# Agentenloser Status konfigurieren

# Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Erste Schritte
Voraussetzungen:
Interstützte Statusbedingungen
Status-Feed aktualisieren
Status Agentenloser Konfigurationsablauf
Agentenlose Statuskonfiguration
Statusbedingung
Statusanforderung
Statusrichtlinie
<u>Client-Bereitstellung</u>
AgentenlosesAutorisierungsprofil
Alternative zur Behebung (optional)
Wiederherstellungsautorisierungsprofil (optional)
Agentenlose Autorisierungsregel
Anmeldeinformationen für Endpunkt konfigurieren
Konfigurieren und Problembehebung für Windows Endpoint
Voraussetzungen für Verifizierung und Fehlerbehebung
Testen der TCP-Verbindung mit Port 5985
Erstellen einer eingehenden Regel, um PowerShell auf Port 5985 zuzulassen
Client-Anmeldedaten für Shell-Anmeldung müssen lokale Administratorberechtigungen haben.
WinRM-Listener wird überprüft
AktivierenPowerShell-RemotingWinRM
PowerShell muss v7.1 oder höher sein. Der Client muss über cURL v7.34 oder höher verfügen:
Ausgabe zum Überprüfen der PowerShell- und cURL-Versionen auf Windows-Geräten
Zusätzliche Konfiguration
MacOS
PowerShell muss v7.1 oder höher sein. Der Client muss über cURL v7.34 oder höher verfügen:
Für MacOS-Clients muss Port 22 für den Zugriff auf SSH offen sein, damit auf den Client zugegriffen werden kann.
Stellen Sie für MacOS sicher, dass dieser Eintrag in der sudoers-Datei aktualisiert wird, um einen Fehler bei der Zertifikatinstallation auf den Endpunkten zu vermeiden:

# Einleitung

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

# Voraussetzungen

# Anforderungen

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

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

# Verwendete Komponenten

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

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

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

# Hintergrundinformationen

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

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

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

# Erste Schritte

Voraussetzungen:

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

muss in der RADIUS-Accounting-Funktion verfügbar sein.

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

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

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



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

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

### Unterstützte Statusbedingungen

•

Dateibedingungen, mit Ausnahme der Bedingungen, die die Dateipfade USER\_DESKTOP und USER\_PROFILE verwenden

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

Anwendungsbedingungen

Bedingungen für externe Datenquellen

•

•

•

٠

•

٠

•

Zusammengesetzte Bedingungen

•

Anti-Malware-Bedingungen

Patch-Verwaltungsbedingung, mit Ausnahme der Prüfungen "Enabled" und "UpToDate"

•

Firewall-Bedingungen

•

Bedingungen für die Festplattenverschlüsselung, mit Ausnahme der auf dem Verschlüsselungsspeicherort basierenden Bedingungsprüfung

Registrierungsbedingungen, mit Ausnahme der Bedingungen, die HCSK als Stammschlüssel verwenden

Nicht unterstützte Statusbedingungen

Problembehebung

Nachfrist

Regelmäßige Neubewertung

Richtlinie für akzeptable Nutzung

Konfigurieren der ISE

.

### Status-Feed aktualisieren

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



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

), und wählen Sie Work Centers > Posture > Settings > Software Updates > Update Now (Work Center > Status > Einstellungen > Software-Updates > Jetzt aktualisieren) aus.

	dentity Services	Engine			Work Centers / P	osture						
ĮI	Bookmarks	Overview	Network Devices	Client Provisioni	ng Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
55	Dashboard	Posture Gene	ral Settings									
	Context Visibility	Endpoint Scr	ipts >	Posture Update	es							
×	Operations	Ressessment	configurations	<ul> <li>Web</li> </ul>	Offline							
U	Policy	Acceptable U	se Policy	* Update Feed URL	https://www.cisco.com/web	Set to Defa						
20	Administration	Software Upo	dates $\checkmark$	Proxy Address								
		Client Prov	visioning	Proxy Port								
	Work Centers	Posture Up	odates			нн мм	SS					
		Proxy Setti	ings	Automatically c	heck for updates starting from initia	delay 17 $ imes$ 58 $ imes$	31 v every	2 hours (j)				
	Interactive Help											
				Save	Update Now	leset						

Status-Feed aktualisieren

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



Konfigurationsablauf ohne Agent

Agentenlose Statuskonfiguration

### Statusbedingung

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

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



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

In diesem Szenario wurde eine Anwendungsbedingung mit dem Namen "Agentless\_Condition\_Application" mit den folgenden Parametern konfiguriert:

· Betriebssystem: Windows All

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

• Prüfen nach: Prozess

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

Prozessname: Kabelgebundene Autokonfiguration

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

· Anwendungsoperator: Wird ausgeführt

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

Running (Wird ausgeführt) oder Not Running (Wird nicht ausgeführt) auswählen. In dieser Instanz wurde Running ausgewählt, um

sicherzustellen, dass der Prozess aktiv ist.

	diale Identity Services	Engine						Work Center	s / Posture	
Щ	Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
55	Dashboard			Application Condition - App	tion Condition Anliantian					
闷	Context Visibility	Conditions Anti-Malw	vare	Application Condition > Ager	tuess_Condition_Aprication					
*	Operations	Anti-Spyv Anti-Virus	vare	Name* Agentless_Condition_/	Application					
U	Policy	Applicatio	n							
<b>å</b> 0	Administration	Compoun	d Compound	Description						
	Work Centers	Dictionary	Simple							
_		Disk Encry	yption							
?	Interactive Help	External C File Firewall Hardware Patch Mar Registry Script Script Service USB	lataSource Attributes hagement	Operating System* Windows All Check By * Process Compliance module Any version						
		Remediation Applicatio Anti-Maiw Anti-Virus File Firewall Launch Pr Link Patch Mar Script	is V	Process Name * Wired AutoConfig Application Operator * Running Cancel	~ Save					

Agentenloser Zustand

### Status-Anforderung

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

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



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

In diesem Fall wurde eine Anwendungsanforderung mit dem Namen "Agentless\_Requirement\_Application" mit den folgenden Kriterien konfiguriert:

· Betriebssystem: Windows All

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

• Statustyp: Agentenlos

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

Bedingungen: Agentless\_Condition\_Application

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

· Sanierungsmaßnahmen:

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

=	E dentity Services	Engine				C	Nork Centers / Post	ture				Q @ (	۵
	Bookmarks Dashboard Context Visibility	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets Ti	roubleshoot Repor	rts Si	iettings				
*	Coperations	Anti-Malware Anti-Spyware	Requirements										
0	Policy	Anti-Virus	Name	Operating S	iystem Compl	lance Module	Posture Type		Conditions	Remediations Actions			
	<ul> <li>Administration</li> </ul>	Compound	Any_AV_Installation_Win	for Windows All	using 3.x or e	artier using	Agent	met if	ANY_av_win_inst then	Message Text Only			
G	Work Centers	Dictionary Compound	Agentless_Requirement_	A for Windows All	using 4.x or la	ter using	Agentiess	met if	Agentless_Conditio then n_Application	Select Remediations			
		Dictionary Simple Disk Encryption	Any_AV_Definition_Win	for Windows All	using 3.x or e	arlier using	Agent	met if	ANY_av_win_def then	AnyAVDefRemediationWin			
6	Interactive Helo	External DataSource	Any_AS_Installation_Win	for Windows All	using 3.x or e	arlier using	Agent	met if	ANY_as_win_inst then	Message Text Only			
			Any_AS_Definition_Win	for Windows All	using 3.x or e	arlier using	Agent	met if	ANY_as_win_def then	AnyASDefRemediationWin			
		Firewall Hardware Attributes	Any_AV_Installation_Mac	for Mac OSX	using 3.x or e	arlier using	Agent	met if	ANY_av_mac_inst then	Message Text Only			
		Patch Management	Any_AV_Definition_Mac	for Mac OSX	using 3.x or e	arlier using	Agent	met if	ANY_av_mac_def then	AnyAVDefRemediationMac			
		Registry	Any_AS_Installation_Mac	tor Mac OSX	using 3.x or e	arlier using	Agent	met if	ANY_as_mac_inst then	Message Text Only			
		Script	Any_AS_Definition_Mac	for Mac OSX	using 3.x or e	arlier using	Agent	met if	ANY_as_mac_def then	AnyASDefRemediationMac			
		Service	Any_AM_Installation_Wir	for Windows All	using 4.x or la	ter using	Agent	met if	ANY_am_win_inst then	Message Text Only			
			Any_AM_Definition_Win	for Windows All	using 4.x or la	ter using	Agent	met if	ANY_am_win_def then	AnyAMDefRemediationWin			
		Remediations >	Any_AM_Installation_Ma	c for Mac OSX	using 4.x or la	iter using	Agent	met if	ANY_am_mac_inst then	Message Text Only			
		(Basedon mark)	Any_AM_Definition_Mac	for Mac OSX	using 4.x or la	iter using	Agent	met if	ANY_am_mac_def then	AnyAMDefRemediationMac			
		Allowed Protocols	Any_AM_Installation_Lin	for Linux All	using 4.x or la	ter using	Agent	met if	ANY_am_lin_inst then	Select Remediations			
		Authorization Profiles	Any_AM_Definition_Lin	for Linux All	using 4.x or la	ter using	Agent	met if	ANY_am_lin_def then	Select Remediations			
		Downloadable ACLs	USB_Block	for Windows All	using 4.x or la	ter using	Agent	met if	USB_Check then	USB_Block			
			Default_AppVis_Requires ent_Win	m for Windows All	using 4.x or la	ter using	Agent	met if	Default_AppVis_Co then ndition_Win	Select Remediations			
			Default_AppVis_Requires	m for Mac OSX	using 4.x or la	ter using	Agent	met if	Default_AppVis_Co then ndition Mar	Select Remediations			
			Note: Remediation Action is filtered Remediation Actions are not a Remediations Actions are not	based on the operating sy pplicable for Application ( applicable for Agentiess P	ystem and stealth mode sel Conditions (configured usin Posture type.	ection. g the Provision By Category	y or Provision By Everything op	ptions), Hard	dware Conditions, and Externa	I Data source conditions.		Save Res	et

Agentenlose Anforderung

### Statusrichtlinie



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

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

In diesem Szenario wurde eine Statusrichtlinie mit dem Namen "Agentless\_Policy\_Application" mit den folgenden Parametern konfiguriert:

· Regelname: Agentless\_Policy\_Application

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

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

Statustyp: Agentenlos

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

· Sonstige Voraussetzungen:

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

	esco Identity Services	Engi	ne							Work	k Cent	ers / Posture	)				Q
н	Bookmarks	Over	rview	Network Devices	s Client Provisioning	Policy Elements	P	osture Policy F	Polic	y Sets Troubl	leshoo	t Reports	Setti	ings			
	Dashboard Context Visibility		Post	ure Policy													
×	Operations		Define the	e Posture Policy by co	infiguring rules based on operation	ng system and/or other	cond	litions.									
0	Policy																
<b>a</b> .,	Administration		Status	Policy Options	Rule Name	Identity Groups		Operating Systems		Compliance Mod	dule	Posture Type	•	Other Conditions	Requirements		
(a)	Work Centers			Policy Options	Default_AntiMalware_Policy_Ma c	Any		Mac OSX		4_x or later		d Agent			Any_AM_Installation_Ma Edit c		
				Poll +	Agentiess_Policy_Applicatic	Any +		Windows All +		4.x or later		d Agentless		and (Optional) Dictio +	Agenties × Done		
(?)	Interactive Help			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	any Any		Mac OSX		4.x or later		d Temporal Agen			Agentless_Requirem	ent_Appli 🎽 🏮	
				Policy Options	Default_AntiMalware_Policy_Win	i Any		Windows All		4.x or later		d Agent			Any_AM_Installation_WI Edit		
			0	Policy Options	Default_AntiMalware_Policy_Win_temporal	t Any		Windows All		4.x or later		id Temporal Agen			Any_AM_Installation_Wi Edit		
				Policy Options	Default_AppVis_Policy_Mac	Any		Mac OSX		4.x or later		d Agent			Default_AppVis_Require Edit ment_Mac		
				Policy Options	Default_AppVis_Policy_Mac_te mporal	: Any		Mac OSX		4.x or later		d Temporal Agen			Default_AppVis_Require Edit ment_Mac_temporal		
				Policy Options	Default_AppVis_Policy_Win	Any		Windows All		4.x or later		d Agent			Default_AppVis_Require Edit ment_Win		
				Policy Options	Default_AppVis_Policy_Win_te mporal	i Any		Windows All		4.x or later		d Temporal Agen			Default_AppVIs_Require Edit ment_Win_temporal		
				Policy Options	Default_Firewall_Policy_Mac	Any		Mac OSX		4.x or later		d Agent			Default_Firewall_Require Edit ment_Mac		
			٥	Policy Options	Default_Firewall_Policy_Mac_te mporal	i Any		Mac OSX		4.x or later		d Temporal Agen			Default_Firewall_Require Edit ment_Mac_temporal		
				Policy Options	Default_Firewall_Policy_Win	Any		Windows All		4.x or later		d Agent			Default_Firewall_Require Edit ment_Win		
				Policy Options	Default_Firewall_Policy_Win_te mporal	Any		Windows All		4.x or later		id Temporal Agen	et.		Default_Firewall_Require Edit ment_Win_temporal		
				Policy Options	Default_Hardware_Attributes_P olicy_Mac	i Any		Mac OSX		4.x or later		d Agent			Default_Hardware_Attrib Edit utes_Requirement_Mac		
				Policy Options	Default_Hardware_Attributes_P	Any		Mac OSX		4.x or later		d Temporal Agen			Default_Hardware_Attrib Edit		
																	we la

Agentenlose Statusrichtlinie

### **Client-Bereitstellung**

### Schritt 1 - Herunterladen von Ressourcen

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

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



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

≡	dentity Services	Engine								Work Cent	ers / Posture	
IJ	Bookmarks	Overview	Network Devices	Client Pro	visioning	Policy Elemen	its	Posture Policy	Policy S	ets Troubleshoo	t Reports	Settings
5	Dashboard	Client Provis	ioning Policy									
녢	Context Visibility	Resources		Reso	urces							
×	Operations	Client Provis	ioning Portal									
- 0	Policy			🖉 Edit	+ Add ^ (	Duplicate f	) Dele	ete				
•	Administration			O	Agent resour	ces from Cisco site			Version	Last Update	Description	
-	Administration				Agent resour	ces from local disk		OsXSPWizard	2.7.0.1	2023/05/17 23:11:40	Supplicant Provis	sioning
- 61	Work Centers				Native Suppli	cant Profile		oAgentlessWind	5.0.529.0	2023/05/17 23:11:47	With CM: 4.3.28	68.6145
					Agent Config	uration		ve Supplicant Pro	Not Applic	2016/10/06 15:01:12	Pre-configured N	lative S
	Interactive Help				Agent Postur	e Profile		SPWizard	3.2.0.1	2023/05/17 23:11:40	Supplicant Provis	sioning
					AMP Enabler	Profile		oTemporalAgent	5.0.529.0	2023/05/17 23:11:41	With CM: 4.3.28	68.6145
					Cisco-ISE-NSF	,	Nati	ve Supplicant Pro	Not Applic	2023/05/18 00:14:39	Pre-configured N	lative S
					CiscoAgentles	sOSX 5.0.005	Cisc	coAgentlessOSX	5.0.529.0	2023/05/17 23:11:50	With CM: 4.3.24	90.4353
				0	CiscoTempora	AgentOSX 5	Cisc	coTemporalAgent	5.0.533.0	2023/05/17 23:11:44	With CM: 4.3.24	90.4353

Ressourcen

.

### Mitarbeiterressourcen von Cisco Website



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

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

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

≡	dialo Identity Services	Engine	Work Centers / Posture	
			Resources	
	Context Visibility Operations			
	work Centers		Clsco-Agentiess Windows 5.	
			WinSPWitzard 3.2.0.1         AnyConnectComplianceModuleW Cisco Secure Client Windows Compliance Module 4.3.4164.8192	
			ClscoTemporalAgentWindo AnyConnectComplianceModuleW Clsco Secure Client WindowsARM64 Compliance Module 4.3.4114.8192 Clsco-ISE-NSP AnyConnectComplianceModuleW Clsco Secure Client WindowsARM64 Compliance Module 4.3.4164.8192	
			CliscoAgentless OSX 5.0.00! CliscoAgentless OSX 5.1.5.29 CliscoAgentless OSX With CM: 4.3.3609.6400	
			CiscoTemporalAgentOSX 5 CiscoAgentiess CiscoAgentie	
			CiscoAgenilessWindows 5.1.6.6 Cisco Ageniless for Windows With CM: 4.3.4164.8192	
			Cisco Temporal Agent OSX 5.1.5.29 Cisco Temporal Agent for OSX With CM: 4.3.3609.6400  Cisco Temporal Agent OSX 5.1.6.6 Cisco Temporal Agent for OSX With CM: 4.3.3656.6400  Cisco Temporal 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 Temps 4.3.3656.64
			Cancel	J

Mitarbeiterressourcen von der Cisco Website

### Schritt 2 - Konfigurieren der Client-Bereitstellungsrichtlinie

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

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

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



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

), und wählen Sie Work Centers > Posture > Client Provisioning > Client Provisioning Policy aus. Klicken Sie auf den Pfeil nach unten, und wählen Sie Neue Richtlinie oben einfügen oder Neue Richtlinie unten einfügen, Oben duplizieren oder Unten duplizieren aus: • Regelname: Agentless\_Client\_Provisioning\_Policy

Gibt den Namen der Client-Bereitstellungsrichtlinie an.

Betriebssystem: Alle Windows

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

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

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

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



### •Klicken Sie auf Save (Speichern).

Agentenlose Client-Bereitstellungsrichtlinie



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

Agentenloses Autorisierungsprofil (Autorisierungsprofil)

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



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

In diesem Konfigurationsbeispiel wird Authorization Profile als Agentless\_Authorization\_Profile bezeichnet.

Agentenloser Status im Autorisierungsprofil aktivieren.

•

•

٠

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

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

Klicken Sie auf Speichern.

	alada Identity Services E	Engine	Policy / Policy Elements
Ш	Bookmarks	Dictionaries Conditions R	sults
	Dashboard		Authorization Profile
PS 15	Context Visibility	Authentication >	* Name Agentiess_Authorization_Profi
*	Operations	Authorization  Authorization Profiles	Description
0	Policy	Downloadable ACLs	* Access Type
80	Administration	Profiling >	ACCESS_ACCEPT
ก็ไ	Work Centers	Posture >	Network Device Profile Elise v
	- Interestive Hele	Client Provisioning >	Service Template
G	Interactive Help		Agentless Posture
			Passive Identity Tracking 🔲 🕦
			Common Tasks
			DACL Name PERMIT_ALL_IPV4_TRAFFIC V
			Pv6 DACL Name
			ACL (Filter-ID)
			✓ Advanced Attributes Settings
			Belect an item         v         -         +
			~ Attributes Details
			Access Type = ACCESS_ACCEP1 DACL = PERMIT_ALL_IPV4_TRAFFIC

Agentenloses Autorisierungsprofil

Alternative zur Behebung (optional)

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

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



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

=				Work Centers				
н						Portals & Components		
55								
1d		Guest	Portals					
*								
0								
20					tal Tana		×	
, Fi		Create Gue	st Portal -	Choose Por	tal Type			
		Choose the type of port	tal you want to create.					
?		<ul> <li>Sponsored-Guest</li> <li>Sponsors create</li> <li>Self-Registered G</li> <li>Guests provide</li> <li>Hotspot Guest Por</li> </ul>	Portal e guests' accounts. Gu uest Portal information to automat tal	ests cannot create their ically create an accoun	r own accounts. t, with sponsor approval a	is an optional requirement.		
		Guests can acce	ess the network without	it credentials, but you c	an add a welcome messag	ge and AUP.		
						Cancel Continue		
			te an authorization poli /ork Centers > Guest A					

Hotspot-Gastportal

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

# • Warning • Gentless Flow Failure ! • Varning • Gentless Flow Failure ! Dear User, We regret to inform you that your recent attempt to orinplete the Agentless flow has failed. This process is crucial for your seamless interaction with our system, and its failure may affect the functionality and ervices you can access. Thank you for your attention to this matter. We pologize for any inconvenience this may have caused. Understool

Fehlgeschlagener Status Agentenlos

### Behebungs-Autorisierungsprofil (optional)



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

.

), wählen Sie Policy > Policy Elements > Results > Authorization > Authorization Profilesund erstellen Sie ein Authorization Profile für die Behebung.

In diesem Konfigurationsbeispiel erhält den Namen Authorization Profile mit Remediation\_Authorization\_Profile.

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

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

Klicken Sie auf Speichern.

•

٠

•

$\equiv$ dealer identity Services	Engine	Policy / Policy Elements
JII Bookmarks	Dictionaries Conditions	suits
Dashboard     Context Visibility	Authentication >	Authorization Profiles > Remediation_Authorization_Profile Authorization Profile
	Authorization Profiles Downloadable ACLs	* Name temediation_Authorization_Pr
2 Administration	Profiling >	Description
H Work Centers	Posture >	* Access Type ACCESS_ACCEPT V
Interactive Help	Cillent Provisioning >	Network Device Profile  Service Template Track Movement G Service SPosture SPosture Service SPosture
		✓ Common Tasks     ✓ More Redirection (CWA, MDM, NSP, CPP)     O     Hor Spot ACL
		Static IP/Host name/FOON Suppress Profile CoA for endpoints in Logical Profile Auto Smart Port -
		✓ Advanced Attributes Settings
		Select an Item* +
		Attributes Details Acces Type + ACDSS, ACDS7 Acces Type + CDSS, ACDS7 Acces Type + CDSS, ACDS7 Acces Type + Transfer do Husseper Externationups acce-so-par + uf-redired-https://p.ort/port/portal/pateway/tecatorid-Secsion/drialue8portal-6673aad-dth-4cea-862-472509c1c7738acton=owa80pe=-dw
		Accest Priper # ACIES, ACIEST MAL = Linked, Acces dico-ar-pair = ul-redirect=https://proof/portal/gateway/hesolonid=Secsionid/Naluetportal=6673aaef-df0=4cae-86/2-672559t:1c7738action=cwalkgpe=drw

Behebungsautorisierungsregel

Agentenlose Autorisierungsregel

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



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



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

### Unbekannt\_Compliance\_Redirect:

### •Bedingungen:

Konfigurieren Sie Network\_Access\_Authentication\_Passed UND **Compliance\_Unknown\_Devices** mit dem Ergebnis "Agentless Posture". Diese Bedingung löst den agentenlosen Datenfluss aus.

· Beispielbedingungen:

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

Die Bedingung Compliance\_Unknown\_Devices muss konfiguriert werden, da der ursprüngliche Status unbekannt ist.

• Autorisierungsprofil:

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

Conditions Studio			8 ×
Library	Editor		
Search by Name • • • • • • • • • • • • • • • • • • •		luisagar ExternalGroups	
ii 🗉 sa 💿			
: E BYOD_is_Registered		Compliance_Unknown_Devices	
:: Catalyst_Switch_Local_Web_Authentication			
Compliance_Unknown_Devices			Save
: Compliant_Devices			
EAP-MSCHAPv2			
# EAP-TLS ①			



### Nicht konforme\_Geräte\_Umleitung:

• Bedingungen: Konfigurieren Sie Network\_Access\_Authentication\_Passed und Non\_Compliant\_Devices, wobei das Ergebnis auf DenyAccess festgelegt ist. Alternativ können Sie die Sanierungsoption verwenden, wie in diesem Beispiel gezeigt.

· Beispielbedingungen:

Konfigurieren einer AD-Gruppenbedingung zum Segmentieren des Datenverkehrs

Die Bedingung **Compliance\_Unknown\_Devices** muss so konfiguriert werden, dass beschränkte Ressourcen zugewiesen werden, wenn der Status nicht konform ist.

· Autorisierungsprofil:

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

Conditions Studio										0 ×
Library		Editor								
Search by Name				luisagar-Exte	roalGrou	ne				® <sup>®</sup>
	t 🕈		4	Equals		luisagar.com/Users/AD-PostureGroup	ID ×			
# 🗉 56										
# EYOD_Is_Registered			Non.	_Compliant_Devic	es					
Catalyst_Switch_Local_Web_Authentication										
: E Compliance_Unknown_Devices								, ,	cate	Save
: E Compliant_Devices										
EAP-MSCHAPv2										
🗄 📄 EAP-TLS										
# 🗐 Guest_Flow										
# E MAC_In_SAN										
:: E Network_Access_Authentication_Passed										
: 🗐 Non_Cisco_Profiled_Phones										
E Non_Compliant_Devices										

Nicht konforme Autorisierungsregel

### Compliant\_Geräte\_Zugriff:

### •Bedingungen:

Konfigurieren Sie Network\_Access\_Authentication\_Passed und Compliant\_Devices, wobei das Ergebnis auf PermitAccess festgelegt ist.

· Beispielbedingungen:

Konfigurieren einer AD-Gruppenbedingung zum Segmentieren des Datenverkehrs

Die Bedingung Compliance\_Unknown\_Devices muss so konfiguriert werden, dass kompatible Geräte den richtigen Zugriff erhalten.

· Autorisierungsprofil:

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

Conditions Studio			@ ×
Library	Editor		
		histores Esternal/Course	
♥ □		Equals V Inisager.com/Users/AD-PostureGroup -	
ii 🗄 56 🛛 🕜			
: BYOD_is_Registered	AND	Compliant_Devices	
: Catalyst_Switch_Local_Web_Authentication			
E Compliance_Unknown_Devices			
Compliant_Devices			5440
E EAP-MSCHAPv2			
EAP-TLS			
: B Guest_Flow			
: B MAC_In_SAN O			

Autorisierungsregel für Konformität

### Alle Autorisierungsregeln

≡ dentity Services Engin	e Policy / Policy Sets		Q (	) ()	Q   X
<b>J</b> Bookmarks	Policy Sets Agentless_PS			<b>s</b>	Save
Dashboard	Status Policy Set Name Description Conditions		Allowed Protocols / Serv	er Sequ	ance Hits
Context Visibility					
Operations	Agentiess_PS     Retwork Access NetworkDeviceName EQUALS PostureSwitch				
Administration					
Work Centers	> Authentication Policy(2) > Authentication Policy(2)				
	> Authorization Policy - Global Exceptions				
? Interactive Help	VAuthorization Policy(4)				
		Results			
	Status Rule Name Conditions	Profiles	Security Groups	Hits	Actions
	Unisnown_Compliance_Redir     AND     Compliance_Uninnown_Devices     Compliance_Uninnown_Devices     Compliance_Uninnown_Devices	Agentless_Authorization_P			
	NonCompilant_Devices_Red     AND     Revisager ExternalGroups EQUALS_Misager.com/Uterst/AD-PostureGroup     Revisager.com/Uterst/AD-PostureGroup     Non_Compilant_Devices	Remediation_Authorization			
	Compliant_Devices_Access     AND     Compliant_Devices_Access     And     Compliant_Devices     Compliant_Devices     Compliant_Devices     Compliant_Devices	PermitAccess 0 +			
	Default	DenyAccess // +			
					Save

### Autorisierungsregeln

### Anmeldeinformationen für Endpunkt konfigurieren



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

), wählen Sie Administration > Settings > Endpoint Scripts > Login Configuration aus, und konfigurieren Sie die Client-Anmeldedaten für die Anmeldung bei Clients.

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

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

### Windows-Domänenbenutzer:

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

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

≡	aloghe Identity Services I	Engine								Administration / System
Щ	Bookmarks	Deployment Licensi	ng Ce	rtificates Loggi	ng Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
	Dashboard	Client Provisioning		E a la stat l						
ц.	Context Visibility	FIPS Mode		Endpoint I	_ogin Configi	iration				
×	Operations	Security Settings		Credentials to login t	o endpoints					
Ð	Policy	General MDM / UEM Settings		Windows Domain Us	er Windows Local Use	n MAC Loc	al 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-Domänenbenutzer

Lokaler Windows-Benutzer:

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

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

≡	diada Identity Services	Engine		Administration / System
Щ	Bookmarks	Deployment Licensing C	ertificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
- 55	Dashboard	Client Provisioning		
ы М	Context Visibility	FIPS Mode	Endpoint Login Configuration	
×	Operations	Security Settings Alarm Settings	Credentials to login to endpoints	
0	Policy	General MDM / UEM Settings	Windows Domain User (Windows Local User) MAC Local User	
20	Administration	Posture >		
ส์เ	Work Centers	Profiling	Agetless	
		Protocols >		
?	Interactive Help	Endpoint Scripts ~	Password	
		Login Configuration		
		Settings		
		Proxy		Reset Save
		SMTP Server		
		SMS Gateway		
		System Time		
		API Settings		
		Data Connect		

Lokaler Windows-Benutzer

### Konten überprüfen

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

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



Konten überprüfen



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

Lokaler MAC-Benutzer: Konfigurieren Sie das lokale Konto, das die Cisco ISE für den Zugriff auf den Client über SSH verwendet. Das lokale Konto muss in der Lage sein, Powershell und Powershell remote auszuführen. Geben Sie im Feld Benutzername den Kontonamen des lokalen Kontos ein. Um einen Mac OS-Kontonamen anzuzeigen, führen Sie diesen Befehlwhoami im Terminal aus:

### Einstellungen



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

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

Dieser Screenshot zeigt die Standardwerteinstellungen:

≡	dentity Services	Engine									Administration / System	
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
	Dashboard Context Visibility	Client Provisionin FIPS Mode	ng	Settir	igs							
*	Operations Policy	Security Settings Alarm Settings General MDM / U	JEM Settings	🥑 Upload e 🗌 Endpoint	ndpoint script exe script execution v	cution logs to ISE verbose logging						
20	Administration	Posture		> Endpoints pr	rocessor batch siz							
-fi	Work Centers	Profiling										
		Protocols		> 5	ocessing concurr	ency for MAC						
?	Interactive Help	Endpoint Scripts	s .	Endpoints pr	rocessing concurr	ency for windows						
		Settings										
		Proxy SMTP Server SMS Gateway		Max retry at 30	tempts for OS ide	ntification						
		System Time										
		API Settings Data Connect		2000	en retries for OS	identification(msec)						
		Network Succes	s Diagnostics	> Endpoint pay 1000	gination batch size	e						
		DHCP & DNS Services Max Sessions Light Data Distribution Endpoint Replication		Log retentio 7	n period on endpo	pints (Days)						
		Interactive Help Enable TAC Sup;	port Cases	Connection	Time out(sec)							
				Max retry at 3	tempts for Conne	ction						
				Port Number 5985	r for Powershell C	connection*						
				Port Number 22	for SSH Connect	tion*						
						Save						

Endpunkt-Skript-Einstellungen

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

Konfigurieren und Problembehebung für Windows Endpoint



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

Voraussetzungen für Verifizierung und Fehlerbehebung

Testen der TCP-Verbindung mit Port 5985

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

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

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

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

Connection failed to WinRM

Erstellen einer eingehenden Regel, um PowerShell auf Port 5985 zuzulassen

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

File Action View Help							
File       Action       View       Help         Image: Second Sec	Inbound Rules Name	Group @FirewallAPI.dll,-80200 @FirewallAPI.dll-80200 @FirewallAPI.dll-80200 ate. What type of rule would you like to crea Program Rule that controls connections for a @ Port Rule that controls connections for a @ Predefined: @FirewallAPI.dll,-80200 Rule that controls connections for a @ Custom	Profile All All te? program. TCP or UDP port	Enabled Yes Yes	Action Allow Allow	Ove A No No	Actions Inbound Rules New Rule Y Prof y Stat y Gro
		Custom rule.	<	Back	Next >	с	ancel

### Schritt 2- Wählen Sie unter Protokolle und Ports die Option TCP und Lokale Ports angeben, geben Sie die Portnummer 5985

(Standardport für PowerShell-Remoting) ein, und klicken Sie auf Weiter:

P Windows Defender Firewall with Advanced Security								
File Action View Help								
♦ ♦ 2 🔜 🔒 🛛 📩								
Pindows Defender Firewall with Advanced Security on Local Computer	Inbound Rules						Actions	_
Inbound Rules	Name	Group	Profile	Enabled	Action	Ove ^	Inbound Rule	s
Connection Security Rules	@FirewallAPI.dll,-80201	@FirewallAPI.dll,-802	All 00	Yes	Allow	No	🐹 New Rule	e
> 🐱 Monitoring	© FirewallAPI.dll80206	@FirewallAPI.dll802	All 00	Yes	Allow	No	ly F	Prof
	🛉 🕍 New Inbound Rule Wizard						×	State
	Protocol and Ports						v	Grou
	Specify the protocols and ports to white	ch this rule applies.						
	Steps:						r	
	Rule Type	Does this rule apply to TCP or UE	OP?				Lis	st
	Protocol and Ports	( TCP						
	Action	O UDP						
	Profile							
	i 🧿 Name	Does this rule apply to all local po	orts or specific local po	orts?				
		○ All local ports						
		Specific local ports:	5985					
	1		Example: 80, 443	5000-5010				
	1							
	1							
				Rack	Nexts		leade	
				Back	IVEXL >		anoel	
	Ł					>		

Protokolle und Ports

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

PWindows Defender Firewall with Advanced Security on Local Computer	Inbound Rules						Actions	_
Cutbound Rules	Name	Group	Profile	Enabled	Action	Ove ^	Inbound Rules	
Supervision Security Rules	Contraction  Con	@FirewallAPI.dll-80200	All din the rule.	Yes	Allow	No	× y Pr y Sta	rof tate
	Steps: Protocol and Ports Action Profile Name	hat action should be taken when a co Allow the connection This includes connections that are pr Allow the connection if it is see This includes only connections that h will be secured using the settings in II Rule node. Customze. Block the connection	nnection matc otected with II ave been auti Psec propertie	hes the specific spec	ed conditions those are no using IPsec. ne Connectio	r? x. Connection n Security	is ancel	t

Aktion

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

P Windows Defender Firewall with Advanced Security on Local Computer	Inbound Rules						Actions	
🗱 Inbound Rules	Name	Group	Profile	Enabled	Action	Ove ^	Inbound Rul	les
Cutbound Rules	M @FirewallAPI dll -80201	@FirewallAPI dll -80200	All	Vec	Allow	No	Mary Pu	de.
Connection Security Rules	M @FirewallAPI dll -80206	@FirewallAPI dll -80200		Vec	Allow	No	New Ku	
Connection Security Rules	C CritewallAPI.dll80201 C CritewallAPI.dll80206 Profile Specify the profiles for which this rule applies Steps: Rule Type Protocol and Ports Action Profile Name V	©FirewallAPI.dll, 80200 @FirewallAPI.dll -80200 @FirewallAPI.dll -80200 s. /hen does this rule apply? Domain Applies when a computer is connected or work place. Public Applies when a computer is connected	All All ed to its corpor	Yes Yes ate domain. network locatio	Allow Allow on, such as a n.	No No	X New Ru	le Pro Stat Gro
				< Back	Next >	Ca	ancel	

Profil

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

P Windows Defender Firewall with Advanced Security on Local Computer	Inbound Rules								
Inbound Rules Connection Security Rules Monitoring	Name	Group @FirewallAPI.dll,-80200 @FirewallAPI.dll80200 of this rule.	Profile All All	Enabled Yes Yes	Action Allow Allow	Ove ^ No No	Inbound R		
	Steps: Protocol and Ports Action Profile Name	Name: Allow PowerShell Port 5985		< Back	Finish		ancel		

Name

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

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

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



Lokale Administratorberechtigungen

### WinRM-Listener wird überprüft

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

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

### Aktivieren von PowerShell Remoting WinRM

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

# Enable the WinRM service Enable-PSRemoting -Force # Start the WinRM service Start-Service WinRM # Set the WinRM service to start automatically Set-Service -Name WinRM -StartupType Automatic

### **Erwartete Ausgabe:**

C: \Windows\system32> Enable-PSRemoting -Force WinRM is already set up to receive requests on this computer. WinRM has been updated for remote management. WinRM firewall exception enabled. -Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

C: \Windows\system32> Start-Service WinRM

### C: \Windows\system32> Set-Service -Name WinRM -StartupType Automatic

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

### Überprüfen der PowerShell- und cURL-Versionen unter Windows

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

### Überprüfen der PowerShell-Version

### **Unter Windows:**

### 1. Öffnen Sie PowerShell:

- · Drücken Sie Win + X, und wählen Sie Windows PowerShell oder Windows PowerShell (Admin) aus.
- 2. Führen Sie den folgenden Befehl aus: \$PSVersionTable.PSVersion
- · Dieser Befehl gibt die Versionsdetails von PowerShell aus, die auf Ihrem System installiert sind.

### Überprüfen der cURL-Version

### **Unter Windows:**

### 1. Eingabeaufforderung öffnen:

- Drücken Sie Win + R, geben Sie cmd ein, und klicken Sie auf Enter.
- 2. Führen Sie den Befehl: curl --version
- · Dieser Befehl zeigt die auf Ihrem System installierte Version von cURL an.

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

C: \Windows\system32> \$PSVersionTable.PSVersion Major Minor Build Revision ----- 7 1 19041 4291

C: \Windows\system32>

C: \Windows\system32>

C: \Windows \system32>**curl --version curl 8.4.0 (Windows) libcurl/8.4.0 Schannel WinIDN** Release-Date: 2023-10-11 Protocols: dict file ftp ftps http https imap imaps pop3 pop3s smtp smtps telnet ftp ftps http https Features: AsynchNS HSTS HTTPS-proxy IDN IPv6 Kerberos Largefile NTLM SPNEGO SSL SSPI threadsafe Unicode UnixSockets c: \Windows\system32>

### Zusätzliche Konfiguration

Mit diesem Befehl wird der Computer so konfiguriert, dass er bestimmten Remotehosts für WinRM-Verbindungen vertraut: Set-Item WSMan:\localhost\Client\TrustedHosts -Value <Client-IP>

C: \Windows\system32> Set-Item WSMan:\localhost\Client\TrustedHosts -Value x.x.x WinRM Security Configuration. This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list cannot be authenticated. The client can send

credential information to these computers. Are you sure that you want to modify this list? [Y] Yes [N] No [S] Suspend [?] Help (default is "y"): Y PS C: \Windows \system32> -

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

MacOS

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

### **Unter MacOS:**

### 1. Terminal öffnen:

- Terminal finden Sie unter Anwendungen > Dienstprogramme.
- 2. Führen Sie den Befehl: pwsh -Command '\$PSVersionTable.PSVersion'



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

### **Unter MacOS:**

### 1. Terminal öffnen:

- Terminal finden Sie unter Anwendungen > Dienstprogramme.
- 2. Führen Sie den Befehl: curl --version
- · Dieser Befehl muss die auf Ihrem System installierte Version von cURL anzeigen.

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

### **Detaillierte Anleitung:**

### 1. Systemeinstellungen öffnen:

· Navigieren Sie im Apple-Menü zu Systemeinstellungen.

### 2. Remote-Anmeldung aktivieren:

- · Gehe zu Freigabe.
- · Aktivieren Sie das Kontrollkästchen neben Remote Login (Remote-Anmeldung).

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

### 3. Firewall-Einstellungen überprüfen:

- · Wenn die Firewall aktiviert ist, müssen Sie sicherstellen, dass SSH-Verbindungen zugelassen werden.
- · Gehen Sie zu Systemeinstellungen > Sicherheit und Datenschutz > Firewall.
- · Klicken Sie auf die Schaltfläche Firewall Options (Firewall-Optionen).
- Überprüfen Sie, ob **Remote Login** oder **SSH** aufgeführt und zugelassen ist. Wenn es nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Hinzufügen** (+), um es hinzuzufügen.

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

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

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

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

### 5. SSH-Zugriff testen:

- · Öffnen Sie von einem anderen Gerät aus ein Terminal oder einen SSH-Client.
- · Verbindungsversuch mit dem macOS-Client über dessen IP-Adresse:ssh username@<macOS-client-IP>
- · Ersetzen Sie den Benutzernamen durch das entsprechende Benutzerkonto und <macOS-client-IP> durch die IP-Adresse des macOS-Clients.

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

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

### Voraussetzungen

- · Administratorzugriff auf dem macOS-System.
- · Grundlegende Kenntnisse der Terminalbefehle

### Schritte zum Aktualisieren der Sudoers-Datei

### 1. Terminal öffnen:

• Terminal finden Sie unter Anwendungen > Dienstprogramme.

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

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

· Sie werden aufgefordert, Ihr Administratorkennwort einzugeben.

### 3. Suchen Sie den entsprechenden Abschnitt:

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

### 4. Erforderlichen Eintrag hinzufügen:

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

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

### 5. Speichern und beenden:

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

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

### 6. Überprüfen Sie die Änderungen:

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

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

· Diese Befehle können ohne Eingabe eines Kennworts ausgeführt werden.

## Informationen zu dieser Übersetzung

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