Configurar sin agentes de estado

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Getting Started
  - Requisitos previos:
  - Condiciones de postura admitidas
  - Condiciones de postura no admitidas
- Configuración de ISE
  - Actualizar fuente de estado
  - Flujo de configuración sin agente de estado
  - Configuración de estado sin agente
    - Condición de postura
    - Requisito de posición
    - Política de estado
    - Aprovisionamiento de clientes
    - Perfil de autorización sin agente
    - Alternativa a la remediación (opcional)
    - Perfil de autorización de remediación (opcional)
    - Regla de autorización sin agente
    - Configurar credenciales de inicio de sesión de terminal
- Configuración y solución de problemas del extremo de Windows
  - Verificación y solución de problemas previos
    - Probando la conexión TCP al puerto 5985
    - Creación de reglas de entrada para permitir PowerShell en el puerto 5985
    - Las credenciales del cliente para el inicio de sesión del shell deben tener privilegios de administrador local
    - Validando agente de escucha WinRM
    - Habilitar RemotingWinRM de PowerShell
    - Powershell debe ser v7.1 o posterior. El cliente debe tener cURL v7.34 o posterior:
    - Resultado para comprobar las versiones de PowerShell y cURL en dispositivos Windows
    - Configuración adicional
    - MacOS
    - Powershell debe ser v7.1 o posterior. El cliente debe tener cURL v7.34 o posterior:
    - Para clientes MacOS, el puerto 22 para acceder a SSH debe estar abierto para acceder al cliente
    - Para MacOS, asegúrese de actualizar esta entrada en el archivo sudoers para evitar que se produzca un error en la instalación del certificado en los terminales:

Introducción

Este documento describe cómo configurar Posture Agentless en ISE y qué se requiere en el terminal para ejecutar el script sin agente.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE).
- Condición.
- PowerShell y SSH
- Windows 10 o posterior.

Componentes Utilizados

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

- Identity Services Engine (ISE) versión 3.3.
- Paquete CiscoAgentlessWindows 5.1.6.6
- Windows 10

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 estado de ISE realiza una evaluación del cliente. El cliente recibe la política de requisitos de estado de ISE, realiza la recopilación de datos de estado, compara los resultados con la política y envía los resultados de la evaluación de vuelta a ISE.

A continuación, ISE determina si el dispositivo es conforme o no en función del informe de estado.

La postura sin agente es uno de los métodos de postura que recopila información de postura de los clientes y se elimina automáticamente al finalizar sin que el usuario final deba realizar ninguna acción. La condición sin agente se conecta con el cliente mediante privilegios administrativos.

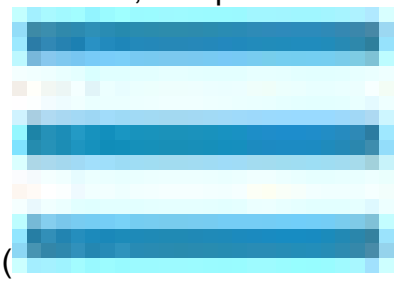
Getting Started

Requisitos previos:

- El cliente debe ser accesible a través de su dirección IPv4o IPv6, y esa dirección IP debe estar disponible en la contabilidad RADIUS.

- El cliente debe ser accesible desde Cisco Identity Services Engine (ISE) a través de su dirección IPv4 o IPv6. Además, esta dirección IP debe estar disponible en la contabilidad RADIUS.
- Los clientes Windows y Mac son compatibles actualmente:
    - Para los clientes Windows, el puerto 5985 para acceder a powershell en el cliente debe estar abierto. Powershell debe ser v7.1o posterior. El cliente debe tener cURL v7.34 o posterior.
    - Para clientes MacOS, el puerto 22 para acceder a SSH debe estar abierto para acceder al cliente. El cliente debe tener cURL v7.34 o posterior.
- Las credenciales del cliente para el inicio de sesión del shell deben tener privilegios de administrador local.
- Ejecute la actualización de la fuente de estado para obtener los clientes más recientes, como se describe en los pasos de configuración. Compruebe lo siguiente:
- Para MacOS, asegúrese de que esta entrada se actualice en el archivo sudoers para evitar que se produzca un error en la instalación del certificado en los terminales: Compruebe lo siguiente:

```
ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
```

- Para MacOS, la cuenta de usuario configurada debe ser una cuenta de administrador. El estado sin agente para MacOS no funciona con ningún otro tipo de cuenta, aunque conceda más privilegios.Para ver esta ventana, haga clic en elMenúIcono () y elija Administration > System > Settings > Endpoint Scripts > Login Configuration > MAC Local User.
- En caso de que se produzcan cambios en las actividades relacionadas con los puertos en los clientes de Windows debido a las actualizaciones de Microsoft, debe volver a configurar el flujo de trabajo de configuración de estado sin agente para los clientes de Windows.

Condiciones de postura admitidas

- Condiciones de archivo, excepto las condiciones que utilizan las rutas de acceso USER_DESKTOP y USER_PROFILE

- Condiciones de servicio, excepto Demonio del sistema y Demonio o Comprobaciones de agente de usuario en macOS
- Condiciones de aplicación
- Condiciones del origen de datos externo
- Condiciones compuestas
- Condiciones anti-malware
- Condición de administración de parches, excepto las comprobaciones de estadoHabilitado yHasta Fecha
- Condiciones del firewall
- Condiciones de cifrado de disco, excepto la comprobación de condición basada en la ubicación de cifrado
- Condiciones del Registro, excepto las condiciones que utilizan HCSK como clave raíz

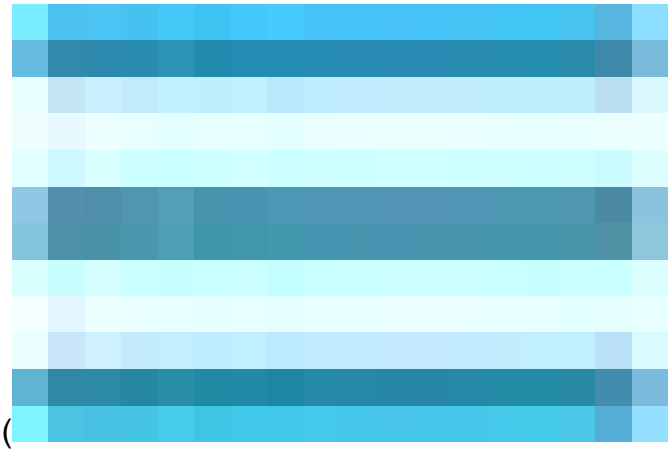
Condiciones de postura no admitidas

- Corrección
- Período de gracia
- Reevaluación periódica
- Política de uso aceptable

Configuración de ISE

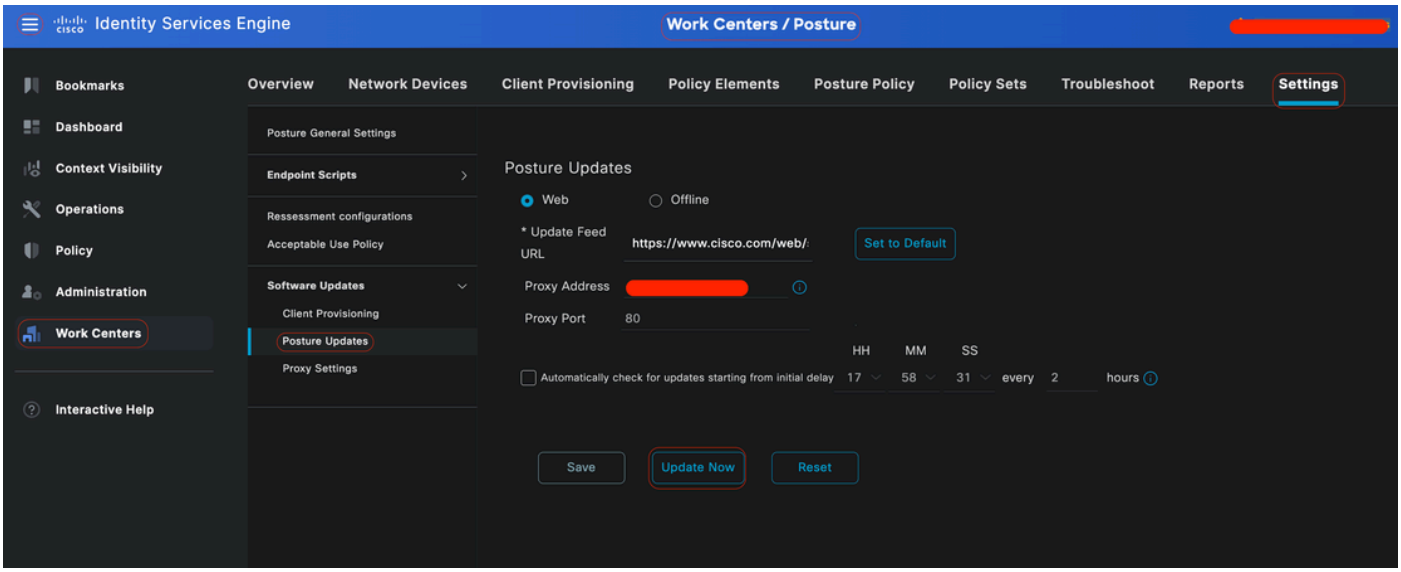
Actualizar fuente de estado

Se recomienda actualizar la fuente de estado antes de comenzar a configurar la fuente de estado.



En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y seleccione Centros de trabajo > Estado > Configuración > Actualizaciones de software >

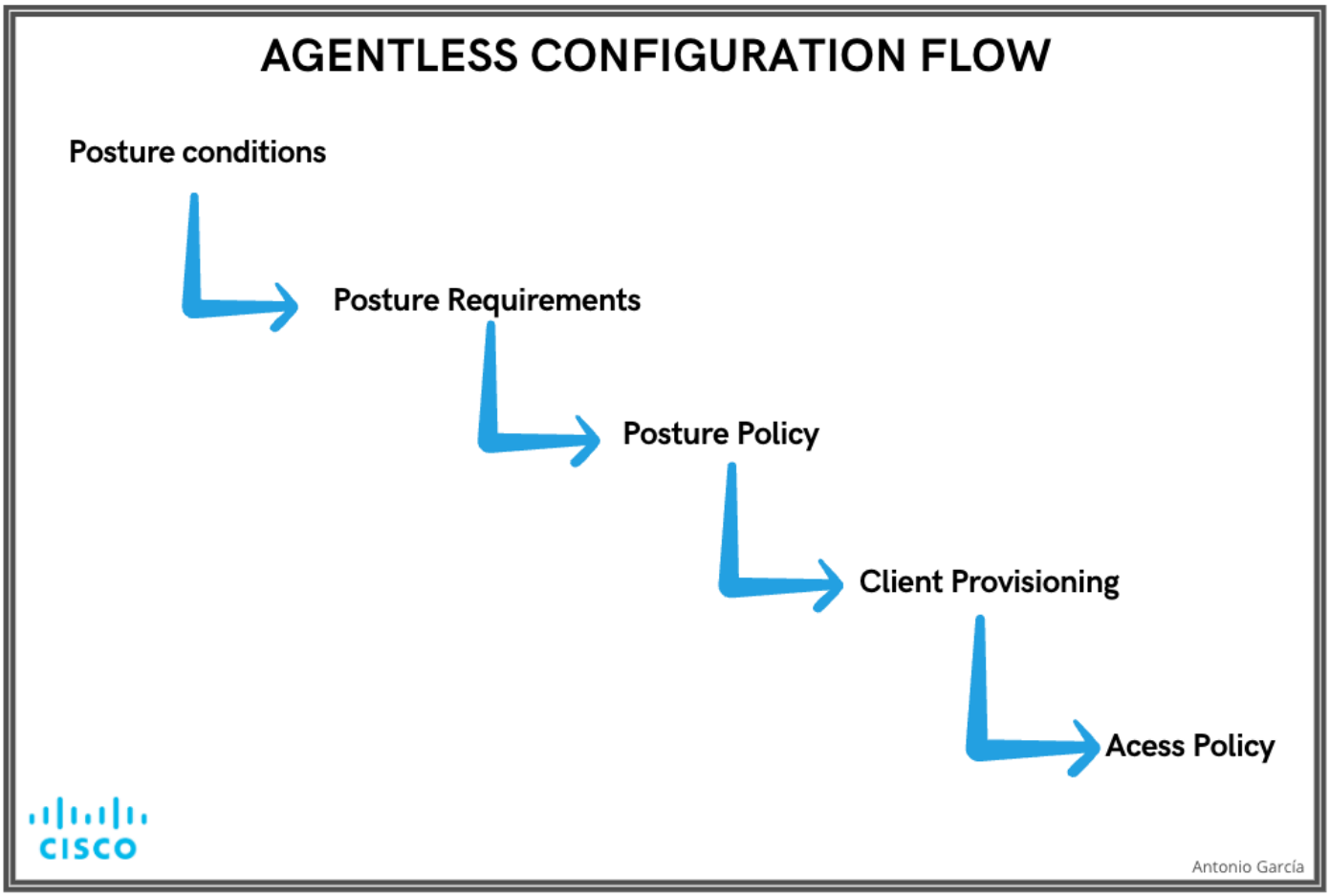
Actualizar ahora.



Actualizando fuente de estado

Flujo de configuración sin agente de estado

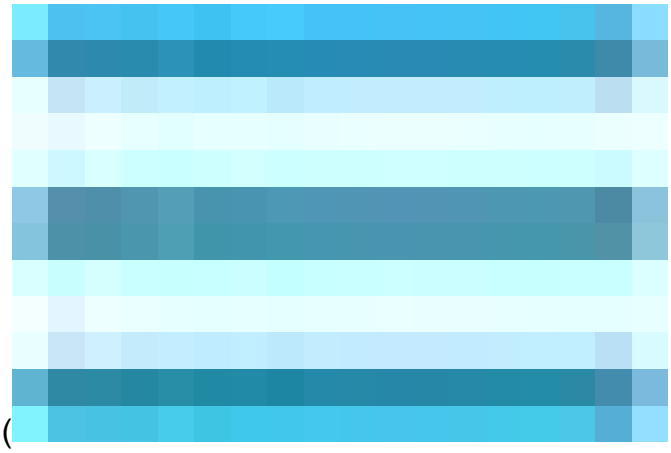
La configuración de Posture Agentless se debe realizar en orden, ya que la primera configuración será necesaria para la siguiente, y así sucesivamente. Observó que la remediación no está en el flujo; sin embargo, más adelante este documento tratará una alternativa para configurar la remediación.



Configuración de estado sin agente

Condición de postura

Las condiciones de estado son el conjunto de reglas de nuestra política de seguridad que definen un terminal compatible. Algunos de estos elementos incluyen la instalación de un firewall, software antivirus, anti-malware, revisiones, cifrado de disco y más.



En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y seleccione Centros de trabajo > Postura > Elementos de política > Condiciones, haga clic en Agregar y cree una o más Condiciones de postura que utilicen la postura sin agente para identificar el requisito. Una vez creada la Condición, haga clic en Guardar.

En este escenario, una condición de aplicación denominada "Agentless_Condition_Application" se configuró con estos parámetros:

•Sistema operativo: Todo de Windows

Esta condición se aplica a cualquier versión del sistema operativo Windows, lo que garantiza una amplia compatibilidad entre los diferentes entornos de Windows.

· Verificar por: Proceso

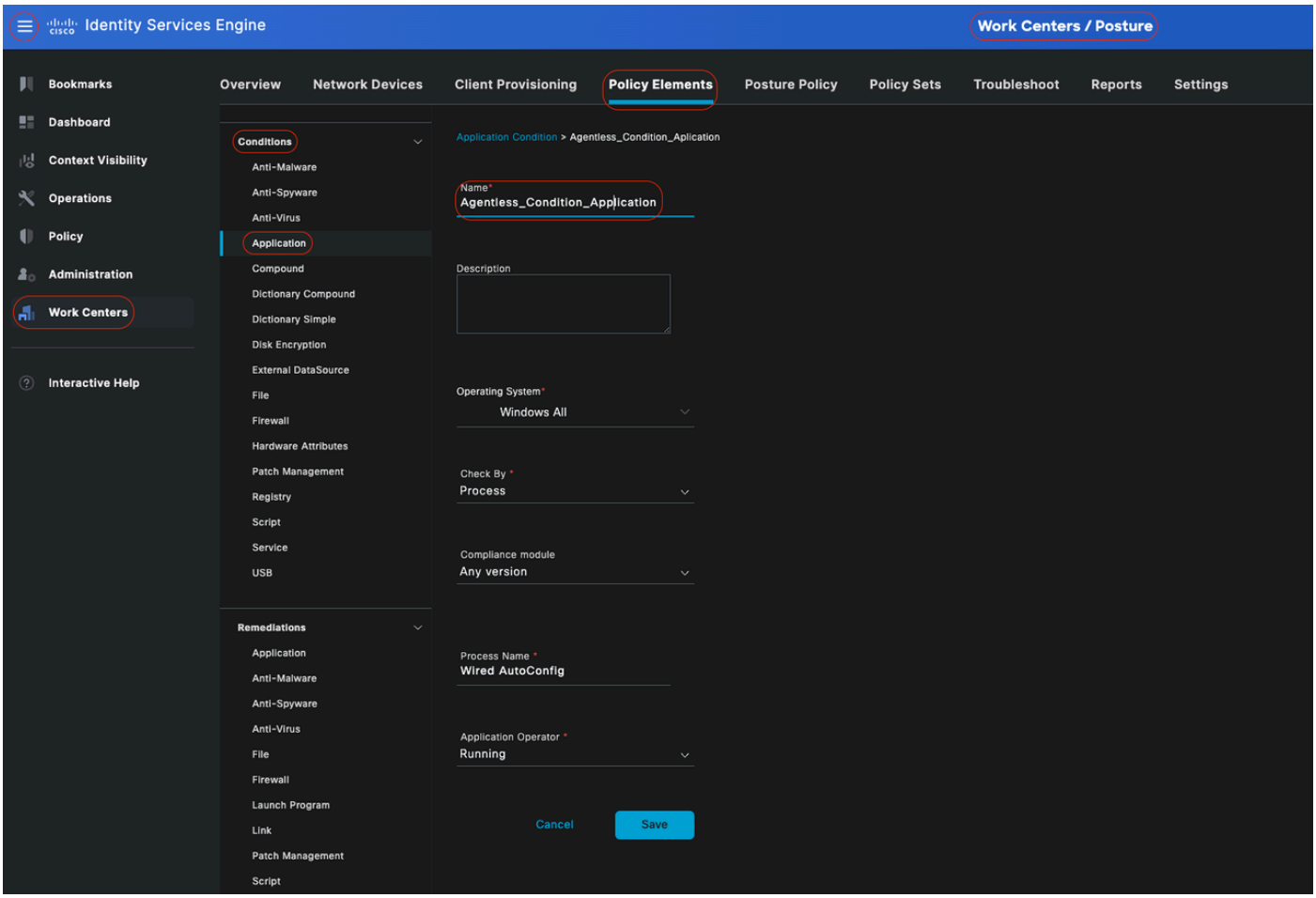
El sistema supervisa los procesos dentro del dispositivo. Tiene la opción de seleccionar Process o Application; en este caso, se eligió Process.

•Nombre del proceso: Configuración automática por cable

El proceso Wired AutoConfig es el proceso que el módulo compatible va a registrar el dispositivo. Este proceso se encarga de configurar y administrar las conexiones de red por cable, incluida la autenticación IEEE 802.1X.

· Operador de aplicaciones: Ejecutándose

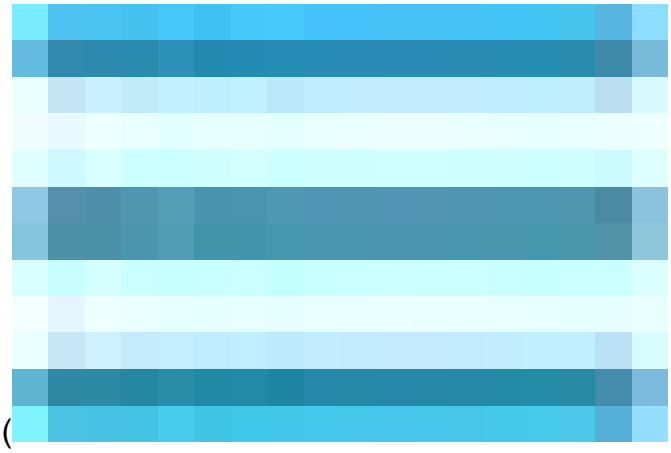
El módulo de cumplimiento verifica si el proceso de configuración automática por cable se está ejecutando actualmente en el dispositivo. Tiene la opción de seleccionar En ejecución o No en ejecución. En este caso, se seleccionó Running para asegurarse de que el proceso está activo.



Condición sin agente

Requisito de estado

Un requisito de estado es un conjunto de condiciones compuestas o una sola condición que se puede vincular a una función y a un sistema operativo. Todos los clientes que se conectan a la red deben cumplir los requisitos obligatorios durante la evaluación de estado para cumplir los requisitos de la red.



En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y seleccione Centros de trabajo > Postura > Elementos de política > Requisito. Haga clic en la flecha hacia abajo y seleccione Insertar nuevo requisito y cree uno o más Requisito de postura que utilice una postura sin agente. Una vez creado el requisito, haga clic en Finalizado y, a continuación, en Guardar.

En este caso, un requisito de aplicación denominado "Agentless_Requirement_Application" se configuró con estos criterios:

•Sistema operativo: Todo de Windows

Este requisito se aplica a cualquier versión del sistema operativo Windows, lo que garantiza que es aplicable a todos los entornos de Windows.

· Tipo de postura: Sin agente

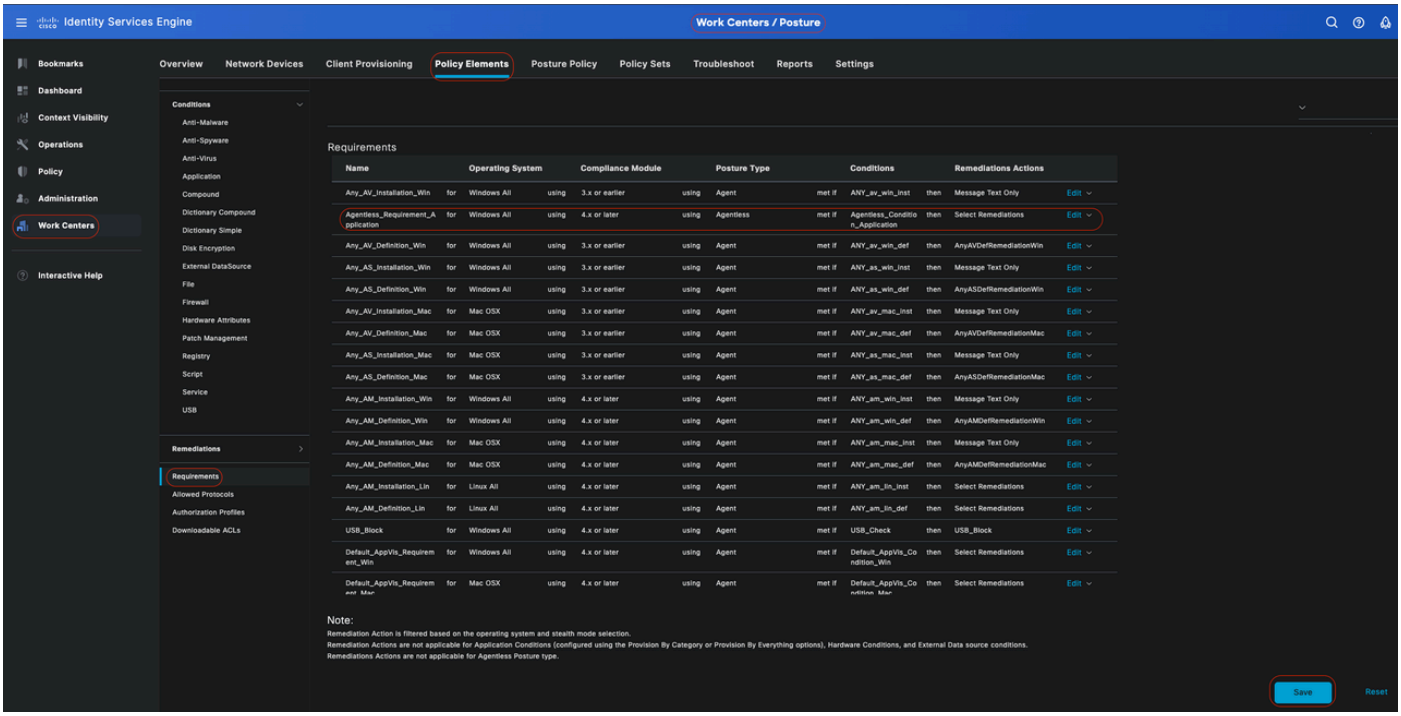
Esta configuración se establece para un entorno sin agente. Las opciones disponibles son Agente, Agente sigiloso, Agente temporal y Sin agente. En este escenario, se seleccionó Agentless.

•Condiciones: Aplicación_de_condición_sin_agente

Esto especifica la condición que el módulo de condición de ISE y el módulo de conformidad comprobarán en los procesos del dispositivo. La condición seleccionada es Aplicación_de_condición_sin_agente.

· Acciones de remediación:

Dado que esta configuración es para un entorno sin agente, no se admiten acciones de remediación y este campo aparece atenuado.



Requisito sin agente

Política de estado

En la GUI de Cisco ISE, haga clic en el iconoMenú (

) y seleccione Centros de trabajo > Postura > Política de postura. Haga clic en la flecha hacia abajo y seleccione Insertar nuevo requisito y cree una o más reglas de política de postura admitidas que utilicen una postura sin agente para ese requisito de postura. Una vez creada la política de estado, haga clic en Finalizado y, a continuación, en Guardar.

En este escenario, se ha configurado una política de estado denominada "Agentless_Policy_Application" con estos parámetros:

· Nombre de regla: Aplicación_de_política_sin_agente

Este es el nombre designado para la política de postura en este ejemplo de configuración.

•Sistema operativo: Todo de Windows

La directiva se establece para aplicarse a todas las versiones del sistema operativo Windows, lo que garantiza una amplia compatibilidad entre los distintos entornos de Windows.

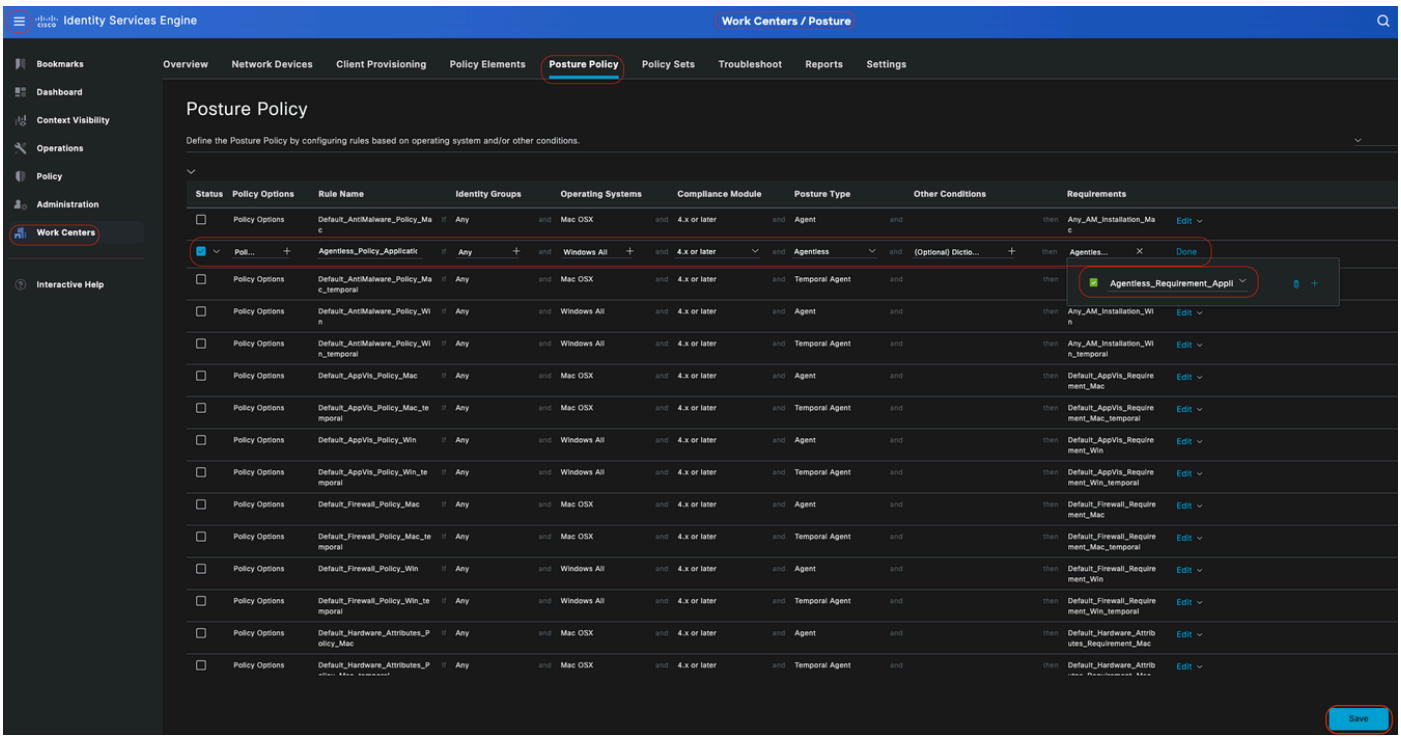
· Tipo de postura: Sin agente

Esta configuración se establece para un entorno sin agente. Las opciones disponibles son Agente, Agente sigiloso, Agente temporal y Sin agente. En este escenario, se ha seleccionado Agentless.

· Otras condiciones:

En este ejemplo de configuración, no se han creado condiciones adicionales. Sin embargo, tiene

la opción de configurar condiciones específicas para asegurarse de que sólo los dispositivos de destino están sujetos a esta directiva de estado, en lugar de todos los dispositivos de Windows de la red. Esto puede resultar especialmente útil para la segmentación de la red.



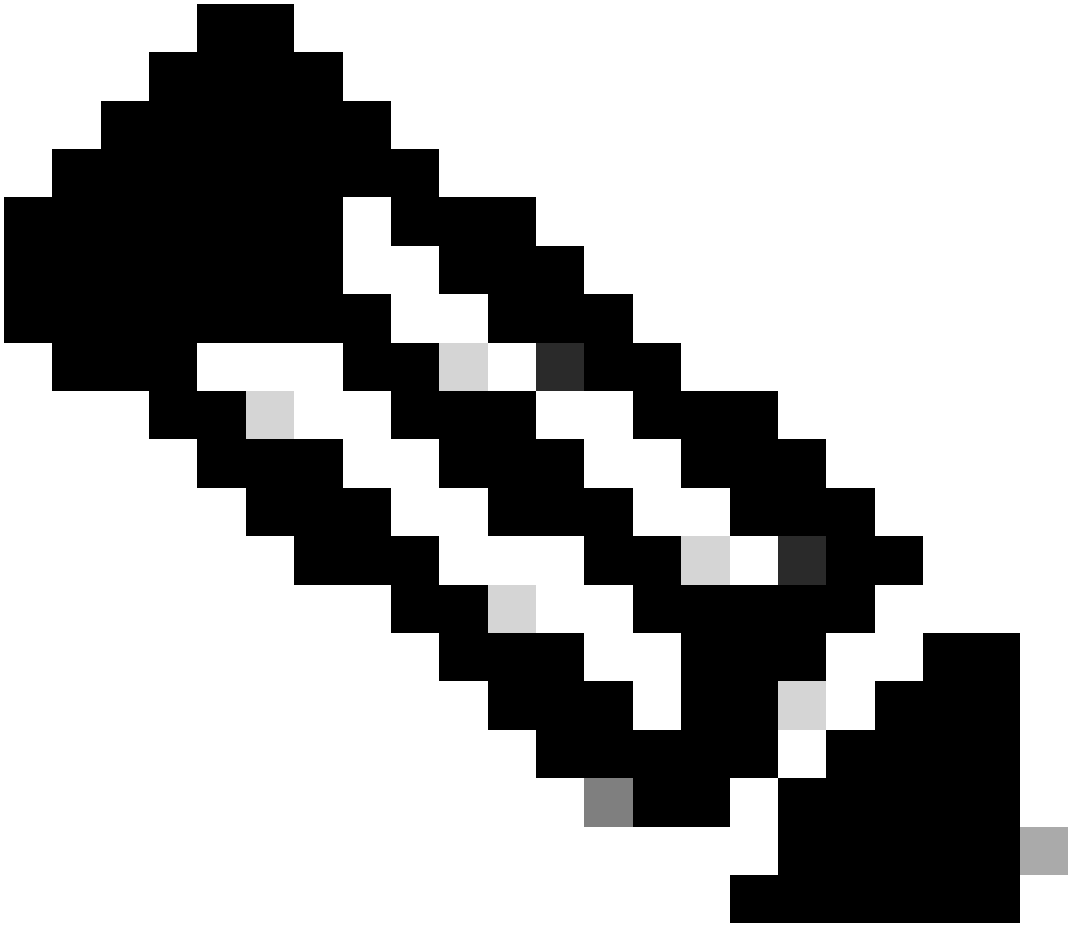
Política sin agentes de estado

Aprovisionamiento de clientes

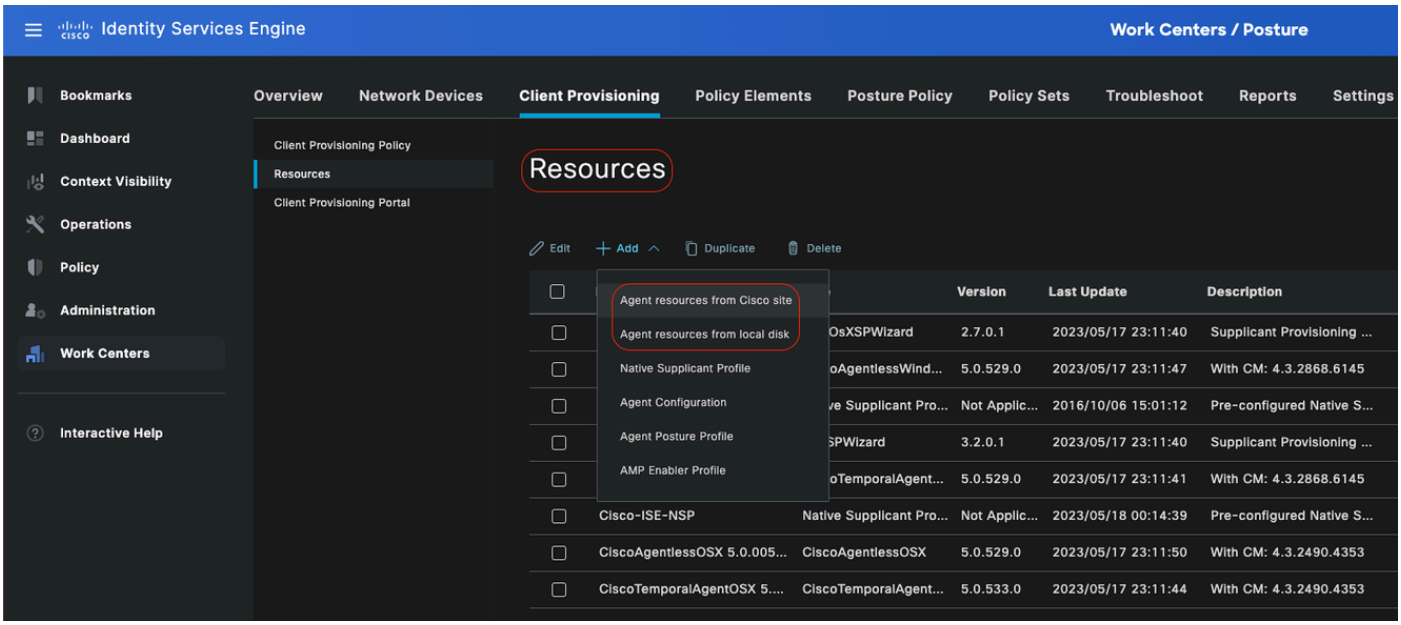
Paso 1: Descarga de recursos

Para comenzar a configurar el aprovisionamiento de clientes, primero debe descargar los recursos necesarios y tenerlos disponibles en ISE para poder utilizarlos posteriormente en la directiva de aprovisionamiento de clientes.

Hay dos formas de agregar recursos a ISE: Recursos de agente desde el sitio de Cisco y Recursos de agente desde el disco local. Dado que está configurando Agentless, se le solicitará que acceda al sitio de recursos de agente de Cisco para realizar la descarga.



Nota: Para utilizar estos recursos de agente del sitio de Cisco, ISE PAN necesita acceso a Internet.



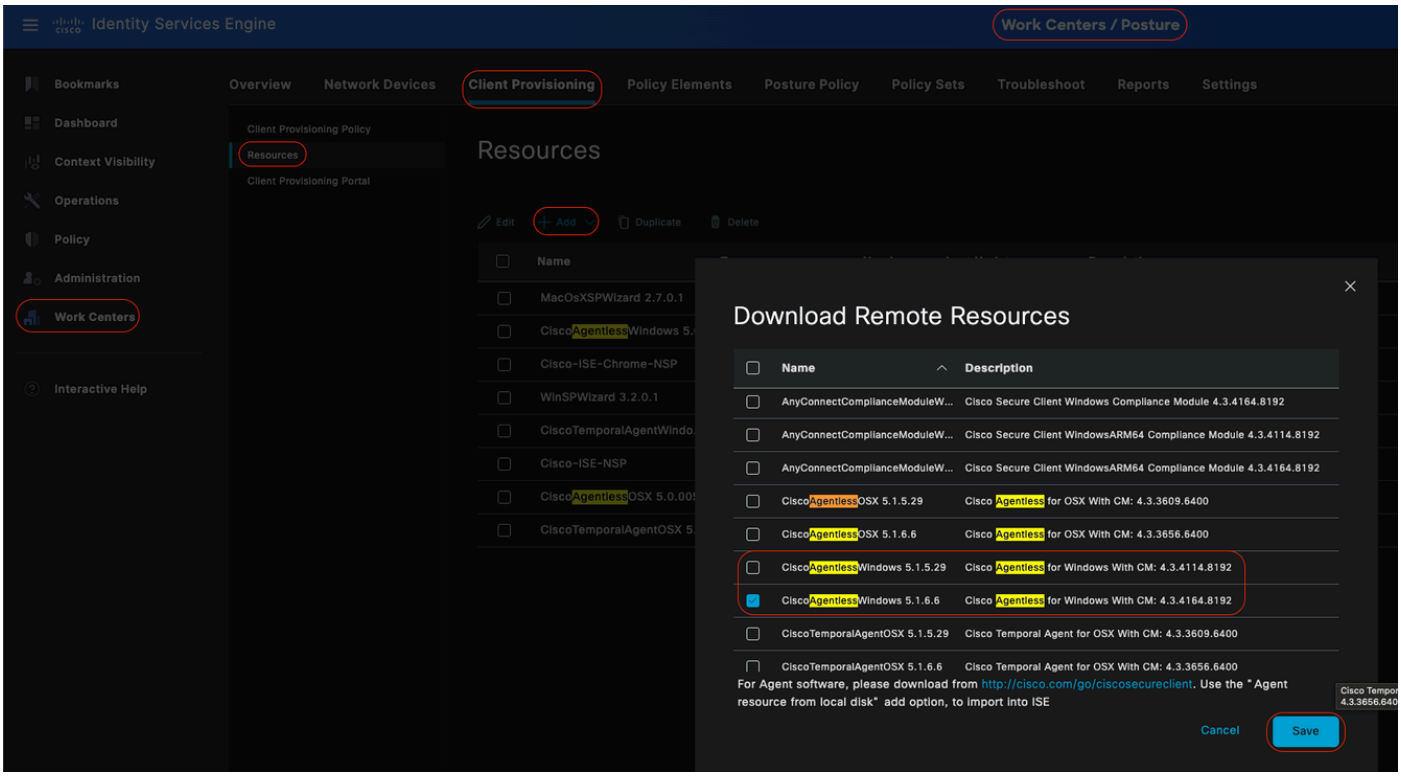
Recursos

Recursos de agentes del sitio de Cisco

En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y seleccione Centros de trabajo > Estado > Aprovisionamiento de cliente > Recursos. Haga clic en Agregar , seleccione Recursos de agente del sitio de Cisco, haga clic en Guardar.

Desde el sitio de Cisco, solo puede descargar el módulo de cumplimiento. El sistema muestra los dos módulos de cumplimiento más recientes que se pueden descargar. El paquete de recursos CiscoAgentlessWindows 5.1.6.6 está seleccionado para este ejemplo de configuración, esto sólo se aplica a dispositivos Windows.

.



Recursos de agentes del sitio de Cisco

Paso 2: Configuración de la Política de Aprovisionamiento del Cliente

Al configurar el Agente de estado, necesita dos recursos diferentes (AnyConnect o Secure Client y Compliance Module),

Asigne ambos recursos en Configuración del agente junto con el Perfil de postura del agente para que pueda utilizar esta Configuración del agente en su Política de aprovisionamiento de clientes.

Sin embargo, al configurar Agentless de postura, no es necesario configurar Agent Configuration o Agent Posture Profile, en lugar de ello, solo se descarga el paquete sin agente de Agent Resources desde el sitio de Cisco.

En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y seleccione Centros de trabajo > Condición > Aprovisionamiento del cliente > Política de aprovisionamiento del cliente. Haga clic en la flecha hacia abajo y seleccione Insertar nueva política encima o Insertar nueva política debajo, Duplicar arriba o Duplicar abajo:

- Nombre de regla: Agentless_Client_Provisioning_Policy

Especifica el nombre de la directiva de aprovisionamiento de clientes.

- Sistema operativo: Windows All

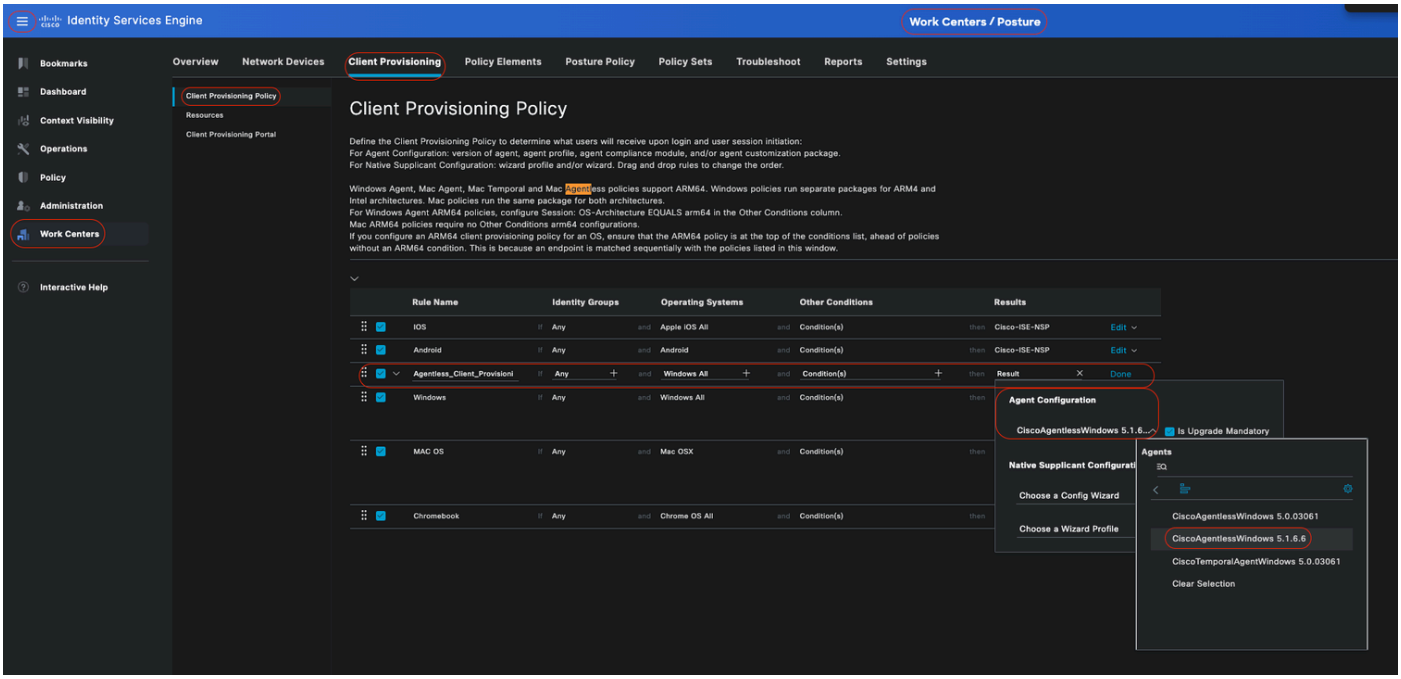
Esto garantiza que la directiva se aplica a todas las versiones del sistema operativo Windows.

- Otras condiciones: no se ha configurado ninguna condición específica en este ejemplo. Sin embargo, puede configurar condiciones para asegurarse de que sólo los dispositivos deseados coincidan con esta directiva de aprovisionamiento de clientes, en lugar de con todos los dispositivos de Windows de la red. Esto resulta especialmente útil para la segmentación de la red.

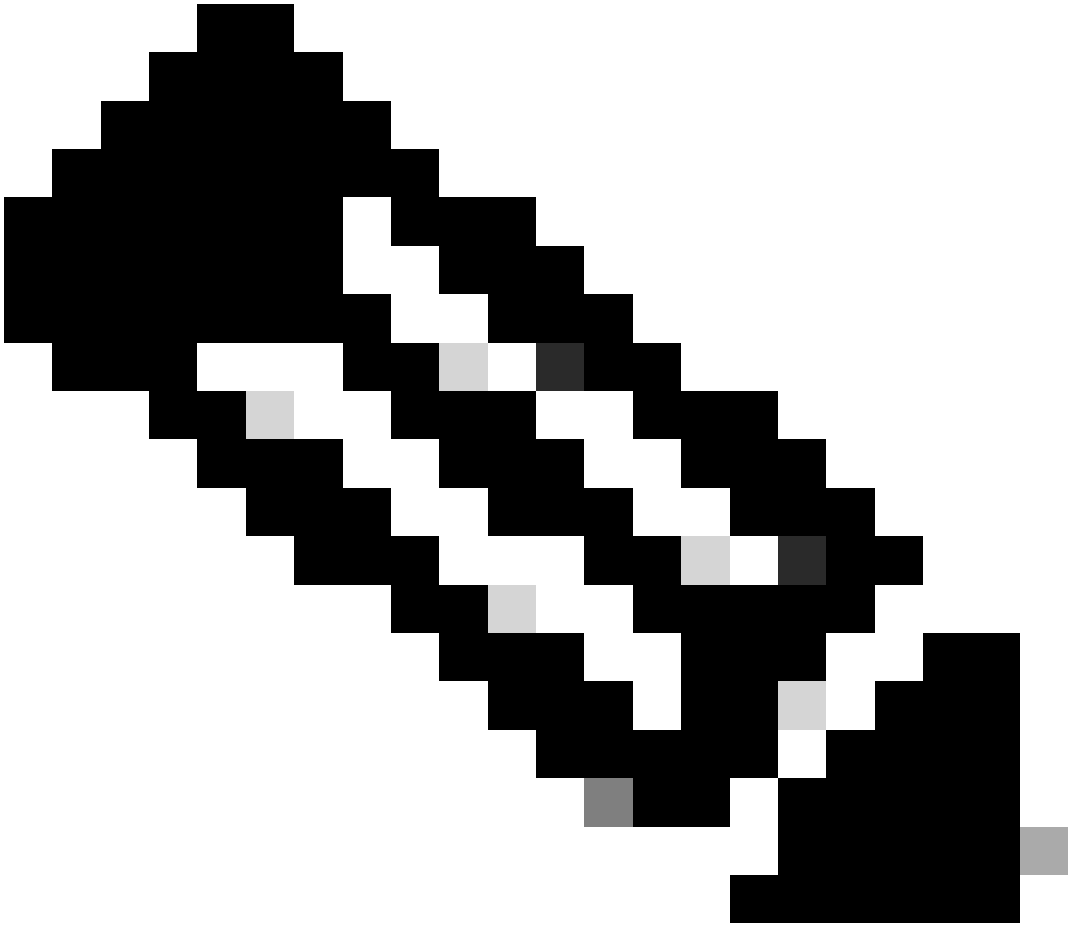
Ejemplo: Si utiliza Active Directory, puede incorporar grupos de Active Directory en la directiva para precisar los dispositivos afectados.

- Resultados: seleccione el paquete o agente de configuración adecuado. Dado que está realizando la configuración para un entorno sin agente, elija el paquete CiscoAgentlessWindows 5.1.6.6, que ya ha descargado anteriormente del sitio Recursos de agente de Cisco. Este paquete sin agente contiene todos los recursos necesarios (Software sin agente y Módulo de cumplimiento) necesarios para que se ejecute Posture Agentless.

•Haga clic en Save (Guardar).



Política de aprovisionamiento de clientes sin agentes



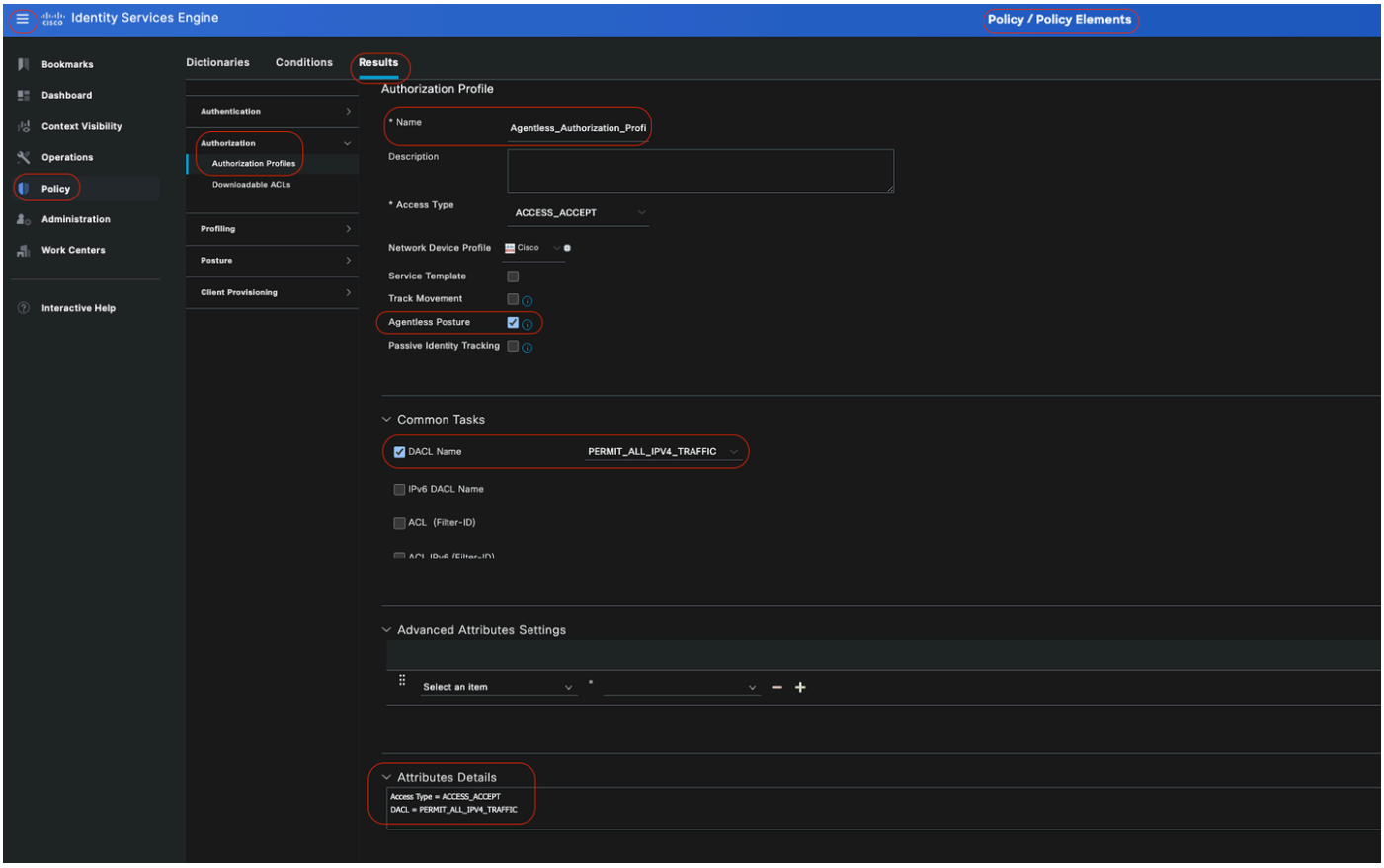
Nota: Asegúrese de que sólo una política de aprovisionamiento de clientes satisfaga las condiciones de cualquier intento de autenticación. Si se evalúan varias políticas simultáneamente, pueden producirse comportamientos inesperados y posibles conflictos.

Perfil de autorización sin agente

En la GUI de Cisco ISE, haga clic en el iconoMenú (

) y elija Policy > Policy Elements > Results > Authorization > Authorization Profiles y cree un Authorization Profile que evalúe los resultados de la postura sin agente.

- En este ejemplo de configuración, denominado Authorization Profile como Agentless_Authorization_Profile.
- Activar estado sin agente en el perfil de autorización.
- Utilice este perfil solo para postura sin agente. No lo utilice también para otros tipos de postura.
- CWA y ACL de redirección no son necesarios para el estado sin agente. Puede utilizar VLAN, DACL o ACL como parte de las reglas de segmentación. Para que sea sencillo, sólo se configura una dACL (que permite todo el tráfico ipv4) además de la verificación de estado sin agente en este ejemplo de configuración.
- Haga clic en Guardar.



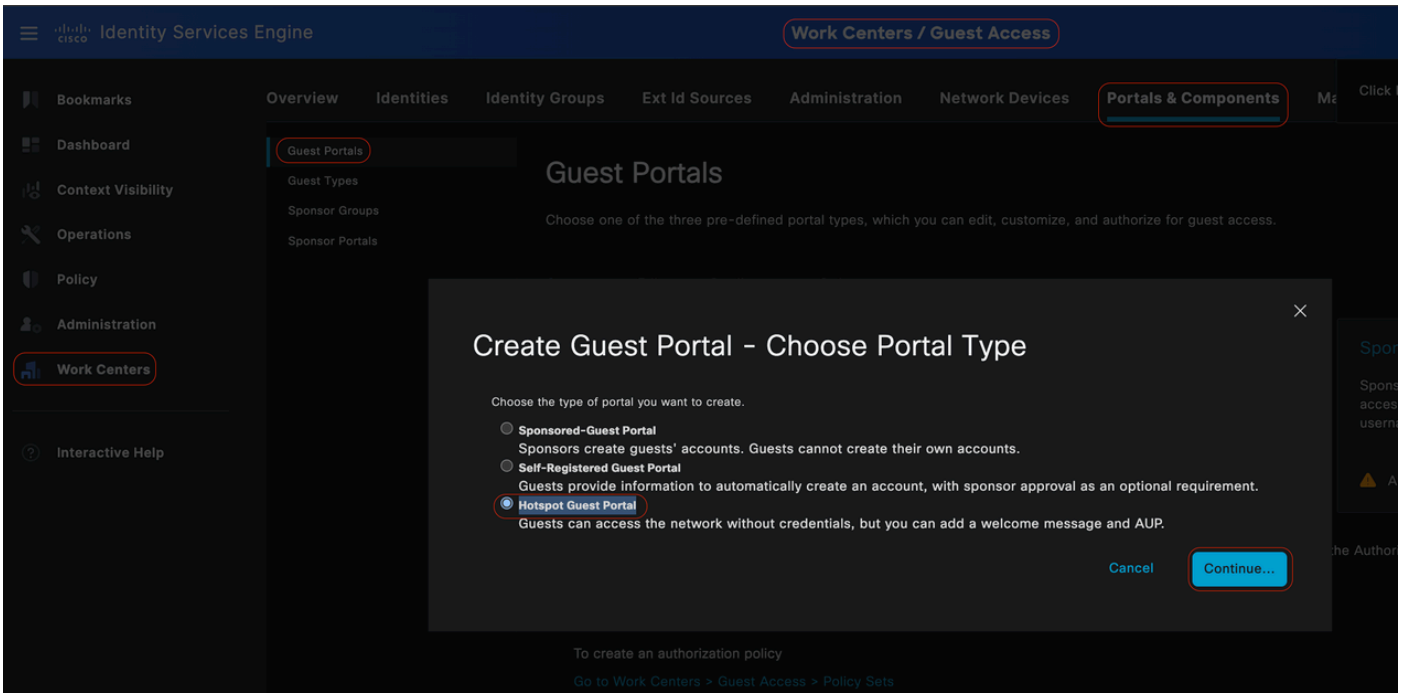
Perfil de autorización sin agente

Alternativa a la remediación (opcional)

No está disponible el soporte para la remediación en el flujo sin agente. Para solucionar este problema, puede implementar un portal de zonas Wi-Fi personalizado para mejorar el conocimiento de los usuarios sobre el cumplimiento de los terminales. Cuando un terminal se identifica como no conforme, los usuarios pueden ser redirigidos a este portal. Este enfoque garantiza que los usuarios estén informados sobre el estado de conformidad de sus terminales y

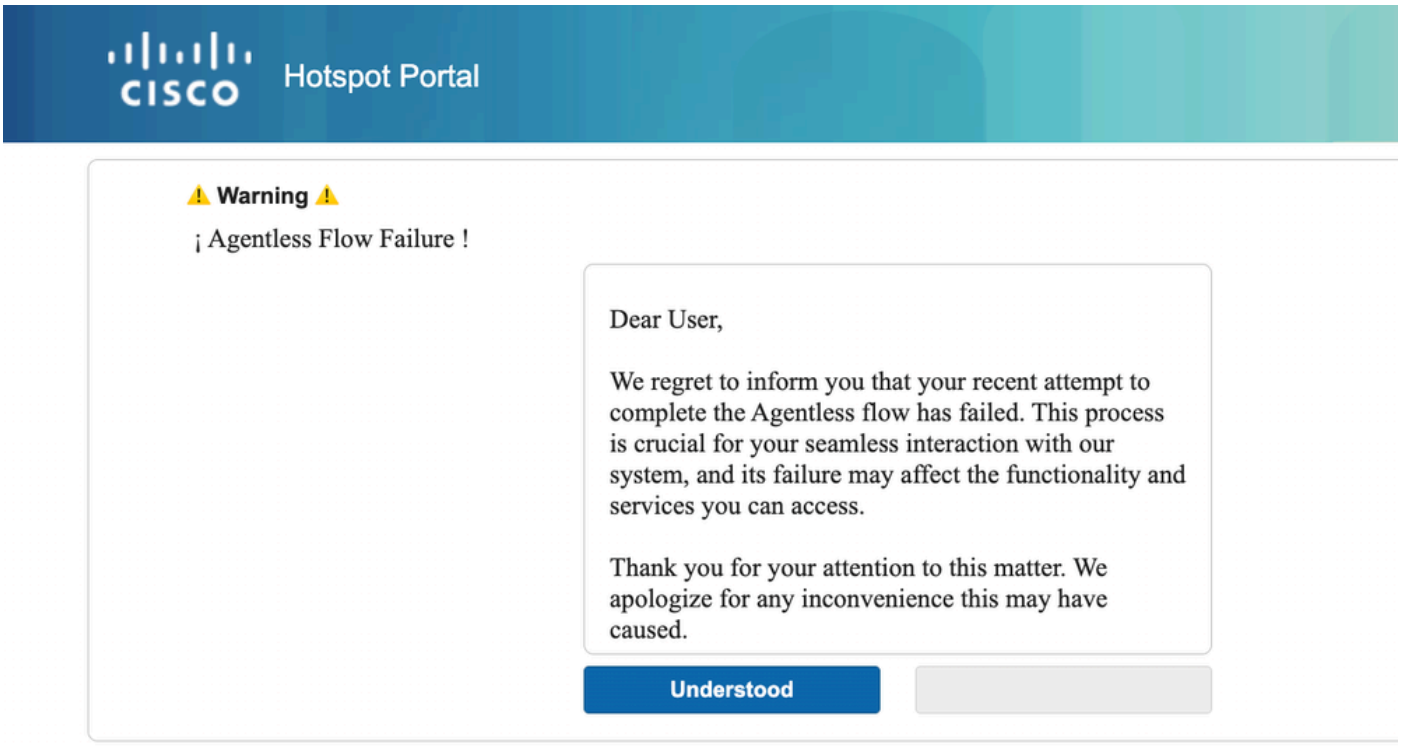
puedan tomar las medidas adecuadas para corregir cualquier problema.

En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y seleccione Centros de trabajo > Acceso de invitado > Portales y componentes >Portales de invitado. Haga clic en Crear > Seleccionar portal de invitado de zona Wi-Fi > Continuar: . En este ejemplo de configuración, el portal de zonas Wi-Fi se denomina Agentless_Warning.



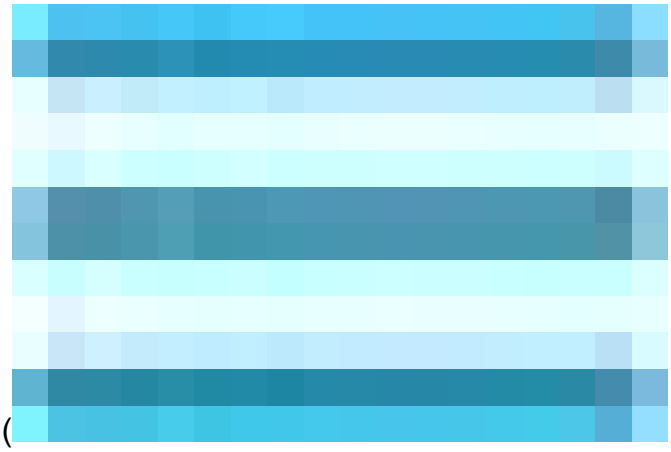
Portal de invitados de zona Wi-Fi

En la configuración del portal, tiene la capacidad de personalizar los mensajes que se muestran a los usuarios finales para ajustarlos a sus requisitos específicos. Este es solo un ejemplo de vista personalizada del portal:



Postura errónea sin agente

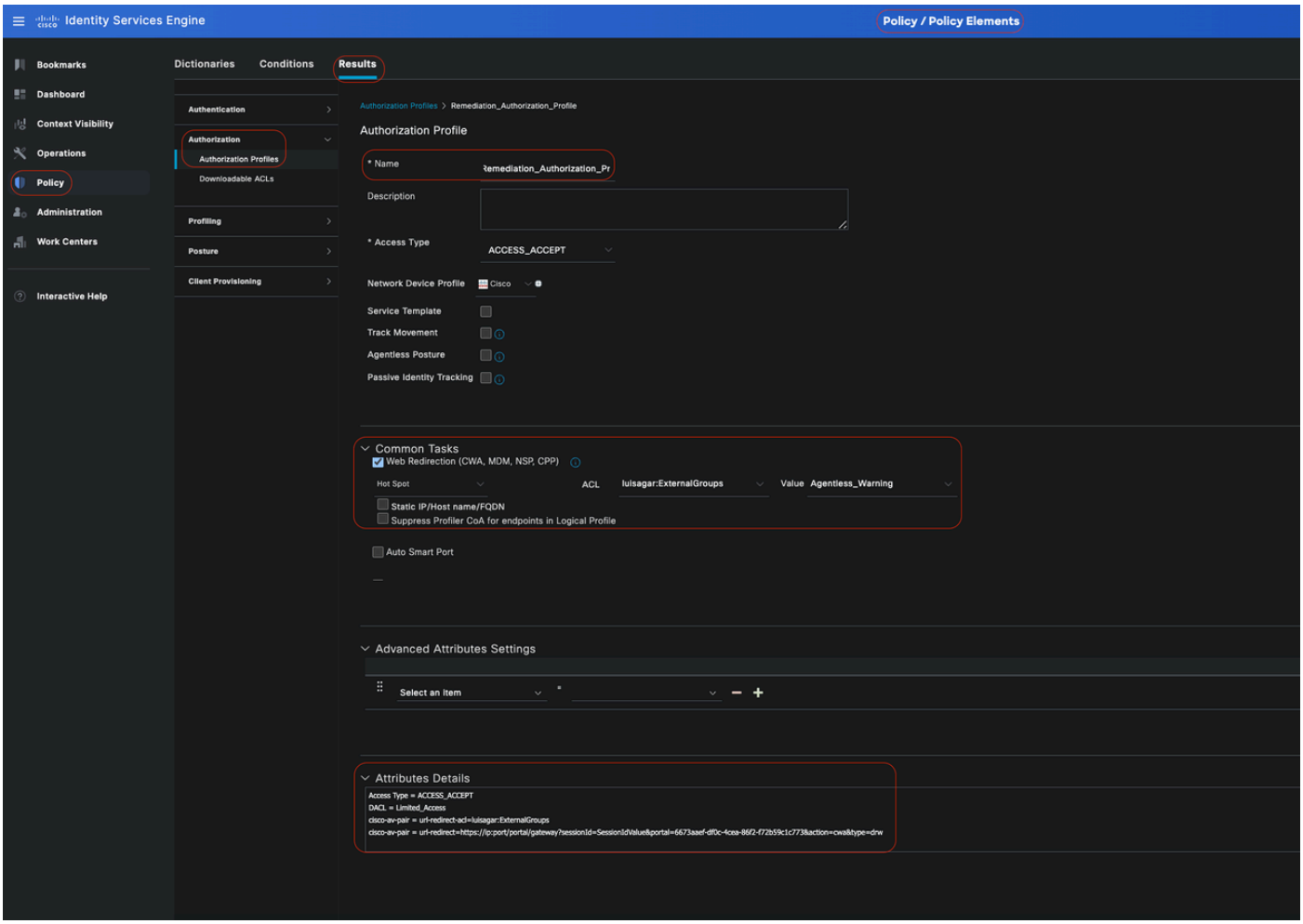
Perfil de autorización de remediación (opcional)



En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y elija Policy > Policy Elements > Results > Authorization > Authorization Profiles y cree un Authorization Profile para su remediación.

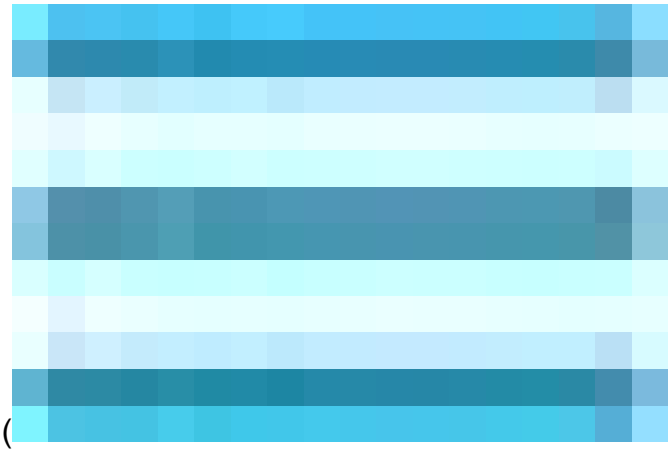
- En este ejemplo de configuración, denominado Authorization Profile como Remediation_Authorization_Profile.
- Por motivos de simplicidad, este ejemplo de configuración solo incluye una lista de control de acceso (dACL) descargable denominada Limited_Access que permite un acceso limitado, adaptado a las necesidades específicas de su organización.
- Se ha configurado la función Web Redirection, que incluye un grupo externo y el punto de conexión, lo que mejora el conocimiento del usuario sobre el cumplimiento de los terminales.

- Click Save.

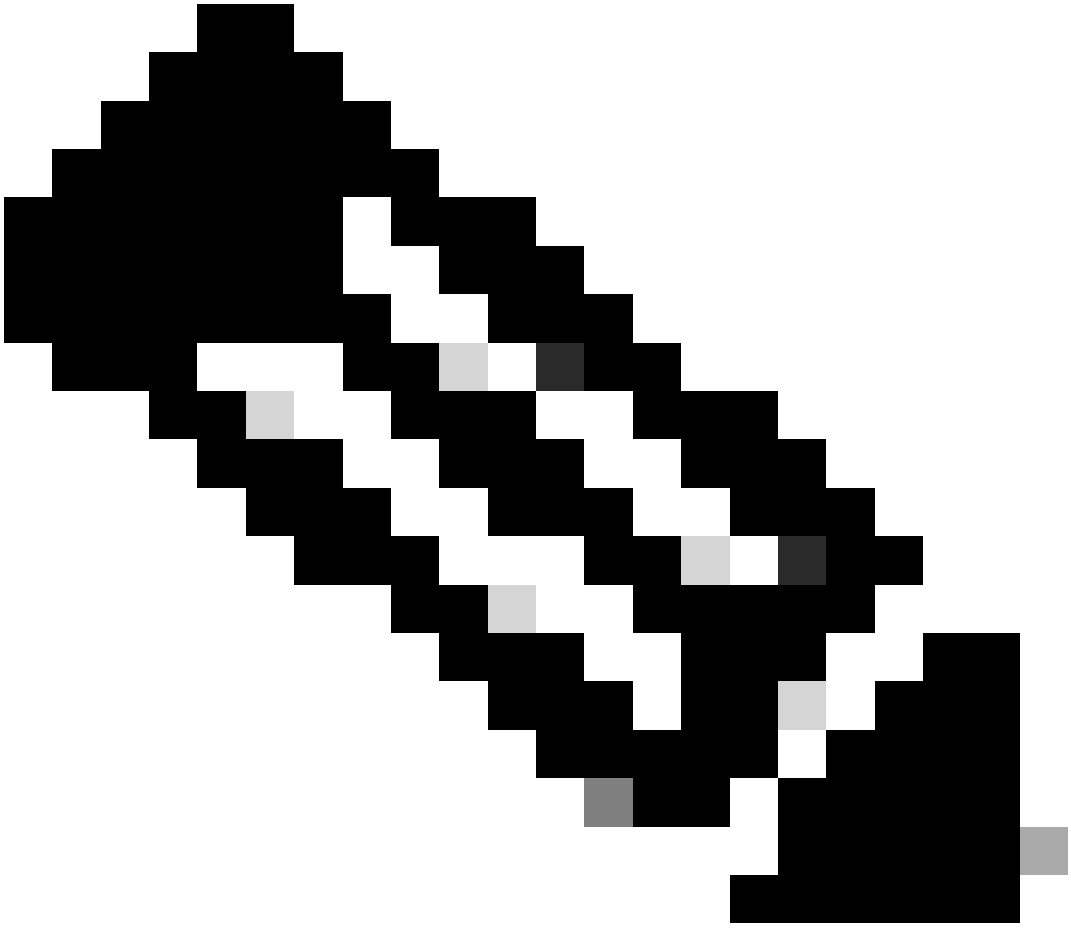


Regla de autorización de remediación

Regla de autorización sin agente



En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y elijaDirectiva > Conjuntos de directivas y expanda Directiva de autorización. Habilite y configure estas tres directivas de autorización:



Nota: Estas reglas de autorización deben configurarse en el orden especificado para garantizar que el flujo de estado funcione correctamente.

Unknown_Compliance_Redirect:

•Condiciones:

Configure Network_Access_Authentication_Passed Y Compliance_Unknown_Devices con el resultado establecido en Postura sin agente. Esta condición activa el flujo sin agente.

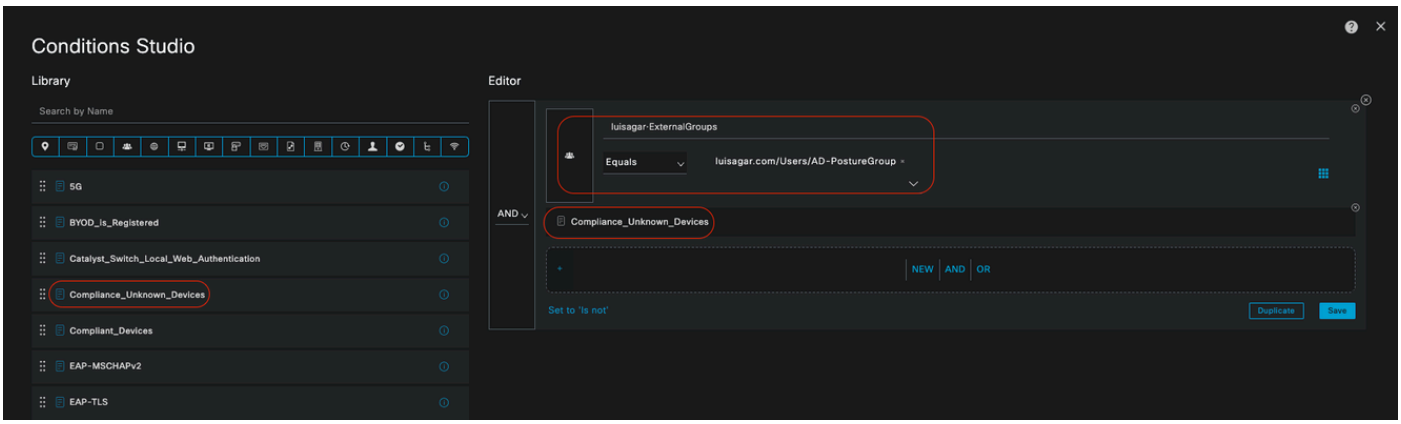
· Condiciones de ejemplo:

Configure una condición de grupo de Active Directory (AD) para segmentar el tráfico.

La condición Compliance_Unknown_Devices debe configurarse ya que el estado inicial es desconocido.

· Perfil de autorización:

Asigne Agentless_Authorization_Profile a esta regla de autorización para asegurarse de que los dispositivos pasan por el flujo de estado sin agente. Esta condición contiene flujo sin agente para que los dispositivos que alcancen este perfil puedan iniciar un flujo sin agente.



Regla de autorización desconocida

Dispositivos_no_conformes_Redirigir:

•Condiciones: Configure Network_Access_Authentication_Passed y Non_Compliant_Devices con el resultado establecido en DenyAccess. También puede utilizar la opción de remediación, como se muestra en este ejemplo.

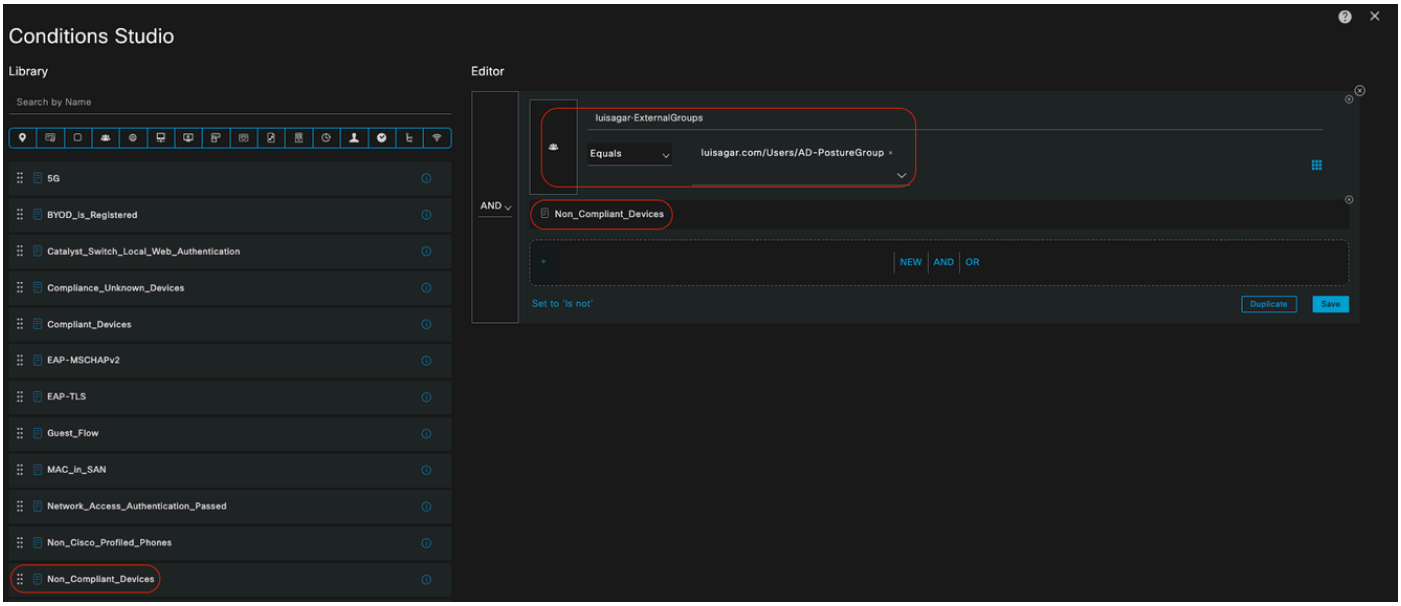
· Condiciones de ejemplo:

Configure una condición de grupo de AD para segmentar el tráfico.

La condición Compliance_Unknown_Devices se debe configurar para asignar recursos limitados cuando el estado no sea conforme.

· Perfil de autorización:

Asigne Remediation_Authorization_Profile a esta regla de autorización para notificar a los dispositivos no conformes su estado actual a través de Hotspot Portal o para Denegar acceso.



Regla de autorización de no conformidad

Acceso_de_dispositivos_compatibles:

•Condiciones:

Configure Network_Access_Authentication_Passed y Compliant_Devices con el resultado establecido en PermitAccess.

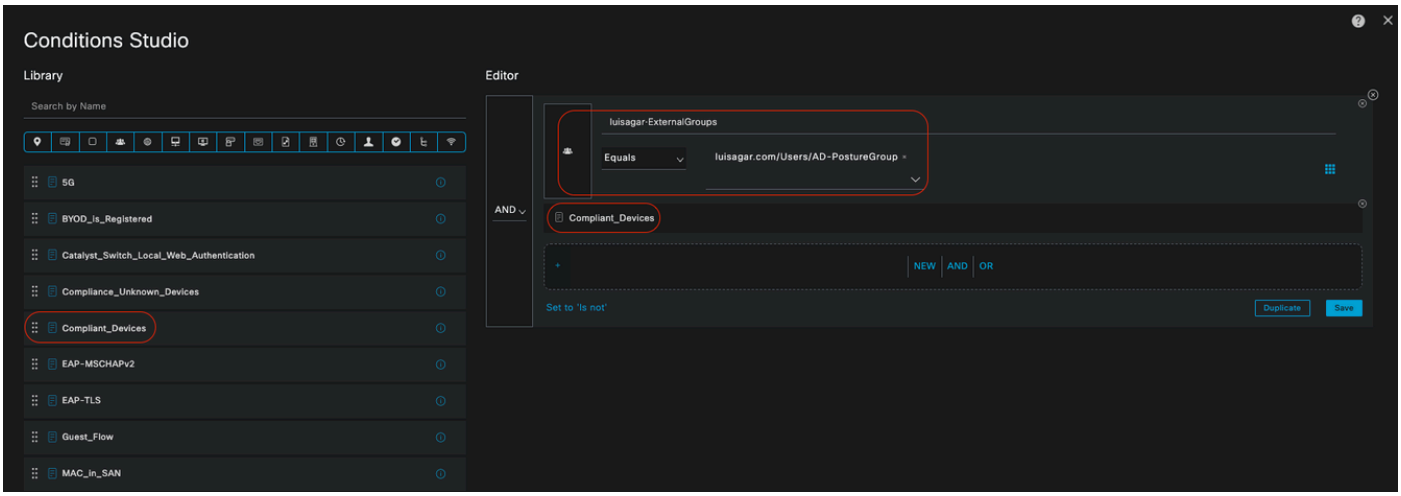
· Condiciones de ejemplo:

Configure una condición de grupo de AD para segmentar el tráfico.

La condición Compliance_Unknown_Devices se debe configurar para que los dispositivos compatibles tengan el acceso adecuado.

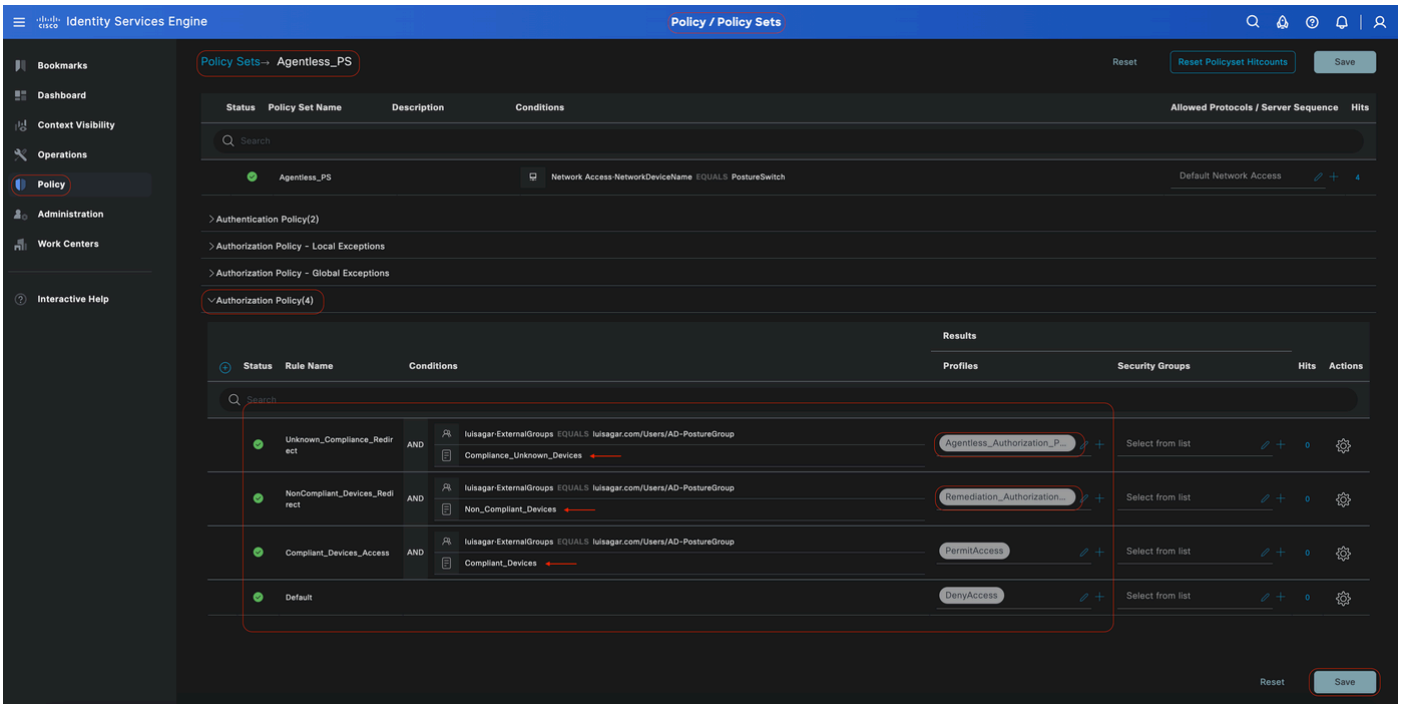
· Perfil de autorización:

Asigne PermitAccess a esta regla de autorización para garantizar que los dispositivos compatibles tengan acceso. Este perfil se puede personalizar para satisfacer las necesidades de su organización.



Regla de autorización conforme

Todas las reglas de autorización



Reglas de autorización

Configurar credenciales de inicio de sesión de terminal

En la GUI de Cisco ISE, haga clic en el iconoMenú ( ) y elija Administration > Settings > Endpoint Scripts > Login Configuration, y configure las credenciales del cliente para iniciar sesión en los clientes.

Las secuencias de comandos de terminales utilizan estas mismas credenciales, por lo que Cisco ISE puede iniciar sesión en los clientes.

Para los dispositivos Windows, sólo debe configurar las dos primeras fichas (Usuario de dominio de Windows y Usuario local de Windows)

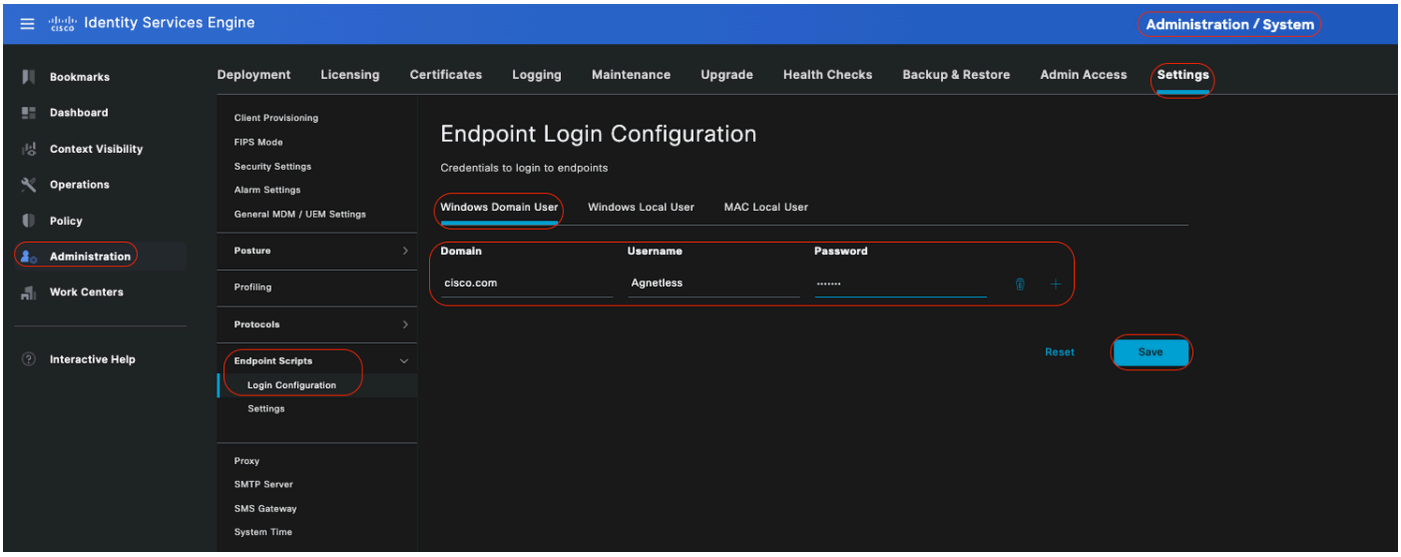
**

- Usuario de dominio de Windows:

Configure las credenciales de dominio que Cisco ISE debe utilizar para iniciar sesión en un cliente mediante SSH. Haga clic en el icono de Plugin e ingrese tantos inicios de sesión de Windows como necesite. Para cada dominio, introduzca los valores necesarios en los campos

Dominio,Nombre de usuario y Contraseña. Si configura las credenciales de dominio, se omiten las credenciales de usuario local configuradas en la fichaUsuario local de Windows.

Si administra extremos de Windows que utilizan una evaluación de estado sin agente a través de un dominio de Active Directory, asegúrese de proporcionar el nombre de dominio junto con las credenciales que poseen privilegios administrativos locales.

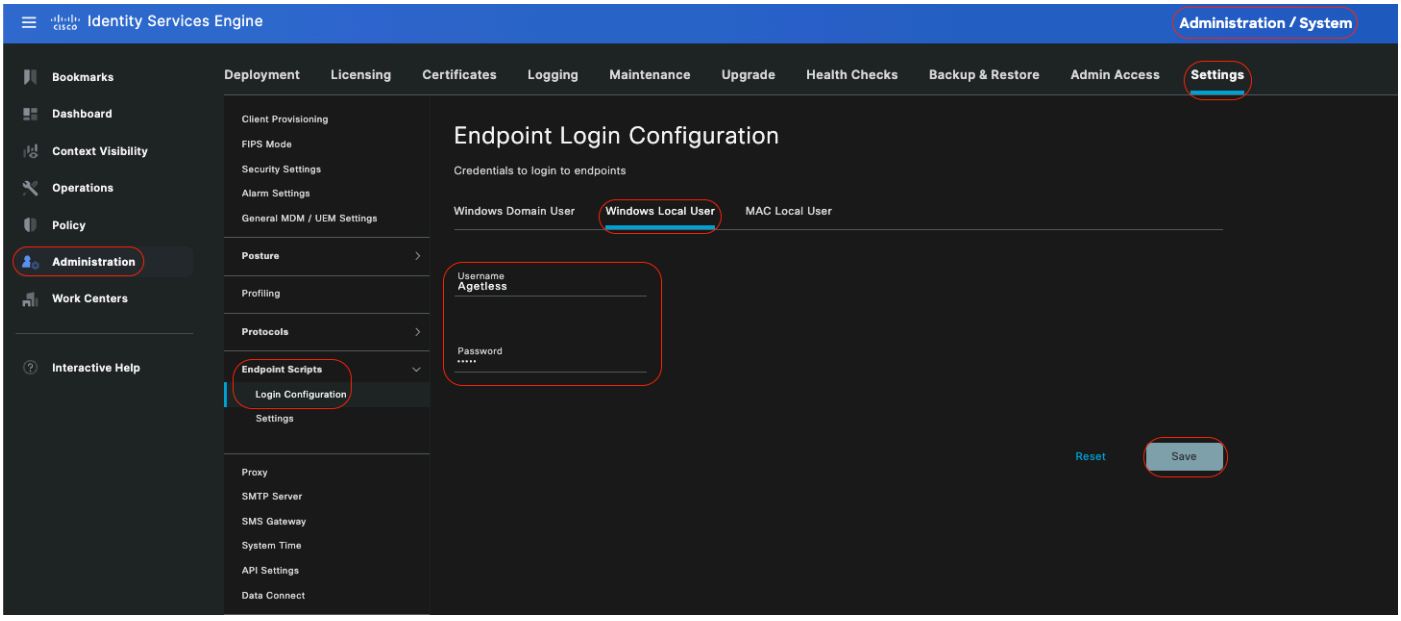


Usuario de dominio de Windows

- Usuario local de Windows:

Configure la cuenta local que Cisco ISE utiliza para acceder al cliente mediante SSH. La cuenta local debe poder ejecutar PowerShell y PowerShell de forma remota.

Si no administra terminales de Windows que utilizan una evaluación de estado sin agente a través de un dominio de Active Directory, asegúrese de proporcionar credenciales que tengan privilegios administrativos locales.

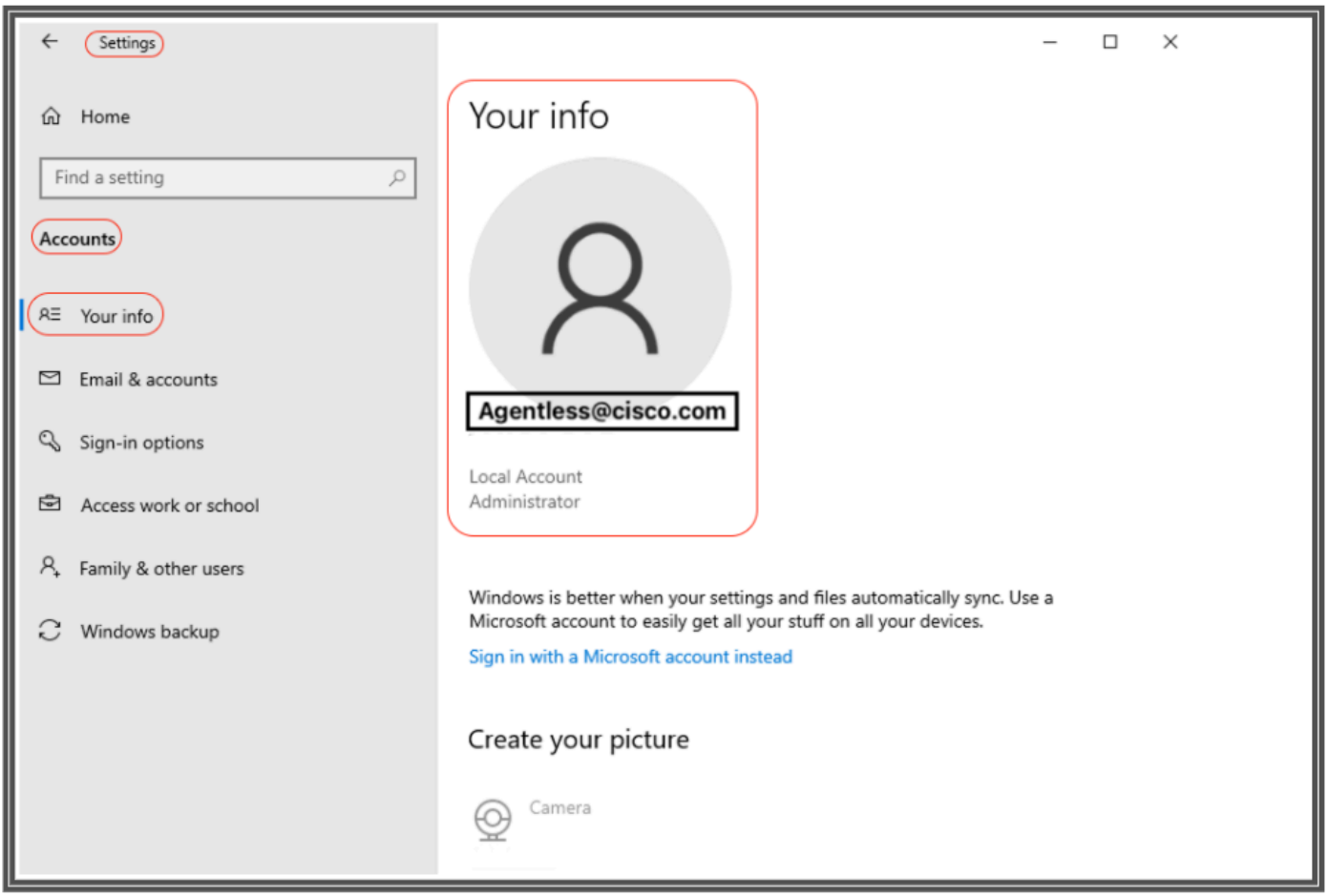


Usuario local de Windows

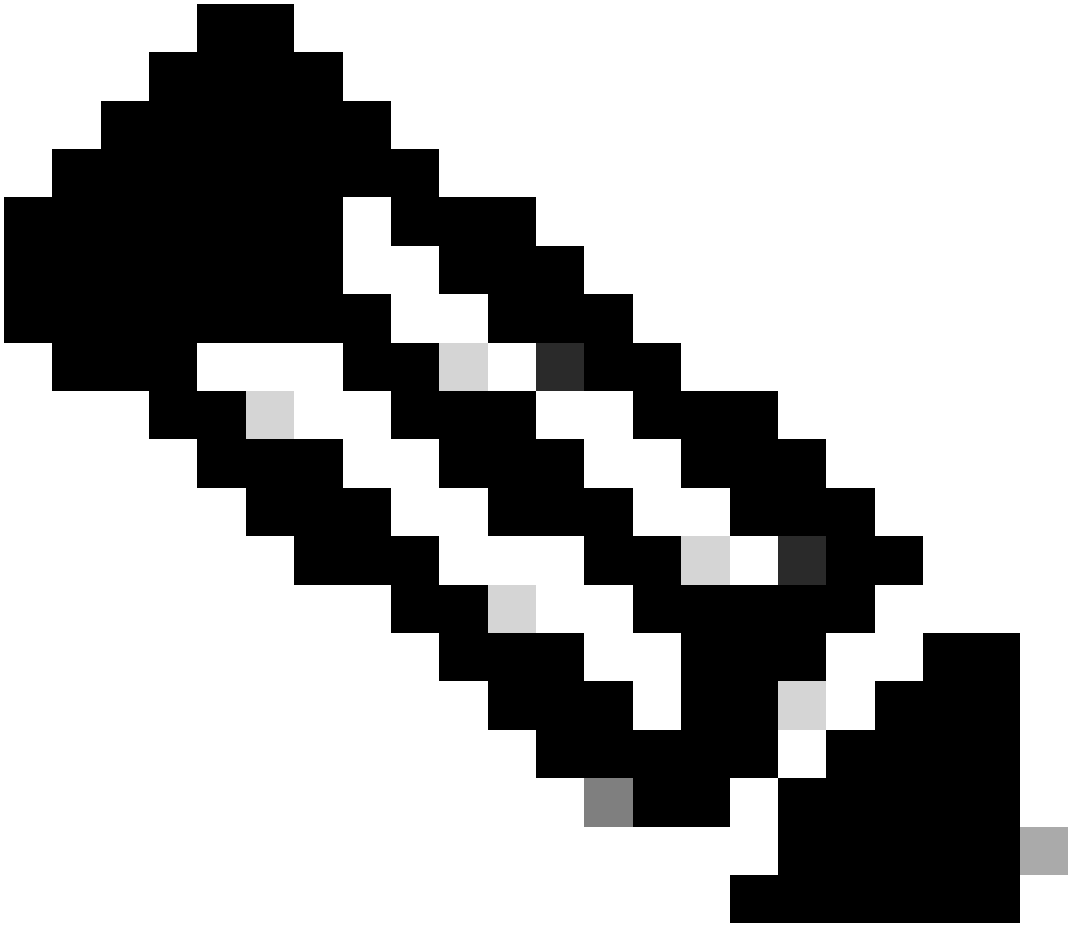
Verificar cuentas

Para comprobar las cuentas de usuario de dominio de Windows y las cuentas de usuario local de Windows para poder agregar con precisión los datos adecuados en Credenciales de inicio de sesión de terminal, utilice este procedimiento:

Usuario local de Windows: Con la GUI (aplicación de configuración), haga clic en el botón WindowsStart, seleccione Settings (el icono del engranaje), haga clic en Accounts y seleccione Your info:



Verificar cuentas



Nota: Para MacOS, puede consultar MAC Local User. Sin embargo, en este ejemplo de configuración, no verá la configuración de MacOS.

- Usuario local de MAC: Configure la cuenta local que Cisco ISE utiliza para acceder al cliente mediante SSH. La cuenta local debe poder ejecutar PowerShell y PowerShell de forma remota. En el campoNombre de usuario, introduzca el nombre de la cuenta local.

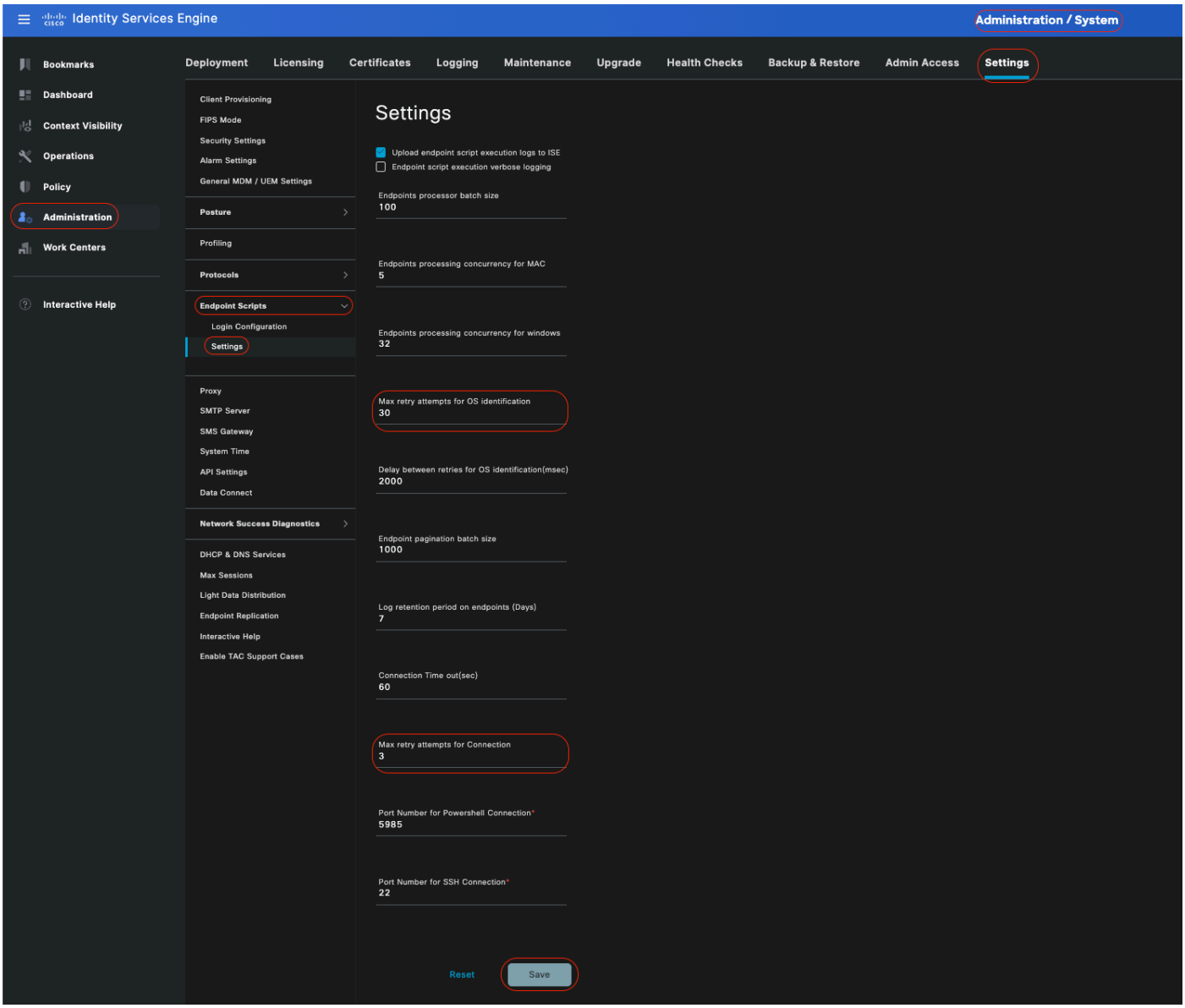
Para ver un nombre de cuenta de Mac OS, ejecute este comando`whoami`en el terminal:

Configuración

En la GUI de Cisco ISE, haga clic en el iconoMenú (

) y elija Administration > Settings > Endpoint Scripts > Settings, y configureMax retry tries para la identificación del sistema operativo, Delay between retries for OS identification, etc. Estos parámetros determinan la rapidez con la que se pueden confirmar los problemas de conectividad. Por ejemplo, un error que indica que el puerto de PowerShell no está abierto aparece en los registros sólo después de que no se hayan agotado todos los reintentos.

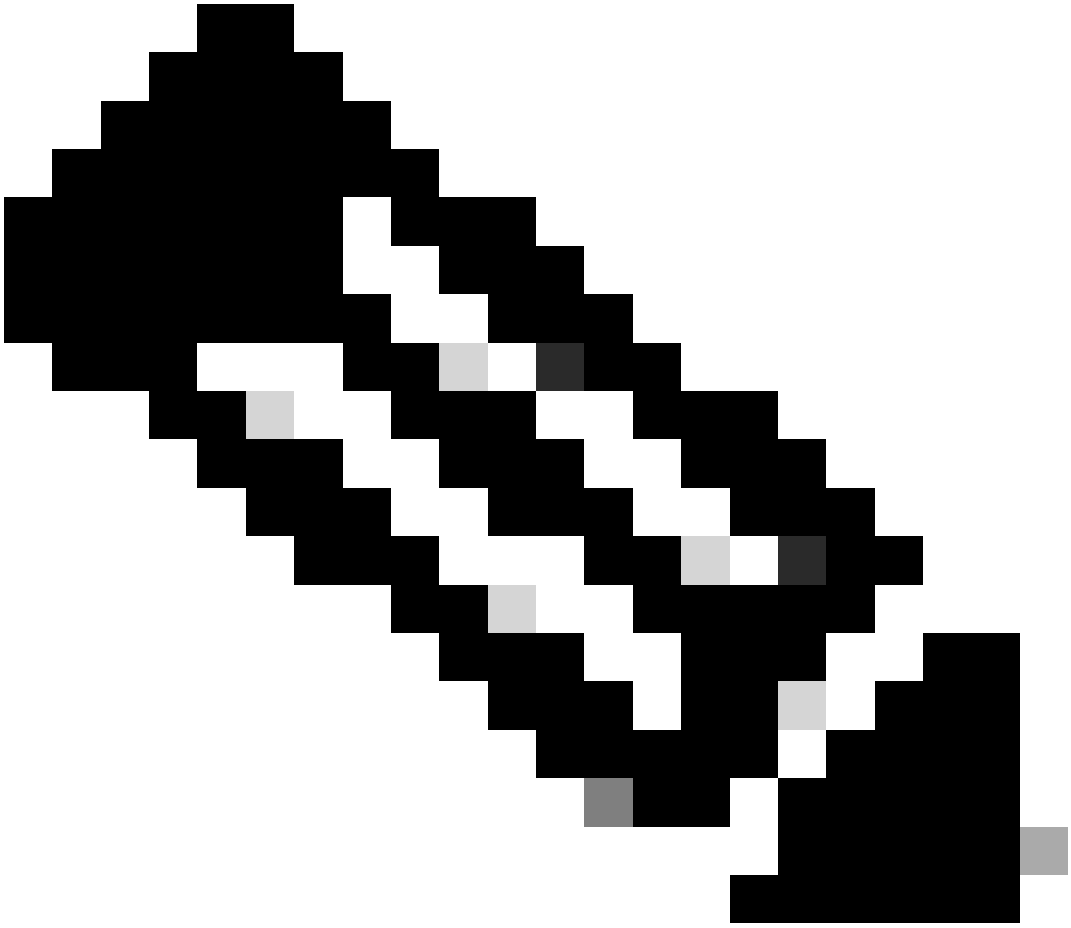
Esta captura de pantalla muestra los valores predeterminados:



Configuración de script de terminal

A medida que los clientes se conectan con una postura sin agente, puede verlos en los registros en directo.

Configuración y solución de problemas del extremo de Windows



Nota: Estas son algunas recomendaciones para comprobar y aplicar en su dispositivo Windows; sin embargo, debe consultar la documentación de Microsoft o ponerse en contacto con el soporte técnico de Microsoft si encuentra problemas como privilegios de usuario, acceso a PowerShell, etc.

Verificación y solución de problemas previos

Probando la conexión TCP al puerto 5985

Para los clientes Windows, se debe abrir el puerto 5985 para acceder a powershell en el cliente. Ejecute este comando para confirmar la conexión TCP al puerto 5985: **Test-NetConnection -ComputerName localhost -Port 5985**

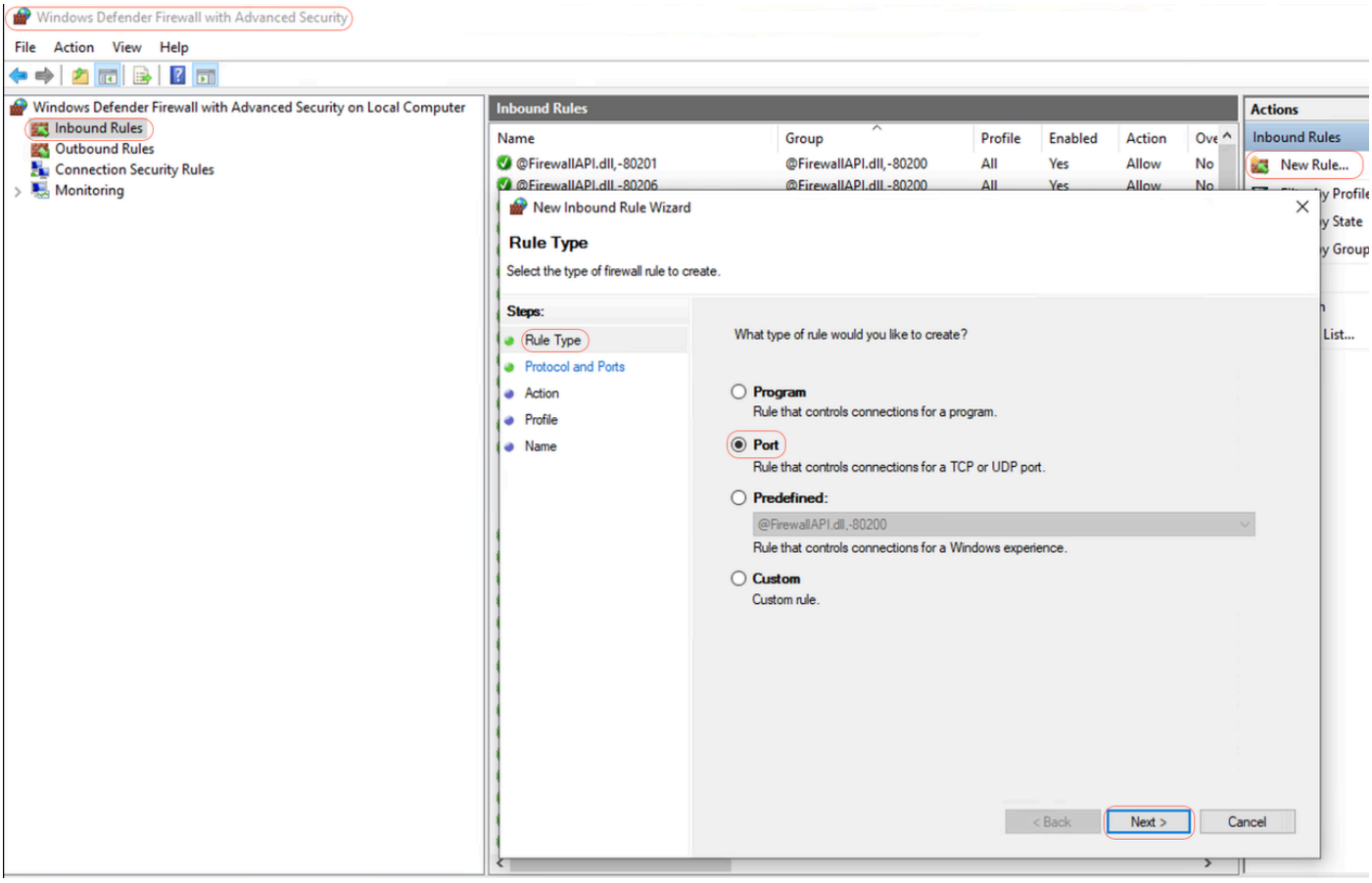
El resultado que se muestra en esta captura de pantalla indica que la conexión TCP al puerto 5985 en localhost falló. Esto significa que el servicio WinRM (Administración remota de Windows), que utiliza el puerto 5985, no se está ejecutando o no está configurado correctamente.

```
PS C:\Windows\system32> Test-NetConnection -Computer localhost -Port 5985
WARNING: TCP connect to (::1 : 5985) failed
WARNING: TCP connect to (127.0.0.1 : 5985) failed


ComputerName            : localhost
RemoteAddress           : ::1
RemotePort              : 5985
InterfaceAlias          : Loopback Pseudo-Interface 1
SourceAddress           : ::1
PingSucceeded           : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False



PS C:\Windows\system32> ^C
```

Connection failed to WinRM

Creación de reglas de entrada para permitir PowerShell en el puerto 5985

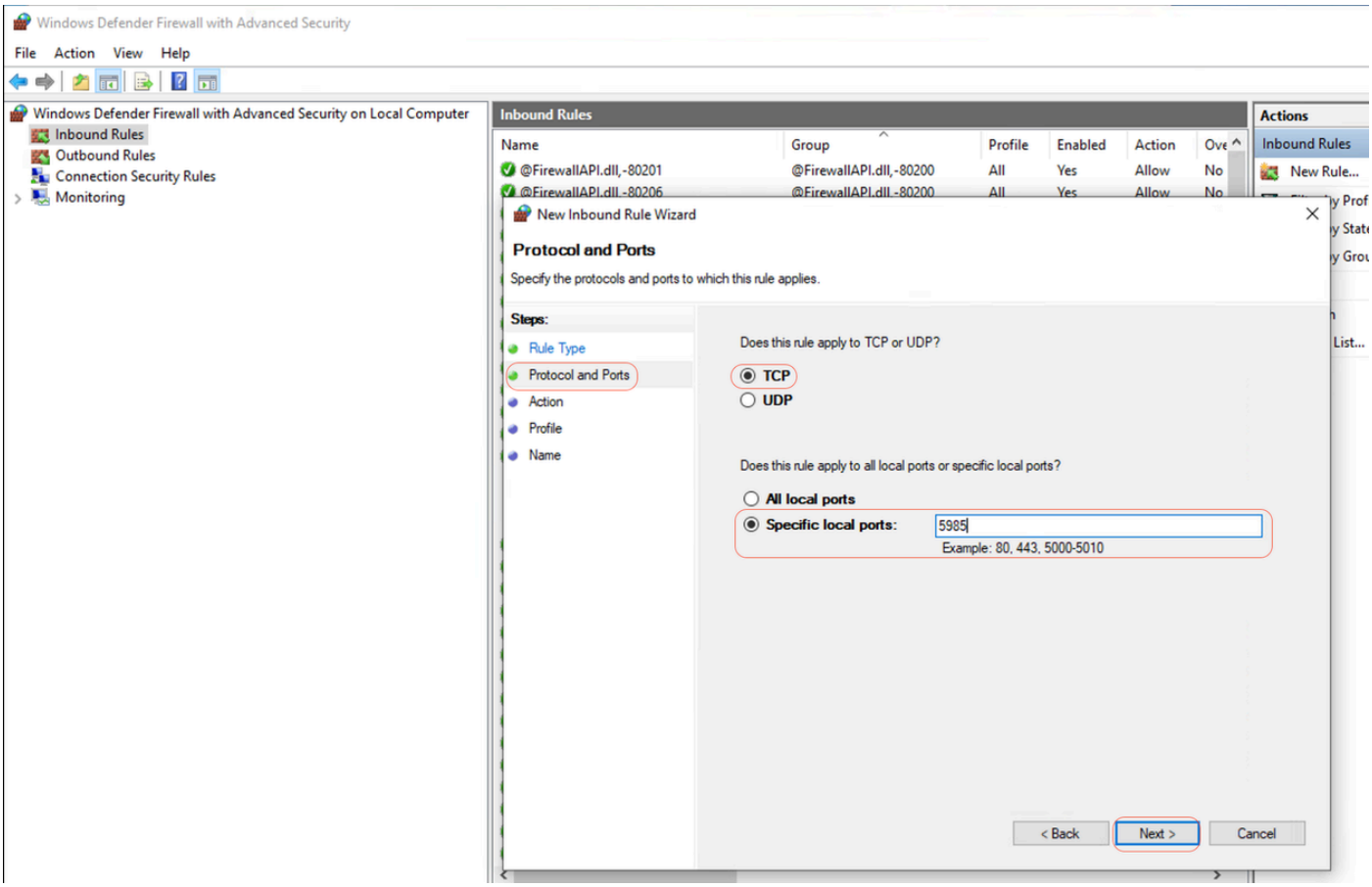
Paso 1- En la GUI de Windows, vaya a la barra de búsqueda, escriba Firewall de Windows con seguridad avanzada, haga clic en él y seleccione Ejecutar como administrador > Reglas de entrada > Nueva regla > Tipo de regla > Puerto > Siguiente:



Nueva regla de entrada: puerto

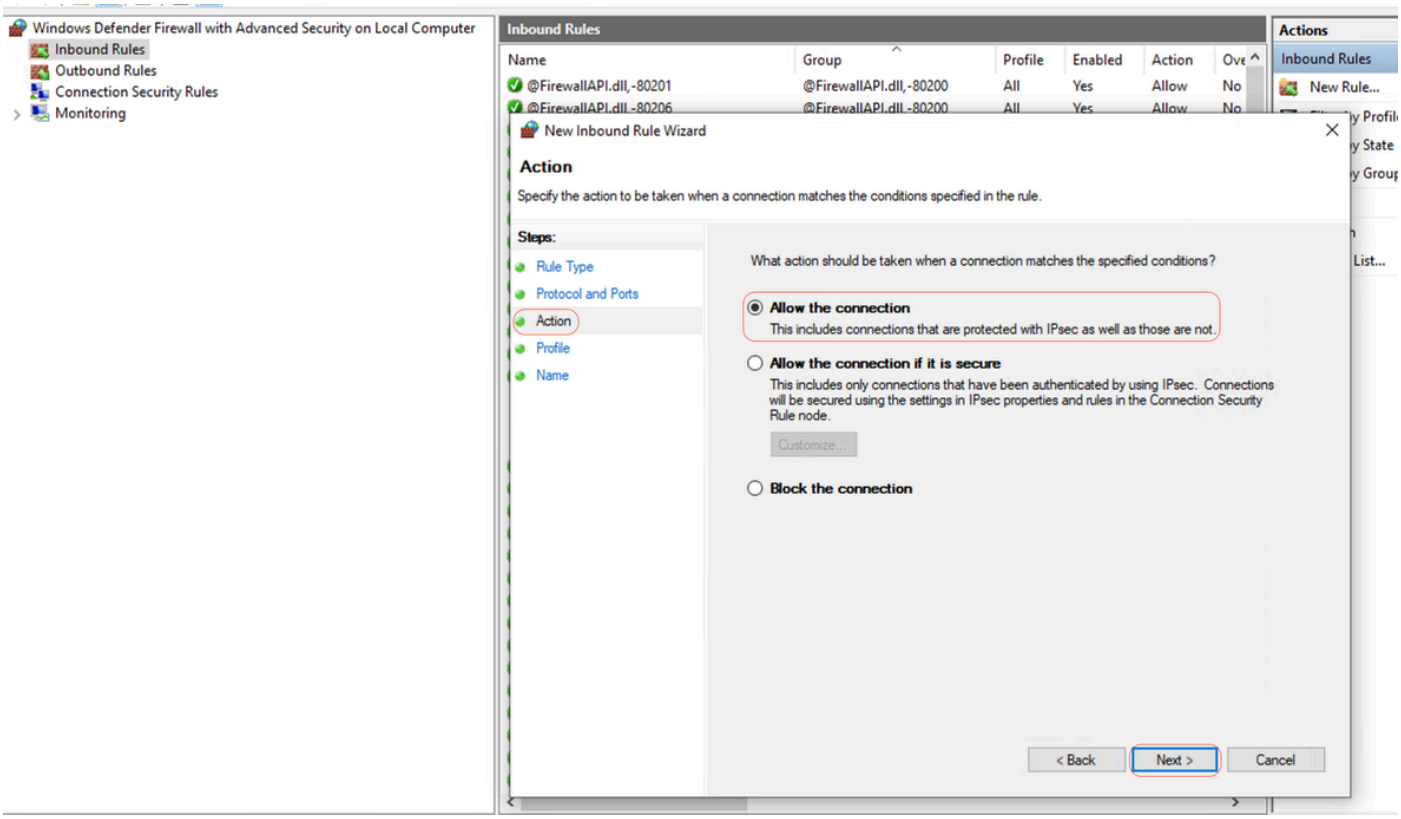
Paso 2: en Protocolos y puertos, seleccione TCP y Especificar puertos locales, escriba el número

de puerto 5985 (Puerto predeterminado para la comunicación remota de PowerShell) y haga clic en Siguiente:



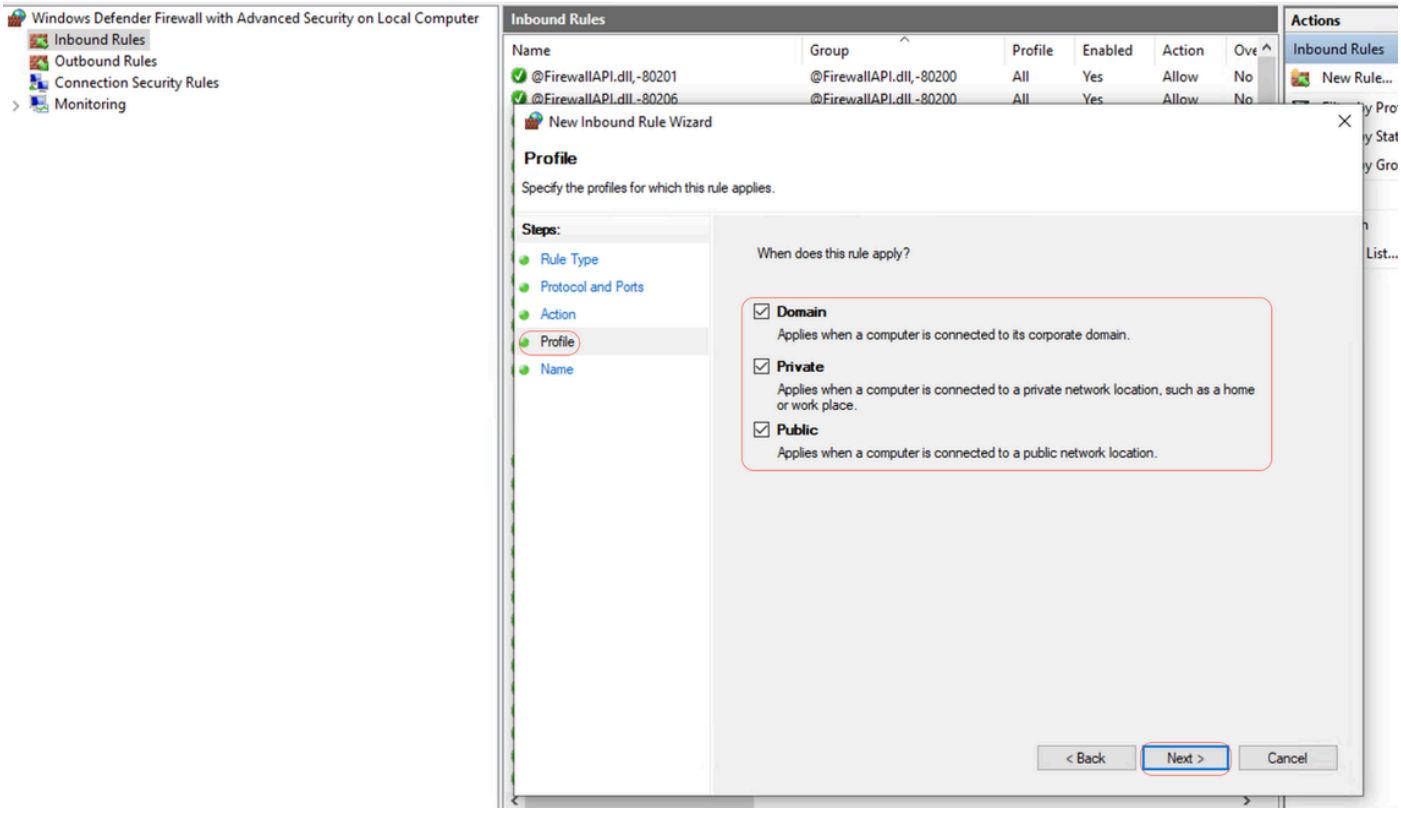
Protocolos y puertos

Paso 3- Bajo Acción > Seleccione Permitir la conexión > Siguiente:



Acción

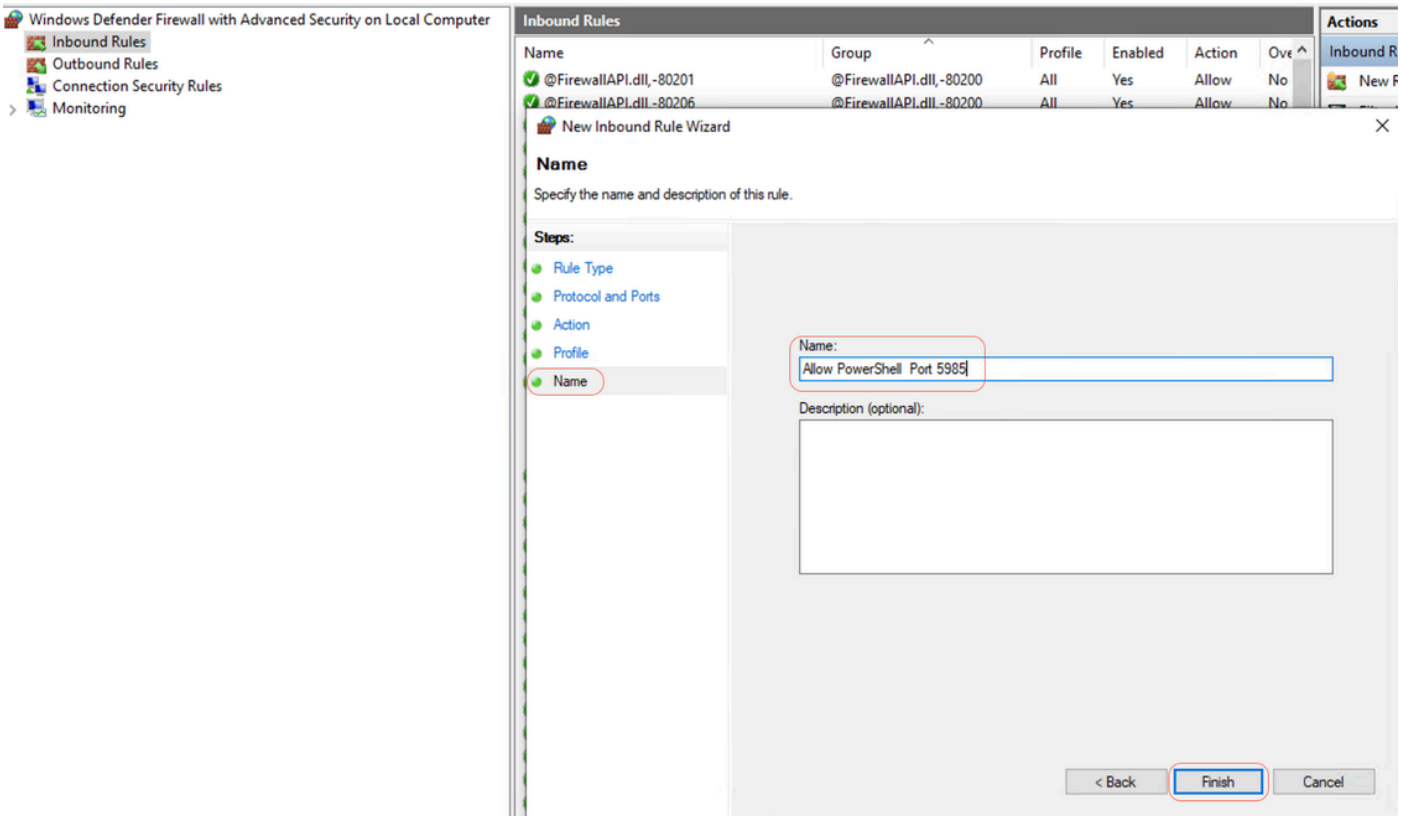
Paso 4 - En Perfil, marque las casillas de verificación Dominio, Privado, y Público y haga clic en Siguiente:



Perfil

Paso 5- En Nombre, ingrese un nombre para la regla, como Permitir PowerShell en el puerto

5985 y haga clic en Finalizar:

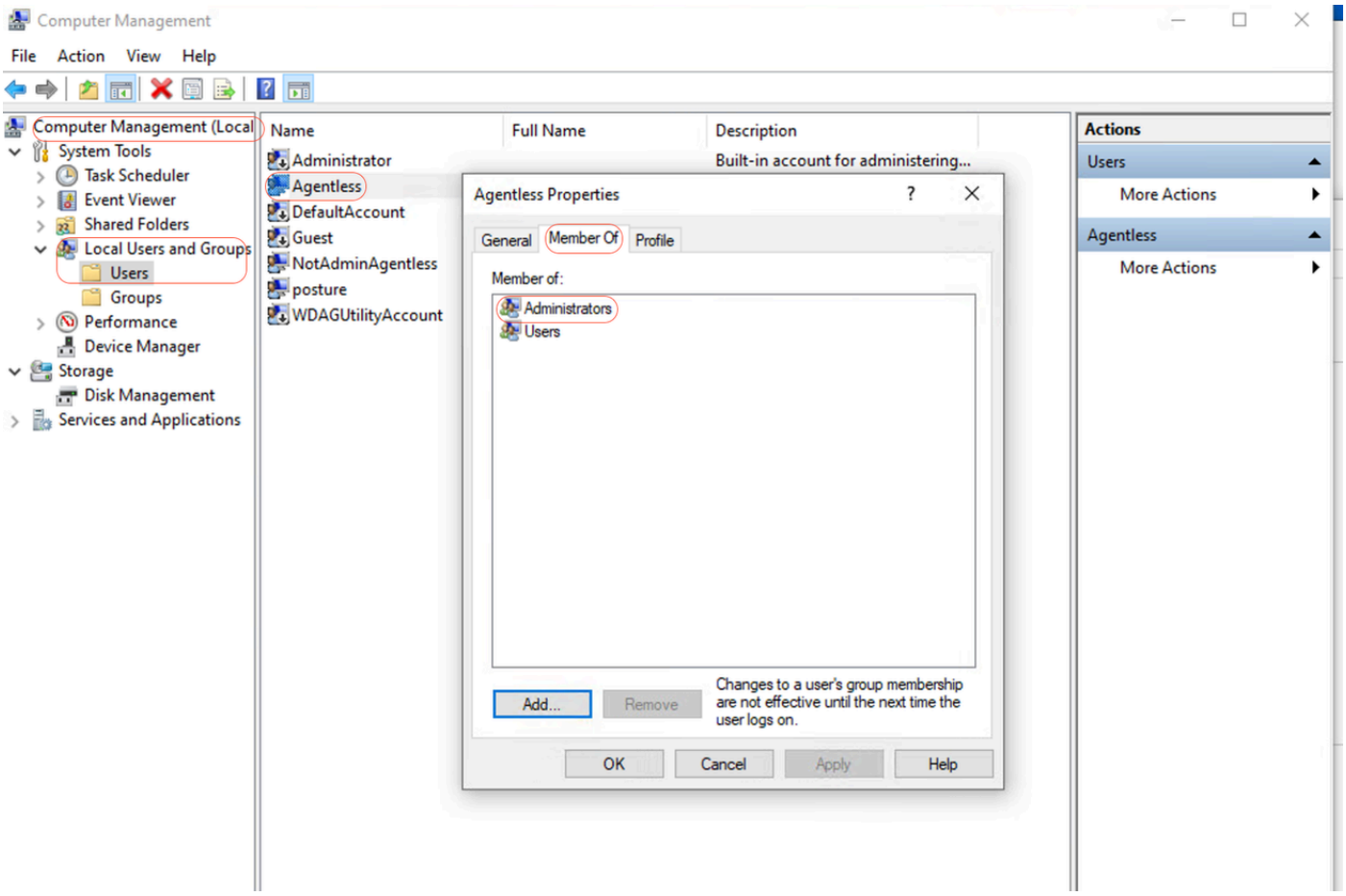


Nombre

Las credenciales del cliente para el inicio de sesión del shell deben tener privilegios de administrador local

Las credenciales del cliente para el inicio de sesión del shell deben tener privilegios de administrador local. Para confirmar si tiene privilegios de administrador, siga estos pasos:

En la GUI de Windows, vaya a Configuración > Administración de equipos > Usuarios y grupos locales > Usuarios > Seleccione la cuenta de usuario (en este ejemplo, la opción Cuenta sin agente está seleccionada) > Miembro de, la cuenta debe tener el grupo Administradores.



Privilegios de administrador local

Validando agente de escucha WinRM

Asegúrese de que el receptor WinRM esté configurado para HTTP en el puerto 5985:

C: \Windows\system32> **winrm enumerate winrm/config/listener** Listener Address = * **Transport = HTTP Port = 5985** Hostname Enabled = true URLPrefix = wsman CertificateThumbprint C: \Windows\system32>

Habilitar PowerShell Remoting WinRM

Para asegurarse de que el servicio se está ejecutando y configurado para iniciarse automáticamente, siga estos pasos:

Enable the WinRM service **Enable-PSRemoting -Force** # Start the WinRM service **Start-Service WinRM** # Set the WinRM service to start automatically **Set-Service -Name WinRM -StartupType Automatic**

Resultado esperado:

C: \Windows\system32> **Enable-PSRemoting -Force** WinRM is already set up to receive requests on this computer. WinRM has been updated for remote management. WinRM firewall exception enabled. -Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

C: \Windows\system32> **Start-Service WinRM**

C: \Windows\system32> **Set-Service -Name WinRM -StartupType Automatic**

Powershell debe ser v7.1 o posterior. El cliente debe tener cURL v7.34 o posterior:

Cómo comprobar las versiones de PowerShell y cURL en Windows

Asegurarse de que está utilizando las versiones adecuadas de PowerShell ; cURL es esencial para Posture Agentless:

Comprobando versión de PowerShell

En Windows:

1. Abrir PowerShell:

· Presione Win + X y seleccione Windows PowerShell o Windows PowerShell (Admin).

2. Ejecute el comando:$PSVersionTable.PSVersion

· Este comando genera los detalles de la versión de PowerShell instalada en el sistema.

Comprobando versión de cURL

En Windows:

1. Abrir símbolo del sistema:

· Presione Win + R, escriba cmd y haga clic en Enter.

2. Ejecute el comando: curl --version

· Este comando muestra la versión de cURL instalada en su sistema.

Resultado para comprobar las versiones de PowerShell y cURL en dispositivos Windows

C: \Windows\system32> **$PSVersionTable.PSVersion** Major Minor Build Revision ----- ----- ----- ----- 7 1 19041 4291

C: \Windows\system32>

C: \Windows\system32>

C: \Windows \system32>**curl --version curl 8.4.0 (Windows) libcurl/8.4.0 Schannel WinIDN** Release-Date: 2023-10-11 Protocols: dict file ftp ftps http https imap imaps pop3 pop3s smtp smtps telnet tftp ftps http https Features: AsynchNS HSTS HTTPS-proxy IDN IPv6 Kerberos Largefile NTLM SPNEGO SSL SSPI threadsafe Unicode UnixSockets c: \Windows\system32>

Configuración adicional

Este comando configura el equipo para que confíe en hosts remotos específicos para conexiones WinRM: Set-Item WSMan:\localhost\Client\TrustedHosts -Value

C: \Windows\system32> **Set-Item WSMan:\localhost\Client\TrustedHosts -Value x.x.x.x** WinRM Security Configuration. This command

modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list cannot be authenticated. The client can send credential information to these computers. Are you sure that you want to modify this list? [Y] Yes [N] No [S] Suspend [?] Help (default is "y"): **Y** PS C: \Windows \system32> -

El cmdlet test-wsman con los parámetros -Authentication Negotiate y -Credential es una herramienta eficaz para comprobar la disponibilidad y la configuración del servicio WinRM en un equipo remoto: test-wsman

-Authentication Negotiate -Credential

MacOS

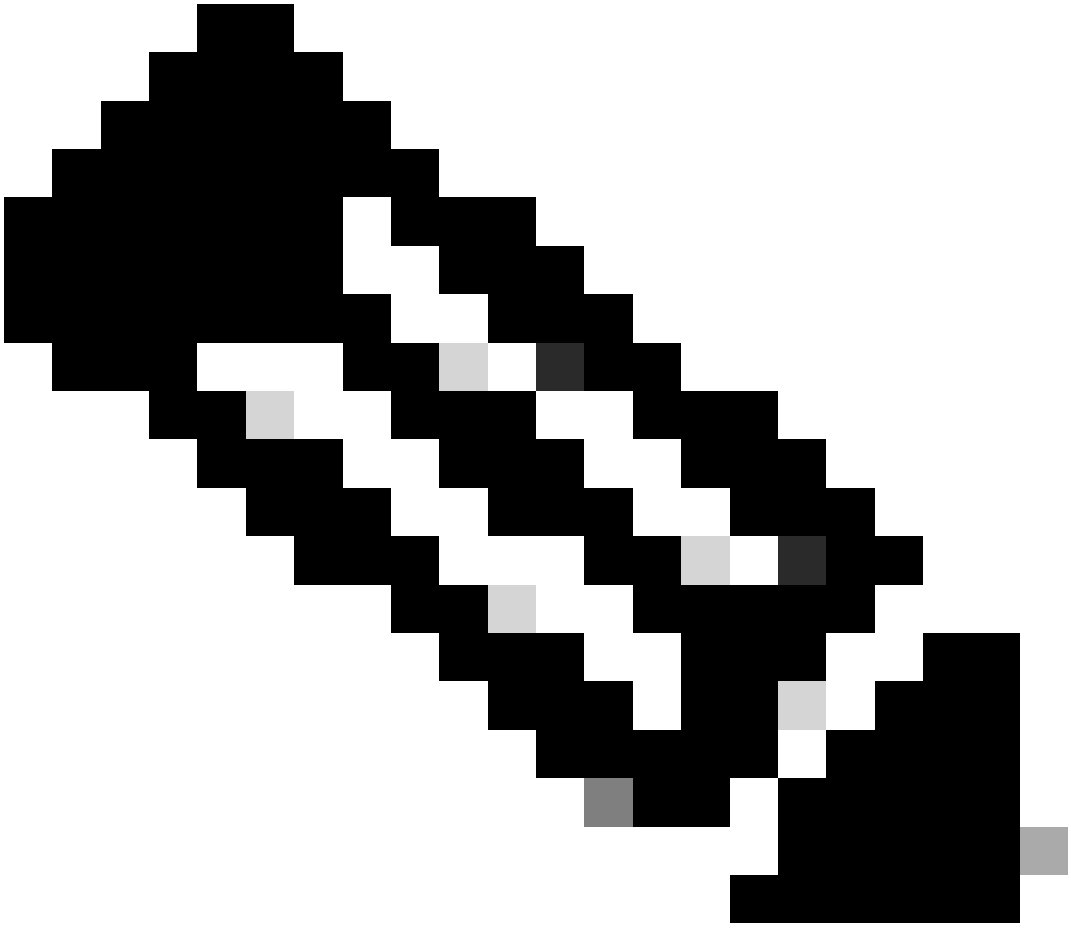
Powershell debe ser v7.1 o posterior. El cliente debe tener cURL v7.34 o posterior:

En macOS:

1. Terminal abierto:

· Puede encontrar Terminal en Aplicaciones > Utilidades.

2. Ejecute el comando: pwsh -Command '$PSVersionTable.PSVersion'



Nota: Nota: · Asegúrese de tener PowerShell Core (pwsh) instalado. Si no es así, puede instalarlo a través de Homebrew (asegúrese de que tiene Himebrew instalar): brew install --cask powershell

En macOS:

1. Terminal abierto:

· Puede encontrar Terminal en Aplicaciones > Utilidades.

2. Ejecute el comando: curl --version

· Este comando debe mostrar la versión de cURL instalada en su sistema.

Para clientes MacOS, el puerto 22 para acceder a SSH debe estar abierto para acceder al cliente

Guía paso a paso:

1. Preferencias del sistema abierto:

· Vaya a Preferencias del sistema desde el menú Apple.

2. Activar inicio de sesión remoto:

· Vaya a Compartir.

· Marque la casilla junto a Inicio de sesión remoto.

· Asegúrese de que la opción Permitir acceso para esté establecida en los usuarios o grupos adecuados. Al seleccionar All users, cualquier usuario con una cuenta válida en el Mac puede iniciar sesión a través de SSH.

3. Verifique la configuración del firewall:

· Si el firewall está habilitado, debe asegurarse de que permite conexiones SSH.

· Vaya a Preferencias del sistema > Seguridad y privacidad > Firewall.

· Haga clic en el botón Opciones de firewall.

· Verifique que Remote Login o SSH aparezcan en la lista y estén permitidos. Si no aparece en la lista, haga clic en el botón Agregar (+) para agregarlo.

4. Puerto abierto 22 vía terminal (si es necesario):

· Abra la aplicación Terminal desde Applications > Utilities.

· Utilice el comando pfctl para verificar las reglas de firewall actuales y asegúrese de que el puerto 22 esté abierto:sudo pfctl -sr | grep 22

· Si el puerto 22 no está abierto, puede agregar manualmente una regla para permitir SSH: echo "pass in proto tcp from any to any port 22" | sudo pfctl -ef -

5. Prueba de acceso SSH:

· Desde otro dispositivo, abra un terminal o un cliente SSH.

· Intente conectarse al cliente macOS usando su dirección IP:ssh username@<macOS-client-IP>

· Reemplace username con la cuenta de usuario apropiada y <macOS-client-IP> con la dirección IP del cliente macOS.

Para MacOS, asegúrese de actualizar esta entrada en el archivo sudoers para evitar que se produzca un error en la instalación del certificado en los terminales:

Al administrar los terminales macOS, es crucial asegurarse de que se puedan ejecutar comandos administrativos específicos sin requerir una solicitud de contraseña.

Prerequisites

· Acceso de administrador en la máquina macOS.

· Familiaridad básica con los comandos de Terminal.

Pasos para actualizar el archivo Sudoers

1. Terminal abierto:

· Puede encontrar Terminal en Aplicaciones > Utilidades.

2. Edite el archivo Sudoers:

· Utilice el comando visudo para editar de forma segura el archivo sudoers. Esto garantiza que cualquier error de sintaxis se detecta antes de guardar el archivo.sudo visudo

· Se le pedirá que introduzca la contraseña de administrador.

3. Encuentre la sección adecuada:

· En el editor de visudo, navegue hasta la sección donde se definen las reglas específicas del usuario. Normalmente, se encuentra hacia la parte inferior del archivo.

4. Añada la entrada necesaria:

· Agregue esta línea para otorgar al usuario especificado permiso para ejecutar los comandos security y osascript sin una contraseña:

```
ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
```

· Reemplace <macadminusername> por el nombre de usuario real del administrador de macOS.

5. Guardar y salir:

· Si está utilizando el editor predeterminado (nano), presione Ctrl + X para salir, luego presione Y para confirmar los cambios y finalmente presione Enter para guardar el archivo.

· Si utiliza vi o vim, pulse Esc, escriba :wq y pulse Enterpara guardar y salir.

6. Verifique los cambios:

· Para asegurarse de que los cambios han surtido efecto, puede ejecutar un comando que requiera los permisos de sudo actualizados. Por ejemplo:

```
sudo /usr/bin/security find-certificate -a sudo /usr/bin/osascript -e 'tell application "Finder" to display dialog "Test"'
```

· Estos comandos se pueden ejecutar sin solicitar una contraseña.

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).