Configurar postura sem agente

Contents

Introdução

Este documento descreve como configurar o Posture Agentless no ISE e o que é necessário no

endpoint para executar o script sem agente.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity Services Engine (ISE).
- Postura.
- PowerShell e SSH
- Windows 10 ou posterior.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity Services Engine (ISE) versão 3.3.
- Pacote CiscoAgentlessWindows 5.1.6.6
- Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A postura do ISE executa uma avaliação do cliente. O cliente recebe a política de requisitos de postura do ISE, realiza a coleta de dados de postura, compara os resultados com a política e envia os resultados da avaliação de volta ao ISE.

Em seguida, o ISE determina se o dispositivo está em conformidade ou não com base no relatório de postura.

A postura sem agente é um dos métodos de postura que reúne informações de postura de clientes e se remove automaticamente após a conclusão, sem exigir qualquer ação do usuário final. A postura sem agente conecta-se ao cliente usando privilégios administrativos.

Getting Started

Pré-requisitos:

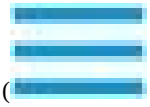
- O cliente deve estar acessível por meio de seu endereço IPv4ou IPv6, e esse endereço IP deve estar disponível na contabilidade RADIUS.

- O cliente deve estar acessível do Cisco Identity Services Engine (ISE) através de seu endereço IPv4 ou IPv6. Além disso, esse endereço IP deve estar disponível na contabilidade RADIUS.
- Clientes Windows e Mac são atualmente suportados:
    - Para clientes Windows, a porta 5985 para acessar o powershell no cliente deve estar aberta. O Powershell deve ser v7.1 ou posterior. O cliente deve ter cURL v7.34 ou posterior.
    - Para clientes MacOS, a porta 22 para acessar o SSH deve estar aberta para acessar o cliente. O cliente deve ter cURL v7.34 ou posterior.
- As credenciais do cliente para o logon do shell devem ter privilégios de administrador local.
- Execute a atualização do feed de postura para obter os clientes mais recentes, conforme descrito nas etapas de configuração. Verifique:
- Para MacOS, certifique-se de que esta entrada seja atualizada no arquivo sudoers para evitar falha de instalação de certificado nos pontos finais: Por favor verifique:

<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

•

Para MacOS, a conta de usuário configurada deve ser uma conta de administrador. A postura sem agente para MacOS não funciona com



nenhum outro tipo de conta, mesmo que você conceda mais privilégios.Para exibir essa janela, clique no ícone Menuicon ( ) e **escolhaAdministração > Sistema >** Configurações > **Scripts de endpoint** > Logon **Configuração >** Usuário local MAC**.**

•

No caso de alterações em atividades relacionadas a portas em clientes Windows devido a atualizações da Microsoft, é necessário reconfigurar o fluxo de trabalho de configuração de postura sem agente para clientes Windows.

Condições de postura suportadas

•

Condições de arquivo, exceto as condições que usam os caminhos de arquivo USER_DESKTOP e USER_PROFILE

•

Condições de serviço, exceto verificações do daemon e daemon do sistema ou agente do usuário no macOS

- Condições de aplicação
- Condições da Fonte de Dados Externa
- Condições compostas
- Condições antimalware
- Condição de gerenciamento de patches, exceto **as** verificações de condição **EnabledandUp To**
- Condições de firewall
- Condições de criptografia de disco, exceto a verificação de condição baseada no local de criptografia
- Condições do Registro, exceto as condições que usam HCSK como chave raiz

Condições de postura não suportadas

- Correção
- Período de carência

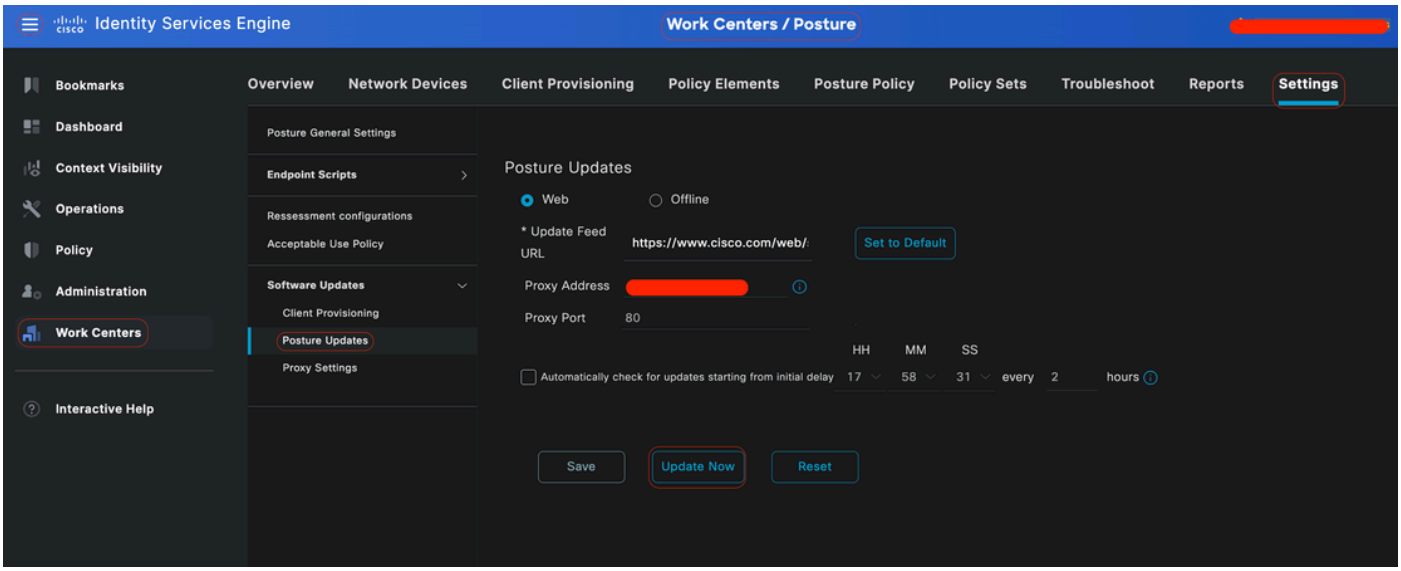
- Reavaliação periódica
- Política de uso aceitável

Configuração do ISE

Atualizar feed de postura

É recomendável atualizar o Feed de postura antes de começar a configurar o Posture.

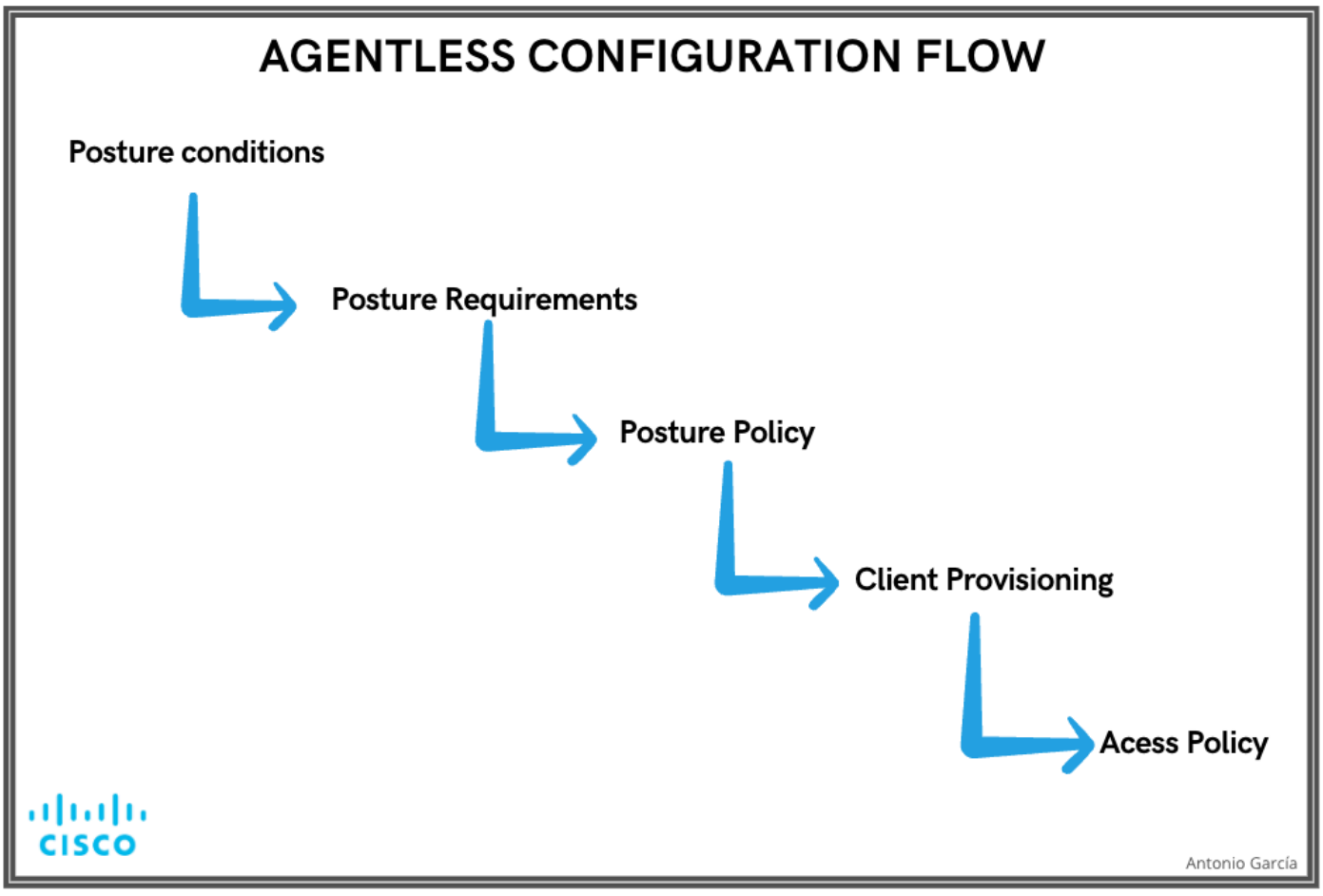
Na GUI do Cisco ISE, clique no ícone Menuicon () e escolha **Work Centers > Posture >** Settings > Software Updates > Update Now.



Atualizando feed de postura

Fluxo de configuração sem agente de postura

A opção Sem agente de postura deve ser configurada para que a primeira configuração seja necessária para a próxima e assim por diante. Observado que a correção não está no fluxo; no entanto, posteriormente, este documento abordará uma alternativa para configurar a correção.



Fluxo de configuração sem agente

Configuração de postura sem agente

Condição de postura

Condições de postura são o conjunto de regras em nossa política de segurança que definem um endpoint compatível. Alguns desses itens incluem a instalação de um firewall, software antivírus, antimalware, hotfixes, criptografia de disco e muito mais.

Na GUI do Cisco ISE, clique no ícone Menuicon () e escolha **Centros de trabalho > Postura >** Elementos de política > Condições, clique em Adicionar e crie uma ou mais condições de Postura **que usam postura sem agente para identificar o requisito.** Quando a **condição** for criada, clique em **Salvar**.

Neste cenário, uma condição de aplicativo chamada **"Agentless_Condition_Application"** foi configurada com estes parâmetros:

· **Sistema operacional:** Todos no Windows

Essa condição se aplica a qualquer versão do sistema operacional Windows, garantindo ampla compatibilidade entre diferentes ambientes Windows.

· **Verificar por:** Processo

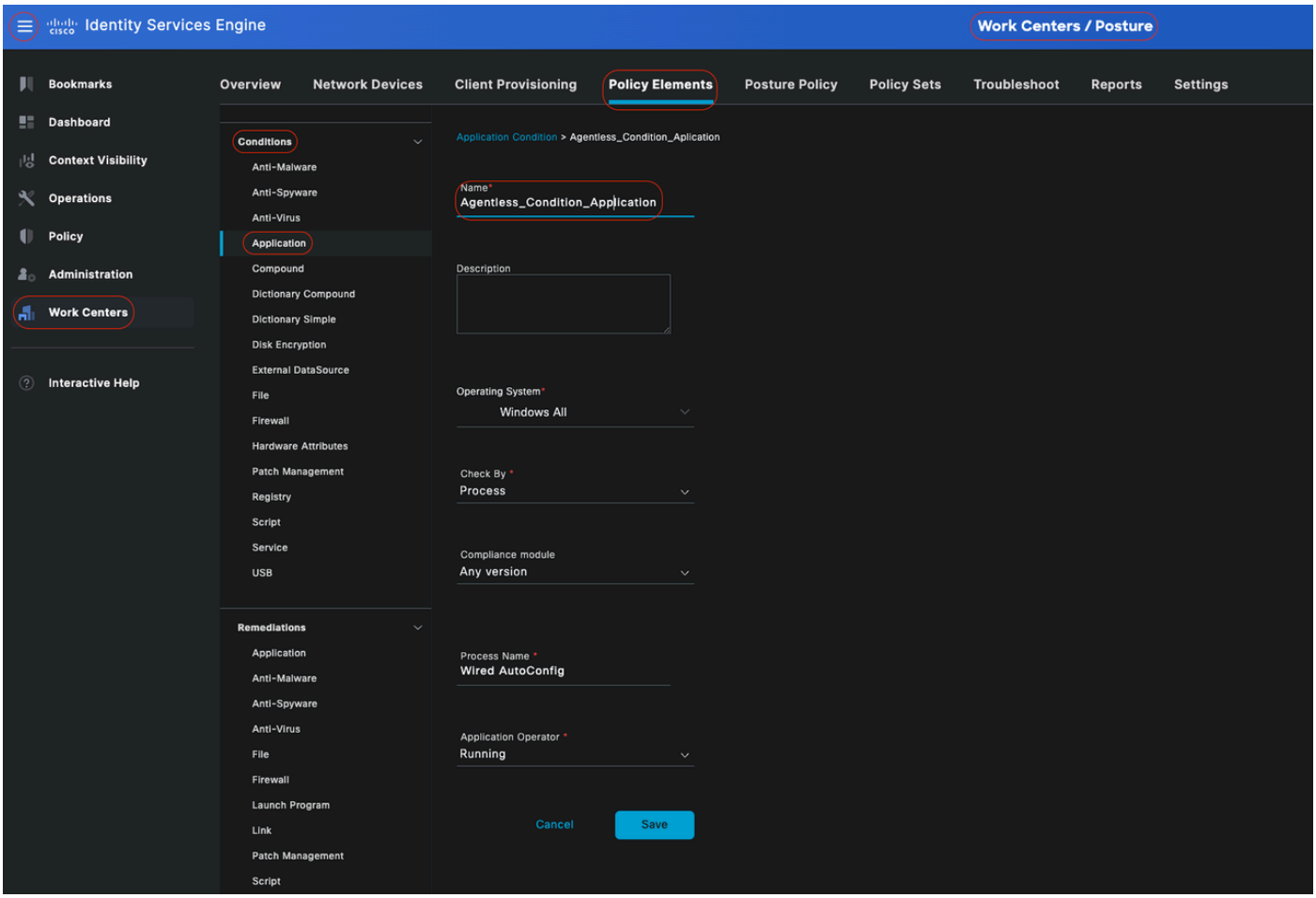
O sistema monitora processos dentro do dispositivo. Você tem a opção de selecionar **Process** ou **Application**; neste caso, **Process** foi escolhido.

· **Nome do processo:** Configuração automática com fio

O processo **Wired AutoConfig** é o módulo compatível com o processo que fará o check-in do dispositivo. Esse processo é responsável por configurar e gerenciar conexões de rede com fio, incluindo a Autenticação IEEE 802.1X.

· **Operador de aplicativos:** Execução

O módulo de conformidade verifica se o processo de **configuração automática com fio** está em execução no dispositivo. Você tem a opção de selecionar **Running** ou **Not Running**. Neste exemplo, **Running** foi selecionado para garantir que o processo está ativo.



Condição sem agente

Requisito de postura

Um requisito de postura é um conjunto de condições compostas ou apenas uma condição que pode ser vinculada a uma função e um sistema operacional. Todos os clientes que se conectam à sua rede devem atender aos requisitos obrigatórios durante a avaliação da postura para se tornarem compatíveis na rede.

Na GUI do Cisco ISE, clique no ícone do menu ( ) e escolha **Centros de trabalho > Postura** > **Política** Elementos > Requisito**.** Clique na seta para **baixo** e selecione **Inserir novo** requisito **e**

crie um ou mais Requisito que usam postura sem agente. Depois que o **requisito** for criado, clique em **Concluído** e em **Salvar**.

Nesse caso, um requisito de aplicativo chamado **"Agentless_Requirement_Application"** foi configurado com estes critérios:

· **Sistema operacional:** Todos no Windows

Esse requisito se aplica a qualquer versão do sistema operacional Windows, garantindo que seja aplicável em todos os ambientes Windows.

· **Tipo de postura:** sem agente

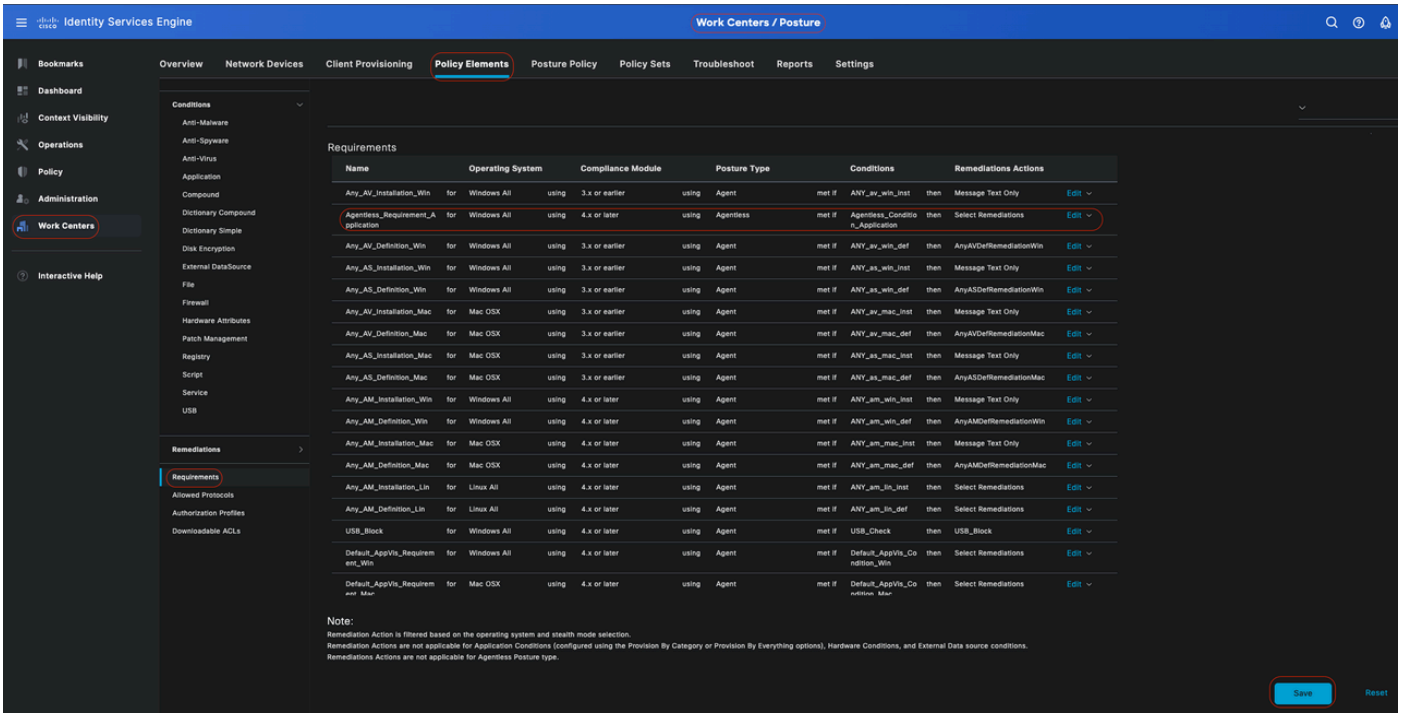
Essa configuração é definida para um ambiente sem agente. As opções disponíveis incluem **Agent**, **Agent Stealth**, **Temporal Agent** e **Agentless**. Neste cenário, **Agentless** foi selecionado.

· **Condições: Agentless_Condition_Application**

Isso especifica a condição que o ISE Posture Module e o Compliance Module verificarão nos processos do dispositivo. A condição selecionada é **Agentless_Condition_Application**.

· **Ações de correção:**

Como essa configuração é para um ambiente sem agente, as Ações de correção não são suportadas e esse campo fica esmaecido.



Requisito sem agente

Política de postura

Na GUI do Cisco ISE, clique no ícone do menu (

) e **escolhaWork** Centers **>** Posture > Posture **Policy.** Clique na **seta para baixo** e selecione **Inserir novo requisito**, e crie uma ou mais regras suportadas de **Postura**Política **que usem a postura sem agente para esse requisito de postura.** Quando a **Política de postura** for criada, clique em **Concluído** e em **Salvar**.

Neste cenário, uma política de postura chamada **"Agentless_Policy_Application"** foi configurada com estes parâmetros:

· **Nome da regra:** Agentless_Policy_Application

Este é o nome designado para a Política de postura neste exemplo de configuração.

· **Sistema operacional:** Todos no Windows

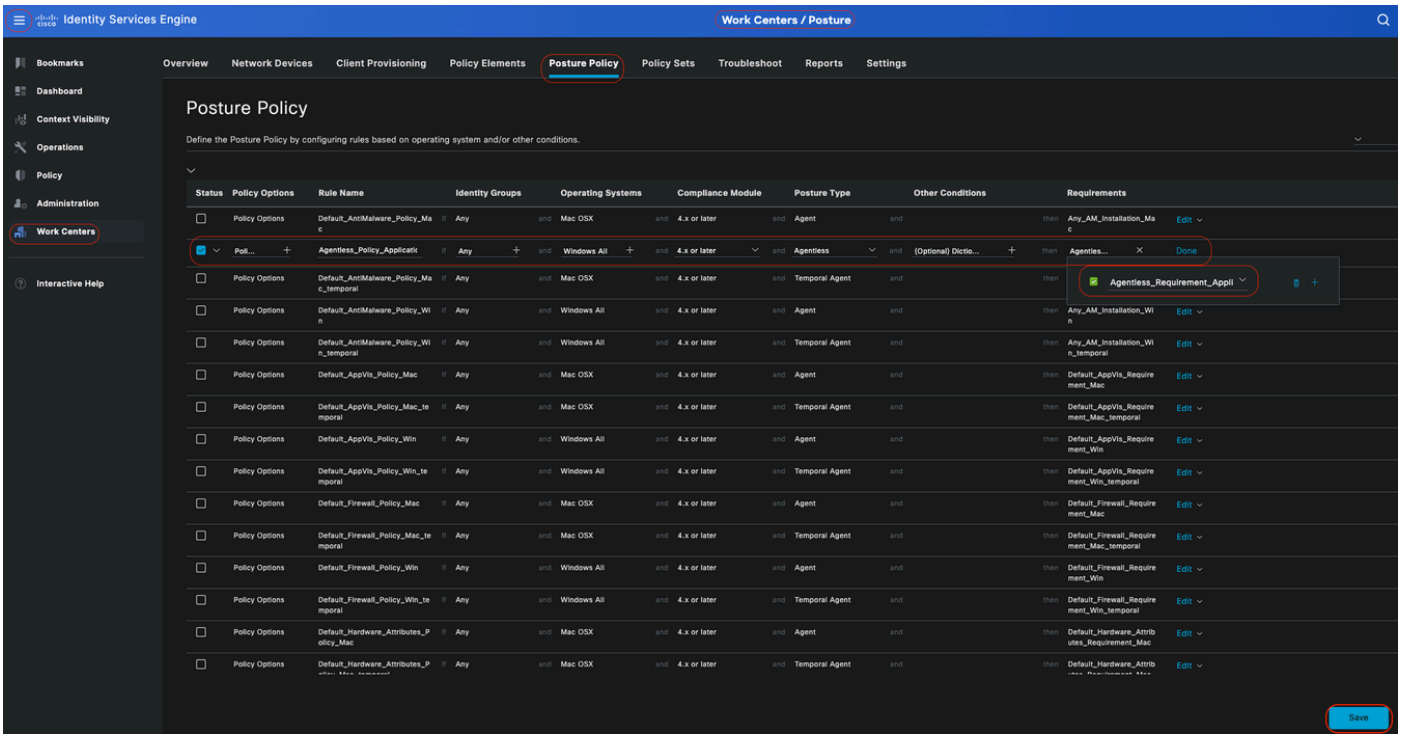
A política está definida para ser aplicada a todas as versões do sistema operacional Windows, garantindo ampla compatibilidade entre diferentes ambientes Windows.

· **Tipo de postura:** sem agente

Essa configuração é definida para um ambiente sem agente. As opções disponíveis incluem **Agent**, **Agent Stealth**, **Temporal Agent** e **Agentless**. Neste cenário, **Agentless** foi selecionado.

· **Outras condições:**

Neste exemplo de configuração, nenhuma condição adicional foi criada. No entanto, você tem a opção de configurar condições específicas para garantir que somente os dispositivos de destino estejam sujeitos a essa Política de postura, em vez de todos os dispositivos Windows na rede. Isso pode ser particularmente útil para segmentação de rede.



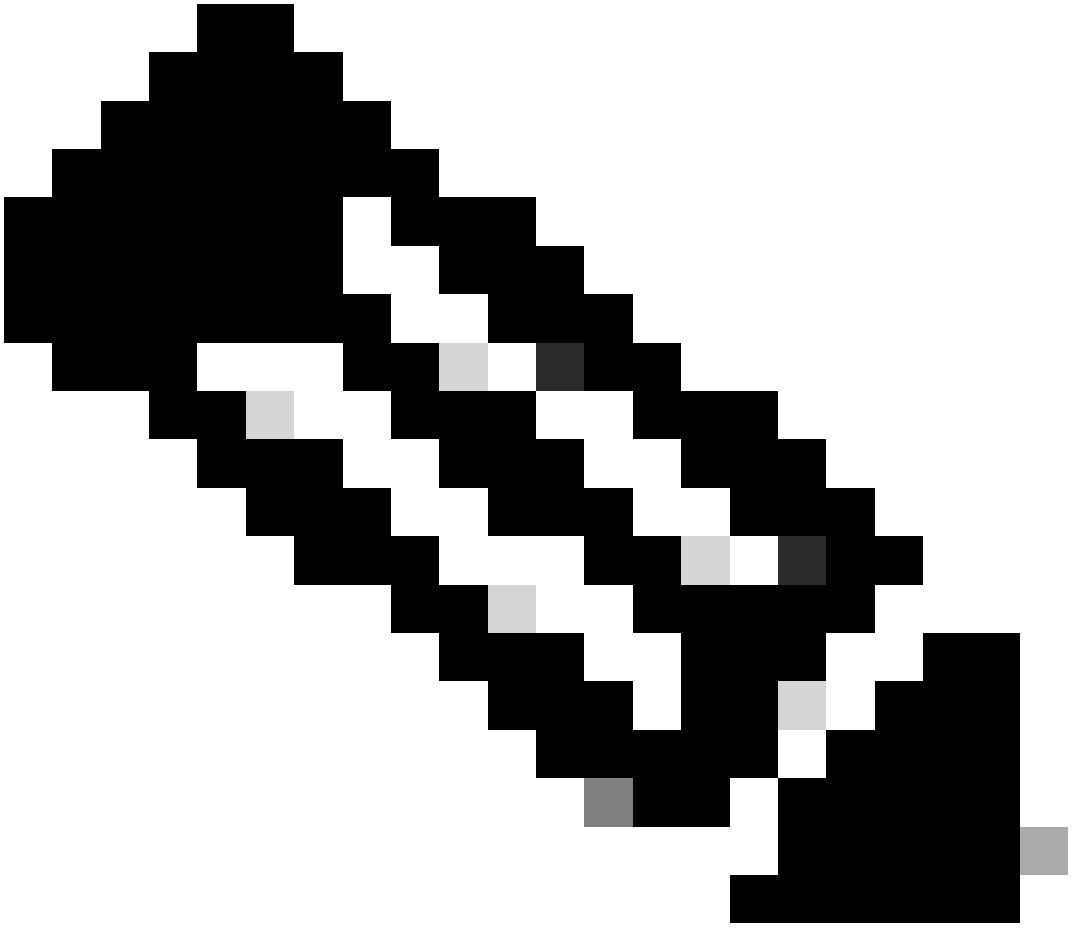
Política sem agente de postura

Provisionamento de clientes

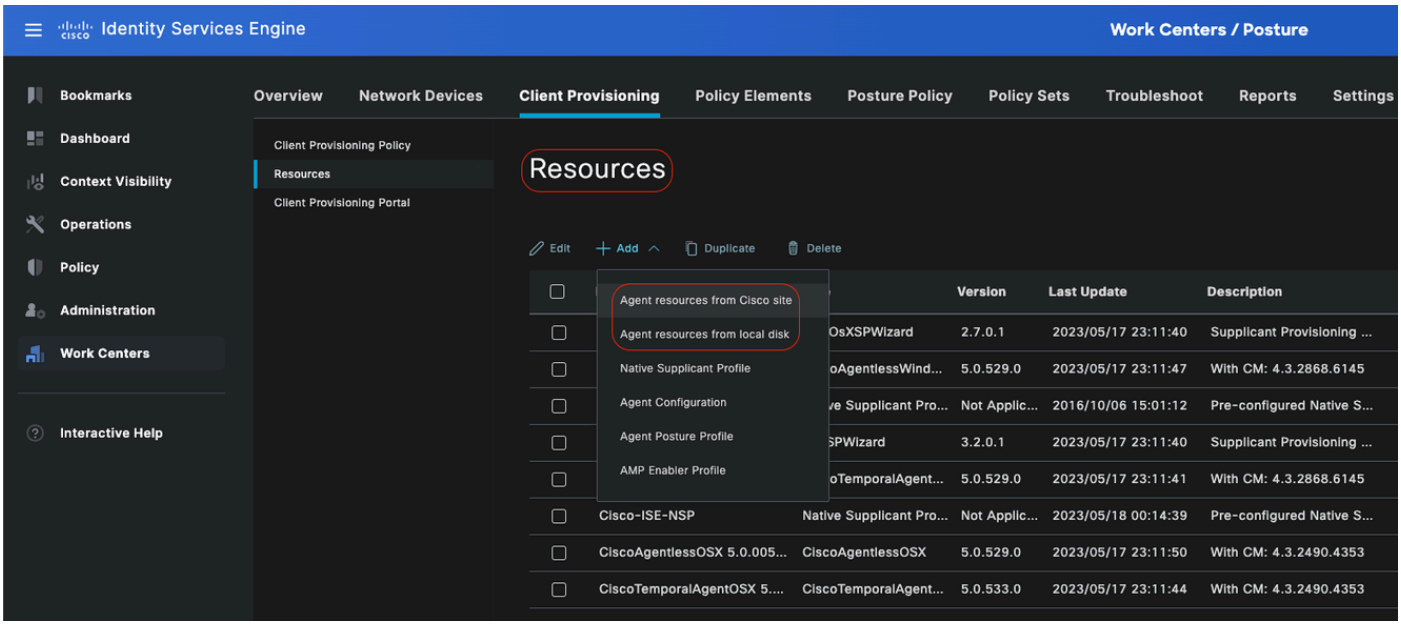
Etapa 1 - Baixar recursos

Para começar a configurar o provisionamento de clientes, você deve primeiro fazer o download dos recursos necessários e tê-los disponíveis no ISE para que possa usá-los posteriormente na Política de provisionamento de clientes.

Há duas maneiras de adicionar recursos ao ISE: **Recursos do agente do site da Cisco** e **Recursos do agente do disco local**. Como você está configurando o sem agente, é necessário passar por **Recursos de agente do site da Cisco** para fazer o download.



Observação: para usar esses **recursos de agente do site da Cisco**, o ISE PAN precisa de acesso à Internet.



Recursos

Recursos de agente do site da Cisco

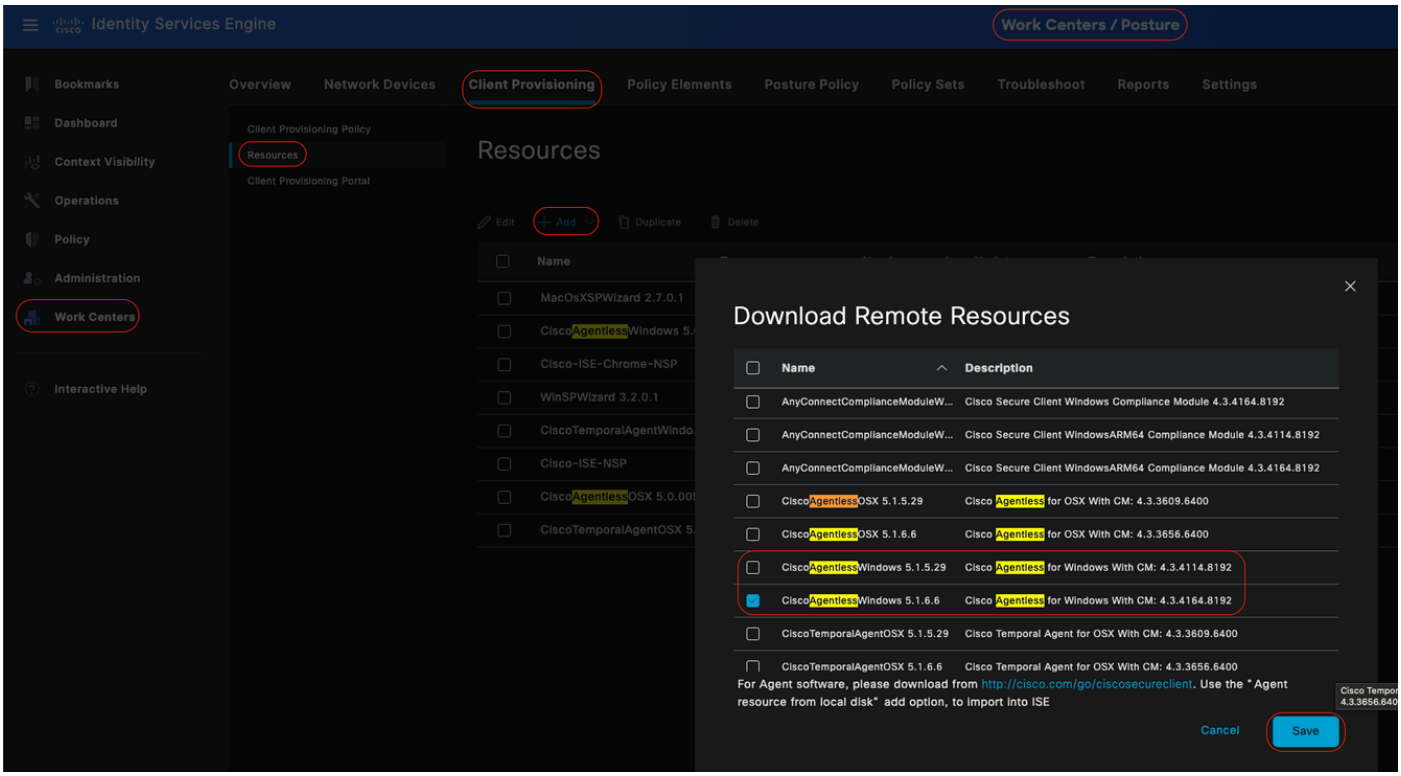
Na GUI do Cisco ISE, clique no ícone Menuicon (

) e escolha **Centros de trabalho** > Postura > Provisionamento de cliente > Recursos. Clique em **Adicionar** , selecione **Recursos do agente no site da Cisco** e clique em **Salvar**.

No site da Cisco, você só pode baixar o módulo de conformidade. O sistema mostra os dois módulos de conformidade mais recentes para download. O pacote de recursos **CiscoAgentlessWindows 5.1.6.6** está selecionado para este exemplo de configuração, que se destina apenas a dispositivos Windows.

.

Recursos do



agente do site da Cisco

Etapa 2 - Configurar a política de provisionamento do cliente

Ao configurar o Agente de postura, você precisa de dois recursos diferentes (**AnyConnect** ou **Secure Client** e **Módulo de conformidade**),

Mapeie ambos os recursos em **Configuração do agente** junto com o **Perfil de postura do agente** para que você possa usar essa **Configuração do agente** em sua **Política de provisionamento do cliente.**

No entanto, ao configurar o Posture Agentless, não há necessidade de configurar **Agent Configuration** ou **Agent Posture Profile**, em vez disso, você só pode baixar o pacote sem agente de **Agent Resources do site da Cisco**.

Na GUI do Cisco ISE, clique no ícone Menuicon ( ) e escolha **Centros de trabalho** > Postura > Provisionamento de cliente > Política de provisionamento de cliente. Clique na **seta para** baixo e selecione **Inserir nova política acima** ou **Inserir nova política abaixo**, **Duplicar acima** ou **Duplicar abaixo:**

- **Nome da regra: Agentless_Client_Provisioning_Policy**

Especifica o nome da Política de Provisionamento de Cliente.

- **Sistema operacional:** Todos no Windows

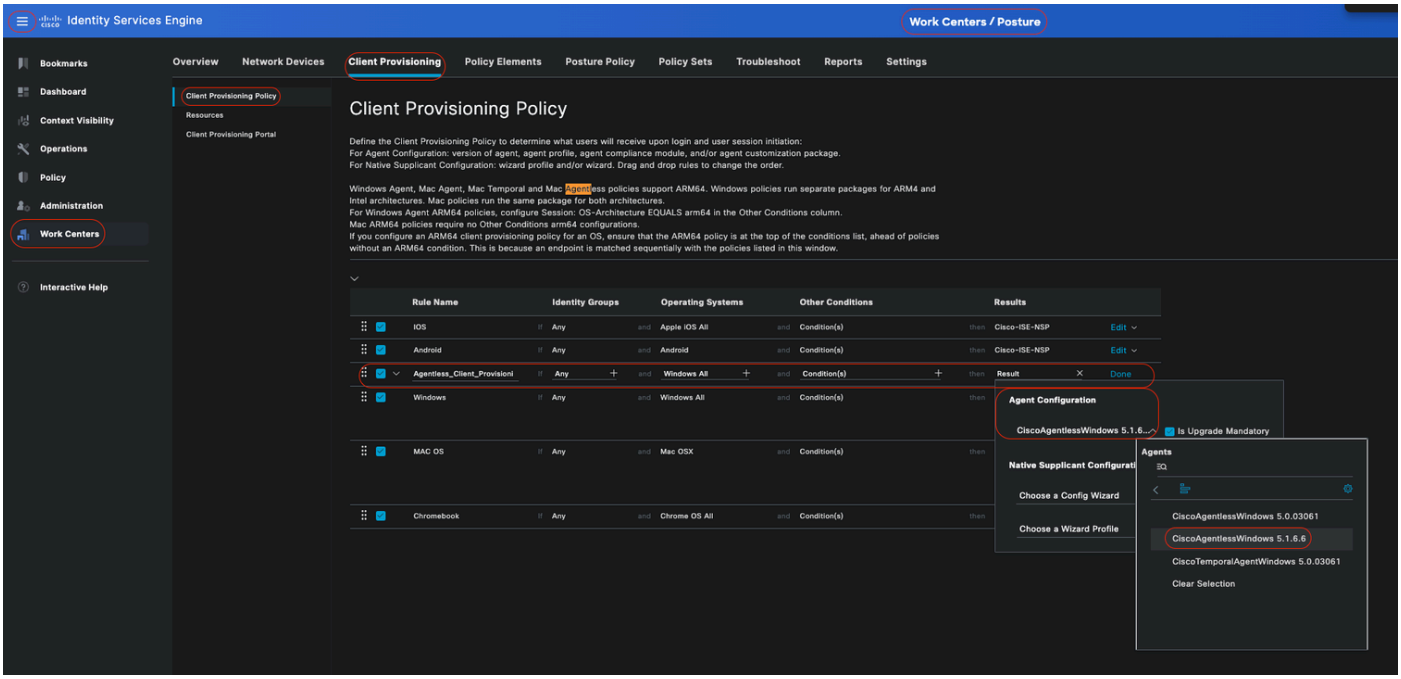
Isso garante que a política se aplique a todas as versões do sistema operacional Windows.

- **Outras Condições:** Nenhuma condição específica é configurada neste exemplo. No entanto, você pode configurar condições para garantir que somente os dispositivos desejados correspondam a esta Política de Provisionamento de Cliente, em vez de todos os dispositivos Windows na rede. Isso é particularmente útil para segmentação de rede.

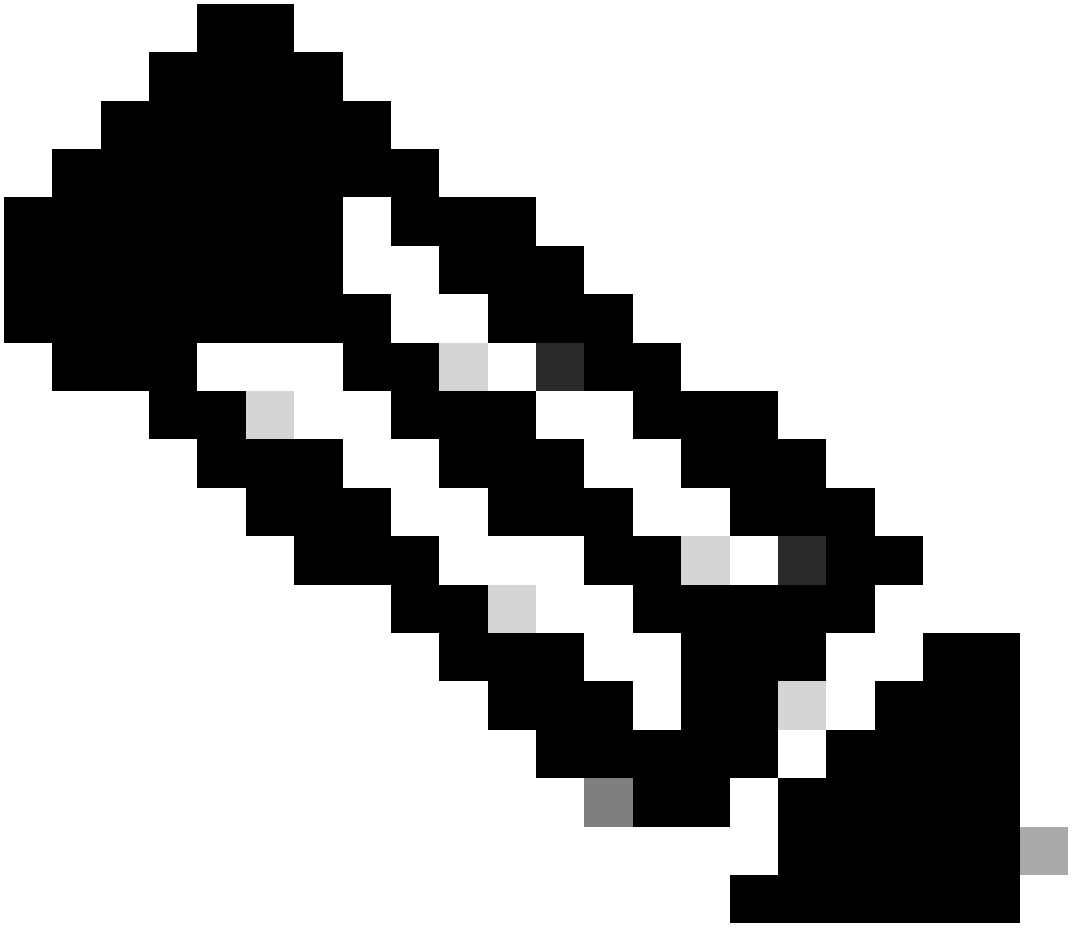
Exemplo: Se você estiver usando o Ative Diretory, poderá incorporar grupos do Ative Diretory à sua política para refinar quais dispositivos são afetados.

- **Resultados:** Selecione o pacote ou o agente de configuração apropriado. Como você está configurando o para um ambiente sem agente, escolha o pacote **CiscoAgentlessWindows 5.1.6.6**, que você baixou anteriormente do **Recursos do agente do site da Cisco**. Este pacote sem agente contém todos os recursos necessários (**Software sem agente** e **Módulo de conformidade**) necessários para que o Posture Agentless seja executado.

•Clique em Salvar



Política de provisionamento de cliente sem agente



Observação: certifique-se de que apenas uma Política de Provisionamento de Cliente satisfaça as condições para qualquer tentativa de autenticação. Se várias políticas forem avaliadas simultaneamente, isso pode levar a comportamentos inesperados e conflitos em potencial.

Perfil de **autorização sem agente**

Na GUI do Cisco ISE, clique no ícone Menuicon (

) e escolhaPolicy > Policy **Elements >** Results > **Authorization >** Authorization Profiles e crie um **Authorization** Profile **que avalie os resultados da Postura sem Agente.**

- Neste exemplo de configuração, chamado Perfil de autorização como **Agentless_Authorization_Profile**.

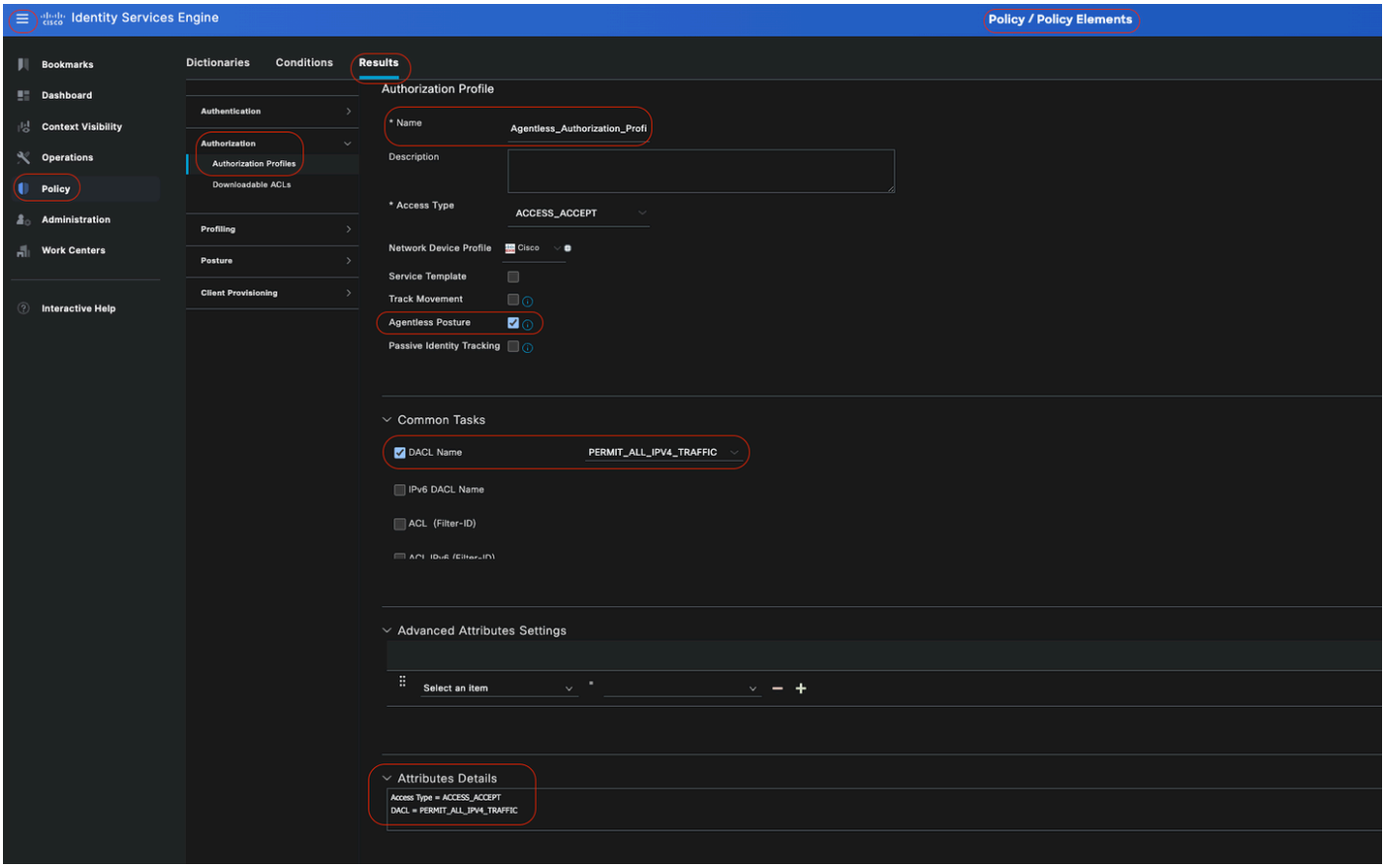
- Habilitar postura sem agente no perfil de autorização.

- Use este perfil somente para **Postura sem Agente**. Não o utilize também para outros tipos de postura.

- O CWA e a ACL de redirecionamento não são necessários para a postura sem agente. Você pode usar VLANs, DACLs ou ACLs como parte de suas regras de segmentação. Para simplificar, apenas um dACL (permitindo todo o tráfego ipv4) é configurado além da verificação de postura sem agente neste exemplo de configuração.

-

Clique em **Save**.



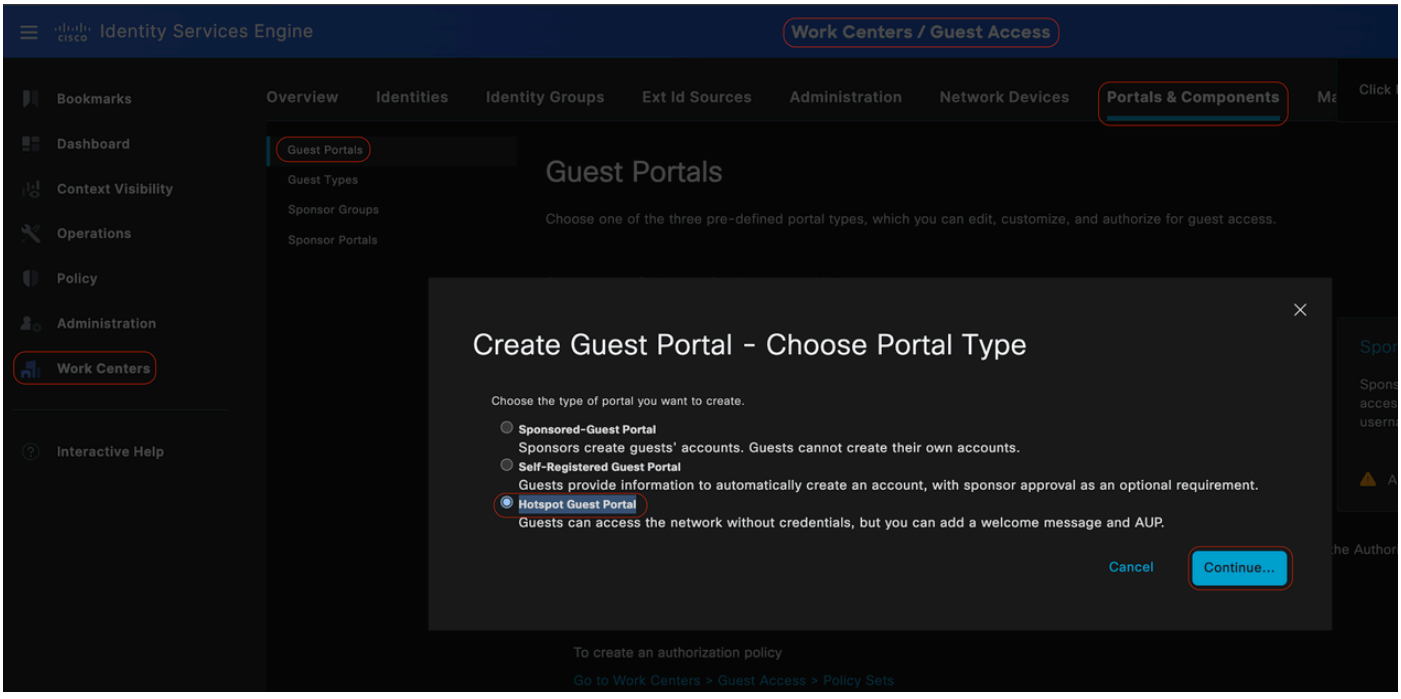
Perfil de autorização sem agente

Alternativa para usar a correção (opcional)

O suporte para correção no fluxo sem agente não está disponível. Para resolver esse problema, você pode implementar um portal de hotspots personalizado para aumentar a conscientização do usuário com relação à conformidade de endpoints. Quando um endpoint é identificado como não compatível, os usuários podem ser redirecionados para esse portal. Essa abordagem garante que os usuários sejam informados sobre o status de conformidade de seus endpoints e possam tomar as medidas apropriadas para corrigir qualquer problema.

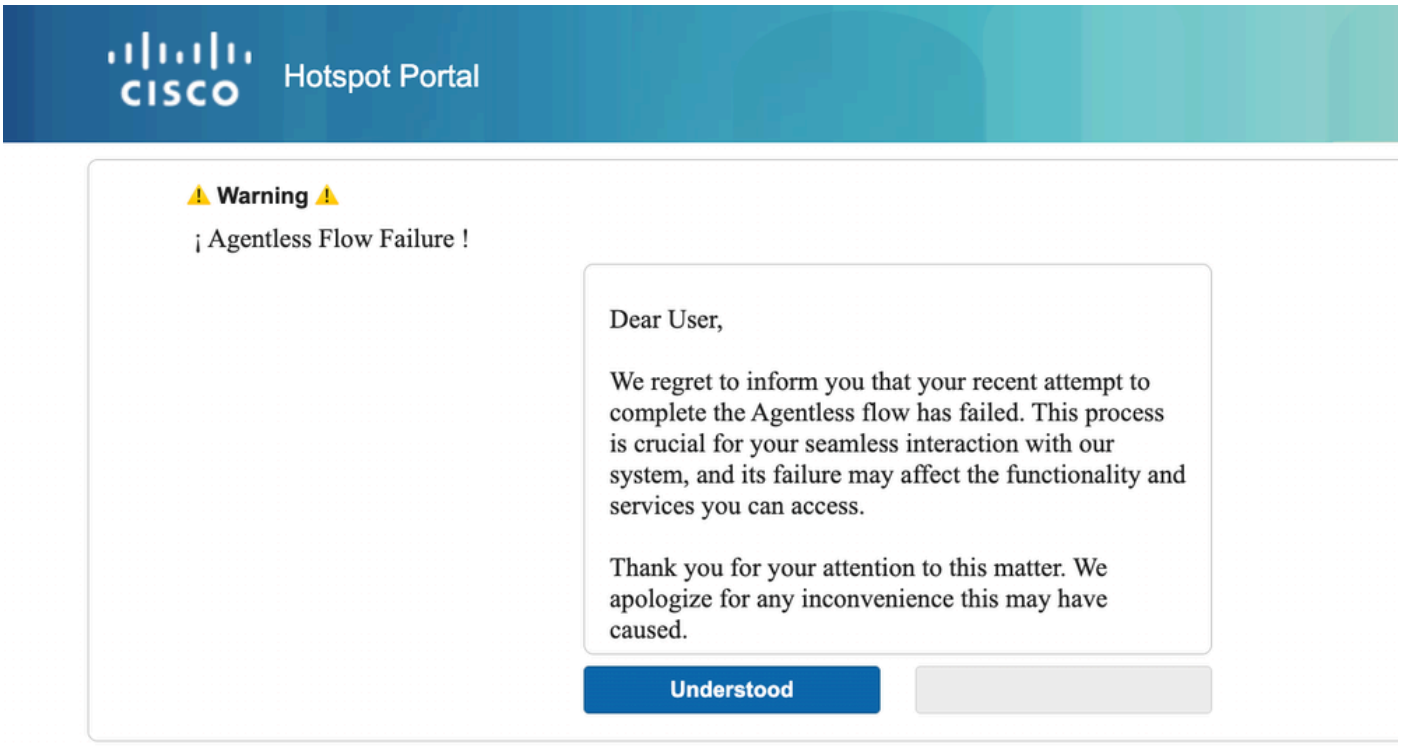
Na GUI do Cisco ISE, clique no ícone do menu (

) e escolha **Centros de trabalho** > **Acesso de convidado** > **Portais e componentes** >**Portais de convidado.** Clique em **Create** > Select **Hotspot Guest Portal** > **Continue:** . Neste exemplo de configuração, o Hotspot Portal é nomeado como **Agentless_Warning**.



Portal de Convidado do Hotspot

Nas configurações do portal, você tem a capacidade de personalizar as mensagens exibidas para os usuários finais para alinhá-las aos seus requisitos específicos. Este é apenas um exemplo de visualização personalizada do portal:



Falha sem agente de postura

Perfil de **Autorização de Remediação (Opcional)**

Na GUI do Cisco ISE, clique no ícone Menuicon ( ) e escolhaPolicy > Policy **Elements >** Results > **Authorization >** Authorization Profiles e crie um **Authorization** Profile **para sua correção.**

- Neste exemplo de configuração, chamado Perfil de autorização como **Remediation_Authorization_Profile**.

-

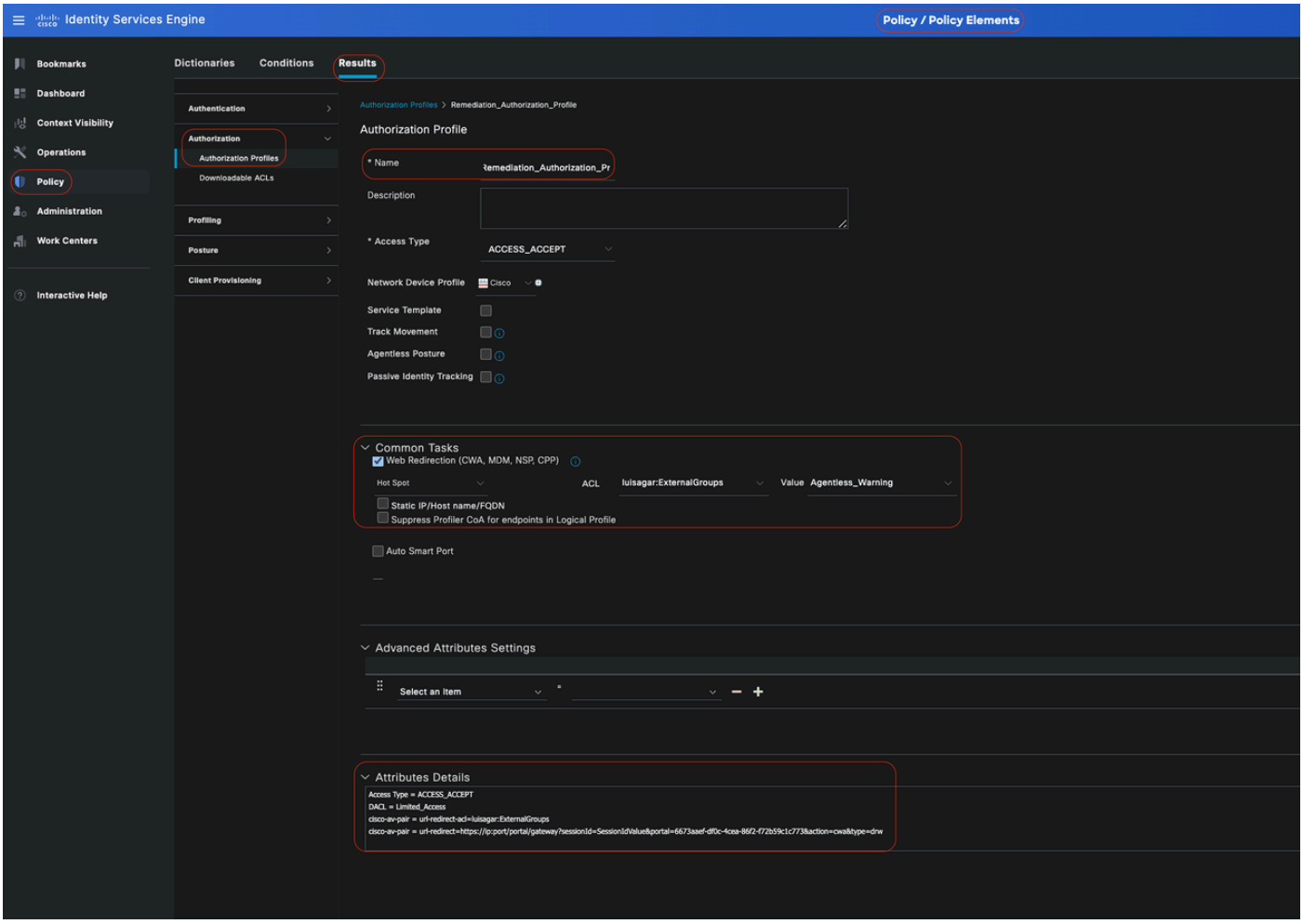
Por uma questão de simplicidade, este exemplo de configuração inclui apenas uma lista de controle de acesso (dACL - Access Control List) para download, denominada **Limited_Access**, que permite acesso limitado, adaptado às necessidades específicas da sua organização.

-

O recurso **Redirecionamento da Web** foi configurado, incluindo um grupo externo e o hotspot, aumentando a conscientização do usuário sobre a conformidade do endpoint.

-

Click **Save**.

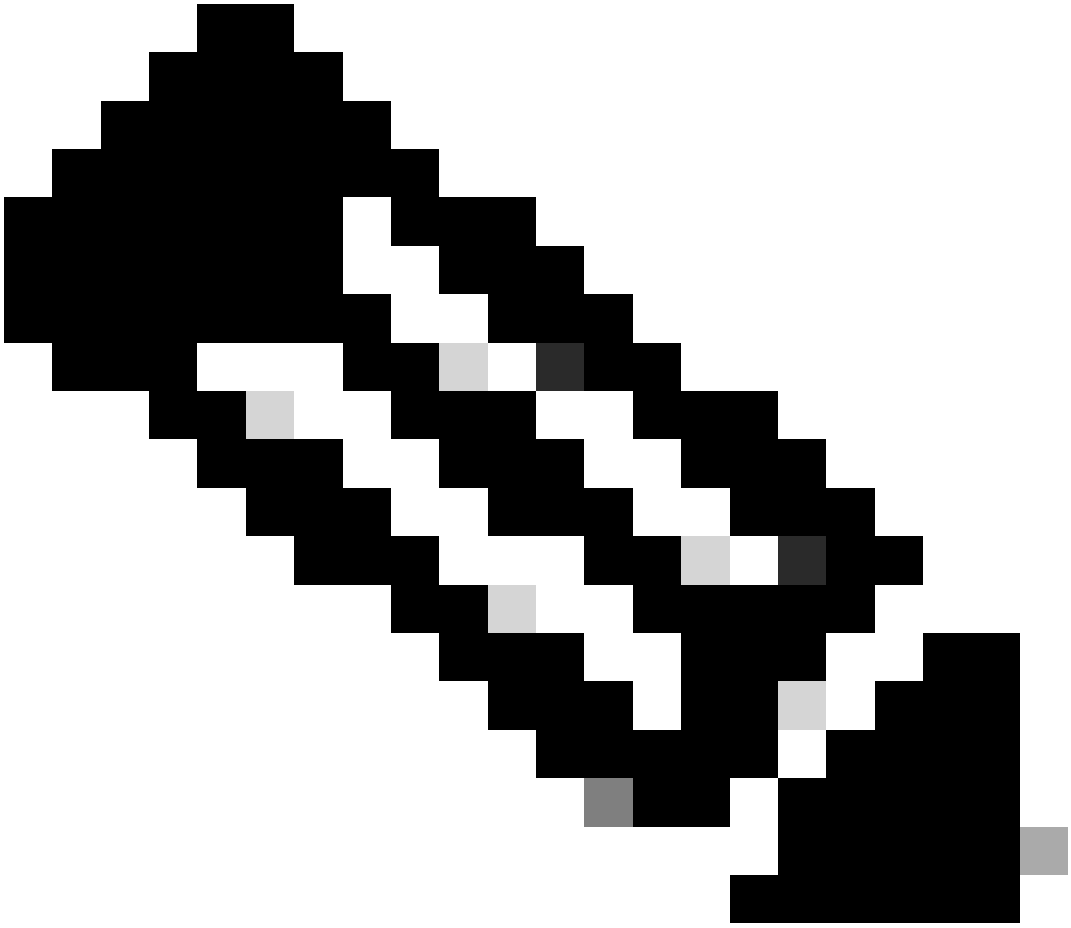


Regra de Autorização de Remediação

Regra de autorização sem agente

Na GUI do Cisco ISE, clique no ícone do menu (

) e escolhaPolicy > Policy Setse expanda Authorization Policy. Habilite e configure estas três políticas de Autorização:



Observação: essas regras de autorização devem ser configuradas na ordem especificada para garantir que o fluxo de postura funcione corretamente.

Redirecionamento_conformidade_desconhecido:

•**Condições:**

Configure Network_Access_Authentication_Passed AND **Compliance_Unknown_Devices** com o resultado definido como Postura sem Agente. Essa condição aciona o fluxo sem agente.

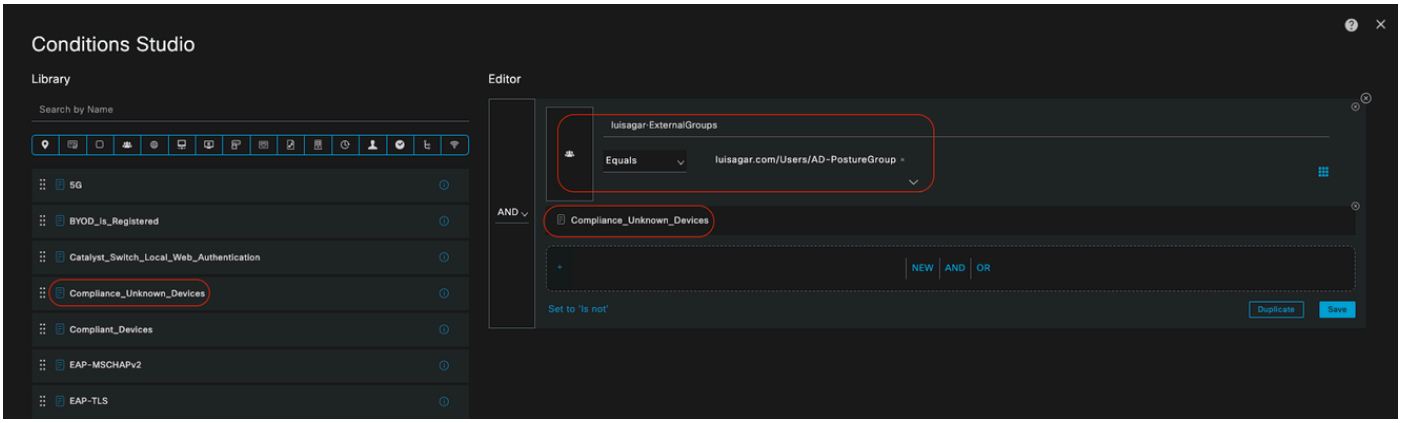
· **Exemplos de condições:**

Configure uma condição de Grupo do Ative Diretory (AD) para segmentar o tráfego.

A condição **Compliance_Unknown_Devices** deve ser configurada porque o estado de postura inicial é desconhecido.

· Perfil de autorização:

Atribua **Agentless_Authorization_Profile** a esta regra de autorização para garantir que os dispositivos passem pelo fluxo de postura sem agente. Essa condição contém um fluxo sem agente, de modo que os dispositivos que acessam esse perfil podem iniciar um fluxo sem agente.



Regra de Autorização Desconhecida

Dispositivos_Não Compatíveis_Redirecionar:

· Condições: Configure Network_Access_Authentication_Passed e Non_Compliant_Devices com o resultado definido como **DenyAccess**. Como alternativa, você pode usar a opção de remediação, conforme demonstrado neste exemplo.

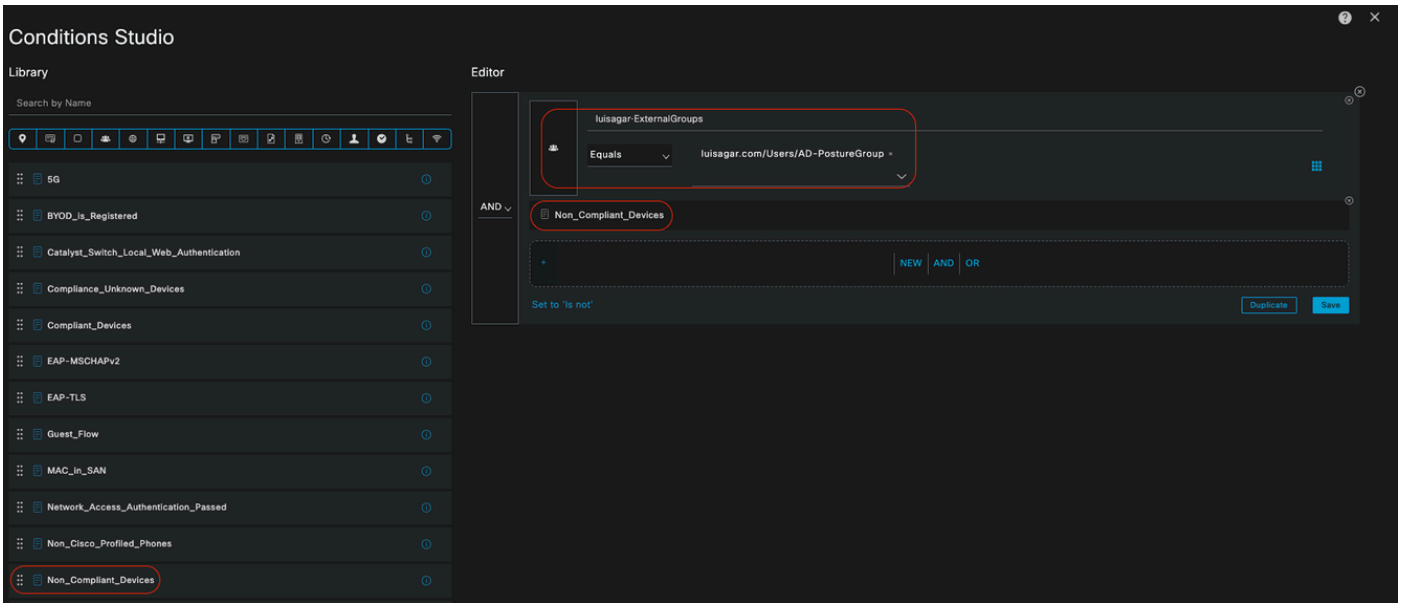
· Exemplos de condições:

Configure uma condição de Grupo AD para segmentar o tráfego.

A condição **Compliance_Unknown_Devices** deve ser configurada para atribuir recursos limitados quando o estado de postura for não compatível.

· Perfil de autorização:

Atribua **Remediation_Authorization_Profile** a esta Regra de Autorização para notificar dispositivos não compatíveis de seu status atual por meio do **Portal Hotspot** ou para **Negar Acesso**.



Regra de Autorização Não Compatível

Acesso_aos_Dispositivos_Compatíveis:

•Condições:

Configure Network_Access_Authentication_Passed e **Compliant_Devices** com o resultado definido como PermitAccess.

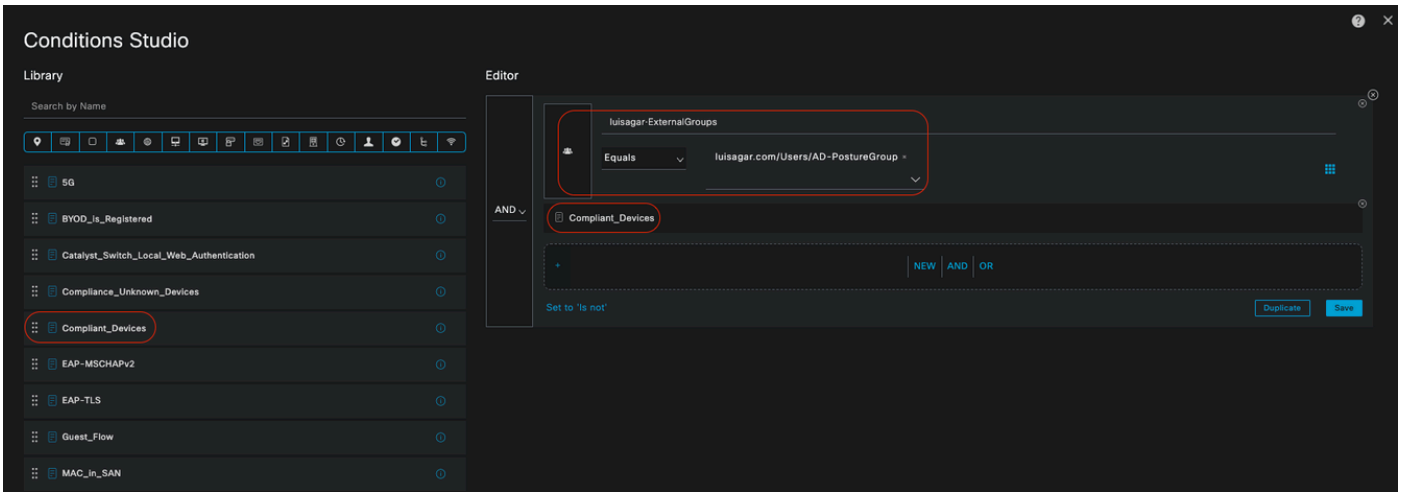
· Exemplos de condições:

Configure uma condição de Grupo AD para segmentar o tráfego.

A condição **Compliance_Unknown_Devices** deve ser configurada para que os dispositivos compatíveis recebam acesso adequado.

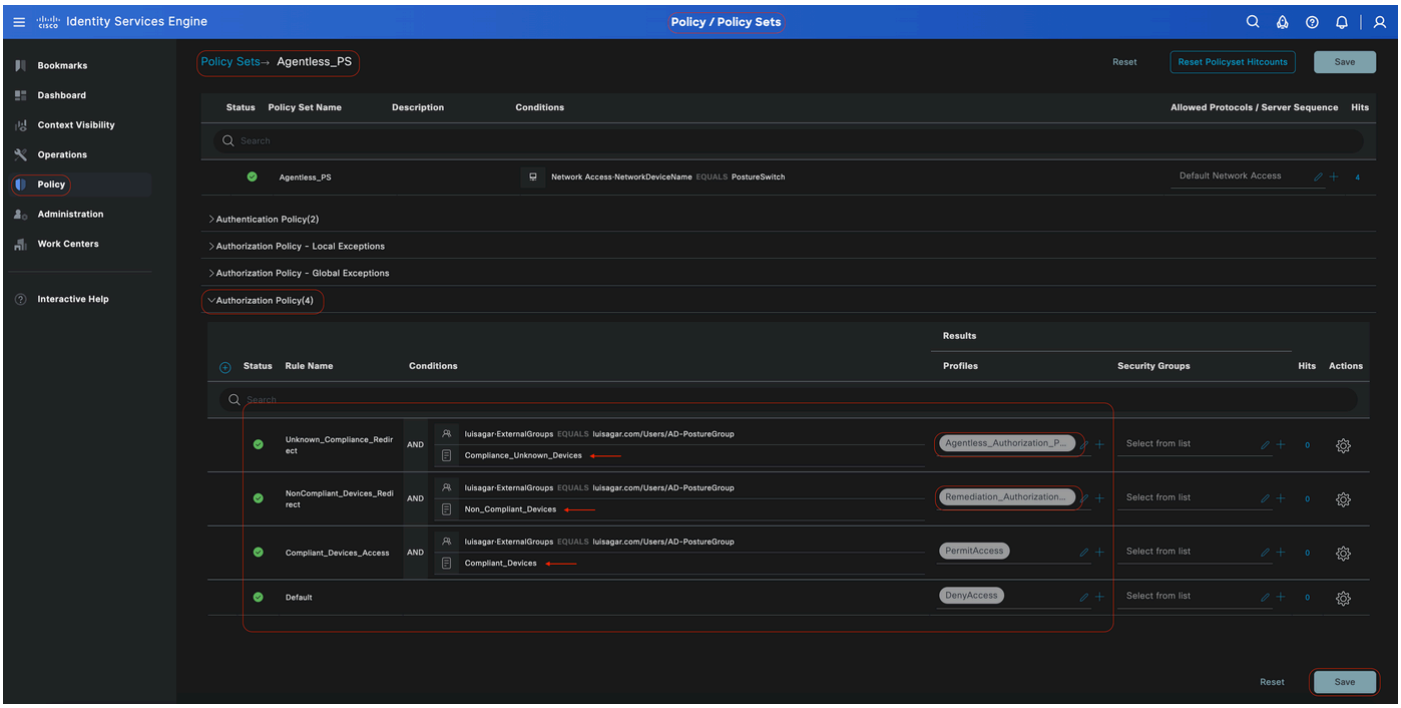
· Perfil de autorização:

Atribua **PermitAccess** a esta Regra de Autorização para garantir que os dispositivos compatíveis tenham acesso. Esse perfil pode ser personalizado para atender às necessidades da sua organização.



Regra de Autorização de Conformidade

Todas as regras de autorização



Regras de Autorização

Configurar Credenciais de Login do Ponto de Extremidade

Na GUI do Cisco ISE, clique no ícone do menu ( ) e escolhaAdministração > Configurações > Scripts de endpoint > Configuração de login e configure as credenciais do cliente para fazer login nos clientes.

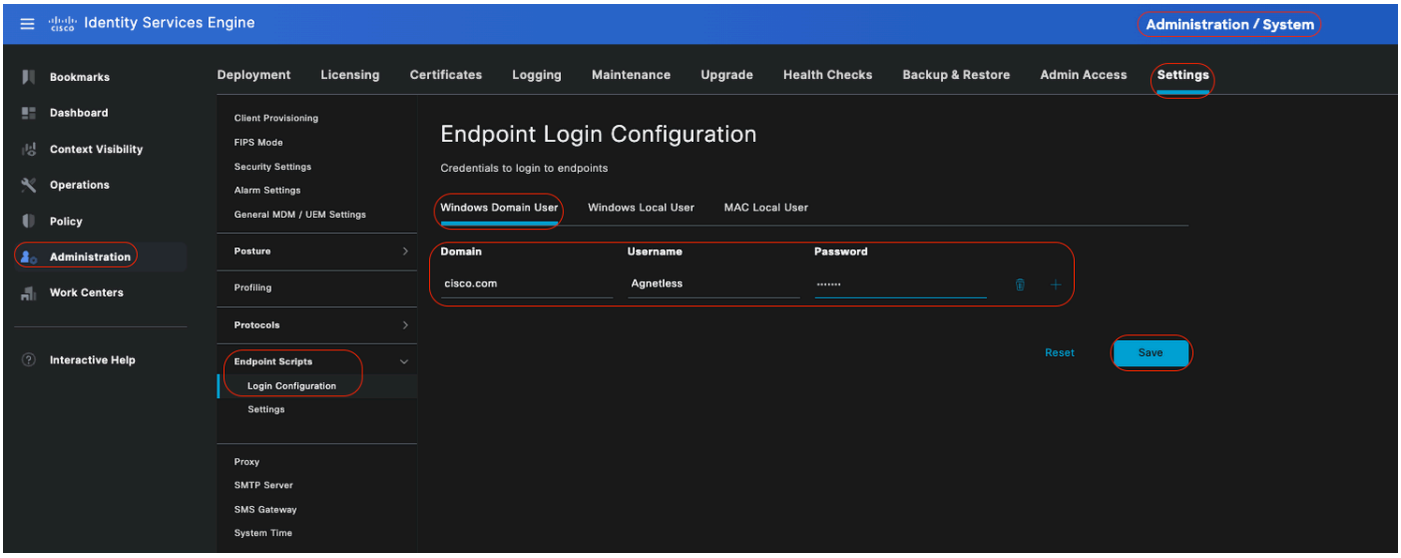
Essas mesmas credenciais são usadas pelos scripts de endpoint para que o Cisco ISE possa fazer logon nos clientes.

Para dispositivos Windows, você configura apenas as duas primeiras guias (**Usuário de Domínio do Windows e Usuário Local do Windows**

- **Usuário de Domínio do Windows:**

Configure as credenciais de domínio que o Cisco ISE deve usar para fazer login em um cliente via SSH. Clique noPlusicon e insira quantos logons do Windows forem necessários. Para cada domínio, insira os valores necessários nos campos Domain,Username, e Passwordfield. Se você configurar credenciais de domínio, as credenciais de usuário local configuradas na guia Usuário Local do Windows serão ignoradas.

Se você estiver administrando endpoints do Windows que utilizam uma avaliação de postura sem agente por meio de um domínio do Ative Diretory, assegure-se de fornecer o nome do domínio junto com as credenciais que possuam privilégios administrativos locais.

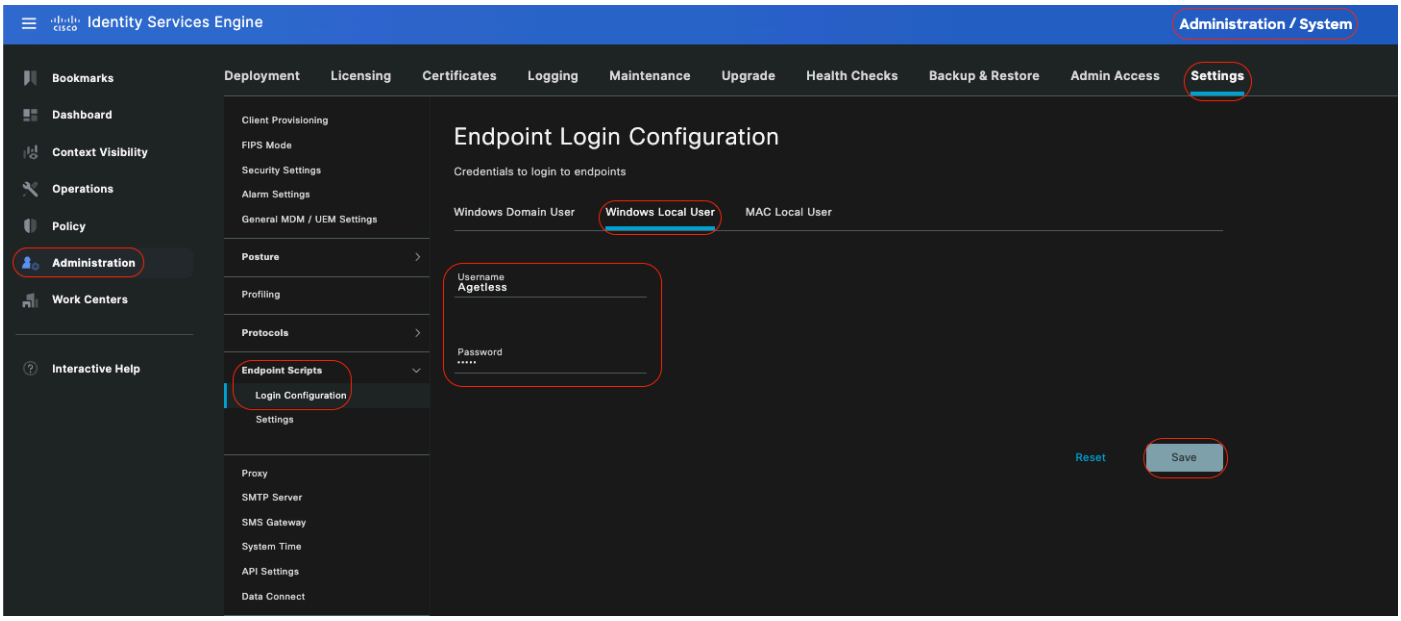


Usuário de Domínio do Windows

- **Usuário Local do Windows:**

Configure a conta local que o Cisco ISE usa para acessar o cliente via SSH. A conta local deve ser capaz de executar o Powershell e o Powershell remoto.

Se você **não** estiver administrando endpoints do Windows que utilizam uma avaliação de postura sem agente por meio de um domínio do Ative Diretory, certifique-se de fornecer credenciais que tenham privilégios administrativos locais.

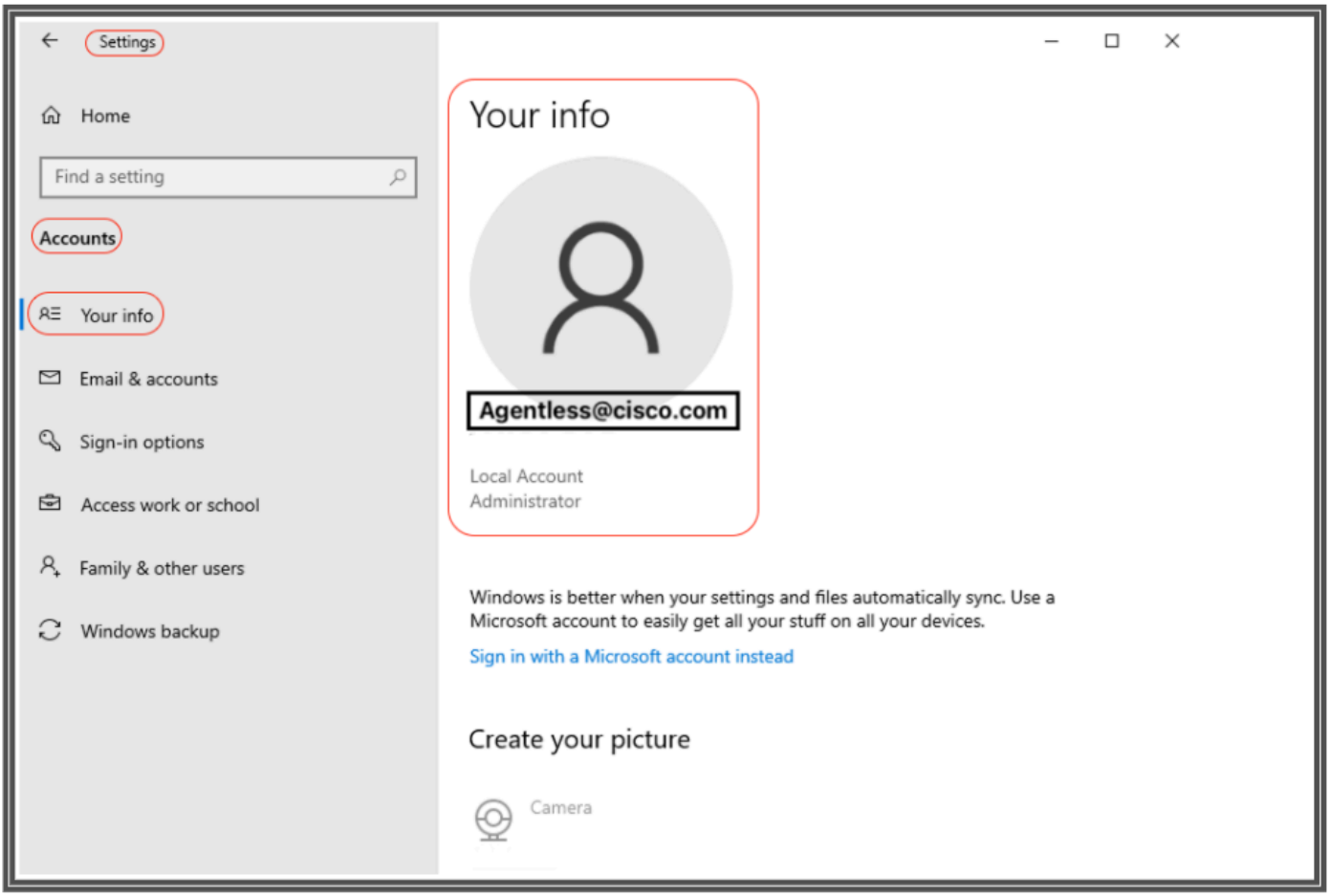


Usuário Local do Windows

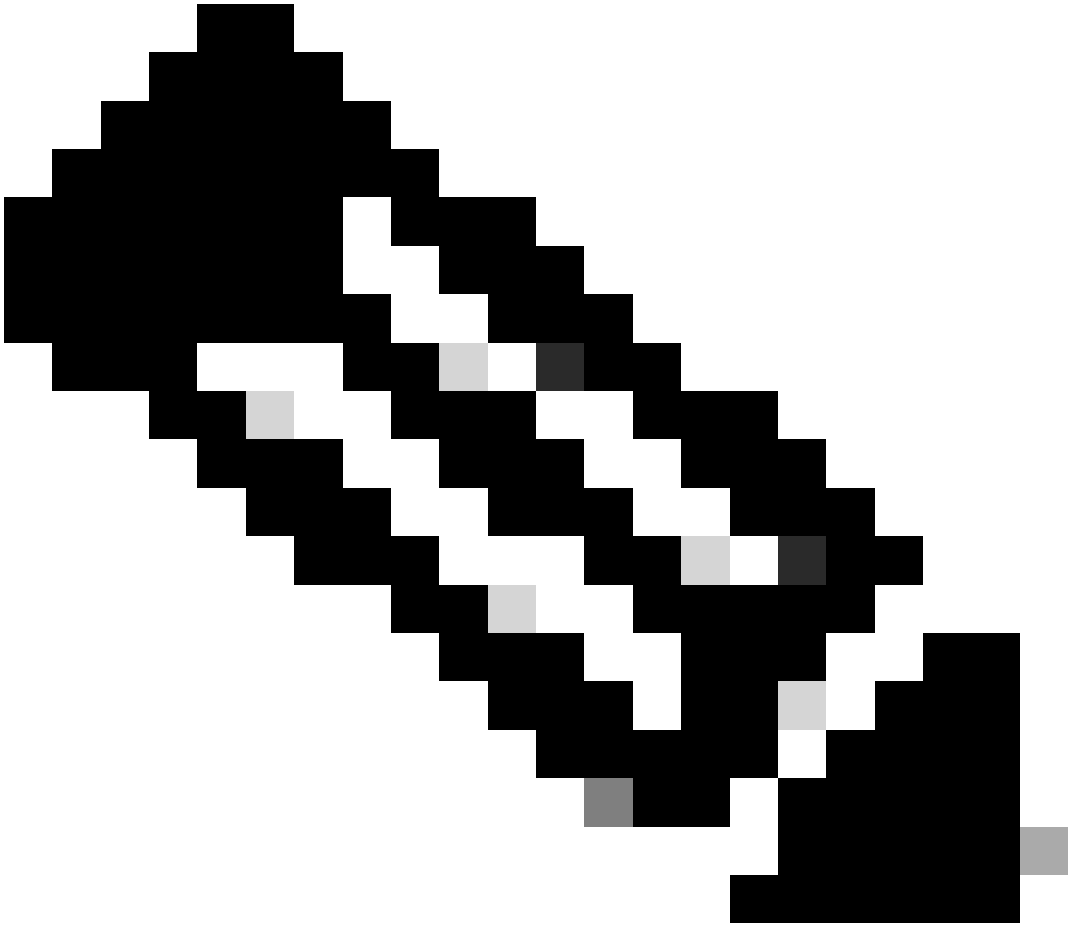
Verificar contas

Para verificar suas contas de usuário de domínio e de usuário local do Windows para que você possa adicionar com precisão os dados apropriados em Credenciais de Logon do Ponto de Extremidade, use este procedimento:

Usuário local do Windows: Usando a GUI (Configurações App) Clique no **botão WindowsStart**, selecione **Configurações** (o ícone da engrenagem), Clique em **Contas** e selecione **Suas informações**:



Verificar contas



Observação: para MacOS, você pode consultar **MAC Local User**. No entanto, neste exemplo de configuração, você não verá a configuração do MacOS.

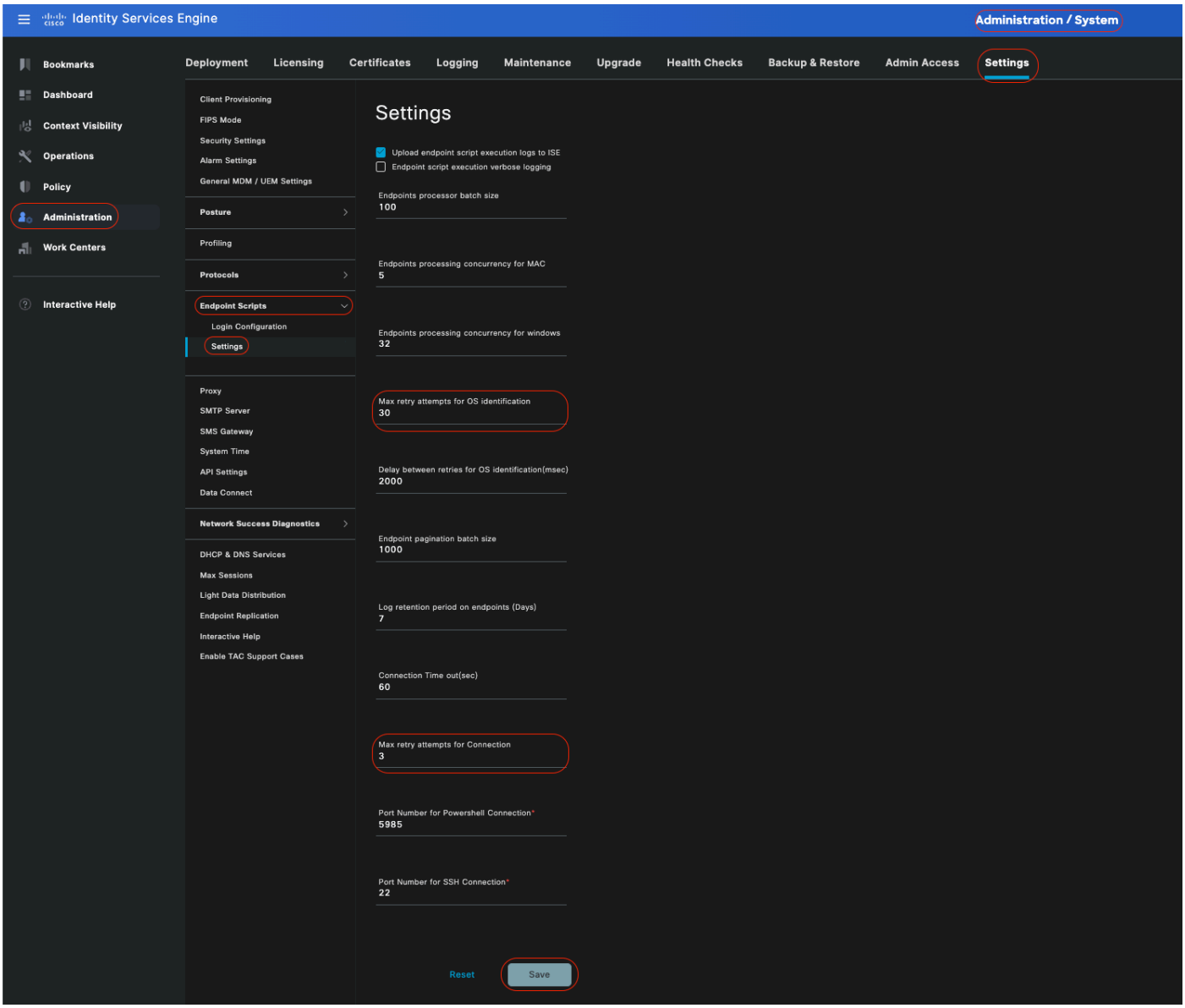
- **Usuário local de MAC:** Configure a conta local que o Cisco ISE usa para acessar o cliente via SSH. A conta local deve ser capaz de executar o Powershell e o Powershell remoto. No campoNome de usuário, insira o Nome da conta local.

Para exibir um Nome de Conta do Mac OS, execute este comandowhoami no Terminal:

Configurações

Na GUI do Cisco ISE, clique no ícone de menu () e **escolhaAdministração > Configurações >** Scripts de endpoint > **Configurações e** configureMáx tentativas de repetição **para identificação do SO,**Atraso entre tentativas de identificação do SO **e assim por diante.** Essas configurações determinam com que rapidez os problemas de conectividade podem ser confirmados. Por exemplo, um erro de que a porta do PowerShell não está aberta é exibido nos logs somente depois que todas as novas tentativas não se esgotam.

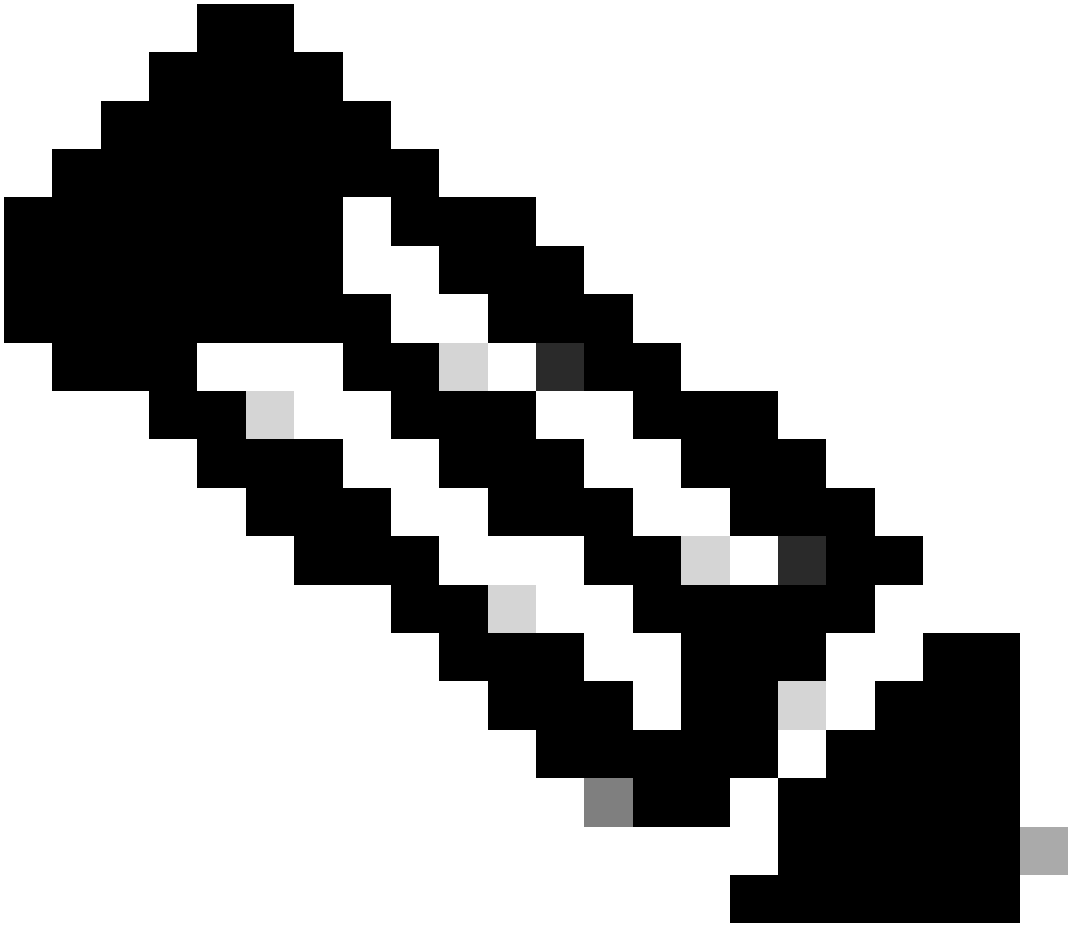
Esta captura de tela mostra as configurações de valor padrão:



Configurações de Script de Ponto de Extremidade

À medida que os clientes se conectam com a postura sem agente, você pode vê-los nos registros em tempo real.

Configurando e Troubleshooting de Windows Endpoint



Observação: estas são algumas recomendações para verificar e aplicar em seu dispositivo Windows; no entanto, você deve consultar a documentação da Microsoft ou entrar em contato com o suporte da Microsoft se encontrar problemas como privilégios de usuário, acesso do PowerShell e assim por diante...

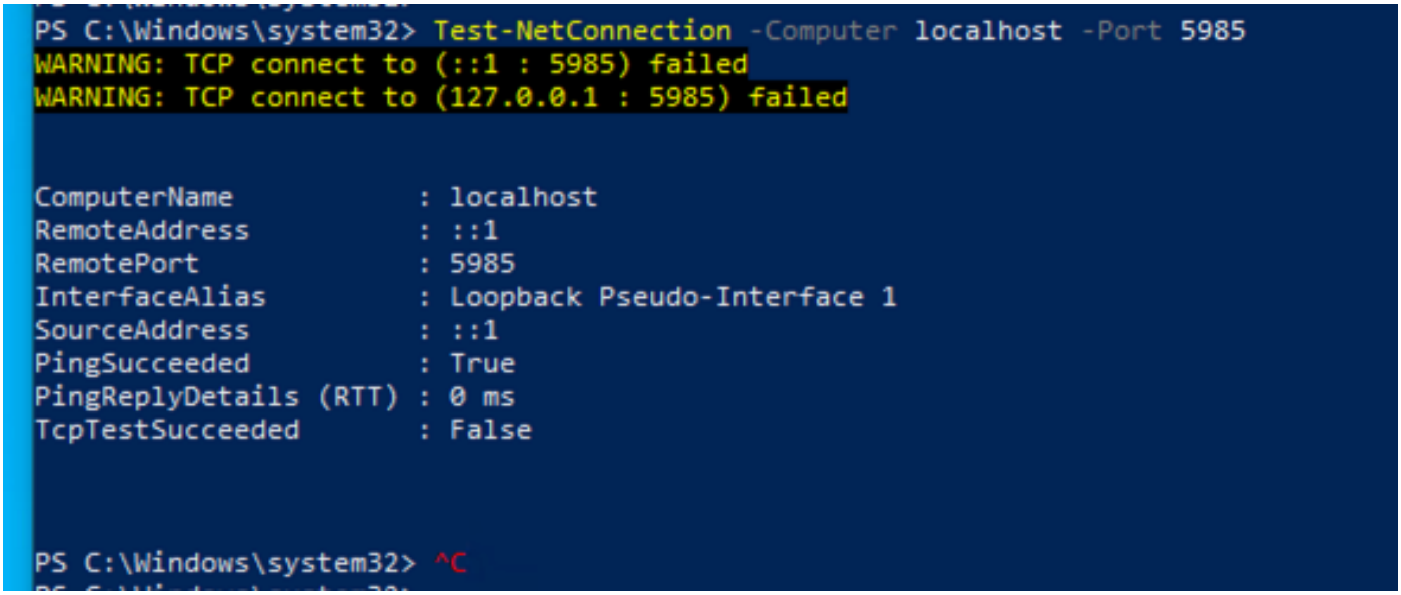
Verificação e Troubleshooting de pré-requisitos

Testando a conexão TCP com a porta 5985

Para clientes Windows, a porta 5985 para acessar o powershell no cliente deve ser aberta. Execute este comando para confirmar a conexão TCP com a porta 5985: **Test-NetConnection -ComputerName localhost -Port 5985**

A saída mostrada nesta captura de tela indica que a conexão TCP com a porta 5985 no localhost falhou. Isso significa que o serviço WinRM

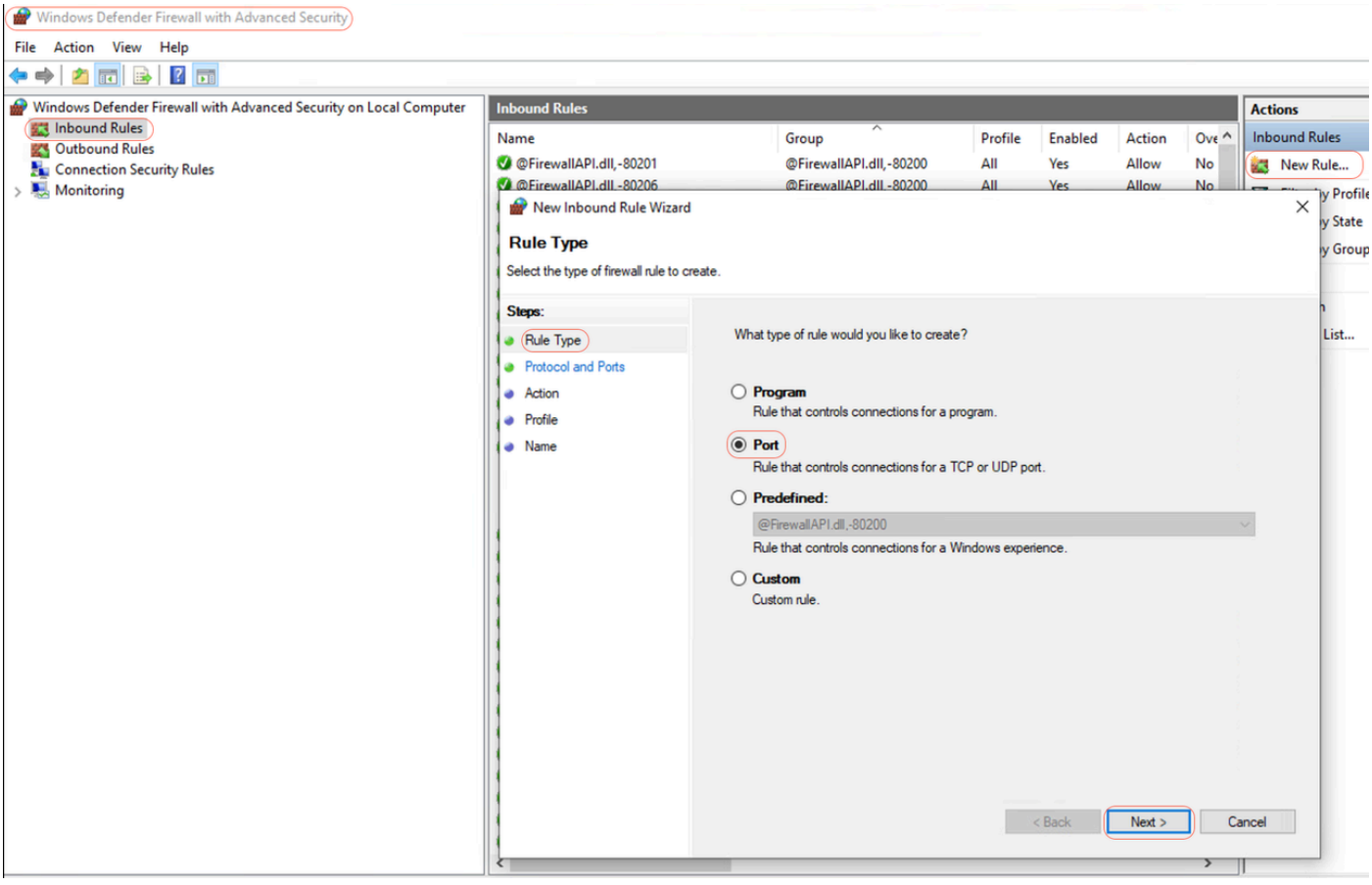
(Windows Remote Management), que usa a porta 5985, não está em execução ou não está configurado corretamente.



Connection failed to WinRM

Criando Regra de Entrada para permitir o PowerShell na porta 5985

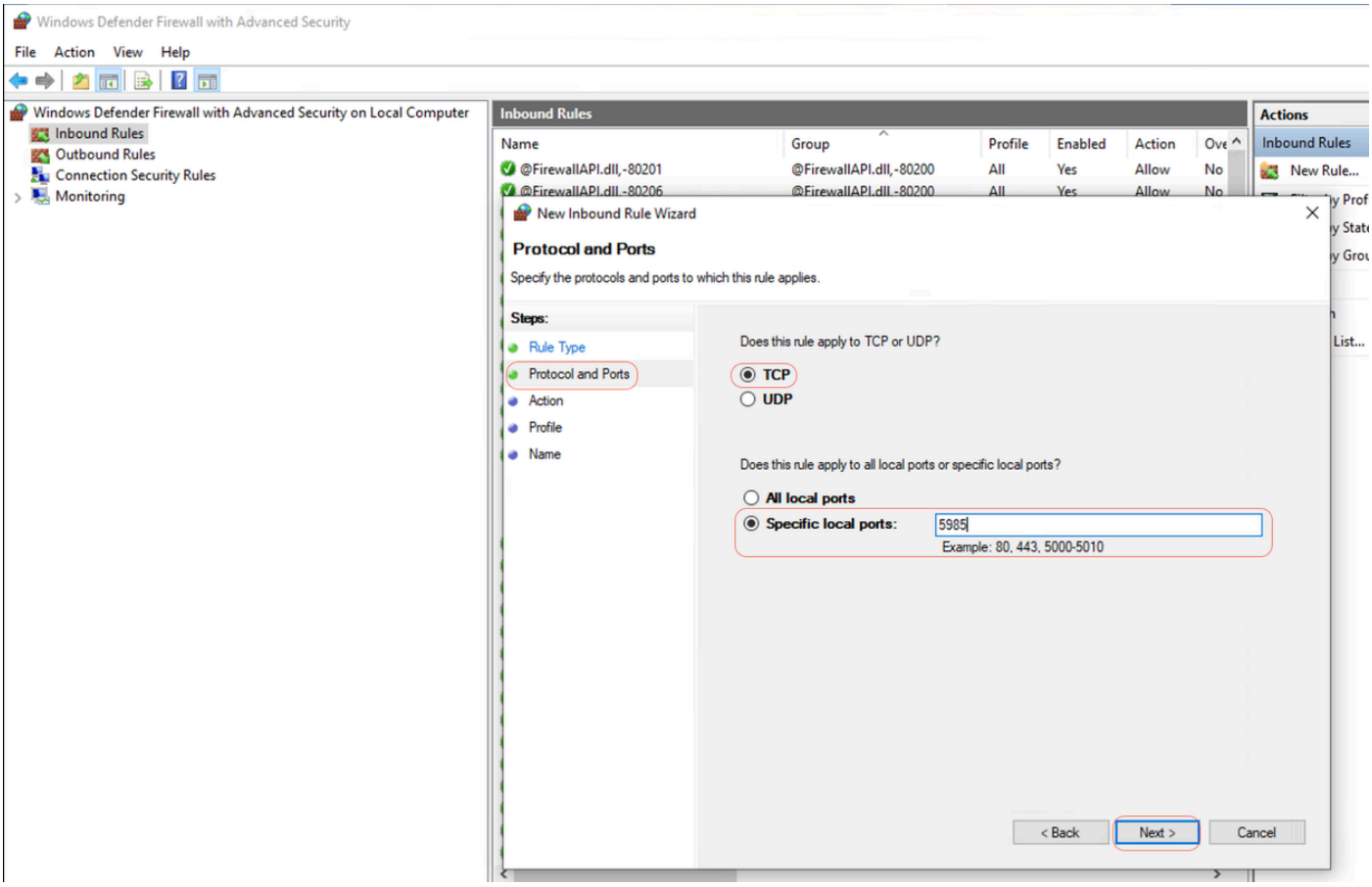
Etapa 1- Na GUI do Windows, vá para **Barra de pesquisa, digite Firewall do Windows com Segurança avançada, clique nele e selecione Executar como administrador > Regras de entrada > Nova regra > Tipo de regra > Porta > Avançar:**



Nova Regra de Entrada - Porta

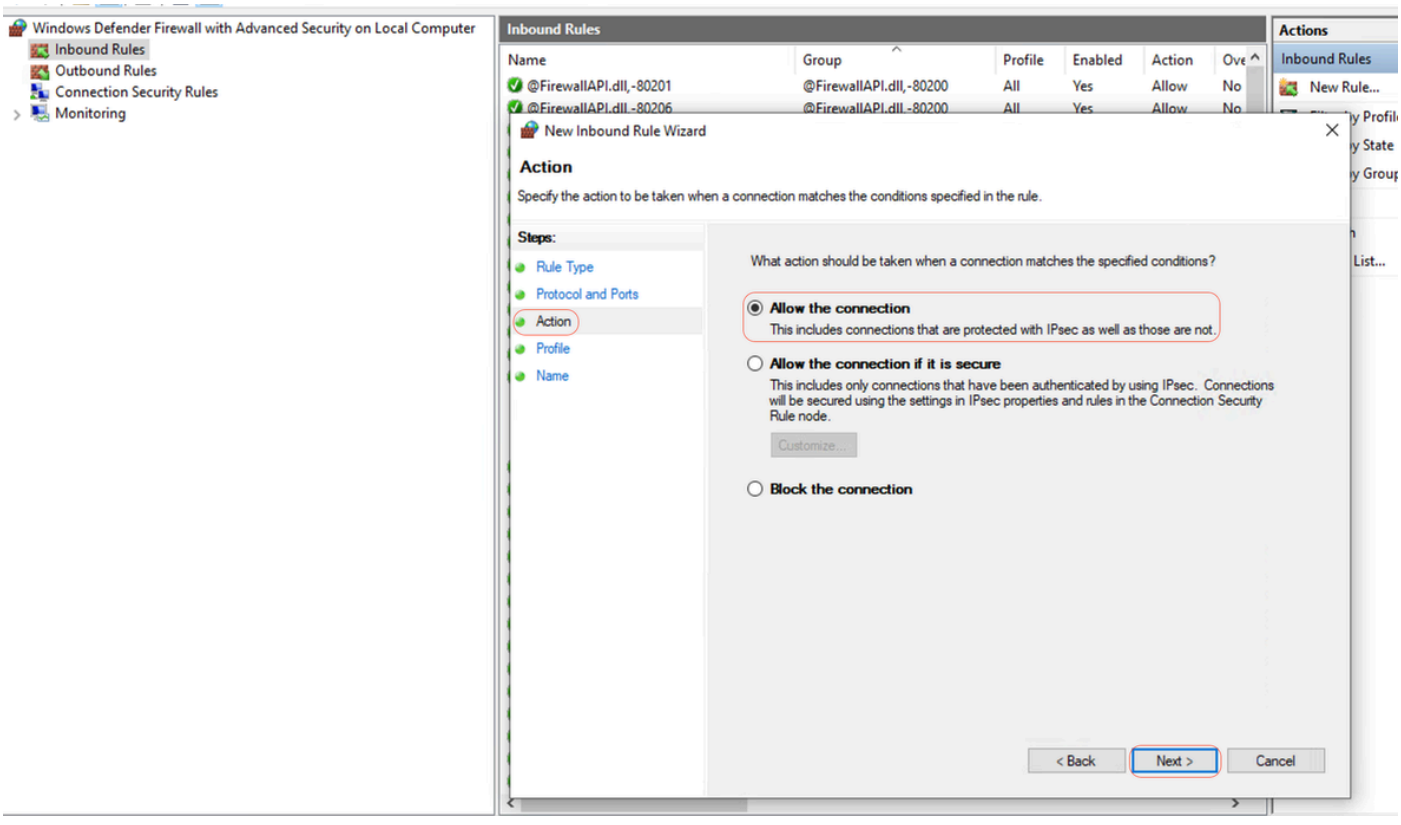
Etapa 2 - Em Protocolos e portas, selecione TCP e Especifique as portas locais, digite o número da porta 5985 (Porta padrão para

PowerShell comunicação remota) e clique em Avançar:



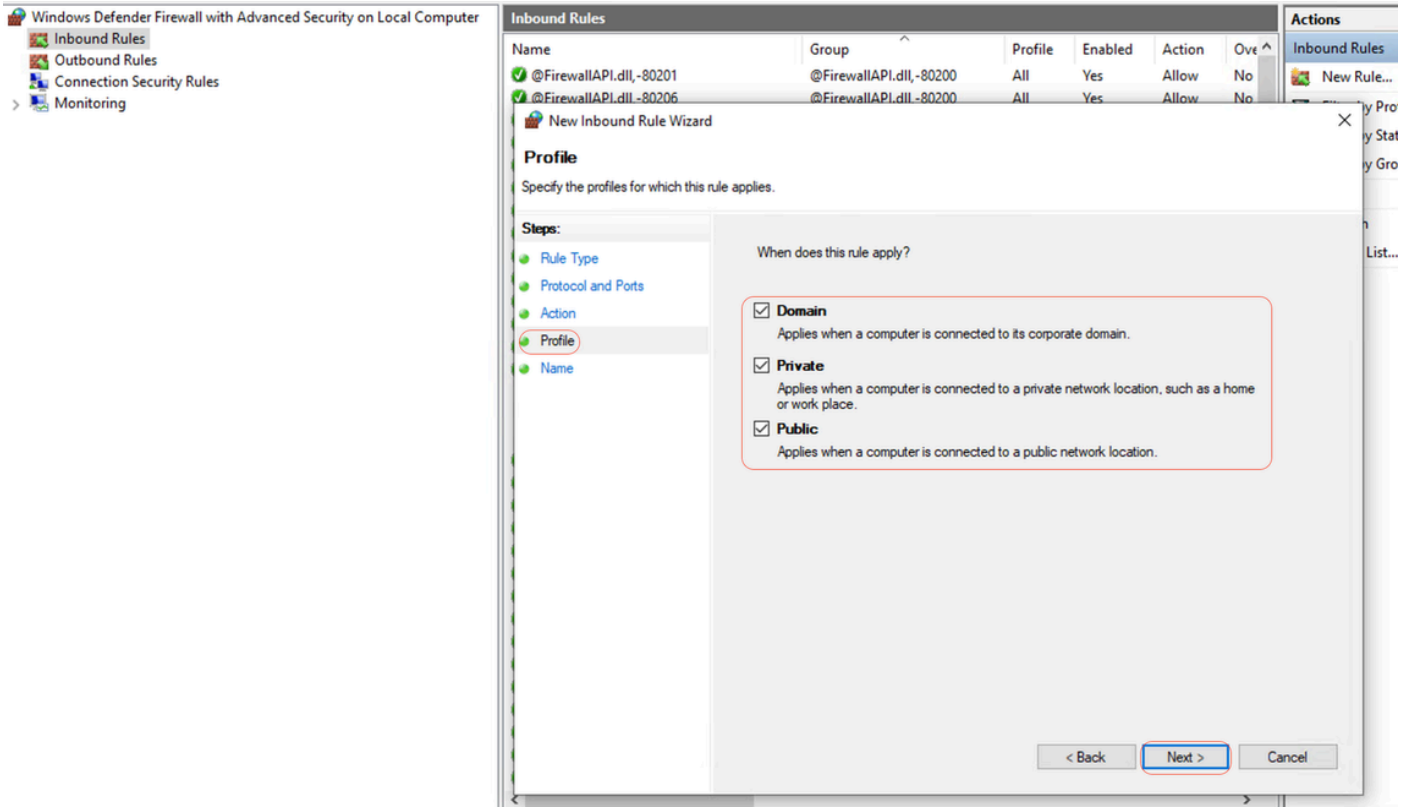
Protocolos e portas

Etapa 3- Em **Ação** > Selecionar **Permitir a conexão** > **Avançar**:



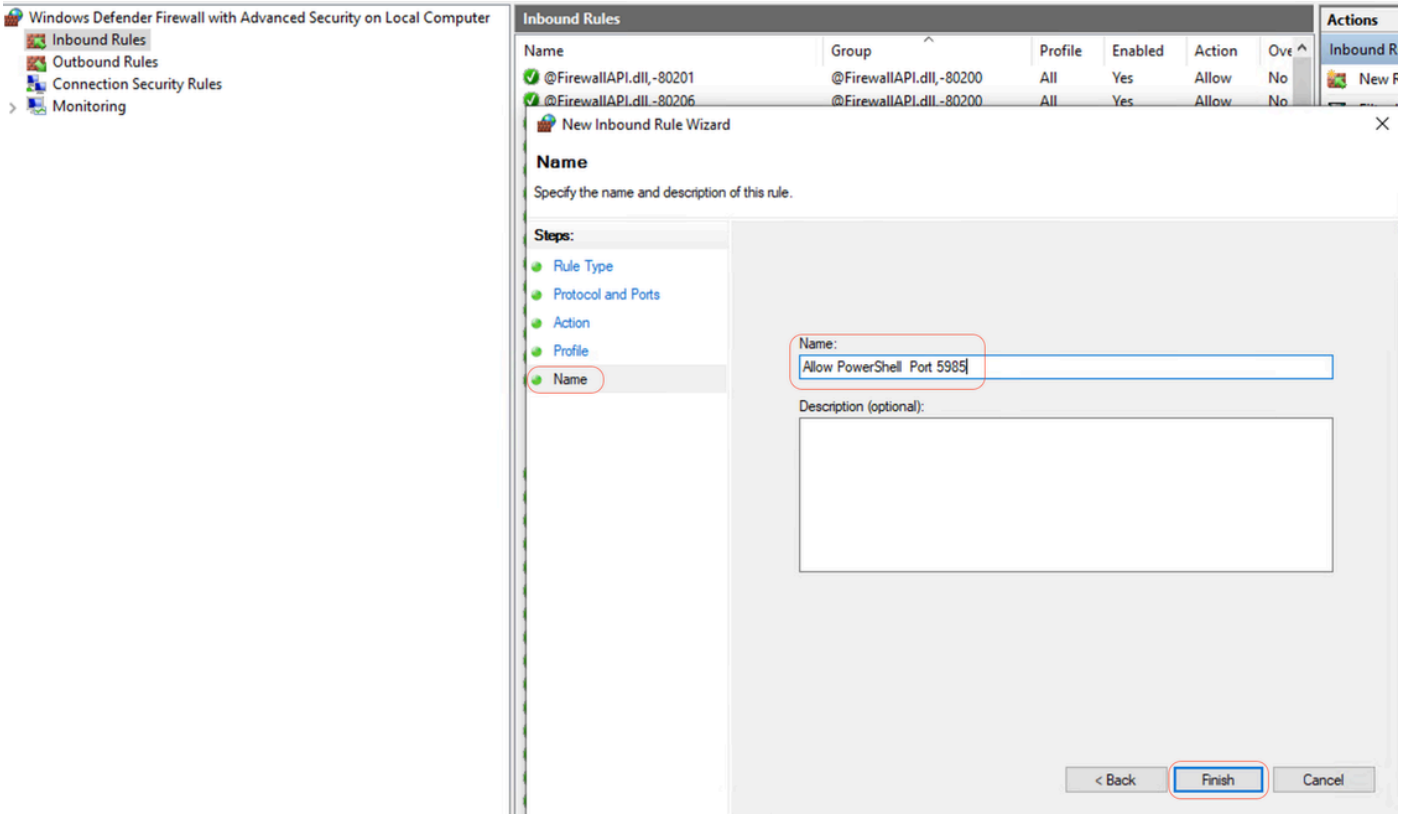
Ação

Etapa 4 - Em **Profile, marque as caixas de seleção Domain, Private e Public** e clique em **Next**:



Profile

Etapa 5- Em **Name**, digite um nome para a regra, como **Allow PowerShell on Port 5985 e clique em Finish**:

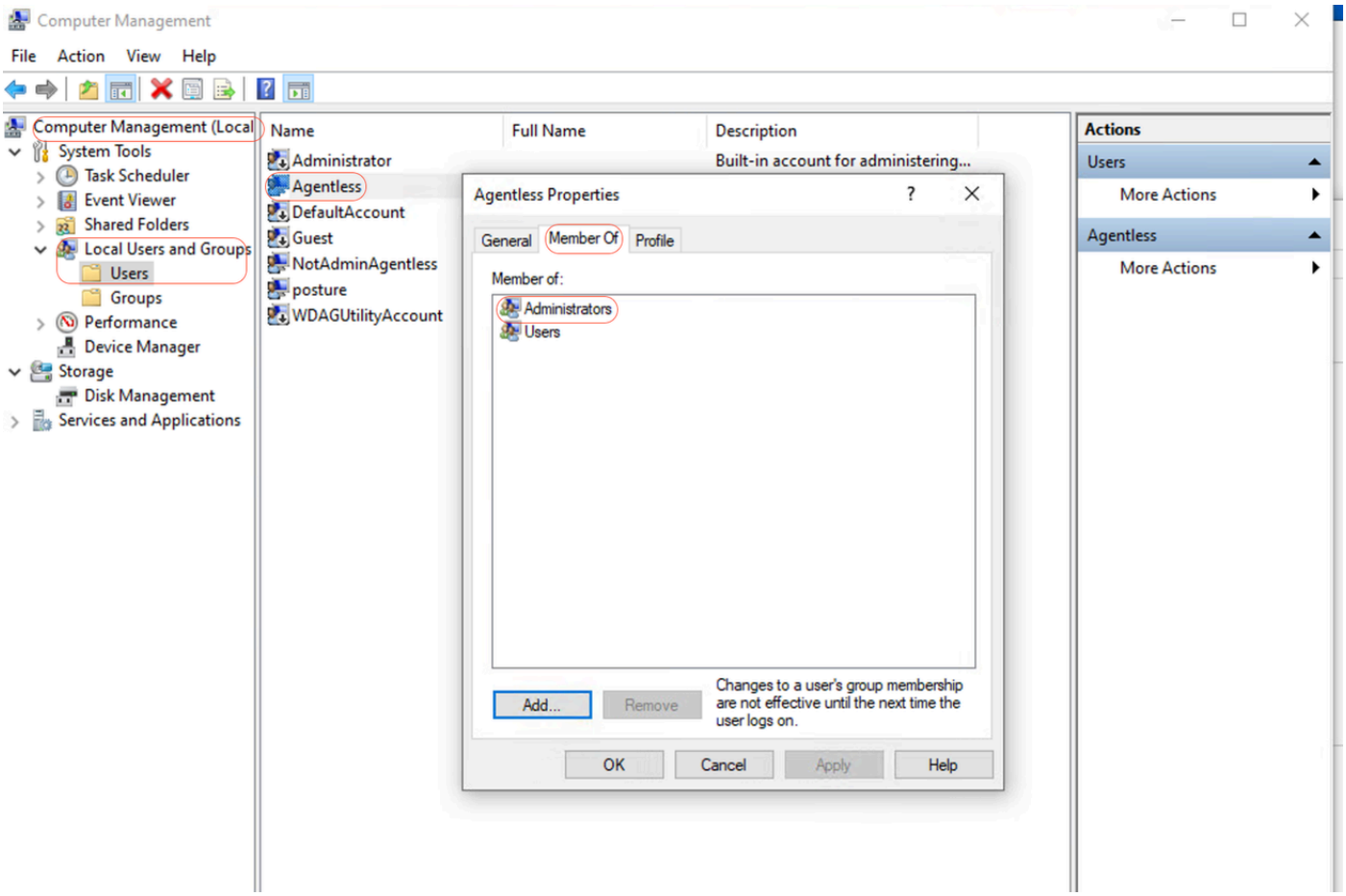


Nome

As credenciais do cliente para o logon do shell devem ter privilégios de administrador local

As credenciais do cliente para o logon do shell devem ter privilégios de administrador local. Para confirmar se você tem privilégios de administrador, verifique estas etapas:

Na GUI do Windows, vá para Configurações > Gerenciamento do computador > Usuários e grupos locais > Usuários > Selecione a conta de usuário (neste exemplo, a conta sem agente está selecionada) > Membro de, a conta deve ter Administradores Grupo.



Privilégios de administrador local

Validando ouvinte WinRM

Verifique se o ouvinte do WinRM está configurado para **HTTP** na porta **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 WinRM de Comunicação Remota do PowerShell

Verifique se o serviço está em execução e configurado para iniciar automaticamente. Siga estas etapas:

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**

Saída esperada:

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**

O Powershell deve ser v7.1 ou posterior. O cliente deve ter cURL v7.34 ou posterior:

Como verificar versões do PowerShell e do cURL no Windows

Certifique-se de estar usando as versões apropriadas do PowerShell ; cURL é essencial para Posture Agentless:

Verificando a Versão do PowerShell

No Windows:

1. **Abrir o PowerShell:**

・Pressione Win + X **e selecione** Windows PowerShell ou **Windows PowerShell (Admin)**.

2.Execute o comando:$PSVersionTable.PSVersion

・Este comando exibe os detalhes da versão do PowerShell instalado no sistema.

Verificando a versão do cURL

No Windows:

1. Abrir Prompt de Comando:

・Pressione Win + R, digite cmd e clique em Enter.

2. Execute o Comando: curl --version

・Esse comando exibe a versão do cURL instalada no sistema.

Saída para verificação das versões do PowerShell e do cURL em 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>

Configuração adicional

Este comando configura sua máquina para confiar em hosts remotos específicos para conexões WinRM: Set-Item WSMan:\localhost\Client\TrustedHosts -Value <Client-IP>

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> -

O cmdlet test-wsman com os parâmetros -Authentication Negotiate e -Credential é uma ferramenta poderosa para verificar a disponibilidade e a configuração do serviço WinRM em um computador remoto: test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

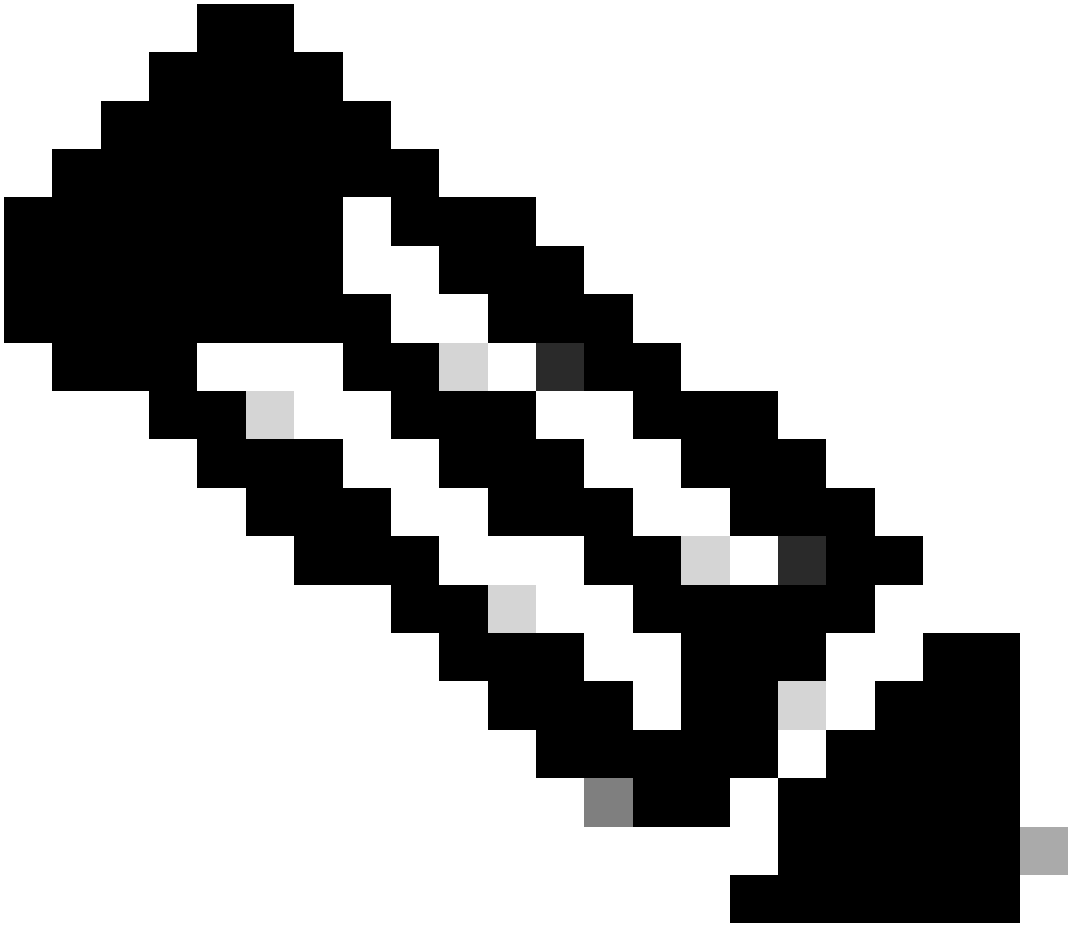
O Powershell deve ser v7.1 ou posterior. O cliente deve ter cURL v7.34 ou posterior:

No MacOS:

1. **Terminal aberto:**

・Você pode encontrar Terminal em **Aplicativos > Utilitários**.

2. Execute o Comando: pwsh -Command '$PSVersionTable.PSVersion'



Observação: Observação: · Verifique se o PowerShell Core (pwsh) está instalado. Se não, você pode instalá-lo através do Homebrew (certifique-se de que você tem Himebrew instalar): brew install --cask powershell

---

No MacOS:

1. **Terminal aberto:**

· Você pode encontrar Terminal em **Aplicativos > Utilitários**.

2. Execute o Comando: curl --version

· Este comando deve exibir a versão do cURL instalada no sistema.

Para clientes MacOS, a porta 22 para acessar o SSH deve estar aberta para acessar o cliente

Guia passo a passo:

1. **Preferências do Sistema Aberto:**

· Navegue até **Preferências do sistema** no menu Apple.

2. **Ativar login remoto:**

· Vá para **Compartilhamento**.

· Marque a caixa ao lado de **Remote Login**.

· Certifique-se de que a opção **Permitir acesso para** esteja definida como os usuários ou grupos apropriados. Selecionar **All users** permite que qualquer usuário com uma conta válida no Mac faça login via SSH.

3. **Verificar Configurações do Firewall:**

· Se o firewall estiver habilitado, você precisará garantir que ele permita conexões SSH.

· Vá para **Preferências do sistema > Segurança e privacidade > Firewall**.

· Clique no botão **Opções de firewall**.

· Verifique se **Remote Login** ou **SSH** está listado e permitido. Se ele não estiver listado, clique no botão **Add** (+) para adicioná-lo.

4. **Abrir a porta 22 através do terminal (se necessário):**

· Abra o **aplicativo Terminal** em **Aplicativos > Utilitários**.

· Use o comando pfctl para verificar as regras de firewall atuais e garantir que a porta 22 esteja aberta:sudo pfctl -sr | grep 22

· Se a porta 22 não estiver aberta, você poderá adicionar manualmente uma regra para permitir SSH:echo "pass in proto tcp from any to any port 22" | sudo pfctl -ef -

5. **Testar o acesso SSH:**

· De outro dispositivo, abra um terminal ou cliente SSH.

· Tente se conectar ao cliente macOS usando seu endereço IP:ssh username@<macOS-client-IP>

· Substitua username pela conta de usuário apropriada e <macOS-client-IP> pelo endereço IP do cliente macOS.

Para MacOS, certifique-se de que esta entrada seja atualizada no arquivo sudoers para evitar falha de instalação de certificado nos endpoints:

Ao gerenciar endpoints macOS, é crucial garantir que comandos administrativos específicos possam ser executados sem exigir um prompt de senha.

Pré-requisitos

· Acesso de administrador na máquina macOS.

· Familiaridade básica com comandos de terminal.

Etapas para atualizar o arquivo Sudoers

1. **Terminal aberto:**

· Você pode encontrar Terminal em **Aplicativos > Utilitários**.

2. **Edite o Arquivo Sudoers:**

· Use o comando visudo para editar com segurança o arquivo sudoers. Isso garante que todos os erros de sintaxe sejam detectados antes de salvar o arquivo.sudo visudo

· Você será solicitado a inserir sua senha de administrador.

3. **Localize a Seção Apropriada:**

· No editor do visudo, navegue para a seção onde as regras específicas do usuário são definidas. Normalmente, isso fica na parte inferior do arquivo.

4. **Adicione a Entrada Obrigatória:**

· Adicione esta linha para conceder ao usuário especificado permissão para executar os comandos security e osascript sem uma senha: <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

· Substitua **<macadminusername> pelo nome de usuário real do administrador do macOS.**

5. **Salvar e Sair:**

· Se você estiver usando o editor padrão (nano), pressione Ctrl + X para sair, depois pressione **Y** para confirmar as alterações e, finalmente, pressione **Enter** para salvar o arquivo.

· **Se estiver usando** vi ou vim, pressione Esc, digite **:wq** e pressione **Enter** para salvar e sair.

6. **Verifique as Alterações:**

· Para garantir que as alterações tenham entrado em vigor, você pode executar um comando que exija as permissões sudo atualizadas. Por exemplo:

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

· Esses comandos podem ser executados sem solicitar uma senha.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.