FMC 6.6.1+ — 升级前后提示

目录

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

要求

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

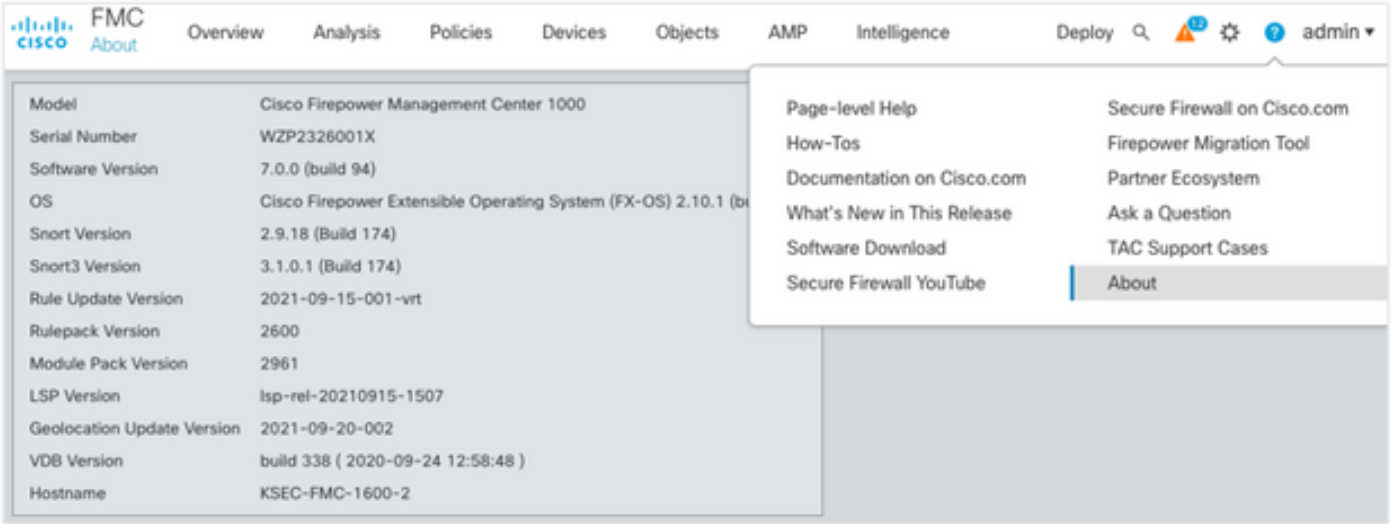
查看目标版本的Firepower版本说明并熟悉：

- 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。



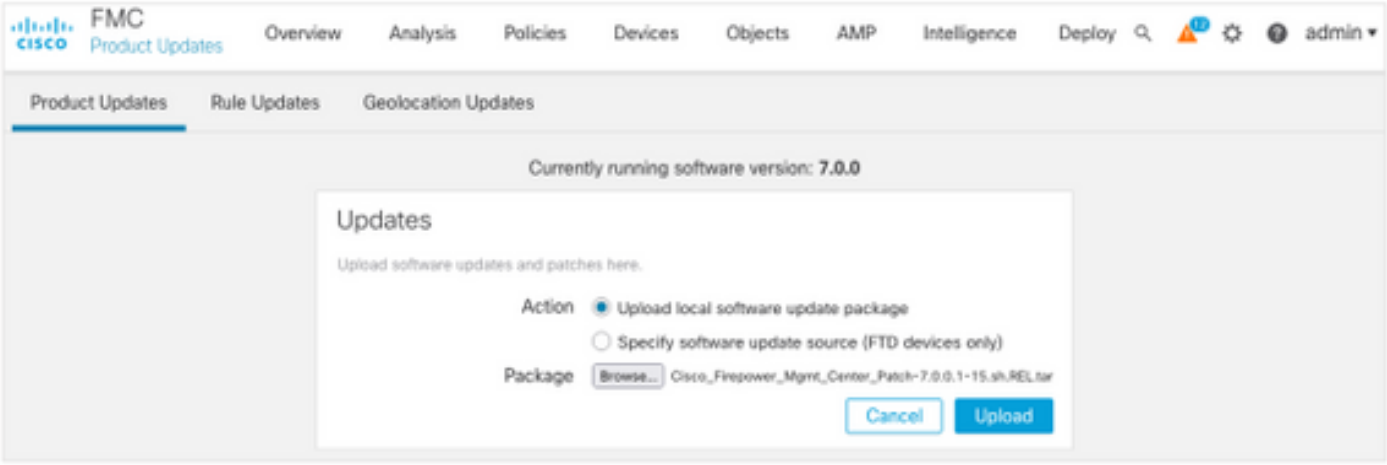
规划升级路径

根据当前和目标FMC软件版本，可能需要临时升级。在《思科Firepower管理中心升级指南》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. 从软件下载页下载升级包。
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**。

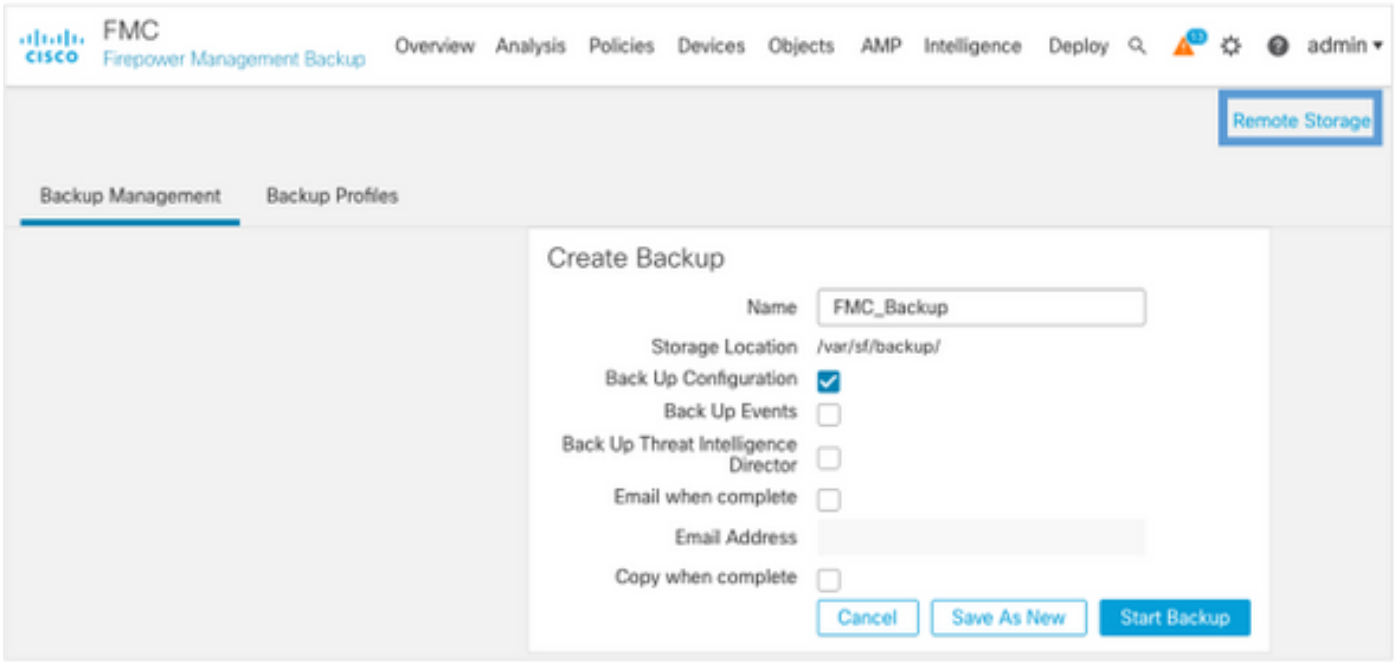


创建FMC备份

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。



有关详细信息，请参阅:

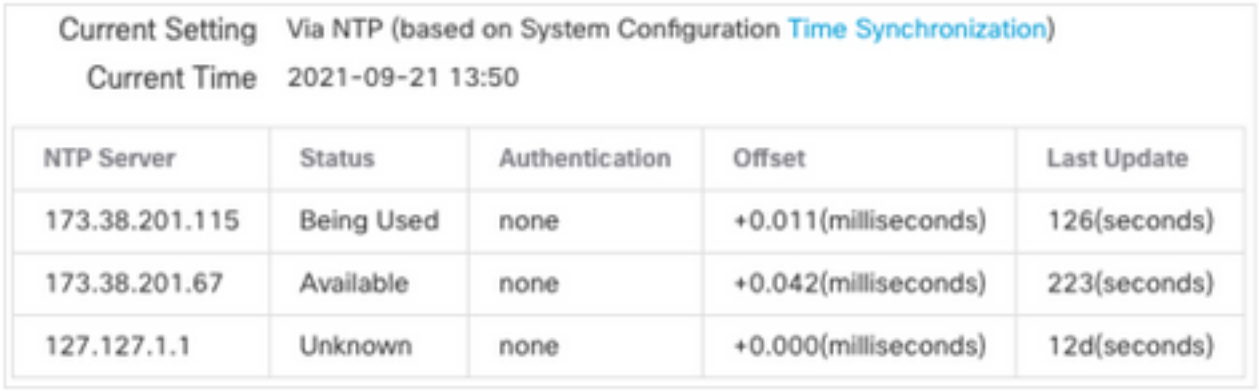
- Firepower管理中心配置指南，版本7.0 — 第章：备份和恢复
- Firepower管理中心配置指南，版本7.0 — 远程存储管理

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。



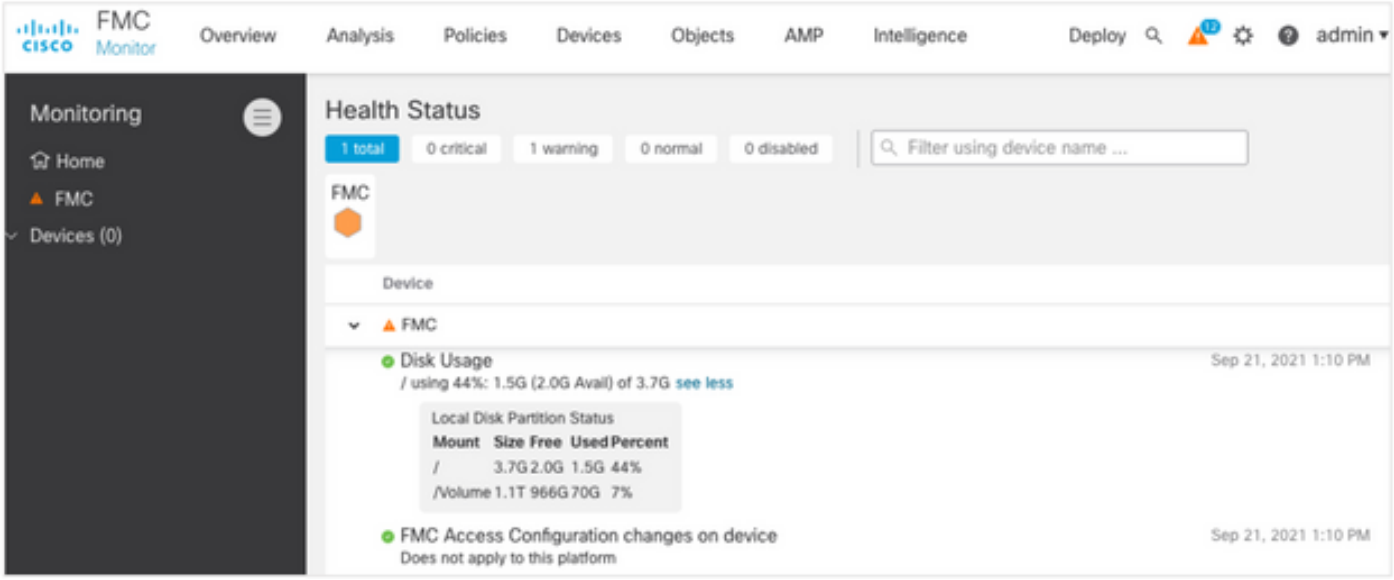
有关详细信息，请参阅《Firepower管理中心配置指南7.0版 — 时间和时间同步》。

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。

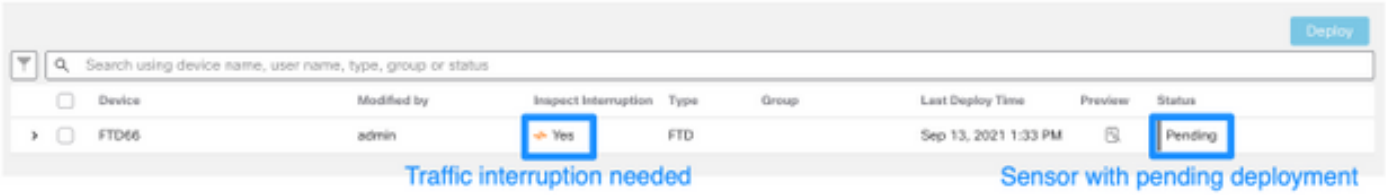


部署所有挂起的策略更改

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

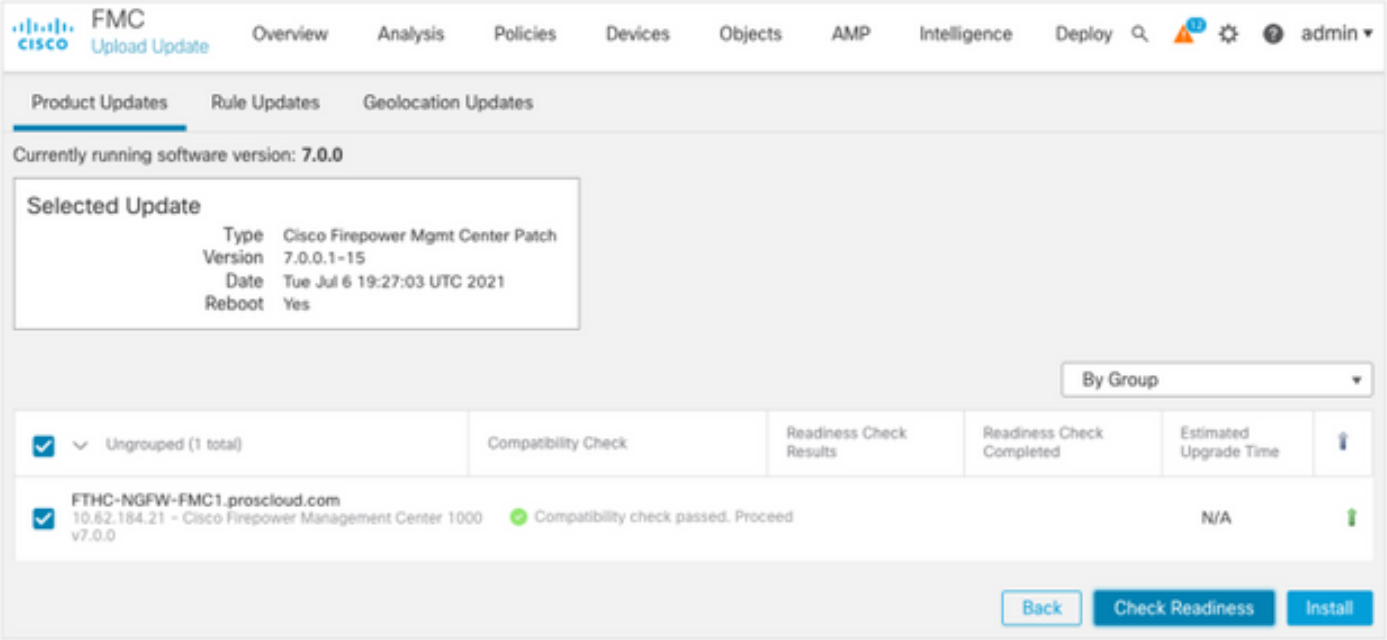


运行Firepower软件就绪性检查

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**。



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

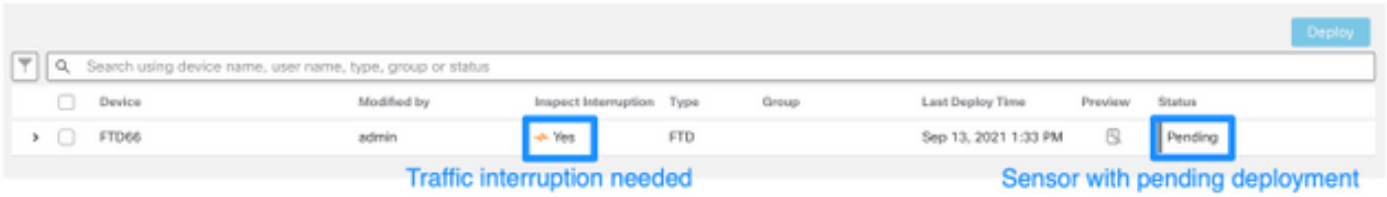
FMC升级后的首要任务

部署所有挂起的策略更改

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



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。

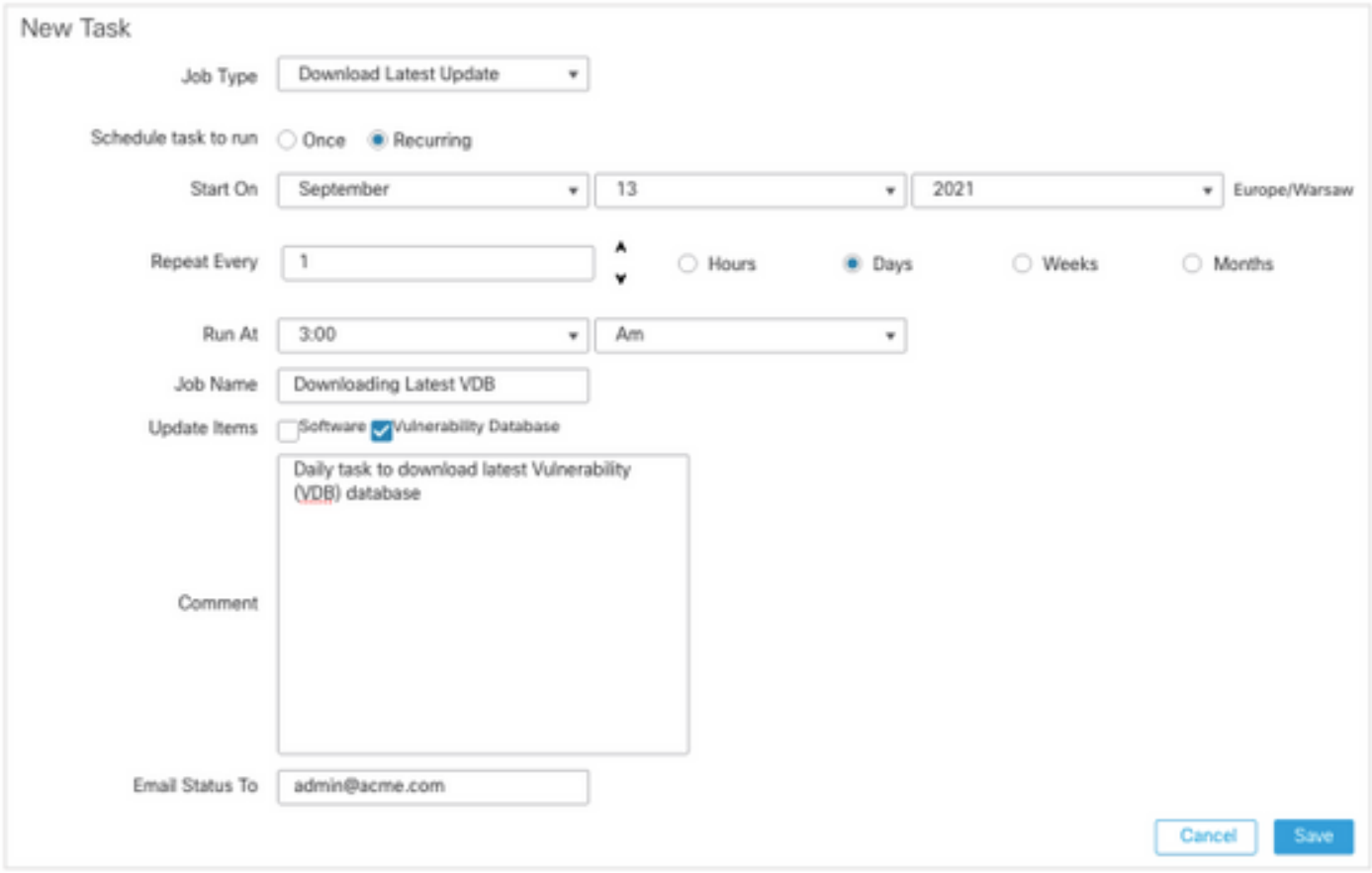
注意：如果FMC没有互联网访问权，则可以直接从software.cisco.com下载VDB软件包。

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。

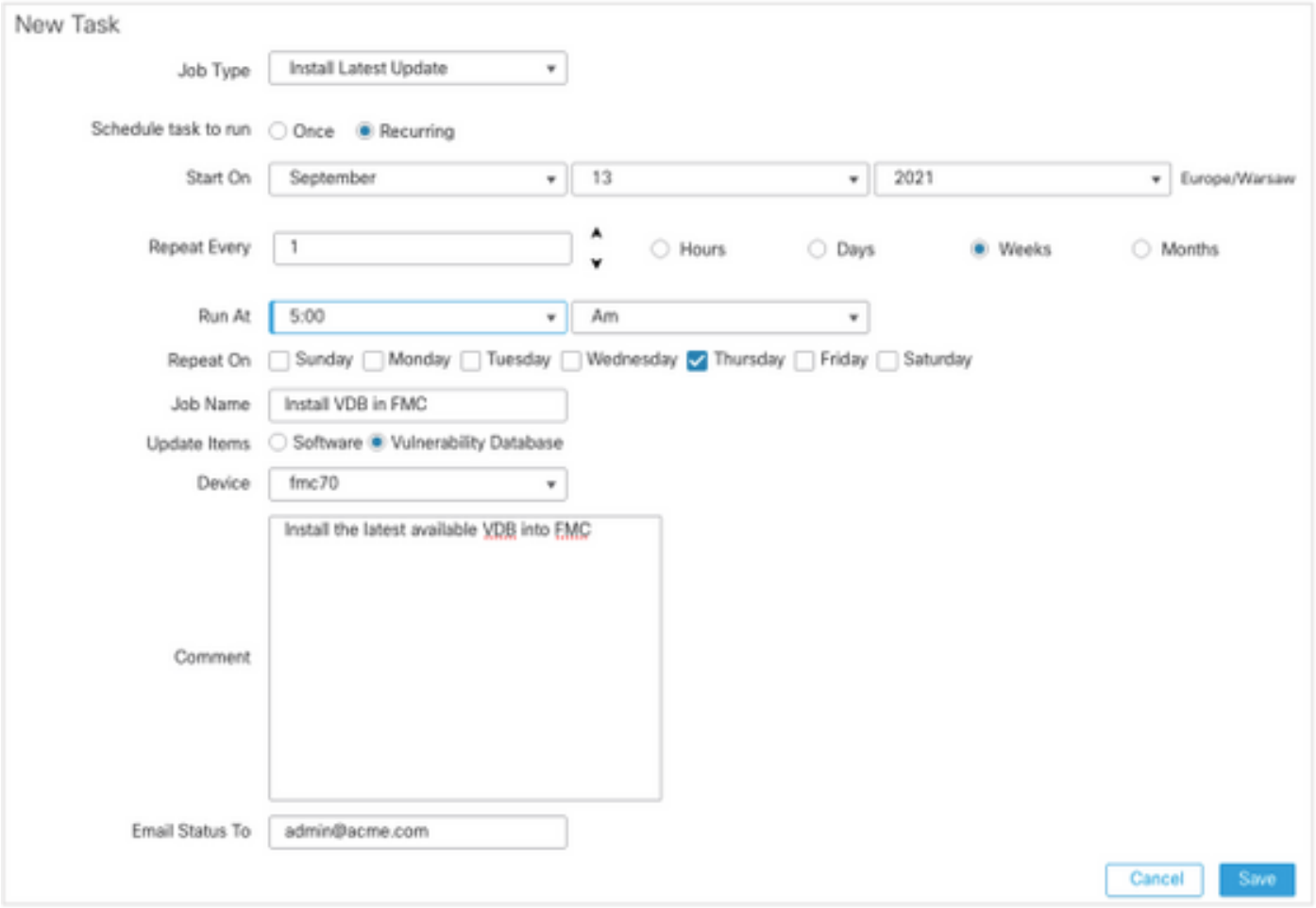
要每天从www.cisco.com检查VDB，请完成以下步骤：

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。



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。



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

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，需要从FMC到www.cisco.com的可达性。

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。

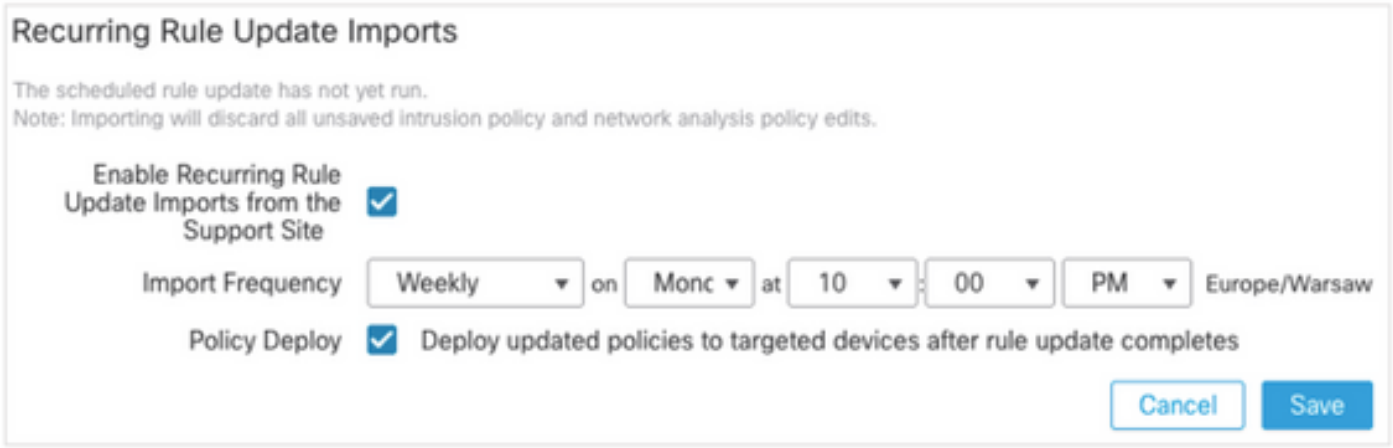
注意：如果FMC没有互联网访问权，则SRU和LSP软件包可以直接从software.cisco.com下载。

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**.



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。

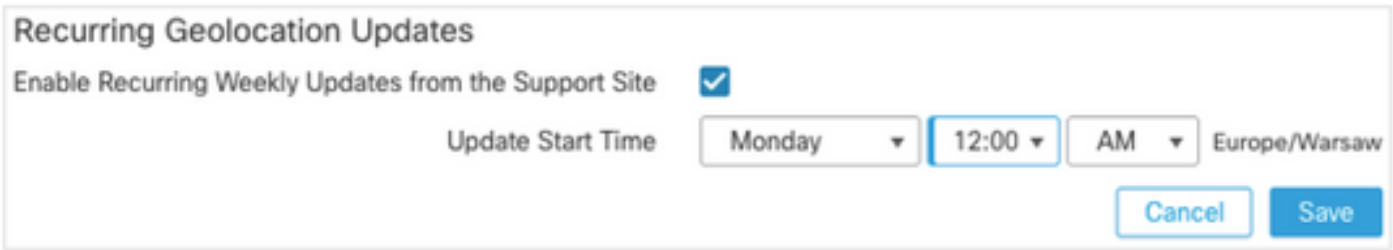
要直接从www.cisco.com下载地理定位更新，需要从FMC到www.cisco.com的可达性。

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**.

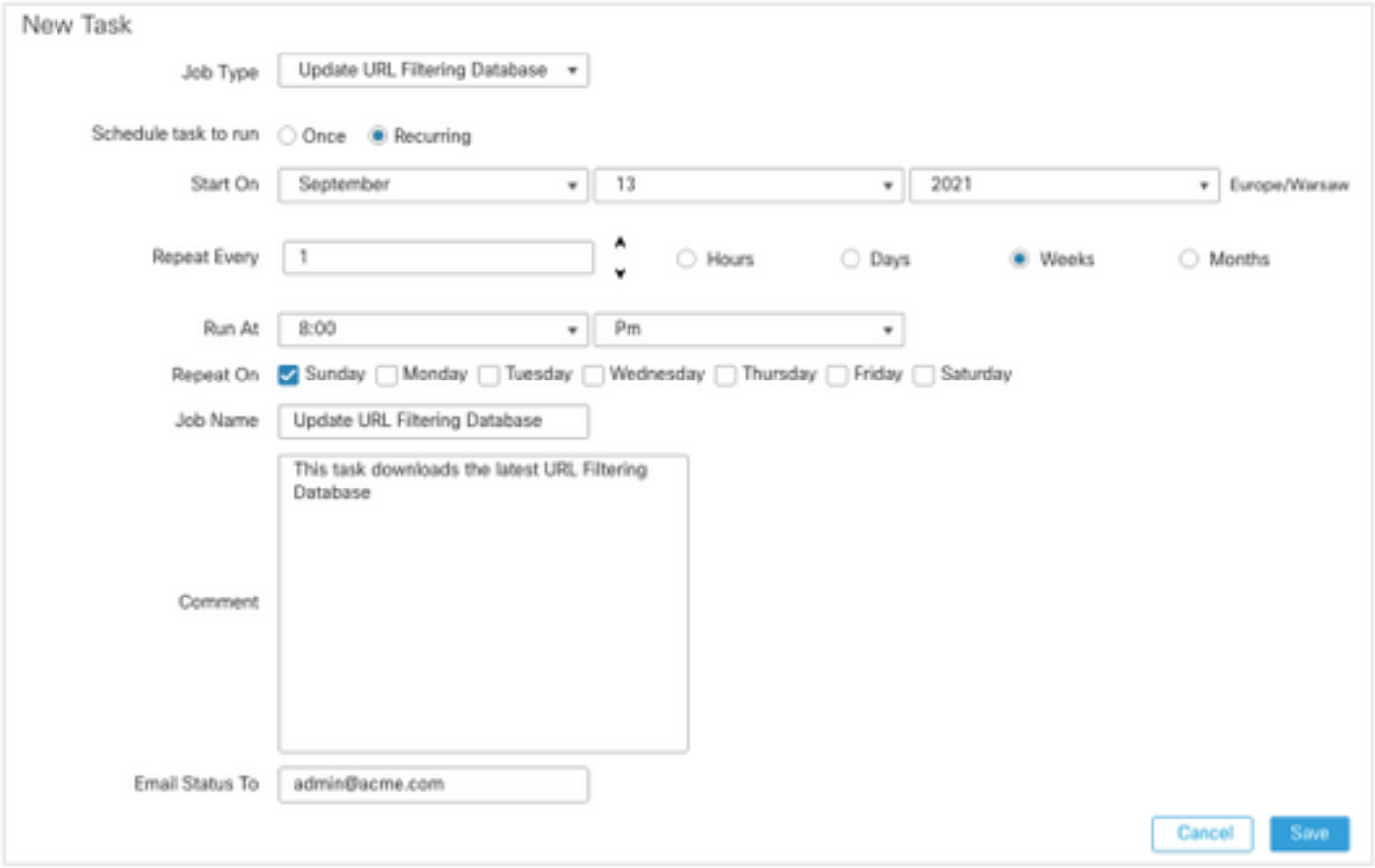


有关详细信息，请参阅《Firepower管理中心配置指南7.0版 — 更新地理定位数据库(GeoDB)》。

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**.

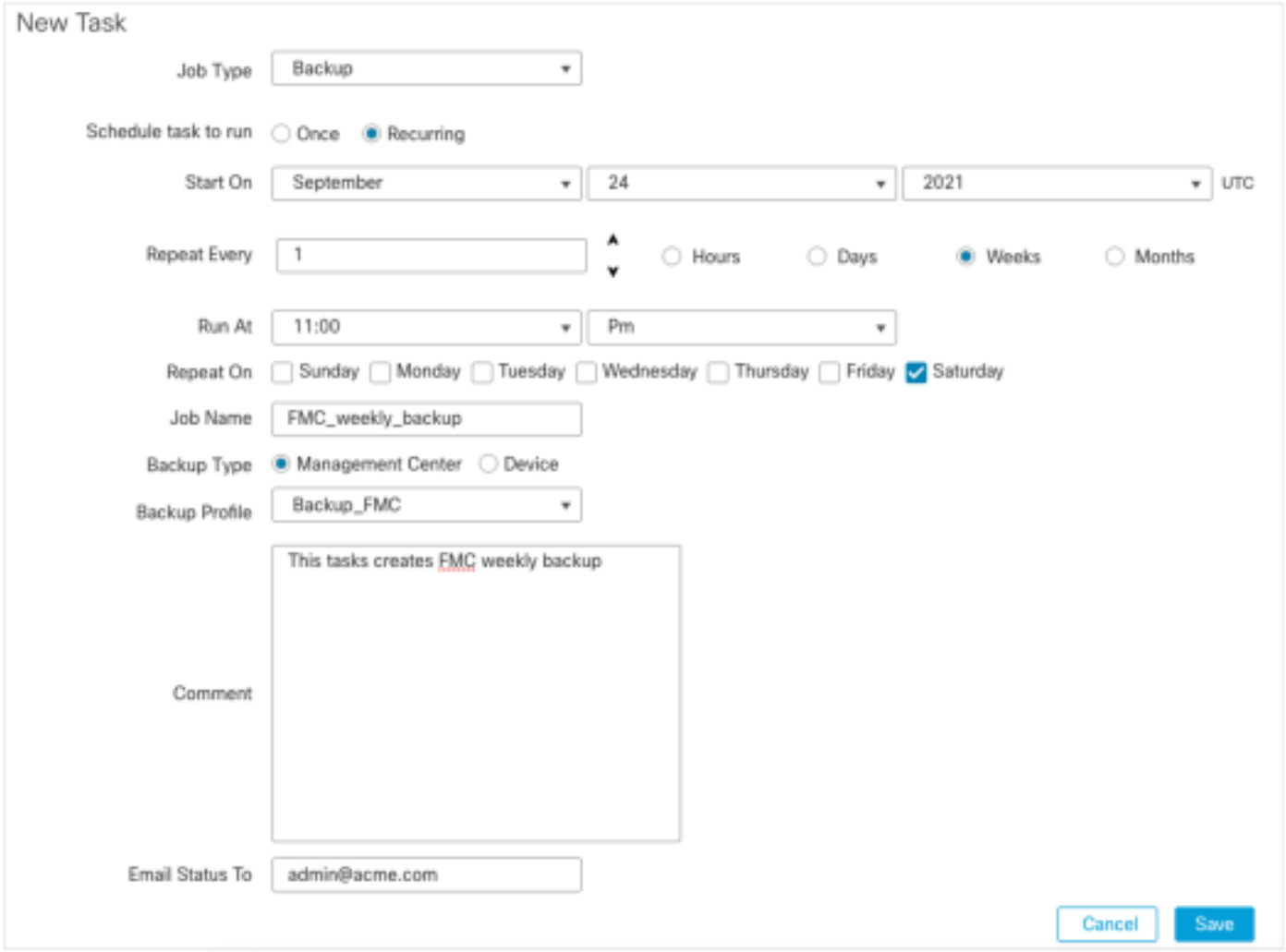


有关详细信息，请参阅《Firepower管理中心配置指南，版本7.0 — 使用计划任务自动执行URL过滤更新》。

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**.

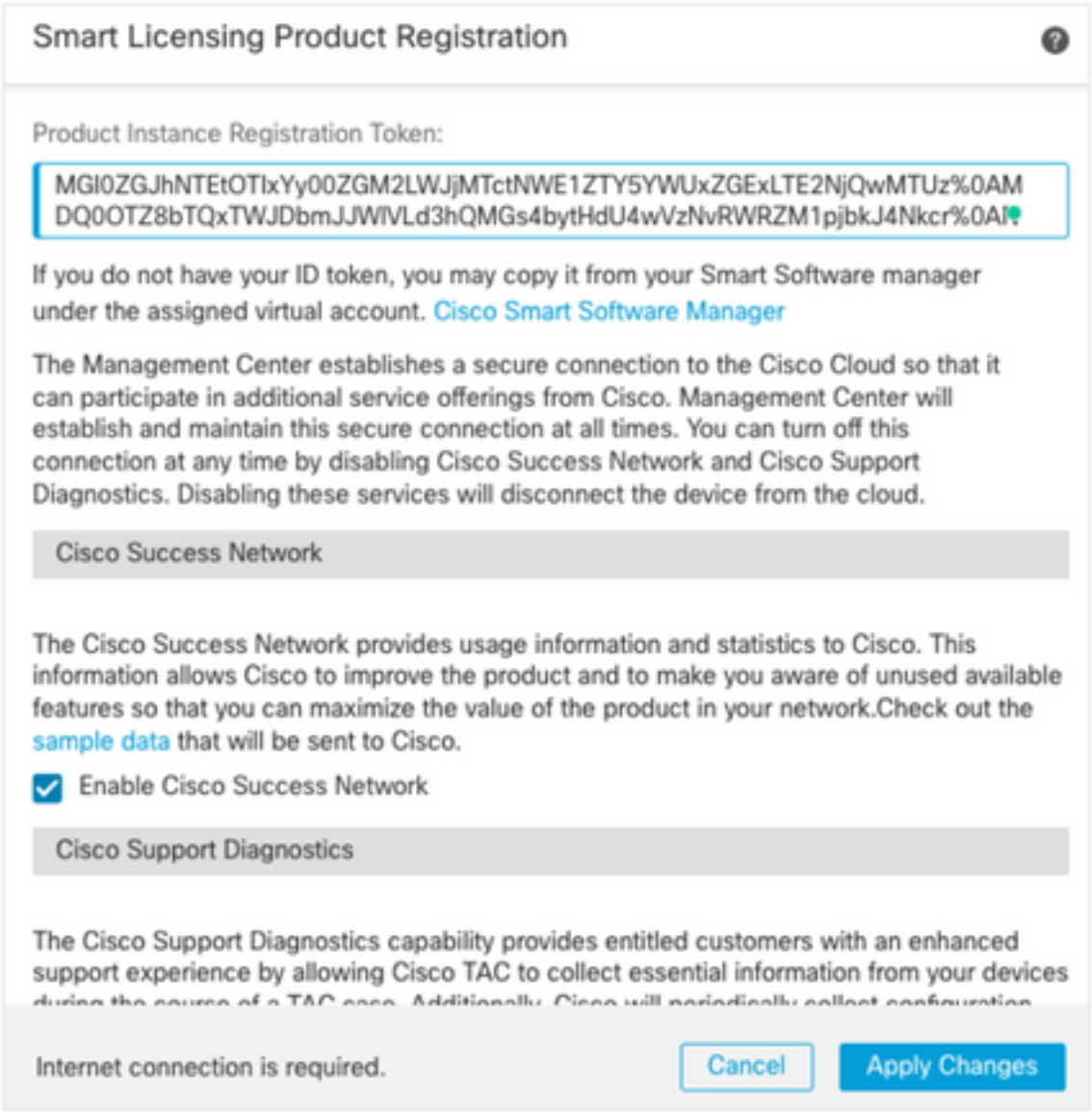


有关详细信息，请参阅《Firepower管理中心配置指南7.0版 — 第章》：备份和恢复.

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。



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，请参阅《Firepower管理中心配置指南7.0版 — 变量集》。

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

1. 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。

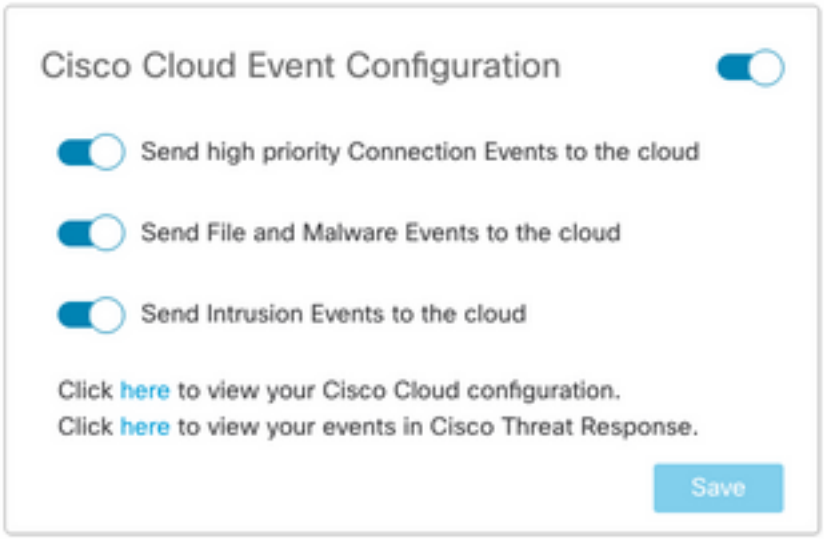
思科云区域

1. 云区域需要与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

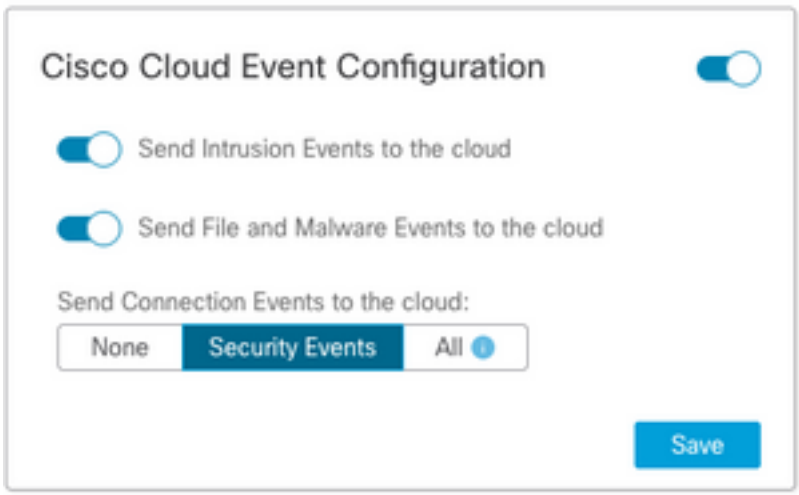
1. 确保以下三种选项：**选择将高优先级连接事件发送到云**、将**文件和恶意软件事件发送到云**以及将**入侵事件发送到**云。
2. **保存更改。**



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。**



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

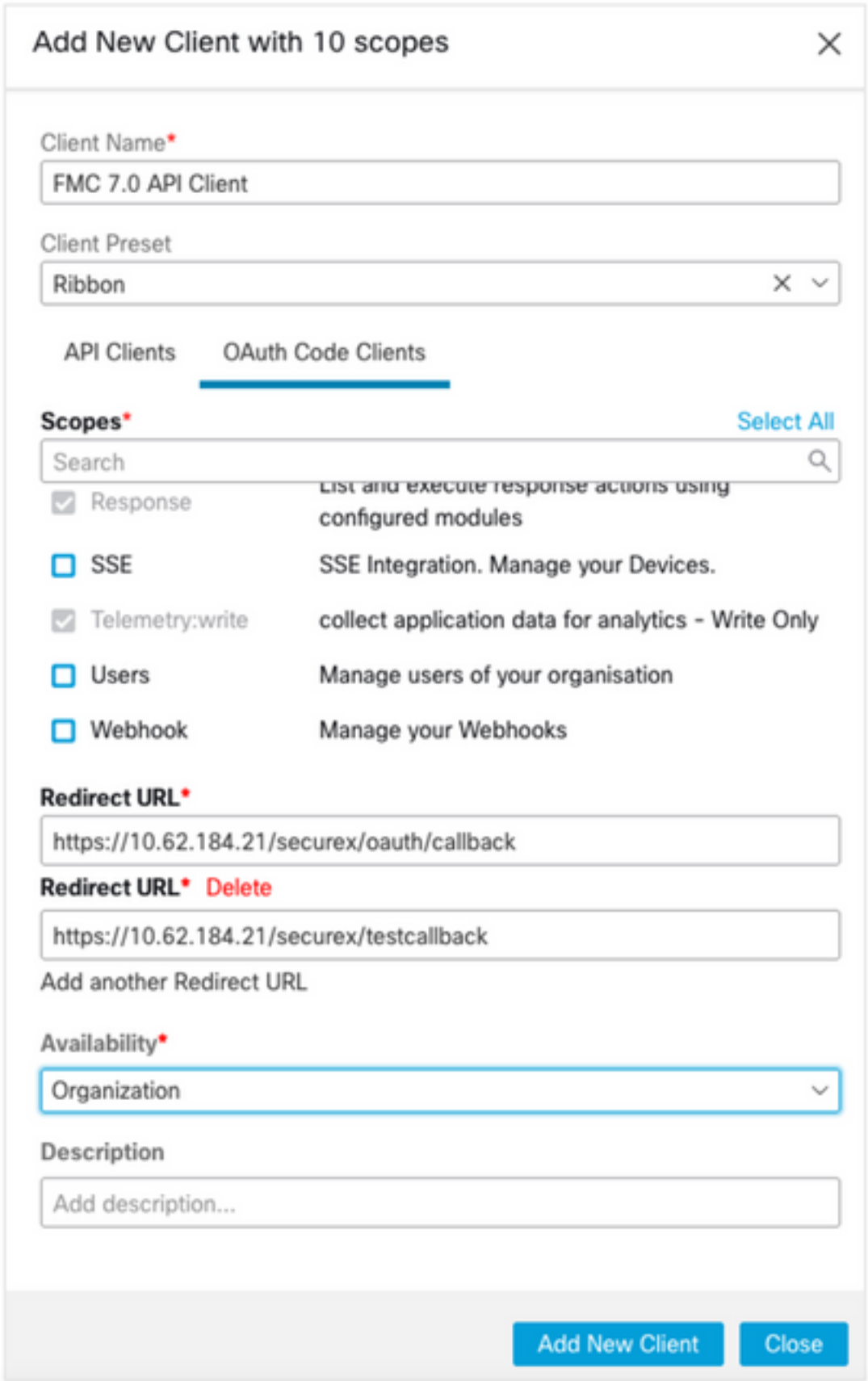
注意：此选项适用于FMC版本7.0+。

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**。



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。

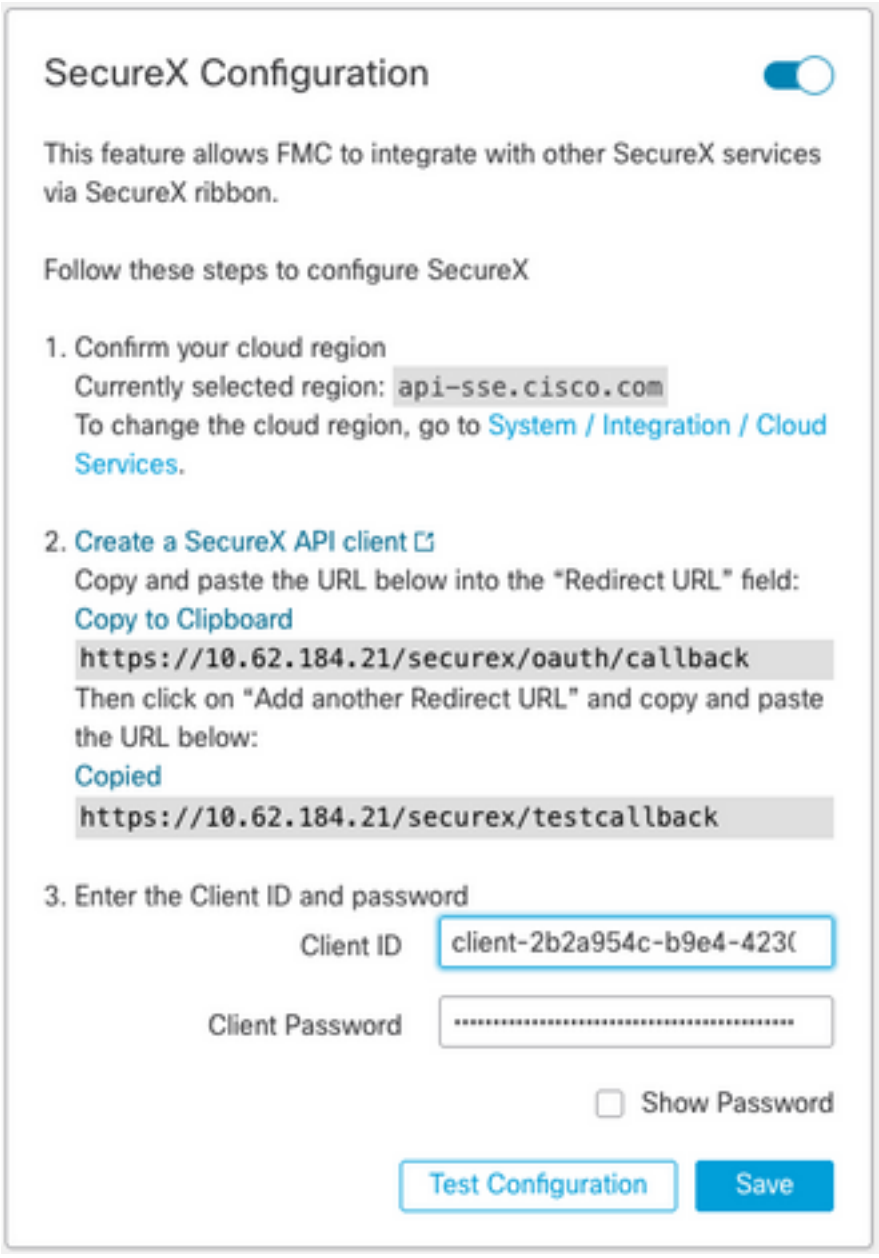
5.选择“测**试配置**”。

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。



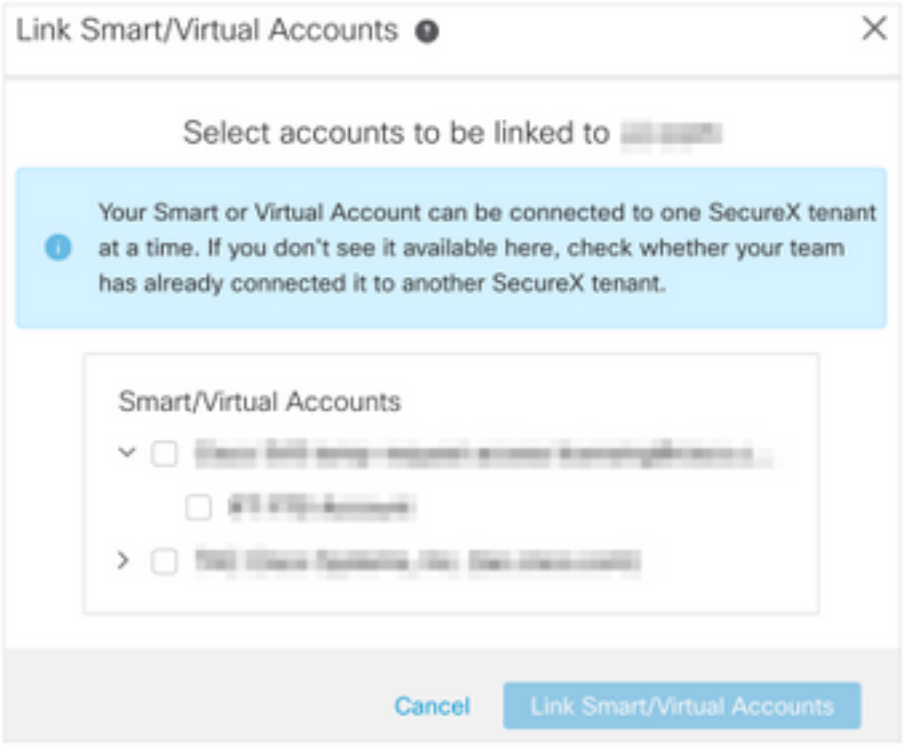
5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

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。**



- 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》。

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