FMC 6.6.1+ — 升级前后提示

目录

简介 先决条件 要求 使用的组件 FMC升级前的首要任务 选择FMC目标软件版本 验证当前FMC型号和软件版本 规划升级路径 上传升级包 创建FMC备份 检验NTP同步 验证磁盘空间 部署所有挂起的策略更改 运行Firepower软件就绪性检查 FMC升级后的首要任务 部署所有挂起的策略更改 验证是否安装了最新漏洞和指纹数据库 验证Snort规则和轻量安全包的当前版本 验证地理定位更新当前版本 使用计划任务自动执行URL过滤数据库更新 配置定期备份 确保智能许可证已注册 查看变量集的配置 验证云服务实施 URL 过滤 面向网络的 AMP 思科云区域 思科云事件配置 启用SecureX集成 集成SecureX功能区 将连接事件发送到SecureX 集成安全终端(面向终端的AMP) 集成安全恶意软件分析(Threat Grid)

简介

本文档介绍在将思科安全防火墙管理中心(FMC)升级到6.6.1+版之前和之后要完成的验证和配置最 佳实践。

先决条件

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Hardware:思科FMC 1000
- •软件:版本7.0.0(内部版本94)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

FMC升级前的首要任务

选择FMC目标软件版本

查看目<u>标版本的</u>Firepower版本说明并熟悉:

- •兼容性
- •特性和功能
- •已解决的问题
- 已知问题

验证当前FMC型号和软件版本

验证当前FMC型号和软件版本:

- 1. 导航至"帮**助">"关于**"。
- 2. 验证型号和软件版本。

cisco /	FMC About	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	٩	₽	٥	0	admin 🕶
Model Serial Nu Software OS Snort Ver Snort3 V Rule Upd Rule pack Module F LSP Vers Geolocat VDB Vers	umber e Version fersion date Version k Version Pack Version sion tion Update V sion	Cisc W25 7.0. Cisc 2.9. 3.1. 202 260 296 Isp- tersion 202 built	co Firepower Ma P2326001X 0 (build 94) co Firepower Ext 18 (Build 174) 1-09-15-001-v 0 1 rel-20210915-1 1-09-20-002 d 338 (2020-09	nagement Cen tensible Operat rt 1507 2-24 12:58:48	ter 1000 ing System (F)	(-OS) 2.10.1 (br	Page How- Docu What Softv Secu	-level Help Tos mentation on Cisco.com 's New in This Release vare Download re Firewall YouTube	S P A T A	ecure irepow artner sk a Q AC Su bout	Firew ver M Ecos uesti	vall or igratii ysten ion t Case	n Cisc on To n	co.com iol

规划升级路径

根据当前和目标FMC软件版本,可能需要临时升级。在《思科<u>Firepower管理中心升级指南</u>》中 ,查**看升级路径:"Firepower管理中**心"部分并规划升级路径。

上传升级包

要将升级包上传到设备,请完成以下步骤:

- 1. 从软件下载页下载<u>升级</u>包。
- 2. 在FMC中,导航至System > Updates。
- 3. 选择上**传更新**。
- 4. 单击"Upload local software update package(上传本地软件更新包)"单选按钮。
- 5. 单击Browse,然后选择包。
- 6. 单击Upload。

diada cisco	FMC Product Upda	Over	view	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	٩	4	¢	0	admin •
Produ	ct Updates	Rule Update	es	Geolocation Up	dates										
					Curren	tly running sof	tware version:	7.0.0							
			U	pdates											
			Up	icad software upd	ates and patch	es here.									
					Action	Upload loc	al software upd	iate packag	90						
						 Specify so 	ftware update s	ource (FTD	devices only)						
					Package	Browse Cisc	o_Firepower_Mgr	rt_Center_Pat	10h-7.0.0.1-15.sh.REL.1	a.					
								Car	cel Upload						

创建FMC备份

备份是一个重要的灾难恢复步骤,它允许在升级发生灾难性故障时恢复配置。

- 1. 导航至**系统>工具>备份/恢复**。
- 2. 选择"Firepower管理备份"。
- 3. 在Name字段中,输入备份名称。
- 4. 选择应包含在备份中的存储位置和信息。
- 5. 单击"Start Backup(开始备份)"。
- 6. 从"通知">"任务"中,监控备份创建进度。

提示:我们强烈建议备份到安全的远程位置并验证传输是否成功。可以从"备份管理"页配置远 程存储。

dialia cisco	FMC Firepower Manage	ement Backup	Overview	Analysis	Policies	Devices	Object	s AMP	Intelligence	Deploy	۹	4	¢	0	admin •
													Rer	note	Storage
Backup	p Management	Backup Profile	es												
				Cr	eate Ba	ackup									
						N	lame [FMC_Ba	ckup						
					S	torage Loc	ation /	var/sf/bacl	kup/						
					Back U	Jp Configur	ation [
						Back Up Ev	vents								
				В	ack Up Th	reat Intellig Din	ence ector								
					Email	when com	plete								
						Email Add	iress								
					Copy	when com	plete								
							(Cancel	Save As I	lew	Start	Backu	p -		

有关详细信息,请参阅:

- Firepower管理中心配置指南,版本7.0 第章:备份和恢复
- Firepower管理中心配置指南,版本7.0 远程存储管理

检验NTP同步

要成功升级FMC,需要NTP同步。要检查NTP同步,请完成以下步骤:

- 1. 导航至**系统>配置>时间**。
- 2. 验证NTP状态。

注意:状态:"正在使用"表示设备与NTP服务器同步。

Current Setting Current Time	Via NTP (based 2021-09-21 13	a NTP (based on System Configuration Time Synchronization) 021-09-21 13:50										
NTP Server	Status	Authentication	Offset	Last Update								
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)								
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)								
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)								

有关详细信息,请参阅《Firepower管理中心配置指南7.0版—时间和时间同步》。

验证磁盘空间

根据FMC型号和目标版本,确保有足够的可用磁盘空间,否则升级失败。要检查可用的FMC磁盘空间,请完成以下步骤:

1. 导航至System > Health > Monitor。

- 2. 选择FMC。
- 3. 展开菜单并搜索"Disk Usage(磁盘使用)"。
- 4. 磁盘空间要求可在"时间测试"和"磁盘空间要求"中找到。

cisco FMC Monitor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	₽	¢	0	admin 🔻
Monitoring ŵ Home ▲ FMC ~ Devices (0)	•	Health S	O critical	1 warning	0 normal 0) disabled	Q. Filter using device	name					
		A FI O DI / 1	ce MC isk Usage using 44%: 1.50 Local Disk Pr Mount Size / 3.70 /Volume 1.11 MC Access C pes not apply to	a (2.0G Avail) of artition Status Free UsedPer 3.2.0G 1.5G 449 1.966G.70G 7% configuration clo b this platform	3.7G see less cent 6 hanges on dev	ice				S	tp 21,	2021	1:10 PM

部署所有挂起的策略更改

在更新或补丁安装之前,需要将更改部署到传感器。为确保部署所有挂起的更改,请完成以下步骤 :

- 1. 导航至**部署>部署**。
- 2. 选择列表中的所有设备并部署。

警告: Inspect Intercuption列指示流量中断

								Deploy .
T Q. Search using device name	user name, type, group or status							
Device	Modified by	Inspect Interrup	ption Type	Group	Last Deploy Time	Preview	Status	
> FTD66	admin	🚸 Yes	FTD		Sep 13, 2021 1:33 PM	3.	Pending	
	Traffic in	terruption n	eeded		Sensor	with r	ending	deployment

运行Firepower软件就绪性检查

就绪性检查评估Firepower设备对软件升级的准备情况。

要执行软件就绪性检查,请完成以下步骤:

- 1. 导航至**系统>更新**。
- 2. 选择目标版**本旁**的安装图标。
- 3. 选择FMC并单击"检查就绪性"。
- 4. 在弹出窗口中,单击OK。
- 5. 从通知>任务监控就绪性检查流程。

cisco	FMC Upload Upda	Ne Ove	erview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	٩	40	¢	0	admin 🕶
Produ	ct Updates	Rule Upp	iates	Geolocation I	Updates										
Current	y running soft	ware versio	n: 7.0.0												
Selec	cted Update	e Type Version Date Reboot	Cisco Fin 7.0.0.1-1 Tue Jul 6 Yes	epower Mgmt C 5 19:27:03 UTC :	enter Patch 2021					By G	iroup				×
	 Ungrouped ((1 total)			Compatibility	/ Check	Re	adiness Check sults	Readiness Completed	Check		Estin Upgr	nated rade Ti	me	1
	THC-NGFW-FI 0.62.184.21 - C 7.0.0	MC1.proscio lisco Firepow	oud.com er Manage	ement Center 100	00 🕝 Comp	atibility check pa	ssed. Proceed					N	/A		т
									Bac		Check	Read	iness		Install

有关详细信息,请参<u>阅Cisco Firepower管理中心升级指南— Firepower软件就绪性检查</u>。

FMC升级后的首要任务

部署所有挂起的策略更改

每次更新或补丁安装后,都需要立即将更改部署到传感器。为确保部署所有挂起的更改,请完成以 下步骤:

- 1. 导航至部署>部署。
- 2. 选择列表中的所有设备,然后单击Deploy。

警告: Inspect Intercuption列指示流量中断

						Deploy				
C Search using device name,	user name, type, group or status									
Device	Modified by	Inspect Interrupt	tion Type	Group	Last Deploy Time Preview Status					
> _ FTD66	admin	🔸 Yes	FTD		Sep 13, 2021 1:33 PM 🕓 Pending					
Traffic interruption needed Sensor with pending deploym										

验证是否安装了最新漏洞和指纹数据库

要验证当前指纹(VDB)版本,请完成以下步骤:

- 1. 导航至"帮**助">"关于**"。
- 2. 验证VDB版本。

要直接从cisco.com下载VDB更新,需要从FMC访问cisco.com。

1. 导航至系统>更新>产品更新。

- 2. 选择"Download updates"。
- 3. 安装可用的最新版本。
- 4. 之后必须重新部署传感器。

注意:如果FMC没有互联网访问权,则可以直接从software.cisco.com下载VDB软件包。

建议安排任务以执行自动VDB包下载和安装。

作为一种好的做法,请每天检查VDB更新,并在周末将其安装在FMC上。

要每天从www.cisco.com检查VDB,请完成以下步骤:

- 1. 导航至系统>工具>计划。
- 2. 单击Add Task。
- 3. 从作业**类型下**拉列表中,选择下载最新更新。
- 4. 要运行计划任务,请单击循环单选按钮。
- 5. 每天重复该任务,并在凌晨3:00或工作时间外运行。
- 6. 对于**更新项**,选中漏**洞数据库**复选框。

New Task						
Job Type	Download Latest Update	•				
Schedule task to run	Once Recurring					
Start On	September	• 13		* 20	21	▼ Europe/Warsaw
Repeat Every	1	□ ≎	⊖ Hours	Days	○ Weeks	 Months
Run At	3:00	• Am		٠		
Job Name	Downloading Latest VDB					
Update Items	Software Vulnerability Database					
Comment	Daily task to download latest Vulr (VDB) database	verability				
Email Status To	admin@acme.com					Cancel Save

要将最新VDB安装到FMC中,请每周设置定期任务:

- 1. 导航至**系统>工具>计划**。
- 2. 单击Add Task。
- 3. 从作业**类型下**拉列表中,选择安**装最新更新**。
- 4. 要运**行计划任务**,请单击定期单选按钮。
- 5. 每1周重复一次该任务,并在上午5:00或工作时间外运行。
- 6. 对于**更新项**,选中漏**洞数据库**复选框。

New Task					
Job Type	Install Latest Update •				
Schedule task to run	Once Recurring				
Start On	September +	13	* 2021		▼ Europe/Warsaw
Repeat Every	1	Hours	O Days	Weeks	O Months
Run At	5:00 ¥	Am	٣		
Repeat On	Sunday Monday Tuesday	🗌 Wednesday 🛃 Thur	rsday 🗌 Friday 🗌 Sat	unday	
Job Name	Install VDB in FMC				
Update Items	 Software Vulnerability Database 				
Device	fmc70 v				
	Install the latest available VDB into EN	MC			
Comment					
Email Status To	admin@acme.com				
					Cancel Save

有关详细信息,<u>请参阅《Firepower管理中心配置指南7.0版—更新漏洞数据库(VDB)》</u>

验证Snort规则和轻量安全包的当前版本

要验证当前Snort规则(SRU)、轻量安全包(LSP)和地理定位版本,请完成以下步骤:

- 1. 导航至"帮**助">"关于**"。
- 2. 验证规则更新版本和LSP版本。

要直接从www.cisco.com下载SRU和LSP,<u>需</u>要从FMC到www.cisco.com<u>的可</u>达性。

- 1. 导航至System > Updates > Rule Updates。
- 2. 从一次性规则更新/规则导入选项卡中,选择从支持站点下载新规则更新。
- 3. 选择 Import。
- 4. 随后将配置部署到传感器。

注意:如果FMC没有互联网访问权,则SRU和LSP软件包可以直接从software.cisco.com下载 。

入侵规则更新是累积的,建议始终导入最新更新。

要启用Snort规则更新(SRU/LSP)的每周下载和部署,请完成以下步骤:

- 1. 导航至System > Updates > Rule Updates。
- 2. 在Recurring Rule Update Imports**选项卡中**,选中**Enable Recurring Rule Update Imports from the Support Site**复选框。

3. 选择每周导入频率,选择一周中某天和下午晚些时候进行下载和策略部署。

4. Click Save.

Recurring Rule Opdate Imports	
The scheduled rule update has not yet run. Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.	
Enable Recurring Rule Update Imports from the Support Site Import Frequency Weekly I on Monc I at 10 I :00 I PM I Europe/Wars Policy Deploy I Deploy updated policies to targeted devices after rule update completes Cancel Save	BW

有关详细信息,请参阅《Firepower管理中心配置指南7.0版—更新入侵规则》。

验证地理定位更新当前版本

要验证当前地理定位版本,请完成以下步骤:

- 1. 导航至"帮**助">"关于**"。
- 2. 验证地理**定位更新版本**。

要直接从www.cisco.com下载地理定<u>位更</u>新,需要从FMC到www.cisco.com<u>的可</u>达性。

- 1. 导航至System > Updates > Geolocation Updates。
- 2. 从One-Time Geolocation Update(一次性地理定位更新)选项卡中,选择Download and install geolocation update from the Support Site。
- 3. 单击 Import。

注意:如果FMC没有互联网访问权,则Geolocation Updates软件包可以直接从 software.cisco.com下载。

要打开自动地理定位更新,请完成以下步骤:

- 1. 导航至System > Updates > Geolocation Updates。
- 2. 在Recurring Geolocation Updates部分,选中Enable Recurring Weekly Updates from **the Support Site复选框。**
- 3. 选择导入频率为每周,选择星期一午夜。
- 4. Click Save.

Recurring Geolocation Updates						
Enable Recurring Weekly Updates from the Support Site	\checkmark					
Update Start Time	Monday	•	12:00 🔻	AM	*	Europe/Warsaw
					Cance	el Save

有关详细信息,<u>请参阅《Firepower管理中心配置指南7.0版—更新地理定位数据库(GeoDB)》</u>。

使用计划任务自动执行URL过滤数据库更新

为确保URL过滤的威胁数据是最新的,系统必须从思科综合安全情报(CSI)云获取数据更新。要自动 执行此过程,请执行以下步骤:

- 1. 导航至**系统>工具>计划**。
- 2. 单击Add Task。
- 3. 从作业类型下拉列表中,选择更新URL过滤数据库。
- 4. 要运**行计划任务**,请单击循环单选按钮。
- 5. 每周重复该任务,并在周日或下班时间的晚上8:00运行该任务。
- 6. Click Save.

New Task					
Job Type	Update URL Filtering Database 🔹				
Schedule task to run	Once Recurring				
Start On	September •	13	* 2021		• Europe/Warsaw
Repeat Every	1	C Hours	O Days	Weeks	 Months
Run At	8:00 *	Pm	*		
Repeat On	Sunday 🗌 Monday 🗌 Tuesday 🗌	Wednesday 🗌 Thursda	r 🗌 Friday 🗌 Satur	day	
Job Name	Update URL Filtering Database				
Comment	This task downloads the latest URL Fi Database	Itering			
Email Status To	admin@acme.com				Cancel Save

有关详细信息,请<u>参阅《Firepower管理中心配置指南,版本7.0 — 使用计划任务自动执行URL过滤</u> 更新》。

配置定期备份

作为灾难恢复计划的一部分,建议执行定期备份。

- 1. 确保您处于全局域中。
- 2. 创建FMC备份配置文件。有关详细信息,请参阅创建FMC备份部分。
- 3. 导航至**系统>工具>计划**。
- 4. 单击Add Task。
- 5. 从作业**类型下**拉列表中,选择备**份。**
- 6. 要运行计划任务,请单击循环单选按钮。
 必须调整备份频率以满足组织的需求。我们建议在维护时段或其他低使用时间创建备份。
- 7. 对于**备份类**型,单击管理中心单选按钮。
- 8. 从Backup Profile下拉列表中,选择Backup Profile。
- 9. Click Save.

New Task		
Job Type	Backup +	
Schedule task to run	Once Recurring	
Start On	September • 24 • 2021 • U	UTC
Repeat Every	1 Hours Days 🖲 Weeks O Months	
Run At	11:00 v Pm v	
Repeat On	🗌 Sunday 📄 Monday 📄 Tuesday 📄 Wednesday 📄 Thursday 📄 Friday 🛃 Saturday	
Job Name	FMC_weekly_backup	
Backup Type	Management Center O Device	
Backup Profile	Backup_FMC +	
	This tasks creates EMC weekly backup	
Comment		
Email Status To	admin@acme.com	
	Cancel Save	e

有关详细信息,请参阅《Firepower管理中心配置指南7.0版 — 第章》:备份和恢复.

确保智能许可证已注册

要向思科智能软件管理器注册思科防火墙管理中心,请完成以下步骤:

- 1. 在https://software.cisco.com中, 导航至Smart Software Manager > Manage licenses。
- 2. 导航至"**库存">"**常规"选项卡并创**建新令牌**。
- 3. 在FMC UI中,导航至**System > Licenses > Smart Licenses**。
- 4. 单击"Register(注册)"。
- 5. 插入在思科智能软件许可门户中生成的令牌。
- 6. 确保启用了思科成功网络。
- 7. 单击"**应用更改**"。
- 8. 验证智能许可证状态。

Smart Licensing Product Registration	0
Product Instance Registration Token:	
MGI0ZGJhNTEtOTIxYy00ZGM2LWJjMTctNWE1ZTY5YWUxZGExLTE2NjQwMTUz%0AM DQ00TZ8bTQxTWJDbmJJWIVLd3hQMGs4bytHdU4wVzNvRWRZM1pjbkJ4Nkcr%0AM	1
If you do not have your ID token, you may copy it from your Smart Software manager under the assigned virtual account. Cisco Smart Software Manager	
The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.	
Cisco Success Network	
The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused avail features so that you can maximize the value of the product in your network. Check out th sample data that will be sent to Cisco.	able
Enable Cisco Success Network	
Cisco Support Diagnostics	
The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your de during the course of a TAC case. Additionally, Cisco will periodically collect confouration	/ices
Internet connection is required. Cancel Apply Change	es

有关详细信息,请参阅《Firepower管理中心配置指南7.0版 — 注册智能许可证》。

查看变量集的配置

确保HOME_NET变量仅包含组织中的内部网络/子网。不正确的变量集定义会对防火墙的性能产生 负面影响。

- 1. 导航至对**象>变量集**。
- 2. 编辑入侵策略使用的变量集。允许每个入侵策略使用不同设置设置一个变量集。
- 3. 根据您的环境调整变量,然后单击"保存"。

其他关注的变量是DNS_SERVERS或HTTP_SERVERS。

有关详细信息,请<u>参阅《Firepower管理中心配置指南7.0版—变量集》</u>。

验证云服务实施

为了利用不同的云服务,导航至System > Integration > Cloud Services。

URL 过滤

- 1. 启用URL过滤并允许自动更新,打开查询未知URL的思科云。
 更频繁的缓存URL过期要求对云进行更多查询,从而导致网络加载更慢。
- 2. 保存更改。

提示:对于缓存URL过期,请保留默认**Never**。如果需要更严格的Web重新分类,可以相应修 改此设置。

面向网络的 AMP

- 4. 确保两个设置都已打开: 启用自动本地恶意软件检测更新和与思科共享来自恶意软件事件的 URI。
- 2. 在FMC 6.6.X中,禁用传统端口32137用于面向网络的AMP,因此使用的TCP端口是443。
- 3. 保存更改。

注意:此设置在FMC 7.0+中不再可用,端口始终为443。

思科云区域

- 五区域需要与SecureX组织区域匹配。如果未创建SecureX组织,请选择离FMC安装更近的区域: APJ地区、欧盟地区或美国地区。
- 2. 保存更改。

思科云事件配置

用于FMC 6.6.x

- 4. 确保以下三种选项:选择将高优先级连接事件发送到云、将文件和恶意软件事件发送到云以及 将入侵事件发送到云。
- 2. 保存更改。



用于FMC 7.0+

- 1. 确保同时选择以下两个选项:将入侵事件发送到云,并将文件和恶意软件事件发送到云。
- 2. 对于连接事件的类型,如果安全分析和日志记录解决方案正在使用中,请选择All。对于 SecureX,请仅选择"安**全事件"**。

3. 保存更改。

Cisco Clo	oud Event Conf	figuration	
C Sen	d Intrusion Events to	the cloud	
Send Conn	d File and Malware E	ivents to the clou	d
	Council Durate	A11 🔿	
None	Security Events	All 😈	

启用SecureX集成

SecureX集成可即时了解整个思科安全产品的威胁形势。要连接SecureX并启用功能区,请执行以 下步骤:

集成SecureX功能区

注意:此选项适用于FMC版本7.0+。

- 1. 登录SecureX并创建API客户端: 在客户端名称字段中,输入FMC的描述性名称。例如 ,FMC 7.0 API客户端。单击Oauth Code Clients选项卡。在"客户端预设"下拉列表中,选择功 能区。它选择范围:案例本, Enchred:read,全球英特尔:read, Inspect:read,通知,轨道 ,私有英特尔,简档,响应,遥测:write。添加FMC中显示的两个重定向URL: URL 重定向: <FMC URL>/securex/oauth/callback
- 第二个重定向URL:<FMC_URL>/securex/testcallback

1. 在可用性下拉列表中,选择组织。单击Add New Client。

Add New Client w	ith 10 scopes ×
Client Name*	
FMC 7.0 API Client	
Client Preset	
Ribbon	× ×
API Clients OAut	h Code Clients
Scopes*	Select All
Search	٩
Response	configured modules
SSE	SSE Integration. Manage your Devices.
Telemetry:write	collect application data for analytics - Write Only
Users	Manage users of your organisation
U Webbook	Manage your Webbooks
	incluge year treatenie
Redirect URL*	leasurey leasth leallhack
Padiract UPI * Dalata	securex/oauth/caliback
https://10.62.184.21/	eanuray/testcallback
Add another Redirect I	IDI
Availability*	
Organization	~
Description	
Add description	
Add description	
Add description	

2.从FMC导航至System > SecureX。

3.打开右上角的切换,确认显示的区域与SecureX组织匹配。

4.复制客户端ID和客户端密码并粘贴到FMC中。

5.选择"测**试配置"**。

6.登录SecureX以授权API客户端。

7.保存更改并刷新浏览器,以便查看底部显示的功能区。

8.展开功能区,然后选择"获**取SecureX"**。如果出现提示,请输入SecureX凭证。

9. SecureX功能区现在对您的FMC用户完全正常工作。

SecureX Configuration
This feature allows FMC to integrate with other SecureX services via SecureX ribbon.
Follow these steps to configure SecureX
 Confirm your cloud region Currently selected region: api-sse.cisco.com To change the cloud region, go to System / Integration / Cloud Services.
2. Create a SecureX API client [] Copy and paste the URL below into the "Redirect URL" field: Copy to Clipboard https://10.62.184.21/securex/oauth/callback Then click on "Add another Redirect URL" and copy and paste the URL below: Copied https://10.62.184.21/securex/testcallback
3. Enter the Client ID and password
Client ID client-2b2a954c-b9e4-423(
Client Password
Show Password
Test Configuration Save

5YVPsGdzrkX8q8q0yYI-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

注意:如果任何其他FMC用户需要访问功能区,则该用户需要使用SecureX凭证登录功能区。

将连接事件发送到SecureX

- 1. 在FMC中,导航至**System > Integration > Cloud Services**,并确保**Cisco Cloud Event Configuration**发送入侵、文件和恶意软件事件,如**Turn on Cloud Services**部分所述。
- 2. 确保FMC已注册到智能许可证,如注册智**能许可证部分所**述。

- 3. 记下FMC中"系统">"许可证">"智能许可证"下显示的"已分配虚拟帐户名称"。
- 4. 将FMC注册到SecureX: 在SecureX中,导航至管理>设备。选择Manage Devices。确保浏览器允许弹出窗口。登录安全服务交换(SSE)。导航至"工具"菜单>"链接智能/虚拟帐户"。选择"链接更多帐户"。选择分配给FMC的虚拟帐户(第3步)。选择链接智能/虚拟帐户。

Link	Smart/Virtual Accounts • ×
	Select accounts to be linked to
0	Your Smart or Virtual Account can be connected to one SecureX tenant at a time. If you don't see it available here, check whether your team has already connected it to another SecureX tenant.
	Smart/Virtual Accounts
	Cancel Link Smart/Virtual Accounts

- •确保FMC设备列在设备中。
- •导航至云**服务选**项卡,打开Cisco SecureX威胁响应和事件功能。
- •选择"事件处理"功能旁边的"其他服务设置"(齿轮图标)。
- 在"常规"选项卡中,选择与Talos共享事件数据。
- 在"自动升级事件"选项卡的"按事件类型"部分,选择所有可用事件类型并保存。
- 5.在主SecureX门户中,导航至"集成模块">"Firepower",然后添加"Firepower"集成模块。

6.创建新控制面板。

7.添加Firepower相关磁贴。

集成安全终端(面向终端的AMP)

要启用与Firepower部署的安全终端(面向终端的AMP)集成,请执行以下步骤:

- 1. 导航至AMP > AMP Management。
- 2. 选择**添加AMP云连接**。
- 3. 选择云并**注册**。

注意:状态Enabled表示已建立与云的连接。

集成 安全恶意软件分析(Threat Grid)

默认情况下,Firepower管理中心可以连接到公共Cisco Threat Grid云,以便提交文件和检索报告。 无法删除此连接。不过,建议选择最接近您的部署云的:

- 1. 导航至AMP > Dynamic Analysis Connections。
- 2. 单击"操作"部分中的**编辑**(铅笔图标)。
- 3. 选择正确的云名称。
- 4. 要关联Threat Grid帐户以获取详细报告和高级沙盒功能,请单击"关**联"**图标。

有关详细信息,请<u>参阅《Firepower管理中心配置指南7.0版 — 启用对公共云中动态分析结果的访问</u> <u>》</u>。

有关本地线程网格设备集成,请参阅<u>《Firepower管理中心配置指南7.0版—现场动态分析设备</u> (<u>Cisco Threat Grid</u>)》。