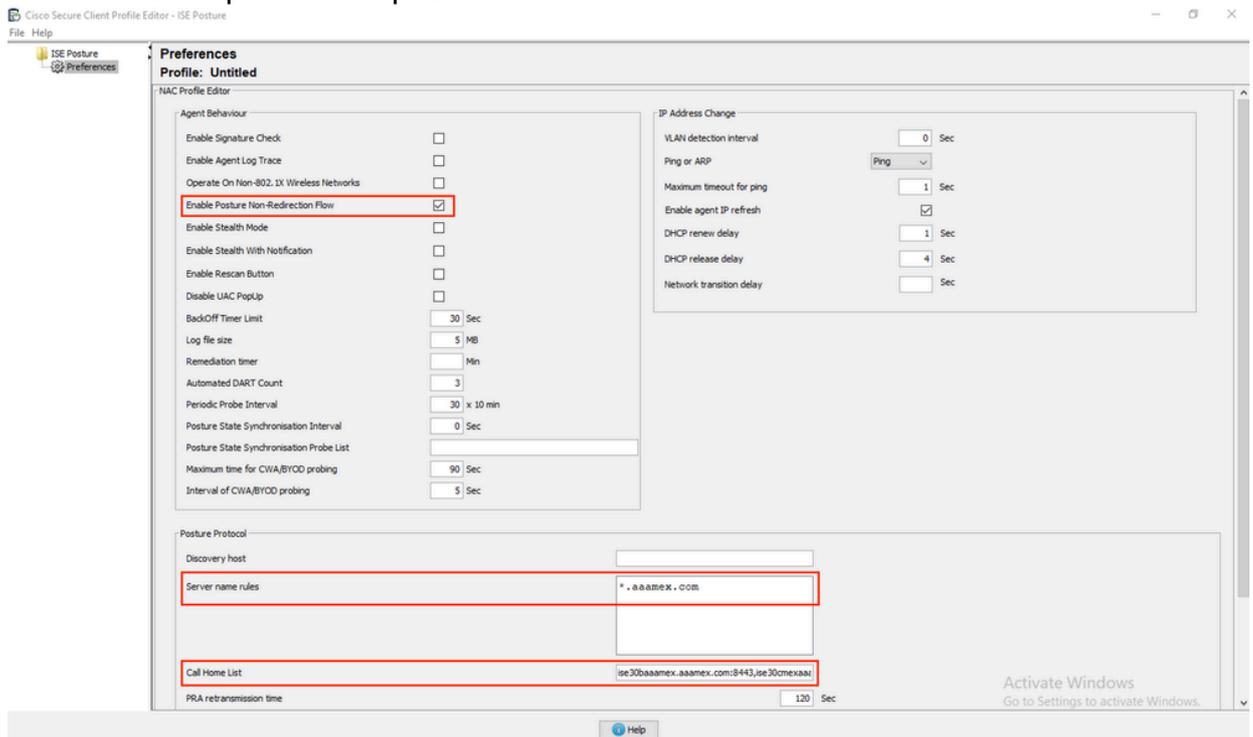
Aprovisionamiento manual (previo a la implementación)

1. Descargue e instale Cisco Secure Client Profile Editor desde [Cisco Software Download](#).

Paquete Profile Editor

2. Abrir el editor de perfiles de postura de ISE:

- Asegúrese de que Enable Posture Non-Redirection Flow esté habilitado.
- Configure las reglas de nombre de servidor separadas por comas. Elija una de estas configuraciones:
 - Un solo asterisco * para permitir la conexión a cualquier PSN.
 - Valores comodín (por ejemplo, *.aaamex.com) para permitir la conexión a cualquier PSN en dominios específicos.
 - Lista de FQDN de PSN, separados por comas, para restringir la conexión a PSN específicos. Si se utiliza, esta lista debe coincidir con la lista de inicio de llamada.
- Configure Call Home List para especificar la lista de PSN separados por comas. Asegúrese de agregar el puerto del portal de aprovisionamiento de clientes con el formato FQDN:puerto o IP:puerto.



Configuración del perfil de postura con Profile Editor



Nota: Consulte el paso 4 de la sección de políticas de aprovisionamiento de clientes para obtener instrucciones sobre cómo verificar el puerto del portal de aprovisionamiento de clientes si es necesario.

3. Guarde el perfil como ISEPostureCFG.xml.

4. Repita los pasos 2 y 3 para crear un nuevo perfil de estado para cada lista de inicio de

llamada en uso.

5. Descargue el paquete de implementación previa de Cisco Secure Client de [Descarga de software de Cisco](#).

Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files	19-Dec-2022	71.39 MB	  
cisco-secure-client-win-5.0.01242-predeploy-k9.zip			
Advisories			

Paquete de preimplementación de Cisco Secure Client

6. Distribuya el perfil y los archivos de instalación en un archivo de almacenamiento o copie los archivos en los clientes.

 **Advertencia:** Asegúrese de que los mismos archivos de Cisco Secure Client también se encuentran en las cabeceras a las que planea conectarse: Firewall seguro ASA, ISE, etc. Incluso cuando se utiliza el aprovisionamiento manual, ISE se debe configurar para el aprovisionamiento de clientes con la versión de software correspondiente. Consulte la sección Configuración de políticas de aprovisionamiento de clientes para obtener instrucciones detalladas.

7. En el cliente, abra el archivo zip y ejecute el comando de configuración para instalar los módulos de estado de ISE y de núcleo. Alternativamente, los archivos msi individuales se pueden utilizar para instalar cada módulo, en este caso, debe asegurarse de que el módulo core-vpn se instale primero.

Name	Type
Profiles	File folder
Setup	File folder
cisco-secure-client-win-5.0.01242-core-vpn-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-dart-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-iseposture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nam-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nvm-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-posture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-sbl-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-umbrella-predeploy-k9	Windows Installer Package
Setup	Application
setup	HTML Application

Contenido del paquete de preimplementación de Cisco Secure Client

Select the Cisco Secure Client 5.0.01242 modules you wish to install:

- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- Select All

- Diagnostic And Reporting Tool

- Lock Down Component Services

Install Selected

Instalador de Cisco Secure Client



Consejo: Instale la herramienta de diagnóstico e informes que se utilizará para solucionar problemas.

8. Una vez finalizada la instalación, copie el archivo posture profile xml en las siguientes ubicaciones:

- Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
- MacOS: /opt/cisco/secureclient/iseposture/

Portal de aprovisionamiento de clientes (Web Deploy)

El portal de aprovisionamiento de clientes de ISE se puede utilizar para instalar el módulo de

estado de ISE de Cisco Secure Client y el perfil de estado de ISE. También se puede utilizar para insertar el perfil de estado solo si el módulo de estado de ISE ya está instalado en el cliente.

1. Vaya a Centros de trabajo > Estado > Aprovisionamiento del cliente > Portal de aprovisionamiento del cliente para abrir la configuración del portal. Expanda la sección Configuración del portal y busque el campo Método de autenticación, seleccione la Secuencia de origen de identidad que se utilizará para la autenticación en el portal.
2. Configure los grupos de identidad internos y externos que estén autorizados para utilizar el Portal de aprovisionamiento de clientes.

Authentication method: * Certificate_Request_Sequence ▾
Configure authentication methods at:
[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available		Chosen
ADAAMEX:saamex.com/AAUnit/AAAGroup	>	provisioning
ADAAMEX:saamex.com/Builtin/Account Operat		ADAAMEX:saamex.com/Users/Domain Users
ADAAMEX:saamex.com/Builtin/Administrators	<	
ADAAMEX:saamex.com/Builtin/Backup Operato		
ADAAMEX:saamex.com/Builtin/Certificate Servi		

[Choose all](#) [Clear all](#)

Método de autenticación y grupos autorizados en la configuración del portal

3. En el campo Nombre de dominio completo (FQDN), configure la URL que utilizan los clientes para acceder al portal. Para configurar varios FQDN, introduzca los valores separados por comas.

Fully qualified domain name (FQDN): clientprovisioning.aaamex

Idle timeout: 10
1-30 (minutes)

Display language: Use browser locale

Fallback language: English - English ▾

Always use: English - English ▾

4. Configure los servidores DNS para resolver la URL del portal en los PSN de la lista de inicio de llamadas correspondiente.
5. Proporcione el FQDN a los usuarios finales para acceder al portal e instalar el software de estado de ISE.

 Nota: Para hacer uso del FQDN del portal, los clientes deben tener la cadena de certificados de administración de PSN, así como la cadena de certificados del portal instalada en el almacén de confianza, y el certificado de administración debe contener el FQDN del portal en el campo SAN.

Política de aprovisionamiento de clientes

El aprovisionamiento de clientes se debe configurar en ISE independientemente del tipo de aprovisionamiento (preimplementación o implementación web) que se utilice para instalar Cisco Secure Client en los terminales.

1. Descargue el paquete de implementación de cabecera de Cisco Secure Client desde

[Descarga de software de Cisco.](#)

Paquete Cisco Secure Client Webdeploy

Cisco Secure Client Headend Deployment Package (Windows) 19-Dec-2022 91.38 MB  
cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg
Advisories 

2. Descargue el paquete webdeploy del módulo de cumplimiento de ISE más reciente de

[Descarga de software de Cisco.](#)

All Release ▾	 AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf
SecureFWPosture >	
ISEComplianceModule ▾	
ISEComplianceModule	
Android >	
NVM >	
5.0 >	

File Information	Release Date	Size	 
ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later. 	30-Jan-2023	19.59 MB	
cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg Advisories 			

3. En ISE, navegue hasta Centros de trabajo > Estado > Aprovisionamiento del cliente > Recursos y haga clic en Agregar > Recursos de agente desde el disco local. Seleccione Cisco Provided Packages en el menú desplegable Category (Categoría) y cargue el Cisco Secure Client Headend Deployment Package descargado anteriormente. Repita el mismo proceso para cargar el módulo de conformidad.

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

Agent Resources From Local Disk

Category: Cisco Provided Packages

Browse... cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 5.0...	AnyConnectDesktopWind...	5.0.1242.0	Cisco Secure Client for Windo...

Submit Cancel

Cargar los paquetes proporcionados por Cisco en ISE

4. De nuevo en la pestaña Resources, haga clic en Add > Agent Posture Profile. En el perfil:
 - Configure un nombre que se pueda utilizar para identificar el perfil y la lista de inicio de llamada dentro de ISE.
 - Asegúrese de que Enable extra probes so non-redirection flow can work esté configurado en Yes.
 - Configure Discovery Backup Server List. Seleccione los PSN que coincidan con la lista de inicio de llamada que se está configurando.
Esta es la lista de PSN guardados en ConnectionData.xml después de la primera conexión.
 - Configure las reglas de nombre de servidor separadas por comas. Elija una de estas configuraciones:
 - Un solo asterisco * para permitir la conexión a cualquier PSN.
 - Valores comodín (por ejemplo, *.aaamex.com) para permitir la conexión a cualquier PSN en dominios específicos.
 - Lista de FQDN de PSN, separados por comas, para restringir la conexión a PSN específicos. Si se utiliza, esta lista debe coincidir con la lista de inicio de llamada.
 - Configure Call Home List para especificar la lista de PSN separados por comas.

Asegúrese de agregar el puerto del portal de aprovisionamiento de clientes con el formato FQDN:puerto o IP:puerto.

Para buscar o modificar el puerto CPP, vaya a Centros de trabajo > Estado > Aprovisionamiento del cliente > Portal de aprovisionamiento del cliente, seleccione el portal en uso, expanda Configuración del portal y busque el puerto HTTP.

* Name: CSC Redirectionless

Description:

Redirectionless Posture LAB - 2 PSNs

Configuración del perfil de postura del agente

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		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	2 PSN(s)	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	*.asamex.com	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	ise30baasamex.asamex.com:8443,ise30cmexaaa.a	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.
Back-off Timer	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Configuración del protocolo de posición en el perfil de posición del agente

5. De nuevo en la pestaña Resources, haga clic en Add > Agent Configuration. Seleccione el paquete Cisco Secure Client y el Módulo de cumplimiento que se utilizarán.

 Advertencia: Si Cisco Secure Client se ha implementado previamente en los clientes, asegúrese de que la versión en ISE coincida con la versión en los terminales. Si se utiliza ASA o FTD para la implementación web, la versión de este dispositivo también puede coincidir.

6. Desplácese hasta la sección Selección de postura y seleccione el perfil que se creó en el paso 1. Haga clic en Enviar en la parte inferior de la página para guardar la configuración.

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1.2.042 

* Configuration
Name:

SecureClient Configuration Redirectionless

Description:

Redirectionless Lab Call Home List 1

Description Value Notes

* 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

Diagnostic

7. Vaya a Centros de trabajo > Estado > Aprovisionamiento del cliente
> Política de aprovisionamiento del cliente. Busque la directiva que se utiliza para el sistema operativo necesario y haga clic en Editar. Haga clic en el signo + de la columna Resultados y seleccione la configuración del agente del paso 5 de la sección Configuración del agente. Haga clic en Guardar en la parte inferior de la página.

 Nota: En el caso de varias listas de inicio de llamada, utilice el campo Otras condiciones para enviar el perfil correcto a los clientes correspondientes. En este ejemplo, Grupo de ubicación de dispositivo se utiliza para identificar el perfil de estado que se envía en la política.

 Consejo: Si se configuran varias políticas de aprovisionamiento de clientes para el mismo sistema operativo, se recomienda hacerlas mutuamente excluyentes; es decir, un cliente determinado solo puede alcanzar una política a la vez. Los atributos RADIUS se pueden utilizar en la columna Otras condiciones para diferenciar una política de otra.

Agent Configuration

SecureClient Configuration Re ...

Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard 

Choose a Wizard Profile 

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"/>	Windows	If Any	and Windows All	and DEVICE:Location EQUALS All Locations#US#WEST	then SecureClient Configuration Redirectionless	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 ▾
☰ <input checked="" type="checkbox"/>	MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 5.0.00533 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP	Edit ▾
☰ <input checked="" type="checkbox"/>	Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP	Edit ▾

Save

Reset

Política de aprovisionamiento de clientes

8. Repita los pasos del 4 al 7 para cada lista de inicio de llamadas y el perfil de estado correspondiente que esté utilizando. Para los entornos híbridos, se pueden utilizar los mismos perfiles para los clientes de redirección.

Autorización

Perfil de autorización

1. Vaya a Directiva > Elementos de directiva > Resultados > Autorización > ACL descargables y haga clic en Agregar.
2. Cree una DACL para permitir el tráfico a DNS, DHCP (si se utiliza), ISE PSN y bloquear otro tráfico. Asegúrese de permitir el acceso a cualquier otro tráfico que sea necesario antes del acceso conforme final.

* Name

Description

IP version IPv4 IPv6 Agnostic ?

* DACL Content

1234567	permit udp any any eq domain
8910111	permit udp any any eq bootps
2131415	permit ip any host <ipn 1 IP address>
1617181	permit ip any host <ipn 2 IP address>
9202122	permit icmp any any
2324252	deny ip any any
6372629	
3031323	
3343536	
3738394	
0414243	

Check DACL Syntax

DACL is valid

Configuración de DACL

permit udp any any eq domain
 permit udp any any eq bootps
 permit ip any host

permit ip any host

deny ip any any

 **Precaución:** Algunos dispositivos de terceros no pueden admitir DACL; en estos casos, es necesario utilizar un ID de filtro u otros atributos específicos del proveedor.



Consulte la documentación del proveedor para obtener más información. Si no se utilizan DACL, asegúrese de configurar la ACL correspondiente en el dispositivo de red.

3. Vaya a Directiva > Elementos de directiva > Resultados > Autorización > Perfiles de autorización y haga clic en Agregar. Dé un nombre al perfil de autorización y seleccione DACL name en Common Tasks. En el menú desplegable, seleccione la DACL creada en el

Authorization Profiles > Redirectionless posture

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name

paso 2.

Perfil de autorización



Nota: Si no se utilizan DACL, utilice Filter-ID de Tareas comunes o Configuración avanzada de atributos para insertar el nombre de ACL correspondiente.

4. Repita los pasos del 1 al 3 para cada lista de inicio de llamada en uso. Para los entornos híbridos, solo es necesario un único perfil de autorización para la redirección. La configuración del perfil de autorización para la redirección está fuera del alcance de este documento.

Política de autorización

1. Navegue hasta Policy > Policy Sets y abra el policy set en uso o cree uno nuevo.
2. Desplácese hacia abajo hasta la sección Directiva de autorización. Cree una política de autorización mediante Session PostureStatus NOT_EQUALS Compliant y seleccione el perfil de autorización creado en la sección anterior.

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Compliant	Session-PostureStatus EQUALS Compliant	Compliant access x	Select from list	0	⚙️
✓	Redirectionless	AND <ul style="list-style-type: none"> DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant 	Redirectionless posture x	Select from list	0	⚙️
✓	Redirection	AND <ul style="list-style-type: none"> Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection 	Redirection posture x	Select from list	0	⚙️
✓	Default		DenyAccess x	Select from list	0	⚙️

Políticas de autorización

- Repita el paso 2 para cada perfil de autorización con su lista de inicio de llamada correspondiente en uso. Para los entornos híbridos, solo es necesaria una política de autorización para la redirección.

Troubleshoot

Cumplimiento de Cisco Secure Client y estado No aplicable (pendiente) en ISE

Sesiones antiguas/fantasma

La presencia de sesiones obsoletas o fantasma en la implementación puede generar fallos intermitentes y aparentemente aleatorios con detección de estado sin redirección, lo que da lugar a que los usuarios se queden atascados en una postura de acceso desconocido/no aplicable en ISE, mientras que la interfaz de usuario de Cisco Secure Client muestra acceso conforme.

[Las sesiones obsoletas](#) son sesiones antiguas que ya no están activas. Se crean mediante una solicitud de autenticación y un inicio de contabilización, pero no se recibe ninguna detención de contabilización en PSN para borrar la sesión.

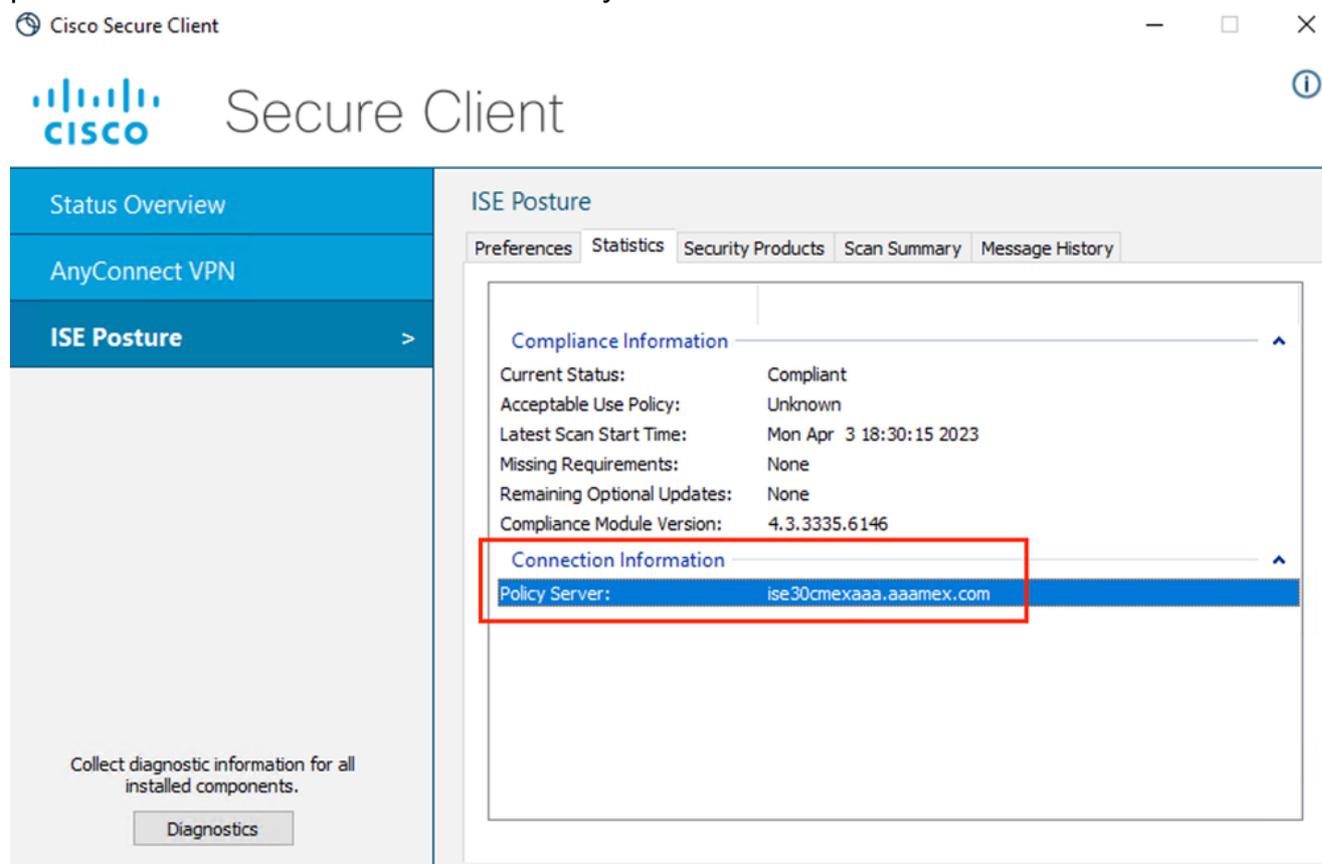
[Las sesiones fantasma](#) son sesiones que nunca estuvieron realmente activas en un PSN en particular. Se crean mediante una actualización intermedia de contabilidad, pero no se recibe ninguna detención de contabilidad en PSN para borrar la sesión.

Identificar

Para identificar un problema de sesión obsoleta/fantasma, verifique el PSN utilizado en el análisis del sistema en el cliente y compárelo con el PSN que realiza la autenticación:

- En la IU de Cisco Secure Client, haga clic en el icono de engranaje en la esquina inferior

izquierda. En el menú de la izquierda, abra la sección Postura de ISE y navegue hasta la pestaña Estadísticas. Tome nota de Policy Server en Connection Information.



Servidor de políticas para estado de ISE en Cisco Secure Client

2. En los registros en directo de RADIUS de ISE, tenga en cuenta lo siguiente:

- Cambio de estado
- Cambio en el servidor
- Sin cambios en la directiva de autorización y el perfil de autorización
- No CoA live log

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
Apr 03, 2023 07:32:52.3...	●		0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	Ise30cmexaaa	Compliant	Redirectionless posture
Apr 03, 2023 07:32:40.7...	✓			#ACSACL#-IP-...			Ise30baaamex		
Apr 03, 2023 07:32:40.6...	✓			redirectionless	00:50:5...	Posture Lab >> Redirectionless	Ise30baaamex	NotApplicable	Redirectionless posture

Registros en directo para sesiones antiguas/fantasma

3. Abra la sesión en vivo o los detalles del registro en vivo de la última autenticación. Tome nota de Policy Server, si difiere del servidor observado en el paso 1, esto indica un problema con las sesiones obsoletas/fantasma.

Overview

Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

Authentication Details

Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691

Policy Server	ise30baaamex
---------------	--------------

Event	5200 Authentication succeeded
Username	redirectionless

Servidor de políticas en detalles de registro activo

Solución

Las versiones de ISE posteriores al parche 6 y al parche 3 de ISE 2.6 implementan [RADIUS Session Directory](#) como solución para el escenario de sesión fantasma/obsoleto en el flujo de estado sin redirección.

1. Vaya a Administration > System > Settings > Light Data Distribution y verifique que la casilla de verificación Enable RADIUS Session Directory esté habilitada.

The screenshot shows the ISE Settings page with the 'Settings' tab selected. The left sidebar contains a list of settings categories, with 'Light Data Distribution' highlighted in a red box. The main content area is titled 'RADIUS Session Directory' and contains the following text: 'Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.' Below this text is a checkbox labeled 'Enable RADIUS Session Directory' which is checked and highlighted in a red box. The next section is 'Endpoint Owner Directory' with the text: 'Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address connecting to ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling service, disabling this option will use legacy Profiler owners directory.' Below this is a checked checkbox labeled 'Enable Endpoint Owner Directory'. The final section is 'Advanced Settings' with the text: 'Configure the following options for RSD and EPOD.' Below this text are two settings: 'Batch size' set to '10' and 'Items' with a circular refresh icon.

Activar el directorio de sesión RADIUS

2. Desde ISE CLI, verifique que ISE Messaging Service se esté ejecutando en todos los PSN ejecutando el comando show applications status ise.

```
lise30cmexaaa/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	12434
Database Server	running	112 PROCESSES
Application Server	running	33093
Profiler Database	running	19622
ISE Indexing Engine	running	42923
AD Connector	running	60317
M&T Session Database	running	19361
M&T Log Processor	running	33283
Certificate Authority Service	disabled	
EST Service	disabled	
SXP Engine Service	disabled	
Docker Daemon	running	14791
TC-NAC MongoDB Container	running	18594
TC-NAC Core Engine Container	running	18981
VA Database	running	53465
VA Service	running	53906
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	running	55480
PassiveID Syslog Service	running	56312
PassiveID API Service	running	57153
PassiveID Agent Service	running	58079
PassiveID Endpoint Service	running	59138
PassiveID SPAN Service	running	60059
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	16526
ISE API Gateway Database Service	running	18463
ISE API Gateway Service	running	23052

Servicio de mensajería ISE en ejecución



Nota: Este servicio hace referencia al método de comunicación que se utiliza para RSD entre PSN y que se puede ejecutar independientemente del estado de la configuración del servicio de mensajería de ISE para syslog que se puede establecer desde la IU de ISE.

3. Navegue hasta ISE Dashboard y localice el dashlet Alarmas. Verifique si existen alarmas de error de link de cola. Haga clic en el nombre de la alarma para ver más detalles.

Severity	Name	Occu...	Last Occurred
	queue	x	
	Queue Link Error	2143	37 mins ago

Last refreshed: 2023-04-03 14:45:19

Alarmas de error de enlace de cola

4. Verifique si las alarmas se generan entre los PSN utilizados para el estado.

Alarms: Queue Link Error

Description

The queue link between two nodes in the ISE deployment is down.

Suggested Actions

Please check and restore connectivity between the nodes. Ensure that the nodes and the ISE Messaging Service are up and running. Ensure that ISE Messaging Service ports are not blocked by firewall. Please note that these alarms could occur between nodes, when the nodes are being registered to deployment or manually-synced from PSPAN or when the nodes are in out-of-sync state or when the nodes are getting restarted.

Rows/Page 100 << 1 / 22 >> Go 2143 Total Rows

Refresh Acknowledge

<input type="checkbox"/> Time Stamp	Description	Cause= {tis_alert;" unknown Ca"}	Details
<input type="checkbox"/> Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From Ise30cmexaaa.aamex.com To Ise30baaamex.aamex.com; Cause={tis_alert;" unkno...		
<input type="checkbox"/> Apr 03 2023 21:07:00.959 PM	Queue Link Error: Message=From Ise30baaamex.aamex.com To Ise30cmexaaa.aamex.com; Cause={tis_alert;" unkno...		

Detalles de la alarma de error de enlace de cola

5. Pase el ratón sobre la descripción de la alarma para ver todos los detalles y tome nota del campo Causa. Las dos causas más comunes del error de link de cola son:

- Tiempo de espera: indica que las solicitudes enviadas por un nodo a otro nodo en el puerto 8671 no se responden dentro del umbral. Para remediar, verifique que el puerto TCP 8671 esté permitido entre los nodos.
- CA desconocida: indica que la cadena de certificados que firma el certificado de

mensajería ISE no es válida o está incompleta. Para remediar este error:

- a. Vaya a Administration > System > Certificates > Certificate signing requests.
- b. Haga clic en Generar solicitudes de firma de certificado (CSR).
- c. En el menú desplegable, seleccione ISE Root CA y haga clic en la cadena Replace ISE Root CA Certificate.
Si la CA raíz de ISE no está disponible, navegue hasta Certificate Authority > Internal CA settings y haga clic en Enable Certificate Authority, luego vuelva a CSR y regenere la CA raíz.
- d. Genere una nueva CSR y seleccione ISE Messaging Service en el menú desplegable.
- e. Seleccione todos los nodos de la implementación y vuelva a generar el certificado.



Nota: Se espera que observe las alarmas de error de link de cola con la causa Unknown CA o Econndened mientras se regeneran los certificados. Supervise las alarmas después de la generación del certificado para confirmar que el problema se ha resuelto.

Rendimiento

Identificar

Los problemas de rendimiento, como la alta utilización de la CPU y el alto promedio de carga relacionados con el estado sin redirección, pueden afectar a los nodos de PSN y MnT, y a menudo van acompañados o precedidos de estos eventos:

- Aleatorio o intermitente, ningún servidor de políticas detectó errores, en Cisco Secure Client.
- El límite máximo de recursos alcanzado en los informes para el grupo de subprocesos del servicio Portal alcanzó los eventos de valor de umbral. Navegue hasta Operaciones > Informes > Informes > Auditoría > Auditoría de operaciones para ver los informes.
- La consulta de posición a la búsqueda MNT es una alarma alta. Estas alarmas solo se generan en ISE 3.1 y versiones posteriores.

Solución

Si el rendimiento del despliegue se ve afectado por una postura sin redirección, esto suele ser indicativo de una implementación ineficaz. Se recomienda revisar estos aspectos:

- Número de PSN utilizados por lista de inicio de llamadas. Considere la posibilidad de reducir el número de PSN que se pueden utilizar para el estado por terminal o dispositivo de red según el diseño.
- Puerto del portal de aprovisionamiento de clientes en la lista de inicio de llamadas. Asegúrese de que el número de puerto del portal se incluye después de la dirección IP o FQDN de cada nodo.

Para mitigar el impacto:

1. Borre connectiondata.xml de los terminales eliminando el archivo de la carpeta Cisco Secure Client y reinicie el servicio de estado de ISE o Cisco Secure Client. Si no se reinician los servicios, el archivo antiguo se regenera y los cambios no surten efecto. Esta acción también se puede realizar después de revisar y modificar las listas de inicio de llamada.
2. Utilice las DACL u otras ACL para bloquear el tráfico a los PSN de ISE para las conexiones de red donde no sea relevante:
 - En el caso de conexiones en las que el estado no se aplica en las políticas de autorización, pero que se aplican a terminales con el módulo de estado ISE de Cisco Secure Client instalado, bloquee el tráfico de los clientes a todos los PSN de ISE para los puertos TCP 8905 y el puerto del portal de aprovisionamiento de clientes. Esta acción también se recomienda para el estado con implementación de redirección.
 - Para conexiones en las que se aplica el estado en las políticas de autorización, permita el tráfico de los clientes al PSN de autenticación y bloquee el tráfico a otros PSN en la implementación. Esta acción puede implementarse temporalmente mientras se revisa el diseño.

[Authorization Profiles](#) > Redirectionless-PSN1

Authorization Profile

* Name	Redirectionless PSN1
Description	Authorization profile for redirectionless posture with DACL allowing traffic only to PSN1, DNS and DHCP
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> ⓘ
Agentless Posture	<input type="checkbox"/> ⓘ
Passive Identity Tracking	<input type="checkbox"/> ⓘ

Common Tasks

DACL Name redirectionless_posture_psn1

Perfil de autorización con DACL para PSN único

Compliant		Session-PostureStatus EQUALS Compliant	Compliant access x
Redirectionless PSN1	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant Network Access-ISE Host Name EQUALS ise30baamex.aaamex.com	Redirectionless PSN1 x
Redirectionless PSN2	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant Network Access-ISE Host Name EQUALS ise30cmexaaa.aaamex.com	Redirectionless PSN2 x
Redirection	AND	Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection	Redirection posture x

Políticas de autorización por PSN

Contabilidad

La contabilidad RADIUS es esencial para la gestión de sesiones en ISE. Dado que el estado se basa en una sesión activa que se va a realizar, una configuración incorrecta o inexistente de la contabilidad también puede afectar a la detección del estado y al rendimiento de ISE. Es importante verificar que la contabilización esté configurada correctamente en el dispositivo de red para enviar solicitudes de autenticación, inicio de contabilización, detención de contabilización y actualizaciones de contabilización a un único PSN para cada sesión.

Para verificar los paquetes de contabilización recibidos en ISE, navegue hasta Operaciones > Informes > Informes > Terminales y usuarios > Contabilización RADIUS.

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).