ポスチャエージェントレスの設定

内容

はじめに

このドキュメントでは、ISEでポスチャエージェントレス(PAP)を設定する方法と、エージェントレススクリプトを実行するためにエンドポイントで必要な操作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine(ISE)を使用します。
- ポスチャ.
- PowerShellとSSH
- Windows 10以降

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)3.3バージョン
- パッケージCiscoAgentlessWindows 5.1.6.6
- Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ISEポスチャは、クライアント側の評価を実行します。クライアントはISEからポスチャ要件ポリシーを受信し、ポスチャデータ収集を実行し、結果をポリシーと比較し、アセスメント結果をISEに返します。

ISEは、ポスチャレポートに基づいて、デバイスが準拠しているか非準拠であるかを判断します。

エージェントレスポスチャは、クライアントからポスチャ情報を収集し、エンドユーザの操作を必要とせずに完了時に自動的にポスチャを削除するポスチャ方法の1つです。エージェントレスポスチャは、管理者権限を使用してクライアントに接続します。

はじめに

前提条件

- クライアントはIPv4またはIPv6アドレスを介して到達可能であり、そのIPアドレスがRADIUSアカウンティングで使用可能である必要があります。

- クライアントは、IPv4またはIPv6アドレスを使用してCisco Identity Services Engine(ISE)から到達可能である必要があります。また、このIPアドレスはRADIUSアカウンティングで使用できる必要があります。
- 現在、WindowsクライアントとMacクライアントがサポートされています。
    - Windowsクライアントでは、クライアントのPowerShellにアクセスするためのポート5985が開いている必要があります。Powershellはv7.1以降である必要があります。クライアントにはcURL v7.34以降が必要です。
    - MacOSクライアントの場合、SSHにアクセスするためのポート22がクライアントにアクセスするために開いている必要があります。クライアントにはcURL v7.34以降が必要です。
- シェルログイン用のクライアントクレデンシャルには、ローカル管理者権限が必要です。
- 設定手順の説明に従って、ポスチャフィードのアップデートを実行し、最新のクライアントを取得します。次の点を確認してください。
- MacOSの場合は、エンドポイントでの証明書のインストールエラーを回避するために、sudoersファイルでこのエントリが更新されていることを確認します。次の点を確認してください。

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

-

MacOSの場合、設定するユーザアカウントは管理者アカウントである必要があります。MacOSのエージェントレスポスチャは、権限を付与した場合でも、他のアカウントタイプでは機能しません。このウィンドウを表示するには、メニューアイコン(

)をクリックし、Administration > System > Settings > Endpoint Scripts > Login > MAC Local Userの順に選択します。

- Microsoftからのアップデートが原因でWindowsクライアントのポート関連アクティビティが変更された場合、Windowsクライアントのエージェントレスポスチャ設定ワークフローを再設定する必要があります。

サポートされるポスチャ条件

- ファイル条件。ただし、USER_DESKTOPおよびUSER_PROFILEファイルパスを使用する条件は除きます。
- サービス条件（macOSでのシステムデーモンとデーモンまたはユーザエージェントのチェックを除く）
- 適用条件
- 外部データソースの条件
- 複合条件
- マルウェア対策条件
- パッチ管理条件(**EnabledandUp To** Dateconditionチェックを除く)
- ファイアウォールの状態

- ディスクの暗号化条件（暗号化の場所に基づく条件チェックを除く）
- HCSKをルートキーとして使用する条件を除くレジストリ条件

サポートされていないポスチャ条件

- 修復方法
- 猶予期間
- 定期的再評価
- アクセプタブルユースポリシー

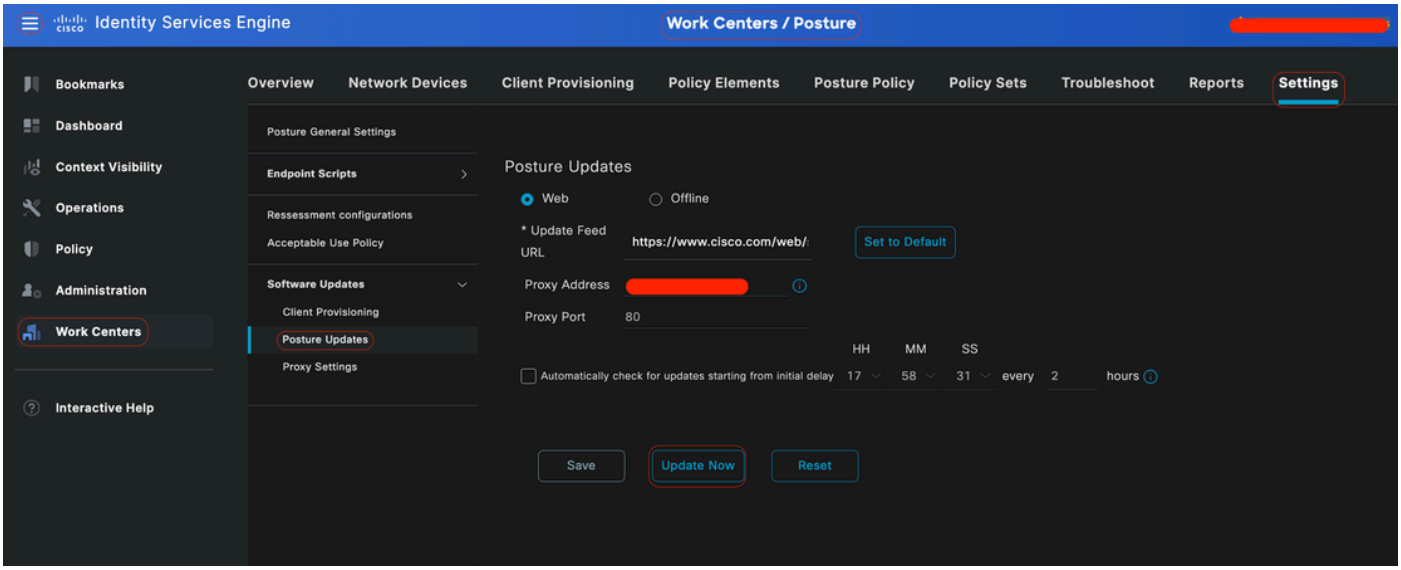
ISEの設定

ポスチャフィードの更新

ポスチャの設定を開始する前に、ポスチャフィードを更新することをお勧めします。

Cisco ISE GUIでメニューをクリックし(

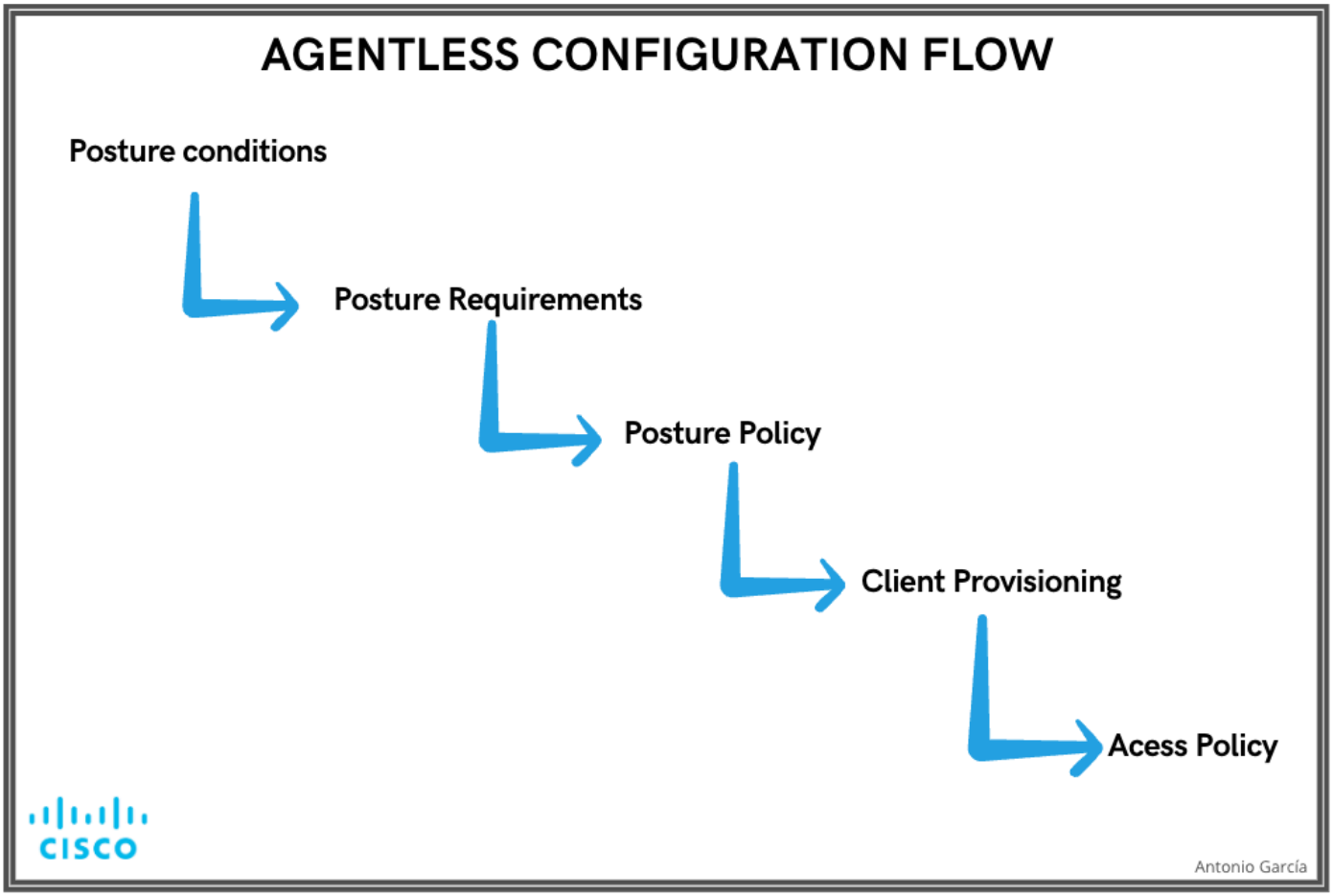
)、**Work Centers** > **Posture** > **Settings** > **Software Updates** > **Update Now**の順に選択します。



ポスチャフィードの更新

ポスチャエージェントレス設定フロー

最初の設定は次の設定に必要になるため、ポスチャエージェントレスは順番に設定する必要があります。修復はフローには含まれていないことに注意してください。ただし、このドキュメントの後半では、修復を設定する別の方法について説明します。



エージェントレス設定のフロー

エージェントレスポスチャ設定

ポスチャ条件

ポスチャ条件は、準拠するエンドポイントを定義するセキュリティポリシーの一連のルールです。これらの項目の一部には、ファイアウォール、アンチウイルスソフトウェア、アンチマルウェア、ホットフィックス、ディスク暗号化などのインストールが含まれます。

Cisco ISE GUIで、メニュー(

)をクリックし、**Work Centers** > Posture > **Policy Elements** > Conditionsの順に選択し、Addをクリックして、エージェントレスポスチャを使用する1つ以上のPosture **Conditions**を作成し、要件を特定します。**Condition**が作成されたら、**Save**をクリックします。

このシナリオでは、「**Agentless_Condition_Application**」という名前のアプリケーション条件が次のパラメータで設定されています。

・オペレーティングシステム：Windows All

この条件は、Windowsオペレーティングシステムのバージョンに適用され、異なるWindows環境全体で幅広い互換性を確保します。

・チェック**基準**：プロセス

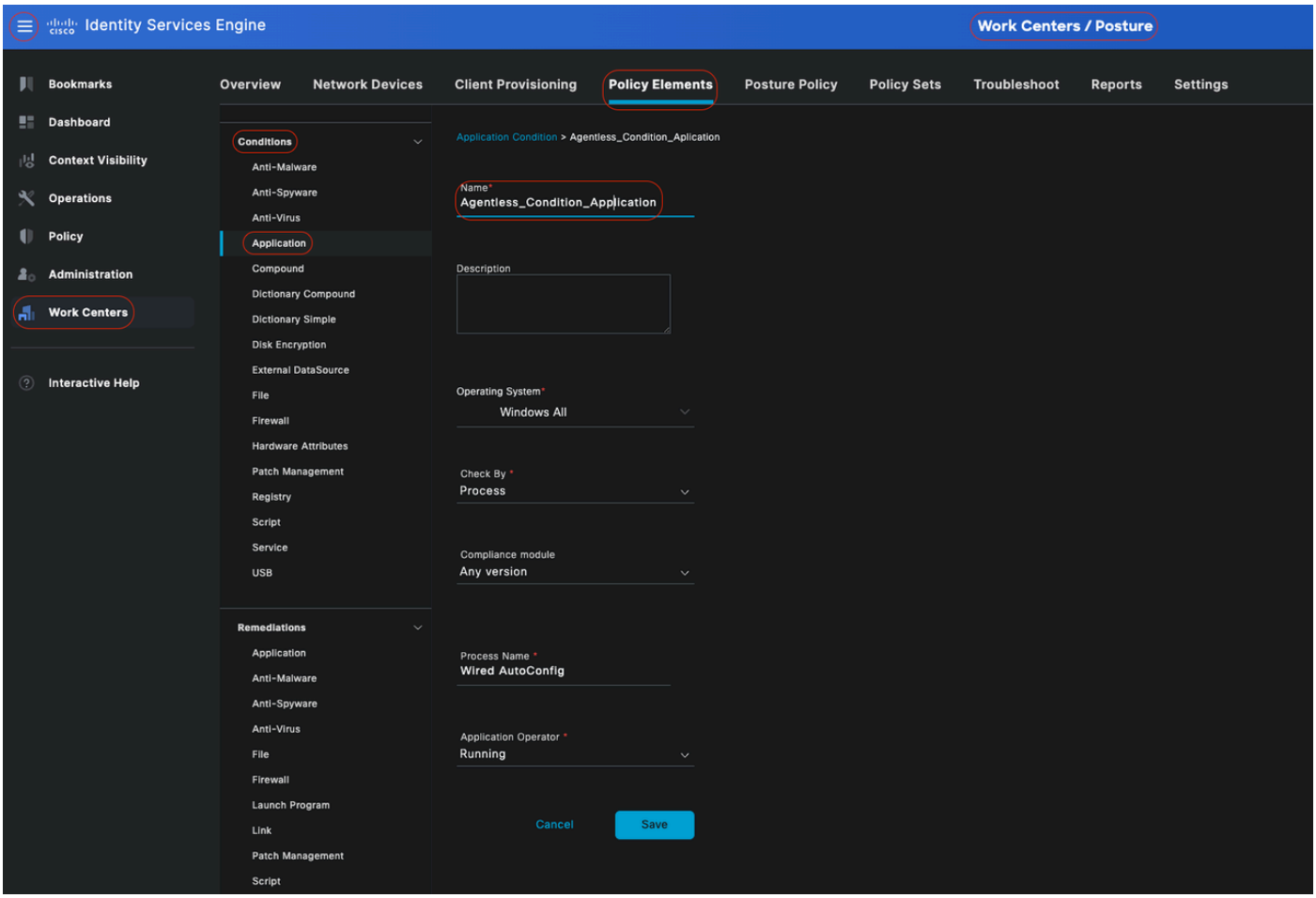
システムはデバイス内のプロセスを監視します。**Process**または**Application**のいずれかを選択できます。この場合は、**Process**が選択されています。

・プロセス**名**：Wired AutoConfig

Wired AutoConfigプロセスは、Compliant Module(IOS)がデバイスをチェックインするプロセスです。このプロセスは、IEEE 802.1X認証を含む有線ネットワーク接続の設定と管理を担当します。

・アプリケーション**演算子**：実行中

コンプライアンスモジュールは、**有線AutoConfig**プロセスがデバイスで現在実行されているかどうかを確認します。**Running**または**Not Running**のいずれかを選択できます。この例では、プロセスがアクティブであることを確認するために**Running**が選択されています。



エージェントレス状態

ポスチャ要件

ポスチャ要件は、複合条件のセット、またはロールとオペレーティングシステムにリンクできる1つの条件です。ネットワークに接続するすべてのクライアントは、ポスチャ評価中にネットワーク上で準拠するために必須の要件を満たす必要があります。

Cisco ISE GUIで、メニュー(

)をクリックして、**Work Centers** > **Posture** > **Policy** Elements > Requirementの順に選択します。 下矢印をクリックして**Insert** new **Requirement**を選択し、Agentless postureを使用する1つ以上の**PostureRequirement**を作成します。**要件**が作成されたら、**Done**、**Save**の順にクリックします。

この場合、「**Agentless_Requirement_Application**」という名前のアプリケーション要件は、次の基準で設定されています。

・オペレーティングシステム：Windows All

この要件は、すべてのバージョンのWindowsオペレーティング・システムに適用され、すべてのWindows環境に適用されます。

・ポスチャタイプ：エージェントレス

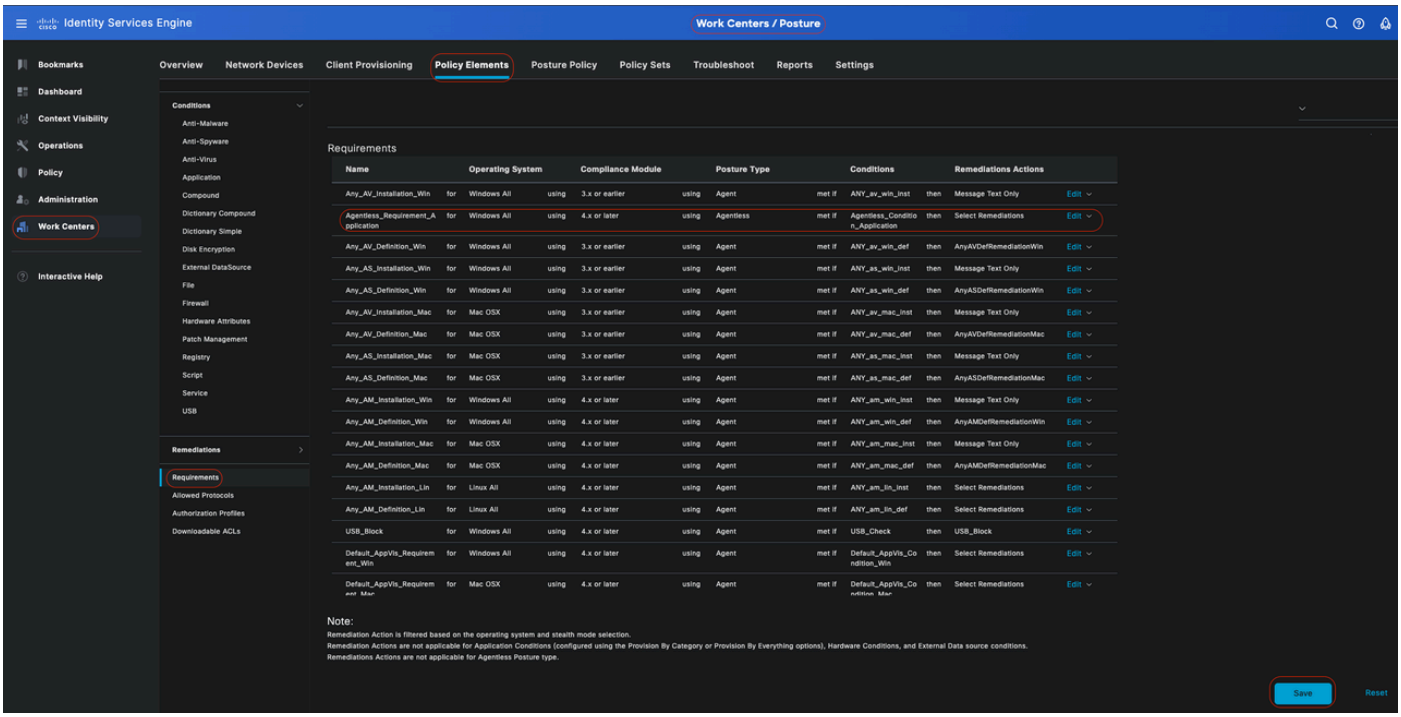
この設定は、エージェントレス環境に対して設定されます。使用可能なオプションには、**Agent**、**Agent Stealth**、**Temporal Agent**、および**Agentless**があります。このシナリオでは、エージェントレスが選択されました。

・条件：**Agentless_Condition_Application**

これは、ISEポスチャモジュールとコンプライアンスモジュールがデバイスのプロセス内でチェックする条件を指定します。選択された条件は**Agentless_Condition_Application**です。

•修復アクション:

この設定はエージェントレス環境を対象としているため、修復アクションはサポートされず、このフィールドはグレー表示されます。



エージェントレス要件

ポスチャ ポリシー

Cisco ISE GUIで、メニューアイコン(

)をクリックし、Work Centers > Posture > Posture Policyの順に選択します。 **下矢印**をクリックして**Insert new Requirement**を選択し、そのポスチャ要件にエージェントレスポスチャを使用する、サポートされている1つ以上のポスチャポリシールールを作成します。 ポスチャポリシーが作成されたら、**Done**、**Save**の順にクリックします。

このシナリオでは、「**Agentless_Policy_Application**」という名前のポスチャポリシーが次のパラメータで設定されています。

・ **ルール名：**Agentless_Policy_Application

これは、この設定例でポスチャポリシーに指定されている名前です。

・ オペレーティングシステム：Windows All

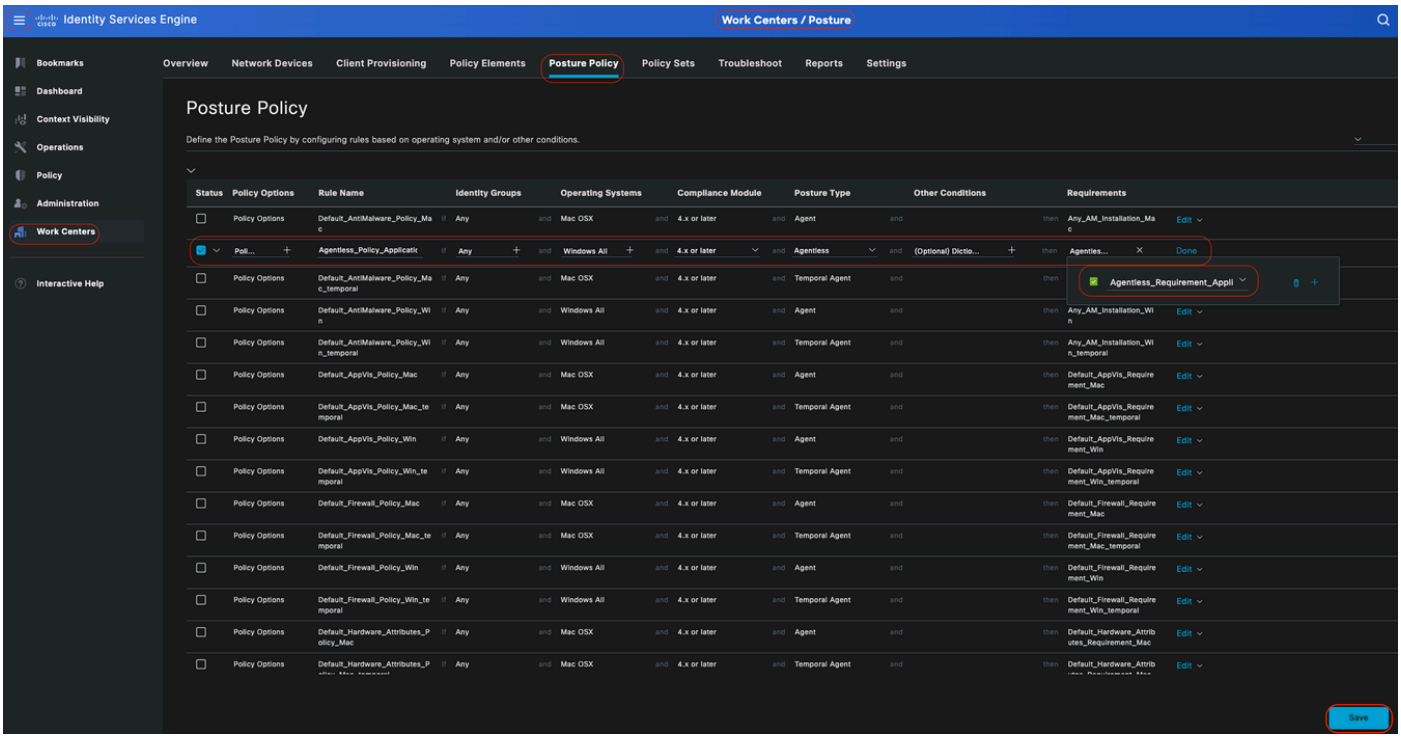
このポリシーは、Windowsオペレーティングシステムのすべてのバージョンに適用されるように設定されており、異なるWindows環境全体で幅広い互換性を確保します。

・ ポスチャタイプ：エージェントレス

この設定は、エージェントレス環境に対して設定されます。使用可能なオプションには、**Agent**、**Agent Stealth**、**Temporal Agent**、および**Agentless**があります。このシナリオでは、エージェントレスが選択されています。

•その他の条件：

この設定例では、追加の条件は作成されていません。ただし、ネットワーク上のすべてのWindowsデバイスではなく、対象デバイスだけがこのポスチャポリシーの対象となるように特定の条件を設定するオプションがあります。これは、ネットワークのセグメント化に特に役立ちます。



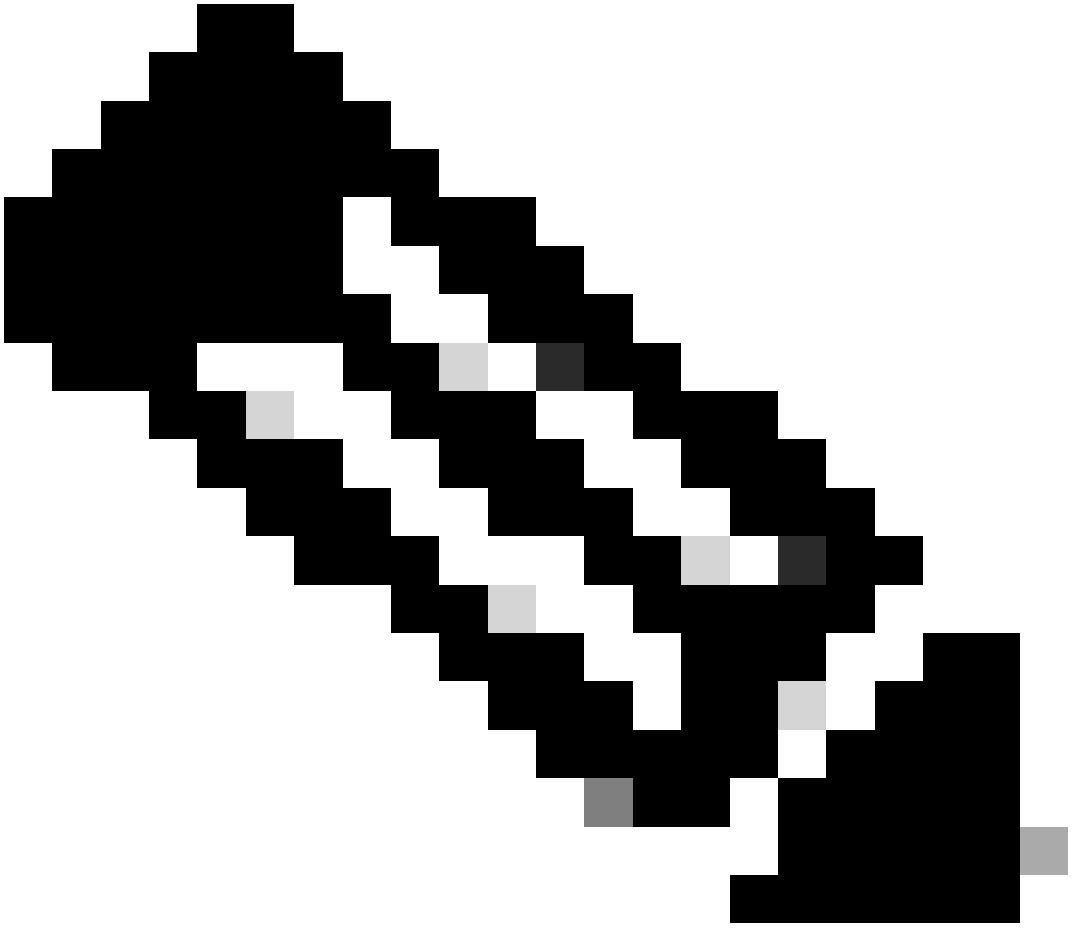
ポスチャエージェントレスポリシー

クライアント プロビジョニング

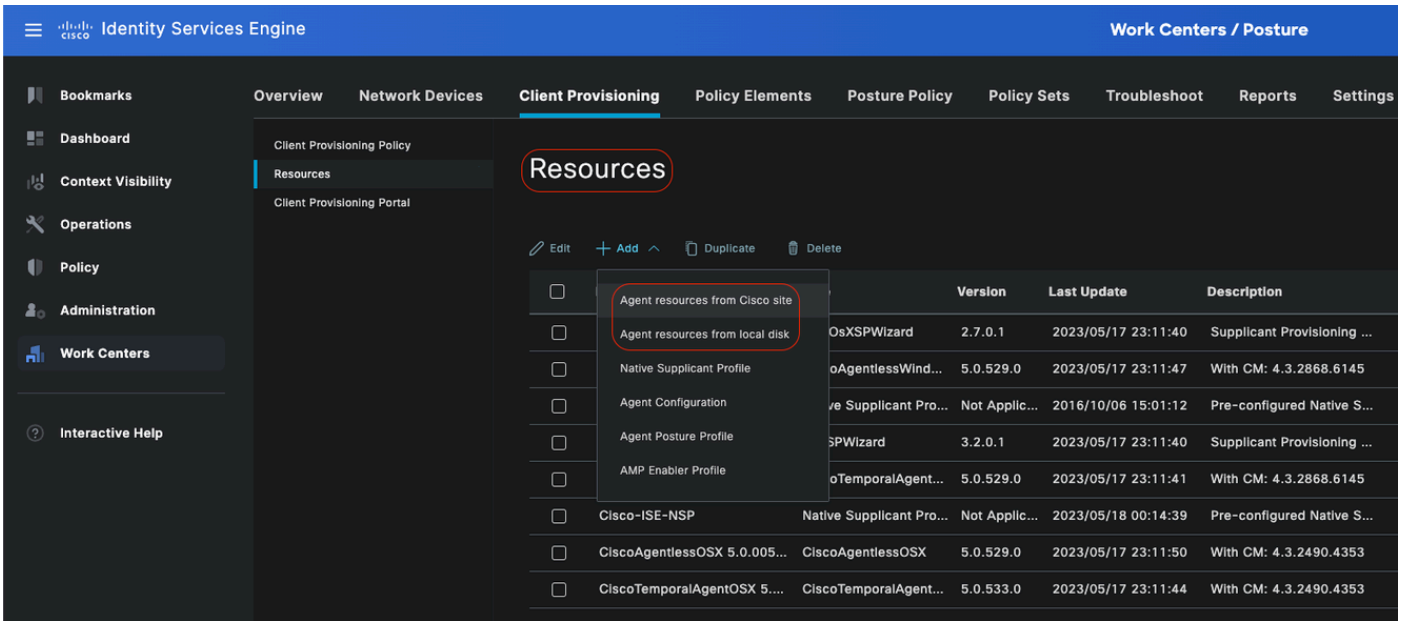
ステップ1：リソースのダウンロード

クライアントプロビジョニングの設定を開始するには、最初に必要なリソースをダウンロードし、後でクライアントプロビジョニングポリシーで使用できるようにISEで使用できるようにする必要があります。

ISEにリソースを追加する方法は、シスコサイトのエージェントリソースとローカルディスクのエージェントリソースの2つです。エージェントレスを設定しているため、ダウンロードするにはシスコのサイトからエージェントリソースにアクセスする必要があります。



注：このエージェントリソースをシスコのサイトから使用するには、ISE PANがインターネットアクセスを必要とします。



リソース

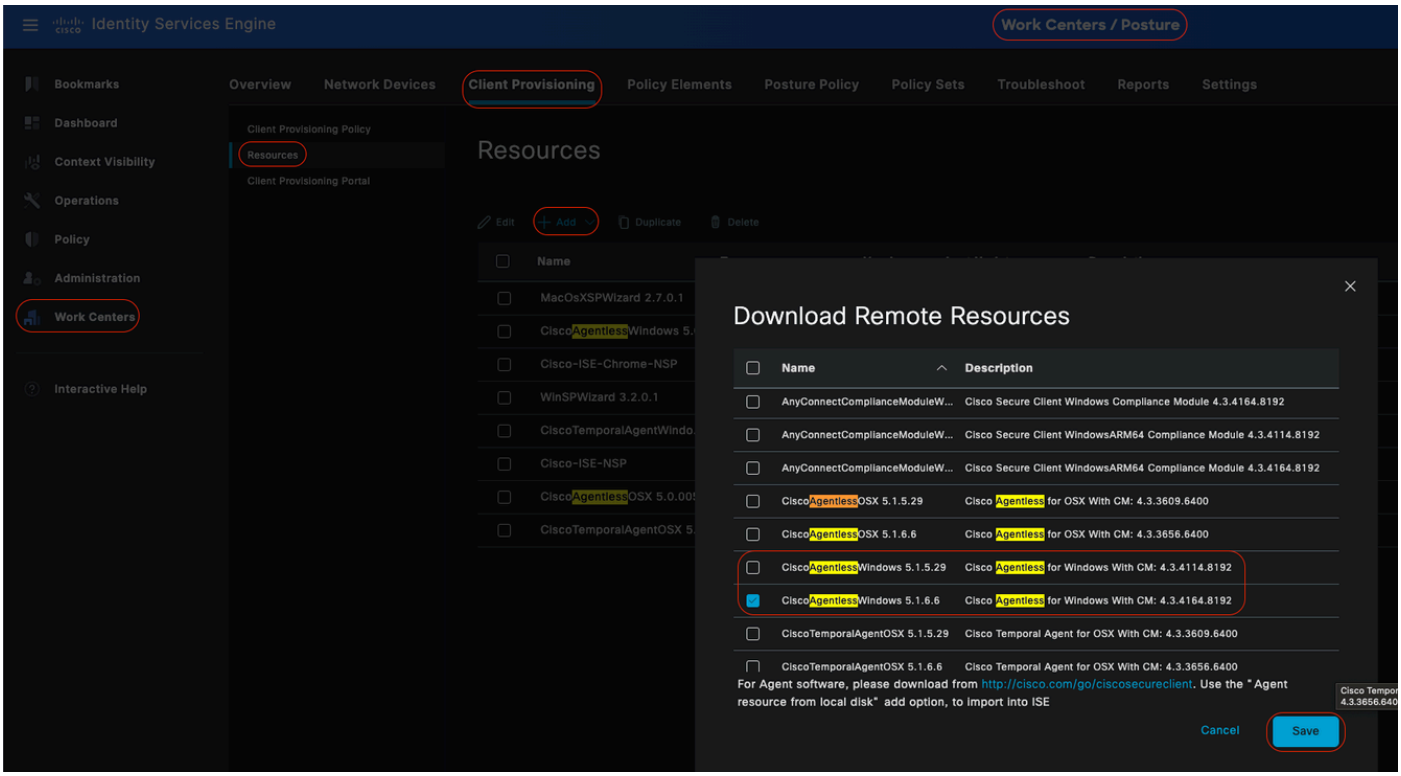
シスコのサイトからのエージェントリソース

Cisco ISE GUIで、メニュー( )をクリックし、Work Centers > **Posture** > **Client Provisioning** > **Resources**の順に選択します。 **Add**をクリックし、**Agent Resources from Cisco site**を選択して、**Save**をクリックします。

シスコのサイトからダウンロードできるのは、コンプライアンスモジュールだけです。ダウンロードする最新の2つのコンプライアンスモジュールが表示されます。この設定例では、リソースパッケージ「**CiscoAgentlessWindows 5.1.6.6**」が選択されています。これは、Windowsデバイス専用です。

.

シスコのサイトからのエー



ジェントリソース

ステップ2：クライアントプロビジョニングポリシーの設定

ポスチャエージェントを設定する場合、2つの異なるリソース(**AnyConnect**またはセキュアクライアントとコンプライアンスモジュール)が必要です。

Agent Configurationの下の両方のリソースを**Agent Posture Profile**とともにマッピングし、この**Agent Configuration**をクライアントプロビジョニングポリシーで使用できるようにします。

ただし、ポスチャエージェントレス(PAgP)を設定する場合は、エージェント設定またはエージェントポスチャプロファイルを設定する必要はなく、シスコサイトのエージェントリソースからエージェントレスパッケージをダウンロードするだけです。

Cisco ISE GUIで、メニュー(

)をクリックし、Work Centers > **Posture** > **Client Provisioning** > **Client Provisioning Policy**の順に選択します。 矢印をクリックして、**Insert new policy above**または**Insert new policy below**、**Duplicate above**または**Duplicate below**を選択します。

- ルール名：**Agentless_Client_Provisioning_Policy**

クライアントプロビジョニングポリシーの名前を指定します。

- オペレーティングシステム：Windows All

これにより、ポリシーがWindowsオペレーティングシステムのすべてのバージョンに適用されます。

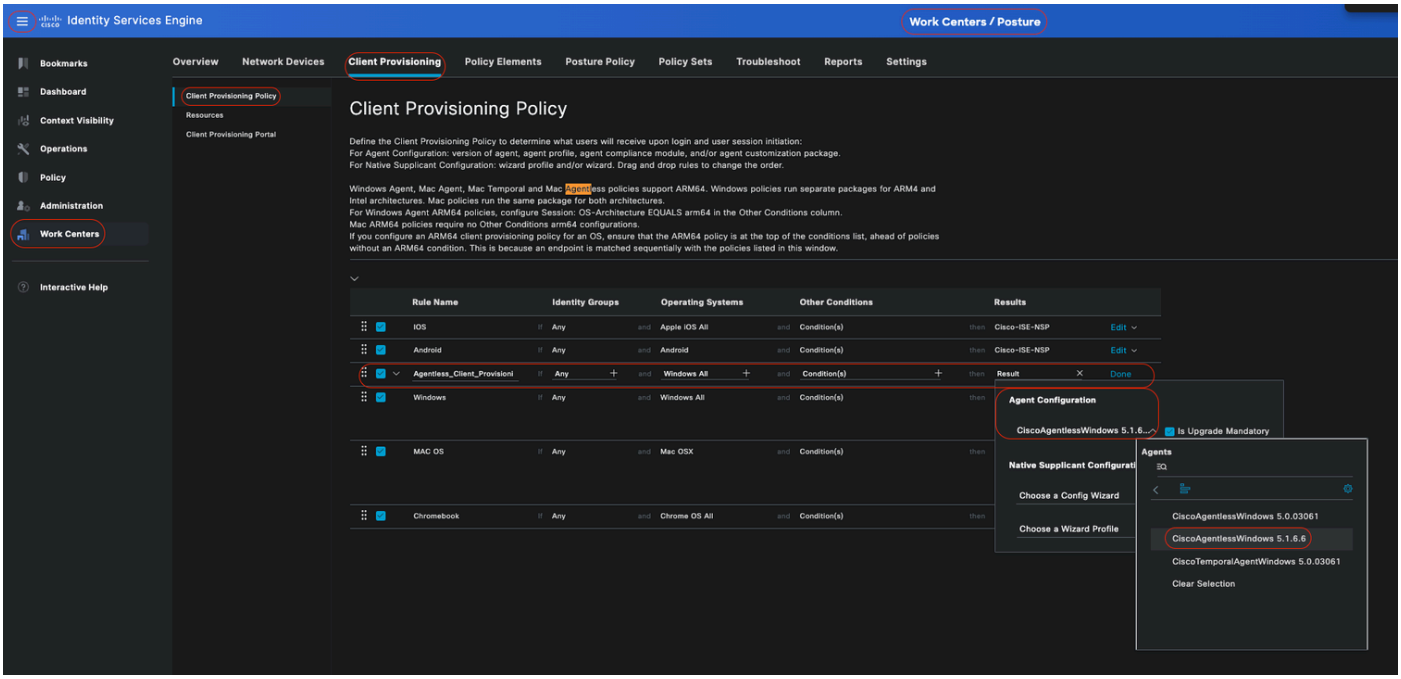
- その他の条件：この例では、特定の条件は設定されていません。ただし、ネットワーク内のすべてのWindowsデバイスではなく、必要なデバイスだけがこのクライアントプロビジョニングポリシーに一致するように条件を設定できます。これは、ネットワークのセグメント化に特に役立ちます。

例： Active Directoryを使用している場合は、ポリシーにActive Directoryグループを組み込んで、影響を受けるデバイスを絞り込むことができます。

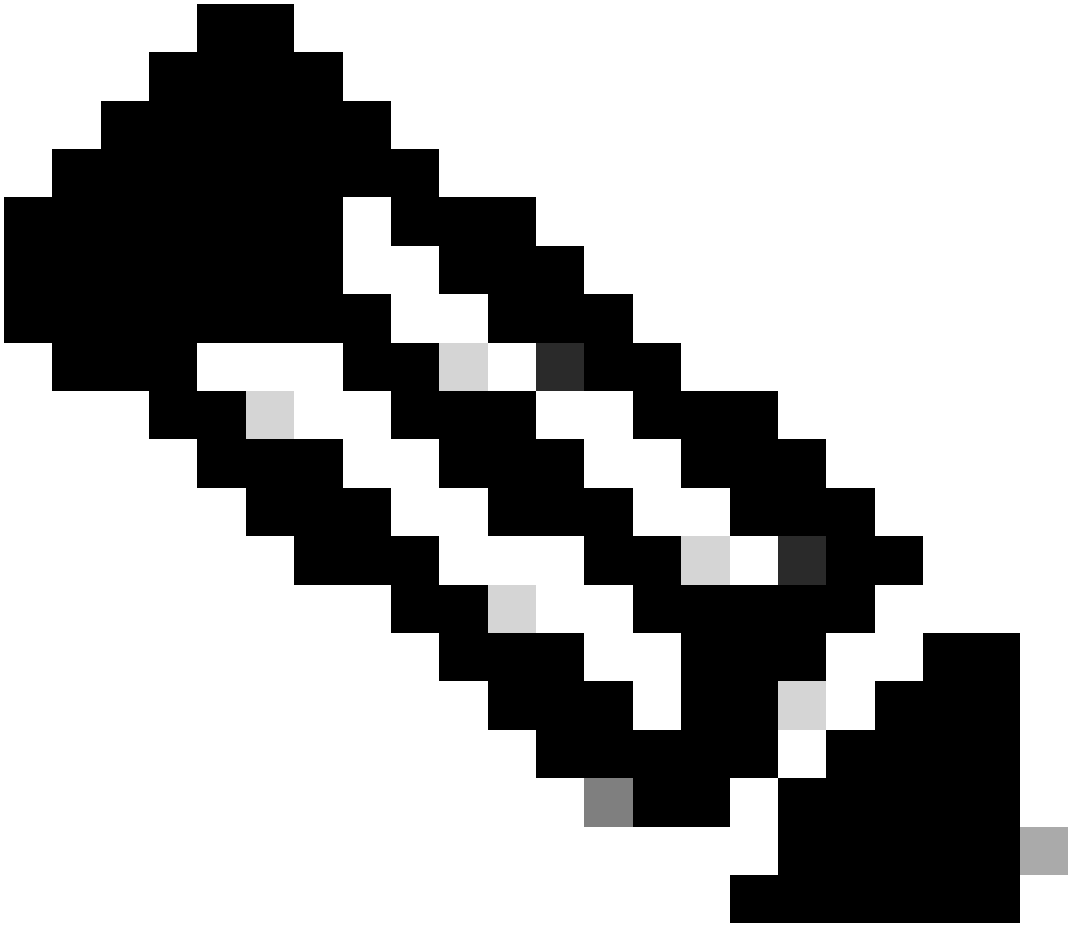
- **結果：**適切なパッケージまたは構成エージェントを選択します。エージェントレス環境を設定するため、事前にシスコのサイトからのエージェントリソースからダウンロードしたパッケージ**CiscoAgentlessWindows 5.1.6.6**を選択します。こ

のエージェントレスパッケージには、ポスチャエージェントレス(PD)の実行に必要なすべてのリソース(エージェントレスソフトウェアおよびコンプライアンスモジュール)が含まれています。

・ Saveをクリックします



エージェントレスクライアントプロビジョニングポリシー



注:1つのクライアントプロビジョニングポリシーのみが任意の認証試行の条件を満たしていることを確認します。複数のポリシーが同時に評価されると、予期しない動作や競合が発生する可能性があります。

エージェントレス認証プロファイル

Cisco ISE GUIで、メニューアイコン(

)をクリックし、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に選択し、エージェントレスポスチャの結果を評価するAuthorization Profileを作成します。

- この設定例では、認可プロファイルに**Agentless_Authorization_Profile**という名前を付けます。

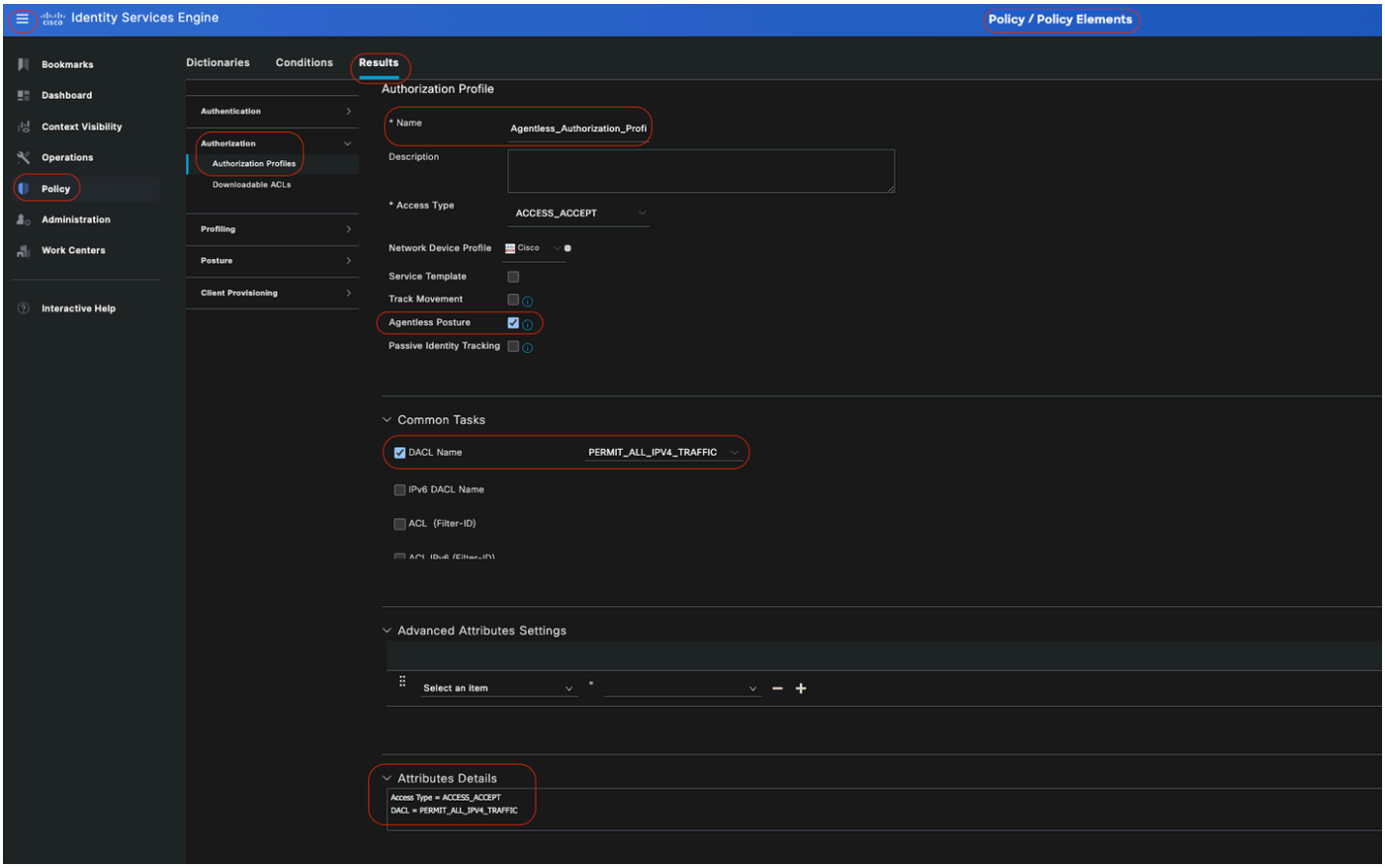
- 認可プロファイルでエージェントレスポスチャを有効にします。

- このプロファイルは、エージェントレスポスチャに対してのみ使用します。他のポスチャタイプにも使用しないでください。

- エージェントレスポスチャでは、CWAおよびリダイレクトACLは必要ありません。セグメンテーションルールの一部として、VLAN、DACL、またはACLを使用できます。 シンプルにするために、この設定例のエージェントレスポスチャチェックの他に、dACL（すべてのipv4トラフィックを許可）だけを設定します。

-

[Save] をクリックします。



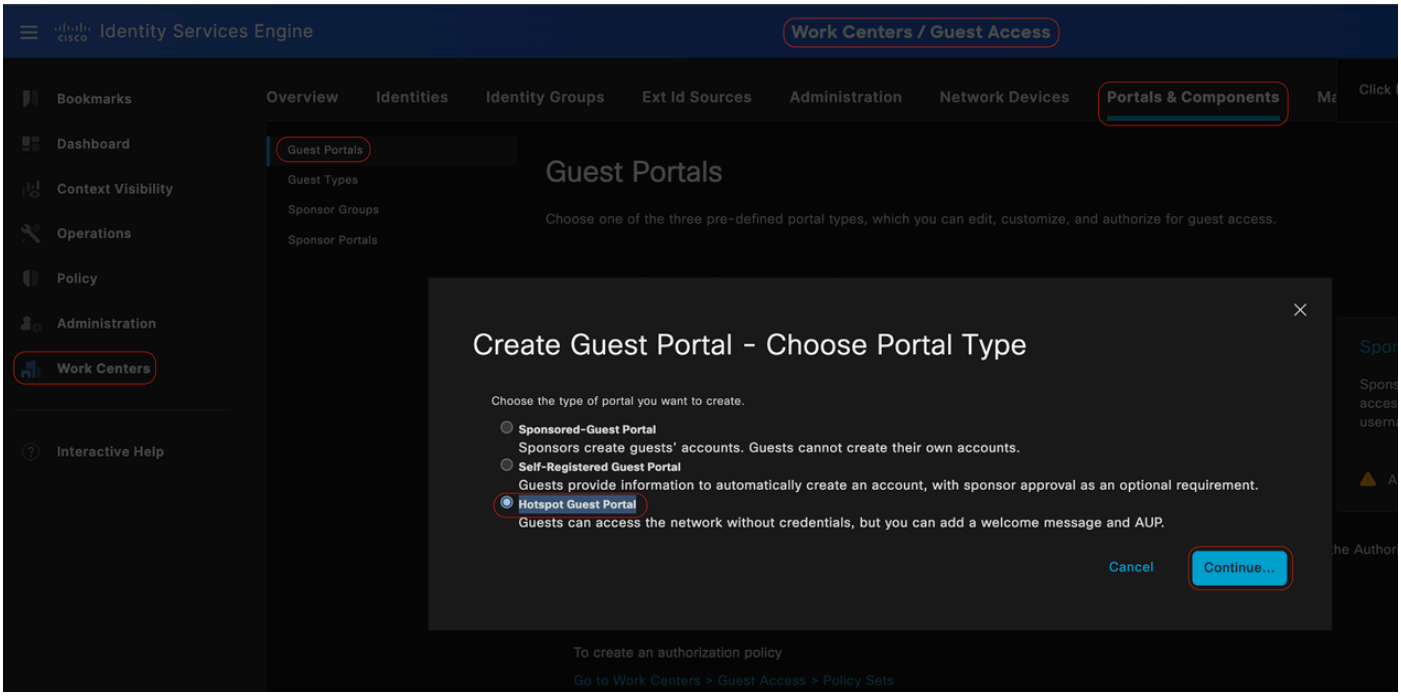
エージェントレス認証プロファイル

修復を使用する代替手段 (オプション)

エージェントレスフローでの修復のサポートは利用できません。この問題に対処するには、カスタマイズされたホットスポットポータルを実装して、エンドポイントのコンプライアンスに関するユーザ認識を強化します。エンドポイントが非準拠と識別されると、ユーザはこのポータルにリダイレクトされます。このアプローチにより、ユーザはエンドポイントのコンプライアンスステータスを知らされ、問題を修正するための適切なアクションを実行できます。

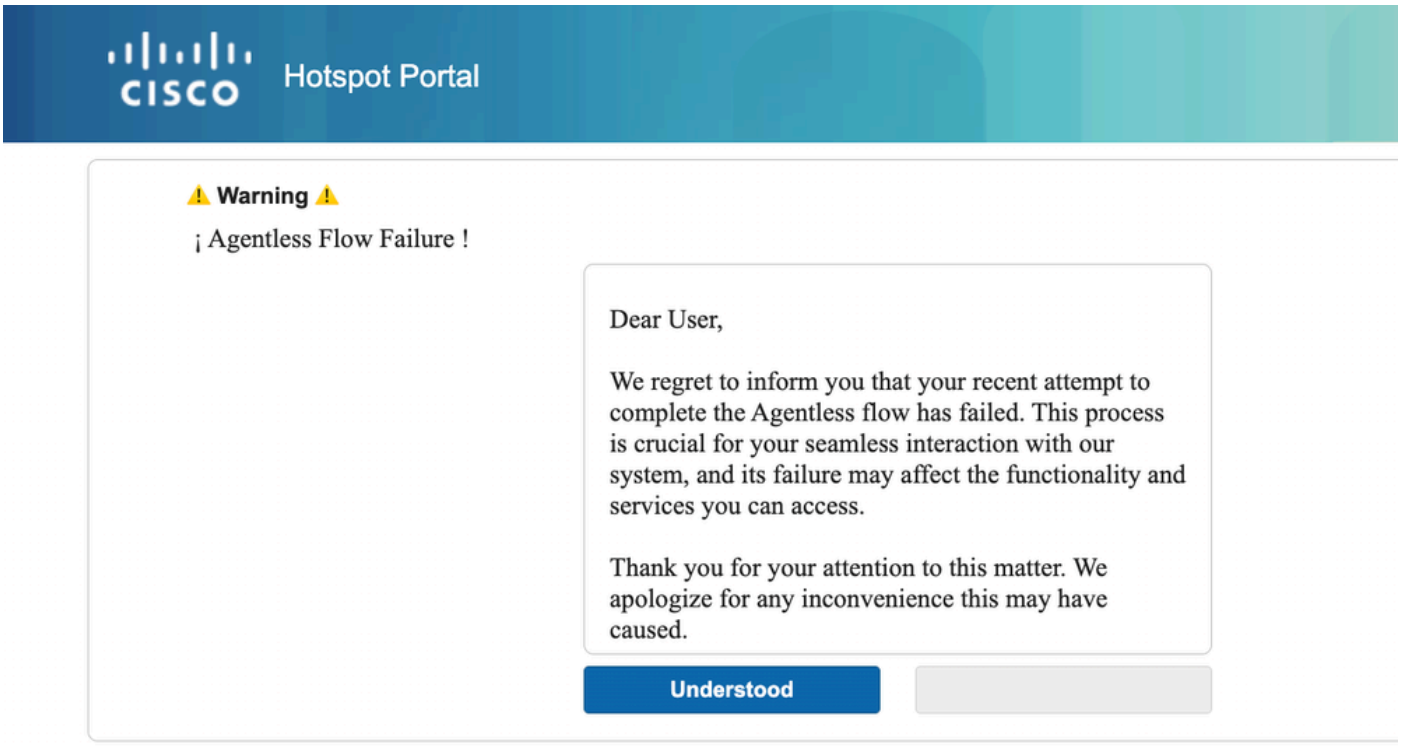
Cisco ISE GUIで、メニュー(

)をクリックし、Work Centers > Guest Access > Portals & Components > Guest Portalsの順に選択します。 **Create** > **Select Hotspot Guest Portal** > **Continue:**の順にクリックします。この設定例では、ホットスポットポータルは**Agentless_Warning**という名前になっています。



ホットスポットゲストポータル

ポータル設定では、特定の要件に合わせてエンドユーザに表示されるメッセージをカスタマイズできます。これは、カスタマイズされたポータルビューの例です。



失敗したポスチャエージェントレス

修復許可プロファイル（オプション）

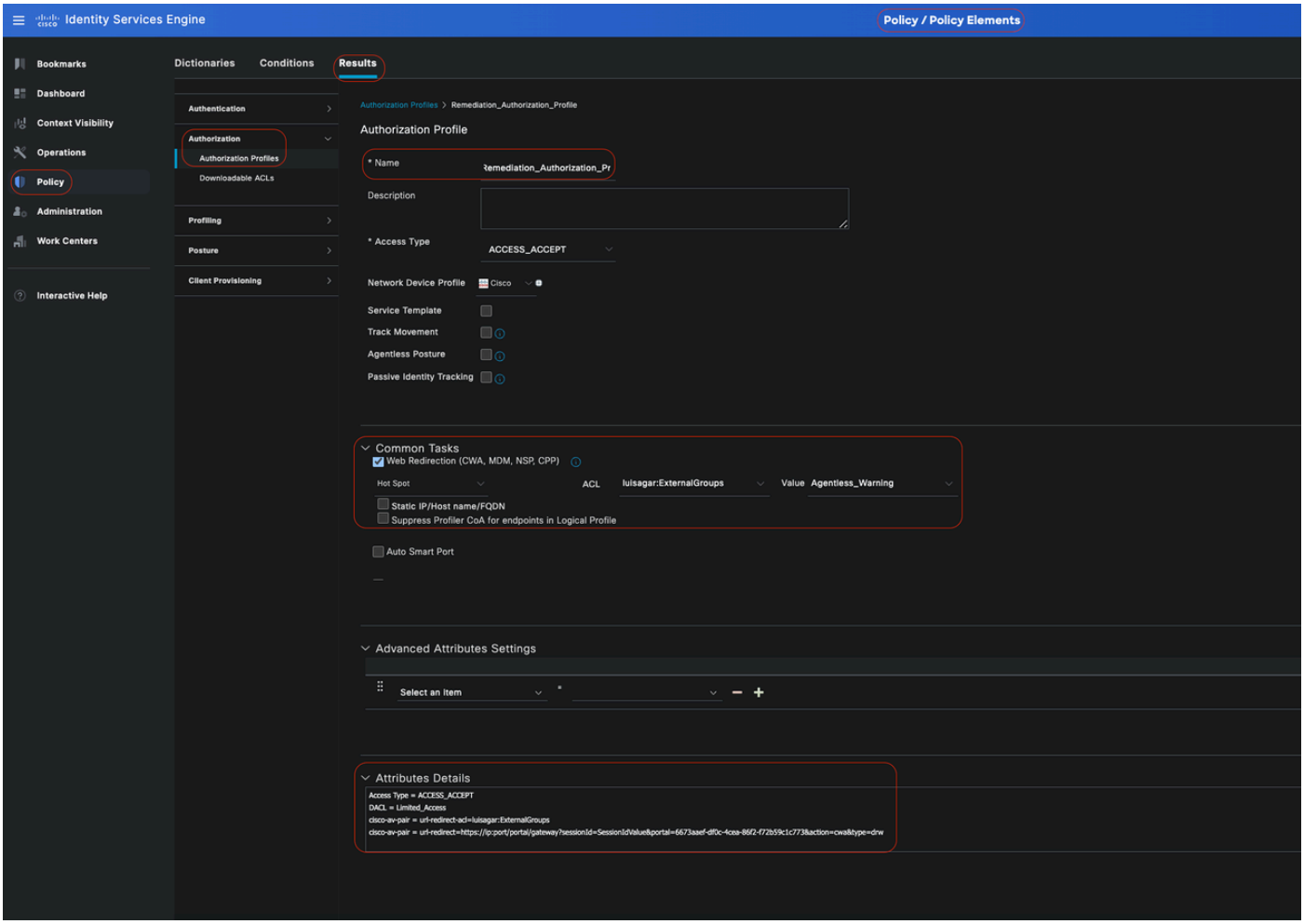
Cisco ISE GUIで、メニューアイコン( )をクリックし、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に選択し、修復用のAuthorization Profileを作成します。

- この設定例では、認可プロファイルに**Remediation_Authorization_Profile**という名前を付けます。

- 簡単にするために、この設定例には、**Limited_Access**という名前のダウンロード可能アクセスコントロールリスト(dACL)だけが含まれています。このリストでは、組織の特定のニーズに合わせて調整された制限付きアクセスが許可されます。

- 外部グループとホットスポットを含む**Web**リダイレクション機能が設定されているため、エンドポイントのコンプライアンスに関するユーザの認識が向上します。

- [Save] をクリックします。

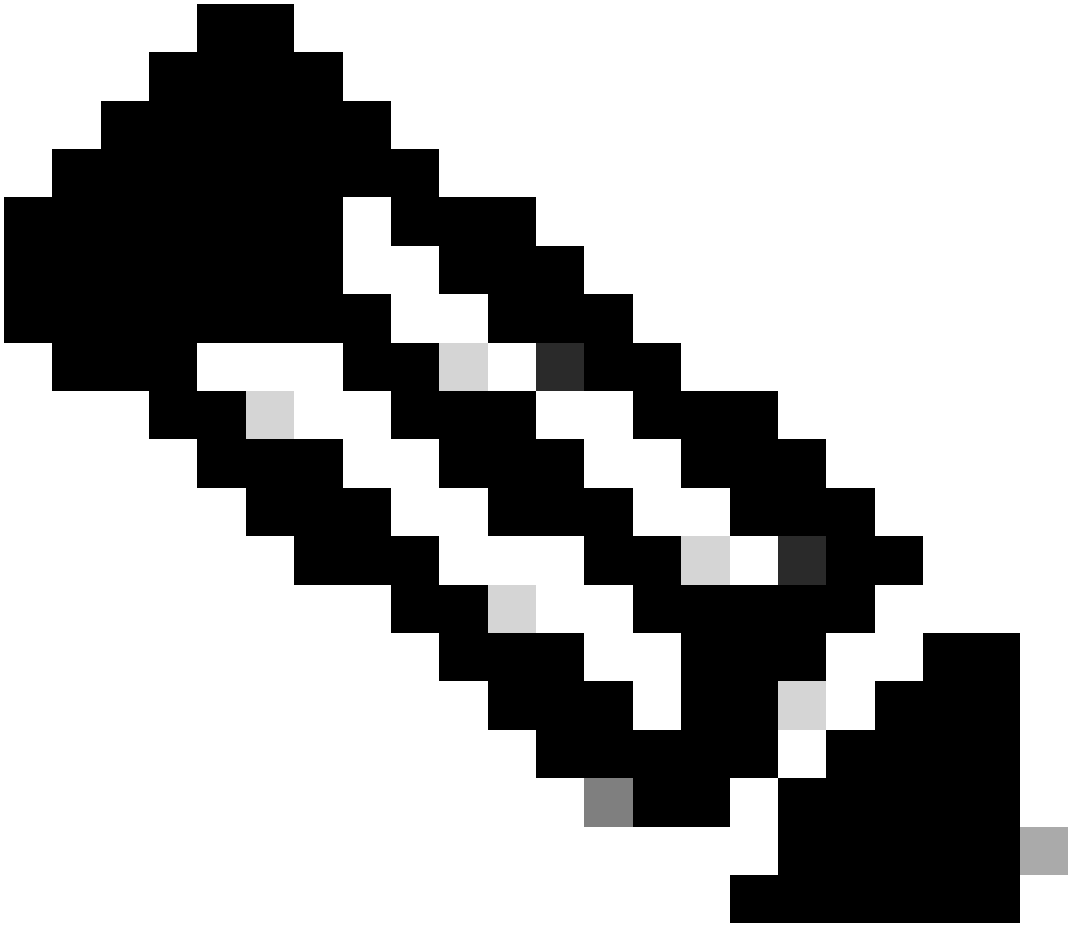


修復承認規則

エージェントレス認証ルール

Cisco ISE GUIで、メニュー(

)をクリックし、Policy > PolicySetの順に選択し、Authorization Policyを展開します。次の3つの認可ポリシーをイネーブルにして設定します。



注：ポスチャフローが正しく動作するためには、これらの許可ルールを指定の順序で設定する必要があります。

Unknown_Compliance_Redirect:

•条件：

結果をエージェントレスポスチャに設定して、Network_Access_Authentication_PassedとCompliance_Unknown_Devicesを設定します。この状態が発生すると、エージェントレスフローが開始されます。

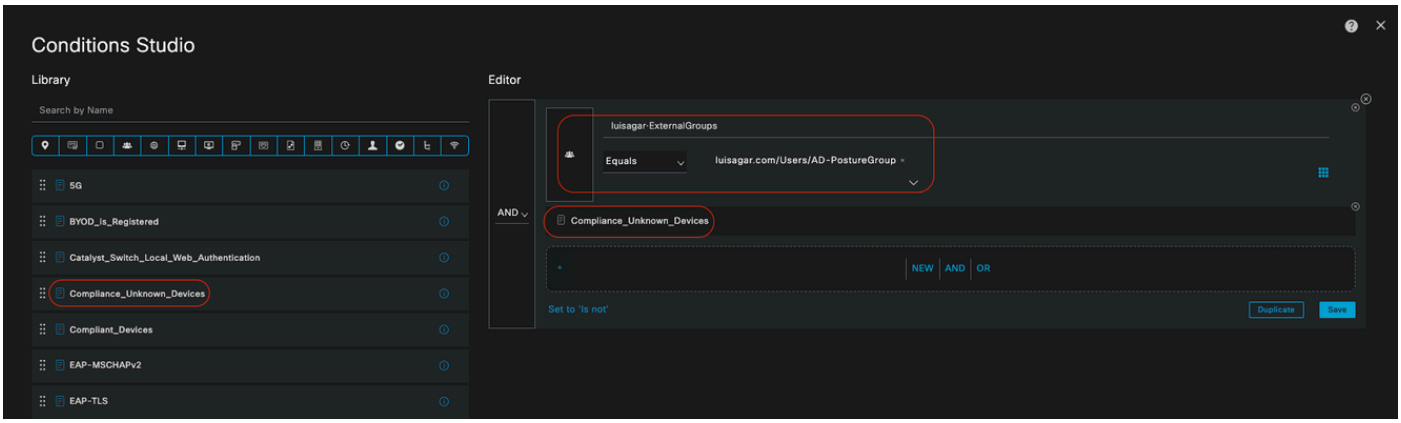
・条件例：

トラフィックをセグメント化するためのActive Directory(AD)グループ条件を設定します。

初期ポスチャ状態が不明なため、**Compliance_Unknown_Devices**条件を設定する必要があります。

•許可プロファイル：

デバイスがエージェントレスポスチャフローを通過できるようにするには、この許可ルールに**Agentless_Authorization_Profile**を割り当てます。 この状態にはエージェントレスフローが含まれるため、このプロファイルに一致するデバイスはエージェントレスフローを開始できます。



不明な許可ルール

NonCompliant_Devices_Redirect:

・ 条件：結果をDenyAccessに設定して、Network_Access_Authentication_PassedおよびNon_Compliant_Devicesを設定します。別の方法として、この例に示すように修復オプションを使用することもできます。

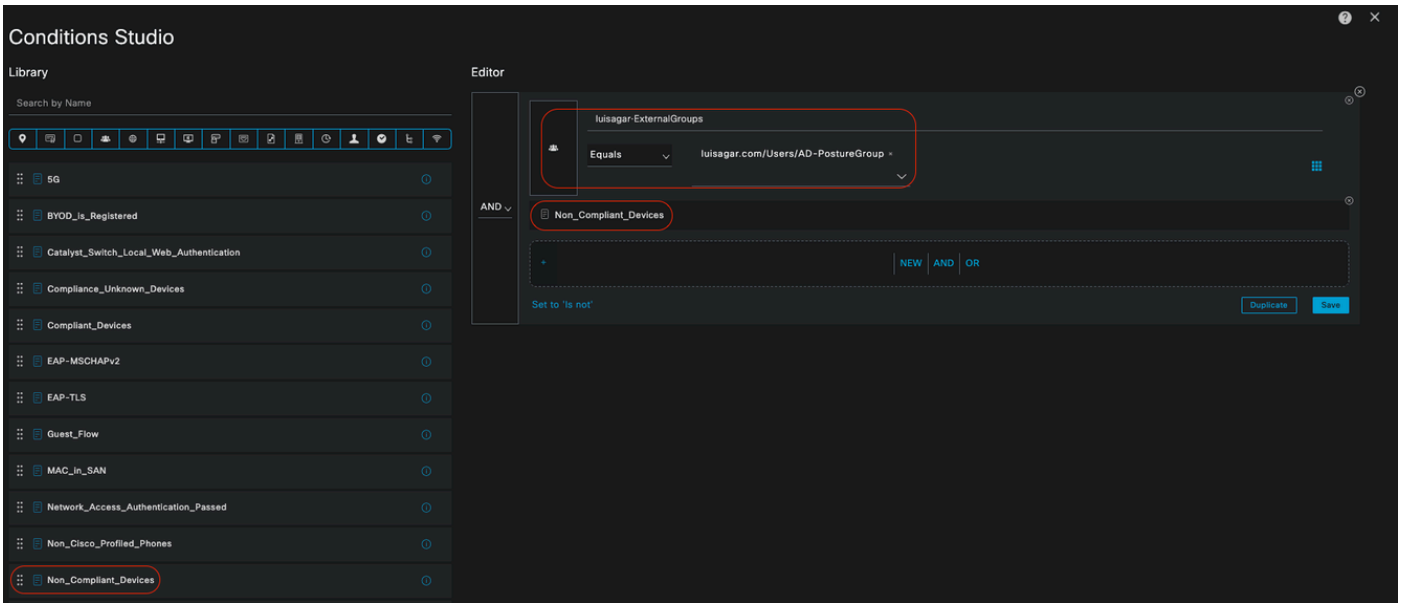
・ 条件例：

トラフィックをセグメント化するためのADグループ条件を設定します。

Compliance_Unknown_Devices条件は、ポスチャ状態が非準拠の場合に限られたリソースを割り当てるように設定する必要があります。

•許可プロファイル：

この認可ルールに**Remediation_Authorization_Profile**を割り当てて、ホットスポットポータルを介して非準拠デバイスに現在のステータスを通知するか、アクセスの**拒否**を実行します。



非準拠の許可ルール

Compliant_Devices_Access:

•条件：

Network_Access_Authentication_PassedとCompliant_Devicesを設定し、結果セットをPermitAccessに設定します。

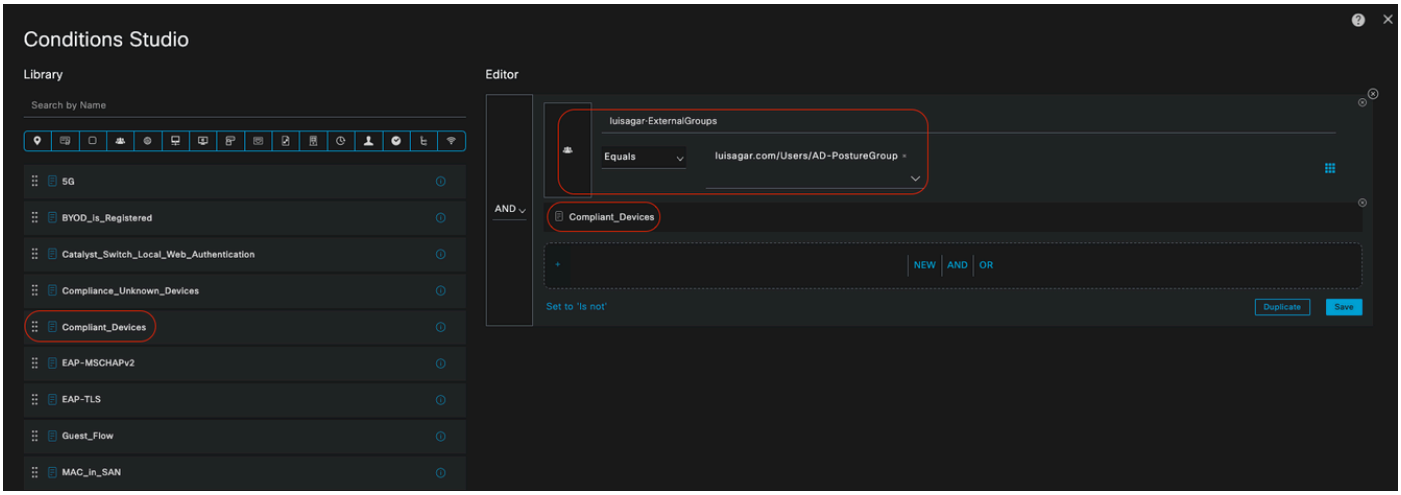
・ 条件例：

トラフィックをセグメント化するためのADグループ条件を設定します。

Compliance_Unknown_Devices条件は、準拠するデバイスが適切なアクセスを許可されるように設定する必要があります。

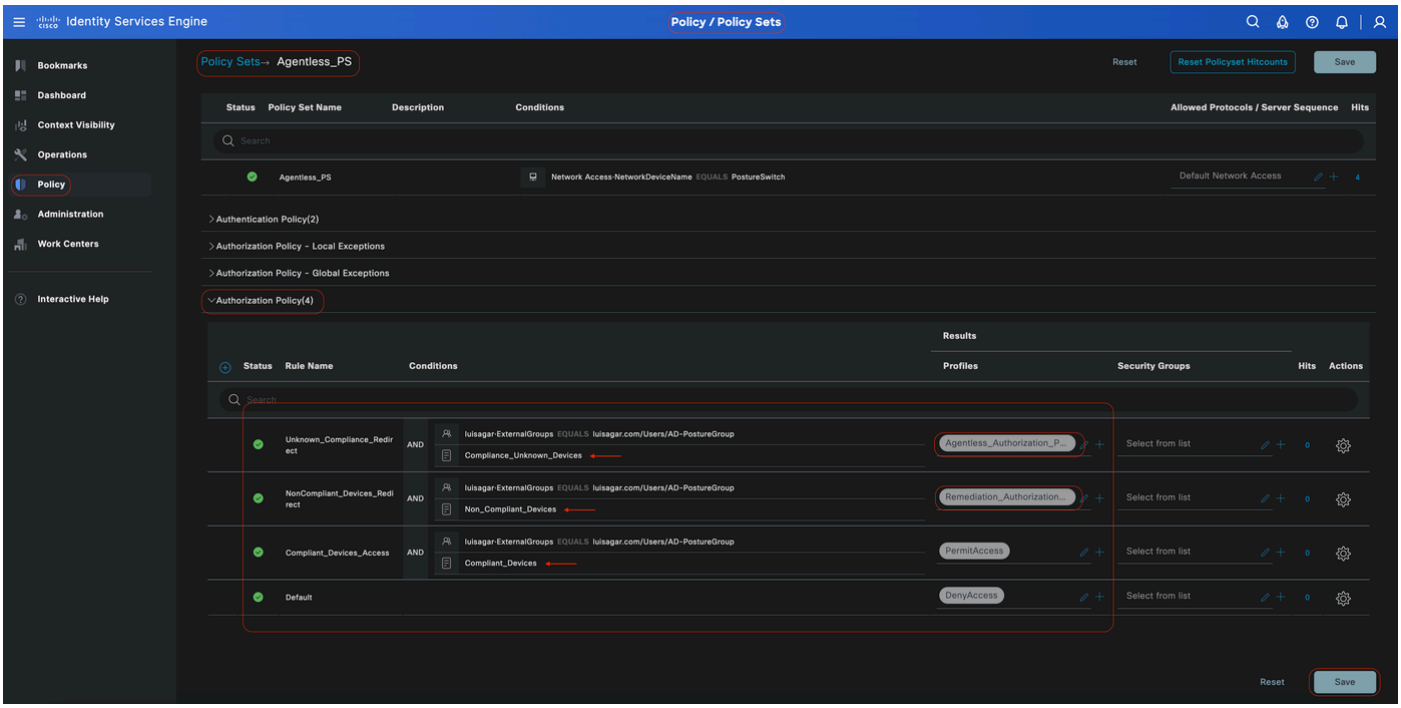
•許可プロファイル：

この許可ルールに**PermitAccess**を割り当てて、準拠するデバイスがアクセスできるようにします。このプロファイルは、組織のニーズに合わせてカスタマイズできます。



準拠する許可ルール

すべての許可ルール



認可ルール

エンドポイントログインクレデンシャルの設定

Cisco ISE GUIで、メニュー( )をクリックし、Administration > Settings > Endpoint Scripts > Login Configurationの順に選択し、クライアントにログオンするためのクライアントのクレデンシャルを設定します。

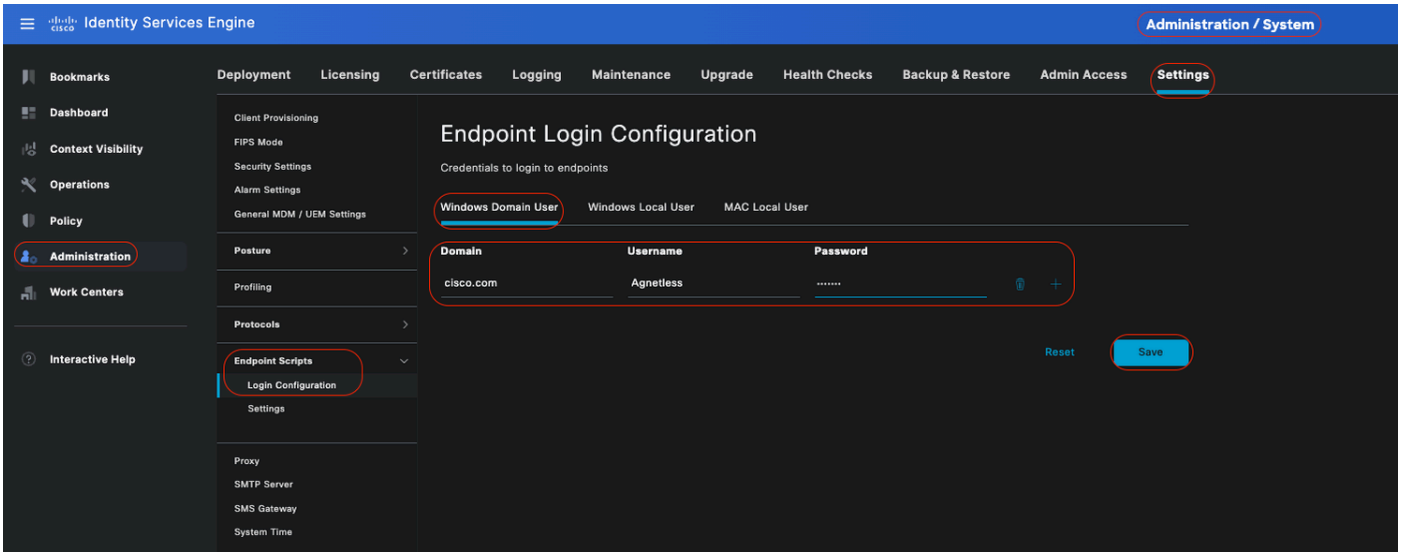
エンドポイントスクリプトによってこれと同じクレデンシャルが使用されるため、Cisco ISEはクライアントにログインできます。

Windowsデバイスの場合、最初の2つのタブ(**Windows Domain User**と**Windows Local User**

- **Windows**ドメインユーザ**:**

Cisco ISEがSSH経由でクライアントにログインするために使用する必要があるドメインクレデンシャルを設定します。プラスアイコンをクリックし、必要な数のWindowsログインを入力します。各ドメインのDomain、Username、およびPasswordfieldsに必要な値を入力します。ドメインクレデンシャルを設定する場合、Windowsのローカルユーザタブで設定されたローカルユーザのクレデンシャルは無視されます。

Active Directoryドメインを介してエージェントレスポスチャ評価を利用するWindowsエンドポイントを管理している場合は、ローカル管理者権限を持つクレデンシャルとともにドメイン名を指定してください。

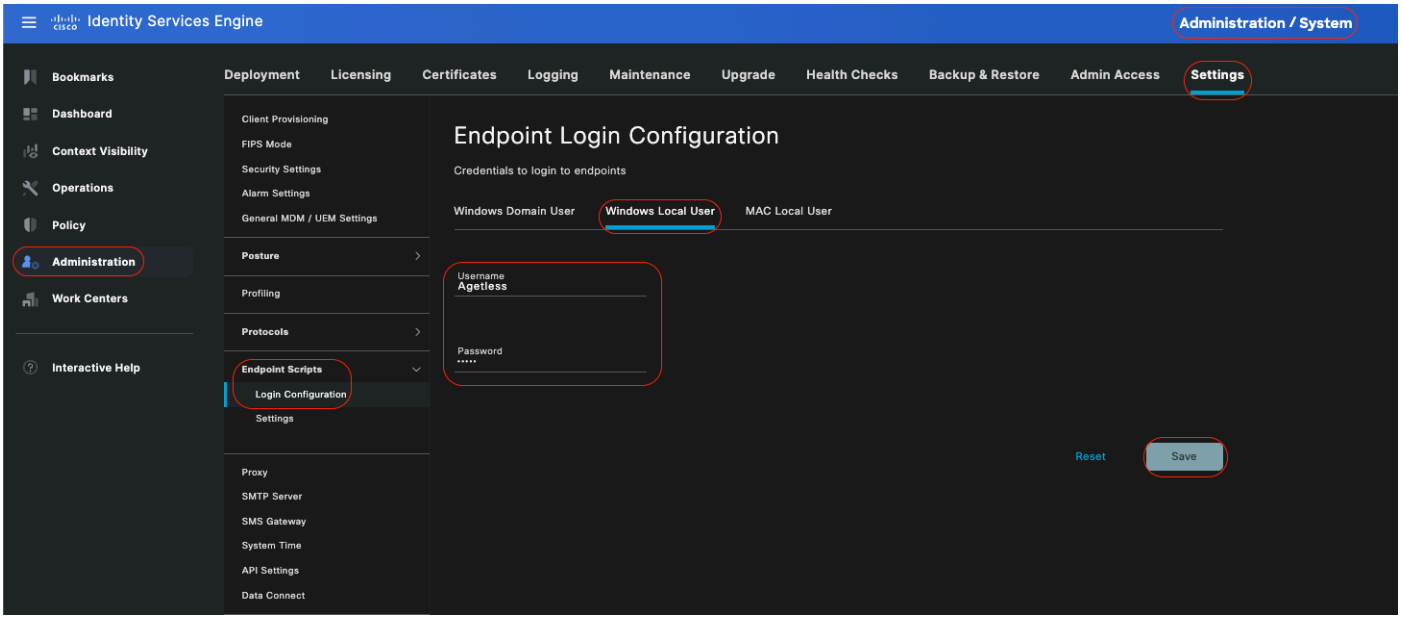


*Windows*ドメインユーザ

- **Windows**ローカルユーザ**:**

Cisco ISEがSSH経由でクライアントにアクセスするために使用するローカルアカウントを設定します。ローカルアカウントは、PowershellおよびPowershellリモートを実行できる必要があります。

Active Directoryドメイン経由でエージェントレスポスチャ評価を利用するWindowsエンドポイントを管理していない場合、ローカル管理者権限を持つクレデンシャルを提供してください。

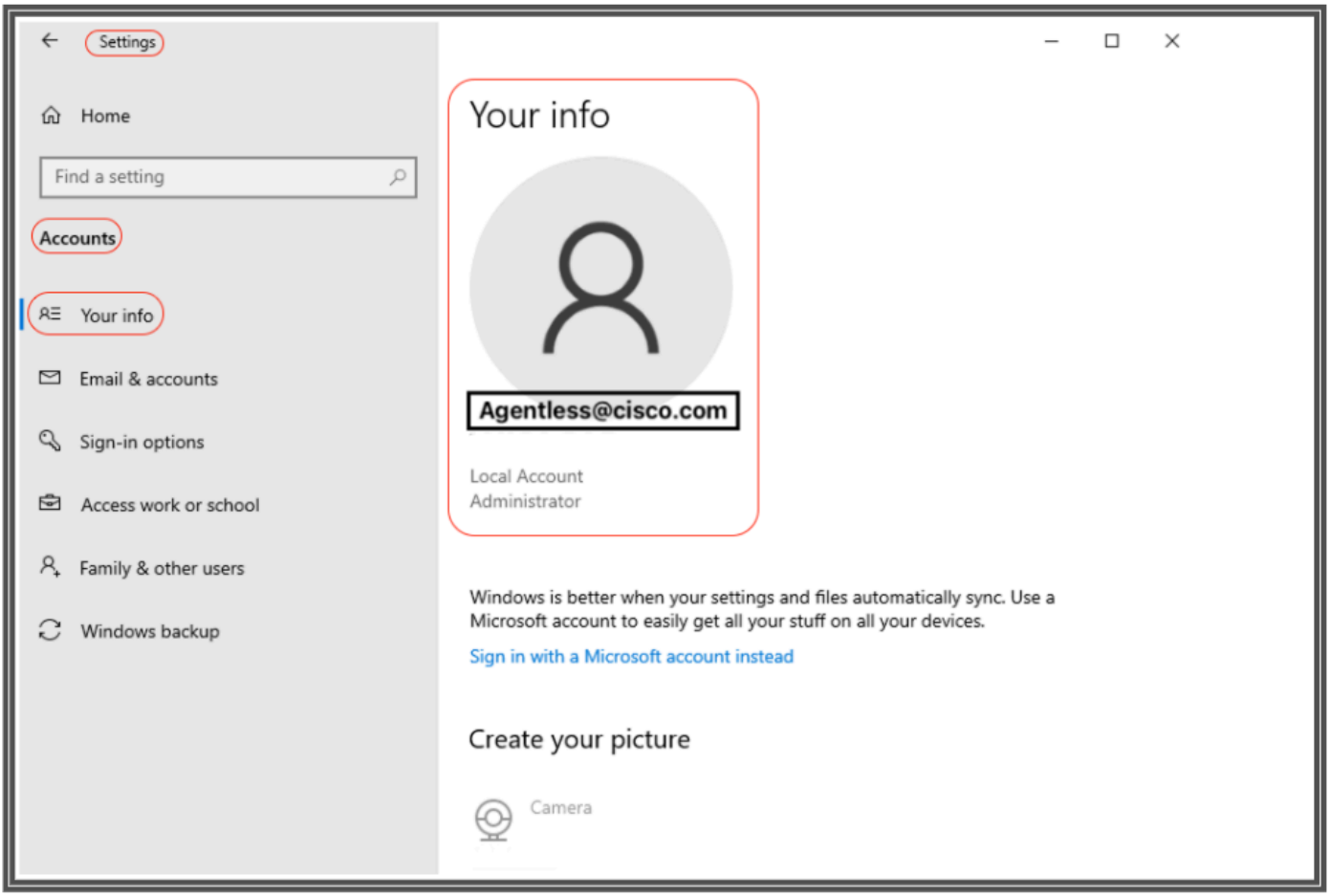


*Windows*ローカルユーザ

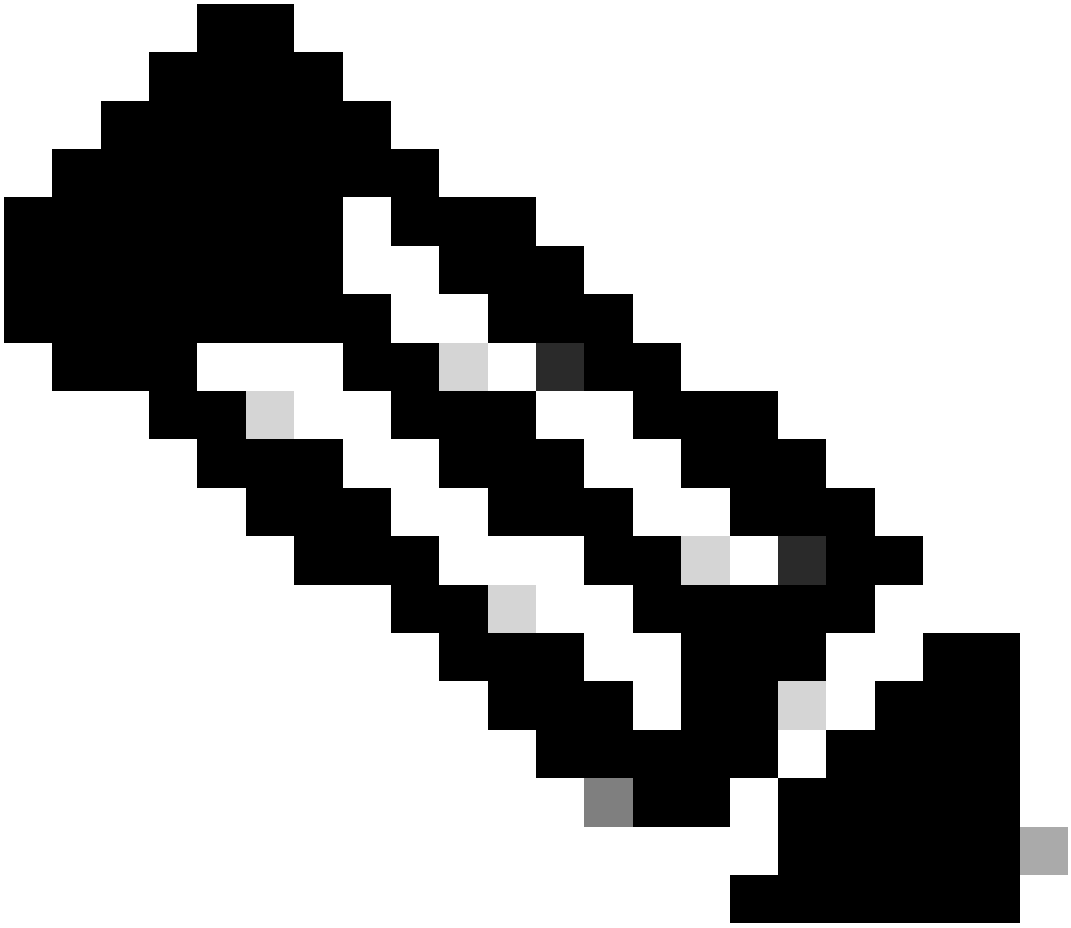
アカウントの確認

Endpoint Login Credentialsの下に適切なデータを正確に追加できるように、Windowsドメインユーザと Windowsローカルユーザアカウントを確認するには、次の手順を使用します。

Windowsローカルユーザ：GUIの使用（設定アプリケーション）:「**WindowsStart**」ボタンをクリックし、「**Settings**」（歯車のアイコン）を選択します。次に、「**Accounts**」をクリックし、「**Your info**」を選択します。


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

アカウントの確認



注:MacOSの場合は、「**MAC**ローカルユーザ」を参照できます。この設定例では、MacOSの設定は表示されません。

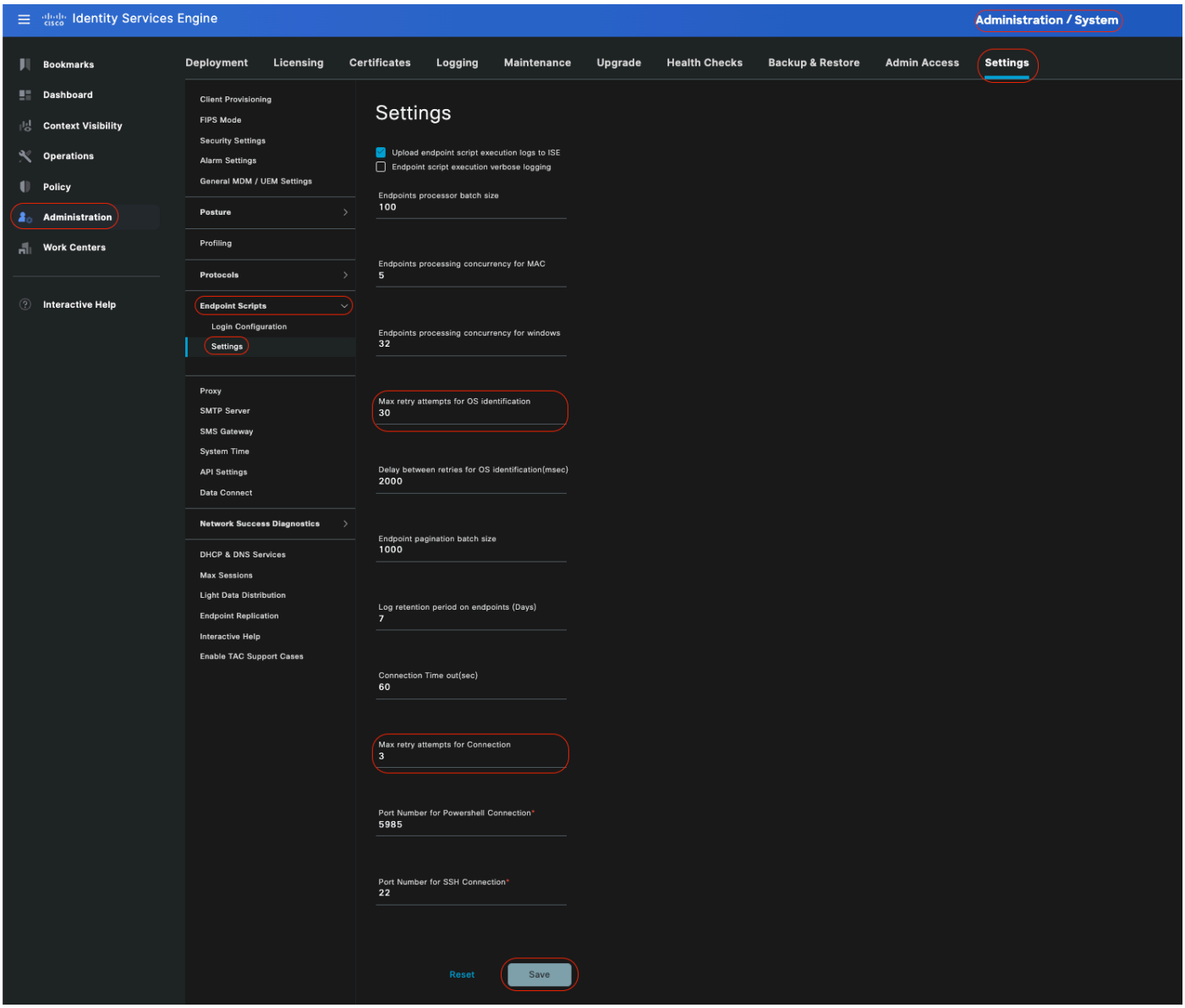
- **MAC**ローカルユーザ**:**Cisco ISEがSSH経由でクライアントにアクセスするために使用するローカルアカウントを設定します。ローカルアカウントは、PowershellおよびPowershellリモートを実行できる必要があります。Usernamefieldで、ローカルアカウントのアカウント名を入力します。

Mac OSアカウント名を表示するには、端末で次のコマンドwhoamiを実行します。

Settings

Cisco ISE GUIで、メニュー()をクリックし、**Administration** > Settings > **Endpoint Scripts** > Settingsの順に選択し、OSの識別のための最大再試行回数、**OSの識別のための再試行間隔**などを設定します。これらの設定により、接続の問題をどれだけ迅速に確認できるかが決まります。たとえば、PowerShellポートが開いていないことを示すエラーは、すべての再試行が完了していない場合にのみログに表示されます。

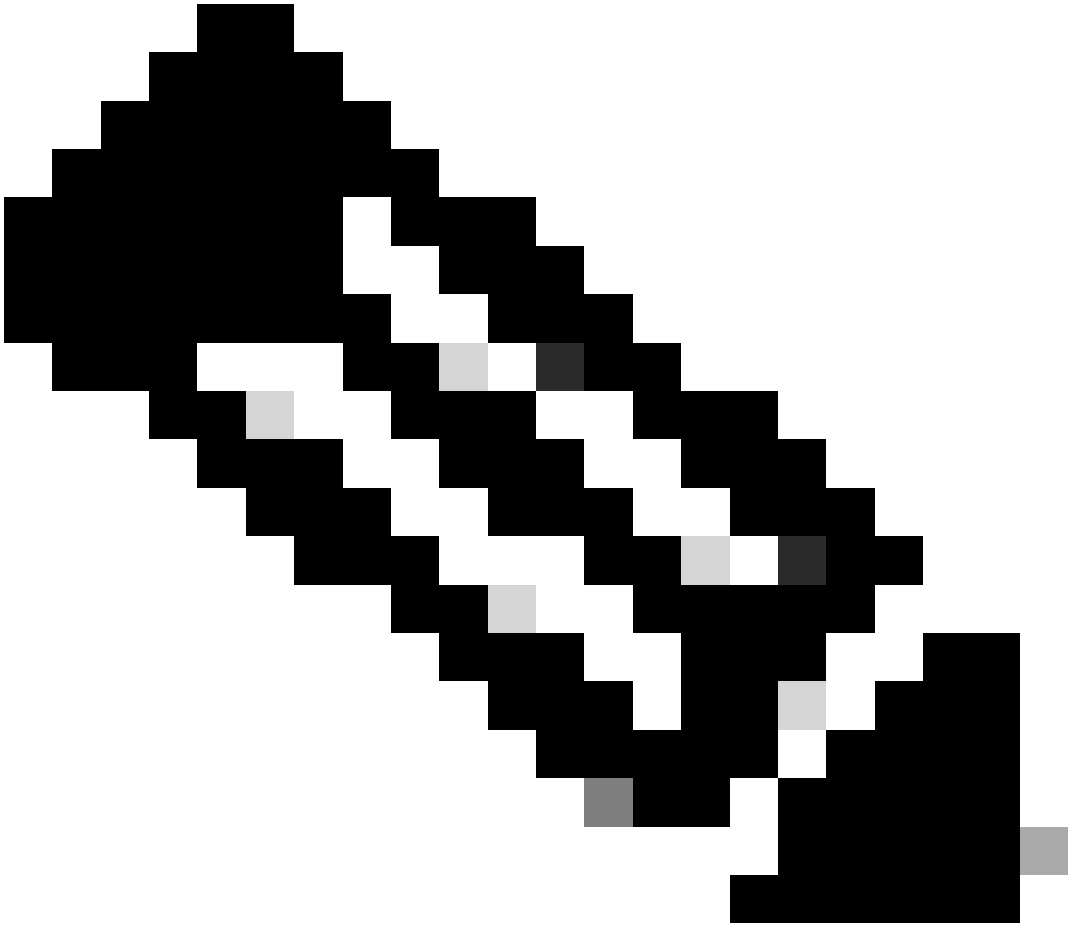
次のスクリーンショットは、デフォルト値の設定を示しています。



エンドポイントスクリプトの設定

クライアントがエージェントレスポスチャで接続すると、ライブログで確認できます。

Windowsエンドポイントの設定とトラブルシューティング



注：これらは、お使いのWindowsデバイスにチェックして適用するための推奨事項です。ただし、ユーザー権限やPowerShellアクセスなどの問題が発生した場合は、Microsoftのドキュメントを参照するか、Microsoftサポートに問い合わせる必要があります。

前提条件の確認とトラブルシューティング

ポート5985へのTCP接続のテスト

Windowsクライアントの場合、クライアントのPowerShellにアクセスするためのポート5985を開く必要があります。次のコマンドを実行して、ポート5985へのTCP接続を確認します。 **Test-NetConnection -ComputerName localhost -Port 5985**

このスクリーンショットに示されている出力は、localhostのポート5985へのTCP接続が失敗したことを示しています。これは、ポ

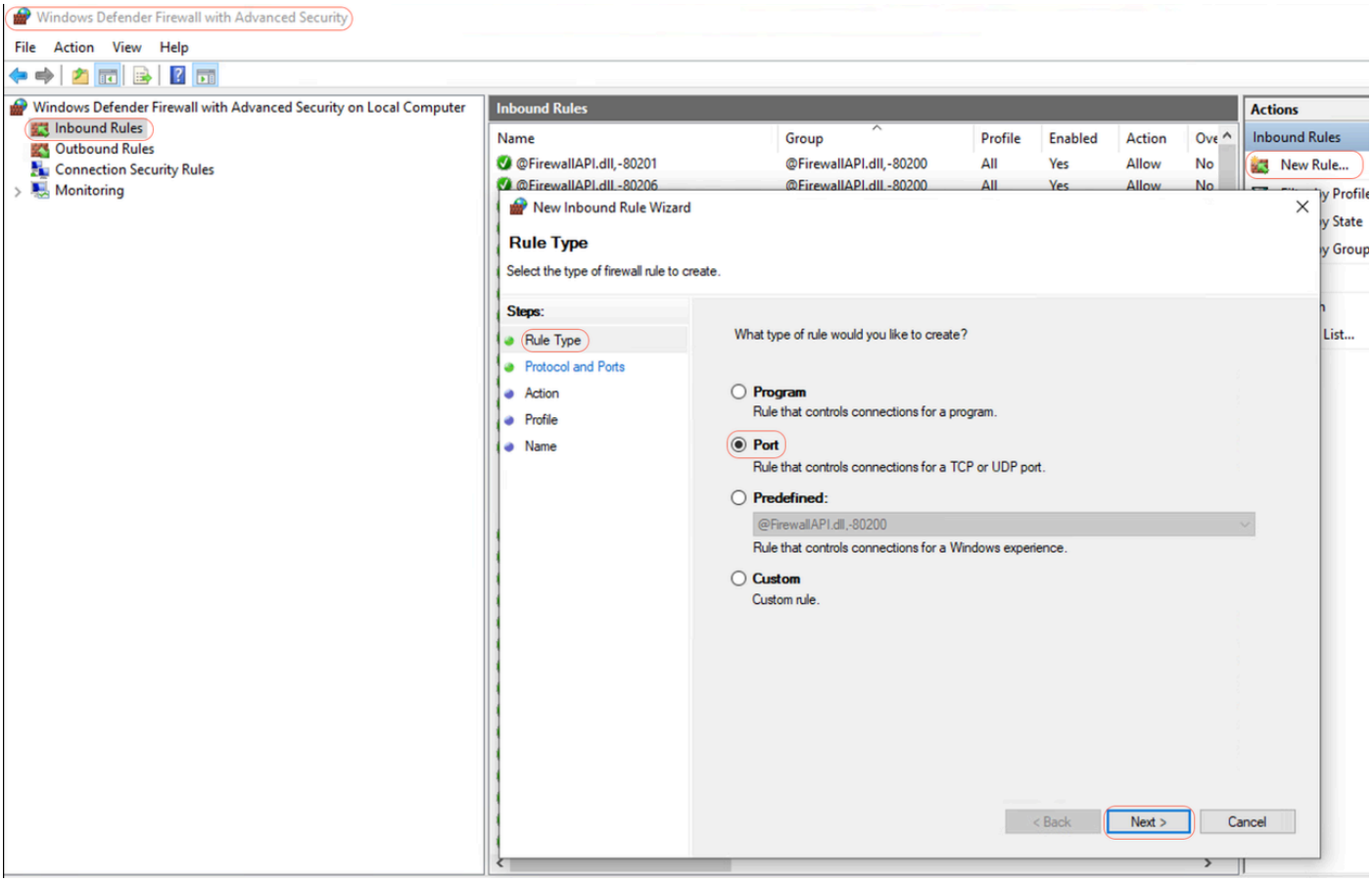
ート5985を使用するWinRM（Windowsリモート管理）サービスが実行されていないか、正しく構成されていないことを意味します。

```
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

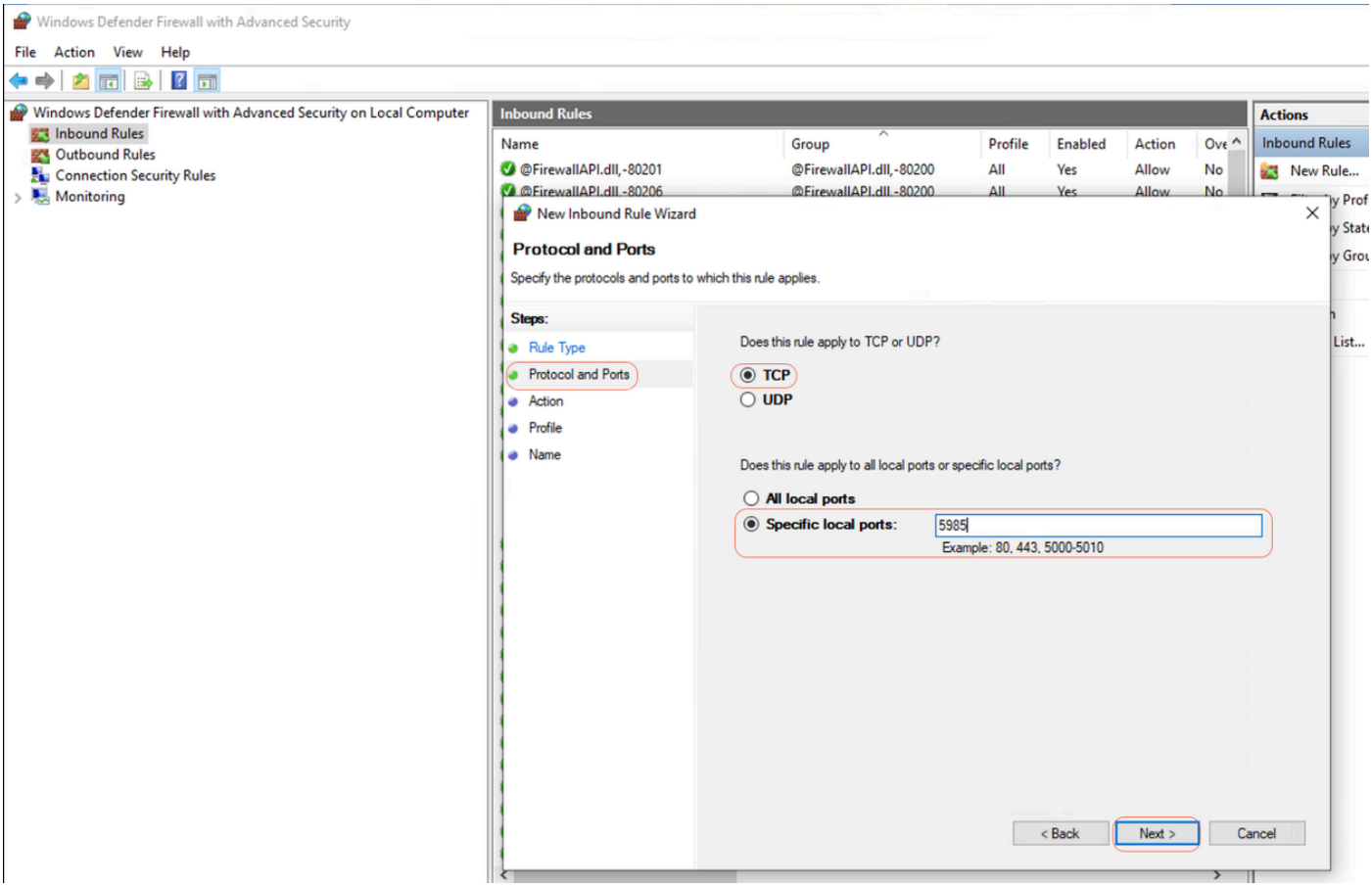
ポート5985でPowerShellを許可する受信規則を作成しています

ステップ1:Windows GUIで、検索バーに移動し、**Windows Firewall with Advanced Security**と入力してクリックし、**Run as administrator > Inbound Rules > New Rule > Rule Type > Port > Next**の順に選択します。



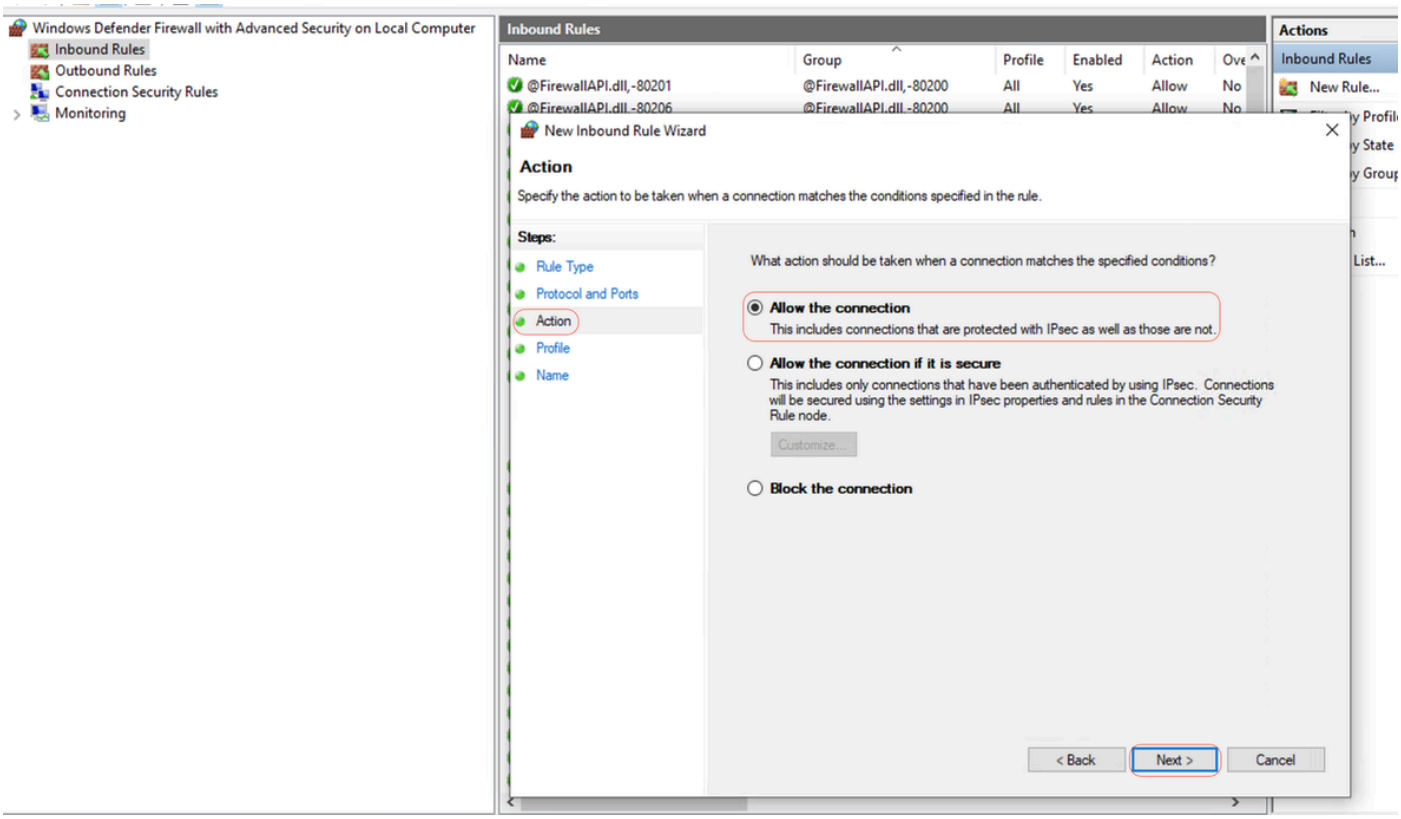
新しい受信の規則 – ポート

ステップ2- **Protocols and Portsで、TCP and Specify local portsを選択し、ポート番号5985(PowerShellリモート処理用のデフォルトポート)を入力して、Nextをクリックします。**



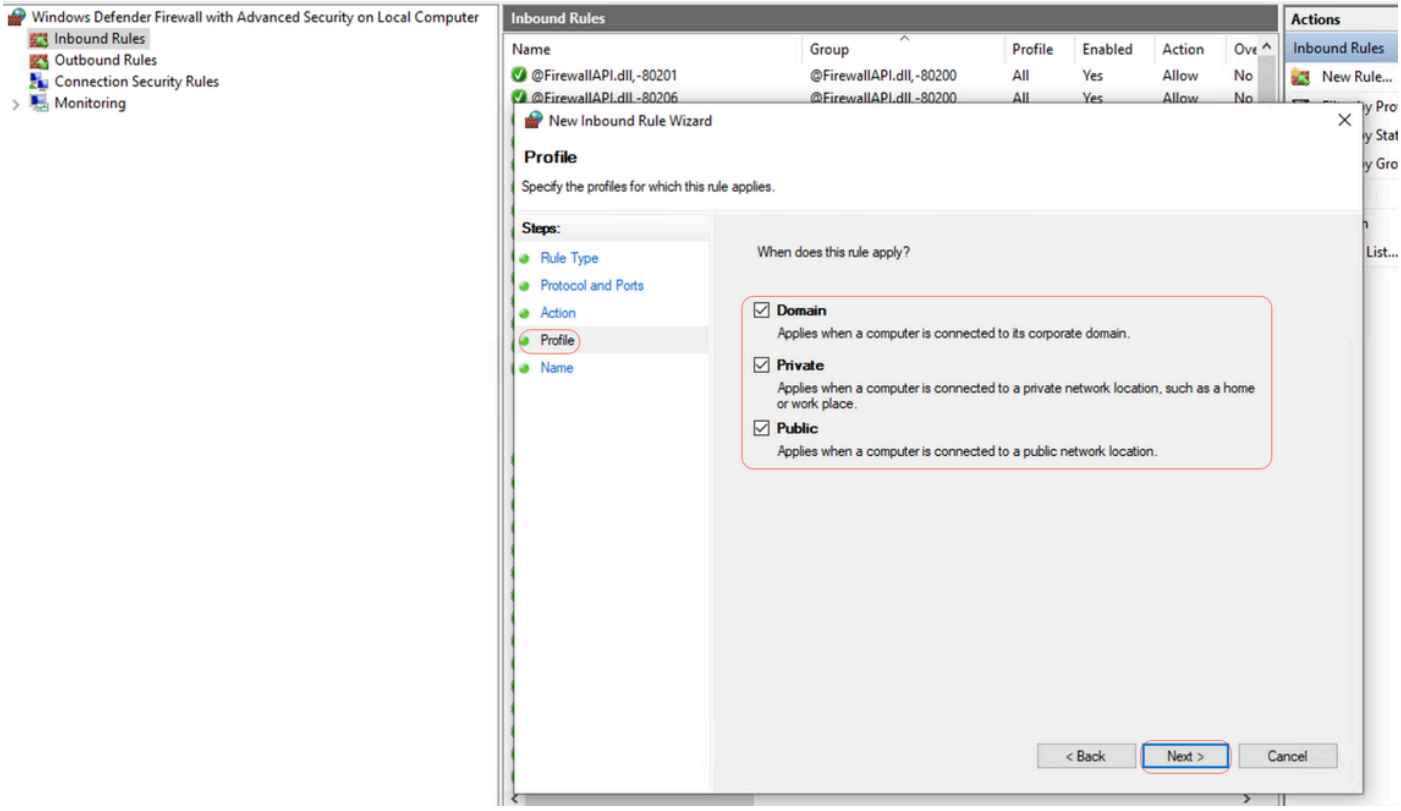
プロトコルとポート

ステップ3: Actionの**下で、Allow the connection** > **Next**の順に選択します。



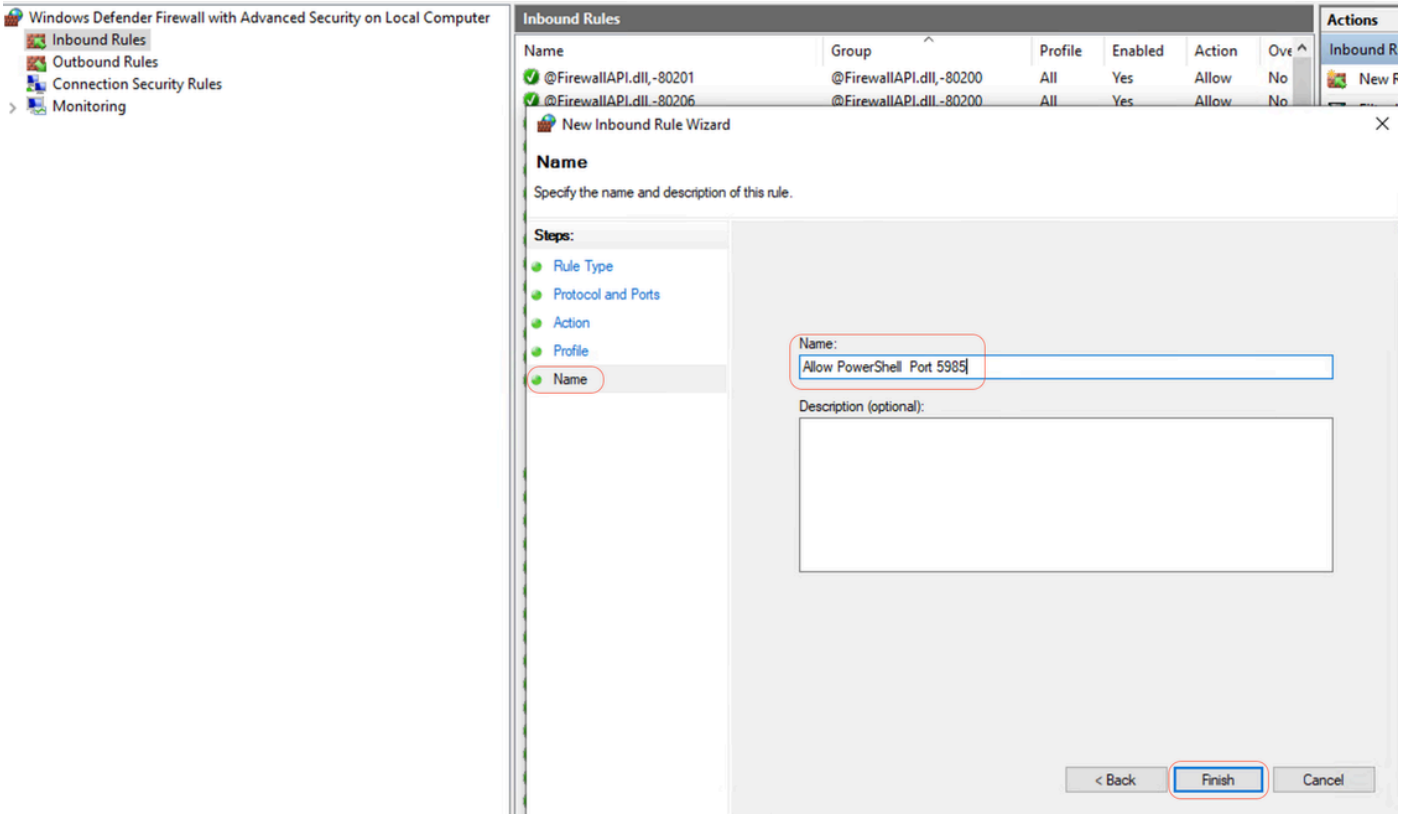
アクション

ステップ4:**Profile**の下で、**Domain**、**Private**、および**Public**の各チェックボックスをオンにして、**Next**をクリックします。



profile

ステップ**5:**[名前]で、ルールの名前(例：**Allow PowerShell on Port 5985**)を入力し、[完了]をクリックします。

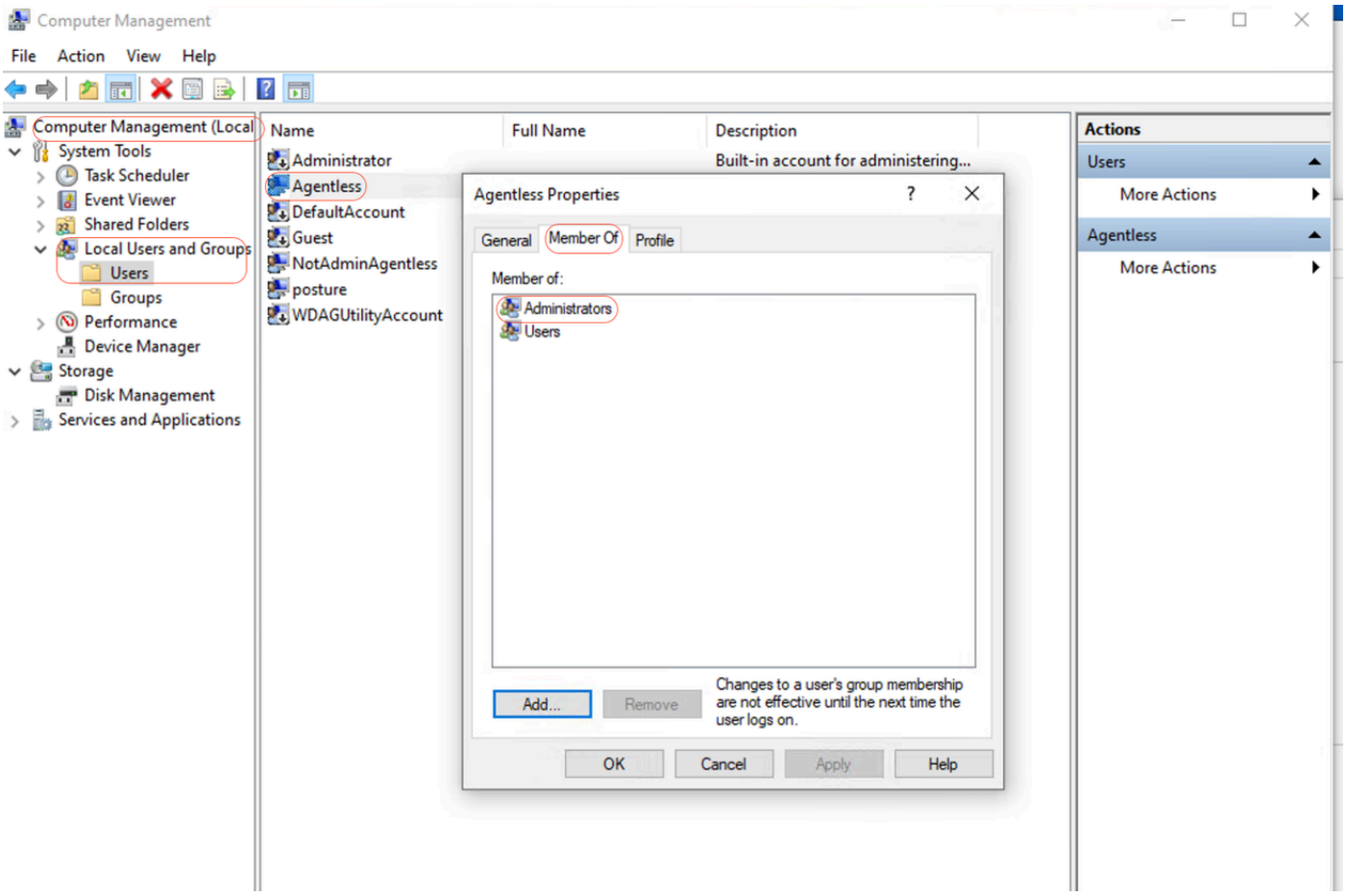


[名前(Name)]

シェルログイン用のクライアントクレデンシャルには、ローカル管理者権限が必要です

シェルログイン用のクライアントクレデンシャルには、ローカル管理者権限が必要です。 管理者権限を持っているかどうかを確認するには、次の手順を確認します。

Windows GUIの場合、Settings > Computer Management > Local Users and Groups > Users > Select the User Account(この例ではAgentless Accountを選択) > Member of, account must have Administrators Groupの順に移動します。



ローカル管理者権限

WinRMリスナーを検証しています

WinRMリスナーがポート**5985**で**HTTP**用に設定されていることを確認します。

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

PowerShellリモート処理WinRMを有効にする

サービスが実行され、自動的に起動するように設定されていることを確認するには、次の手順を実行します。

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**

予想される出力：

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はv7.1以降でなければなりません。クライアントにはcURL v7.34以降が必要です。

WindowsでPowerShellとcURLのバージョンを確認する方法

適切なバージョンのPowerShellを使用していることを確認します。ポスチャエージェントレスにはcURLが不可欠です。

PowerShellバージョンの確認

Windows の場合：

1. **PowerShellを開きます：**

・ Win + Xキーを押して、Windows PowerShellまたはWindows PowerShell (Admin)を選択します。

2. 次のコマンドを実行します。$PSVersionTable.PSVersion

・このコマンドは、システムにインストールされているPowerShellのバージョン詳細を出力します。

cURLバージョンの確認

Windows の場合：

1. コマンドプロンプトを開きます。

・ Win + Rキーを押し、cmdと入力して、**Enter**キーをクリックします。

2. 次のコマンドを実行します。 curl --version

・このコマンドは、システムにインストールされているcURLのバージョンを表示します。

WindowsデバイスのPowerShellとcURLのバージョンを確認するための出力

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>

追加設定

このコマンドは、WinRM接続の特定のリモートホストを信頼するようにコンピューターを構成します。 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> -

test-wsmanコマンドレットに-Authentication Negotiateパラメーターと-Credentialパラメーターを指定すると、リモートコンピューター上のWinRMサービスの可用性と構成を確認するための強力なツールになります。 test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

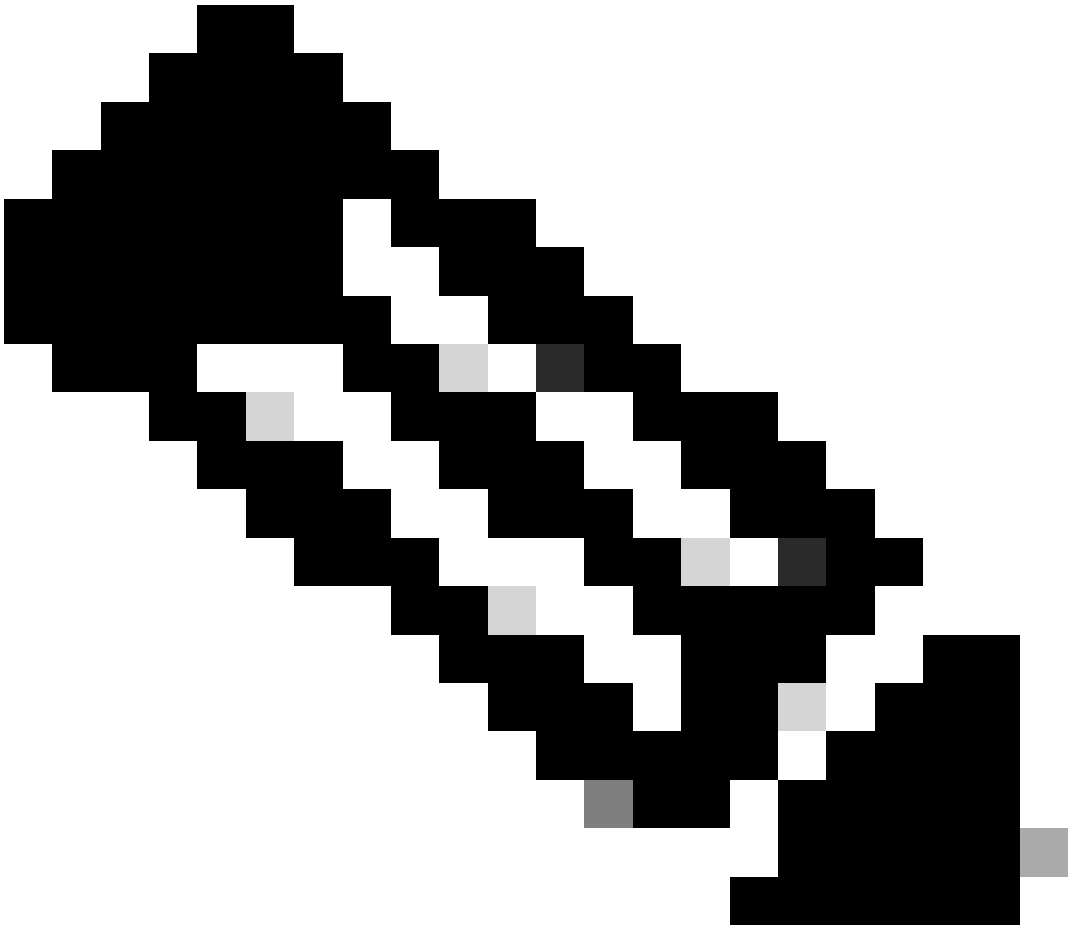
Powershellはv7.1以降でなければなりません。クライアントにはcURL v7.34以降が必要です。

macOSの場合

1. ターミナルを開きます。

・ Terminalは**Applications > Utilities**にあります。

2. 次のコマンドを実行します。 pwsh -Command '$PSVersionTable.PSVersion'



注：注：・ PowerShellコア(pwsh)がインストールされていることを確認します。インストールされていない場合は、Homebrewを使用してインストールできます（Himebrewがインストールされていることを確認してください）。 brew install --cask powershell

---

macOSの場合

1. ターミナルを開きます。

・ Terminalは**Applications** > **Utilities**にあります。

2. 次のコマンドを実行します。 curl --version

・このコマンドは、システムにインストールされているcURLのバージョンを表示する必要があります。

MacOSクライアントの場合、SSHにアクセスするためのポート22がクライアントにアクセスするために開いている必要があります

ステップバイステップガイド：

1. システム環境設定を開きます。

・ Appleメニューから**System Preferences**に移動します。

2. リモートログインを有効にします。

・共有に移動します。

・ Remote Loginの横にあるボックスをオンにします。

・ Allow access forオプションが適切なユーザまたはグループに設定されていることを確認します。**All users**を選択すると、Mac上で有効なアカウントを持つすべてのユーザがSSH経由でログインできます。

3. ファイアウォール設定の確認：

・ファイアウォールが有効な場合、SSH接続を許可することを確認する必要があります。

・ System Preferences > Security & Privacy > Firewallの順に開きます。

・ Firewall Optionsボタンをクリックします。

・ リモートログインまたは**SSH**がリストされ、許可されていることを確認します。リストされていない場合は、**Add**ボタン(+)をクリックして追加します。

4. ターミナル経由でポート22を開きます（必要な場合）。

・ Applications > Utilitiesで**Terminal**アプリケーションを開きます。

・ pfctlコマンドを使用して現在のファイアウォールルールを確認し、ポート22が開いていることを確認します。sudo pfctl -sr | grep 22

・ポート22が開いていない場合は、手動でルールを追加してSSHを許可できます：echo “pass in proto tcp from any to any port 22” | sudo pfctl -ef -

5. **SSHアクセスのテスト：**

・別のデバイスから、端末またはSSHクライアントを開きます。

・ IPアドレスssh username@<macOS-client-IP>を使用して、macOSクライアントへの接続を試みます。

・ usernameを適切なユーザアカウントに置き換え、<macOS-client-IP>をmacOSクライアントのIPアドレスに置き換えます。

MacOSでは、エンドポイントでの証明書インストールの失敗を回避するために、sudoersファイルで次のエントリが更新されていることを確認してください。

macOSエンドポイントを管理する場合、パスワードプロンプトを必要とせずに特定の管理コマンドを実行できることが重要です。

前提条件

・ macOSマシンでの管理者アクセス。

・端末コマンドに関する基本的な知識。

Sudoersファイルを更新する手順

1. **ターミナルを開きます。**

・ Terminalは**Applications > Utilities**にあります。

2. **Sudoersファイルを編集します。**

・ sudoersファイルを安全に編集するには、visudoコマンドを使用します。これにより、ファイルを保存する前に構文エラーが検出されます。sudo visudo

・管理者パスワードの入力を求められます。

3. **適切なセクションを検索します。**

・ ビジュアル表示エディタで、ユーザー固有のルールが定義されているセクションに移動します。通常、これはファイルの最下行きです。

4. **必要なエントリを追加します。**

・ 次の行を追加して、指定したユーザに、パスワードなしでsecurityコマンドとosascriptコマンドを実行する権限を付与します：<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

・ **<macadminusername>**を、macOS管理者の実際のユーザ名に置き換えます。

5. 保存して終了します。

・デフォルトのエディタ(nano)を使用している場合は、Ctrl + Xキーを押して終了し、Yキーを押して変更を確認します。最後に、Enterキーを押してファイルを保存します。

・ viまたはvimを使用している場合は、Escキーを押して:wqと入力し、Enterキーを押して保存し、終了します。

6. 変更の確認：

・変更が有効になったことを確認するために、更新されたsudo権限を必要とするコマンドを実行できます。例：

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

・これらのコマンドは、パスワードの入力を求めるプロンプトを表示せずに実行できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。