Agentenloser Status konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Posture Agentless in ISE konfiguriert wird und was auf dem Endpunkt erforderlich ist, um Agentless Script auszuführen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE).
- Status:
- PowerShell und SSH
- Windows 10 oder höher

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine (ISE) 3.3 Version
- Paket CiscoAgentlessWindows 5.1.6.6
- Windows 10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der ISE-Status führt eine clientseitige Bewertung durch. Der Client erhält die Statusanforderungsrichtlinie von der ISE, führt die Statusdatenerfassung durch, vergleicht die Ergebnisse mit der Richtlinie und sendet die Bewertungsergebnisse zurück an die ISE.

Anhand des Statusberichts kann die ISE dann feststellen, ob das Gerät den Richtlinien entspricht oder nicht.

Agentenloser Status ist eine der Statusmethoden, die Statusinformationen von Clients sammelt und sich nach Abschluss automatisch entfernt, ohne dass der Endbenutzer eine Aktion ausführt. Agentenloser Status stellt über Administratorberechtigungen eine Verbindung zum Client her.

Erste Schritte

Voraussetzungen:

- Der Client muss über seine IPv4- oder IPv6-Adresse erreichbar sein, und diese IP-Adresse

muss in der RADIUS-Accounting-Funktion verfügbar sein.

- Der Client muss von der Cisco Identity Services Engine (ISE) über seine IPv4- oder IPv6-Adresse erreichbar sein. Außerdem muss diese IP-Adresse in der RADIUS-Accounting verfügbar sein.
- Windows- und Mac-Clients werden derzeit unterstützt:
    - Für Windows-Clients muss der Port 5985 für den Zugriff auf Powershell auf dem Client geöffnet sein. PowerShell muss v7.1 oder höher sein. Der Client muss über cURL v7.34 oder höher verfügen.
    - Für MacOS-Clients muss Port 22 für den Zugriff auf SSH offen sein, damit auf den Client zugegriffen werden kann. Der Client muss über cURL v7.34 oder höher verfügen.
- Die Client-Anmeldeinformationen für die Shell-Anmeldung müssen über lokale Administratorberechtigungen verfügen.
- Führen Sie das Statusfeed-Update aus, um die neuesten Clients zu erhalten, wie in den Konfigurationsschritten beschrieben. Bitte überprüfen Sie:
- Stellen Sie für MacOS sicher, dass dieser Eintrag in der sudoers-Datei aktualisiert wird, um einen Fehler bei der Zertifikatinstallation auf den Endpunkten zu vermeiden: Überprüfen Sie:

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

•

Für MacOS muss das konfigurierte Benutzerkonto ein Administratorkonto sein. Der agentenlose Status für MacOS funktioniert nicht mit anderen Kontotypen, selbst wenn Sie mehr Berechtigungen gewähren.Um dieses Fenster anzuzeigen, klicken Sie auf das Menuicon (

) und **wählen Sie Administration > System > Settings > Endpoint Scripts** > Login **Configuration > MAC Local User (Administration > System > Einstellungen > Endpunktskripte** > Anmeldungskonfiguration > **Lokaler Benutzer) aus.**

-

Wenn sich die portbezogenen Aktivitäten auf Windows-Clients aufgrund von Updates von Microsoft ändern, müssen Sie den Workflow für die Konfiguration des Agentenstatus für Windows-Clients neu konfigurieren.

Unterstützte Statusbedingungen

-

Dateibedingungen, mit Ausnahme der Bedingungen, die die Dateipfade USER_DESKTOP und USER_PROFILE verwenden

-

Dienstbedingungen, außer System Daemon- und Daemon- oder Benutzer-Agent-Prüfungen in MacOS

-

Anwendungsbedingungen

- Bedingungen für externe Datenquellen
- Zusammengesetzte Bedingungen
- Anti-Malware-Bedingungen
- Patch-Verwaltungsbedingung, mit Ausnahme **der** Prüfungen **"Enabled**" und "UpToDate"
- Firewall-Bedingungen
- Bedingungen für die Festplattenverschlüsselung, mit Ausnahme der auf dem Verschlüsselungsspeicherort basierenden Bedingungsprüfung
- Registrierungsbedingungen, mit Ausnahme der Bedingungen, die HCSK als Stammschlüssel verwenden

Nicht unterstützte Statusbedingungen

- Problembehebung
- Nachfrist
-

Regelmäßige Neubewertung

-

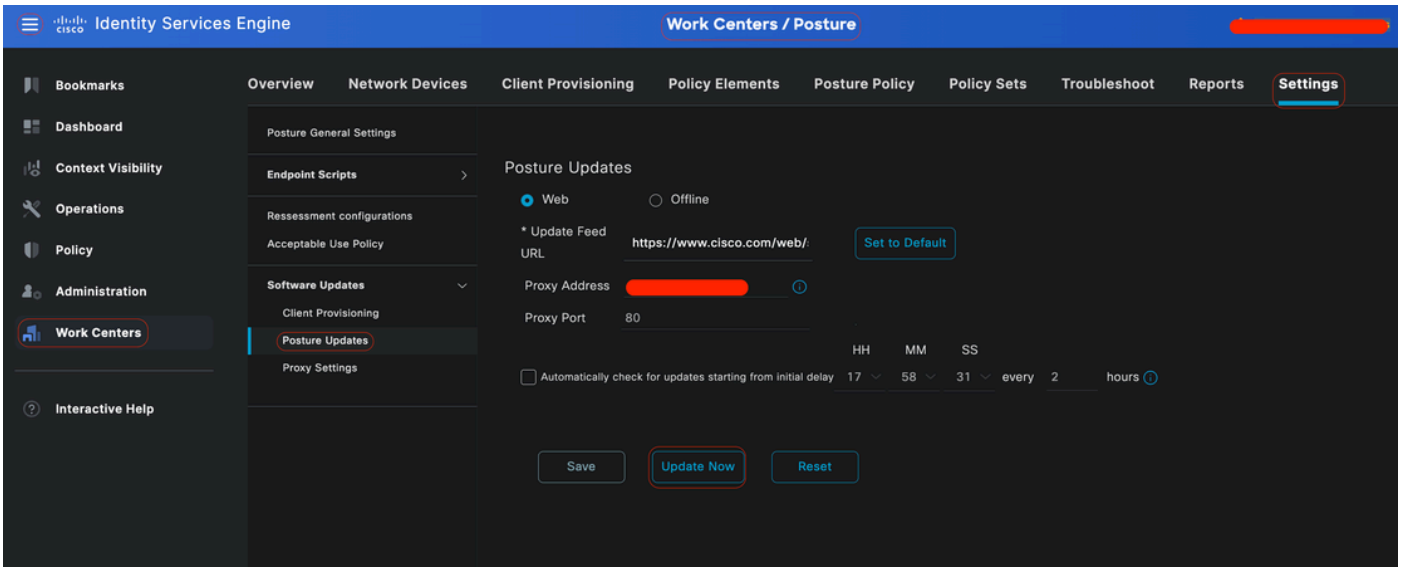
Richtlinie für akzeptable Nutzung

Konfigurieren der ISE

Status-Feed aktualisieren

Es wird empfohlen, den Status-Feed zu aktualisieren, bevor Sie mit der Konfiguration von Status beginnen.

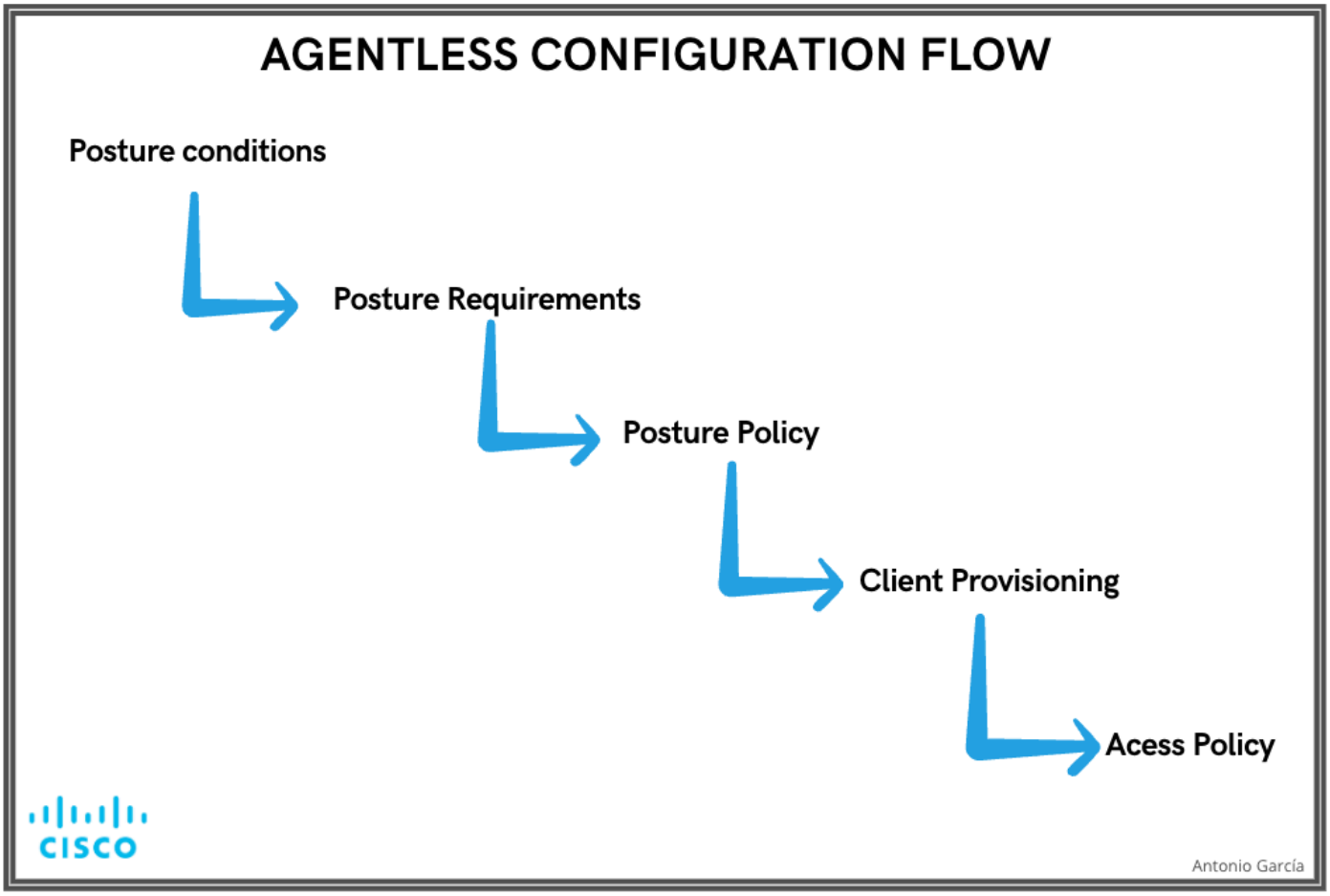
Klicken Sie in der Cisco ISE-GUI auf das Menusymbol ( ), und wählen Sie **Work Centers > Posture > Settings** > **Software Updates** > **Update Now (Work Center > Status** > **Einstellungen** > **Software-Updates** > Jetzt aktualisieren) aus.



Status-Feed aktualisieren

Status Agentenloser Konfigurationsablauf

Status Agentenlos muss der Reihe nach konfiguriert werden, da die erste Konfiguration für die nächste erforderlich ist usw. Behebung ist nicht geplant. Später wird in diesem Dokument jedoch eine Alternative zur Konfiguration von Behebung beschrieben.



Konfigurationsablauf ohne Agent

Agentenlose Statuskonfiguration

Statusbedingung

Statusbedingungen sind die Regeln in unseren Sicherheitsrichtlinien, die einen konformen Endpunkt definieren. Einige dieser Elemente umfassen die Installation einer Firewall, Antivirus-Software, Anti-Malware, Hotfixes, Festplattenverschlüsselung und mehr.

Klicken Sie in der Cisco ISE-GUI auf das Menusymbol (

), wählen Sie **Work Centers > Posture > Policy Elements** > Conditions, klicken Sie auf Add , und erstellen Sie ein oder mehrere Posture **Conditions,** die die Anforderung mithilfe von Agentenloser Posture identifizieren. Klicken Sie nach dem Erstellen der **Bedingung** auf **Speichern**.

In diesem Szenario wurde eine Anwendungsbedingung mit dem Namen **"Agentless_Condition_Application"** mit den folgenden Parametern konfiguriert:

- Betriebssystem: Windows All

Diese Bedingung gilt für alle Versionen des Windows-Betriebssystems und gewährleistet umfassende Kompatibilität für verschiedene Windows-Umgebungen.

- Prüfen nach: Prozess

Das System überwacht die Prozesse innerhalb des Geräts. Sie können entweder **Prozess** oder **Anwendung** auswählen; in diesem Fall wurde **Prozess** ausgewählt.

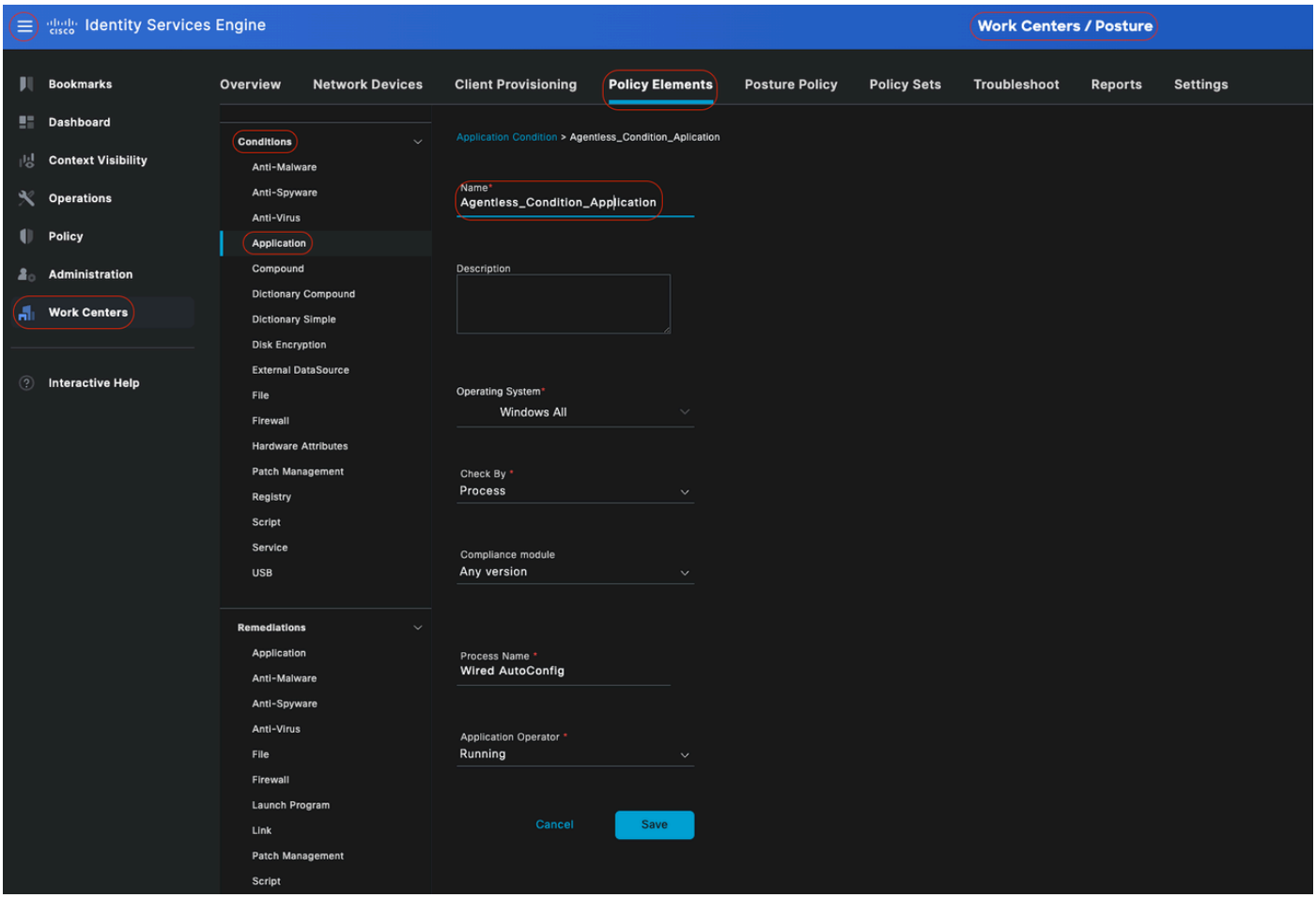
- Prozessname: Kabelgebundene Autokonfiguration

Der **Prozess "Wired AutoConfig**" (Kabelgebundene Autokonfiguration) ist der Prozess, mit dem das Modul das Gerät eincheckt. Dieser Prozess ist für die Konfiguration und das Management von kabelgebundenen Netzwerkverbindungen einschließlich der IEEE 802.1X-Authentifizierung zuständig.

- Anwendungsoperator: Wird ausgeführt

Das Compliance-Modul überprüft, ob der **kabelgebundene AutoConfig**-Prozess derzeit auf dem Gerät ausgeführt wird. Sie können entweder

Running (Wird ausgeführt) oder **Not Running (Wird nicht ausgeführt)** auswählen. In dieser Instanz wurde **Running** ausgewählt, um sicherzustellen, dass der Prozess aktiv ist.



Agentenloser Zustand

Status-Anforderung

Eine Statusanforderung ist ein Satz zusammengesetzter Bedingungen oder nur eine Bedingung, die mit einer Rolle und einem Betriebssystem verknüpft werden kann. Alle Clients, die eine Verbindung mit Ihrem Netzwerk herstellen, müssen die während der Statusüberprüfung erforderlichen Anforderungen erfüllen, um die Netzwerkrichtlinien zu erfüllen.

Klicken Sie in der Cisco ISE-GUI auf das Menü (

), und wählen Sie **Work Centers > Posture** > **Policy Elements** > **Requirement aus**. Klicken Sie auf den **Pfeil nach unten**, und wählen Sie **Insert new Requirement (Neue Anforderung einfügen) aus**, und erstellen Sie eine oder mehrere **PostureRequirement (Statusanforderungen)**, für die Agentenlose Statusüberprüfung verwendet wird. Wenn die **Anforderung** erstellt wurde, klicken Sie auf **Fertig** und dann auf **Speichern**.

In diesem Fall wurde eine Anwendungsanforderung mit dem Namen **"Agentless_Requirement_Application"** mit den folgenden Kriterien konfiguriert:

- Betriebssystem: Windows All

Diese Anforderung gilt für jede Version des Windows-Betriebssystems und stellt sicher, dass sie für alle Windows-Umgebungen gilt.

- Statustyp: Agentenlos

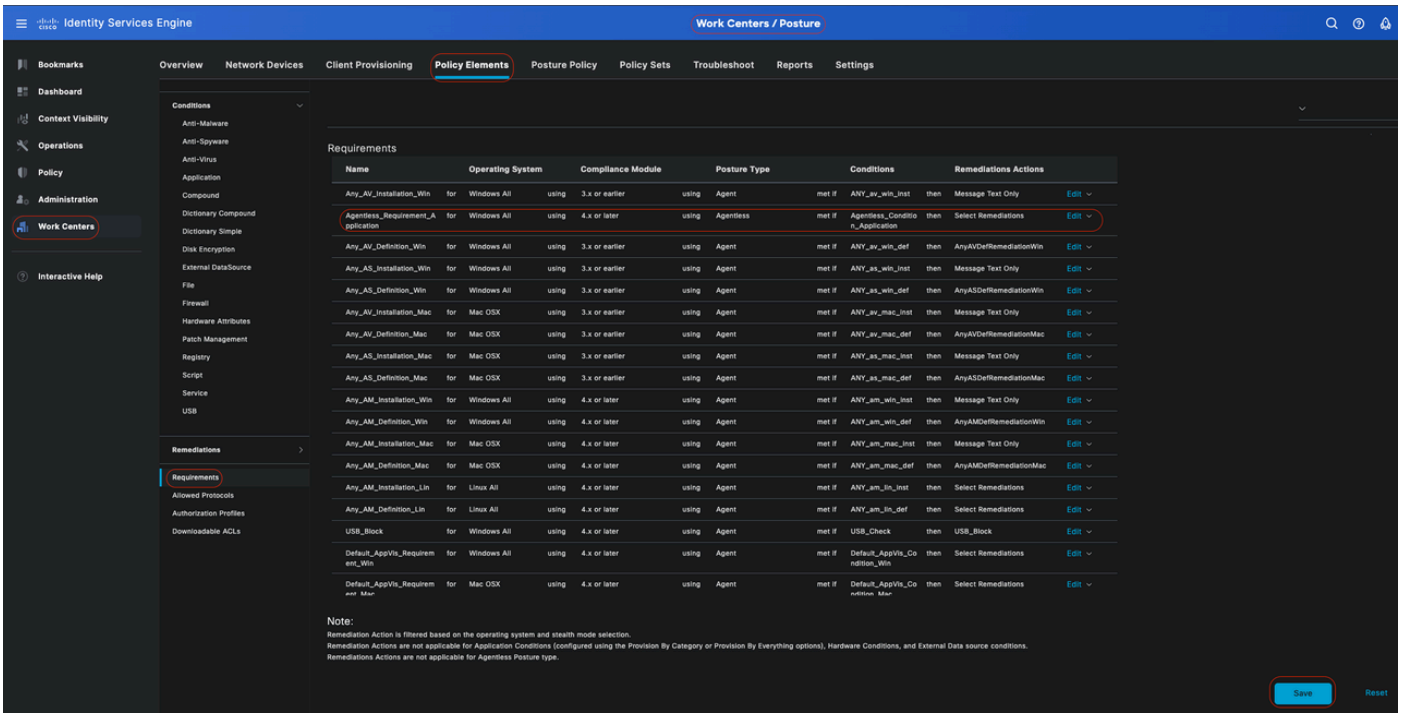
Diese Konfiguration ist für eine agentenlose Umgebung festgelegt. Zu den verfügbaren Optionen gehören **Agent**, **Agent Stealth**, **Temporal Agent** und **Agentless**. In diesem Szenario wurde **Agentenlos** ausgewählt.

- Bedingungen: **Agentless_Condition_Application**

Dies legt die Bedingung fest, die das ISE-Statusmodul und das Compliance-Modul innerhalb der Prozesse des Geräts überprüfen. Die ausgewählte Bedingung ist **Agentless_Condition_Application**.

- Sanierungsmaßnahmen:

Da diese Konfiguration für eine agentenlose Umgebung vorgesehen ist, werden keine Korrekturmaßnahmen unterstützt, und dieses Feld ist abgeblendet.



Agentenlose Anforderung

Statusrichtlinie

Klicken Sie in der Cisco ISE-GUI auf das Menü ( ) und **wählen Sie Work Centers** > **Posture** > **Posture** Policy (**Work Center** > **Posture** > **Posture** Policy). Klicken Sie auf den **Abwärtspfeil,** und wählen Sie **Neue Anforderung einfügen**, und erstellen Sie eine oder mehrere unterstützte **Statusrichtlinien**-Regeln, die Agentenlose Statusinformationen für diese Statusanforderung verwenden. Sobald die **Statusrichtlinie** erstellt wurde, klicken Sie auf **Fertig** und dann auf **Speichern**.

In diesem Szenario wurde eine Statusrichtlinie mit dem Namen **"Agentless_Policy_Application"** mit den folgenden Parametern konfiguriert:

- Regelname: Agentless_Policy_Application

Dies ist der in diesem Konfigurationsbeispiel für die Statusrichtlinie festgelegte Name.

- Betriebssystem: Windows All

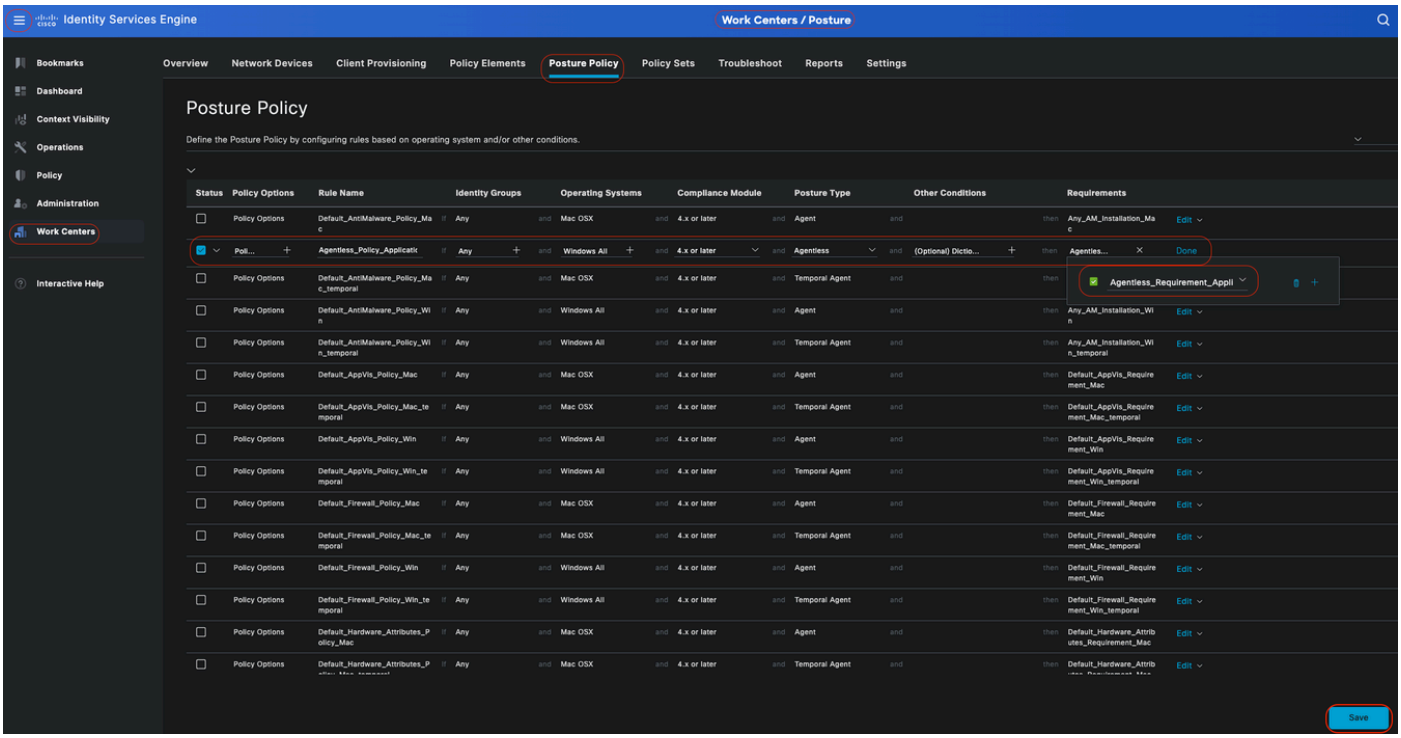
Die Richtlinie ist so festgelegt, dass sie für alle Versionen des Windows-Betriebssystems gilt, sodass eine umfassende Kompatibilität für verschiedene Windows-Umgebungen gewährleistet ist.

- Statustyp: Agentenlos

Diese Konfiguration ist für eine agentenlose Umgebung festgelegt. Zu den verfügbaren Optionen gehören **Agent**, **Agent Stealth**, **Temporal Agent** und **Agentless**. In diesem Szenario wurde **Agentenlos** ausgewählt.

- Sonstige Voraussetzungen:

In diesem Konfigurationsbeispiel wurden keine zusätzlichen Bedingungen erstellt. Sie haben jedoch die Möglichkeit, bestimmte Bedingungen zu konfigurieren, um sicherzustellen, dass nur Zielgeräte dieser Statusrichtlinie unterliegen und nicht alle Windows-Geräte im Netzwerk. Dies kann insbesondere für die Netzwerksegmentierung nützlich sein.



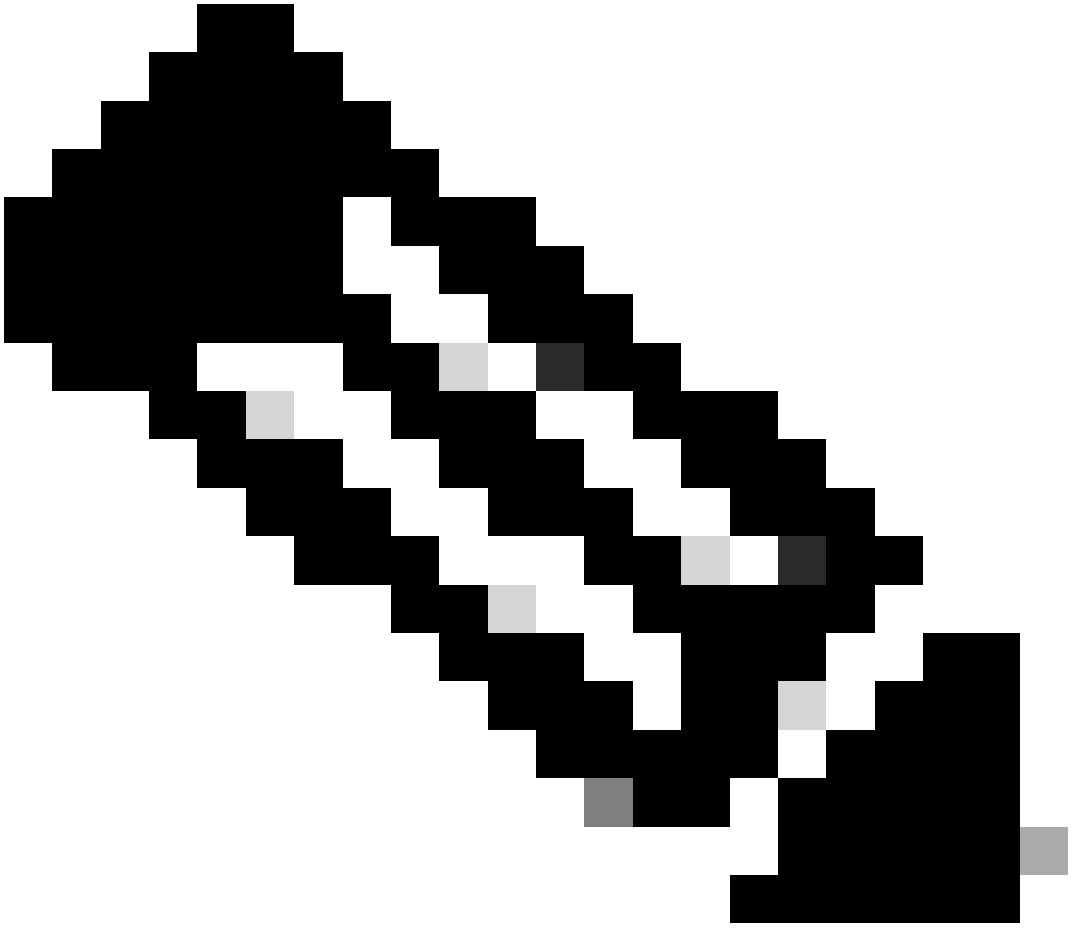
Agentenlose Statusrichtlinie

Client-Bereitstellung

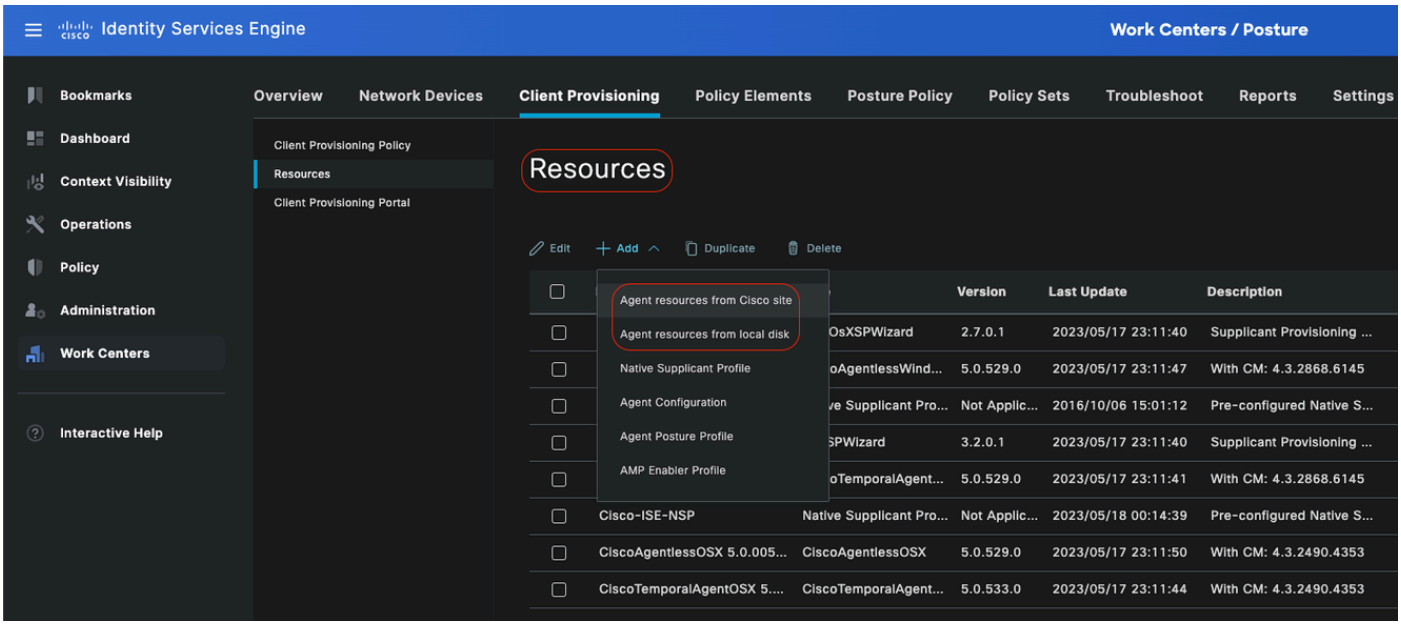
Schritt 1 - Herunterladen von Ressourcen

Um mit der Konfiguration der Client-Bereitstellung zu beginnen, müssen Sie zunächst die erforderlichen Ressourcen herunterladen und in der ISE verfügbar machen, damit Sie sie später in der Client-Bereitstellungsrichtlinie verwenden können.

Es gibt zwei Möglichkeiten, der ISE Ressourcen hinzuzufügen: **Agenten-Ressourcen von der Cisco-Website** und **Agenten-Ressourcen von der lokalen Festplatte**. Da Sie Agentenlos konfigurieren, müssen Sie die **Agentenressourcen von der Cisco Website** durchsuchen**,** um sie herunterzuladen.



Hinweis: Zur Verwendung dieser **Agent-Ressourcen von der Cisco Website** benötigt die ISE PAN einen Internetzugang.



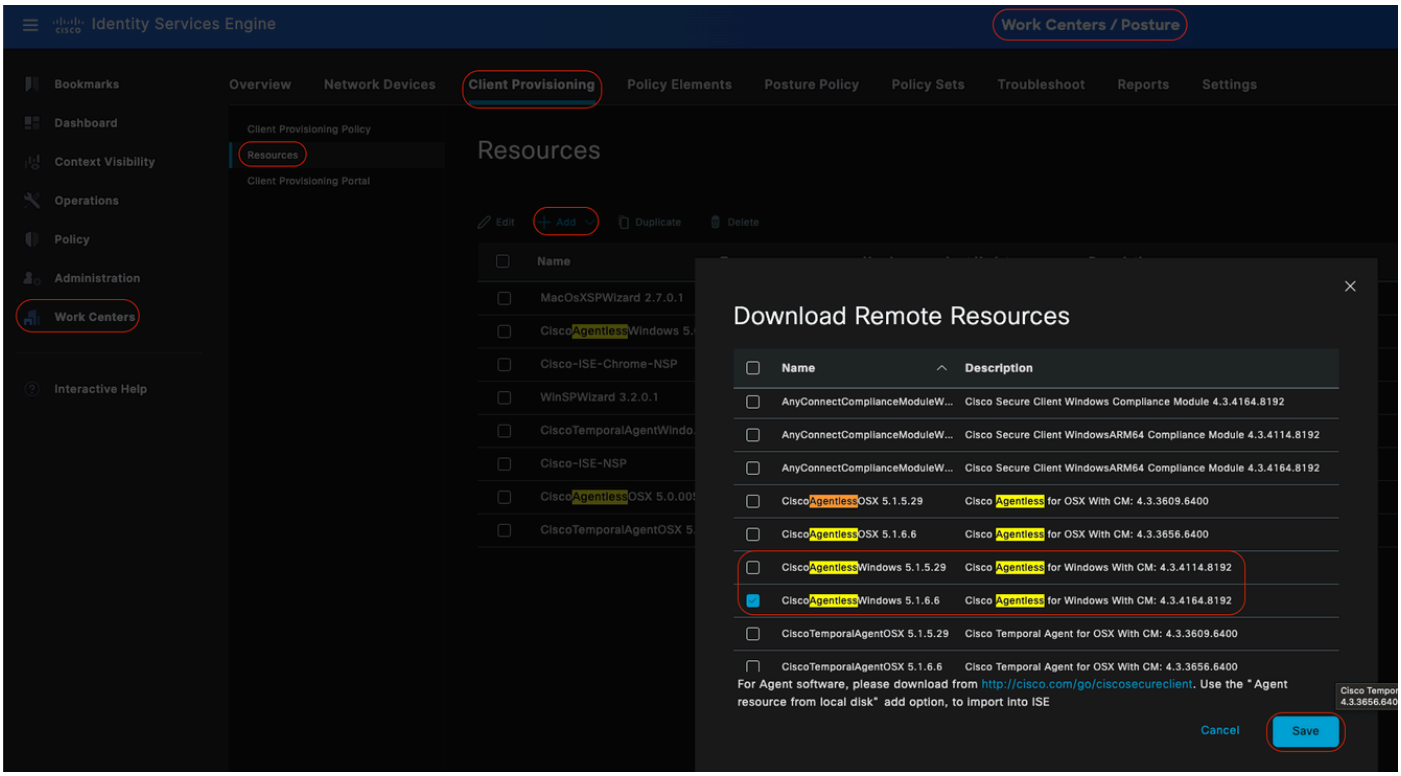
Ressourcen

Mitarbeiterressourcen von Cisco Website

Klicken Sie in der Cisco ISE-GUI auf das Menü ( ), und wählen Sie **Work Centers** > **Posture** > **Client Provisioning** > **Resources (Work Center** > Status > **Client-Bereitstellung** > **Ressourcen) aus**. Klicken Sie auf **Hinzufügen**, wählen Sie **Agent-Ressourcen von der Cisco Website aus**, und klicken Sie auf **Speichern**.

Am Cisco Standort können Sie nur das Compliance-Modul herunterladen. Das System zeigt die beiden neuesten Compliance-Module an, die heruntergeladen werden müssen. Das Ressourcenpaket **CiscoAgentlessWindows 5.1.6.6** wurde für dieses Konfigurationsbeispiel ausgewählt. Dies ist nur für Windows-Geräte gedacht.

.



Mitarbeiterressourcen von der Cisco Website

Schritt 2 - Konfigurieren der Client-Bereitstellungsrichtlinie

Bei der Konfiguration von Posture Agent benötigen Sie zwei verschiedene Ressourcen (**AnyConnect** oder **Secure Client** und **Compliance Module**).

Ordnen Sie beide Ressourcen unter **Agentenkonfiguration** zusammen mit dem **Agentenstatusprofil zu,** sodass Sie diese **Agentenkonfiguration** in Ihrer **Clientbereitstellungsrichtlinie** verwenden können**.**

Bei der Konfiguration von Posture Agentless ist es jedoch nicht erforderlich, die **Agentenkonfiguration** oder das **Agentenstatusprofil** zu konfigurieren. Stattdessen können Sie das Agentenlose Paket nur von den **Agentenressourcen von der Cisco Website** herunterladen.

Klicken Sie in der Cisco ISE-GUI auf das Menusymbol ( ), und wählen Sie **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Policy** aus**.** Klicken Sie auf den **Pfeil nach** unten, und wählen Sie **Neue Richtlinie oben einfügen** oder **Neue Richtlinie unten einfügen**, **Oben duplizieren** oder Unten duplizieren aus:

- **Regelname: Agentless_Client_Provisioning_Policy**

Gibt den Namen der Client-Bereitstellungsrichtlinie an.

- **Betriebssystem:** Alle Windows

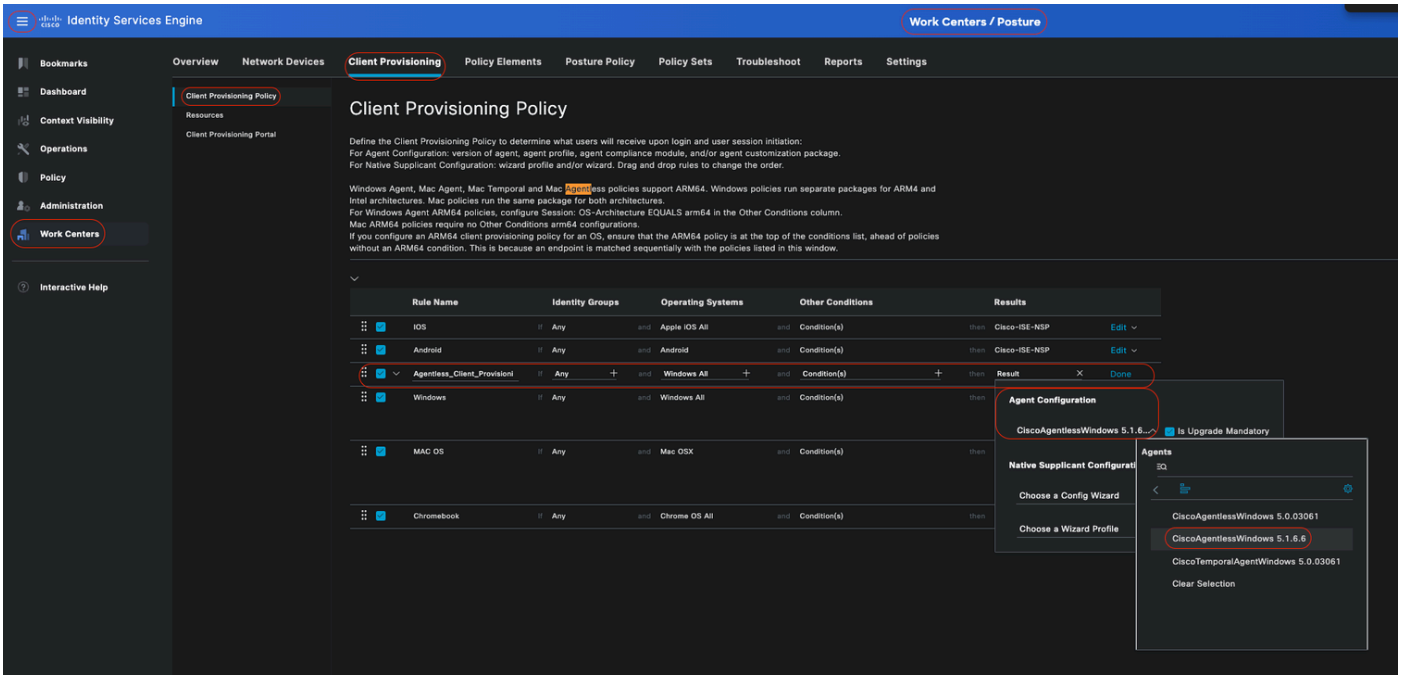
Dadurch wird sichergestellt, dass die Richtlinie für alle Versionen des Windows-Betriebssystems gilt.

- **Andere Bedingungen:** In diesem Beispiel sind keine spezifischen Bedingungen konfiguriert. Sie können jedoch Bedingungen konfigurieren, um sicherzustellen, dass nur die gewünschten Geräte mit dieser Client-Bereitstellungsrichtlinie übereinstimmen und nicht alle Windows-Geräte im Netzwerk. Dies ist besonders bei der Netzwerksegmentierung nützlich.

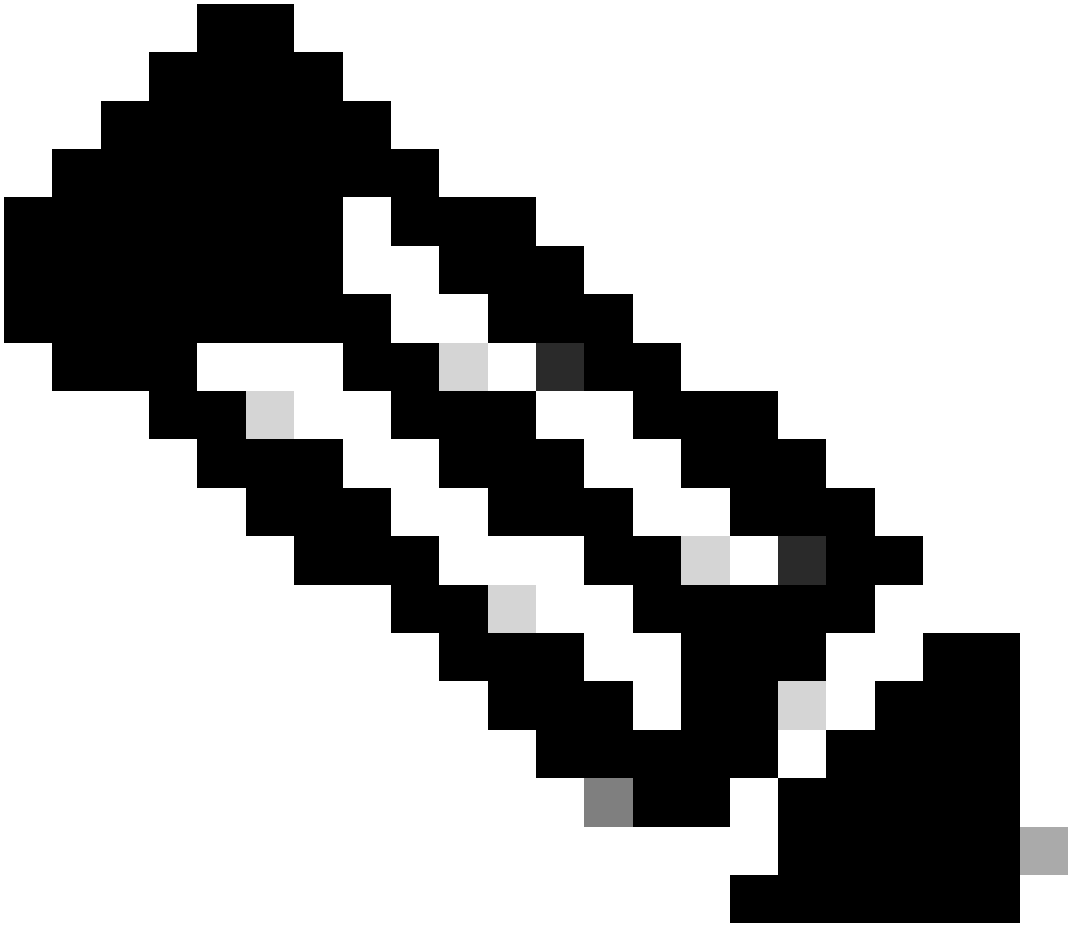
Beispiel: Wenn Sie Active Directory verwenden, können Sie Active Directory-Gruppen in die Richtlinie integrieren, um die betroffenen Geräte zu verfeinern.

- **Ergebnisse:** Wählen Sie das entsprechende Paket oder den entsprechenden Konfigurations-Agent aus. Da Sie für eine agentenlose Umgebung konfigurieren, wählen Sie das Paket **CiscoAgentlessWindows 5.1.6.6 aus,** das Sie zuvor von der **Agentenressource von Cisco** heruntergeladen haben. Dieses agentenlose Paket enthält alle erforderlichen Ressourcen (**Agentenlose Software** und **Compliance-Modul**), die zur Ausführung von Posture Agentless erforderlich sind.

•Klicken Sie auf Save (Speichern).



Agentenlose Client-Bereitstellungsrichtlinie



Hinweis: Stellen Sie sicher, dass nur eine Client-Bereitstellungsrichtlinie die Bedingungen für einen bestimmten Authentifizierungsversuch erfüllt. Wenn mehrere Richtlinien gleichzeitig ausgewertet werden, kann dies zu unerwarteten Verhaltensweisen und potenziellen Konflikten führen.

Agentenloses **Autorisierungsprofil (Autorisierungsprofil)**

Klicken Sie in der Cisco ISE-GUI auf das Menü (

), wählen Sie Policy > Policy **Elements > Results > Authorization > Authorization Profilesund erstellen Sie ein Authorization Profile, das die Ergebnisse aus Agentless Posture auswertet.**

- In diesem Konfigurationsbeispiel wird Authorization Profile als **Agentless_Authorization_Profile** bezeichnet.

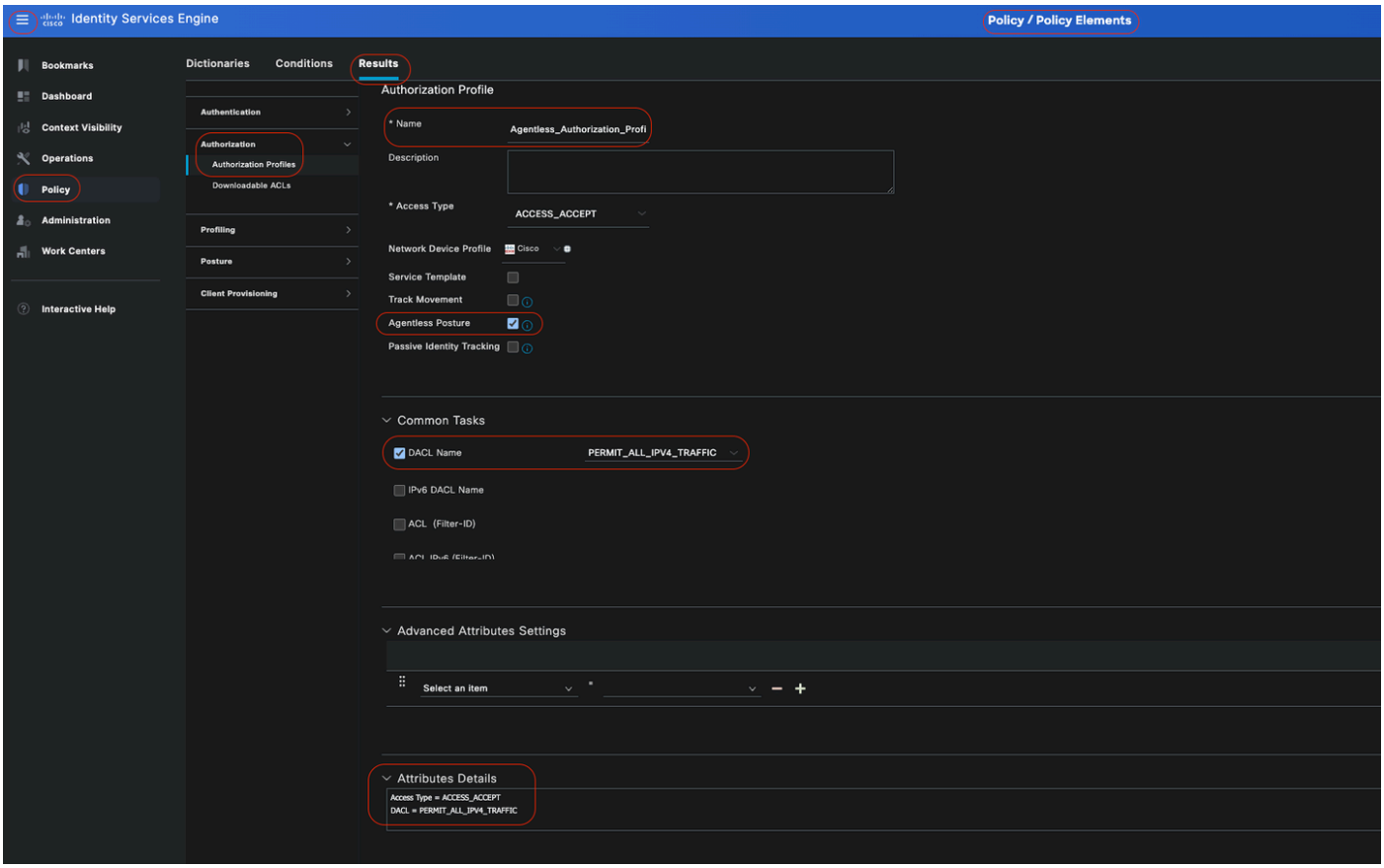
- Agentenloser Status im Autorisierungsprofil aktivieren.

- Verwenden Sie dieses Profil nur für **Agentenlose Statusinformationen**. Verwenden Sie diese Option nicht auch für andere Haltungsarten.

- Für Agentenlosen Status sind keine CWA und Umleitungs-ACL erforderlich. Sie können VLANs, DACLs oder ACLs als Teil Ihrer Segmentierungsregeln verwenden. Um es einfach zu halten, wird in diesem Konfigurationsbeispiel neben der Agentless Posture-Prüfung lediglich eine dACL (die den gesamten IPv4-Verkehr zulässt) konfiguriert.

-

Klicken Sie auf **Speichern**.



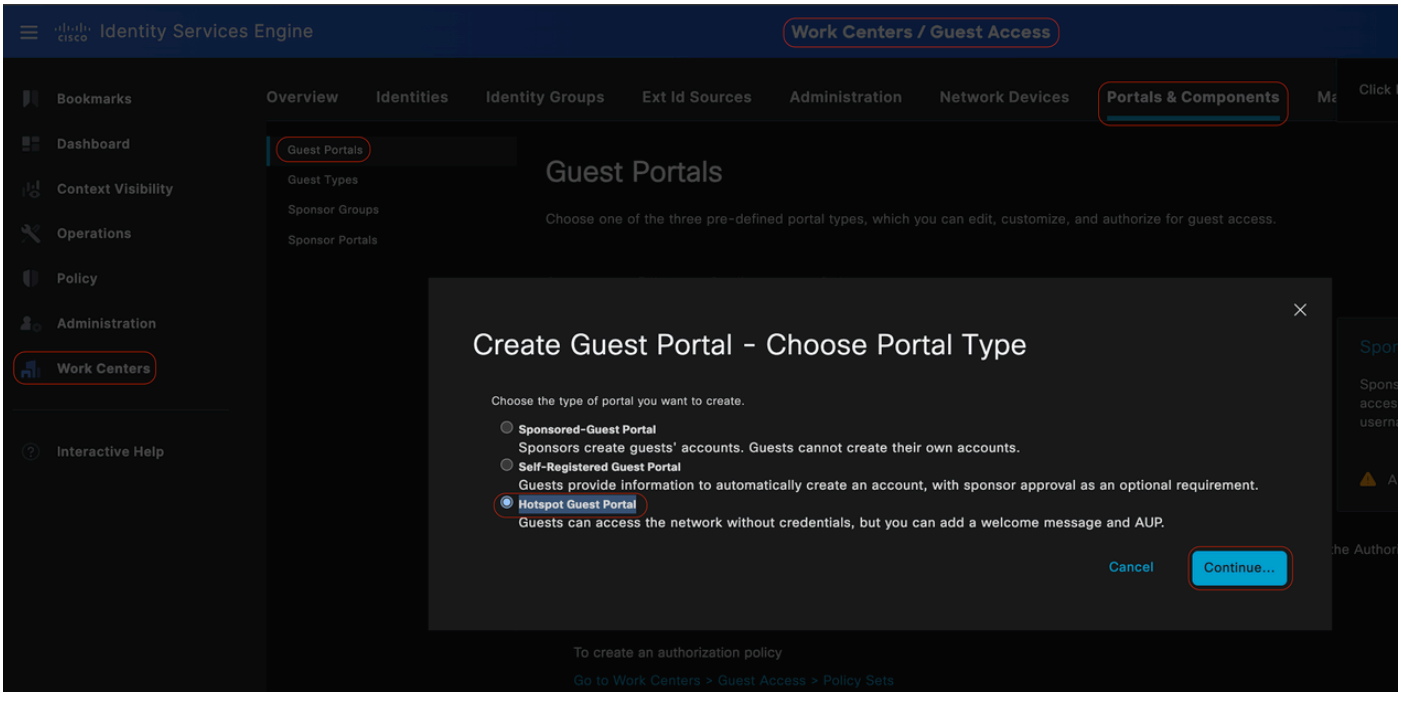
Agentenloses Autorisierungsprofil

Alternative zur Behebung (optional)

Es ist keine Unterstützung für die Behebung des agentenlosen Datenflusses verfügbar. Um dies zu erreichen, können Sie ein angepasstes Hotspot-Portal implementieren, das die Benutzer hinsichtlich der Endpunkt-Compliance sensibilisiert. Wenn ein Endgerät als nicht konform erkannt wird, können Benutzer zu diesem Portal umgeleitet werden. Mit diesem Ansatz wird sichergestellt, dass Benutzer über den Compliance-Status ihrer Endgeräte informiert sind und geeignete Maßnahmen zur Behebung von Problemen ergreifen können.

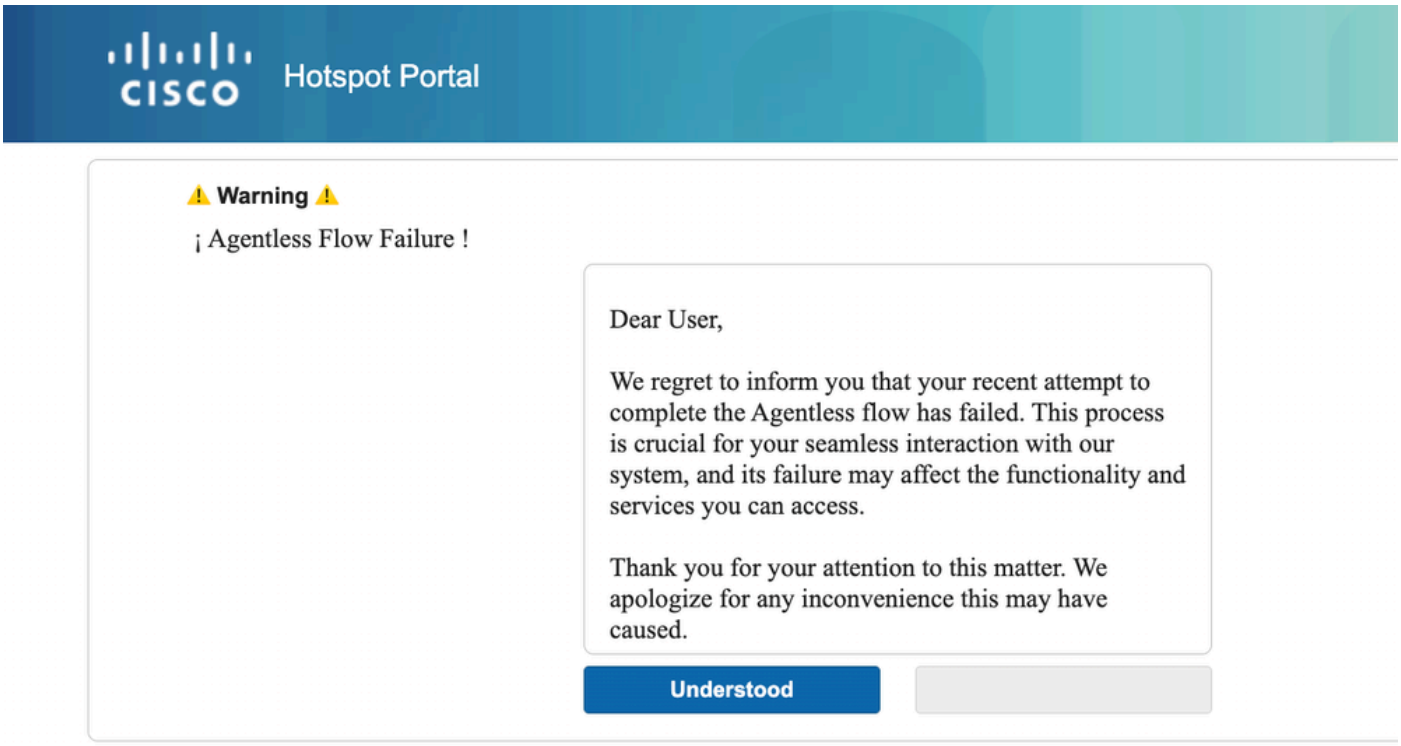
Klicken Sie in der Cisco ISE-GUI auf das Menusymbol (

) und wählen Sie **Work Centers** > **Guest Access** > **Portals & Components** >**Guest Portals aus**. Klicken Sie auf **Erstellen** > **Hotspot-Gastportal** auswählen > **Weiter:** . In diesem Konfigurationsbeispiel erhält das Hotspot-Portal den Namen **Agentless_Warning**.



Hotspot-Gastportal

In den Portaleinstellungen können Sie die für Endbenutzer angezeigten Meldungen an Ihre spezifischen Anforderungen anpassen. Dies ist nur ein Beispiel für eine benutzerdefinierte Portalansicht:



Fehlgeschlagener Status Agentenlos

Behebungs-**Autorisierungsprofil (optional)**

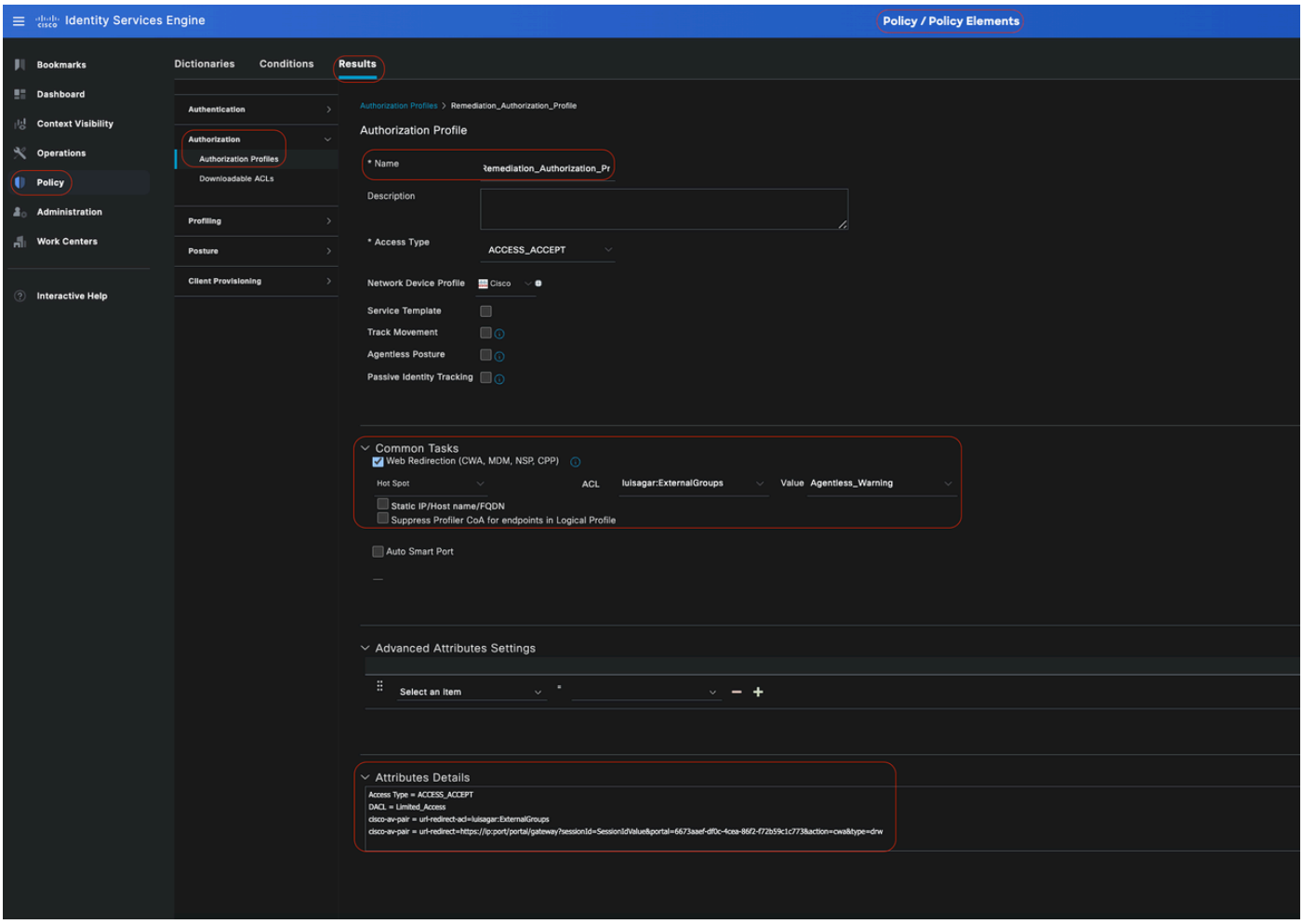
Klicken Sie in der Cisco ISE-GUI auf das Menü ( ), wählen Sie Policy > Policy **Elements > Results > Authorization > Authorization Profilesund erstellen Sie ein Authorization Profile für die Behebung.**

- In diesem Konfigurationsbeispiel erhält den Namen Authorization Profile mit **Remediation_Authorization_Profile**.

- Der Einfachheit halber enthält dieses Konfigurationsbeispiel nur eine herunterladbare Zugriffskontrollliste (Access Control List, dACL) mit dem Namen **Limited_Access,** die einen eingeschränkten Zugriff ermöglicht, der auf die spezifischen Anforderungen Ihres Unternehmens zugeschnitten ist.

- Die **Webumleitungsfunktion** wurde konfiguriert, einschließlich einer externen Gruppe und des Hotspots, sodass die Benutzer besser über die Endpunkt-Compliance informiert sind.

- Klicken Sie auf **Speichern**.

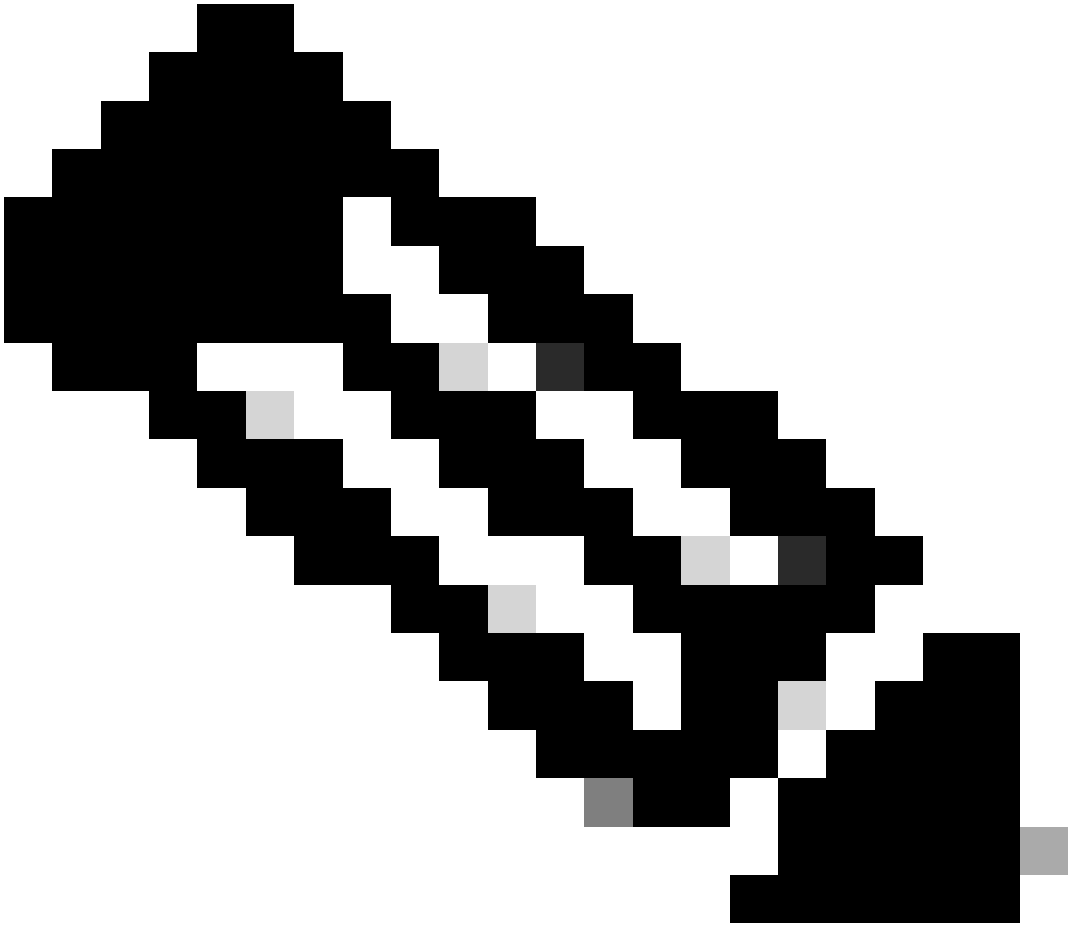


Behebungsautorisierungsregel

Agentenlose Autorisierungsregel

Klicken Sie in der Cisco ISE-GUI auf das Menuicon (

) und **wählen Sie Policy** > **Policy Sets** aus, und erweitern Sie **Authorization Policy (Autorisierungsrichtlinie)**. Aktivieren und konfigurieren Sie die folgenden drei Autorisierungsrichtlinien:



Hinweis: Diese Autorisierungsregeln müssen in der angegebenen Reihenfolge konfiguriert werden, um sicherzustellen, dass der Status ordnungsgemäß ausgeführt wird.

Unbekannt_Compliance_Redirect:

•Bedingungen:

Konfigurieren Sie Network_Access_Authentication_Passed UND **Compliance_Unknown_Devices** mit dem Ergebnis "Agentless Posture". Diese Bedingung löst den agentenlosen Datenfluss aus.

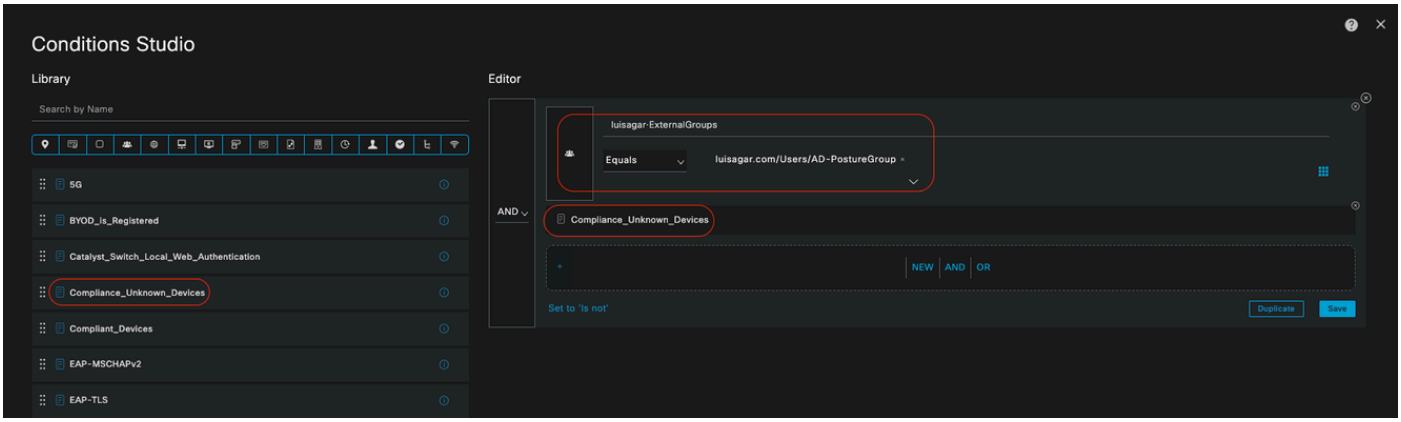
- Beispielbedingungen:

Konfigurieren einer Active Directory (AD)-Gruppenbedingung zum Segmentieren des Datenverkehrs

Die Bedingung **Compliance_Unknown_Devices** muss konfiguriert werden, da der ursprüngliche Status unbekannt ist.

- Autorisierungsprofil:

Weisen Sie **Agentless_Authorization_Profile** dieser Autorisierungsregel zu, um sicherzustellen, dass Geräte den Agentless Posture-Fluss durchlaufen. Diese Bedingung enthält Agentenlosen Fluss, sodass Geräte, die auf dieses Profil zugreifen, Agentenlosen Fluss initiieren können.



Unbekannte Autorisierungsregel

Nicht konforme_Geräte_Umleitung:

- Bedingungen: Konfigurieren Sie Network_Access_Authentication_Passed und Non_Compliant_Devices, wobei das Ergebnis auf DenyAccess festgelegt ist. Alternativ können Sie die Sanierungsoption verwenden, wie in diesem Beispiel gezeigt.

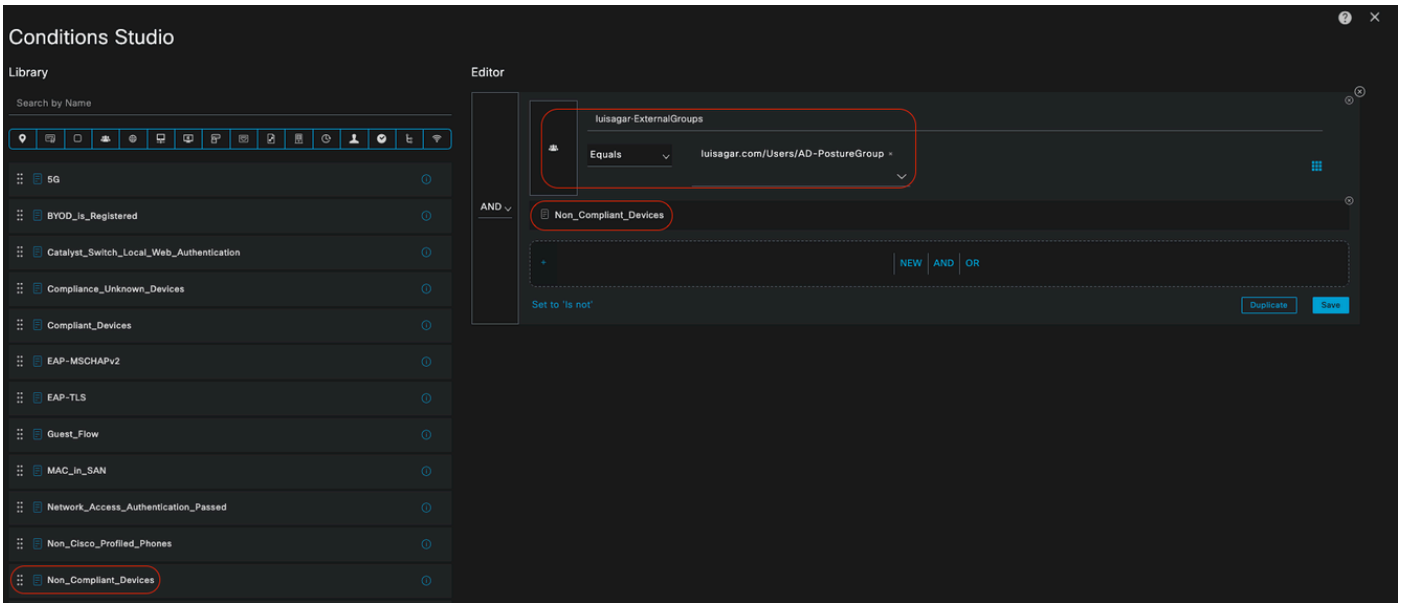
- Beispielbedingungen:

Konfigurieren einer AD-Gruppenbedingung zum Segmentieren des Datenverkehrs

Die Bedingung **Compliance_Unknown_Devices** muss so konfiguriert werden, dass beschränkte Ressourcen zugewiesen werden, wenn der Status nicht konform ist.

- Autorisierungsprofil:

Weisen Sie dieser Autorisierungsregel **Remediation_Authorization_Profile** zu, um nicht konforme Geräte über das **Hotspot-Portal** über ihren aktuellen Status zu informieren oder den **Zugriff** zu **verweigern**.



Nicht konforme Autorisierungsregel

Compliant_Geräte_Zugriff:

•Bedingungen:

Konfigurieren Sie Network_Access_Authentication_Passed und **Compliant_Devices**, wobei das Ergebnis auf PermitAccess festgelegt ist.

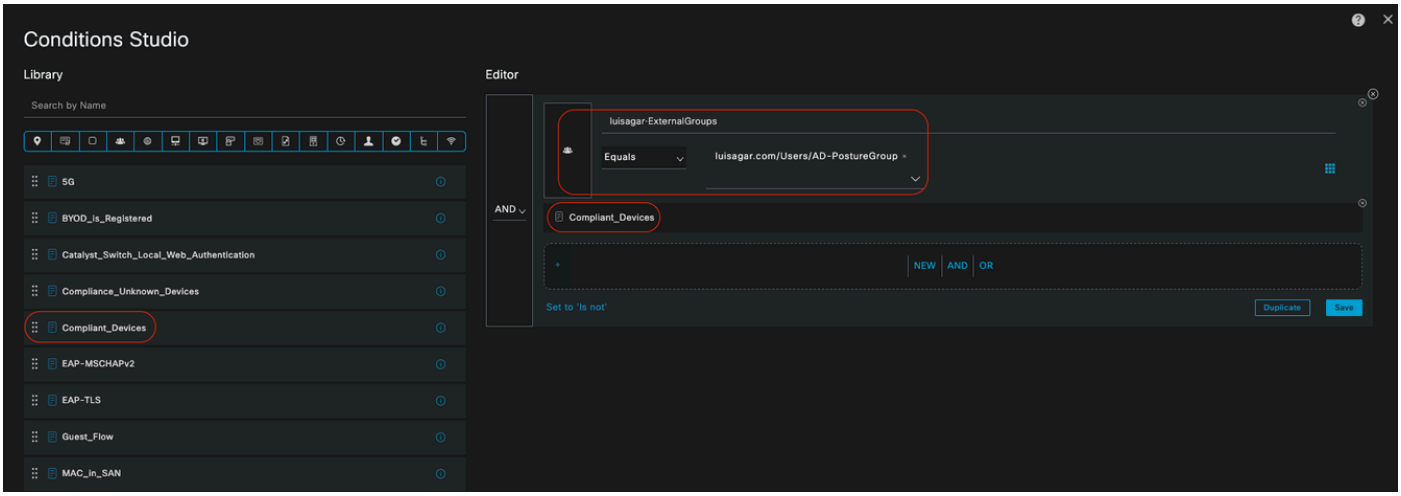
- Beispielbedingungen:

Konfigurieren einer AD-Gruppenbedingung zum Segmentieren des Datenverkehrs

Die Bedingung **Compliance_Unknown_Devices** muss so konfiguriert werden, dass kompatible Geräte den richtigen Zugriff erhalten.

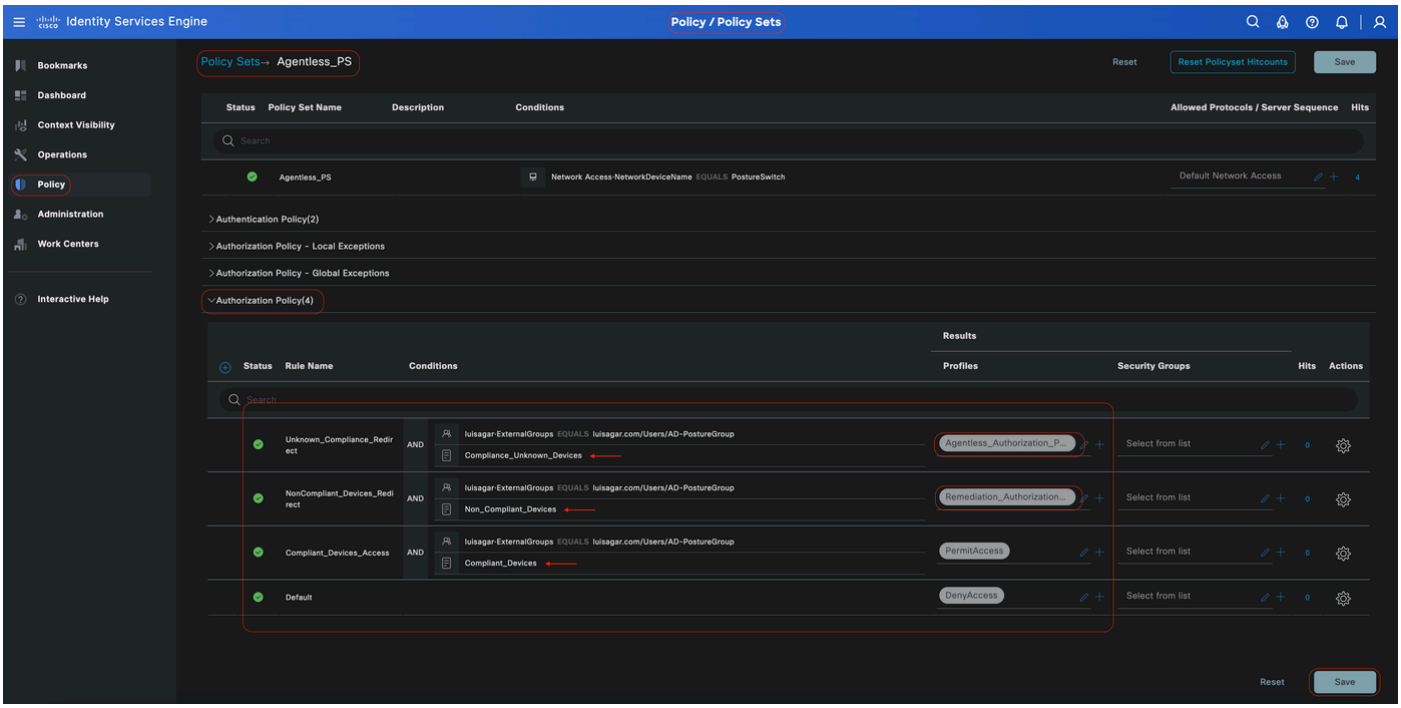
- Autorisierungsprofil:

Weisen Sie dieser Autorisierungsregel **PermitAccess** zu, um sicherzustellen, dass kompatible Geräte Zugriff erhalten. Dieses Profil kann an die Anforderungen Ihres Unternehmens angepasst werden.



Autorisierungsregel für Konformität

Alle Autorisierungsregeln



Autorisierungsregeln

Anmeldeinformationen für Endpunkt konfigurieren

Klicken Sie in der Cisco ISE-GUI auf das Menuicon ( ), **wählen Sie Administration > Settings > Endpoint Scripts > Login Configuration aus, und konfigurieren Sie die Client-Anmeldedaten für die Anmeldung bei Clients.**

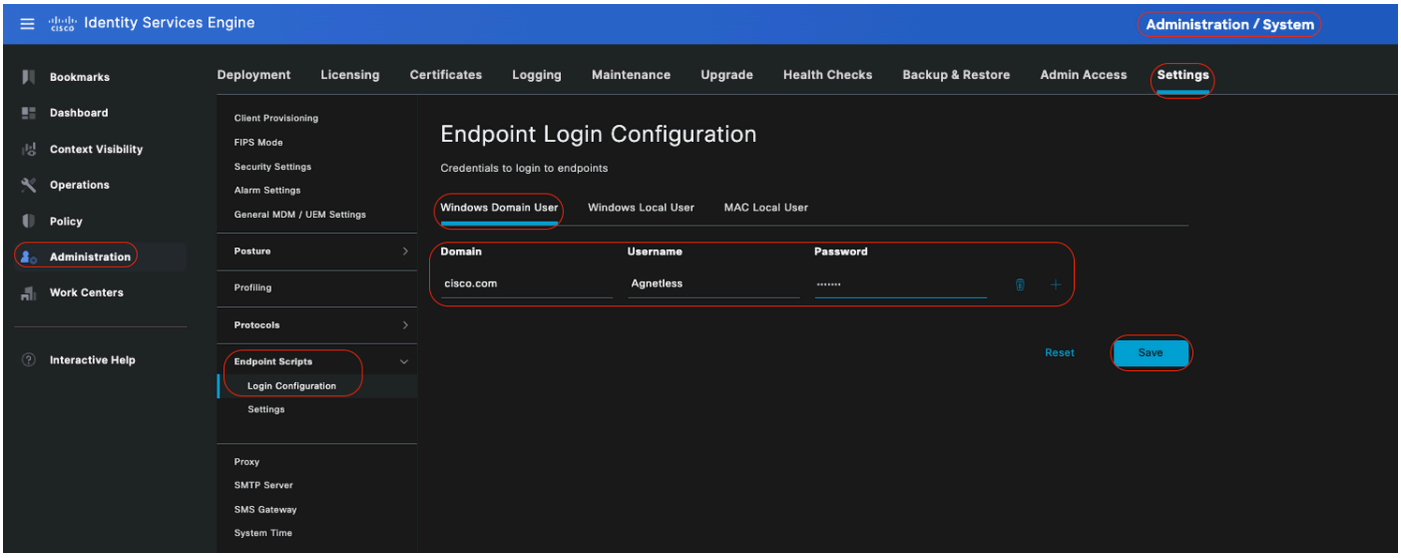
Dieselben Anmeldeinformationen werden von den Endpunktskripts verwendet, sodass sich die Cisco ISE bei den Clients anmelden kann.

Bei Windows-Geräten konfigurieren Sie nur die beiden ersten Registerkarten (**Windows-Domänenbenutzer und lokaler Windows-Benutzer).**

- **Windows-Domänenbenutzer:**

Konfigurieren Sie die Domänenanmeldeinformationen, die die Cisco ISE für die Anmeldung bei einem Client über SSH verwenden muss. Klicken Sie auf das Plusicon und geben Sie so viele Windows-Anmeldungen ein, wie Sie benötigen. Geben Sie für jede Domäne die erforderlichen Werte in dieFelder Domain,Username undPasswordein. Wenn Sie Domänenanmeldeinformationen konfigurieren, werden die Anmeldeinformationen des lokalen Benutzers, die auf der Registerkarte Lokaler Windows-Benutzer konfiguriert sind, ignoriert.

Wenn Sie Windows-Endpunkte verwalten, die eine agentenlose Statusüberprüfung über eine Active Directory-Domäne verwenden, stellen Sie sicher, dass Sie den Domänennamen zusammen mit Anmeldeinformationen angeben, die über lokale Administratorberechtigungen verfügen.

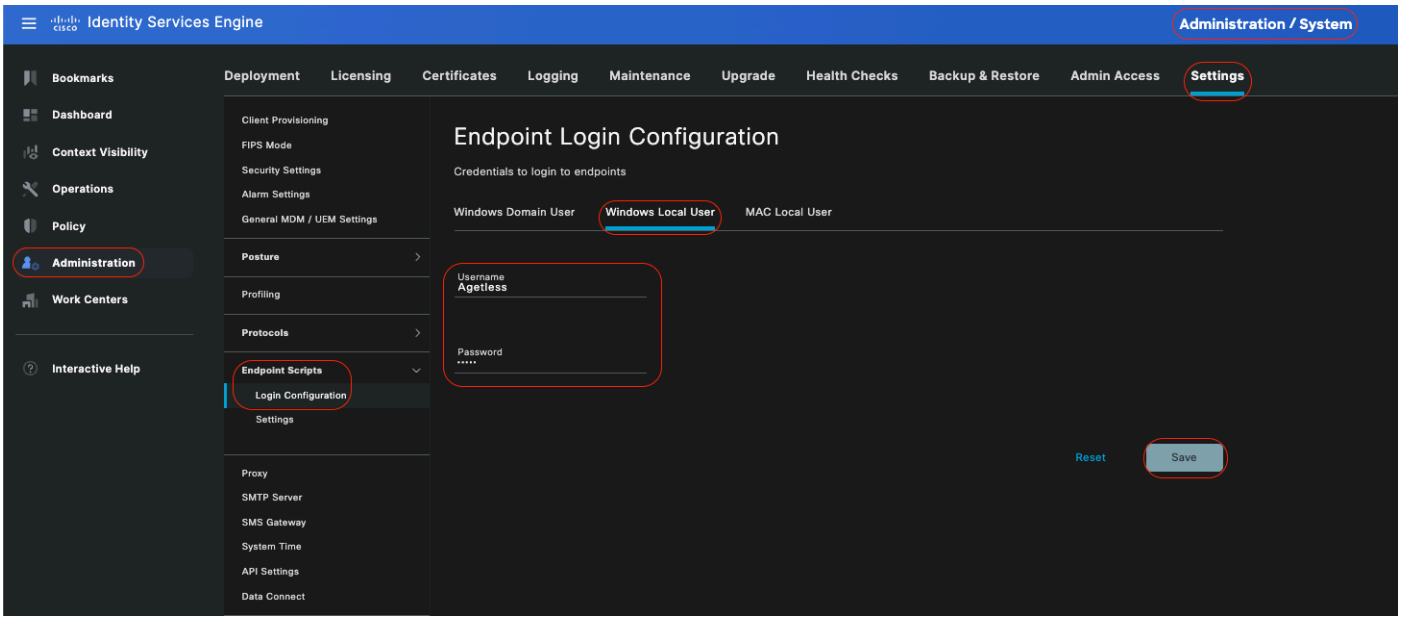


Windows-Domänenbenutzer

- **Lokaler Windows-Benutzer:**

Konfigurieren Sie das lokale Konto, das die Cisco ISE für den Zugriff auf den Client über SSH verwendet. Das lokale Konto muss in der Lage sein, Powershell und Powershell remote auszuführen.

Wenn Sie **keine** Windows-Endpunkte verwalten, die eine agentenlose Statusüberprüfung über eine Active Directory-Domäne verwenden, stellen Sie sicher, dass Anmeldeinformationen mit lokalen Administratorberechtigungen bereitgestellt werden.

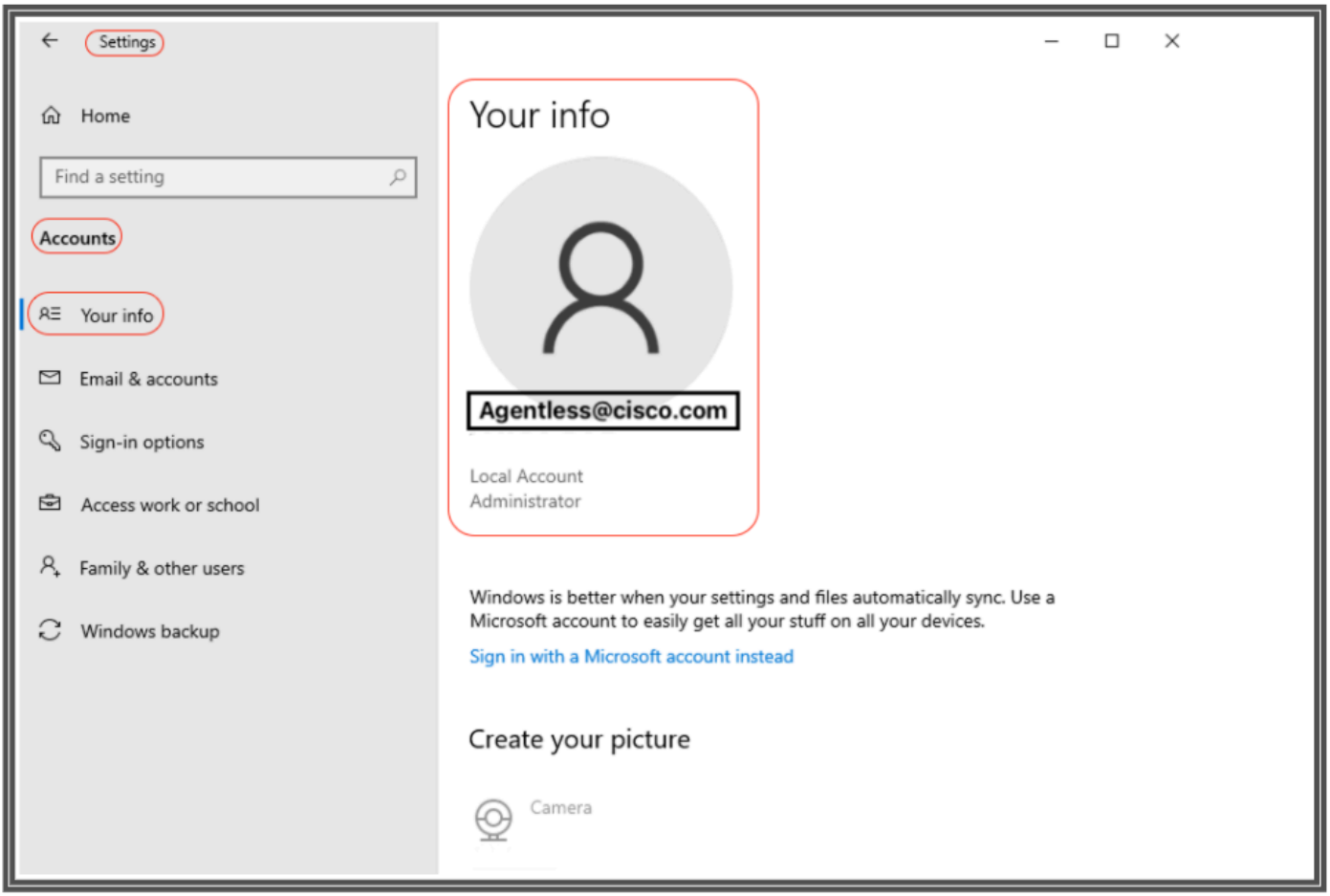


Lokaler Windows-Benutzer

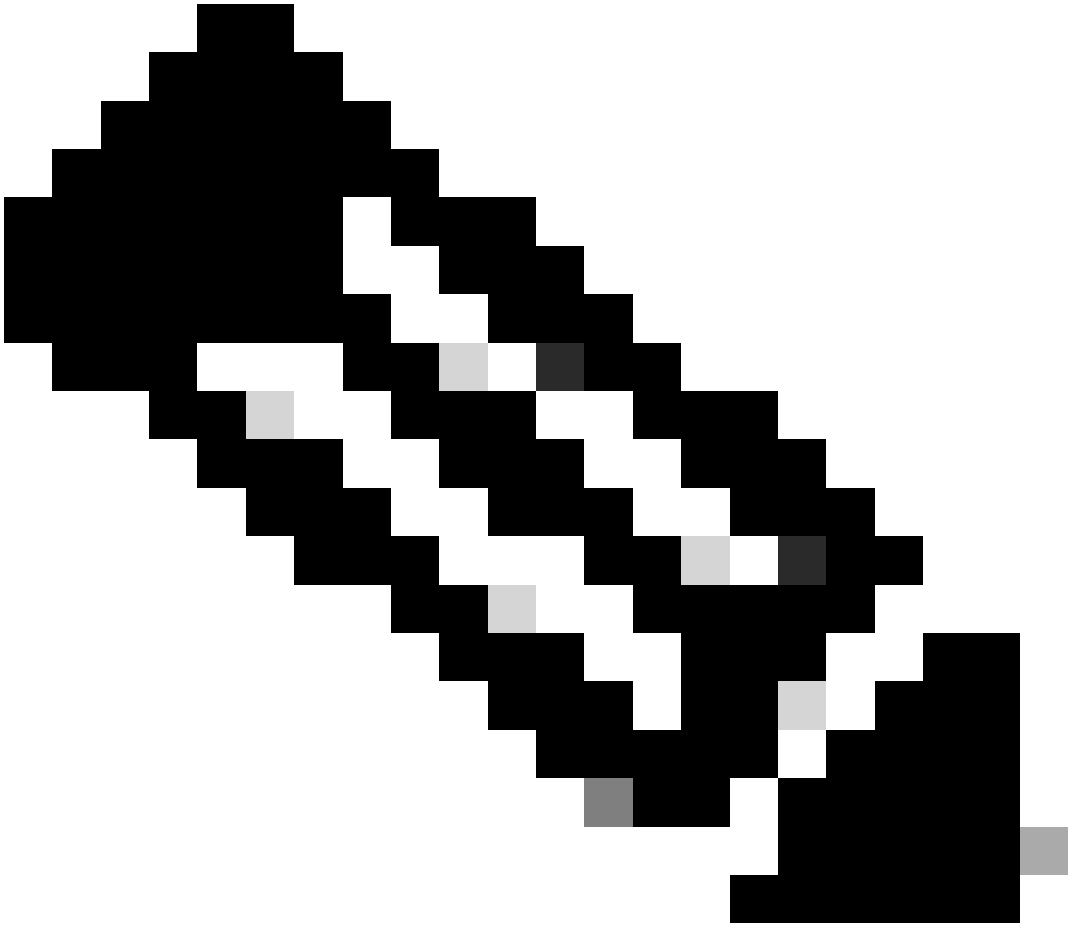
Konten überprüfen

Gehen Sie folgendermaßen vor, um Ihre Windows-Domänenbenutzer- und lokalen Windows-Benutzerkonten zu überprüfen, damit Sie die entsprechenden Daten unter Endpoint Login Credentials (Anmeldeinformationen für Endpunkt) korrekt hinzufügen können:

Lokaler Windows-Benutzer: Verwenden Sie die GUI (Einstellungen-App) Klicken Sie auf die **WindowsStart**-Schaltfläche, wählen Sie **Einstellungen (**das Zahnrad-Symbol), klicken Sie auf **Konten**, und wählen Sie **Ihre Informationen**:



Konten überprüfen



Hinweis: Für MacOS können Sie auf **Lokaler MAC-Benutzer** verweisen. In diesem Konfigurationsbeispiel wird die MacOS-Konfiguration jedoch nicht angezeigt.

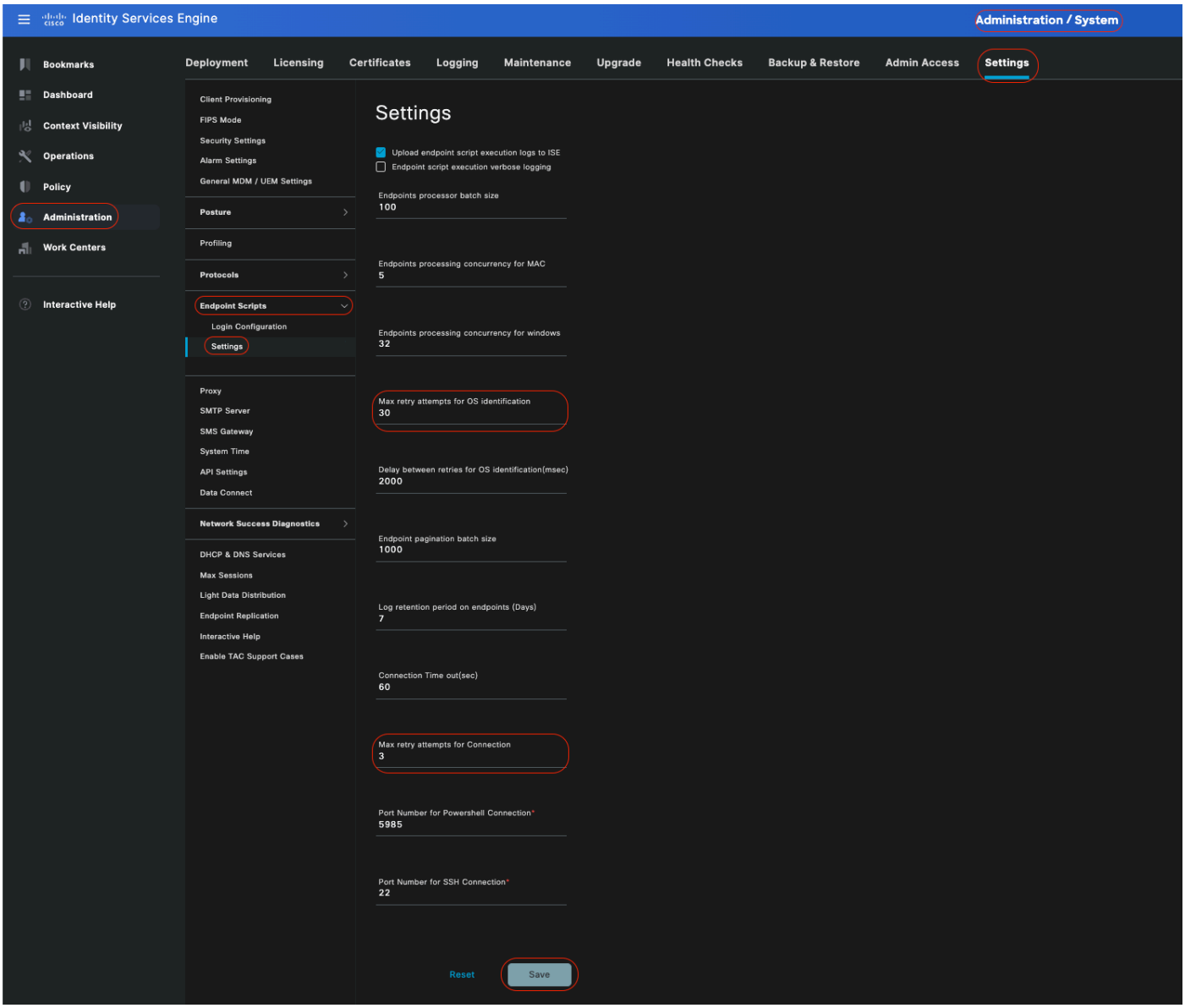
- **Lokaler MAC-Benutzer:** Konfigurieren Sie das lokale Konto, das die Cisco ISE für den Zugriff auf den Client über SSH verwendet. Das lokale Konto muss in der Lage sein, Powershell und Powershell remote auszuführen. Geben Sie im Feld Benutzername den Kontonamen des lokalen Kontos ein.

Um einen Mac OS-Kontonamen anzuzeigen, führen Sie diesen Befehlwhoami im Terminal aus:

Einstellungen

Klicken Sie in der Cisco ISE-GUI auf das Menuicon (), **wählen Sie Administration > Settings > Endpoint Scripts > Settings, und konfigurieren Sie Max. Wiederholungsversuche** für die Betriebssystemidentifizierung, **Verzögerung zwischen Wiederholungsversuchen für die Betriebssystemidentifizierung** usw. Diese Einstellungen legen fest, wie schnell Verbindungsprobleme bestätigt werden können. Beispiel: Ein Fehler, dass der PowerShell-Port nicht geöffnet ist, wird erst in Protokollen angezeigt, nachdem nicht alle erneuten Versuche ausgeschöpft wurden.

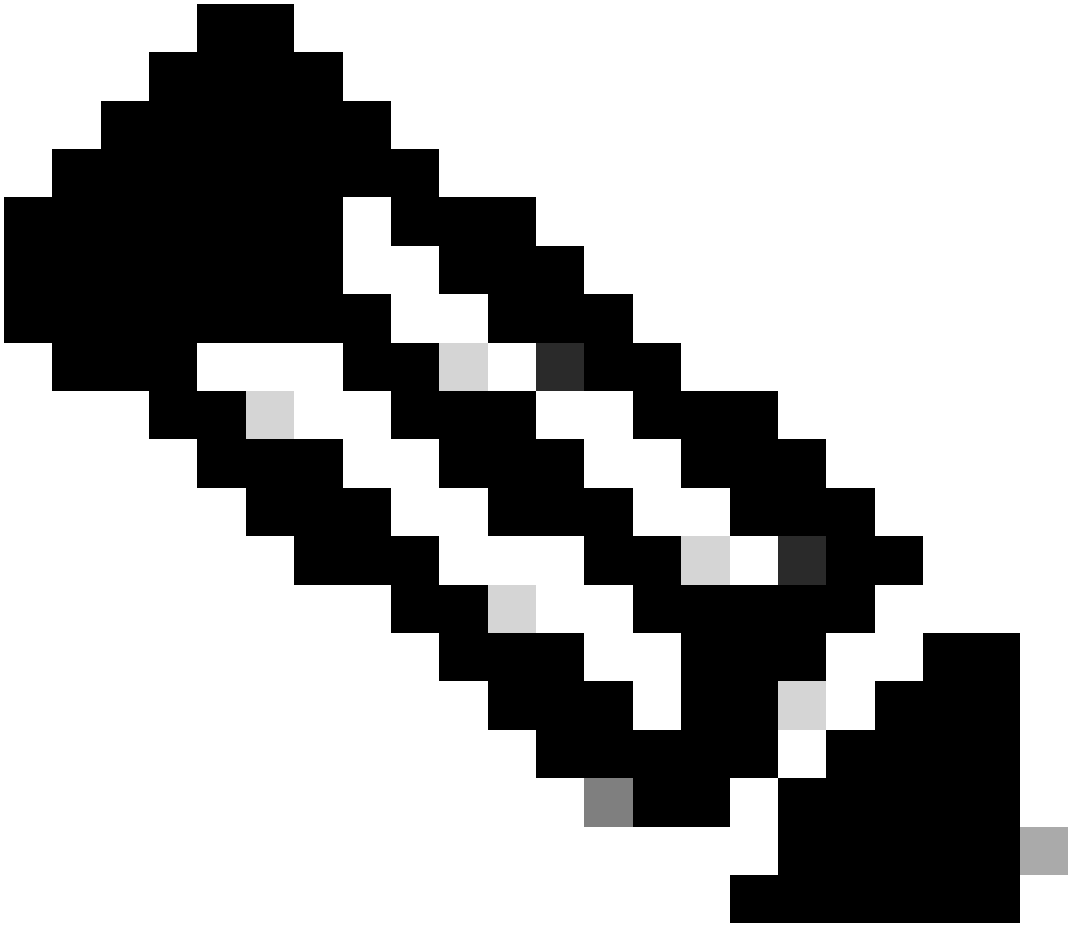
Dieser Screenshot zeigt die Standardwerteinstellungen:



Endpunkt-Skript-Einstellungen

Wenn Clients eine Verbindung mit einem agentenlosen Status herstellen, werden sie in den Live-Protokollen angezeigt.

Konfigurieren und Problembehebung für Windows Endpoint



Hinweis: Dies sind einige Empfehlungen, die Sie auf Ihrem Windows-Gerät überprüfen und anwenden sollten. Sie müssen jedoch die Microsoft-Dokumentation lesen oder sich an den Microsoft-Support wenden, wenn Probleme wie Benutzerberechtigungen, PowerShell-Zugriff usw. auftreten.

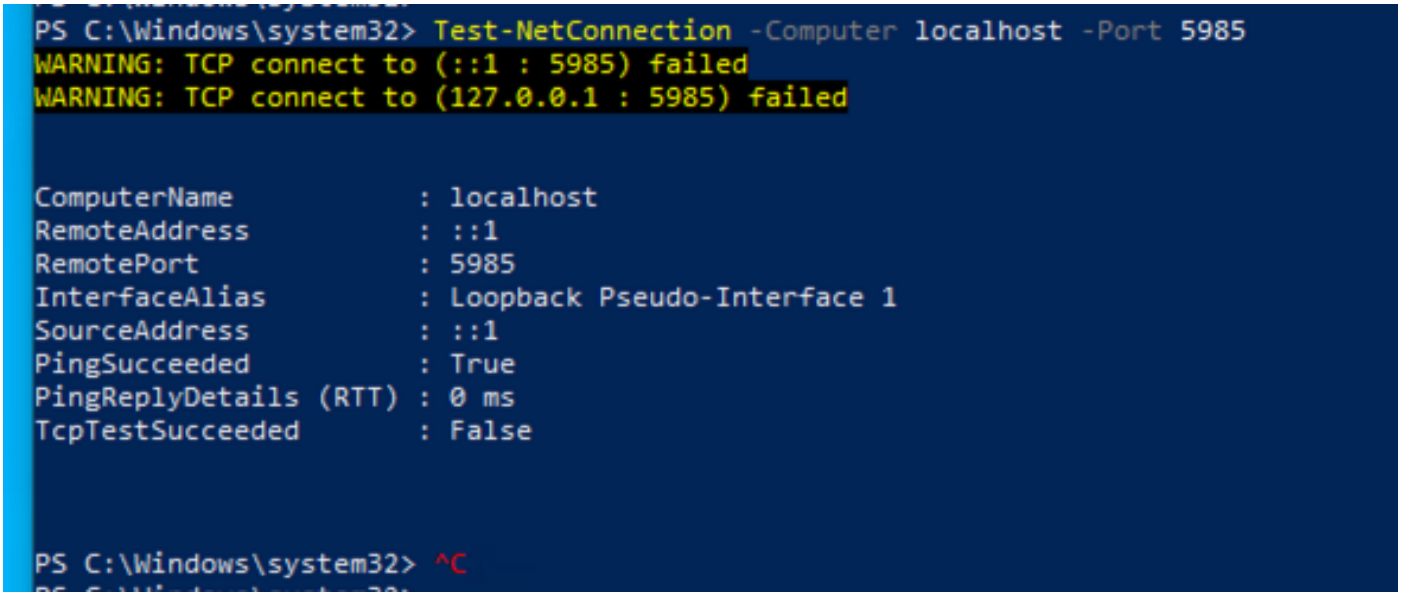
Voraussetzungen für Verifizierung und Fehlerbehebung

Testen der TCP-Verbindung mit Port 5985

Für Windows-Clients muss der Port 5985 für den Zugriff auf Powershell auf dem Client geöffnet werden. Führen Sie diesen Befehl aus, um die TCP-Verbindung mit Port 5985 zu bestätigen: **Test-NetConnection -ComputerName localhost -Port 5985**

Die Ausgabe in diesem Screenshot zeigt an, dass die TCP-Verbindung mit Port 5985 auf localhost fehlgeschlagen ist. Das bedeutet, dass der

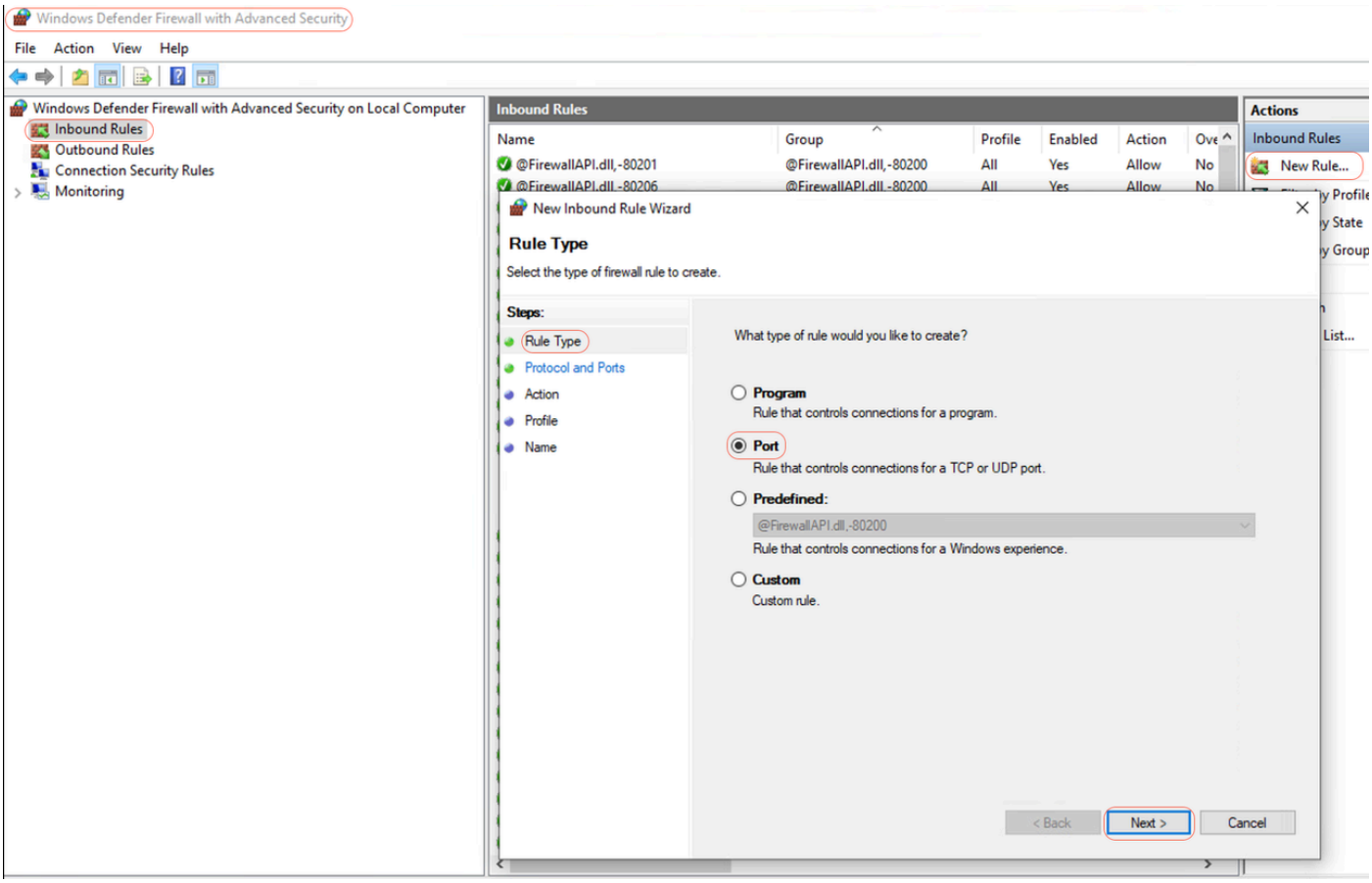
WinRM-Dienst (Windows Remote Management), der den Port 5985 verwendet, nicht ausgeführt wird oder nicht ordnungsgemäß konfiguriert ist.



Connection failed to WinRM

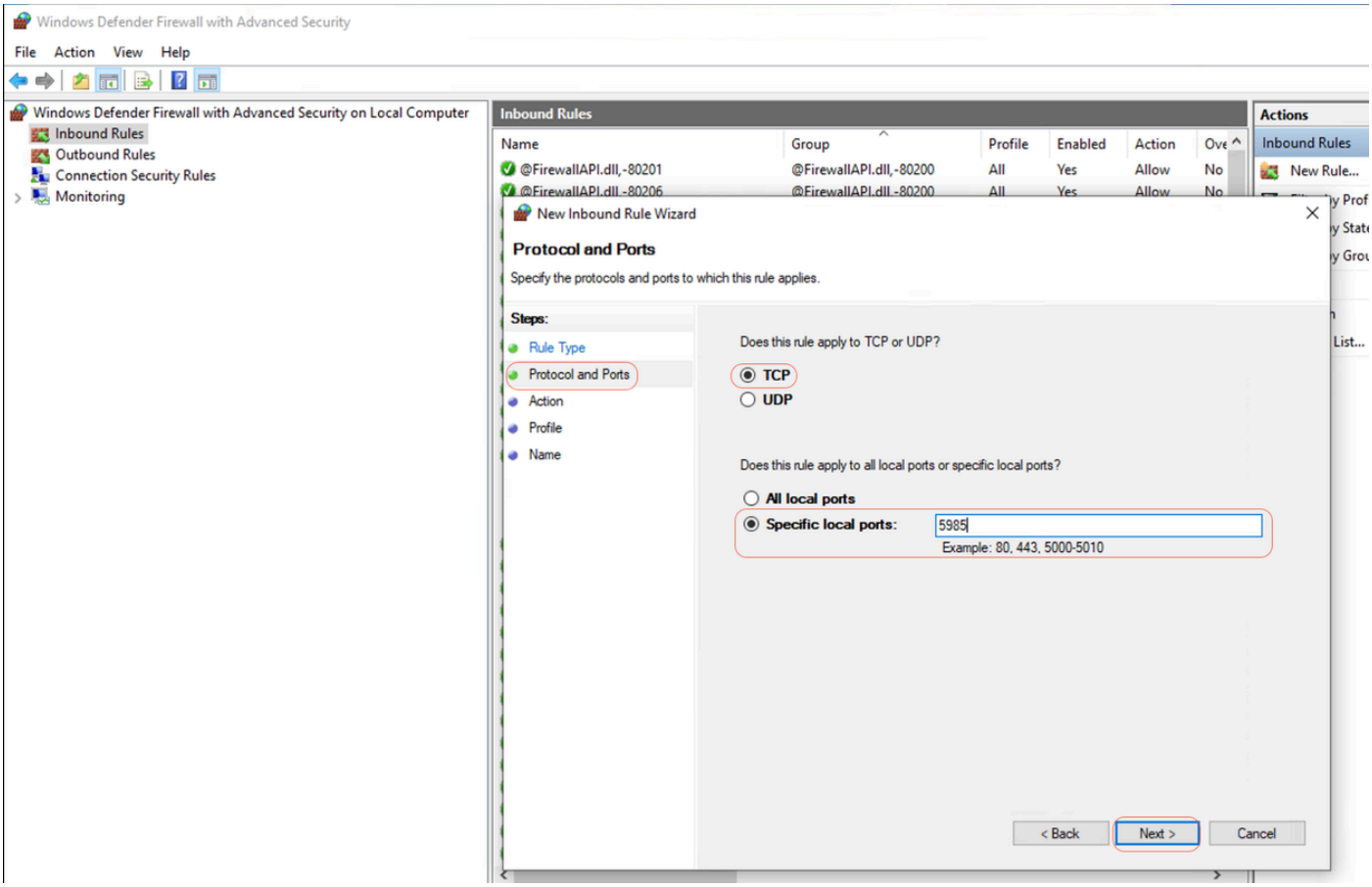
Erstellen einer eingehenden Regel, um PowerShell auf Port 5985 zuzulassen

Schritt 1- Gehen Sie in der Windows-GUI zur Suchleiste, geben Sie Windows-Firewall mit erweiterter Sicherheit ein, klicken Sie darauf und wählen Sie Als Administrator ausführen > Eingehende Regeln > Neue Regel > Regeltyp > Port > Weiter aus:



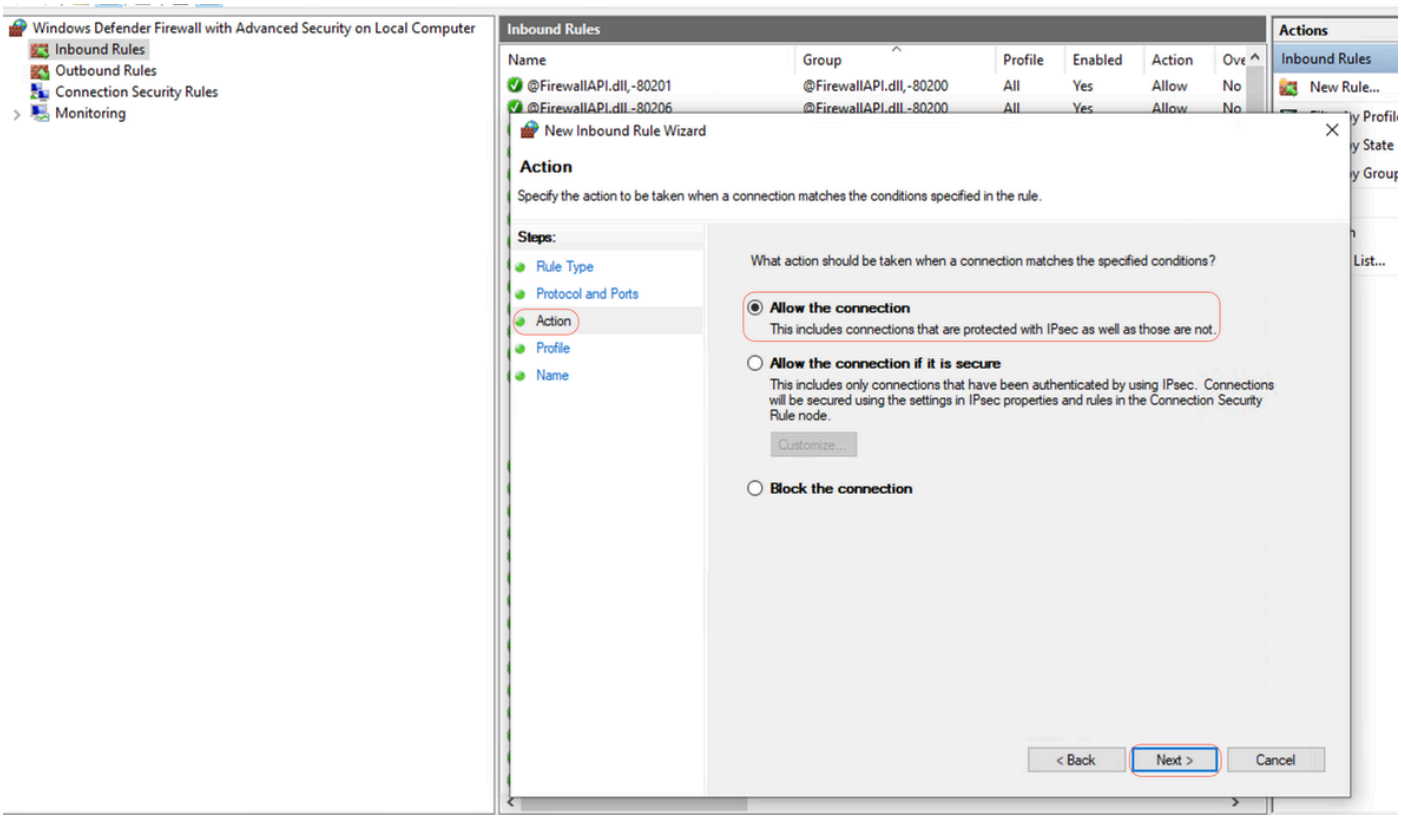
Neue eingehende Regel - Port

Schritt 2- Wählen Sie unter Protokolle und Ports die Option TCP und Lokale Ports angeben, geben Sie die Portnummer 5985 (Standardport für **PowerShell**-Remoting) ein, und klicken Sie auf **Weiter**:



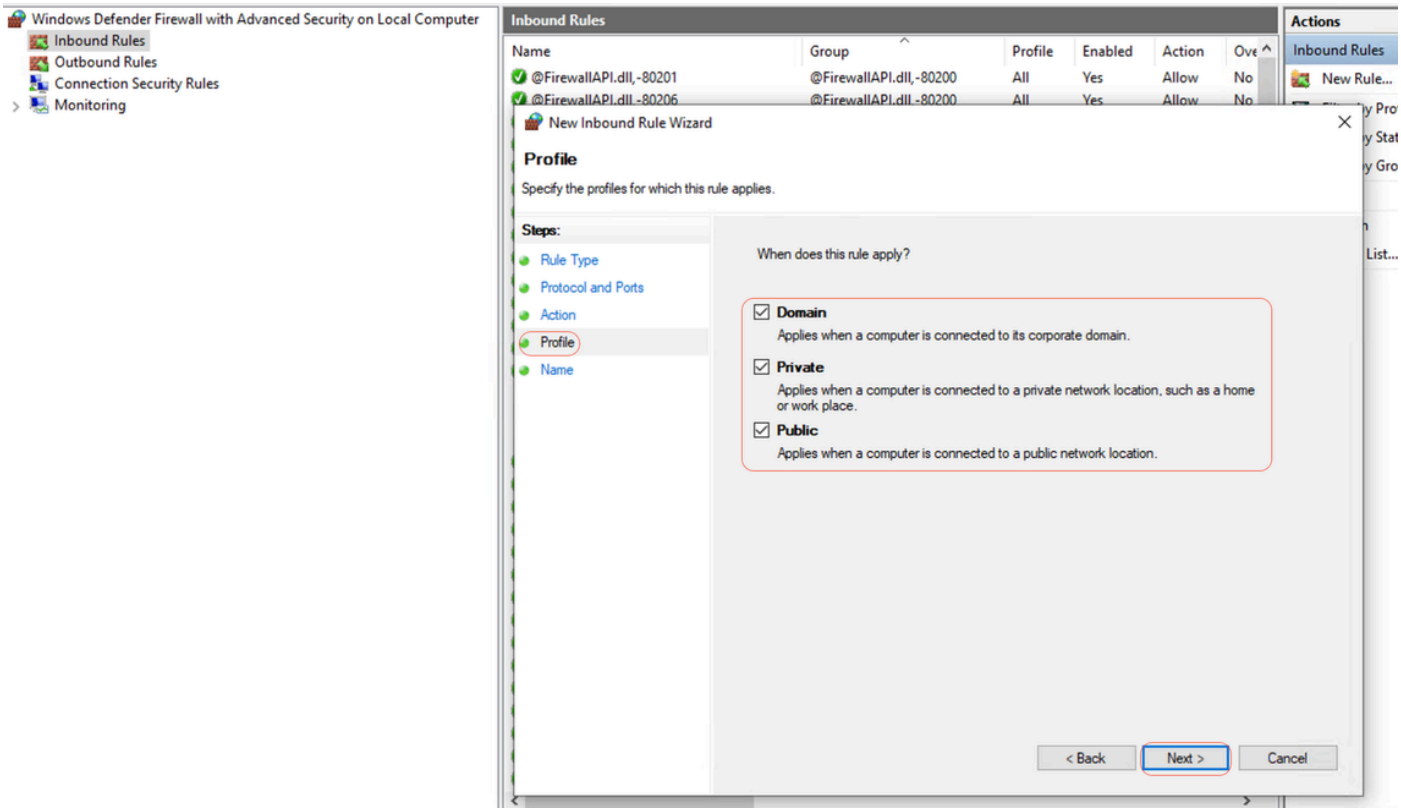
Protokolle und Ports

Schritt 3 - Wählen Sie unter **Aktion** > **Verbindung zulassen** > **Weiter aus**:



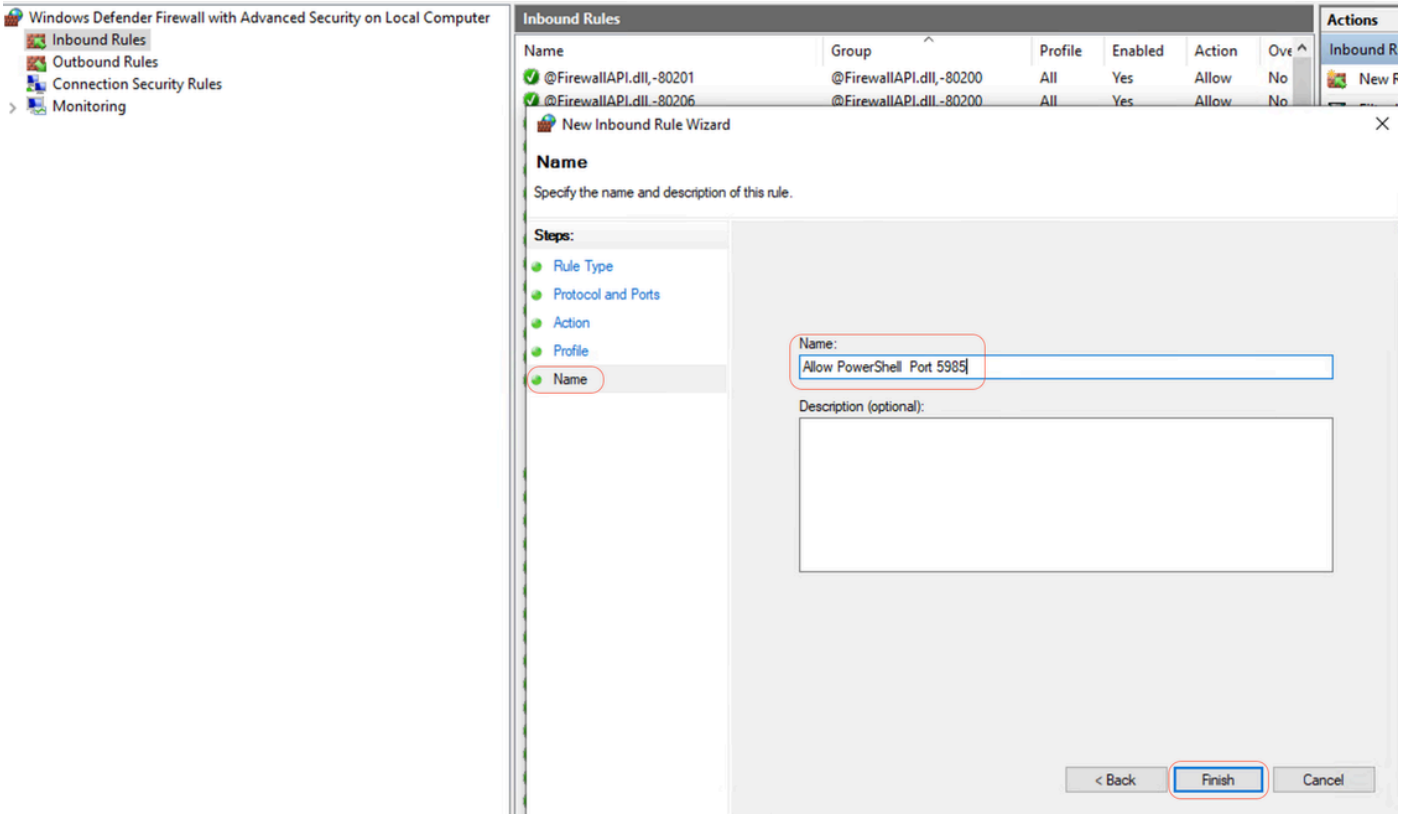
Aktion

Schritt 4: Aktivieren Sie unter Profil die Kontrollkästchen **Domäne**, **Privat** und **Öffentlich,** und klicken Sie auf **Weiter**:



Profil

Schritt 5: Geben Sie unter **Name** einen Namen für die Regel ein, z. B. **PowerShell auf Port 5985 zulassen,** und klicken Sie auf **Fertig stellen**:

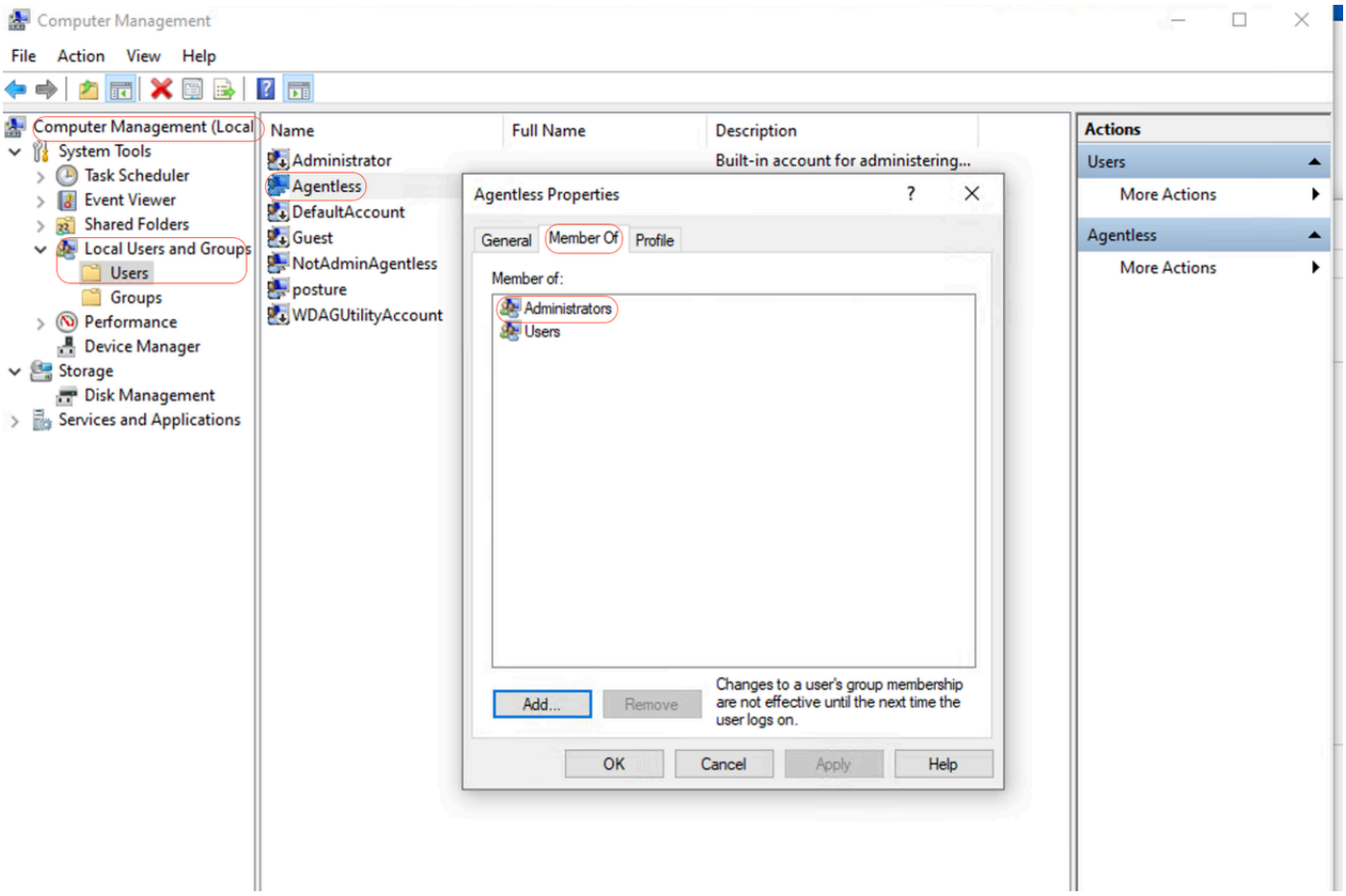


Name

Client-Anmeldedaten für Shell-Anmeldung müssen lokale Administratorberechtigungen haben.

Die Client-Anmeldeinformationen für die Shell-Anmeldung müssen über lokale Administratorberechtigungen verfügen. Um zu bestätigen, ob Sie über Administratorberechtigungen verfügen, gehen Sie wie folgt vor:

Gehen Sie in der Windows-GUI zu Einstellungen > Computerverwaltung > Lokale Benutzer und Gruppen > Benutzer > Benutzerkonto auswählen (in diesem Beispiel **ist** Agentless **Account ausgewählt) > Mitglied von, das Konto muss über eine Administratorgruppe verfügen.**



Lokale Administratorberechtigungen

WinRM-Listener wird überprüft

Stellen Sie sicher, dass der WinRM-Listener für **HTTP** auf Port **5985** konfiguriert ist:

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

Aktivieren von PowerShell Remoting WinRM

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass der Service ausgeführt wird und so konfiguriert ist, dass er automatisch startet:

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**

Erwartete Ausgabe:

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 muss v7.1 oder höher sein. Der Client muss über cURL v7.34 oder höher verfügen:

Überprüfen der PowerShell- und cURL-Versionen unter Windows

Stellen Sie sicher, dass Sie die entsprechenden Versionen von PowerShell verwenden. cURL ist für Posture Agentless von entscheidender Bedeutung:

Überprüfen der PowerShell-Version

Unter Windows:

1. **Öffnen Sie PowerShell:**

- Drücken Sie Win + X, und wählen Sie **Windows PowerShell** oder **Windows PowerShell (Admin) aus**.

2. Führen Sie den folgenden Befehl aus:$PSVersionTable.PSVersion

- Dieser Befehl gibt die Versionsdetails von PowerShell aus, die auf Ihrem System installiert sind.

Überprüfen der cURL-Version

Unter Windows:

1. Eingabeaufforderung öffnen:

- Drücken Sie Win + R, geben Sie cmd ein, und klicken Sie auf **Enter**.

2. Führen Sie den Befehl: curl --version

- Dieser Befehl zeigt die auf Ihrem System installierte Version von cURL an.

Ausgabe zum Überprüfen der PowerShell- und cURL-Versionen auf Windows-Geräten

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>

Zusätzliche Konfiguration

Mit diesem Befehl wird der Computer so konfiguriert, dass er bestimmten Remotehosts für WinRM-Verbindungen vertraut: 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> -

Das Cmdlet test-wsman mit den Parametern -Authentication Negotiate und -Credential ist ein leistungsstarkes Tool zum Überprüfen der Verfügbarkeit und Konfiguration des WinRM-Diensts auf einem Remotecomputer: test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

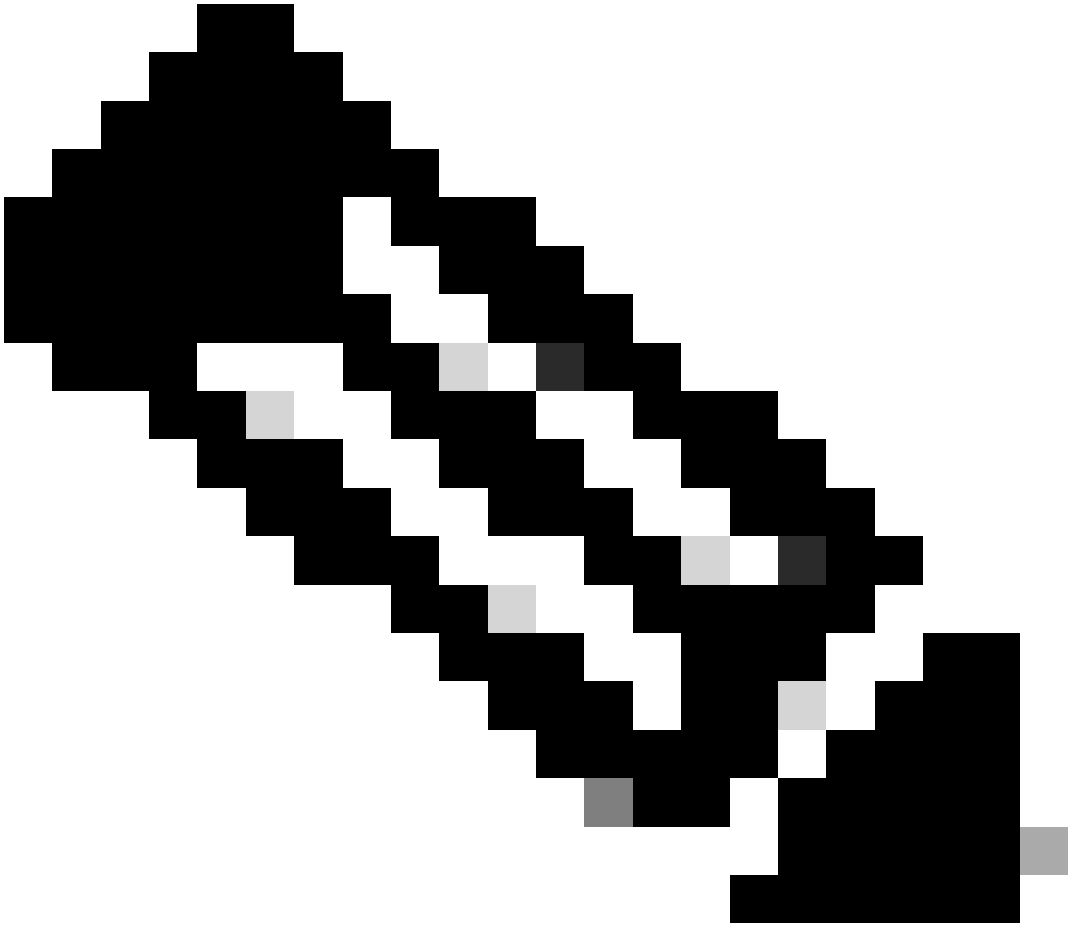
PowerShell muss v7.1 oder höher sein. Der Client muss über cURL v7.34 oder höher verfügen:

Unter MacOS:

1. **Terminal öffnen:**

- Terminal finden Sie unter **Anwendungen > Dienstprogramme**.

2. Führen Sie den Befehl: pwsh -Command '$PSVersionTable.PSVersion'



Hinweis: Hinweis: ・ Stellen Sie sicher, dass PowerShell Core (pwsh) installiert ist. Wenn nicht, können Sie es über Homebrew installieren (stellen Sie sicher, dass Sie Himebrew installieren): brew install --cask powershell

---

Unter MacOS:

1. **Terminal öffnen:**

・ Terminal finden Sie unter **Anwendungen > Dienstprogramme**.

2. Führen Sie den Befehl: curl --version

・ Dieser Befehl muss die auf Ihrem System installierte Version von cURL anzeigen.

Für MacOS-Clients muss Port 22 für den Zugriff auf SSH offen sein, damit auf den Client zugegriffen werden kann.

Detaillierte Anleitung:

1. **Systemeinstellungen öffnen:**

・ Navigieren Sie im Apple-Menü zu **Systemeinstellungen**.

2. **Remote-Anmeldung aktivieren:**

・ Gehe zu **Freigabe**.

・ Aktivieren Sie das Kontrollkästchen neben **Remote Login (Remote-Anmeldung)**.

・ Stellen Sie sicher, dass die Option **Zugriff zulassen für** auf die entsprechenden Benutzer oder Gruppen eingestellt ist. Durch Auswahl von **Alle Benutzer** kann sich jeder Benutzer mit einem gültigen Konto auf dem Mac über SSH anmelden.

3. **Firewall-Einstellungen überprüfen:**

・ Wenn die Firewall aktiviert ist, müssen Sie sicherstellen, dass SSH-Verbindungen zugelassen werden.

・ Gehen Sie zu **Systemeinstellungen > Sicherheit und Datenschutz > Firewall**.

・ Klicken Sie auf die Schaltfläche **Firewall Options (Firewall-Optionen**).

・ Überprüfen Sie, ob **Remote Login** oder **SSH** aufgeführt und zugelassen ist. Wenn es nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Hinzufügen** (+), um es hinzuzufügen.

4. **Port 22 bei Bedarf über Terminal öffnen:**

- Öffnen Sie die **Terminal**-Anwendung unter **Anwendungen > Dienstprogramme**.

- Verwenden Sie den Befehl pfctl, um die aktuellen Firewall-Regeln zu überprüfen und sicherzustellen, dass Port 22 offen ist:sudo pfctl -sr | Grep 22

- Wenn Port 22 nicht geöffnet ist, können Sie manuell eine Regel hinzufügen, um SSH:echo "pass in proto tcp from any to any port 22" zuzulassen. | sudo pfctl -ef -

5. **SSH-Zugriff testen:**

- Öffnen Sie von einem anderen Gerät aus ein Terminal oder einen SSH-Client.

- Verbindungsversuch mit dem macOS-Client über dessen IP-Adresse:ssh username@<macOS-client-IP>

- Ersetzen Sie den Benutzernamen durch das entsprechende Benutzerkonto und <macOS-client-IP> durch die IP-Adresse des macOS-Clients.

Stellen Sie für MacOS sicher, dass dieser Eintrag in der sudoers-Datei aktualisiert wird, um einen Fehler bei der Zertifikatinstallation auf den Endpunkten zu vermeiden:

Bei der Verwaltung von macOS-Endpunkten muss sichergestellt werden, dass bestimmte Administrationsbefehle ohne Kennwortanforderung ausgeführt werden können.

Voraussetzungen

- Administratorzugriff auf dem macOS-System.

- Grundlegende Kenntnisse der Terminalbefehle

Schritte zum Aktualisieren der Sudoers-Datei

1. **Terminal öffnen:**

- Terminal finden Sie unter **Anwendungen > Dienstprogramme**.

2. **Bearbeiten Sie die Sudoers-Datei:**

- Benutzen Sie den visudo Befehl, um die sudoers Datei sicher zu bearbeiten. Dadurch wird sichergestellt, dass Syntaxfehler vor dem Speichern der Datei abgefangen werden.sudo visudo

- Sie werden aufgefordert, Ihr Administratorkennwort einzugeben.

3. **Suchen Sie den entsprechenden Abschnitt:**

- Navigieren Sie im visudo Editor zu dem Abschnitt, in dem benutzerspezifische Regeln definiert sind. Normalerweise befindet sich dies am Ende der Datei.

4. **Erforderlichen Eintrag hinzufügen:**

- Fügen Sie diese Zeile hinzu, um dem angegebenen Benutzer die Berechtigung zum Ausführen der Sicherheits- und OSSCRIPT-Befehle ohne Kennwort zu erteilen: <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

- Ersetzen Sie **<macadminusername>** durch den tatsächlichen Benutzernamen des macOS-Administrators.

5. **Speichern und beenden:**

- Wenn Sie den Standard-Editor (nano) verwenden, drücken Sie Strg + X, um den Vorgang zu beenden, dann drücken Sie Y, um die Änderungen zu bestätigen, und schließlich die Eingabetaste, um die Datei zu speichern.

- Wenn Sie vi oder vim **verwenden**, drücken Sie Esc, geben Sie :wq ein, und drücken Sie die Eingabetaste, um zu speichern und den Vorgang zu beenden.

6. **Überprüfen Sie die Änderungen:**

- Um sicherzustellen, dass die Änderungen wirksam werden, können Sie einen Befehl ausführen, der die aktualisierten Sudo-Berechtigungen erfordert. Beispiele:

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

- Diese Befehle können ohne Eingabe eines Kennworts ausgeführt werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.