



## 查找

---

以下主题介绍如何查找关于 Firepower 系统可能了解或可能不了解的实体的信息：

- [介绍查找，第 1 页](#)
- [执行 Whois 查找，第 1 页](#)
- [查找 URL 类别和信誉，第 2 页](#)
- [查找 IP 地址的地理位置信息，第 3 页](#)

## 介绍查找

如果您的管理中心已连接到互联网，则可以使用手动查找功能查找以下信息：

- 任何 IP 地址的区域信息注册表 (RIR) 信息 (whois)。
- URL 类别和信誉通过 URL 过滤功能分类。
- 任何 IP 地址的地理位置信息：国家/地区名称、国家/地区代码和大洲名称。（为了确保您使用的是最新的地理位置信息，思科强烈建议您定期更新管理中心上的地理位置数据库 (GeoDB)。

## 执行 Whois 查找

### 开始之前

- 确保管理中心能够访问互联网；请参阅[安全、互联网接入和通信端口](#)。

### 过程

---

**步骤 1** 选择分析 > 高级 > **Whois**。

**步骤 2** 输入 IP 地址，然后点击**搜索**。

---

# 查找 URL 类别和信誉

您可以手动查找 URL 的类别和信誉。使用此功能可以了解如何评估特定的 URL，以便计划、调整或解决策略处理问题，或者调查通过思科解决方案之外的源引起您注意的可能有问题的 URL。这些结果中的类别和声望与 URL 过滤功能使用的类型和信誉相同。

## 开始之前

- 管理中心必须具有 Internet 访问权限；请参阅[安全、互联网接入和通信端口](#)。
- 必须启用 URL 过滤和向思科云查询未知 URL 选项。请参阅《[Cisco Secure Firewall Management Center 设备配置指南](#)》中的 URL 过滤一章。
- 必须至少有一个设备注册到管理中心，并且为其分配了有效的 URL 过滤许可证。
- 您必须是管理员或安全分析师用户才能执行此任务。

## 过程

---

**步骤 1** 选择分析 > 高级 > URL。

**步骤 2** 以任何通用格式输入多达 250 个 URL 和公共可路由的 IP 地址（例如，URL 可以包含或不包含“http”、“www”，可以是子域，也可以缩短）。用空格或回车分隔每个输入项。

不支持星号 (\*) 这类通配符。

**步骤 3** 点击 Search。

如果输入了很多 URL，并且网络速度很慢，处理可能需要几分钟的时间。

如果看到 URL 无效的错误信息，请检查拼写或尝试不同的 URL 形式。例如，添加或省略“www”或“http(s)”前缀。

一个 URL 可能属于多达六类别，但只有一个声誉。

**步骤 4**（可选）通过点击列标题对结果进行排序。

**步骤 5**（可选）要将结果保存为 CSV 文件，请点击导出 CSV。

CSV 文件中包含一个用于名誉级别的附加列，因此您可以按风险排序。对于系统风险数据不足的 URL，零 (0) 表示未知风险。

---

## 下一步做什么

如果要查看可能的类别和信誉列表，请转到策略 (Policies) > 访问控制 (Access Control) > 访问控制 (Access Control)，点击策略或添加新的策略，点击添加规则 (Add Rule)，然后点击 URL。

# 查找 IP 地址的地理位置信息

可以使用地理位置查找功能来查找国家/地区名称、ISO 3166-1 三位数字的国家/地区代码，以及与任何 IP 地址相关联的大陆名称。

## 过程

---

**步骤 1** 选择分析 > 高级 > 地理位置。

**步骤 2** 要查看一个或多个 IP 地址的地理位置信息，请输入该地址或这些地址，然后点击**搜索**。可以指定 IPv4 地址、IPv6 地址，或者二者。使用逗号、分号、回车或任何空格字符来分隔多个地址。

**提示** 点击**清除**以清除文本框。

**步骤 3** 或者，可以点击列标题对数据进行排序。可按除“IP 地址”外的任何字段进行排序。

**步骤 4** （可选）要将结果另存为 CSV 文件，请点击**导出 CSV**。

---



## 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。