管理

通过导航到 **管理** > **来**访问以下管理视图。

管理

通过导航到 **管理** > **来**访问以下管理视图。

API 密钥

导航至 **管理** > **API** > **密钥** 以查看此页面。

搜索

使用搜索栏搜索或过滤包含关键字的 API 密钥列表。您必须至少使用三个字符才能进行搜索。

API 密钥表和操作

此表列出了 多云防御 组件为您的云服务提供商创建的所有 API 密钥。查看角色、密钥 ID、将密钥添加到 多云防御的日期以及密钥到期日期。

您可以在此处创建或删除 API 密钥。请注意，这些密钥由 多云防御 生成，与您的云服务提供商可能为维护通信而创建的密钥无关。继续阅读以了解更多信息。

在 多云防御中创建 API 密钥

请使用以下程序创建新的 API 密钥：

步骤 1 导航至 **管理** > **管理** > **API 密钥**。

步骤 2 点击**创建 API 密钥 (Create API Key)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 确认 多云防御 自动生成的 **邮箱地址** 。您无法更改此选项。

步骤 5 使用下拉菜单选择其中一个关键角色：

- **admin_read_only** - 此角色限制交互，因此您无法修改或操作任何内容，并且只能“查看”可用数据。
- **admin_read_rw** - 此角色允许您读取和修改可用数据。

步骤 6 为 **API 密钥生命周期 (天)**输入适当的值。默认值为 365 天。

步骤 7 点击**保存 (Save)**。

从 多云防御删除 API 密钥

请使用以下程序删除 API 密钥：

步骤 1 导航到 **管理** > **管理** > **API 密钥**。

步骤 2 从表中选择 API 密钥并选中复选框，使其突出显示。

步骤 3 点击**删除 (Delete)**。

步骤 4 确认要删除的密钥，然后点击 **确定**。密钥会立即从 多云防御中删除。

账户级别设置

此页面显示 多云防御中使用的一些标签，包括应用标签和自定义标签。继续阅读以了解更多信息。

应用标记

应用标记是一个字符串，用作进程或线程自动分类的分类标准之一。通过标记，您可以根据自己的独特要求对应用进行分组，以便搜索应用并查找漏洞。请注意，并非所有云服务提供商都支持使用应用标签。

创建应用标签

请使用以下程序创建应用标签：请注意，这些标签仅供内部使用，可能无法从您的云服务提供商的界面识别或提供。

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **应用标签** 表中，点击 **创建**。

步骤 3 默认情况下，应用标签的类型为 `APPLICATION_TAG_KEYS` 。

步骤 4 输入标签的简短 **说明** 。这有助于识别或区分可能具有相似名称或概念的其他标签。

步骤 5 至少输入一个 **值**。在每个值后 `按 Enter 键` 可创建多个值。请注意，这些值区分大小写。

步骤 6 点击**保存**。标签已创建并在表中可用。

编辑应用标记

使用以下程序编辑已在 多云防御中创建的现有应用标记。您不能使用此程序修改在云服务提供商界面中创建的标签。

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **应用标签** 表中，找到要编辑的应用标签，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**编辑**。

步骤 4 修改以下参数：

- **说明** - 您可以编辑或删除说明。
- **标签值** - 您可以在此处添加或删除标签。

步骤 5 点击**保存**。或者，您可以随时取消而不保存更改。

删除应用标记

使用以下程序删除现有应用标记：

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **应用标签** 表中，找到要编辑的应用标签，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**删除 (Delete)**。

步骤 4 确认要删除应用标记，然后点击 **确定**。

自定义标记

自定义标签是简单的数据片段，可提供有关项目的详细信息，并可以轻松找到具有相同标签的相关项目。您可以使用标记轻松识别或区分对象、策略、规则等。

创建自定义标记

使用以下程序在 多云防御中创建自定义标记。请注意，这些标签仅供内部使用，可能无法从您的云服务提供商的界面识别或提供。

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **自定义标签** 表中，点击 **创建**。

步骤 3 输入标签的 **值** 。这有助于识别或区分可能具有相似名称或概念的其他标签

步骤 4 至少输入一个 **值**。

步骤 5 点击**保存**。标签已创建并在表中可用。

编辑自定义标记

使用以下程序修改现有自定义标记：

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **自定义标记** 表中，找到要编辑的应用标记，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**编辑**。

步骤 4 修改以下参数：

- 密钥。
- 值。

步骤 5 点击**保存**。或者，您可以随时取消而不保存更改。

删除自定义标记

使用以下程序删除现有自定义标记：

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **自定义标记** 表中，找到要编辑的应用标记，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**删除 (Delete)**。

步骤 4 确认要删除应用标记，然后点击 **确定**。

系统

系统 页面是一个历史文档，其中至少列出了一年的更新。您可以使用这些详细信息获取一般知识，查找正确的版本说明，以及联系思科支持以获取产品帮助。此处显示以下信息集合：

组件

本部分显示 多云防御控制器 和用户界面的当前版本。请注意，您无法从此页面强制更新或回滚到以前的版本。

网关映像

网关映像表指示 多云防御网关 的升级时间、网关的版本和持续时间，以及建立网关的时区。

Talos/网络入侵

此表显示来自思科 Talos 情报小组的所有更新。这些更新将独立于正常产品软件版本推送到思科产品。

Web 保护

此表显示针对最新 Web 应用漏洞和威胁的所有 Web 应用防火墙 (WAF) 核心和 trustwave 规则更新。

电表

计量 页面显示 多云防御 的总体使用情况和为您的云服务提供商创建的网关实例的使用情况图表。

过滤器 (Filters)

使用位于页面顶部的过滤器来确定页面中显示的数据。您可以通过选择月份和年份来更改此视图。您可以使用这些过滤器设置生成使用情况报告。

生成使用报告

您可以从此页面为两个选项中的任何一个生成使用情况报告。导航到 **管理** > **管理** > **计量** 并展开页面 **过滤器** 部分中的 **下载** 下拉选项，以选择使用情况或实例。该文件作为 .csv 文件下载到本地。使用过滤选项确定生成报告的时间范围。

使用记录

使用情况记录 表详细列出了与您的租户关联的账户数量、与账户交互的小时数，以及在“过滤器”部分选择的每月哪几天。您可以根据使用量/月比确定哪些天最活跃。

实例记录

实例记录 表显示以下实例统计信息：

- 账户名称。
- 按云服务提供商划分的账户类型。
- 实例 ID。
- 实例类型。
- 可用性区域。
- 网关。
- 已开始 - 创建网关实例的时间。
- 已结束 - 网关实例到期或终止。

警报配置文件

通过导航到 **管理** > **警报配置文件**访问以下管理视图。

服务 和 **警报** 页面重点关注来自 多云防御的警报。 **警报** 页面重点介绍警报的发送目标， **警报** 页面详细介绍发送到已配置终端的警报。对于理想的配置，请花时间在两个页面中设置条目，以成功并全面优化控制面板中的警报机会。

服务

导航至 **管理** > **管理** > **服务** 以查看此页面。

服务侧重于 您要将警报发送到的位置。请注意，您必须提供来自第三方应用的条件，才能成功配置此页面上的任何选项。

搜索

使用搜索栏搜索或过滤包含关键字的服务列表。您必须至少使用三个字符才能进行搜索。

服务表和操作

此表列出了由多云防御组件为您的云服务提供商创建的所有服务。查看服务的名称、类型和更新日期。

您可以在此处创建或删除服务。请注意，这些服务由多云防御生成，与您的云服务提供商可能提供的服务无关。

创建服务

使用以下程序创建服务：

开始之前

您必须在第三方消息传送应用上启用或允许服务通知或集成。

步骤 1 导航至 **管理** > **管理** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的其他服务。

步骤 5 使用下拉菜单选择服务 **类型**：

- Pager Duty。
- ServiceNow。
- Slack。

- Datadog。
- Microsoft Sentinel。
- Microsoft Teams。
- Webex
- Splunk。

步骤 6 根据服务类型，在系统提示时填写以下条目：

- API 密钥。
- API URL。
- Azure 日志表名称。
- Azure 日志分析工作空间 ID
- （对于 Splunk 可选）索引。

步骤 7 点击**保存 (Save)**。

编辑服务

使用以下程序编辑现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **编辑**。
步骤 4 修改服务的以下方面：

- 名称。
- 说明。
- Type。
- 类型特定的配置条件。

步骤 5 点击 **保存** 来确认更改。在任何时候，点击 **取消** 以关闭窗口并取消更改。

下一步做什么

您可能需要 **刷新** 页面才能看到任何更改。

克隆服务

使用以下程序克隆现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **克隆**。
步骤 4 将生成服务的克隆。默认情况下，仅保留服务 **类型** 和任何服务特定的配置条件。
步骤 5 在**名称 (Name)** 中输入唯一的名称。
步骤 6 （可选）输入说明。
步骤 7 点击 **保存** 来确认更改。在任何时候，点击 **取消** 以关闭窗口并取消更改。

下一步做什么

您可能需要 **刷新** 页面才能查看对表的更改或添加。

导出服务

使用以下程序导出现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **导出**。
步骤 4 多云防御 生成导出向导。
步骤 5 点击 **下载** 在本地下载 terrform，或点击 **复制代码** 复制 JSON 资源以手动粘贴到 terroform 脚本中。
步骤 6 在 terrform 提示符下，执行窗口下半部分提供的命令： `terraform import "ciscomcd_alert_profile". "servicename" <number in table>`
步骤 7 在 terraform 中按照提示完成任务。控制面板中没有其他步骤。

删除服务

使用以下程序删除现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **删除**。
步骤 4 确认要删除服务，然后点击 **确定**。

步骤 5 服务已从 多云防御中删除。

警报

“警报”页面重点介绍发送 **到** 第三方终端的警报。我们强烈建议配置警报和服务，以利用警报机会。

创建警报

请使用以下程序创建警报：

步骤 1 导航至 **管理** > **管理** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的其他服务。

步骤 5 选择 **警报配置文件**。目前， `Pagerduty` 是唯一可用的选项。

步骤 6 使用下拉菜单选择警报 **类型**。

- 系统日志。
- 审核日志。
- 证据开示。

步骤 7 （可选）使用下拉菜单选择 **子类型**。请注意，这些选项可能会更改或不可用，具体取决于您在步骤 6 中选择的类型：

- 网关。
- 账户。
- 管理员。
- 洞察力规则。

步骤 8 使用下拉菜单并选择 **严重性**级别：

- 信息。
- 警告。
- 中。
- 高。
- 严重。

步骤 9 默认情况下，**启用 (Enabled)** 复选框处于选中状态。此选项指定警报配置文件是否处于活动和可用状态。如果它被禁用， 多云防御 在发出警报时不包括它。

下一步做什么

服务 以指定将这些警报发送到的目标。

编辑警报

使用以下程序编辑现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。
步骤 2 找到并选择表中的警报，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **编辑**。
步骤 4 编辑警报配置文件的任何字段和选项。请注意，某些可用字段可能会根据您的选择而变化。
步骤 5 点击 **保存** 来确认更改。您可以随时点击 **取消** 以取消更改并关闭编辑窗口。

克隆警报

使用以下程序克隆现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。
步骤 2 找到并选择表中的警报，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **编辑**。
步骤 4 生成警报的副本。默认情况下，仅保留 **警报配置文件** 和 **类型** 。
步骤 5 编辑警报的任何剩余字段和选项。请注意，某些可用字段可能会根据您的选择而变化。
步骤 6 点击 **保存** 来确认更改。您可以随时点击 **取消** 以取消更改并关闭编辑窗口。

导出警报

使用以下程序导出现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。
步骤 2 找到并选择表中的警报，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **导出**。
步骤 4 多云防御 生成导出向导。
步骤 5 点击 **下载** 在本地下载 terrform，或点击 **复制代码** 复制 JSON 资源以手动粘贴到 terroform 脚本中。

步骤 6 在terrform提示符下，执行窗口下半部分提供的命令： `Terraform import "ciscomcd_alert_rule"."alertname"<number in table>`。

步骤 7 在 terraform 中按照提示完成任务。控制面板中没有其他步骤。

删除警报

使用以下程序删除现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。

步骤 2 找到并选择表中的警报，使其突出显示。

步骤 3 展开操作下拉菜单，然后点击 **删除**。

步骤 4 确认要删除服务，然后点击 **确定**。

步骤 5 警报已从 多云防御中删除。

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。