Comprender y configurar la condición de estado de ISE del servicio macOS

Contenido

Introducción

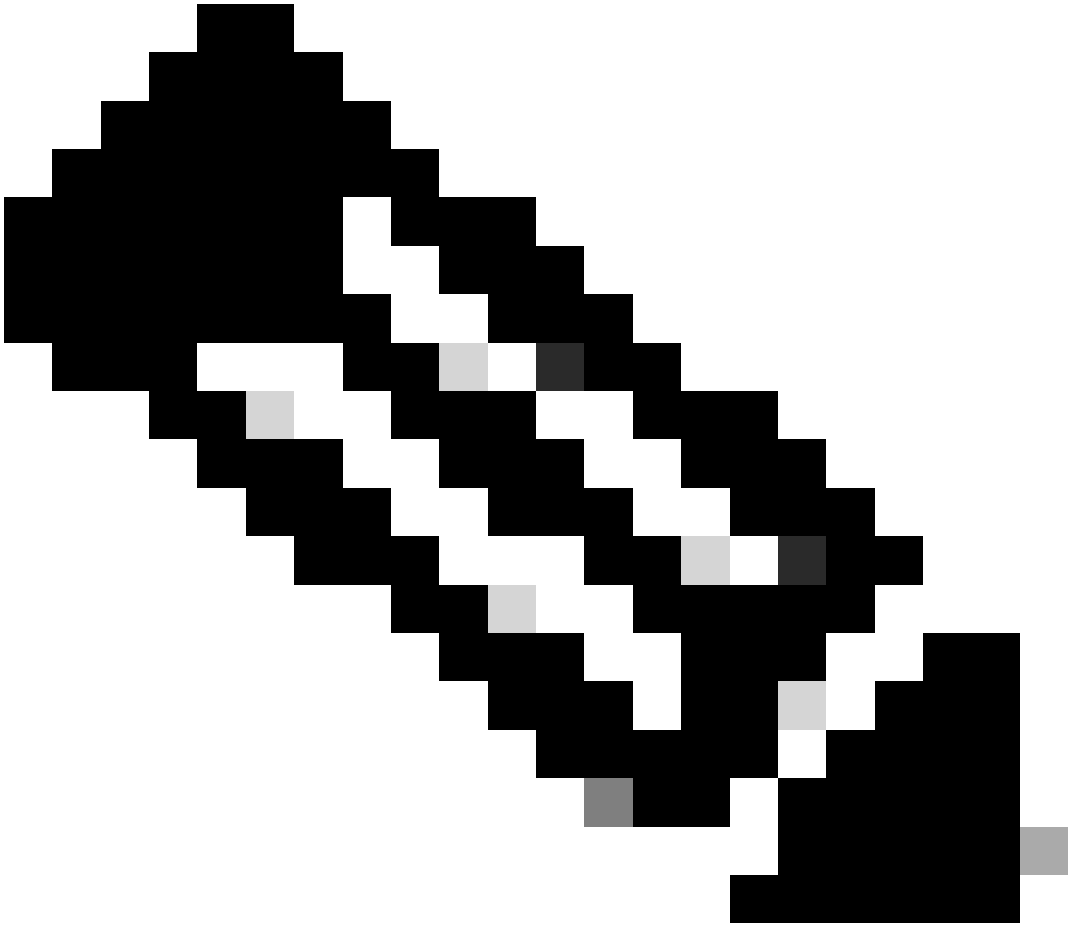
Este documento describe el proceso de configuración de la condición de servicio de macOS en Cisco ISE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de macOS.
- Conocimiento del flujo de estado de ISE.



Nota: Este documento cubre la configuración para la condición de servicio de macOS. Este documento no trata la configuración de la postura inicial.

Componentes Utilizados

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

- Parche 1 de Cisco ISE 3.3
- dispositivo macoOS que ejecuta Sonoma 14.3.1
- Cisco Secure Client 5.1.2.42
- Compliance Module versión 4.3.3432.64000

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.

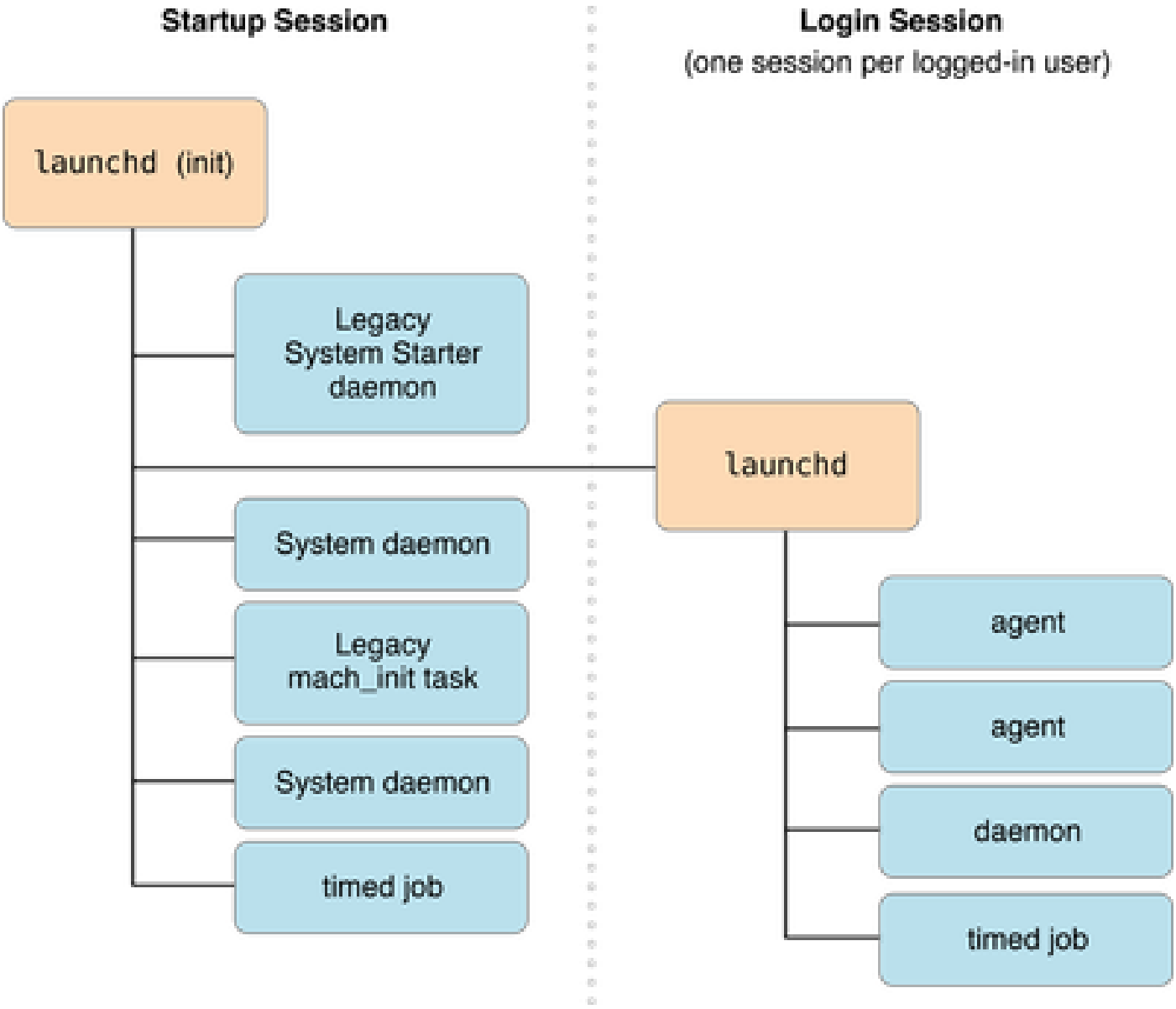
Antecedentes

La condición de servicio de macOS es útil cuando tiene que usar un caso para verificar si un servicio está cargado en el dispositivo macOS, y también le permite verificar si se está ejecutando o no. La condición de servicio de macOS puede verificar dos tipos de servicio diferentes: demonios y agentes.

Un daemon es un programa que se ejecuta en segundo plano como parte del sistema general (es decir, no está vinculado a un usuario concreto). Un demonio no puede mostrar ninguna GUI; más concretamente, no está permitido conectarse al servidor de windows. Un servidor web es el ejemplo perfecto de un demonio.

Un agente es un proceso que se ejecuta en segundo plano en nombre de un usuario determinado. Los agentes son útiles porque pueden hacer cosas que los demonios no pueden, como acceder de forma fiable al directorio principal del usuario o conectarse al servidor de ventanas. Un programa de supervisión de calendario es un buen ejemplo de agente.

En el siguiente diagrama puede ver cómo se carga cada uno en función del inicio del dispositivo y del inicio de sesión del usuario:



Puede encontrar más información sobre demonios y agentes aquí en la documentación de Apple

Los demonios y agentes disponibles en su dispositivo macOS se encuentran en las siguientes ubicaciones:

Ubicación	Descripción
~/Biblioteca/IniciarAgentes	Agentes por usuario proporcionados por el usuario.
/Library/LaunchAgents	Agentes por usuario proporcionados por el administrador.
/Library/LaunchDaemons	Demonios de todo el sistema proporcionados por el administrador.

/System/Library/LaunchAgents	Agentes por usuario de OS X
/System/Library/LaunchDaemons	Demonios de OS X System wide

Puede verificar la lista de cada categoría desde el terminal macOS con estos comandos:

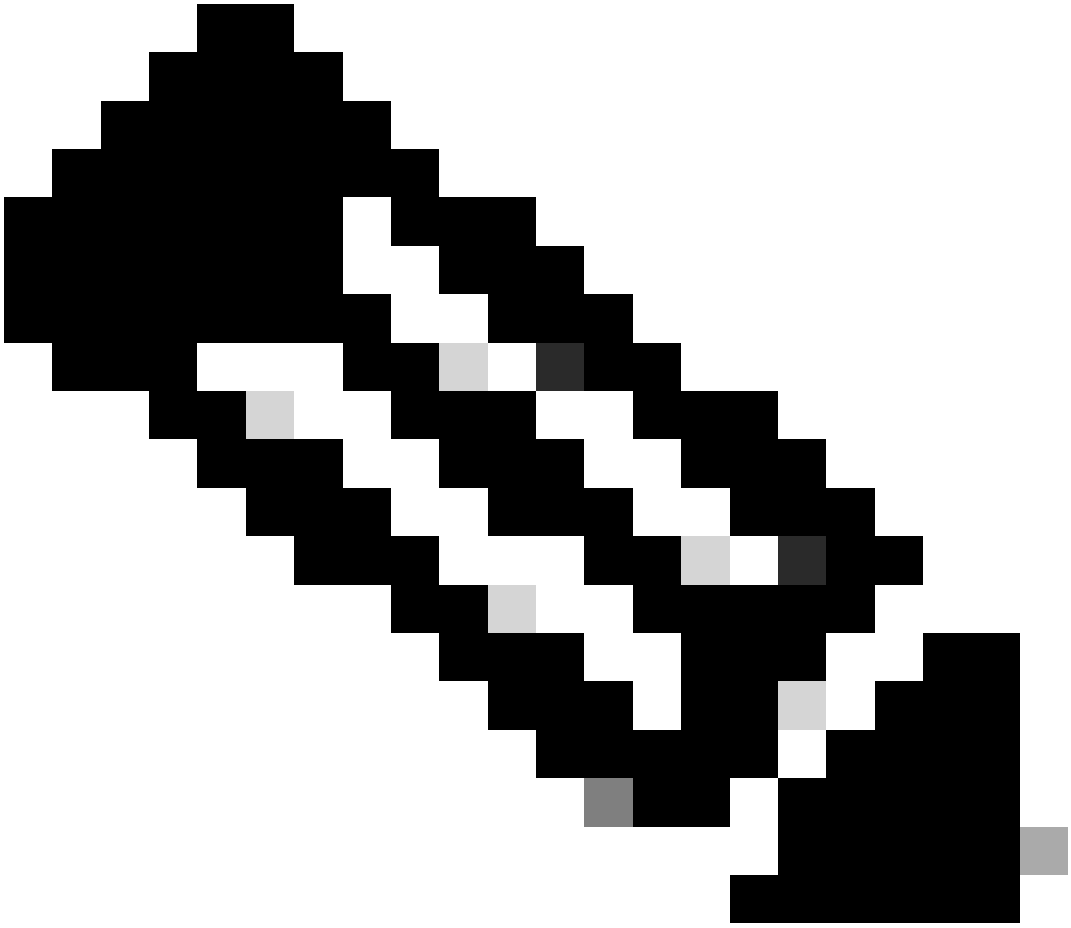
ls -ltr ~/Library/LaunchAgents
ls -ltr /Library/LaunchAgents
ls -ltr /Library/LaunchDaemons
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/LaunchDaemons

Las ubicaciones anteriores pueden mostrar todos los demonios y agentes que están disponibles en el dispositivo macOS; sin embargo, no todos están cargados o en ejecución.

Configurar

La configuración para la condición de servicio de macOS se puede realizar mediante estos pasos:

1. Identifique el nombre de servicio que desea comprobar.
2. (Opcional) Compruebe los detalles del servicio para definir si es un agente o un daemon.
3. Seleccione el operador de servicio que desea evaluar.
4. Configure la política de requisitos y estado para dicha condición.



Nota: La condición de estado del servicio requiere privilegios elevados para funcionar; por lo tanto, es IMPRESCINDIBLE que Cisco Secure Client (anteriormente AnyConnect) - Guía de referencia de ISE PSN

Identifique el nombre de servicio que desea comprobar

ISE Posture Compliance Module puede comprobar los servicios que se han cargado, ejecutado y cargado, y que se están ejecutando con código de salida.

Para verificar los servicios que se cargan, utilice el comando sudo launchctl dumpstate.

Para verificar los servicios que están cargados y que tienen un código de salida, utilice el comando sudo launchctl list.

Los comandos anteriores pueden mostrar abruptamente una gran cantidad de información; en su lugar, utilice estos comandos para mostrar simplemente el nombre real del servicio:

Para comprobar sólo los nombres de servicio cargados, utilice este comando:

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed |.*/||;s| = {$||'

Para verificar solamente los nombres de servicio que están cargados y tienen un código de salida, utilice este comando:

sudo launchctl list | awk '{if (NR>1) print $3}'

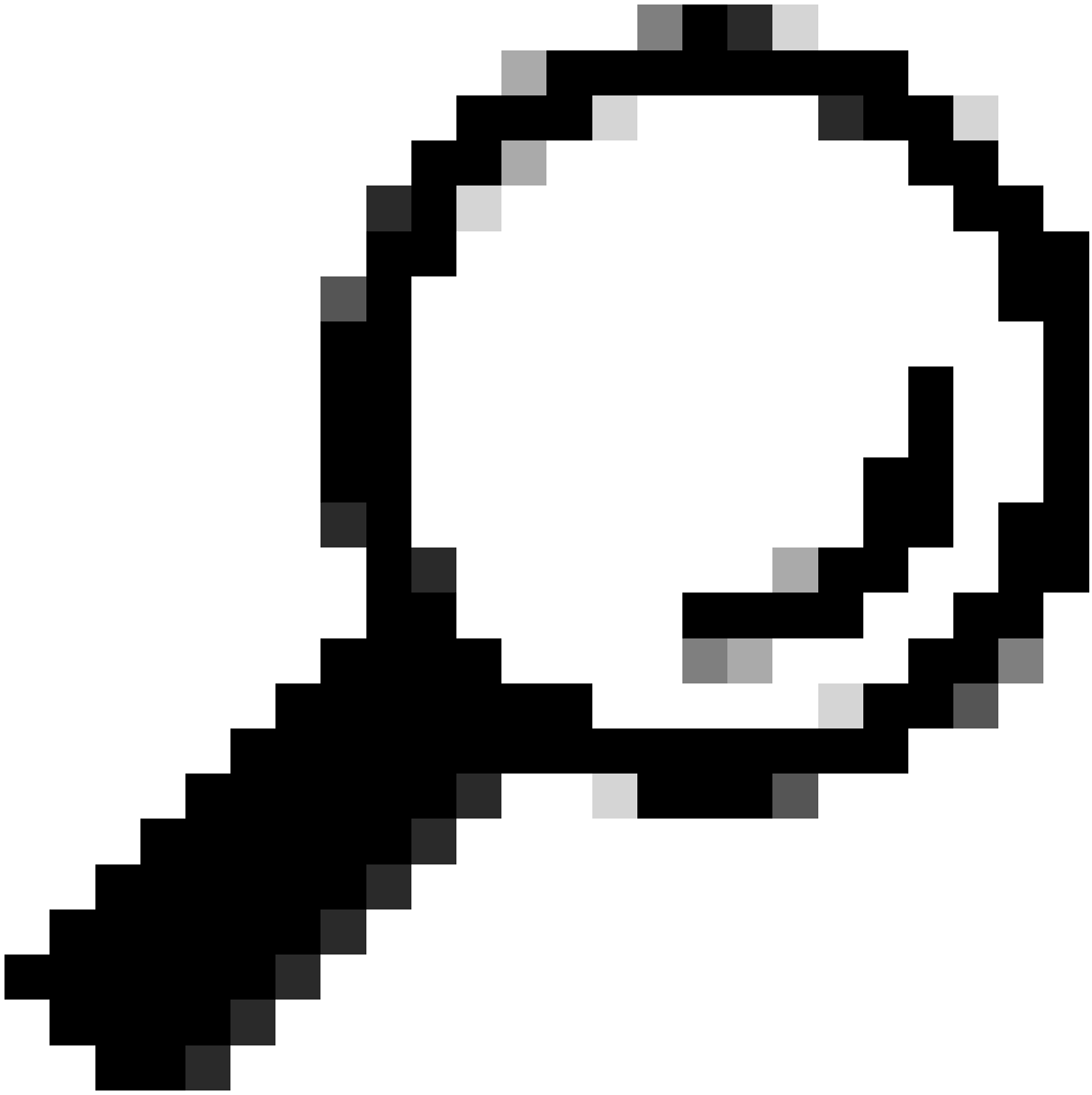
Estos comandos muestran mucha información, por lo que al final de cada comando se recomienda utilizar otro filtro grep para encontrar el servicio que está buscando.
Por ejemplo, si busca un servicio específico de un proveedor, puede utilizar una palabra clave como filtro en el y.

Para el caso de los servicios de Cisco, los comandos serían algo así:

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed |.*/||;s| = {$||' | grep -i cisco
sudo launchctl list | awk '{if (NR>1) print $3}' | grep -i cisco

(Opcional) Compruebe los detalles del servicio para definir si es un agente o un demonio

En la segunda parte de la configuración de esta condición, debe verificar si su servicio es de tipo daemon o de tipo agente.



Consejo: Este paso es opcional, ya que ISE le permite seleccionar la opción para Daemon o Agente de usuario, por lo que puede seleccionar esa opción y omitir esta parte.

En caso de que desee ser granular en esta condición, puede verificar el tipo haciendo lo siguiente:

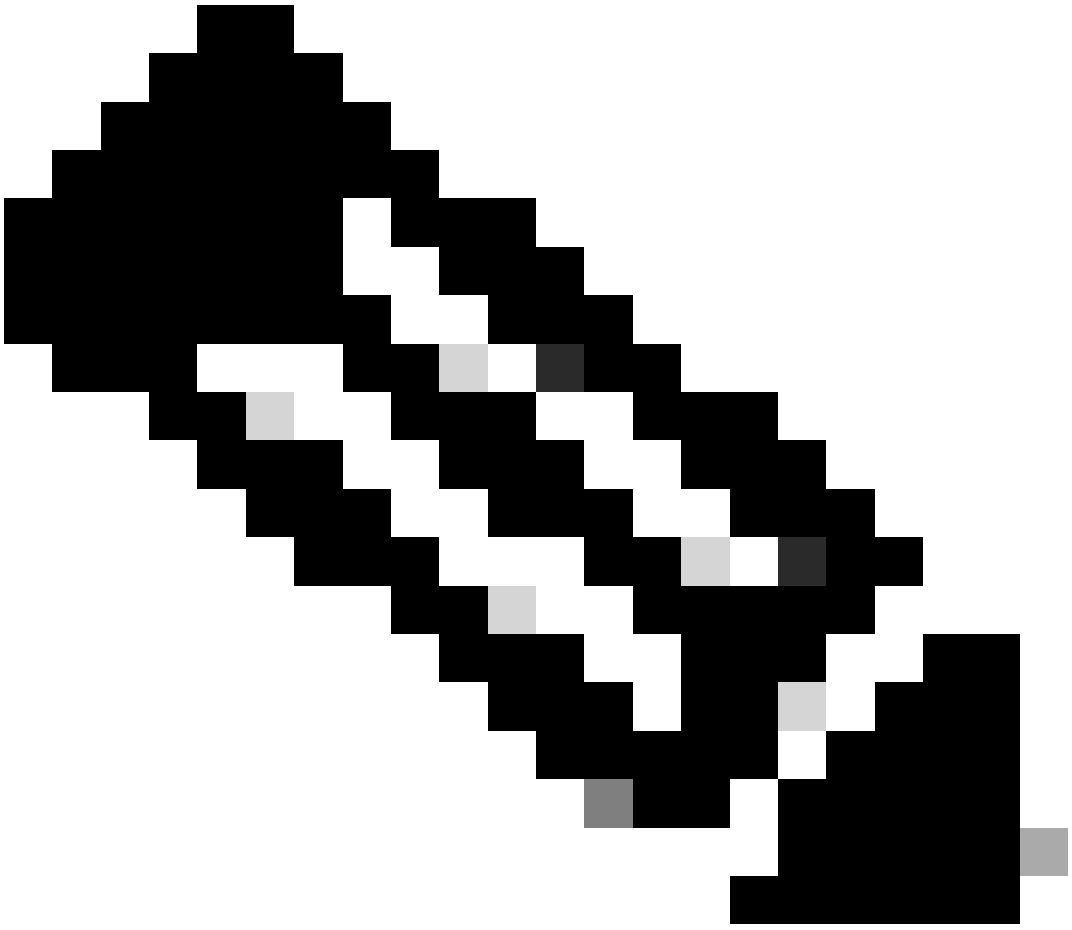
1. En primer lugar, verifique el nombre completo de launchctl del servicio con el comando sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed |.*/||;s| = {$||' | grep -i {Su nombre de servicio}

Por ejemplo, para el comando sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$//' | grep -i com.cisco.secureclient.iseposture, el resultado es: gui/501/com.cisco.secureclient.iseposture.

2. Verifique el tipo de servicio con el comando sudo launchctl print { Your launchctl service name } | grep -i 'type = Launch'

Siguiendo el ejemplo, para el comando: sudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch', el resultado es: type = LaunchAgent.

Esto significa que el tipo de servicio es Agente; de lo contrario, mostraría type = LaunchDaemon.



> Nota: En caso de que la información esté vacía, seleccione la opción Daemon Or User Agent en ISE para la configuración del tipo de servicio.

Seleccione el operador de servicios que se evaluará

ISE le permite seleccionar 5 operadores de servicios diferentes:

- Cargado
- No cargado
- Cargado y en ejecución
- Cargado con código de salida
- Cargado y en ejecución o con código de salida

Servicios cargados

Son todos los servicios que se enumeran al utilizar estos dos comandos:

```
sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed |.*/||;s| = {$||'
sudo launchctl list | awk '{if (NR>1) print $3}'
```

Servicios no cargados

¿Están definidos todos los servicios que tienen su lista de propiedades (plist), pero que no se han cargado, o servicios que ni siquiera tienen una lista de propiedades (plist) definida, por lo que no se pueden cargar en absoluto?

Estos servicios no son fáciles de identificar, y es más común para el caso de uso cuando desea verificar que un servicio específico no debe existir en el dispositivo macOS.
Por ejemplo, si desea evitar que el servicio de zoom se cargue en el dispositivo macOS, puede poner aquí us.zoom.ZoomDaemon como el valor para el servicio, de esta manera se asegura de que zoom no se está ejecutando o no está instalado en absoluto.

Hay servicios que no se pueden desinstalar y se define su lista de propiedades.
Por ejemplo, con este comando, puede ver que dhcp6d plist está definido:

```
ls -ltr /System/Library/LaunchDaemons | grep com.apple.dhcp6d.plist
```

Al comprobar la lista de servicios, puede ver que no está cargado:

```
sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed |.*/||;s| = {$||' | grep -i com.apple.dhcp6d
sudo launchctl list | awk '{if (NR>1) print $3}' | grep -i com.apple.dhcp6d
```

Si establece el valor en com.apple.dhcp6d", el dispositivo macOS es compatible, ya que aunque la lista de servicios está definida, el servicio no se carga.

Cargado y en ejecución

No todos los servicios están en ejecución, hay varios estados para cada servicio, como en ejecución, no en ejecución, en espera, cerrado, no inicializado, etc.

Para comprobar todos los servicios que se están ejecutando, utilice este comando:

sudo grep -B 10 -A 10 -E "^\s*state = running" << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed |.*/||;s| = {$||'

Los servicios enumerados con el comando anterior encontraron la condición de operador de servicio Cargado y en ejecución.

Cargado con código de salida

Algunos servicios pueden terminar con un código de salida esperado o inesperado, estos servicios pueden enumerarse con el comando:

sudo grep -B 10 -A 10 "state = e" << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$//'

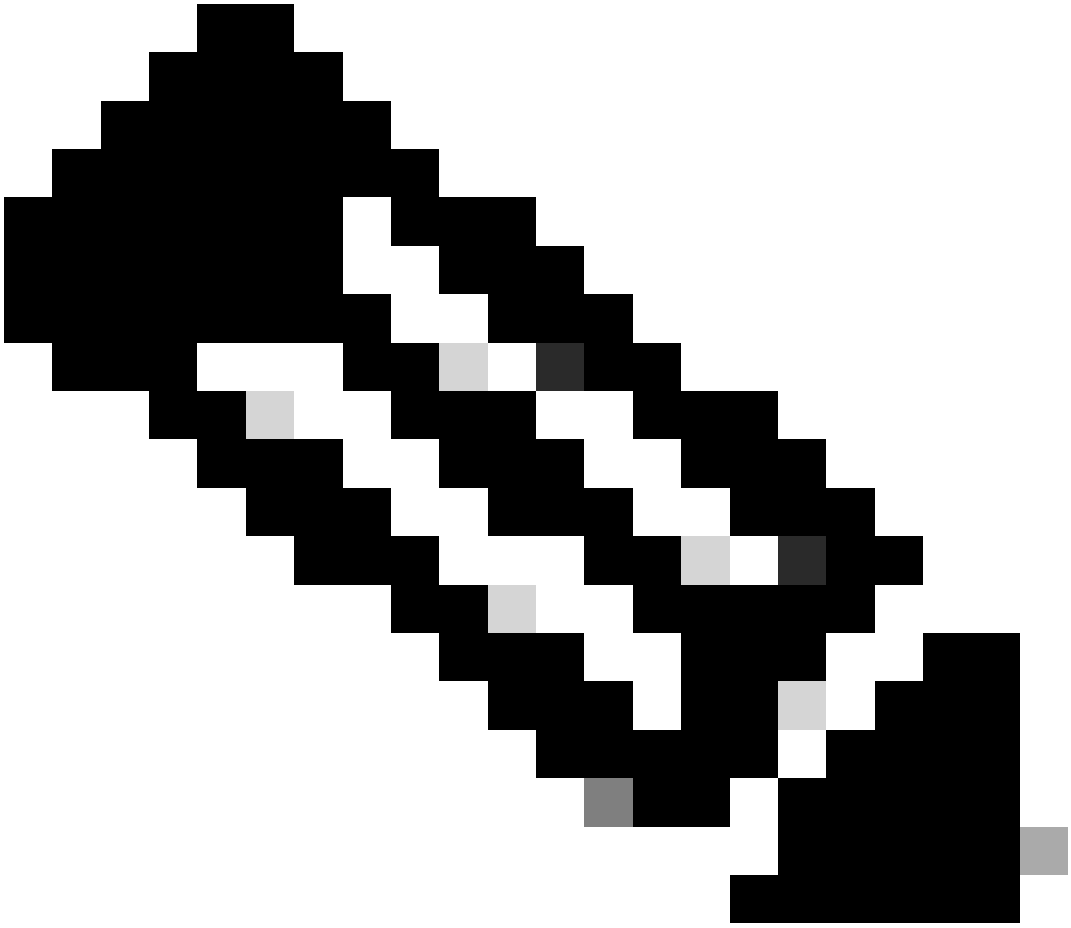
Para conocer su código de salida, puede elegir cualquier servicio y utilizar el comando:

sudo launchctl print { Your launchctl service name } | grep -i 'último código de salida'

Por ejemplo:

sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i 'último código de salida'

cuyo resultado es: último código de salida = 0

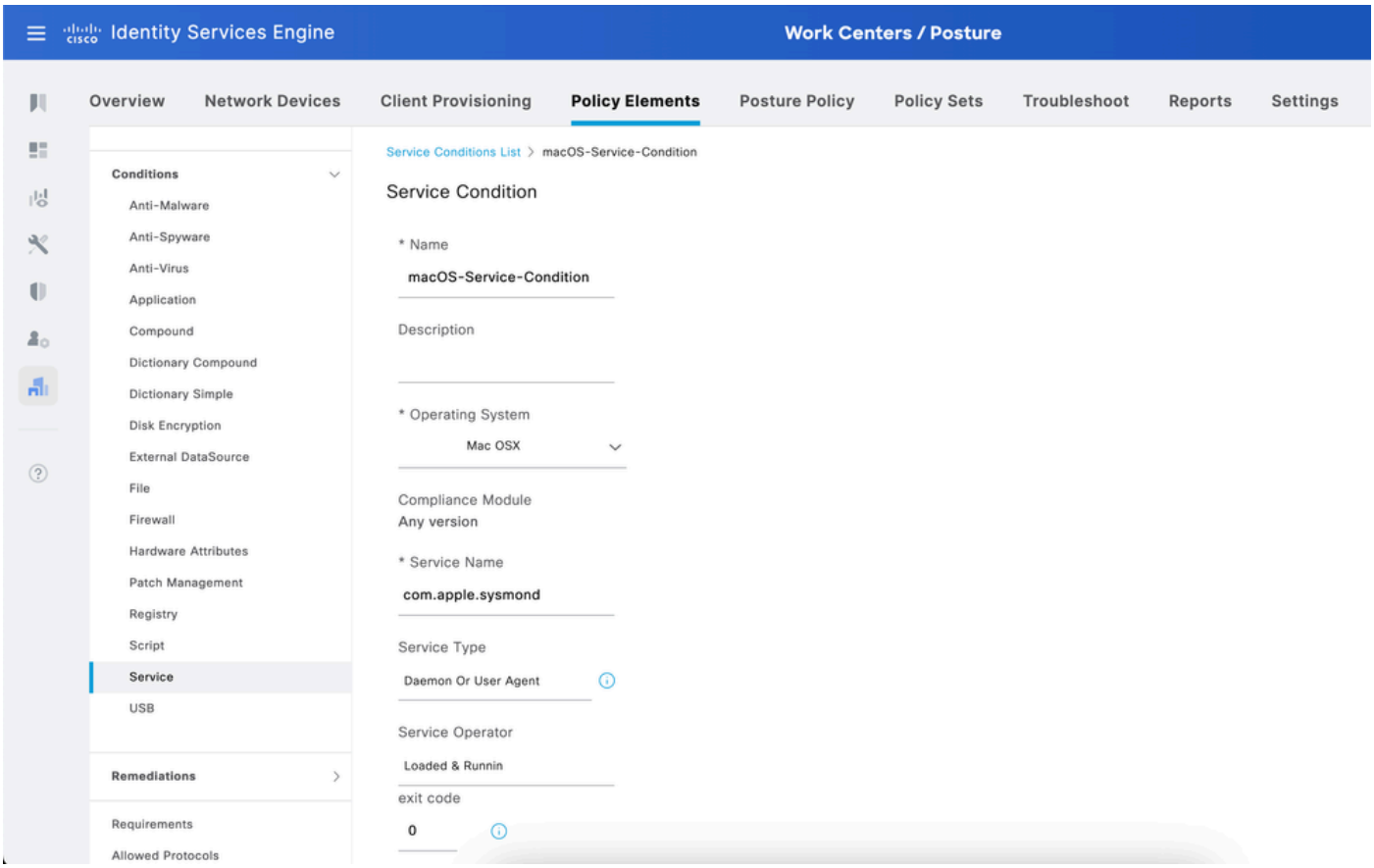


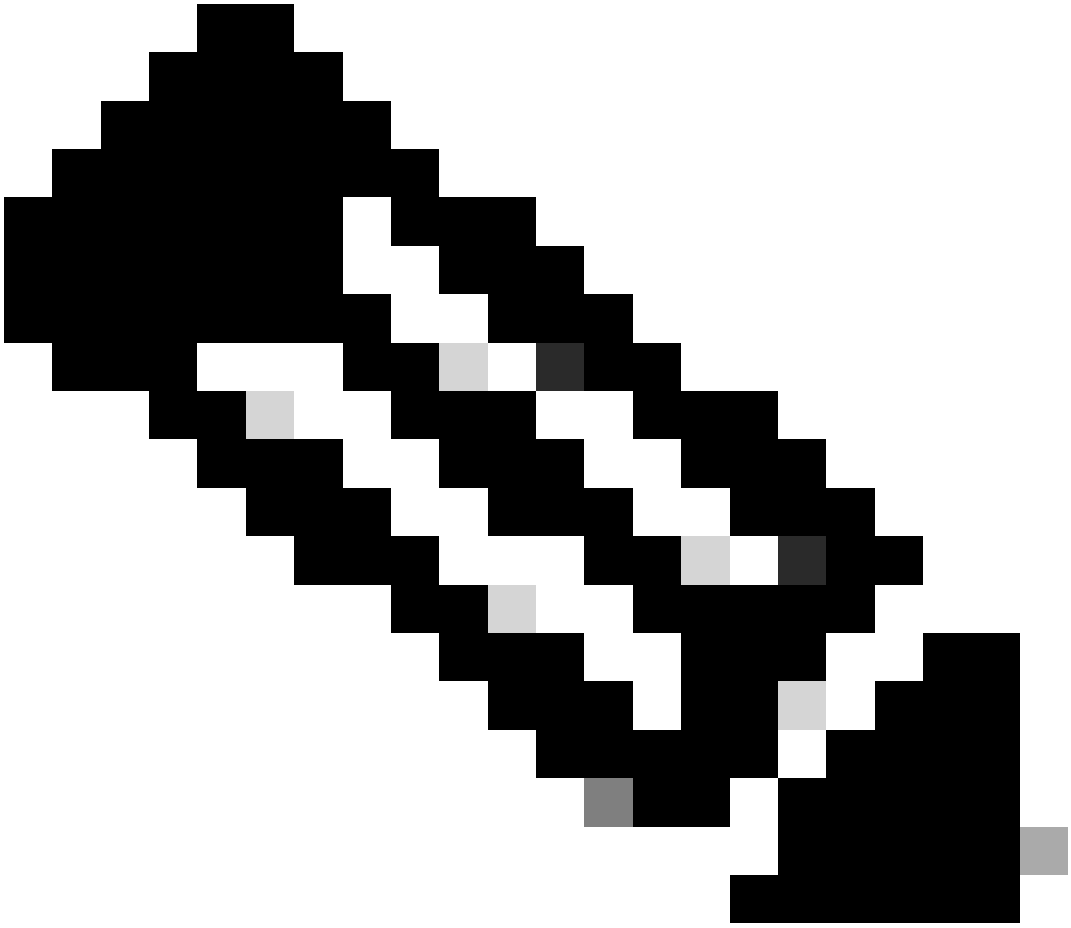
> Nota: Aquí el código de salida 0 generalmente significa que todo fue hecho correctamente por el servicio. Si un equipo no coincide con el 0 como código de salida, significa que el servicio no realizó la acción esperada.

Cargado y en ejecución o con código de salida

Esta última opción funciona cuando el servicio está Cargado y en ejecución o Cargado con código de salida.

Esta imagen muestra un ejemplo de una condición de servicio de macOS.


Identity Services Engine
Work Centers / Posture
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall
Hardware Attributes
Patch Management
Registry
Script
Service
USB
Remediations
Requirements
Allowed Protocols
Service Conditions List > macOS-Service-Condition
Service Condition
* Name
macOS-Service-Condition
Description
* Operating System
Mac OSX
Compliance Module
Any version
* Service Name
com.apple.sysmond
Service Type
Daemon Or User Agent
Service Operator
Loaded & Runnin
exit code
0

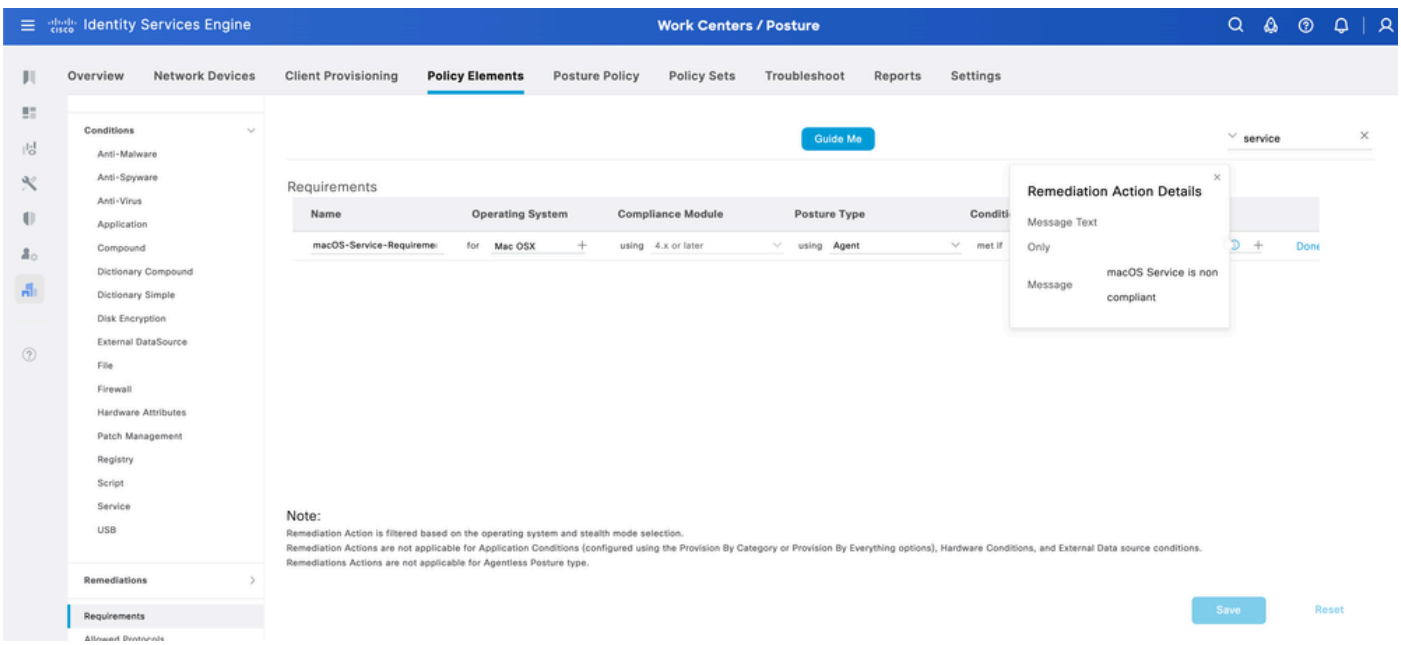


Nota: Actualmente, solo se admite el nombre de servicio exacto. Hay una solicitud de mejora para admitir caracteres comodín en los nombres de servicio, ID de bug de Cisco CSCwf01373

Configurar la directiva de requisitos y estado para dicha condición

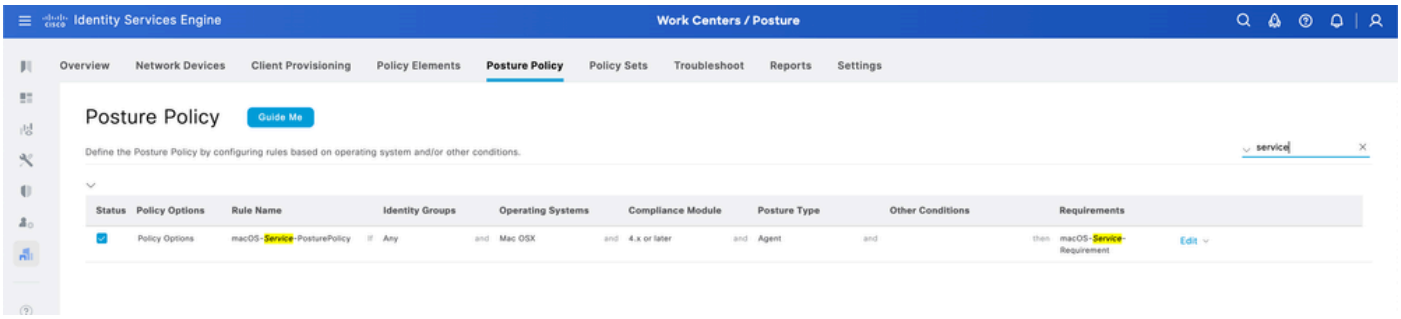
Una vez configurada la condición, debe crear un requisito para dicha condición, utilice la opción Message Test Only para este requisito.
Vaya a ISE > Centros de trabajo > Estado > Requisitos para crearlo.

Nota: No hay opciones de corrección para las condiciones de servicio.



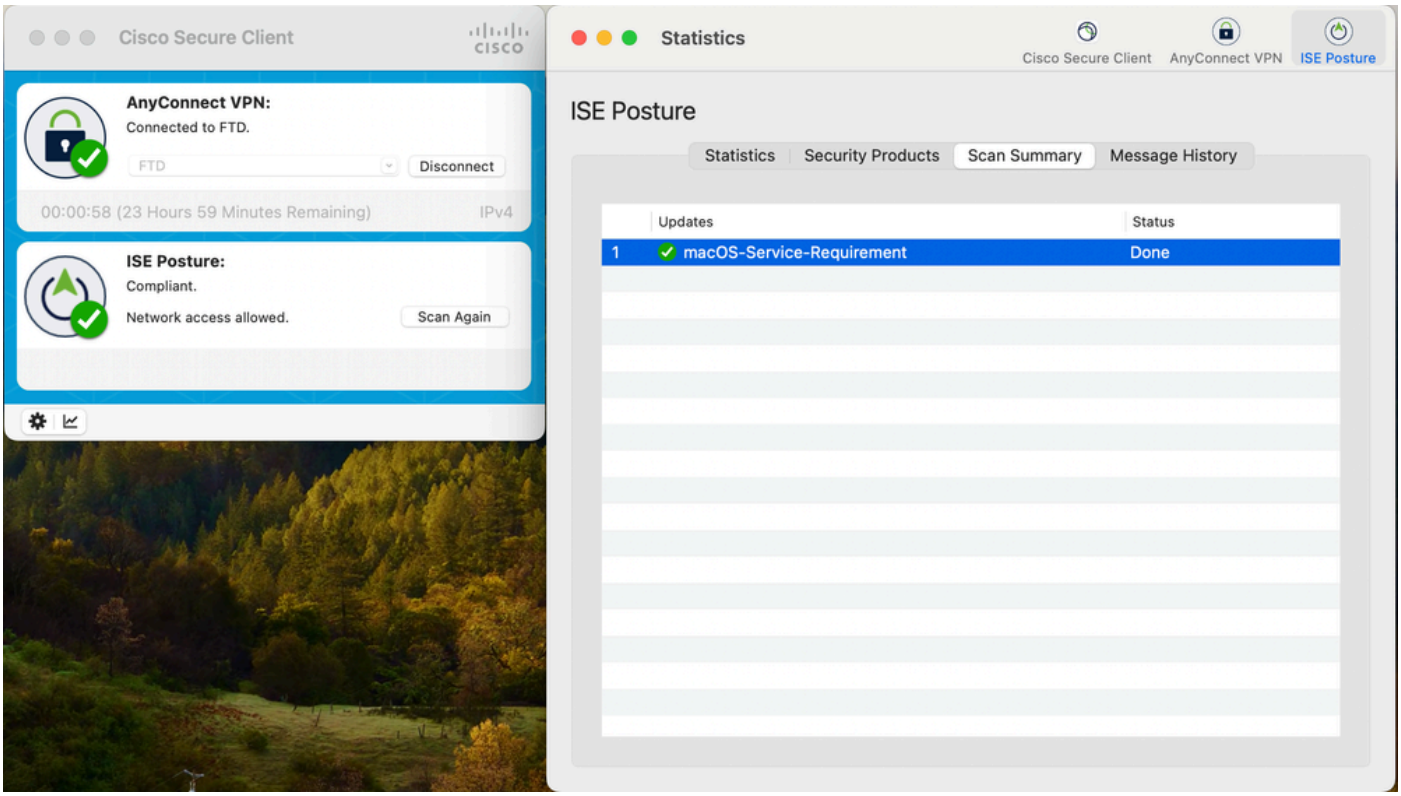
Una vez hecho esto, el último paso es configurar la política de postura que utiliza el requisito creado.
Vaya a ISE > Centros de trabajo > Condición > Política de condición para crear la política.

Habilite la nueva política, asígnele el nombre que desee y seleccione el requisito que acaba de crear.

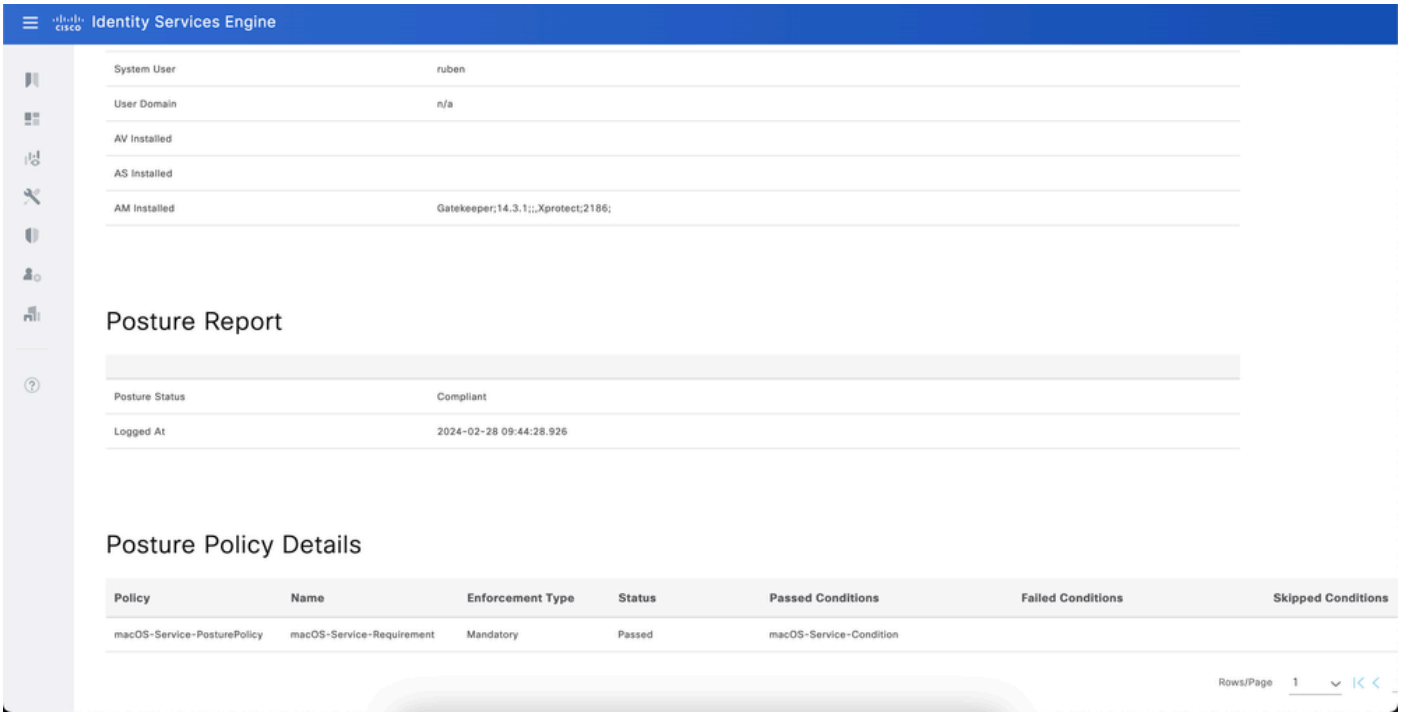


Verificación

Puede verificar que la condición de estado de macOS se ha superado o ha fallado desde la propia GUI de Cisco Secure Client.



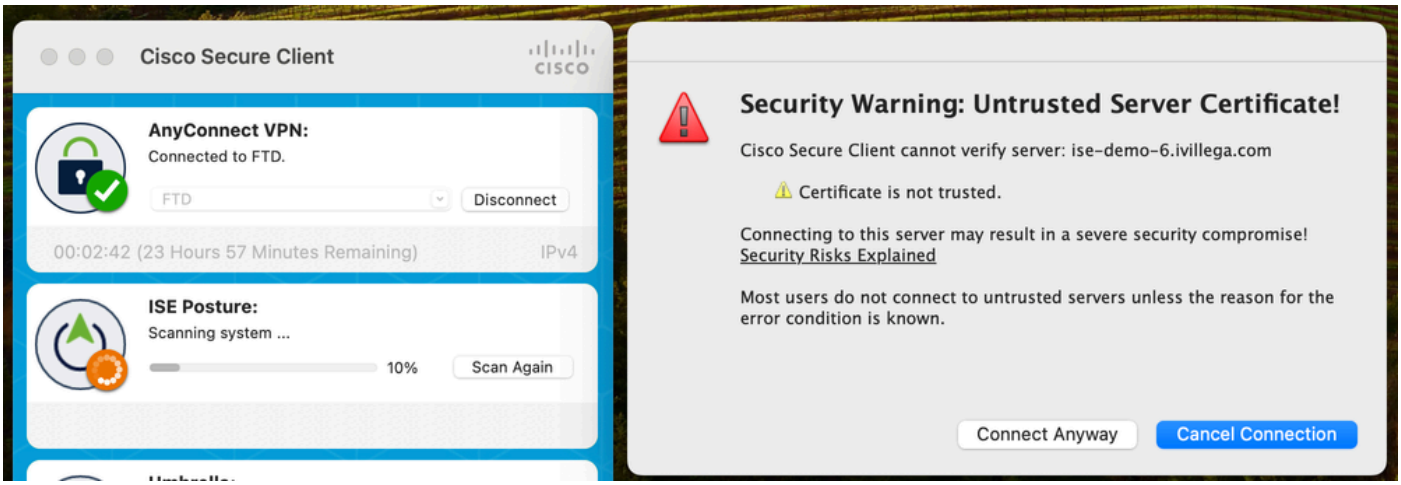
Asimismo, puede consultar el informe de estado de ISE en ISE > Operaciones > Informes > Terminales y usuarios > Evaluación de estado por terminal.



Troubleshoot

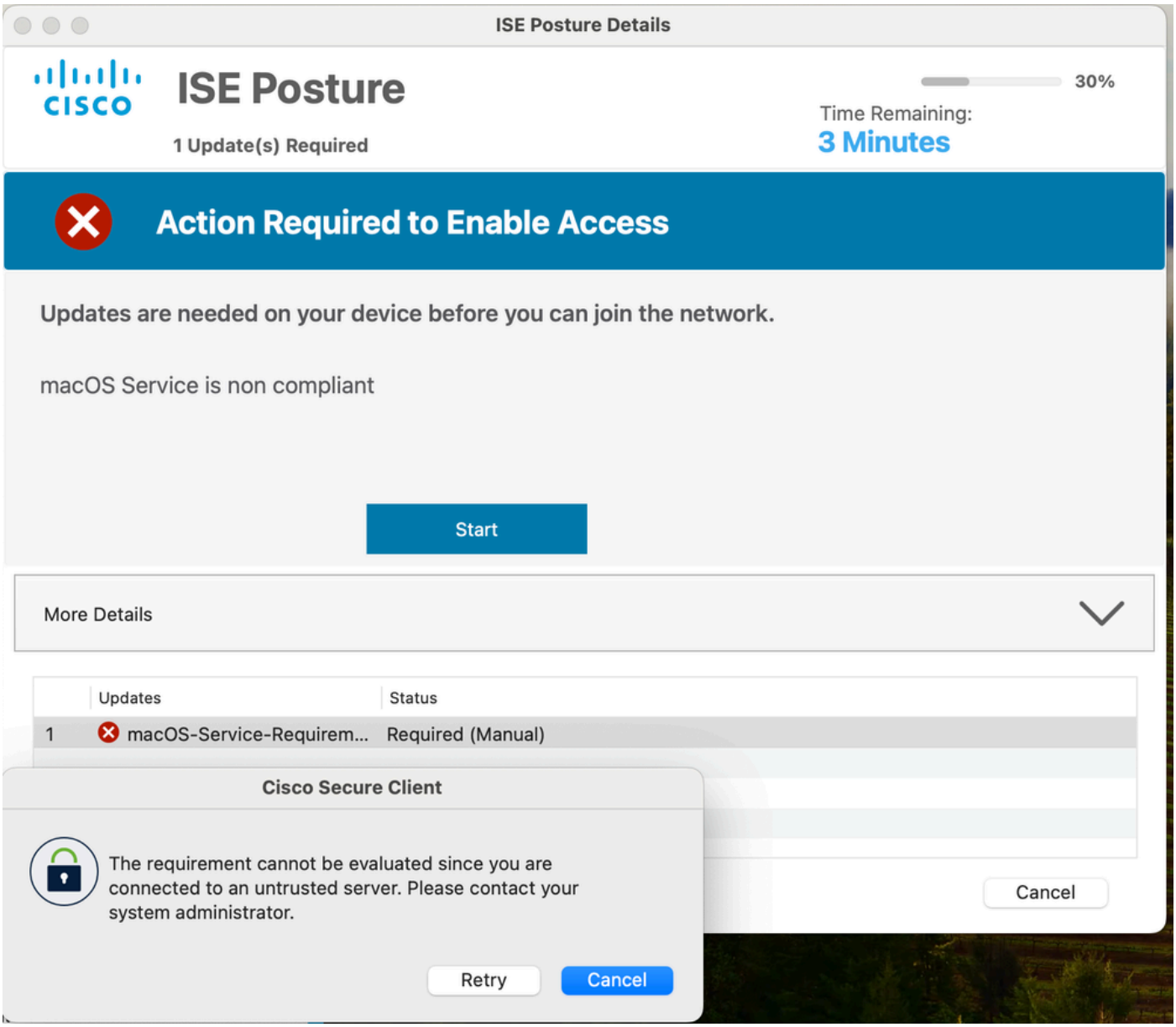
Problemas comunes que puede encontrar al configurar esta condición de estado del servicio macOS son:

Certificado no fiable



Como se ha indicado anteriormente, la condición de servicio requiere permisos elevados. Es imprescindible que el servidor confíe en el certificado para el proceso de análisis de estado.

De lo contrario, encontrará este error:

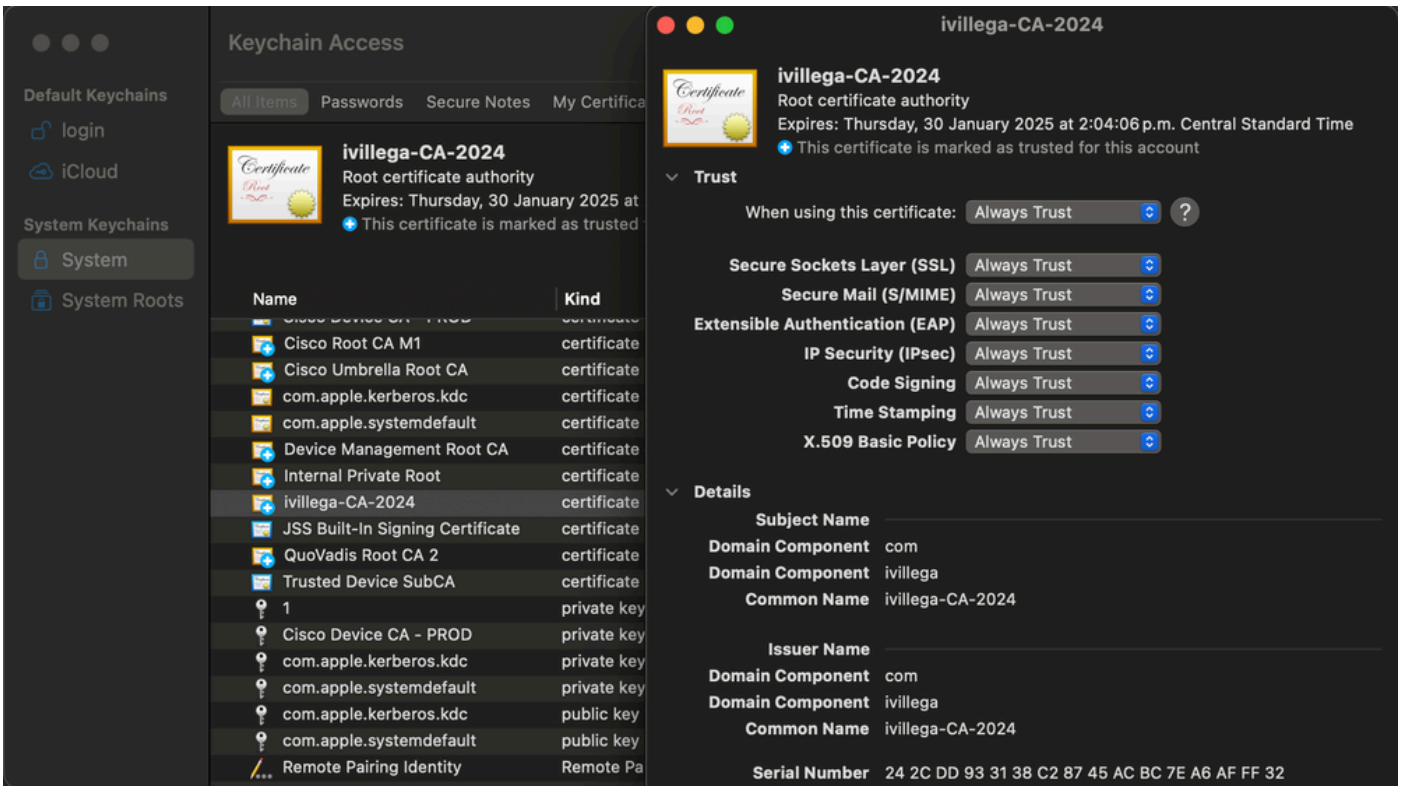


El módulo de estado de ISE detecta los servidores PSN por dirección IP o por nombre de dominio completamente calificado (FQDN). Se recomienda disponer de los archivos de configuración de estado para detectar los nodos de ISE mediante FQDN, por lo que los certificados Admin y Portal (Portal de aprovisionamiento de clientes) deben incluir el FQDN en el campo CN o SAN. También puede utilizar un certificado comodín para esto, los certificados comodín son compatibles con este flujo.

Debido a los valores del sistema, no se puede confiar en el campo CN en el futuro. Incluya la entrada de comodín o FQDN en el campo SAN como práctica recomendada.

En caso de que se detecten PSN de ISE a través de la dirección IP en lugar del FQDN, es obligatorio que la dirección IP de los nodos se incluya en el campo CN o en el campo SAN de los certificados vinculados al uso del administrador y el portal.

Los módulos de estado de ISE confían en el certificado presentado por el servidor ISE. Si su CA está en el almacén de certificados del sistema del acceso a la cadena de claves de macOS, esta CA debe tener la configuración Al utilizar este certificado establecida en Confianza siempre.



Puede encontrarse con el comportamiento incorrecto de que incluso cuando el certificado se carga correctamente y se cumplen todos los requisitos CN y SAN, el sistema macOS sigue sin confiar en el certificado. En estos casos, abra la aplicación de acceso a la cadena de claves, navegue hasta la pestaña Almacén de certificados del sistema y elimine el certificado CA desde allí.

Luego, navegue hasta la aplicación macOS Terminal y ejecute este comando: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain

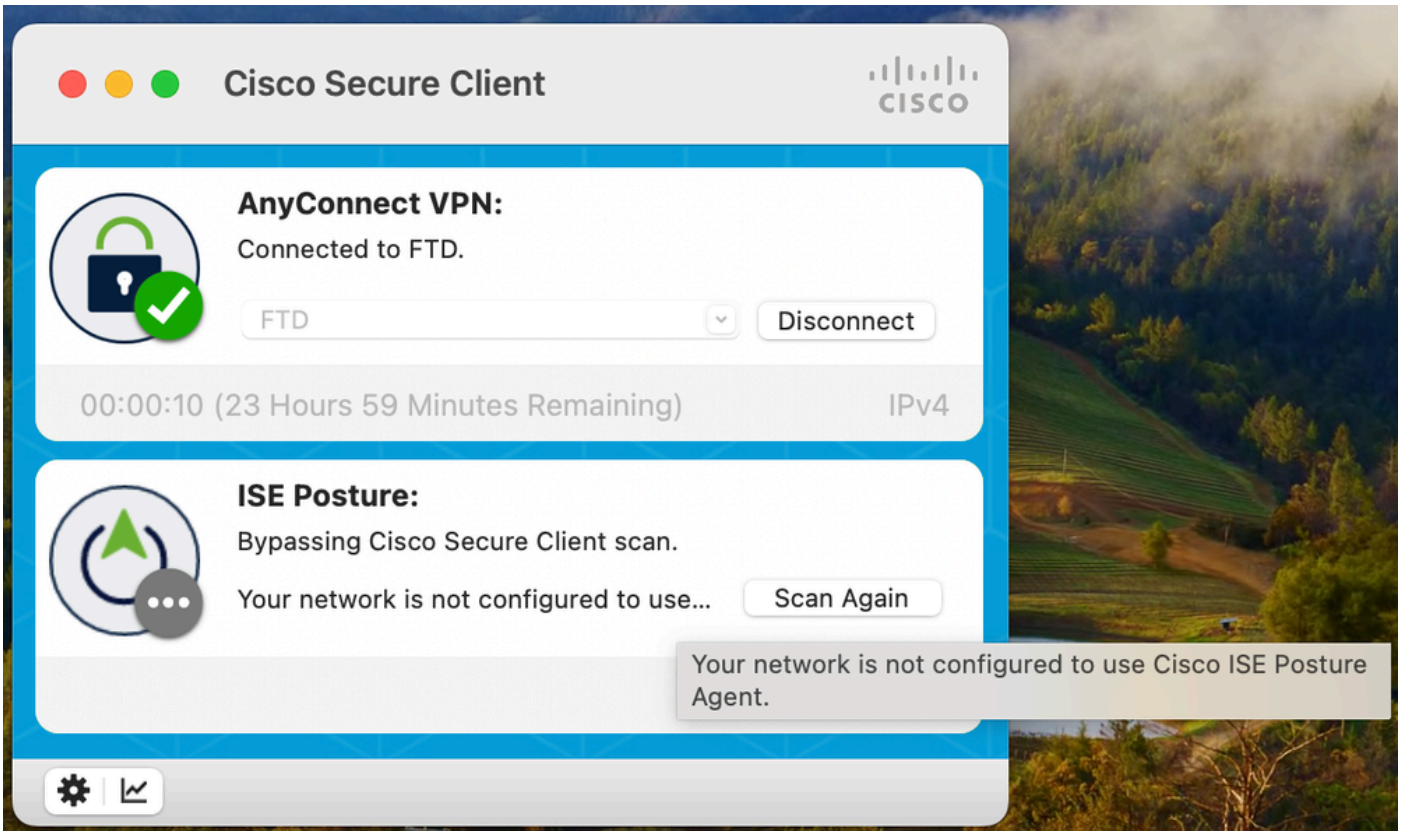
{Ruta de acceso al certificado de la CA}

Por ejemplo, si el certificado está en el escritorio, el comando es el siguiente: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

Después de ejecutar el comando, reinicie el equipo y vuelva a intentarlo.

Omitiendo análisis de Cisco Secure Client

También puede aparecer el mensaje de error "Omitiendo Cisco Secure Client Scan" y "Su red no está configurada para utilizar Cisco ISE Posture Agent":



Este mensaje aparece porque no hay perfiles configurados en el Aprovisionamiento del cliente en ISE > Centros de trabajo > Estado > Aprovisionamiento del cliente > Políticas de aprovisionamiento del cliente.
Aunque puede que vea una condición para los sistemas operativos Mac OSX, eso no significa que esté cubriendo todas las versiones de macOS.

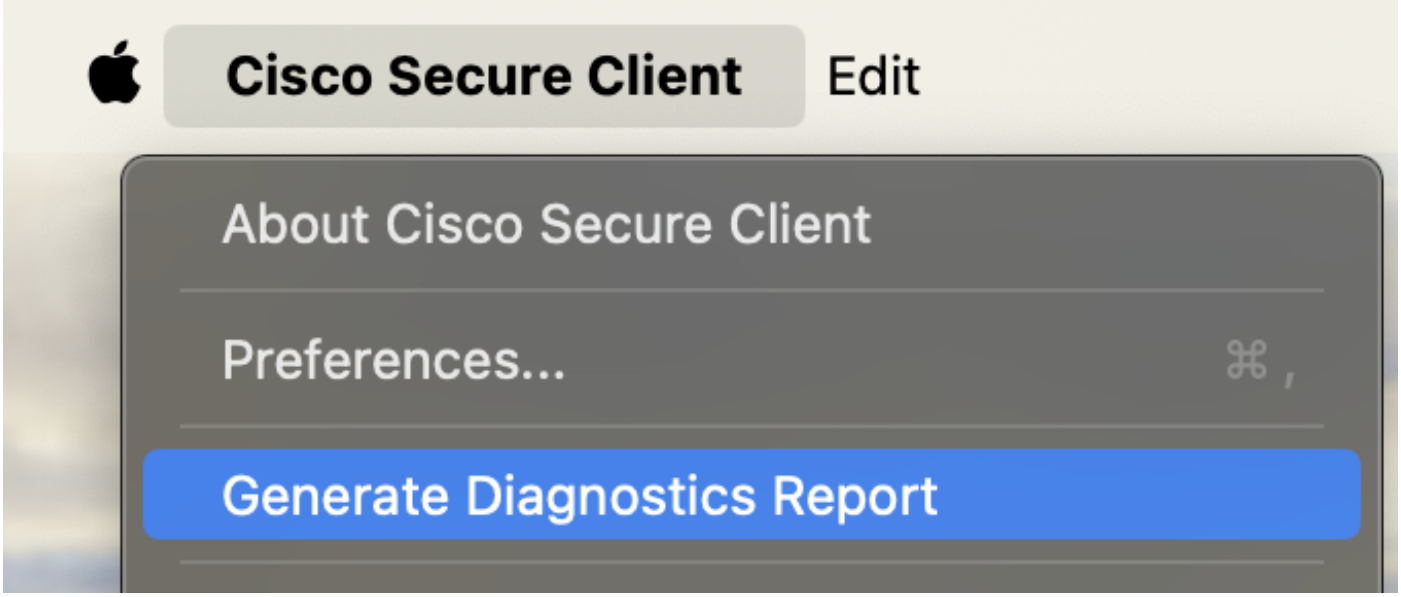
De forma predeterminada, ISE no incluye las últimas versiones de macOS, como Sequoia (15.6.x), para evitar este mensaje, asegúrese de que se actualiza esa postura.

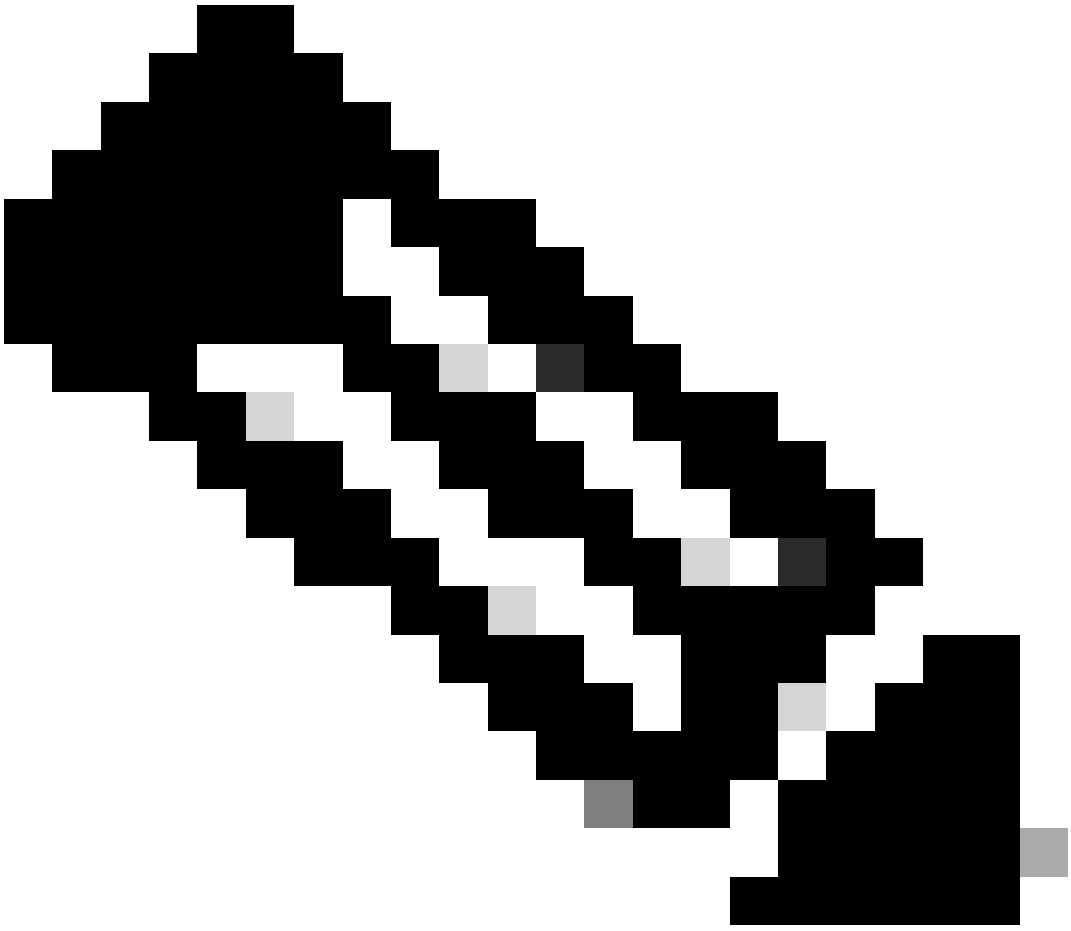
Debe actualizar la fuente de estado desde ISE > Centros de trabajo > Estado > Configuración > Actualizaciones de software > Actualizaciones de estado.

Esto se puede actualizar en línea directamente desde ISE, o en línea a través de un archivo zip que se puede descargar aquí desde el sitio Posture Offline

Otros problemas

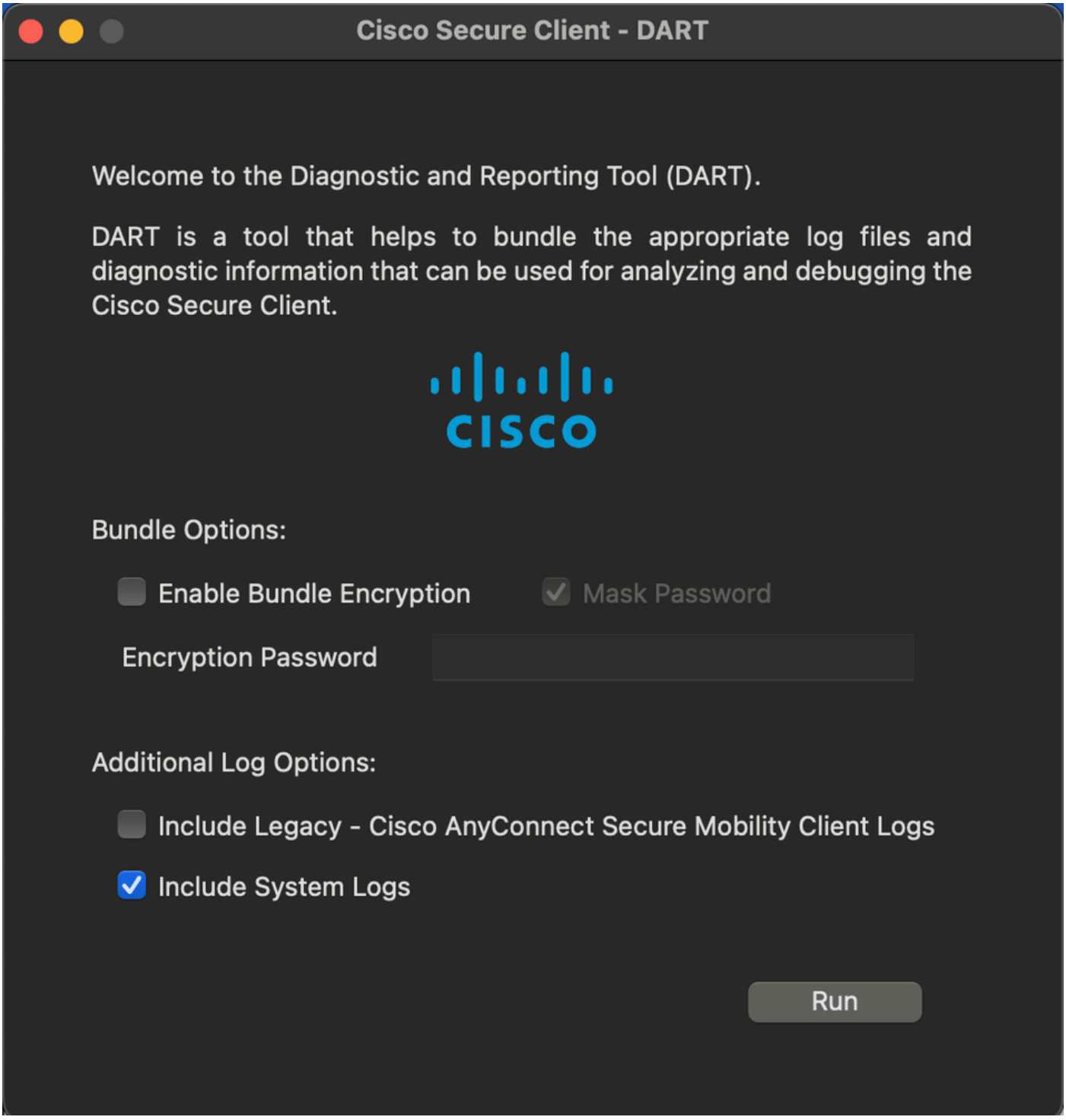
Si desea profundizar en los detalles, puede recopilar un paquete DART del dispositivo MacOS que se ha colocado. Para ello, debe tener instalado el módulo DART y, a continuación, con la aplicación Cisco Secure Client activa, navegue hasta la barra de menú y haga clic en Cisco Secure Client y, a continuación, en Generar informes de diagnóstico.



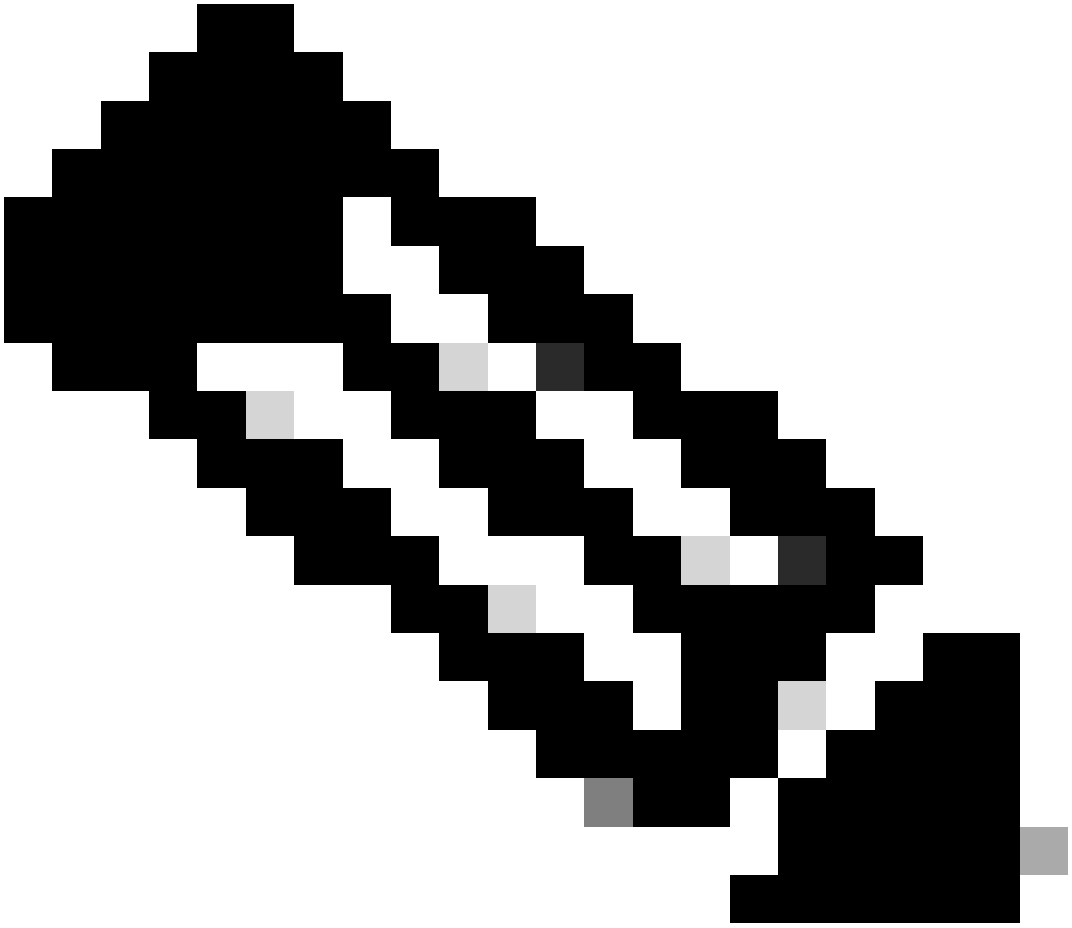


Nota: Es importante tener la opción Include System Logs habilitada al generar el paquete

DART; de lo contrario, el paquete DART no incluirá la información del módulo de estado de ISE.



Por motivos de seguridad, es posible que algunos de los registros estén cifrados y no sean visibles, pero en el archivo unified_log.log del paquete DART es posible que vea registros similares, como se muestra a continuación:



Nota: Este ejemplo de registro es para la condición de servicio de macOS configurada en este documento.

```
[Tue Feb 27 10:30:58.576 2024][csc_iseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 File
```

```
macOS-Service-Condition
```

```
3
```

303

com.apple.sysmond

running

0

)
[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: processPostureData Thread Id: 0x4A9FD7C0 File: Au

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: SMP_initCheck Thread Id: 0x4A9FD7C0 File: SMNavPo

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

",isElevationAllowed:1,nRemediationTimeLeft:0}
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 Fi

macOS-Service-Condition

3

```
303

com.apple.sysmond

running

0

)
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: Rqmt.cpp
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: CheckSvc.
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: completeCheck Thread Id: 0x4A9FD7C0 File: Rqm
```

Además, puede establecer el componente posture en el nivel de registro de depuración en el nodo ISE PSN que autentica y coloca el terminal.

Puede configurar este nivel de registro desde ISE > Operations > Troubleshoot > Debug Wizard > Debug Log Configuration. Haga clic en el PSN Hostname y cambie el nivel de registro del componente Posture de INFO a DEBUG.

Utilizando el mismo ejemplo para la condición de servicio de macOS, puede ver registros similares dentro de ise-psc.log:

```
2024-02-27 10:30:58.658 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.runtime.Pos

ISE: 3.3.0.430

ISE: 2.x
```

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

2024-02-27 10:30:58.659 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.util.Status

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

]

```
2024-02-27 10:31:06.044 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-8][[]] cisco.cpm.posture.util.AgentU
```

Si los problemas persisten, eleve un ticket TAC con el equipo 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).