# 计划

以下主题介绍如何安排任务：



# 关于任务安排

可安排各种任务在指定时间运行一次或反复运行。

任务在后端UTC中安排的，这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于任务是以UTC为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季中的一个小时开始。

某些任务由初始设置过程自动安排或执行：

- 下载并安装最新 VDB 的一次性任务。
- 用于下载最新可用修补程序和 VDB的每周计划任务，其中包括最新 VDB。
- 执行 防火墙管理中心 本地存储的仅配置备份的每周计划任务。

您应查看每周任务并在必要时进行调整。或者，安排新的周期性任务以实际更新 VDB 和/或软件，并部署配置。

**重要事项** 我们强烈建议您查看计划任务，确保这些任务在您预期的时间执行。有些任务（例如，那些涉及自动化软件更新的任务，或者要求将更新推送到托管设备的任务）可能会显著增加低带宽网络的负载。应安排此类任务在网络使用量较低的时段运行。其他任务（例如部署配置）可能会导致流量中断。您应在维护窗口期间安排此类任务。

# 任务安排的要求和前提条件

### 型号支持

任意。

### 支持的域

任意

### 用户角色

- 管理员
- 维护用户

# 配置周期性任务

使用相同流程为所有类型的任务设置周期性任务的频率。

请注意，Web 界面上大多数页面中显示的时间为本地时间，由您在本地配置中指定的时区决定。而且，防火墙管理中心将在适当时自动调整本地显示的夏令时 (DST) 时间。但是，从 DST 到标准时以及从标准时到 DST 跨越转换日期的周期性任务不会调整转换。即，如果创建的某项任务安排在标准时上午 2:00 执行，则它将于 DST 上午 3:00 运行。同理，如果创建的某项任务安排在 DST 上午 2:00 执行，则它将于标准时上午 1:00 运行。

### 过程

**步骤 1** 选择 **系统 (⚙) > 工具 > 计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从**作业类型 (Job Type)** 列表中，选择要安排的任务类型。

**步骤 4** 点击 **安排要运行的任务** 选项旁边的 **周期性** 。

**步骤 5** 在 **Start On** 字段中，指定想要开始周期性任务的日期。

**步骤 6** 在 **Repeat Every** 字段中，指定想要任务重复的频率。

可键入数字，或者点击 **向上**（▲） 和 **向下**（▼） 指定时间间隔。例如，键入 2 并点击 **天数** 让任务每两天运行一次。

**步骤 7** 在 **Run At** 字段中，指定想要开始周期性任务的时间。

**步骤 8** 如需每周或每月运行一次任务，请在**重复日期 (Repeat On)** 字段中选择要运行任务的天数。

**步骤 9** 为作业命名。

**步骤 10** 为正在创建的任务类型选择其余选项：

- “备份”(Backup) - 安排备份作业，如 计划 防火墙管理中心 备份 ，第 3 页 中所述。
- “下载 CRL”(Download CRL) - 安排证书撤销列表下载，如配置证书撤销列表下载 ，第 5 页 中所述。
- “部署策略”(Deploy Policies) - 安排策略部署，如自动执行策略部署 ，第 6 页中所述。
- “Nmap 扫描”(Nmap Scan) - 安排 Nmap 扫描，如安排 Nmap 扫描 ，第 7 页中所述。
- “报告”(Report) - 安排报告生成，如 自动执行报告生成 ，第 8 页中所述 。
- Cisco 建议规则 - 安排自动更新，如 自动生成 思科 建议 ，第 10 页中所述。
- “下载最新更新”(Download Latest Update) - 安排软件或 VDB 更新下载，如自动执行软件下载 ，第 11 页或自动执行 VDB 更新下载 ，第 14 页中所述。
- “安装最新更新” - 安排在 防火墙管理中心 或托管设备上安装软件或 VDB 更新，如 自动执行软件安装 ，第 13 页 或 自动执行 VDB 更新安装 ，第 14 页中所述
- “推送最新更新”(Push Latest Update) - 安排将软件更新推送到托管设备，如自动执行软件推送 ，第 12 页中所述。
- “更新 URL 过滤数据库”(Update URL Filtering Database) - 安排 URL 过滤数据的自动更新，如使用已安排任务自动执行 URL 过滤更新 ，第 15 页中所述 。

**步骤 11** 点击**保存**。

# 计划的备份

您可以在 Cisco Secure Firewall Management Center 上使用调度程序自动执行自己的备份。您还可以从防火墙管理中心安排远程设备备份。 有关备份的信息，请参阅 备份/恢复。

请注意，并非所有设备都支持远程备份。

## 计划 防火墙管理中心 备份

您可以使用防火墙管理中心上的调度程序来自动执行防火墙管理中心和设备备份。请注意，并非所有设备都支持远程备份。有关详细信息，请参阅备份/恢复。

**注释** 作为初始配置的一部分， 系统会安排每周仅限配置的 防火墙管理中心 备份（本地存储）。我们建议您查看此任务，并在必要时进行更改，如 此主题。

### 开始之前

创建指定您的备份首选项的备份配置文件。请参阅创建备份配置文件。

您必须在全局域中才能执行此任务。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 从 **Job Type** 列表中，选择 **Backup**。

**步骤 3** 指定要备份 **一次** 还是 **定期**备份。

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 对于定期任务，请参阅 配置周期性任务 ， 第 2 页。

**步骤 4** 输入 **作业名称**。

**步骤 5** 对于**备份类型 (Backup Type)**，点击**管理中心 (Management Center)**。

**步骤 6** 选择 **备份配置文件**。

**步骤 7** （可选）输入 **注释**。

请保持注释简短。他们将显示在计划日历页面的“任务详细信息”部分中。

**步骤 8** （可选）在 **邮件发送状态：** 字段中输入邮件地址或邮件地址的逗号分隔列表。

有关设置邮件中继服务器以发送任务状态消息的信息，请参阅 配置邮件中继主机和通知地址。

**步骤 9** 点击**保存**。

# 安排远程设备备份

您可以使用 防火墙管理中心 上的调度程序来自动执行 防火墙管理中心 和设备备份。请注意，并非所有设备都支持远程备份。有关详细信息，请参阅备份/恢复。

您必须在全局域中才能执行此任务。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 从 **Job Type** 列表中，选择 **Backup**。

**步骤 3** 指定要备份 **一次** 还是 **定期**备份。

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 对于定期任务，请参阅 配置周期性任务 ， 第 2 页。

**步骤 4** 输入 **作业名称**。

**步骤 5** 对于**备份类型**，请点击**设备**。

**步骤 6** 选择一个或多个设备。

如果您的设备未列出，则表示它不支持远程备份。

**步骤 7** 如果未配置远程备份存储，请选择是否要 **检索到管理中心**。

- 已启用（默认）：将备份保存到 `/var/sf/remote-backup/` 中的 防火墙管理中心。
- 已禁用：将备份保存到 `/var/sf/backup/`中的设备。

如果配置了远程备份存储，则远程保存备份文件，并且此选项无效。有关详细信息，请参阅管理备份和远程存储。

**步骤 8** （可选）输入 **注释**。

请保持注释简短。他们将显示在计划日历页面的“任务详细信息”部分中。

**步骤 9** （可选）在 **邮件发送状态：** 字段中输入邮件地址或邮件地址的逗号分隔列表。

有关设置邮件中继服务器以发送任务状态消息的信息，请参阅 配置邮件中继主机和通知地址。

**步骤 10** 点击**保存**。

# 配置证书撤销列表下载

必须使用 防火墙管理中心。

当支持在启用用户证书或审核日志证书的设备上的本地配置中下载证书吊销列表 (CRL) 时，系统会自动创建下载 CRL 任务。可以使用计划程序来编辑任务以设置更新频率。

### 开始之前

- 启用并配置用户证书，或者审核日志证书并设置一个或多个CRL下载URL。有关详细信息，请参阅 需要有效的 HTTPS 客户端证书 和 需要有效的审核日志服务器证书 。

### 过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **作业类型**中，选择 **下载 CRL**。

**步骤 4** 指定要如何安排 CRL 下载，**一次 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

**步骤 7** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须在防火墙管理中心上配置一台有效的邮件中继服务器，以发送状态消息。

**步骤 8** 点击**保存**。

**相关主题**

配置邮件中继主机和通知地址

# 自动执行策略部署

在 防火墙管理中心 中修改配置设置后，必须将这些更改部署到受影响的设备。

⚠

**注意** 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为和部署或激活时重启 Snort 进程的配置。

**过程**

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **作业类型**，选择 **部署策略**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 在**设备 (Device)** 字段中，选择要部署策略的设备。

**步骤 7** 根据需要选中或取消选中 **跳过最新设备的部署** 复选框。

默认情况下，系统会启用**跳过最新设备的部署**以提高策略部署过程中的性能。

**注释**
如果从 防火墙管理中心 Web 界面发起的策略部署正在进行，则系统不会执行已安排的部署策略任务。相应地，如果已安排的策略部署任务正在进行，则系统不允许从 Web 界面发起策略部署。

**步骤 8** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中。注释字段必须包含 3 到 255 个字符，并且不能包含连字符 (-)、冒号 (:) 和括号 () 之外的任何特殊字符。

**步骤 9** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 10** 点击**保存**。

**相关主题**

配置邮件中继主机和通知地址

需要部署的配置更改

# Nmap 扫描自动化

您可在网络上安排定期 Nmap 目标扫描。自动化扫描允许您刷新 Nmap 扫描之前提供的信息。由于 Firepower 系统无法更新 Nmap 提供的数据，因此需要定期重新扫描以保持数据为最新。还可安排扫描，使其自动在网络主机上测试未识别的应用或服务器。

请注意，发现管理员也可使用 Nmap 扫描作为补救。例如，主机上发生的操作系统冲突可能会触发 Nmap 扫描。运行扫描可以获取主机的最新操作系统信息，这样可以解决冲突。

如果之前未曾使用 Nmap 扫描功能，则在定义计划扫描之前，需要配置 Nmap 扫描。

**相关主题**

Nmap 扫描

## 安排 Nmap 扫描

Nmap 使用 Nmap 扫描结果替换系统检测到的主机操作系统、应用或服务器之后，系统不再更新 Nmap 替换的主机信息。Nmap 提供的服务和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如果计划使用 Nmap 扫描主机，则可能要设置定期安排的扫描，以使 Nmap 提供的操作系统、应用或服务器保持最新。如从网络删除主机并重新添加，则将丢弃任何 Nmap 扫描结果，系统假设监控主机的所有操作系统和服务数据。

**过程**

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **Job Type**，选择 **Nmap Scan**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 在 **Nmap 补救**字段中，选择 Nmap 补救。

**步骤 7** 在 **Nmap 目标 (Nmap Target)** 字段中，选择扫描目标。

**步骤 8** 在**域 (Domain)** 字段中，选择要扩充其网络映射的域。

**步骤 9** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

提示
注释字段显示在日历计划页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

**步骤 10** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 11** 点击**保存**。

相关主题

配置邮件中继主机和通知地址

Nmap 扫描

# 自动执行报告生成

可自动生成报告，以使它们按固定间隔运行。

开始之前

- 对于风险报告以外的报告：创建报告模板。有关详细信息，请参阅报告模板。
- 如果要使用调度程序分发邮件报告，请配置邮件中继主机并指定报告收件人和消息信息。请参阅配置邮件中继主机和通知地址和（对于风险报告以外的报告） 在生成时通过邮件分发报告或（对于风险报告）生成、查看和打印风险报告。
- （可选）设置或更改计划报告的文件名、输出格式、时间窗口或邮件分发设置。请参阅指定计划报告的报告生成设置， 第 9 页。
- 如果您选择 PDF 作为报告输出格式，请查看报告模板并确认模板每个部分中的结果数量不超过 PDF 的相关限制。有关信息，请参阅报告模板字段。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从**作业类型 (Job Type)** 列表，选择一个作业。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务， 第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 在**报告模板 (Report Template)** 字段中，选择风险报告或报告模板。

**步骤 7** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

**步骤 8** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**注释**
配置此选项**不会**分发报告。

**步骤 9** 如果不想在报告没有数据时（例如，当报告期间未发生特定类型的事件时）接收报告邮件附件，请选中**如果报告为空，仍附加到邮件中 (If report is empty, still attach to email)** 复选框。

**步骤 10** 点击**保存**。

## 指定计划报告的报告生成设置

您必须具有管理员或安全分析师权限才能执行此任务。

要指定或更改计划报告的文件名、输出格式、时间窗口或邮件分发设置，请执行以下操作：

### 过程

**步骤 1** 选择**概述 > 报告 > 报表模板**。

**步骤 2** 针对要更改的报告模板，点击**编辑**。

**步骤 3** 如果您将选择 PDF 输出：

a) 查看报告中是否有任何部分在结果数量旁边显示一个黄色三角形。
b) 如果您看到任何黄色三角形，请将光标悬停在该三角形上，以查看该部分 PDF 输出允许的最大结果数。
c) 对于带有黄色三角形的每个部分，将结果数量减少到低于该限制的数量。
d) 如果没有其他黄色三角形，请点击**保存**。

**步骤 4** 点击**生成 (Generate)**。

**注释**
如果要更改报告生成设置而不立即生成报告，则必须从模板配置页中点击**生成**。如果从模板列表视图中点击**生成**，系统不会保存更改，除非您生成报表。

**步骤 5** 修改设置。

**步骤 6** 要保存新设置而不生成报告，请点击**取消**。

要保存新设置并生成报告，请点击**生成**，然后跳过此过程中的其余步骤。

**步骤 7** 点击**保存**。

**步骤 8** 如果您看到有关保存的提示，即使您未进行更改，请点击**确定**。

# 自动生成 思科 建议

可使用自定义入侵策略中最近保存的配置设置，根据网络发现数据，自动生成规则状态建议。

注释 如果系统自动为入侵策略生成预定建议并且不保存更改，则必须丢弃在入侵策略中所做出的更改，而且如果想要策略反映自动生成的建议，还必须执行此策略。

当任务运行时，系统自动生成建议规则状态，并且根据策略的配置修改入侵规则的状态。已修改的规则状态在下次部署入侵策略时生效。

### 开始之前

- 在入侵策略中配置 思科 建议的规则，如 《Cisco Secure Firewall Management Center 设备配置指南》中所述。
- 如果要通过邮件发送任务状态消息，请配置有效的邮件中继服务器。
- 您必须具有 IPS 智能许可证才能生成建议。

### 过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **作业类型**中，选择 **Firepower 建议规则**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中输入名称。

**步骤 6** 在**策略 (Policies)** 旁边，选择要在其中生成建议的一个或多个入侵策略。选中 **所有策略** 复选框以选择所有策略。

**步骤 7** （可选）在**注释 (Comment)** 字段中输入备注。

请保持注释简短。注释显示在计划日历页面的“任务详细信息”(Task Details) 部分中。

**步骤 8** （可选）要通过邮件发送任务状态消息，请在**邮件状态收件人：(Email Status To:)** 字段中输入邮件地址（或以逗号分隔的多个邮件地址）。

**步骤 9** 点击**保存**。

**相关主题**

冲突和更改：网络分析和入侵策略
关于 Cisco 建议的规则
配置邮件中继主机和通知地址

# 软件升级自动化

您可以自动下载 修补程序， 并应用维护版本和修补程序。

要升级 防火墙管理中心，请安排下载和安装任务。要升级受管设备，请安排下载、推送和安装任务。确保在任务之间留出足够的时间；例如，计划在推送仍在运行时进行的安装将失败。

主要版本不支持此功能。 需要访问互联网才能下载升级包。计划对设备组进行升级时，升级将同时在所有分组设备上运行。

**注释** 作为初始配置的一部分，系统会安排每周下载。我们建议您查看此任务，并在必要时进行更改，如自动执行软件下载，第 11 页。 此任务仅下载更新。您负责安装此任务下载的任何更新。

**相关主题**

管理接口
更新

## 自动执行软件下载

使用此程序可安排 补丁下载的下载。您必须在全局域中。

### 开始之前

确保 防火墙管理中心可以访问互联网。

### 过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **Job Type** 列表，选择 **Download Latest Update**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 选中 **更新项目**旁边的 **软件** 复选框。

**步骤 7** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

**步骤 8** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 9** 点击**保存**。

**相关主题**

配置邮件中继主机和通知地址

## 自动执行软件推送

如果想要在托管设备上自动安装软件更新，必须先将更新推送至设备，然后再安装。

创建向托管设备推送软件更新的任务时，确保在推送任务与预定安装任务之间预留充分时间，以便将更新复制至设备。

您必须在全局域中才能执行此任务。

### 过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **Job Type** 列表，选择 **Push Latest Update**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 从**设备 (Device)** 下拉列表中，选择要更新的设备。

**步骤 7** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

**步骤 8** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 9** 点击**保存**。

**相关主题**

配置邮件中继主机和通知地址

## 自动执行软件安装

请确保在向托管设备推送更新的任务与安装更新的任务之间预留充分的时间。

您必须在全局域中才能执行此任务。

**注意** 视乎正在安装的更新，设备可能在安装软件之后重新启动。

### 过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从**作业类型 (Job Type)** 列表中，选择**安装最新更新 (Install Latest Update)**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 在 **设备** 下拉列表中，选择要在其上安装更新的设备 （包括 防火墙管理中心） 。

**步骤 7** 选中**更新项目 (Update Items)** 旁边的**软件 (Software)** 复选框。

**步骤 8** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

**步骤 9** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 10** 点击**保存**。

### 相关主题

配置邮件中继主机和通知地址

# 漏洞数据库更新自动化

可以使用安排功能更新思科漏洞数据库 (VDB)，从而确保正在使用最新信息评估网络主机。您必须将下载、安装和后续部署安排为单独的任务，以便在任务之间留出足够的时间。

**注释** 防火墙管理中心 上的初始设置会自动下载并安装思科提供的最新 VDB，作为一次性操作。它还会安排每周任务，以下载最新可用软件更新，其中包括最新 VDB。我们建议您查看此每周任务，并在必要时进行调整。或者，安排新的周期性任务，以便实际更新 VDB 和/或软件并部署配置。

### 相关主题

管理接口

## 自动执行 VDB 更新下载

您必须在全局域中才能执行此任务。

### 开始之前

请确保 防火墙管理中心能够访问互联网。

### 过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **Job Type** 列表，选择 **Download Latest Update**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

**步骤 7** （可选）在 **注释** 字段中输入简要注释。

**步骤 8** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 9** 点击**保存**。

### 相关主题

配置邮件中继主机和通知地址

## 自动执行 VDB 更新安装

在 VDB 更新下载任务与更新安装任务之间预留足够的时间。

您必须在全局域中才能执行此任务。

⚠

**注意** 在大多数情况下，VDB 更新后的第一次部署会重新启动 Snort 进程，从而中断流量检查。系统会在发生这种情况时向您发出警告 （更新的应用检测器和操作系统指纹需要重新启动；漏洞信息不需要）。在此中断期间，流量是被丢弃还是不经进一步检查直接通过，将取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从**作业类型 (Job Type)** 列表中，选择**安装最新更新 (Install Latest Update)**。

**步骤 4** 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 2 页以了解详细信息。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 从**设备**下拉列表中，选择 防火墙管理中心。

**步骤 7** 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

**步骤 8** （可选）在 **注释** 字段中输入简要注释。

**步骤 9** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 10** 点击**保存**。

相关主题

配置邮件中继主机和通知地址

# 使用已安排任务自动执行 URL 过滤更新

为了确保 URL 过滤的威胁数据为最新，系统必须从思科综合安全智能 (CSI) 云获取数据更新。

默认情况下，在启用URL过滤时，也会启用自动更新。但是，如果需要控制这些更新的发生时间，请使用本主题中所述的程序，而不要使用默认更新机制。

尽管每日更新往往较小，如果距离上次更新已超过五天，新 URL 过滤数据可能需要 20 分钟才能下载完成，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

开始之前

- 请确保防火墙管理中心能够访问互联网:安全、互联网接入和通信端口 。
- 确保您拥有 URL 过滤许可证并启用 URL 过滤。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 使用类别和信誉启用 *URL* 过滤。
- 验证 **集成** > **其他集成** > **云服务** 上的 **URL 过滤**下未选中**启用自动更新**。
- 您必须在全局域中才能执行此任务。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。

**步骤 2** 点击**添加任务 (Add Task)**。

**步骤 3** 从 **Job Type** 列表，选择 **Update URL Filtering Database**。

**步骤 4** 指定要如何安排更新，**一次性 (Once)** 或者**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 对于定期任务，请参阅 配置周期性任务 ， 第 2 页。

**步骤 5** 在**作业名称 (Job Name)** 字段中键入名称。

**步骤 6** 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中。请保持注释简短。

**步骤 7** 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入电子邮件地址（或以逗号分隔的多个电子邮件地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

**步骤 8** 点击**保存**。

相关主题

配置邮件中继主机和通知地址

# 预定任务审核

添加预定任务后，即可查看这些任务，评估它们的状态。在页面的“查看选项”(View Options) 部分，查使用日历和预定任务列表查看预定任务。

Calendar 视图选项可用于查看哪些预定任务在哪天发生。

“任务列表”(Task List) 显示一列任务及其状态。打开日历时，任务列表出现在日历下方。此外，也可通过从日历中选择日期或任务来查看它。

可编辑先前创建的预定任务。如果想要测试一次预定任务，确保参数正确，此功能特别有用。稍后，任务成功完成后，即可将其更改为周期性任务。

可从“计划视图”(Schedule View) 页面执行两类删除。可删除尚未运行的特定一次性任务，也可删除周期性任务的每个实例。如果删除周期性任务的一个实例，该任务的所有实例均将删除。如果删除预定运行一次的任务，则仅删除该任务。

# 任务列表详细信息

表 *1:* 任务列表列

| 列 | 说明 |
|---|---|
| 名称 | 显示预定任务的名称及与其关联的注释。 |
| 类型 | 显示预定任务的类型。 |
| 开始时间 (Start Time) | 显示预定任务的开始日期和时间。 |
| 频率 (Frequency） | 显示任务的运行频率。 |
| 上次运行时间 | 显示实际开始日期和时间。<br>对于周期性任务，这适用于最近执行。 |
| 上次运行状态 | 描述预定任务的当前状态。<br>• **复选标记**（） 指明任务已成功运行。<br>• 问号图标 (**问号** （）) 指明任务处于未知状态。<br>• 感叹号图标 () 指明任务已失败。<br>对于周期性任务，这适用于最近执行。 |
| 下次运行时间 | 显示周期性任务的下次执行时间。<br>为一次性任务显示“不适用”(N/A)。 |
| 创建者 | 显示创建预定任务的用户的名称。 |
| 编辑 | 编辑预定任务。 |
| 删除 | 删除预定任务。 |

# 在日历中查看预定任务

您可以在日历上查看计划任务。

## 过程

**步骤 1** 选择 **系统** () > **工具** > **计划**。

**步骤 2** 可使用日历视图执行以下任务：

- 点击 **双左箭头** （|<） 可后退一年。
- 点击 **单左箭头**（<） 可后退一个月。
- 点击 **单右箭头**（>） 可向前移动一个月。
- 点击 **双右箭头**（>|） 可向前移动一年。
- 点击**今天 (Today)**，返回当前月份和年份。
- 点击**添加任务 (Add Task)**，安排新任务。
- 点击一个日期，在日历下方的任务列表中查看所有预定任务的特定日期。
- 点击在某个日期发生的特定任务，在日历下方的任务列表中查看此任务。

# 编辑预定任务

您可以编辑计划任务。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。
**步骤 2** 在日历上，点击要编辑的任务，或者任务出现的日期。
**步骤 3** 在 **任务详细信息** 表中，点击要编辑的任务旁边的 **编辑** (✎) 。
**步骤 4** 编辑任务。
**步骤 5** 点击**保存**。

# 删除预定任务

您可以删除计划任务。

过程

**步骤 1** 选择 **系统** (⚙) > **工具** > **计划**。
**步骤 2** 在日历中，点击要删除的任务。对于周期性任务，请点击任务的实例。
**步骤 3** 在 **任务详情** 表中，点击 **删除** (🗑)，然后确认您的选择。

# 计划任务的历史记录

| 功能 | 防火墙管理中心最低版本 | 最低版本 | 详细信息 |
|---|---|---|---|
| 已弃用：维护版本的计划下载。 | 7.2.6<br>7.4.1 | 任意 | **升级影响。计划的下载任务停止检索维护版本。**<br>**下载最新更新**计划任务不再下载维护版本；现在，它仅下载最新的适用补丁和 VDB 更新。要将维护（和主要）版本直接下载到防火墙管理中心，请使用**系统**（⚙）>**产品升级**。<br>版本限制：不支持 防火墙管理中心 版本 7.3.x 或 7.4.0。 |
| 自动 VDB 下载。 | 7.3.0 | 任意 | 初始设置计划每周执行一次任务，以下载最新的可用软件更新，现在包括最新的VDB。我们建议您查看此每周任务并在必要时进行调整，同时安排新的每周任务来实际更新VDB。您必须部署配置，新的应用检测器和操作系统指纹才会生效。<br>新增/修改的屏幕：默认情况下，系统创建的 **每周软件下载** 计划任务中的 **漏洞数据库** 复选框现在处于启用状态。 |
| 自动入侵规则更新。 | 6.6 | 任意 | 初始设置现在会启用每日入侵规则更新。我们建议您查看此任务，并在必要时进行调整。要让更新后的规则生效，您必须部署配置。 |
| 自动软件下载和配置备份。 | 6.5 | 任意 | 初始设置现在会安排每周任务以便：<br>• 为 FMC 及其托管设备下载最新的可用软件更新。<br>• 执行本地存储的仅配置备份。<br>我们建议您查看这些任务，并在必要时进行调整。 |
| 为许多托管设备安排远程备份。 | 6.4 | 任意 | 安排设备备份。<br>新增/修改的屏幕：配置定期备份时，您现在可以选择**备份类型 (Backup Type)**：管理中心与设备。<br>平台限制：设备必须支持按需备份；请参阅 备份和还原要求。 |

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。