配置状态无代理

目录

简介

本文档介绍如何在ISE中配置安全评估无代理，以及在运行无代理脚本的终端中需要什么。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)。
- 状态。
- PowerShell和SSH
- Windows 10或更高版本。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE) 3.3版本。
- 软件包CiscoAgentlessWindows 5.1.6.6
- Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

ISE终端安全评估执行客户端评估。客户端从ISE接收终端安全评估要求策略，执行终端安全评估数据收集，将结果与策略进行比较，并将评估结果发送回ISE。

然后，ISE根据安全评估报告确定设备是否合规。

无代理状态是从客户端收集状态信息并在完成后自动删除自己的状态方法之一，无需最终用户执行任何操作。无代理状态使用管理权限连接到客户端。

入门指南

先决条件:

- 客户端必须可通过其IPv4或IPv6地址访问，并且该IP地址必须在RADIUS记账中可用。
- 客户端必须通过其IPv4或IPv6地址从思科身份服务引擎(ISE)访问。此外，此IP地址必须在RADIUS记账中可用。
- 当前支持Windows和Mac客户端：
    - 对于Windows客户端，要访问客户端上的powershell，必须打开端口5985。Powershell必须是v7.1或更高版本。客户端必须具有cURL v7.34或更高版本。
    - 对于MacOS客户端，访问SSH的端口22必须打开才能访问客户端。客户端必须具有

cURL v7.34或更高版本。

- 外壳登录的客户端凭证必须具有本地管理员权限。
- 运行状态源更新以获取最新客户端，如配置步骤中所述。请检查：
- 对于MacOS，请确保在sudoers文件中更新此条目，以避免终端上的证书安装故障：请检查：

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

- 对于MacOS，配置的用户帐户必须是管理员帐户。MacOS的无代理安全评估不适用于任何其他帐户类型，即使您授予了更多权限。要查看此窗口，请点击Menuicon ()并选择**Administration > System > Settings > Endpoint Scripts** > Login **Configuration > MAC Local User**。
- 如果由于Microsoft的更新导致Windows客户端中的端口相关活动发生更改，您必须重新配置Windows客户端的无代理状态配置工作流。

支持的终端安全评估条件

- 文件条件，但使用USER_DESKTOP和USER_PROFILE文件路径的条件除外
- 服务条件，但macOS上的系统守护程序和守护程序或用户代理检查除外

- 申请条件
- 外部数据源条件
- 复合条件
- 防恶意软件情况
- 修补程序管理条件，**EnabledandUp To** Datecondition检查除外
- 防火墙条件
- 磁盘加密条件，基于加密位置的条件检查除外
- 注册表条件，使用HCSK作为根键的条件除外

不支持的终端安全评估条件

- 补救
-

宽限期

- 定期重新评估

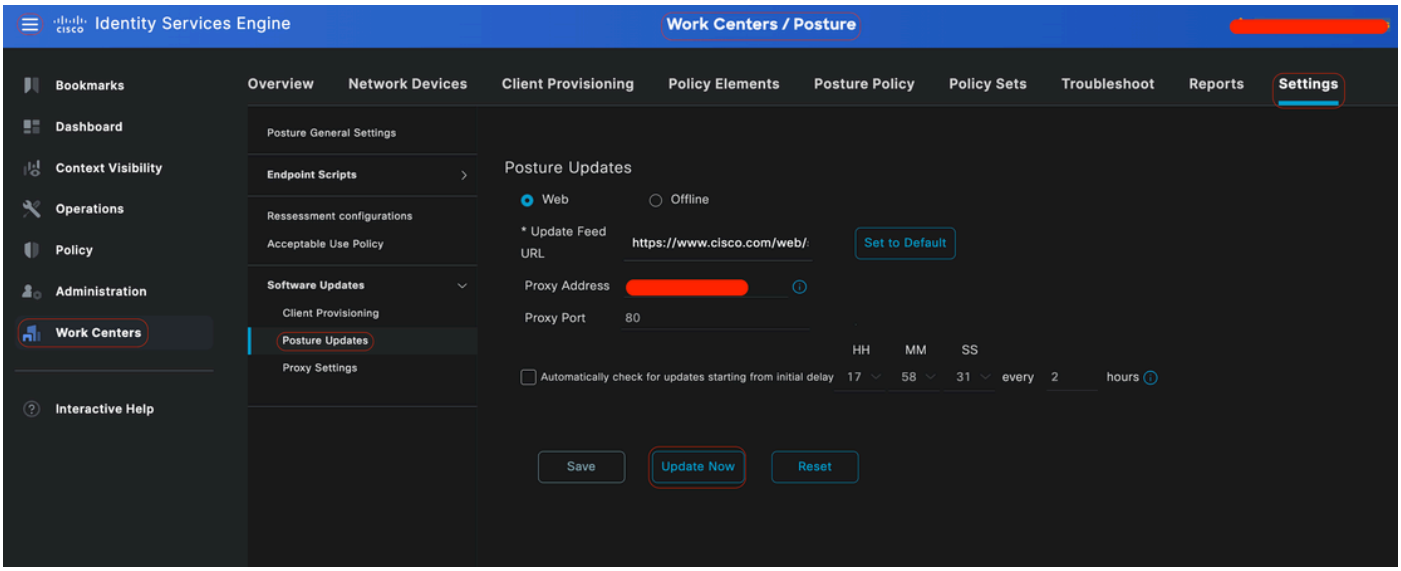
- 可接受的使用策略

配置ISE

更新状态馈送

建议先更新状态馈送，然后再开始配置状态。

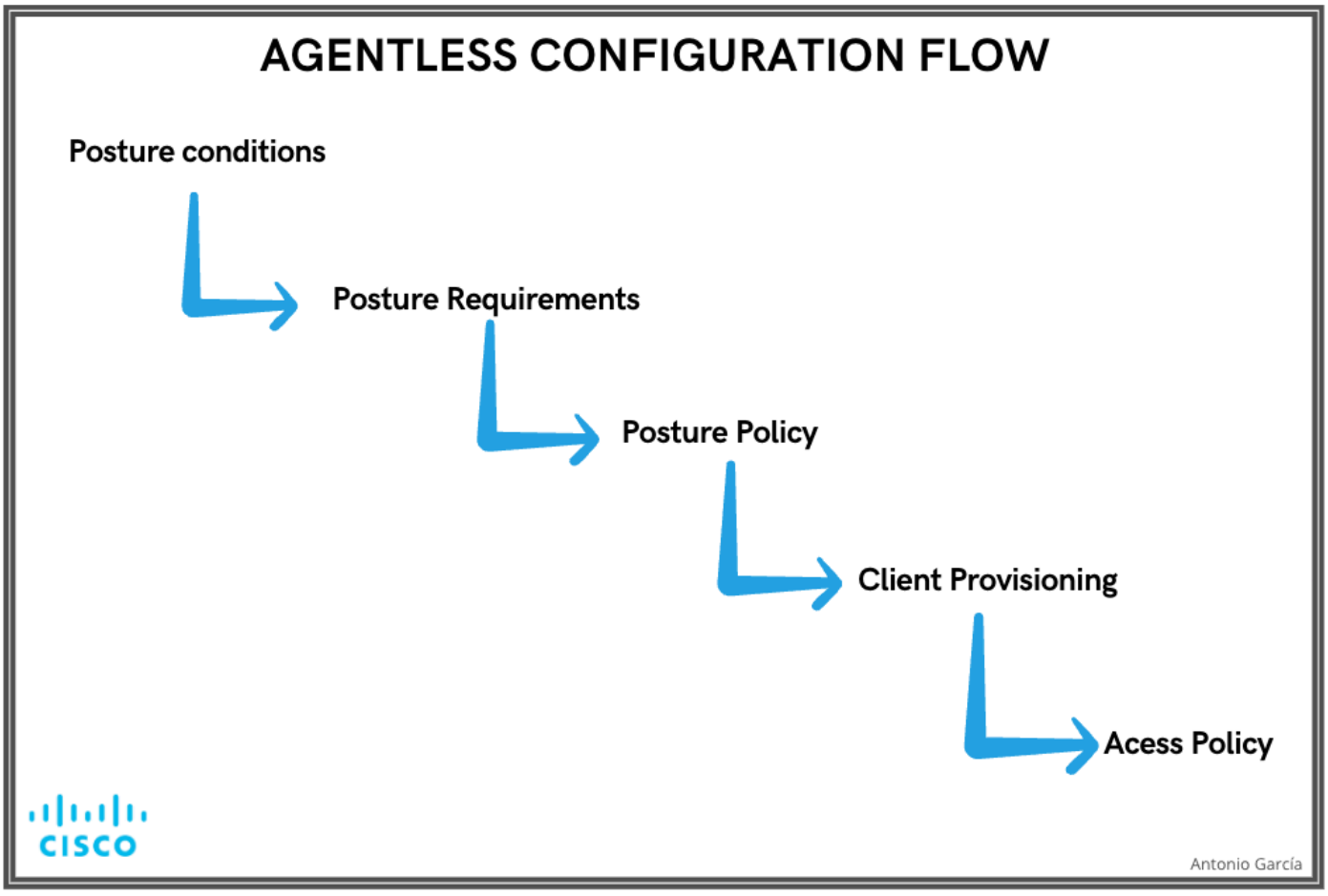
在思科ISE GUI中，点击Menuicon ()并选择**Work Centers > Posture > Settings** > **Software Updates** > **Update Now**。



更新状态馈送

状态无代理配置流程

状态无代理必须配置顺序，因为下一个配置需要第一个配置，依此类推。请注意，补救不在流程中；但是，本文档稍后将介绍配置补救的备选方案。



无代理配置流程

无代理状态配置

状况条件

状态条件是我们安全策略中定义合规端点的规则集。其中一些项目包括安装防火墙、防病毒软件、防恶意软件、修补程序、磁盘加密等。

在思科ISE GUI中，点击Menuicon ()并选择**Work Centers > Posture > Policy Elements** > Conditions，点击Add，并创建一个或多个使用Agentless posture的Posture条件**以确定要求**。创建条件后，单击**保存**。

在此方案中，名为**“Agentless_Condition_Application”的**应用条件使用以下参数配置：

·**操作系统**：Windows全部

此条件适用于任何版本的Windows操作系统，确保不同Windows环境的广泛兼容性。

·检查依据：流程

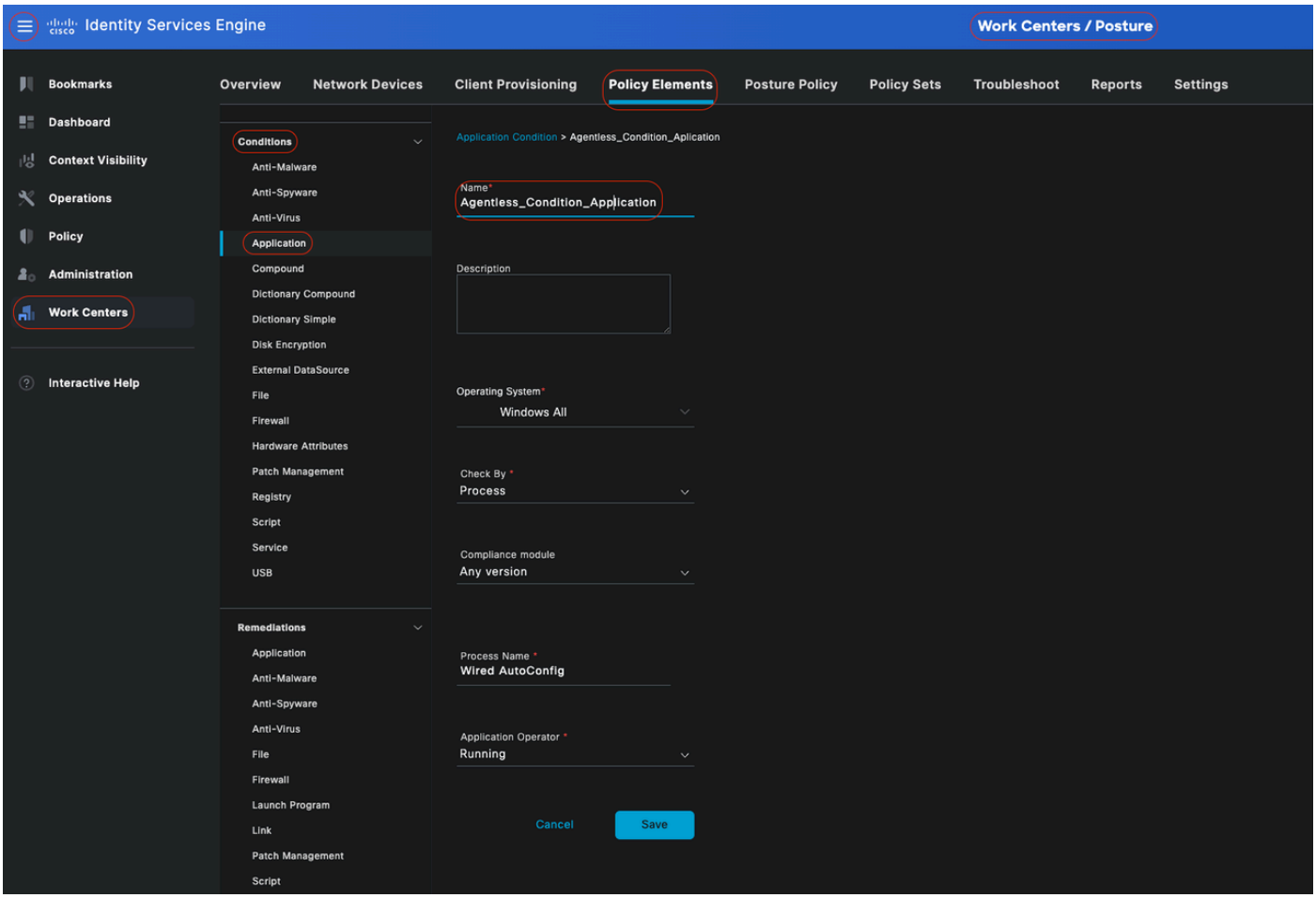
系统监控设备内的进程。您可以选择**Process**或**Application**；在这种情况下，选择**Process**。

·进程名称：有线自动配置

有线自动配置进程是进程兼容模块将签入设备。此过程负责配置和管理有线网络连接，包括IEEE 802.1X身份验证。

·应用操作员：运行

合规性模块验证**有线AutoConfig**进程是否当前正在设备上运行。您可以选择**Running**或**Not Running**。在本示例中，选择**Running**以确保该进程处于活动状态。



无代理条件

状态要求

状态要求是一组复合条件或仅一个可与角色和操作系统链接的条件。连接到网络的所有客户端必须满足安全评估期间的强制性要求，才能在网络上合规。

在思科ISE GUI中，点击Menuicon ( )并选择**Work Centers** > **Posture** > **Policy Elements** > **Requirement**。 点击下箭头并选择**Insert** new **Requirement**，然后创建一个或多个

使用无代理状态的**PostureRequirement**。创建**要求**后，点击**完成**，然后点击**保存**。

在本例中，名为**“Agentless_Requirement_Application”的**应用要求使用以下标准配置：

·**操作系统**：Windows全部

此要求适用于任何版本的Windows操作系统，确保它适用于所有Windows环境。

·状态类型：无代理

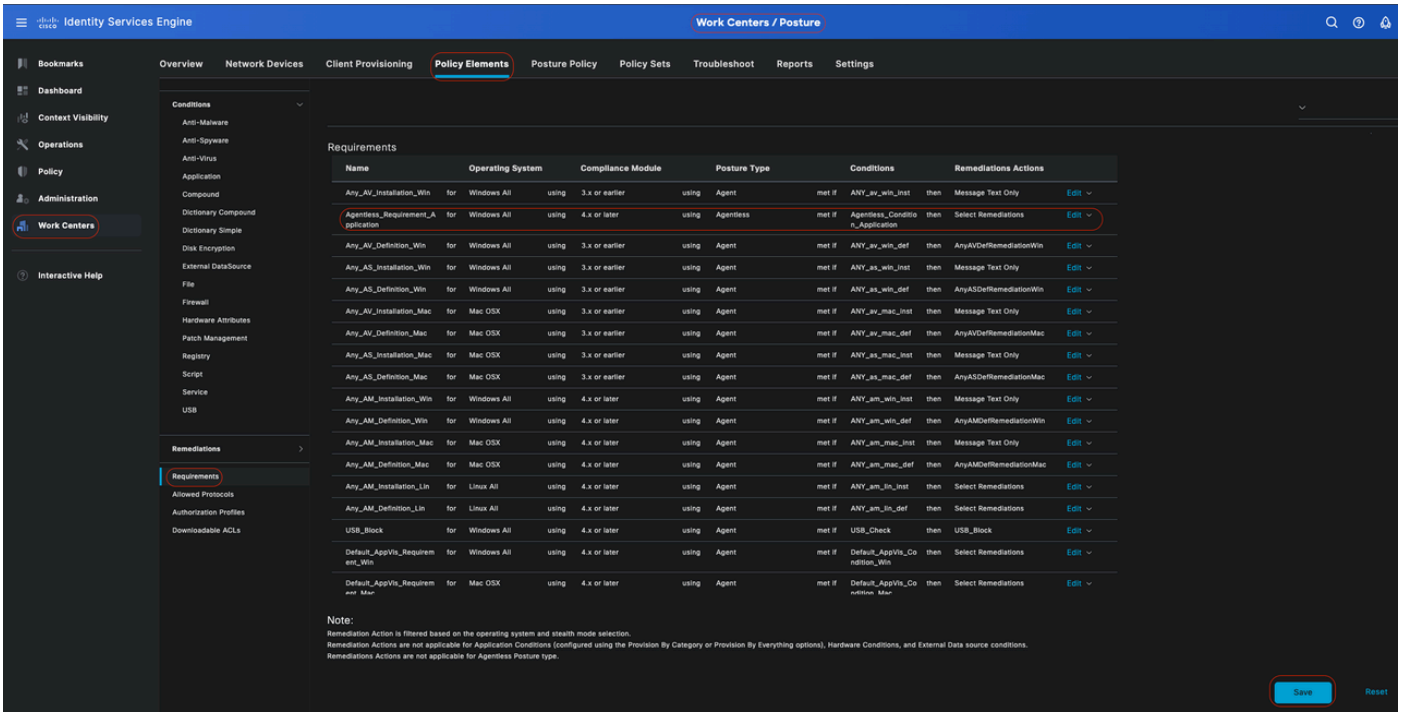
此配置是为无代理环境设置的。可用选项包括**Agent**、**Agent Stealth**、**Temporal Agent**和**Agentless**。在本场景中，选择了**Agentless**。

·条件：**Agentless_Condition_Application**

此关键字指定ISE终端安全评估模块和合规性模块将在设备进程内检查的条件。所选条件为**Agentless_Condition_Application**。

·补救措施：

由于此配置用于无代理环境，因此不支持补救操作，此字段将灰显。



无代理要求

安全评估策略

在思科ISE GUI中，点击Menuicon (

)并选择**Work Centers** > Posture > Posture **Policy**。 点击向下箭头，选择**Insert new Requirement**，然后创建一个或多个支持**Posture Policy**规则，这些规则使用无代理状态来满足该状态要求。 创建终端安全评估策略后，点击**完成**，然后点击**保存**。

在此场景中，名为**“Agentless_Policy_Application”的**安全评估策略已使用以下参数配置：

·**规则名称**：Agentless_Policy_Application

这是此配置示例中安全评估策略的指定名称。

·**操作系统**：Windows全部

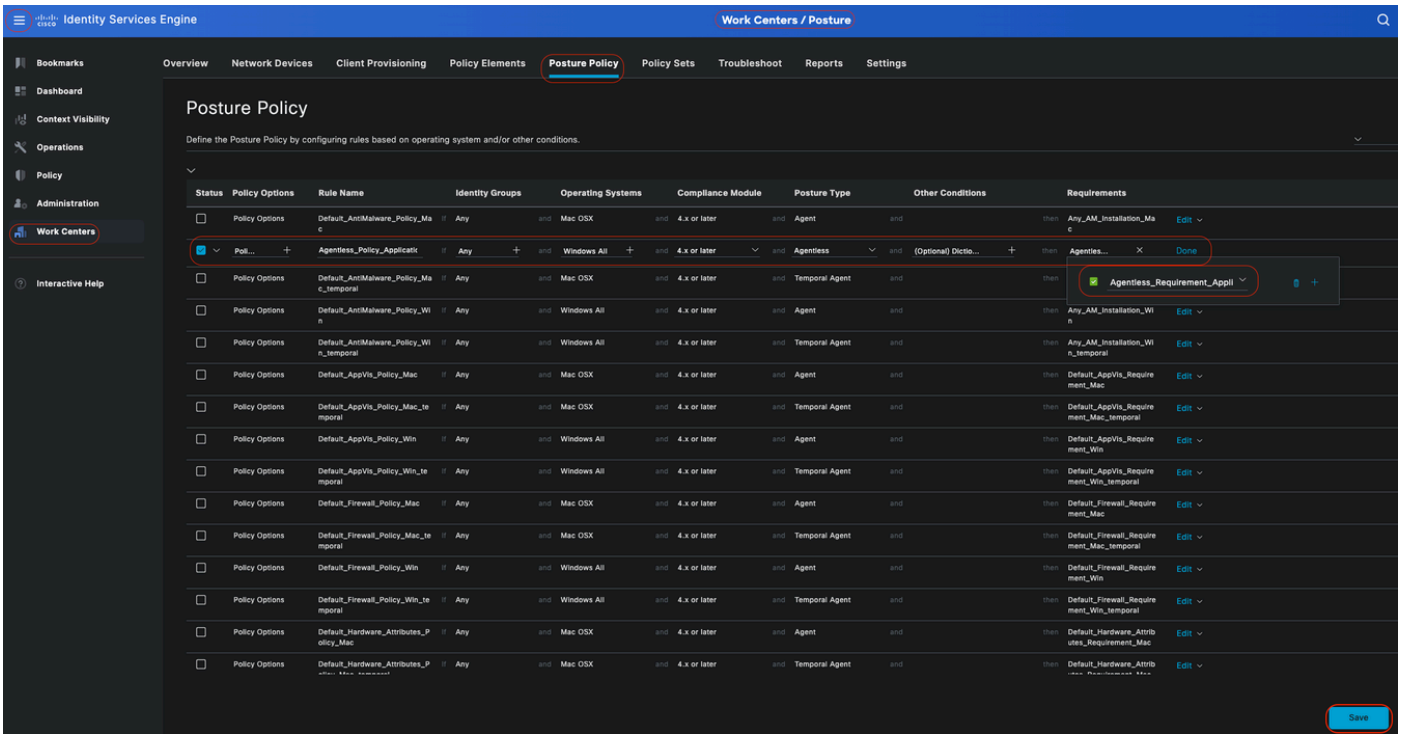
该策略已设置为应用于所有Windows操作系统版本，确保不同Windows环境的广泛兼容性。

·状态类型：无代理

此配置是为无代理环境设置的。可用选项包括**Agent**、**Agent Stealth**、**Temporal Agent**和**Agentless**。在本场景中，已选择**Agentless**。

·**其他条件**：

在此配置示例中，尚未创建其他条件。但是，您可以选择配置特定条件，以确保只有目标设备受此安全评估策略的约束，而不是网络上的所有Windows设备。这对于网络分段特别有用。



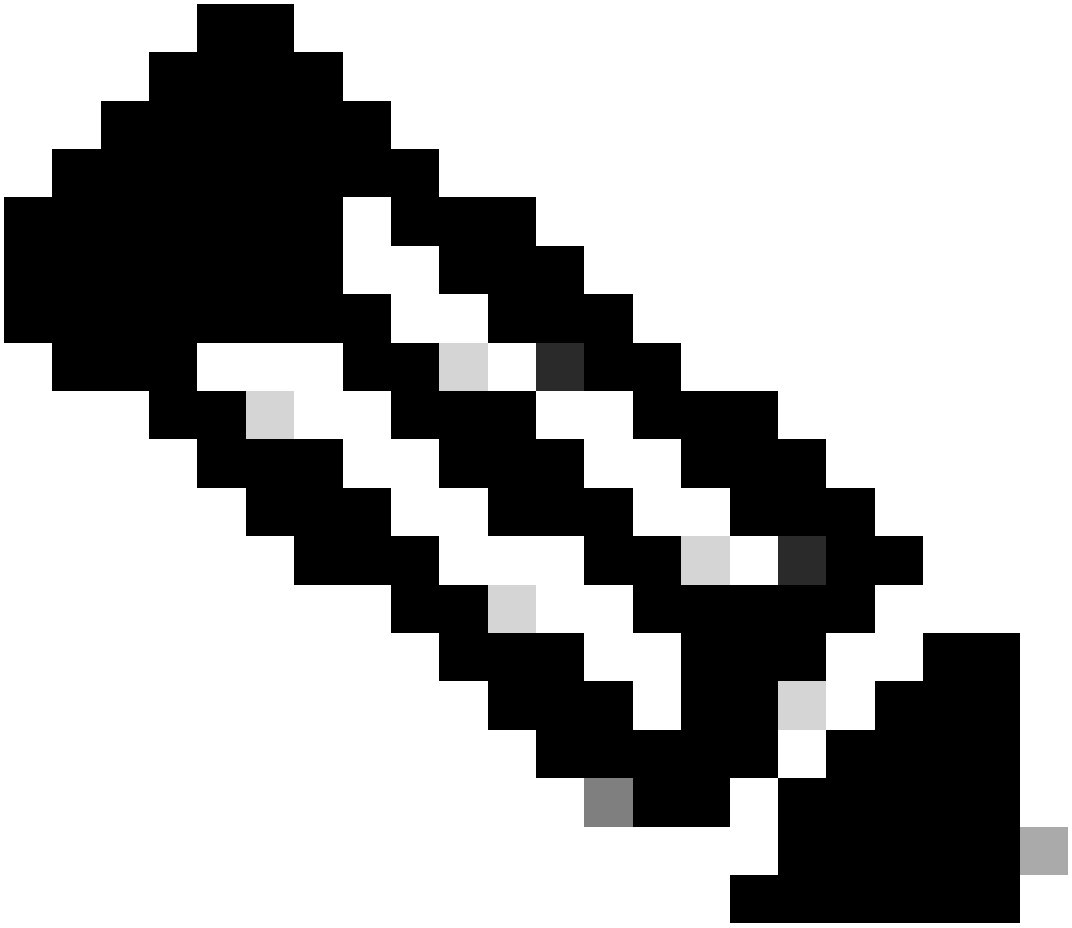
状态无代理策略

客户端调配

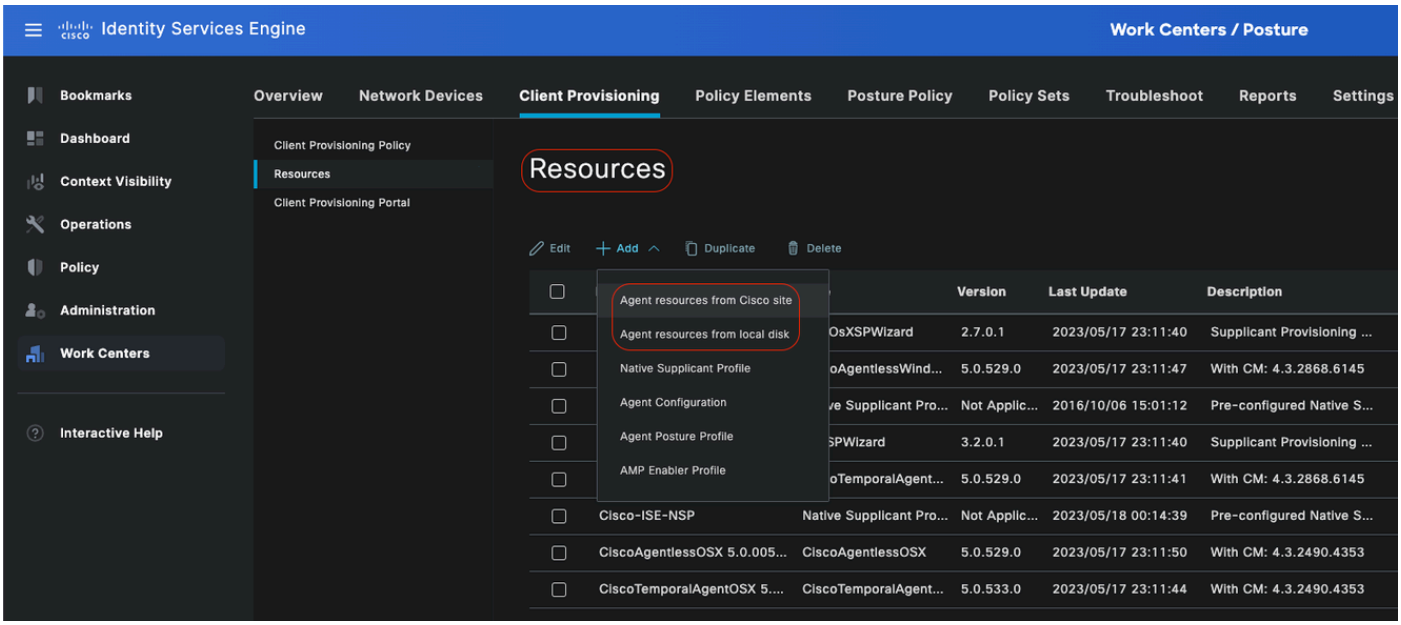
第1步-下载资源

要开始配置客户端调配，您必须首先下载所需的资源并在ISE中提供，以便您稍后可以在客户端调配策略中使用这些资源。

有两种将资源添加到ISE的方法：**Cisco站点的Agent Resources**和**Local disk的Agent Resources**。由于您正在配置无代理，因此您需要通过**思科站点上的代理**资源进行下载。



注意：要使用**思科站点的此代理资源**，ISE PAN需要访问互联网。



相关资源

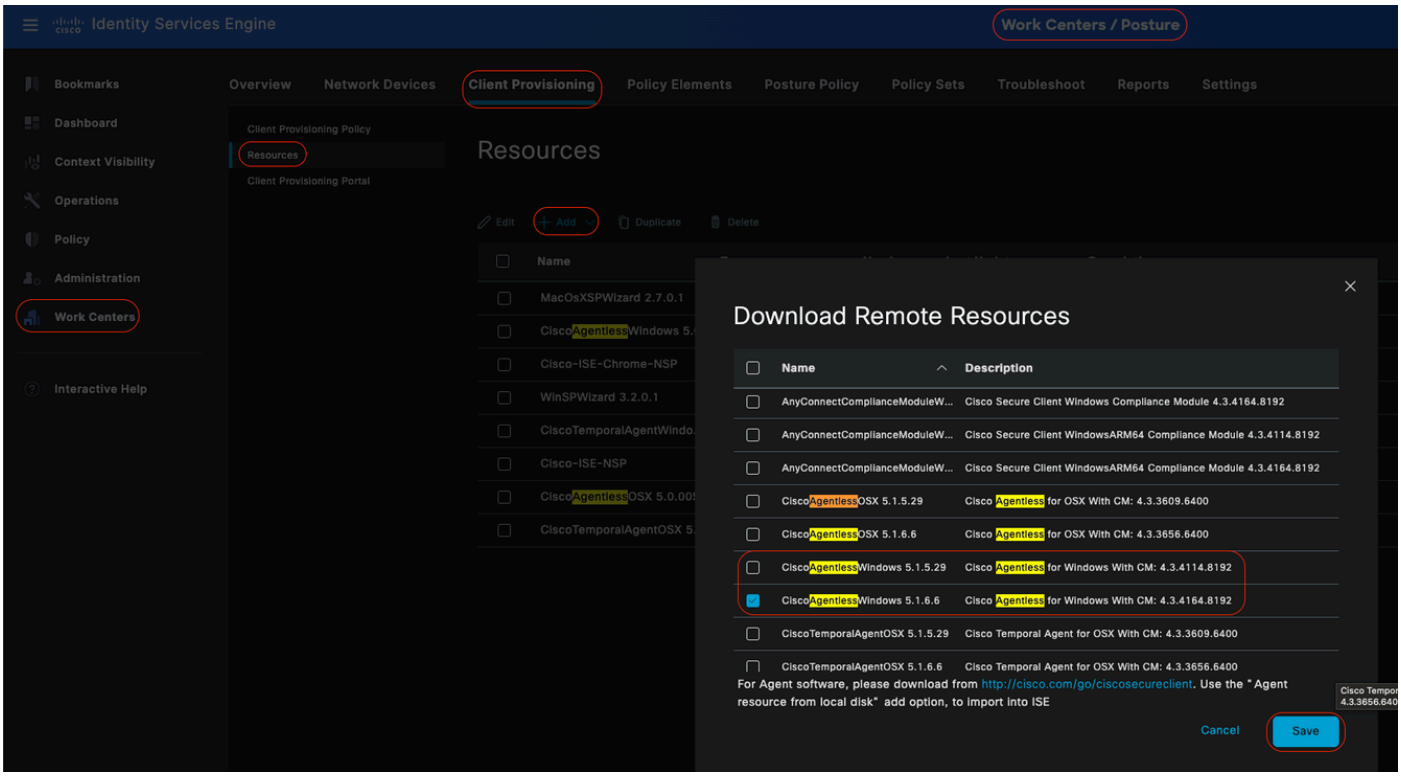
来自思科站点的座席资源

在思科ISE GUI中，点击Menuicon ( )并选择**Work Centers** > **Posture** > **Client Provisioning** > **Resources**。 单击**Add**，选择**Agent Resources from Cisco site**，然后单击**Save**。

您只能从思科站点下载合规性模块。系统显示要下载的两个最新合规性模块。已为此配置示例选择了资源包**CiscoAgentlessWindows 5.1.6.6**，该配置示例仅适用于Windows设备。

.

思科站点的



座席资源

第2步-配置客户端调配策略

配置终端安全评估代理时，您需要两种不同的资源(**AnyConnect**或**安全客户端**和**合规性模块**)，

将**代理配置**下的两个资源与**代理**状态配置文件进行映射，以便您能够在**客户端调配策略**中使用此**代理配置**。

但是，在配置安全评估无代理时，不需要配置**代理配置**或**代理安全**评估配置文件，您只需要从**思科站点的代理**资源下载无代理软件包。

在思科ISE GUI中，点击Menuicon ( )并选择**Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Policy**。 点击下箭头，然后选择**Insert new policy above**或**Insert new policy below**、**Duplicate above**或**Duplicate below**：

- 规则名称：**Agentless_Client_Provisioning_Policy**

此关键字指定客户端调配策略的名称。

- **操作系统**：Windows All

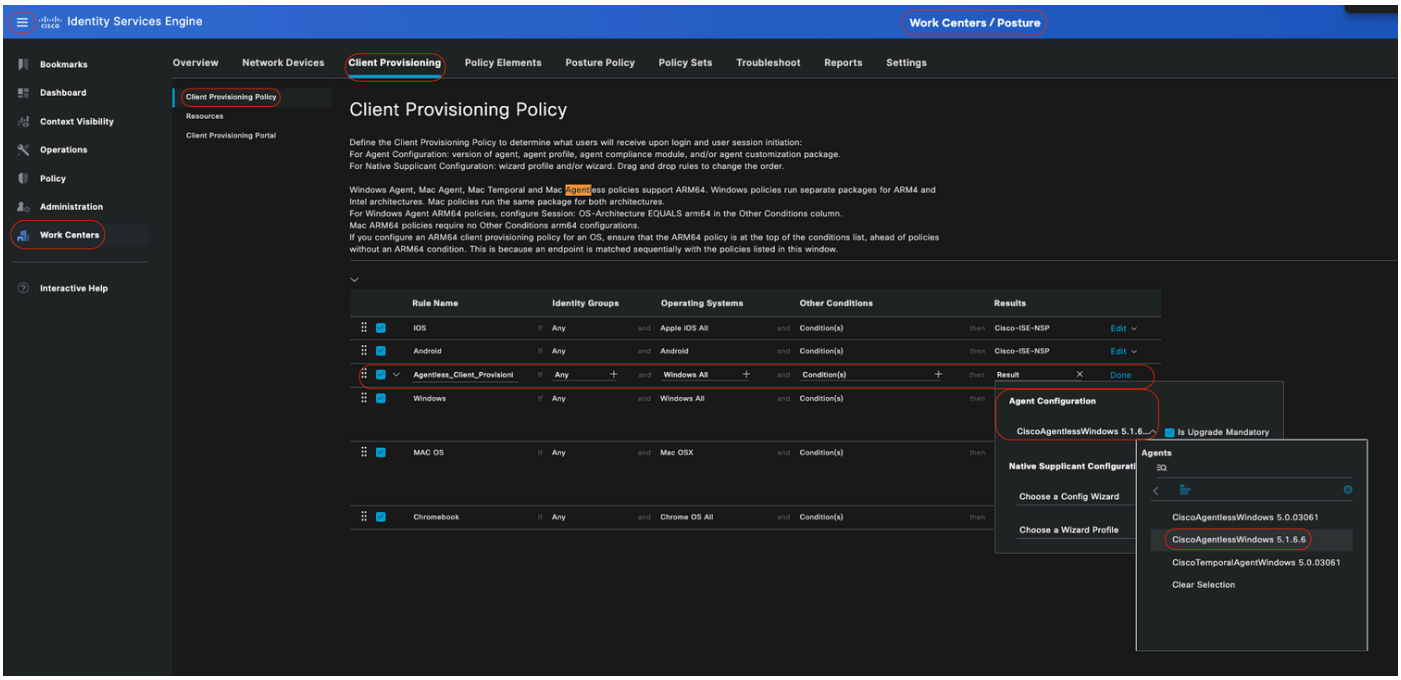
这可确保该策略适用于Windows操作系统的所有版本。

- **Other Conditions**：本示例中未配置任何特定条件。但是，您可以配置条件以确保仅所需设备与此客户端调配策略匹配，而不是匹配网络中的所有Windows设备。这对于网络分段尤其有用。

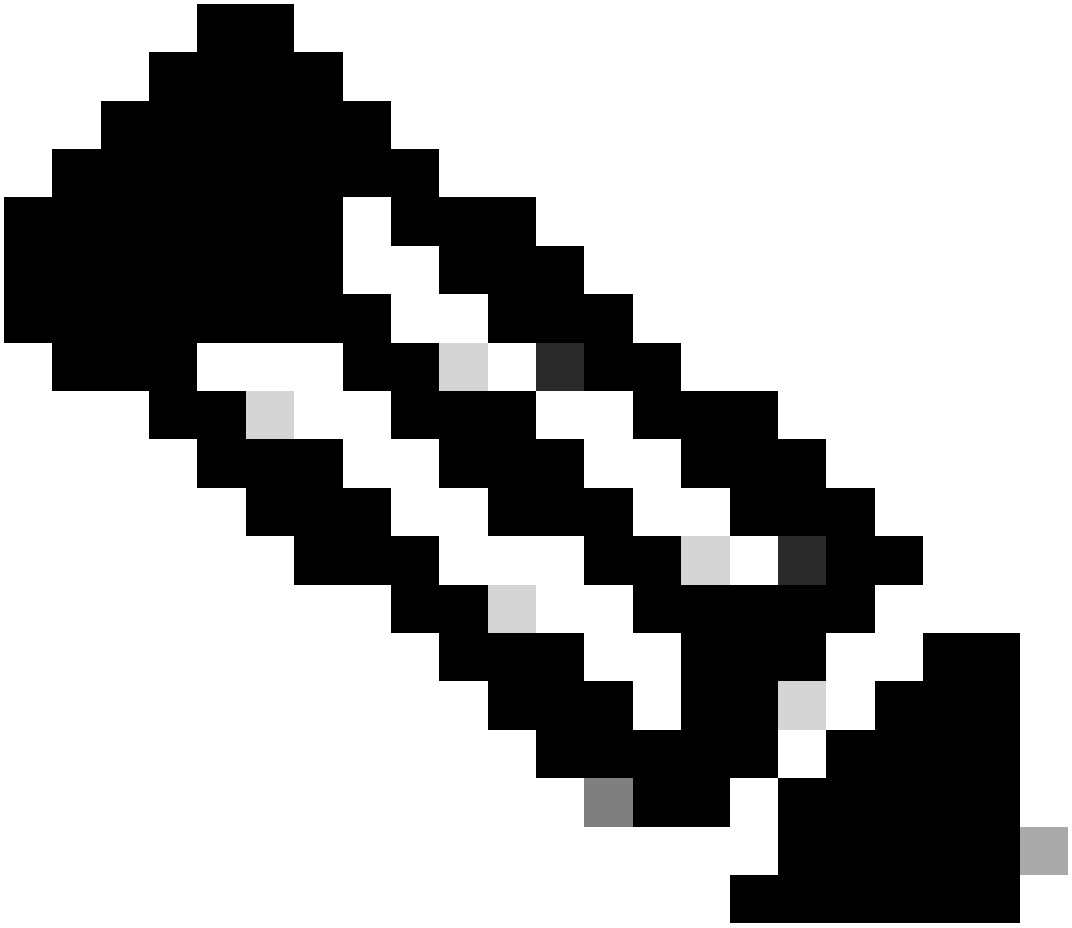
示例：，如果您使用的是Active Directory，您可以将Active Directory组整合到策略中，以细化受影响的设备。

- 结果：选择适当的程序包或配置代理。由于您是为无代理环境进行配置，因此请选择先前从**代理**资源（从**Cisco站点**）下载的软件包**CiscoAgentlessWindows 5.1.6.6**。此无代理软件包包含运行状态无代理所需的所有必要资源(**无代理**软件和**合**规性模块)。

•点击保存



无代理客户端调配策略



注意：确保只有一个客户端调配策略满足任何给定身份验证尝试的条件。如果同时评估多个策略，可能会导致意外行为和潜在冲突。

无代理**授权配置文件**

在思科ISE GUI中，点击Menuicon (

)并选择Policy > Policy **Elements > Results > Authorization > Authorization Profiles**并创建一个**Authorization** Profile来评估无代理状态的结果。

- 在此配置示例中，将授权配置文件命名为**Agentless_Authorization_Profile**。

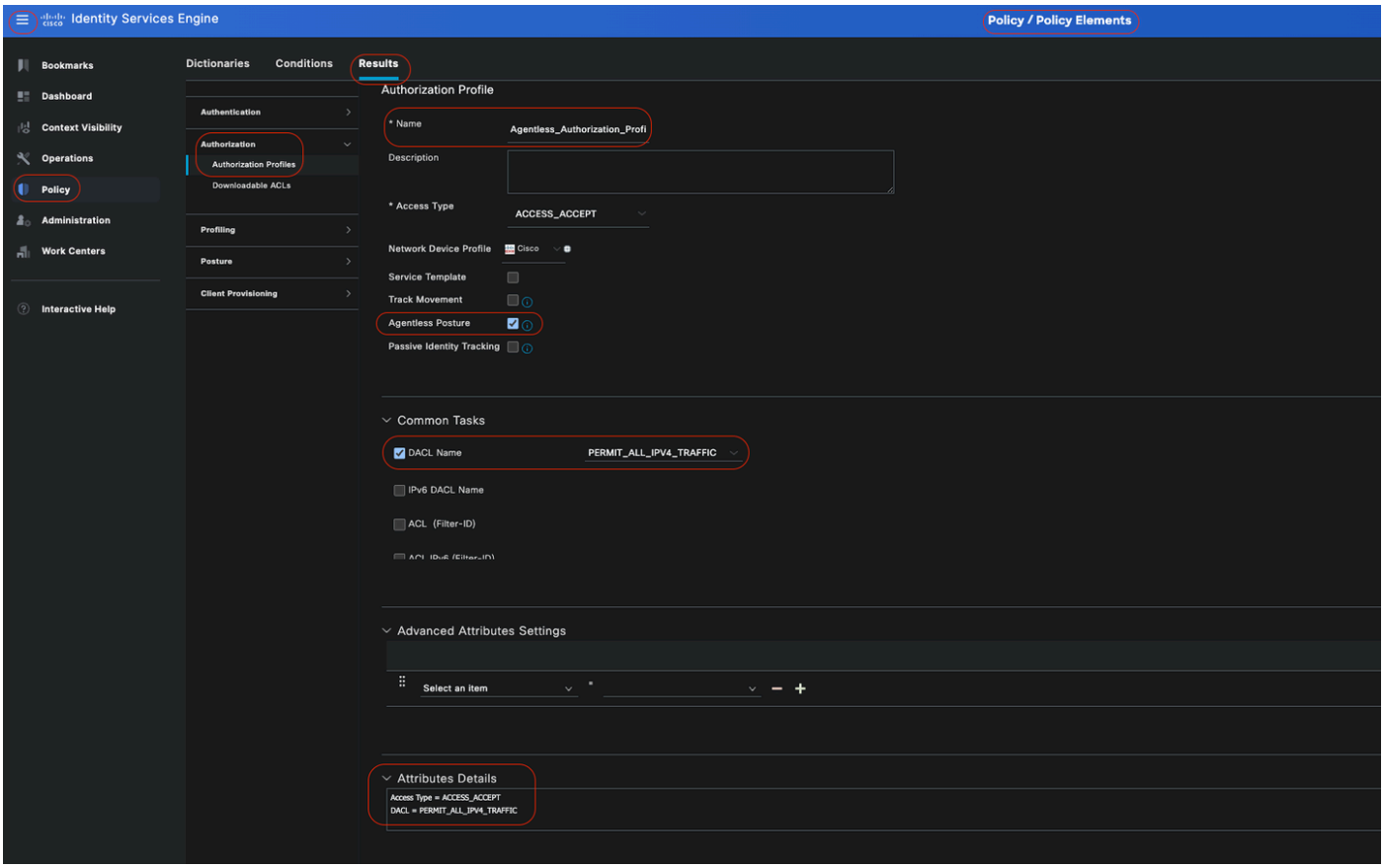
- 在授权配置文件中启用无代理状态。

- 此配置文件仅用于**Agentless Posture**。请勿将此情况用于其他安全评估类型。

- 无代理状态不需要CWA和重定向ACL。可以将VLAN、DACL或ACL用作分段规则的一部分。 为简单起见，除本配置示例中的无代理状态检查外，仅配置dACL（允许所有ipv4流量）。

-

单击**Save**。



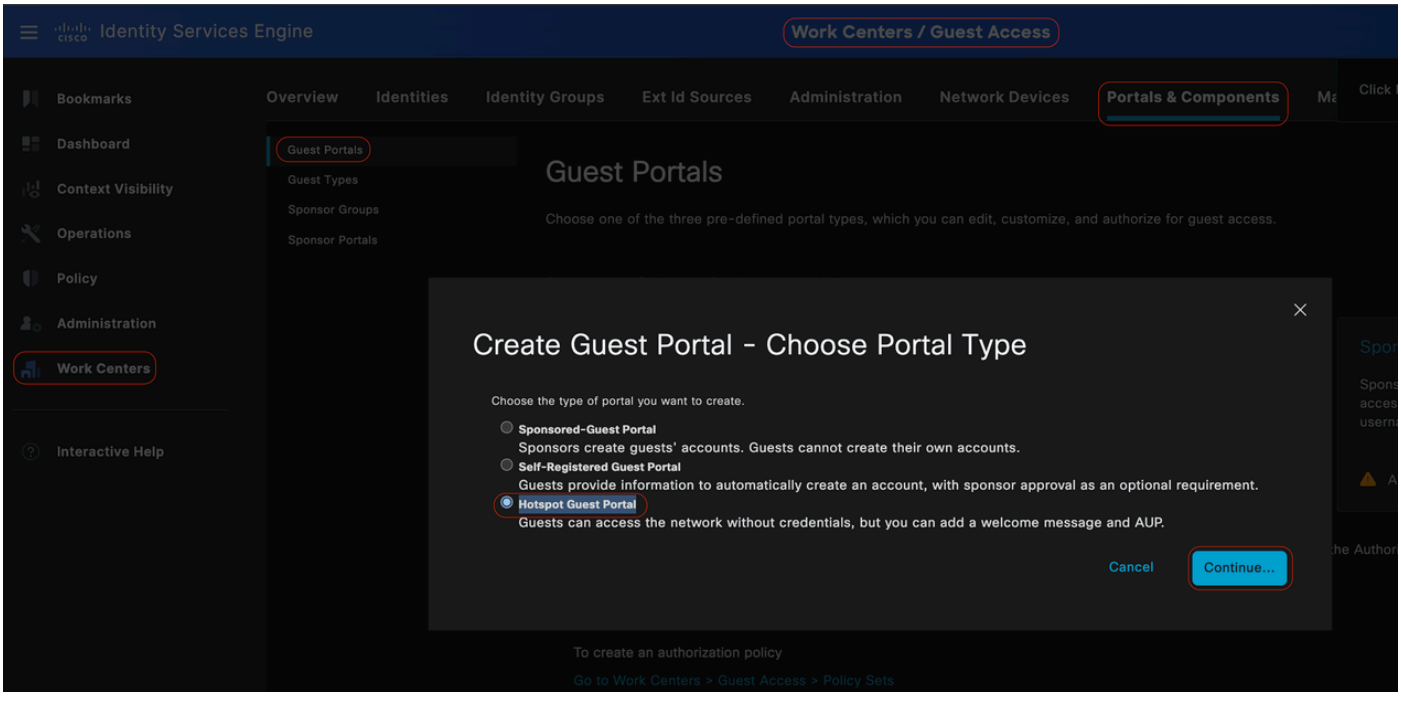
无代理授权配置文件

使用补救的替代方案（可选）

无代理流量中的补救支持不可用。为解决此问题，您可以实施自定义热点门户，以增强用户关于终端合规性的感知。当终端被识别为不合规时，可将用户重定向到此门户。此方法可确保用户了解其终端的合规状态，并可采取适当操作来纠正任何问题。

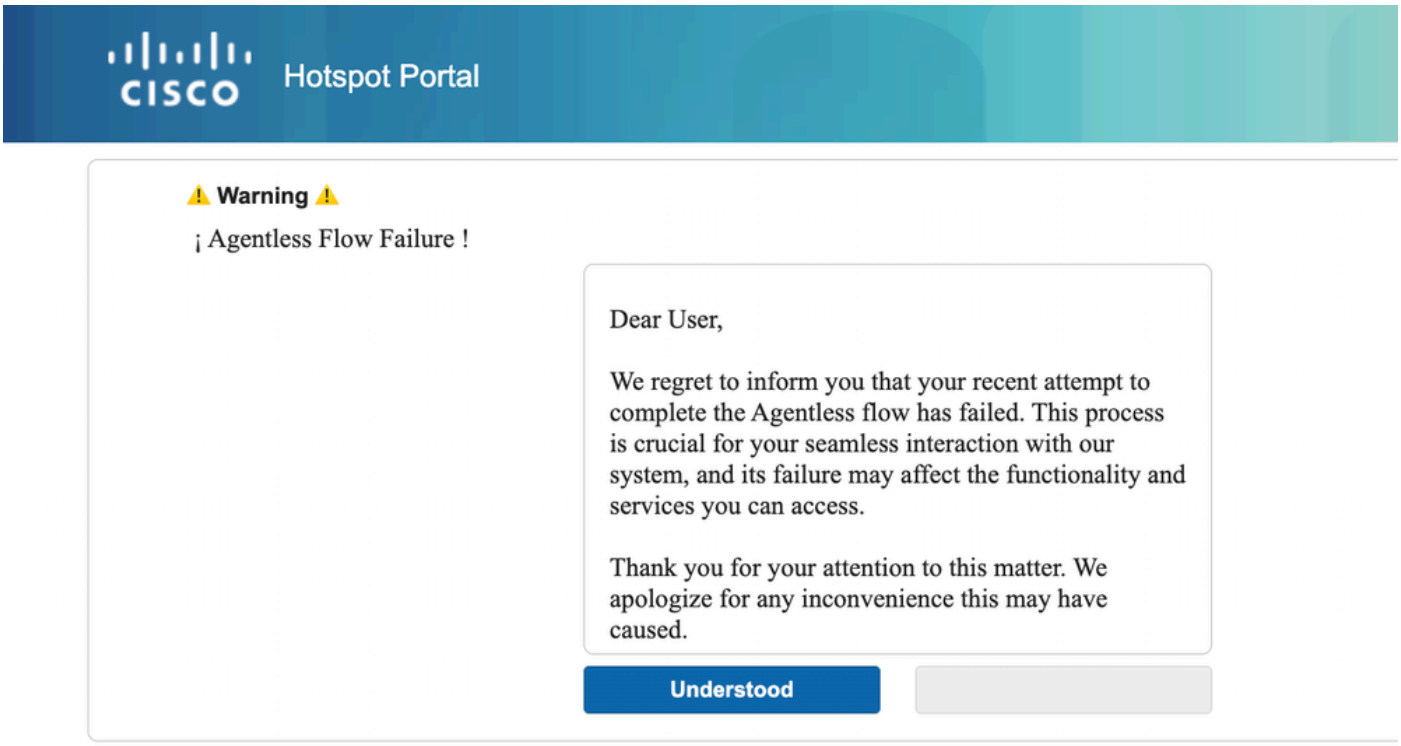
在思科ISE GUI中，点击Menuicon (

)，然后选择**工作中心(Work Centers)** > **访客访问权限(Guest Access)** > **门户和组件(Portals & Components)** >**访客门户(Guest Portals)**。 点击**创建**>选择**热点访客门户** > **继续**：。在此配置示例中，热点门户被命名为**Agentless_Warning**。



热点访客门户

在门户设置中，您可以自定义向最终用户显示的消息以符合您的特定要求，这只是自定义门户视图的一个示例：



故障状态无代理

补救授权配置文件（可选）

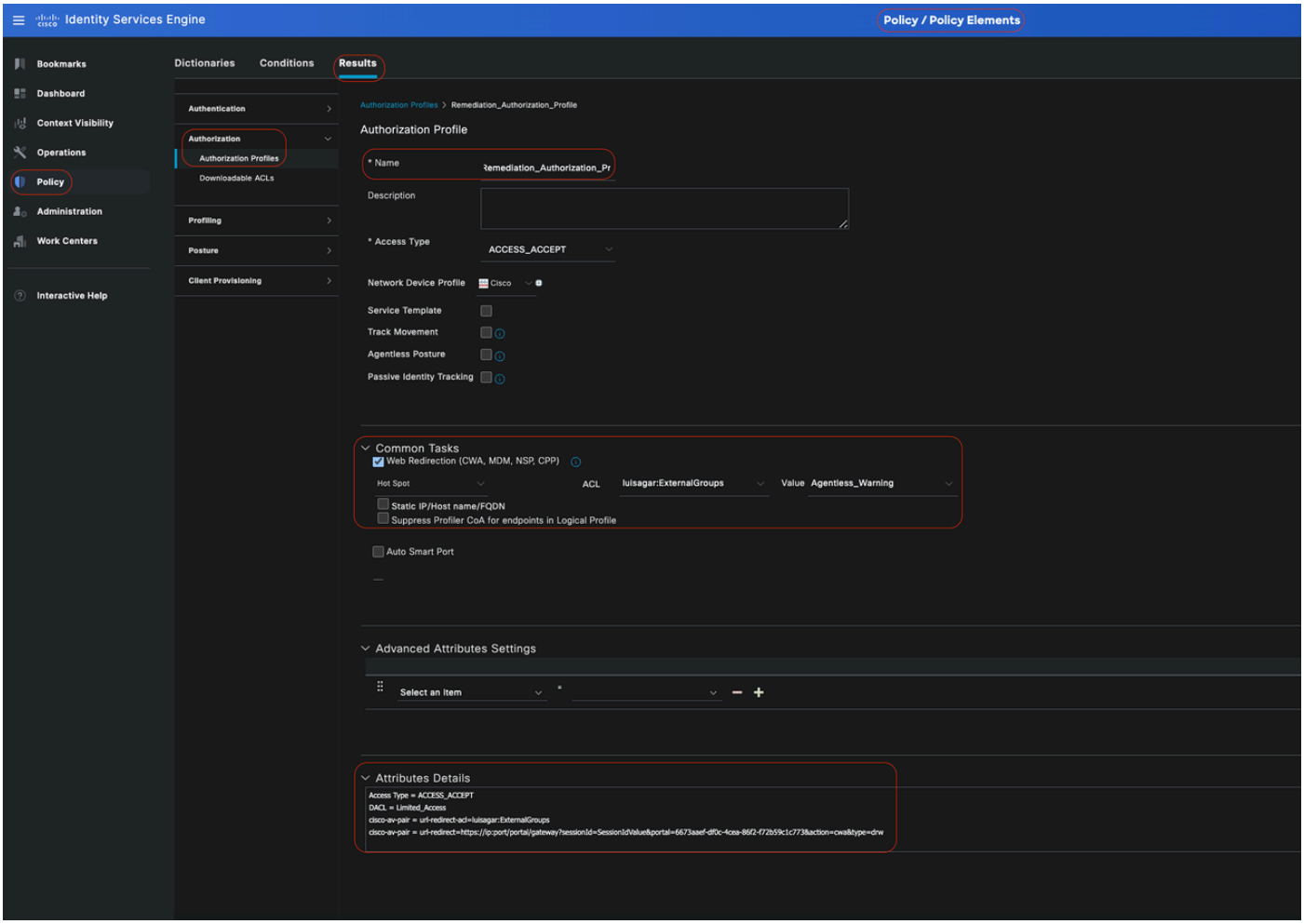
在思科ISE GUI中，点击Menuicon ( )并选择Policy > Policy **Elements > Results > Authorization > Authorization Profiles**并创建用于补救的**Authorization Profile**。

- 在此配置示例中，将授权配置文件命名为**Remediation_Authorization_Profile**。

- 为简单起见，本配置示例仅包括根据贵组织的特定需求而定制的名为**Limited_Access**的可下载访问控制列表(dACL)，该列表允许有限访问。

- 已配置**Web重定向**功能，包括外部组和热点，以增强用户关于终端合规性的感知。

- Click **Save**.

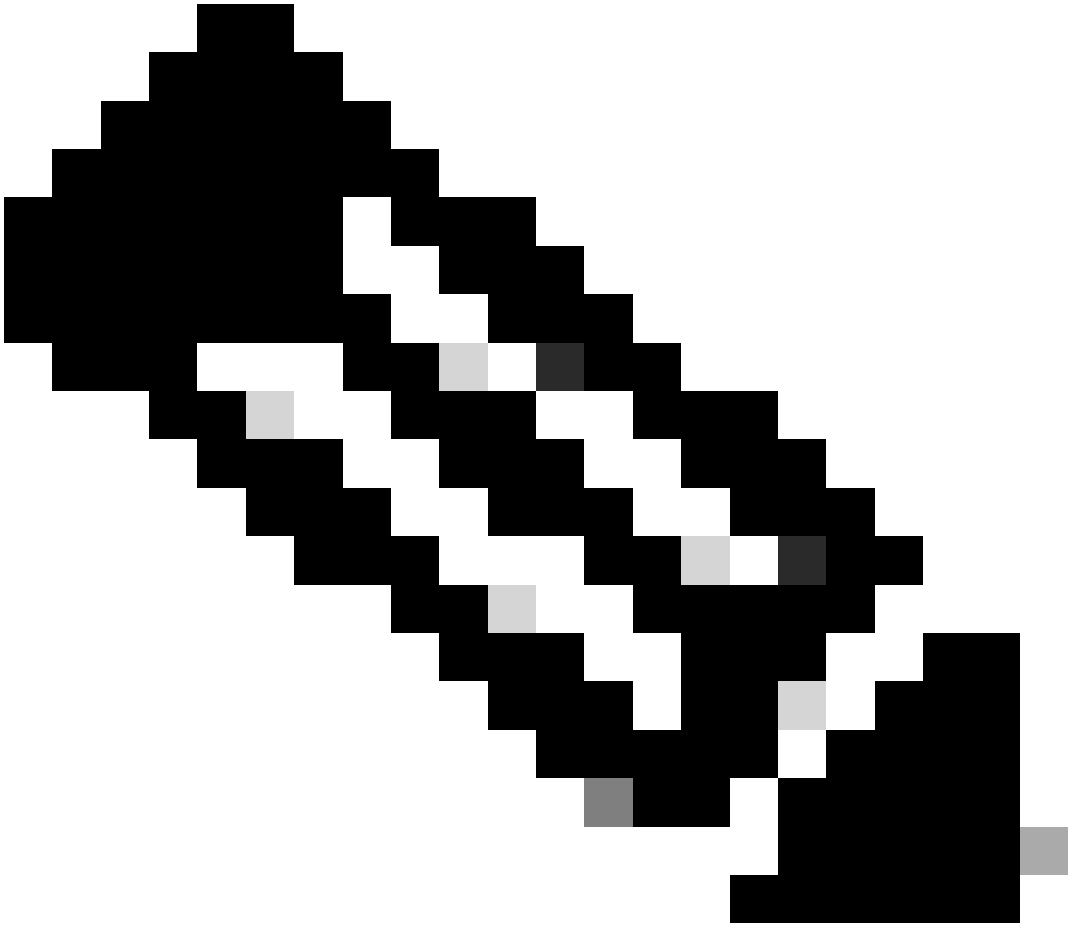


补救授权规则

无代理授权规则

在思科ISE GUI中，点击Menuicon (

)，然后选择策略 > 策略集并展开授权策略。启用并配置以下三个授权策略：



注意：必须按指定配置这些授权规则，以确保状态流正常运行。

Unknown_Compliance_Redirect：

•条件:

配置Network_Access_Authentication_Passed和**Compliance_Unknown_Devices**，并将结果设置为**Agentless Posture**。此条件触发无代理流量。

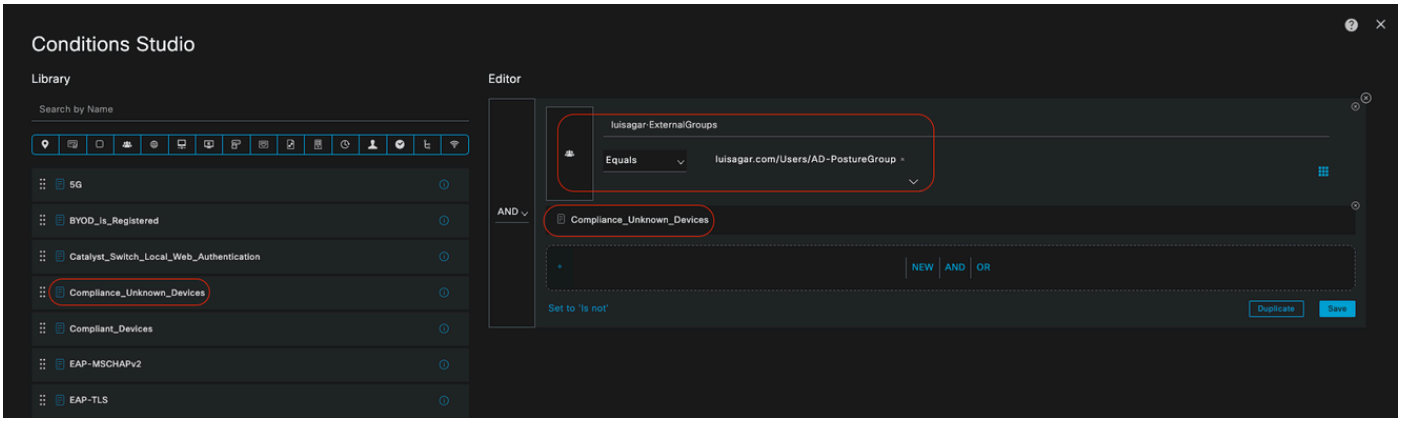
·示例条件：

配置Active Directory (AD)组条件以分段流量。

由于初始状态未知，必须配置**Compliance_Unknown_Devices**条件。

· **授权配置文件：**

将**Agentless_Authorization_Profile** 分配到此授权规则，以确保设备通过无代理状态流。 此条件包含无代理流量，因此符合此配置文件的设备可以启动无代理流量。



未知授权规则

NonCompliant_Devices_Redirect：

· **条件：**配置Network_Access_Authentication_Passed和Non_Compliant_Devices，结果设置为DenyAccess。或者，您可以使用remediation选项，如本示例所示。

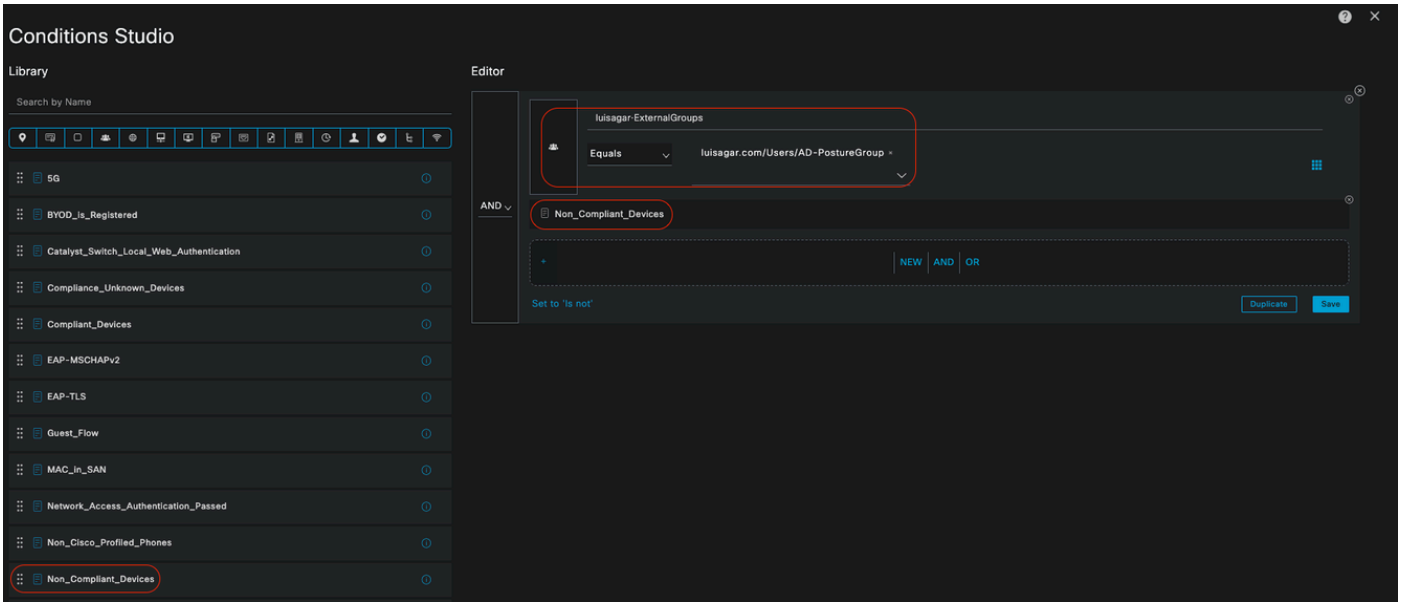
· **示例条件：**

配置AD组条件以分段流量。

安全评估状态不合规时，必须配置**Compliance_Unknown_Devices**条件以分配有限的资源。

· **授权配置文件：**

将**Remediation_Authorization_Profile** 分配给此授权规则，以通过热点门户向不合规设备通知其当前状态或**拒绝**访问。



不合规授权规则

Compliant_Devices_Access：

•条件:

配置Network_Access_Authentication_Passed和**Compliant_Devices**，结果集为**PermitAccess**。

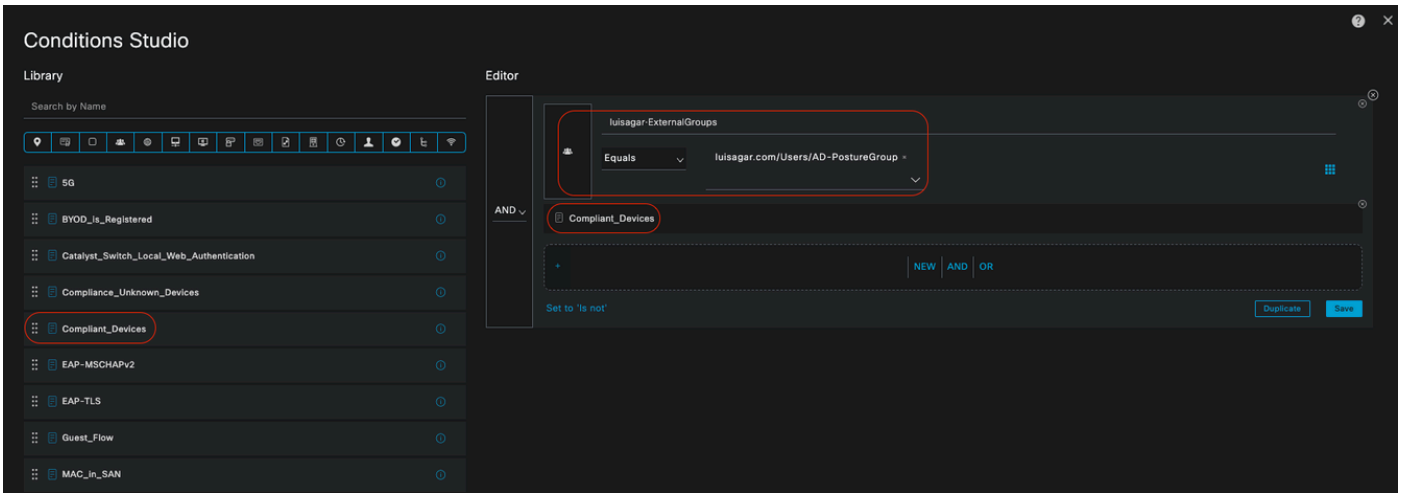
· 示例条件：

配置AD组条件以分段流量。

必须配置**Compliance_Unknown_Devices**条件，才能向合规设备授予适当的访问权限。

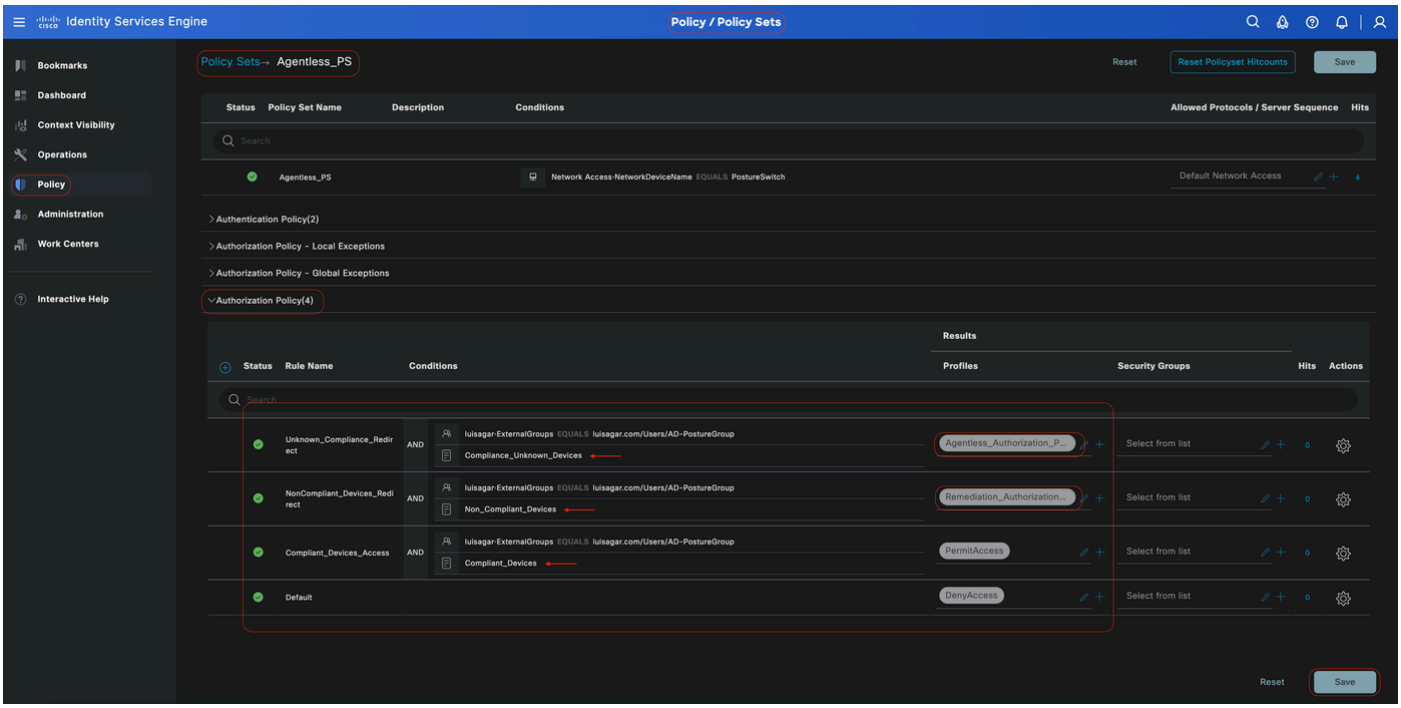
· 授权配置文件：

向此授权规则分配**PermitAccess**，以确保合规设备具有访问权限。此配置文件可自定义以满足贵组织的需求。



合规授权规则

所有授权规则



授权规则

配置终端登录凭证

在思科ISE GUI中，点击Menuicon ()并选择**Administration** > **Settings** > **Endpoint Scripts** > **Login Configuration**，然后配置客户端凭证以登录到客户端。

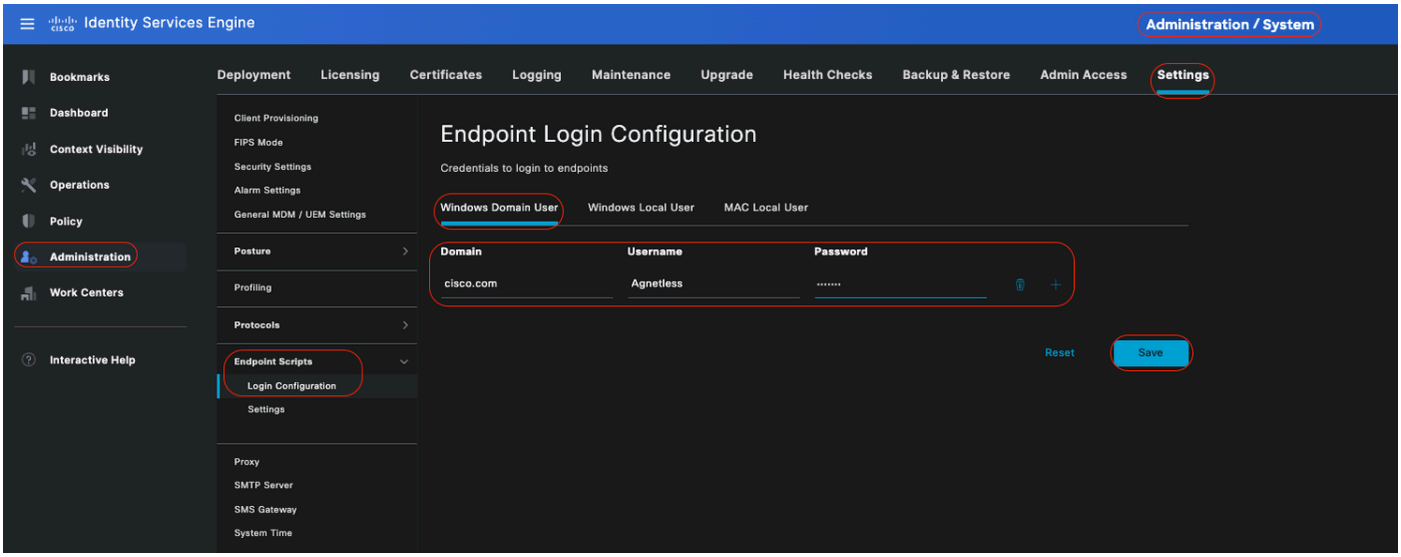
这些相同的凭证由终端脚本使用，因此Cisco ISE可以登录到客户端。

对于Windows设备，只需配置前两个选项卡(**Windows域用户和Windows本地用户)**

- **Windows域用户：**

配置Cisco ISE必须用来通过SSH登录客户端的域凭证。单击Plusicon并根据需要输入多个Windows登录。对于每个域，请在Domain、Username和Passwordfield中输入所需的值。如果配置域凭据，则会忽略Windows本地用户选项卡中配置的本地用户凭据。

如果您管理通过Active Directory域使用无代理状态评估的Windows终端，请确保提供域名以及具有本地管理权限的凭据。

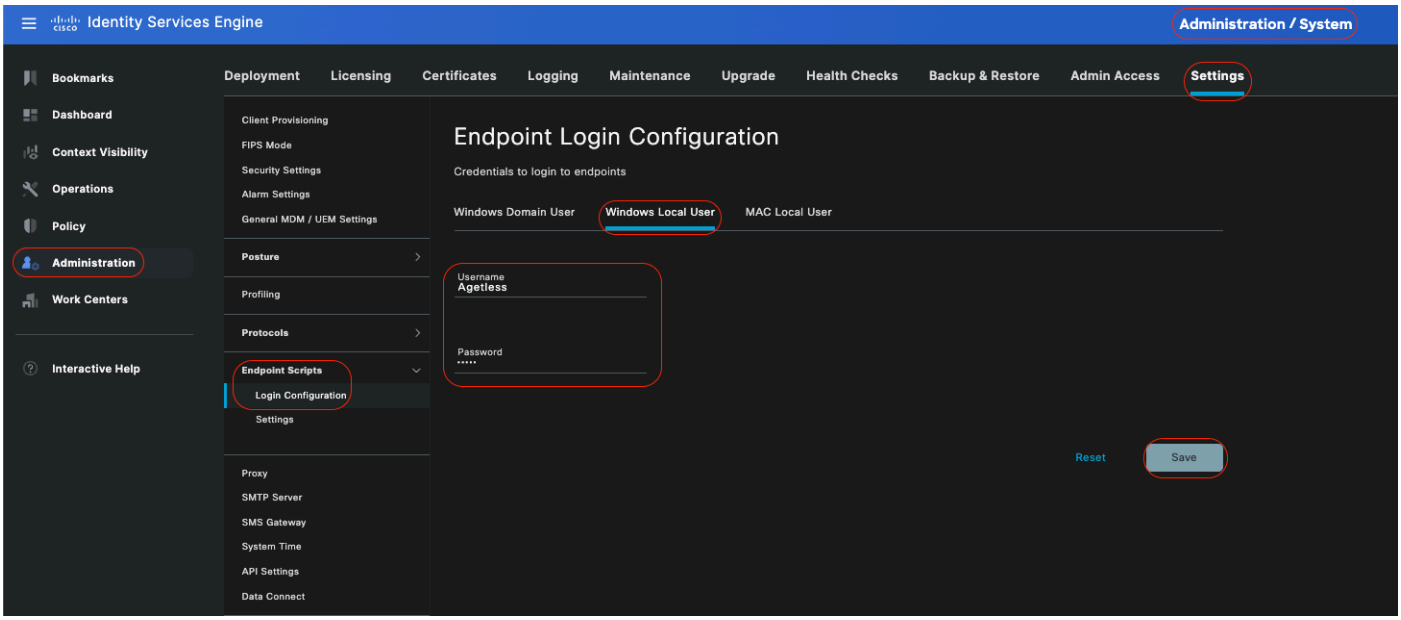


Windows域用户

- **Windows本地用户：**

配置Cisco ISE用于通过SSH访问客户端的本地帐户。本地帐户必须能够运行Powershell和Powershell remote。

如果不管理通过Active Directory域使用无代理状态评估的Windows终结点，请确保提供具有本地管理权限的凭据。

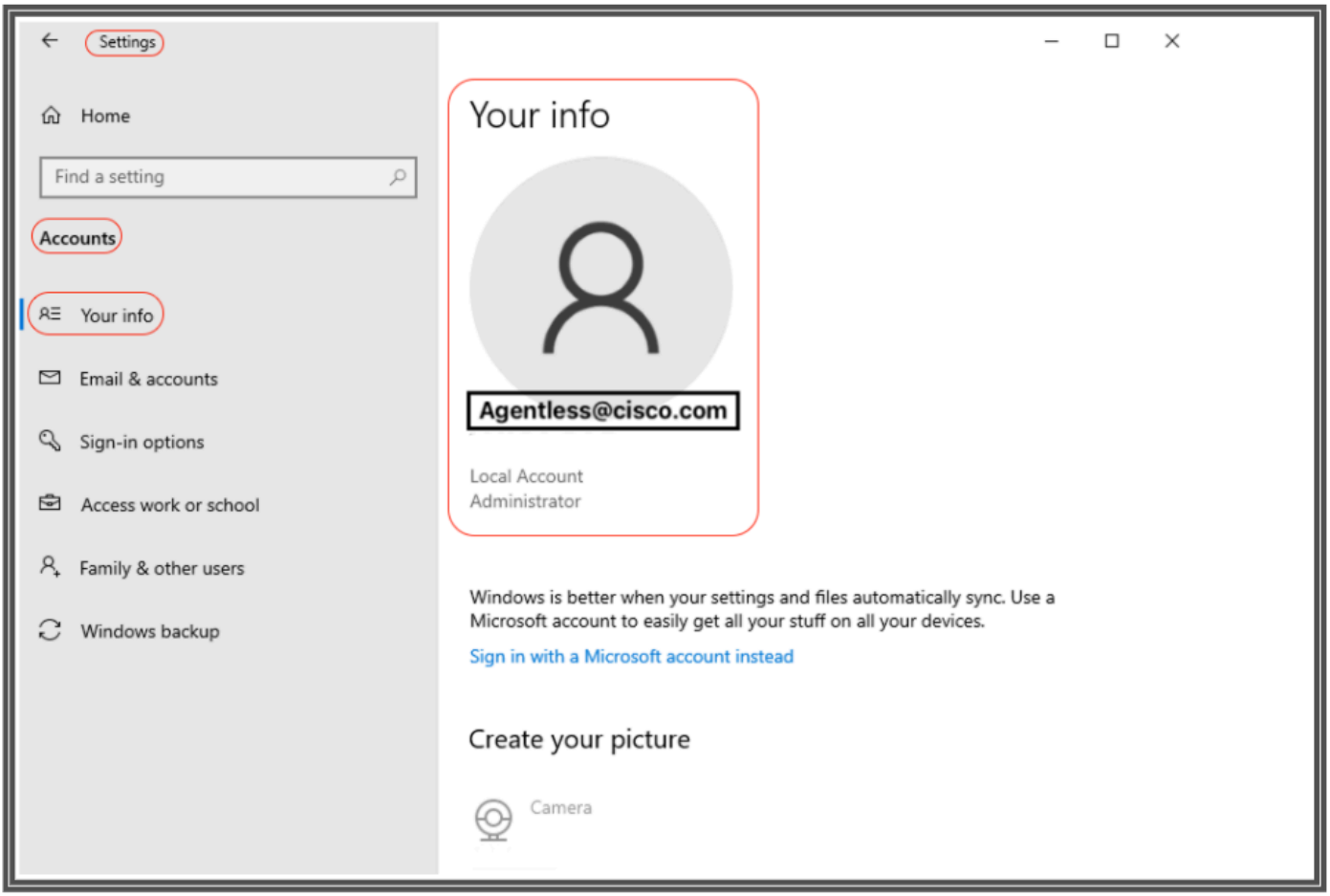


Windows本地用户

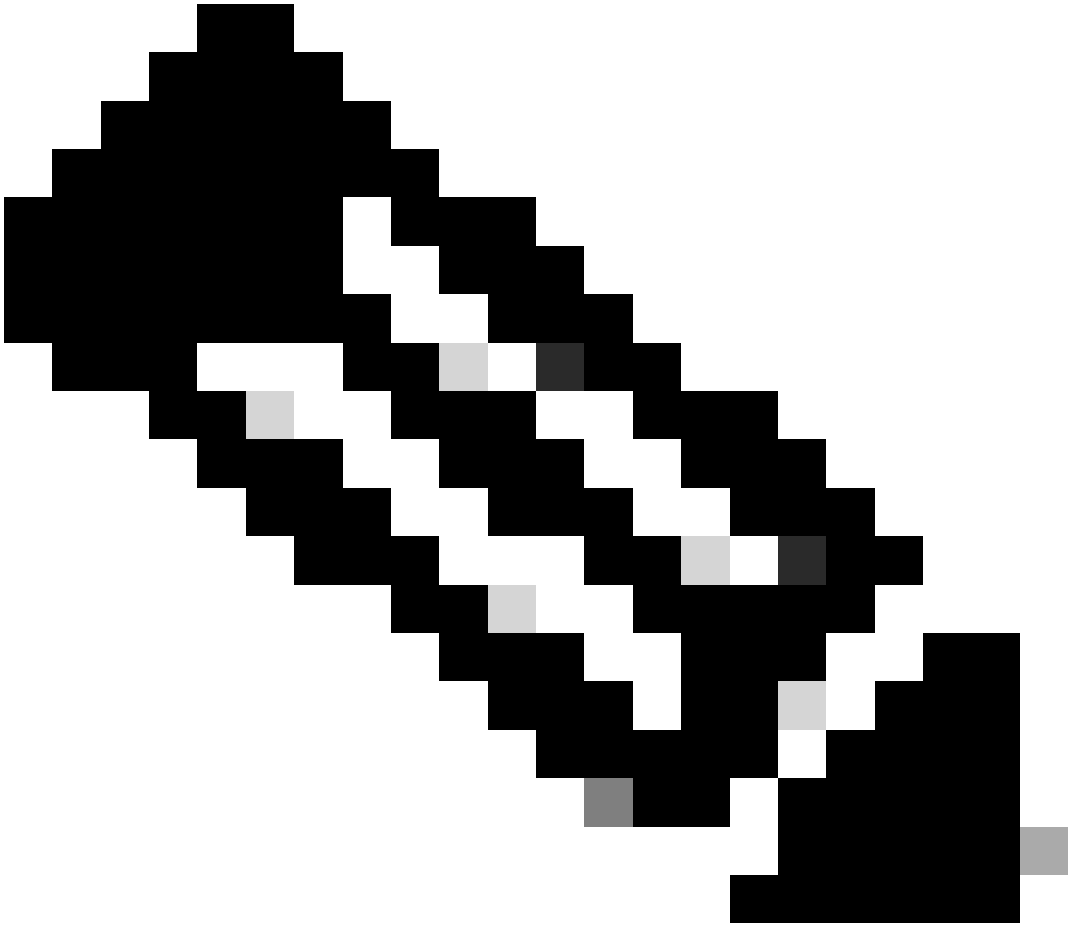
验证帐户

要验证您的Windows域用户和Windows本地用户帐户，以便您可以准确在“终端登录凭证”(Endpoint Login Credentials)下添加相应的数据，请使用此程序：

Windows本地用户：使用GUI（设置应用）单击**WindowsStart**按钮，选择**Settings**（齿轮图标），单击**Accounts**，然后选择**Your info**：


Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Windows backup
Your info
Agentless@cisco.com
Local Account
Administrator
Windows is better when your settings and files automatically sync. Use a Microsoft account to easily get all your stuff on all your devices.
Sign in with a Microsoft account instead
Create your picture
Camera

验证帐户



注意：对于MacOS，您可以参考**MAC本地用户**。但是，在此配置示例中，您不会看到MacOS配置。

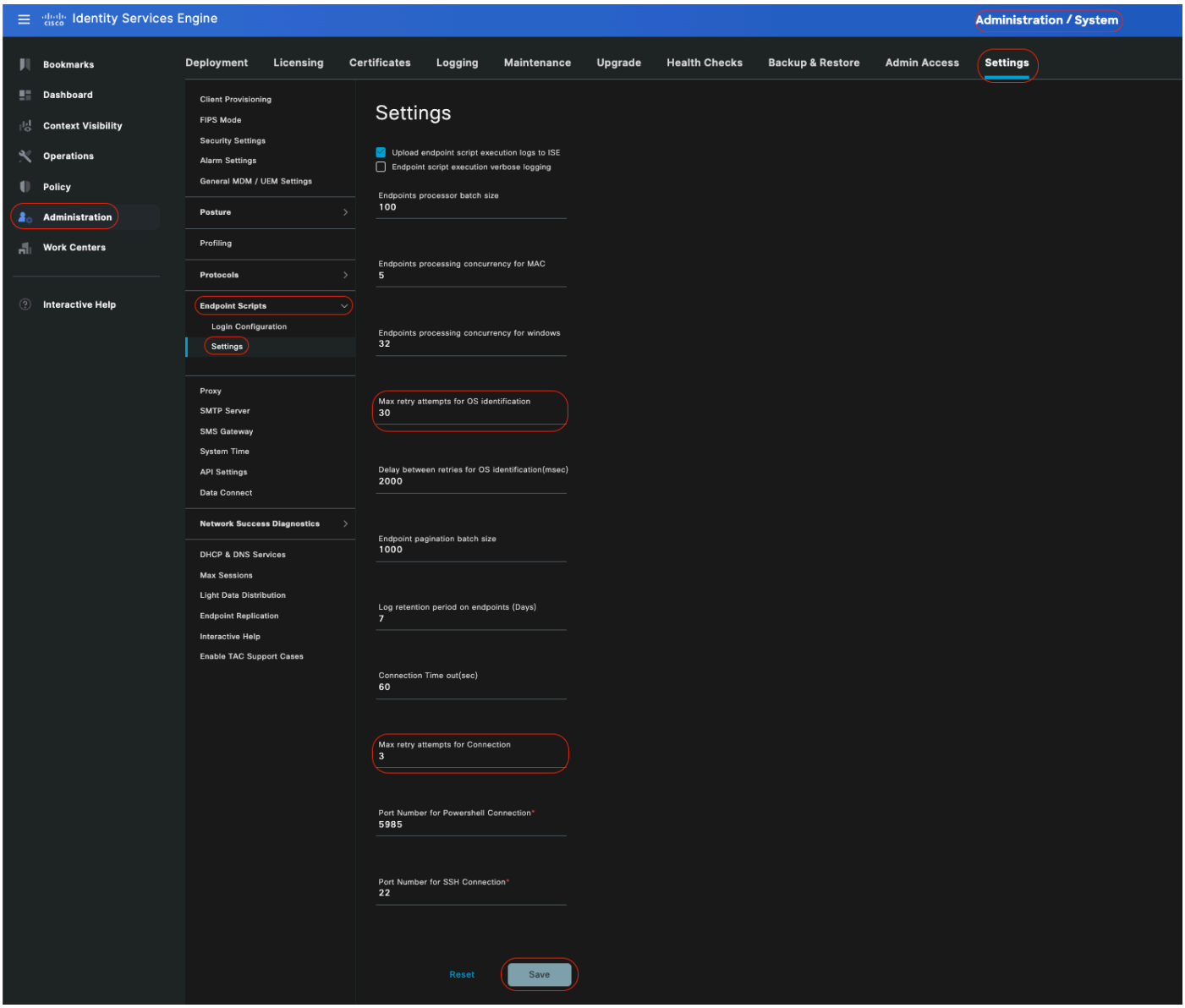
- **MAC本地用户：**配置Cisco ISE用于通过SSH访问客户端的本地帐户。本地帐户必须能够运行Powershell和Powershell remote。在Usernamefield中，输入本地帐户的帐户名。

要查看Mac OS帐户名称，请在终端中运行以下命令whoami：

设置

在思科ISE GUI中，点击Menuicon (
)并选择**Administration > Settings > Endpoint Scripts > Settings，并configureMax retry attempts** for OS identification、**Delay between retries for OS identification等**。这些设置决定了确认连接问题的速度。例如，只有在所有重试未用完之后，日志中才会显示PowerShell端口未打开的错误。

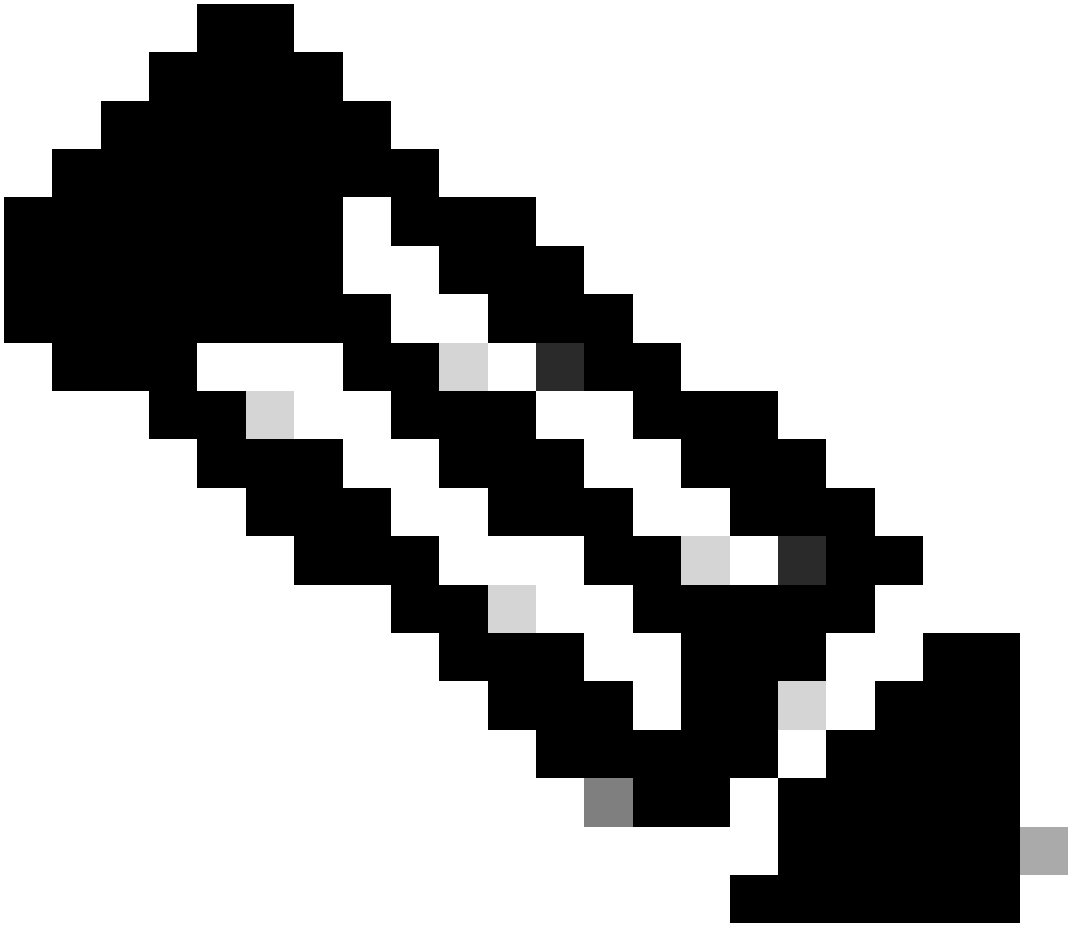
此屏幕截图显示默认值设置：



终端脚本设置

当客户端采用无代理状态进行连接时，您可以在实时日志中看到它们。

配置Windows终端并进行故障排除



注意：这些是一些建议以在Windows设备上检查并应用；但是，如果遇到诸如用户权限、PowerShell访问等问题，您必须参考Microsoft文档或联系Microsoft支持人员……

验证和故障排除前提条件

测试到端口5985的TCP连接

对于Windows客户端，必须打开端口5985以访问客户端上的powershell。运行此命令以确认到端口5985的TCP连接： **Test-NetConnection -ComputerName localhost -Port 5985**

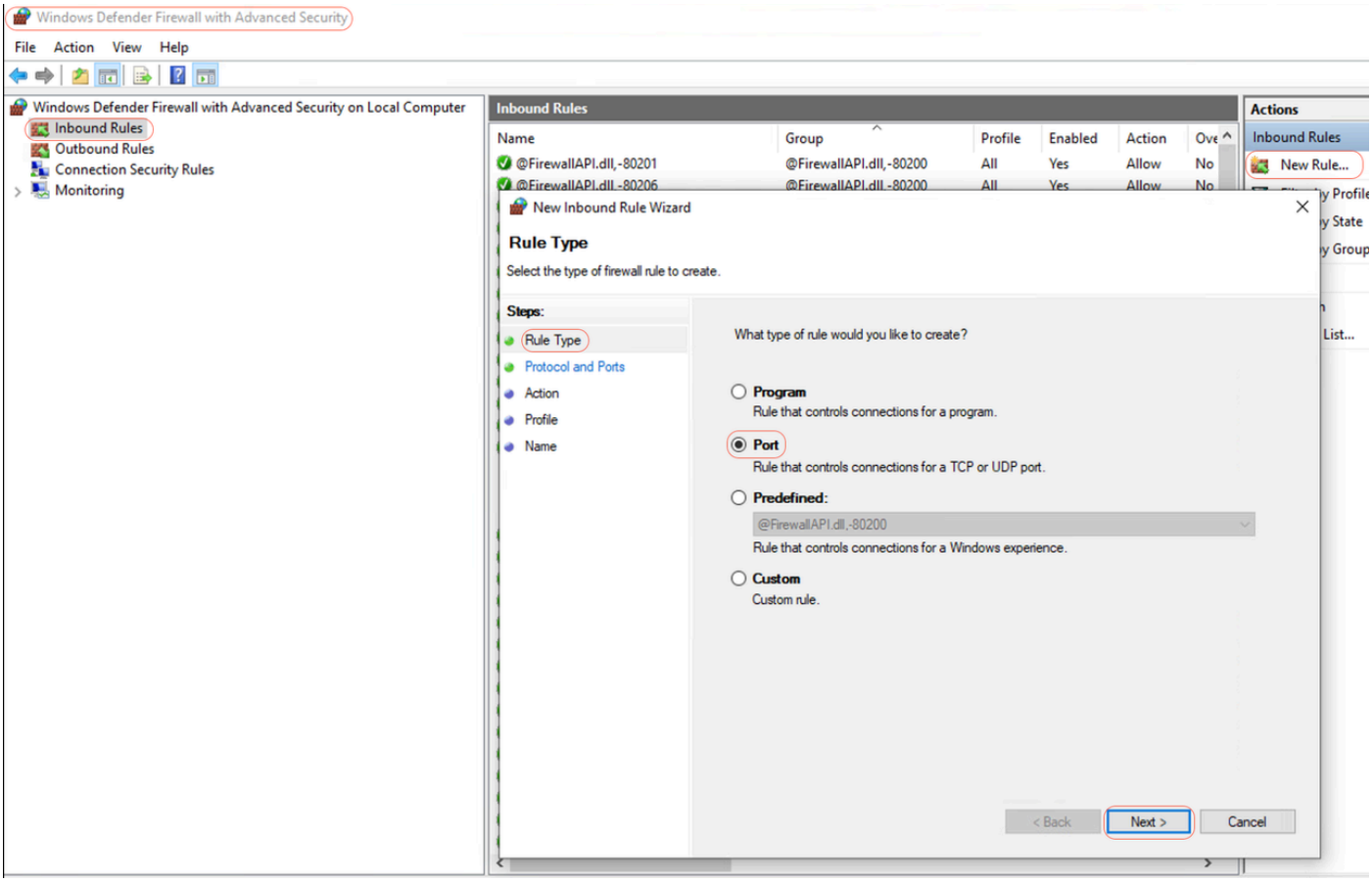
此屏幕截图中所示的输出表明到localhost上的端口5985的TCP连接失败。这意味着使用端口5985的WinRM（Windows远程管理）服务未运行或未正确配置。

```
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

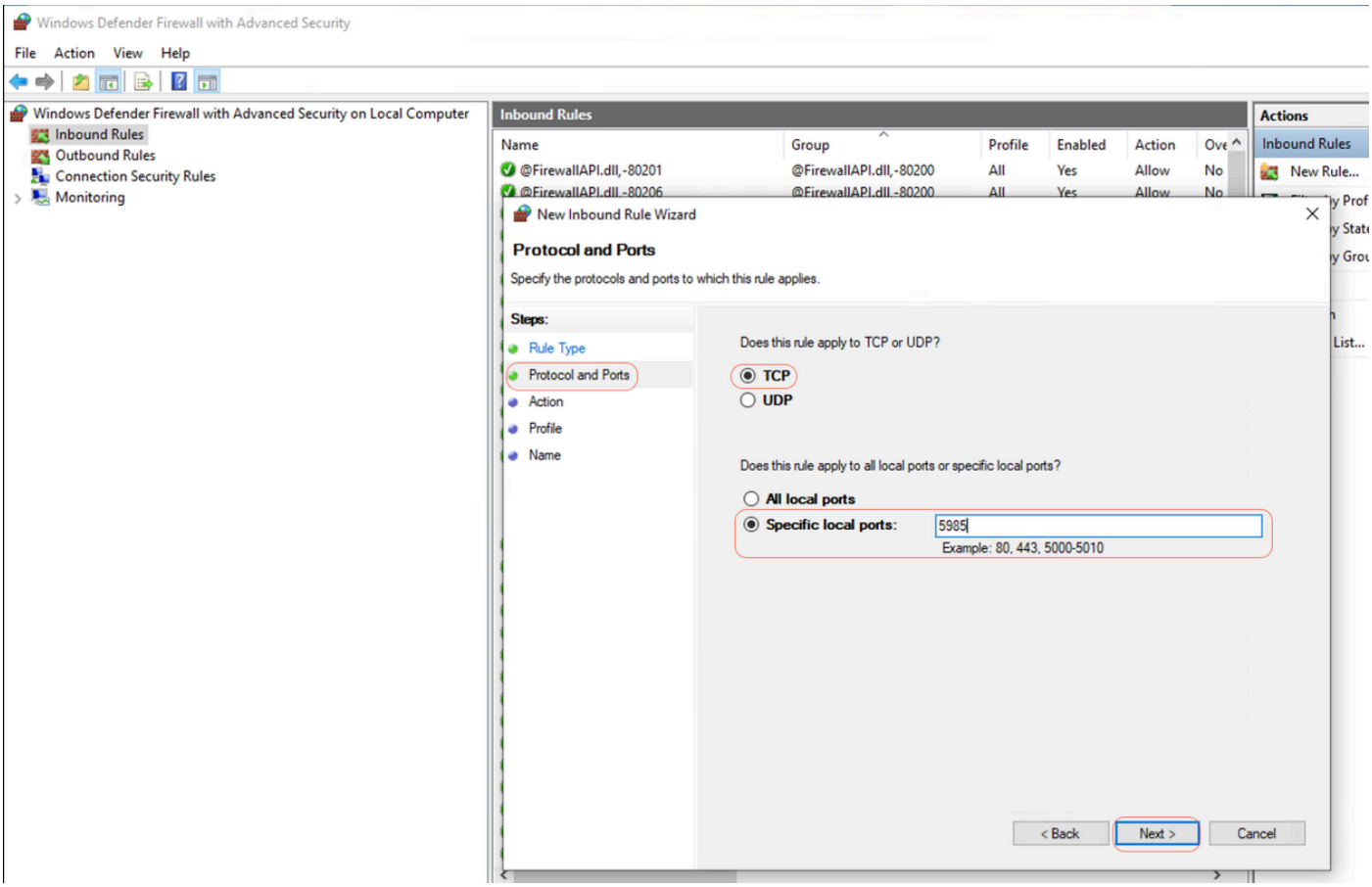
创建入站规则以允许5985端口上的PowerShell

第1步-在 Windows GUI**中，转到搜索栏，键入Windows Firewall with Advanced Security，单击并选择Run as administrator > Inbound Rules > New Rule > Rule Type > Port > Next：**



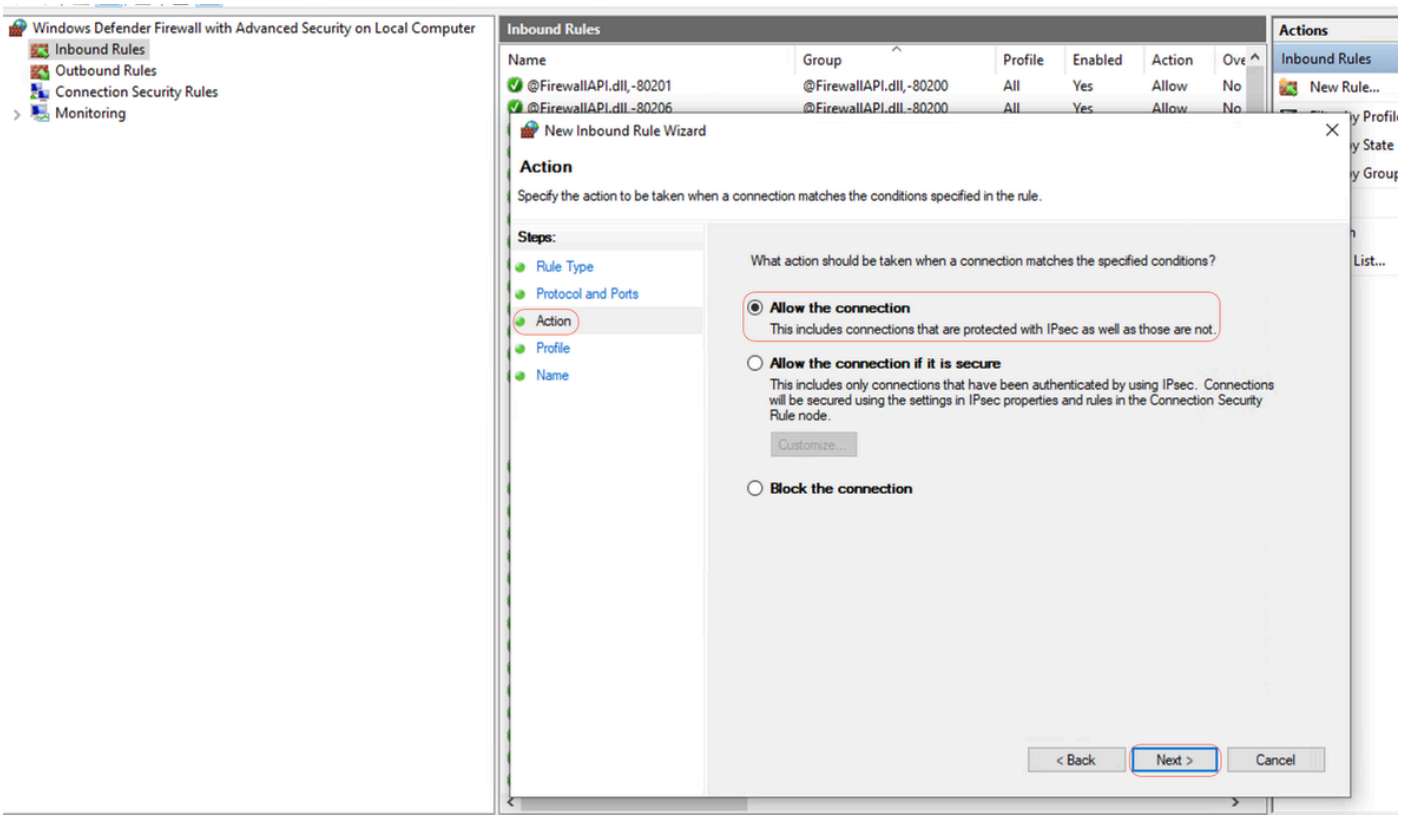
新建入站规则-端口

第2步-在协议和端口下，选择TCP和指定本地端口，键入端口号5985(PowerShell远程处理的默认端口)并点击下一步：



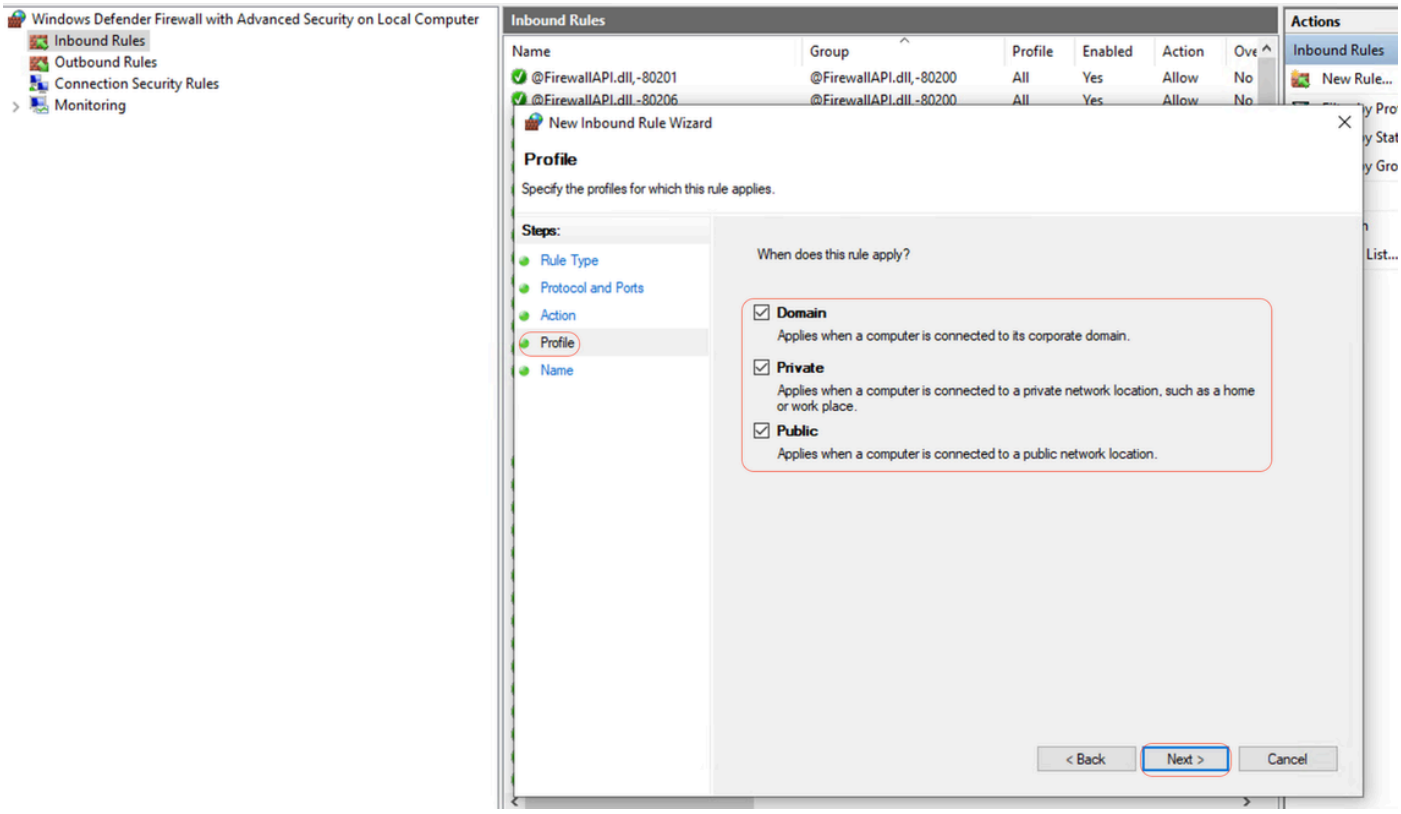
协议和端口

第3步-在操作>选择**允许连接**>**下一步**下：



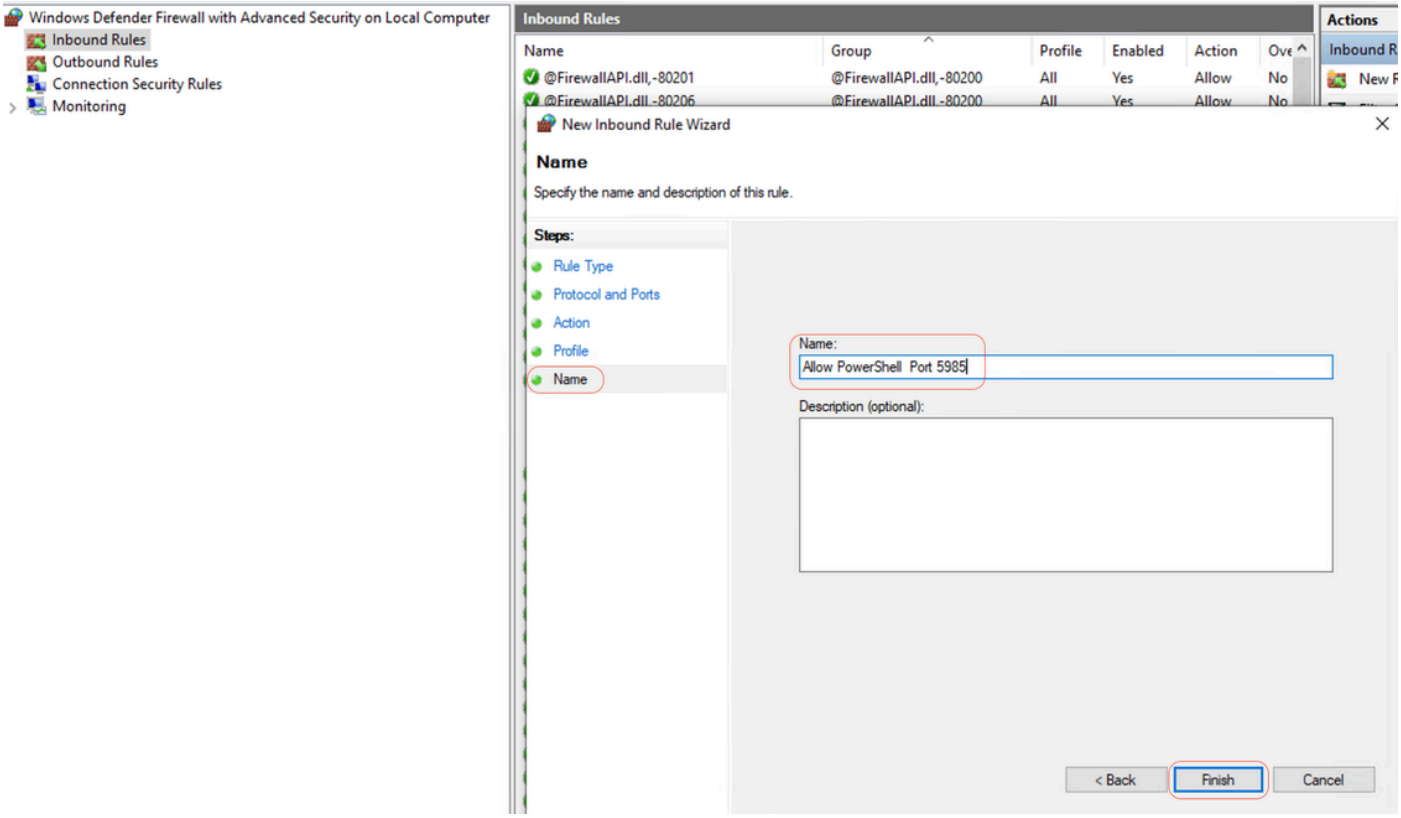
操作

第4步-在配置文件下，选中域、专用和公共复选框，然后单击下一步：



配置文件

第5步-在名称下，输入规则名称，如在端口5985上允许PowerShell，然后单击完成：

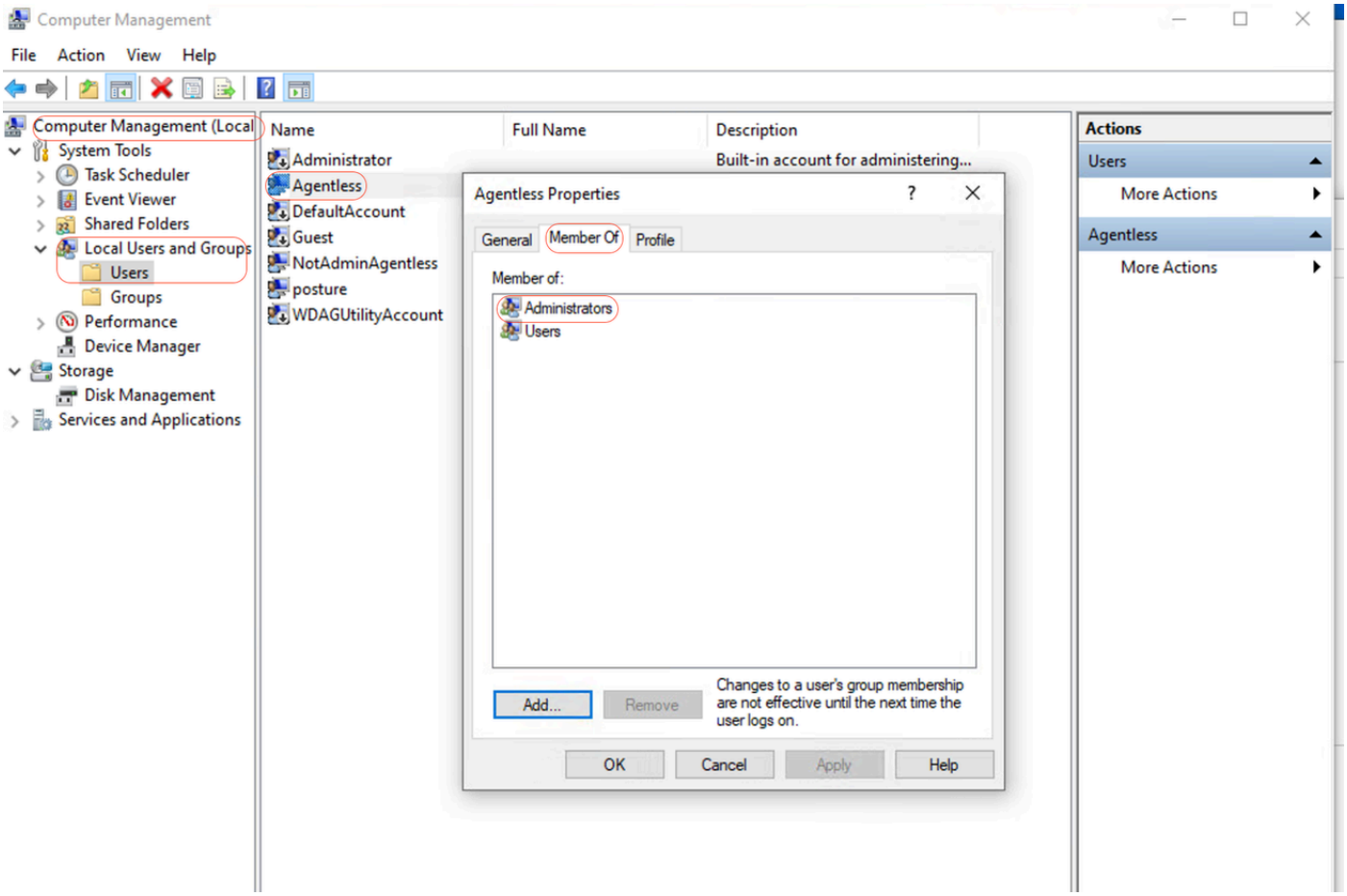


名称

外壳登录的客户端凭证必须具有本地管理员权限

外壳登录的客户端凭证必须具有本地管理员权限。 要确认是否具有管理员权限，请检查以下步骤：

在Windows GUI中，转至Settings > Computer Management > Local Users and Groups > Users > Select the User Account(在本例中，无代理帐户已选中) > **Member of**，帐户必须具有AdministratorsGroup。



本地管理员权限

正在验证WinRM侦听程序

确保在端口**5985**上为**HTTP**配置了WinRM侦听程序：

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

启用PowerShell Remoting WinRM

确保服务正在运行且已配置为自动启动，请执行以下步骤：

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**

预期输出：

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必须是v7.1或更高版本。客户端必须具有cURL v7.34或更高版本：

如何在Windows上检查PowerShell和cURL版本

确保您使用的PowerShell版本正确；cURL对于状态无代理程序至关重要：

检查PowerShell版本

在 Windows 上：

1. **Open PowerShell：**

·按Win + X并选择Windows PowerShell或Windows PowerShell (Admin)。

2. 执行命令：$PSVersionTable.PSVersion

·此命令输出系统上安装的PowerShell的版本详细信息。

检查cURL版本

在 Windows 上：

1. 打开命令提示符：

·按Win + R，键入cmd，然后单击Enter。

2.执行命令： curl --version

·此命令显示系统上安装的cURL版本。

用于检查Windows设备上的PowerShell和cURL版本的输出

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>

其他配置

此命令将计算机配置为信任特定远程主机进行WinRM连接： 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> -

带有-Authentication Negotiate和-Credential参数的test-wsman cmdlet是用于验证远程计算机上WinRM服务的可用性和配置的功能强大的工具： test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

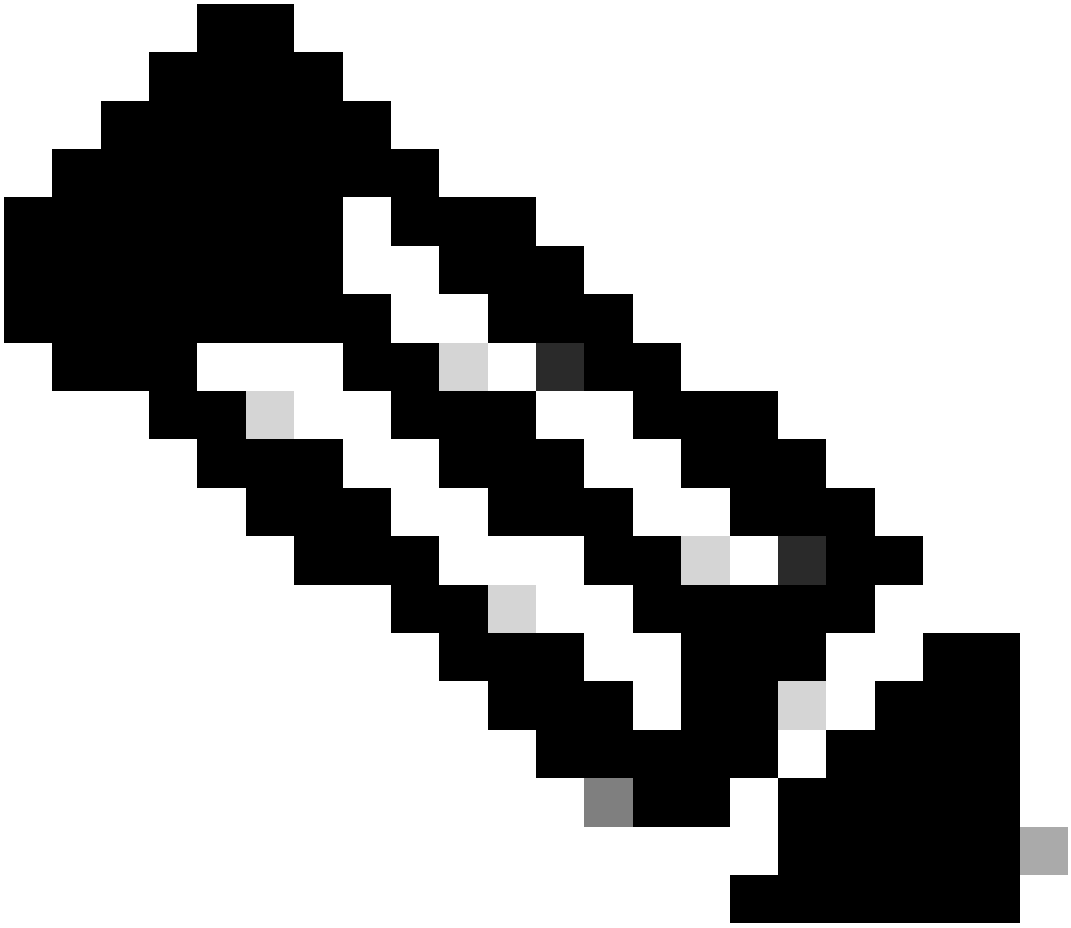
Powershell必须是v7.1或更高版本。客户端必须具有cURL v7.34或更高版本：

在macOS上：

1.开放终端：

·您可以在**Applications > Utilities**中找到终端。

2.执行命令： pwsh -Command '$PSVersionTable.PSVersion'



注：注： ·确保已安装PowerShell核心(pwsh)。如果没有，您可以通过Homebrew安装它（请确保您已安装了Himebrew）： brew install --cask powershell

---

在macOS上：

1.开放终端：

·您可以在**Applications > Utilities**中找到终端。

2.执行命令： curl --version

·此命令必须显示系统上安装的cURL版本。

对于MacOS客户端，访问SSH的端口22必须打开才能访问客户端

分步指南：

1. **打开系统首选项：**

·从Apple菜单导航到**系统首选项**。

2. **启用远程登录：**

·转到**共享**。

· 选中**Remote Login**旁边的框。

·确保**Allow access for**选项已设置为适当的用户或组。选择**All users**允许在Mac上具有有效帐户的任何用户通过SSH登录。

3. **验证防火墙设置：**

·如果启用了防火墙，则需要确保它允许SSH连接。

·转至**System Preferences > Security & Privacy > Firewall**。

·单击**Firewall Options**按钮。

·检查**Remote Login**或**SSH**是否已列出并允许。如果未列出，请点击**添加**按钮(+)进行添加。

4.**通过终端打开端口22（如有必要）：**

·从**Applications > Utilities**打开**Terminal**应用程序。

·使用pfctl命令检查当前防火墙规则并确保端口22处于打开状态：sudo pfctl -sr | grep 22

·如果端口22未打开，您可以手动添加规则以允许SSH：echo “pass in proto tcp from any to any port 22” | sudo pfctl -ef -

5. **测试SSH访问：**

· 从其他设备打开终端或SSH客户端。

·尝试使用其IP地址连接到macOS客户端：ssh username@<macOS-client-IP>

·用正确的用户帐户替换username，用macOS客户端的IP地址替换<macOS-client-IP>。

对于MacOS，请确保在sudoers文件中更新此条目，以避免终端上的证书安装失败：

在管理macOS终端时，确保无需密码提示即可执行特定管理命令至关重要。

先决条件

· macOS计算机上的管理员访问权限。

·基本熟悉终端命令。

更新Sudoers文件的步骤

1.开放终端：

·您可以在**Applications > Utilities**中找到终端。

2. 编辑**Sudoers**文件：

·使用visudo命令安全编辑sudoers文件。这可确保在保存文件之前捕获到任何语法错误。sudo visudo

·系统将提示您输入管理员密码。

3.查找相应部分：

·在Visudo编辑器中，导航到定义用户特定规则的部分。通常，此位置位于文件底部。

4. **添加所需的**条目：

· 添加以下行，向指定用户授予在不使用口令的情况下运行security和osascript命令的权限： <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

·用macOS管理员的实际用户名替换**<macadminusername>**。

5. **保存并退出：**

·如果使用默认编辑器(nano)，请按Ctrl + X退出，然后按Y确认更改，最后按Enter保存文件。

· **如果使用**vi或vim，请按Esc，键入：wq，然后按Enter**保存并退出。**

6.验证更改：

·为确保更改生效，您可以运行需要已更新sudo权限的命令。例如：

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

· 无需提示输入口令即可执行这些命令。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。