

# 使用安全客户端 ISE 安全评估模块和 Cisco Secure Firewall Management Center 来评估终 端合规性

**首次发布日期:** 2023 年 7 月 27 日

# 使用安全客户端ISE安全评估模块和CiscoSecureFirewallManagement Center来评估终端合规性

简介

Cisco Secure 客户端的识别服务引擎 (ISE) 安全评估模块可帮助您在允许终端连接到您的网络之前对 其进行评估。评估可以针对特定版本的防病毒软件、反间谍软件、文件、注册表项等。在安全评估 期间,所有连接到您网络的客户端都必须符合强制性要求。

ISE 安全评估模块可执行客户端评估。客户端从 ISE 获得安全评估要求策略、执行安全评估数据收集、将结果与策略进行比较,并将评估结果发送回 ISE。

安全评估合规性状态	说明
合规	如果已为终端定义匹配的终端安全评估策略,则 终端的终端安全评估合规性状态会设置为合规。
	当进行安全评估时,终端会满足匹配的安全评估 策略中定义的所有强制性要求,并被授予网络访 问权限。
不合规	当为某个终端定义匹配的安全评估策略,但该策 略在安全评估过程中未能满足所有强制性要求 时,该终端的安全评估合规性状态为不合规。
	不合规的终端会将安全评估要求与补救操作匹 配,并且应对该终端授予对补救资源的有限网络 访问权限以便自行补救。

安全评估服务将安全评估状态分类为:

安全评估合规性状态	说明
未知	如果没有为终端定义匹配的终端安全评估策略,则终端的终端安全评估合规性状态可能设置为未知。
	如果安全评估策略已启用但其安全评估评估尚未 进行,客户端代理也未提供合规报告,则终端也 可能具有此状态。

### 优势

使用威胁防御配置 ISE 安全评估模块具有以下显著优势:

- •易于分发和管理每个终端上的 ISE 安全评估模块和配置文件。
- 在终端连接到企业网络之前轻松评估终端合规性。

# 本指南适用对象

此使用案例主要面向希望使用管理中心来配置 ISE 安全评估模块以进行终端合规性评估的网络管理员。

## 系统要求

下表显示了此功能支持的平台。

产品	版本	本文档使用的版本
Cisco Secure Firewall Threat Defense(之前的 Firepower 威胁防御/FTD)	6.3 及更高版本	7.3
Cisco Secure Firewall Management Center (之前的 Firepower 管理中心/FMC)	6.7 及更高版本	7.3
Cisco Secure Client (之前的 AnyConnect)	4.0 及更高版本	5.0
Cisco ISE	2.0 及更高版本	3.1

# 前提条件

确保:

- 使用管理员权限访问思科 ISE 服务器。
- •已将安全客户端软件包和安全客户端配置文件编辑器从思科软件下载中心下载到本地主机。

- •已将安全客户端配置文件编辑器安装到本地主机。
- 已将 ISE 合规性模块从思科软件下载中心下载到本地主机。
- •托管威胁防御中已配置的 ISE 服务器详细信息。请参阅在管理中心配置 ISE。
- •在管理中心配置远程访问 VPN。

#### 许可证

- ISE Premier 许可证。
- •以下安全客户端许可证之一:

仅 Secure Client Premier、Secure Client Advantage 或 Secure Client VPN。

• 管理中心 Essentials(以前称为 Base)许可证必须允许导出控制功能。

依次选择**系统 (System) > 许可证 (Licenses) > 智能许可证 (Smart Licenses)** 以在管理中心验证此功能。

### 在管理中心配置 ISE

您必须在管理中心将 ISE 服务器配置为:

- 允许来自远程接入 VPN 的威胁防御的 AAA 请求。
- •从 ISE 接收安全评估要求策略。
- •将评估结果发送到 ISE。

您必须创建 RADIUS 服务器对象,并使用 ISE 服务器详细信息对其进行配置。

过程

- 步骤1 依次选择对象 (Objects) > 对象管理 (Object Management) > AAA 服务器 (AAA Server) > Radius 服 务器组 (RADIUS Server Group)。
- 步骤 2 点击添加 RADIUS 服务器组 (Add RADIUS Server Group)。
- 步骤3 输入名称和重试间隔时间。

ISE						
Description:			٦			
Group Accountir	ng Mode:					
Single						
Retry Interval:*	(1-10	) Second	S			
10						
Deelerer						
Realms:						
Enable autho	orize only	•				
Enable authors:	orize only im account (1-1	vupdate	6			
Enable authorithe     Enable interi Interval:* 24	orize only im account (1-1	▼ update 120) hours	5 ]			
Content of the second seco	orize only im account (1- mic authori	vupdate 120) hours zation	5 ]			
Contemporary interval: Co	orize only im account (1-1 mic authoria (102	update 120) hours zation 24-65535	) )			
Realms: Enable authors Enable interior Interval:* 24 Enable dyna Port:* 1700	orize only im account (1-1 mic authori (10)	vupdate 120) hours zation 24-65535	s )			
Realms: Enable authors Enable interinterval:* 24 Enable dyna Port:* 1700 RADIUS Servers	orize only im account (1-1 mic authori (10) (Maximum	vupdate 120) hours zation 24-65535 16 server	5 ) ) <b>s)</b>			
Realms: Enable authors Enable intering Interval:* 24 Enable dyna Port:* 1700 RADIUS Servers IP Address/Hos	orize only im account (1- mic authoria (10) (Maximum thame	update 120) hours zation 24-65535 16 server	s ) ) s)			

- 步骤4 将端口配置为1700。
- 步骤5 点击+以添加 ISE 服务器。
- 步骤6 输入 ISE 服务器的 IP 地址。
- 步骤7 将身份验证端口 (Authentication Port) 保留为 1812。
- 步骤8 配置密钥。

输入共享密钥,以便对托管设备(客户端)和 ISE 服务器之间的数据进行加密。

- **步骤9** 在确认密钥 (Confirm Key) 字段中再次输入密钥。 在 ISE 中添加威胁防御时需要使用此密钥。
- 步骤10 其余参数使用默认值。
- 步骤11 点击保存(Save)。

# 使用管理中心配置 ISE 安全评估模块的端到端程序

以下流程图说明使用管理中心配置安全客户端 ISE 安全评估模块的工作流程。



步骤	应用程序	说明
1	ISE终端安全评估配置文件编辑 器	使用 ISE 安全评估配置文件编辑器配置安全 评估配置文件,第6页
2	ISE	在 ISE 中配置威胁防御,第8页
3	ISE	将 ISE 安全评估配置文件、安全客户端软件 包和 ISE 合规性模块上传到 ISE,第9页
4	ISE	在 ISE 中配置安全客户端配置,第11页
5	ISE	在 ISE 中创建客户端调配策略,第 12 页
6	ISE	在 ISE 中配置安全评估策略,第 13 页
7	ISE	在 ISE 中为安全评估状态配置可下载的 ACL,第 16 页

步骤	应用程序	说明
8	ISE	在 ISE 中为安全评估状态配置授权配置文件,第 17 页
9	ISE	在 ISE 中为安全评估状态配置授权策略,第 18 页
10	管理中心	在管理中心使用 ISE 安全评估模块配置远程 访问 VPN 组策略,第 19页
11	管理中心	在管理中心菜单栏中,点击 <b>部署 (Deploy)</b> , 然后选择 <b>部署 (Deployment)</b> 。

## 使用 ISE 安全评估配置文件编辑器配置安全评估配置文件

独立的安全客户端配置文件编辑器软件包包含ISE安全评估配置文件编辑器。使用此编辑器创建ISE 安全评估配置文件,然后将其上传到ISE 和管理中心。

过程

步骤1 选中启用安全评估非重定向流 (Enable posture non-redirection flow) 复选框。

ISE Posture	Preferences Profile: Untitled		
	Agent Behaviour		
	Enable Signature Check		
	Enable Agent Log Trace		
	Operate On Non-802. 1X Wireless Networks		
	Enable Posture Non-Redirection Flow		
	Enable Stealth Mode		
	Enable Stealth With Notification		
	Disable EDR Internet Check		
	Enable Rescan Button		
	Disable UAC PopUp		
	BackOff Timer Limit	30	Sec
	Log file size	5	MB
	Remediation timer		Min
	Automated DART Count	3	
	Periodic Probe Interval	30	x 10 min
	Posture State Synchronisation Interval	0	Sec
	Posture State Synchronisation Probe List		
	Maximum time for CWA/BYOD probing	90	Sec

步骤2 以\*形式输入服务器名称规则。

这些规则包含由通配符、逗号分隔名称组成的列表,用于定义代理可以连接到的服务器。例如, example1.cisco.com 或 \*.cisco.com。

步骤3 使用 ISE 的 FQDN 或 IP 地址配置 Call Homes 列表。

- Poeture Protocol	
Discovery host	
Server name rules	*
Call Home List	
PRA retransmission time	120 Sec
Retransmission delay	60 Sec
Retransmission limit	4

下一步做什么

在 ISE 中配置威胁防御, 第8页

## 在 ISE 中配置威胁防御

### 过程

- **步骤1**登录 ISE。
- 步骤2 依次选择管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)。
- 步骤3 点击添加 (Add)。
- 步骤4 输入威胁防御的名称、说明和 IP 地址。
- 步骤5 从设备配置文件 (Device Profile) 下拉列表中选择 Cisco。
- 步骤 6 展开 RADIUS 身份验证设置 (RADIUS Authentication Settings)。
- 步骤7 配置共享密钥 (Shared Secret) 和 CoA 端口 (CoA Port)。

使用在威胁防御中用于配置 ISE 的密钥和端口。有关更多信息,请参阅在管理中心配置 ISE。

### 将 ISE 安全评估配置文件、安全客户端软件包和 ISE 合规性模块上传到 ISE

E Cisco ISE					Admir	histration · Networ	k Resources
Network Devices Network	k Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Servi
letwork Devices	Network Devices L	list > FTD2					
efault Device	Network Dev	rices					
evice Security Settings		(11) (1					
	Name	FTD2					
	Description						
	IP Address	~ * IP :	/				
	Device Profile	the Cisco	× (j)				
	Model Name		~				
	Software Version		~				
		· · · · · · · · · · · · · · · · · · ·					
	Network Dev	rice Group					
	Device Type	All Device Types	✓ Set To De	fault			
	IPSEC	No	Y Set To De	fault			
	Location	All Locations	✓ Set To De	fault			
	🔽 🗸 R	ADIUS Authentication Setti	ings				
	RAD	IUS UDP Settings					
	Proto	col RADIUS					
	Share	d Secret	Show				
		se Second Shared Secret					
	networ	kDevices.secondSharedSecret		Show			
		CoA Port 1700		Set To Default			
	RAD	IUS DTLS Settings 🕕					
	_ D	TLS Required ()					
	Share	d Secret radius/dtls	0				

步骤8 点击保存(Save)。

## 将 ISE 安全评估配置文件、安全客户端软件包和 ISE 合规性模块上传到 ISE

过程

- 步骤1 依次选择工作中心 (Work Centers) > 安全评估 (Posture) > 客户端调配 (Client Provisioning) > 资源 (Resources)。
- 步骤2点击添加 (Add),然后选择来自本地磁盘的代理资源 (Agent resources from local disk)。

≡ Cisco	ISE			Work C	enters · Posture
Overview	Network Devices	Client Pro	ovisioning	Policy Elements	Posture Policy
Client Provisioning Resources	Policy	Resou	urces		
Client Provisioning	Portal	🖉 Edit 🛛 –	+ Add 🔨	🗍 Duplicate 🏾 🗍 De	lete
			Agent resou	urces from Cisco site	,
			Agent resou	urces from local disk	onnectDesktopWind

步骤3 从类别 (Category) 下拉列表中,选择思科提供的软件包 (Cisco Provided Packages)。

- 步骤4点击选择文件(Choose File),然后从本地主机中选择以下选项之一:
  - 1. ISE 安全评估配置文件 (ISEPostureCFG.xml)
  - 2. 安全客户端软件包
  - 3. ISE 合规性模块

步骤5 点击提交 (Submit)。

步骤6点击确认(Confirm)以验证校验和。

Please confirm this package's hash matches : SHA-1:bc91eb141b96fc78f3e8969bb6f9cea3553daa50 SHA-256:e010e327ea2f8df2b13925d680024e97d9e94d45fe700142fa6d7a7bd3597768 SHA- 512:af925524d6653be63033b1c56c0bcc168ec9f0b5903d617a0a436ed7fb7d6c2cab90	W	/arning
SHA-1:bc91eb141b96fc78f3e8969bb6f9cea3553daa50 SHA-256:e010e327ea2f8df2b13925d680024e97d9e94d45fe700142fa6d7a7bd3597768 SHA- 512:af925524d6653be63033b1c56c0bcc168ec9f0b5903d617a0a436ed7fb7d6c2cab90	Please confirm th	his package's hash matches :
512:af925524d6653be63033b1c56c0bcc168ec9f0b5903d617a0a436ed7fb7d6c2cab90	SHA-1:bc91eb141b96fc78f3e8969bb6f SHA-256:e010e327ea2f8df2b13925d68 SHA-	9cea3553daa50 30024e97d9e94d45fe700142fa6d7a7bd3597768
5fbfe0699abcee3d54003472326e42a5de0831c2e052d	512:af925524d6653be63033b1c56c0bc 5fbfe0699abcee3d54003472326e42a5c	cc168ec9f0b5903d617a0a436ed7fb7d6c2cab90a3 de0831c2e052d

步骤7	重复步骤 2	至6	以上传剩余的两个文件。
-----	--------	----	-------------

E Cisco ISE		Work Center	s · Posture			Evaluation Mode 70 Days
Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Se	ets Troubleshoot	Reports Settings
Client Provisioning Policy	$\ensuremath{ \mathcal{O}}$ Edit $\ensuremath{+}$ Add $\ensuremath{\sim}$	📋 Duplicate 🏾 🎁 Dele	ete			
Resources	Name	Тур	e	Version	Last Update	Description
Client Provisioning Portal	AnyConnectC	omplianceModuleWi Any	ConnectComplianceM	4.3.3534.81	2023/06/24 08:26:48	Cisco Secure Client Windows
	CiscoTempora	alAgentOSX 4.10.02 Cisc	coTemporalAgentOSX	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
	Cisco-ISE-Ch	rome-NSP Nati	ve Supplicant Profile	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Suppli
	CiscoAgentle	ssOSX 4.10.02051 Cisc	coAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353
	MacOsXSPWi	zard 2.7.0.1 Mac	OsXSPWizard	2.7.0.1	2021/08/09 19:12:27	Supplicant Provisioning Wizar
	CiscoAgentle:	ssWindows 4.10.02 Cisc	coAgentlessWindows	4.10.2051.0	2021/08/09 19:12:33	With CM: 4.3.2227.6145
	AnyConnect C	Configuration Any	ConnectConfig	Not Applicable	2023/06/24 16:05:27	
	Cisco-ISE-NS	SP Nati	ve Supplicant Profile	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Suppli
	WinSPWizard	3.0.0.3 Wins	SPWizard	3.0.0.3	2021/08/09 19:12:27	Supplicant Provisioning Wizar
	CiscoTempora	alAgentWindows 4.1 Cisc	coTemporalAgentWind	4.10.2051.0	2021/08/09 19:12:28	With CM: 4.3.2227.6145
	AnyConnectD	esktopWindows 5.0 Anyo	ConnectDesktopWind	5.0.3072.0	2023/06/26 18:45:44	Cisco Secure Client for Wind
	AC-Posture-F	Profile Any	ConnectProfile	Not Applicable	2023/06/26 17:57:02	

## 在 ISE 中配置安全客户端配置

安全客户端配置(ISE 中的 AnyConnect 配置)是安全客户端软件及其不同的配置文件,例如客户端的安全客户端二进制包、ISE 合规性模块、ISE 模块配置文件、自定义和 AnyConnect 的语言包。

过程

- 步骤1 依次选择工作中心 (Work Centers) > 安全评估 (Posture) > 客户端调配 (Client Provisioning) > 资源 (Resources)。
- 步骤2 点击添加 (Add),然后选择 AnyConnect 配置 (AnyConnect Configuration)。
- 步骤3 从选择 AnyConnect 软件包 (Select AnyConnect Package) 下拉列表中选择安全客户端软件包。
- 步骤4 从合规性模块 (Compliance Module) 下拉列表中选择 ISE 合规性模块。

<b>≡ Cisco</b> ISE			Work Cer	nters · Posture	
Overview Network Devices	Client Provisioning	Polic	y Elements	Posture Policy	Policy Sets
Client Provisioning Policy	AnyConnect Configuration > N	lew Any(	Connect Configura	tion	
Resources					
Client Provisioning Portal	* Select AnyConnect Package:		CiscoSecureCli	ientDesktopWindows !	5.0 ~
	* Configuration Name:		AnyConnect Co	onfiguration	
	Description:			le le	
	Description Value Not	tes			
	* Compliance Module	Cis	coSecureClient	ComplianceModuleW	~
	Cisco Secure Client N	Module	e Selection		

- **步骤 5** 在 Cisco Secure 客户端模块选择 (Cisco Secure Client Module Selection)下, ISE 安全评估默认已启用。
- **步骤 6** 在配置文件选择 (Profile Selection),从 ISE 安全评估 (ISE Posture) 下拉列表中选择 ISE 安全评估文件。
- 步骤7 点击提交 (Submit)。

## 在 ISE 中创建客户端调配策略

用户根据客户端调配策略从 ISE 接收特定版本的资源,例如代理、代理合规性模块或代理自定义配置文件。

### 过程

步骤1选择策略 (Policy) > 客户端调配 (Client Provisioning)。
步骤2点击编辑 (Edit),然后选择插入以上新策略 (Insert new policy above)。
步骤3 输入策略名称,然后选择操作系统。
步骤4点击结果 (Results)下的+,然后从代理 (Agent)下拉列表中选择 AnyConnect 配置。

exercises	Client	Provisioning	g Pol	icy							
ient Provisioning Portal	Define the C For Agent C For Native S	lient Provisioning Policy to onfiguration: version of ag upplicant Configuration: v	o determin jent, agent izard prof	e what users will n t profile, agent con ile and/or wizard. I	eceive u npliance Drag and	pon login and user sessio module, and/or agent cus I drop rules to change the	n initiatio stomizatio order.	m: on package.			
	~										
		Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
	ii 📼	AC_Windows	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect Configuration	E
	H 🖸	IOS	If	Any	and	Apple IOS All	and	Condition(s)	then	Cisco-ISE-NSP	8
	8 🖂	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	
	# 🜌	Windows	If	Any	and	Windows All	and	Condition(s)	then	CiscoTemporalAgentWin dows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP	
	8	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	CiscoTemporalAgentDSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-	

步骤5点击保存(Save)。

### 在 ISE 中配置安全评估策略

安全评估策略、安全评估要求和安全评估条件将确定终端的合规性状态。

#### 过程

步骤1 配置安全评估条件。

- 依次选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 安全评估 (Posture)。
   您可以选择一个或多个安全评估条件。
- 2. 点击防恶意软件 (Anti-Malware) 以选择防恶意软件条件。

您可以选择预定义的防恶意软件条件或创建新的防恶意软件条件。对于 Windows,您可以选择 "ANY\_am\_win\_inst"防恶意软件安全评估条件。

<b>≡ Cisco</b> ISE		Policy · Policy Elements
Dictionaries Conditions	Results	
Library Conditions Smart Conditions Time and Date	Anti-Malware (	Conditions
Profiling	🖉 Edit 🕂 Add 📋 Duplica	ate 🧻 Delete
Posture ~	Name	Description
Anti-Malware		Anno Abd in the United schools as
Anti-Spyware	ANY_am_win_inst	Any AM Installation check on
Anti-Virus	ANY_am_win_def	Any AM definition check on
Application	ANY_am_mac_inst	Any AM installation check on
Compound	ANY_am_mac_def	Any AM definition check on M
Dictionary Simple	ANY_am_lin_inst	Any AM installation check on
Disk Encryption	ANY_am_lin_def	Any AM definition check on Li
External DataSource		
File		

### 步骤2 配置安全评估要求。

# 依次选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 安全评估 (Posture) > 要求 (Requirements)。

安全评估要求是与补救操作相关的一组安全评估条件。您可以从多个默认或预定义安全评估要求中 选择一个,或创建一个新的安全评估要求。

对于 Windows,您可以选择"Any\_AM\_Installation\_Win"防恶意软件安全评估要求。

				,	,							• • • •
Dictionaries Co	onditions	Results										
Authentication	>					Guide Me						~
Authorization	>	Requirements										
Profiling	>	Name		Operating System	n	Compliance Module		Posture Type		Conditions		Remediations Actions
		Any_AS_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	AnyConnect	met if	ANY_as_mac_inst	then	Message Text Only
osture	~	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	AnyConnect	met if	ANY_as_mac_def	then	AnyASDefRemediationMac
Remediation Actions	~	Any_AM_Installation_Win	for	Windows All	using	4.x or later	using	AnyConnect	met if	ANY_am_win_inst	then	Message Text Only
Requirements		Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	AnyConnect	met if	ANY_am_win_def	then	AnyAMDefRemediationWir
Client Provisioning	>	Any_AM_Installation_Mac	for	Mac OSX	using	4.x or later	using	AnyConnect	met if	ANY_am_mac_inst	then	Message Text Only
		Any_AM_Definition_Mac	for	Mac OSX	using	4.x or later	using	AnyConnect	met if	ANY_am_mac_def	then	AnyAMDefRemediationMa
		Note: Remediation Action is filtered based o Remediation Actions are not applicabl Remediations Actions are not applicab	n the o le for Ap ole for A	perating system and steall plication Conditions (confi gentless Posture type.	h mode se igured usin	ection. g the Provision By Category or Pr	ovision By E	verything options), Hardware Co	nditions, an	d External Data source cor	nditions.	Save Res

### 步骤3 配置安全评估策略。

1. 选择策略 (Policy) > 终端安全评估 (Posture)。

您必须通过根据操作系统和一个或多个安全评估要求配置规则来定义安全评估策略。

对于 Windows, 您可以选择 "Default\_AntiMalware\_Policy\_Win" 防恶意软件安全评估策略。

Post	ure Policy	1												
Define the	Posture Policy by c	onfiguring rules based on operat	ing system and/or oth	er conc	litions.							~		Q
~														
Status	Policy Options	Rule Name	Identity Groups		Operating Systems		Compliance Module		Posture Type	Other Conditions		Requirements		
	Policy Options	Default_AntiMalware_Policy_Ma c	If Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and	then	Any_AM_Installation_Ma c	Edit 🗸	
	Policy Options	Default_AntiMalware_Policy_Ma c_temporal	If Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Any_AM_Installation_Ma c_temporal	Edit 🗸	_
	Policy Options	Default_AntiMaiware_Policy_Win	If Any	and	Windows All	and	4.x or later	and	AnyConnect	and	then	Any_AM_Installation_Win	Edit 🛩	
	Policy Options	Default_AntiMalware_Policy_Wi n_temporal	if Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Any_AM_Installation_Wi n_temporal	Edit 🛩	
	Policy Options	Default_AppVis_Policy_Mac	If Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and	then	Default_AppVis_Require ment_Mac	Edit 🛩	
	Policy Options	Default_AppVis_Policy_Mac_te mporal	If Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Mac_temporal	Edit ~	
	Policy Options	Default_AppVis_Policy_Win	If Any	and	Windows All	and	4.x or later	and	AnyConnect	and	then	Default_AppVis_Require ment_Win	Edit 🗸	
	Policy Options	Default_AppVis_Policy_Win_te mporal	If Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Win_temporal	Edit 🗸	
	Policy Options	Default_Firewall_Policy_Mac	If Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and	then	Default_Firewall_Require ment_Mac	Edit 🗸	
	Policy Options	Default_Firewall_Policy_Mac_te mporal	If Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Mac_temporal	Edit ~	
-														
												Save	Reset	

- 2. 选中状态 (Status) 复选框以启用安全评估策略。
- 3. 点击保存 (Save)。

### 在 ISE 中为安全评估状态配置可下载的 ACL

您必须为"未知"(Unknown)、"不合规"(Noncompliant)和"合规"(Compliant)安全评估状态配置 可下载 ACL (DACL)。默认授权 DACL 也可用。

### 过程

- 步骤1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 可下载的 ACL (Downloadable ACLs)。
- 步骤2 点击添加 (Add)。
- 步骤3 输入名称和说明。
- 步骤4点击所需 IP 版本的单选按钮。
- 步骤5 输入 DACL 的值。

Downloadable ACL I	List > Posture_Unknown
Downloadable	ACL
* Name	Posture_Unknown
Description	
IP version	IPv4 ○ IPv6 ○ Agnostic i
* DACL Content	1234567 nermit udn anv anv eq domain
	8910111 permit ip any host xx.xx
	2131415
	1617181
	9202122
	6272829
	3031323
	3343536
	3738394
	U414245

### 步骤6 点击提交 (Submit)。

步骤7 重复步骤2至6,为剩余的安全评估状态创建 DACL。

"未知" (Unknown)、"不合规" (Noncompliant) 和"合规" (Compliant) 安全评估状态的 DACL 示例:

DACL 的类型	说明	DACL
安全评估未知 DACL	允许流向 DNS 和策略服务 (PSN)的流量。	permit udp any any eq domain permit ip any host x.x.x.x
安全评估不合规 DACL	拒绝访问专用子网, 仅允许互 联网流量。	deny ip any x.x.x.x 255.255.255.0 permit ip any any

DACL 的类型	说明	DACL
安全评估合规 DACL	允许所有流量。	permit ip any any

### 下一步做什么

使用这些 DACL 来配置授权配置文件。有关详细信息,请参阅在 ISE 中为安全评估状态配置授权配置文件。

## 在 ISE 中为安全评估状态配置授权配置文件

您必须为"未知"(Unknown)、"不合规"(Noncompliant)和"合规"(Compliant)安全评估状态创建 三个授权配置文件。

过程

- 步骤1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。
- 步骤2 为每个安全评估状态创建授权配置文件。
- 步骤3 点击添加 (Add)。
- 步骤4 输入名称。
- 步骤5 从访问类型 (Access Type) 下拉列表中选择 ACCESS\_ACCEPT。
- 步骤 6 从网络设备配置文件 (Network Device Profile) 下拉列表中选择 Cisco。
- 步骤7 在常见任务 (Common Tasks) 下,选中 DACL 名称 (DACL Name) 复选框,然后从下拉列表中选择 安全评估状态的 DACL。

您可以在属性详细信息 (Attributes Details) 下查看已配置的属性。

以下示例显示了"未知"(Unknown)状态的授权配置文件。

Authorization Profiles > FT	D_VPN_Unknown		
Authorization Profi	le		
* Name	FTD_VPN_Unknown		
Description			
* Access Type	ACCESS_ACCEPT ~	<i>h</i>	
Network Device Profile	🚓 Cisco 🗸 🕀		
Service Template			
Track Movement			
Agentless Posture			
Passive Identity Tracking			
DACL Name	Posture_Unknown ~		
IPv6 DACL Name			
- ACL			1
<ul> <li>Attributes Details</li> </ul>			
Access Type = ACCESS_ACCEPT			
DACL = Posture_Unknown			

### 步骤8 点击提交 (Submit)。

步骤9 重复步骤3至8,为剩余的安全评估状态创建授权配置文件。

### 下一步做什么

使用这些授权配置文件来配置授权策略。有关详细信息,请参阅在 ISE 中为安全评估状态配置授权策略。

## 在 ISE 中为安全评估状态配置授权策略

您必须为每种安全评估状态创建授权策略。

### 过程

步骤1 依次选择策略 (Policy) > 策略集 (Policy Sets)。

### 步骤2 在视图(View)列中,点击默认策略旁边的箭头图标。

Policy Sets			Reset Reset Policyset Hitcounts Save
🛞 Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search			
		+	
Oefault	Default policy set		Default Network Access 🙁 🗸 + 365 503

步骤3展开授权策略(Authorization Policy)。

- 步骤4点击状态(Status)列旁边的+。
- 步骤5 使用安全评估状态 (Posture Status) 和身份组 (Identity Group) 作为策略的条件。
- 步骤6 从安全评估状态的下拉列表中选择适当的授权配置文件。
- 步骤7 点击保存 (Save)。
- 步骤8 对其余授权策略重复步骤4至7。

下图显示了安全评估状态的授权策略。

ISCO ISE			Policy · Policy Sets		0	9	) ,0
0	Default	Default	Guide Me		Default Network Access	∞ ~	+ 27
Authentic	cation Policy (4)						
Authoriza	ation Policy - Local Exceptions						
Authoriza	ation Policy - Global Exception	s					
Authoriza	ation Policy (15)						
				Results			
🕣 Sta	tus Rule Name	Cond	tions	Profiles	Security Groups	Hits	Action
Q Se	arch						
•	FTD-VPN-POSTURE- COMPLIANT	AND	b Session-PostureStatus EQUALS Compliant A InternalUser-IdentityGroup EQUALS User Identity Groups:RADIUS-FTD2-ANYCONNECT	FTD-VPN-Compliant × +	Select from list $\sim$ +	27	ŝ
			E Session-PostureStatus EQUALS NonCompliant	FTD-VPN-NONCOMPLI $\times$ $\vee$ +	Select from list $\sim+$	0	<u>ئې</u>
•	FTD-VPN-POSTURE- NONCOMPLIANT	AND	R InternalUser-IdentityGroup EQUALS User Identity Groups:RADIUS-FTD2-ANYCONNECT				

## 在管理中心使用 ISE 安全评估模块配置远程访问 VPN 组策略

### 开始之前

在管理中心配置远程接入 VPN 策略。

### 过程

- 步骤1 登录管理中心 Web 接口。
- 步骤2 选择设备 (Devices) > 远程访问 (Remote Access)。
- 步骤3 选择远程访问 VPN 策略,然后点击编辑 (Edit)。
- 步骤4 选择连接配置文件,然后点击编辑(Edit)。
- 步骤5 点击编辑组策略 (Edit Group Policy)。
- 步骤6 点击安全客户端 (Secure Client) 选项卡。
- 步骤7 点击客户端模块 (Client Module), 然后点击+。
- 步骤8 从客户端模块 (Client Module) 下拉列表中选择 ISE 安全评估模块。
- 步骤9 从要下载的配置文件 (Profile to download) 下拉列表中选择 ISE 配置文件。
- 步骤 10 选中启用模块下载 (Enable module download) 复选框。
- 步骤11 点击添加 (Add)。

Edit Group Policy				0
Name:* DfltGrpPolicy Description: General Secure	Client Advanced			
Profile Management Profile Client Modules	Download optional client m download from the Firewal configured here.	nodules to the endpoi II Threat Defense of or	nt. Secure Clier nly the modules	nt requests that are +
SSL Settings	Client Module	Profile	Download	
Connection Settings Custom Attributes	ISE Posture	ISEPostureCFG.xml	0	/1

步骤12 点击保存(Save)。

下一步做什么

- 1. 在威胁防御上部署配置。在管理中心菜单栏中,点击部署 (Deploy),然后选择部署 (Deployment)。
- 2. 使用安全客户端建立与威胁防御的 VPN 连接。
- 3. 验证 ISE 安全评估模块配置。

# 验证 ISE 安全评估模块配置

### 在威胁防御上

在威胁防御 CLI 上使用以下命令来验证 ISE 安全评估模块配置:

show run webvpn: 查看安全客户端配置的详细信息。

> show run webypn
webypn
enable Outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.0.03072-
webdeploy-k9.pkg 1 regex "Windows"
anyconnect profiles ISEPostureCFG.xml disk0:/csm/ISEPostureCFG.xml
anyconnect profiles raftd1.xml disk0:/csm/raftd1.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

**show run group-policy** *<ravpn\_group\_policy\_name>*: 查看安全客户端的 RA VPN 组策略的详细信息。

show run group-policy AC-Posture group-policy AC-Posture internal group-policy AC-Posture attributes banner none wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ikev2 ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value iseposture anyconnect profiles value ISEPostureCFG.xml type iseposture anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

show run aaa-server: 查看 ISE 服务器的详细信息。

```
> show run aaa-server
aaa-server ISE protocol radius
authorize-only
interim-accounting-update periodic 24
dynamic-authorization
aaa-server ISE (Inside) host 
key *****
authentication-port 1812
accounting-port 1813
```

### 在终端上

使用安全客户端建立与威胁防御的 VPN 连接,并验证 ISE 安全评估模块的安装。

S Cisco Secure Client				×
R	AnyConnect VPN: Connected to vpn.remoteftd2.com. vpn.remoteftd2.com		Disconnect	
00:00:31			IP	v4
	<b>ISE Posture:</b> Compliant. Network access allowed.			
* 0				1.1
$\mathbf{Q}$ (I)				cisco

相关文档:

- •《Cisco Identity Services Engine 管理员指南》
- •《Cisco Secure Firewall Management Center 管理和设备配置指南》
- •《Cisco Secure 客户端管理指南》

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

<sup>©</sup> 2023 Cisco Systems, Inc. 保留所有权利。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意,翻译版本仅供参考,如有任何不 一致之处,以本内容的英文版本为准。