



统一事件

以下主题介绍如何使用统一事件：

- [关于统一事件，第 1 页](#)
- [统一事件的要求和必备条件，第 2 页](#)
- [使用统一事件查看器操作，第 2 页](#)
- [在统一事件查看器中设置时间范围，第 4 页](#)
- [统一事件查看器中的事件实时视图，第 5 页](#)
- [统一事件查看器中的过滤器，第 5 页](#)
- [在统一事件查看器中保存搜索，第 6 页](#)
- [在统一事件查看器中加载保存的搜索，第 7 页](#)
- [在统一事件查看器中保存列集，第 7 页](#)
- [在统一事件查看器中加载已保存的列集，第 8 页](#)
- [统一事件查看器列说明，第 8 页](#)
- [统一事件的历史记录，第 9 页](#)

关于统一事件

统一事件为您提供多种类型（连接、入侵、文件、恶意软件和一些安全相关的连接事件）的单一屏幕视图。相互关联的事件在表中堆叠在一起，以提供有关安全事件的统一视图和更多上下文。如果“统一事件”表中有入侵事件，请点击入侵事件以突出显示关联的连接事件。现在，您可以将连接事件与入侵事件关联，以便更好地解决网络问题，而无需在多个事件查看器之间切换。

统一事件表可高度自定义。您可以创建和应用自定义过滤器，以微调事件查看器上显示的信息。统一事件查看器还可以选择保存您经常用于特定需求的自定义过滤器，然后快速加载已保存的过滤器。此外，您可以通过添加或删除列、固定列或拖动列并重新排序来创建定制的事件查看器表。

通过“统一事件”表中的**实时视图**选项，您可以实时查看防火墙事件并监控网络上的活动。例如，如果您是防火墙管理员，在进行策略更改后实时查看事件更新可以帮助您确保在网络上正确实施策略更改。

统一事件的要求和必备条件

型号支持

任意。

支持的域

任意。

用户角色

- 管理员
- 安全分析师

使用统一事件查看器操作

在单个表中查看和处理各种防火墙事件，而无需在多个事件查看器之间切换。

使用此视图：

- 在统一视图中查找不同类型事件之间的关系。
- 实时查看策略更改的影响。

开始之前

您必须具有 **管理员** 或 **安全分析师** 权限才能执行以下任务。

过程

步骤 1 选择 **分析 > 统一事件**。

步骤 2 选择时间范围（固定或滑动）。有关详细信息，请参阅 [在统一事件查看器中设置时间范围](#) 主题。

步骤 3 如果要在 Secure Network Analytics 设备上远程存储事件，并且有充分的理由更改数据源，请选择数据源。请查看 [在 Cisco Secure Network Analytics 设备上存储的连接事件中的 Cisco Secure Firewall Management Center 工作中的重要信息](#)。

步骤 4 您可以过滤统一事件查看器最初显示的大量防火墙事件，以了解网络中事件的更精细情景。有关详细信息，请参阅 [统一事件查看器中的过滤器](#)。

步骤 5 选择更多选项：

收件人	相应操作
自定义列	<ul style="list-style-type: none"> • 添加或删除列： 点击列选择器 (☰) 并选择列。 注释 包含许多列可能会降低性能。您可以通过展开事件行查看事件详细信息来查看隐藏列的数据。 • 对列重新排序： 拖放列标题。 • 将列固定（冻结）到表的左侧或右侧，使它们不会滚动： 将列拖至表的左侧或右侧。 或者，将列标题拖放到固定区域。 要取消固定列，请将该列拖出固定区域。 • 调整列大小。 • 将列恢复为默认设置。 • 保存列集。有关详细信息，请参阅 在统一事件查看器中保存列集 主题。 <p>数据始终按时间排序，最新事件排在最前面。</p>
识别相关事件	<p>点击一行可突出显示与此事件相关的其他事件。</p> <p>如果需要，过滤事件以显示足够小的事件集。</p> <p>注释 连接的发起方不一定与恶意软件文件的发送方相同。通过使用 源或目标 IP 过滤器过滤统一事件查看器，搜索与连接事件关联的文件或恶意软件事件。</p>
查看事件详情	<p>点击行左端的 >（拓展）图标。事件详细信息不包括没有要显示的数据的字段。</p> <p>提示 双击事件可查看 事件详细信息 窗格。当 事件详细信息 窗格打开时，点击表中的任何事件以加载该事件的详细信息。</p>
实时查看事件	<p>点击 上线。有关详细信息，请参阅 统一事件查看器中的事件实时视图。</p> <p>如果事件流过快，请输入过滤条件。</p>
查看可用于单元格值的选项	<p>点击单元格右端的 选项 图标。</p>
交叉启动到外部资源	<p>点击表格单元格中的点可查看与该数据相关的其他选项（如有）。</p> <p>有关详细信息，请参阅 使用基于 Web 的资源的事件调查。</p>

收件人	相应操作
打开多个统一事件查看器选项卡/窗口	<p>您可以使用多个浏览器选项卡或窗口显示统一事件查看器的不同视图。每个新选项卡或窗口都具有最近修改的选项卡/窗口的特征。</p> <p>要将任何打开的选项卡/窗口设置为模板，请对其进行细微更改。</p> <p>多个选项卡中的查询按顺序处理。</p> <p>根据视图（例如，复杂查询或传入事件速率较高时在实时视图模式的查看），如果同时打开超过 4 个选项卡，性能可能会降低。</p>
保存搜索	<p>将自定义搜索保存为您的收藏，并在以后快速加载。有关详细信息，请参阅 在统一事件查看器中保存搜索 主题。</p>
为查询结果添加书签或共享	<p>将 URL 加入书签或复制粘贴到浏览器窗口中。</p> <p>如果您的 URL 使用滑动时间范围，则稍后将检索不同的事件。列可视性、大小和顺序以及实时流设置不会在 URL 中捕获。</p>

在统一事件查看器中设置时间范围

在统一事件查看器中配置时间范围，以查看特定时间段的防火墙事件。当您更改时间范围时，统一事件查看器会自动刷新以反映您的更改。

您选择的时间范围不适用于事件查看器中的其他表。例如，您在查看连接事件时选择的时间范围不适用于统一事件查看器，反之亦然。



重要事项 如果您的时间段延长到超出连接事件的保留期，请在 **分析 > 连接 > 安全情报事件** 下的表中查找安全情报事件。

开始之前

您必须具有 **管理员** 或 **安全分析师** 权限才能执行此任务。

过程

步骤 1 选择 **分析 > 统一事件**。

默认情况下，统一事件查看器显示过去一小时的事件。

步骤 2 点击当前时间范围。

步骤 3 选择以下其中一个选项：

- 如果要查看固定时间范围内的事件，请点击 **固定时间范围** 并选择 **开始时间** 和 **结束时间**。

提示 点击 **现在** 快速将当前时间设置为 **结束时间**。

- 如果您想配置指定长度的滑动式默认时间窗口，点击 **滑动式时间范围**。

设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。刷新事件视图时，时间窗口会“滑动”，以便始终显示最后一小时的事件。

步骤 4 点击应用。

统一事件查看器中的事件实时视图

将统一事件查看器配置为实时显示防火墙事件，而无需手动刷新事件查看器。在 **实时视图** 模式下，当网络中发生安全事件时，会实时显示事件日志，这有助于您更好地解决问题。

开始之前

您必须具有 **管理员** 或 **安全分析师** 权限才能执行此任务。

过程

步骤 1 选择 **分析 > 统一事件**。

默认情况下，统一事件查看器显示最近一小时的事件。

步骤 2 要查看实时事件更新，请点击 **上线**。

新事件将填充在事件表的顶部。时间范围部分显示一个计时器，通知您统一事件查看器的运行时间。

下一步做什么

要退出实时视图模式，请点击 **实时**。

统一事件查看器中的过滤器

统一事件查看器最初显示过去一小时内的多种类型的防火墙事件。您可以过滤统一事件的默认视图，以获取更精细的网络活动情景图片。过滤器支持排除和包含过滤条件。

过滤器可帮助您快速访问关键信息。例如，如果您是防火墙管理员，并且要允许或拒绝某些用户访问特定应用，则可以设置用户搜索条件以扫描防火墙日志。事件查看器显示与搜索条件匹配的事件日志。

开始之前

您必须具有 **管理员** 或 **安全分析师** 权限才能执行以下任务。

过程

步骤 1 选择 **分析 > 统一事件**。

步骤 2 输入过滤器条件：

- 要手动输入过滤条件，请在搜索文本字段中键入确切的条件，或从下拉列表中选择条件。然后，提供过滤条件值。输入值时，系统会尽可能在下拉列表中提示您建议。
- 点击表中事件的单元格中的点，然后选择一个选项以在过滤条件中包括或排除该值。

提示

- 使用 **Ctrl+点击** (Windows) 或 **Command-点击** (Mac) 键快速添加包含过滤条件。
- 使用 **Alt+点击** (Windows) 或 **Option 点击** (Mac) 键快速添加排除过滤条件。

- 请细化您的过滤条件。有关通配符和搜索行为的重要信息，请参阅 [事件搜索](#)
- 在值字段中，在值前面添加运算符（例如 <、>、! 等）。例如，在 **操作** 字段中输入 `!Allow` 可查找操作不是“允许”的所有事件。

步骤 3 执行搜索。

提示 您可以使用 **Ctrl+Enter** (Windows) 或 **Command-Enter** (Mac) 键盘命令启动搜索。

与其他事件查看器表不同，当显示的列都具有相同的值时，统一事件查看器中的事件不会聚合。与过滤条件匹配的每个事件都单独列出。

下一步做什么

要保存自定义过滤器，请参阅 [在统一事件查看器中保存搜索](#) 主题。

在统一事件查看器中保存搜索

开始之前

您必须具有 **管理员** 或 **安全分析师** 权限才能保存列集。

过程

步骤 1 选择 **分析 > 统一事件**。

步骤 2 按照 [统一事件查看器中的过滤器](#) 主题的过滤器中的说明建立搜索条件。

步骤 3 点击 **搜索** (🔍) 图标。

步骤 4 点击 **+保存搜索**。

步骤 5 指定搜索的名称，然后点击 **确定** (✓) 图标。

下一步做什么

要加载已保存的搜索，请参阅 [在统一事件查看器中加载保存的搜索](#) 主题。

在统一事件查看器中加载保存的搜索

开始之前

- 您必须具有 **管理员** 或 **安全分析师** 权限才能执行此任务。
- 按照 [在统一事件查看器中保存搜索](#) 主题的说明建立已保存搜索。

过程

步骤 1 选择 **分析 > 统一事件**。

步骤 2 点击搜索文本框上的 **搜索** (🔍) 图标，然后选择要加载的已保存搜索。

步骤 3 或者，点击 **打开已保存的搜索详细信息面板** 图标，然后选择已保存的搜索以查看所选搜索的过滤条件。点击 **应用搜索** 以加载搜索。

在统一事件查看器中保存列集

开始之前

您必须具有 **管理员** 或 **安全分析师** 权限才能保存列集。

过程

步骤 1 选择 **分析 > 统一事件**。

步骤 2 点击列选择器图标 (☰)，然后选择要保存的列集。

步骤 3 从 **已保存的列集** 下拉列表中，点击 **+ 从当前选择创建列集**。

步骤 4 指定列集的名称，然后点击 **确定** (✓) 图标。

下一步做什么

要加载已保存的列集，请参阅 [在统一事件查看器中加载已保存的列集](#) 主题。

在统一事件查看器中加载已保存的列集

开始之前

- 您必须具有 **管理员** 或 **安全分析师** 权限才能执行此任务。
- 保存收藏夹列集，如 [在统一事件查看器中保存列集](#) 主题中所述。

过程

步骤 1 选择 **分析 > 统一事件**。

步骤 2 点击列选择器图标 (☰)。

步骤 3 从 **已保存的列集** 下拉列表中，选择要加载的列集。

统一事件查看器列说明

某些字段中的值取决于事件类型。字段对应关系如下：

统一事件查看器字段名称	连接或安全情报事件字段名称	入侵事件字段名称	文件事件字段名称	恶意软件事件字段名称
时间	首个数据包 参见下文注意事项。	时间	时间	时间
活动类型	--	--	--	--
操作	操作	内联结果	操作	操作
原因	原因	原因	(不适用)	(不适用)
源 IP	发起方 IP	源 IP	发送 IP	发送 IP
目标 IP	响应方 IP	目标 IP	接收 IP	接收 IP
源端口/ICMP 类型	源端口	源端口	发送端口	发送端口
目标地端口/ICMP 代码	目的端口	目的端口	接收端口	接收端口

统一事件查看器字段名称	连接或安全情报事件字段名称	入侵事件字段名称	文件事件字段名称	恶意软件事件字段名称
Web 应用程序	Web 应用程序	Web 应用程序	Web 应用程序	Web 应用程序
规则	访问控制规则	访问控制规则	(不适用)	(不适用)
策略	访问控制策略	入侵策略	文件策略	文件策略
设备	设备	设备	设备	设备
NAT 源 IP	NAT 源 IP	(不适用)	(不适用)	(不适用)
NAT 目标 IP	NAT 目标 IP	(不适用)	(不适用)	(不适用)
NAT 源端口	NAT 源端口	(不适用)	(不适用)	(不适用)
NAT 目标端口	NAT 目标端口	(不适用)	(不适用)	(不适用)
MITRE	(不适用)	MITRE	MITRE	MITRE
规则组	(不适用)	规则组	(不适用)	(不适用)

有关字段说明，请参阅以下主题：

- [连接和 安全相关连接 事件字段](#)
- [入侵事件字段](#)
- [文件和恶意软件事件字段](#)

另请参阅[有关发起方/响应方，源/目标和发件人/接收方字段的说明](#)。



注释 即使您在连接开始时未启用日志记录，系统也会将此值用作统一事件查看器中的时间字段。要确定是否在连接开始和结束时记录了连接事件，请展开事件的行以查看详细信息。如果连接的两端均已记录，您会看到 **最后一个数据包** 字段。

统一事件的历史记录

特性	版本	详细信息
保存常用搜索	7.3	将列集和搜索保存为收藏项，稍后快速启动它们。
统一事件查看器	7.0	查看和处理具有多种事件类型的单个表：连接（包括安全情报）、入侵、文件和恶意软件。 新增/修改的页面： 分析 > 统一事件 下面的新页面。 支持的平台： 管理中心

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。