配置狀態無代理

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

快速入門

- 必要條件:
- 支援的狀態條件
- 不支援的狀態條件

配置ISE

- 更新狀態摘要
- 狀態無代理配置流程
- 無代理狀態配置
  - 狀態條件
  - 狀況要求
  - 狀態策略
  - 使用者端布建
  - 無代理授權配置檔案
  - 使用補救的替代方案（可選）
  - 補救授權配置檔案（可選）
  - 無代理授權規則
  - 配置終端登入憑據

配置Windows終端並進行故障排除

- 檢驗和故障排除前提條件
  - 測試到埠5985的TCP連線
  - 建立入站規則以允許埠5985上的PowerShell
  - Shell登入的客戶端憑據必須具有本地管理員許可權
  - 正在驗證WinRM偵聽程式
  - EnablePowerShell RemotingWinRM
  - Powershell必須是v7.1或更高版本。客戶端必須具有cURL v7.34或更高版本：
  - 在Windows裝置上檢查PowerShell和cURL版本的輸出
  - 其他組態
  - MacOS
  - Powershell必須是v7.1或更高版本。客戶端必須具有cURL v7.34或更高版本：
  - 對於MacOS客戶端，訪問SSH的埠22必須打開才能訪問客戶端
  - 對於MacOS，請確保在sudoers檔案中更新此條目，以避免終端上的證書安裝失敗：

簡介

本文檔介紹如何在ISE中配置終端安全評估無代理程式以及在終端中運行無代理程式指令碼所需要執行的操作。

必要條件

需求

思科建議您瞭解以下主題：

- 身份服務引擎(ISE)。
- 姿勢。
- PowerShell和SSH
- Windows 10或更高版本。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分辨識服務引擎(ISE) 3.3版。
- 套件CiscoAgentlessWindows 5.1.6.6
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

ISE終端安全評估執行客戶端評估。客戶端從ISE接收終端安全評估要求策略，執行終端安全評估資料收集，將結果與策略進行比較，並將評估結果傳送回ISE。

然後，ISE根據狀態報告確定裝置是否合規。

無代理安全評估是一種從客戶端收集安全評估資訊並在完成時自動刪除自己的安全評估方法，無需終端使用者執行任何操作。無代理狀態使用管理許可權連線到客戶端。

快速入門

必要條件:

- 使用者端必須可透過其IPv4或IPv6位址存取，而且該IP位址必須在RADIUS計量中可用。
- 使用者端必須可透過其IPv4或IPv6位址從思科辨識服務引擎(ISE)連線。此外，此IP地址必須在RADIUS記賬中可用。
- 目前支援Windows和Mac使用者端：
    - 對於Windows客戶端，必須打開埠5985才能訪問客戶端上的powershell。Powershell必須是v7.1或更高版本。客戶端必須具有cURL v7.34或更高版本。
    - 對於MacOS客戶端，訪問SSH的埠22必須打開才能訪問客戶端。客戶端必須具有cURL

v7.34或更高版本。

- Shell登入的客戶端憑據必須具有本地管理員許可權。
- 按照配置步驟中的說明，運行狀態饋送更新以獲取最新的客戶端。請檢查：
- 對於MacOS，請確保在sudoers檔案中更新此條目，以避免終端上的證書安裝失敗：請檢查：

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

- 對於MacOS，配置的使用者帳戶必須是管理員帳戶。MacOS的無代理狀態不適用於任何其他帳戶型別，即使您授予了更多許可權。要檢視此窗口，請按一下Menuicon ()並**選擇Administration > System > Settings > Endpoint Scripts** > Login **Configuration > MAC Local User**。
- 如果Microsoft的更新導致Windows客戶端中的埠相關活動發生變化，您必須重新配置Windows客戶端的無代理狀態配置工作流。

支援的狀態條件

- 檔案條件，使用USER_DESKTOP和USER_PROFILE檔案路徑的條件除外
- 服務條件，但macOS上的系統守護程式和守護程式或使用者代理檢查除外

- 申請條件
- 外部資料來源條件
- 複合條件
- 防惡意軟體情況
- 修補程式管理條件，但EnabledandUp到日期條件檢查除外
- 防火牆狀況
- 磁碟加密條件，基於加密位置的條件檢查除外
- 登錄檔條件，使用HCSK作為根鍵的條件除外

不支援的狀態條件

- 修正
-

寬限期

- 定期重新評估

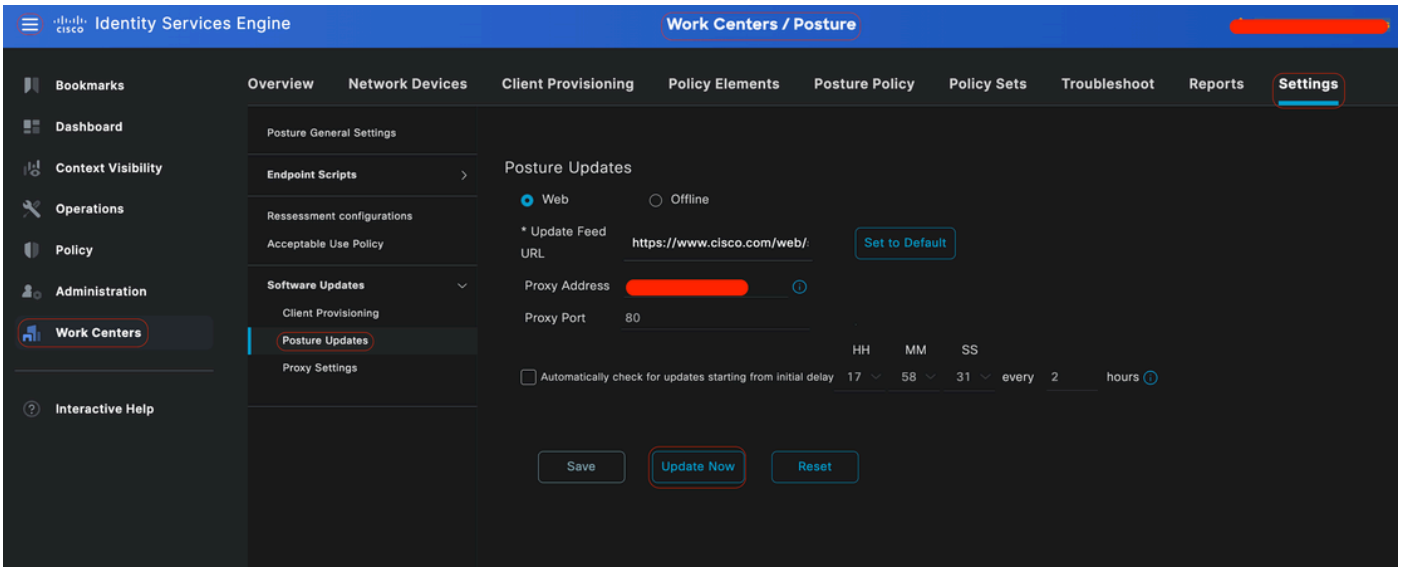
- 可接受的使用策略

配置ISE

更新狀態摘要

建議在開始配置狀態之前更新狀態源。

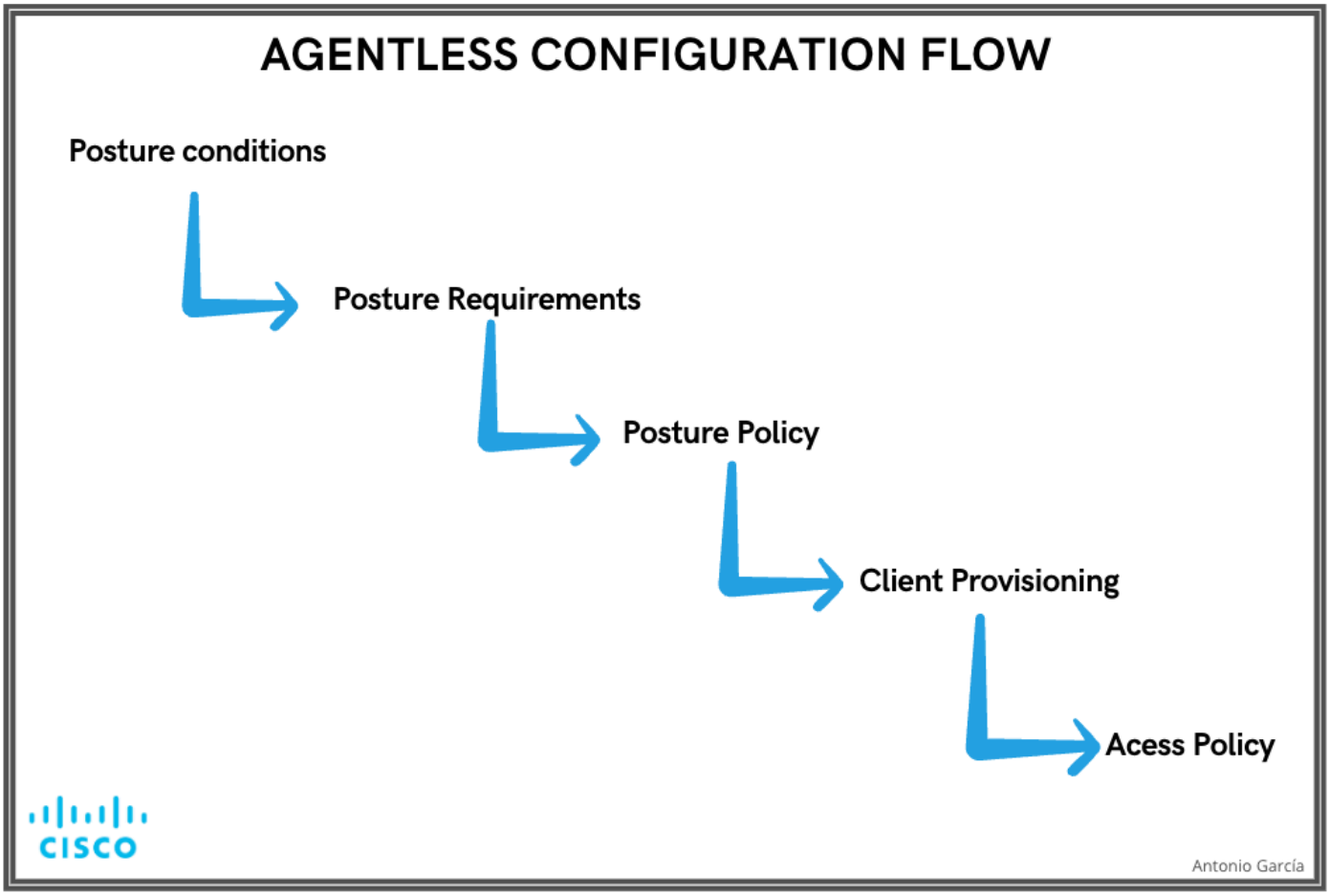
在思科ISE GUI中，點選選單圖示(
)，然後選擇**工作中心(Work Centers) >狀態(Posture) >設定(Settings)** >軟體更新(**Software Updates**) >立即更新(**Update Now**)。



更新狀態饋送

狀態無代理配置流程

必須配置無狀態代理，因為下一個配置需要第一個配置，依此類推。請注意，Remediation不在流程中；但是，本文檔稍後將介紹配置Remediation的替代方法。



無代理配置流

無代理狀態配置

狀態條件

狀態條件是我們安全策略中定義合規端點的規則集。其中一些專案包括安裝防火牆、防病毒軟體、防惡意軟體、修補程式、磁碟加密等。

在Cisco ISE GUI中，點選Menuicon ()，選擇**Work Centers** > **Posture** > **Policy Elements** > **Conditions**，點選Add，建立一個或多個使用Agentless posture的Posture **Conditions以辨識需求**。建立**條件**後，按一下**儲存**。

在此場景中，名為「**Agentless_Condition_Application**」的應用條件使用以下引數配置：

·**作業系統**：Windows All

此條件適用於任何版本的Windows作業系統，確保不同Windows環境的廣泛相容性。

·**檢查依據**：程式

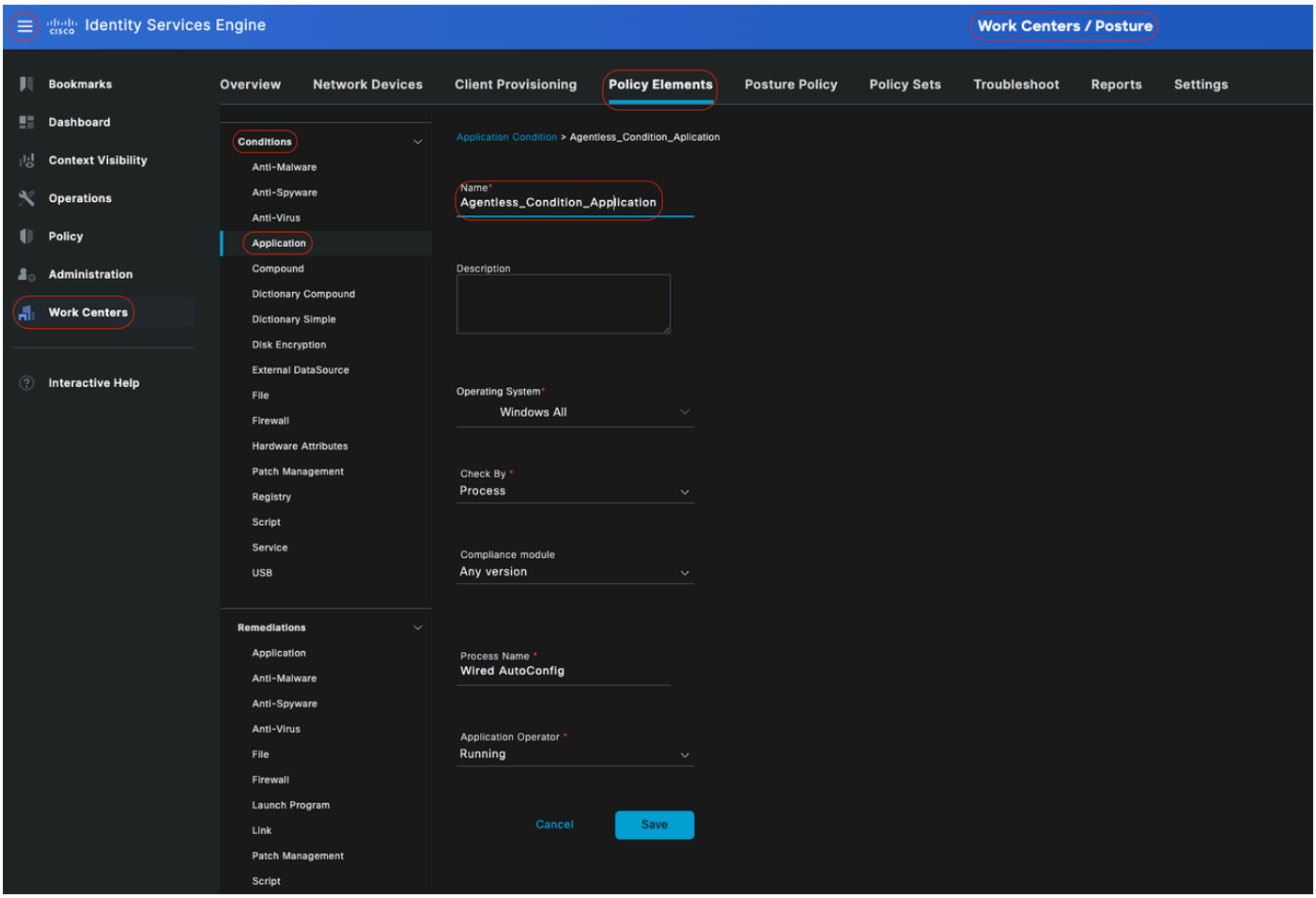
系統監控裝置內的進程。您可以選擇選擇**Process**或**Application**；在這種情況下，選擇**Process**。

·**進程名稱**：有線自動配置

有線自動配置進程是進程相容模組即將簽入裝置。此過程負責配置和管理有線網路連線，包括IEEE 802.1X身份驗證。

·**應用程式操作員**：執行

合規性模組驗證裝置上當前是否正在運行**有線AutoConfig**進程。您可以選擇**Running**或**Not Running**。在本例中，選擇**Running**以確保進程處於活動狀態。



無代理程式條件

狀態要求

姿勢要求是一組複合條件，或僅一個可與角色和作業系統連結的條件。連線到網路的所有客戶端必須在狀態評估期間滿足強制性要求，才能在網路上實現合規性。

在思科ISE GUI中，點選選單圖示( )，然後選擇**工作中心(Work Centers) >狀態(Posture)> 策略元素(Policy Elements) > 要求(Requirement)。** 點選下箭頭並選擇**Insert**

new Requirement，然後建立一個或多個使用無代理狀態的**PostureRequirement**。建立**要求**後，點選**完成**，然後點選**儲存**。

在這種情況下，名為「**Agentless_Requirement_Application**」的應用要求配置了以下條件：

·**作業系統**：Windows All

此要求適用於任何版本的Windows作業系統，確保它適用於所有Windows環境。

·**狀態型別**：無代理

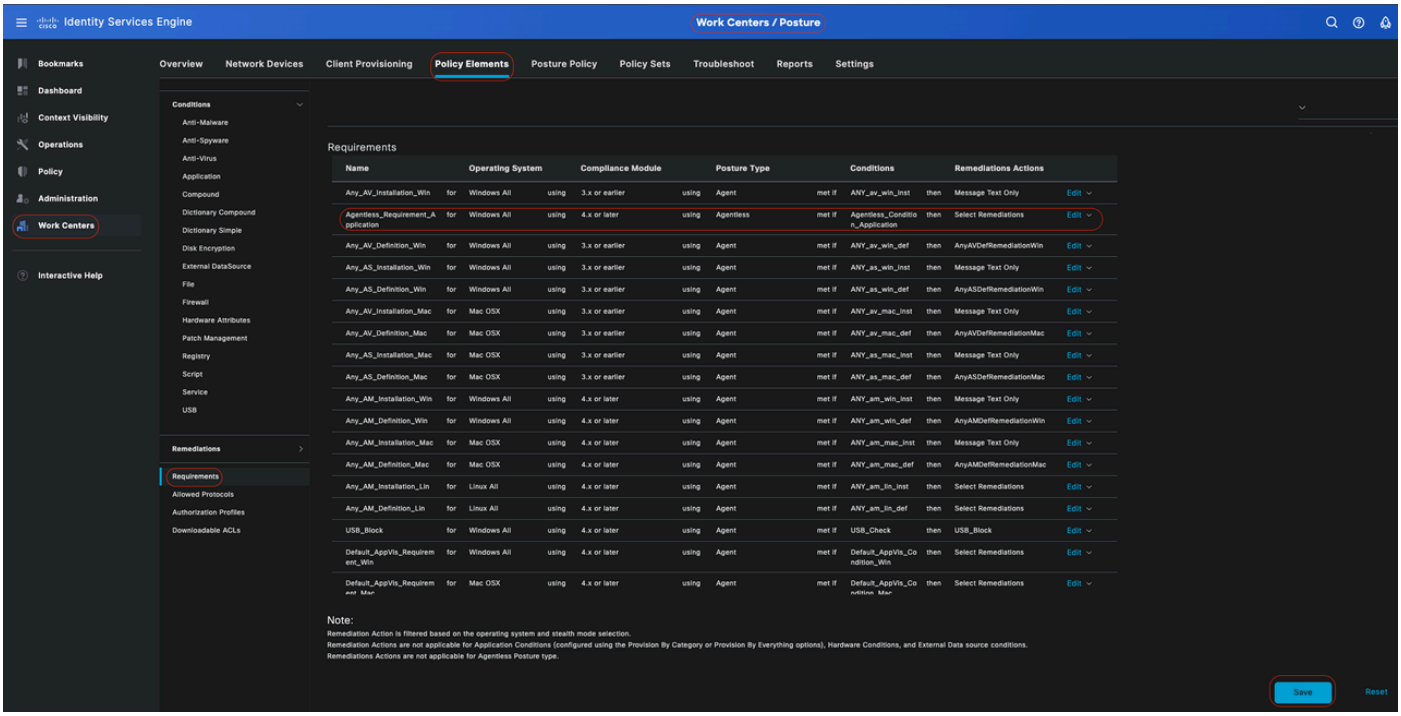
此配置是為無代理環境設定的。可用選項包括**Agent**、**Agent Stealth**、**Temporal Agent**和**Agentless**。在此場景中，選擇了**Agentless**。

·**條件**：**Agentless_Condition_Application**

這指定ISE終端安全評估模組和合規性模組將在裝置進程內檢查的條件。所選條件為**Agentless_Condition_Application**。

·**補救行動**：

由於此配置用於無代理環境，因此不支援補救操作，並且此欄位呈灰色顯示。



無代理程式需求

狀態策略

在思科ISE GUI中，點選選單圖示(

)並**選擇工作中心**>狀態>狀態**策略**。 點選**向下箭頭**並選擇**Insert new Requirement**，然後建立針對該狀況要求使用無代理狀況的一個或多個受支援的**狀況策略**規則。 **終端安全評估策略**建立後，點選**完成**，然後點選**儲存**。

在本場景中，名為「**Agentless_Policy_Application**」的狀態策略已使用以下引數配置：

·**規則名稱：**Agentless_Policy_Application

這是此配置示例中安全評估策略的指定名稱。

·**作業系統：**Windows All

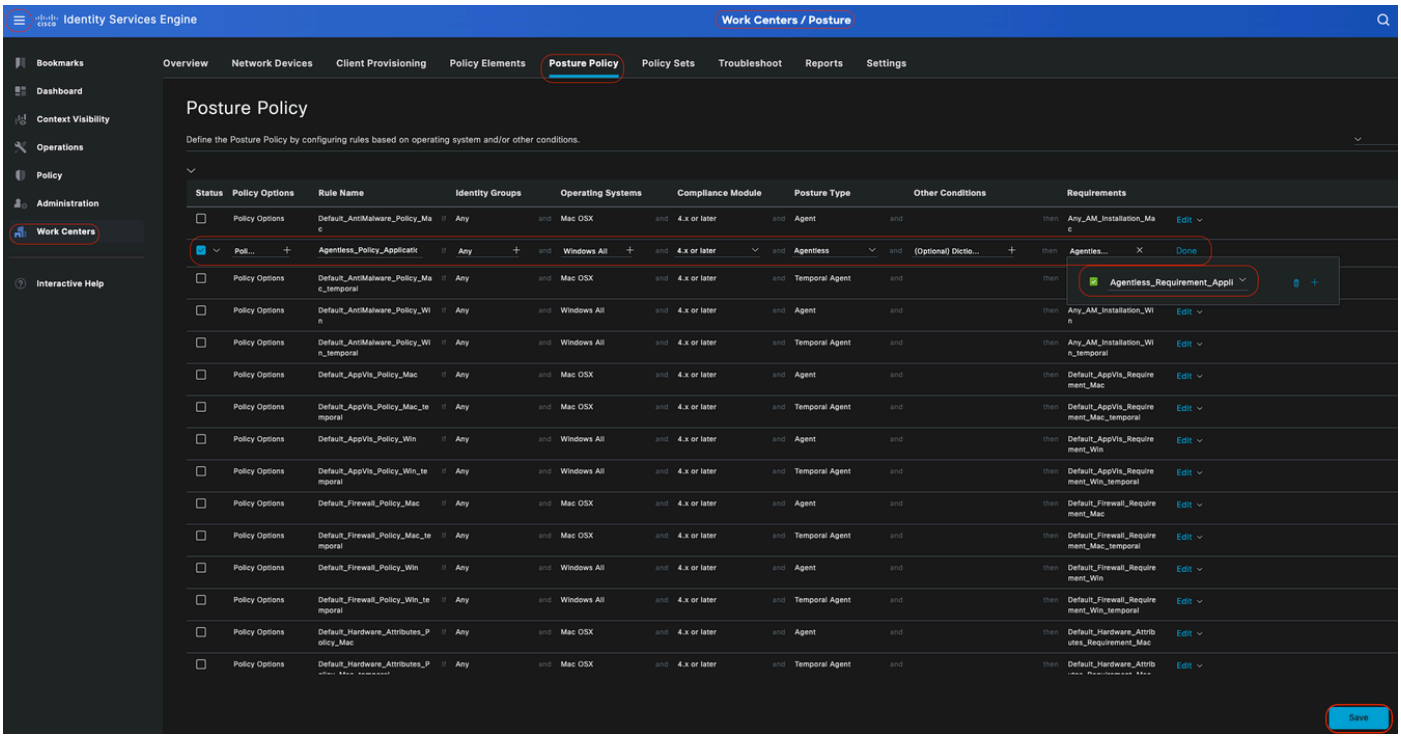
此策略設定為應用於所有Windows作業系統版本，確保不同Windows環境的廣泛相容性。

·**狀態型別：**無代理

此配置是為無代理環境設定的。可用選項包括**Agent**、**Agent Stealth**、**Temporal Agent**和**Agentless**。在本場景中，已選擇**Agentless**。

·**其他條件：**

在此組態範例中，尚未建立任何其他條件。但是，您可以選擇配置特定條件，以確保僅目標裝置受此安全評估策略約束，而不是受網路上所有Windows裝置的約束。這對於網路分段特別有用。



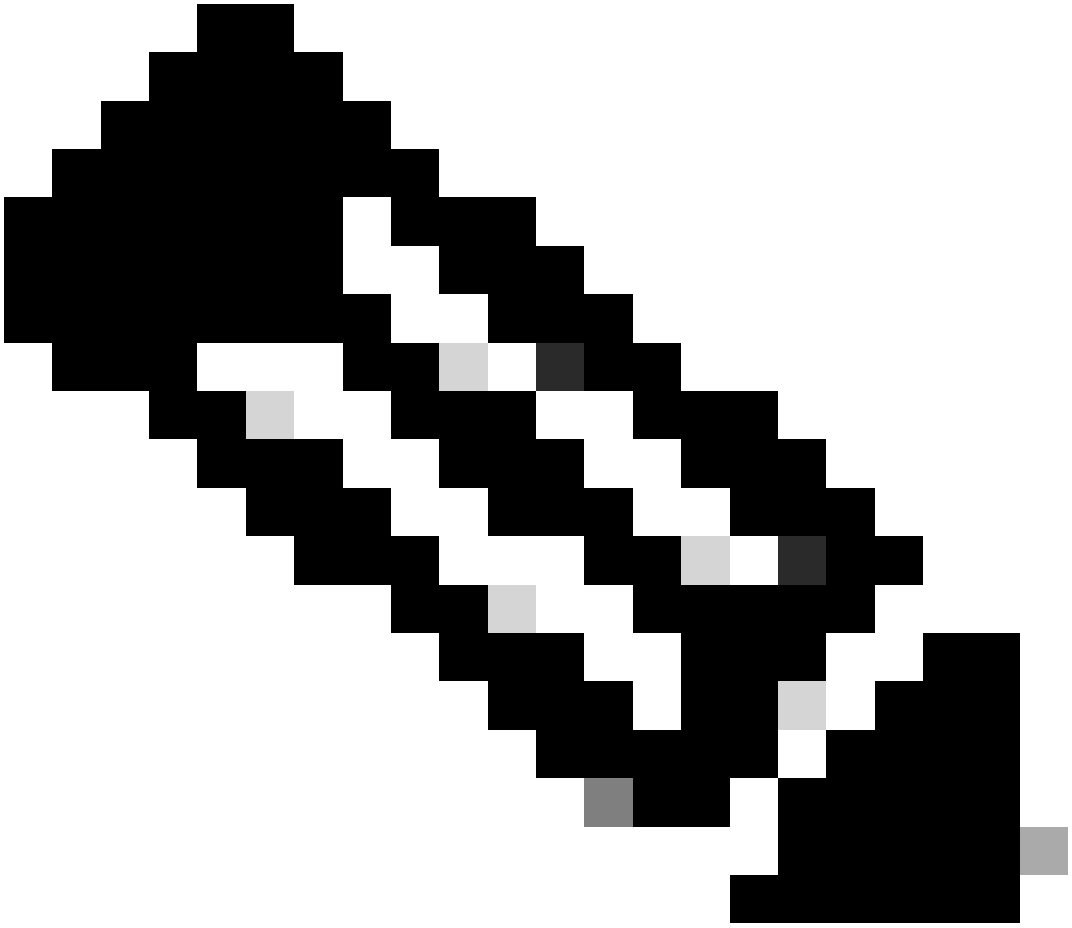
狀態無代理策略

使用者端布建

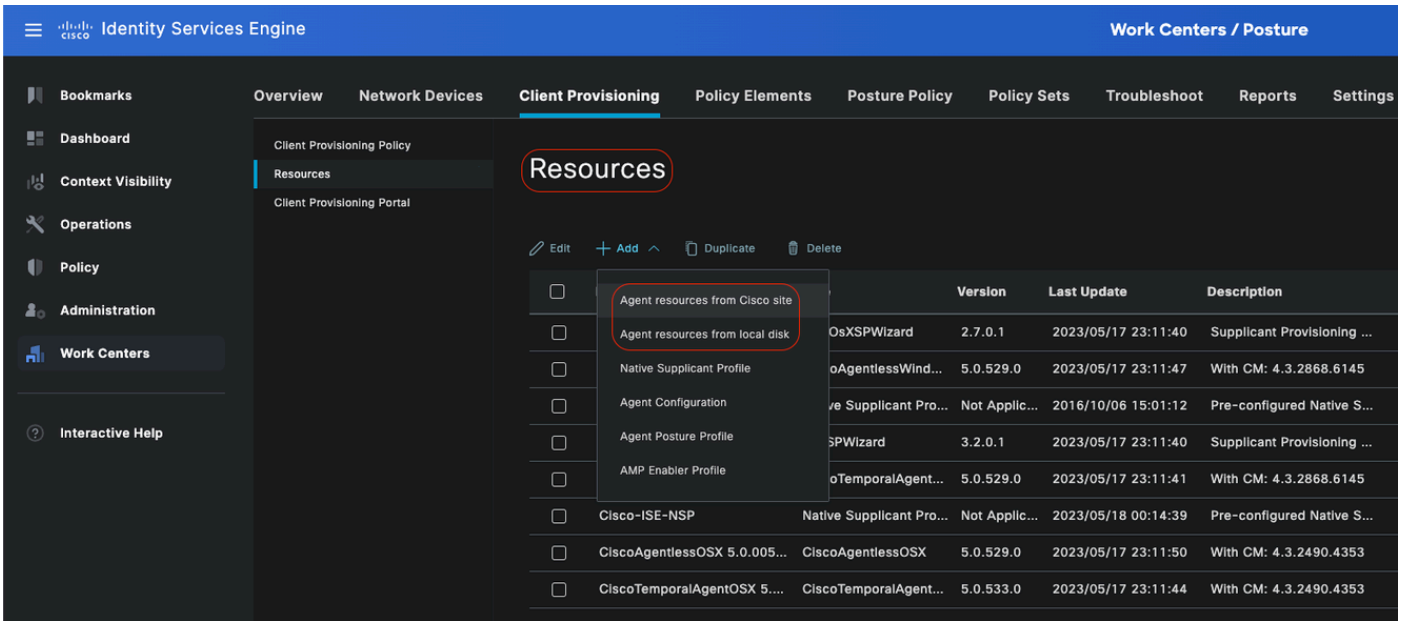
步驟1 -下載資源

要開始配置客戶端調配，您必須先下載所需的資源並在ISE中提供，以便您以後可以在客戶端調配策略中使用這些資源。

向ISE增加資源有兩種方法，**Agent Resources from Cisco site**和**Agent Resources from Local disk**。由於您正在配置無代理，因此您需要透過**Cisco站點上的代理資源**進行下載。



注意：要使用**思科站點的此代理資源**，ISE PAN需要網際網路接入。



資源

來自思科站點的代理資源

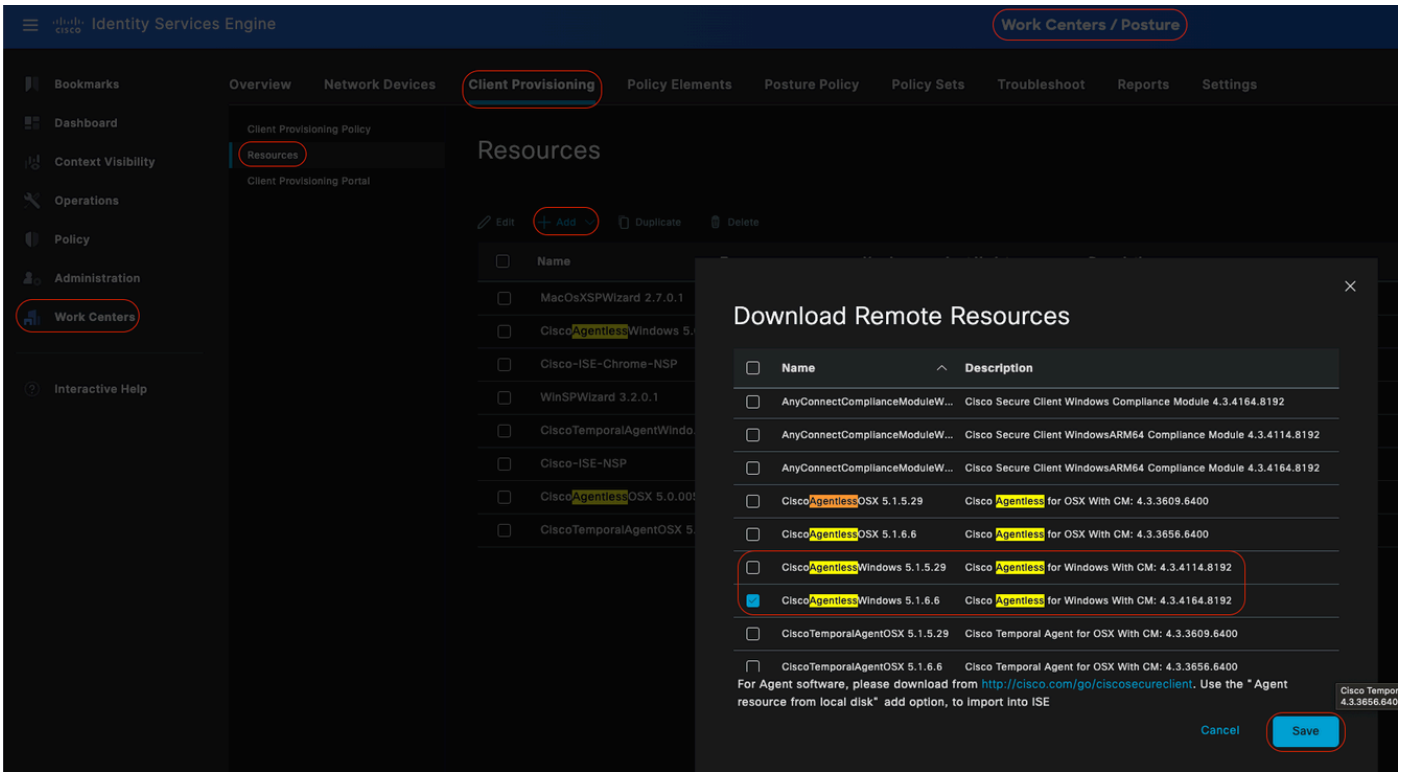
在思科ISE GUI中，點選選單圖示(

)並選擇**工作中心**>**狀態**>**客戶端調配**> **資源**。 按一下**Add**，選擇**Agent Resources from Cisco site**，然後按一下**Save**。

您只能從思科站點下載合規性模組。系統顯示要下載的兩個最新合規性模組。資源包**CiscoAgentlessWindows 5.1.6.6**已針對此配置示例進行選擇，這意味著僅適用於Windows裝置。

.

思科站點的



座席資源

第2步-配置客戶端調配策略

配置終端安全評估代理時，您需要兩個不同的資源(**AnyConnect**或**安全客戶端**和**合規性模組**)，

對映**Agent Configuration**下的兩個資源以及**Agent Posture Profile**，以便您可以在**Client Provisioning Policy**中使用此**Agent Configuration**。

但是，配置狀態無代理時，不需要配置**代理配置**或**代理狀態配置檔案**，只需從**思科站點的代理資源**下載無代理軟體套件。

在思科ISE GUI中，點選選單圖示(
)並選擇**Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Policy**。 點選下**箭頭**，然後選擇**Insert new policy above**或**Insert new policy below**、**Duplicate above**或**Duplicate below**：

- **規則名稱：Agentless_Client_Provisioning_Policy**

這會指定使用者端布建原則的名稱。

- **作業系統：**Windows All

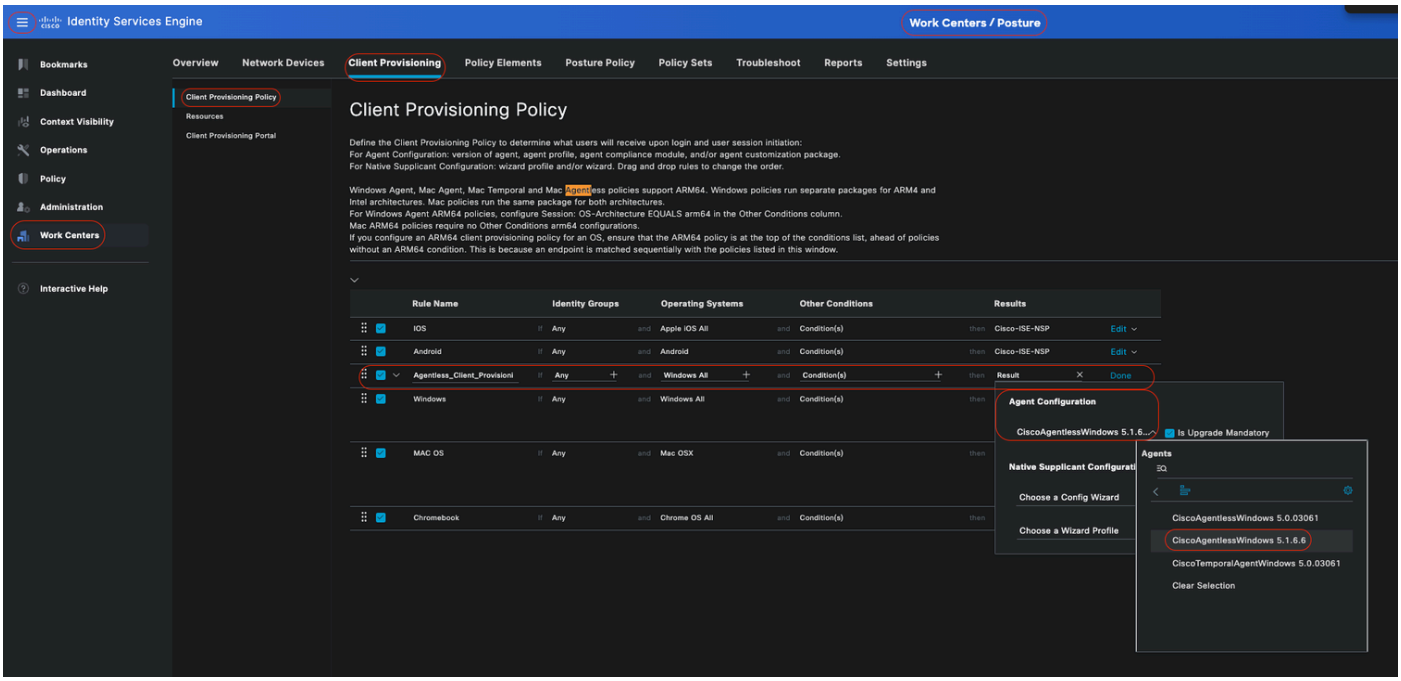
這可確保該策略適用於所有Windows作業系統版本。

- **其他條件：**此示例中未配置任何特定條件。但是，您可以配置條件，確保只有所需裝置與此客戶端調配策略匹配，而不是網路中所有的Windows裝置。這對於網路分段特別有用。

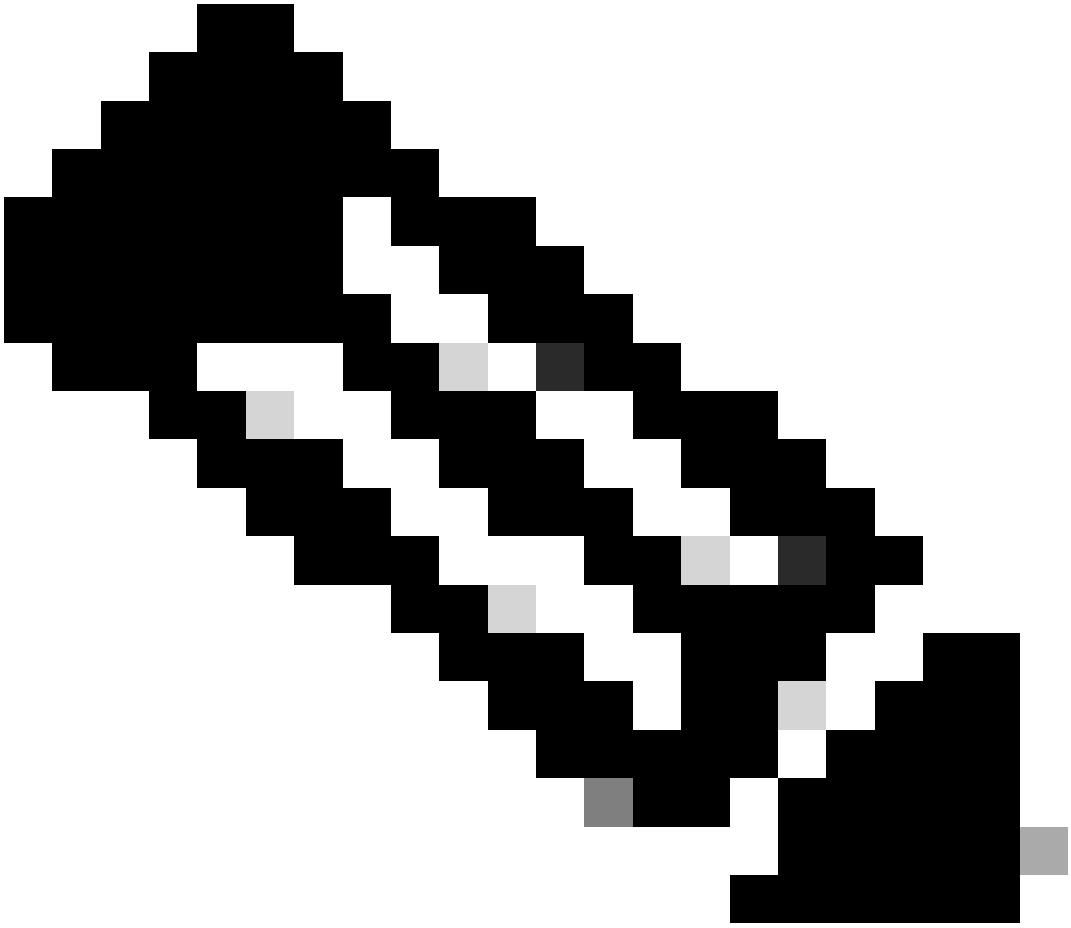
示例：，如果您正在使用Active Directory，可以將Active Directory組併入策略中以細化受影響的裝置。

- **結果：**選取適當的套裝程式或組態代理程式。由於您是為無代理環境進行配置，因此請選擇軟體套件**CiscoAgentlessWindows 5.1.6.6**，您之前已經從**Cisco站點的代理資源**下載了該軟體套件。此無代理軟體套件包含運行狀態無代理所需的所有必要資源(**無代理軟體**和**合規性模組**)。

·按一下**儲存**



無代理客戶端調配策略



注意：請確保只有一個客戶端調配策略滿足任何給定身份驗證嘗試的條件。如果同時評估多個策略，則可能會導致意外行為和潛在衝突。

無代理**授權配置檔案**

在思科ISE GUI中，點選選單圖示(

)並選擇Policy > Policy **Elements > Results > Authorization > Authorization Profiles並建立評估無代理安全評估結果的Authorization Profile**。

- 在此配置示例中，將授權配置檔案命名為**Agentless_Authorization_Profile**。

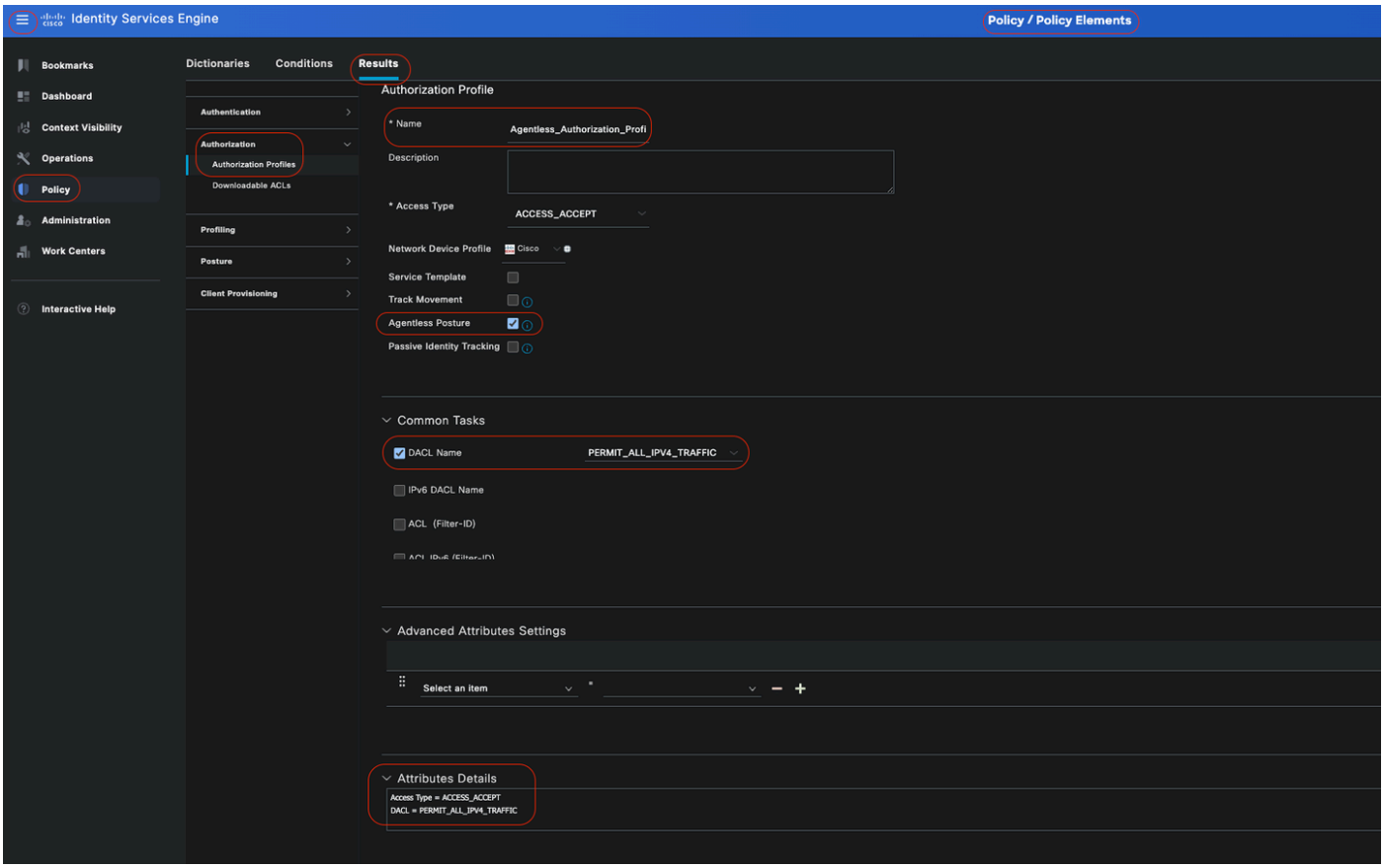
- 在授權配置檔案中啟用無代理狀態。

- 此配置檔案僅用於**Agentless Posture**。請勿將其用於其他姿勢型別。

- 無代理狀態不需要CWA和重定向ACL。您可以使用VLAN、DACL或ACL作為分段規則的一部分。 為簡單起見，除了本配置示例中的無代理狀態檢查外，僅配置了一個dACL（允許所有ipv4流量）。

-

按一下**Save**。



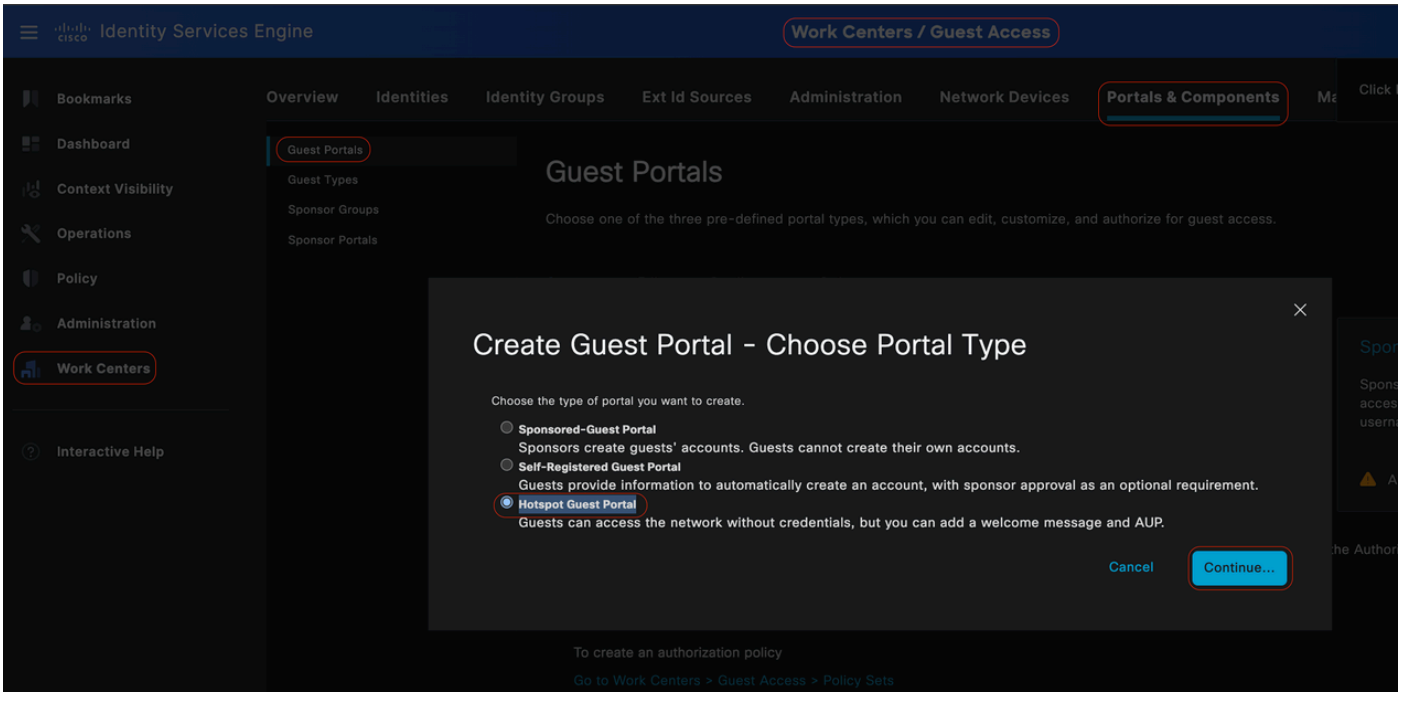
無代理授權配置檔案

使用補救的替代方案（可選）

無代理程式流中不支援補救。要解決此問題，您可以實施自定義熱點門戶，以增強使用者關於終端合規性的感知。當終端被辨識為不合規時，使用者可以重定向到此門戶。此方法可確保使用者瞭解其終端的合規性狀態，並可採取適當措施糾正任何問題。

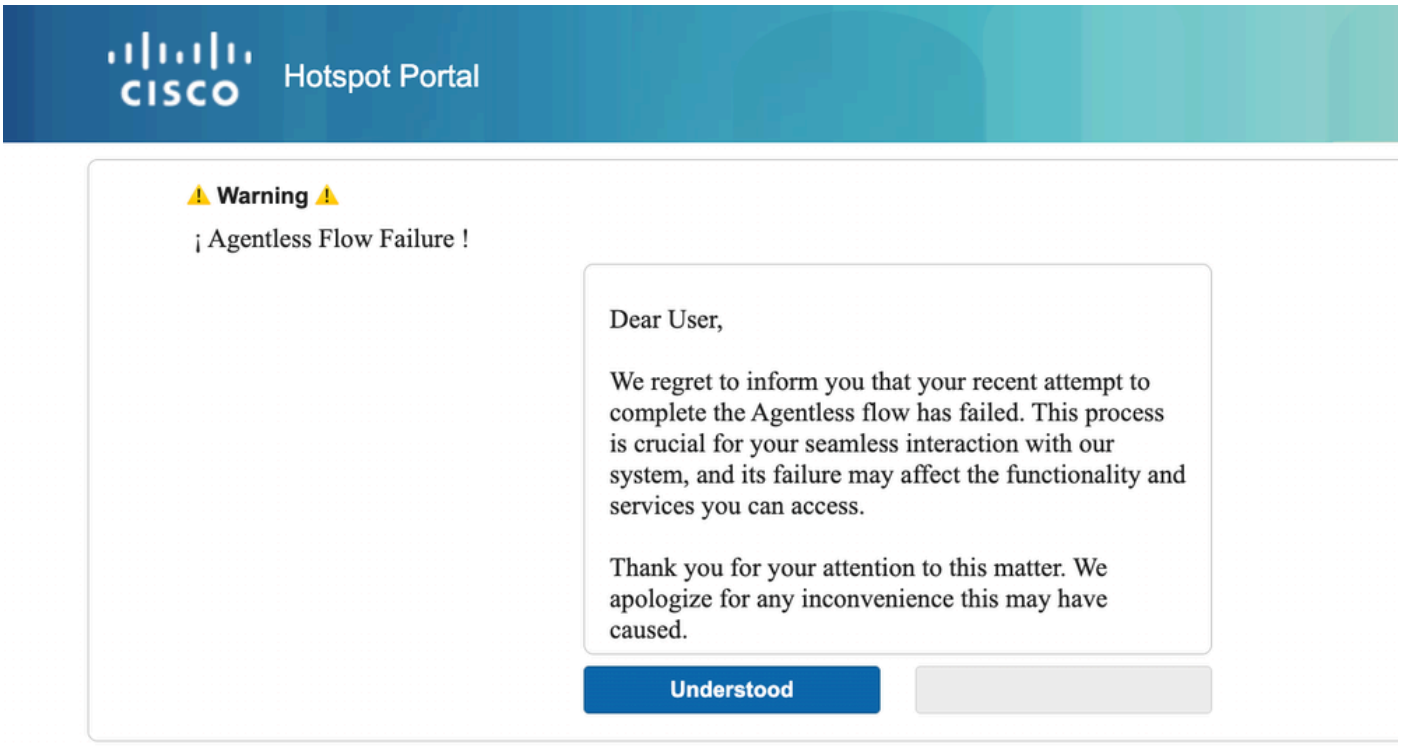
在Cisco ISE GUI中，點選Menuicon (

)，然後選擇**Work Centers** > **Guest Access** > **Portals & Components** >**Guest Portals**。 點選**建立**>選擇**熱點訪客門戶**> **繼續：**。在此配置示例中，熱點門戶被命名為**Agentless_Warning**。



熱點訪客門戶

在門戶設定中，您可以自定義向終端使用者顯示的消息以符合您的特定要求，這只是自定義門戶檢視的一個示例：



故障狀態無代理

補救授權配置檔案（可選）

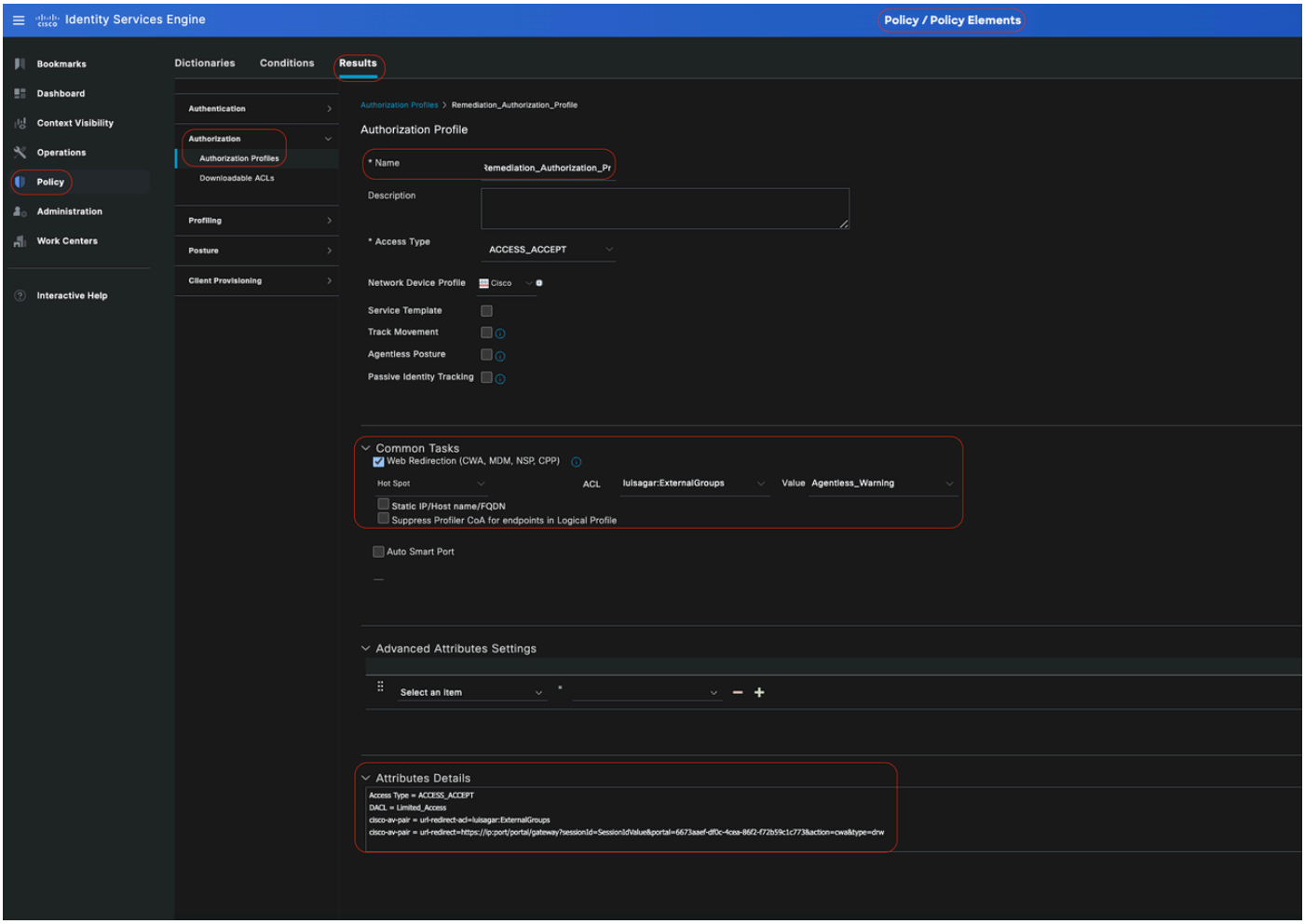
在思科ISE GUI中，點選選單圖示( )，然後選擇策略>策略**元素>結果>授權>授權配置檔案，並為您的補救建立授權配置檔案。**

- 在此配置示例中，將授權配置檔案命名為**Remediation_Authorization_Profile**。

- 為簡單起見，本配置示例僅包括名為**Limited_Access**的可下載訪問控制清單(dACL)，該清單允許根據您組織的特定需求而定製的有限訪問。

- 已配置**Web重定向**功能，包括外部組和熱點，增強使用者關於端點合規性的意識。

- 按一下**Save**。

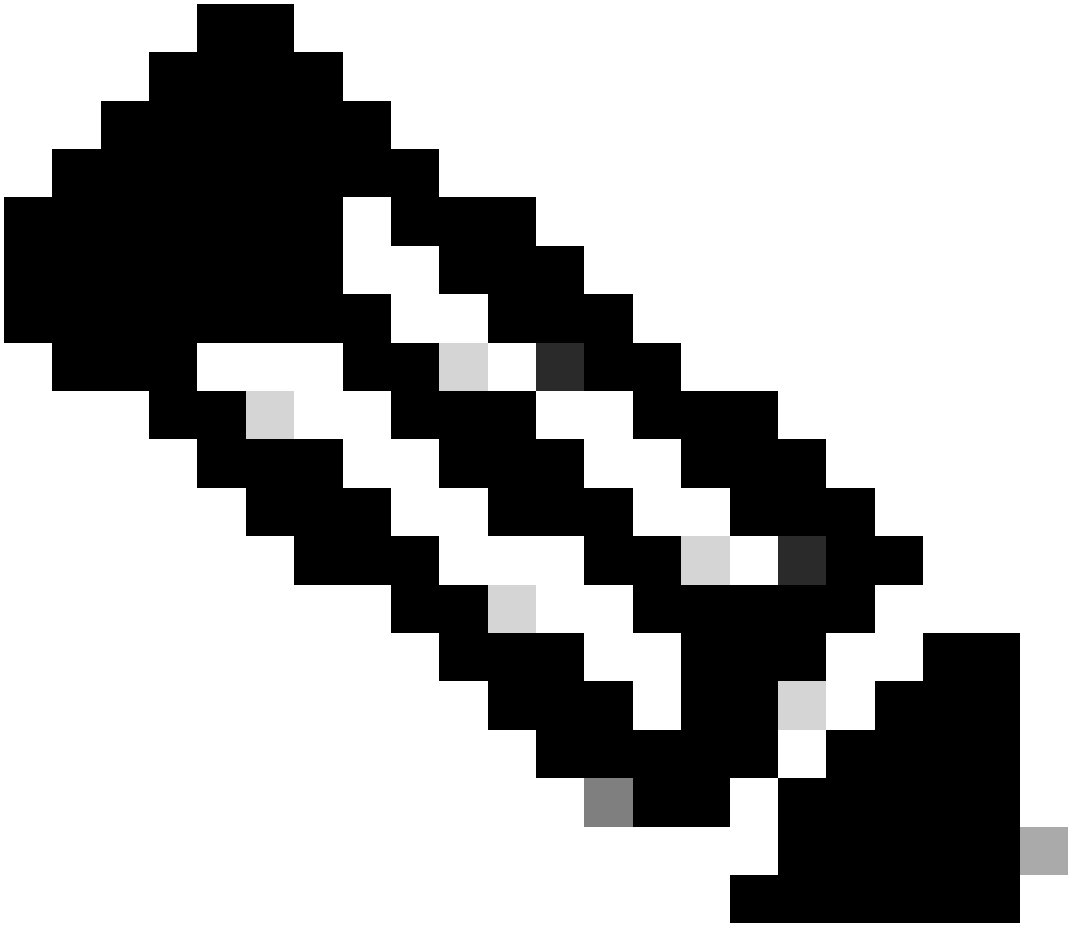


修正授權規則

無代理授權規則

在思科ISE GUI中，點選Menuicon (

)，然後選擇Policy > Policy Set並展開Authorization Policy。啟用和配置以下三個授權策略：



注意：必須按指定配置這些授權規則，以確保狀態流正常運行。

Unknown_Compliance_Redirect：

•狀況:

配置Network_Access_Authentication_Passed和**Compliance_Unknown_Devices**，並將結果設定為**Agentless Posture**。此情況會觸發無代理流量。

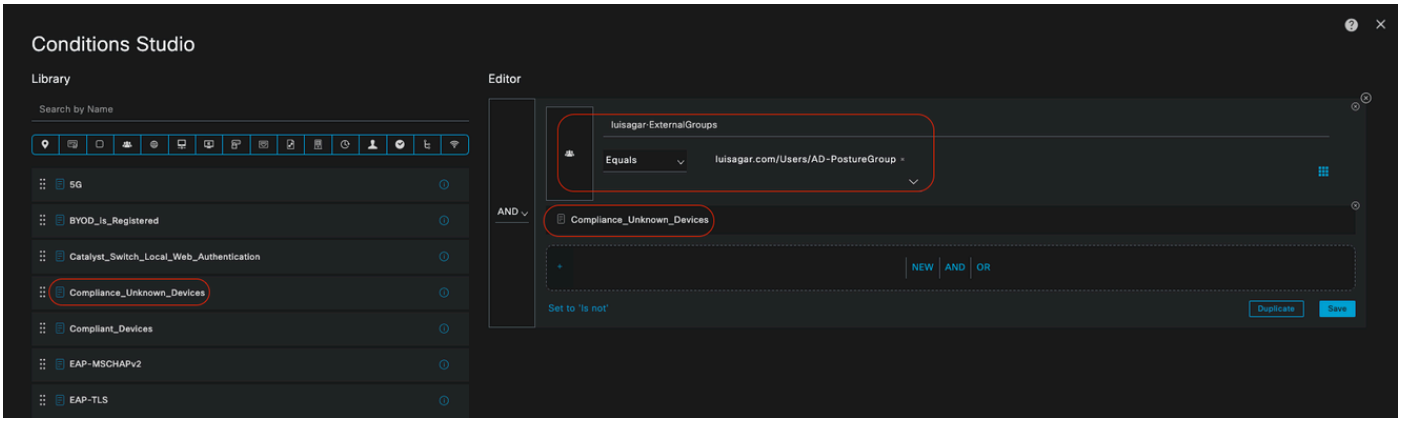
·示例條件：

配置Active Directory (AD)組條件以分段流量。

Compliance_Unknown_Devices條件必須配置為初始狀態未知。

· 授權配置檔案：

將**Agentless_Authorization_Profile** 分配到此授權規則，以確保裝置透過無代理狀態流。 此條件包含無代理程式流，因此符合此配置檔案的裝置可以啟動無代理程式流。



未知的授權規則

NonCompliant_Devices_Redirect：

· 條件：配置Network_Access_Authentication_Passed和Non_Compliant_Devices，結果集為DenyAccess。或者，您可以使用補救選項，如本示例所示。

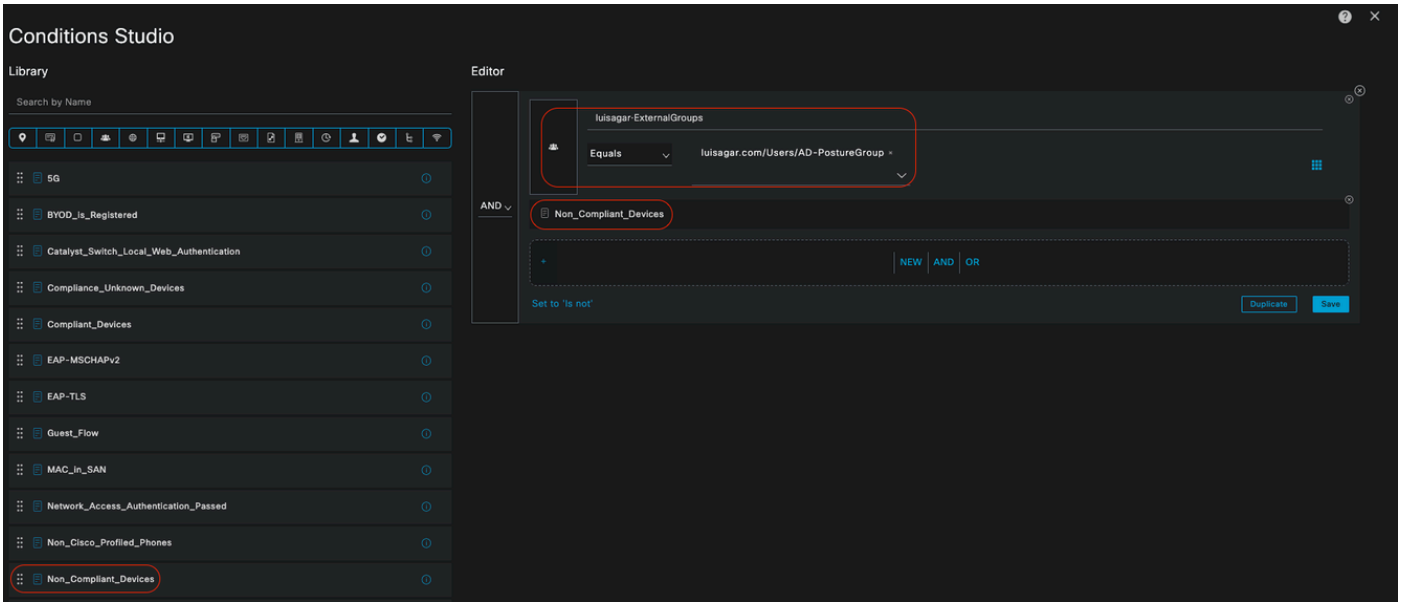
· 示例條件：

配置AD組條件以分段流量。

當終端安全評估狀態不相容時，必須配置**Compliance_Unknown_Devices**條件以分配有限的資源。

· 授權配置檔案：

將**Remediation_Authorization_Profile** 分配到此授權規則，以透過**熱點門戶**通知不相容裝置其當前狀態，或進行**拒絕**訪問。



不符合的授權規則

Compliant_Devices_Access：

•狀況:

使用結果集**PermitAccess**配置Network_Access_Authentication_Passed和**Compliant_Devices**。

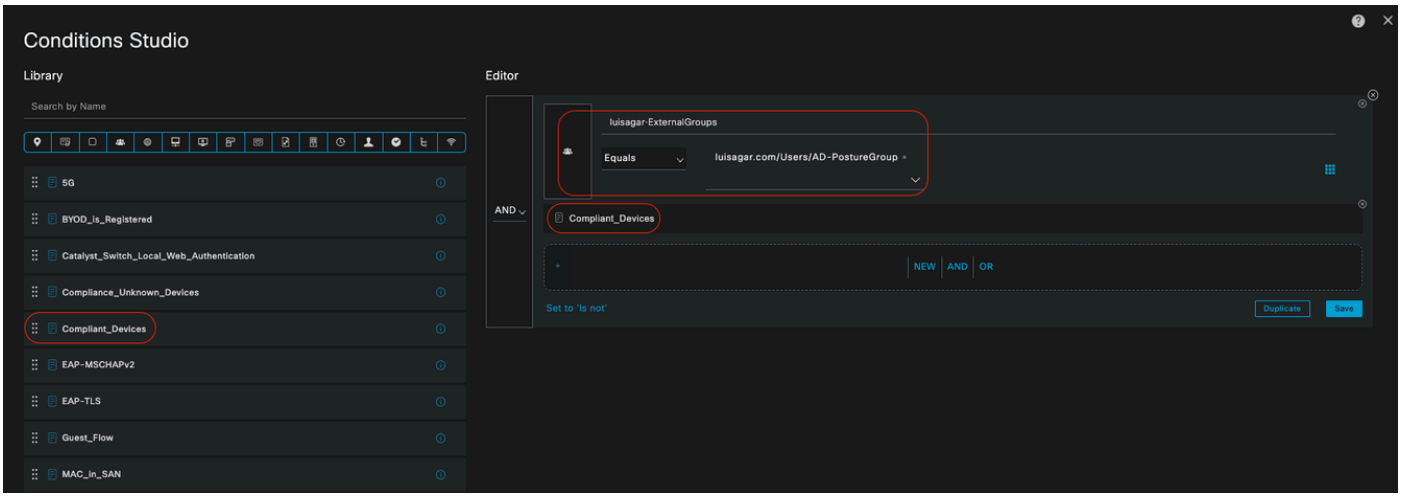
· 示例條件：

配置AD組條件以分段流量。

必須配置**Compliance_Unknown_Devices**條件才能向相容裝置授予適當的訪問許可權。

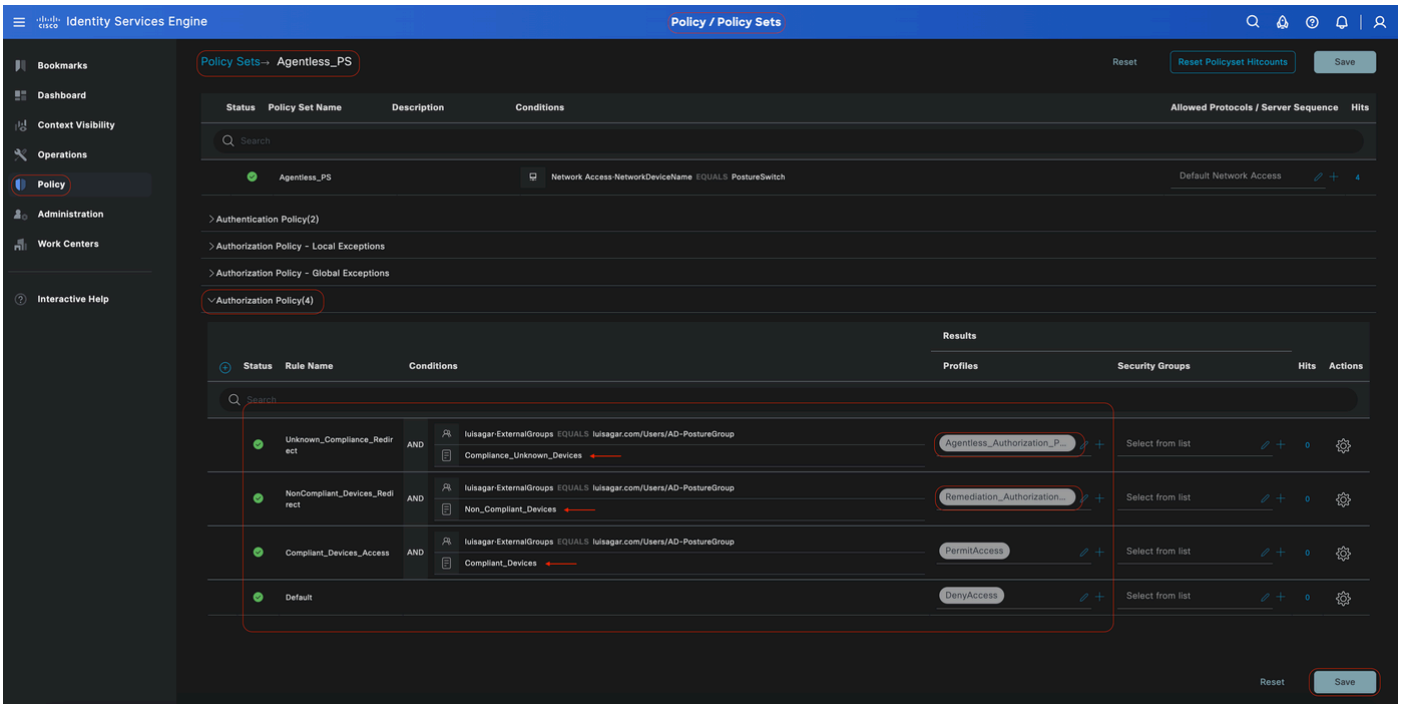
· 授權配置檔案：

向此授權規則分配**PermitAccess**，以確保合規裝置具有訪問許可權。您可以自訂此設定檔以滿足貴組織的需求。



相容授權規則

所有授權規則



授權規則

配置終端登入憑據

在思科ISE GUI中，點選選單圖示( )並**選擇Administration** > **Settings** > **Endpoint Scripts** > **Login Configuration**，然後配置客戶端憑證以登入客戶端。

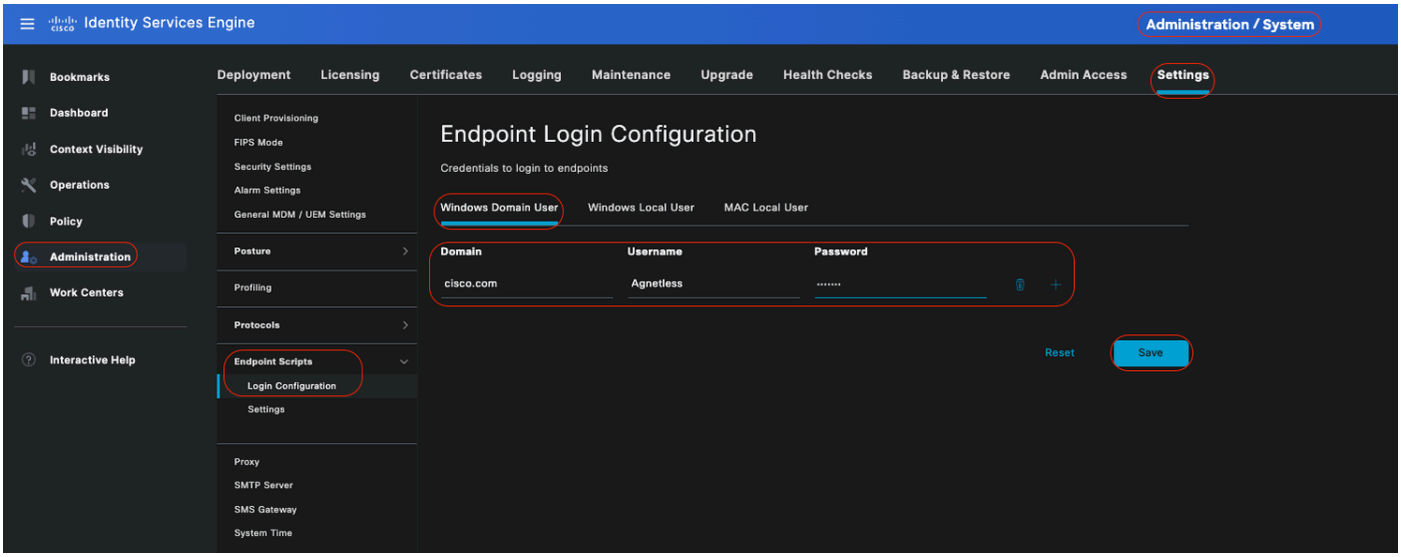
這些相同的憑證由終端指令碼使用，以便思科ISE可以登入到客戶端。

對於Windows裝置，只需配置兩個前頁籤**(Windows域使用者和Windows本地使用者)**

- **Windows域使用者：**

配置思科ISE必須用來透過SSH登入客戶端的域憑證。按一下Plusicon，並視需要輸入多個Windows登入。對於每個域，請在Domain、Username和Passwordfield中輸入所需的值。如果配置域憑據，則在Windows本地使用者頁籤中配置的本地使用者憑據將被忽略。

如果您管理透過Active Directory域使用無代理狀態評估的Windows終端，請確保提供域名以及具有本地管理許可權的憑據。

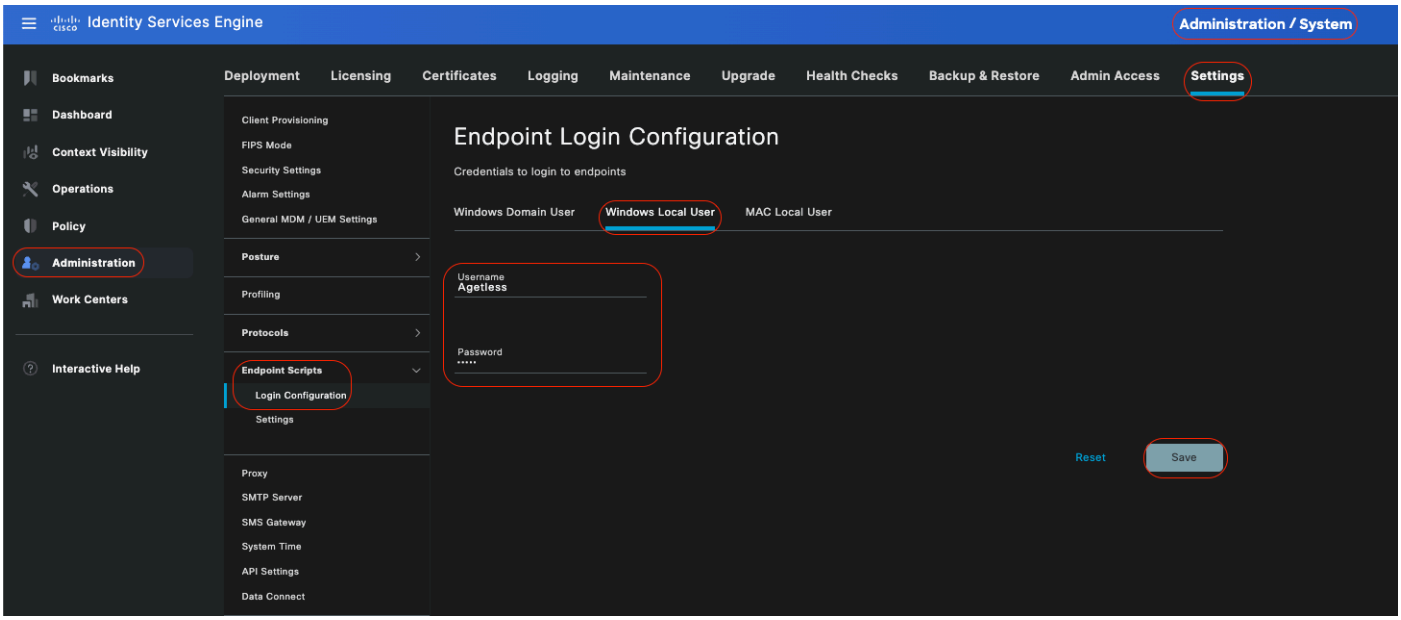


Windows域使用者

- **Windows本地使用者：**

配置思科ISE用於透過SSH訪問客戶端的本地帳戶。本地帳戶必須能夠運行Powershell和Powershell遠端。

如果您不管理透過Active Directory域使用無代理狀態評估的Windows端點，請確保提供具有本地管理許可權的憑據。

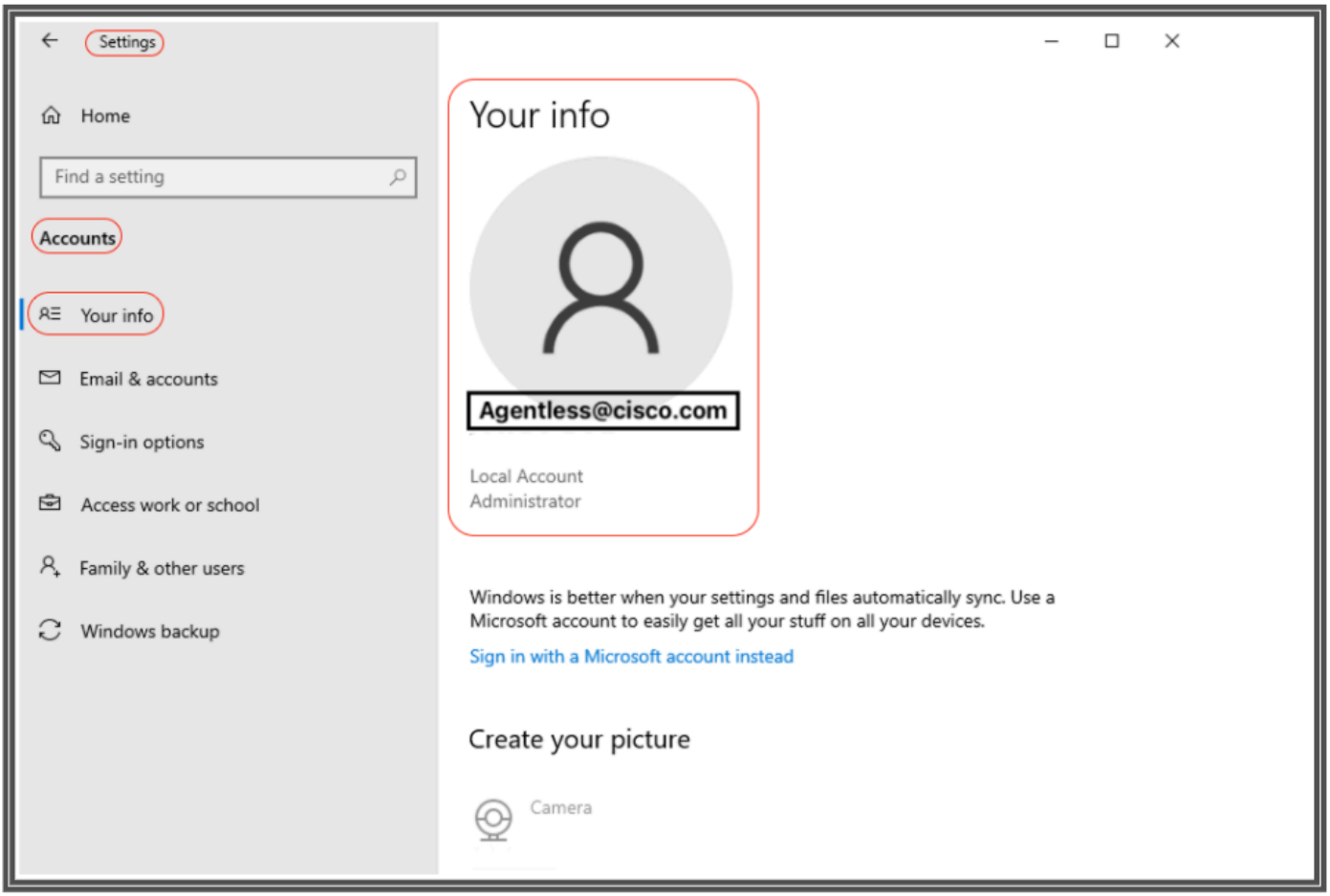


*Windows*本地使用者

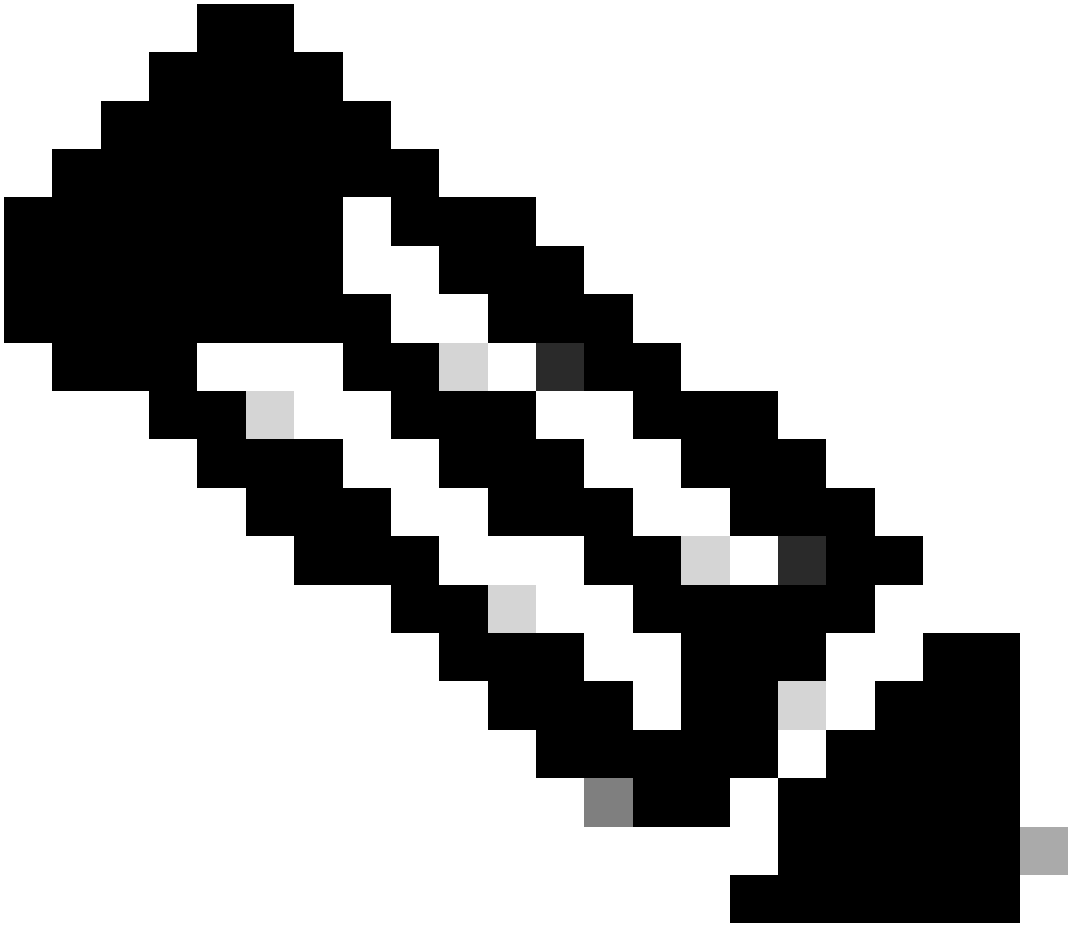
驗證帳戶

要驗證您的Windows域使用者和Windows本地使用者帳戶，以便您可以在「終端登入憑據」下準確增加適當的資料，請使用以下步驟：

Windows本地使用者：使用GUI（設定應用）按一下**WindowsStart**按鈕，選擇**設定**（齒輪圖示），按一下**帳戶**，然後選擇您的資訊：


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

驗證帳戶



注意：對於MacOS，您可以參閱**MAC Local User**。但是在本配置示例中，您不會看到MacOS配置。

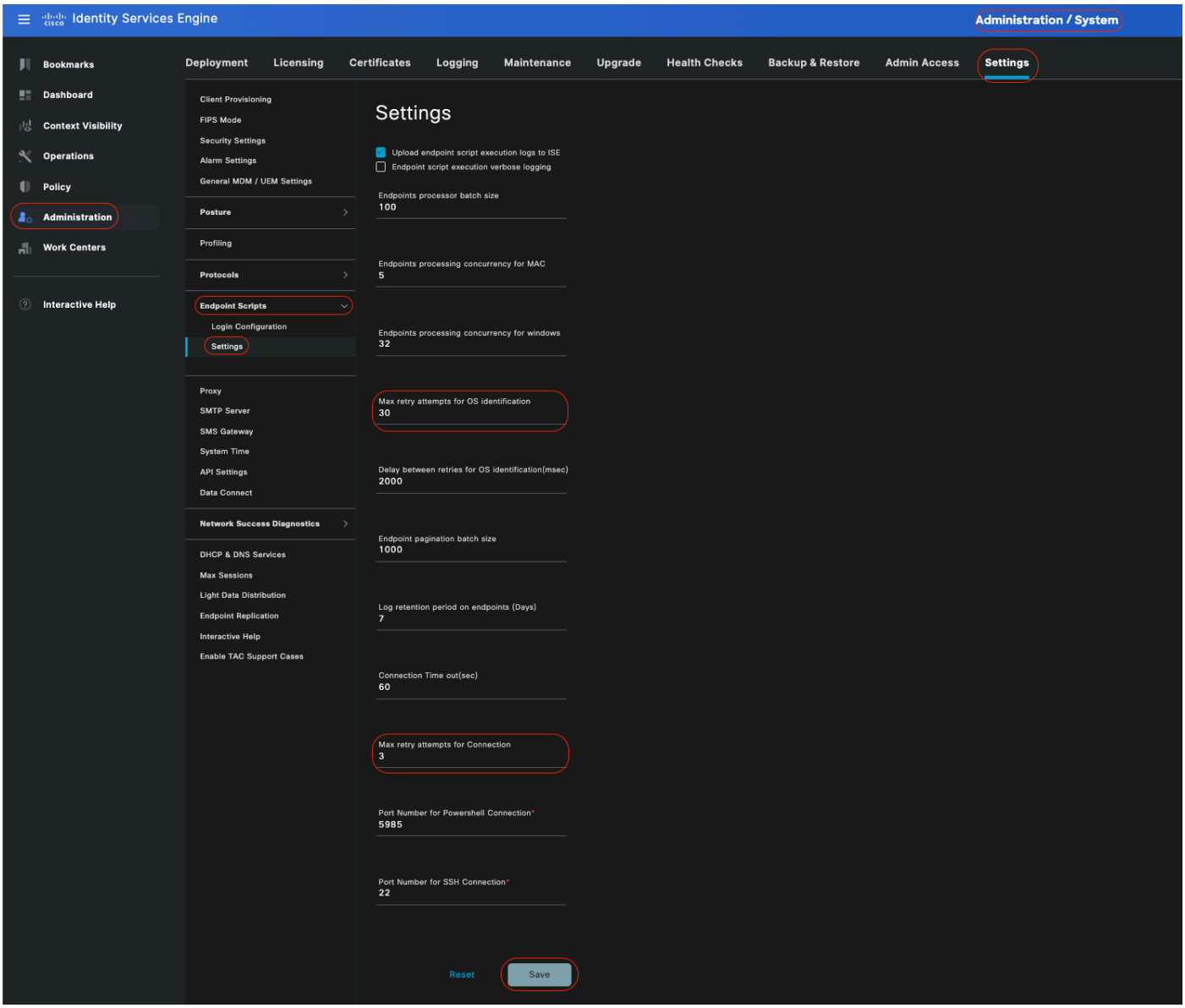
- **MAC Local User：**配置Cisco ISE用於透過SSH訪問客戶端的本地帳戶。本地帳戶必須能夠運行Powershell和Powershell遠端。在Username欄位中，輸入本地帳戶的帳戶名稱。

要檢視Mac OS帳戶名，請在終端中運行以下命令whoami：

設定

在思科ISE GUI中，點選選單圖示(
)並**選擇管理(Administration) > 設定(Settings) > 終端指令碼(Endpoint Scripts) > 設定(Settings)，然後為OS標識配置Max retry attempts for OS identification，Delay between retries for OS identification等**。這些設定決定了確認連線問題的速度。例如，只有在所有重試未用完的情況下，日誌中才會顯示PowerShell埠未打開的錯誤。

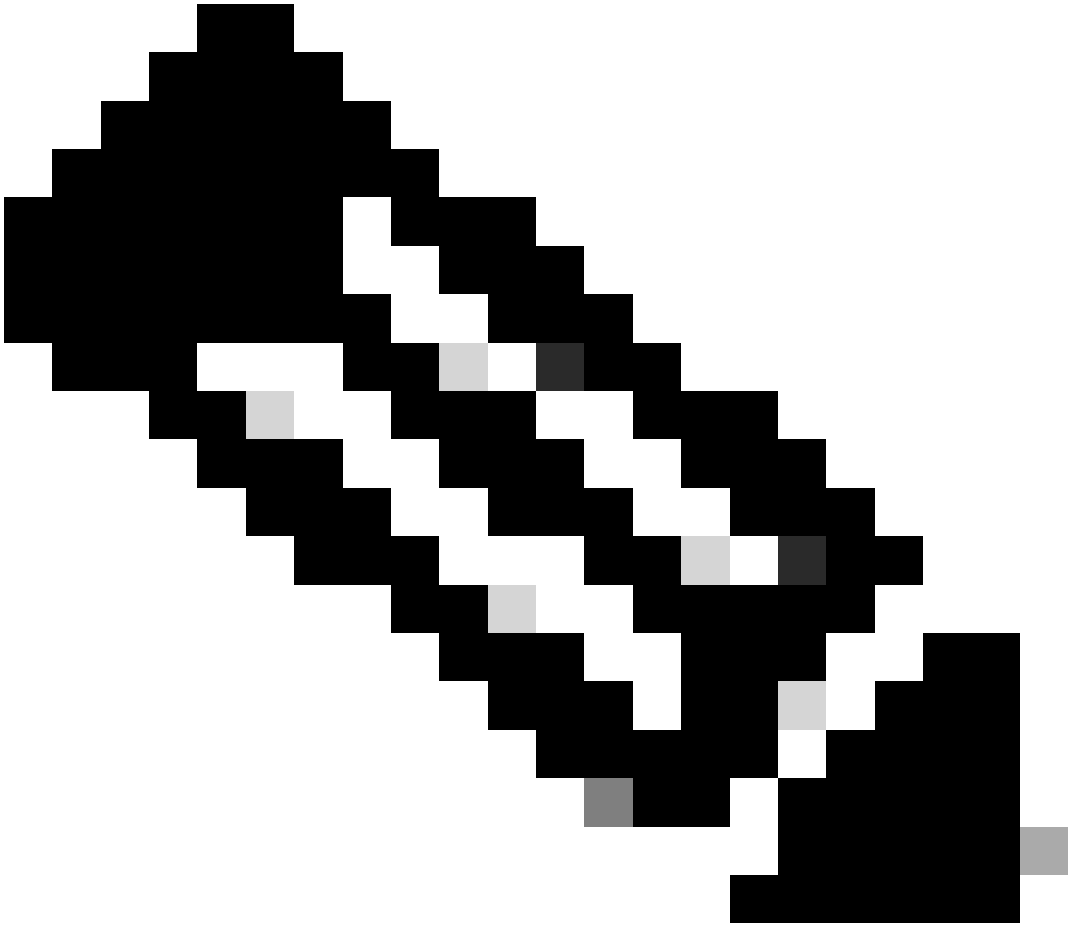
此螢幕截圖顯示了預設值設定：



終端指令碼設定

當客戶端使用無代理狀態進行連線時，您可以在即時日誌中看到它們。

配置Windows終端並進行故障排除



注意：這些是一些建議，可在Windows裝置上檢查並應用；但是，如果遇到使用者許可權、PowerShell訪問等問題，您必須參考Microsoft文檔或聯絡Microsoft支援人員……

檢驗和故障排除前提條件

測試到埠5985的TCP連線

對於Windows客戶端，必須打開埠5985以訪問客戶端上的powershell。運行此命令以確認到埠5985的TCP連線： **Test-NetConnection -ComputerName localhost -Port 5985**

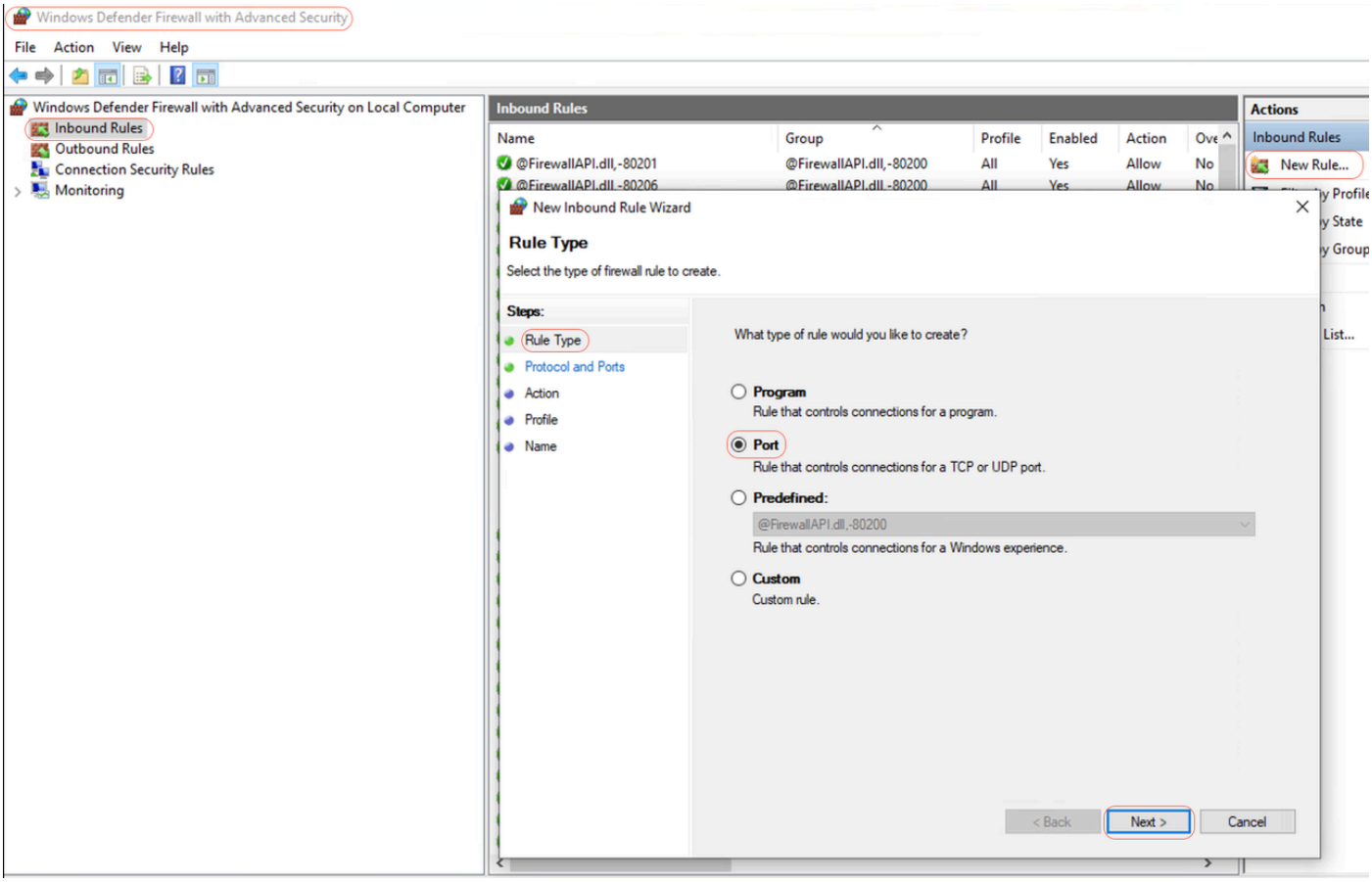
此螢幕截圖中所示的輸出表明到localhost上埠5985的TCP連線失敗。這表示使用連線埠5985的WinRM（Windows遠端管理）服務未執行或未正確設定。

```
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

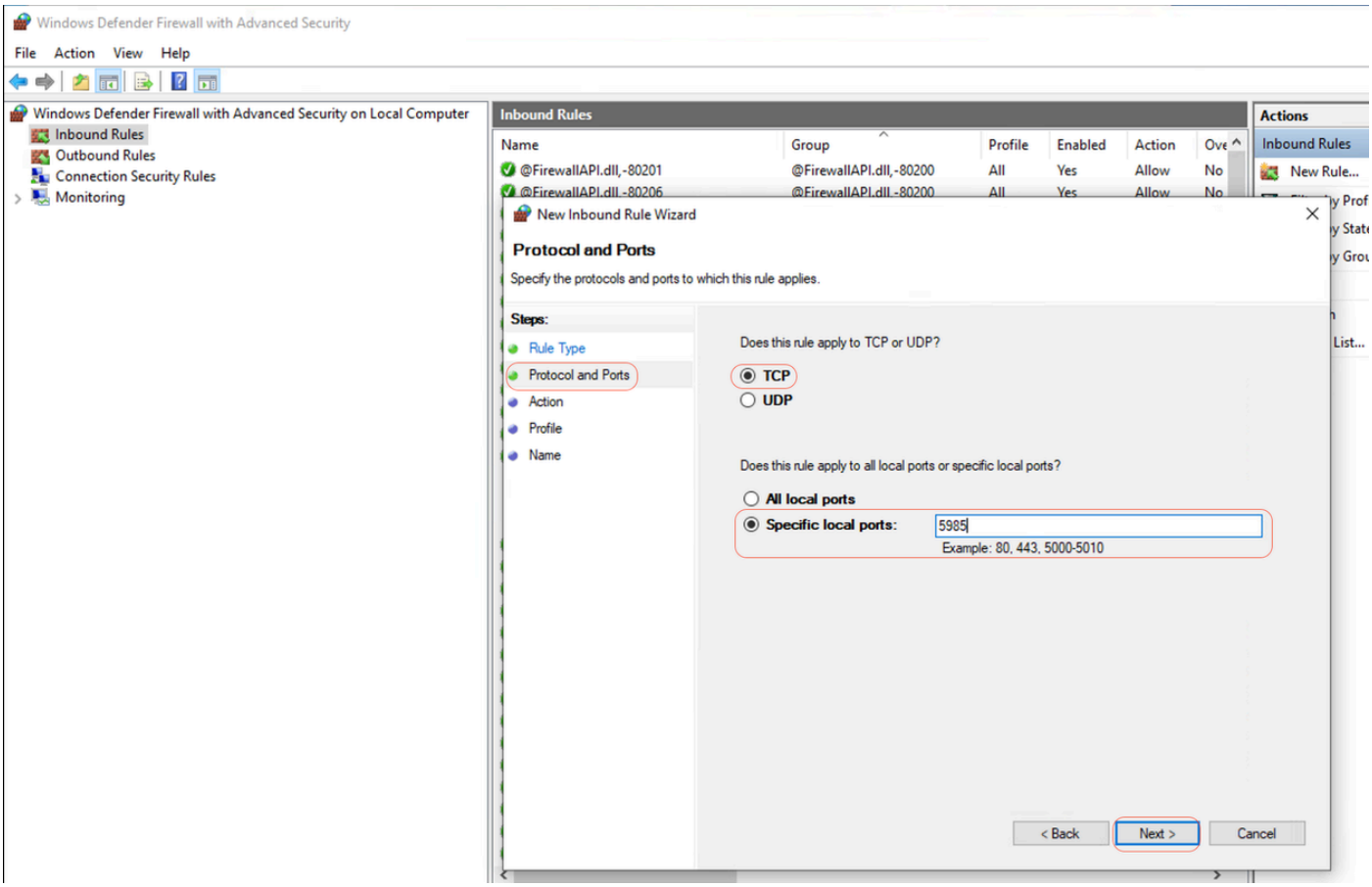
建立入站規則以允許埠5985上的PowerShell

第1步-在Windows GUI中，轉至**搜尋欄，鍵入具有高級安全性的Windows Firewall，按一下該欄並選擇Run as administrator > Inbound Rules > New Rule > Rule Type > Port > Next：**



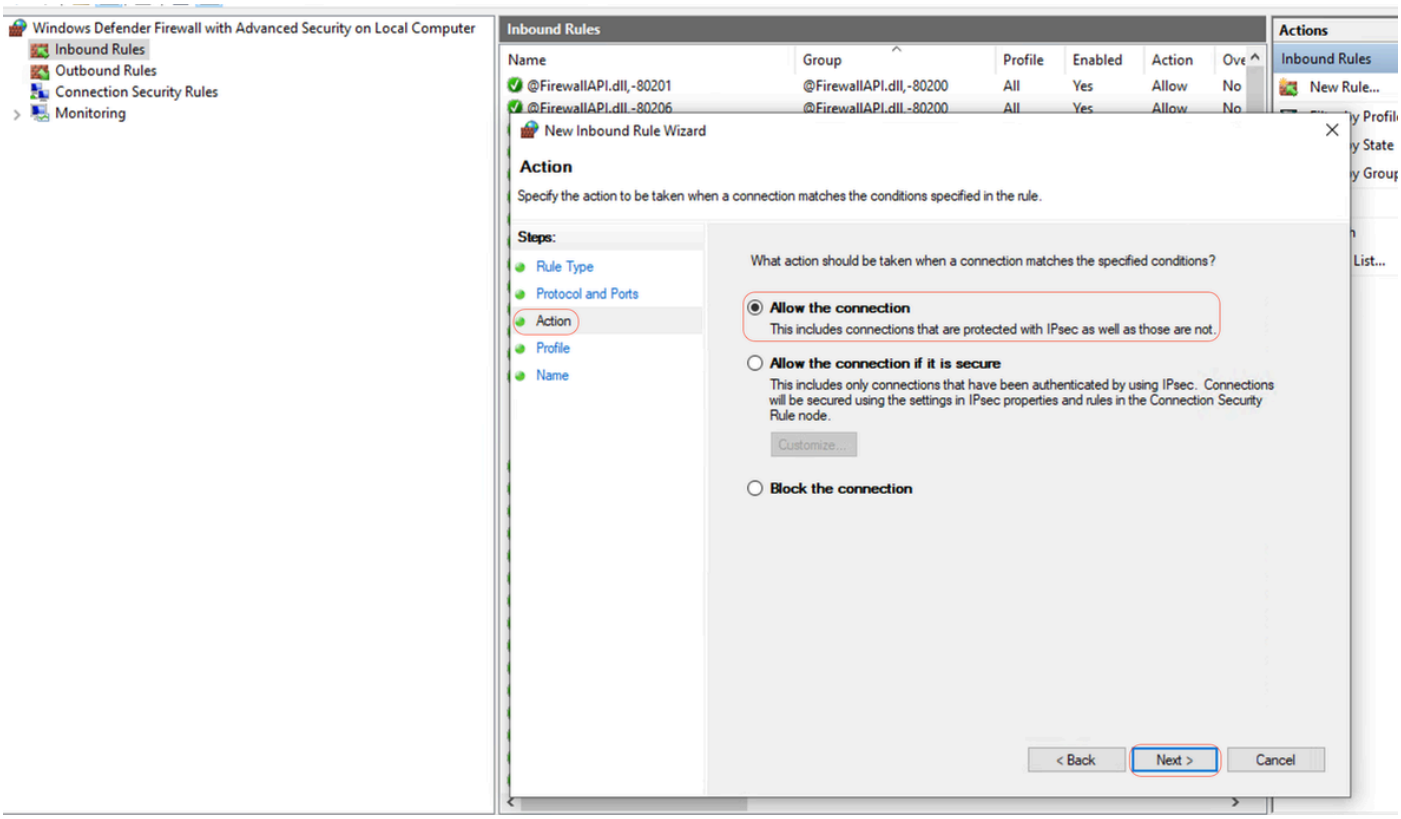
新建入站規則-埠

第2步-在協定和埠下，選擇TCP和指定本地埠，鍵入埠號5985(PowerShell遠端處理的預設埠)並按一下Next：



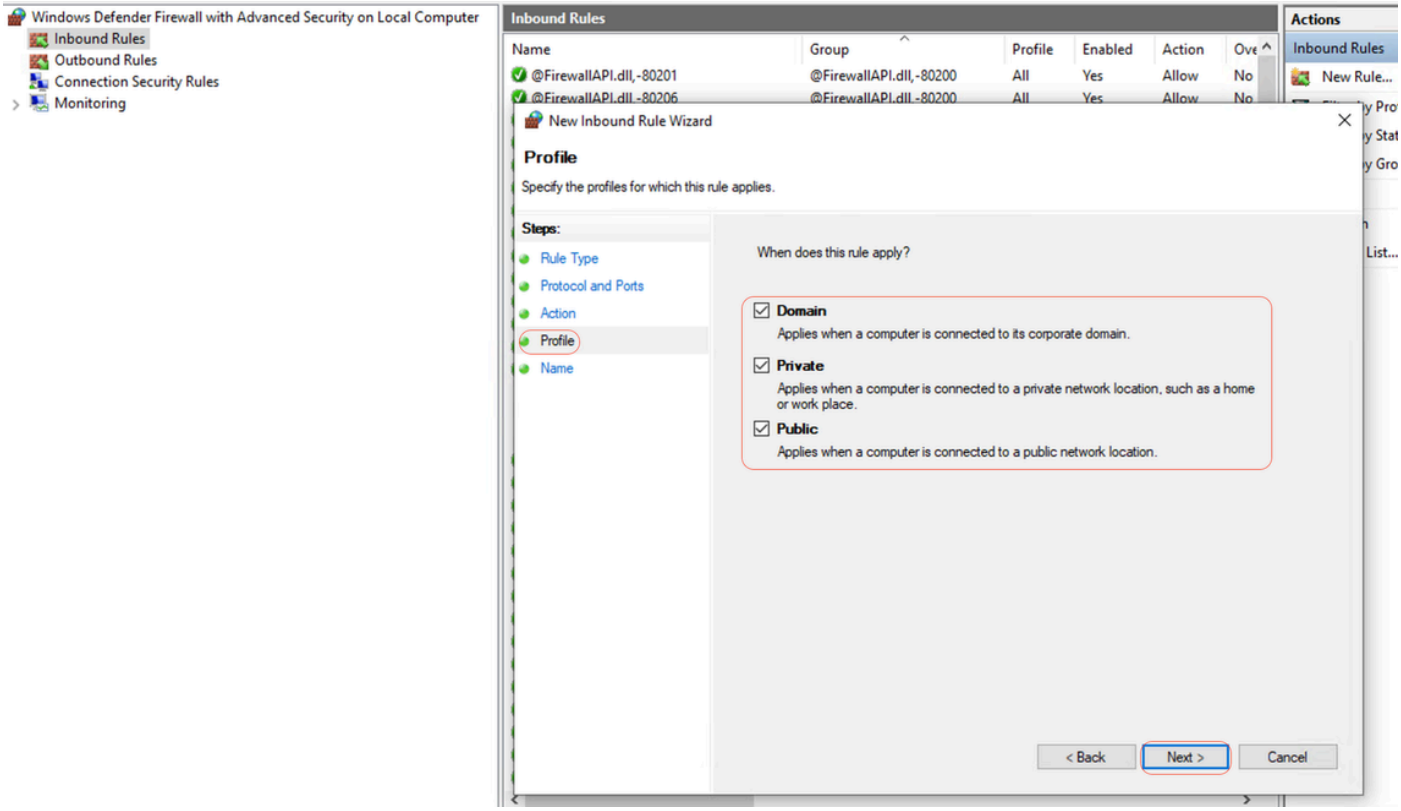
協定和埠

第3步-在操作>選擇允許連線>下一步下：



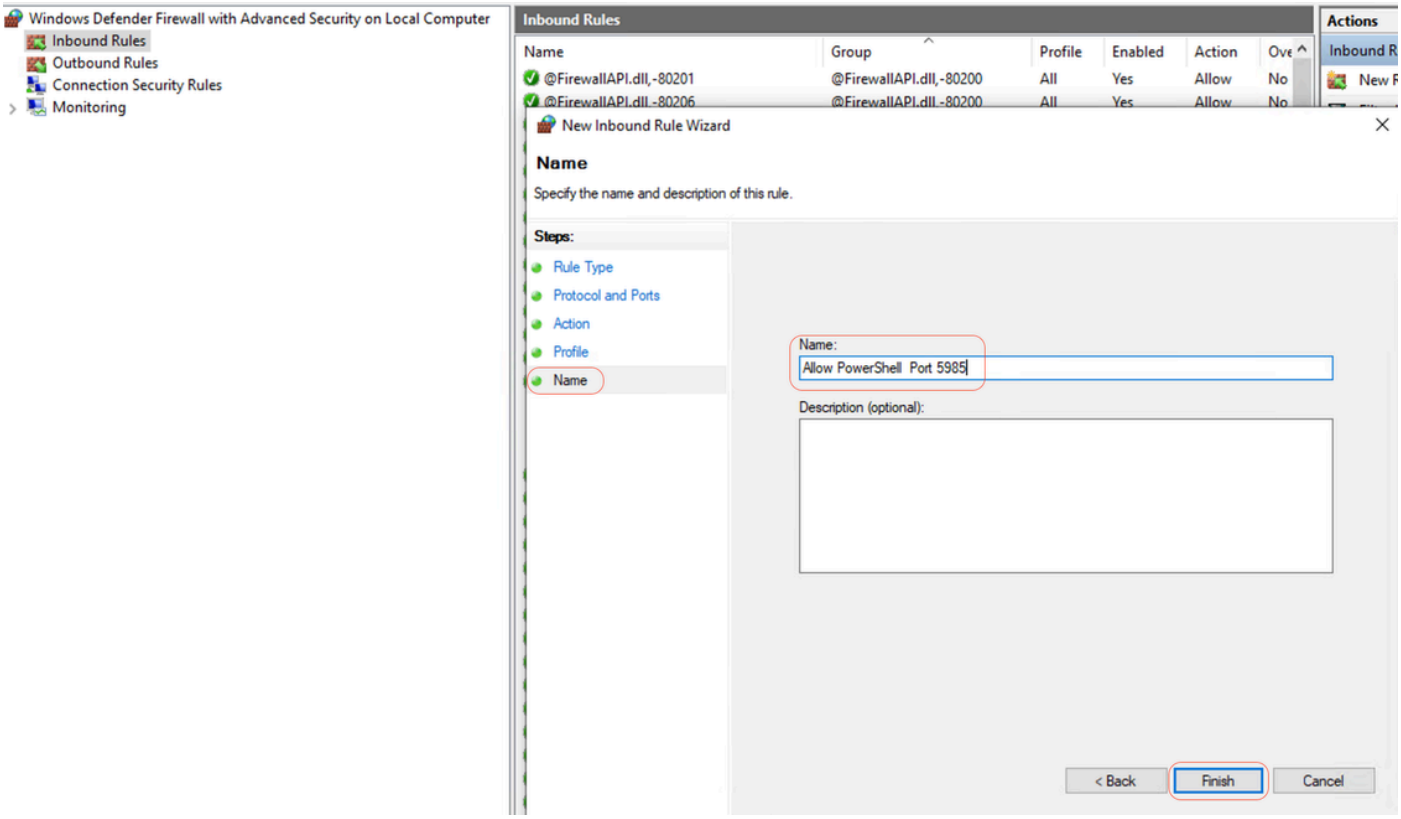
動作

第4步-在配置檔案下，選中Domain、Private和Public覈取方塊，然後按一下Next：



設定檔

第5步-在名稱下，輸入規則名稱，例如允許在埠5985上使用PowerShell，然後按一下完成：

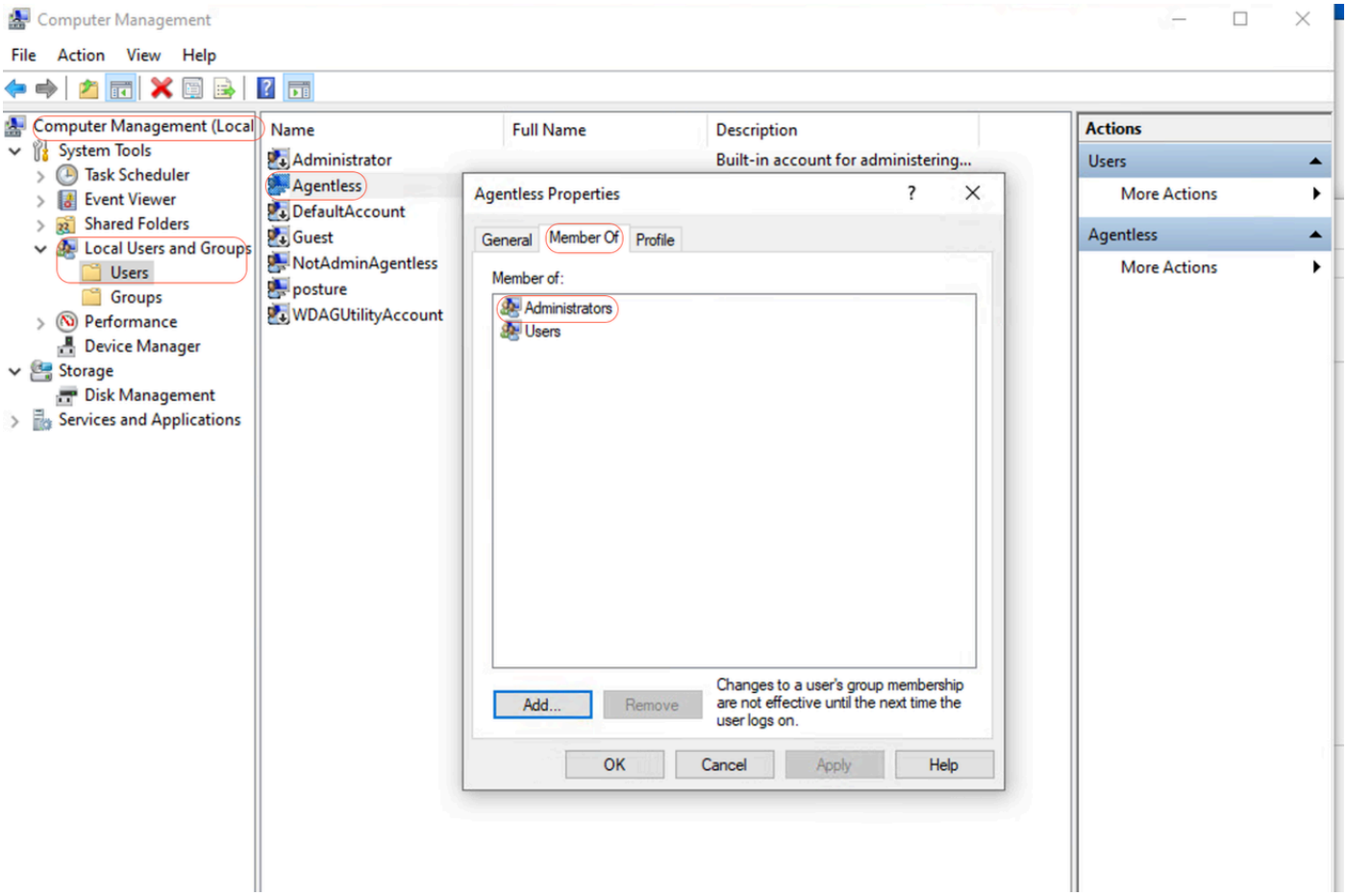


名稱

Shell登入的客戶端憑據必須具有本地管理員許可權

Shell登入的客戶端憑據必須具有本地管理員許可權。 要確認是否具有管理員許可權，請檢查以下步驟：

在Windows GUI中，轉至「設定」(Settings) >「電腦管理」(Computer Management) >「本地使用者和組」(Local Users and Groups) >「使用者」(Users) >「選擇使用者帳戶」(Select the User Account)(在本例中，無代理帳戶已選中) >「帳戶的成員」(Member of)，帳戶必須具有Administrators組。



本地管理員許可權

正在驗證WinRM偵聽程式

確保已在埠5985上為HTTP配置WinRM偵聽程式：

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

啟用PowerShell遠端處理WinRM

確保服務正在運行且已配置為自動啟動，請執行以下步驟：

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**

預期輸出：

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必須是v7.1或更高版本。客戶端必須具有cURL v7.34或更高版本：

如何在Windows上檢查PowerShell和cURL版本

確保您使用的是適當版本的PowerShell；cURL對於安全評估無代理程式至關重要：

正在檢查PowerShell版本

若為 Windows：

1. **Open PowerShell：**

·按Win + X，然後選擇Windows PowerShell或Windows PowerShell (Admin)。

2. 執行命令：$PSVersionTable.PSVersion

·此命令輸出系統上安裝的PowerShell的版本詳細資訊。

正在檢查cURL版本

若為 Windows：

1. 打開命令提示符：

·按Win + R，鍵入cmd，然後按一下Enter。

2.執行命令： curl --version

·此命令顯示系統上安裝的cURL版本。

在Windows裝置上檢查PowerShell和cURL版本的輸出

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>

其他組態

此命令將電腦配置為信任特定遠端主機進行WinRM連線： 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> -

具有-Authentication Negotiate和-Credential引數的test-wsman cmdlet是驗證遠端電腦上WinRM服務的可用性和配置的強大工具： test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

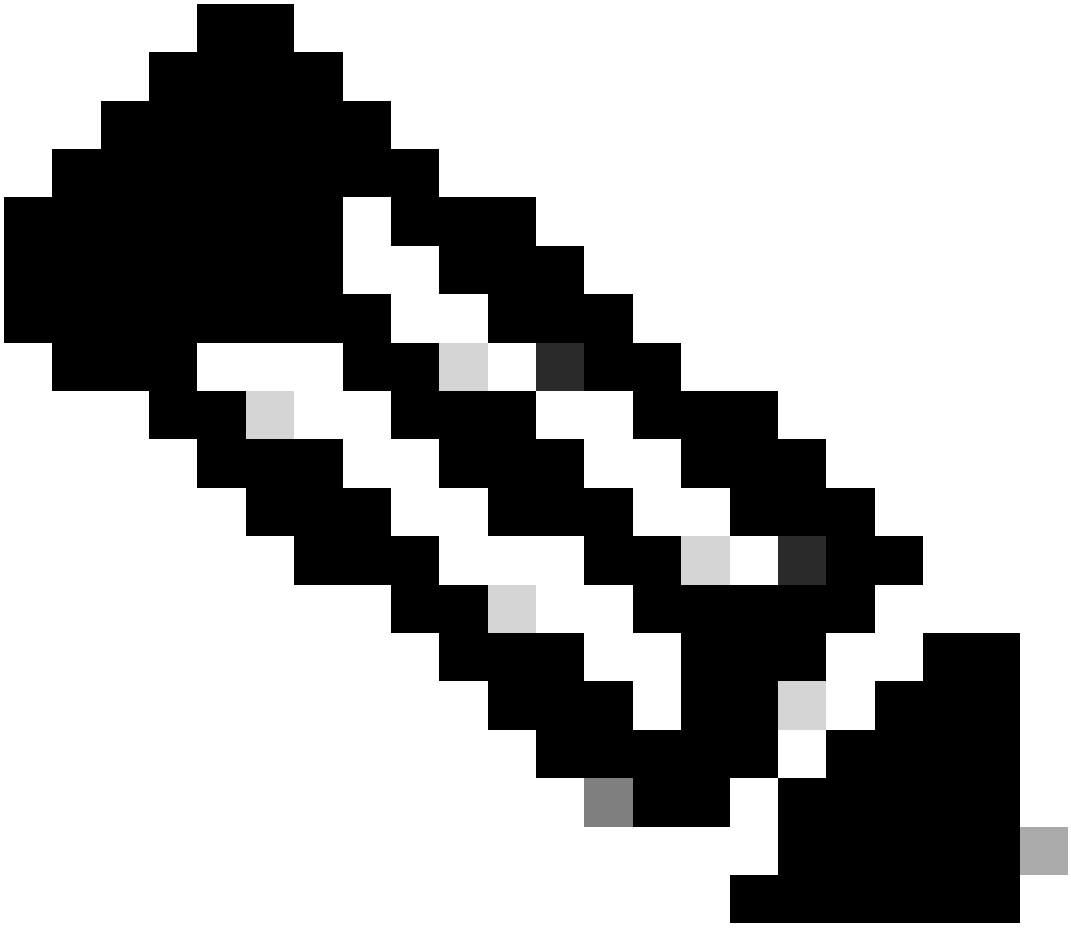
Powershell必須是v7.1或更高版本。客戶端必須具有cURL v7.34或更高版本：

在macOS上：

1. **開放式終端：**

·您可在**Applications > Utilities**中找到終端。

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



註：註： ·確保已安裝PowerShell核心(pwsh)。如果沒有，您可以透過Homebrew進行安裝（確保您已安裝Himebrew）： brew install --cask powershell

在macOS上：

1. **開放式終端：**

·您可在**Applications > Utilities**中找到終端。

2.執行命令： curl --version

·此命令必須顯示系統上安裝的cURL版本。

對於MacOS客戶端，訪問SSH的埠22必須打開才能訪問客戶端

逐步指南：

1.**開啟系統偏好設定：**

·從Apple選單導航到**System Preferences**。

2. **啟用遠端登入：**

·轉到**共用**。

· 選中**Remote Login**旁邊的覈取方塊。

·確保**Allow access for**選項已設定為相應的使用者或組。選擇**All users**允許在Mac上具有有效帳戶的任何使用者透過SSH登入。

3. **驗證防火牆設定：**

·如果啟用了防火牆，您需要確保它允許SSH連線。

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

·點選**防火牆選項**按鈕。

·檢查是否列出並允許使用**Remote Login**或**SSH**。如果未列出，請按一下**Add**按鈕(+)進行增加。

4.**透過終端機開啟連線埠22（如有必要）：**

·從**Applications > Utilities**打開**Terminal**應用程式。

·使用pfctl命令檢查當前防火牆規則並確保埠22處於打開狀態：sudo pfctl -sr | grep 22

·如果埠22未打開，您可以手動增加規則以允許SSH：echo 「pass in proto tcp from any to any port 22」 | sudo pfctl -ef -

5. **測試SSH訪問：**

· 從其他裝置打開終端或SSH客戶端。

· 嘗試使用其IP地址連線到macOS客戶端：ssh username@<macOS-client-IP>

· **用相應的使用者帳戶替換**username，用macOS客戶端的IP地址替換<macOS-client-IP>。

對於MacOS，請確保在sudoers檔案中更新此條目，以避免終端上的證書安裝失敗：

管理macOS終端時，確保無需密碼提示即可執行特定的管理命令至關重要。

必要條件

· macOS電腦上的管理員訪問許可權。

·基本熟悉終端命令。

更新Sudoers檔案的步驟

1. **開放式終端：**

·您可在**Applications** > **Utilities**中找到終端。

2. **編輯Sudoers檔案：**

·使用visudo命令可安全編輯sudoers檔案。這樣可確保儲存檔案前會捕捉到任何語法錯誤。sudo visudo

· 系統將提示您輸入管理員密碼。

3.**查詢相應部分：**

·在Visudo編輯器中，導航到定義使用者特定規則的部分。通常情況下，這是指向檔案底部。

4.**新增必要專案：**

· 增加以下行，向指定的使用者授予在不使用口令的情況下運行security和osascript命令的許可權： <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

·用macOS管理員的實際使用者名稱替換**<macadminusername>**。

5. **儲存並退出：**

·如果使用預設編輯器(nano)，請按Ctrl + X退出，然後按Y確認更改，最後按Enter儲存檔案。

· **如果使用**vi或vim**，請按**Esc**，鍵入**：wq**，然後按**Enter**儲存並退出**。

6.**驗證更改：**

· 為確保更改生效，您可以運行需要更新sudo許可權的命令。舉例來說：

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

· 無需提示輸入口令即可執行這些命令。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。