# FTD 控制面板



## 关于 FTD 控制面板

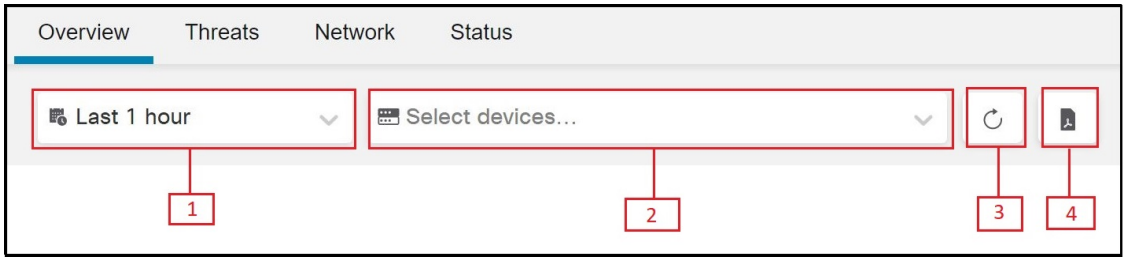
FTD 控制面板为您提供状态概览视图，包括所有 CDO 管理的威胁防御设备收集和生成的事件数据。

您可以使用此控制面板来查看与部署中的设备状态和整体运行状况相关的综合信息。FTD 控制面板提供的信息取决于您如何在系统中许可、配置和部署设备。虽然 FTD 控制面板会显示所有 CDO 管理的威胁防御设备的数据，但您也可以选择过滤基于设备的数据。您还可以选择时间范围以便显示特定时间范围内的数据。

此控制面板使用选项卡显示预定义构件：提供对系统的不同方面的见解的小型独立组件。例如，“网络活动”(Network Activity) 构件显示了事件图，其中可显示有关所有连接、恶意软件和入侵事件的信息。控制面板中的构件均已预定义且无法自定义。有权访问 CDO 租户的所有 CDO 用户均会看到此控制面板。

- 控制面板不会显示历史事件的任何事件统计信息。
- 由于汇聚服务批处理每五分钟进行一次汇聚，因此从事件汇聚到统计信息显示之间可能会存在五分钟的延迟。

**图 *1: FTD* 控制面板**



| 编号 | 说明 |
| --- | --- |
| 1 | 允许您更改时间范围以反映短至前一小时，或长至前一年的时间周期信息。当您更改时间范围时，构件会自动更新事件数据以反映新的时间范围。 |
| 2 | 允许您根据所选的设备来过滤事件数据。如果未选择任何设备，构件将显示所有可用的事件数据。 |
| 3 | 重新启动事件数据查询 |
| 4 | 以 PDF 输出格式显示事件数据。您可以选择在本地计算机上下载或保存此 PDF 的副本。 |

# 查看 FTD 控制面板

从 CDO 菜单中，选择 **分析 (Analytics)** > **FTD 控制面板 (FTD Dashboard)** 以查看 **FTD 控制面板 (FTD Dashboard)**。

默认情况下，租户的主页将显示**概述 (Overview)** 选项卡。

控制面板包括每个选项卡下列出的构件：“威胁”(Threat)、“网络”(Network)、“应用和用户”(Application and Users) 以及“状态”(Status) 选项卡。

下表列出了每个选项卡下的可用构件：

| 选项卡名称 | 可用构件 |
| --- | --- |
| 概述 | 所有可用构件 |
| 威胁 | • 排名靠前的入侵规则<br>• 排名靠前的入侵攻击者<br>• 排名靠前的入侵目标<br>• 排名靠前的恶意软件签名<br>• 排名靠前的恶意软件发件人<br>• 排名靠前的恶意软件接收者<br>• 按处理结果排列的恶意软件事件 |

| 选项卡名称 | 可用构件 |
| --- | --- |
| 网络 | • 网络活动<br>• 事件活动<br>• 访问控制操作<br>• 排名靠前的访问控制策略<br>• 排名靠前的访问控制规则<br>• 排名靠前的设备<br>• 排名靠前的用户 |
| 状态 | • 运行不正常的设备<br>• 排名靠前的已加载设备 |

# FTD 控制面板构件

FTD 控制面板会显示预定义的构件，它们可为您提供当前系统状态的概览视图。这些视图包括：

- 威胁防御 设备托管的 FMC 收集和生成的事件相关数据。
- 有关部署中的设备的状态和整体运行状况的信息。

## 排名靠前的入侵规则构件

**排名靠前的入侵规则构件 (Top Intrusion Rules)** 构件会显示在指定时间范围内发生的入侵事件计数，并按优先级进行组织。这些计数包括有丢弃数据包和不同影响的入侵事件的统计数据。生成的列表可滚动。

## 排名靠前的入侵攻击者构件

**排名靠前的入侵攻击者 (Top Intrusion Attackers)** 构件以条形图形式显示受监控网络中排名靠前的攻击性主机 IP 地址（导致这些事件的地址）的入侵事件的计数。

## 排名靠前的入侵目标构件

**排名靠前的入侵目标 (Top Intrusion Targets)** 构件以条形图形式显示受监控网络中排名靠前的目标主机 IP 地址（导致这些事件的连接中的目标）的入侵事件计数。

# 排名靠前的恶意软件签名构件

**排名靠前的恶意软件签名 (Top Malware Signatures)** 构件显示在网络流量中检测到的排名靠前的文件发送主机 IP 地址发出的恶意软件签名计数。

# 排名靠前的恶意软件发件人构件

**排名靠前的恶意软件发件人 (Top Malware Senders)** 构件显示在网络流量中检测到的排名靠前的文件发送主机 IP 地址发出的恶意软件威胁计数。

# 排名靠前的恶意软件接收者构件

**排名靠前的恶意软件接收者 (Top Malware Receivers)** 构件显示在网络流量中检测到的所有排名靠前的文件接收主机 IP 地址发出的恶意软件威胁计数。

# 按处理结果排列的恶意软件事件构件

**按处理结果排列的恶意软件事件 (Malware Events by Disposition)** 构件显示托管设备检测到包含恶意软件的文件时生成的所有恶意软件事件处置情况的计数。

# 网络活动构件

**网络活动 (Network Activity)** 构件显示基于连接事件信息的所有入口和出口数据速率。

# 事件活动构件

**事件活动 (Event Activity)** 构件显示最近一小时内发生的事件计数以及数据库中可用的每种事件类型的总数。

# 访问控制操作构件

**访问控制操作 (Access Control Actions)** 构件可显示基于每个事件允许或阻止的访问控制操作记录的事件计数。如果将光标悬停在饼形图上，则可以查看允许和阻止的操作百分比。

# 排名靠前的访问控制策略构件

**排名靠前的访问控制策略 (Top Access Control Policies)** 构件会显示生成事件的排名靠前的访问控制策略的计数。

## 排名靠前的访问控制规则构件

**排名靠前的访问控制规则 (Top Access Control Rules)** 构件显示用于每个事件的访问控制规则的前五个计数。这些计数可以按字节数或事件数排序。

## 排名靠前的设备构件

**排名靠前的设备 (Top Devices)** 构件显示每台设备的事件计数。这些计数可以按字节数或事件数排序。

## 排名靠前的用户构件

**排名靠前的用户 (Top Users)** 构件会显示与最高入侵事件计数关联的受监控网络上的用户。它主要从入侵检测 (IDS) 的“用户统计数据”(User Statistics) 和“入侵事件”(Intrusion Events) 表提取数据。它显示授权的用户数据。

## 运行状况不佳的设备构件

**运行不正常的设备 (Unhealthy Devices)** 构件显示 CDO 管理的威胁防御设备的当前编译运行状况。

## 排名靠前的已加载设备构件

**排名靠前的已加载设备构件 (Top Loaded Devices)** 构件显示威胁防御设备列表以及 CPU 使用情况信息。

# 修改 FTD 控制面板的时间设置

您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。当您更改时间范围时，可按时间限制构件自动更新以反映新的时间范围。

任何图形中的最大数据点数为 300，时间设置确定在每个数据点内汇总的时间。以下是每个时间范围的 FTD 控制面板中的数据点数量和覆盖的时间范围：

- 1 小时 = 12 个数据点，每个数据点 5 分钟
- 6 小时 = 72 个数据点，每个数据点 5 分钟
- 1 天 = 288 个数据点，每个数据点 5 分钟
- 1 周 = 300 个数据点，每个数据点 33.6 分钟
- 2 周 = 300 个数据点，每个数据点 67.2 分钟
- 30 天 = 300 个数据点，每个数据点 144 分钟
- 90 天 = 300 个数据点，每个数据点 432 分钟

- 180 天 = 300 个数据点，每个数据点 864 分钟
- 1 年 = 300 个数据点，每个数据点 1752 分钟

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。