# **Configure Posture Agentless**

## Contents

Introduction	
Prerequisites	
Requirements	
Components Used	
Background Information	
Getting Started	
Prerequisites:	
Supported Posture Conditions	
Unsupported Posture Conditions	
<b>ConfiguratingISE</b>	
Update Posture Feed	
Posture Agentless Configuration Flow	
Agentless Posture Configuration	
Posture Condition	
PostureRequirement	
Posture Policy	
Client Provisioning	
AgentlessAuthorization Profile	
Alternative to use remediation (Optional)	
Remediation Authorization Profile (Optional)	
Agentless Authorization Rule	
Configure Endpoint Login Credentials	
Configurating and Troubleshooting Windows Endpoint	
Verifying and Troubleshooting prerequisites	
TestingTCP connection to port 5985	
Creating Inbound Rule to allow PowerShell on port 5985	
Client credentials for shell login must have local admin privileges	
Validating WinRM listener	
EnablePowerShell RemotingWinRM	
Powershell must be v7.1or later. The client must have cURL v7.34 or later:	
Output for checking the PowerShell and cURL versions on Windows devices	
Additional Configuration	
MacOS	
For MacOS clients, port 22 to access SSH must be open to access the client	
For MacOS, ensure that this entry is updated in the sudoers file to avoid certificate installation failure	
on the endpoints:	

## Introduction

This document describes how to configure Posture Agentless in ISE and what is required in the endpoint to run Agentless script.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE).
- Posture.
- PowerShell and SSH
- Windows 10 or later.

## **Components Used**

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) 3.3 version.
- Package CiscoAgentlessWindows 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. If your network is live, ensure that you understand the potential impact of any command.

## **Background Information**

ISE Posture performs a client-side evaluation. The client receives the posture requirement policy from ISE, performs the posture data collection, compares the results against the policy, and sends the assessment results back to the ISE.

ISE then determines whether device is complaint or non-compliant based on Posture Report.

Agentless posture is one of posture methods that gathers posture information from clients and automatically removes itself upon completion without requiring any action from the end user. Agentless Posture connects to the client using administrative privileges.

## **Getting Started**

## **Prerequisites:**

- The client must be reachable through its IPv4or IPv6address, and that IP address must be available in RADIUS accounting.
- The client must be reachable from the Cisco Identity Services Engine (ISE) through its IPv4 or IPv6 address. Additionally, this IP address must be available in RADIUS accounting.
- Windows and Mac clients are currently supported:
  - For Windows clients, port 5985 to access powershell on the client must be open. Powershell must be v7.1or later. The client must have cURL v7.34 or later.
  - For MacOS clients, port 22 to access SSH must be open to access the client. The client must have cURL v7.34 or later.

- Client credentials for shell login must have local admin privileges.
- Run the posture feed update to get the latest clients, as described in the configuration steps. Please check:
- For MacOS, ensure that this entry is updated in the **sudoers** file to avoid certificate installation failure on the endpoints: Please check:

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

• For MacOS, the user account that is configured must be an administrator account. Agentless posture for MacOS does not work with any other account type, even if you grant more privileges. To view this



window, click the**Menu**icon (

) and chooseAdministration > System > Settings > Endpoint Scripts > Login Configuration > MAC Local User.

• In case of changes in port-related activities in Windows clients due to updates from Microsoft, you must have to reconfigure the agentless posture configuration workflow for Windows clients.

## **Supported Posture Conditions**

- File conditions, except the conditions that use the USER\_DESKTOP and USER\_PROFILE file paths
- Service conditions, except System Daemon and Daemon or User Agent checks on macOS
- Application conditions
- External Data Source conditions
- Compound conditions
- Anti-malware conditions
- Patch management condition, except the Enabled and Up To Date condition checks
- Firewall conditions
- Disk encryption conditions, except the encryption location-based condition check

• Registry conditions, except the conditions that use HCSK as root key

## **Unsupported Posture Conditions**

- Remediation
- Grace period
- Periodic Reassessment
- Acceptable Use-policy

## **Configurating ISE**

## **Update Posture Feed**

It is recommend to update Posture Feed before starting to configure Posture.



In the Cisco ISE GUI, click the**Menu**icon ( ) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Update Now**.

	dentity Services I	Engine	Work Centers / Posture	
рц	Bookmarks	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports	
55	Dashboard	Posture General Settings		
	Context Visibility	Endpoint Scripts >	Posture Updates	
×	Operations	Ressessment configurations	• Web Offline	
U	Policy	Acceptable Use Policy	* Update Feed URL https://www.cisco.com/web/: Set to Default	
<b>a</b> .,	Administration	Software Updates 🗸 🗸	Proxy Address	
		Client Provisioning	Proxy Port 80	
(a)	Work Centers	Posture Updates	нн мм ss	
	Interactive Help	Proxy Settings	Automatically check for updates starting from initial delay 17 $\vee$ 58 $\vee$ 31 $\vee$ every 2 hours ()	
			Save Update Now Reset	

Updating Posture Feed

## **Posture Agentless Configuration Flow**

Posture Agentless must be configured in order as the first configuration is going to be required for the next one and so on. Noticed that Remediation is not in the flow; however, later this document is going to cover an alternative for configuring Remediation.



Agentless Config Flow

## **Agentless Posture Configuration**

## **Posture Condition**

Posture conditions are the set of rules in our security policy that define a compliant endpoint. Some of these items include the installation of a firewall, anti-virus software, anti-malware, hotfixes, disk encryption and more.

In the Cisco ISE GUI, click the Menuicon (



) and choose Work Centers > Posture > Policy Elements > Conditions, Click on Add ,and create one or more Posture Coditions that use Agentless posture to identify the requirement. Once the Condition is created, click Save.

In this scenario, an Application Condition named "Agentless\_Condition\_Application" was configured with these parameters:

• Operating System: Windows All

This condition applies to any version of the Windows operating system, ensuring broad compatibility across different Windows environments.

• Check by: Process

The system monitors processes within the device. You have the option to select either **Process** or **Application**; in this case, **Process** was chosen.

• Process Name: Wired AutoConfig

The **Wired AutoConfig** process is the process Compliant Module is going to check in the device. This process is responsible for configuring and managing wired network connections, including IEEE 802.1X Authentication.

## • Application Operator: Running

The Compliance Module verifies whether the **Wired AutoConfig** process is currently running on the device. You have the option to select either **Running** or **Not Running**. In this instance, **Running** was selected to ensure that the process is active.

Bookmarks Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Toubleshoot Reports S   Context Visibility Anti-Makavee Anti	
Dashboard   Context Visibility   Anti-Malware   Application   Application   Application   Application   Application   Application   Distemary Compound   Prevail   Hardware Attributes   Patch Management   Registry   Script   Service   USB	ettings
Context Visibility Anti-Malware   Coperations Anti-Spyware   Anti-Virus Anti-Virus   Policy Application   Administration Compound   Dictionary Simple Disk Enerption   Dictionary Simple Disk Enerption   Biteractive Help File   File Operating System:   File Poress   File Operating System:   File Process   File Operating System:   File Process   Script Script   Service Compliance module   USB Any version	
Noperations Anti-Spyware   Anti-Virus   Policy   Agnitication   Compound   Dictionary Simple   Dictionary Simple   Disk Encryption   External DataSource   File   Process   Parovare Attributes   Parovare Attributes   Script   Script   Service   Compliance module   Any version	
Policy   Administration   Compound   Dictionary Compound   Dictionary Compound   Dictionary Simple   Dictionary Simple   Disk Encryption   External DataSource   File   File   File   Patch Management   Hardware Attributes   Patch Management   Compliance module   USB	
Administration   Compound   Dictionary Simple   Disk Encryption   External DataSource   File   Patch Management   Check By *   Process   Script   Script   Stript   Stript </th <th></th>	
Work Centers     Dictionary Simple   Disk Encryption     External DataSource   File   Pite   Pite   Mindows All     Hardware Attributes   Patch Management   Check By *   Patch Management   Script   Script   Script   Stript   USB   Any version	
Interactive Help     Disk Encryption     External DataSource     File     Operating System*     File     Pile     Mindows All     Patch Management     Check By**     Patch Management     Script   Service   Service   USB     Any version	
Interactive Help       External DataSource         File       Operating System*         Firewall       Windows All         Hardware Attributes       Hardware Attributes         Patch Management       Check By *         Registry       Process         Script       Script         USB       Any version	
Patch Management     Check By *       Registry     Process     ~       Script     -       Service     Compliance module       USB     Any version     ~	
Service Compliance module USB Any version ~	
Remediations     Process Name *       Application     Process Name *       Anti-Maiware     Wired AutoConfig       Anti-Spyware	
Anti-Virus Application Operator " File <u>Running ~</u>	
Firewall Launch Program Link Cancel Save Patch Management Solution	

Agentless Condition

## **Posture Requirement**

A posture requirement is a set of compound conditions or just one condition that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.



In the Cisco ISE GUI, click the**Menu**icon (

) and choose Work Centers > Posture > Policy Elements > Requirement. Click the down arrow and select Insert new Requirement, and create one or more PostureRequirement that use Agentless posture. Once the Requirement is created, click Done and then Save.

In this case, an Application Requirement named "Agentless\_Requirement\_Application" was configured with these criteria:

## • Operating System: Windows All

This requirement applies to any version of the Windows operating system, ensuring it is applicable across all Windows environments.

### • Posture Type: Agentless

This configuration is set for an Agentless environment. Available options include Agent, Agent Stealth, Temporal Agent, and Agentless. In this scenario, Agentless was selected.

## • Conditions: Agentless\_Condition\_Application

This specifies the condition that the ISE Posture Module and Compliance Module are going to check within the device's processes. The selected condition is **Agentless\_Condition\_Application**.

### • Remediation Actions:

Since this configuration is for an Agentless environment, Remediation Actions are not supported, and this field is grayed out.

=	dentity Services	s Engine							W	ork Centers / Postu	re				Q	0 Q
щ	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	r Elements Po	sture f	Policy Policy Sets	Tro	ubleshoot Reports	s S	ettings				
55 18	Dashboard Context Visibility	Conditions Anti-Male	v sare													
*	Operations	Anti-Spyv Anti-Virus	vare I	Requirements		Operating System		Compliance Module		Desture Trees		Conditions	Romediations Astions			
	Policy	Applicatio		Any AV Installation Win	for .	Windows All	usiaa	3 x or earlier	usien	Agent	mat if	ANY as whe last that	Massage Text Only			
2. ()	Administration	Dictionary	o / Compound	Agentiess_Requirement_	A for	Windows All	using	4.x or later	using	Agentiess	met if	Agentiess_Conditio the	Select Remediations			
	Work Centers	Dictionary Disk Enco	/ Simple	Any_AV_Definition_Win		Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_def the	AnyAVDefRemediationWin			
		External C	ataSource	Any_AS_Installation_Win		Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_inst the	Message Text Only			
G	Interactive Help			Any_AS_Definition_Win		Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def the	AnyASDefRemediationWin			
		Firewall	Attributes	Any_AV_Installation_Mac		Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_inst the	Message Text Only			
		Patch Ma	nagement	Any_AV_Definition_Mac		Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_def the	AnyAVDefRemediationMac			
		Registry		Any_AS_Installation_Mac		Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_inst the	Message Text Only			
		Script		Any_AS_Definition_Mac		Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def the	AnyASDefRemediationMac			
		USB		Any_AM_Installation_Win		Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_inst the	Message Text Only			
				Any_AM_Definition_Win		Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_def the	AnyAMDefRemediationWin			
		Remediation	s >	Any_AM_Installation_Mac	: for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_inst the	Message Text Only			
		Requirement		Any_AM_Demnition_Mac	for	Mac USA	using	4.x or later	using	Agent	met if	ANY_am_inac_der ther	Select Remediations	Edit -		
		Allowed Prot	pcols	Any AM Definition Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY am in def the	Select Remediations			
		Downloadabl	e ACLs	USB_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check the	USB_Block			
				Default_AppVis_Requiren ent_Win		Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Co then ndition_Win	Select Remediations			
				Default_AppVis_Requirem		Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Co ther odition Mac	Select Remediations			
				Note: Remediation Action is filtered t Remediation Actions are not as Remediations Actions are not a	based on oplicable opplicable	the operating system a for Application Condition for Agentiess Posture	nd stealt ins (confi type.	n mode selection. gured using the Provision By (	Category	or Provision By Everything optic	ns), Har	dware Conditions, and Extern	al Data source conditions.		Save	Reset

Agentless Requirement

## **Posture Policy**

In the Cisco ISE GUI, click the Menuicon (



) and choose **Work Centers** > **Posture** > **Posture Policy.** Click the **down arrow** and select **Insert new Requirement**, and create one or more supported **Posture Policy** rules that use Agentless posture for that Posture Requirement. Once the **Posture Policy** is created, click **Done** and then **Save**.

In this scenario, a Posture Policy named "Agentless\_Policy\_Application" has been configured with these parameters:

• Rule Name: Agentless\_Policy\_Application

This is the designated name for the Posture Policy in this configuration example.

• Operating System: Windows All

The policy is set to apply to all versions of the Windows operating system, ensuring broad compatibility across different Windows environments.

• Posture Type: Agentless

This configuration is set for an Agentless environment. Available options include Agent, Agent Stealth, Temporal Agent, and Agentless. In this scenario, Agentless has been selected.

## • Other Conditions:

In this configuration example, no additional conditions have been created. However, you have the option to configure specific conditions to ensure that only targeted devices are subject to this Posture Policy, rather than all Windows devices on the network. This can be particularly useful for network segmentation.

E altala Identity Servic	es Engi	ine								Work C	ente	rs / Posture						Q
Bookmarks	Over	rview	Network Devices	s Client Provisioning	Policy Elements	P	osture Policy	Polic	y Sets	Troublest	100t	Reports	Setti	ngs				
한 Dashboard 이상 Context Visibility		Post	ure Policy	affertion siles beend on an esti			111											
☆ Operations		Denne tri	e Posture Policy by co	miguning rules based on operati	ng system and/or other	cono	iuons.											
Policy		Status	Policy Options	Rule Name	Identity Groups		Operating System	15	Complia	ince Module		Posture Type		Other Conditions	Requirements			
Administration		D	Policy Options	Default_AntiMalware_Policy_Ma c	if Any		Mac OSX		d 4.x or late	H.		Agent			Any_AM_Installation_Ma c			
			Poll +	Agentless_Policy_Applicatic	if <u>Any +</u>		Windows All +		d 4.x or late			Agentless		(Optional) Dictio +	Agenties ×			
Interactive Help			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	lf Any		Mac OSX		d 4.x or late			Temporal Agent			Agentless_Re	equirement_Appli 🎽		
			Policy Options	Default_AntiMalware_Policy_Win			Windows All		d 4.x or late			Agent			Any_AM_Installation_Wi n			
			Policy Options	Default_AntiMalware_Policy_Win_temporal	lf Any		Windows All		d 4.x or late			Temporal Agent			Any_AM_Installation_Wi n_temporal			
			Policy Options	Default_AppVis_Policy_Mac	lf Any		Mac OSX		d 4.x or late			Agent			Default_AppVis_Require ment_Mac			
			Policy Options	Default_AppVis_Policy_Mac_te mporal	ii Any		Mac OSX		d 4.x or late			Temporal Agent			Default_AppVis_Require ment_Mac_temporal			
			Policy Options	Default_AppVis_Policy_Win	lf Any		Windows All		d 4.x or late			Agent			Default_AppVis_Require ment_Win			
			Policy Options	Default_AppVis_Policy_Win_te mporal	lf Any		Windows All		d 4.x or late	и		Temporal Agent			Default_AppVis_Require ment_Win_temporal			
			Policy Options	Default_Firewall_Policy_Mac	lf Any		Mac OSX		d 4.x or late	м		Agent			Default_Firewall_Require ment_Mac			
			Policy Options	Default_Firewall_Policy_Mac_te mporal	lf Any		Mac OSX		d 4.x or late			Temporal Agent			Default_Firewall_Require ment_Mac_temporal			
			Policy Options	Default_Firewall_Policy_Win	lf Any		Windows All		d 4.x or late			Agent			Default_Firewall_Require ment_Win			
			Policy Options	Default_Firewall_Policy_Win_te mporal	lf Any		Windows All		d 4.x or late	н		Temporal Agent			Default_Firewall_Require ment_Win_temporal			
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	if Any		Mac OSX		d 4.x or late			Agent			Default_Hardware_Attrib utes_Requirement_Mac			
			Policy Options	Default_Hardware_Attributes_P	If Any		Mac OSX		d 4.x or late			Temporal Agent			Default_Hardware_Attrib			
																		Save

Posture Agentless Policy

## **Client Provisioning**

## **Step 1- Downloading Resources**

To start configuring Client Provisioning, you must first download the required resources and have them available in ISE so you can later use them in the Client Provisioning Policy.

There are two ways to add resources to ISE, **Agent Resources from Cisco site** and **Agent Resources from Local disk**. Since you are configuring Agentless, you are required to go through **Agent Resources from Cisco site** to download.



Note: To use this Agent Resources from Cisco site, ISE PAN needs internet access.

≡	dentity Services	Engine						Work Cente	ers / Posture	
- M	Bookmarks	Overview	Network Devices	Client Prov	visioning Policy Elemen	ts Posture Policy	Policy S	ets Troubleshoot	Reports	Settings
55	Dashboard	Client Provis	ioning Policy							
교	Context Visibility	Resources		Reso	urces					
	· · · · · · · · · · · · · · · · · · ·	Client Provis	ioning Portal							
×	Operations				- Andre Dumliante 🖷	Delete				
•	Policy					Delete				
	Administration				Agent resources from Cisco site		Version	Last Update	Description	
-0	Administration				Agent resources from local disk	OsXSPWizard	2.7.0.1	2023/05/17 23:11:40	Supplicant Provisi	oning
កា	Work Centers				Native Supplicant Profile	oAgentlessWind	5.0.529.0	2023/05/17 23:11:47	With CM: 4.3.286	8.6145
					Agent Configuration	e Supplicant Pro	Not Applic	2016/10/06 15:01:12	Pre-configured Na	ative S
(?)	Interactive Help				Agent Posture Profile					
					AND Eachier Drofile	SPWizard	3.2.0.1	2023/05/17 23:11:40	Supplicant Provisi	oning
					AMP Enabler Profile	oTemporalAgent	5.0.529.0	2023/05/17 23:11:41	With CM: 4.3.286	8.6145
					Cisco-ISE-NSP	Native Supplicant Pro	Not Applic	2023/05/18 00:14:39	Pre-configured Na	ative S
					CiscoAgentlessOSX 5.0.005	CiscoAgentlessOSX	5.0.529.0	2023/05/17 23:11:50	With CM: 4.3.249	0.4353
					CiscoTemporalAgentOSX 5	CiscoTemporalAgent	5.0.533.0	2023/05/17 23:11:44	With CM: 4.3.249	0.4353

## Agent Resources from Cisco site



In the Cisco ISE GUI, click the**Menu**icon (

) and choose Work Centers > Posture > Client Provisioning > Resources. Click Add , Select Agent Resources from Cisco site, click Save.

From Cisco site, you can only dowload Compliance Module. System shows the two most recent Compliance Modules to download. Resource package **CiscoAgentlessWindows 5.1.6.6** is selected for this configuration example, this is only meant for windows devices.

$\equiv \frac{1}{1000}$ Identity Services I		
Bookmarks		
Dashboard	Resources	
Context visionity		
Policy		
Administration	MacOsXSPWizard 2.7.0.1     Download Remote Resources	
<ol> <li>Interactive Help</li> </ol>	Cisco-ISE-Chrome-NSP Name A Description	
	WinSPWizard 3.2.0.1         AnyConnectComplianceModuleW         Cisco Secure Client Windows Compliance Module 4.3.4164.8192           Cisco TemporalAgentWindo         AnyConnectComplianceModuleW         Cisco Secure Client WindowsARM64 Compliance Module 4.3.4114.8192	
	Cisco-ISE-NSP AnyConnectComplianceModuleW Cisco Secure Client WindowsARM64 Compliance Module 4.3.4164.8192 CiscoAgentiess OSX 5.0.00 CiscoAgentiess OSX 5.1.5.29 Cisco	
	CiscoTemporalAgentOSX 5 CiscoAgentiessOsX 5.1.6.6 Cisco Agentiess for OSX With CM: 4.3.3656.6400	
	CiscoAgentiessWindows 5.1.5.29 Cisco Agentiess for Windows With CM: 4.3.4114.8192 CiscoAgentiessWindows 5.1.6.6 Cisco Agentiess for Windows With CM: 4.3.4164.8192	
	CiscoTemporalAgentOSX 5.1.5.29 CiscoTemporal Agent for OSX With CM: 4.3.3609.6400  CiscoTemporalAgentOSX 5.1.6.6 CiscoTemporal Agent for OSX With CM: 4.3.3656.6400	
	For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the *Agent resource from local disk* add option, to import into ISE	Cisco Tempo 4.3.3656.640

Agent Resources from Cisco site

## **Step 2- Configuring Client Provisioning Policy**

When configuring Posture Agent, you need two different resources (**AnyConnect** or **Secure Client** and **Compliance Module**),

Map both resources under **Agent Configuration** along with the **Agent Posture Profile** so you can use this **Agent Configuration** in your **Client Provisioning Policy.** 

However, when configuring Posture Agentless, there is no need to configure **Agent Configuration** or Agent Posture Profile, instead you only download Agentless package from Agent Resources from Cisco site.



In the Cisco ISE GUI, click the Menuicon (

) and choose Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Click on down arrow and select Insert new policy above or Insert new policy below, Duplicate above or Duplicate below:

Rule Name: Agentless\_Client\_Provisioning\_Policy

This specifies the name of the Client Provisioning Policy.

• Operating System: Windows All

This ensures that the policy applies to all versions of the Windows operating system.

• **Other Conditions:** No specific conditions are configured in this example. However, you can configure conditions to ensure that only the desired devices match this Client Provisioning Policy, rather than all Windows devices in the network. This is particularly useful for network segmentation.

**Example:** If you are using Active Directory, you can incorporate Active Directory groups into your policy to refine which devices are affected.

- **Results:** Select the appropriate package or configuration agent. Since you are configuring for an agentless environment, choose the package **CiscoAgentlessWindows 5.1.6.6**, which you have previously downloaded from the Agent Resources from Cisco site. This agentless package contains all necessary resources (**Agentless Software** and **Compliance Module**) required for Posture Agentless to run.
- Click Save

E dentity Services	Engine											Work C	enters	Posture					_
<b>J</b> Bookmarks	Overview	Network Devices	Client Prov	visioning	Policy Elements	s Posture Poli	cy	Policy Sets	Trouble	shoot	Reports	Settings							
Dashboard     Context Visibility     Operations     Policy     Andinistration     Vork Center	Client Previsioning Policy Resources Client Previsioning Portal	Client Provisioning Policy Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: wizard profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order. Windows Agent, Mac: Agent, Mac: Agent, Mac: Temporal and Mac. More and the order of the order o																	
③ Interactive Help				Rule Name 105 Android Agentiess_ Windows MAC 05 Chromeboo	Client Provided	Identity Groups           Avy           Avy           Avy           Avy           Avy		Operating Sy Agole IOS All Android Windows All Windows All Mee OSX	+	and Ca and Ca and Ca and Ca and Ca	ther Conditions andElon(s) condition(s) andElon(s)			Results Cilco-152-1529 Cilco-152-1529 Result X Agent Configuratio CiscoAgentessWi Native Supplicant C Choose a Wizard	Edit v Edit v Done n n ndows 5.1 1 nfigurati Wizard Profile	.6	Is Upgrade Mandatory	0.03061 1.6.6 www.5.0.03061	•

Agentless Client Provisioning Policy



**Note**: Ensure that only one Client Provisioning Policy satisfies the conditions for any given authentication attempt. If multiple policies are evaluated simultaneously, it can lead to unexpected behaviors and potential conflicts.

## **Agentless Authorization Profile**



In the Cisco ISE GUI, click the Menuicon (

) and choose**Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** and create an **Authorization Profile** that evaluates the results from Agentless Posture.

- In this configuration example, named Authorization Profile as Agentless\_Authorization\_Profile.
- Enable Agentless posture in the authorization profile.
- Use this profile only for Agentless Posture. Do not also use this for other posture types.
- CWA and Redirect ACL is not required for Agentless posture. You can use VLANs, DACLs, or ACLs as part of your segmentation rules. To keep it simple, just a dACL (allowing all ipv4 traffic) is configured besides the Agentless Posture check in this configuration example.
- Click on Save.

	dentity Services E	Engine	Policy / Policy Elements
Ц	Bookmarks	Dictionaries Conditions	Results
51	Dashboard		Authorization Profile
	Context Visibility	Authentication >	* Name Agentless_Authorization_Profi
×	Operations	Authorization V	Description
6	Policy	Downloadable ACLs	
			*Access Type ACCESS ACCEPT ~
<b>a</b> o	Administration	Profiling	
ส์เ	Work Centers	Posture >	
_		Client Provisioning >	Service remplate
	Interactive Help		Agentiess Posture
			Passive identity Tracking D 0
			✓ Common Tasks
			DACL Name PERMIT_ALL_IPV4_TRAFFIC ~
			Pró DACL Name
			CL (Filter-ID)
			Ari Ibadi (Elitari It)
			Eelect an Item         v         -         +
			Actinoutes Detains     Actors hold actions to the action of the action of the action of the action of the actions

Agentless Authorization Profile

## Alternative to use remediation (Optional)

Support for remediation in the agentless flow is not available. To address this, you can implement a customized hotspot portal to enhance user awareness regarding endpoint compliance. When an endpoint is identified as non-compliant, users can be redirected to this portal. This approach ensures that users are informed about the compliance status of their endpoints and can take appropriate actions to rectify any issues.



In the Cisco ISE GUI, click the**Menu**icon (

) and choose Work Centers > Guest Access > Portals & Components > Guest Portals. Click Create > Select Hotspot Guest Portal > Continue: . In this configuration example, Hotspot Portal is named as Agentless\_Warning.



Hotspot Guest Portal

In the portal settings, you have the capability to customize the messages displayed to end-users to align with your specific requirements, this is just an example of customized portal view:

CISCO Hotspot Portal	
▲ Warning ▲ ¡ Agentless Flow Failure !	
	Dear User, We regret to inform you that your recent attempt to complete the Agentless flow has failed. This process is crucial for your seamless interaction with our system, and its failure may affect the functionality and services you can access. Thank you for your attention to this matter. We apologize for any inconvenience this may have caused
	Understood

Failed Posture Agentless

## **Remediation Authorization Profile (Optional)**

In the Cisco ISE GUI, click the Menuicon (



) and choose**Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** and create an **Authorization Profile** for your remediation.

- In this configuration example, named Authorization Profile as **Remediation\_Authorization\_Profile**.
- For the sake of simplicity, this configuration example includes only a downloadable Access Control List (dACL) named **Limited\_Access** that permits limited access, tailored to the specific needs of your organization.
- The **Web Redirection** feature has been configured including an external group and the hotspot, enhancing user awareness regarding endpoint compliance.
- Click Save.

≡	dentity Services E	ingine	Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions Re	sults
	Dashboard Context Visibility Operations Policy Administration Work Centers	Authentication     >       Authorization Profiles     >       Downloadable ACLs     >       Profiling     >       Positure     >       Client Provisioning     >	Authorization Profile S > Remediation_Authorization_Profile  Authorization Profile  Name  Remediation_Authorization_Pr  Description  Access Type Access_Accept  Network Device Profile  Gisco
			Tack Movement  Agendess Posture  Passive Identity Tracking  Common Tasks  Velve Redirection (CWA, MDM, NSP, CPP)  Act Isuisagar:ExternalGroups  Value Agentless_Warning  Suppress Profiler CoA for endpoints in Logical Profile  Auto Smart Port  Auto Smart Port
			Advanced Attributes Settings      Select an Item v * +

Remediation Authorization Rule

## **Agentless Authorization Rule**



In the Cisco ISE GUI, click theMenuicon ( ) and **choosePolicy** > **Policy Sets**and expand **Authorization Policy**. Enable and configure these three Authorization policies:



**Note**: These Authorization Rules must be configured in the specified order to ensure the posture flow operates correctly.

## **Unknown\_Compliance\_Redirect:**

## • Conditions:

Configure Network\_Access\_Authentication\_Passed AND **Compliance\_Unknown\_Devices** with the result set to Agentless Posture. This condition triggers the Agentless Flow.

## • Example Conditions:

Configure an Active Directory (AD) Group condition to segment traffic.

The **Compliance\_Unknown\_Devices** condition must be configured as the initial posture state is unknown.

### • Authorization Profile:

Assign **Agentless\_Authorization\_Profile** to this Authorization Rule to ensure devices go through the Agentless Posture flow. This condition contains Agentless Flow so devices hitting this profile can initiate

## Agentless flow.

Conditions Studio			0 ×
Library	Editor		
		hult same Esternal Remote	
♥ □ 0 ★ ● ₽ ₽ ₽ ₪ 2 ≣ C <b>1 €</b> ৳ ♥		Equals V Inisagar.com/Users/AD-PostureGroup =	
ii 🛙 56 🛛 🔿			
: BYOD_Is_Registered		Compliance_Unknown_Devices	
: Catalyst_Switch_Local_Web_Authentication			
Compliance_Unknown_Devices		Set to "Is not"	Save
: Compliant_Devices			
EAP-MSCHAPv2			
ii 🖻 EAP-TLS 📀			

Unknown Authorization Rule

## NonCompliant\_Devices\_Redirect:

• **Conditions:** Configure Network\_Access\_Authentication\_Passed and Non\_Compliant\_Devices with the result set to DenyAccess. Alternatively, you can use the remediation option, as demonstrated in this example.

#### • Example Conditions:

Configure an AD Group condition to segment traffic.

The **Compliance\_Unknown\_Devices** condition must be configured to assign limited resources when the posture state is non-compliant.

### • Authorization Profile:

Assign **Remediation\_Authorization\_Profile** to this Authorization Rule to notify non-compliant devices of their current status through **Hotspot Portal** or to **Deny Access**.

Conditions Studio										0 ×
Library		Editor								
				luisagar-Exter	rnalGrou	ins				®
•         •	t 후			Equala		huisagar com///	eere/AD-Rostur	raGroup ×		
# 🗏 56				Equais		iuisagai.com/o	seis/AD-Fostur			
# BYOD_Is_Registered			Non_	Compliant_Device	es					
: Catalyst_Switch_Local_Web_Authentication										
: E Compliance_Unknown_Devices										Sauce
: E Compliant_Devices										Jave
EAP-MSCHAPv2										
🗄 🖻 EAP-TLS										
🗄 🗐 Guest_Flow										
H E MAC_In_SAN										
: SNetwork_Access_Authentication_Passed										
: SNon_Cisco_Profiled_Phones										
ii S Non_Compliant_Devices										

Non-Compliant Authorization Rule

**Compliant\_Devices\_Access:** 

## • Conditions:

Configure Network\_Access\_Authentication\_Passed and **Compliant\_Devices** with the result set to PermitAccess.

## • Example Conditions:

Configure an AD Group condition to segment traffic.

The **Compliance\_Unknown\_Devices** condition must be configured so that compliant devices are granted proper access.

### • Authorization Profile:

Assign **PermitAccess** to this Authorization Rule to ensure compliant devices have access. This profile can be customized to meet the needs of your organization.

			0 ×
Conditions Studio			
Library	Editor		
		luisaar-External@ruins	
		Equals      Usisger.com/Users/AD-PostureGroup =	
∷ 🗄 50 0			
: BYOD_is_Registered	AND	Compliant_Devices	
Catalyst_Switch_Local_Web_Authentication			
: Dompliance_Unknown_Devices			
E Compliant_Devices			are .
EAP-MSCHAPv2			
E EAP-TLS			
: Guest_Flow			
E MAC_In_SAN			

Compliant Authorization Rule

## All Authorization rules

≡ diade Identity Services Eng	ine Policy / Policy Sets		Q	<b>a</b> @	Q   A					
J Bookmarks	Policy Sets Agentless_PS			nts	Save					
≣≣ Dashboard  ८  Context Visibility २९ Operations	Status         Policy Set Name         Description         Conditions           Q         Search		Allowed Protocols / Se	ver Sequ	ence Hits					
Policy	Agentiess_PS     Adventiesticn Bollinu(9)									
📲 Work Centers	Authorization Policy - Local Exceptions Authorization Policy - Global Exceptions									
⑦ Interactive Help	Interactive Help <ul> <li>Authorization Policy(4)         </li> </ul> <ul> <li>Interactive Help</li> <li>Authorization Policy(4)         </li> </ul> <ul> <li>Interactive Help</li> <li>Interactive Help</li> <li>Interactive Help</li> </ul> <ul> <li>Authorization Policy(4)</li> <li>Interactive Help</li> <li>Interactive Help</li> <li>Interactive Help</li> <li>Interactive Help</li> <li>Interactive Help</li> </ul> <ul> <li>Interactive Help</li> </ul> <ul> <li>Interactive Help</li> <li>Interactive Help</li></ul>									
	Status Rule Name Conditions	Profiles	Security Groups	Hits	Actions					
	Unknown_Compliance_Redir     AND     AND     AND     AND     Compliance_Linknown_Devices     AND     Compliance_Linknown_Devices	Agentless_Authorization_P								
	NonCompilant_Devices_Red AND     AND     Ano_Compilant_Devices_Compilant_Devices_Compilant_Devices     Non_Compilant_Devices	Remediation_Authorization								
	Compliant_Devices_Access     An     An     Luisagar-ExternalGroups TQUALS huisagar.com/Ukers/AD-PostureGroup     Compliant_Devices      Compliant_Devices	PermitAccess / +								
	Default	DenyAccess 0 +								
				et (	Save					

## **Configure Endpoint Login Credentials**



In the Cisco ISE GUI, click theMenuicon (

) and choose Administration > Settings > Endpoint Scripts > Login Configuration, and configure the client credentials to log onto clients.

These same credentials are used by the Endpoint Scripts so Cisco ISE can log in to clients.

For windows devices, you only configure the two first tabs (Windows Domain User and Windows Local User

### • Windows Domain User:

Configure the domain credentials that Cisco ISE must use to log in to a client via SSH. Click thePlusicon and enter as many Windows logins as you need. For each domain, enter the required values in theDomain,Username, andPasswordfields. If you configure domain credentials, the local user credentials that are configured in theWindows Local Usertab are ignored.

If you are administering Windows endpoints that utilize an Agentless posture assessment through an Active Directory domain, ensure to supply the domain name along with credentials possessing local administrative privileges.

≡	aliado Identity Services I	Engine								Administration / System
Щ	Bookmarks	Deployment Licensi	ng Ce	rtificates Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
	Dashboard	Client Provisioning								
Ъ	Context Visibility	FIPS Mode		Endpoint Lo	ogin Configu	ration				
×	Operations	Security Settings Alarm Settings		Credentials to login to e	endpoints					
•	Policy	General MDM / UEM Settings		Windows Domain User	Windows Local User	MAC Loca	l User			
20	Administration	Posture		Domain	Username		Password			
ส์เ	Work Centers	Profiling		cisco.com	Agnetless					
		Protocols								
?	Interactive Help	Endpoint Scripts							Reset	Save
		Login Configuration								
		Settings								
		Proxy								
		SMTP Server								
		SMS Gateway								
		System Time								

## • Windows Local User:

Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote.

If you are **not** administering Windows endpoints that utilize an Agentless posture assessment through an Active Directory domain, ensure to provide credentials which has local administrative privileges.

≡	dentity Services	Engine		Administration / System
<b>P</b> I	Bookmarks	Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Settings
- 55	Dashboard	Client Provisioning		
р.	Context Visibility	FIPS Mode	Endpoint Login Configuration	
×	Operations	Security Settings	Credentials to login to endpoints	
0	Policy	General MDM / UEM Settings	Windows Domain User Windows Local User MAC Local User	
20	Administration	Posture >		
គា	Work Centers	Profiling	Agerless	
		Protocols >		
?	Interactive Help	Endpoint Scripts ~	Password	
		Login Configuration		
		Settings		
		Proxv	Reset	Save
		SMTP Server		
		SMS Gateway		
		System Time		
		API Settings		
		Data Connect		

Windows Local User

### Veify Accounts

To verify your Windows domain user and Windows local user accounts so you can accurately add the appropriate data under Endpoint Login Credentials, please use this procedure:

Windows local user: Using the GUI (Settings App) Click on the WindowsStart button, select Settings (the gear icon), Click on Accounts, and select Your info:



Verify Accounts



**Note**: For MacOS, you can refer to **MAC Local User**. Howerver in this configuration example, you are not going to see MacOS configuration.

• MAC Local User: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote. In theUsernamefield, enter the Account Name of the local account.

To view a Mac OS Account Name, run this commandwhoami in the Terminal:

## Settings

In the Cisco ISE GUI, click the Menuicon (



) and chooseAdministration > Settings > Endpoint Scripts > Settings, and configureMax retry attempts for OS identification,Delay between retries for OS identification and so on. These settings determine how quickly connectivity issues can be confirmed. For example, an error that the PowerShell port is not open displays in logs only after all retries are not exhausted.

This screenshot shows default value settings:

$\equiv \frac{\mathrm{diade}}{\mathrm{cisco}}$ Identity Services I	Engine									Administration / System
Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
<ul> <li>Dashboard</li> <li>Context Visibility</li> <li>Operations</li> <li>Policy</li> </ul>	Client Provisionia FIPS Mode Security Settings General MDM / I	ng 3 JEM Settings	Settin	ngs endpoint script exe : script execution rocessor batch siz	ecution logs to ISE verbose logging ze					
Administration	Posture									
Work Centers	Protocols		Endpoints p	rocessing concurr	rency for MAC					
⑦ Interactive Help	Endpoint Script: Login Configu	s Iration	Endpoints p	rocessing concurr	rency for windows					
	Proxy SMTP Server SMS Gateway System Time		Max retry at 30	tempts for OS ide	Intification					
	API Settings Data Connect		Delay betwee 2000	een retries for OS	identification(msec)					
	Network Succes	as Diagnostics rvices	> Endpoint pa 1000	gination batch siz	e					
	Max Sessions Light Data Distribution Endpoint Replication		Log retentio 7	n period on endp	oints (Days)					
	Interactive Help Enable TAC Support Cases	Connection 60	Time out(sec)							
			Max retry at 3	tempts for Conne	ction					
			Port Numbe 5985	r for Powershell C	connection*					
			Port Numbe 22	r for SSH Connec	tion*					
				Reset	Save					

Endpoint Script Settings

As clients connect with Agentless posture, you can see them in the Live Logs.

## **Configurating and Troubleshooting Windows Endpoint**



**Note**: These are some recommendations to check and apply on your windows device; however, you must refer to Microsoft documentation or contact Microsoft support if encountering issues such as user privileges, PowerShell access and so on...

## Verifying and Troubleshooting prerequisites

## **Testing TCP connection to port 5985**

For Windows clients, port 5985 to access powershell on the client must be opened. Run this command to confirm TCP connection to port 5985: Test-NetConnection -ComputerName localhost -Port 5985

The output shown in this screenshot indicates that the TCP connection to port 5985 on localhost failed. This means that the WinRM (Windows Remote Management) service, which uses port 5985, is not running or is not properly configured.

PS C:\Windows\system32 WARNING: TCP connect t WARNING: TCP connect t	<pre>&gt; Test-NetConnection -Computer localhost -Port 5985 o (::1 : 5985) failed o (127.0.0.1 : 5985) failed</pre>
ComputerName RemoteAddress RemotePort InterfaceAlias SourceAddress PingSucceeded PingReplyDetails (RTT) TcpTestSucceeded	: localhost : ::1 : 5985 : Loopback Pseudo-Interface 1 : ::1 : True : 0 ms : False
PS C:\Windows\system32	

Connection failed to WinRM

## **Creating Inbound Rule to allow PowerShell on port 5985**

**Step 1-** In Windows GUI, go to **Search Bar**, type **Windows Firewall with Advanced Security**, click on it and select **Run as administrator** > **Inbound Rules** > **New Rule** > **Rule Type** > **Port** > **Next**:

Windows Defender Firewall with Advanced Security							
File Action View Help							
🗢 🔿 😰 🔂 🔂 🖬							
Windows Defender Firewall with Advanced Security on Local Computer	Inbound Rules						Actions
Inbound Rules	Name	Group	Profile	Enabled	Action	Ove ^	Inbound Rules
Control Contro	@ @FirewallAPLdll -80201	@FirewallAPLdll -80200	All	Ves	Allow	No	New Rule
Monitoring	@EirewallAPI.dll -80206	@FirewallAPI.dll80200	All	Yes	Allow	No	
1 - Montoning	🕴 💣 New Inbound Rule Wizard						×
	Rule Type						y State
		-					y Grou
	i Select the type of firewall fulle to creat	e.					
	Steps:						n
	Rule Type	What type of rule would you like to creat	te?				List
	Protocol and Ports						
	Action	O Program					
	Profile	Rule that controls connections for a	program.				
	<ul> <li>Name</li> </ul>	Port					
		Rule that controls connections for a	TCP or UDP po	ort.			
		O Predefined:					
		@FirewallAP1.dll,-80200					~
		Rule that controls connections for a	Windows expe	ience.			
		Custom					
		Custom rule.					
	1						
	1						
	4					_	
	1			< Back	Next >	C	ancel
						>	

New Inbound Rule - Port

**Step 2-** Under **Protocols and Ports**, select **TCP** and **Specify local ports**, type port number **5985** (Default port for **PowerShell** remoting) and click **Next**:



Protocols and Ports

## **Step 3-** Under **Action** > **Select Allow the connection** > **Next**:

P Windows Defender Firewall with Advanced Security on Local Computer	Inbound Rules								
Cotherend Pades	Name	Group	Profile	Enabled	Action	Ove ^	Inbound Ru	les	
Connection Security Rules	@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Allow	No	🚉 New Ru	ıle	
> ቘ Monitoring	@FirewallAPLdll -80206     Wew Inbound Rule Wizard     Action     Specify the action to be taken when a conner	©FirewallAPI.dll80200 All Yes Allow No.						/ Profil / State / Grou	
	Steps: Rule Type W	hat action should be taken when a co	nnection matc	hes the specifi	ed conditions	?	l I	List	
	Action     Profile	Allow the connection This includes connections that are pr	otected with I	osec as well as	those are no	xt.			
	Name     O	Allow the connection if it is secure     This includes only connections that have been authenticated by using IPsec. Connection     will be secured using the settings in IPsec properties and rules in the Connection Security     Rule node.     Customize     Block the connection							
				< Back	Next >		ancel		

Step 4- Under Profile, check the Domain, Private, and Public checkboxes and click Next:



Profile

Step 5- Under Name, Enter a name for the rule, such as Allow PowerShell on Port 5985 and click Finish:

Windows Defender Firewall with Advanced Security on Local Computer	Inbound Rules						Actions
Inbound Rules	Name	Group	Profile	Enabled	Action	Ove ^	Inbound
Connection Security Bules	SirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Allow	No	Rew New
Monitoring	DirewallAPI.dll80206	@FirewallAPI.dll-80200	All	Yes	Allow	No	-
	Wew Inbound Rule Wizard Name Specify the name and description of the Steps:	his rule.					×
	Rule Type     Protocol and Ports						
	Action						
	Profile	Name:					_
	Name	Allow PowerShell Port 5985					
		Description (optional):					
				< Back	Finish		incel

## Client credentials for shell login must have local admin privileges

Client credentials for shell login must have local admin privileges. To confirm whether having Admin privileges, please check this steps:

In Windows GUI, go to Settings > Computer Management > Local Users and Groups > Users > Select the User Account (in this example, Agentless Account is selected) > Member of, account must have Administrators Group.



Local Admin Privileges

### Validating WinRM listener

Ensure that the WinRM listener is configured for HTTP on 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>

### **Enable PowerShell Remoting WinRM**

Ensure service is running and configured to start automatically, go through these steps:

# 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** 

## **Expected output:**

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 must be v7.1 or later. The client must have cURL v7.34 or later:

#### How to Check PowerShell and cURL Versions on Windows

Ensuring that you are using the appropriate versions of PowerShell; cURL is essential for Posture Agentless:

#### **Checking PowerShell Version**

#### **On Windows:**

#### 1. Open PowerShell:

• Press Win + X and select Windows PowerShell or Windows PowerShell (Admin).

2. Execute the command: \$PSVersionTable.PSVersion

• This command outputs the version details of PowerShell installed on your system.

#### **Checking cURL Version**

#### **On Windows:**

### 1. Open Command Prompt:

- Press Win + R, type cmd, and click Enter.
- 2. Execute the Command: curl --version
- This command displays the version of cURL installed on your system.

### Output for checking the PowerShell and cURL versions on Windows devices

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>

### **Additional Configuration**

This command configures your machine to trust specific remote hosts for WinRM connections: Set-Item WSMan:\localhost\Client\TrustedHosts -Value <Client-IP>

C: \Windows\system32> Set-Item WSMan:\localhost\Client\TrustedHosts -Value 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> -

The test-wsman cmdlet with the -Authentication Negotiate and -Credential parameters is a powerful tool for verifying the availability and configuration of the WinRM service on a remote machine: test-wsman <Client-IP> - Authentication Negotiate -Credential <Accountname>

## MacOS

## Powershell must be v7.1 or later. The client must have cURL v7.34 or later:

## On macOS:

- 1. Open Terminal:
- You can find Terminal in Applications > Utilities.
- 2. Execute the Command: pwsh -Command '\$PSVersionTable.PSVersion'



**Note**: Note: • Ensure you have PowerShell Core (pwsh) installed. If not, you can install it via Homebrew (make sure you have Himebrew install): brew install --cask powershell

## On macOS:

- 1. Open Terminal:
- You can find Terminal in **Applications > Utilities**.
- 2. Execute the Command: curl --version
- This command must display the version of cURL installed on your system.

## For MacOS clients, port 22 to access SSH must be open to access the client

## **Step-by-Step Guide:**

- 1. Open System Preferences:
- Navigate to System Preferences from the Apple menu.

## 2. Enable Remote Login:

- Go to Sharing.
- Check the box next to **Remote Login**.

• Ensure that the **Allow access for** option is set to the appropriate users or groups. Selecting **All users** allows any user with a valid account on the Mac to log in via SSH.

## 3. Verify Firewall Settings:

• If the firewall is enabled, you need to ensure that it allows SSH connections.

## • Go to System Preferences > Security & Privacy > Firewall.

• Click on the Firewall Options button.

• Check that **Remote Login** or **SSH** is listed and allowed. If it is not listed, click the **Add** button (+) to add it.

## 4. Open Port 22 via Terminal (if necessary):

• Open the **Terminal** application from **Applications** > **Utilities**.

 $\bullet$  Use the pfctl command to check the current firewall rules and ensure port 22 is open:sudo pfctl -sr | grep 22

• If port 22 is not open, you can manually add a rule to allow SSH:echo "pass in proto tcp from any to any port 22" | sudo pfctl -ef -

## 5. Test SSH Access:

• From another device, open a terminal or SSH client.

• Attempt to connect to the macOS client using its IP address:ssh username@<macOS-client-IP>

• Replace username with the appropriate user account and <macOS-client-IP> with the IP address of the macOS client.

# For MacOS, ensure that this entry is updated in the sudoers file to avoid certificate installation failure on the endpoints:

When managing macOS endpoints, it is crucial to ensure that specific administrative commands can be executed without requiring a password prompt.

## Prerequisites

- Administrator access on the macOS machine.
- Basic familiarity with Terminal commands.

## Steps to Update the Sudoers File

## 1. Open Terminal:

• You can find Terminal in **Applications > Utilities**.

## 2. Edit the Sudoers File:

• Use the visudo command to safely edit the sudoers file. This ensures that any syntax errors are caught before saving the file.sudo visudo

• You are going to be prompted to enter your administrator password.

## 3. Find the Appropriate Section:

• In the visudo editor, navigate to the section where user-specific rules are defined. Typically, this is towards the bottom of the file.

## 4. Add the Required Entry:

• Add this line to grant the specified user permission to run the security and osascript commands without a password: <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

• Replace **<macadminusername>** with the actual username of the macOS admin.

## 5. Save and Exit:

• If you are using the default editor (nano), press Ctrl + X to exit, then press Y to confirm the changes, and finally press Enter to save the file.

• If using vi or vim, press Esc, type :wq, and press Enter to save and exit.

## 6. Verify the Changes:

• To ensure that the changes have taken effect, you can run a command that requires the updated sudo permissions. For example:

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

• These commands can be executed without prompting for a password.