Configura postura senza agenti

Sommario

Introduzione

Questo documento descrive come configurare Posture Agentless in ISE e cosa è necessario nell'endpoint per eseguire lo script Agentless.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE).
- Postura.
- PowerShell e SSH
- Windows 10 o versione successiva.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Identity Services Engine (ISE) versione 3.3.
- Pacchetto Cisco Agentless Windows 5.1.6.6
- Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

ISE Posture esegue una valutazione lato client. Il client riceve la policy sui requisiti di postura da ISE, esegue la raccolta dei dati di postura, confronta i risultati con la policy e invia i risultati della valutazione all'ISE.

ISE determina quindi se il dispositivo è conforme o meno in base al report postura.

La postura senza agente è uno dei metodi di postura che raccoglie informazioni sulla postura dai clienti e si rimuove automaticamente al completamento senza richiedere alcuna azione da parte dell'utente finale. Postura senza agente si connette al client utilizzando i privilegi amministrativi.

Per iniziare

Prerequisiti:

- Il client deve essere raggiungibile tramite il relativo indirizzo IPv4o IPv6 e tale indirizzo IP deve essere disponibile nell'accounting RADIUS.

- Il client deve essere raggiungibile da Cisco Identity Services Engine (ISE) tramite il relativo indirizzo IPv4 o IPv6. Inoltre, questo indirizzo IP deve essere disponibile nell'accounting RADIUS.
- I client Windows e Mac sono attualmente supportati:
    - Per i client Windows, la porta 5985 per accedere a PowerShell deve essere aperta. Powershell deve essere v7.1 o versione successiva. Il client deve avere cURL v7.34 o versione successiva.
    - Per accedere ai client MacOS, la porta 22 deve essere aperta per accedere al client SSH. Il client deve avere cURL v7.34 o versione successiva.
- Le credenziali client per l'accesso alla shell devono disporre dei privilegi di amministratore locale.
- Eseguire l'aggiornamento del feed di postura per ottenere i client più recenti, come descritto nei passaggi di configurazione. Verificare:
- Per MacOS, assicurarsi che questa voce sia aggiornata nel file sudoers per evitare errori di installazione del certificato sugli endpoint: Controllare:

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

•

Per MacOS, l'account utente configurato deve essere un account amministratore. La postura senza agente per MacOS non funziona con altri tipi di account, anche se si concedono più privilegi.Per visualizzare questa finestra, fare clic sull'icona Menu () e **scegliereAmministrazione > Sistema > Impostazioni > Script endpoint** > **Configurazione di** accesso **> Utente locale MAC.**

•

In caso di modifiche nelle attività relative alle porte nei client Windows dovute agli aggiornamenti di Microsoft, è necessario riconfigurare il flusso di lavoro di configurazione della postura senza agente per i client Windows.

Condizioni di postura supportate

•

Condizioni di file, ad eccezione delle condizioni che utilizzano i percorsi di file USER_DESKTOP e USER_PROFILE

•

Condizioni del servizio, ad eccezione dei controlli System Daemon e Daemon o User Agent su macOS

- Condizioni dell'applicazione
- Condizioni origine dati esterna
- Condizioni composte
- Condizioni antimalware
- Condizione di gestione delle patch, ad eccezione **dei** controlli **EnabledandUp To** Datecondition
- Condizioni del firewall
- Condizioni di crittografia del disco, ad eccezione della verifica della condizione basata sulla posizione di crittografia
- Condizioni del Registro di sistema, ad eccezione di quelle che utilizzano HCSK come chiave radice

Condizioni di postura non supportate

- Correzione
-

Periodo di tolleranza

- Rivalutazione periodica

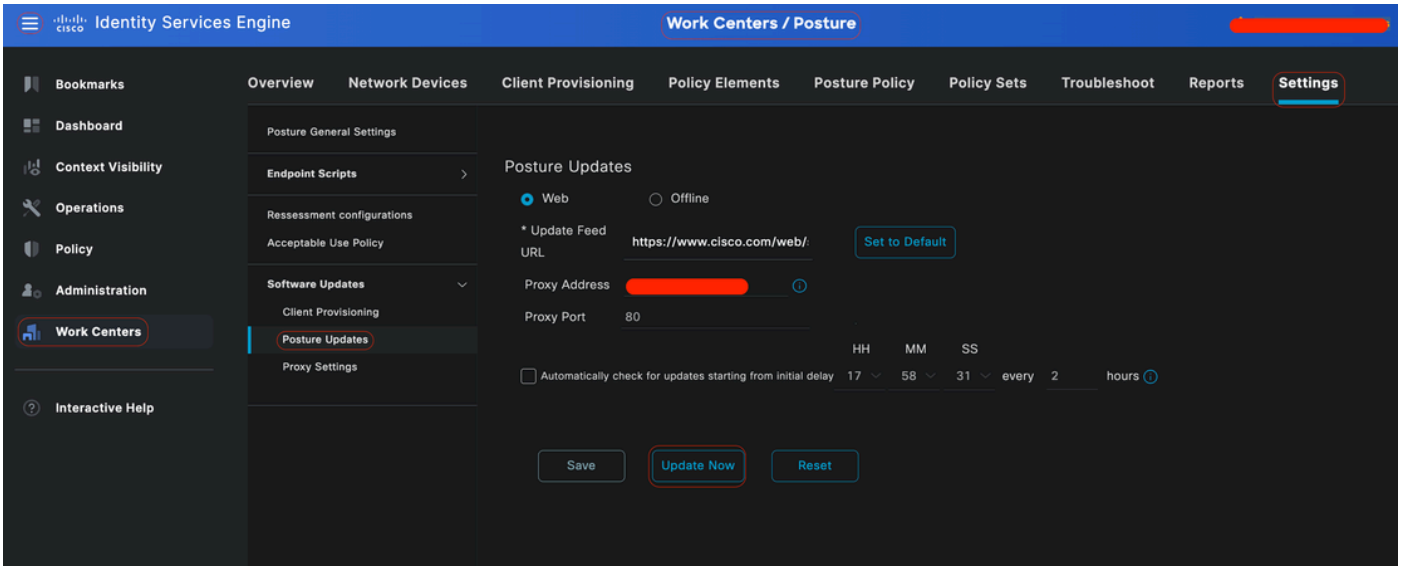
- Regole d'uso accettabili

Configurazione di ISE

Aggiorna feed postura

Si consiglia di aggiornare l'alimentazione prima di iniziare a configurare la postura.

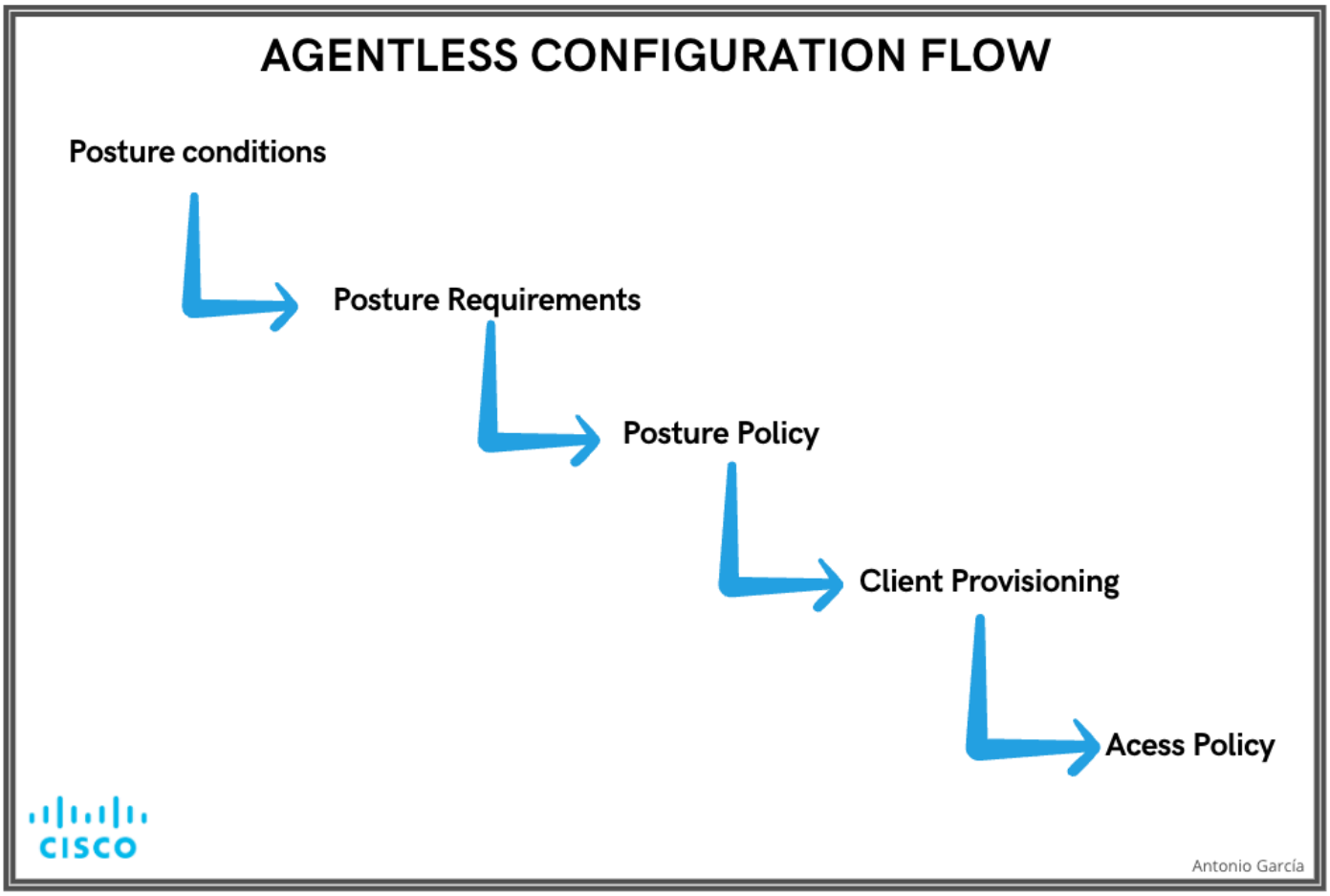
Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu ( ) e scegliere **Work Center > Posture > Settings** > **Software Updates** > **Update Now**.



Aggiornamento feed postura

Flusso di configurazione senza agente di postura

La configurazione senza agente di postura deve essere eseguita perché la prima configurazione sarà necessaria per quella successiva e così via. Si noti che il monitoraggio e l'aggiornamento non sono inclusi nel flusso. In seguito, tuttavia, verrà illustrata un'alternativa per la configurazione del monitoraggio e dell'aggiornamento.



Flusso di configurazione senza agente

Configurazione postura senza agente

Condizione di postura

Le condizioni di postura sono l'insieme di regole nei criteri di sicurezza che definiscono un endpoint conforme. Alcuni di questi elementi includono l'installazione di un firewall, software anti-virus, anti-malware, aggiornamenti rapidi, crittografia del disco e altro ancora.

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (

) e scegliere **Centri di lavoro > Postura > Elementi della policy** > Condizioni, fare clic su Aggiungi, quindi creare una o più **condizioni di** postura che utilizzino la postura senza agente per identificare il requisito. Una volta creata la **condizione**, fare clic su **Salva**.

In questo scenario, una condizione dell'applicazione denominata **"Agentless_Condition_Application"** è stata configurata con i seguenti parametri:

・**Sistema operativo:** Windows All

Questa condizione si applica a qualsiasi versione del sistema operativo Windows, garantendo un'ampia compatibilità tra diversi ambienti Windows.

・**Check-by:** Elaborazione

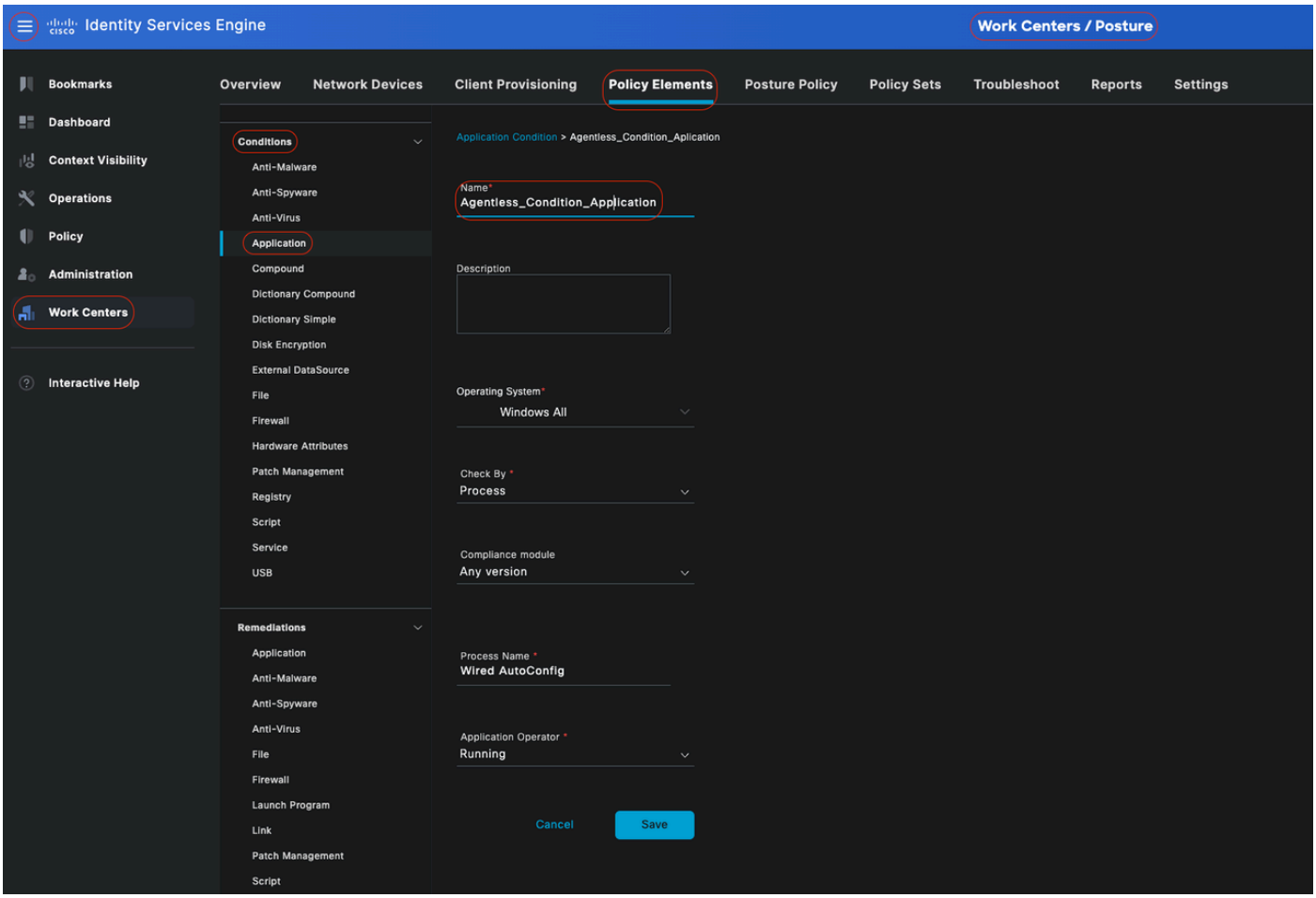
Il sistema esegue il monitoraggio dei processi all'interno del dispositivo. È possibile selezionare **Process** o **Application**; in questo caso, è stato scelto **Process**.

・**Nome processo:** configurazione automatica reti cablate

Il processo **Wired AutoConfig** è il processo Compliant Module sta per eseguire il check-in del dispositivo. Questo processo è responsabile della configurazione e della gestione delle connessioni di rete cablate, inclusa l'autenticazione IEEE 802.1X.

・**Operatore applicazione:** in esecuzione

Il modulo di conformità verifica se il processo **Wired AutoConfig** è attualmente in esecuzione sul dispositivo. È possibile selezionare **In esecuzione** o **Non in esecuzione**. In questo caso, **Running** è stato selezionato per assicurare che il processo sia attivo.



Condizione senza agente

Requisito postura

Un requisito di postura è un insieme di condizioni composte o una sola condizione che può essere collegata a un ruolo e a un sistema operativo. Tutti i client che si connettono alla rete devono soddisfare i requisiti obbligatori durante la valutazione della postura per diventare conformi sulla rete.

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu ( ) e scegliere **Centri di lavoro > Postura** > **Elementi delle policy** > **Requisito**. Fare clic sulla **freccia giù** e selezionare **Inserisci nuovo requisito**, quindi creare uno o più **PostureRequirement** che utilizzano la postura senza agente. Una volta creato il **requisito**, fare clic su **Chiudi** e quindi su **Salva**.

In questo caso, un requisito applicazione denominato **"Agentless_Requirement_Application"** è stato configurato con i seguenti criteri:

· **Sistema operativo:** Windows All

Questo requisito si applica a qualsiasi versione del sistema operativo Windows, assicurandone l'applicabilità in tutti gli ambienti Windows.

· **Tipo di postura:** senza agente

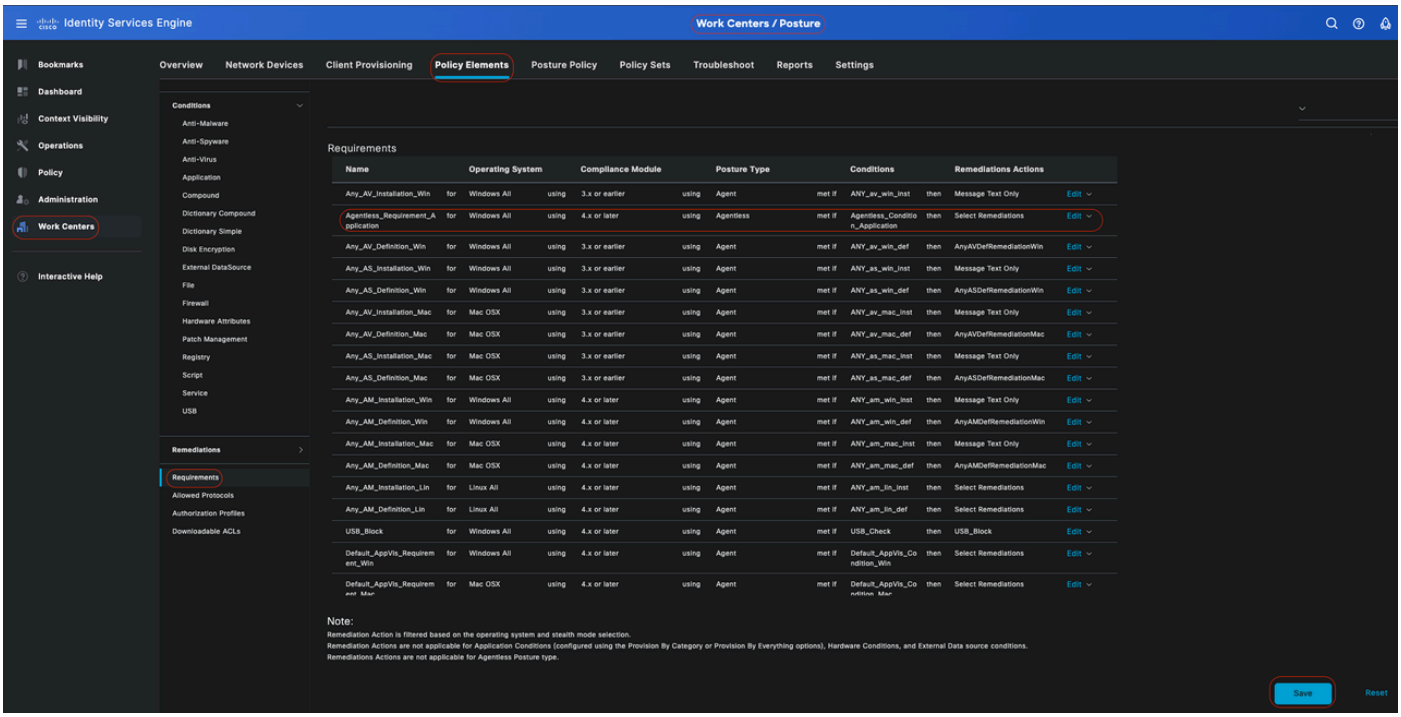
Questa configurazione è impostata per un ambiente senza agenti. Le opzioni disponibili includono **Agent**, **Agent Stealth**, **Temporal Agent** e **Agentless**. In questo scenario è stato selezionato **Agentless**.

· **Condizioni: Agentless_Condition_Application**

Specifica la condizione che ISE Posture Module e Compliance Module dovranno verificare nei processi del dispositivo. La condizione selezionata è **Agentless_Condition_Application**.

· **Azioni correttive:**

Poiché questa configurazione è per un ambiente senza agente, le azioni di risoluzione non sono supportate e questo campo è disattivato.



Requisito senza agente

Criteri di postura

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (

) e **scegliere Centri di lavoro** > **Postura** > **Postura Policy.** Fare clic sulla **freccia rivolta verso il basso** e selezionare **Inserisci nuovo requisito**, quindi creare una o più regole dei **criteri di postura** supportate che utilizzano la postura senza agente per il requisito di postura specifico. Una volta creato il **criterio di postura**, fate clic su **Fine (Done)** e quindi su **Salva (Save)**.

In questo scenario, un criterio di postura denominato **"Agentless_Policy_Application"** è stato configurato con i seguenti parametri:

· **Nome regola:** Agentless_Policy_Application

Questo è il nome designato per il criterio di postura in questo esempio di configurazione.

· **Sistema operativo:** Windows All

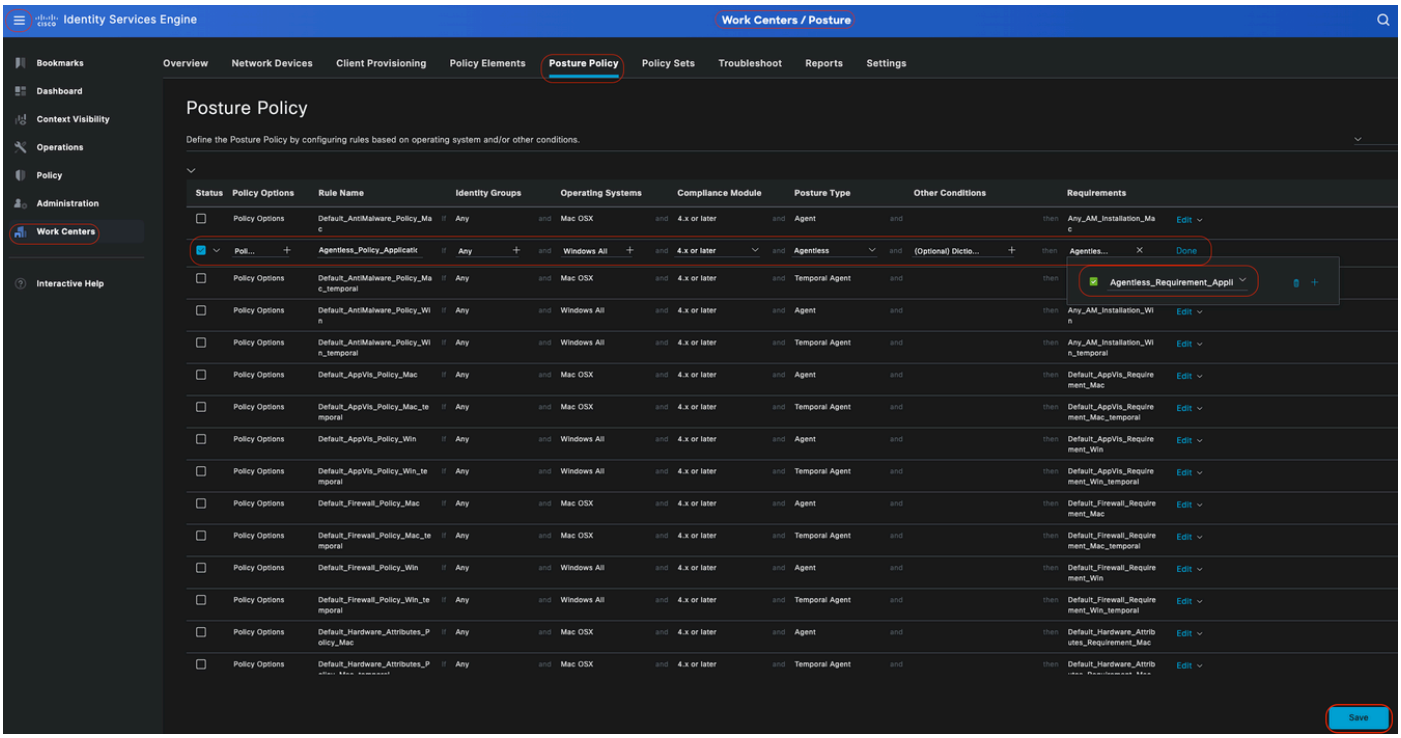
Il criterio è impostato per essere applicato a tutte le versioni del sistema operativo Windows, garantendo un'ampia compatibilità tra diversi ambienti Windows.

· **Tipo di postura:** senza agente

Questa configurazione è impostata per un ambiente senza agenti. Le opzioni disponibili includono **Agent**, **Agent Stealth**, **Temporal Agent** e **Agentless**. In questo scenario, è stato selezionato **Agentless**.

· **Altre condizioni:**

In questo esempio di configurazione non sono state create condizioni aggiuntive. Tuttavia, è possibile configurare condizioni specifiche per garantire che solo i dispositivi di destinazione siano soggetti a questo criterio di postura, anziché a tutti i dispositivi Windows della rete. Ciò può essere particolarmente utile per la segmentazione della rete.



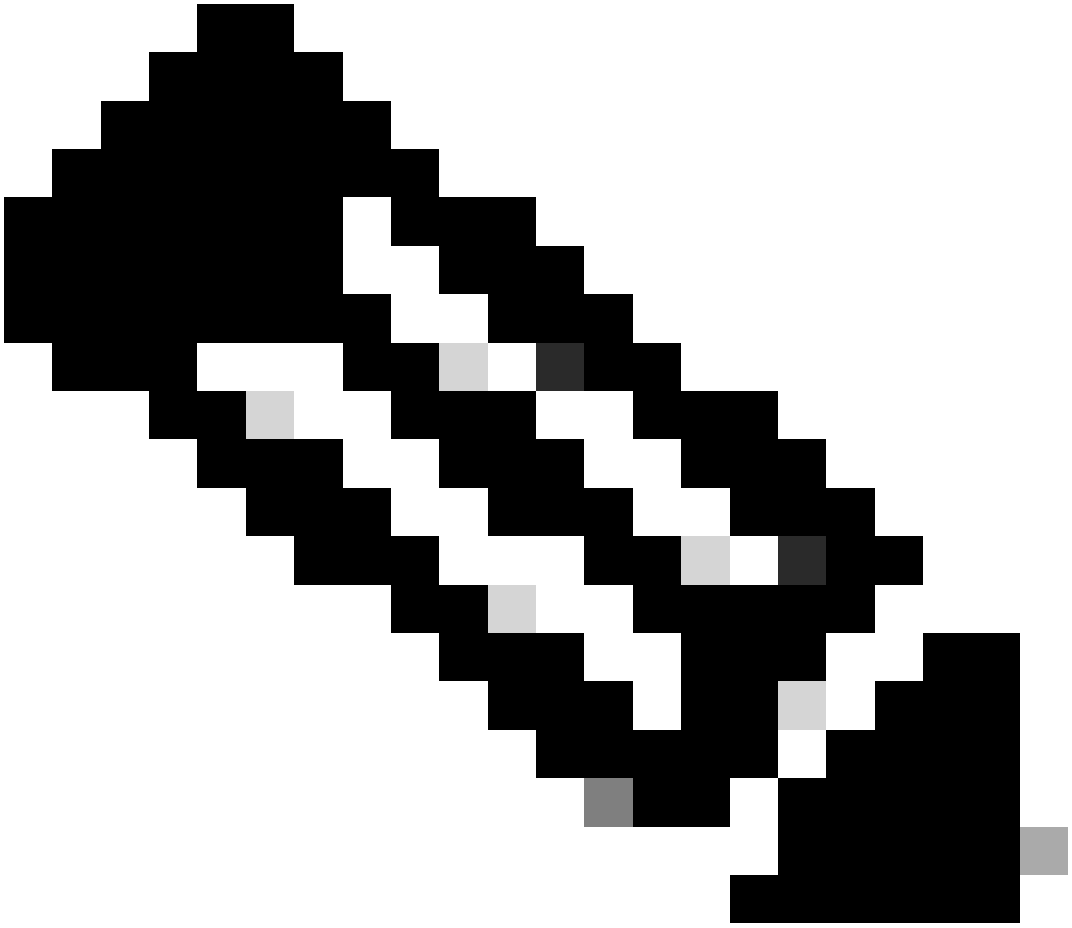
Criterio postura senza agente

Provisioning client

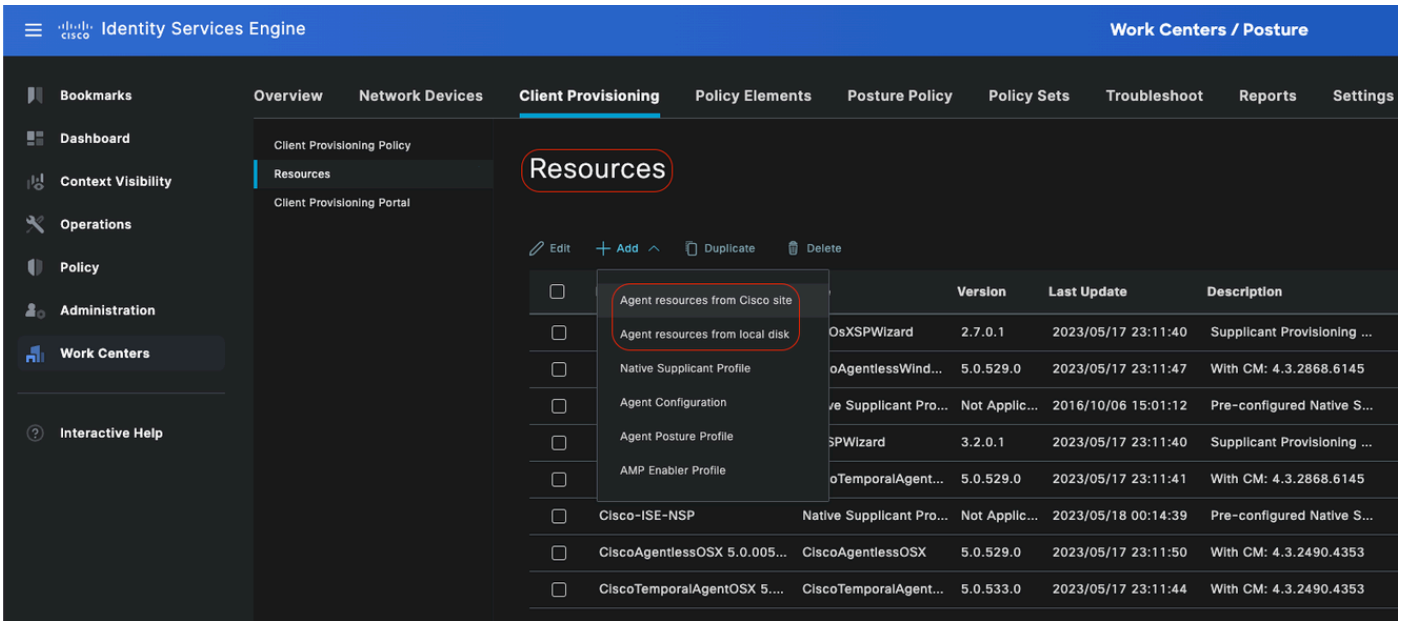
Fase 1 - Download delle risorse

Per avviare la configurazione del provisioning client, è necessario innanzitutto scaricare le risorse necessarie e renderle disponibili in ISE in modo da poterle utilizzare in un secondo momento in Client Provisioning Policy.

Esistono due modi per aggiungere risorse ad ISE: **risorse agente dal sito Cisco** e **risorse agente dal disco locale**. Poiché si sta configurando la modalità senza agente, è necessario passare attraverso le **risorse agente dal sito Cisco** per scaricare.



Nota: per utilizzare le **risorse dell'agente dal sito Cisco**, ISE PAN deve disporre dell'accesso a Internet.



Risorse

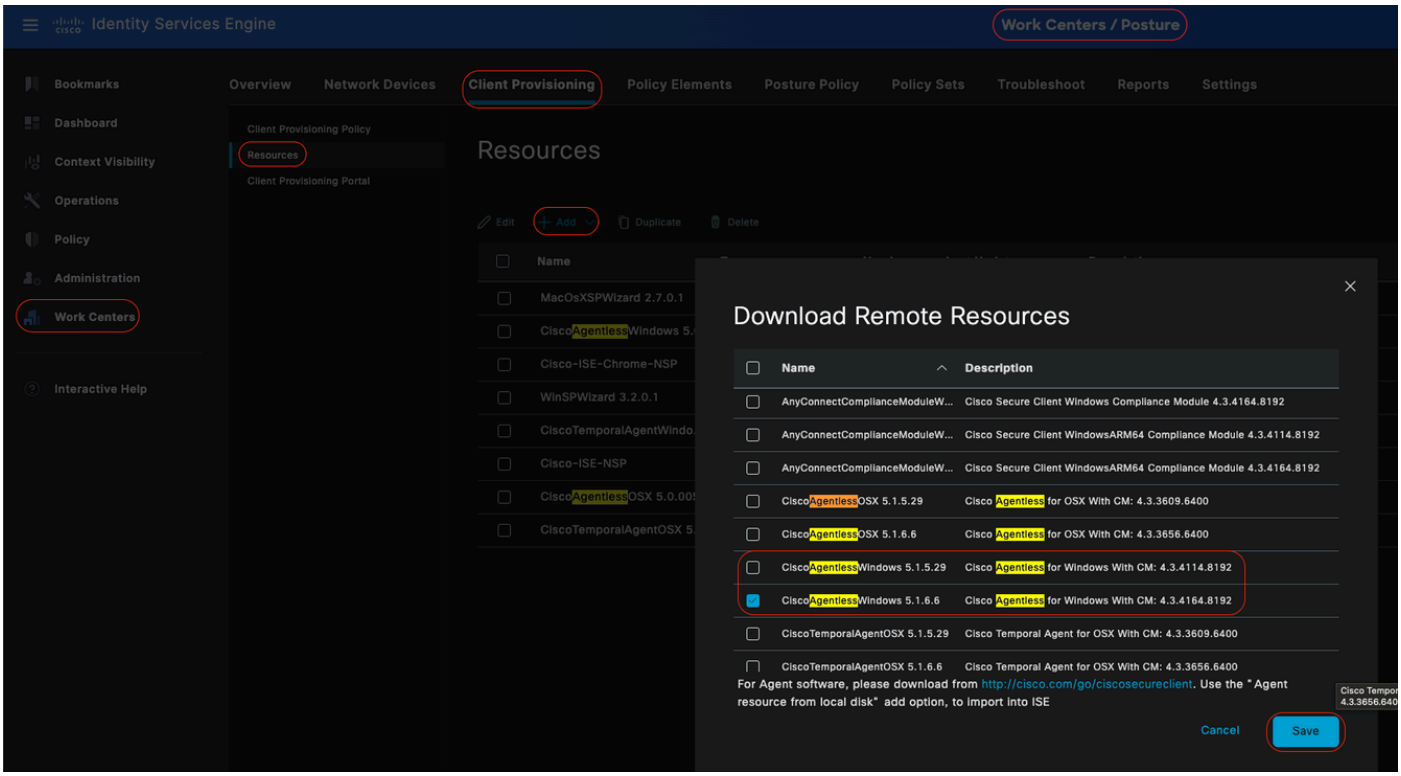
Risorse agente dal sito Cisco

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu ( ) e scegliere **Centri di lavoro** > **Postura** > **Provisioning client** > **Risorse**. Fare clic su **Add** , Select **Agent Resources from Cisco site**, quindi su **Save**.

Dal sito Cisco, è possibile scaricare solo il Modulo di conformità. Nel sistema vengono visualizzati i due moduli di conformità più recenti da scaricare. Pacchetto di risorse **CiscoAgentlessWindows 5.1.6.6** selezionato per questo esempio di configurazione. È destinato solo ai dispositivi Windows.

.

Risorse



agente dal sito Cisco

Fase 2 - Configurazione dei criteri di provisioning client

Quando si configura Posture Agent, sono necessarie due risorse diverse (**AnyConnect** o **Secure Client** e **Compliance Module**),

Eseguire il mapping di entrambe le risorse in **Configurazione agente** insieme al **profilo di postura agente** in modo da poter utilizzare questa **configurazione agente** nei criteri di **provisioning client.**

Tuttavia, quando si configura una postura senza agente, non è necessario configurare la **configurazione dell'agente** o il **profilo di postura dell'agente**, ma è sufficiente scaricare il pacchetto senza agente solo **dalle risorse dell'agente dal sito Cisco**.

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu ( ) e scegliere **Workcenter** > **Postura** > **Client Provisioning** > **Client Provisioning Policy**. Fare clic sulla **freccia rivolta verso il** basso e selezionare **Inserisci nuovo criterio sopra** o **Inserisci nuovo criterio sotto**, **Duplica sopra** o **Duplica sotto:**

- **Nome regola: Agentless_Client_Provisioning_Policy**

Specifica il nome del criterio di provisioning client.

- **Sistema operativo:** Windows All

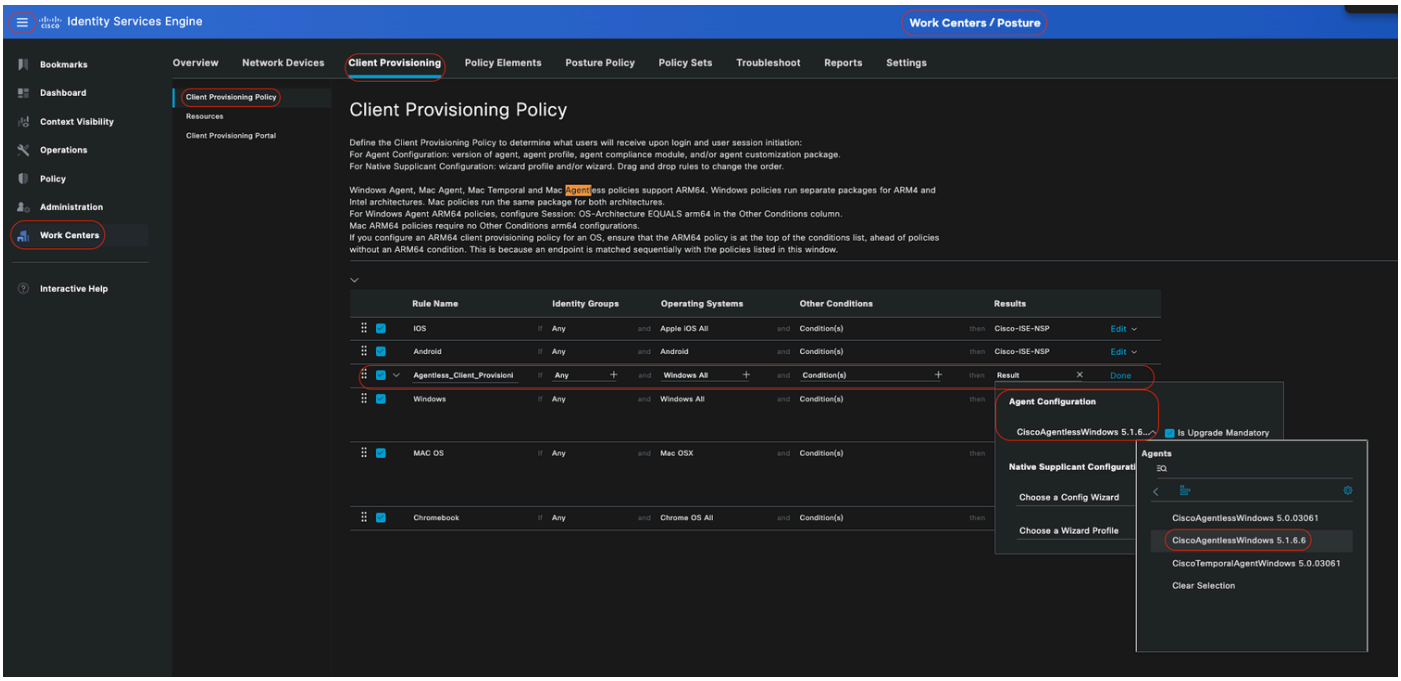
In questo modo il criterio verrà applicato a tutte le versioni del sistema operativo Windows.

- **Altre condizioni:** in questo esempio non sono configurate condizioni specifiche. È tuttavia possibile configurare le condizioni in modo che solo i dispositivi desiderati soddisfino questo criterio di provisioning client, anziché tutti i dispositivi Windows della rete. Ciò è particolarmente utile per la segmentazione della rete.

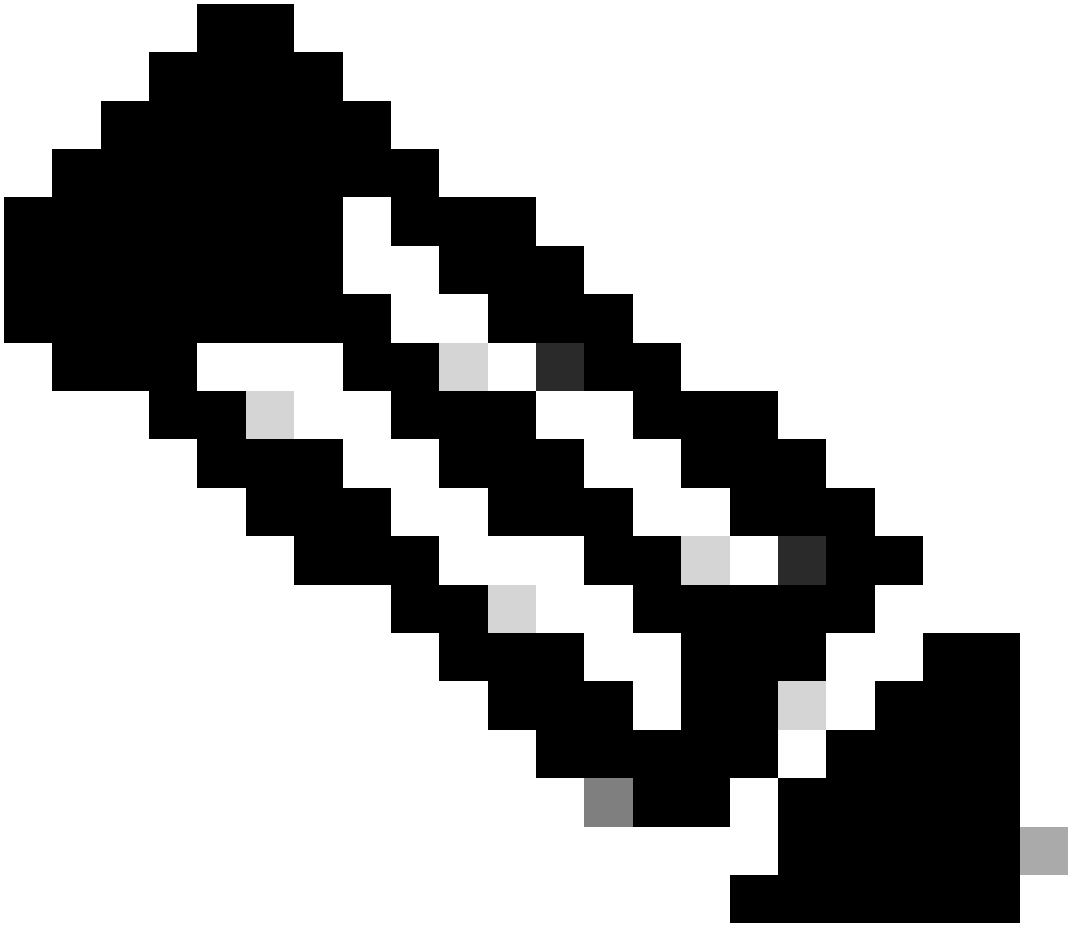
Esempio: se si utilizza Active Directory, è possibile incorporare i gruppi di Active Directory nei criteri per individuare i dispositivi interessati.

- **Risultati:** selezionare il package o l'agente di configurazione appropriato. Poiché si sta configurando un ambiente senza agente, scegliere il pacchetto **Cisco Agentless Windows 5.1.6.6**, precedentemente scaricato dal **sito Risorse agente da Cisco**. Questo pacchetto senza agente contiene tutte le risorse necessarie (**Software senza agente** e **Modulo di conformità**) necessarie per l'esecuzione di Posture senza agente.

•Fare clic su Salva.



Criterio di provisioning client senza agente



Nota: verificare che solo un criterio di provisioning client soddisfi le condizioni per ogni tentativo di autenticazione. Se si valutano più criteri contemporaneamente, è possibile che si verifichino comportamenti imprevisti e potenziali conflitti.

Profilo di autorizzazione senza agente

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu (

) e scegliere Policy > **Elementi** della policy **> Risultati > Autorizzazione > Profili di autorizzazione, quindi creare un profilo di autorizzazione** che valuti i risultati dalla postura senza agente.

- In questo esempio di configurazione, denominato Profilo di autorizzazione come **Agentless_Authorization_Profile**.

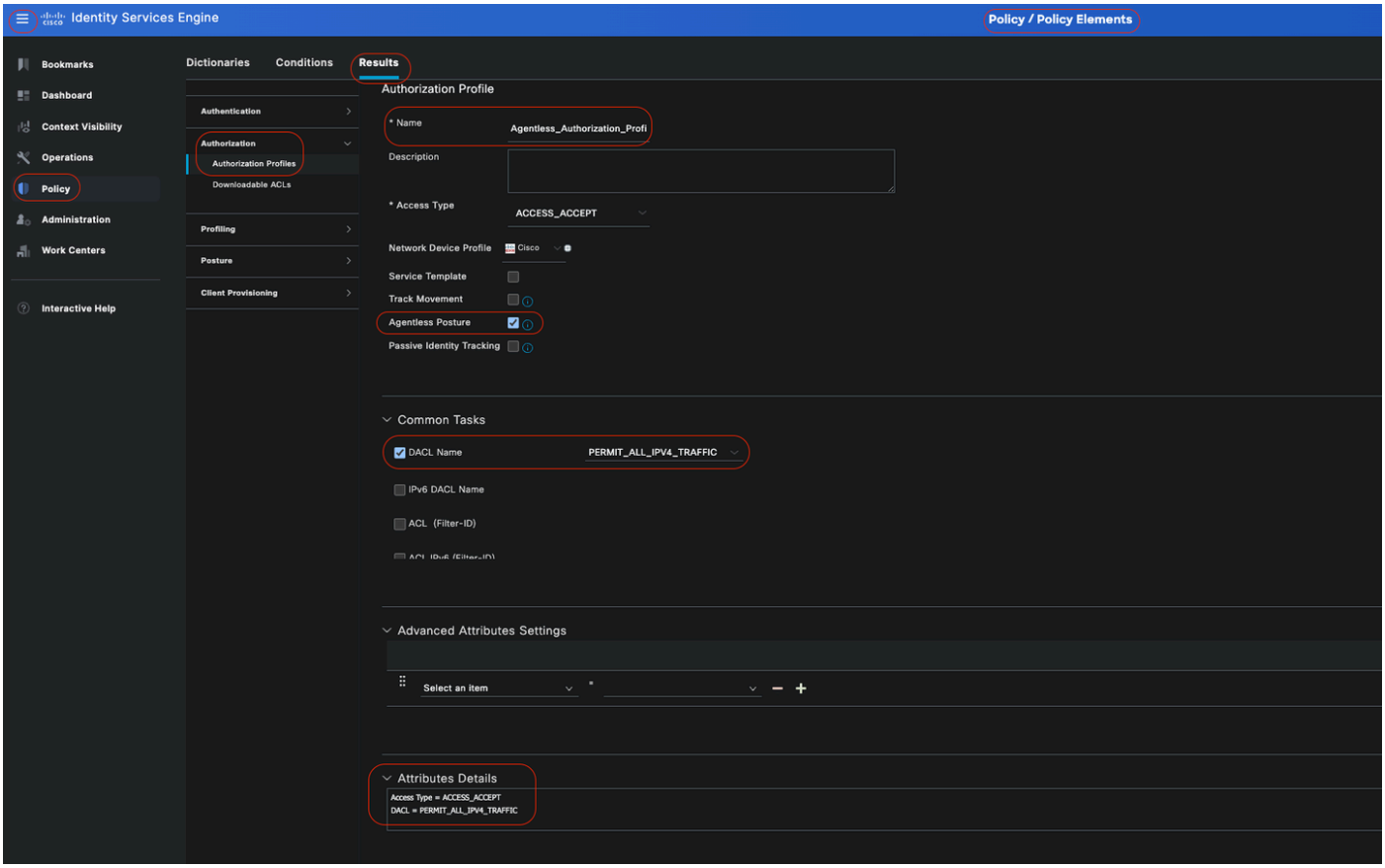
- Abilitare la postura senza agente nel profilo di autorizzazione.

- Utilizzare questo profilo solo per la **postura senza agente**. Non utilizzatelo anche per altri tipi di postura.

- CWA e ACL di reindirizzamento non sono richiesti per la postura senza agente. È possibile usare VLAN, DACL o ACL come parte delle regole di segmentazione. Per semplificare le procedure, oltre al controllo della postura senza agente in questo esempio di configurazione, è configurato solo un dACL (che consente tutto il traffico ipv4).

-

Fare clic su **Save**.



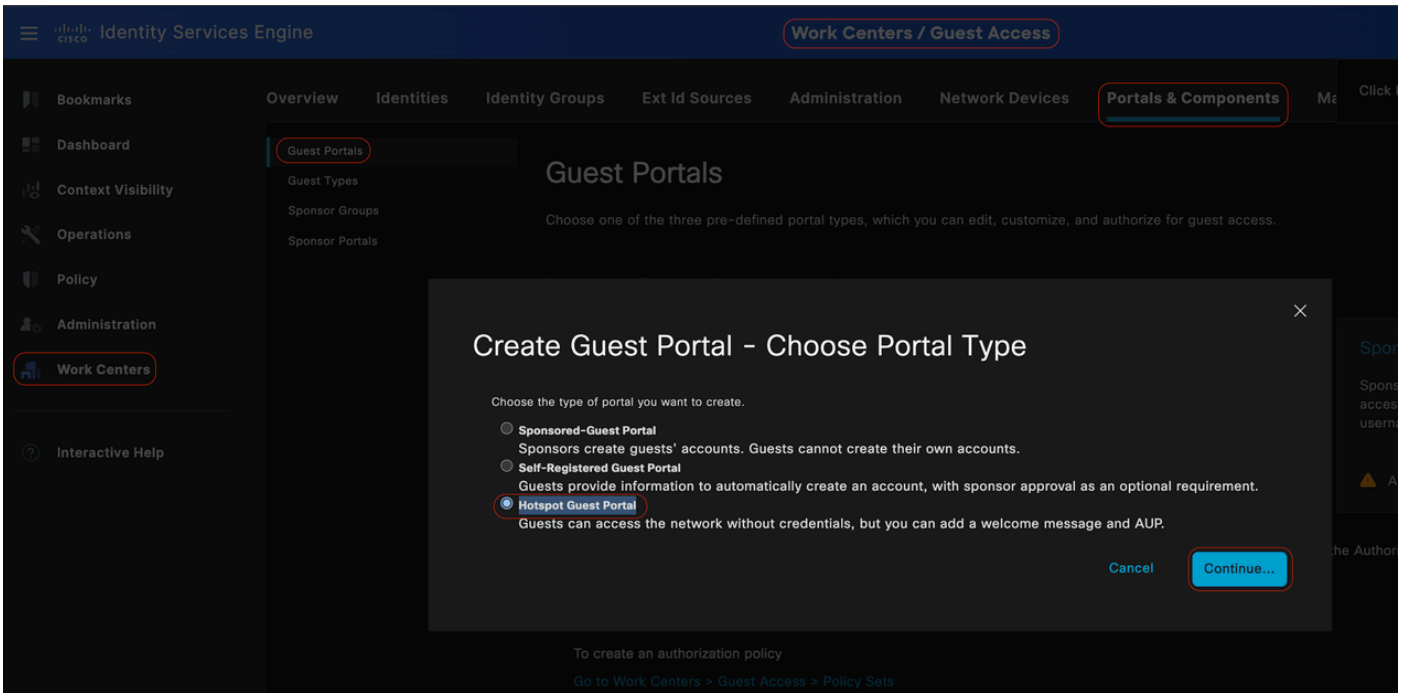
Profilo di autorizzazione senza agente

Alternativa all'utilizzo della risoluzione (facoltativa)

Supporto per la correzione nel flusso senza agente non disponibile. Per risolvere questo problema, è possibile implementare un portale di hotspot personalizzato per aumentare la consapevolezza degli utenti in merito alla conformità degli endpoint. Quando un endpoint viene identificato come non conforme, gli utenti possono essere reindirizzati a questo portale. Questo approccio garantisce che gli utenti siano informati sullo stato di conformità dei loro endpoint e possano intraprendere le azioni appropriate per correggere eventuali problemi.

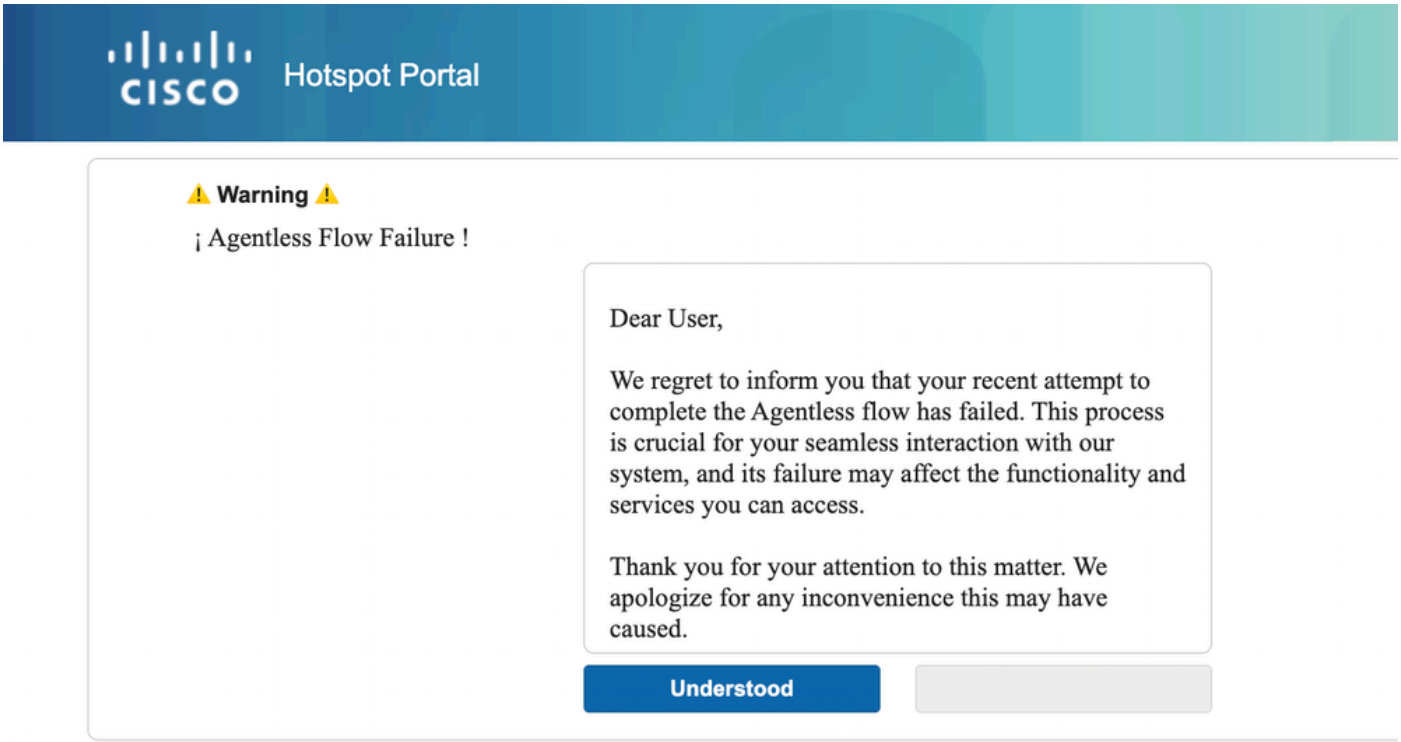
Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (

) e scegliere **Work Center** > **Guest Access** > **Portals & Components** >**Guest Portals.** Fare clic su **Create** > Select **Hotspot Guest Portal** > **Continue:** . In questo esempio di configurazione, il portale hotspot è denominato **Agentless_Warning**.



Portale guest hotspot

Nelle impostazioni del portale è possibile personalizzare i messaggi visualizzati agli utenti finali in modo da allinearli ai requisiti specifici. Si tratta solo di un esempio di visualizzazione personalizzata del portale:



Agente di postura non riuscito

Profilo di autorizzazione monitoraggio e aggiornamento **(facoltativo)**

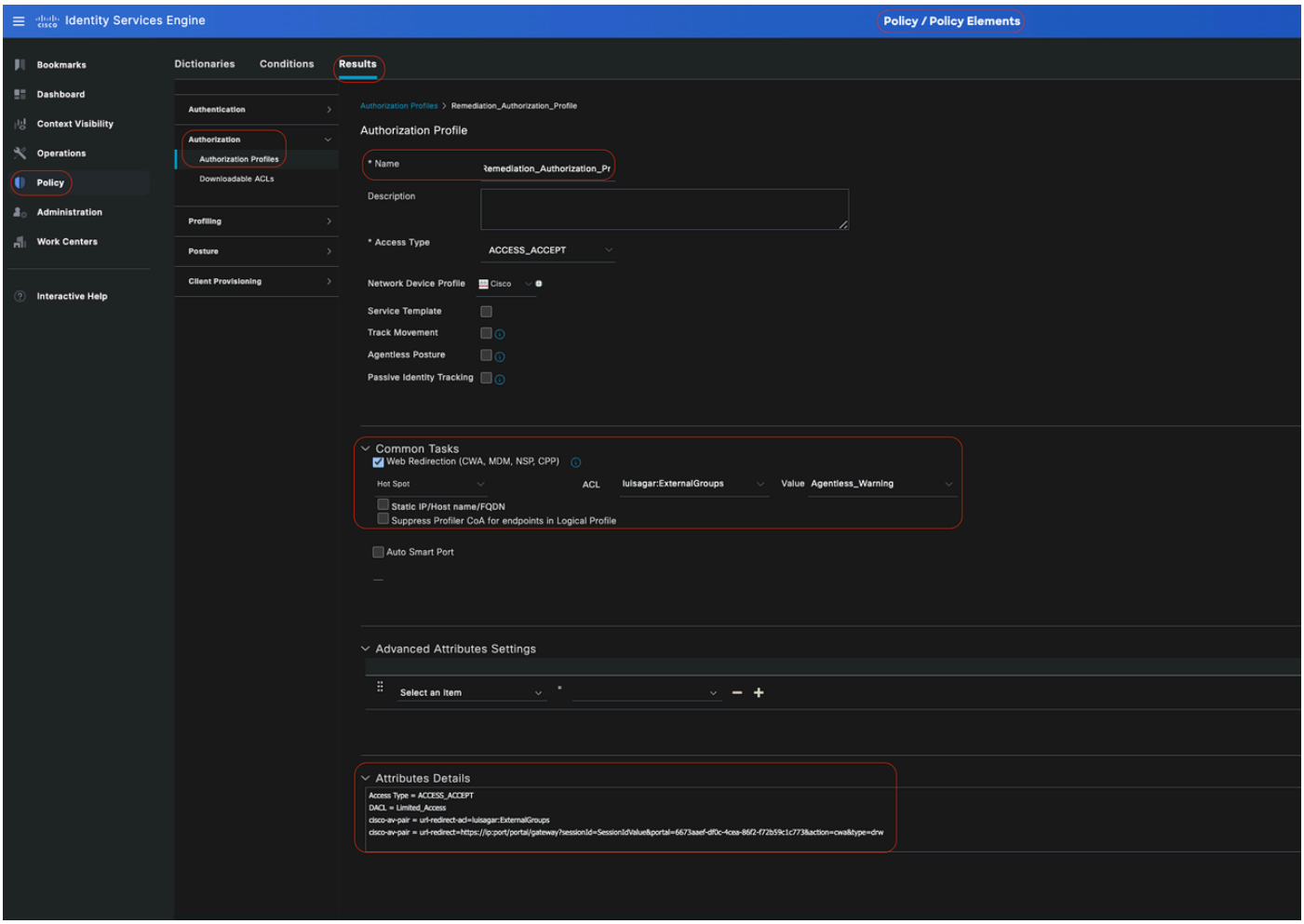
Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (), scegliere Policy > **Elementi della** policy **> Risultati > Autorizzazione > Profili di autorizzazione e creare un profilo di autorizzazione** per la risoluzione del problema.

- In questo esempio di configurazione, denominato Profilo di autorizzazione come **Profilo_autorizzazione_risoluzione**.

- Per semplicità, questo esempio di configurazione include solo un elenco di controllo di accesso (Access Control List, dACL) scaricabile denominato **Limited_Access** che consente un accesso limitato e personalizzato in base alle esigenze specifiche dell'organizzazione.

- La funzionalità **Reindirizzamento Web** è stata configurata includendo un gruppo esterno e l'hotspot, in modo da aumentare la consapevolezza dell'utente in merito alla conformità degli endpoint.

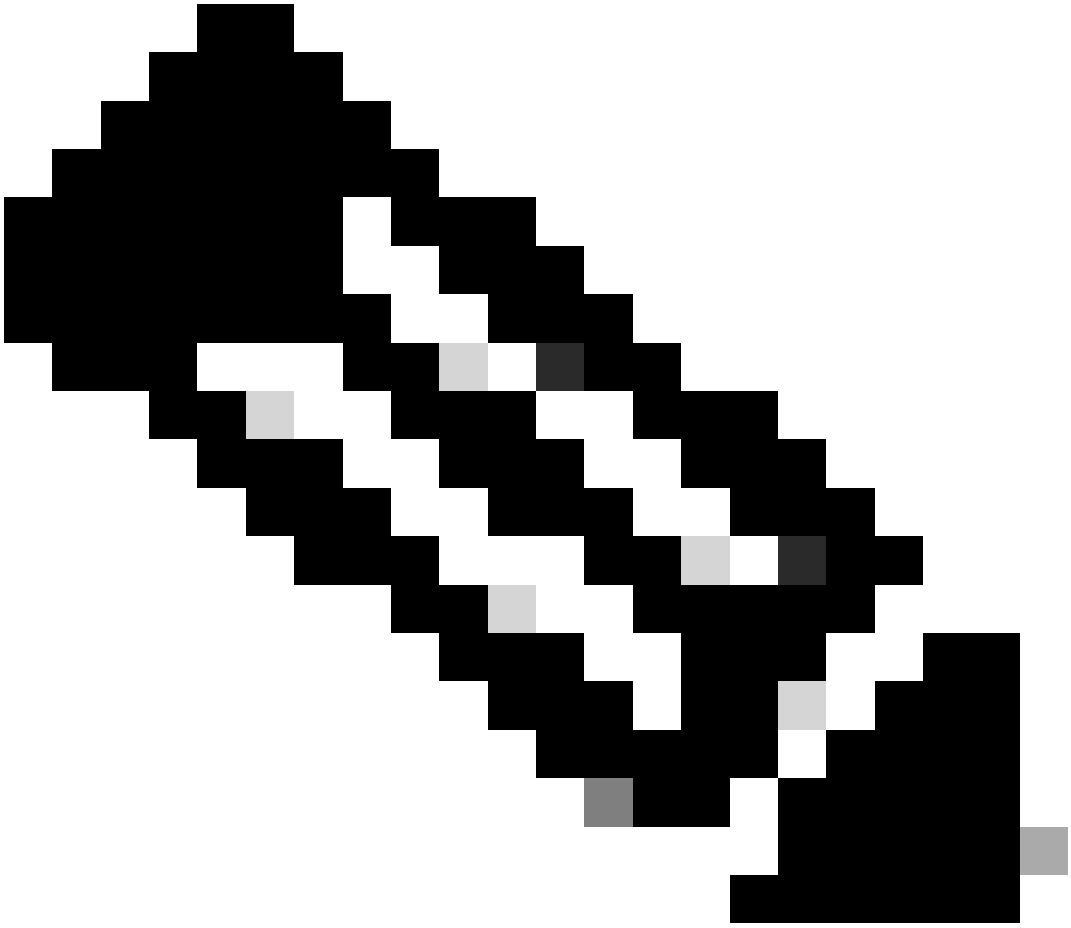
- Fare clic su **Save** (Salva).



Regola di autorizzazione monitoraggio e aggiornamento

Regola di autorizzazione senza agente

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu ( ), **quindi selezionare Policy** > **Policy** Settings ed espandere **Authorization Policy**. Abilitare e configurare i tre criteri di autorizzazione seguenti:



Nota: queste regole di autorizzazione devono essere configurate nell'ordine specificato per garantire il corretto funzionamento del flusso di postura.

Unknown_Compliance_Redirect:

•Condizioni:

Configurare Network_Access_Authentication_Passed AND **Compliance_Unknown_Devices** con il set di risultati impostato su Postura senza agente. Questa condizione attiva il flusso senza agente.

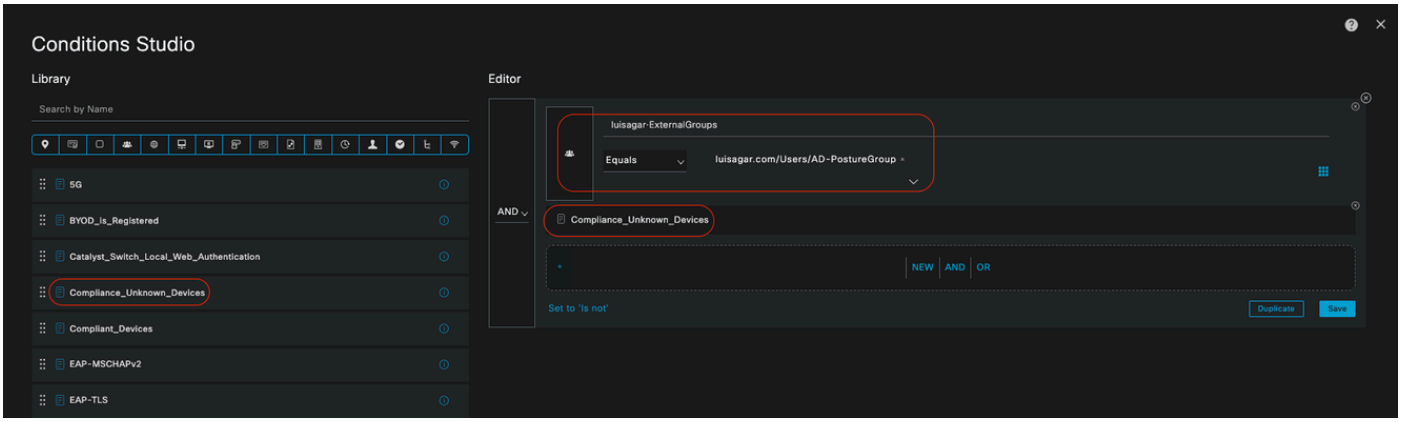
· Condizioni di esempio:

Configurare una condizione del gruppo di Active Directory (AD) per segmentare il traffico.

La condizione **Compliance_Unknown_Devices** deve essere configurata perché lo stato di postura iniziale è sconosciuto.

· Profilo di autorizzazione:

Assegnare **Agentless_Authorization_Profile** a questa regola di autorizzazione per garantire che i dispositivi passino attraverso il flusso della postura senza agente. Questa condizione contiene il flusso senza agente in modo che i dispositivi che utilizzano questo profilo possano avviare il flusso senza agente.



Regola di autorizzazione sconosciuta

NonCompliant_Devices_Redirect:

· Condizioni: configurare Network_Access_Authentication_Passed e Non_Compliant_Devices con il risultato impostato su DenyAccess. In alternativa, è possibile utilizzare l'opzione di correzione, come illustrato in questo esempio.

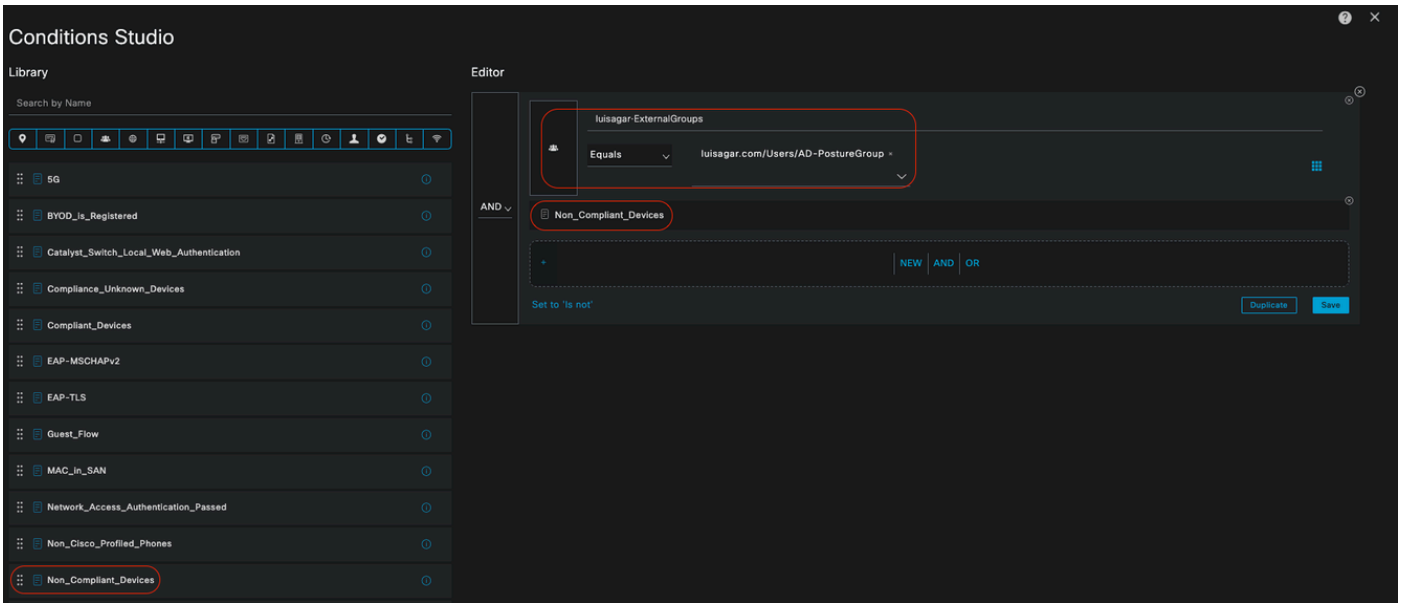
· Condizioni di esempio:

Configurare una condizione del gruppo AD per segmentare il traffico.

La condizione **Compliance_Unknown_Devices** deve essere configurata per assegnare risorse limitate quando lo stato della postura non è conforme.

· Profilo di autorizzazione:

Assegnare **Remediation_Authorization_Profile** a questa regola di autorizzazione per notificare lo stato corrente ai dispositivi non conformi tramite il **portale hotspot** o per negare l'**accesso**.



Regola di autorizzazione non conforme

Accesso_Dispositivi_Conformi:

•Condizioni:

Configurare Network_Access_Authentication_Passed e **Compliant_Devices** con il set di risultati impostato su PermitAccess.

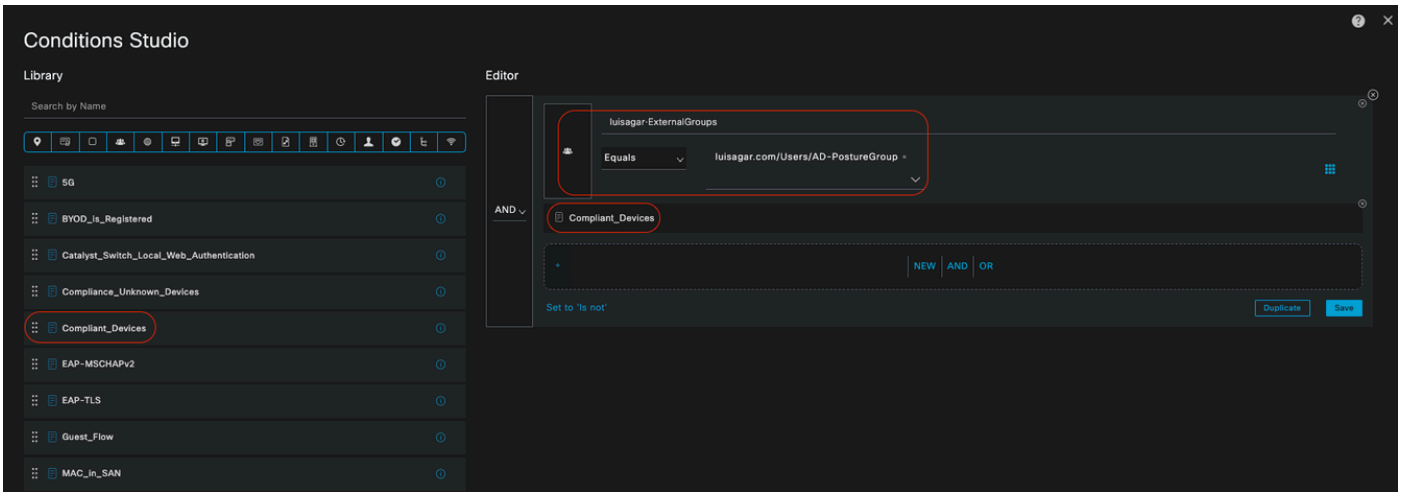
· Condizioni di esempio:

Configurare una condizione del gruppo AD per segmentare il traffico.

La condizione **Compliance_Unknown_Devices** deve essere configurata in modo che ai dispositivi conformi venga concesso l'accesso appropriato.

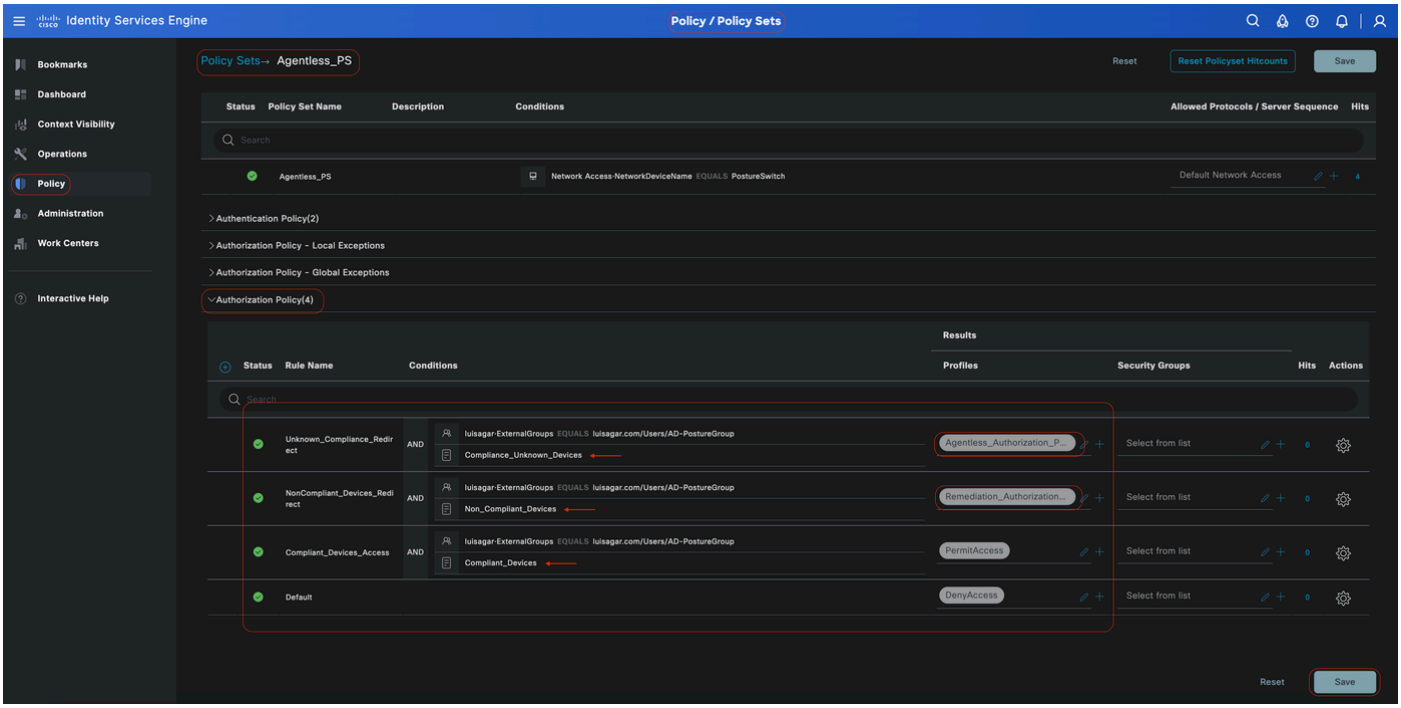
· Profilo di autorizzazione:

Assegnare **PermitAccess** a questa regola di autorizzazione per garantire l'accesso ai dispositivi conformi. Questo profilo può essere personalizzato in base alle esigenze dell'organizzazione.



Regola di autorizzazione conforme

Tutte le regole di autorizzazione



Regole di autorizzazione

Configura credenziali di accesso endpoint

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu ( ), **quindi selezionare Amministrazione** > **Impostazioni** > **Script endpoint** > **Configurazione di accesso** e configurare le credenziali del client per l'accesso ai client.

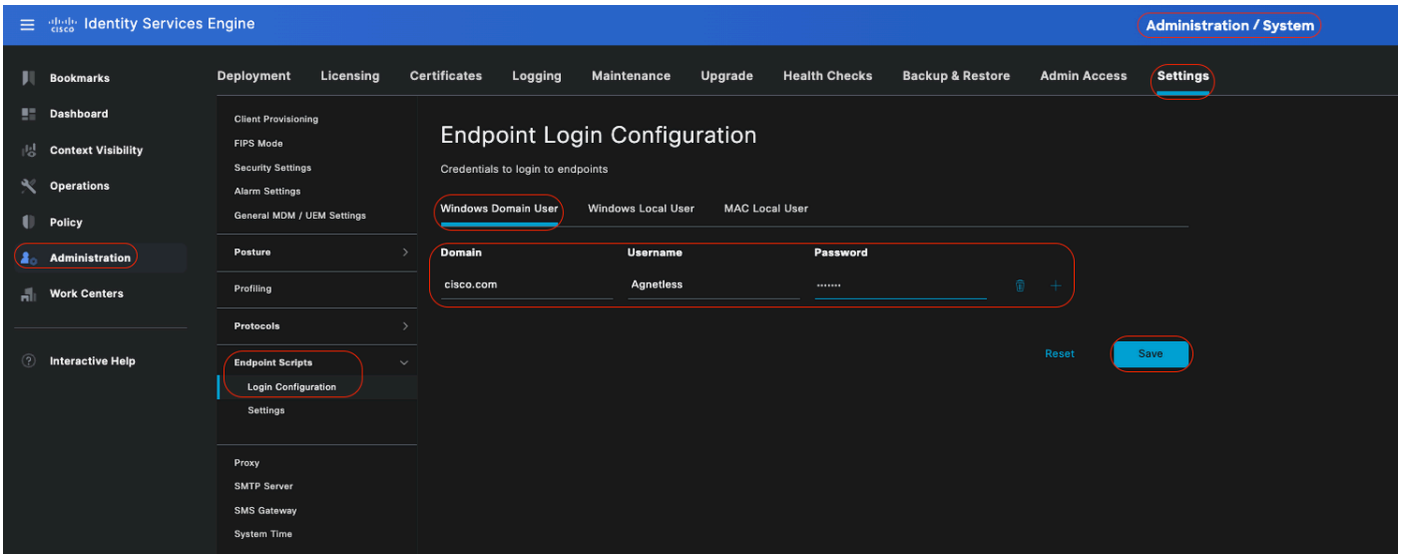
Queste stesse credenziali vengono utilizzate dagli script dell'endpoint in modo che Cisco ISE possa accedere ai client.

Per i dispositivi Windows, è possibile configurare solo le prime due schede (**Utente del dominio Windows e Utente locale Windows)**

- **Utente del dominio di Windows:**

Configurare le credenziali del dominio che Cisco ISE deve usare per accedere a un client tramite SSH. Fare clic sull'icona Plus e immettere tutti gli accessi Windows necessari. Per ogni dominio, immettere i valori richiesti nei campi Dominio, Nome utente, e Password. Se si configurano le credenziali del dominio, le credenziali dell'utente locale configurate nella scheda Utente locale di Windows verranno ignorate.

Se si amministrano endpoint Windows che utilizzano una valutazione della postura senza agente tramite un dominio di Active Directory, assicurarsi di fornire il nome di dominio insieme alle credenziali che dispongono di privilegi amministrativi locali.



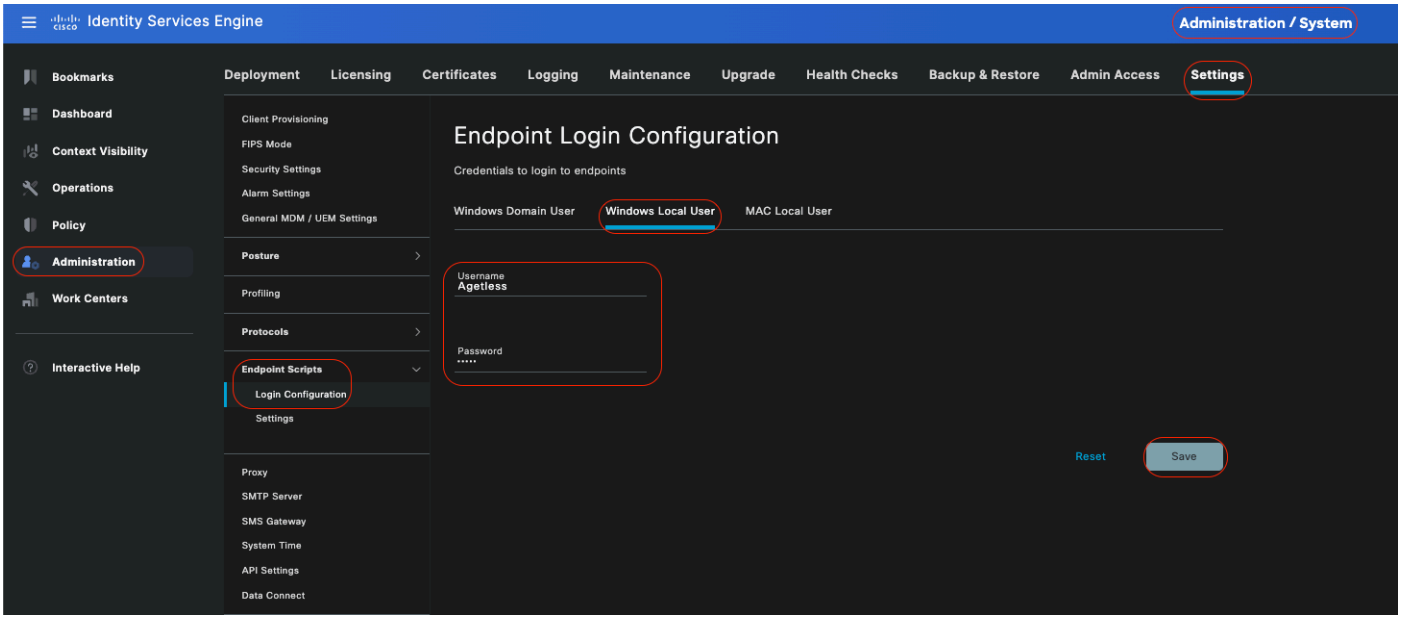
Utente del dominio di Windows

- **Utente locale di Windows:**

Configurare l'account locale usato da Cisco ISE per accedere al client tramite SSH. L'account locale deve essere in grado di eseguire Powershell

e Powershell in modalità remota.

Se **non** si amministrano endpoint Windows che utilizzano una valutazione della postura senza agente tramite un dominio Active Directory, assicurarsi di fornire credenziali che dispongano di privilegi amministrativi locali.

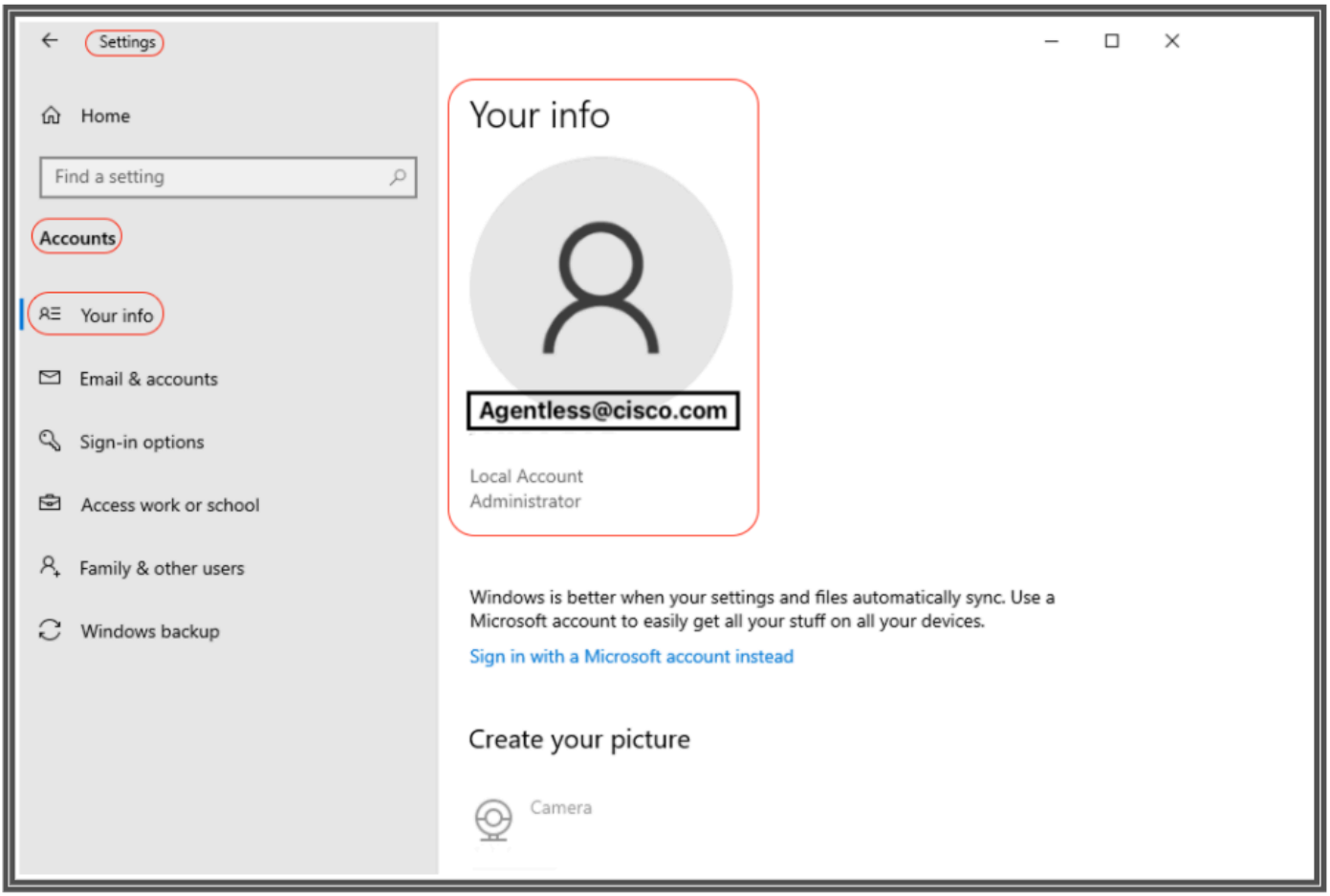


Utente locale di Windows

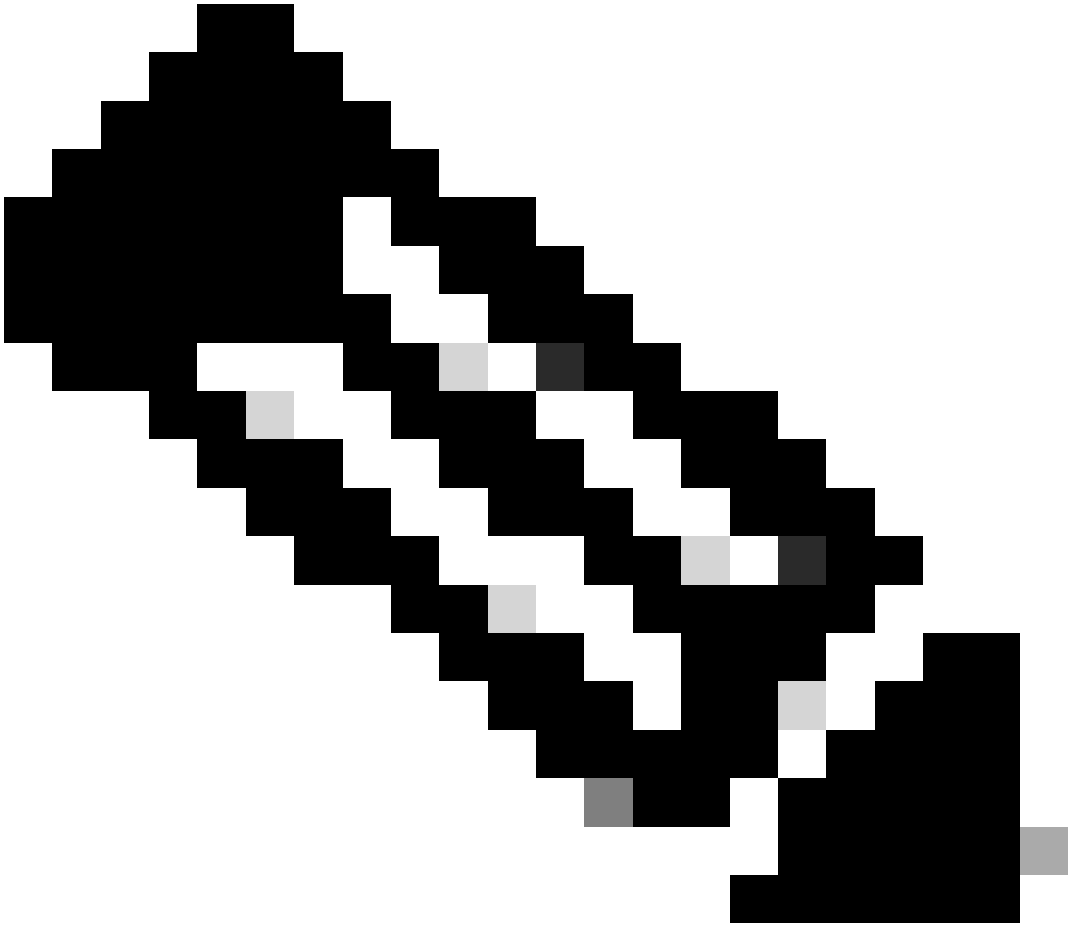
Verifica account

Per verificare gli account utente del dominio Windows e gli account utente locali di Windows in modo da poter aggiungere correttamente i dati appropriati in Credenziali di accesso endpoint, utilizzare la procedura seguente:

Utente locale di Windows: Uso della GUI (Settings App) Fare clic sul pulsante **WindowsStart**, selezionare **Settings** (l'icona a forma di ingranaggio), Fare clic su **Accounts**, quindi selezionare **Your info**:



Verifica account



Nota: per MacOS, è possibile fare riferimento a **Utente locale MAC**. Tuttavia, in questo esempio di configurazione, non verrà visualizzata la configurazione di MacOS.

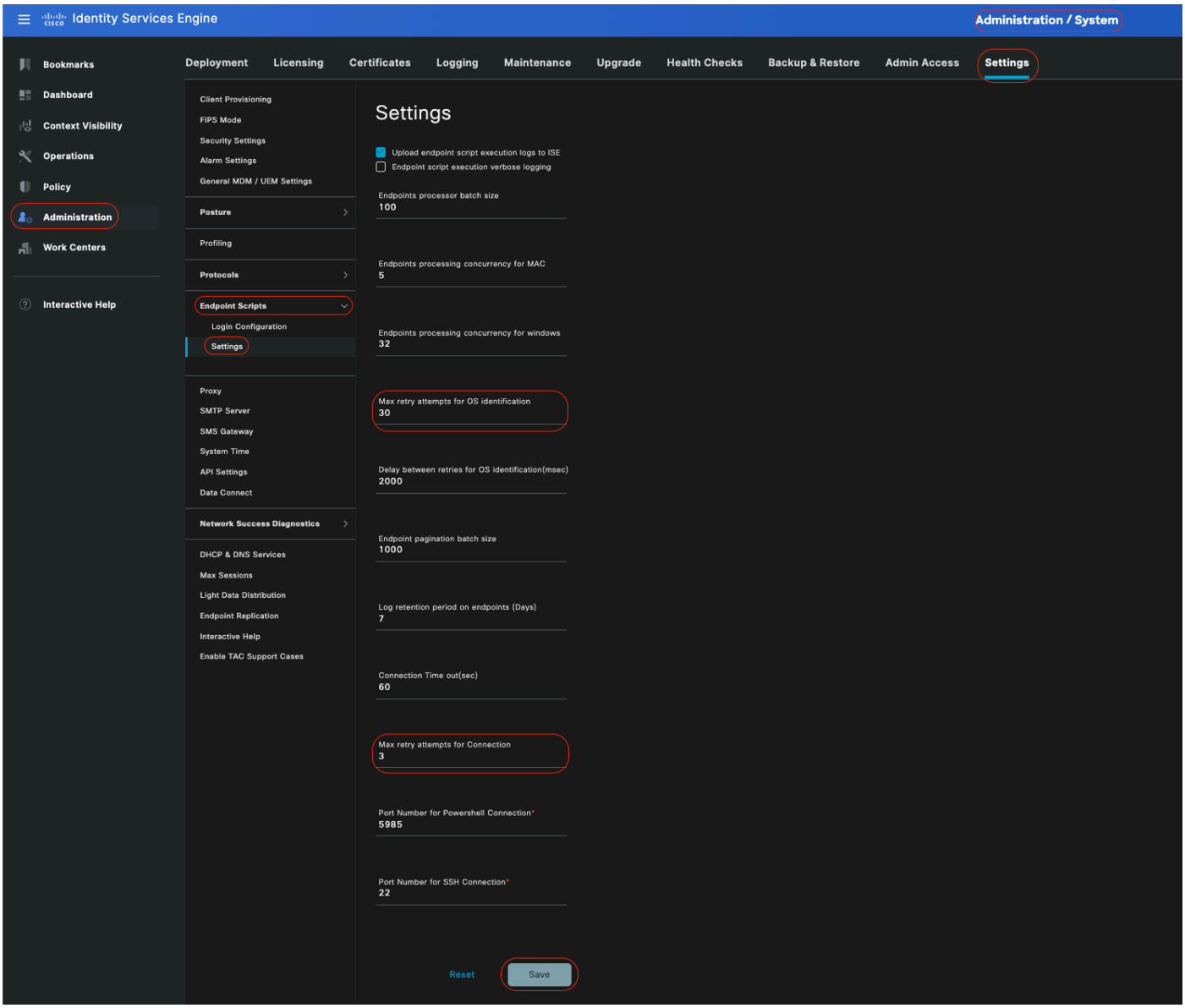
- **Utente locale MAC:** configurare l'account locale usato da Cisco ISE per accedere al client tramite SSH. L'account locale deve essere in grado di eseguire Powershell e Powershell in modalità remota. Nel campo Nome utente, immettere il nome dell'account locale.

Per visualizzare un nome account Mac OS, eseguire questo comandowhoami nel terminale:

Impostazioni

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (), **quindi selezionare Amministrazione > Impostazioni > Script endpoint > Impostazioni e configurareNumero massimo di tentativi** per l'identificazione del sistema operativo,**Ritardo tra i tentativi di identificazione del sistema operativo** e così via. Queste impostazioni determinano la velocità di conferma dei problemi di connettività. Ad esempio, un errore che indica che la porta di PowerShell non è aperta viene visualizzato nei log solo dopo che tutti i tentativi non sono stati esauriti.

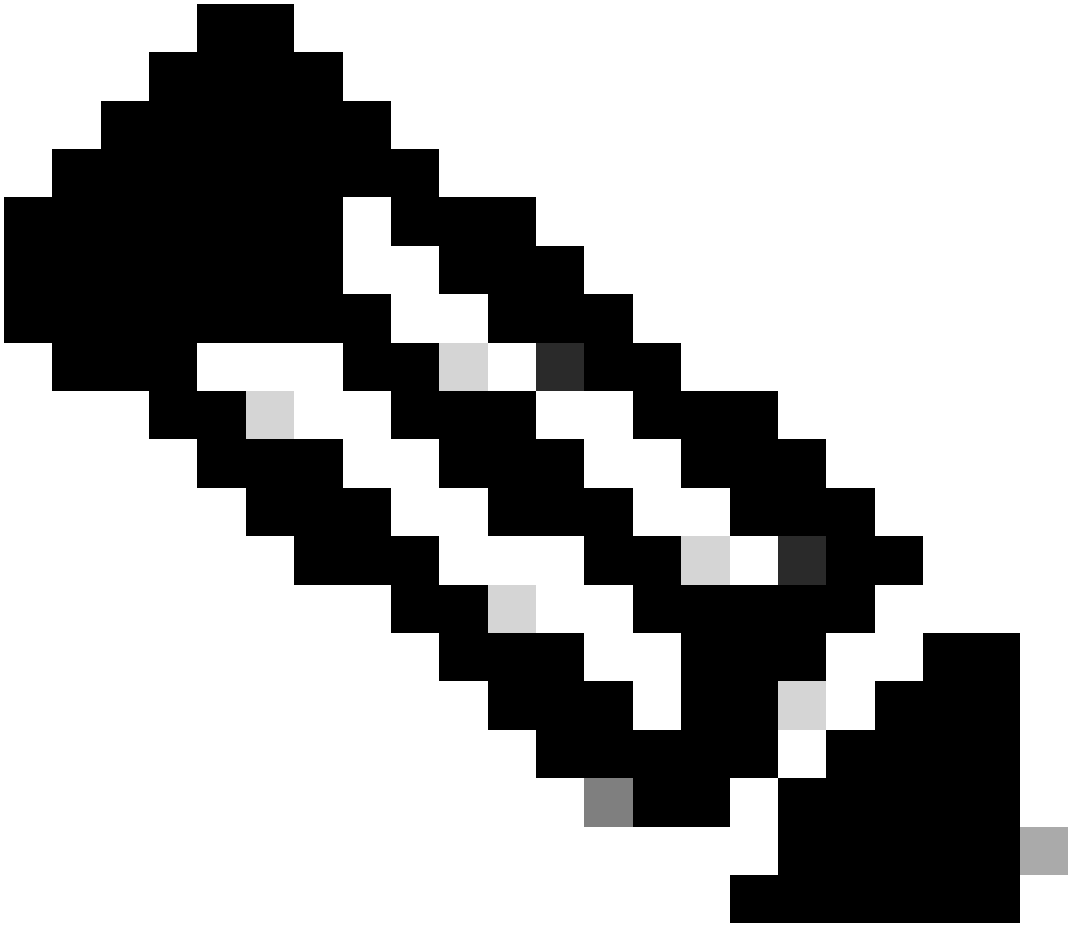
In questa schermata vengono mostrate le impostazioni dei valori predefiniti:



Impostazioni script endpoint

Quando i client si connettono con la postura senza agente, è possibile visualizzarli nei Live Log.

Configurazione e risoluzione dei problemi di Windows Endpoint



Nota: questi sono alcuni consigli da controllare e applicare sul dispositivo Windows. Tuttavia, è necessario fare riferimento alla documentazione di Microsoft o contattare il supporto tecnico Microsoft in caso di problemi quali privilegi utente, accesso PowerShell e così via...

Prerequisiti per la verifica e la risoluzione dei problemi

Test della connessione TCP alla porta 5985

Per i client Windows, è necessario aprire la porta 5985 per accedere a PowerShell sul client. Eseguire questo comando per confermare la connessione TCP alla porta 5985: **Test-NetConnection -ComputerName localhost -Port 5985**

L'output mostrato in questa schermata indica che la connessione TCP alla porta 5985 su localhost non è riuscita. Ciò significa che il servizio

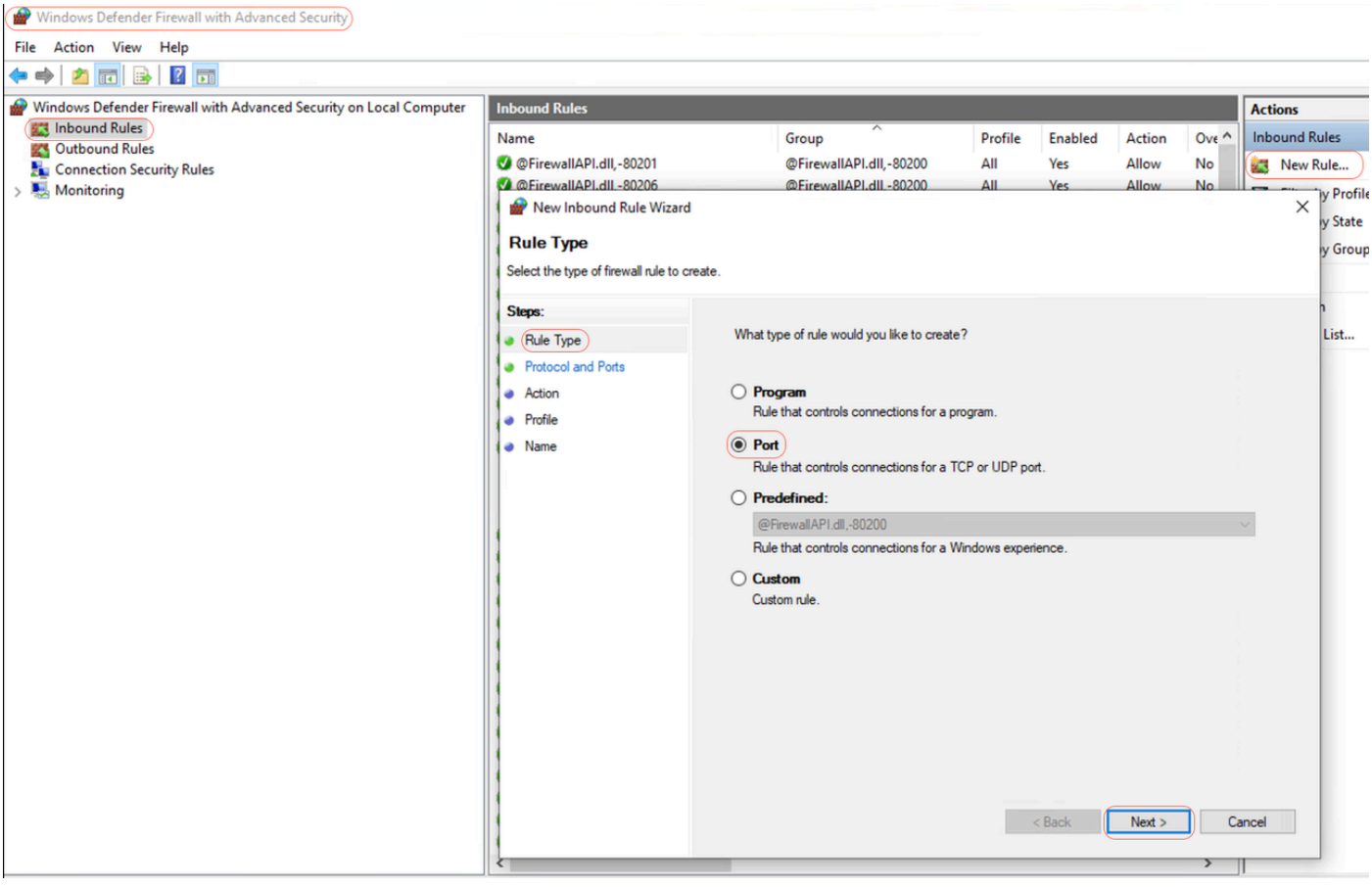
Gestione remota Windows, che utilizza la porta 5985, non è in esecuzione o non è configurato correttamente.

```
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

Creazione della regola in entrata per consentire PowerShell sulla porta 5985

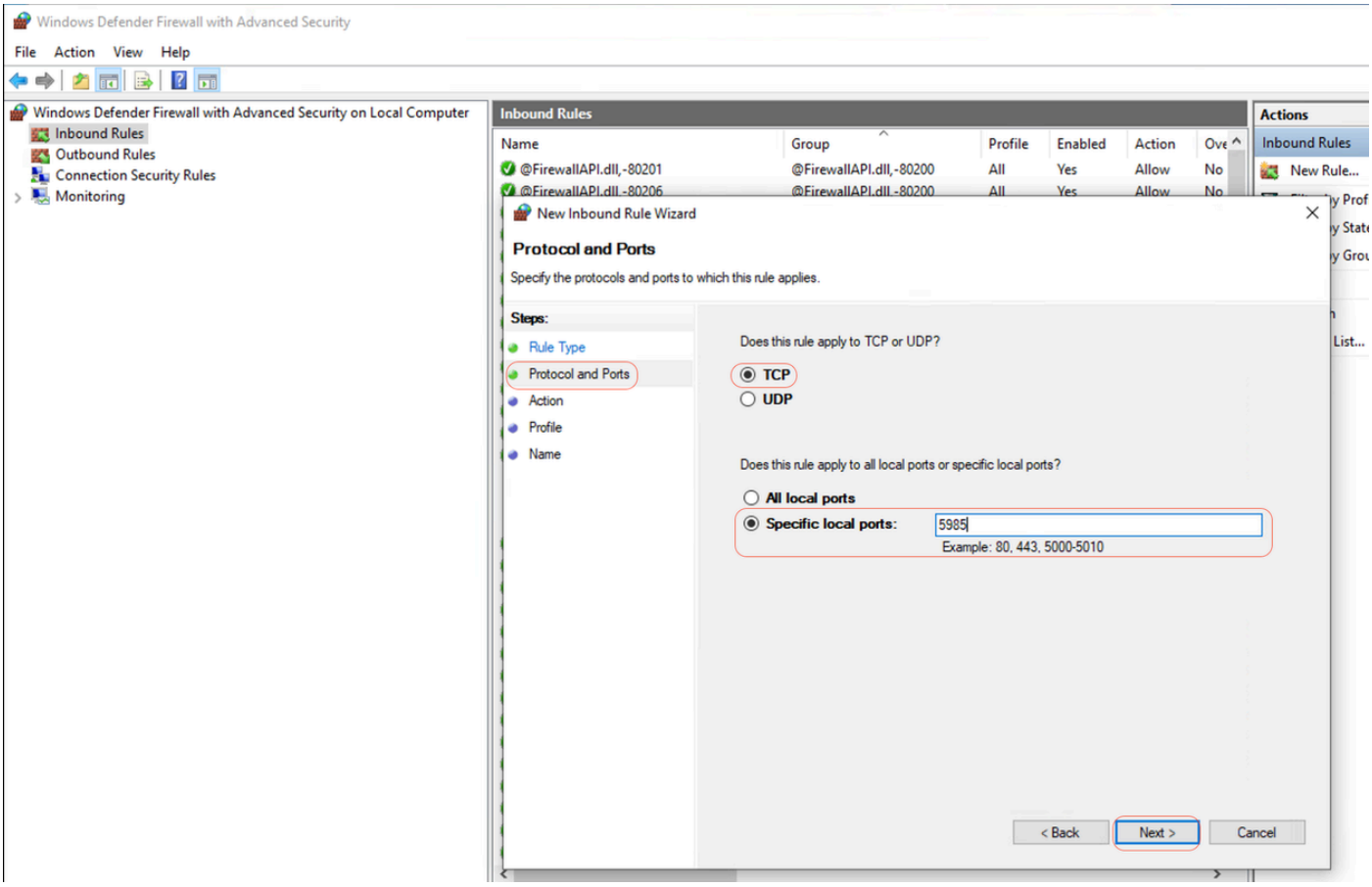
1- Nell'interfaccia utente di Windows, andare alla barra di ricerca, digitare Windows Firewall con sicurezza avanzata, fare clic su di esso e selezionare Esegui come amministratore > Regole in entrata > Nuova regola > Tipo di regola > Porta > Avanti:



Nuova regola connessioni in entrata - Porta

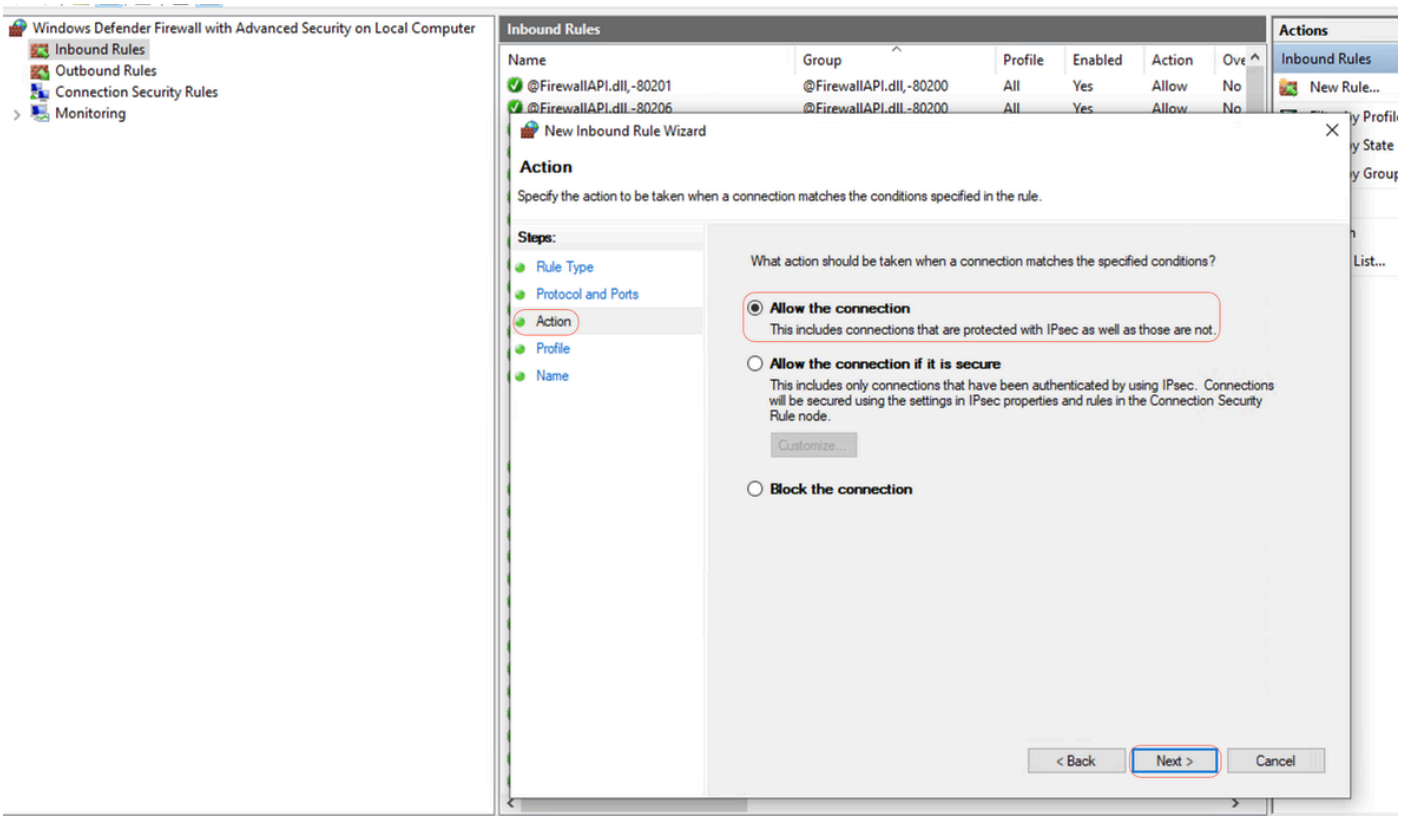
Passaggio 2- In Protocolli e porte, selezionare TCP e Specificare le porte locali, digitare il numero di porta 5985 (porta predefinita per la

comunicazione remota di **PowerShell**) e fare clic su **Avanti**:



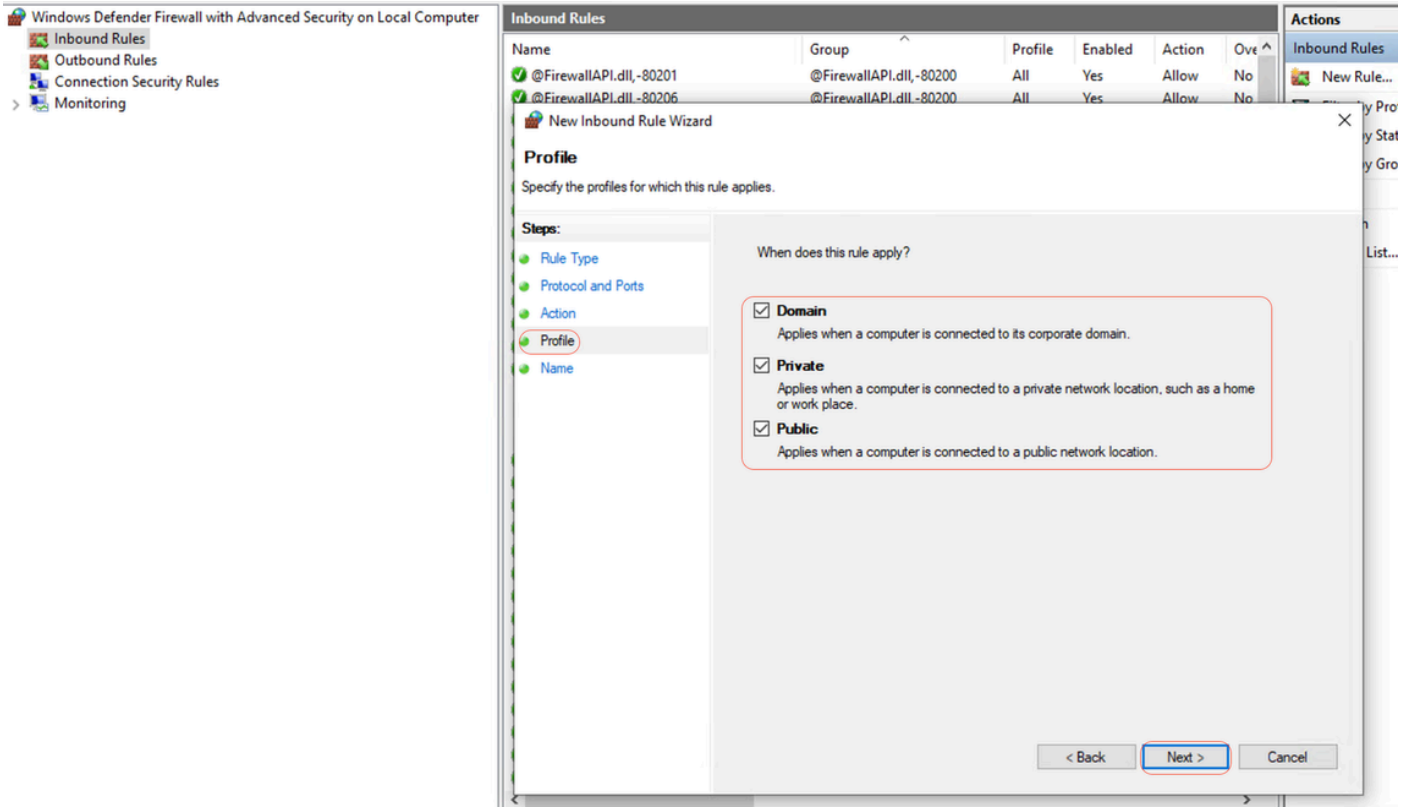
Protocolli e porte

3- In **Azione** > Seleziona **Consenti connessione** > **Avanti**:



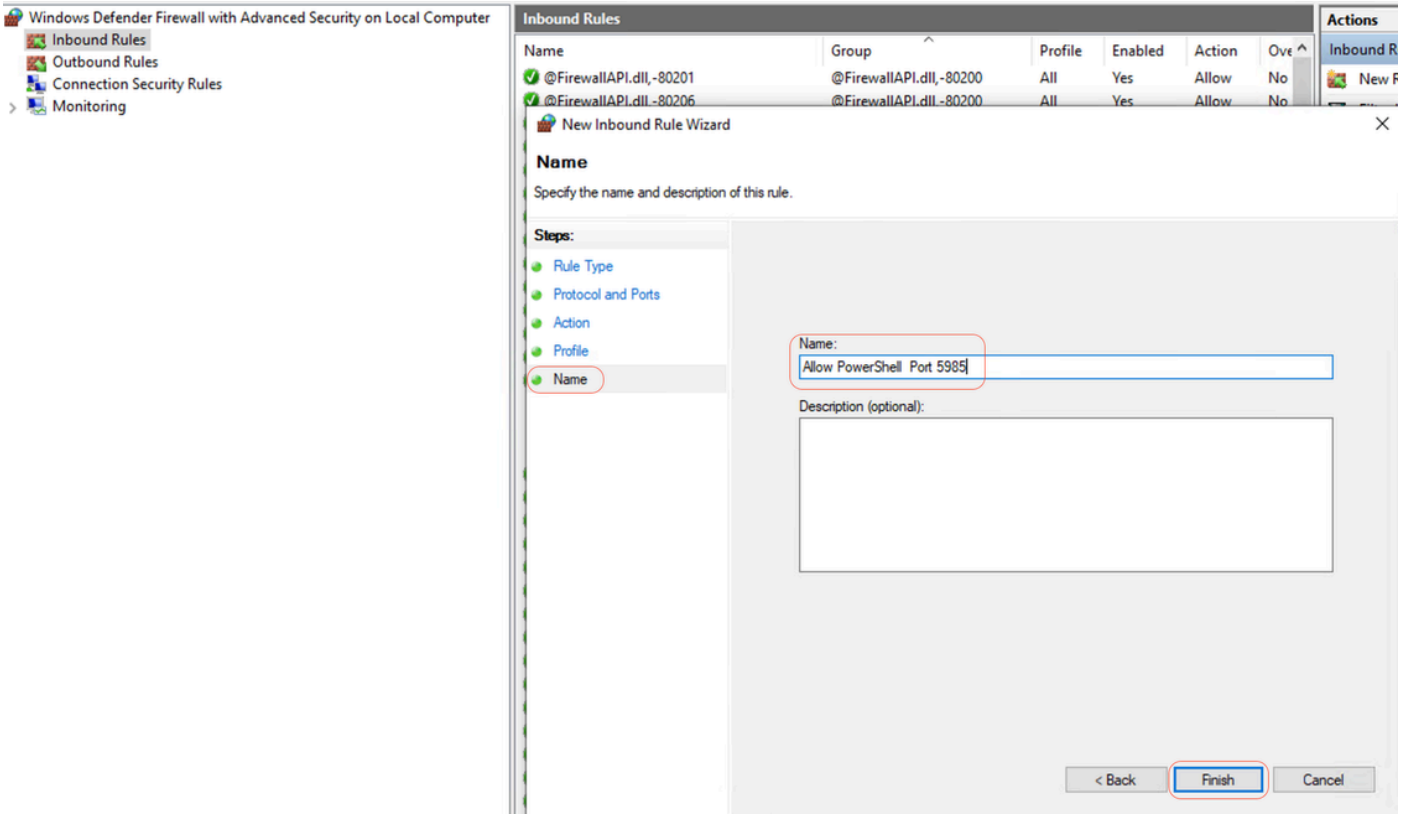
Azione

4- In Profilo, selezionare le caselle di controllo **Dominio**, **Privato** e **Pubblico** e fare clic su **Avanti**:



Profilo

5- In **Nome**, immettere un nome per la regola, ad esempio **Consenti PowerShell sulla porta 5985** e fare clic su **Fine**:

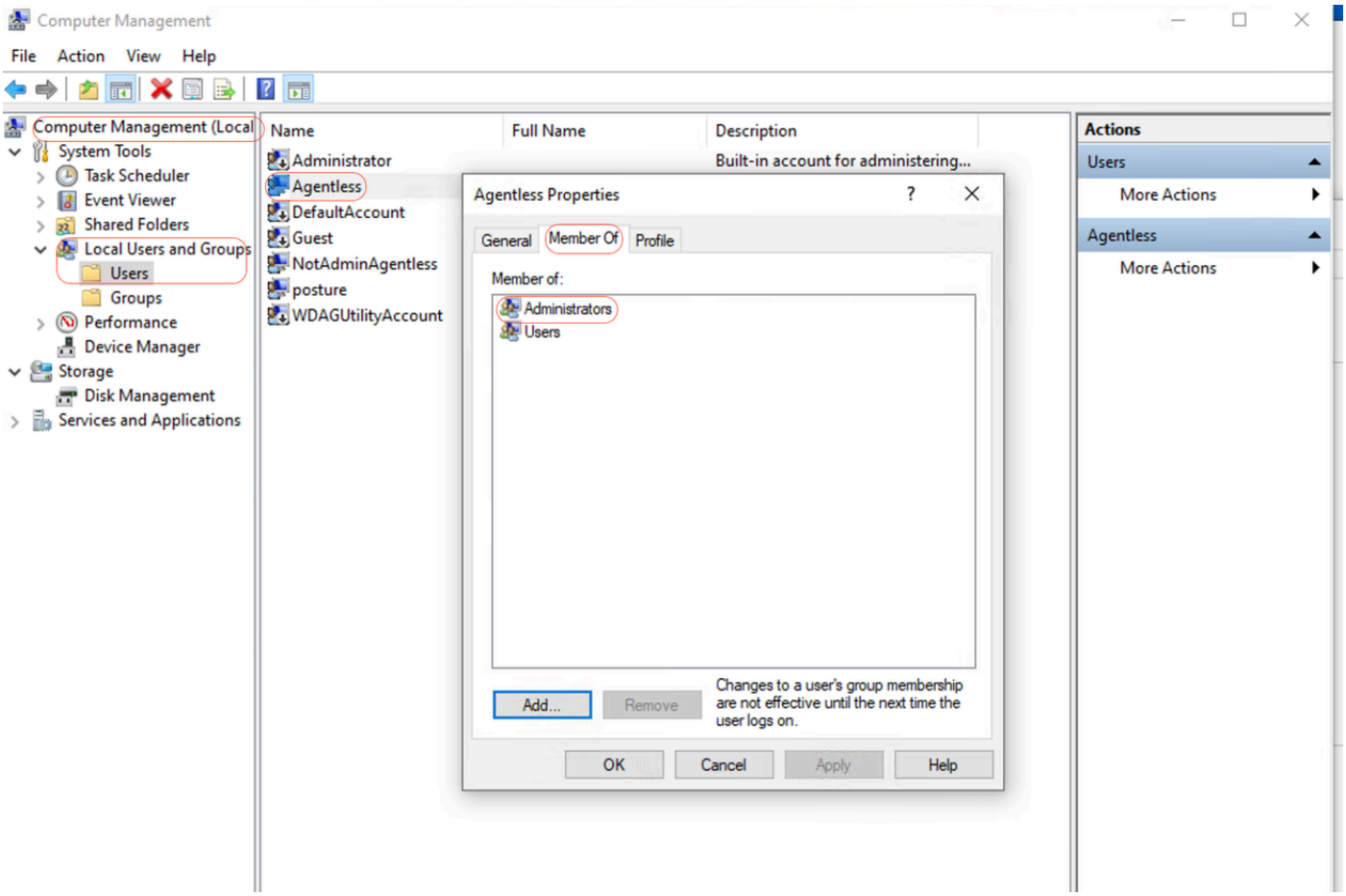


Nome

Le credenziali client per l'accesso alla shell devono disporre di privilegi di amministratore locale

Le credenziali client per l'accesso alla shell devono disporre dei privilegi di amministratore locale. Per confermare se si dispone dei privilegi di amministratore, verificare questa procedura:

Nell'interfaccia utente di Windows, andare a Impostazioni > Gestione computer > Utenti e gruppi locali > Utenti > Selezionare l'account utente (in questo esempio, **è selezionato Account** senza agente**) > Membro di, l'account deve avere Administrators** Group.



Privilegi di amministratore locale

Convalida del listener di Gestione remota Windows

Verificare che il listener di Gestione remota Windows sia configurato per **HTTP** sulla porta **5985**:

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

Abilita Gestione remota Windows PowerShell

Verificare che il servizio sia in esecuzione e configurato per l'avvio automatico, eseguire la procedura seguente:

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**

Output previsto:

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 deve essere v7.1 o versione successiva. Il client deve avere cURL v7.34 o versione successiva:

Come verificare le versioni di PowerShell e cURL in Windows

Accertarsi di utilizzare le versioni appropriate di PowerShell ; cURL è essenziale per la postura senza agenti:

Verifica della versione di PowerShell

In Windows:

1. **Aprire PowerShell:**

・Premere Win + X e selezionare **Windows PowerShell** o **Windows PowerShell (Admin)**.

2.Eseguire il comando:$PSVersionTable.PSVersion

・Tramite questo comando vengono restituiti i dettagli della versione di PowerShell installata nel sistema.

Verifica della versione di cURL

In Windows:

1. Apri prompt dei comandi:

・Premere Win + R, digitare cmd, quindi fare clic su **Enter**.

2. Eseguire il comando: curl --version

・Con questo comando viene visualizzata la versione di cURL installata nel sistema.

Output per il controllo delle versioni di PowerShell e cURL nei dispositivi 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>

Configurazione aggiuntiva

Questo comando configura il computer in modo che consideri attendibili host remoti specifici per le connessioni di Gestione remota Windows: 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> -

Il cmdlet test-wsman con i parametri -Authentication, Negotiate e -Credential è un potente strumento per verificare la disponibilità e la configurazione del servizio Gestione remota Windows in un computer remoto: test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

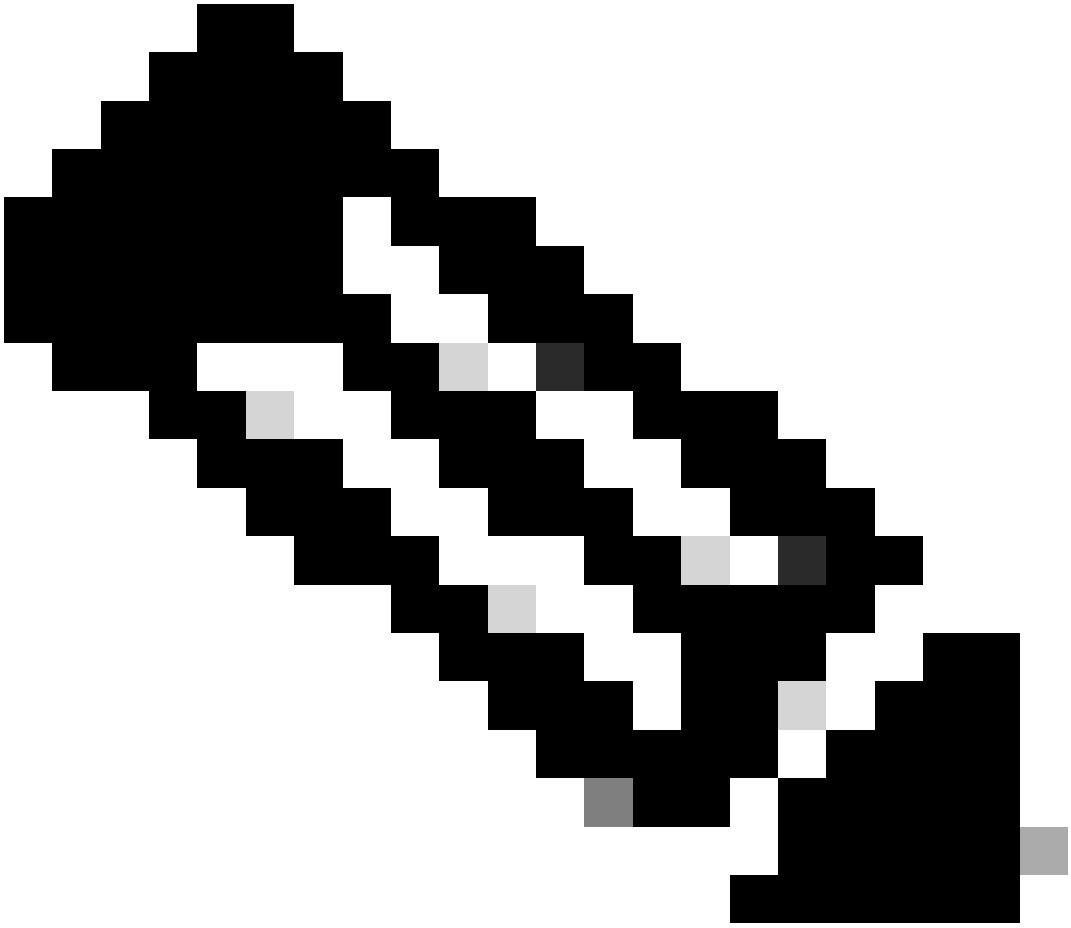
PowerShell deve essere v7.1 o versione successiva. Il client deve avere cURL v7.34 o versione successiva:

Su macOS:

1. **Aprire il terminale:**

- È possibile trovare Terminale in **Applicazioni > Utilità**.

2. Eseguire il comando: pwsh -Command '$PSVersionTable.PSVersion'



Nota: · Assicurarsi che PowerShell Core (pwsh) sia installato. In caso contrario, è possibile installarlo tramite Homebrew (assicurarsi di avere installato Himebrew): brew install --cask powershell

Su macOS:

1. **Aprire il terminale:**

· È possibile trovare Terminale in **Applicazioni > Utilità**.

2. Eseguire il comando: curl --version

· Questo comando deve visualizzare la versione di cURL installata nel sistema.

Per accedere ai client MacOS, la porta 22 deve essere aperta per consentire l'accesso al client SSH

Guida dettagliata:

1. **Preferenze di sistema aperte:**

· Passare a **Preferenze di sistema** dal menu Apple.

2. **Abilita accesso remoto:**

· Passare alla **condivisione**.

· Selezionare la casella accanto a **Accesso remoto**.

· Assicurarsi che l'opzione **Consenti accesso per** sia impostata sugli utenti o sui gruppi appropriati. Selezionando **All users** (Tutti gli utenti), qualsiasi utente con un account valido sul Mac può accedere tramite SSH.

3. **Verificare le impostazioni del firewall:**

· Se il firewall è abilitato, verificare che consenta le connessioni SSH.

· Selezionare **System Preferences > Security & Privacy > Firewall (Preferenze di sistema > Protezione e privacy > Firewall)**.

· Fare clic sul pulsante **Opzioni firewall**.

· Verificare che l'accesso **remoto** o **SSH** sia elencato e consentito. Se non è presente nell'elenco, fare clic sul pulsante **Aggiungi** (+) per aggiungerlo.

4. **Aprire la porta 22 attraverso il terminale (se necessario):**

· Aprire l'applicazione **Terminale** da **Applicazioni > Utilità**.

· Utilizzare il comando pfctl per verificare le regole firewall correnti e assicurarsi che la porta 22 sia aperta:sudo pfctl -sr | grep 22

· Se la porta 22 non è aperta, è possibile aggiungere manualmente una regola per permettere a SSH:echo "di passare la porta TCP da qualsiasi porta a qualsiasi porta 22" | sudo pfctl -ef -

5. **Test dell'accesso SSH:**

· Da un altro dispositivo, aprire un terminale o un client SSH.

· Tentativo di connessione al client macOS tramite il relativo indirizzo IP:ssh nomeutente@<macOS-client-IP>

· Sostituire il nome utente con l'account utente appropriato e <macOS-client-IP> con l'indirizzo IP del client macOS.

Per MacOS, assicurarsi che questa voce venga aggiornata nel file sudoers per evitare errori di installazione del certificato sugli endpoint:

Quando si gestiscono gli endpoint macOS, è fondamentale garantire che specifici comandi amministrativi possano essere eseguiti senza richiedere una password.

Prerequisiti

・Accesso come amministratore sul computer macOS.

・Conoscenza di base dei comandi del terminale.

Procedura per l'aggiornamento del file Sudoers

1. **Aprire il terminale:**

・È possibile trovare Terminale in **Applicazioni > Utilità**.

2. **Modificare il file Sudoers:**

・Utilizzare il comando visudo per modificare in modo sicuro il file sudoers. In questo modo, gli eventuali errori di sintassi vengono rilevati prima del salvataggio del file.sudo visudo

・Verrà richiesto di immettere la password amministratore.

3. **Consultare la sezione pertinente:**

・Nell'editor visudo, passare alla sezione in cui sono definite le regole specifiche dell'utente. In genere, si trova nella parte inferiore del file.

4. **Aggiungere la voce richiesta:**

・Aggiungere questa riga per concedere all'utente specificato l'autorizzazione a eseguire i comandi security e osascript senza una password: <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

・Sostituire **<macadminusername>** con il nome utente effettivo dell'amministratore macOS.

5. **Salva ed esci:**

・Se si utilizza l'editor predefinito (nano), premere Ctrl + X per uscire, quindi premere Y per confermare le modifiche e infine premere Invio per salvare il file.

・**Se si utilizza** vi o vim, premere Esc, digitare :wq, quindi premere Invio per salvare e uscire.

6. **Verificare le modifiche:**

・Per assicurarsi che le modifiche siano state applicate, è possibile eseguire un comando che richiede le autorizzazioni sudo aggiornate. Ad esempio:

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

・Questi comandi possono essere eseguiti senza richiedere una password.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).