



数据清除和存储

- [存储在 FMC 上的数据](#)，第 1 页
- [外部数据存储](#)，第 3 页
- [数据存储历史记录](#)，第 5 页

存储在 FMC 上的数据

对象	请参阅
有关 FMC 上数据存储的一般信息	磁盘使用率构件
清除旧数据	从管理中心数据库清除数据 ，第 2 页
允许外部访问 FMC 上的数据（这是一项高级功能）	外部数据库访问
备份	管理备份和远程存储 和子主题
报告	配置本地存储
事件	连接日志记录 数据库 和子主题
网络发现数据	网络发现数据存储设置 和 《 Cisco Secure Firewall Management Center 设备配置指南 》中的后续主题
文件	《 Cisco Secure Firewall Management Center 设备配置指南 》的 网络恶意软件保护和文件策略 一章中有关存储文件的信息，包括最佳实践。 调整文件和恶意软件检测性能和存储 《 Cisco Secure Firewall Management Center 设备配置指南 》
数据包数据	《 Cisco Secure Firewall Management Center 设备配置指南 》中的 编辑常规设置

对象	请参阅
用户和用户活动	<p>《Cisco Secure Firewall Management Center 设备配置指南》中的用户数据库</p> <p>《Cisco Secure Firewall Management Center 设备配置指南》中的用户活动数据库</p>

从管理中心 数据库清除数据

您可以使用数据库清除页面从 管理中心 数据库清除发现、身份、连接和安全情报数据文件。请注意，清除数据库时，会重新启动相应的进程。



注意 清除数据库会从管理中心中移除指定的数据。删除数据后，该数据无法恢复。

开始之前

您必须具有管理员或安全分析师权限才能清除数据。您只能在全局域中。

过程

步骤 1 选择系统 (⚙️) > 工具 > 数据清楚。

步骤 2 在 **发现和身份** 下，执行以下任何或所有操作：

- 选中 **网络发现事件 (Network Discovery Events)** 复选框以从数据库删除所有网络发现事件。
- 选中 **主机 (Hosts)** 复选框以从数据库删除所有主机和主机 危害表现标志。
- 选中 **用户活动 (User Activity)** 复选框以从数据库删除所有用户活动事件。
- 选中 **用户身份 (User Identities)** 复选框以从数据库删除所有用户登录信息和用户历史记录数据，以及用户危害表现标志。

注释 不会删除 Microsoft Azure AD 领域的用户活动事件、用户登录和用户历史记录数据。

步骤 3 在 **Connections** 下，执行以下任一或所有步骤：

- 选中 **连接事件 (Connection Events)** 复选框以从数据库删除所有连接数据。
- 选中 **连接摘要事件 (Connection Summary Events)** 复选框以从数据库删除所有连接摘要数据。
- 选中 **安全情报事件 (Security Intelligence Events)** 复选框以从数据库删除所有安全情报数据。

注释 选中 **连接事件** 复选框不会删除安全情报事件。带有安全情报数据的连接仍将显示在“安全情报事件”页面上（位于“分析”>“连接”菜单下）。同样，选中 **安全情报事件 (Security Intelligence Events)** 复选框不会删除具有关联安全情报数据的连接事件。

- 步骤 4** 点击清除所选事件 (**Purge Selected Events**)。
项目会被清除，且相应进程会重启。

外部数据存储

您可以选择使用远程数据存储来存储某些类型的数据。

对象	请参阅
备份	管理备份和远程存储 和子主题 远程存储设备 和子主题
报告	远程存储设备 和子主题 将报告移至远程存储器
事件	有关 使用外部工具的事件分析 中的系统日志和其他资源的信息 在思科 Cisco Secure Cloud Analytics 中的远程数据存储 ，第 4 页 Secure Network Analytics 设备上的远程数据存储 ，第 4 页 如果您远程存储连接事件，请考虑在 FMC 上禁用连接事件的存储。有关信息，请参阅 数据库 以及子主题。



- 重要事项** 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

安全分析和日志记录 远程事件存储选项的比较

将事件数据存储到 管理中心外部的类似但不同的选项：

本地	SaaS
您购买、许可并设置防火墙后的存储系统。	您购买许可证和数据存储计划，并将数据发送到思科云。

本地	SaaS
支持的事件类型： <ul style="list-style-type: none"> • 连接 • 安全情报 • 入侵 • 文件和恶意软件 • LINA 	支持的事件类型： <ul style="list-style-type: none"> • 连接 • 安全情报 • 入侵 • 文件和恶意软件
支持系统日志和直接集成。	支持系统日志和直接集成。
<ul style="list-style-type: none"> • 查看 Cisco Secure Network Analytics 管理器上的所有事件。 • 从 FMC 事件查看器交叉启动，以查看 Cisco Secure Network Analytics 管理器上的事件。 • 在 FMC 中查看远程存储的连接和安全情报事件 	在 CDO 中查看事件，或者 Secure Network Analytics，具体取决于您的许可证。从 FMC 事件查看器交叉启动。
有关更多信息，请参阅 Secure Network Analytics 设备上的远程数据存储 ，第 4 页中的链接。	有关更多信息，请参阅 在思科 Cisco Secure Cloud Analytics 中的远程数据存储 ，第 4 页中的链接。

在思科 Cisco Secure Cloud Analytics 中的远程数据存储

使用 安全分析和日志记录 (SaaS) 将选定的 Firepower 事件数据发送到 Cisco Secure Cloud Analytics。支持的事件：连接、安全情报、入侵、文件和恶意软件。

关于详细信息，请参阅 <https://cisco.com/go/firepower-sal-saas-integration-docs> 中的 *Firepower* 管理中心和思科安全分析与日志记录 (SaaS) 集成指南。

您可以直接或通过系统日志发送事件。



重要事项 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

Secure Network Analytics 设备上的远程数据存储

如果您需要比 Firepower 设备更多的数据存储，可以使用 安全分析和日志记录（本地部署）在 Secure Network Analytics 设备上存储 Firepower 数据。有关完整信息，请参阅 <https://cisco.com/go/sal-on-prem-docs> 提供的文档。

您可以在 [管理中心](#) 中查看连接事件，即使它们存储在 Secure Network Analytics 设备上。请参阅在 [Cisco Secure Firewall Management Center](#) 和使用存储在 Secure Network Analytics 设备上的连接事件上工作。



重要事项 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

数据存储历史记录

功能	最低 管理 中心	最低 威胁 防御	详情
免除低优先级连接事件的事件速率限制	7.0	任意	<p>如果您选择不 在 管理中心 上存储连接事件，因为您将它们存储在远程卷上，则这些事件不会计入 管理中心 硬件设备的流量限制。</p> <p>如果使用新的 7.0 配置将事件发送到 安全分析和日志记录（本地部署），则将此设置配置为该集成的一部分。</p> <p>否则，请参阅 数据库事件限制 中的有关连接数据库的信息。</p> <p>新增/修改的页面：无。仅行为更改。</p>
改进了将事件发送到 Secure Network Analytics 设备的流程	7.0	任意	<p>新向导简化了使用 安全分析和日志记录（本地部署）将事件直接发送到 Secure Network Analytics 设备的过程。</p> <p>该向导还允许您在查看 管理中心 上的事件页面时查看远程存储的连接事件，并从 管理中心 交叉启动以查看 Secure Network Analytics 设备上的事件。</p> <p>如果您已将系统配置为使用系统日志发送事件，则将继续使用系统日志发送事件，除非您禁用这些配置。</p> <p>有关详细信息，请参阅 Secure Network Analytics 设备上的远程数据存储，第 4 页中引用的文档。</p> <p>新增/修改的页面：系统 > 日志记录 > 安全分析和日志记录 页面现在显示用于创建交叉启动选项的向导，而不是配置。</p>

功能	最低 管理中心	最低 威胁 防御	详情
Secure Network Analytics 设备上的远程数据存储	6.7	任意	<p>您现在可以使用 安全分析和日志记录（本地部署）远程存储大量 Firepower 事件数据。在 管理中心中查看事件时，您可以快速交叉启动以查看远程数据存储位置中的事件。</p> <p>支持的事件：连接、安全情报、入侵、文件和恶意软件。使用系统日志发送事件。</p> <p>此解决方案取决于运行 Stealthwatch Enterprise (SWE) 版本 7.3 的 Stealthwatch 管理控制台 (SMC) 虚拟版的可用性。</p> <p>请参阅 Secure Network Analytics 设备上的远程数据存储，第 4 页。</p>
在思科 Cisco Secure Cloud Analytics 中的远程数据存储	6.4	任意	<p>使用系统日志发送选定的 Firepower 数据使用 安全分析和日志记录 (SaaS)。支持的事件：连接、安全情报、入侵、文件和恶意软件。</p> <p>关于详细信息，请参阅 https://cisco.com/go/firepower-sal-saas-integration-docs 中的 <i>Firepower</i> 管理中心和思科安全分析与日志记录 (SaaS) 集成指南。</p>

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。