

Implementación de 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 \(implementación web\)](#)
[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 de versiones anteriores de ISE con el flujo de estado de ISE en ISE 2.2](#)

[Gestión 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 3.1
- 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 los siguientes 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 versiones anteriores de ISE con el flujo de posición de ISE en ISE 2.2](#).

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

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

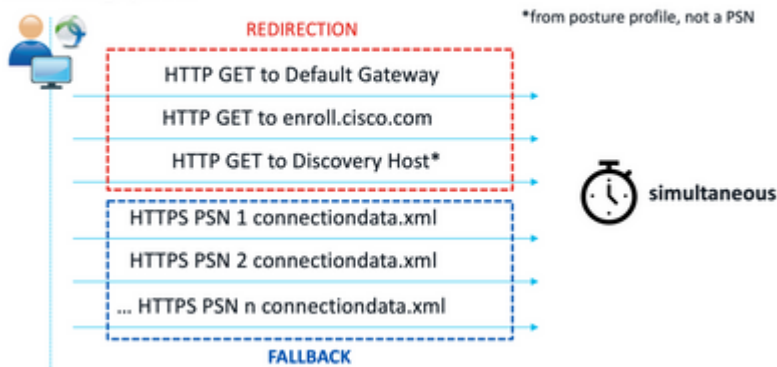
Connectiondata.xml

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

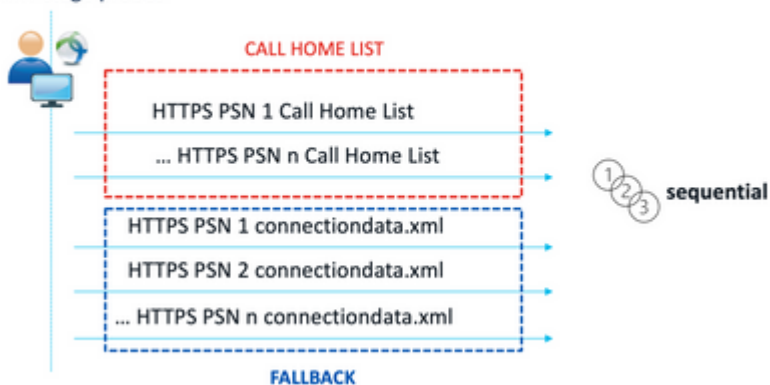
No-MnT stage probes



Sondas de detección de fase 1

Stage 2 discovery probes

MnT stage probes



Sondas de detección de fase 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.

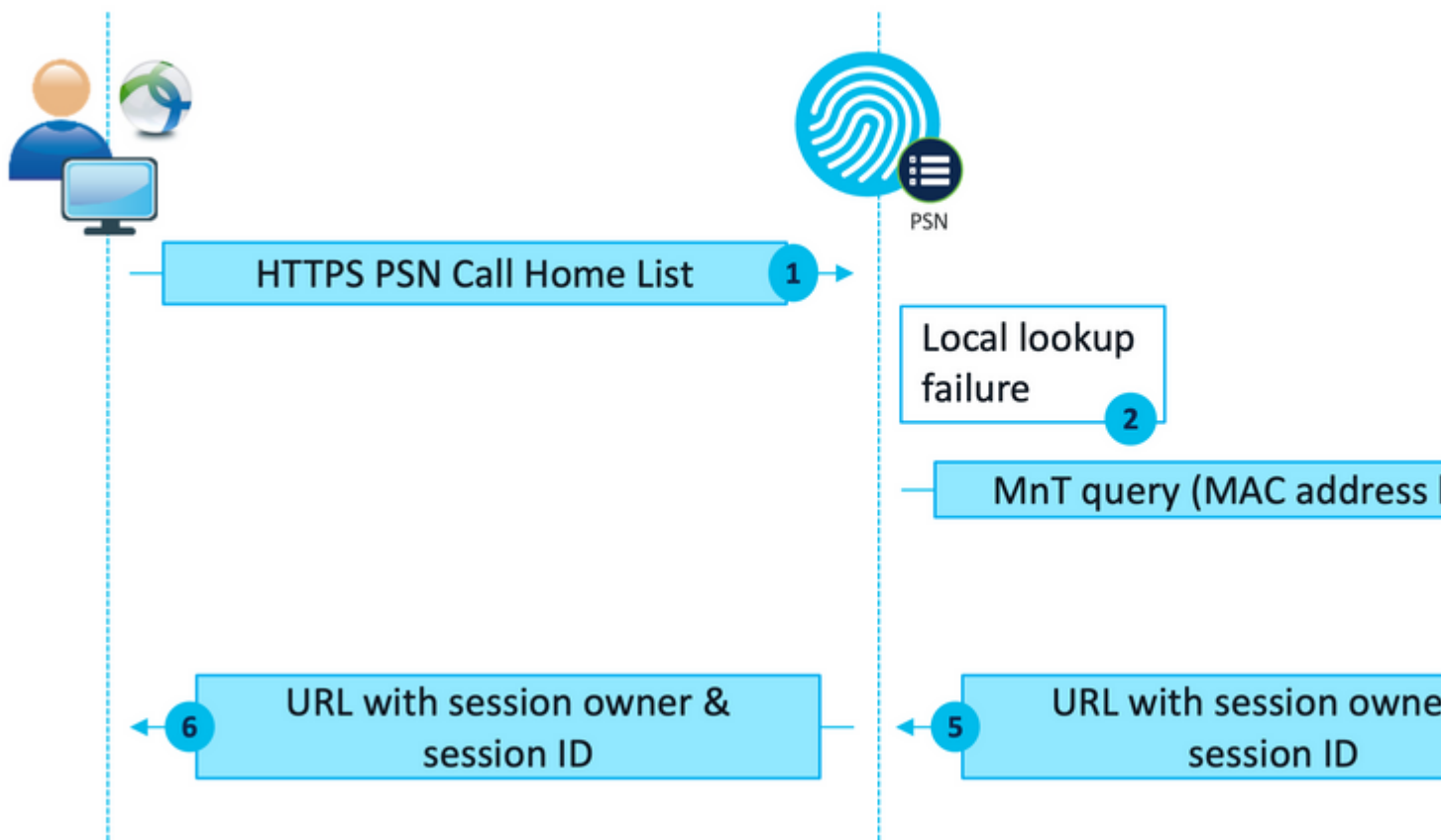
Lista de inicio de llamadas

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 connectiondata.xml, lo crea y mantiene un administrador de ISE y es posible que requiera una fase de diseño para lograr una configuración óptima. La lista de PSN de la lista de inicio de llamada debe coincidir con la lista de servidores de autenticación y cuentas configurada 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 debe limitarse del mismo modo para que coincida con la lista de inicio de llamadas correspondiente.

Al desarrollar la estrategia de distribución de PSN para determinar el número máximo de PSN en cada lista de inicio de llamadas, se pueden tener en cuenta los siguientes aspectos:

- 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)

2. En ISE, navegue hasta **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 del dispositivo 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](#).

Profile Editor (Windows)

19-Dec-2022

15.74 MB

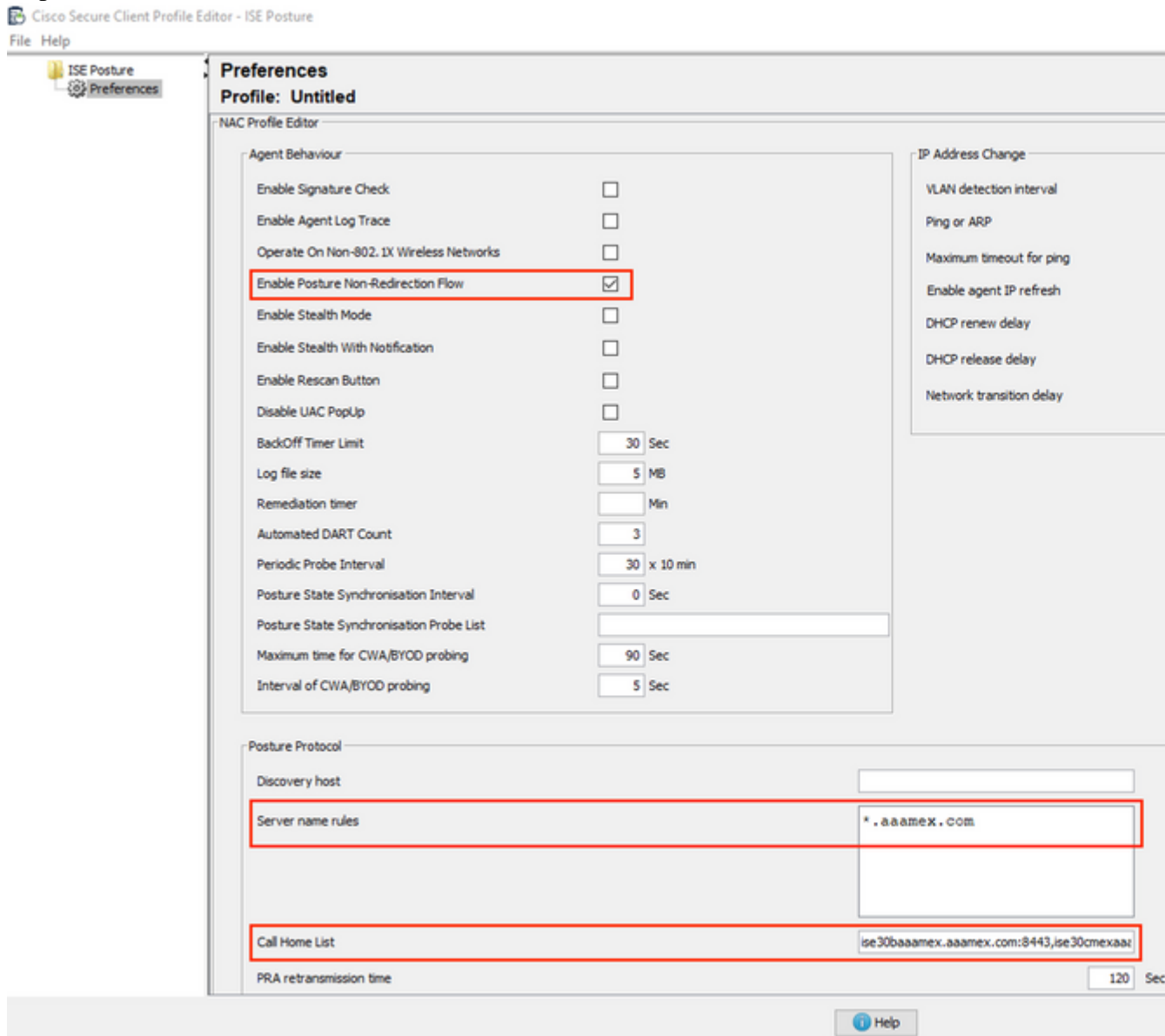
[tools-cisco-secure-client-win-5.0.01242-profileeditor-k9.msi](#)

[Advisories](#)

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. Utilice un solo asterisco * para permitir la conexión a cualquier PSN, valores comodín para permitir la conexión a cualquier PSN en un dominio específico o FQDN de PSN para restringir la conexión a PSN específicos.

- 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 el Editor de perfiles

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

3. Repita el paso 2 para cada lista de inicio de llamada en uso.
4. Descargue el paquete de implementación previa de Cisco Secure Client desde [Descarga de software de Cisco](#).

[cisco-secure-client-win-5.0.01242-predeploy-k9.zip](#)

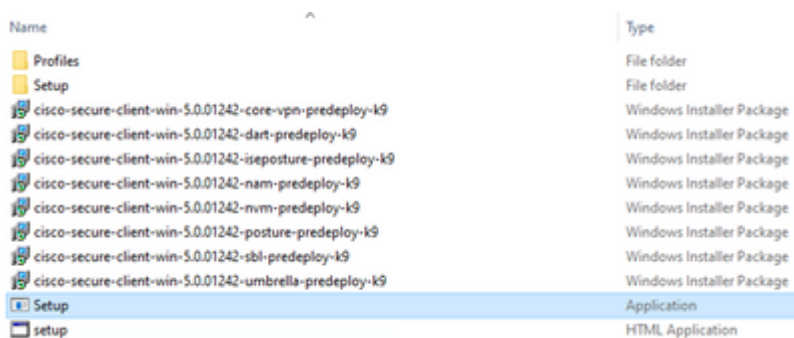
[Advisories](#) 

Paquete de preimplementación de Cisco Secure Client

5. Guarde el perfil como ISEPostureCFG.xml.
6. Distribuya el perfil y los archivos de instalación en un archivo de almacenamiento o copie los archivos en los clientes.

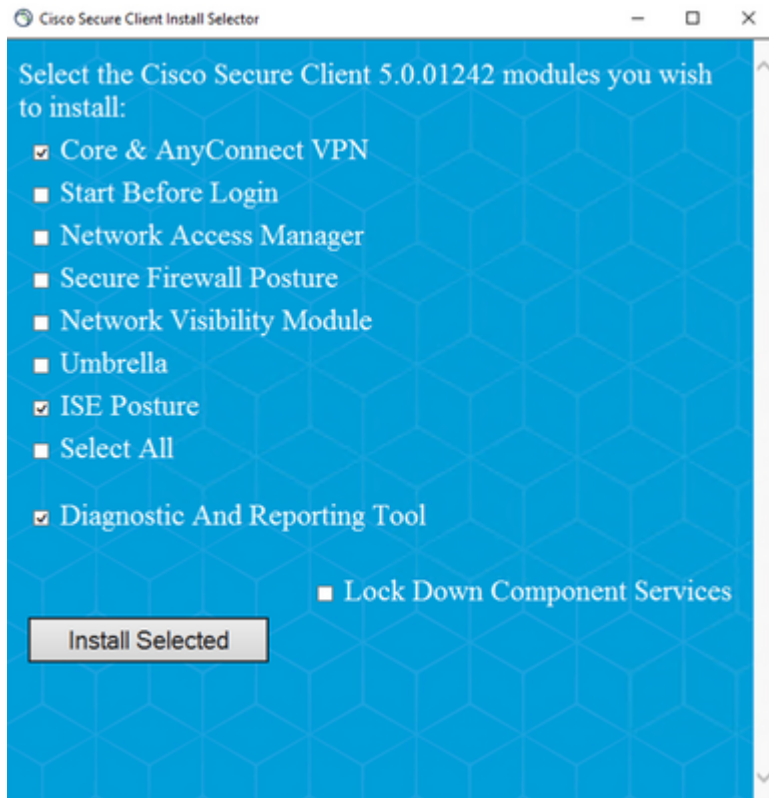
Advertencia: Asegúrese de que los mismos archivos de Cisco Secure Client también se encuentran en las cabeceras a las que tiene pensado conectarse: Secure Firewall ASA, ISE, etc. Incluso cuando se utiliza el aprovisionamiento manual, ISE se debe configurar para el aprovisionamiento de clientes con la 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 en y ejecute el programa de instalación 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



instalador de Cisco Secure Client

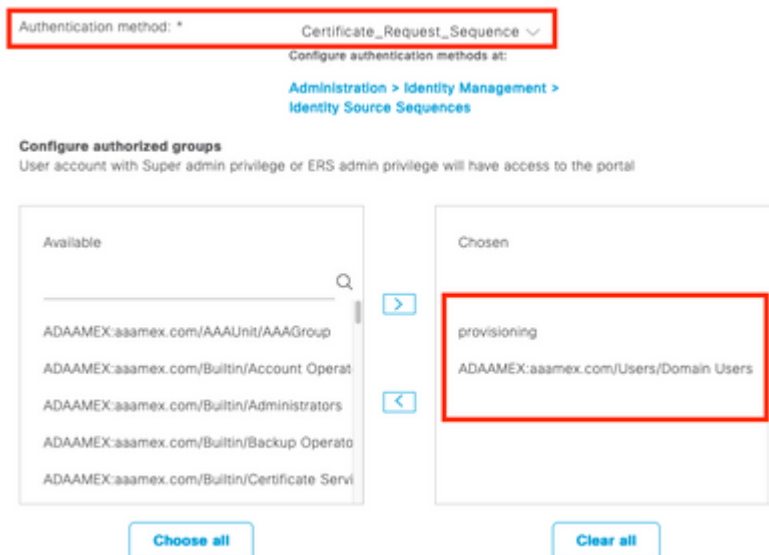
Sugerencia: instale la herramienta de diagnóstico e informes que se utilizará para solucionar problemas.

8. Una vez finalizada la instalación, copie el perfil de estado xml en las siguientes ubicaciones:
 - Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
 - MacOS: /opt/cisco/secureclient/iseposture/

Portal de aprovisionamiento de clientes (implementación web)

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. Navegue hasta **Centros de trabajo > Postura > Aprovisionamiento del cliente > Portal de aprovisionamiento del cliente** para abrir la configuración del portal. Expandir 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 están autorizados para utilizar el portal de aprovisionamiento de clientes.



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.

The screenshot shows the 'Fully qualified domain name (FQDN):' field with the value 'clientprovisioning.aaamex' entered. Below it, the 'Idle timeout:' is set to '10' minutes, with a range of '1-30 (minutes)'. The 'Display language:' is set to 'Use browser locale', and the 'Fallback language:' is 'English - English'. There is also an option for '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 utilizar el 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 web de Cisco Secure Client desde [Descarga de software de Cisco](#).

Cisco Secure Client Headend Deployment Package (Windows) 

19-Dec-2022

91.38

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


[Advisories](#) 

Paquete de implementación web de Cisco Secure Client

2. Descargue el paquete webdeploy del módulo de cumplimiento más reciente de [Cisco Software Download](#).



The screenshot shows the Cisco Software Download interface. On the left, a navigation menu is visible with the following items: All Release (dropdown), SecureFWPosture (dropdown), ISEComplianceModule (dropdown, highlighted with a red box), ISEComplianceModule (sub-item, highlighted with a red box), Android (dropdown), NVM (dropdown), and 5.0 (dropdown). On the right, there is a warning banner for AnyConnect 4.x & Secure Client 5.x. Below the banner is a table with the following content:

File Information	Release Date
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
cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg	
Advisories 	

Paquete webdeploy del módulo de cumplimiento de ISE

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

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 S

Submit

Cancel

Cargar los paquetes proporcionados por Cisco en ISE

- De nuevo en la pestaña **Resources**, haga clic en **Add > AnyConnect Posture Profile**. En el perfil:
 - Configure un **nombre** que se pueda utilizar para identificar el perfil dentro de ISE.
 - Configure las **reglas de nombre de servidor** separadas por comas. Utilice un solo asterisco * para permitir la conexión a cualquier PSN, valores comodín para permitir la conexión a cualquier PSN en un dominio específico o FQDN de PSN para restringir la conexión a PSN específicos.
 - 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.

* Name: CSC Redirectionless

Description: Redirectionless Posture LAB - 2 PSNs

Configuración del perfil de estado de ISE I

Posture Protocol

Parameter	Value	Notes	Description
PSA retransmission time	120 secs		This is the agent retry period if there is a Passive Assessment communication failure.
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery Host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	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.
Server name rules	*.asamex.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	vix.asamex.com:8443	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	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	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till the max time limit is reached

Configuración del perfil de postura de ISE II

Para buscar el puerto que se debe utilizar en la lista de inicio de llamada, vaya a **Centros de trabajo > Estado > Aprovisionamiento del cliente > Portal de aprovisionamiento del cliente**, seleccione el portal en uso y expanda Configuración del portal.

Portals Settings and Customization

Portal Name:
Client Provisioning Portal (default)

Description:
Default portal and user experience user

Language File ▼

[Portal test URL](#)

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:* **8443**

(8000 - 8999)

5. De nuevo en la pestaña **Resources**, haga clic en **Add > AnyConnect 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 de ISE coincida con la versión de los terminales. Si se utiliza ASA o FTD para la implementación web, la versión de este dispositivo también debe coincidir.

6. Desplácese hacia abajo hasta la sección **Selección de posición** y seleccione el perfil que se creó en el paso 1. Haga clic en **Submit** en la parte inferior de la página para guardar la configuración.

* Select AnyConnect Package: CiscoSecureClientDesktopWindows 5.0 ▾

* Configuration Name: AnyConnect Configuration Redirectionless

Description: ISE Redirectionless Posture LAB

Description Value Notes

* Compliance Module: ComplianceModuleWindows 4.3.3335.6146 ▾

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input checked="" type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input checked="" type="checkbox"/>

Configuración de AnyConnect

Profile Selection

* ISE Posture: CSC Redirectionless ▾

VPN ▾

Selección de perfil

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 de AnyConnect del paso 5 de la sección **Configuración del agente**.

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 el ejemplo, Grupo de ubicación de

dispositivos se utiliza para identificar el perfil de estado que se introduce en la política.

Sugerencia: 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 debería poder acceder a una política a la vez. Los atributos RADIUS se pueden utilizar en la columna **Otras condiciones** para diferenciar una política de otra.

Agent Configuration

ect Configuration Redirectionless[▼]

Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard [▼]

Choose a Wizard Profile [▼]

Configuración del agente de políticas de aprovisionamiento de clientes

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.

▼

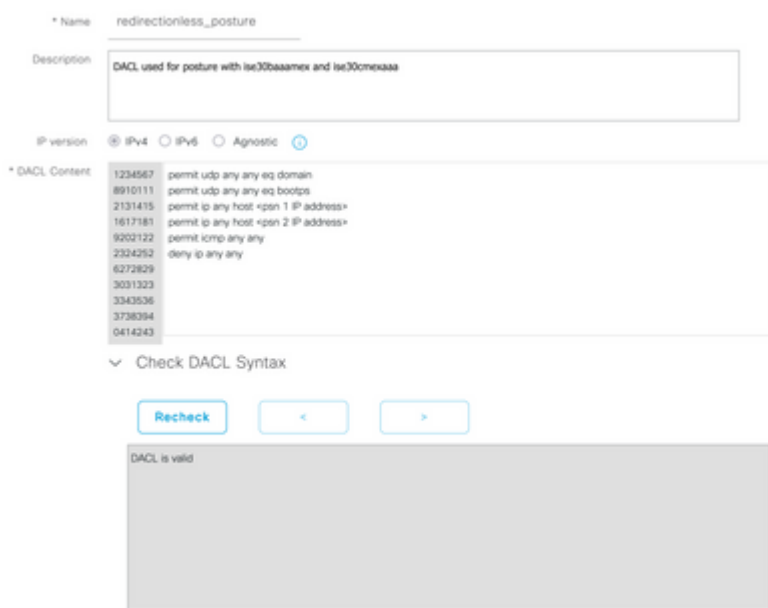
	Rule Name	Identity Groups	Operating Systems	Other Conditions
☰ <input checked="" type="checkbox"/>	IOS	If Any	and Apple iOS All	and Condition(s)
☰ <input checked="" type="checkbox"/>	Android	If Any	and Android	and Condition(s)
☰ <input checked="" type="checkbox"/>	Windows	If Any	and Windows All	and DEVICE:Location EQUALS All Locations#US#WEST
☰ <input checked="" type="checkbox"/>	MAC OS	If Any	and Mac OSX	and Condition(s)
☰ <input checked="" type="checkbox"/>	Chromebook	If Any	and Chrome OS All	and Condition(s)

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. Navegue hasta Directiva > Elementos de política > 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.



configuración 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: es posible que algunos dispositivos de terceros no admitan 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. Asigne un nombre al perfil de autorización y seleccione **DACL name** en **Common Tasks**. En el menú desplegable, seleccione la DACL creada en el paso 2.

[Authorization Profiles](#) > Redirectionless posture

Authorization Profile

* Name	Redirectionless posture
Description	<div style="border: 1px solid #ccc; height: 80px;"></div>
* 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

<input checked="" type="checkbox"/> DACL Name	redirectionless_posture
---	-------------------------

Perfil de autorización

Nota: Si no se utilizan DACL, utilice **Filter-ID** de **Tareas comunes** o **Advanced Attribute Settings** 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 conjunto de políticas 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.

Authorization Policy (4)

Status	Rule Name	Conditions	Profiles
✓	Compliant	Session-PostureStatus EQUALS Compliant	Compliant access ×
✓	Redirectionless	AND ● DEVICE-Posture EQUALS Posture#Redirectionless ● DEVICE-Location EQUALS All Locations#US#WEST ● Session-PostureStatus NOT_EQUALS Compliant	Redirectionless posture ×
✓	Redirection	AND ● Session-PostureStatus NOT_EQUALS Compliant ● DEVICE-Posture EQUALS Posture#Redirection	Redirection posture ×
✓	Default		DenyAccess ×

Políticas de autorización

3. 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.

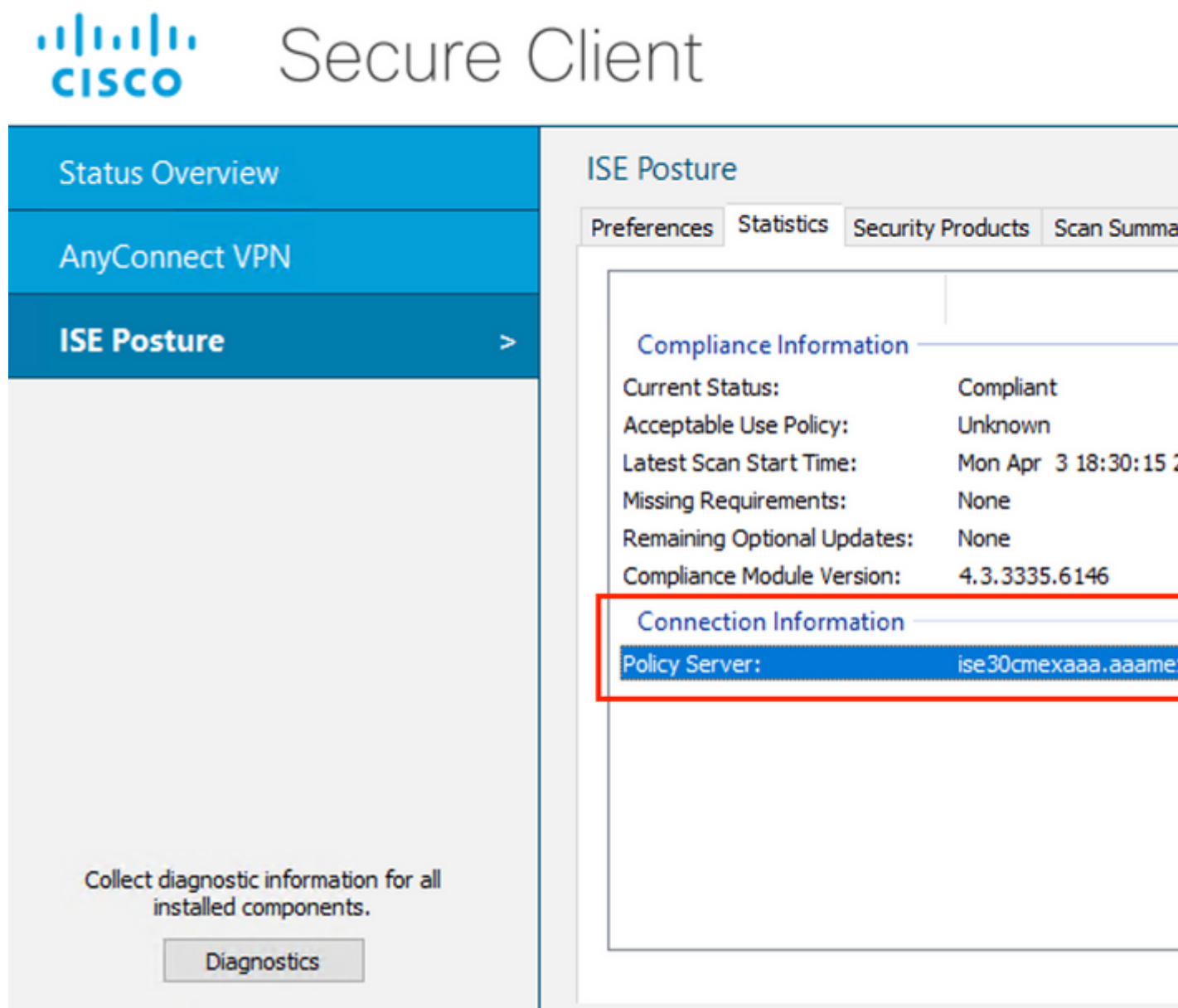
[Las sesiones fantasma](#) son sesiones que nunca estuvieron realmente activas en un PSN en particular. Se crean mediante una actualización intermedia de contabilidad, pero no se recibe ninguna detención de contabilidad en PSN para borrar la sesión.

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:

1. 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.

 Cisco Secure Client



The screenshot shows the Cisco Secure Client interface. On the left is a navigation menu with options: Status Overview, AnyConnect VPN, and ISE Posture (selected). The main area displays the ISE Posture section with tabs for Preferences, Statistics, Security Products, and Scan Summary. The Statistics tab is active, showing Compliance Information and Connection Information. The Connection Information section is highlighted with a red box, showing the Policy Server as ise30cmexaaa.aaame.

Compliance Information	
Current Status:	Compliant
Acceptable Use Policy:	Unknown
Latest Scan Start Time:	Mon Apr 3 18:30:15 2
Missing Requirements:	None
Remaining Optional Updates:	None
Compliance Module Version:	4.3.3335.6146

Connection Information	
Policy Server:	ise30cmexaaa.aaame

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
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa
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

Registros en directo para sesiones antiguas/fantasma

3. Abra la sesión en directo o los detalles del registro en directo 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 que están por encima del parche 6 de ISE 2.6 y del parche 3 de ISE implementan [RADIUS Session Directory](#) como solución para el escenario de sesión fantasma/obsoleto en el flujo de estado sin redirección.

1. Navegue hasta Administración > **Sistema** > **Configuración** > **Distribución de datos ligeros** y verifique que la casilla de verificación **Habilitar el directorio de sesión RADIUS** esté habilitada.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Back

FIPS Mode
Security Settings
Alarm Settings
Posture >
Profiling
Protocols >
Endpoint Scripts >
Proxy
SMTP Server
SMS Gateway
System Time 
ERS Settings
API Gateway Settings
Network Success Diagnostics >
DHCP & DNS Services
Max Sessions
Light Data Distribution

RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

Enable RADIUS Session Directory



Endpoint Owner Directory

Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address in ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling sessions. The option will use legacy Profiler owners directory.

Enable Endpoint Owner Directory

Advanced Settings

Configure the following options for RSD and EPOD.

Batch size
10  Items 

Activar el directorio de sesión RADIUS

- Desde la CLI de ISE, ejecute el comando para verificar que **ISE Messaging Service** se esté ejecutando en **todos los PSN** `show applications status ise`.

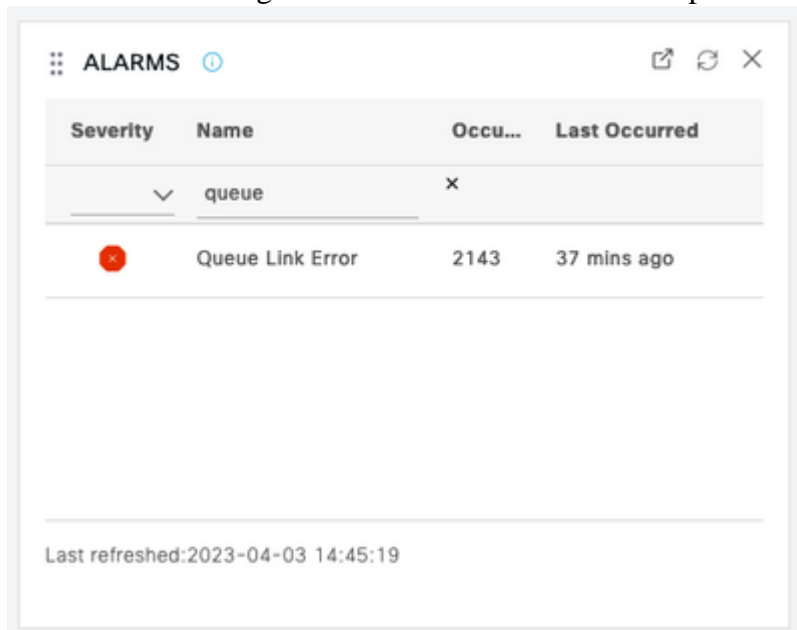
```
ise30cmexaaa/admin# show application status ise
```

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 debe ejecutarse independientemente del estado de la configuración del servicio de mensajería ISE para syslog que se puede establecer desde la interfaz de usuario de ISE.

- 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.



Alarmas de error de enlace de cola

- 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 firewalls or 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

Refresh Acknowledge

<input type="checkbox"/> Time Stamp	Description	Cause={tls_alert;" unknown Ca" }
<input type="checkbox"/> Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From ise30cmexaaa.aaamex.com To ise30baaamex.aaamex.com; Cause={tls_alert;" unkno...	
<input type="checkbox"/> Apr 03 2023 21:07:00.959 PM	Queue Link Error: Message=From ise30baaamex.aaamex.com To ise30cmexaaa.aaamex.com; Cause={tls_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 han respondido 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 de 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 regrese 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 Econn denied mientras se regeneran los certificados, monitoree 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 los siguientes eventos:

- Aleatorio o intermitente *No se detectaron* errores de *servidor de políticas* en Cisco Secure Client
- *El límite máximo de informes alcanzados* para el grupo de *subprocesos del servicio Portal* alcanzó los eventos de *valor de umbral*. Vaya a Operaciones > **Informes > Informes > Auditoría > Auditoría de operaciones** para ver los informes.

- *La consulta de estado a la búsqueda de MNT es una alarma alta.* Estas alarmas solo se generan en las versiones de ISE 3.1 y 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 los siguientes 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 quitando 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 debe realizarse después de revisar y modificar las listas de Call Home.
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 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

<input checked="" type="checkbox"/> DACL Name	redirectionless_posture_psn1
---	------------------------------

Perfil de autorización con DACL para PSN único

✓	Compliant	⌵	Session-PostureStatus EQUALS Compliant
✓	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 Ise30baaamex.aaam
✓	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.aaam
✓	Redirection	AND	⌵ Session-PostureStatus NOT_EQUALS Compliant ⌵ DEVICE-Posture EQUALS Posture#Redirection

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

- [Asistencia técnica 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).