Configurer la posture sans agent

Table des matières

Introduction

Ce document décrit comment configurer Posture Agentless dans ISE et ce qui est requis dans le

point de terminaison pour exécuter le script sans agent.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Services Engine (ISE).
- La posture.
- PowerShell et SSH
- Windows 10 ou version ultérieure.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine (ISE) version 3.3.
- Package CiscoSans agentWindows 5.1.6.6
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La stratégie ISE effectue une évaluation côté client. Le client reçoit la politique d'exigence de posture d'ISE, effectue la collecte des données de posture, compare les résultats à la politique et renvoie les résultats d'évaluation à l'ISE.

ISE détermine ensuite si le périphérique est conforme ou non conforme sur la base du rapport de posture.

La posture sans agent est l'une des méthodes de posture qui collecte des informations de posture auprès des clients et se supprime automatiquement une fois l'opération terminée sans nécessiter d'action de la part de l'utilisateur final. La posture sans agent se connecte au client en utilisant des privilèges d'administration.

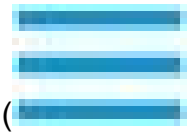
Pour commencer

Conditions préalables:

- Le client doit être accessible via son adresse IPv4ou IPv6 et cette adresse IP doit être disponible dans la comptabilité RADIUS.

- Le client doit être accessible depuis Cisco Identity Services Engine (ISE) via son adresse IPv4 ou IPv6. En outre, cette adresse IP doit être disponible dans la comptabilité RADIUS.
- Les clients Windows et Mac sont actuellement pris en charge :
    - Pour les clients Windows, le port 5985 permettant d'accéder à powershell sur le client doit être ouvert. Powershell doit être v7.1 ou ultérieure. Le client doit disposer de cURL v7.34 ou ultérieure.
    - Pour les clients MacOS, le port 22 pour accéder à SSH doit être ouvert pour accéder au client. Le client doit disposer de cURL v7.34 ou ultérieure.
- Les informations d'identification du client pour la connexion shell doivent avoir des privilèges d'administrateur local.
- Exécutez la mise à jour du flux de posture pour obtenir les clients les plus récents, comme décrit dans les étapes de configuration. Veuillez vérifier :
- Pour MacOS, assurez-vous que cette entrée est mise à jour dans le fichier sudoers pour éviter l'échec de l'installation du certificat sur les terminaux : Veuillez vérifier :

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

- Pour MacOS, le compte utilisateur configuré doit être un compte administrateur. La position sans agent pour MacOS ne fonctionne avec aucun autre type de compte, même si vous accordez plus de privilèges.Pour afficher cette fenêtre, cliquez sur l'icône Menu () et choisissez Administration > System > Settings > Endpoint Scripts > Login Configuration > MAC Local User.
- En cas de changements dans les activités liées aux ports dans les clients Windows en raison des mises à jour de Microsoft, vous devez reconfigurer le flux de travail de configuration de la position sans agent pour les clients Windows.

Conditions de posture prises en charge

- Conditions de fichier, à l'exception des conditions qui utilisent les chemins d'accès aux fichiers USER_DESKTOP et USER_PROFILE
- Conditions de service, à l'exception des vérifications Démon système et Démon ou Agent utilisateur sur macOS
- Conditions d'application
- Conditions de source de données externe

- Conditions composées
- Conditions anti-programme malveillant
- Condition de gestion des correctifs, à l'exception des vérifications de la condition EnabledAndUp To
- Conditions du pare-feu
- Conditions de cryptage du disque, à l'exception de la vérification de la condition de cryptage basée sur l'emplacement
- Conditions du Registre, à l'exception des conditions qui utilisent HCSK comme clé racine

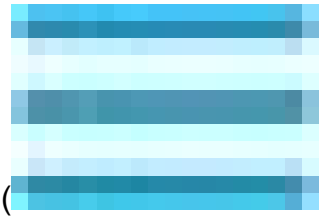
Conditions de posture non prises en charge

- Correction
- Délai de grâce
- Réévaluation Périodique
- Politique d'utilisation acceptable

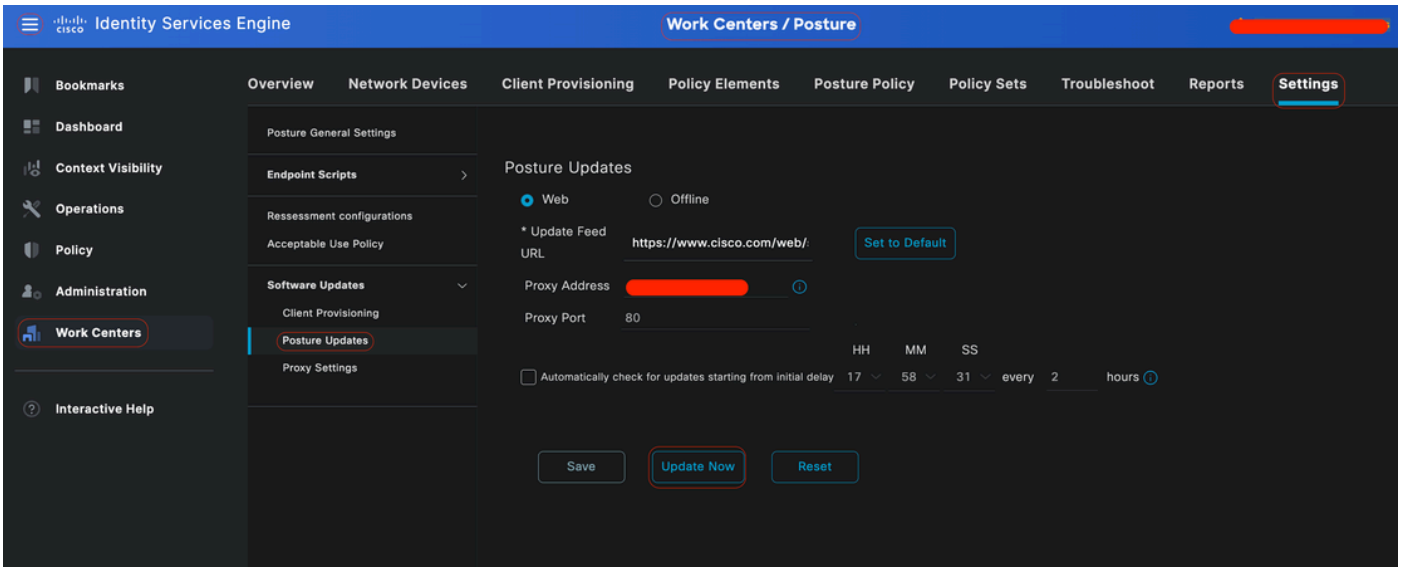
Configuration d'ISE

Mettre à jour le flux Posture

Il est recommandé de mettre à jour Posture Feed avant de commencer à configurer Posture.



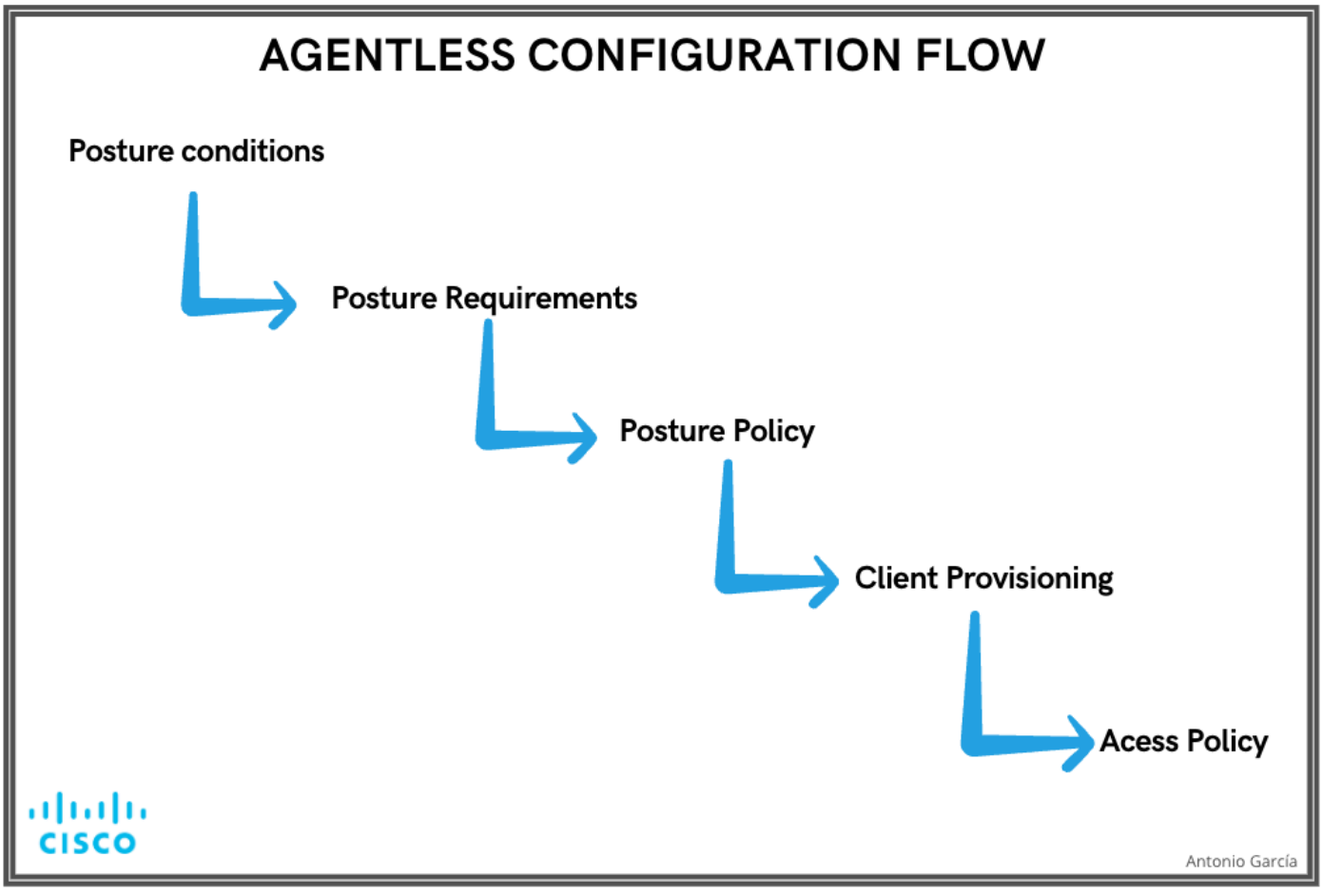
Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Work Centers > Posture > Settings > Software Updates > Update Now.



Mise à jour du flux Posture

Flux de configuration sans agent

Posture Agentless doit être configuré afin que la première configuration soit requise pour la suivante et ainsi de suite. Vous avez remarqué que la correction n'est pas dans le flux ; cependant, plus tard, ce document va couvrir une alternative pour configurer la correction.

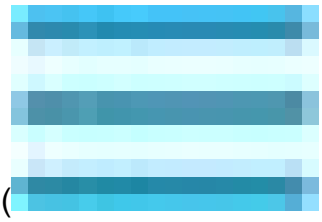


Flux de configuration sans agent

Configuration de la posture sans agent

Condition De Posture

Les conditions de posture sont l'ensemble des règles de notre stratégie de sécurité qui définissent un terminal conforme. Certains de ces éléments incluent l'installation d'un pare-feu, d'un logiciel antivirus, d'un logiciel anti-programme malveillant, de correctifs, de cryptage de disque et plus encore.



Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Work Centers > Posture > Policy Elements > Conditions, cliquez sur Add , et créez une ou plusieurs conditions de posture qui utilisent la posture sans agent pour identifier le besoin. Une fois la condition créée, cliquez sur Enregistrer.

Dans ce scénario, une condition d'application nommée "Agentless_Condition_Application" a été configurée avec les paramètres suivants :

· Système d'exploitation : Tout Windows

Cette condition s'applique à n'importe quelle version du système d'exploitation Windows, garantissant ainsi une compatibilité étendue entre les différents environnements Windows.

· Vérifier par : Process

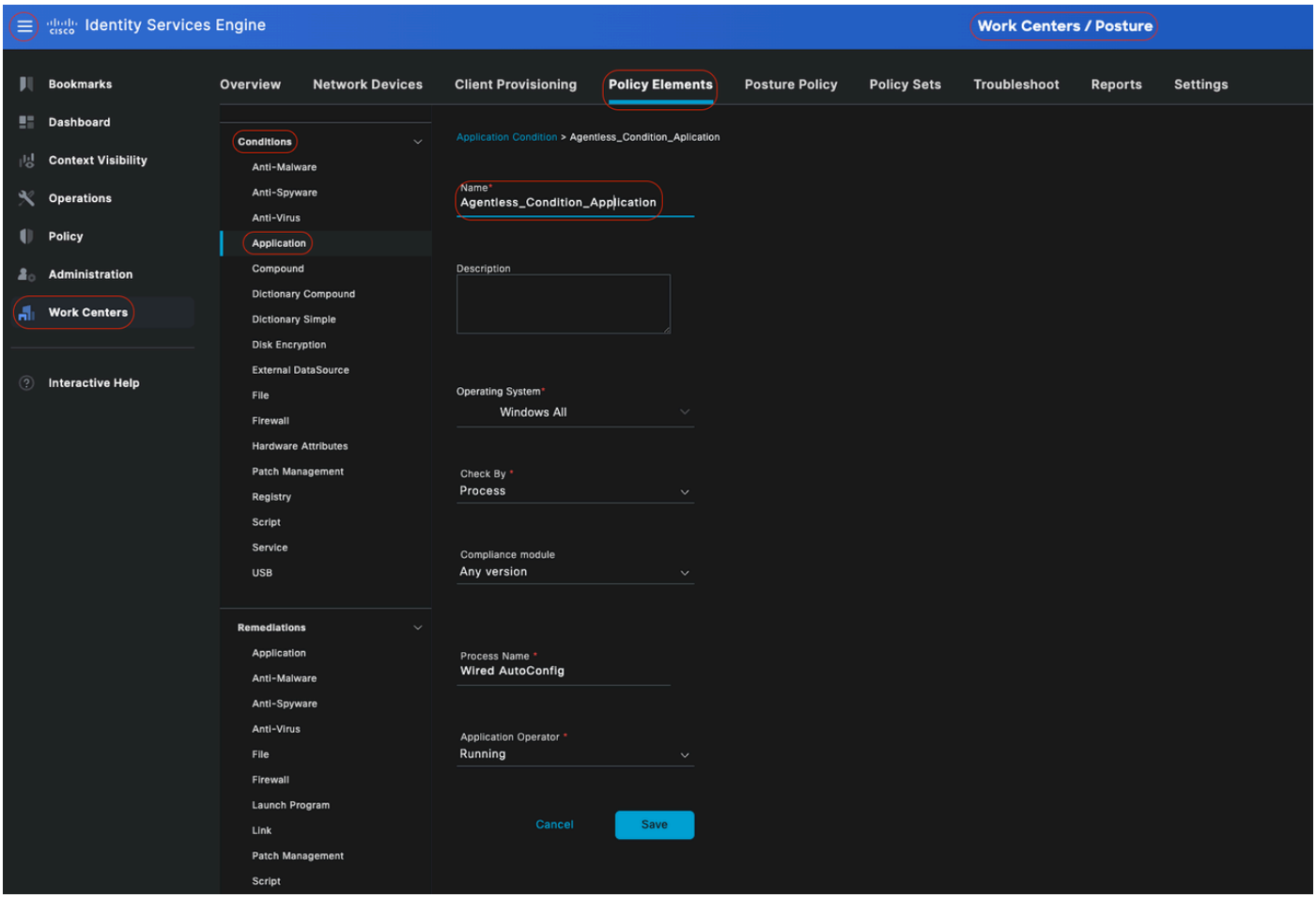
Le système surveille les processus au sein du périphérique. Vous avez la possibilité de sélectionner Processus ou Application ; dans ce cas, Process a été choisi.

•Nom du processus: Configuration automatique câblée

Le processus Wired AutoConfig est le processus que le module conforme va enregistrer dans le périphérique. Ce processus est responsable de la configuration et de la gestion des connexions réseau câblées, y compris l'authentification IEEE 802.1X.

· Opérateur d'application : Marche

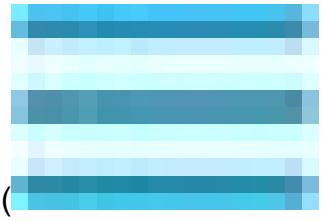
Le module de conformité vérifie si le processus Wired AutoConfig est en cours d'exécution sur le périphérique. Vous avez la possibilité de sélectionner En cours ou Non en cours d'exécution. Dans cette instance, Running a été sélectionné pour s'assurer que le processus est actif.



Condition Sans Agent

Exigence De Posture

Une condition de posture est un ensemble de conditions composées ou une seule condition qui peut être liée à un rôle et à un système d'exploitation. Tous les clients qui se connectent à votre réseau doivent répondre aux exigences obligatoires lors de l'évaluation de la position pour se conformer au réseau.



Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Centres de travail > Posture > Éléments de politique > Exigence. Cliquez sur la flèche vers le bas et sélectionnez Insérer une nouvelle exigence, puis créez une ou plusieurs exigences de posture qui utilisent la posture sans agent. Une fois le besoin créé, cliquez sur Terminé, puis sur Enregistrer.

Dans ce cas, un besoin d'application nommé "Agentless_Requirement_Application" a été configuré avec les critères suivants :

· Système d'exploitation : Tout Windows

Cette exigence s'applique à toutes les versions du système d'exploitation Windows, en s'assurant qu'elle est applicable à tous les environnements Windows.

· Type de posture : Sans Agent

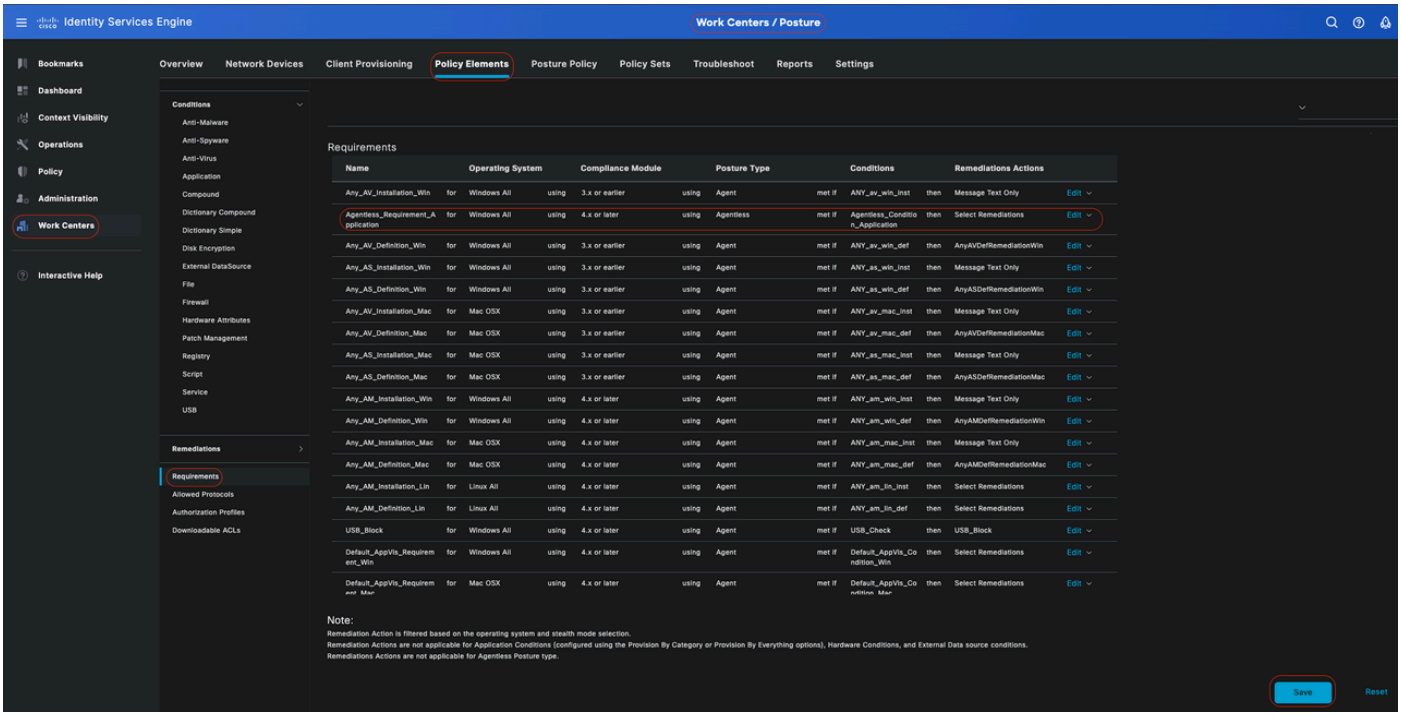
Cette configuration est définie pour un environnement sans agent. Les options disponibles sont Agent, Agent furtif, Agent temporel et Sans agent. Dans ce scénario, Agentless a été sélectionné.

•Modalités: Application_Condition_Sans_Agent

Indique la condition que le module de posture ISE et le module de conformité ISE vont vérifier dans les processus du périphérique. La condition sélectionnée est Agentless_Condition_Application.

· Mesures correctives :

Cette configuration étant destinée à un environnement sans agent, les actions correctives ne sont pas prises en charge et ce champ est grisé.



Exigence Sans Agent

Politique de posture

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Work Centers > Posture > Posture Policy. Cliquez sur la flèche vers le bas et sélectionnez Insert new Requirement, et créez une ou plusieurs règles de stratégie de posture prises en charge qui utilisent la posture sans agent pour cette condition de posture. Une fois la

stratégie de position créée, cliquez sur Terminé, puis sur Enregistrer.

Dans ce scénario, une politique de posture nommée "Agentless_Policy_Application" a été configurée avec les paramètres suivants :

· Nom de la règle : Application_Stratégie_Sans_Agent

Il s'agit du nom désigné pour la politique de posture dans cet exemple de configuration.

· Système d'exploitation : Tout Windows

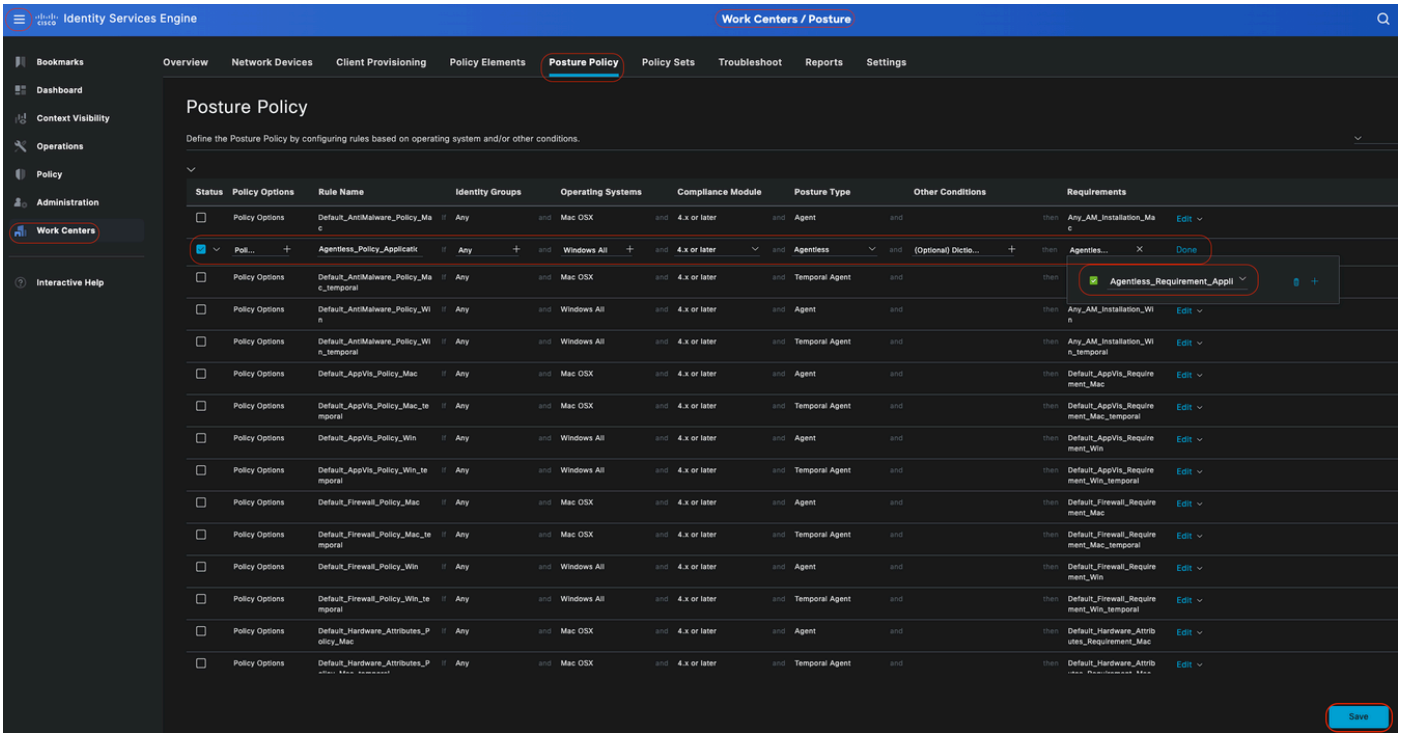
La stratégie est définie pour s'appliquer à toutes les versions du système d'exploitation Windows, assurant ainsi une compatibilité étendue entre les différents environnements Windows.

· Type de posture : Sans Agent

Cette configuration est définie pour un environnement sans agent. Les options disponibles sont Agent, Agent furtif, Agent temporel et Sans agent. Dans ce scénario, Agentless a été sélectionné.

· Autres conditions :

Dans cet exemple de configuration, aucune condition supplémentaire n'a été créée. Cependant, vous avez la possibilité de configurer des conditions spécifiques pour vous assurer que seuls les périphériques ciblés sont soumis à cette stratégie de position, plutôt que tous les périphériques Windows sur le réseau. Cela peut être particulièrement utile pour la segmentation du réseau.



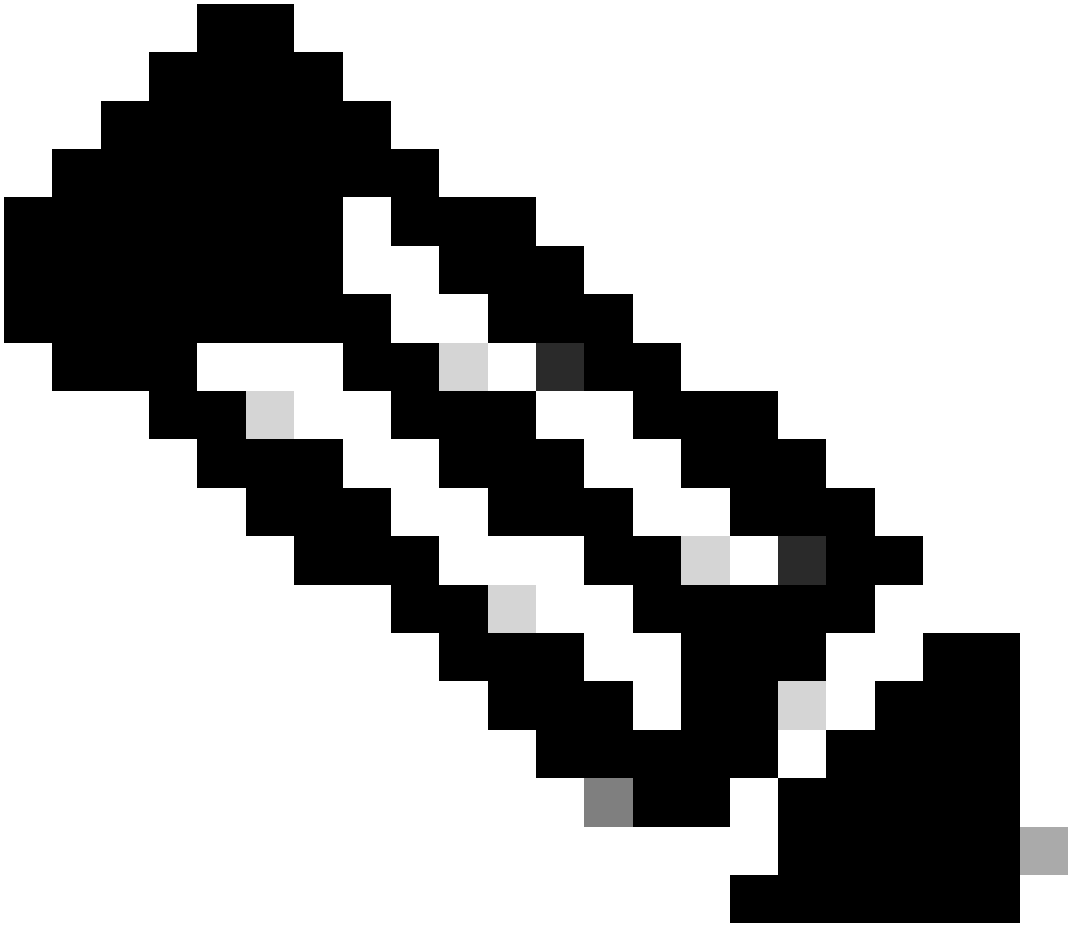
Politique de posture sans agent

Provisionnement client

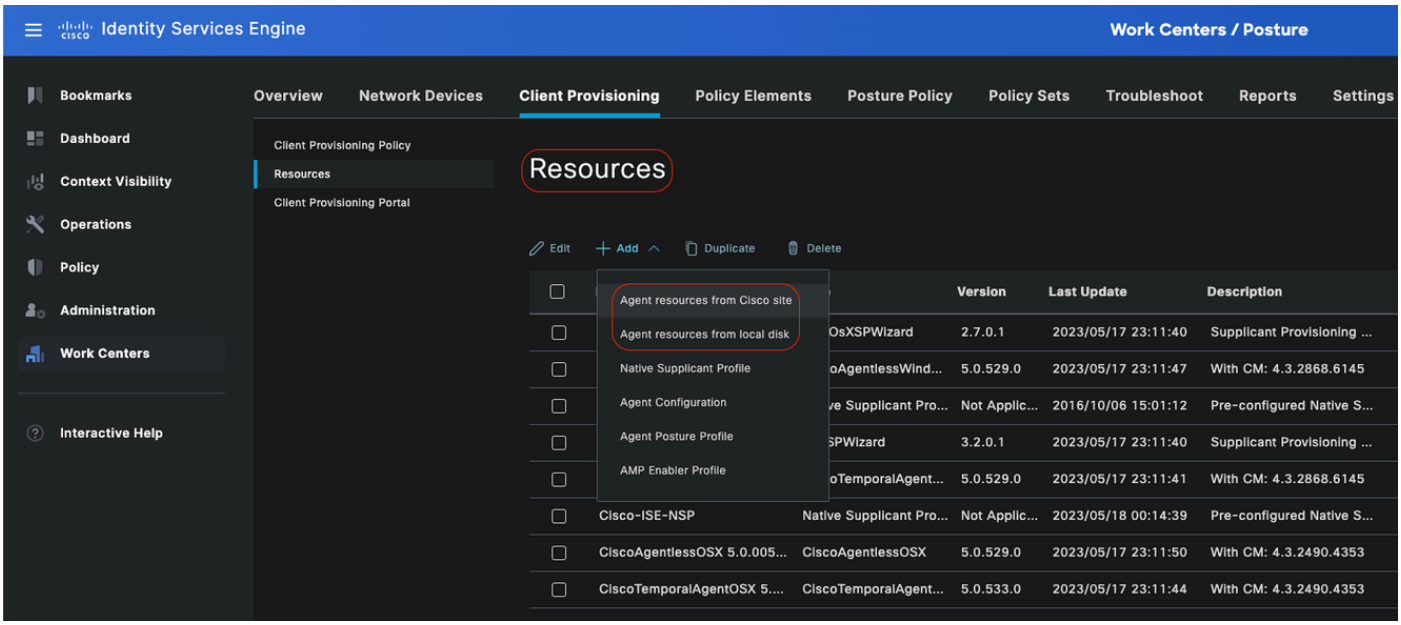
Étape 1 : téléchargement des ressources

Pour commencer à configurer le provisionnement du client, vous devez d'abord télécharger les ressources requises et les mettre à disposition dans ISE afin de pouvoir les utiliser ultérieurement dans la politique de provisionnement du client.

Il existe deux façons d'ajouter des ressources à ISE : Agent Resources from Cisco site et Agent Resources from Local disk. Puisque vous configurez sans agent, vous devez passer par Ressources d'agent du site Cisco pour télécharger.

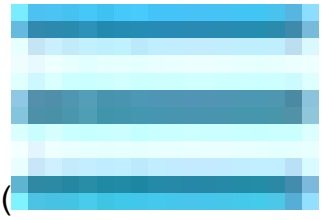


Remarque : Pour utiliser ces ressources d'agent à partir du site Cisco, le PAN ISE a besoin d'un accès Internet.



Ressources

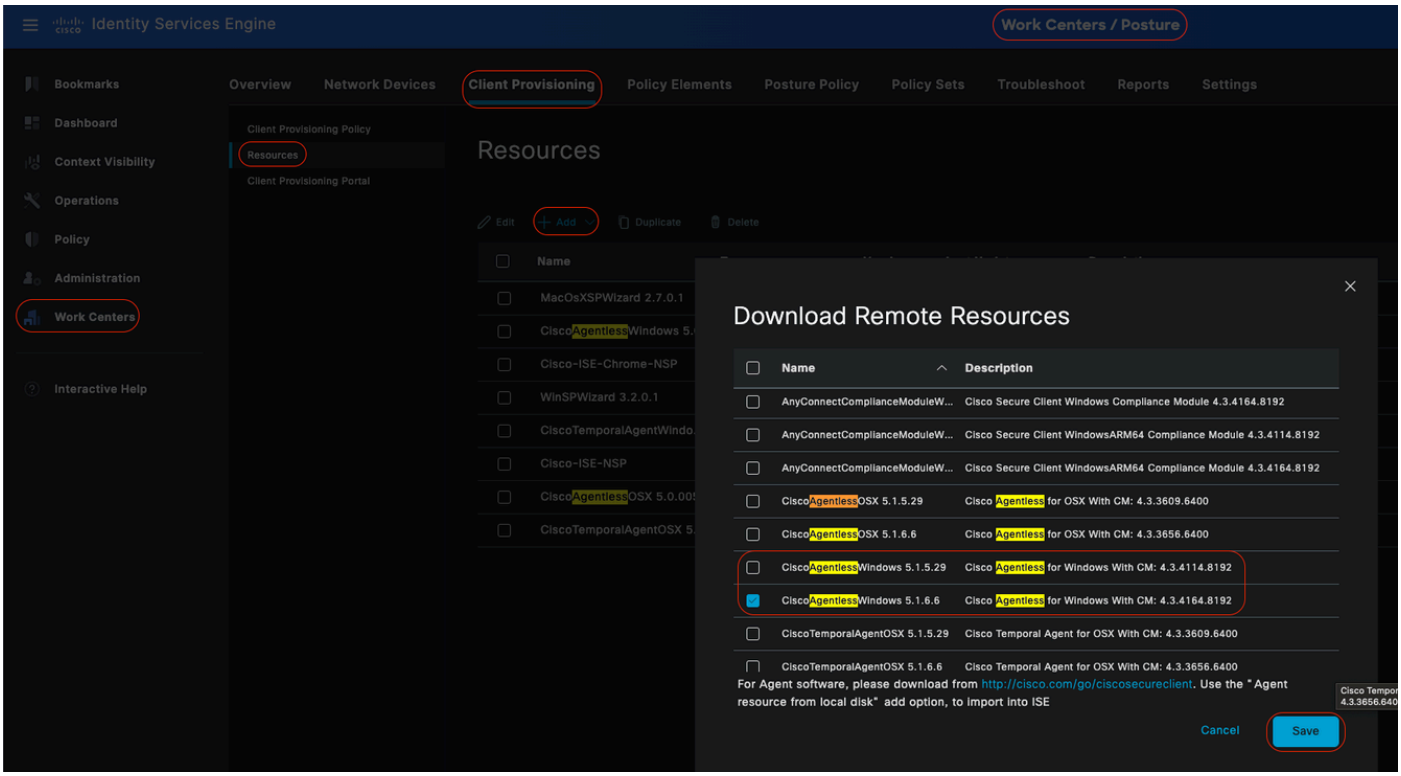
Ressources d'agent du site Cisco



Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add , Select Agent Resources from Cisco site, cliquez sur Save.

À partir du site Cisco, vous pouvez télécharger uniquement le module de conformité. Le système affiche les deux derniers modules de conformité à télécharger. Le package de ressources CiscoAgentlessWindows 5.1.6.6 est sélectionné pour cet exemple de configuration. Il est uniquement destiné aux périphériques Windows.

.



Ressources d'agent du site Cisco

Étape 2 : configuration de la politique de provisionnement du client

Lors de la configuration de Posture Agent, vous avez besoin de deux ressources différentes (AnyConnect ou Secure Client et Compliance Module),

Mappez les deux ressources sous Configuration de l'agent avec le profil de posture de l'agent afin de pouvoir utiliser cette configuration de l'agent dans votre stratégie de mise en service de client.

Cependant, lors de la configuration de Posture Agentless, il n'est pas nécessaire de configurer Agent Configuration ou Agent Posture Profile, au lieu de cela, vous téléchargez seulement le package Agentless à partir de Agent Resources à partir du site Cisco.

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Cliquez sur la flèche vers le bas et sélectionnez Insert new policy above ou Insert new policy below, Duplicate above ou Duplicate below :

- Nom de la règle : Agentless_Client_Provisioning_Policy

Indique le nom de la politique d'approvisionnement du client.

- Système d'exploitation : Windows All

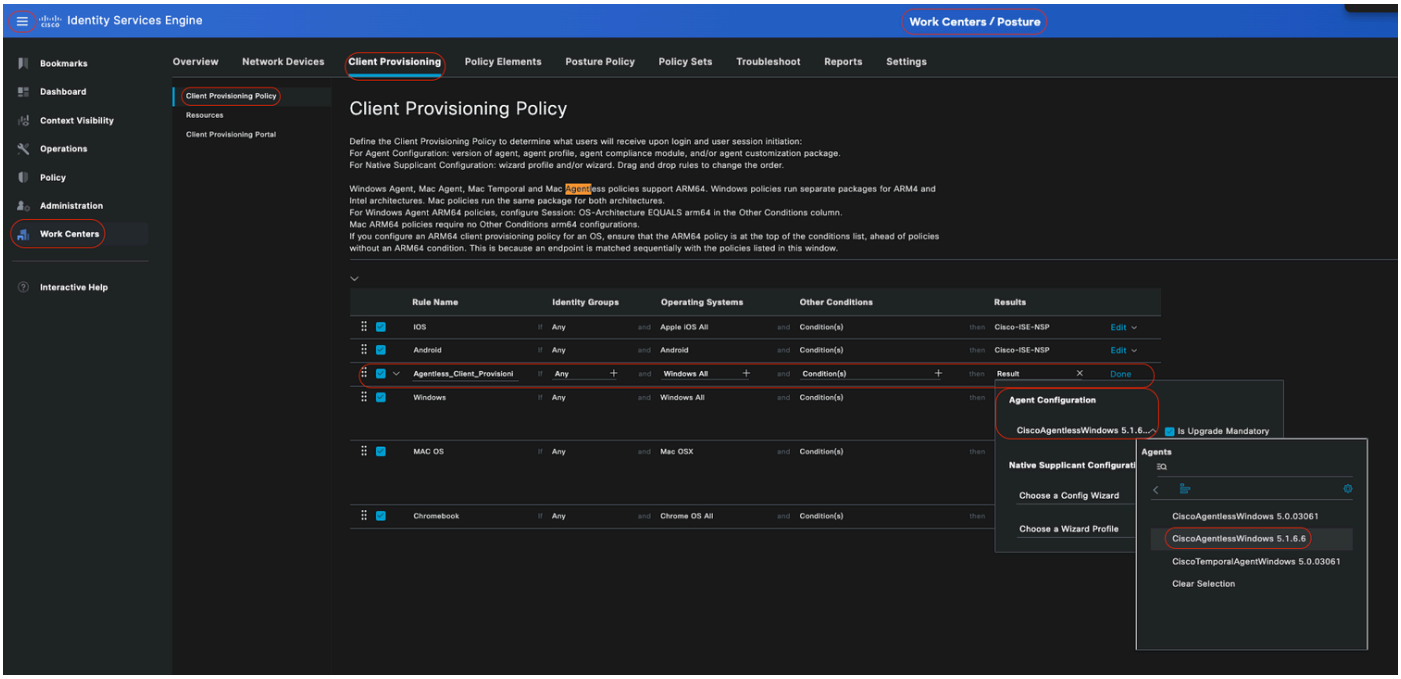
Cela garantit que la stratégie s'applique à toutes les versions du système d'exploitation Windows.

- Autres conditions : aucune condition spécifique n'est configurée dans cet exemple. Cependant, vous pouvez configurer des conditions pour vous assurer que seuls les périphériques souhaités correspondent à cette stratégie d'approvisionnement du client, plutôt que tous les périphériques Windows du réseau. Ceci est particulièrement utile pour la segmentation du réseau.

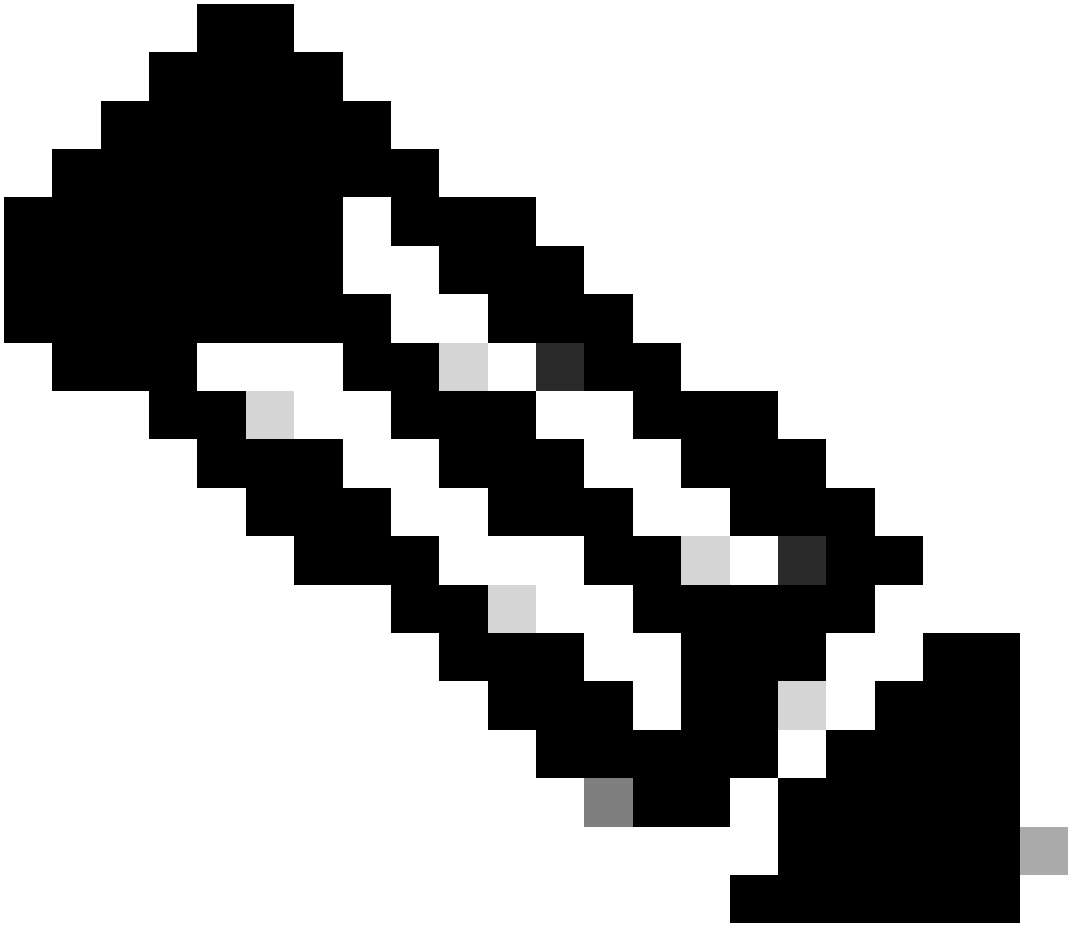
Exemple : Si vous utilisez Active Directory, vous pouvez incorporer des groupes Active Directory dans votre stratégie pour affiner les périphériques affectés.

- Résultats : sélectionnez le package ou l'agent de configuration approprié. Puisque vous configurez pour un environnement sans agent, choisissez le package CiscoAgentlessWindows 5.1.6.6, que vous avez précédemment téléchargé à partir des Ressources d'agent du site Cisco. Ce package sans agent contient toutes les ressources nécessaires (Logiciel sans agent et Module de conformité) nécessaires à l'exécution de Posture Agentless.

•Cliquez sur Save (enregistrer)

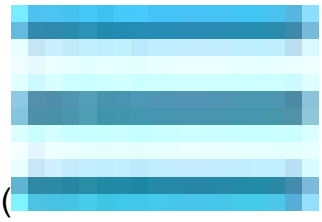


Politique de provisionnement client sans agent



Remarque : Assurez-vous qu'une seule politique de provisionnement du client satisfait les conditions pour toute tentative d'authentification donnée. Si plusieurs stratégies sont évaluées simultanément, cela peut entraîner des comportements inattendus et des conflits potentiels.

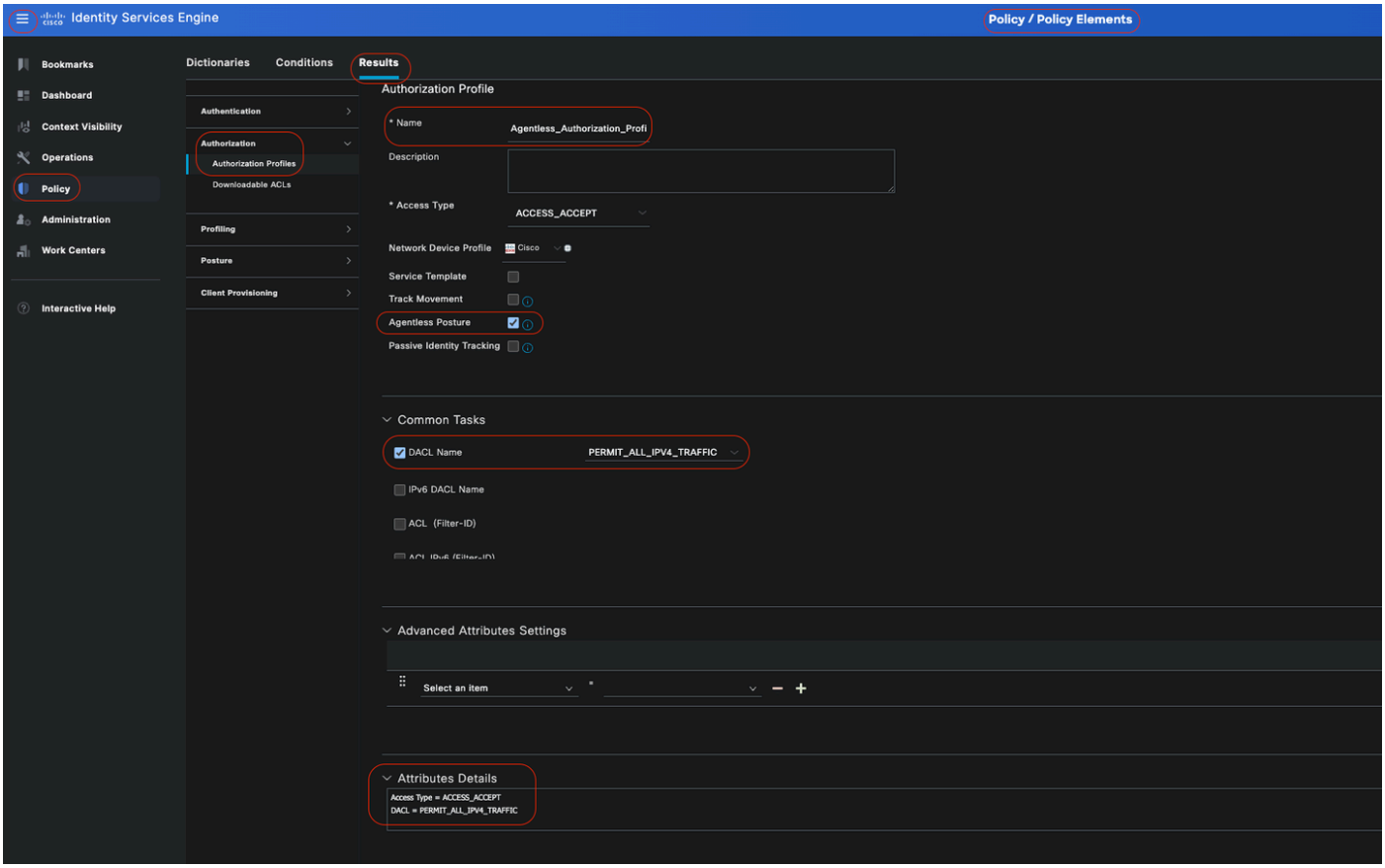
Profil d'autorisation sans agent



Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation et créez un profil d'autorisation pour évaluer les résultats de la position sans agent.

- Dans cet exemple de configuration, nommé Authorization Profile as Agentless_Authorization_Profile.

- Activez la position sans agent dans le profil d'autorisation.
- Utilisez ce profil uniquement pour la posture sans agent. N'utilisez pas cette option pour d'autres types de postures.
- CWA et ACL de redirection ne sont pas requis pour la position sans agent. Vous pouvez utiliser des VLAN, des DACL ou des ACL dans le cadre de vos règles de segmentation. Pour rester simple, seule une dACL (autorisant tout le trafic ipv4) est configurée en plus de la vérification de la position sans agent dans cet exemple de configuration.
- Cliquez sur Enregistrer.



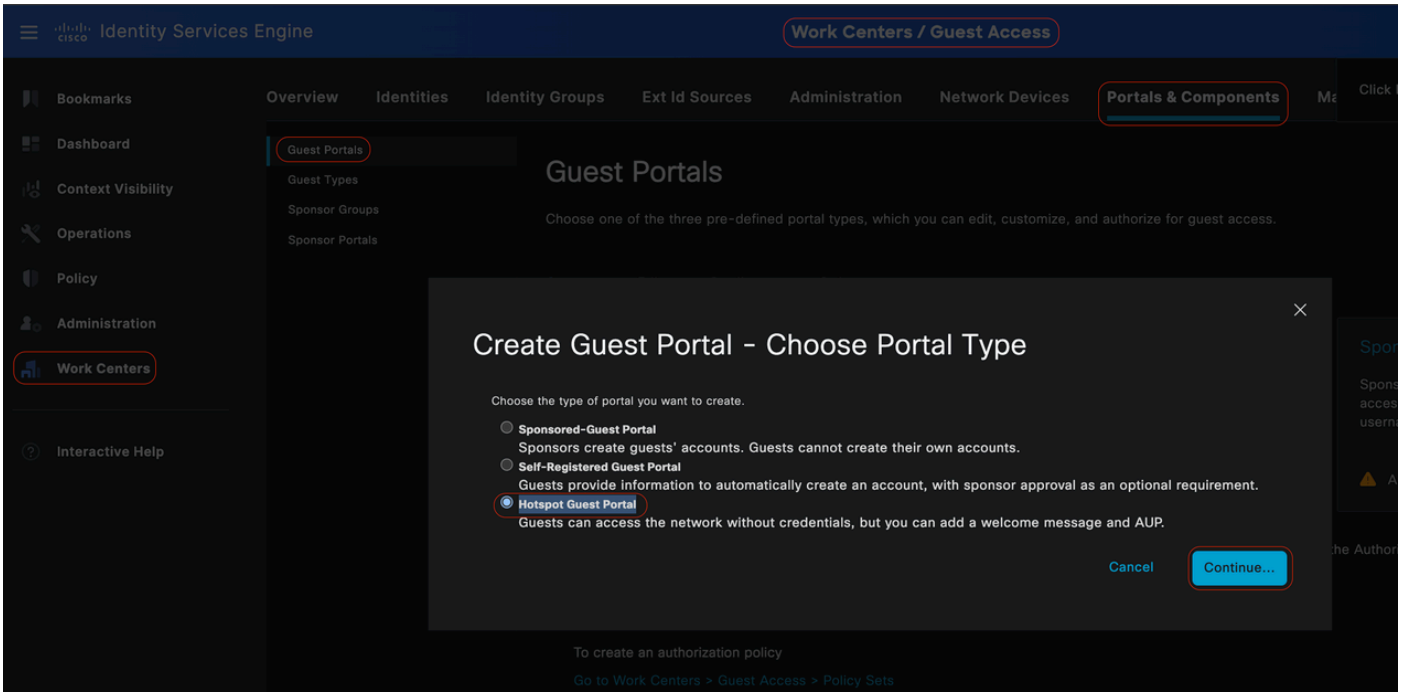
Profil d'autorisation sans agent

Alternative à l'utilisation de mesures correctives (facultatif)

La prise en charge de la correction dans le flux sans agent n'est pas disponible. Pour résoudre ce problème, vous pouvez mettre en oeuvre un portail de hotspot personnalisé afin de sensibiliser davantage les utilisateurs à la conformité des terminaux. Lorsqu'un terminal est identifié comme non conforme, les utilisateurs peuvent être redirigés vers ce portail. Cette approche garantit que les utilisateurs sont informés de l'état de conformité de leurs terminaux et peuvent prendre les mesures appropriées pour corriger les problèmes.

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu (

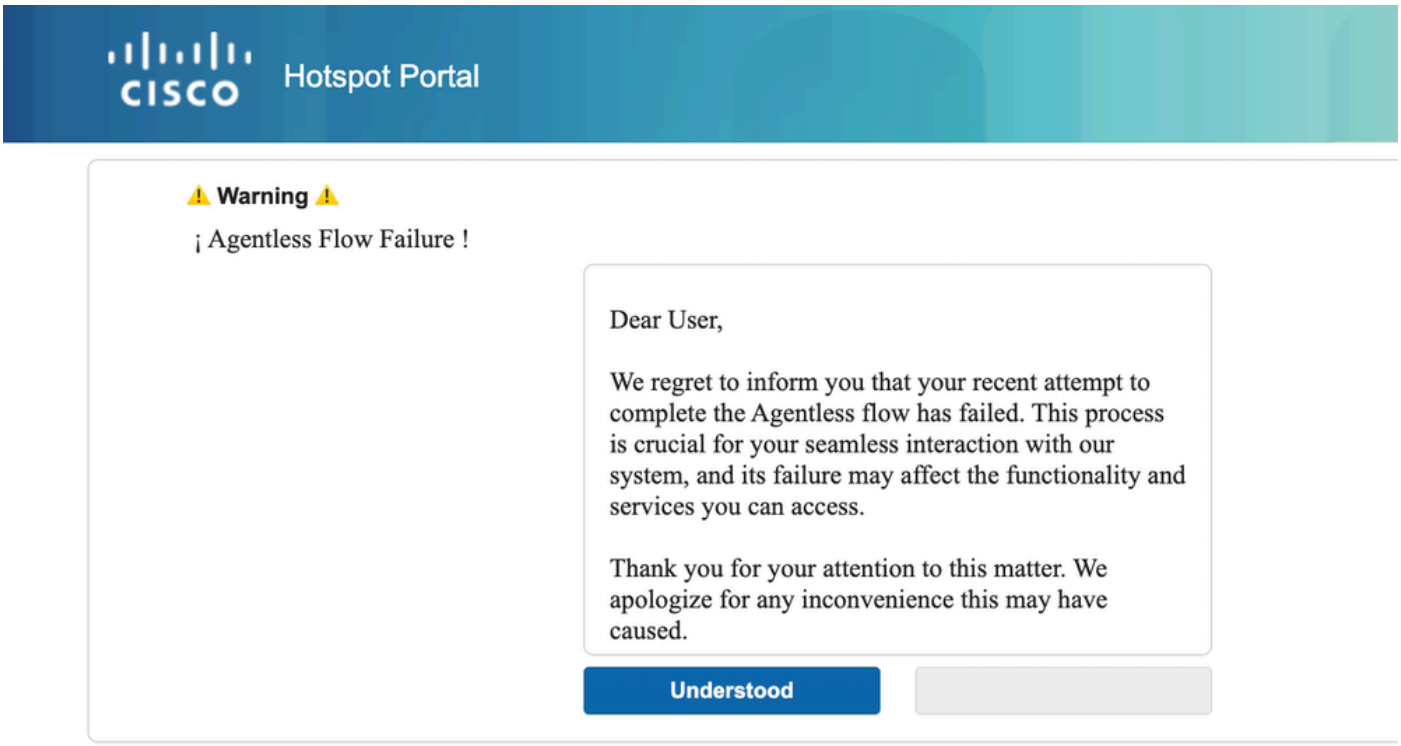
) et choisissez Work Centers > Guest Access > Portals & Components >Guest Portals. Cliquez sur Create > Select Hotspot Guest Portal > Continue: . Dans cet exemple de configuration, Hotspot Portal est nommé Agentless_Warning.



Portail Hotspot Guest

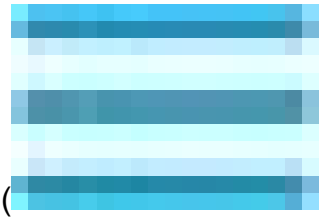
Dans les paramètres du portail, vous avez la possibilité de personnaliser les messages affichés pour les utilisateurs finaux afin de les aligner sur vos besoins spécifiques. Il s'agit simplement d'un

exemple d'affichage personnalisé du portail :



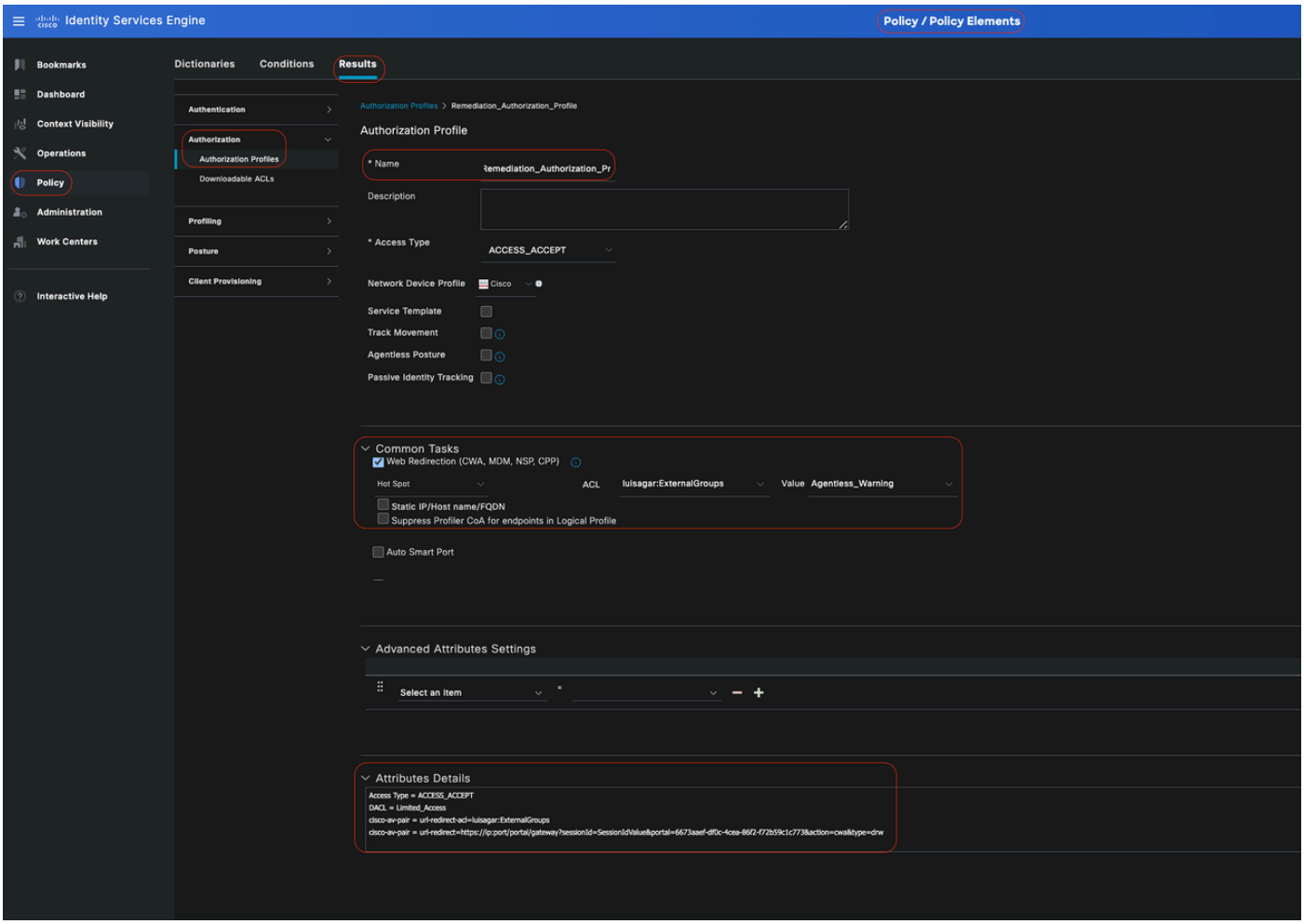
Posture défaillante sans agent

Profil d'autorisation de correction (facultatif)



Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissezStratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation et créez un profil d'autorisation pour votre correction.

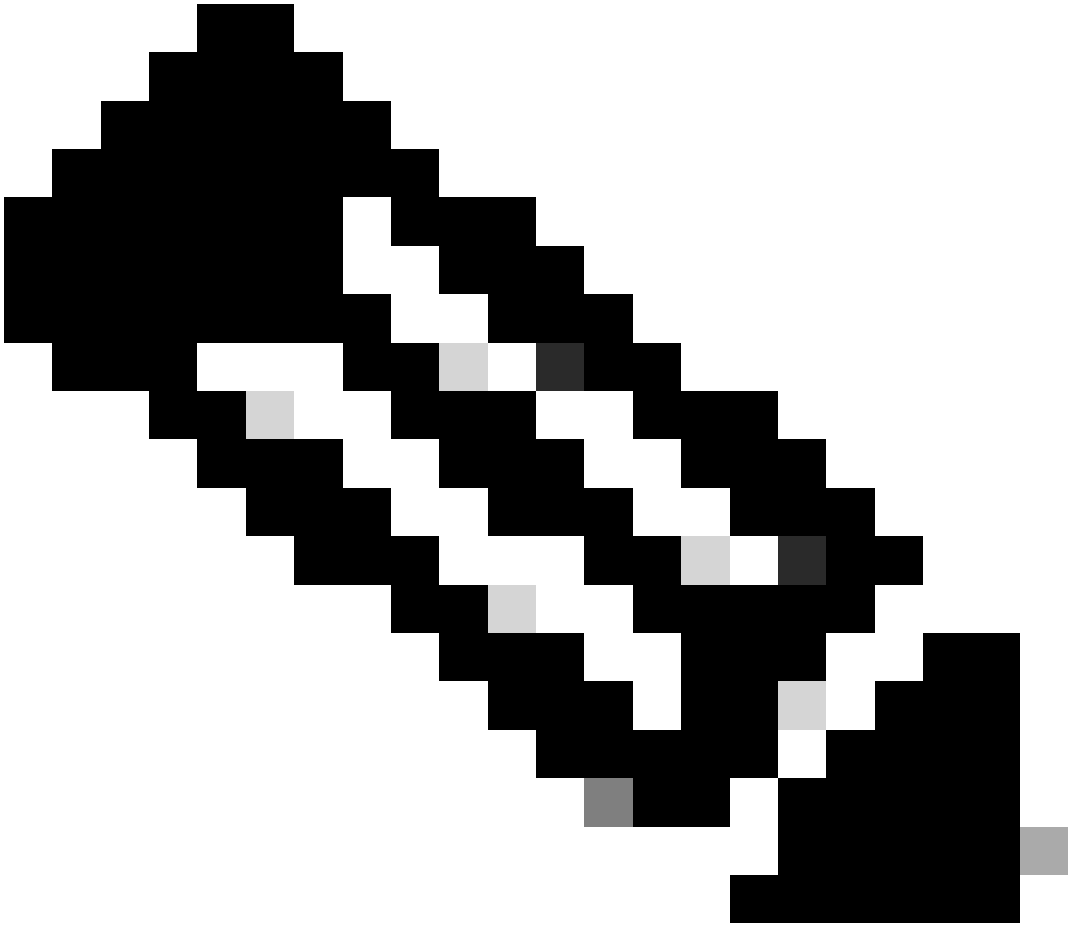
- Dans cet exemple de configuration, nommé Authorization Profile as Remediation_Authorization_Profile.
- Dans un souci de simplicité, cet exemple de configuration inclut uniquement une liste de contrôle d'accès téléchargeable nommée Limited_Access qui autorise un accès limité, adaptée aux besoins spécifiques de votre organisation.
- La fonctionnalité Web Redirection a été configurée, y compris un groupe externe et le point d'accès, ce qui améliore la sensibilisation de l'utilisateur en matière de conformité des terminaux.
- Cliquez sur Save.



Règle d'autorisation de correction

Règle d'autorisation sans agent

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissezStratégie > Jeux de stratégies et développez Stratégie d'autorisation. Activez et configurez ces trois stratégies d'autorisation :



Remarque : Ces règles d'autorisation doivent être configurées dans l'ordre spécifié pour garantir le bon fonctionnement du flux de posture.

Redirection_Conformité_Inconnue :

•Modalités:

Configurez Network_Access_Authentication_Passed ET Compliance_Unknown_Devices avec le jeu de résultats défini sur Agentless Posture. Cette condition déclenche le flux sans agent.

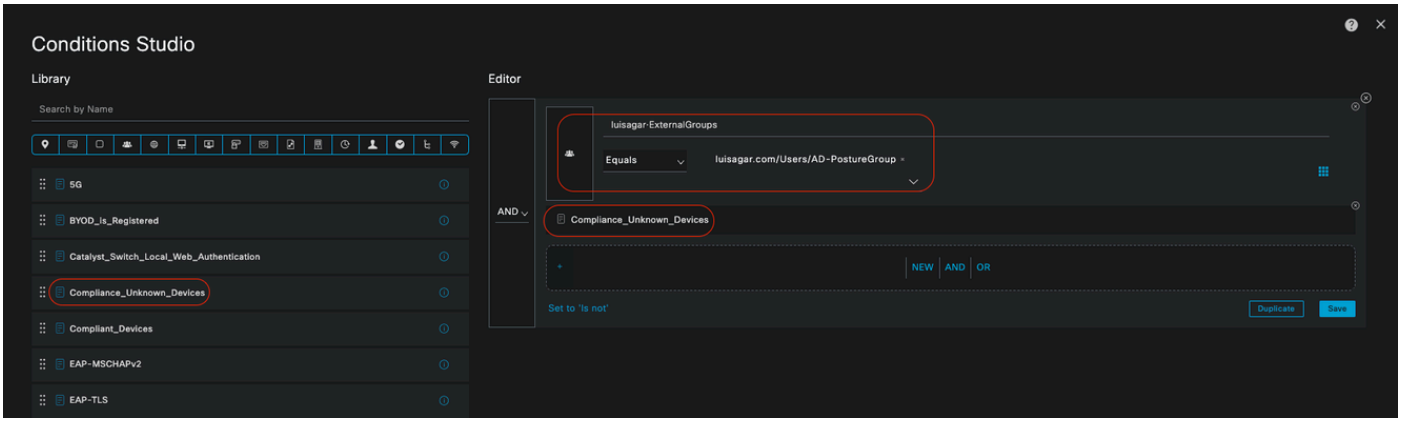
· Exemples de conditions :

Configurez une condition de groupe Active Directory (AD) pour segmenter le trafic.

La condition Compliance_Unknown_Devices doit être configurée car l'état de la position initiale est inconnu.

· Profil d'autorisation :

Affectez Agentless_Authorization_Profile à cette règle d'autorisation pour garantir que les périphériques passent par le flux de posture sans agent. Cette condition contient le flux sans agent afin que les périphériques qui atteignent ce profil puissent lancer le flux sans agent.



Règle d'autorisation inconnue

NonCompliant_Devices_Redirect :

•Modalités: Configurez Network_Access_Authentication_Passed et Non_Compliant_Devices avec le jeu de résultats DenyAccess. Vous pouvez également utiliser l'option de conversion, comme illustré dans cet exemple.

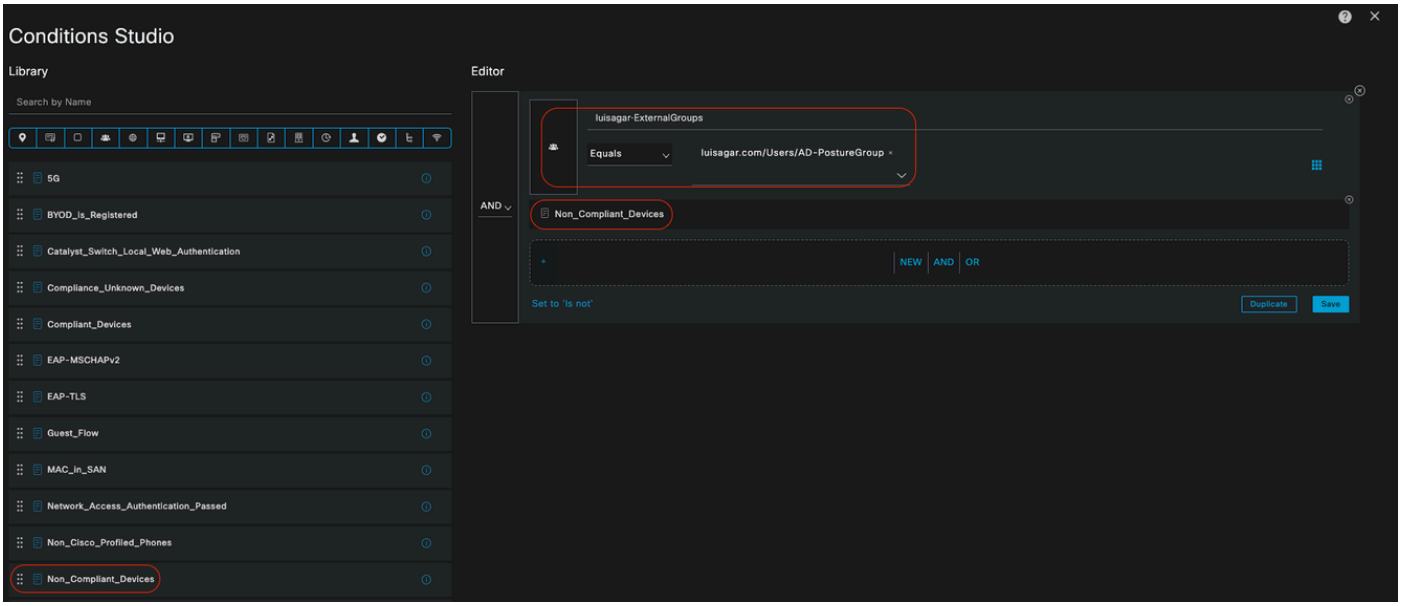
· Exemples de conditions :

Configurez une condition de groupe AD pour segmenter le trafic.

La condition Compliance_Unknown_Devices doit être configurée pour attribuer des ressources limitées lorsque l'état de posture n'est pas conforme.

· Profil d'autorisation :

Attribuez Remediation_Authorization_Profile à cette règle d'autorisation pour notifier les périphériques non conformes de leur état actuel via le portail Hotspot ou pour refuser l'accès.



Règle D'Autorisation Non Conforme

Accès_Périphériques_Conformes :

•Modalités:

Configurez Network_Access_Authentication_Passed et Compliant_Devices avec le jeu de résultats PermitAccess.

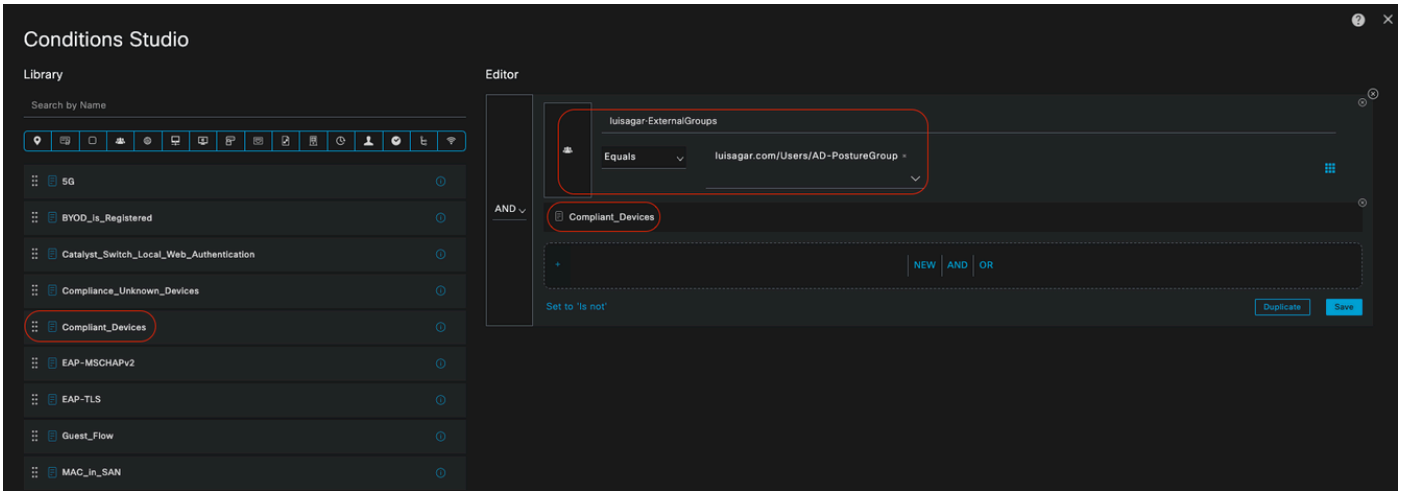
· Exemples de conditions :

Configurez une condition de groupe AD pour segmenter le trafic.

La condition Compliance_Unknown_Devices doit être configurée afin que les périphériques conformes bénéficient d'un accès approprié.

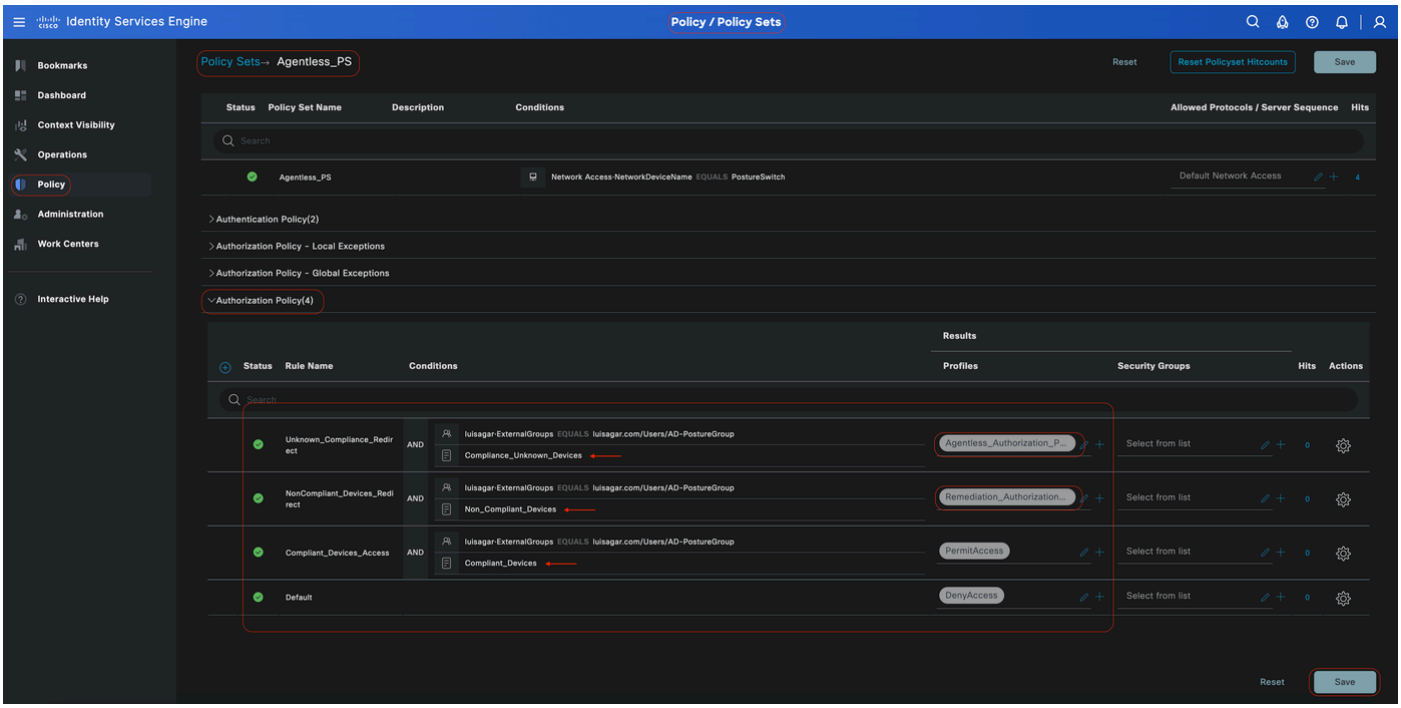
· Profil d'autorisation :

Attribuez PermitAccess à cette règle d'autorisation pour garantir l'accès des périphériques conformes. Ce profil peut être personnalisé pour répondre aux besoins de votre organisation.



règle d'autorisation conforme

Toutes les règles d'autorisation



Règles d'autorisation

Configurer les identifiants de connexion des terminaux

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Administration > Settings > Endpoint Scripts > Login Configuration, et configurez les informations d'identification du client pour se connecter aux clients.

Ces mêmes informations d'identification sont utilisées par les scripts de point de terminaison afin que Cisco ISE puisse se connecter aux clients.

Pour les périphériques Windows, vous ne configurez que les deux premiers onglets (Utilisateur du domaine Windows et Utilisateur local Windows)

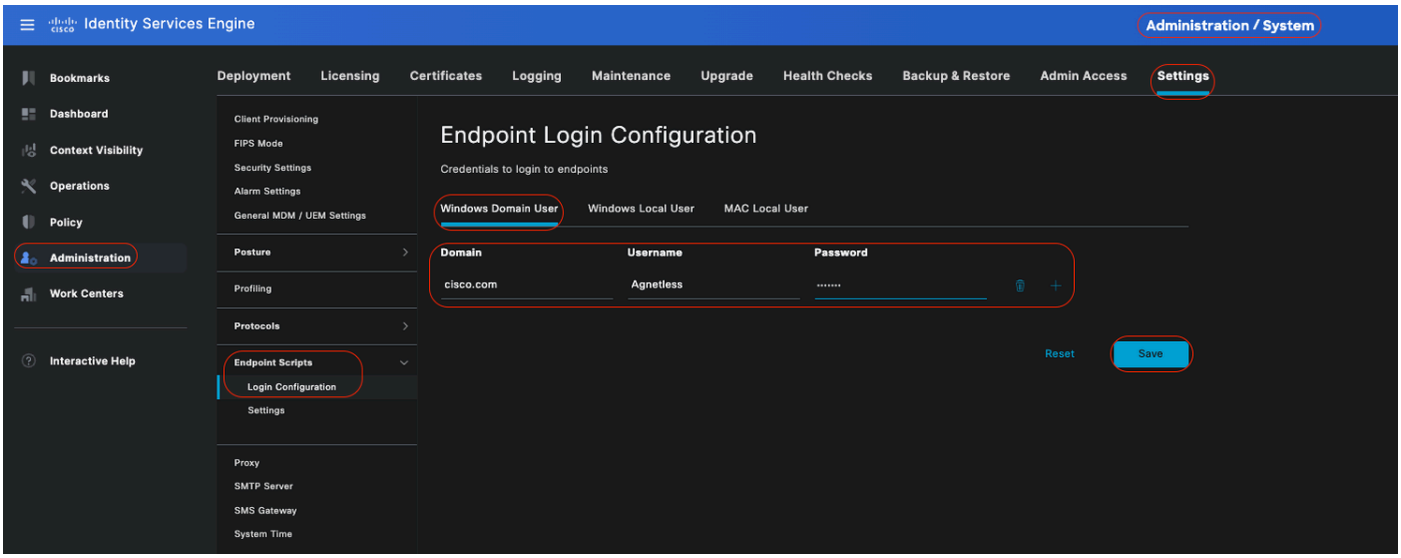
**

- Utilisateur du domaine Windows :

Configurez les identifiants de domaine que Cisco ISE doit utiliser pour se connecter à un client via SSH. Cliquez sur l'icône Plus et entrez autant de connexions Windows que nécessaire. Pour chaque domaine, entrez les valeurs requises dans les champs Domaine, Nom d'utilisateur, et Mot de passe. Si vous configurez des informations d'identification de domaine, les informations d'identification de l'utilisateur local configurées dans l'onglet Utilisateur local Windows sont ignorées.

Si vous administrez des terminaux Windows qui utilisent une évaluation de la position sans agent via un domaine Active Directory, assurez-vous de fournir le nom de domaine ainsi que les

informations d'identification possédant des privilèges d'administration locale.

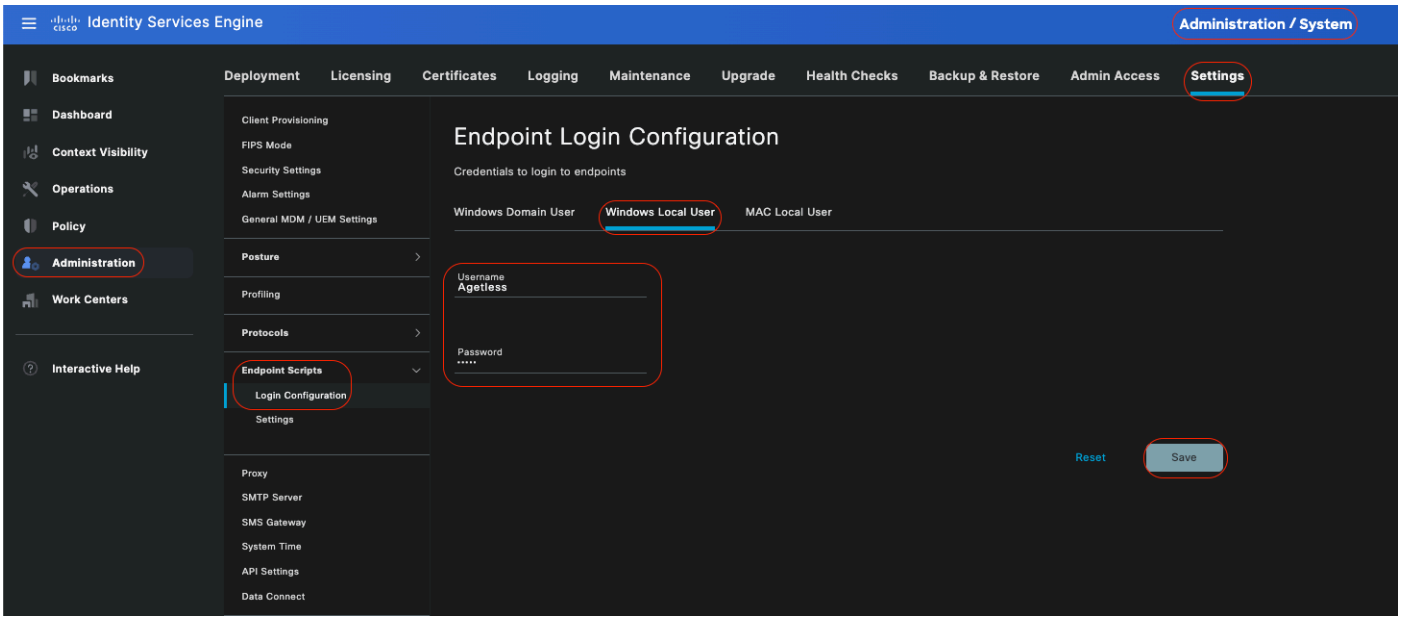


Utilisateur du domaine Windows

- Utilisateur local Windows :

Configurez le compte local que Cisco ISE utilise pour accéder au client via SSH. Le compte local doit pouvoir exécuter Powershell et Powershell à distance.

Si vous n'administrez pas de terminaux Windows qui utilisent une évaluation de la position sans agent via un domaine Active Directory, assurez-vous de fournir des informations d'identification disposant de privilèges d'administration locale.



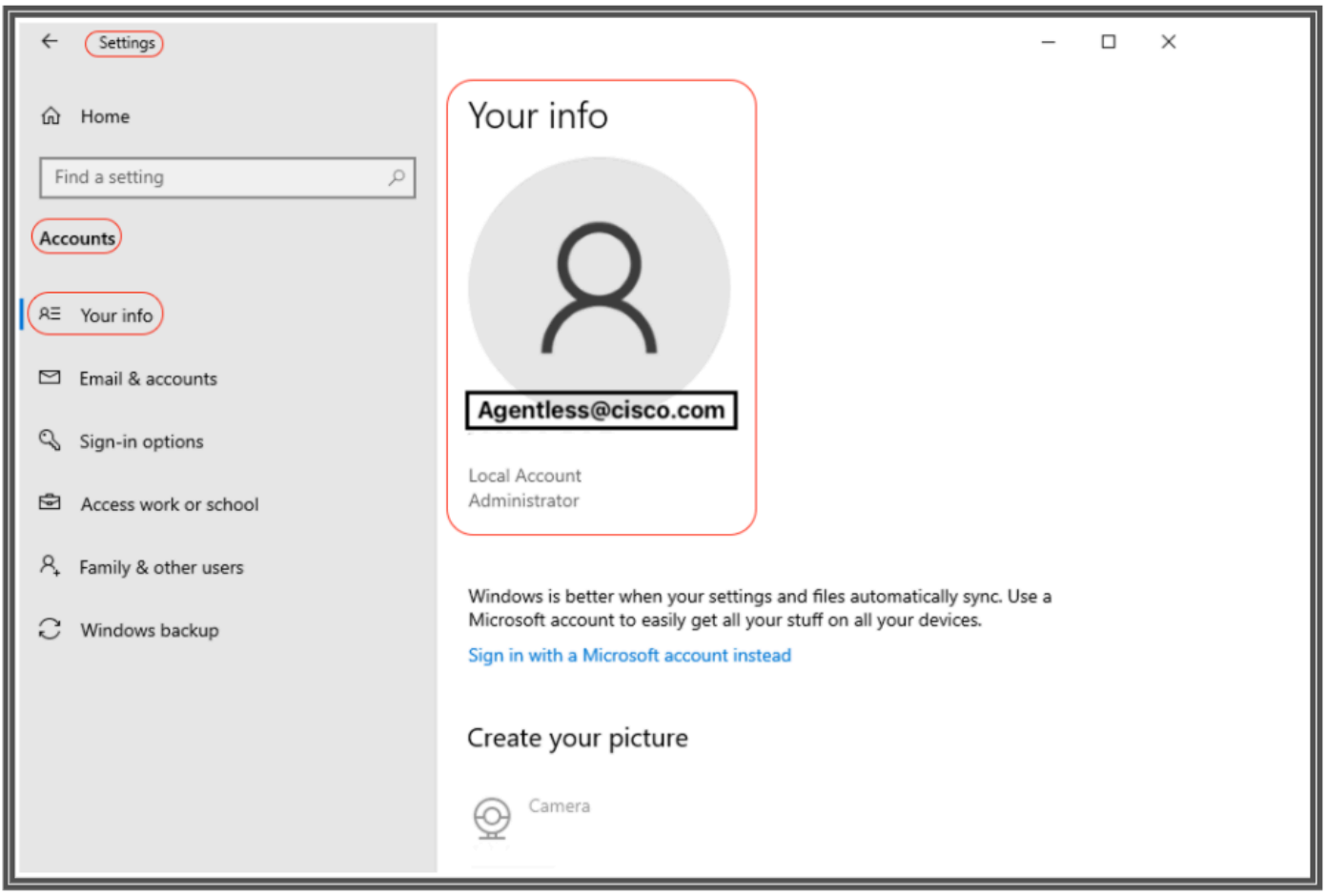
Utilisateur local Windows

Vérifier les comptes

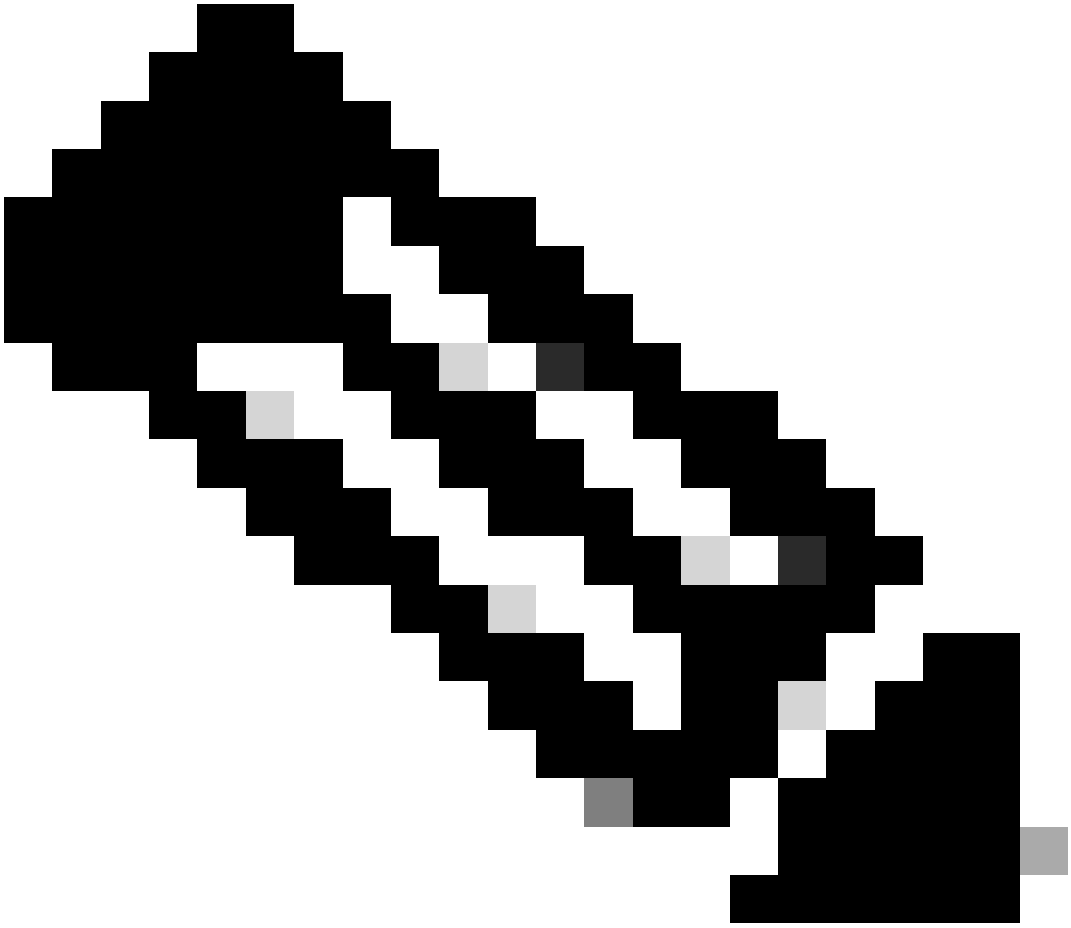
Pour vérifier vos comptes d'utilisateur de domaine Windows et vos comptes d'utilisateur local Windows afin de pouvoir ajouter avec précision les données appropriées sous Informations

d'identification et de connexion du point de terminaison, procédez comme suit :

Utilisateur local Windows : Utilisation de l'interface graphique utilisateur (application Paramètres) Cliquez sur le bouton WindowsStart, sélectionnez Settings (l'icône d'engrenage), cliquez sur Accounts, puis sélectionnez Your info :



Vérifier les comptes



Remarque : Pour MacOS, vous pouvez vous référer à MAC Local User. Cependant, dans cet exemple de configuration, vous ne verrez pas la configuration MacOS.

- Utilisateur local MAC : Configurez le compte local que Cisco ISE utilise pour accéder au client via SSH. Le compte local doit pouvoir exécuter Powershell et Powershell à distance. Dans le champ Nom d'utilisateur, saisissez le nom de compte du compte local.

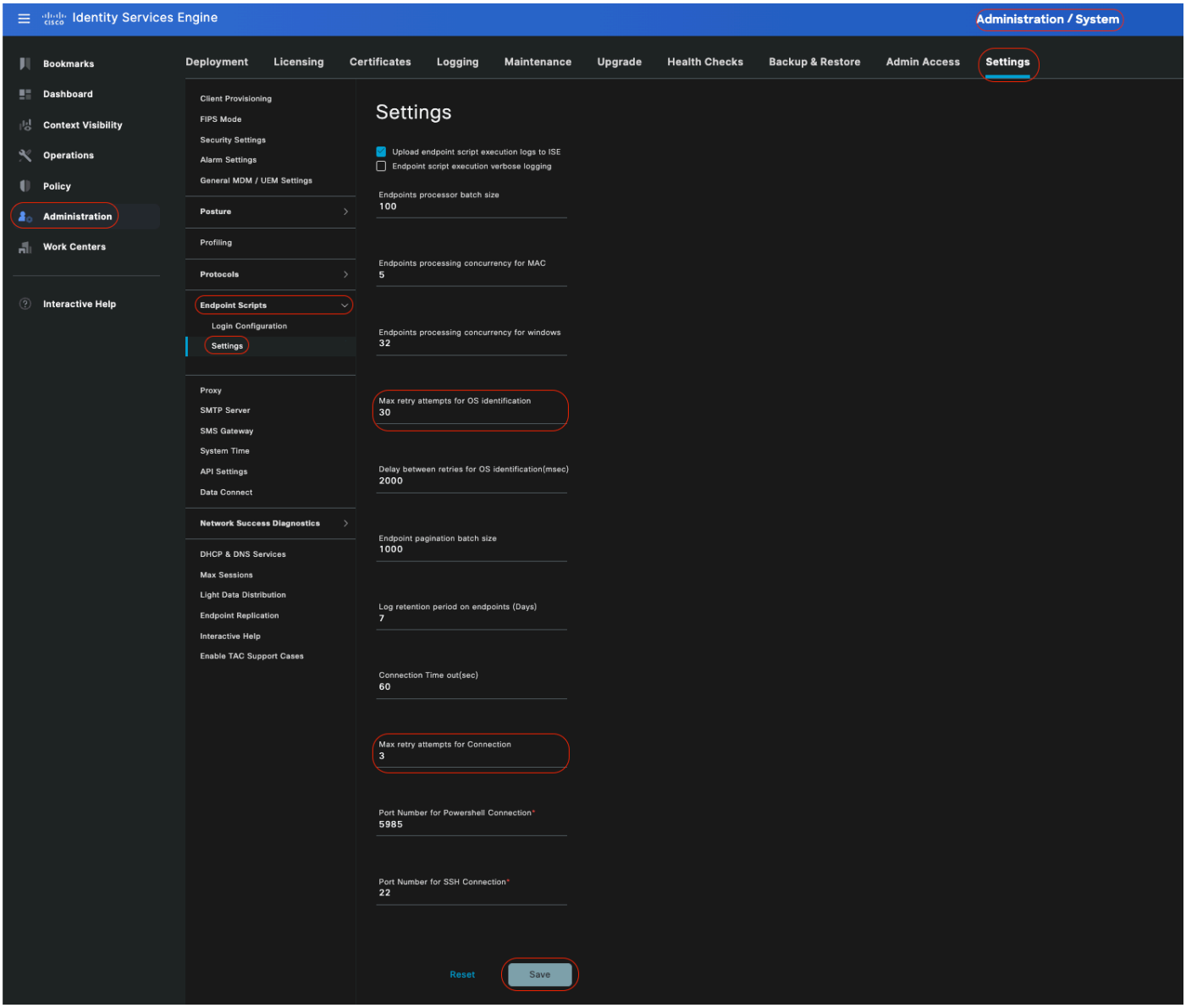
Pour afficher un nom de compte Mac OS, exécutez cette commande`whoami`dans le Terminal :

Paramètres

Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ( ) et choisissez Administration > Settings > Endpoint Scripts > Settings, et configureMax retry

attempts for OS identification,Delay between retries for OS identification et ainsi de suite. Ces paramètres déterminent la rapidité de confirmation des problèmes de connectivité. Par exemple, une erreur indiquant que le port PowerShell n'est pas ouvert s'affiche dans les journaux uniquement une fois que toutes les tentatives ne sont pas épuisées.

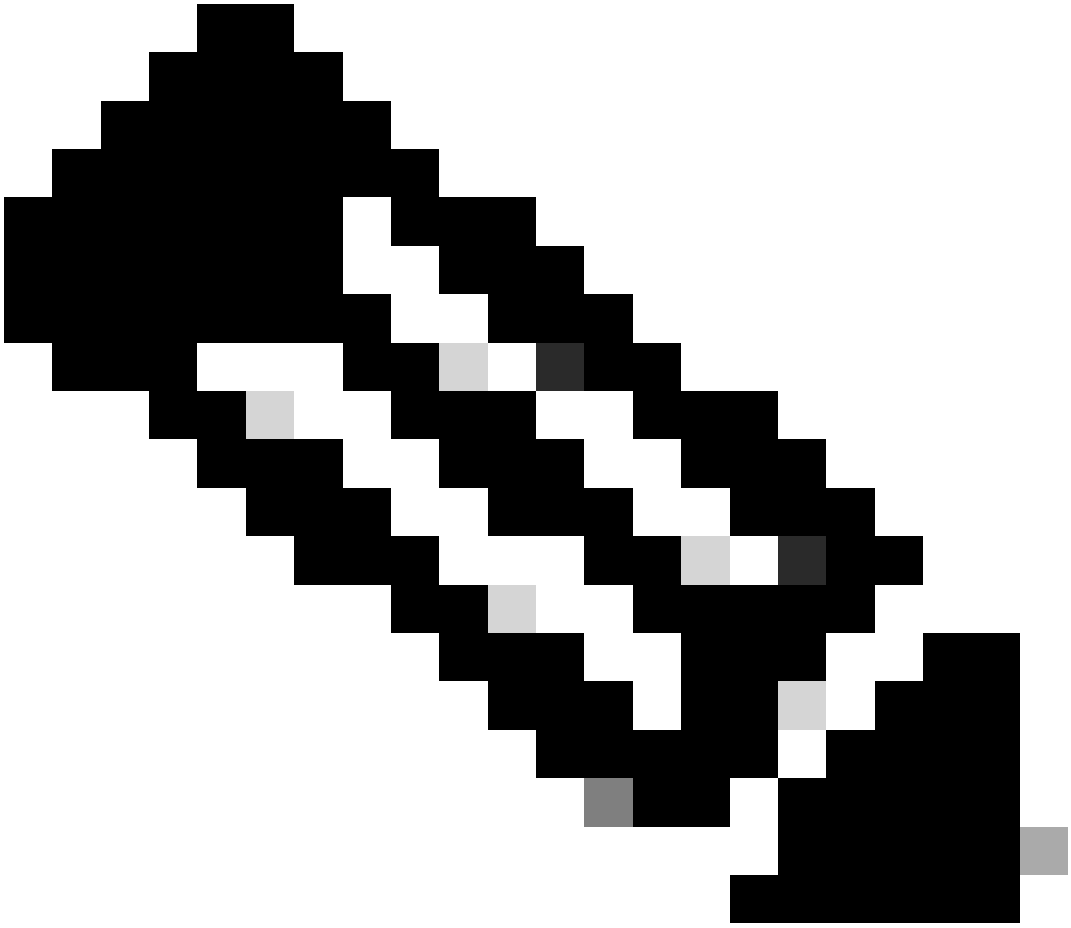
Cette capture d'écran présente les paramètres de valeur par défaut :



Paramètres de script Endpoint

Lorsque les clients se connectent avec une posture sans agent, vous pouvez les voir dans les journaux en direct.

Configuration et dépannage de Windows Endpoint



Remarque : Voici quelques recommandations à vérifier et à appliquer sur votre périphérique Windows ; cependant, vous devez consulter la documentation Microsoft ou contacter le support technique de Microsoft si vous rencontrez des problèmes tels que les privilèges utilisateur, l'accès PowerShell, etc.

Vérification et dépannage des conditions préalables

Test de la connexion TCP au port 5985

Pour les clients Windows, le port 5985 permettant d'accéder à powershell sur le client doit être ouvert. Exécutez cette commande pour confirmer la connexion TCP au port 5985 : **Test-NetConnection -ComputerName localhost -Port 5985**

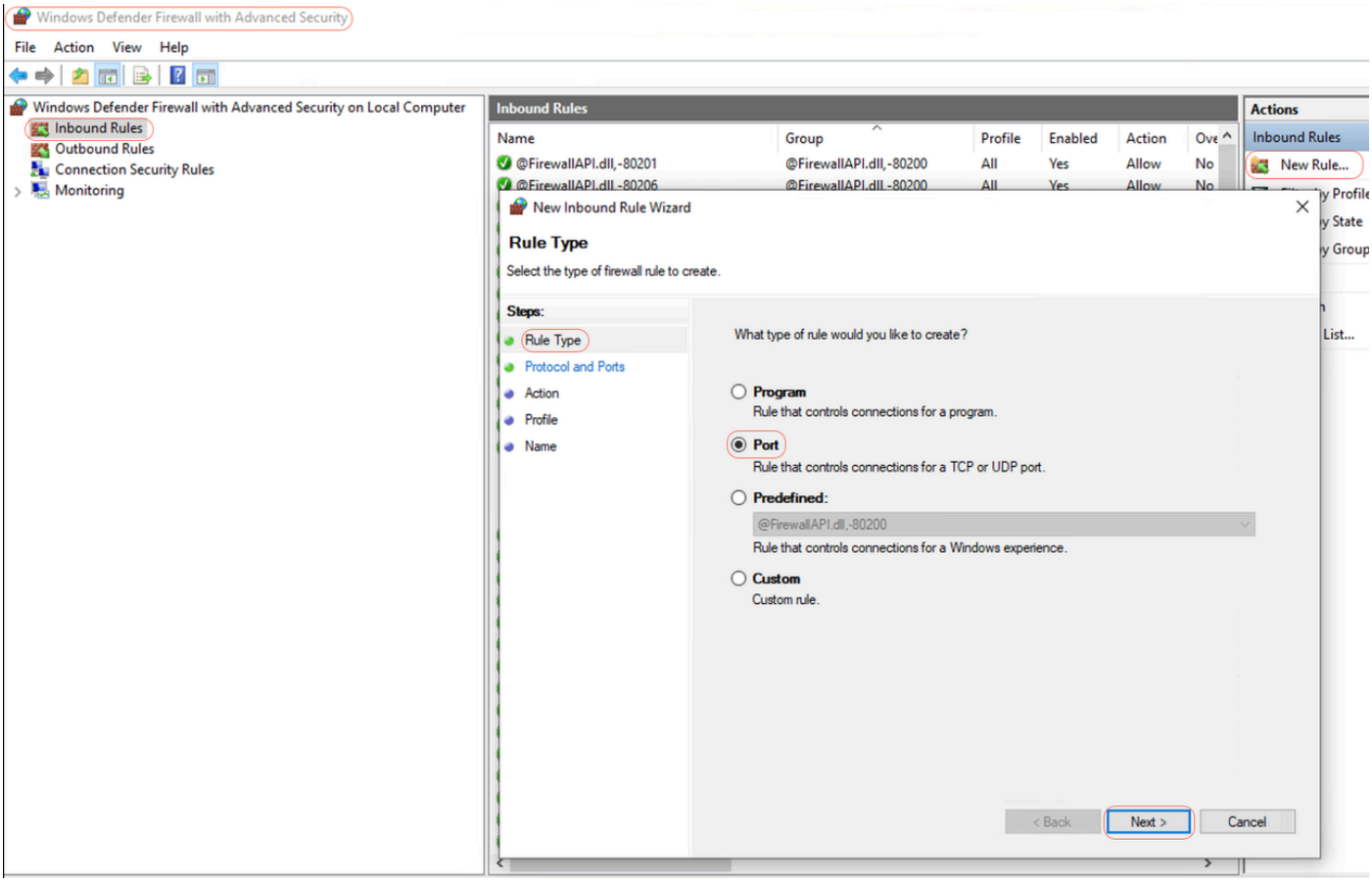
Le résultat affiché dans cette capture d'écran indique que la connexion TCP au port 5985 sur localhost a échoué. Cela signifie que le service WinRM (Gestion à distance de Windows), qui utilise le port 5985, n'est pas en cours d'exécution ou n'est pas correctement configuré.

```
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

Création d'une règle entrante pour autoriser PowerShell sur le port 5985

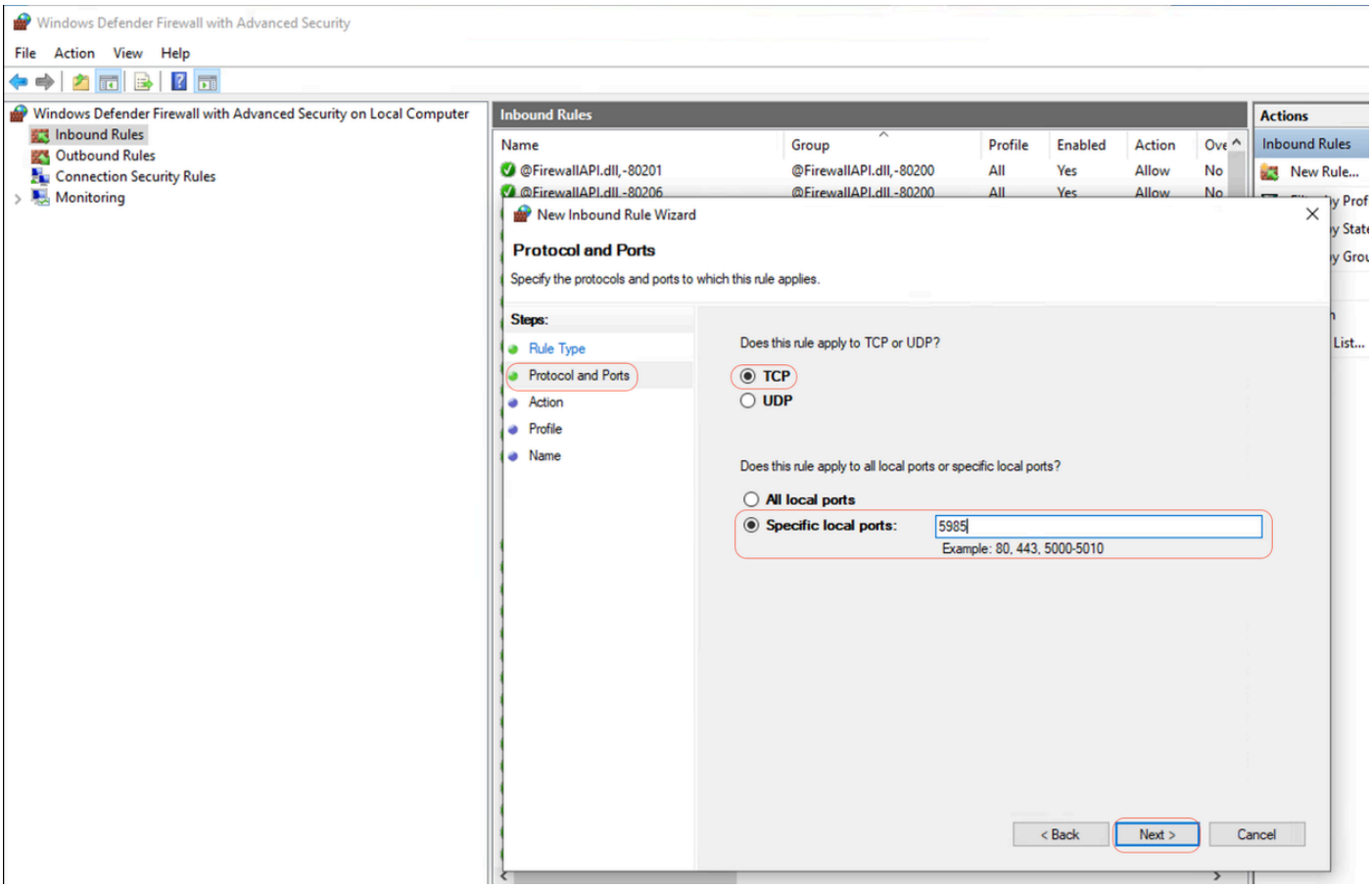
Étape 1 : dans l'interface graphique utilisateur de Windows, accédez à la barre de recherche, tapez Pare-feu Windows avec sécurité avancée, cliquez dessus et sélectionnez Exécuter en tant qu'administrateur > Règles entrantes > Nouvelle règle > Type de règle > Port > Suivant :



Nouvelle règle de trafic entrant - Port

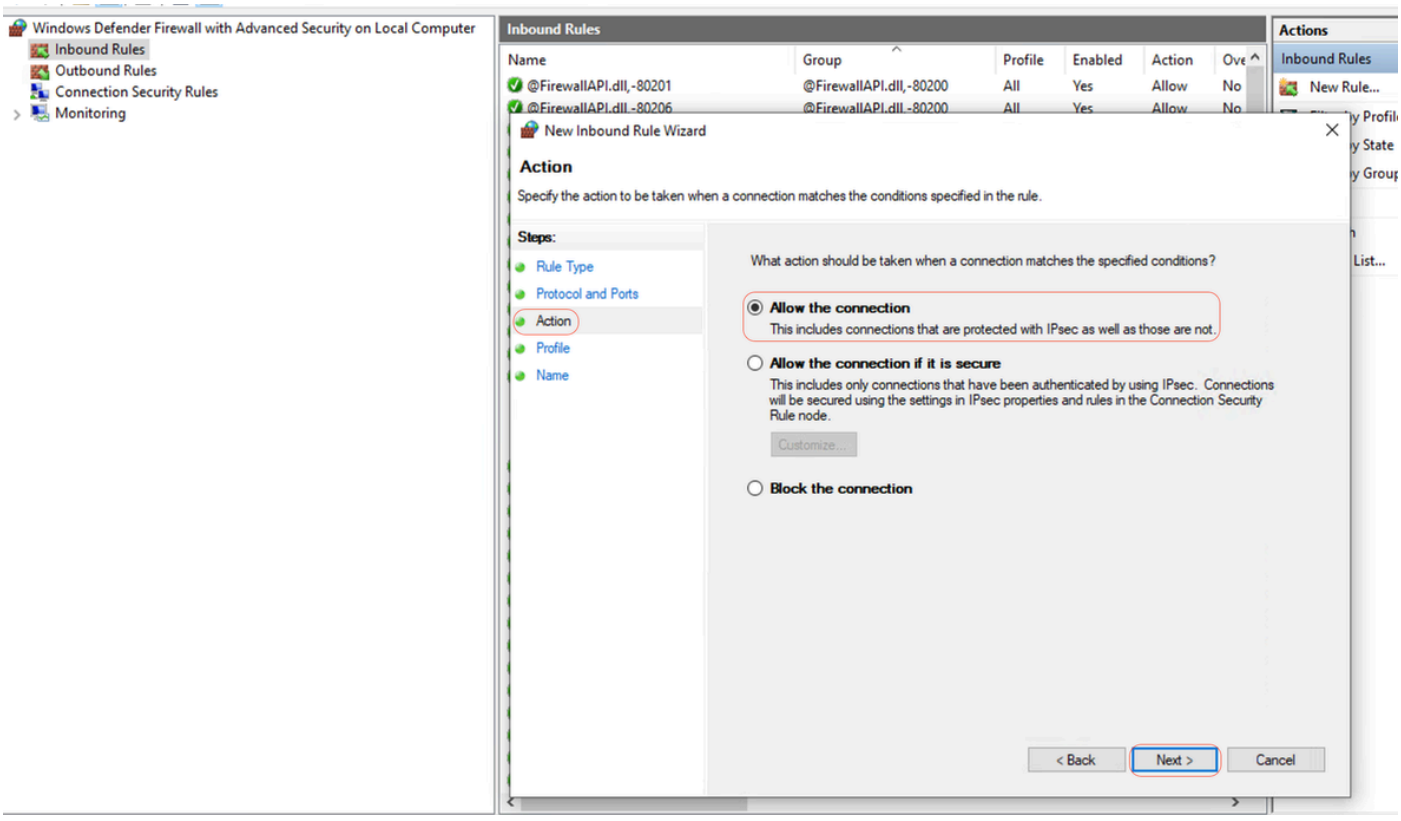
Étape 2 : sous Protocoles et ports, sélectionnez TCP et Spécifier les ports locaux, tapez le

numéro de port 5985 (Port par défaut pour l'accès à distance PowerShell) et cliquez sur Suivant :



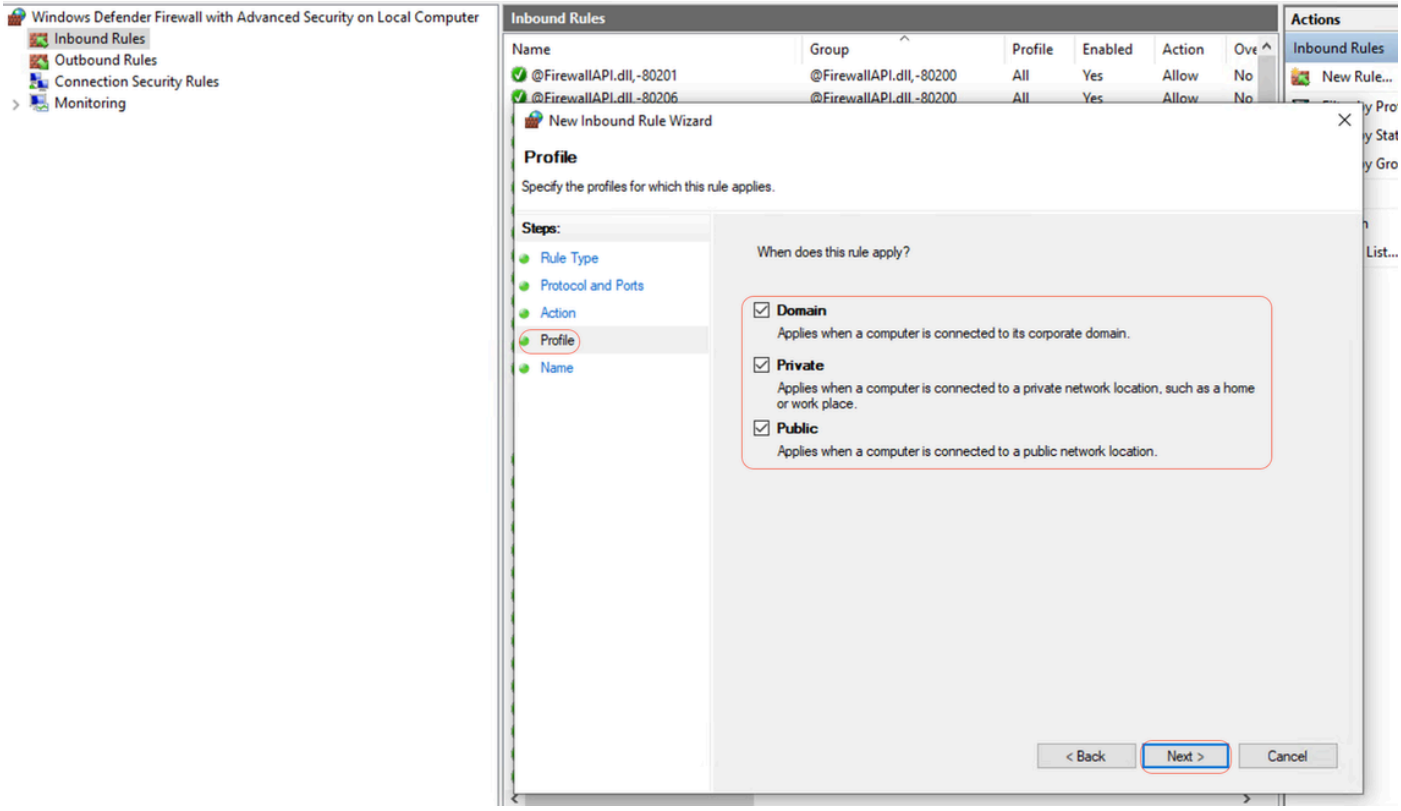
Protocoles et ports

Étape 3 - Sous Action > Sélectionnez Allow the connection > Next:



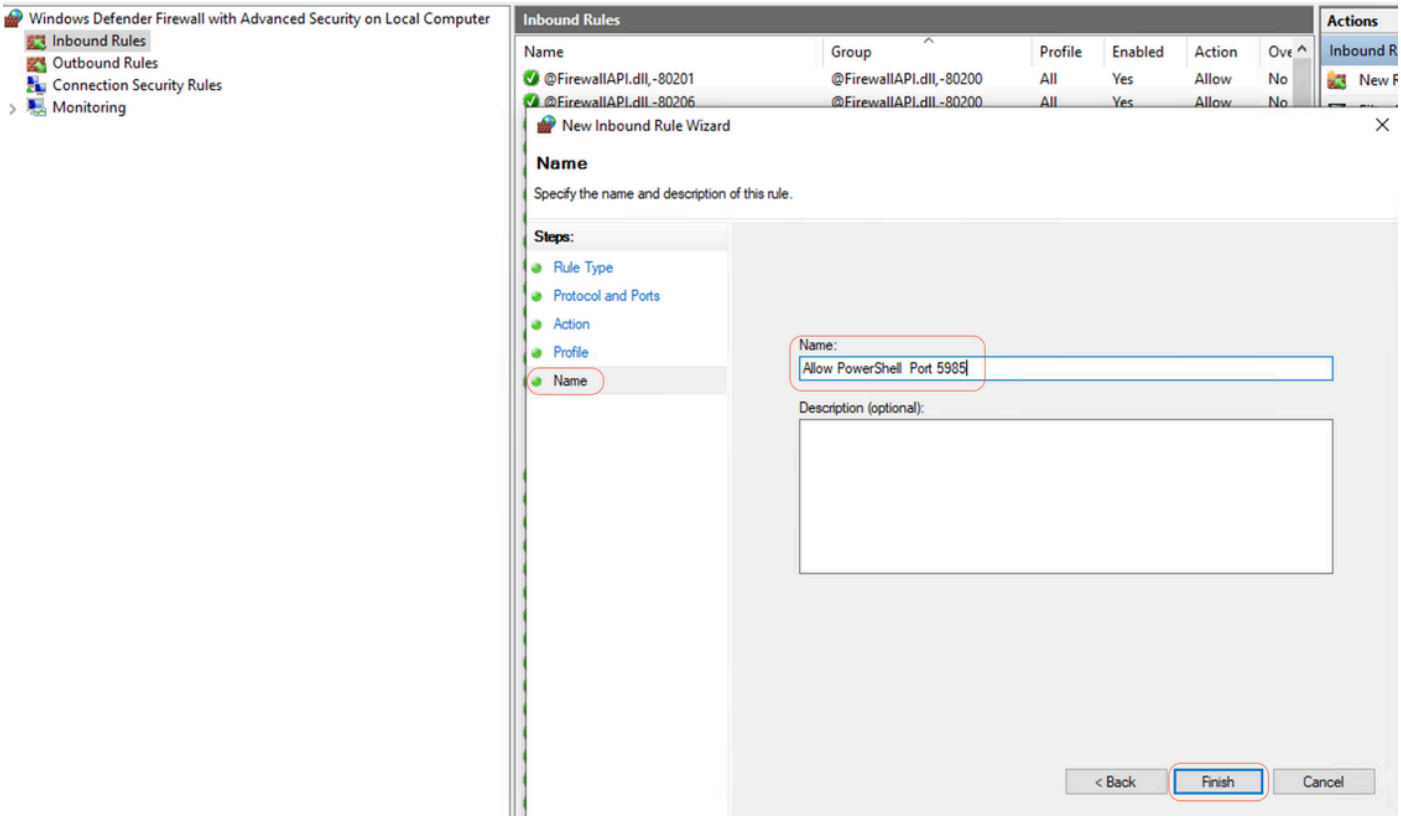
Action

Étape 4 - Sous Profil, cochez les cases Domaine, Privé et Public et cliquez sur Suivant :



Profil

Étape 5 - Sous Nom, entrez le nom de la règle, par exemple Autoriser PowerShell sur le port 5985 et cliquez sur Terminer :

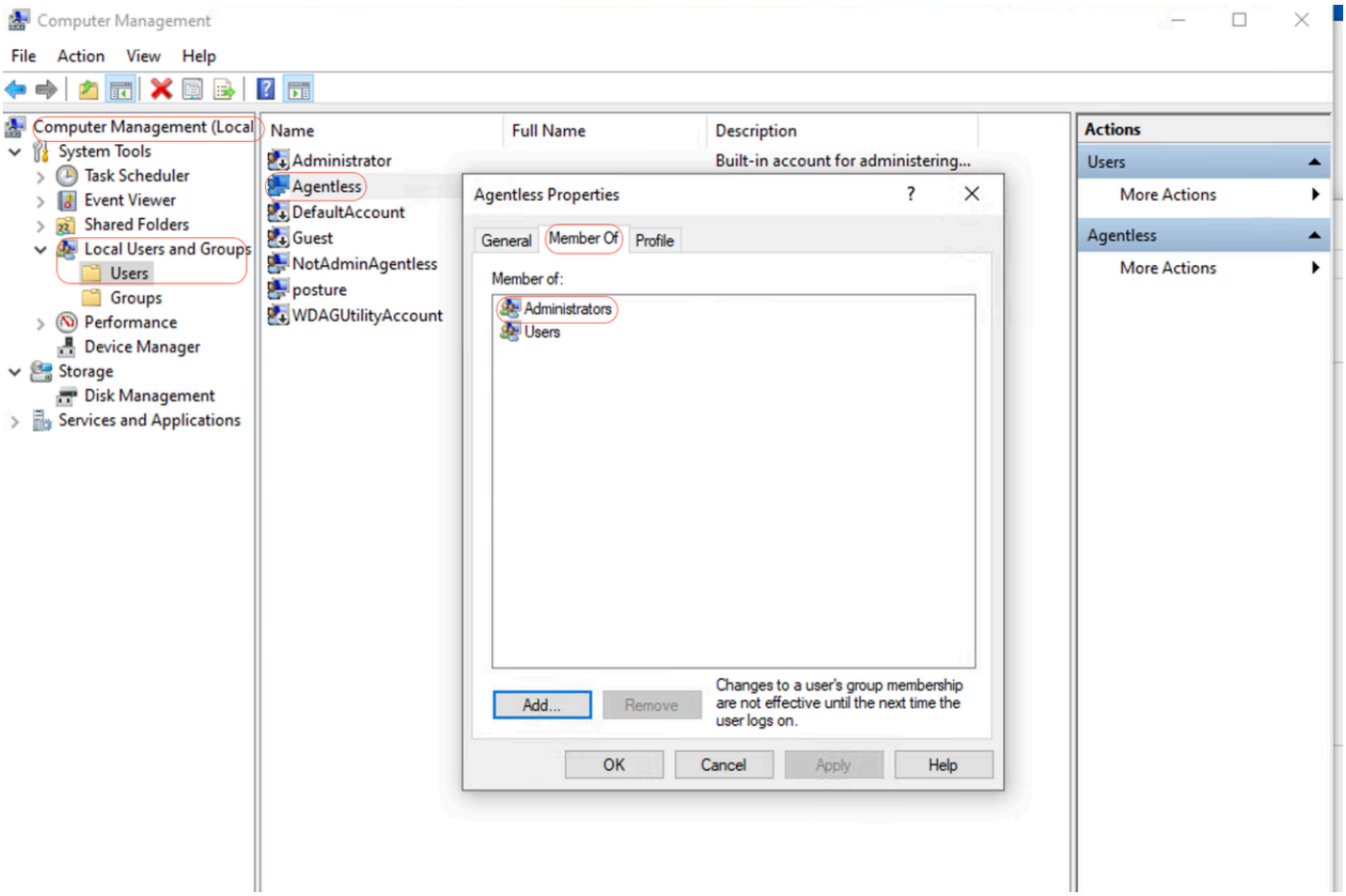


Nom

Les informations d'identification du client pour la connexion shell doivent avoir des privilèges d'administrateur local

Les informations d'identification du client pour la connexion à l'interpréteur de commandes doivent avoir des privilèges d'administrateur local. Pour vérifier si vous avez des privilèges d'administrateur, procédez comme suit :

Dans l'interface utilisateur graphique de Windows, accédez à Paramètres > Gestion de l'ordinateur > Utilisateurs et groupes locaux > Utilisateurs > Sélectionnez le compte d'utilisateur (dans cet exemple, le compte sans agent est sélectionné) > Membre de, le compte doit avoir Administrateurs Groupe.



Privilèges d'administration locale

Validation de l'écouteur WinRM

Assurez-vous que l'écouteur WinRM est configuré pour HTTP sur le port 5985 :

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

Activer WinRM PowerShell à distance

Assurez-vous que le service est en cours d'exécution et configuré pour démarrer automatiquement, procédez comme suit :

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**

Résultat attendu :

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 doit être v7.1 ou ultérieure. Le client doit disposer de cURL v7.34 ou ultérieure :

Comment vérifier les versions PowerShell et cURL sur Windows

Vous assurer que vous utilisez les versions appropriées de PowerShell ; cURL est essentiel pour Posture Agentless :

Vérification de la version PowerShell

Sous Windows :

1. Ouvrez PowerShell :

· Appuyez sur Win + X et sélectionnez Windows PowerShell ou Windows PowerShell (Admin).

2.Exécutez la commande suivante :$PSVersionTable.PSVersion

· Cette commande affiche les détails de version de PowerShell installé sur votre système.

Vérification de la version cURL

Sous Windows :

1. Ouvrir l'invite de commandes :

· Appuyez sur Win + R, tapez cmd, puis cliquez sur Entrée.

2. Exécutez la commande : curl --version

· Cette commande affiche la version de cURL installée sur votre système.

Résultats de la vérification des versions PowerShell et cURL sur les périphériques 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>

Configuration supplémentaire

Cette commande configure votre ordinateur pour faire confiance à des hôtes distants spécifiques pour les connexions WinRM : Set-Item WSMan:\localhost\Client\TrustedHosts -Value

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

L'applet de commande test-wsman avec les paramètres -Authentication Negotiate et -Credential est un outil puissant pour vérifier la disponibilité et la configuration du service WinRM sur un ordinateur distant : test-wsman

-Authentication Negotiate -Credential

MacOS

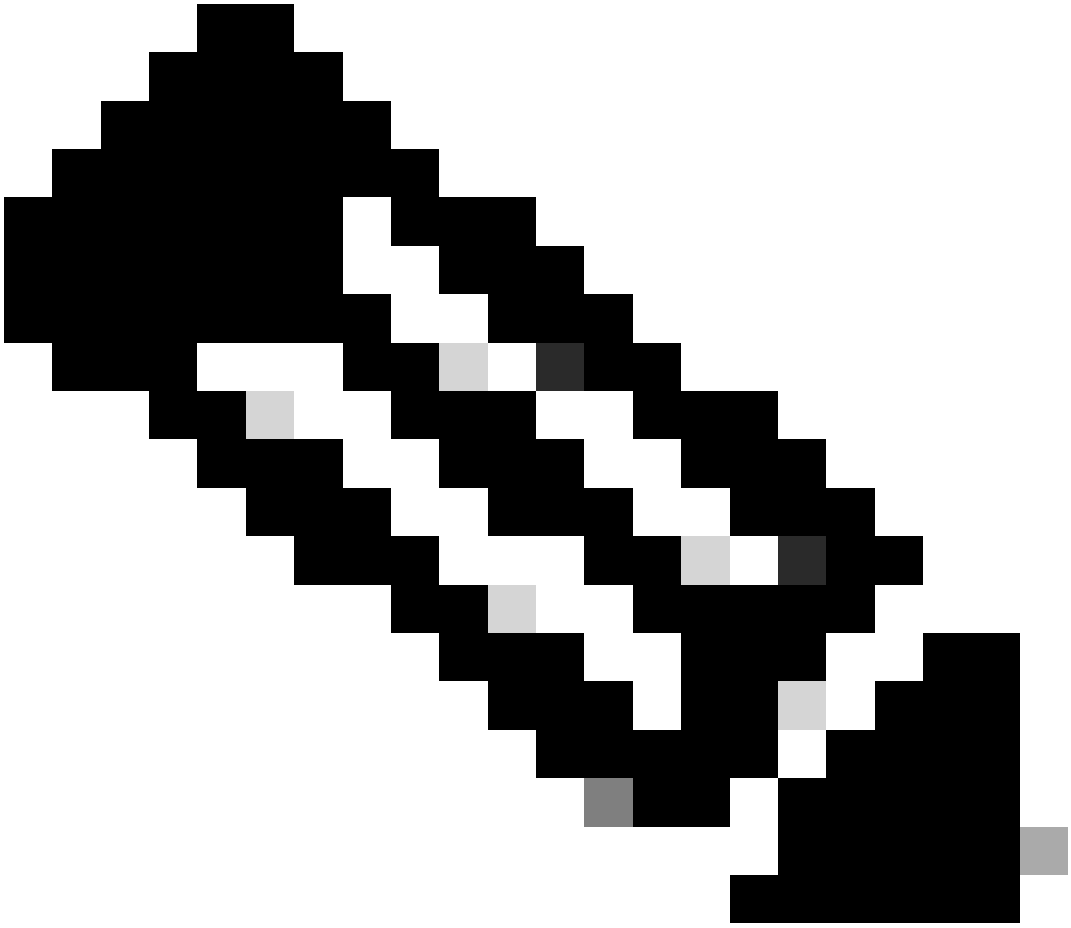
Powershell doit être v7.1 ou ultérieure. Le client doit disposer de cURL v7.34 ou ultérieure :

Sur macOS :

1. Ouvrir le terminal :

· Vous pouvez trouver Terminal dans Applications > Utilities.

2. Exécutez la commande : pwsh -Command '$PSVersionTable.PSVersion'



Remarque : Remarque : · Assurez-vous que PowerShell Core (pwsh) est installé. Si ce n'est pas le cas, vous pouvez l'installer via Homebrew (assurez-vous d'avoir installé Himebrew) : `brew install --cask powershell`

Sur macOS :

1. Ouvrir le terminal :

· Vous pouvez trouver Terminal dans Applications > Utilities.

2. Exécutez la commande : `curl --version`

· Cette commande doit afficher la version de cURL installée sur votre système.

Pour les clients MacOS, le port 22 pour accéder à SSH doit être ouvert pour accéder au client

Guide pas à pas :

1. Préférences système ouvertes :

· Accédez à Préférences système à partir du menu Apple.

2. Activer la connexion à distance :

· Accédez à Partage.

· Cochez la case en regard de Connexion à distance.

· Assurez-vous que l'option Autoriser l'accès pour est définie sur les utilisateurs ou les groupes appropriés. La sélection de Tous les utilisateurs permet à tout utilisateur ayant un compte valide sur le Mac de se connecter via SSH.

3. Vérifiez les paramètres du pare-feu :

· Si le pare-feu est activé, vous devez vous assurer qu'il autorise les connexions SSH.

· Accédez à Préférences système > Sécurité et confidentialité > Pare-feu.

· Cliquez sur le bouton Options de pare-feu.

· Vérifiez que Remote Login ou SSH est répertorié et autorisé. S'il n'est pas répertorié, cliquez sur le bouton Add (+) pour l'ajouter.

4. Ouvrez le port 22 via le terminal (si nécessaire) :

· Ouvrez l'application Terminal à partir de Applications > Utilities.

· Utilisez la commande pfctl pour vérifier les règles de pare-feu actuelles et vous assurer que le port 22 est ouvert : sudo pfctl -sr | grep 22

· Si le port 22 n'est pas ouvert, vous pouvez ajouter manuellement une règle pour permettre à SSH:echo "de passer dans le protocole TCP de n'importe quel port à n'importe quel port 22" | sudo pfctl -ef -

5. Testez l'accès SSH :

· À partir d'un autre périphérique, ouvrez un terminal ou un client SSH.

· Essayez de vous connecter au client macOS à l'aide de son adresse IP : ssh username@<macOS-client-IP>

· Remplacez username par le compte utilisateur approprié et <macOS-client-IP> par l'adresse IP du client macOS.

Pour MacOS, assurez-vous que cette entrée est mise à jour dans le fichier sudoers pour éviter l'échec de l'installation du certificat sur les terminaux :

Lors de la gestion des terminaux macOS, il est essentiel de s'assurer que des commandes d'administration spécifiques peuvent être exécutées sans demander de mot de passe.

Conditions préalables

· Accès administrateur sur la machine macOS.

· Connaissance de base des commandes du terminal.

Étapes de mise à jour du fichier Sudoers

1. Ouvrir le terminal :

· Vous pouvez trouver Terminal dans Applications > Utilities.

2. Modifier le fichier Sudoers :

· Utilisez la commande visudo pour modifier le fichier sudoers en toute sécurité. Cela garantit que toutes les erreurs de syntaxe sont détectées avant d'enregistrer le fichier.sudo visudo

· Vous serez invité à saisir votre mot de passe administrateur.

3. Trouvez la section appropriée :

· Dans l'éditeur de visuels, naviguez jusqu'à la section où les règles spécifiques à l'utilisateur sont définies. Généralement, c'est vers le bas du fichier.

4. Ajoutez l'entrée requise :

· Ajoutez cette ligne pour accorder à l'utilisateur spécifié l'autorisation d'exécuter les commandes security et osascript sans mot de passe :

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

· Remplacez **<macadminusername>** par le nom d'utilisateur réel de l'administrateur macOS.

5. Enregistrer et quitter :

· Si vous utilisez l'éditeur par défaut (nano), appuyez sur Ctrl + X pour quitter, puis appuyez sur Y pour confirmer les modifications, et enfin appuyez sur Entrée pour enregistrer le fichier.

· Si vous utilisez vi ou vim, appuyez sur Esc, tapez : wq, puis appuyez sur Entrée pour effectuer l'enregistrement et quitter l'application.

6. Vérifiez les modifications :

· Pour vous assurer que les modifications ont pris effet, vous pouvez exécuter une commande qui nécessite les autorisations sudo mises à jour. Exemple :

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

· Ces commandes peuvent être exécutées sans demander de mot de passe.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.