paloalto TECHDOCS

IoT Security 管理员指南

February 2024

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

February 14, 2024

Table of Contents

IoT Security 解决方案 9

IoT Security 解决方案结构 10

1 - 设备数据收集 11

2 - 数据分析 11

3 - IoT 设备保护 12

4 - 第三方集成 12

5 - 使用 Prisma Access 代替新一代防火墙 13

IoT Security 解决方案设置 15

1 - 检查防火墙支持和先决条件 15

2 - 加入 IoT Security 16

3 - 准备防火墙 17

4 - 安装证书和许可证 18

5 - 配置日志记录 18

IoT Security 文档 20

IoT Security 文档集 20

一些有用的学习资源 21

IoT Security 入门 23

IoT Security 的防火墙和 PAN-OS 支持 24

IoT Security 先决条件 25

加入 IoT Security 27

在 VM-Series 上使用软件 NGFW 积分上线 IoT Security 34

部署防火墙以实现设备可见性 42

按流量类型收集 DHCP 数据 42

IoT Security 的防火墙部署选项 43

使用 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙 45

为本地 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙 51

使用 Tap 接口实现 DHCP 可见性 53

使用虚拟线路接口实现 DHCP 可见性 54

使用 SNMP 网络发现从交换机了解设备 56

使用 ERSPAN 通过 GRE 隧道发送镜像流量 59

使用 DHCP 服务器配置提高设备可见性 68

当防火墙服务于 DHCP 时规划扩展 71

为 IoT Security 准备好您的防火墙 73

配置日志转发策略 89

控制加入设备的允许流量 91

支持隔离网段 93

配置 IT 安全遥测网关 94
配置 OT 安全遥测网关 96
配置 OT 防火墙 99
IoT Security 与 Prisma Access 集成 102
IoT Security 许可证 105
撤销 IoT Security 订阅 107
停用防火墙和传输许可证 107
CSP 帐户之间的传输防火墙 111
让 IoT Security 订阅过期 111
IoT Security 概述 113
IoT Security 简介 114
IoT Security 与新一代防火墙集成 116
IoT Security 门户 121
垂直主题门户 129
门户主题 129
切换门户主题 137
创建试用 Enterprise IoT Security 租户 138
设备到站点映射 142
基于 IP 地址的站点分配 142
基于防火墙的站点分配 144
将站点分配从防火墙更改为 IP 地址 145
站点和站点组 147
将网站分组 148
网络 156
网络可视化 166
创建可视化地图 166
在可视化地图中查看数据 168
报告 171
配置报告 171
查看报告 173
编辑、复制和禁用报告 178
IoT Security 与防火墙的集成状态 181
具有 Prisma Access 的 IoT Security 集成状态 188
数据质量诊断 190
授权按需 PCAP 191
IoT Security 与第三方产品的集成 192
IoT Security 和 FedRAMP 193
发现 IoT 设备并创建清单 195

IoT 设备发现 196
IoT Security 设备页面 197
IoT Security 设备详细信息页面 204
创建多接口设备 227
具有静态 IP 地址的设备 238
上传静态 IP 设备列表 238
添加静态 IP 设备配置 239
上传只有静态 IP 地址的子网列表 242
添加只有静态 IP 地址的子网 244
IP 端点 245
发现移动设备属性 249
将 IoT Security 设置为发送 PAN-OS 移动设备属性 249
在 IoT Security 中查看移动设备属性 254
自定义属性 256
创建自定义属性并自动应用 256
手动将自定义属性值应用于设备 257
按自定义属性查看设备 258
编辑自定义属性并将其从设备中删除 260
标签管理 261
创建自定义标记并自动应用 262
手动将标记应用于一个或多个设备 262
手动将标记应用于单个设备 266
从设备中删除标记 267

了解 IoT 设备应用 269

IoT 设备应用发现 270

检测 IoT 设备漏洞 277

IoT 设备漏洞检测 278
漏洞概述指示板 279
漏洞页面 285
漏洞详细信息页面 290
IoT 风险评估 297
设备风险 297
设备配置文件风险 300
站点风险 300
组织风险 301
风险评分和严重性 302
调整设备风险评分 302
风险评分变化警报 303

解决风险 304

回应 IoT Security 警报 305

安全警报概述 306
创建警报规则 316
了解安全警报 323
安全警报及系统警报通知 324
根据安全警报采取行动 325
常规安全警报管理 329

推荐安全策略 331

策略规则建议 332
设备配置文件概述 335
设备配置文件行为 339
过滤显示的内容 341
创建策略集 346
查看桑基图 346
查看行为表 349
设备配置文件策略 356
在 IoT Security 中创建策略集 362
将策略集导入 Panorama 371
限制网络访问权限 372

Medical IoT 387

生物医学指示板 388
医疗资产 390
合规风险 391
利用率指示板 393
利用率指示板过滤器 396
使用信息面板 399
MDS2 406
MDS2 社区 412
召回 418

管理 IoT Security 用户 421

创建 IoT Security 用户 422
使用 Palo Alto Networks SSO 对用户进行身份验证并管理 Hub 中的用户角色 422
使用 Active Directory SSO 验证用户并管理 Active Directory 中的用户角色 424

使用任何 SSO 对用户进行身份验证，并在 IoT Security 门户中管理用户角色 428
IoT Security 的用户角色 432

IoT Security 解决方案

这里介绍了构成 IoT Security 解决方案的架构组件。了解各种组件、它们如何协同工作以及如何设置它们。还可以了解为 IoT Security 提供的所有可用教育资源。

- IoT Security 解决方案结构
- IoT Security 解决方案设置
- IoT Security 文档

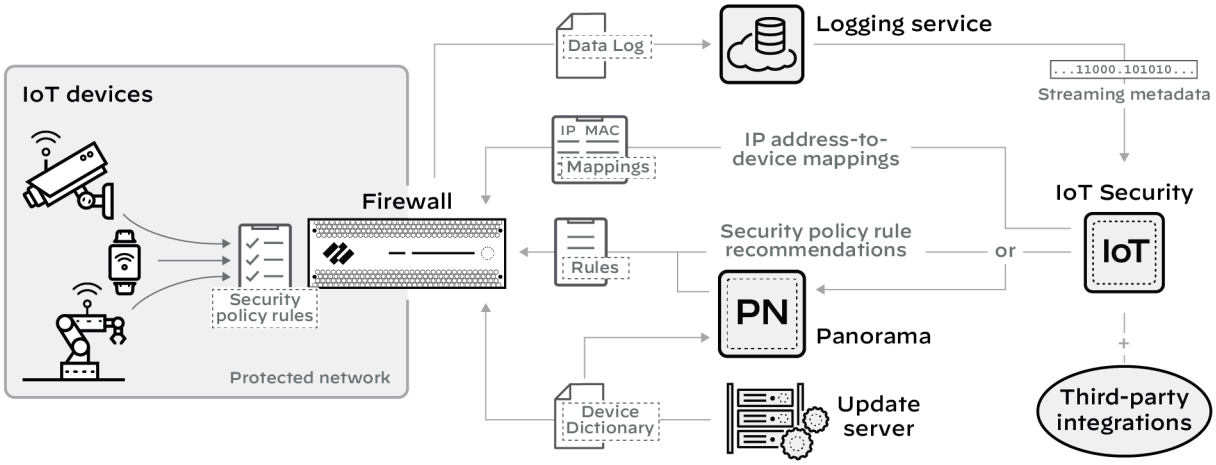
IoT Security 解决方案结构

利用人工智能和机器学习，IoT Security 自动发现和识别所有网络连接的设备并构建数据丰富、动态更新的清单。除了识别 IoT 设备和 IT 设备（例如笔记本电脑和服务器）之外，IoT Security 深入了解网络行为，确定正常行为并辨别可疑行为。当检测到设备漏洞或构成威胁的异常行为时，IoT Security 会通知管理员，而管理员则可以采取行动调查并解决问题。

为了实现这一切，基于云的 IoT Security 应用可与 Palo Alto Networks 新一代防火墙、日志记录服务和更新服务器配合使用，也可选择与 Panorama 和集成的第三方产品配合使用。IoT Security 解决方案的这些元素相互协作以完成以下任务：

- 具有 IoT Security 订阅的防火墙收集有关网络流量的信息，并将其日志转发到日志记录服务，日志记录服务将元数据传输到 IoT Security 来进行分析。
- 更新服务器为防火墙和 Panorama 提供定期更新的设备字典文件，其中包含安全策略规则用于识别设备或 *Device-ID* 的设备属性（配置文件、供应商、类别等）。
- IoT Security 向防火墙推荐基于 Device-ID 的安全策略规则。当 Panorama 提供集中防火墙管理时，IoT Security 通过它向管理防火墙推荐安全策略规则。不使用 Panorama 功能时，IoT Security 直接与防火墙交互。
- IoT Security 将 IP 地址映射到设备并通知防火墙其相应的设备属性，以便它们可以执行引用 IP 地址到设备映射中的属性的基于 Device-ID 的安全策略规则。

为 IoT Security 帐户使用第三方集成附加许可证时，您可以扩展 IoT Security 功能，以便包括产品特定的功能以及包含 IoT 的集成产品功能。



了解构成 IoT Security 解决方案的主要组件：

1 - 设备数据收集

2 - 数据分析

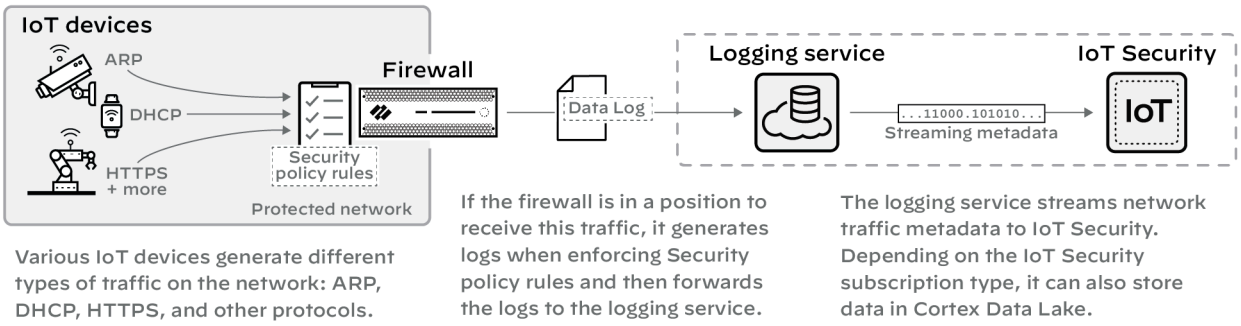
3 - IoT 设备保护

4 - 第三方集成

5 - 使用 Prisma Access 代替新一代防火墙

1 - 设备数据收集

为了让 IoT Security 识别 IoT 设备并建立可接受的网络行为基线，需要分析其网络活动。这就是新一代防火墙的作用所在。它们记录应用安全策略规则的网络流量，然后将日志转发到日志记录服务，以便 IoT Security 访问它们。根据您的 IoT Security 订阅是否包括数据存储，日志记录服务可以将元数据传输到您的 IoT Security 帐户和 Strata Logging Service 例如或只是您的 IoT Security 帐户。



详细说明

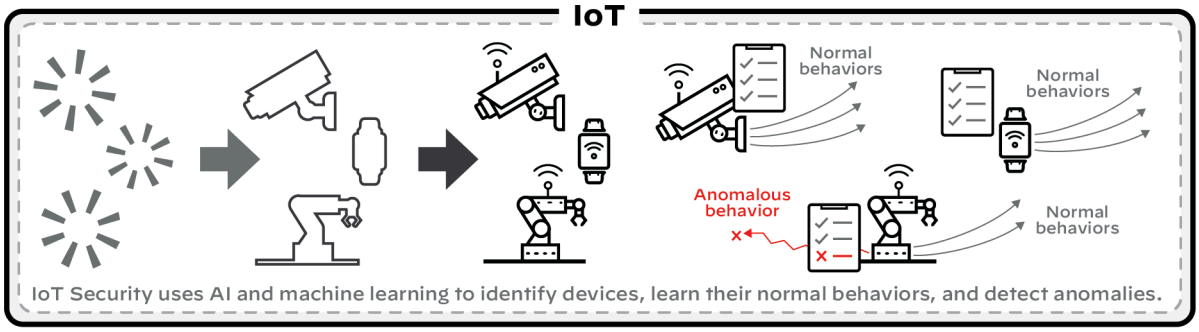
加入 IoT Security

为 IoT Security 准备好您的防火墙

2 - 数据分析

IoT Security 使用人工智能和机器学习算法来分析设备网络行为的众多方面，并将其分为三个级别或层级。从最广泛的层面来看，IoT Security 识别行为相似性，使其算法能够将设备分配给某个设备类别，例如安全相机，即使它还不知道确切的供应商和型号。在下一层，IoT Security 收集某些供应商和型号的安全摄像机共享的更细粒度的行为属性，以为其分配设备配置文件。在第三层，算法为该单个安全相机创建独特行为的模型，例如其使用模式。

除了设备识别之外，IoT Security 将专有和补充机器学习技术应用于威胁检测。它会自动检测设备漏洞并通知 IoT Security 管理员。它还可以检测表明攻击或侦察的异常网络行为并生成安全警报。



详细说明

IoT Security 简介

发现 IoT 设备并创建清单

检测 IoT 设备漏洞

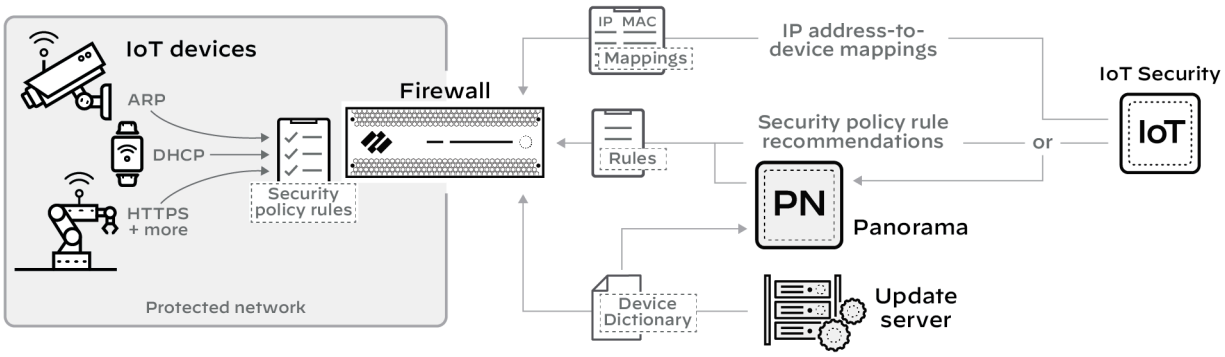
回应 IoT Security 警报

3 - IoT 设备保护

IoT Security 与新一代防火墙协调，为 IoT 设备流量推荐安全策略规则。在识别设备并建立可接受的网络行为基线后，IoT Security 根据观察到的网络行为自动为设备配置文件生成推荐的安全策略规则。然后，Panorama 或防火墙管理员将建议导入 Panorama 或直接导入防火墙，然后决定将哪些建议添加到他们的策略集中。

防火墙和 Panorama 必须具有基于 Device-ID 的安全策略规则的设备配置文件或其他设备属性列表。此列表由更新服务器以设备字典文件的形式提供，防火墙和 Panorama 会定期检查此列表以获取需要下载的更新。

为了让防火墙适当地应用导入的基于 Device-ID 的规则，IoT Security 不断向防火墙发送 IP 地址到设备的映射，其中包括受 IoT Security 监控和保护的所有设备的配置文件和其他属性。



IoT Security 还与 Prisma Access 集成以识别和保护设备。

详细说明

IoT Security 与新一代防火墙集成

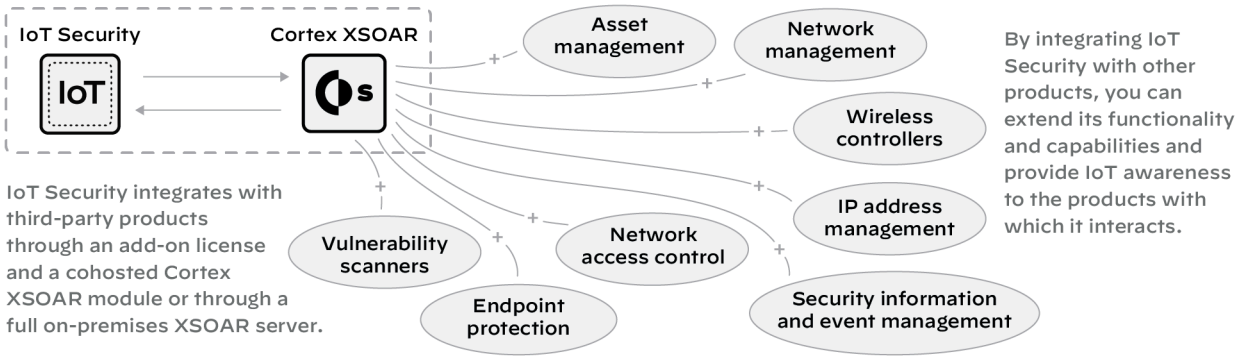
推荐安全策略

4 - 第三方集成

除了通过与新一代防火墙配合保护 IoT 设备之外，IoT Security 还可以与第三方产品集成以执行以下操作：

- 增加设备清单并丰富设备上下文 — 有时是为了 IoT Security有时是为了集成第三方产品
- 扩大集成产品中特定功能的覆盖范围，以包含 IoT
- 扩展 IoT Security 的能力；例如，通过集成，您可以进行漏洞扫描、隔离存在关键漏洞或安全警报的设备，并将访问控制列表 (ACL) 应用于 IoT 设备

IoT Security 通过第三方集成附加组件与其他产品集成，该附加组件基于 Cortex XSOAR 模块。

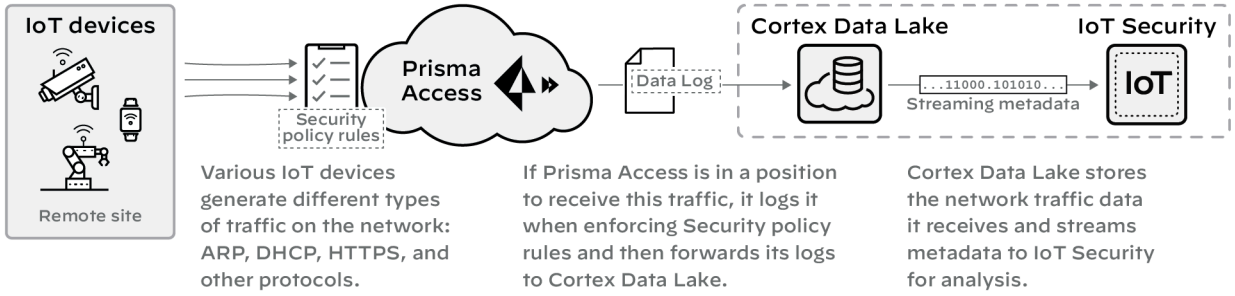


详细说明

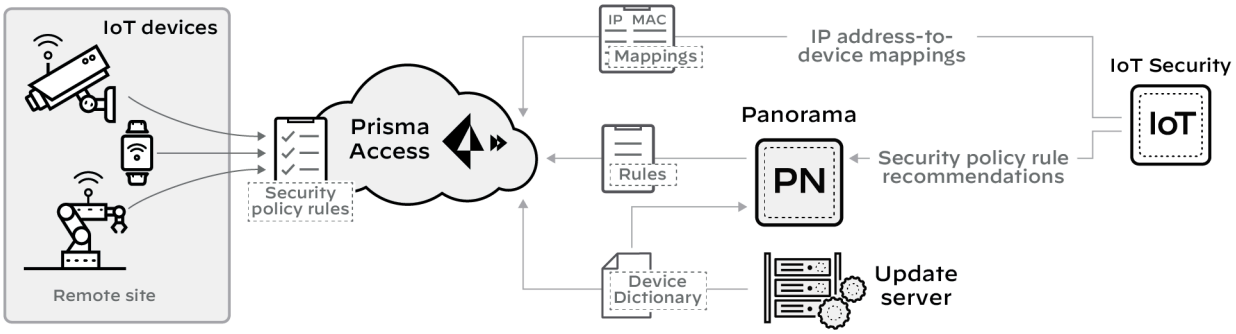
IoT Security 集成指南

5 - 使用 Prisma Access 代替新一代防火墙

将 IoT Security 与 Prisma Access 一起使用时，收集设备数据的过程与前述数据收集过程类似，只是使用 Prisma Access 代替了防火墙。此外，IoT Security 可以与 Prisma SD-WAN ION 设备协调在分支站点收集数据。当 Prisma Access 和 SD-WAN 将数据日志转发到日志记录服务时，必须使用 Strata Logging Service。



IoT Security 通过 Panorama 将安全策略规则建议发送到 Prisma Access。它将 IP 地址到设备的映射直接发送到 Prisma Access。同样，更新服务器将设备字典更新直接发送到 Prisma Access 以及 Panorama。



详细说明

Prisma Access

IoT Security 与 Prisma Access 集成

具有 Prisma Access 的 IoT Security 集成状态
Strata Logging Service
Prisma SD-WAN

IoT Security 解决方案设置

以下是设置 IoT Security 解决方案的主要步骤概述，重点介绍以下三个组成部分：

- 带或不带 Panorama 管理的 Palo Alto Networks 新一代防火墙
- 有或没有 Strata Logging Service 实例的日志记录服务
- IoT Security 应用程序

该解决方案还利用更新服务器进行设备字典文件更新，并利用客户支持门户和 Hub 进行IoT Security用户管理。可选地，IoT Security 与 Prisma Access 和 SD-WAN 集成，并通过 XSOAR 与第三方产品集成。

了解 IoT Security 解决方案设置中涉及的主要步骤：

1 - 检查防火墙支持和先决条件

2 - 加入 IoT Security

3 - 准备防火墙

4 - 安装证书和许可证

5 - 配置日志记录

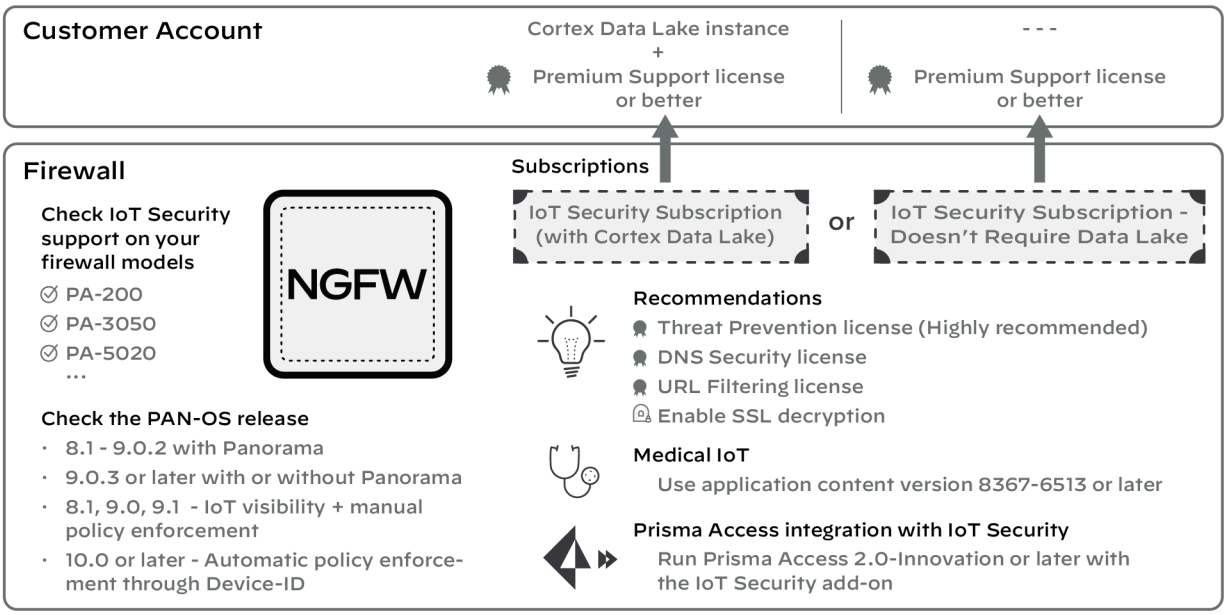
1 - 检查防火墙支持和先决条件

目前，除了少数例外情况，大多数 Palo Alto Networks 防火墙型号都支持 IoT Security，而根据 PAN-OS 版本的不同，功能程度也有所不同：

- PAN-OS 8.1、PAN-OS 9.0 和 PAN-OS 9.1：设备可见性和手动配置的安全策略实施
- PAN-OS 10.0 或更高版本：通过 Device-ID 实现设备可见性和自动安全策略实施

虽然 IoT Security 是一个云应用程序，并且始终运行其最新软件版本，请确保防火墙型号及其上的 PAN-OS 版本支持您想要的功能级别。

此外，还有几个先决条件。例如，每个与 IoT Security 集成的防火墙都必须有一个 IoT Security 订阅。并非网络上的所有防火墙都必须订阅 IoT Security；只有收集网络流量并向其转发日志的设备，以及在 PAN-OS 10.0 之后从其接收策略规则建议和 IP 地址到设备映射的设备。



详细说明

IoT Security 的防火墙和 PAN-OS 支持

IoT Security 先决条件

Medical IoT

IoT Security 与 Prisma Access 集成

2 - 加入 IoT Security

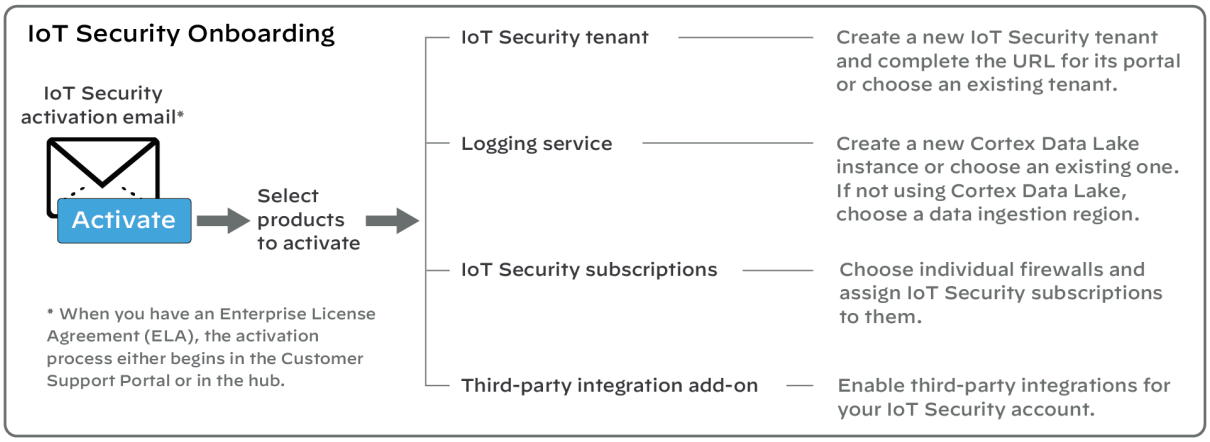
IoT Security 加入流程分为六个步骤，从来自 Palo Alto Networks 的电子邮件中的 **Activate**（激活）链接开始。（如果您有 Enterprise 版许可协议，它将从客户支持门户或中心启动）。在 IoT Security 加入流程中，根据您要激活的内容执行以下操作：

- 创建 IoT Security 租户
- （IoT Security 订阅）激活新的 Strata Logging Service 实例，或者将现有实例与您的 IoT Security 租户

  或

  （IoT Security 订阅 - 不需要数据湖）指定数据提取区域相关联
- 为防火墙订阅 IoT Security 服务

- 可选择激活第三方集成附加组件

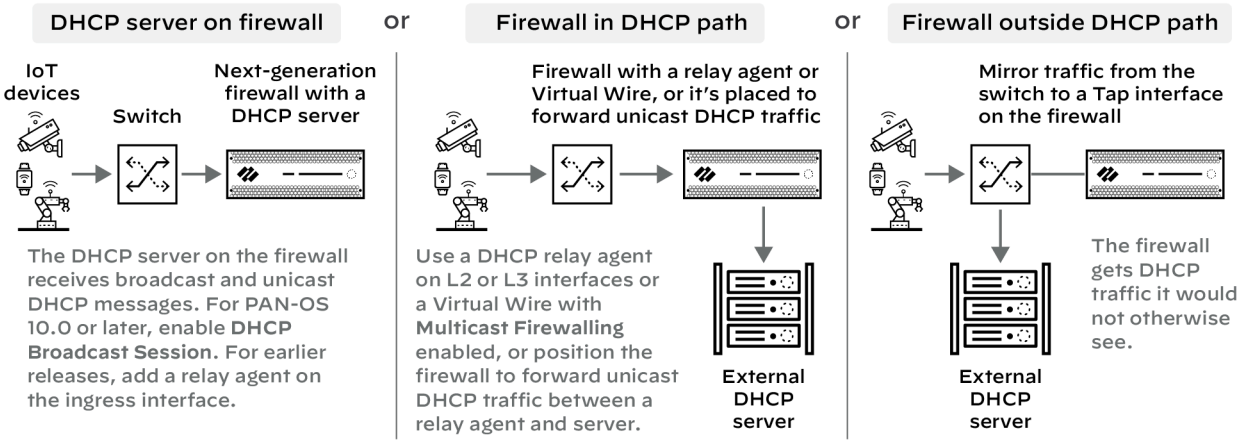


详细说明

加入 IoT Security

3 - 准备防火墙

为了让 IoT Security 发现网络连接的设备并评估其网络行为模式，它需要来自新一代防火墙的高质量网络元数据。因此，必须在网络上安装防火墙，并配置为从流量中收集元数据，并进行转发以便 IoT Security 访问。特别是，DHCP 流量很重要，因为它将动态分配的 IP 地址链接到设备 MAC 地址，使它们可以随时间推移进行跟踪。



防火墙还必须提供 IoT Security 以及设备生成的其他类型流量的元数据。它们通过对网络流量实施策略、创建日志，然后将其转发到日志记录服务来实现这一点，日志记录服务随后将元数据传输到 IoT Security。

详细说明

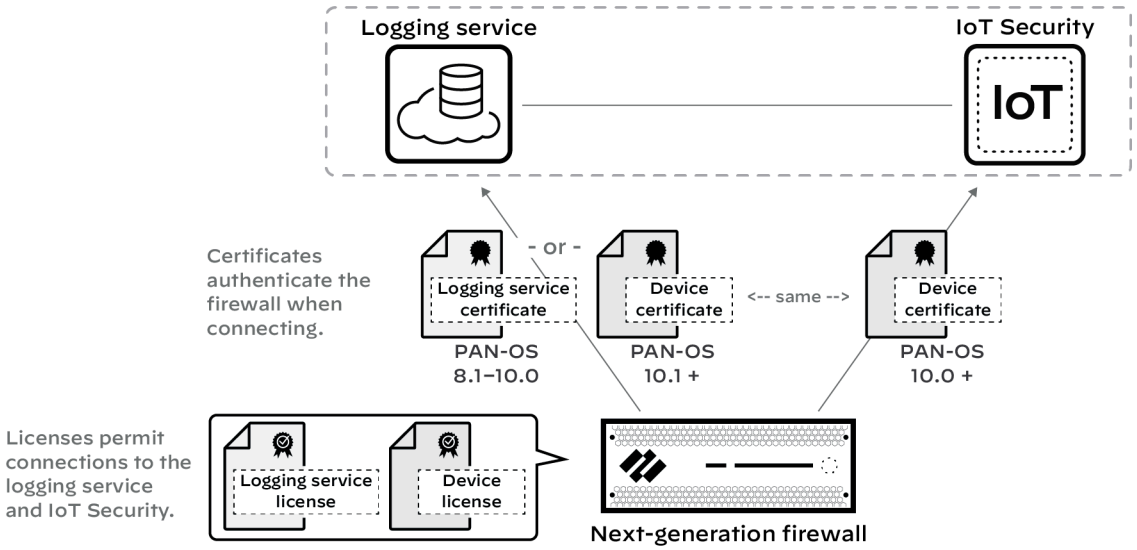
部署防火墙以实现设备可见性

按流量类型收集 DHCP 数据

IoT Security 的防火墙部署选项

4 - 安装证书和许可证

日志记录服务和设备许可证允许新一代防火墙连接到日志记录服务和 IoT Security。日志记录服务和设备证书对这些连接进行验证。防火墙需要这些许可证和证书才能集成 IoT Security。



运行 PAN-OS 8.1–10.0 的防火墙使用日志记录服务证书来保护与日志记录服务的通信，以便它们可以将各种日志转发给它。从 PAN-OS 10.0 开始，当引入 Device-ID 时，防火墙使用设备证书来保护与 IoT Security 的通信，以便获取 IP 地址到设备的映射和推荐的策略规则。（注意：Panorama 管理的防火墙可以通过 Panorama直接从 IoT Security 或间接从 IoT Security 获取建议的策略规则。）从 PAN-OS 10.1 开始，防火墙仅使用一个设备证书来保护与日志记录服务和 IoT Security 的连接。Panorama 还使用设备证书来保护与 IoT Security 的通信。

详细说明

加入 IoT Security

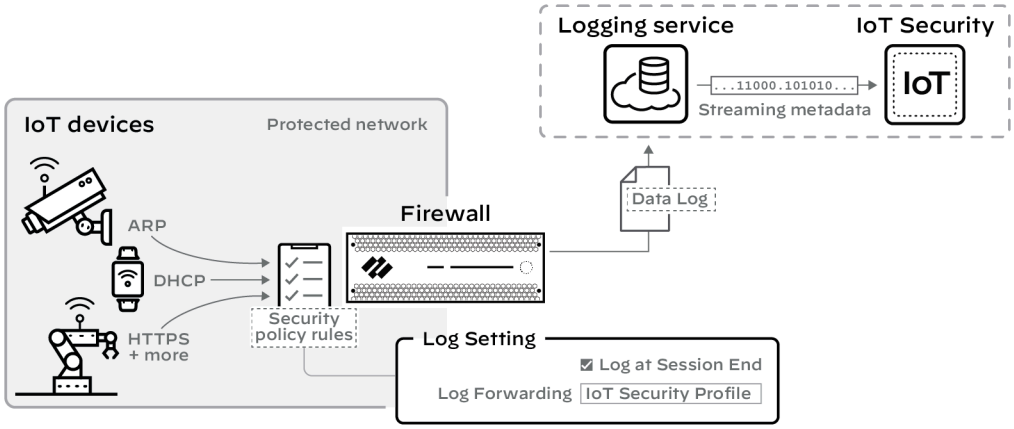
为 IoT Security 准备好您的防火墙

安装设备证书

安装 Panorama 设备证书

5 - 配置日志记录

在防火墙上配置安全策略规则，以记录流量并将日志转发到日志记录服务，并通过 IoT Security 进行访问。网络流量元数据越多，IoT Security 的分析能力越强，它也能越快、越自信地识别设备并建立其正常网络行为的基线。这样，基于 Device-ID 的安全策略规则就能得到更广泛的应用（仅当防火墙对设备身份有很高的信心并且设备在过去一小时内发送或接收了流量时，IoT Security 才向防火墙发送 IP 地址到设备的映射），对设备风险以及真实和潜在的安全威胁也能获得更广泛和更深入的洞察。



详细说明

为 IoT Security 准备好您的防火墙

配置日志转发策略

IoT Security 与防火墙的集成状态

IoT Security 文档

了解可用的 IoT Security 技术文档和培训。

IoT Security 文档集

Palo Alto Networks 技术文档门户中的以下一组技术文档构成了 IoT Security 的主要文档。

IoT Security 最佳实践	本参考推荐了以下主要部署阶段的 IoT Security 最佳实践：
	使用最佳实践规划 IoT Security 部署
	使用最佳实践部署 IoT Security
	使用最佳实践监控 IoT Security 部署
IoT Security 管理员指南	管理员指南介绍了 IoT Security 功能，并解释了如何配置和使用它们。一些章节是关于管理 IoT Security 应用程序的：
	IoT Security 解决方案
	IoT Security 入门
	IoT Security 概述
	管理 IoT Security 用户
	其他章节说明了如何处理与设备和安全相关的数据：
	发现 IoT 设备并创建清单
	了解 IoT 设备应用
	检测 IoT 设备漏洞
	回应 IoT Security 警报
	推荐安全策略
	Medical IoT
IoT Security 集成指南	本指南介绍如何通过 Cortex XSOAR 将 IoT Security 与第三方产品集成。该指南为每个集

	成的双方提供了配置说明。IoT Security 支持与以下类型的系统集成：
	资产管理
	端点保护
	网络管理
	无线网络控制器
	安全信息和事件管理
	网络访问控制
	漏洞扫描
IoT Security API 参考	本参考提供了 IoT Security API 的解释和示例，分为两部分：常用参数和单个 API 请求和响应。

一些有用的学习资源

Palo Alto Networks 还提供以下资源来了解 IoT Security。

PAN-OS 管理员指南中的 Device-ID	PAN-OS 文档描述了 Device-ID 的工作原理，如何为其部署做准备以及如何对其进行配置和管理。它还包括用于故障排除的有用的 CLI 命令。
IoT Security 部署设计指南	本文档介绍了 IoT Security 的典型部署场景和建议。
保护 IoT 环境：参考架构指南	本指南适用于解决方案架构师和工程师，为部署 IoT Security 解决方案提供架构指导。
IoT Security 隐私声明	隐私声明包含有关 IoT Security 解决方案如何捕获、处理和存储信息的信息。
IoT Security 网页	Palo Alto Networks 网站上的此页面概述了 IoT Security 产品和各种材料，例如简报、数据表、报告和案例研究。
知识库文章	几篇文章回答了有关 IoT Security 及其工作原理的常见问题。
每月发布说明	发行说明每月总结新功能和增强功能、外观和行为的变化以及已知和已解决的问题。单

	击右下角的“帮助”(**?**) 图标，并选择 **Product Release**（产品发布），即可在 IoT Security 门户中找到它们。
IoT Security 数字在线培训	该培训课程使您能够介绍 IoT Security 的基础知识，对其进行配置，并准备好防火墙和日志记录服务，使其成为 IoT Security 解决方案的一部分。

IoT Security 入门

了解如何加入 IoT Security 应用，以及如何准备要与 IoT Security 一起使用的防火墙。

- IoT Security 的防火墙和 PAN-OS 支持
- IoT Security 先决条件
- 加入 IoT Security
- 在 VM-Series 上使用软件 NGFW 积分上线 IoT Security
- 部署防火墙以实现设备可见性
- 按流量类型收集 DHCP 数据
- IoT Security 的防火墙部署选项
- 使用 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙
- 为本地 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙
- 使用 Tap 接口实现 DHCP 可见性
- 使用虚拟线路接口实现 DHCP 可见性
- 使用 SNMP 网络发现从交换机了解设备
- 使用 ERSPAN 通过 GRE 隧道发送镜像流量
- 使用 DHCP 服务器配置提高设备可见性
- 当防火墙服务于 DHCP 时规划扩展
- 为 IoT Security 准备好您的防火墙
- 配置日志转发策略
- 控制加入设备的允许流量
- 支持隔离网段
- IoT Security 与 Prisma Access 集成
- IoT Security 许可证
- 撤销 IoT Security 订阅

IoT Security 的防火墙和 PAN-OS 支持

对于运行 PAN-OS 8.1、PAN-OS 9.0 或 PAN-OS 9.1 的 Palo Alto Networks 新一代防火墙，IoT Security 解决方案可根据从防火墙收到的日志提供已发现 IoT 设备的可见性。IoT Security 还使用机器学习 (ML) 来识别漏洞，并根据设备的网络流量行为和动态更新的威胁源评估设备中的风险。虽然这些 PAN-OS 版本不支持通过 Device-ID™ 框架（从 PAN-OS 10.0 开始提供）自动实施 IoT 设备的策略，但您仍然可以在手动向防火墙添加规则时使用 IoT Security 生成的策略规则建议作为参考。无论 PAN-OS 版本如何，IoT Security 始终会生成安全策略规则建议。

运行 PAN-OS 10.0 或更高版本的防火墙通过 Device-ID 自动实施策略。这是一种通过设备类型、供应商、型号或操作系统等属性识别设备，然后将基于设备的策略规则应用于具有匹配属性的设备的机制。

运行 PAN-OS 10.0 或更高版本的所有 Palo Alto Networks 新一代防火墙均完全支持 IoT Security，但以下情况除外。

IoT 设备可见性和策略建议的手动应用（不包括 Device-ID）

- 多虚拟系统 (multi-vsys) 防火墙
- 搭载 PAN-OS 8.1 的 PA-200
- 搭载 PAN-OS 8.1 的 PA-500
- 搭载 PAN-OS 8.1、PAN-OS 9.0 或 PAN-OS 9.1 的 PA-3020
- 搭载 PAN-OS 8.1、PAN-OS 9.0 或 PAN-OS 9.1 的 PA-3050
- 搭载 PAN-OS 8.1、PAN-OS 9.0 或 PAN-OS 9.1 的 PA-3060
- 搭载 PAN-OS 8.1 的 PA-5020
- 搭载 PAN-OS 8.1 的 PA-5050
- 搭载 PAN-OS 8.1 的 PA-5060

无 IoT Security 支持

- PAN-OS 11.1 之前的 CN-Series 防火墙
- VM-50
- VM-200

在选择订阅 IoT Security 服务的防火墙时，请考虑它们支持的 IoT Security 功能类型。需要考虑的另一个因素是各种防火墙型号何时会终止销售和服务支持，以及您何时计划将其更新为较新的型号。但是，即使您为防火墙订阅了 IoT Security，然后在其 IoT Security 许可证有效期还未结束时决定将其退役，您也可以将许可证从该防火墙转移到另一个防火墙，IoT Security 将在后者上继续运行直至订阅期结束。

IoT Security 先决条件

对于 Palo Alto Networks 新一代防火墙，确保您的环境满足部署 IoT Security 的所有先决条件：

- 一个或多个运行 PAN-OS 8.1 至 PAN-OS 9.0.2（具有 Panorama 管理）的防火墙，或者运行 PAN-OS 9.0.3 或更高版本（具有或不具有 Panorama 管理）的防火墙。

  运行 PAN-OS 8.1、PAN-OS 9.0 和 PAN-OS 9.1 的防火墙支持 IoT Security 用于设备可见性和手动策略实施。运行 PAN-OS 10.0 或更高版本的防火墙支持 IoT Security 实现设备可见性和通过 Device-ID 自动实施策略。
- 每个防火墙一个 IoT Security 许可证。

  许可证控制 IoT Security 是否获取防火墙转发到 Palo Alto Networks 基于云的日志记录服务的日志数据，以识别 IoT 设备并评估风险。许可证还控制防火墙是否可以从 IoT Security 拉取 IP 地址到设备映射和策略规则建议，并从更新服务器获取设备字典以用于其安全策略规则。

  （关于 IP 地址到设备映射的说明：IoT Security 使用专利的多层机器学习算法来分析设备行为并识别设备类型、品牌、型号、操作系统和操作系统版本。它将这组属性捆绑成一个逻辑对象，将其映射到设备的 IP 地址，并将其发送到防火墙。这个对象被称为 IP 地址到设备的映射。）

  购买 IoT Security 订阅后，您有 90 天的宽限期来在防火墙上激活许可证。如果您在前 90 天内激活，则订阅从激活日期开始。否则，它将从购买日期后 90 天开始。

  Panorama 管理服务器不需要 IoT Security 许可证。
- 使用 IoT Security 订阅将数据存储在 Strata Logging Service 时，您的每个帐户必须有一个 Strata Logging Service 许可证。（使用 IoT Security 时，不需要数据湖订阅，您也不需要 Strata Logging Service 许可证。）

  您的 Strata Logging Service 订阅可以是新的也可以是现有的，数据湖可以位于美洲、欧盟或亚太地区。无论使用数据湖与否，防火墙都会自动、连续地将日志数据传输到 IoT Security 基础设施中，数据会根据数据类型保留不同时间。有关数据保留的详细信息，请参阅 IoT/OT 安全隐私。

  对于新的 Strata Logging Service 实例，请使用 Cortex 大小计算器计算出您需要的存储量。在进行计算时，请输入具有 IoT Security 许可证的防火墙数量并选择 IoT Security。
- 使用日志记录服务需要高级支持许可证或更高级别许可证。对于 IoT Security 的两种订阅类型，当使用日志记录服务时，这是必需的：IoT Security 订阅和 IoT Security 订阅 — 不需要数据湖。（购买 Strata Logging Service 实例时自动包含高级支持许可证。）
- 要让 IoT Security 获取全面评估风险和检测漏洞所需的所有流量和威胁日志，需要威胁预防许可证。
- 以下许可证和防火墙功能为 IoT Security 提供额外的价值：
  - DNS 安全许可证可帮助 IoT Security 检测与 DNS 相关的威胁和风险。
  - Wildfire 许可证增强了对恶意软件和文件相关漏洞的检测。
  - URL 过滤许可证控制设备可以访问的在线内容以及如何与其交互。
  - 在防火墙上启用 SSL 解密，提高设备识别的覆盖率和准确性。它还可以通过风险评估和威胁检测帮助 IoT Security。

- 在具有医疗设备的网络上使用 IoT Security 时，请确保防火墙上的应用程序内容版本为 8367-6513 或更高版本；也就是说，主版本（由前四位数字标识）为 8367 或更高版本（8368、8369、8370 等），从 8367-6513 开始。这些版本包括医疗保健专用应用程序，允许 IoT Security 发现医疗设备并提供使用数据。他们还允许防火墙安全策略规则包含医疗保健特定的应用程序。
- 将 IoT Security 与 Prisma Access 集成时，Prisma Access 必须运行具有 IoT Security 附加组件的 Prisma Access 2.0-Innovation 版本或更高版本。要了解其他要求，请参阅IoT Security 与 Prisma Access 集成。
- 当 Panorama 管理运行 PAN-OS 10.2 的防火墙时，它需要 3.1 云服务附加组件。

加入 IoT Security

按照加入工作流程为您的 IoT Security 门户创建 URL 并激活防火墙的 IoT Security 订阅。通过加入流程，您可以选择激活 Strata Logging Service 实例来存储数据和 IoT Security 的第三方集成附加组件以扩大其能力。

重要的是保留您从 Palo Alto Networks 收到的 IoT Security 激活电子邮件。它不仅包含机密的激活相关数据，而且如果在完成加入流程后，您还有未使用的 IoT Security 许可证，则可以稍后再次单击电子邮件中的 **Activate**（激活）按钮以重复该过程，从而激活更多防火墙。

（Enterprise 版许可协议）如果您有 Enterprise 版许可协议 (ELA)，请在您的客户支持门户帐户中输入 Palo Alto Networks 发送的授权码，开始激活过程。有关完整的分步说明，请参阅通过通用服务激活附加组件 Enterprise 版许可协议。

当您有 IoT Security 订阅后，加入流程包括以下主要步骤。

STEP 1 | 在来自 Palo Alto Networks 的 IoT Security 激活电子邮件中单击 **Activate**（激活）。

STEP 2 | 登录 Palo Alto Networks Hub。

STEP 3 | 激活 IoT Security。

STEP 4 | 对于防火墙，将设备（防火墙）添加到租户服务组 (TSG) 并关联 IoT Security，可能还有其他应用程序。

STEP 5 | （可选）管理身份和对 IoT Security 的访问权限。

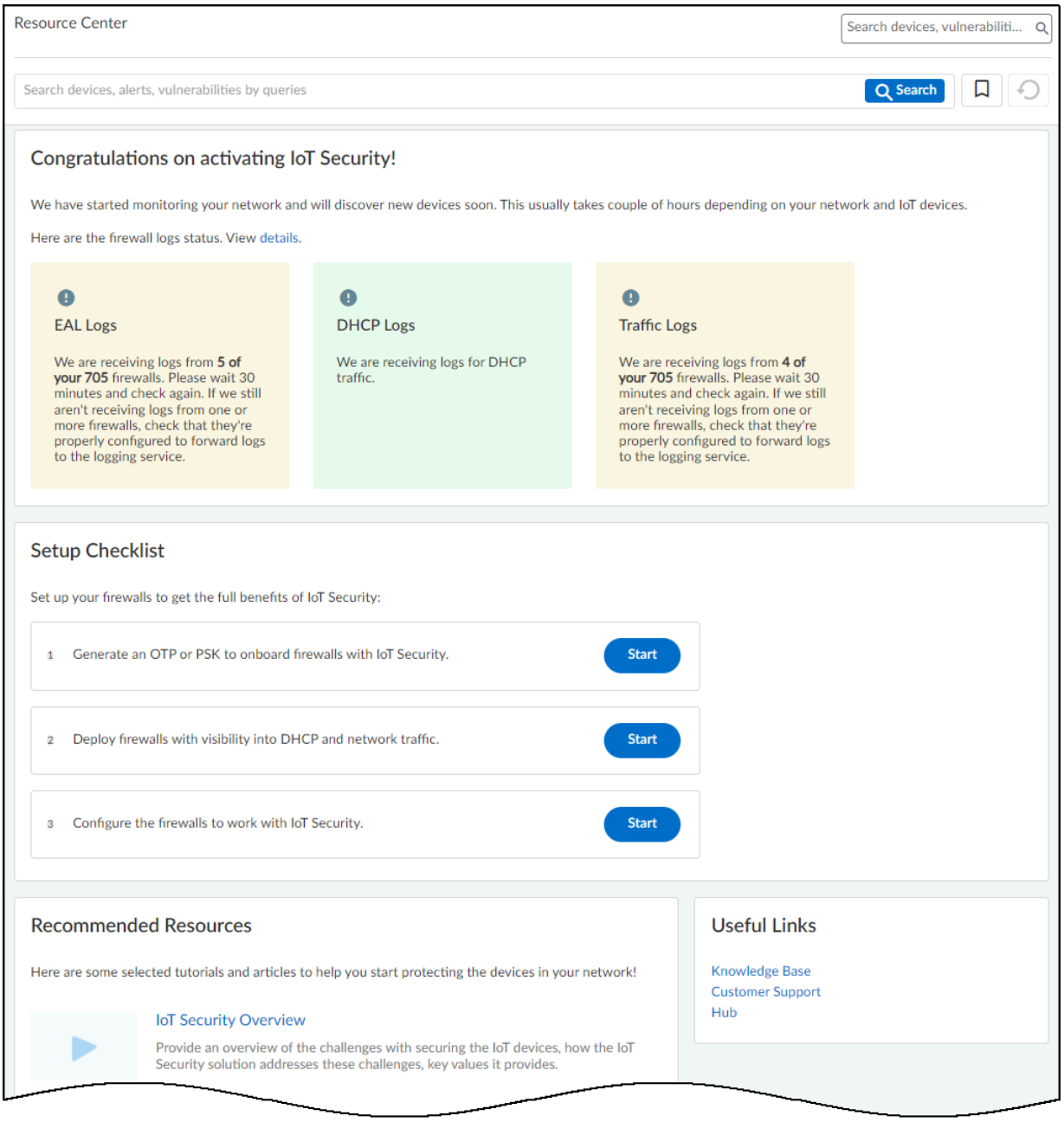
STEP 6 | 将 IoT Security 和防火墙设置为配合工作。

有关前六个步骤的说明，请参阅常见服务：订阅和租户管理。然后返回此处继续设置。

STEP 7 | 登录 IoT Security 门户。

单击租户管理或设备关联页面上的 **IoT Security** 链接。

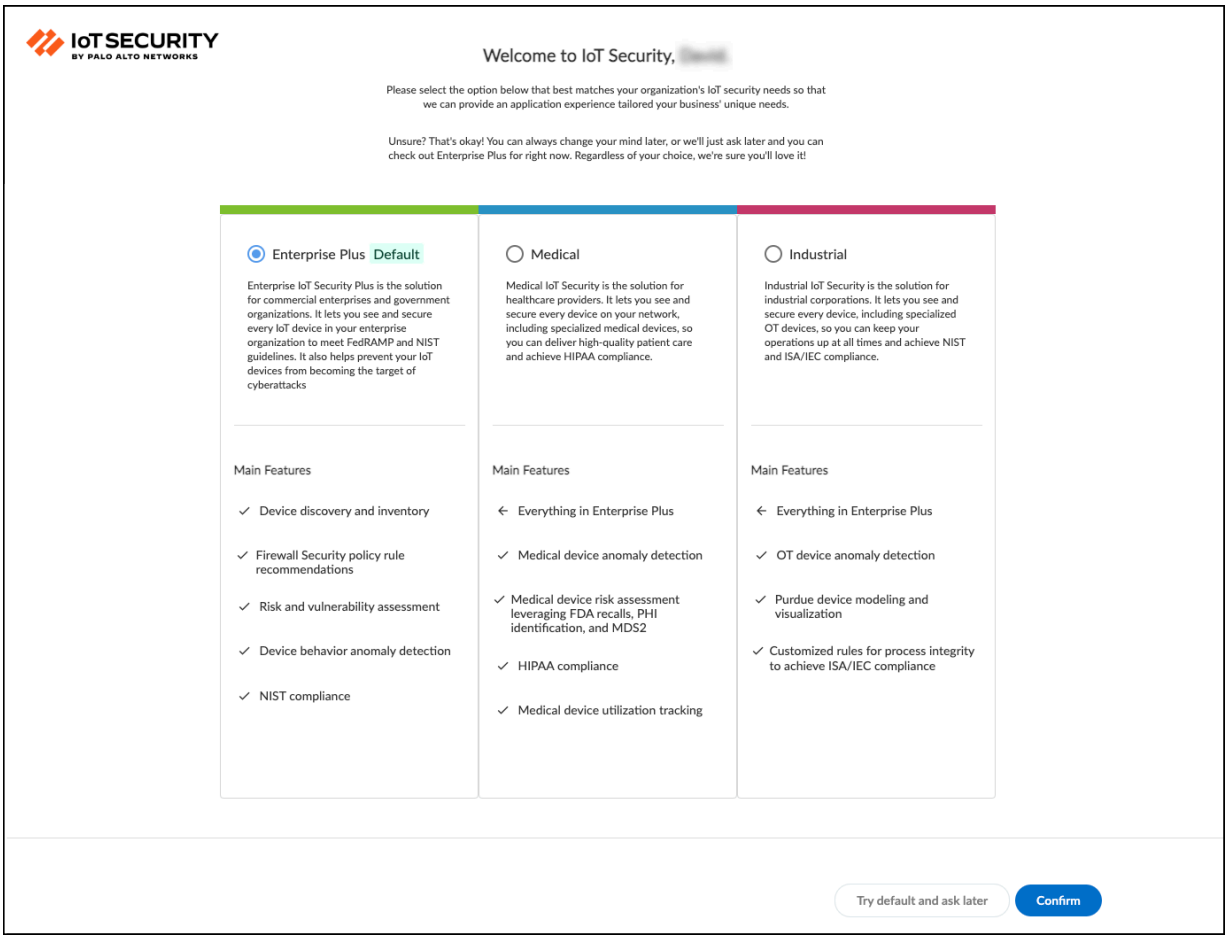
随即出现一个欢迎页面，显示日志记录服务的状态和几个有用的学习资源链接。



STEP 8 | 要访问其余的 Web 界面，请使用左侧的导航菜单。

如果您是具有所有者权限的用户，并且门户没有预定的垂直主题，当您尝试离开欢迎页面时，IoT Security 将提示您选择一个主题：Enterprise IoT Security Plus，还有 Industrial OT 安全或 Medical IoT Security。如果您不选择主题，默认会使用 Enterprise IoT Security Plus 主

题。IoT Security 每次登录时都会继续提示您选择主题，直到您做出选择，或者另一个具有所有者权限的用户做出选择。



如果您是没有所有者权限的用户，并且所有者尚未选择垂直主题，在默认情况下，您将看到 Enterprise IoT Security Plus 主题。否则，如果门户主题已经由 IoT Security 购买的产品或所有者已经设置了主题，那么您看到的主题就是该主题。

您首次登录时门户中可能没有任何数据。防火墙创建网络流量数据日志并将其转发到日志记录服务，日志记录服务再将其传输到 IoT Security 云。平均而言，设备平均只需 30 分钟就会出现在 IoT Security 门户上。根据网络的大小和网络上设备的活动量，所有数据可能需要几天时间才能显示出来。

单击 ***Administration***（管理）> ***Sites and Firewalls***（站点和防火墙）> ***Firewalls***（防火墙）*IoT Security* 门户，以查看日志记录服务正在流式传输到 *IoT Security* 应用的的日志状态。有关更多信息，请参阅 IoT Security 与防火墙的集成状态

在 IoT Security 门户有时间使用其机器学习算法来分析 IoT 设备的网络行为（1-2 天）之后，考虑遵循 IoT Security 用户的典型工作流程：

- 设备可见性 — 了解网络上的 IoT 设备
- 应用程序可见性 — 了解这些设备使用的应用程序和协议
- 设备漏洞 — 了解 IoT 设备漏洞并采取措施缓解这些漏洞，首先是针对最关键的设备，然后再针对其他设备
- 安全警报 — 在安全警报发生时做出响应，根据警报的紧急程度以及目标设备或网络段的重要性确定响应的优先顺序
- 安全策略规则建议 — 根据观察到的网络行为，IoT Security 应用可以生成推荐的安全策略规则，然后您可以将其与新一代防火墙上的规则同步。

根据防火墙上运行的 PAN-OS 版本，您必须生成 OTP 或 PSK 并在防火墙上安装证书，以便它们可以安全地与日志记录服务以及 IoT Security 进行连接。还需要防火墙配置才能启用 IoT Security 的日志记录和日志转发。对于 Enterprise IoT Security Plus、Industrial OT Security 和 Medical IoT Security，您还必须配置 IoT Security 和 PAN-OS，以便应用 Device-ID 来执行安全策略规则。要继续，请参阅为 IoT Security 准备好您的防火墙。

在 VM-Series 上使用软件 NGFW 积分上线 IoT Security

Palo Alto Networks VM-Series 是 Palo Alto Networks 新一代防火墙的虚拟化形式，旨在用于虚拟化或云环境。当您使用 软件 NGFW 积分来为使用固定或灵活的虚拟 CPU (vCPU) 的 VM-Series 付费时，您可以在防火墙注册过程中将 IoT Security 包括在部署配置文件中。

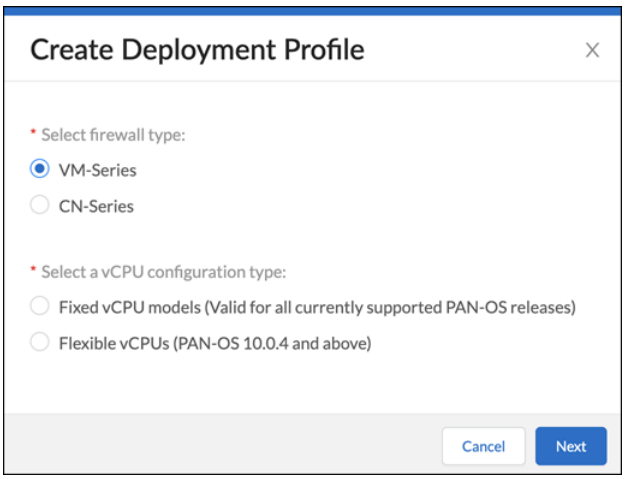
您还可以使用软件 *NGFW* 积分来为具有 *IoT Security* 订阅的 *CN-Series* 付费，只要防火墙在 *Panorama* 管理之下。对于具有 *IoT Security* 的 *CN-Series* 加入说明，请参阅 CN-Series 的 IoT Security 支持。

以下加入流程适用于具有 IoT Security 的 VM-Series 订阅。假设您已经购买了软件 NGFW 积分且已激活它们。此时，您可以使用软件 NGFW 积分购买 VM-Series。

STEP 1 | 为 VM-Series 创建一个或多个部署配置文件。

为您想要部署的每种类型的 VM-Series 模型创建部署配置文件。

1. 登录 客户支持门户 (CSP)，如果您有多个帐户，请选择您想要使用的帐户。
2. 选择 **Products**（产品） > **Software NGFW Credits**（软件 **NGFW** 积分）以查看软件 NGFW 积分指示板。
3. 在指示板上找到您购买的 NGFW 积分池并 **Create Deployment Profile**（创建部署配置文件）。



4. 选择 **VM Series** 和 **Fixed vCPU models (Valid for all currently supported PAN-OS releases)** [固定 **vCPU** 模型（适用于所有当前支持的 **PAN-OS** 版本）] 或 **Flexible vCPUs (PAN-OS**

10.0.4 and above)[灵活 **vCPU**（**PAN-OS 10.0.4** 及以上版本）**]**，然后单击 **Next**（下一步）。

5. 假设您选择 **Fixed vCPU models (Valid for all currently supported PAN-OS releases) [**固定 **vCPU** 模型（适用于所有当前支持的 **PAN-OS** 版本）**]**，请配置以下内容，然后 **Create Deployment Profile**（创建部署配置文件）：

   Profile Name（配置文件名称）：输入部署配置文件的名称。

   Number of Firewalls（防火墙数量）：输入可与此部署配置文件关联的防火墙的最大数量。

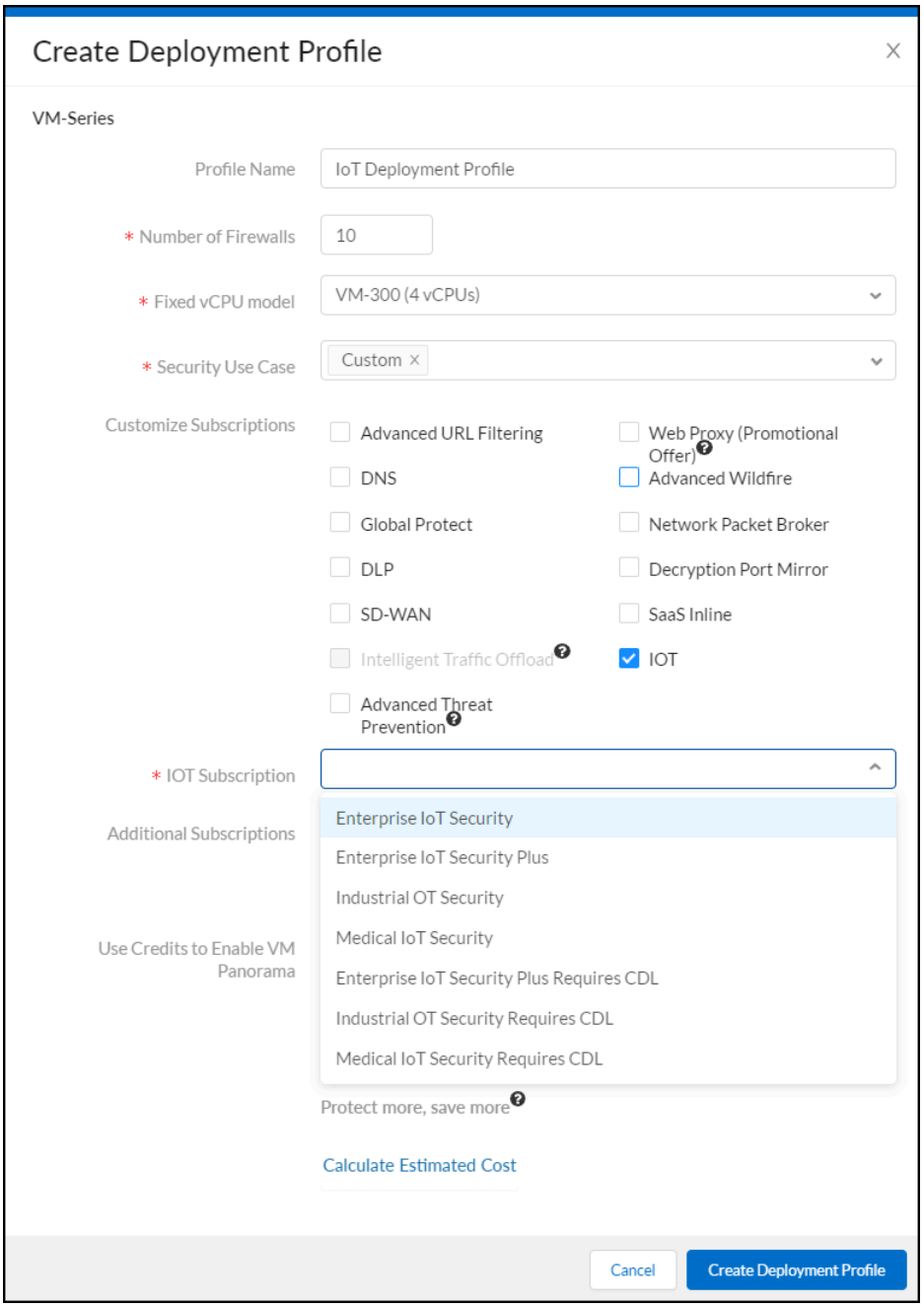
   Fixed vCPU model（固定 **vCPU** 模型）：从列表中选择一个 VM-Series 模型。

   Security Use Case（安全用例）：选择 **Custom**（自定义）。

   Customize Subscriptions（自定义订阅）：清除所有预选项目并选择 **IOT**。

   IOT Subscription（**IOT** 订阅）：在 VM-Series 上选择要激活的 IoT Security 订阅类型。不同类型基于在 Strata Logging Service 中有或没有 流量日志保留的 垂直主题。

   Use Credits to Enable VM Panorama（使用积分启用 **VM Panorama**）：（全部清除）



创建部署配置文件后，它将出现在 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分）页面上的当前部署配置文件表中。

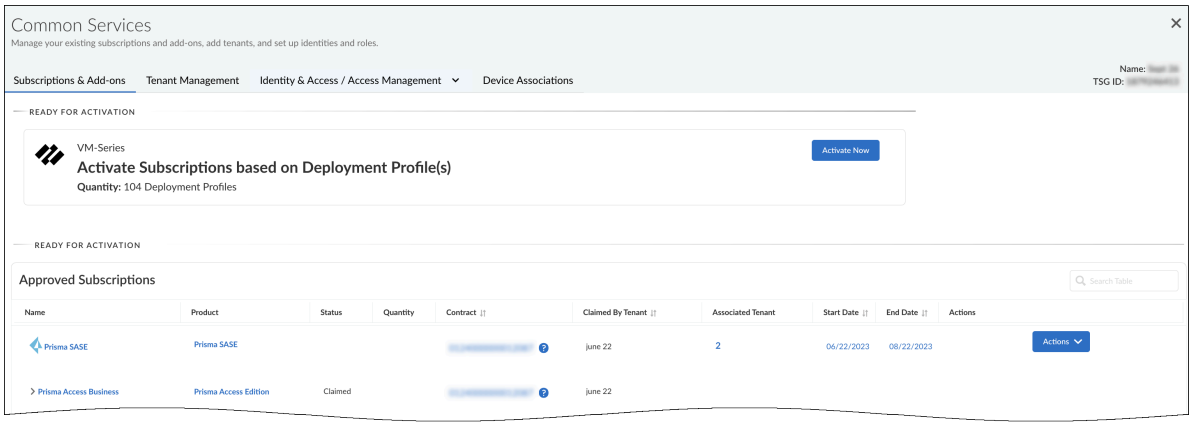
6. （可选）单击 **Create Deployment Profile**（创建部署配置文件**0**后，您可以返回配置并单击 **Calculate Estimated Cost**（计算估计成本），以查看将从您的帐户中扣除多少 **Flex** 积分以及剩余余额的估算值。如果将光标悬停在估算旁边的问号上，您可以看到每个组件的信用细目。
7. 如果您要部署其他类型的防火墙模型，请为每种类型创建一个额外的部署配置文件。

STEP 2 | 根据公共服务中的部署配置文件激活 IoT Security 订阅。

1. 使用您的 Palo Alto Networks 客户支持凭证登录 Hub。

   Hub 从 CSP 获取此帐户的可用部署配置文件。
2. 选择 **Common Services**（常用服务） > **Subscriptions & Add-ons**（订阅和附加组件）。

   您创建的部署配置文件将显示在页面顶部的“准备激活”部分。



3. 单击 **Activate Now**（立即激活）。

   随即显示“根据部署配置文件激活订阅”页面。

4. 配置以下内容 IoT Security 订阅激活设置：

   Customer Support Account（客户支持帐户）：选择具有部署配置文件的 CSP 帐户。

   Recipient（收件人）：使用现有租户或创建一个新租户。

   > 要创建新租户，请将光标悬停在“选择租户”下拉列表顶部的 ***All Tenants***（所有租户）上，然后单击右侧出现的 ***Add***（添加）图标 ***(+)***。输入租户服务组 ***(TSG)*** 的唯一名称并选择一个垂直业务。

   Select Region（选择区域）：当激活不需要订阅 Strata Logging Service 的 IoT Security 时，选择日志记录服务将提取网络流量日志的区域，VM-Series 会将这些流量日志发送到 IoT Security 来进行访问和分析。

   当激活确实需要 Strata Logging Service 的 IoT Security 订阅时，您必须先在同一租户服务组 (TSG) 中拥有已激活的 Strata Logging Service 实例。然后，IoT Security 将默认使用该实例。TSG 可能已有另一个已激活 Strata Logging Service（例如 PA+CDL 或 AIOps+CDL）的产品，或者，在激活 IoT Security 订阅之前，您可能已将激活的独立 Strata Logging Service 实例迁移到 TSG。无论哪种情况，区域都会根据 TSG 中现有数据湖的区域自动填充。

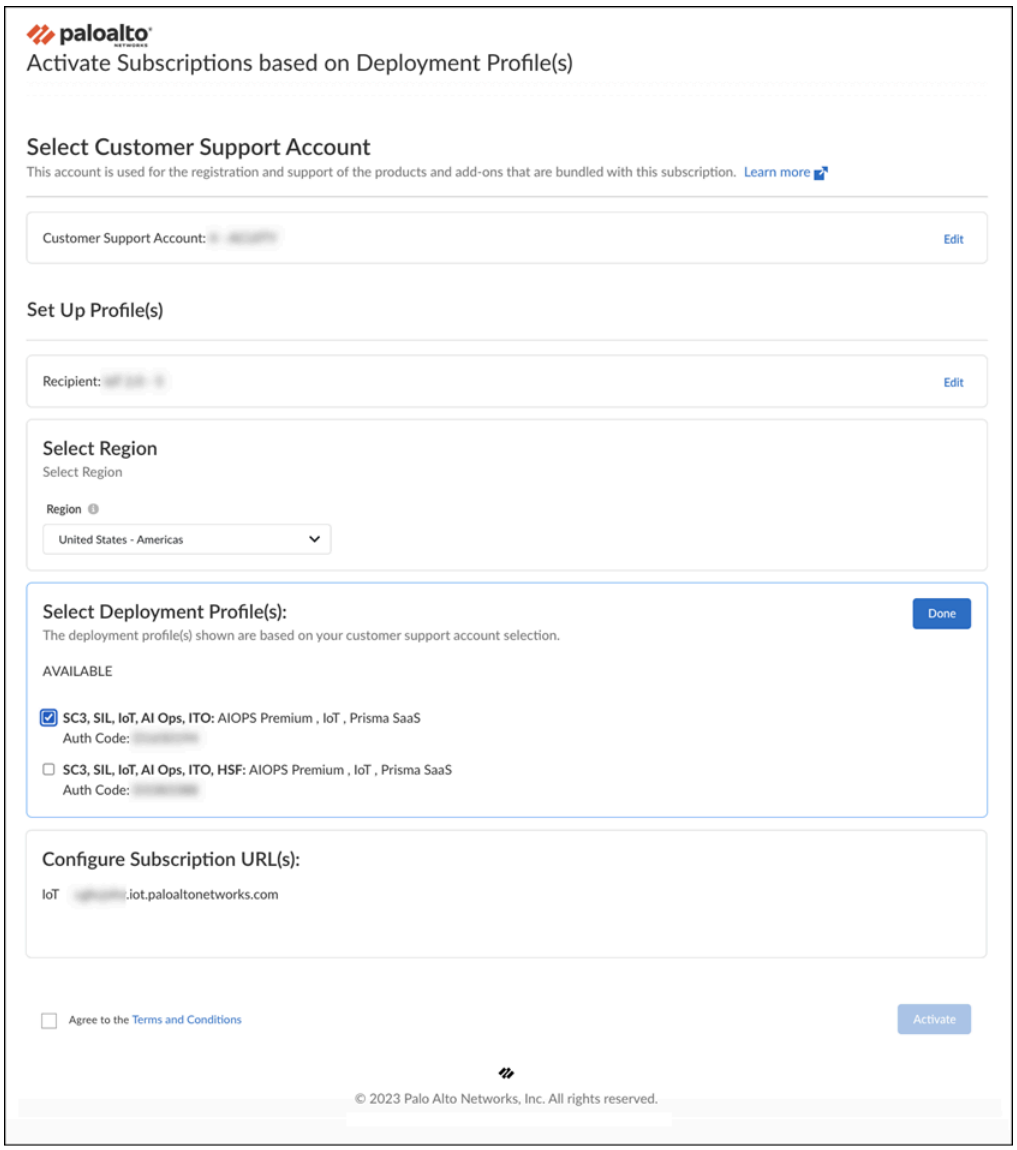
   选择部署配置文件：选择您之前创建的部署配置文件。

   部署配置文件有两个部分：**Available**（可用）和 **Unavailable**（不可用）。如果缺少必需的组件，部署配置文件将出现在“不可用”部分。例如，如果部署配置文件中的 IoT Security 订阅需要 Strata Logging Service但租户服务组 (TSG) 没有该配置文件，则部署配置文件将位

于“不可用”部分。在这种情况下，在尝试激活 IoT Security 之前，您需要激活所需的 Strata Logging Service。

当您创建多个部署配置文件时，它们可能具有不同的 *IoT Security* 订阅。在同一个 *IoT* 租户中使用它们时，第一个部署配置文件中的 *IoT Security* 订阅类型优先于之后添加的其他订阅类型。

配置订阅 **URL**：为您的 IoT Security 应用程序输入唯一的子域名以补全 <subdomain>.iot.paloaltonetworks.com URL。这将是您登录 IoT Security 门户的 URL。



5. **Agree to the Terms and Conditions**（同意条款和条件），然后 **Activate**（激活）。

   Hub 显示租户管理页面，您可以在其中看到 IoT Security TSG 的初始化状态。初始化通常需要几分钟才能完成。

STEP 3 | 通过部署配置文件将防火墙与 IoT Security TSG 中的订阅相关联。

1. 按照注册 VM-Series软件 NGFW 积分）中介绍的两种方法之一注册 VM-Series，然后 **Submit**（提交）注册。

   注册无法访问 *CSP* 的 *VM-Series* 时，您必须输入 *UUID*、*CPU ID*、防火墙上的 *vCPU* 数量以及分配给防火墙的内存量。此信息位于防火墙 *Web* 界面 ***Dashboard***（指示板）页面的常规信息部分。您可以从该部分复制它，并将其粘贴到注册防火墙表单中。通过选择 ***Device***（设备）**>** ***Licenses***（许可证）**>** ***Activate Feature using Auth Code***（使用授权代码激活功能）**>** ***Download Authorization File***（下载授权文件），您还可以将此信息从防火墙 *Web* 界面下载到文本文件中。然后在 *CSP* 中的注册防火墙页面上，***Upload a File for UUID & CPUID***（上传 ***UUID*** 和 ***CPUID*** 的文件）。

   提交防火墙注册后，CSP 会通过部署配置文件将此防火墙与 TSG 关联起来。注册和关联通常需要几分钟才能完成。完成后，您可以在 Hub 的 **Common Services**（常用服务）> **Device Associations**（设备关联）选项卡上看到防火墙。

   在防火墙注册期间，将自动从您的积分池中扣除为虚拟防火墙付费所需的软件 NGFW 积分额度。

2. 通过相同的部署配置文件将更多防火墙关联到 TSG，或者，如果它们是不同类型的防火墙模型，则通过为它们创建的其他部署配置文件关联。

   目前无法延长、续订或退出已在由软件 *NGFW* 积分付费的 *VM-Series* 上激活的 *IoT Security* 许可证。此外，*Enterprise* 版许可协议 *(ELA)* 和 *IoT Security* 不支持 *FedRAMP Moderate* 许可证。

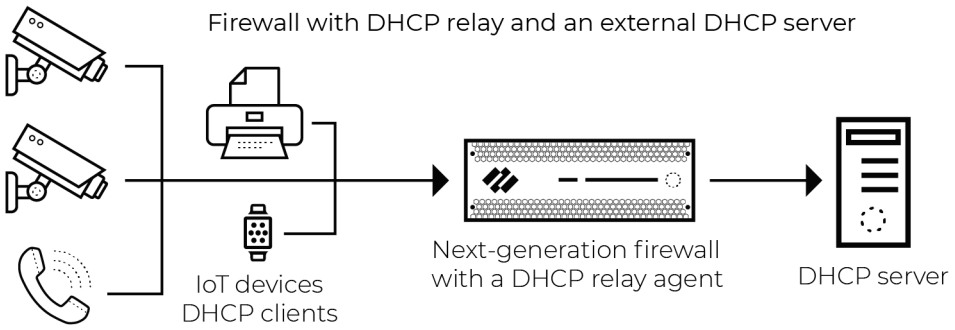
STEP 4 | 配置 VM-Series 可利用 IoT Security 提供网络流量日志。

现在，您已将 IoT Security 加入您的 VM-Series，请按照 为 IoT Security 准备好您的防火墙 中的步骤将其配置为记录网络流量，并将流量日志转发到日志记录服务，然后日志记录服务将网络流量元数据传输到 IoT Security 来进行分析。

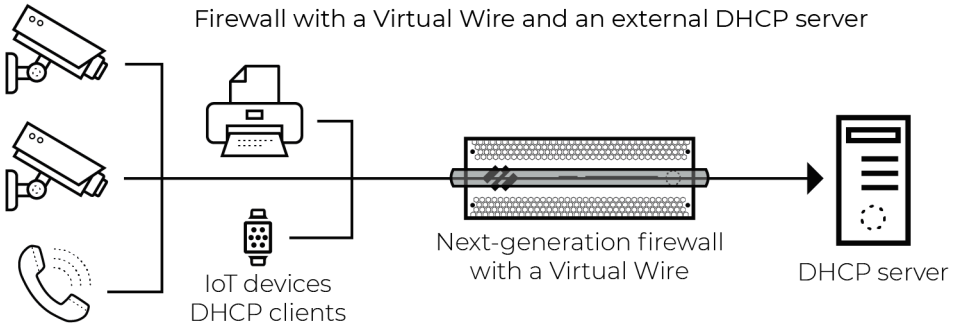
部署防火墙以实现设备可见性

Palo Alto Networks IoT Security 应用使用机器学习根据网络流量（这些作为源还是作为目标）来对 IoT 设备进行分类。为实现此目标，它依赖 Palo Alto Networks 新一代防火墙生成的增强型应用程序日志 (EAL)。

DHCP 流量对 IoT Security 解决方案尤为重要。DHCP 提供了一种创建分类所需的 IP 地址到设备映射（即 IP 地址到 MAC 地址映射）的方法。但是，防火墙通常仅在收到单播 DHCP 消息时才会生成 EAL 条目；例如，当存在集中式 Internet 协议地址管理 (IPAM) 且防火墙或另一个本地设备充当 DHCP 中继代理时。下面是一个示例架构，说明了防火墙为单播 DHCP 流量生成 EAL 的常见情况。



当在启用了多播防火墙的虚拟线 (vWire) 接口上看到数据包时，防火墙会为广播 DHCP 流量生成 EAL 条目，如下所示。



按流量类型收集 DHCP 数据

下表显示了接收单播和广播 DHCP 流量的防火墙接口处于不同模式时的增强型应用程序日志 (EAL) 覆盖范围。

单播 DHCP 流量

防火墙接口部署模式	已生成 **DHCP EAL**
虚拟线路	是
旁接	是

防火墙接口部署模式	已生成 DHCP EAL
第 2 层	是
第 3 层	是

广播 DHCP 流量

防火墙接口部署模式	已生成 DHCP EAL
虚拟线路	是
旁接	否
第 2 层	否
第 3 层	否
防火墙上的 DHCP 服务器（带 VLAN 接口的 L3、L2）	是*
防火墙上的 DHCP 中继代理（带 VLAN 接口的 L3、L2）	是

* 当防火墙是 DHCP 服务器时，生成 EAL 的方法取决于 PAN-OS 版本：

- 当在接口上配置 DHCP 服务器、启用 **DHCP Broadcast Session**（**DHCP** 广播会话）、存在允许 DHCP 流量到达服务器并启用 EAL 转发的安全策略规则时，运行 PAN-OS 10.0 或更高版本的防火墙会在本机生成 EAL。有关更多信息，请参阅为 IoT Security 准备好您的防火墙和配置日志转发策略。
- 运行 PAN-OS 8.1 - 9.1 版本的防火墙需要 configuration-only 解决方法，以便在其中一个防火墙接口上配置 DHCP 服务器时生成 DHCP EAL。有关详细信息，请参阅使用 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙。

IoT Security 的防火墙部署选项

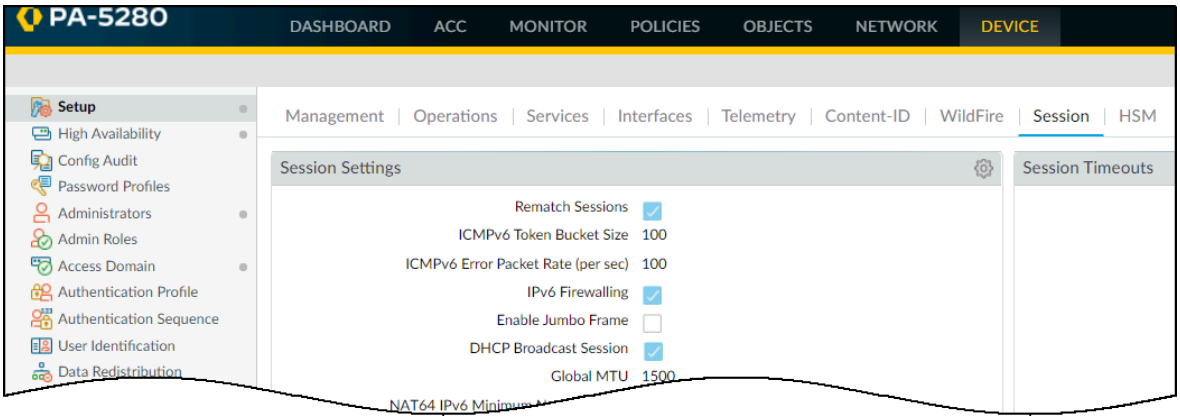
在评估 IoT 设备可见性的部署选项时，有两个基本注意事项：

- 防火墙必须查看流量，以便 IoT 应用程序使用网络流量数据进行分类和分析，并在防火墙本身上执行策略规则。除了 DHCP 流量外，还包括常规操作流量。
- 除了下面概述的例外情况外，防火墙必须查看单播 DHCP 流量才能生成数据，使 IoT Security 能够创建所需的 IP 地址到设备映射。

单播规则的例外情况

- 虚拟线路：当防火墙具有启用了多播防火墙的虚拟线路接口时，它会为广播 DHCP 会话生成增强型应用程序日志 (EAL)。

- 在防火墙上配置了 DHCP 服务器：
  - PAN-OS 8.1 - 9.1：当其中一个接口上的 DHCP 服务器接收到广播 DHCP 流量时，防火墙需要 configuration-only 解决方法才能生成 EAL。
  - PAN-OS 10.0 及更高版本当其中一个接口上的 DHCP 服务器接收到广播 DHCP 流量时，防火墙无需任何解决方法即可生成 EAL。只需启用在 **Device**（设备） > **Setup**（设置） > **Session**（会话）中启用 **DHCP Broadcast Session**（**DHCP** 广播会话）。



  当防火墙接收到 DHCP 广播流量并应用使用增强型应用程序日志转发配置文件的策略规则时，它会记录 DHCP 流量并将其转发到日志记录服务。IoT Security 在这里可以访问要进行分析的数据。
- 在防火墙上配置了 DHCP 中继代理：
  - 在其中一个接口上配置了 DHCP 中继代理时，防火墙会为广播 DHCP 流量生成 EAL。

旁接接口

注意事项 — 如果您使用 Tap 接口来查看防火墙通常看不到的 DHCP 流量，请考虑以下事项：

- 将 Tap 放在已配置 DHCP 的任何路由边界的“北部”。这将确保捕获的流量是单播的，而不是广播的。[如果具有 Tap 接口的防火墙与将流量镜像到它的交换机位于同一广播域中，请在 **Device**（设备） > **Setup**（设置） > **Session**（会话）中启用 **DHCP Broadcast Session**（**DHCP** 广播会话）。]
- 如果将分路器接口添加到现有防火墙，请在实施之前考虑防火墙上的可用容量。虽然分路器接口不会转发流量，但在分路器端口上看到的流量仍会消耗会话表和数据包缓冲区等进程的资源。有关缓解性能影响的指南，请参阅使用 Tap 接口实现 DHCP 可见性

Tap 接口的用例

- 评估
- 在防火墙“南部”的设备上配置了 DHCP 的网络
- 监控不会自然穿越防火墙的网络

虚拟线路接口

注意事项 — 您可能需要在防火墙上使用虚拟线路 (vWire) 接口来了解防火墙通常看不到的 DHCP 流量。以这种方式使用 Tap 接口时，请考虑以下事项：

- 确保虚拟线路已启用组播防火墙。

- 确保虚拟线路位于 DHCP 流量的路径中。此流量可以是广播流量，也可以是单播流量。
- 确保存在允许 DHCP 的安全策略规则，并且已将正确的日志转发配置文件应用于该规则。
- 确保防火墙具有处理额外流量的可用容量。有关缓解性能影响的指南，请参阅使用虚拟线路接口实现 DHCP 可见性。

虚拟线路接口的用例 — 当 DHCP 服务器和防火墙接口位于同一网段时，防火墙只能看到广播 DHCP 流量。将 DHCP 服务器置于虚拟线路接口后面，使防火墙能够为此广播流量创建 EAL。

第 **2** 层和第 **3** 层接口

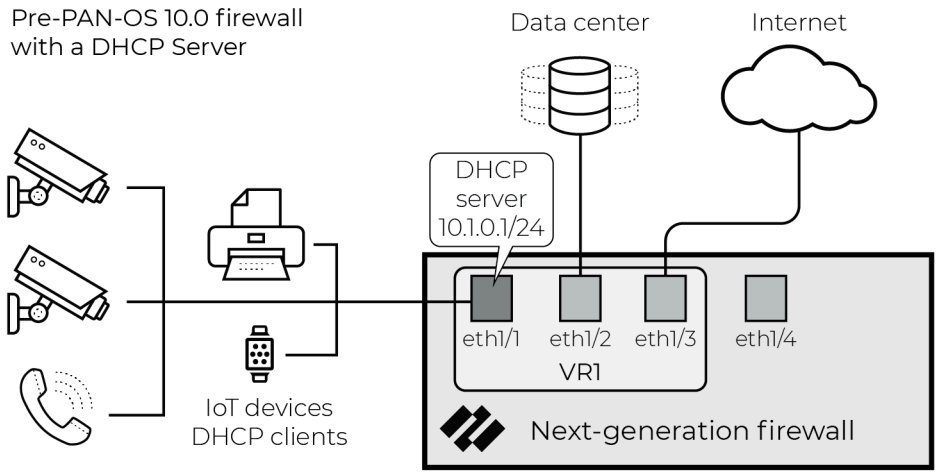
注意事项 — 第 2 层 (L2) 和第 3 层 (L3) 部署都需要单播 DHCP 流量来生成 EAL。在 L2 部署中使用 VLAN 接口时，注意事项与使用第 3 层接口的部署相同：

- 通过防火墙的单播 DHCP 数据包会生成 EAL。
- 当 L3 或 VLAN 接口配置为 DHCP 中继代理时，防火墙会生成 EAL。
- 当 L3 或 VLAN 接口配置为 DHCP 服务器时，防火墙可能会生成 EAL。有关详细信息，请参阅部署防火墙以实现设备可见性中的 DHCP 数据收集（按流量类型）。

使用 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙

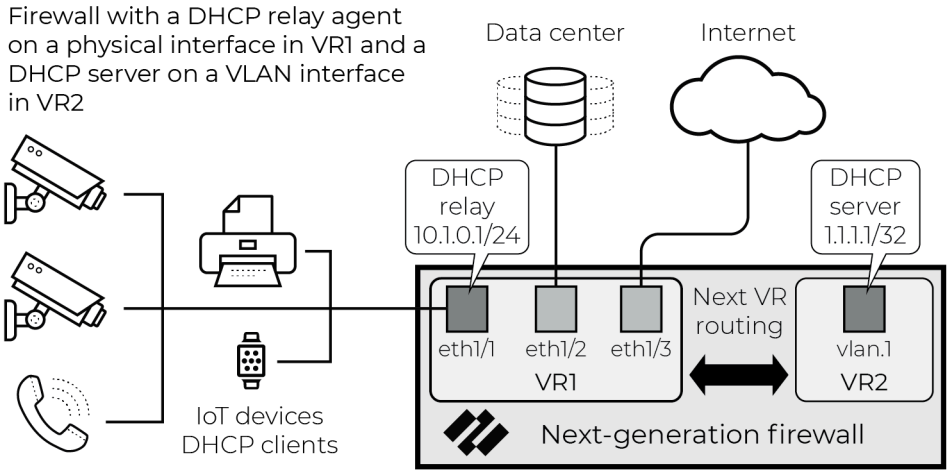
主要挑战是，当防火墙是 DHCP 服务器时，PAN-OS 10.0 之前的版本不会生成增强型应用程序日志 (EAL)，这在分支机构和零售用例中很常见。当防火墙也是 DHCP 服务器时，需要对防火墙进行一些重新配置，以便为 DHCP 流量生成 EAL。您可以通过在其配置中引入 DHCP 中继代理来实现。

对于本节有关 *DHCP* 可见性的其余部分，假定防火墙运行 *PAN-OS 9.1* 或更早版本。



解决方案：在物理接口上配置 **DHCP** 中继代理并在 **VLAN** 接口上配置 **DHCP** 服务器

在防火墙上添加 DHCP 中继代理，以便单播 DHCP 消息经过内容扫描，并且防火墙为其生成 EAL 条目。在防火墙上创建一个 VLAN 接口来托管 DHCP 服务器，并将防火墙的物理接口配置为 DHCP 中继代理。



分析

当上图中的客户端广播 DHCPDISCOVER 消息时，在 ethernet1/1 上配置的 DHCP 中继代理将接收这些消息。对中继代理进行配置，将 DHCPDISCOVER 消息单播到托管 DHCP 服务器的 vlan.1 接口的 IP 地址。请注意以下几点：

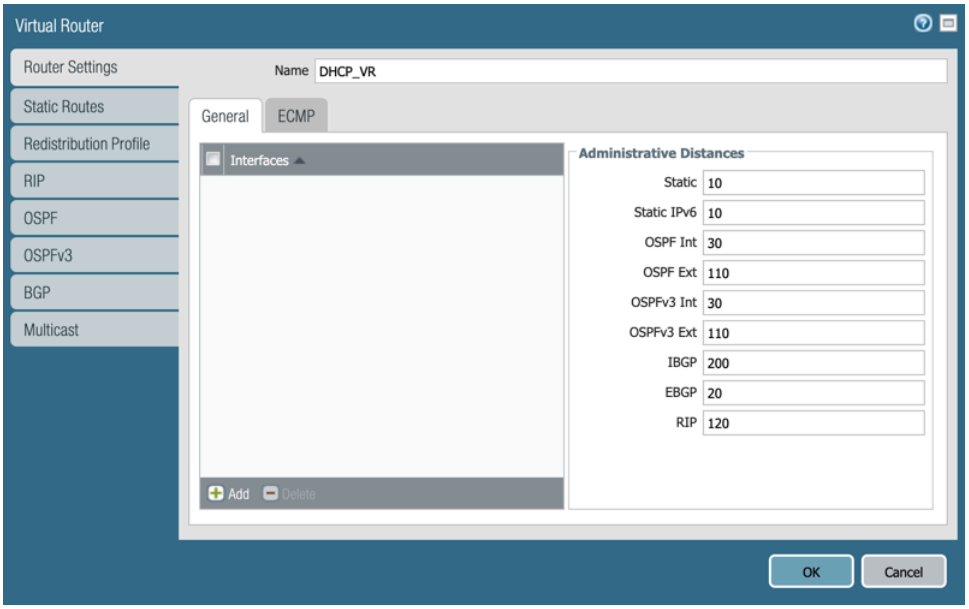
- vlan.1 接口可以具有带有 32 位网络掩码的 IP 地址，以便在将此解决方案扩展到一个物理接口之外时有效地利用地址空间。
- vlan.1 接口位于单独的虚拟路由器中。这会强制单播 DHCP 消息通过数据平面，从而触发防火墙生成 EAL 条目。
- DHCP 服务器配置了与 ethernet1/1 上配置的子网一致的 IP 池。
- 使用 Next-vr 主机路由在 ethernet1/1 和 vlan.1 之间路由单播 DHCP 消息。

由于该解决方案对 DHCP 服务器使用虚拟接口，因此只需通过配置即可实现，而无需对网络进行物理重新配置。此外，即使所有物理接口都在使用中，它也可以实现。

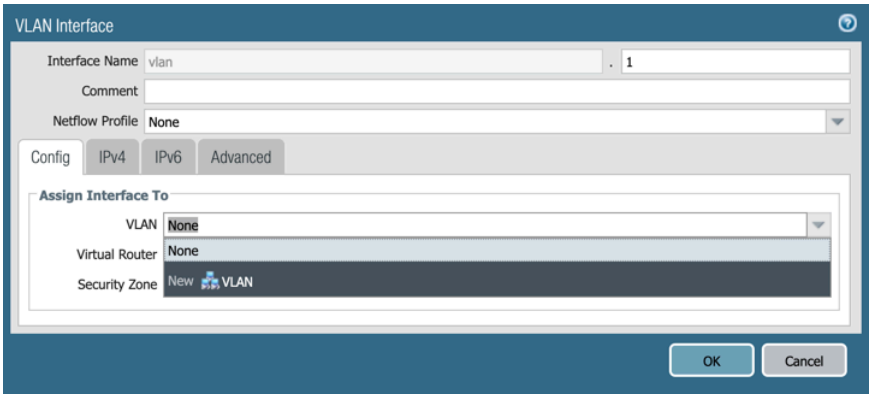
配置

STEP 1 | 保存当前配置的快照。

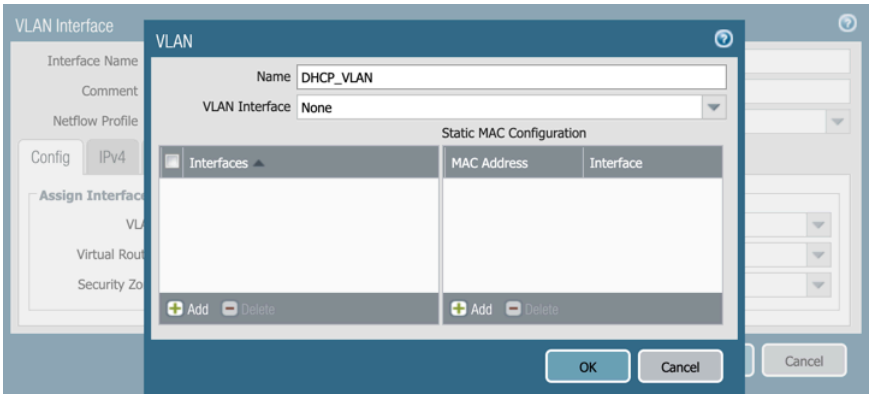
STEP 2 | 配置新的虚拟路由器。



STEP 3 | 配置 VLAN 接口。在 VLAN 下拉列表中，单击 **New**（新建）以创建新的 VLAN。



STEP 4 | 输入新 VLAN 的名称，然后单击 **OK**（确定）。



出现 VLAN 接口配置窗口。

STEP 5 | 在“配置”选项卡上的“分配接口到”部分，选择刚才创建的虚拟路由器和现有 DHCP 服务器配置的相同安全区域。

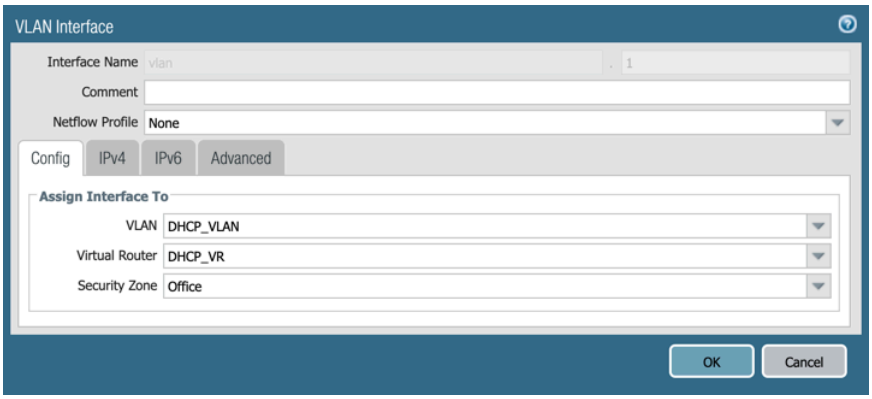
如果选择其他区域或创建新区域，则必须配置允许两个区域之间使用 DHCP 的安全策略规则（参阅配置日志转发策略中的“配置区域间策略”）。

STEP 6 | 启用日志转发。

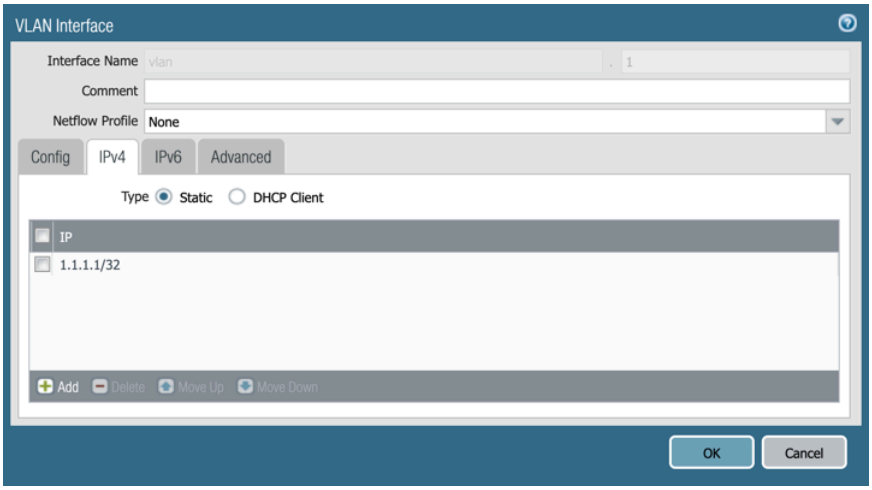
日志转发使防火墙能够将增强的应用程序日志发送到日志记录服务。然后，IoT Security 从该服务提取元数据来进行分析。

STEP 7 | 如果使用相同的安全区域，请记住为区域内策略规则启用日志记录和日志转发。

有关详细信息，请参阅配置日志转发策略中的“配置区域内策略”。

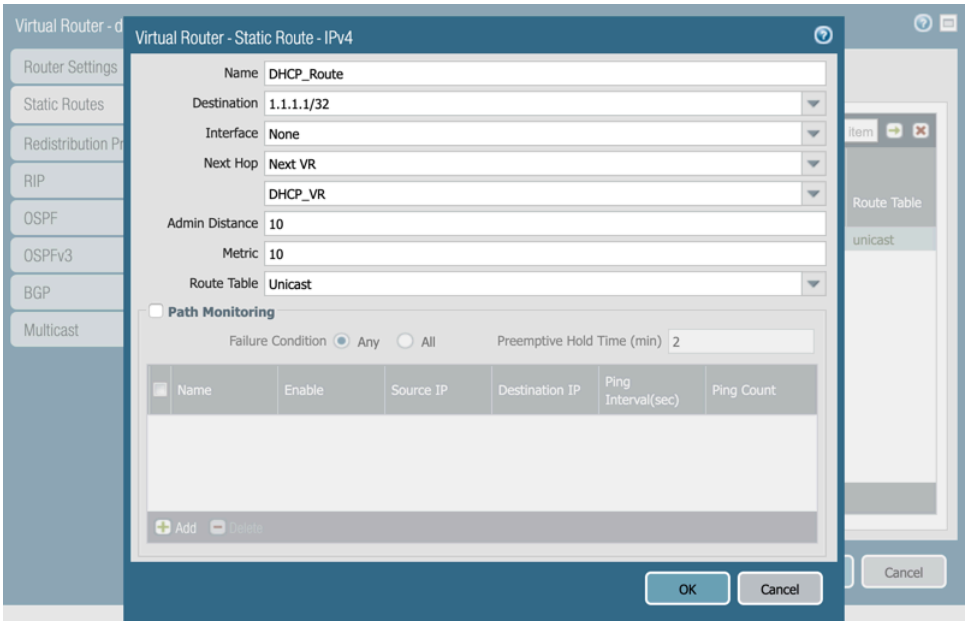


STEP 8 | 在 IPv4 选项卡上，配置主机 IP 地址（即具有 32 位网络掩码的地址），然后单击 **OK**（确定）。



为了测试和故障排除目的，分配一个允许 *VLAN* 接口响应 *Ping* 的接口管理配置文件。如果 *VLAN* 接口与物理接口处于不同的区域，请参阅配置日志转发策略中的“配置区域间策略”。

STEP 9 | 打开现有虚拟路由器，并配置到分配给前面配置的 VLAN 接口 IP 地址的主机路由。



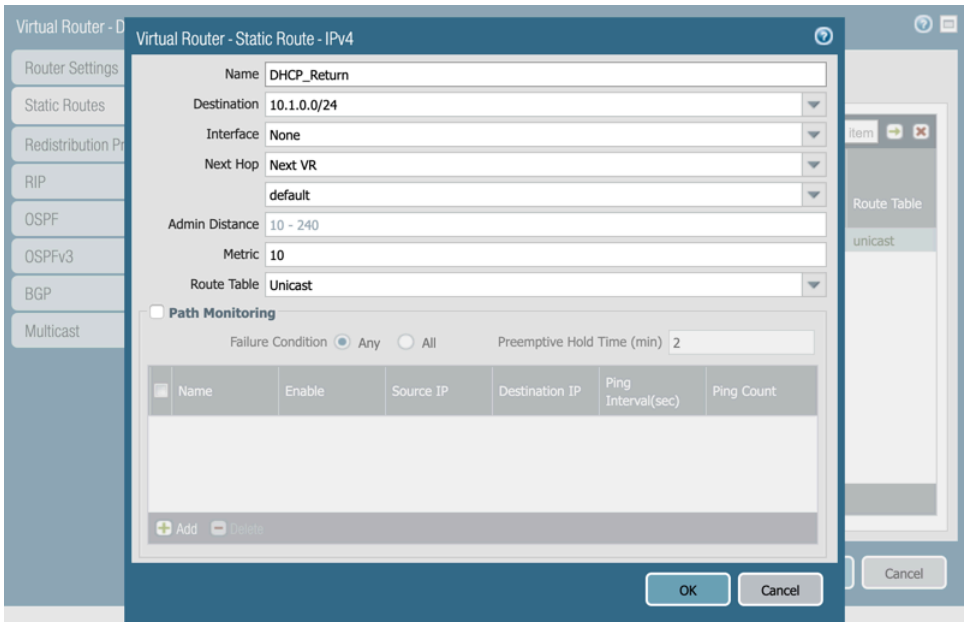
当有多个 *DHCP* 服务器时，可以使用网络路由代替主机路由，以简化配置。有关详细信息，请参阅当防火墙服务于 DHCP 时规划扩展。

STEP 10 | 将接口设置保留为 **None**（无），并选择 **Next VR**（下一个 **VR**）作为下一跳。在“下一跳”下面的下拉列表中，选择您创建的新虚拟路由器。

STEP 11 | 在“静态路由”对话框中单击 **OK**（确定），然后在“虚拟路由器”对话框中单击 **OK**（确定）。

STEP 12 | 打开新的虚拟路由器，并配置到 DHCP 服务器服务的网络的路由。

该配置与下面显示的类似，其中下一跳设置是下一个 VR 和现有虚拟路由器的名称。



创建到 *DHCP* 中继代理的网络路由（而不是主机路由）可使 *DHCP* 服务器的探测功能正常运行。

STEP 13 | 提交这些更改。

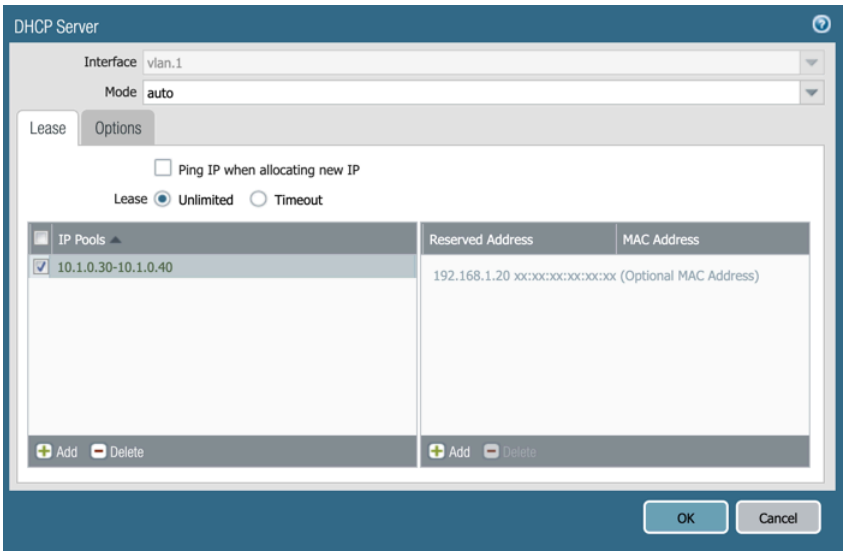
STEP 14 | 测试配置。

如果您分配了允许 Ping 到 VLAN 接口的接口管理配置文件，请通过登录 CLI 并从物理接口 Ping 到 VLAN 接口来测试您的配置：

```
ping source <phy_interf_ip-addr> host <vlan_interf_ip-addr>
```

STEP 15 | 在 VLAN 接口上配置 DHCP 服务器。

包括适当的 IP 池和选项（例如网关和 DNS 服务器），然后单击 **OK**（确定）。



STEP 16 | 在连接本地网络的物理接口上配置 DHCP 中继代理，然后单击 **OK**（确定）。

STEP 17 | 提交配置。

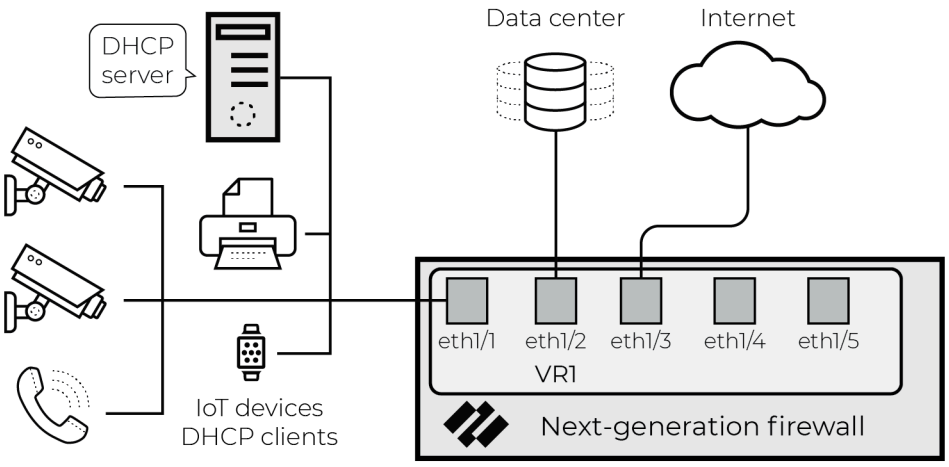
STEP 18 | 通过将客户端连接到本地网络段来测试 DHCP 发布和更新功能。

为本地 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙

当防火墙未接收单播 DHCP 数据包（无论是作为 DHCP 服务器还是中继代理）时，您必须安排它生成或接收这些数据包。本节提供了在 PAN-OS 8.1、PAN-OS 9.0 和 PAN-OS 9.1 中提供 DHCP 流量可见性的说明。

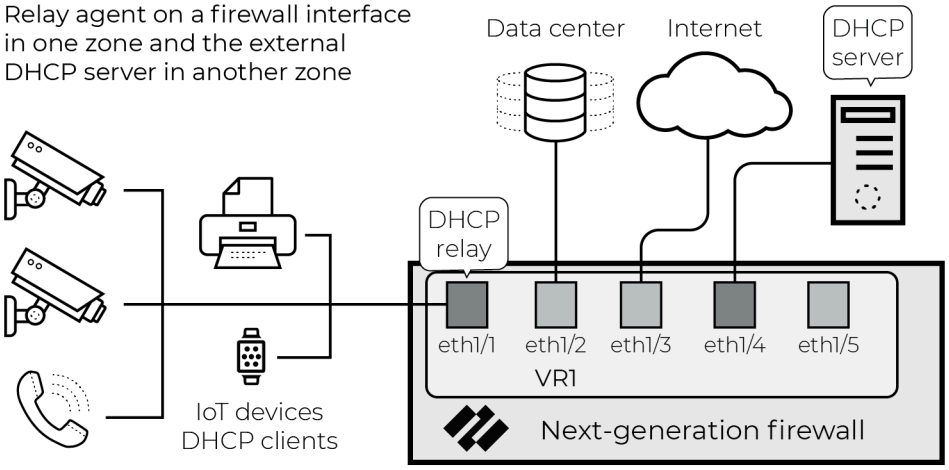
下面的例子中，本地网段上有一个 DHCP 服务器。防火墙接收 DHCP 客户端广播的 DHCPDISCOVER 消息，但未配置为 DHCP 服务器。

External DHCP server and pre-PAN-OS 10.0 firewall



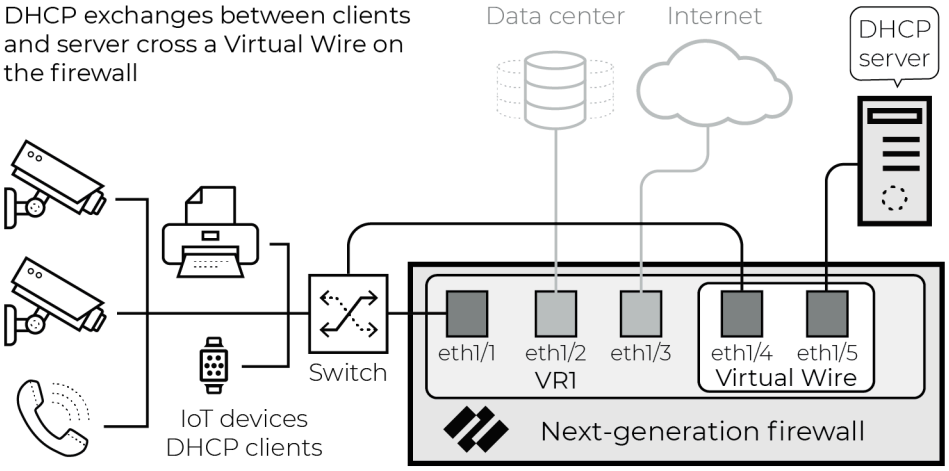
解决方案 **1**：将 **DHCP** 服务器移至其他区域

该解决方案涉及将 DHCP 服务器移至防火墙上的不同区域，并在连接到客户端的防火墙接口上配置 DHCP 中继代理。这会强制生成单播 DHCP 流量，然后防火墙可以使用它来生成增强型应用程序日志 (EAL)。



解决方案 **2**：将 **DHCP** 服务器置于虚拟线路后

将 DHCP 服务器置于虚拟线路接口后，使防火墙能够为交换中的所有数据包生成 EAL。经过正确的配置和物理网络更改后，网络看起来类似于下图：



使用 Tap 接口实现 DHCP 可见性

为了完全了解 DHCP 流量，请在防火墙上部署 Tap 接口。本指南假设您熟悉 PAN-OS 配置，包括 Tap 配置。有关配置 Tap 接口的详细信息，请参阅 PAN-OS 网络管理员指南。

注意事项

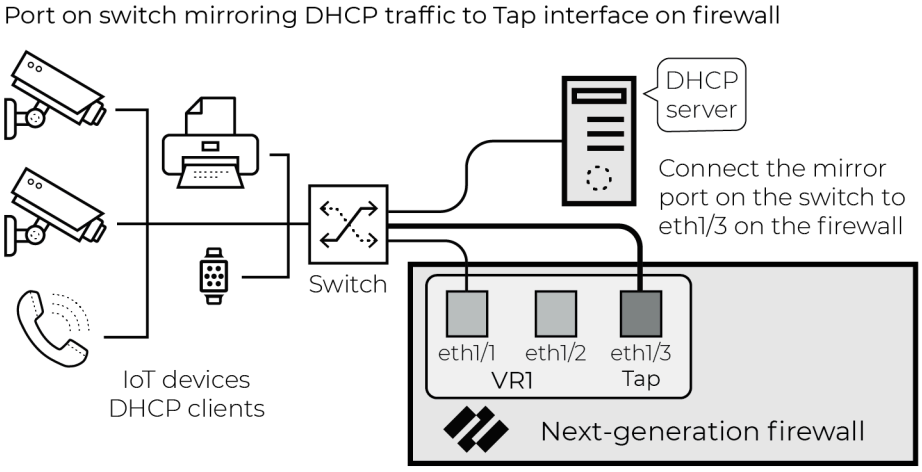
向防火墙上的 Tap 接口发送额外的流量会导致额外的会话负载。造成这种情况的原因有两个：

- 从 DHCP 服务器到互联网、数据中心或其他通常会穿过防火墙的目标的任何流量都会被检查两次。
- 当 Tap 接口接收到通常不会被检查的流时，将会对其进行检查；例如，发往本地网段上其他主机的流。

以下配置部分包括最小化性能影响的选项。

网络架构

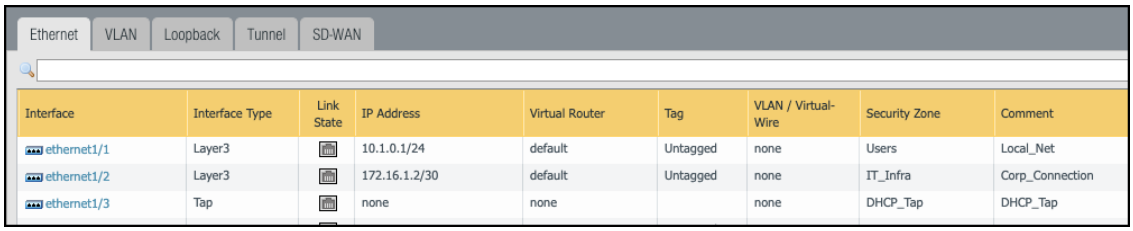
下图说明了该解决方案的总体思路。实际拓扑可能因 DHCP 服务器的位置和 RSPAN（远程交换端口分析器）等技术的使用而有所不同。



此配置的目的是获得防火墙根据其当前配置和网络拓扑通常无法看到的 DHCP 流量的可见性。

配置

STEP 1 | 配置 Tap 接口和区域。



STEP 2 | 配置 Tap 流量的策略规则。

- 第一个策略规则匹配 DHCP 流量并使用与规则库其余部分相同的日志转发配置文件。
- 第二条规则丢弃所有其他流量，从而最大限度地减少防火墙上的额外会话负载。日志转发配置文件未启用。
- 这两条规则均不使用安全配置文件。

STEP 3 | 将 Tap 接口与交换机上的端口镜像连接。

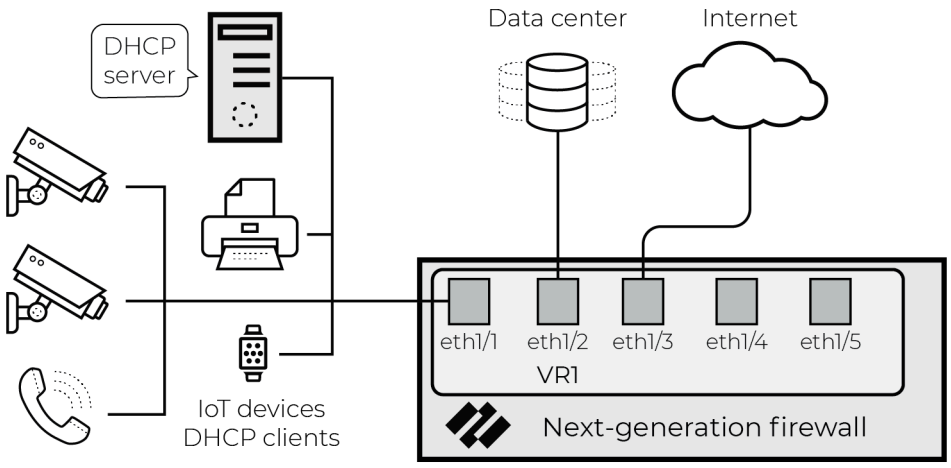
使用虚拟线路接口实现 DHCP 可见性

为了完全了解 DHCP 流量，请在 DHCP 服务器前面部署虚拟线路 (vWire)。本指南假设您熟悉 PAN-OS 配置，包括虚拟线路配置。有关配置虚拟线路接口的详细信息，请参阅 PAN-OS 网络管理员指南。

网络架构

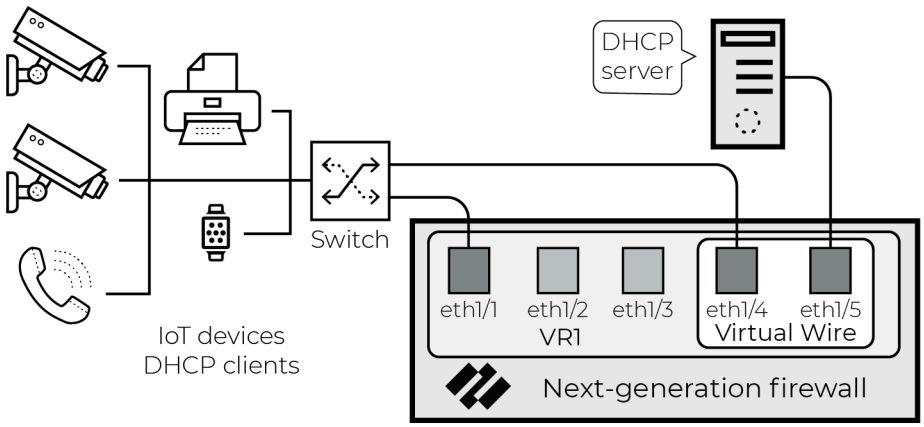
此解决方案适用于 DHCP 服务器与防火墙接口位于同一网段的网络，如下图所示。

External DHCP server and pre-PAN-OS 10.0 firewall



为了全面了解所有四个 DHCP 消息，请将 DHCP 服务器置于虚拟线路接口后面。这样做可以使防火墙为交换中的所有数据包生成增强型应用程序日志 (EAL)。经过正确的配置和物理网络更改后，网络看起来类似于下图：

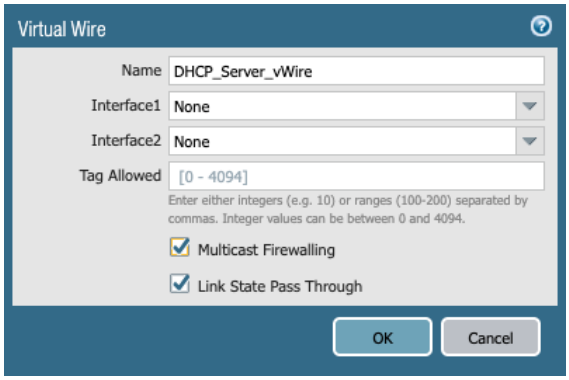
External DHCP server and firewall with a Virtual Wire on the network segment



配置

STEP 1 | 配置虚拟线路接口，并完成区域设置。

虚拟线路对象的配置必须包括多播防火墙：



STEP 2 | 配置策略规则以允许两个虚拟线路接口区域之间的流量。

配置此策略规则以允许服务器当前看到的所有现有流量使用与规则库其余部分相同的日志转发对象。下面的策略优化部分介绍如何优化此策略规则集并防止重复记录。

	Name	Type	Source		Destination		Application	Service	Action	Profile	Options
			Zone	Address	Zone	Address					
1	DHCP_Host_Allow	universal	DHCP_Network_Side DHCP_Server_Side	any	DHCP_Network_Side DHCP_Server_Side	any	any	application-d...	Allow	none	

STEP 3 | 将外部 DHCP 服务器连接到虚拟线路的一侧，并将网络交换机连接到另一侧。

为最大限度减少交换基础设施中的接线，您可以在其中使用隔离的 VLAN，而不是将 DHCP 服务器主机直接与防火墙连接。

策略优化

该解决方案的目标是了解 DHCP 有效负载，同时最大限度地减少对防火墙性能的影响。为此，为虚拟线路区域配置以下策略规则集：

	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
1	DHCP_Traffic	universal	DHCP_Network_Side DHCP_Server_Side	any	DHCP_Network_Side DHCP_Server_Side	any	dhcp	application-d...	Allow	none	
2	DHCP Ping	universal	DHCP_Server_Side	any	DHCP_Network_Side	any	ping	application-d...	Allow	none	
3	DHCP_Host_Allow	universal	DHCP_Network_Side DHCP_Server_Side	any	DHCP_Network_Side DHCP_Server_Side	any	any	application-d...	Allow	none	

- “DHCP_Traffic”策略规则允许 DHCP 与 DHCP 服务器进行通信。此规则使用启用了 EAL 的标准日志转发配置文件。
- “DHCP Ping”策略规则允许从 DHCP 服务器 Ping 到子网的其余部分。这使得 DHCP 服务器能够在将 IP 地址分配给新请求作为租约之前检查该 IP 地址是否有效。此规则不转发日志。
- “DHCP_Host_Allow”策略规则允许所有其他内容进出 DHCP 服务器，并且不会转发流量匹配的日志。

为了最大限度地减少防火墙因此虚拟线路配置而看到的额外会话对性能的影响，未将安全配置文件分配给上述策略规则。如果要对 DHCP 服务器进行微分段，请将“DHCP_Host_Allow”规则替换为更精细的策略规则集，以根据最佳实践允许应用程序。您可以使用该策略规则集中的安全配置文件。

使用 SNMP 网络发现从交换机了解设备

为了识别设备、评估风险并帮助新一代防火墙根据 Device-ID 执行安全策略规则，IoT Security 需要网络流量元数据进行分析。新一代防火墙在应用启用了日志记录的安全策略规则时会提取并记录这些元数据。当规则还启用了日志转发时，防火墙会将日志发送到日志记录服务，然后将元数据流式传输到 IoT Security。

但是，根据防火墙所处的位置，它们可能无法查看所有网络流量，从而导致设备发现差距和设备识别、行为监控和 Device-ID 规则执行的效率降低。为了进一步扩展网络可见性，IoT Security 支持多种选项：

- 在网络交换机上镜像流量，并使用封装远程交换端口分析器 (ERSPAN) 通过 GRE 隧道将镜像流量发送到防火墙。防火墙检查流量、记录流量，然后将日志转发到日志记录服务以供 IoT Security 访问。
- 配置 DHCP 服务器以将其服务器日志作为系统日志消息发送到防火墙。然后，防火墙通过日志记录服务将消息作为子类型为 dhcp-syslog 的增强应用程序日志 (EAL) 转发到 IoT Security。
- 将 IoT Security 与提供资产管理和网络管理等服务的第三方产品相集成。IoT Security 通过 Cortex XSOAR 连接到这些系统，并从中检索其他设备数据，以增强从新一代防火墙以及可选地从网络交换机和 DHCP 服务器学习到的元数据。

在使用 DHCP 为设备分配网络设置的环境中，IP 地址会在有限的时间内动态租用。监控网络行为以识别设备、评估风险和执行 Device-ID 安全策略规则的一个重要部分是将每个设备动态分配的 IP 地址链接到其唯一、不变的 MAC 地址的能力。当新一代防火墙接收到包含 IP 和 MAC 地址的

流量时，它们可以做到这一点。当防火墙没有收到来自所有设备的流量，或者虽然收到了流量但只包含 IP 地址（可能是因为流量跨越了第 2 层域并且设备 MAC 地址已更改为转发设备的 MAC 地址）时，它们仍然可以使用 SNMP 查询整个网络中的交换机来收集 IP 地址到 MAC 地址的绑定。

当使用 SNMP 查询网络交换机和其他转发设备时，防火墙首先通过请求一台交换机（入口点交换机）的链路层发现协议 (LLDP) 邻居和思科发现协议 (CDP) 邻居来开发网络拓扑，然后在整个网络中逐个向邻近交换机和子交换机重复该请求。在获得整个网络或网络有限区域内的交换机和转发设备列表后，防火墙接下来会查询每个设备的 ARP 表以及其他信息。ARP 表包含通过交换机连接到网络的设备的 IP 地址到 MAC 地址绑定信息。防火墙查询的其他设备详细信息包括设备连接的交换机上的物理接口或端口、它们的 VLAN 和子网以及 DHCP 和 DNS 服务器 IP 地址。防火墙收到这些信息后，会创建日志并通过日志记录服务将其发送到 IoT Security。

以下是 SNMP 在 UDP 端口 161 上查询有关 LLDP 邻居和 CDP 邻居、设备 IP 地址到 MAC 地址绑定以及接口或端口信息的示例对象标识符 (OID)：

- OID：1.0.8802.1.1.2.1.4 lldpRemoteSystemsData（LLDP 邻居）
- OID：1.3.6.1.4.1.9.9.23 ciscoCdpMIB（CDP 邻居）
- OID：1.3.6.1.2.1.4.22.1.2 ipNetToMediaPhysAddress（来自 ARP 的 IP 到 MAC 地址绑定）
- OID：1.3.6.1.2.1.4.22.1.1 ipNetToMediaIfIndex（接口或端口信息）

IoT Security 提供 SNMP 网络发现作为 IoT Security 第三方集成附加许可证的一部分，必须购买。从 PAN-OS 11.1 开始，SNMP 网络发现可作为免费附加组件提供给新一代防火墙，不需要附加许可证。虽然使用附加许可证的版本支持每个 IoT Security 租户针对不同网络和网络段执行多组作业，但带有免费附加组件的版本仅支持每个防火墙针对一个网络或网络段执行一组作业。

SNMP 网络发现过程无法遍历不支持 *CDP* 或 *LLDP* 的交换机。

STEP 1 | 登录到防火墙或 Panorama 的 Web 界面并安装 SNMP 网络发现附加组件。

该附加组件允许防火墙向网络上的交换机和路由器发送 SNMP 查询，然后处理收到的响应。

新一代防火墙

选择 **Device**（设备） > **Plugins**（插件），搜索 `network_discovery`，在“操作”列中单击 **Download**（下载），然后在防火墙上 **Install**（安装）插件。

Panorama

1. 选择 **Panorama** > **Plugins**（插件），搜索 `network_discovery`，在“操作”列中单击 **Download**（下载），然后在 Panorama 上 **Install**（安装）插件。
2. 选择 **Panorama** > **Device Deployment**（设备部署） > **Plugins**（插件），在“操作”列中单击 **Install**（安装），选择要安装附加组件的防火墙，然后单击 **OK**（确定）。

STEP 2 | 配置 SNMP 网络发现参数。

以下说明适用于使用单个新一代防火墙上的 PAN-OS Web 界面进行 SNMP 网络发现配置。要在 Panorama 上配置 SNMP 网络发现，请根据需要使用模板和模板堆栈以及入口交换机、发现范围和接口的 IP 地址的模板堆栈变量。

1. 选择 **Device**（设备） > **IoT Security** > **Network Discovery**（网络发现），然后单击 **Edit**（编辑）（齿轮图标）。

   随即出现“SNMP 网络发现设置”对话框，其中“计划设置”选项卡处于活动状态。

2. 在网络发现作业部分，安排防火墙运行作业的频率，以了解网络上或网络定义范围内运行 LLDP 和 CDP 的所有交换机和其他网络转发设备。默认值为每天一次，通常就足够了。

3. 在网络数据刷新作业部分，安排防火墙运行作业的频率，以查询交换机和其他转发设备以获取有关网络和连接到它们的设备的信息。考虑 DHCP 租约时间的更新频率，并安排作业在租约时间的一半时运行，这是 DHCP 客户端开始请求租约续订并可以接收不同的 IP 地址的时候。在没有 DHCP 的环境中，考虑每小时运行一次网络数据刷新作业，这是默认设置。

4. 单击 **Discovery Scope Settings**（发现范围设置）选项卡，然后输入以下内容：

   Entry Point switch（入口点交换机）：输入开始 SNMP 发现过程的入口点交换机的 IP 地址。

   入口点交换机的一个良好选择是核心交换机，因为它通常可以最广泛地访问整个网络的各种分布层和接入层交换机。

   Device IP Address Scope（设备 **IP** 地址范围）：输入 IP CIDR 块的前缀来定义要学习的交换机和端点设备的范围。或者，不要通过输入 **None**（无）来设置范围，否则 SNMP 将收集整个网络的网络拓扑。

   Service Route（服务路由）：如果您的防火墙使用数据接口而不是管理接口来执行 SNMP 网络发现，请设置指定该接口和要查询的网络段的服务路由。

   Device（设备） ***> Setup***（设置） ***> Services***（服务） ***> Service Route Configuration***（服务路由配置） 上配置的服务路由不适用。*SNMP* 网络发现仅使用此处配置的服务路由。

5. 单击 **SNMP Settings**（**SNMP** 设置）选项卡并设置 SNMP 版本并配置您使用的版本和选项所需的设置。

   SNMP Version（**SNMP** 版本）：选择您的交换机支持的 SNMP 版本，**V2** (SNMPv2c) 或 **V3**。如果选择 **V2**，请配置 **Community String**（社区字符串）。如果选择 **V3**，请配置 **Username**（用户名）、**Security Level**（安全级别）、**Authentication Protocol**（身份验证

协议）和 **Password**（密码），以及 **Privacy Protocol**（隐私协议）和 **Password**（密码）设置。

Community String（社区字符串）（用于 SNMP V2）：输入在交换机上配置的 SNMP 社区字符串以允许只读访问。

Username（用户名）（适用于 SNMP V3）：输入具有只读访问权限的 SNMP 用户帐户的用户名。这是防火墙在访问交换机上运行的 SNMP 服务器时使用的帐户。

Security Level（安全级别）（针对 SNMP V3）：选择访问交换机上的 SNMP 服务器的安全级别。

- **noAuthNoPriv**：选择此选项则不对防火墙上的 SNMP 代理和交换机上的 SNMP 服务器之间的通信进行身份验证和加密。
- **authNoPriv**：选择此项表示需要基于 MD5 或 SHA 哈希的身份验证，但不加密防火墙和交换机之间的通信。
- 身份验证权限：选择此项则需要身份验证和加密。

Authentication Protocol（身份验证协议）（针对 SNMP V3）：选择防火墙和交换机之间的通信验证算法：**MD5**（消息摘要算法 **5**）或 SHA-1（安全散列算法 1）的 **SHA**。

Authentication Password（身份雁阵密码）（针对 SNMP V3）：输入身份验证过程中使用的密码。

Privacy Protocol（隐私协议）（针对 SNMP V3）：选择防火墙和交换机之间的通信加密算法：**DES**（数据加密标准）或 **AES**（高级加密标准）。

Privacy Password（隐私密码）（针对 SNMP V3）：输入加密过程中使用的密码。

6. 选择 **Enable SNMP Network Discovery Settings**（启用 **SNMP** 网络发现设置），然后单击 **OK**（确定）。

   启用此功能后，设置将发送到附加组件，附加组件会检查将发送和接收 SNMP 流量的源接口 IP 地址并安排以下任务：

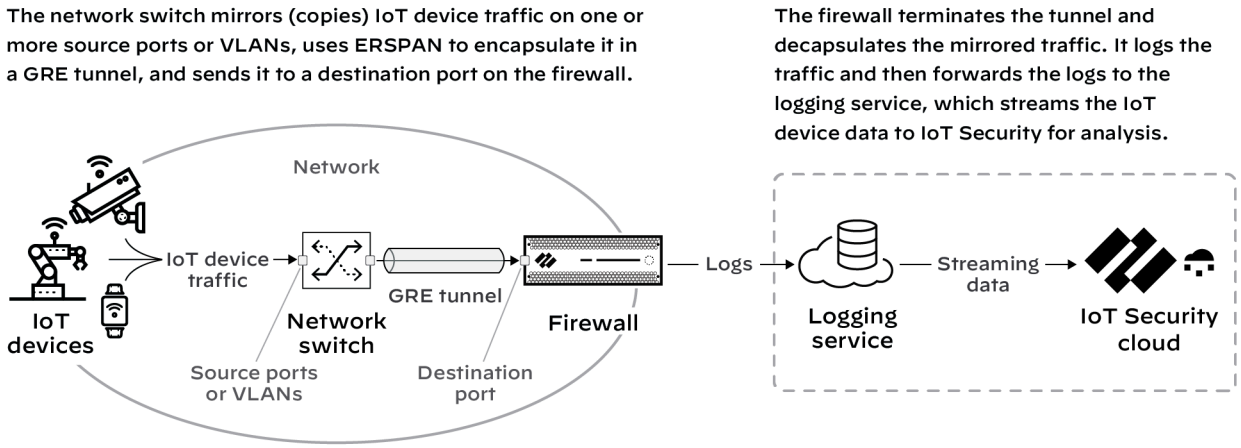
   - 使用 CDP 和 LLDP OID 发送网络发现的 SNMP 查询。
   - 使用 VLAN、子网、交换机接口或端口信息、设备 IP 到 MAC 地址绑定以及每个设备级别的其他属性的各种 OID 发送网络数据刷新的 SNMP 查询。

   SNMP 作业运行后，生成的 SNMP 数据将存储在文件中并转换为增强型应用程序日志。然后防火墙将日志发送到日志记录服务。然后，日志记录服务将数据传输到 IoT Security，后者更新其数据库并在 IoT Security 门户中显示 SNMP 发现网络拓扑数据。

使用 ERSPAN 通过 GRE 隧道发送镜像流量

除非设备流量对防火墙可见，否则防火墙不能将其包含在转发给IoT Security 的日志中。当您需要收集流量不通过防火墙的设备的数据时，请在网络交换机上镜像其流量，并使用封装远程交换端口分析器 (ERSPAN) 通过通用路由封装 (GRE) 隧道将其发送到防火墙。防火墙解封装流量后，会对其进行类似于 TAP 端口上接收的流量的检查。然后，该防火墙会创建增强型应用程序日志 (EAL) 和流量、威胁、WildFire、URL、数据、GTP（启用 GTP 时）、SCTP（启用 SCTP 时）、隧道、身份验证和解密日志。它将它们转发到日志记录服务，IoT Security 可以在其中访问和分析 IoT 设备数据。

您可以将此功能用于需要检查来自远程交换机的流量的任何部署。*IoT Security* 只是一个用例。



此功能需要支持 *ERSPAN* 的交换机，例如 *Catalyst 6500*、*7600*、*Nexus* 和 *ASR 1000* 平台。

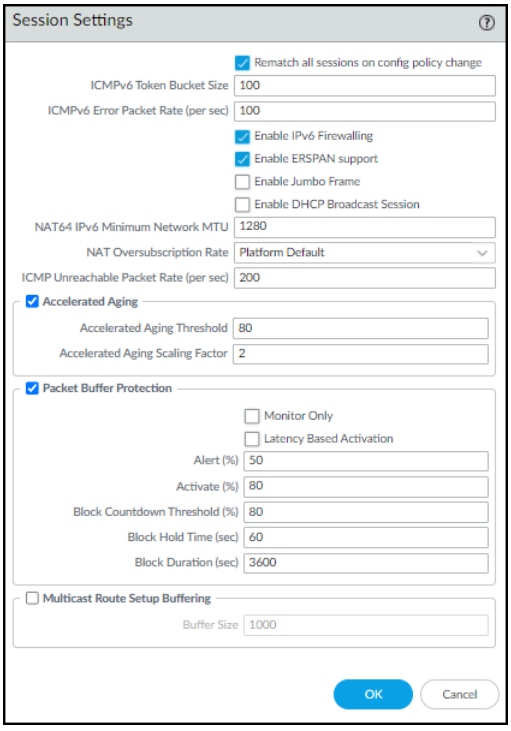
STEP 1 | 配置支持 ERSPAN 的交换机，镜像一个或多个源端口或 VLAN 上的流量，并通过 GRE 隧道将其转发到新一代防火墙上的目标端口。

有关配置说明，请参阅交换机的 *Cisco* 文档。

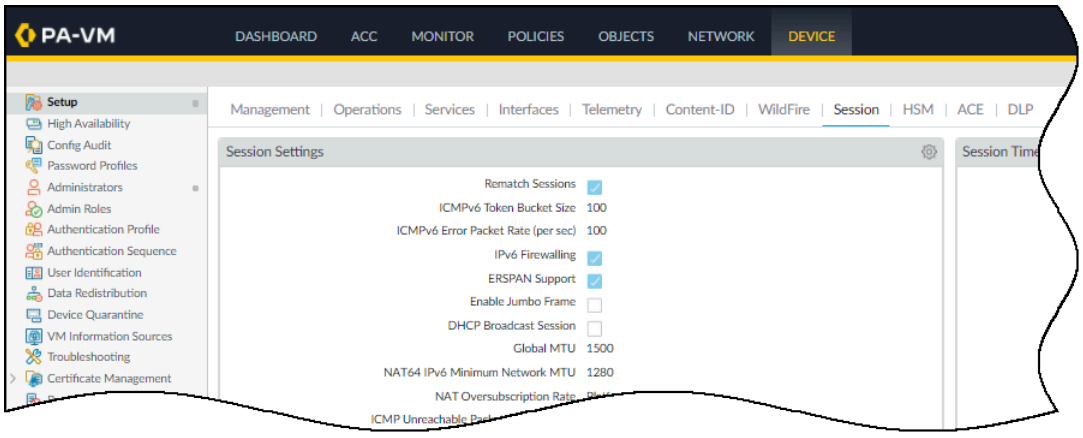
STEP 2 | 在防火墙上启用 ERSPAN 支持。

默认情况下，ERSPAN 支持是禁用的。

1. 登录防火墙并选择 **Device**（设备） **> Session**（会话）。
2. 单击会话设置的 **Edit**（编辑）图标，选择 **Enable ERSPAN Support**（启用 **ERSPAN** 支持），然后单击 **OK**（确定)。



会话设置部分中的 ERSPAN 支持复选框现已选中。



STEP 3 | **Commit**（提交）更改。

STEP 4 | 创建一个第 3 层安全区域，专门用于终止 GRE 隧道并从网络交换机上的源端口接收镜像的 IoT 设备流量。

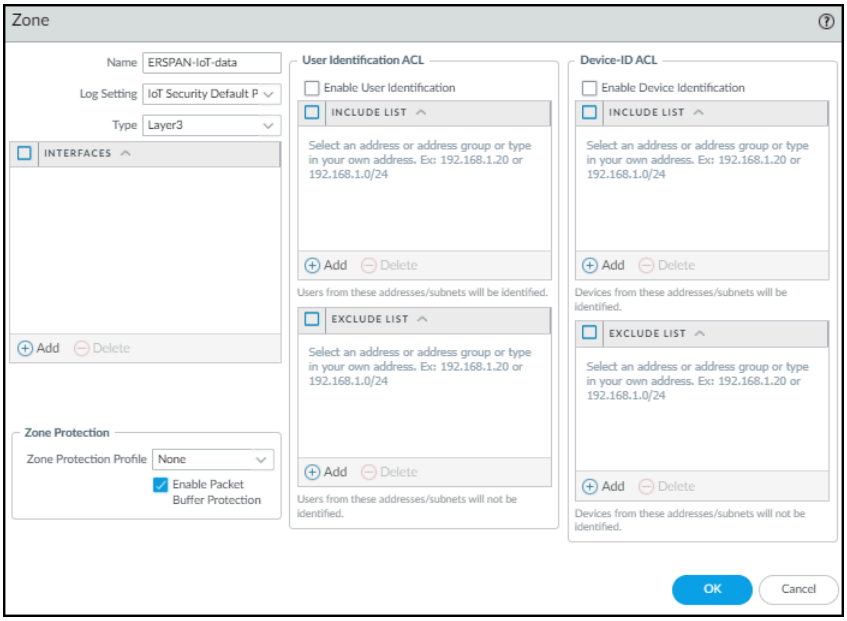
1. 选择 **Network**（网络） > **Zones**（区域），然后 **Add**（添加）一个区域。
2. 输入以下内容并将其他设置保留为默认值：

   Name（名称）：为区域输入一个有意义的名称，例如 **ERSPAN-IoT-data**。

   Log Setting（日志设置）：选择 **IoT Security Default Profile**（**IoT Security** 默认配置文件）或另一个日志转发配置文件，将所需类型的日志发送到 IoT Security 的日志记录服务。

   您必须已经在防火墙上启用日志记录服务。

   Type（类型）：**Layer3**



3. 单击 **OK**（确定）。

STEP 5 | 创建第 3 层接口并将其绑定到刚才创建的区域。

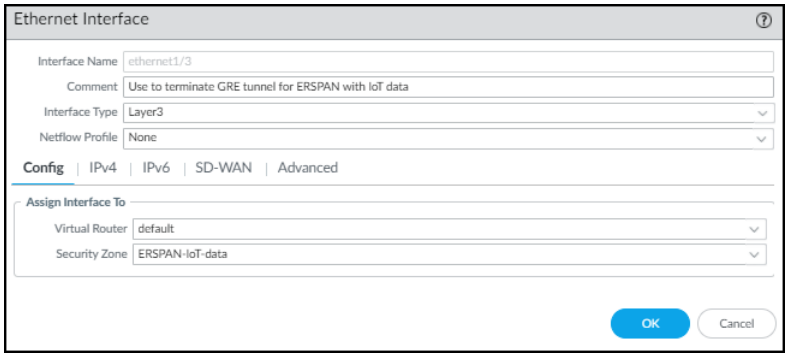
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后单击要从交换机终止 GRE 隧道的以太网接口。可选择使用子接口。
2. 输入以下内容并将其他设置保留为默认值：

   Comment（备注）：输入有关接口的有意义的备注，以供以后参考。

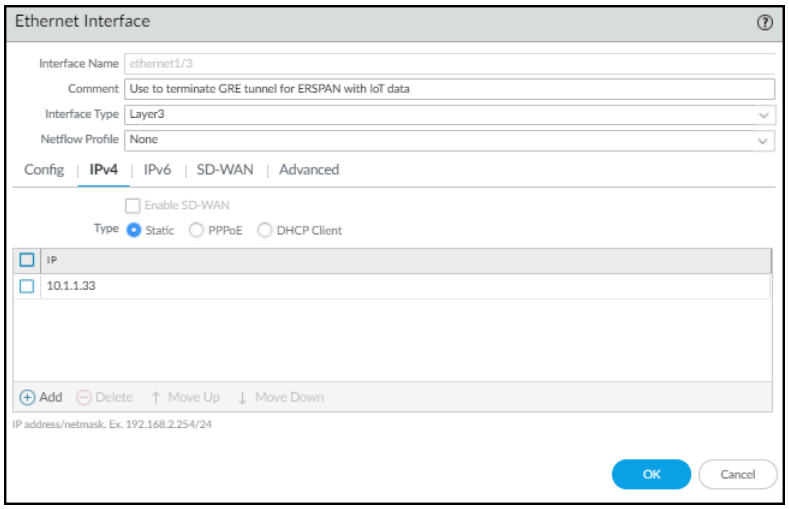
   Interface Type（接口类型）：**Layer3**

   Virtual Router（虚拟路由器）：选择您想要路由到接口的虚拟路由器。考虑使用专门用于 ERSPAN 流量的单独虚拟路由器。

   Security Zone（安全区域）：选择您刚才创建的区域。

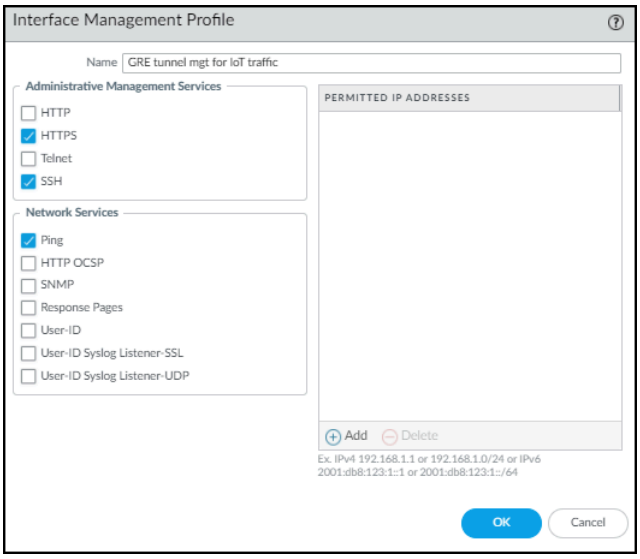


3. 单击 **IPv4**，选择 **Static**（静态）作为地址类型，并为接口 **Add**（添加）IP 地址。



   交换机在其 GRE 隧道配置中使用此地址作为其对等方的 IP 地址。

4. 单击 **Advanced**（高级），然后添加 **New Management Profile**（新管理配置文件）或选择之前定义的配置文件，允许以太网接口接受不同类型的管理流量。



5. 单击 **OK**（确定）保存新的接口管理配置文件，然后再次单击 **OK**（确定）保存以太网接口配置。

STEP 6 | 创建一个隧道接口，其 IP 地址与交换机上相应隧道接口位于同一子网，并将其绑定到刚才创建的区域。

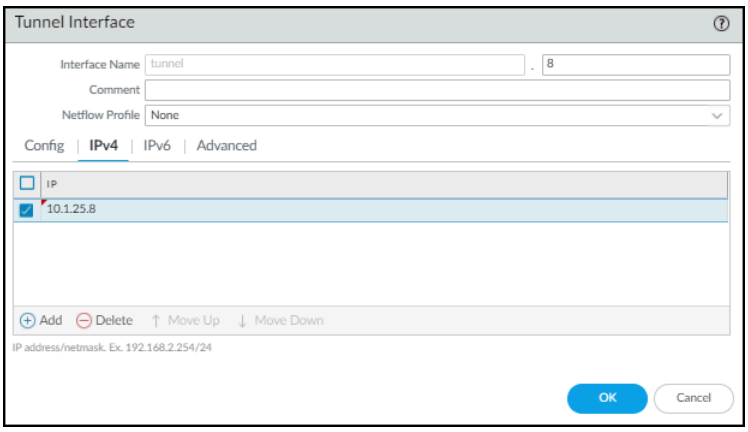
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Tunnel**（隧道），然后从交换机 **Add**（添加）GRE 隧道的逻辑隧道接口。
2. 输入以下内容并将其他设置保留为默认值：

   Interface Name（接口名称）：左侧的字段是只读的，包含文本“隧道”。在右侧的字段中输入一个数字以补全名称。例如，输入 **8** 以创建名称 `tunnel.8`。

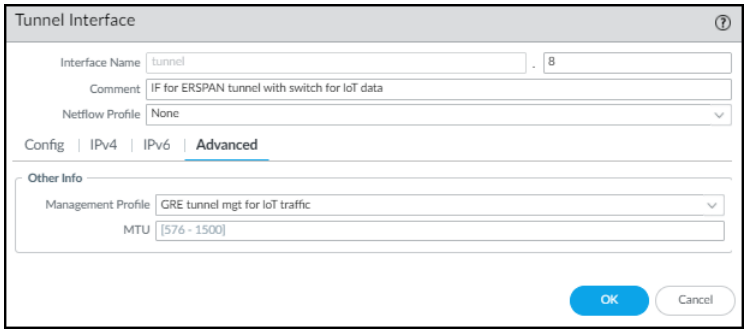
   Virtual Router（虚拟路由器）：选择与第 3 层接口相同的路由器。

   Security Zone（安全区域）：选择与第 3 层接口绑定的同一区域。

3. 单击 **IPv4** 并 **Add**（添加）与交换机上逻辑隧道接口的 IP 地址位于同一子网中的 IP 地址。



4. 单击 **Advanced**（高级）并添加 **New Management Profile**（新管理配置文件），或选择之前定义的配置文件，以允许隧道接口接受不同类型的管理流量。



5. 单击 **OK**（确定）。

STEP 7 | 为 ERSPAN 的虚拟路由器 (VR) 配置静态路由。

1. 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后单击 ERSPAN 的虚拟路由器。
2. 单击 **Static Routes**（静态路由），然后单击 **+ Add**（添加）。
3. 输入以下内容并将其他设置保留为默认值：

   名称：输入静态路由的名称。

   Destination（目标）：**0.0.0.0/0**

   如果您知道交换机以外的子网，请为每个子网创建单独的静态路由。否则，为 *ERSPAN* 使用单独的 *VR* 并设置默认路由。

   Interface（接口）：**ethernet1/3**（您之前配置的接口）

   Next Hop（下一个跃点）：无
4. 单击 **OK**（确定）。

STEP 8 | 配置启用了 ERSPAN 的 GRE 隧道。

1. 选择 **Network**（网络） > **GRE Tunnels**（**GRE** 隧道），然后单击 **+ Add**（添加）。
2. 输入以下内容并将其他设置保留为默认值：

   名称：输入 GRE 隧道的名称；例如，**`GRE-ESPAN-for-IoT-data`**

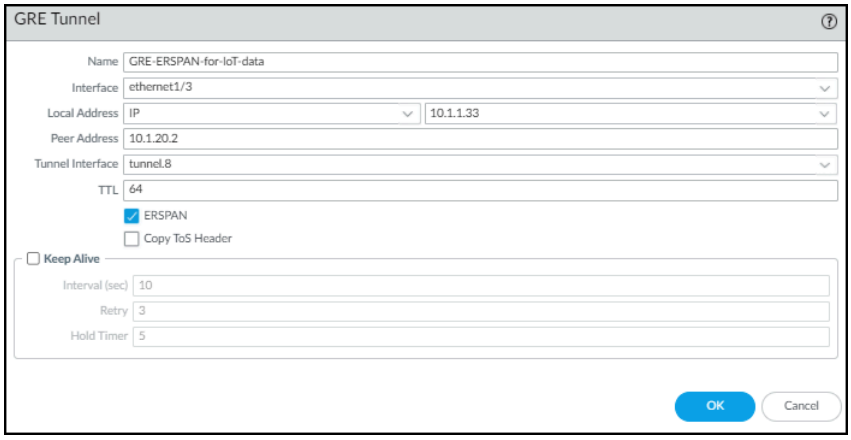
   Interface（接口）：选择为 GRE 隧道终止配置的第 3 层接口。

   Local Address（本地地址）：选择 **IP** 以及 GRE 隧道终止的第 3 层接口的 IP 地址。

   Peer Address（对等设备地址）：输入启动 GRE 隧道的交换机出口接口的 IP 地址。

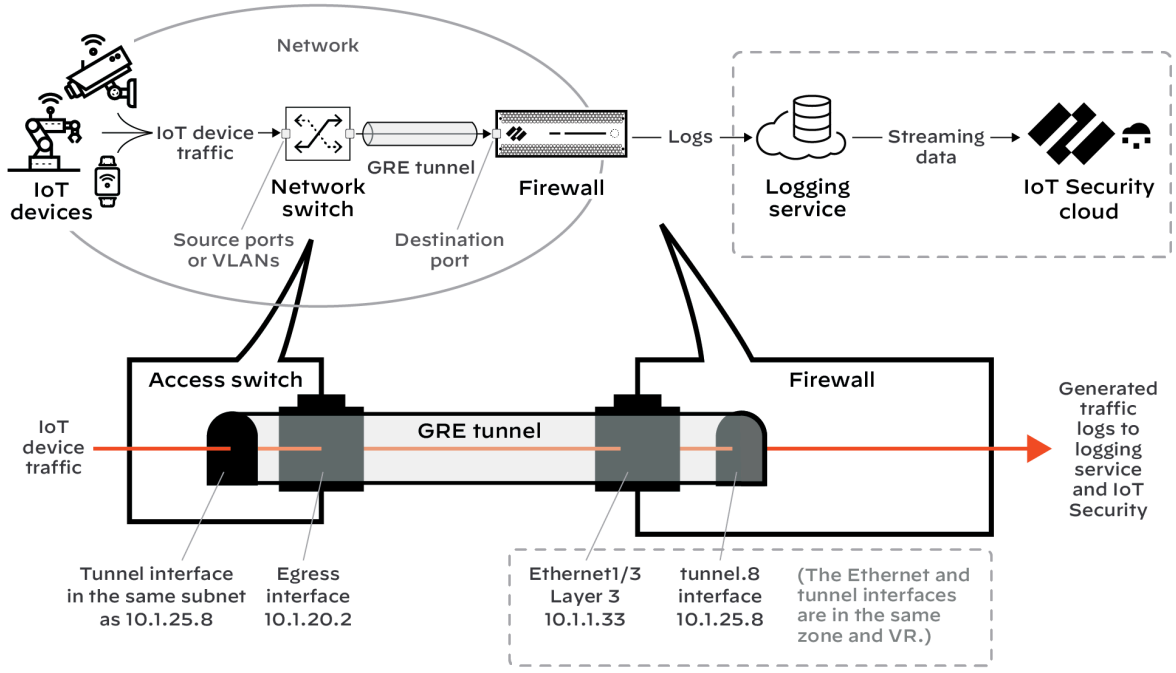
   Tunnel Interface（隧道接口）：选择为 GRE 隧道配置的逻辑隧道接口。

   ERSPAN：（选择）



3. 单击 **OK**（确定）。

   以太网和隧道接口的 IP 地址彼此相关，并且与网络的其余部分相关，如下所示。

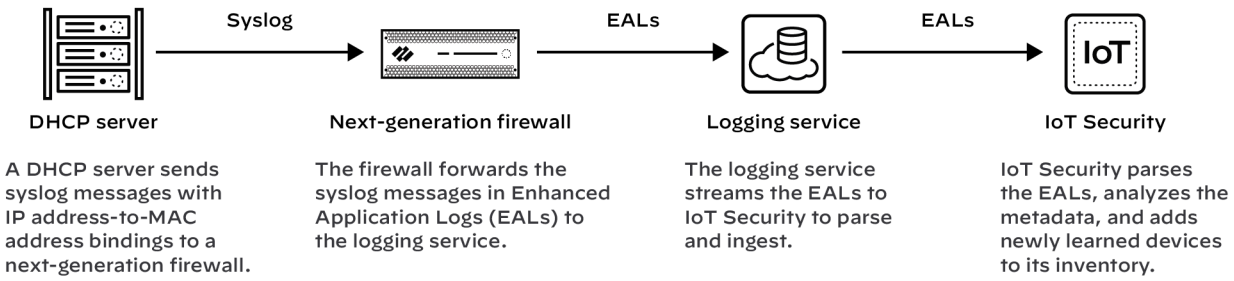


STEP 9 | **Commit**（提交）更改。

使用 DHCP 服务器配置提高设备可见性

IoT Security 依赖于 IP 地址到 MAC 地址的绑定，将观察到的网络行为归因于 IoT 设备并对其进行唯一跟踪。IoT Security 通常使用 DHCP 流量来了解 IP 地址到 MAC 地址的绑定并跟踪 IP 地址的变化。但是，在新一代防火墙不在 DHCP 数据路径中的设计中，您可以使用此方法来提取 DHCP 服务器日志并扩展 DHCP 流量可见性。

在难以将 DHCP 流量路由到或通过防火墙的网络区域中，配置 DHCP 服务器以将其服务器日志作为 syslog 消息发送到防火墙。然后，防火墙通过日志记录服务将消息作为子类型为 dhcp-syslog 的增强应用程序日志 (EAL) 转发到 IoT Security。IoT Security 将进行解析以了解 IP 地址到 MAC 地址的绑定，然后将新了解的设备添加到其清单中。IoT Security 还从服务器日志中了解设备主机名，但 Cisco DHCP 服务器的日志除外。



先决条件

- 具有 syslog 功能的 DHCP 服务器配置为可将消息发送到在新一代防火墙上运行的 syslog 服务器

- 运行 PAN-OS 11.0 或更高版本并具有活动 IoT Security 订阅的新一代防火墙

DHCP 服务器日志提取不适用于 *CN-*、*M-* 和 *WF* 系列新一代防火墙。

设置新一代防火墙

设置您的新一代防火墙，以从一个或多个 DHCP 服务器接收 syslog 消息。防火墙会自动将其收到的 syslog 消息作为 EAL 转发到日志服务，日志服务将其流式传输到 IoT Security 进行解析和分析。

STEP 1 | 向新一代防火墙添加 DHCP 服务器。

登录您的新一代防火墙，选择 **Device**（设备） > **IoT** > **+ Add**（添加），配置以下内容，然后单击 **OK**（确定）：

名称：输入 DHCP 服务器的名称。其最多可以包含 32 个字符，包括空格。

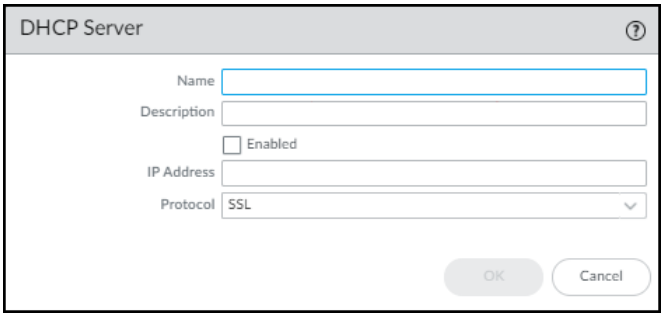
Description（说明）：输入有关 DHCP 服务器的备注，以备将来参考。其最多可以包含 256 个字符，包括空格。

Enabled（已启用）：选择以启用防火墙侦听来自 DHCP 服务器的连接，并在连接到来时进行处理。

IP Address（**IP** 地址）：输入 DHCP 服务器将连接到防火墙的 IP 地址。地址可以是 IPv4 或 IPv6 格式。不允许使用 FQDN。

Protocol（协议）：选择 **TCP**、**UDP** 或 **SSL**。在做出选择时，请考虑对于 DHCP 服务器和防火墙之间的连接来说哪些内容比较重要。TCP 具备传输可靠性，但不具备安全性。UDP 的处理开销更低，速度更快，但可靠性和安全性不足。SSL 提供可靠性和安全性，但会产生更多开销。

防火墙在端口 *10514* 上使用 *TCP* 和 *UDP* 侦听 *DHCP* 服务器连接，并在端口 *16514* 上使用 *SSL* 侦听连接。



STEP 2 | 重复上一步以添加更多 DHCP 服务器。

根据需要，添加更多 DHCP 服务器，以扩展整个网络中 DHCP 流量的可见性。所有新一代防火墙，每个防火墙最多支持 100 个 DHCP 服务器。

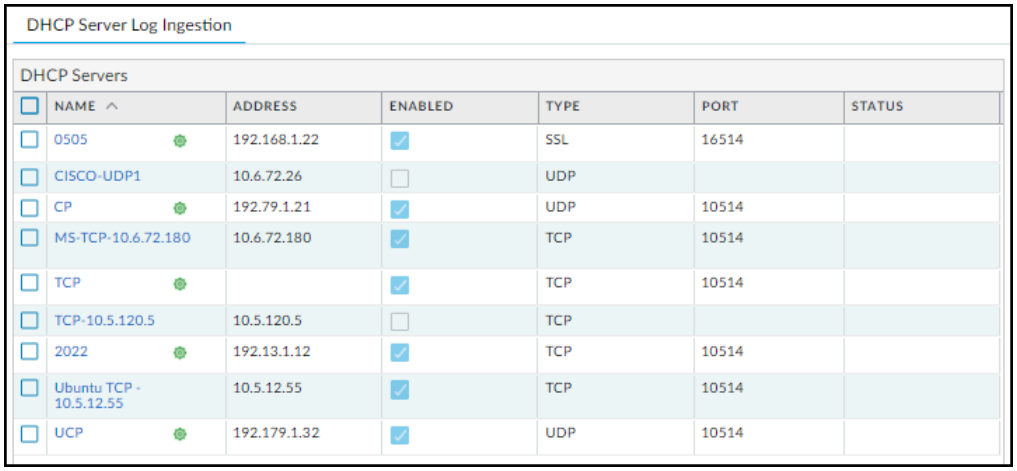
为 Syslog 设置 DHCP 服务器

配置您的 DHCP 服务器，以将其服务器日志的 syslog 消息发送到新一代防火墙上的管理接口。确保将 DHCP 服务器配置为使用防火墙上为其配置的相同协议：TCP、UDP 或 SSL。例如，您可以

使用 DHCP 服务器，例如 Windows、Linux、Cisco 或 Infoblox。有关配置说明，请参阅 DHCP 服务器的文档。

检查 DHCP 服务器连接状态

要查看所有已配置的 DHCP 服务器，请选择 **Device**（设备） > **IoT**。



DHCP 服务器名称旁边的绿色圆圈表示其在 Panorama 中予以配置，并且在本地新一代防火墙的 Web 接口中查看时为只读状态。

当使用 TCP 或 SSL 的 DHCP 服务器当前连接到防火墙时，“状态”列会显示“已连接”。如果在过去两个小时内连接了使用 UDP 的 DHCP 服务器，则“状态”列也会显示“已连接”。在所有其他时间，状态列为空，表示服务器当前未连接到防火墙。

以下 CLI 命令也可用于检查 DHCP 服务器设置、连接状态及其提供给 IoT Security 的数据。

`show iot dhcp-server status { all | server <server-name> }`	输入 `all` 会显示一个表格，其中包含防火墙上配置和启用的所有 DHCP 服务器、连接的端口号及其当前的连接状态。 输入 `server<server-name>` 会显示有关特定 DHCP 服务器及其最近活动的详细信息。
`show iot eal dhcp-syslog-eal`	此命令显示与携带 DHCP 服务器 syslog 消息的 EAL 相关的信息。

当防火墙服务于 DHCP 时规划扩展

本节讨论当防火墙提供 DHCP 服务时如何扩展解决方案，如使用 DHCP 服务器配置 PAN-OS 10.0 之前的防火墙中所述。

将 VLAN 子接口的数量与物理接口对齐

为了保持一致性，请将 VLAN 子接口号与它们所服务的物理接口号对齐。例如，接口 vlan.1 为连接到 ethernet1/1 的网络提供 DHCP 服务。这使得您可以更快地将它们相互关联，并在以后更轻松地解决问题。

Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3	Inside_Manage...		10.1.0.1/24
ethernet1/2	Layer3	Inside_Manage...		10.2.0.1/24
ethernet1/3	Layer3	Inside_Manage...		10.3.0.1/24

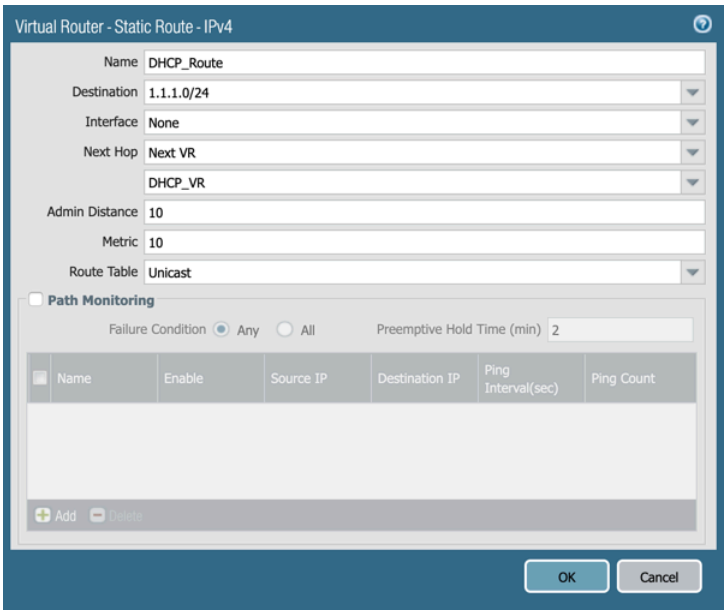
Interface	Management Profile	IP Address	Virtual Router
vlan		none	none
vlan.1	Inside_Manage...	1.1.1.1/32	DHCP_VR
vlan.2	Inside_Manage...	1.1.1.2/32	DHCP_VR
vlan.3	Inside_Manage...	1.1.1.3/32	DHCP_VR

保留 VLAN 子接口的 IP 地址

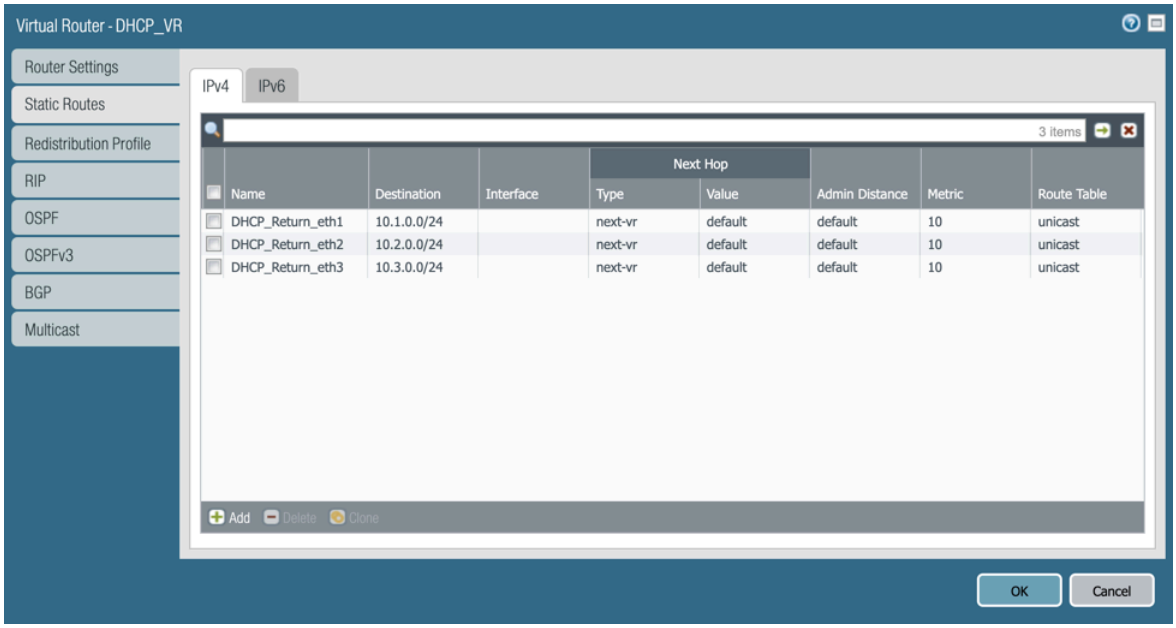
当生产 IP 地址空间用于 VLAN 接口时，为它们提供具有 32 位网络掩码的 IP 地址将节省地址空间。您可以对所有 VLAN 接口使用单个网络的地址（例如 1.1.1.0/24）。由于这些接口仅用于为本地网络提供 DHCP，因此分配给 VLAN 接口的地址不需要在企业的其余部分可路由。从操作上讲，这意味着企业中所有防火墙的 VLAN 接口都可以使用相同的网络空间和地址。

配置到所有 VLAN 接口的网络路由

为多个接口配置此解决方案时，路由配置会略有变化。在默认（生产）虚拟路由器上，您可以配置到 VLAN 接口的网络路由，而不是主机路由集合。下图中，所有 VLAN 接口都有可使用 1.1.1.0/24 路由汇总的地址。



在 DHCP 虚拟路由器上，为 VLAN 接口提供 DHCP 的每个网络添加网络路由，并将默认（生产）虚拟路由器设置为下一跳。为 DHCP 中继代理添加网络路由而不是主机路由可以使 DHCP 服务器上的探测功能正常运行。



为 IoT Security 准备好您的防火墙

以下步骤介绍如何在新一代防火墙上启用日志记录服务，并将其配置为获取和记录网络流量元数据。然后，它解释了如何将收集的元数据转发到基于云的日志记录服务，IoT Security 使用这些服务来识别网络上的各种 IoT 设备。

以下步骤假定您已经完成 IoT Security 加入流程，但仍需要执行以下操作：

- 在防火墙上安装设备许可证和日志记录服务许可证。
- 在防火墙上安装证书（如果尚未安装）。
- 配置防火墙以收集网络流量元数据。
- 配置防火墙，以便将日志中收集的元数据转发到日志记录服务。
- 在具有要使用安全策略规则监视和保护的设备的区域上启用 Device-ID。
- （可选）创建服务路由和安全策略规则，以允许防火墙通过数据接口与日志记录服务、IoT Security 以及更新服务器进行通信。

有关为 *IoT Security* 配置防火墙的其他详细信息，请参阅 Device-ID。

STEP 1 | 安装 IoT Security 功能所需的许可证。

加入 IoT Security 后，请执行以下操作之一，以安装防火墙使用 IoT Security 所需的许可证：

新一代防火墙：：登录每个防火墙，选择 **Device**（设备） > **Licenses**（许可证），然后在 License Management（许可证管理）部分选择 **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）。

或者

Panorama：登录 Panorama，选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证），然后 **Refresh**（刷新）。选择使用 IoT Security 加入的设备并 **Refresh**（刷新）。

该操作将在防火墙上安装 IoT Security 和日志记录服务的许可证。

需要续订 *IoT Security* 许可证时，请在防火墙上使用此检索功能，以便延长许可证到期日期。

STEP 2 | 如有必要，生成一次性密码 (OTP) 和预共享密钥 (PSK) 以获取设备和日志记录服务证书。

此步骤仅适用于具有 *IoT Security*，但“不需要数据湖订阅”的防火墙。如果您的防火墙有 *IoT Security* 订阅（需要 *Strata Logging Service*），请参阅 Strata Logging Service 入门，了解有关生成证书并将其安装在防火墙上的详细信息。

- 搭载 **PAN-OS 10.1** 或更高版本的防火墙

  如果您的防火墙运行 *PAN-OS 10.1* 或更高版本，并且已安装设备证书，请跳过此步骤。您以前为其他 *Palo Alto Networks* 产品安装过设备证书的任何防火墙都已具有此证书，不需要新的证书。您可以在 *PAN-OS Web* 用户界面的指示板页面上的“常规信息”部分检查防火墙是否具有有效的证书。

  运行 PAN-OS 10.1 或更高版本的防火墙需要设备证书，但不需要日志记录服务证书。

  以下新一代防火墙型号在首次连接到客户支持门户 (CSP) 时会自动安装设备证书；因此，您不必在运行这些 PAN-OS 版本的任何这些防火墙上手动安装证书：

  - **PAN-OS 10.1**：PA-410、PA-440、PA-450、PA-460 和 PA-5450 防火墙
  - **PAN-OS 10.2**：PA-410、PA-440、PA-450 和 PA-460 防火墙；PA-1400 系列和 PA-3400 系列防火墙；PA-5410、PA-5420、PA-5430 和 PA-5450 防火墙
  - **PAN-OS 11.0**：PA-400 系列、PA-1400 系列、PA-3400 系列、PA-5400 系列和 PA-5450 系列防火墙

  另外，您以前为其他 Palo Alto Networks 产品安装过设备证书的任何防火墙都已经有了设备证书，不需要新的证书。

  检查以下问题和答案，以确定何时在防火墙上生成和安装设备证书。

防火墙是否已具有设备证书？	防火墙是否已具有日志记录服务证书？	有 **Panorama** 管理的防火墙吗？	做什么？
是	N/A	N/A	跳过此步骤。
否	N/A	是	输入 Panorama 序列号，在客户支持门户中生成 OT，,然后在 Panorama 中输入以生成设备证书。

防火墙是否已具有设备证书？	防火墙是否已具有日志记录服务证书？	有 Panorama 管理的防火墙吗？	做什么？
否	N/A	否	在客户支持门户中生成 OTP，并在防火墙上安装设备证书。

- 使用 **PAN-OS 10.0** 的防火墙

  如果您的防火墙运行 *PAN-OS 10.0* 并且已安装设备和日志记录服务证书，请跳过此步骤。您以前安装过其他 *Palo Alto Networks* 产品的设备证书和日志记录服务证书的任何防火墙都已经有了这些证书，不需要新的证书。您可以在 *PAN-OS Web* 用户界面的指示板页面上的“常规信息”部分检查防火墙是否具有有效的证书。

  检查以下问题和答案，以确定何时在防火墙上生成并安装设备和日志记录服务证书。

防火墙是否已具有设备证书？	防火墙是否已具有日志记录服务证书？	有 Panorama 管理的防火墙吗？	做什么？
是	是	N/A	跳过此步骤。
是	否	是	输入 Panorama 序列号，复制OTP，然后在 Panorama 上安装云服务附加组件时输入。
是	否	否	复制预共享密钥并将其粘贴到 PAN-OS 防火墙中以生成日志记录服务证书。
否	是	是	输入 Panorama 序列号，然后使用 Panorama 生成并在一个或多个防火墙上安装设备证书。
否	是	否	在客户支持门户中生成 OTP，并在防火墙上安装设备证书。
否	否	是	复制 OTP，在 Panorama 上安装云服务附加组件时输入。当 Panorama 向

防火墙是否已具有设备证书？	防火墙是否已具有日志记录服务证书？	有 Panorama 管理的防火墙吗？	做什么？
			没有日志记录服务和设备证书的防火墙推送需要日志记录服务和 IoT Security 的配置时，防火墙会通过请求证书来响应 Panorama。
否	否	否	在客户支持门户中生成 OTP，并在防火墙上安装设备证书。 复制预共享密钥并将其粘贴到 PAN-OS 防火墙中以生成日志记录服务证书。

- 运行 **PAN-OS 8.1–9.1** 的 **Panorama** 托管防火墙

> 如果您的防火墙由 *Panorama* 托管，运行 *PAN-OS 8.1-9.1*，并且已安装日志记录服务证书，请跳过此步骤。您以前安装过其他 *Palo Alto Networks* 产品日志记录服务证书的任何防火墙都不需要新的防火墙。您可以在 *PAN-OS Web* 用户界面的指示板页面上的“常规信息”部分检查防火墙是否具有有效的证书。

检查以下问题和答案，以确定何时在防火墙上生成并安装日志记录服务证书。

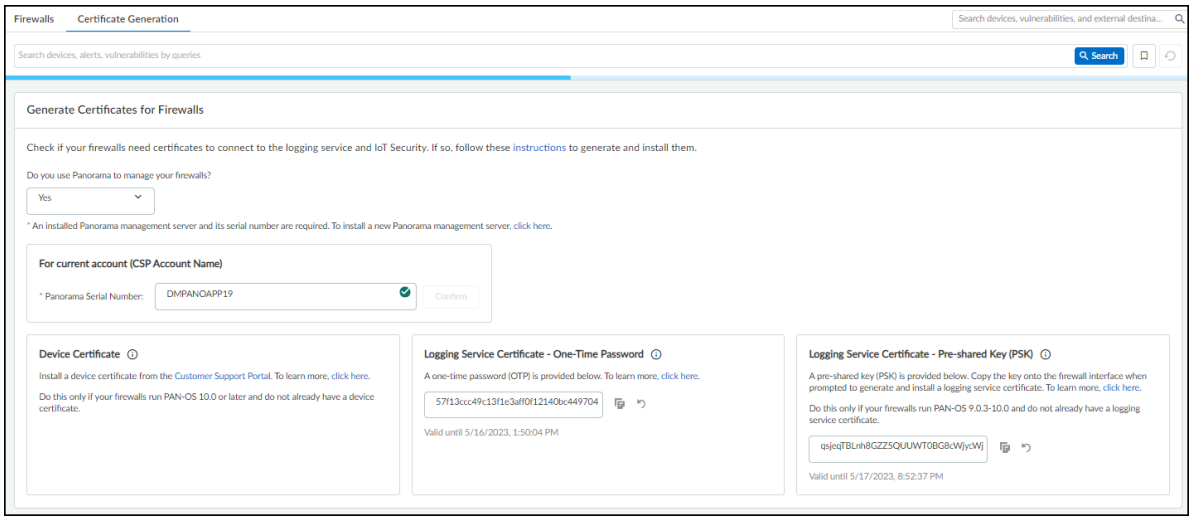
防火墙是否已具有设备证书？	防火墙是否已具有日志记录服务证书？	有 Panorama 管理的防火墙吗？	做什么？
N/A	是	是	跳过此步骤。
N/A	是	否	如果防火墙正在运行 PAN-OS 9.0.3-9.1，无论是否有 Panorama 托管，请跳过此步骤。 运行 PAN-OS 8.1–9.0.2 的防火墙需要 Panorama 才能获得日志记录服务证书。如果您没有使用这些 PAN-OS 版本来使用 Panorama 管理防火墙，则您的防火

防火墙是否已具有设备证书？	防火墙是否已具有日志记录服务证书？	有 **Panorama** 管理的防火墙吗？	做什么？
			墙将无法将日志发送到日志记录服务以支持 IoT Security。
N/A	否	是	复制 OTP，在 Panorama 上安装云服务附加组件时输入。当 Panorama 将需要日志记录服务的配置推送到没有日志记录服务证书的防火墙时，防火墙会通过请求它来响应 Panorama。
N/A	否	否	运行 PAN-OS 8.1–9.0.2 的防火墙需要 Panorama 管理获取日志记录服务证书；如果没有 Panorama，则无法支持 IoT Security。对于运行 PAN-OS 9.0.3-9.1 而没有 Panorama 管理的防火墙，复制预共享密钥并将其粘贴到 PAN-OS 防火墙中，以生成日志记录服务证书。

有关新一代防火墙在与 *IoT Security* 通信时联系以验证证书的站点的信息，请参阅IoT Security 与新一代防火墙集成。

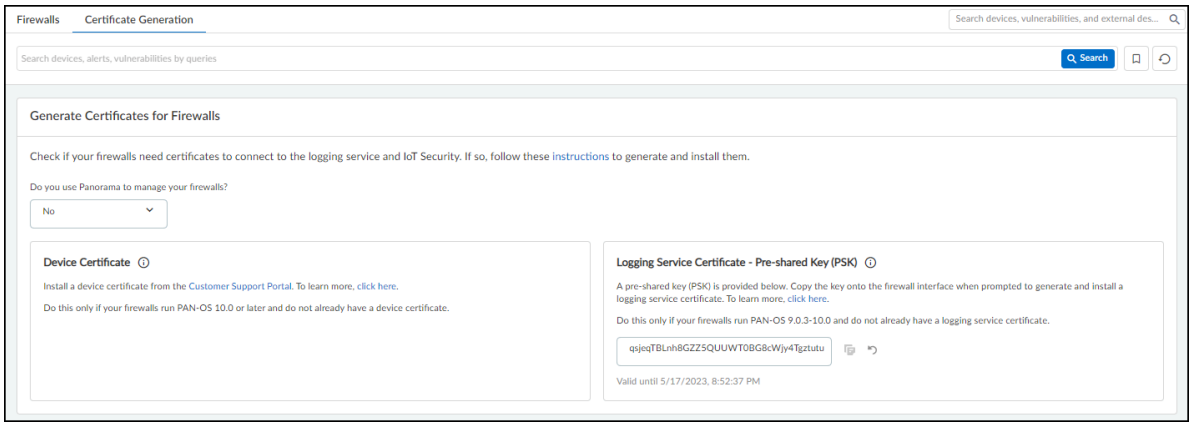
1. 以具有所有者权限的用户身份登录 IoT Security 门户。要能够生成 OTP 和 PSK，必须在客户支持门户 (CSP) 中创建用户帐户，并在身份和访问中的相关租户服务组 (TSG) 中分配超级用户角色。Hub 中的超级用户角色在 IoT Security 中提供所有者权限。
2. 选择 **Administration**（管理） > **Firewalls**（防火墙） > **Certificate Generation**（生成证书）。
3. 如果您使用 Panorama 管理防火墙，请选择 **Yes**（是）并输入其序列号。这会将您的 Panorama 管理服务器链接到此 TSG 中的应用程序。您可以在 **Assets**（资产） > **Devices**（设备）的 Customer Service Portal（客户服务门户）帐户中找到 Panorama 序列

号。选择 **Yes**（是）并输入您的 Panorama 序列号后，IoT Security 将显示获取证书所需的材料，防火墙需要这些材料来保护与 IoT Security 和日志记录服务的连接。



要获取设备证书，请单击客户支持门户的链接，登录到您的帐户，然后按照下面的说明操作。要生成日志记录服务证书，请复制 OTP 或 PSK,然后按照下面的说明进行操作。

如果您不使用 Panorama，请选择 **No**（否）。因为日志记录服务证书的 OTP 仅适用于 Panorama，所以不显示。



在决定需要哪些证书以及如何生成证书时，请考虑以下几点：

Device Certificate（设备证书）：从 PAN-OS 10.0 开始，防火墙需要设备证书才能使用 IoT Security 进行身份验证，从 PAN-OS 10.1 开始，防火墙还需要使用日志记录服务进行身份验证。要在防火墙上直接或通过 Panorama 生成并安装设备证书，请执行以下操作：

- 在每个防火墙上生成并安装设备证书。
- 使用 Panorama 在一个或多个防火墙上生成并安装设备证书。

> 如果设备证书安装在防火墙，以便它可以向日志记录服务和 *IoT Security* 进行身份验证时，防火墙无法解密加密流量以对其进行检查并强制执行策略规则。因此，不要试图在安装了设备证书的防火墙上使用解密策略规则。

登录服务证书 — 一次性密码：Panorama 需要使用其日志记录服务实例验证自身，并为运行 PAN-OS 8.1-10.0 的 Panorama 管理的防火墙获取日志记录服务证书。日志记录服务证书通过日志记录服务验证防火墙。

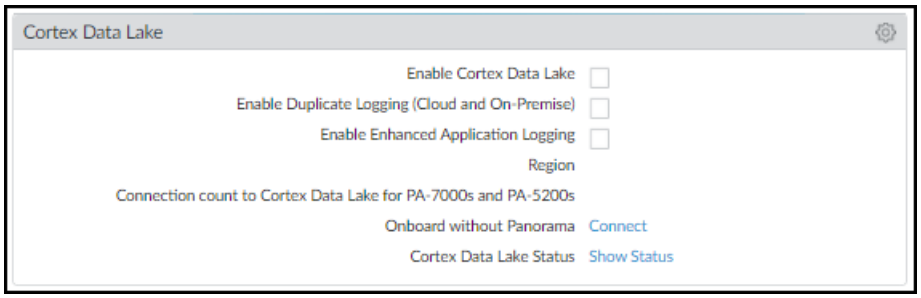
1. 如有必要，重新生成 OTP 并复制它。
2. 以管理员用户身份登录 Panorama 网页界面，然后选择 **Panorama** > **Setup**（设置） > **Management**（管理） > **Device Certificate**（设备证书）和 **Get certificate**（获取证书）。

3. 粘贴 OTP，然后单击 **OK**（确定）。

Logging Service Certificate – **Pre-Shared Key**（日志记录服务证书 — 预共享密钥）：在没有运行 PAN-OS 9.0.3-10.0.x 的 Panorama 管理的情况下，需要在防火墙上生成日志记录服

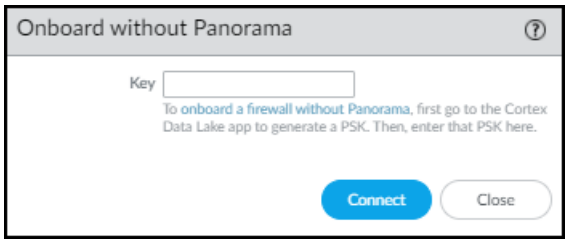
务证书。日志记录服务证书通过日志记录服务验证防火墙。要生成日志记录服务证书，请执行以下操作：

1. 如有必要，重新生成 PSK 并复制它。
2. 登录您的 PAN-OS 9.0.3-10.0.x 防火墙，然后选择 **Device**（设备） > **Setup**（设置） > **Management**（管理）。



3. 在 Strata Logging Service 部分中，单击“在没有 Panorama 的情况下加入”旁的 **Connect**（连接）。

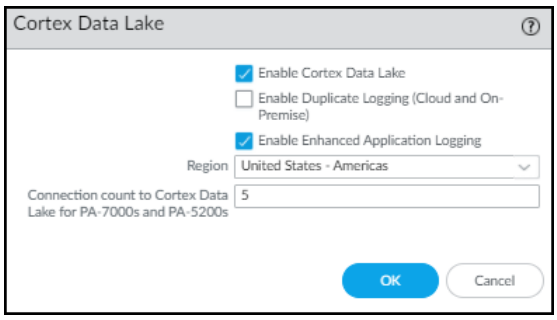
   这将打开“在没有 Panorama 的情况下加入”对话框。



4. 粘贴 PSK 并 **Connect**（连接）。

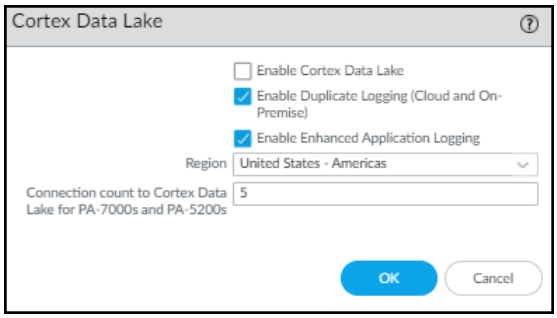
   防火墙首先连接到客户支持门户，提交 PSK，然后下载日志记录服务证书。然后，它使用证书进行身份验证并安全地连接到日志记录服务。

5. 单击 Strata Logging Service 的 **Edit**（编辑）图标（齿轮）。选择 **Enable Strata Logging Service**（启用日志记录服务）和 **Enable Enhanced Application Logging**（启用增强型应用程序日志记录）。



   或者

   如果您拥有 IoT Security — 不需要数据湖许可证，请选择 **Enable Duplicate Logging (Cloud and On-Premises) [**启用重复日志记录（云和本地部署）**]** 和 **Enable Enhanced Application Logging**（启用增强型应用程序日志记录）。



6. 选择日志记录服务将从防火墙接收日志的区域。

   对于 PA-7000 和 PA-5200 型号，请输入从防火墙向日志记录服务发送日志的连接数。范围为 1-20，默认值为 5。

7. 完成后，请单击 **OK**（确定）。

> *"Strata Logging Service"*有些用词不当。防火墙将日志转发到日志记录服务，该服务仅在您使用日志进行数据保留时将其流式传输到 *Strata Logging Service*。一种 *IoT Security*，"不需要数据湖订阅"根本不使用 *Strata Logging Service*，但它仍然需要启用此设置。

STEP 3 | 确保您的防火墙设置为将策略应用于 DHCP 客户端与其 DHCP 服务器之间的 DHCP 流量，并记录其流量。

有关设置防火墙以捕获和记录 DHCP 流量的详细说明，请参阅部署防火墙以实现设备可见性。

如果防火墙运行的是 PAN-OS 10.0 或更高版本，其某个接口上带有 DHCP 服务器，请在 **Device**（设备） > **Setup**（设置） > **Session**（会话）上启用 **DHCP Broadcast Session**（**DHCP** 广播会话）。运行 PAN-OS 10.1.10 或更高版本、PAN-OS 10.2.4 或更高版本以及 PAN-OS 11.0.1 或更高版本的所有防火墙均支持此设置。（有关详细信息，请参阅IoT Security 的防火墙部署选项）

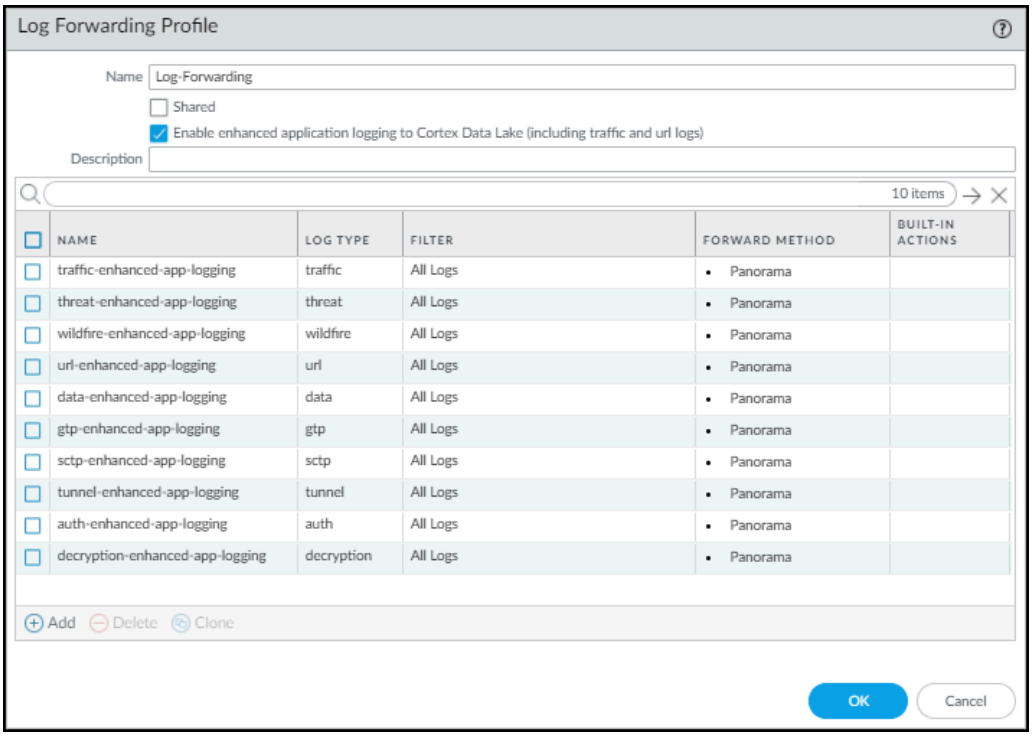
> 除了检测具有动态分配的 *IP* 地址的设备，*IoT Security* 还可以发现和识别具有静态 *IP* 地址的设备。要了解 *IoT Security* 用于执行此操作的多种方法以及如何提供帮助，请参阅具有静态 IP 地址的设备。

STEP 4 | 要将日志转发到日志记录服务，请单击 **Objects**（对象） > **Log Forwarding**（日志转发），然后单击 **Add**（添加）。

在防火墙上配置日志转发配置文件，将增强的应用程序日志发送到日志记录服务，以便 IoT Security 应用能够接收网络流量数据。或者，您可以编辑现有配置文件，而不是添加新配置文件。

STEP 5 | 在日志转发配置文件中，输入一个名称，如 Log-Forwarding，单击 Strata Logging Service 的 **Enable enhanced application logging**（启用增强型应用程序日志记录（包括流量和 URL 日志），然后单击 **OK**（确定）。

*PAN-OS 8.1*引入了增强的应用程序日志记录。



增强型应用程序日志列表会自动填充页面，并将每种类型的所有日志转发到日志记录服务。选择 Strata Logging Service 的 **Enable enhanced application logging**（启用增强型应用程序日志记录）（包括流量和 URL 日志），可使防火墙除捕获这些不同日志类型的会话元数据（常规日志）外，还捕获数据包有效负载数据 (EAL)。当此日志转发配置文件附加到安全策略规则以控制

流量时，防火墙会将这两种类型的数据转发到日志记录服务。您不能从配置文件中删除这些日志，也不能修改过滤器列中的任何过滤器，它们是默认的"所有日志"过滤器。

下面介绍每种日志类型，说明 IoT Security 是否使用它，以及它的用途：

- 流量 — 流量日志包含每个网络会话结束以及可选的网络会话开始的条目。IoT Security 使用流量日志来识别设备、生成策略规则建议、风险评估、设备行为异常检测、关联会话以及发出安全警报。
- **threat** — 威胁日志包含网络流量与附加到新一代防火墙的安全配置文件之一匹配时的条目安全策略规则。IoT Security 使用威胁日志评估风险、检测漏洞、发出安全警报并生成策略规则建议。
- **wildfire** — WildFire® 日志包含有关 WildFire 安全配置文件何时附加到安全策略规则以及文件何时通过网络的条目。IoT Security 使用 WildFire 日志检测特定于 IoT 的基于文件的攻击，发出安全警报，并生成策略规则建议。
- **url** — 每当网络流量与安全策略规则附加的 URL 过滤配置文件匹配时，都会写入 URL 日志。IoT Security 当前不使用 URL 过滤日志。
- **data** — 数据日志可以表示成功的文件数据传输，也可以表示被防火墙阻止的文件传输尝试。IoT Security当前不使用数据日志。
- **gtp**（启用 GTP 时）— 每当防火墙处理来自 3G、4G 和 5G 蜂窝设备的流量时，都会写入 GTP 日志。IoT Security 会使用此流量中的元数据来识别蜂窝设备及其网络行为。如果此类流量不在网络上，防火墙不会生成 GTP 日志，您可以放心忽略 IoT Security 门户中 **Administration**（管理） > **Firewalls**（防火墙）上“状态”列中显示的红色图标。
- **sctp**（启用 SCTP 时）— 每当防火墙处理流控制传输协议流量时，都会写入 SCTP 日志。IoT Security 当前不使用 SCTP 日志。
- **tunnel** — 每当防火墙处理通用路由封装 (GRE) 或空加密 IPsec 流量时，都会写入隧道日志。它们包含有关这些类型隧道内部流量的元数据。IoT Security 当前不使用隧道日志。
- **auth** — 身份验证日志包含有关防火墙看到的身份验证事件的信息。当用户访问受身份验证策略规则控制的网络资源时，会出现这种情况。IoT Security 当前不使用身份验证日志。
- **decryption** — 尽管 IoT Security 使用解密的 SSL 数据来改进设备识别、风险评估和威胁检测，但它不使用解密日志，这对于解决解密问题很有帮助。

如果将日志转发配置文件命名为 *“default”*(全小写)，防火墙将在新安全策略规则创建时 — 或从 IoT Security 导入时 — 自动将其应用于新安全策略规则。从 *IoT Security* 导入安全策略规则建议时，这样可以节省时间和精力。由于导入的规则建议不包含日志转发配置文件，因此您必须在导入规则后手动向每个规则添加一个日志转发配置文件。但是，通过将配置文件命名为“默认”，可以避免此步骤。（请注意，添加新的安全策略规则时将应用“默认”日志转发配置文件，但不会追溯应用于现有规则。）

STEP 6 | 对安全策略规则启用日志转发。

在适用于要收集其数据的流量的安全策略规则上，启用日志转发并选择您刚才创建的日志转发配置文件，以将此流量的增强型应用程序日志发送到日志记录服务。有关信息，请参阅配置日志转发策略。

STEP 7 | 启用想要使用 Device-ID 的所有区域中的 Device-ID，以检测设备，实施安全策略规则。

有关详细的配置说明，请参阅《PAN-OS 管理员指南》中的配置 Device-ID。

STEP 8 | （可选）创建服务路由。

默认情况下，防火墙使用其管理界面将数据日志发送到日志记录服务，从 IoT Security 获取推荐的策略规则集和 IP 地址到设备的映射，并从更新服务器下载设备字典文件。当防火墙使用其管理界面进行所有这些操作时，不需要服务路由和安全策略规则。

但是，当防火墙通过数据接口访问日志记录服务、IoT Security 和更新服务器时，则必须添加标识源数据接口、源接口 IP 地址和服务类型的服务路由。此外，您必须添加区域间安全策略规

则，允许将来自 127.168.0.0/16 的数据服务添加到日志记录服务、IoT Security 和更新服务器所在的目标区域。

当防火墙生成通过数据接口发送的流量时，它会使用 *127.168.0.0/16* 子网中的 *IP* 地址作为其内部源，然后将其转换为源接口的 *IP* 地址。由于安全策略规则应用于 *NAT* 之前的原始源 *IP* 地址，因此源 *IP* 地址必须是 *127.168.0.0/16*，而不是源接口的 *IP* 地址。

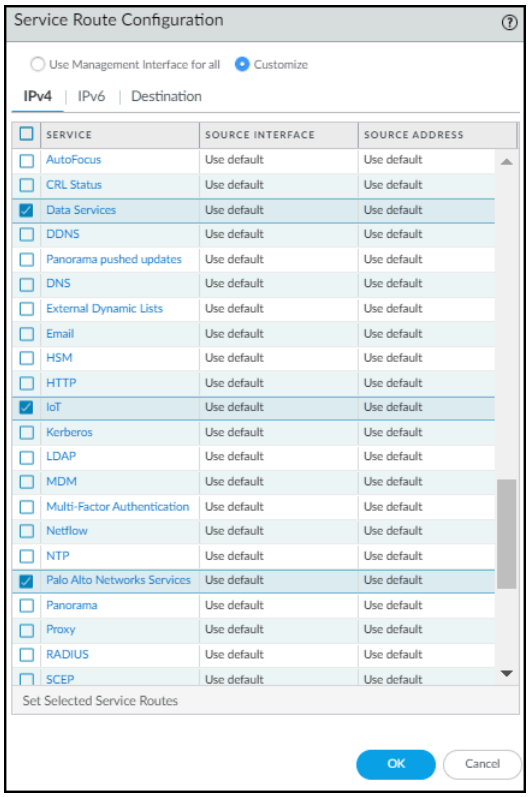
1. 如有必要，请配置数据接口，即 IoT Security 通信所需的源接口。
2. 选择 **Device**（设备） > **Setup**（设定） > **Services**（服务） > **Service Route Configuration**（服务路由配置），然后选择 **Customize**（自定义）。
3. 在 IPv4 选项卡中，选择 **Data Services**（数据服务），然后选择要用作源接口的数据接口。

   其 IP 地址会自动填入源地址字段。此服务路由用于将增强型应用程序日志 (EAL) 转发到日志记录服务。

   Device-ID 和 *IoT Security* 不支持 *IPv6*。
4. 单击 **OK**（确定）。
5. 点击 **IoT**，选择与源接口相同的数据接口，然后点击 **OK**（确定）。

   此服务路由用于从 IoT Security 中提取 IP 地址到设备的映射和策略建议。
6. 点击 **Palo Alto Networks Services**（**Palo Alto Networks** 服务），选择相同的数据接口，然后点击 **OK**（确定）。

   此服务路由用于将除 EAL 之外的其他日志转发到日志记录服务，以及用于从更新服务器拉取设备字典文件。
7. 单击 **OK**（确定）保存您的配置更改。



STEP 9 | （可选）如果您在上一步中创建了服务路由，请添加安全策略规则以允许防火墙使用 IoT Security 所需的服务。

1. 选择 **Policies**（策略） > **Security**（安全） > **+ Add**（添加）。
2. 在 General（常规）选项卡中，输入安全策略规则的名称，然后选择 **interzone**（区域间）作为规则类型。
3. 在 Source（源）选项卡中，选择 **Any**（任何） 作为源区域，然后 **Add 127.168.0.0/16**（添加 **127.168.0.0/16**）作为源地址。
4. 在“目标”选项卡中，**Add**（添加） 具有 IoT Security 的目标区域，然后将您所在区域的 边缘服务 FQDN **Add**（添加）为目标地址。
5. 在 Application（应用程序）选项卡中，**Add paloalto-iot-security**（添加 **paloalto-iot-security**）。

   防火墙使用此应用程序从 IoT Security 中提取 IP 地址到设备的映射和策略建议。
6. 在 Actions（操作）选项卡中，选择 **Allow**（允许），然后单击 **OK**（确定）。
7. 如果您有允许日志服务和更新服务器所在区域中的所有 Intranet 流量的 Intranet 策略规则，则可以使用该规则允许防火墙将日志转发到日志服务并从更新服务器中提取字典文件。

   否则，请创建一个 Intranet 策略规则，允许防火墙通过同一区域中防火墙接口的 IP 地址将这三个应用程序从发送到日志记录服务和更新服务器：

   paloalto-shared-services — 将 EAL 和会话日志转发到日志记录服务

   paloalto-logging-service — 将除 EAL 之外的其他日志转发到日志服务

   paloalto-updates — 从更新服务器中提取设备字典文件

STEP 10 | Commit（提交）配置更改。

配置提交后，防火墙开始生成日志并将其转发到日志记录服务。您可以使用 Hub 中的 Explore 应用程序查看防火墙和日志记录服务之间的日志转发进度。

配置日志转发策略

启用日志转发，以便防火墙将增强型应用程序日志 (EAL) 发送到 Palo Alto Networks 基于云的日志记录服务。然后，IoT Security 会从该服务获取元数据来进行分析。

配置区域间策略

如果 VLAN 接口设置在与它们配对的以太网接口不同的 L3 安全区域中，则必须配置安全策略规则才能使解决方案正常工作。下图显示了已配置多个 VLAN 接口来支持多个以太网接口时的示例规则。

			Source				Destination				
	Name	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	Allow_DHCP_Relay	universal	Office Prod_Line Wireless	10.1.0.1 10.2.0.1 10.3.0.1	any	any	DHCP Zone	1.1.1.0/24	dhcp	application-d...	Allow
2	Allow_DHCP_Probe	universal	DHCP Zone	1.1.1.0/24	any	any	Office	10.1.0.0/24 10.2.0.0/24 10.3.0.0/24	ping	application-d...	Allow
3	Allow_Interface_Testing	universal	Office Prod_Line Wireless	10.1.0.1 10.2.0.1 10.3.0.1	any	any	DHCP Zone	1.1.1.0/24	ping	application-d...	Allow
4	intrazone-default	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
5	interzone-default	interzone	any	any	any	any	any	any	any	any	Deny

策略规则 1：此策略规则允许从分配给接口 ethernet1/1 - ethernet1/3 的区域中继单播 DHCP 消息到 DHCP 区域。此外，启用日志转发并选择您之前创建的日志转发配置文件，以将此流量的 EAL 发送到日志记录服务。

如果将日志转发配置文件命名为“默认”（全部小写），则防火墙将在创建新的安全策略规则时或从 IoT Security 导入安全策略规则时，自动将其应用于新的安全策略规则。执行此操作将在从 *IoT Security* 性导入安全策略规则建议时节省时间和精力。由于导入的规则建议不包含日志转发配置文件，因此您必须在导入规则后手动向每个规则添加一个日志转发配置文件。但是，通过将配置文件命名为“默认”，可以避免此步骤。（请注意，添加新的安全策略规则时将应用“默认”日志转发配置文件，但不会追溯应用于现有规则。）

策略规则 2：此规则允许从 DHCP 区域中的 VLAN 接口对在 ethernet1/1 - ethernet1/3 上配置的网络执行 Ping（ICMP 回显请求）。

策略规则 3：此规则允许从分配给 ethernet1/1 - ethernet1/3 的 IP 地址对 DHCP 区域中配置的 VLAN 接口执行 Ping 操作。

配置区域内策略

您必须覆盖默认区域内策略规则中的日志记录和日志转发设置，以便防火墙将日志转发到日志记录服务。

如果托管 DHCP 服务器的接口与客户端所在的接口位于同一区域，则默认区域内策略规则将应用于此流量，默认情况下，该流量允许此区域内的所有流量，但未启用日志记录和日志转发。因此，您必须通过在默认区域内策略规则上启用日志转发来覆盖此规则。

即使 *DHCP* 服务器与 *DHCP* 客户端位于不同的区域中，并且对其 *DHCP* 流量应用了区域间策略，我们仍然建议您在默认区域内策略规则上启用日志转发，以捕获该区域内流量的增强型应用程序日志。

STEP 1 | 单击 **Policies**（策略） > **Security**（安全），选择 **intrazone-default**，然后单击 **Override**（覆盖）。

此时将显示“安全策略规则”配置窗口。

STEP 2 | 单击 **Actions**（操作），选择 **Log at Session End**（在会话结束时记录），从“日志转发”下拉列表中选择刚才配置的日志转发模板，然后单击 **OK**（确定）。

控制加入设备的允许流量

当新设备加入网络时，必须允许它们正常运行，以便 IoT Security 部门可以通过分析其正常网络行为来识别它们。但是，防火墙通常配置了零信任安全策略规则，这些规则仅允许设备根据其功能所需的网络活动。因此，这些规则可能会无意中阻止新设备的流量，如果允许，则允许 IoT Security 确定其身份。

为了解决此问题，您可以配置一个或多个使用 Device-ID 的加入策略规则，以便仅将规则应用于最近在网络上检测到但尚未确定的设备。要使防火墙强制执行规则，必须将设备归类为加入设备。IoT Security 在可定制的时间段内将低置信度设备归入此类别，该时间段从 IoT Security 首次在网络上检测到它们时开始。设备将继续被归类为“加入设备”，直到 IoT Security 自信地以高于 90 的置信度分数识别它们，或者直到时间段结束。该策略规则不适用于以前识别的其他设备，并且必须配置为允许新设备进行足够的网络访问，以便 IoT Security 部门识别它们。一旦 IoT Security 识别出它们，它就会将它们切换到适合它们的类别。然后，防火墙可以根据其身份应用适当的策略规则。如果 IoT Security 无法自信地识别一个或多个设备且时间期限到期，它仍会将其切换到它认为合适的类别，但由于它们的置信度分数低于 90，因此 IoT Security 不会生成任何安全规则建议。

STEP 1 | 配置安全策略规则，允许来自类别 Device-ID 属性为“加入设备”的任何设备的某些类型的流量。

1. 登录到 PAN-OS 或 Panorama Web 门户，并配置安全策略规则，该规则允许某些 VLAN 或不同 IP 地址子网中的设备预期生成的基本流量类型。例如，包含打印机的 VLAN 规则应仅允许特定于打印机的典型流量，而包含医疗扫描设备的 VLAN 规则应仅允许扫描程序的典型流量类型。
2. 将 Device-ID 组件添加到规则中，并指定 **Onboarding Device**（加入设备）作为设备必须匹配的类别，防火墙才能应用规则。（简而言之，**Add**（添加）关于 **Policies**（策略） > **Security**（安全）的安全策略规则。选择 **Source**（源）选项卡，单击“源设备”部分的 **Add**（添加）部分，然后单击 **Device**（设备）。在弹出的“设备对象”对话框中，在“类别”列表中选择 **Onboarding Device**（加入设备）。
3. 创建其他安全策略规则，指定 **Onboarding Device**（加入设备）作为规则配置的 Device-ID 部分中的类别。

STEP 2 | 在 IoT Security 中启用基于 Device-ID 的新设备加入功能。

1. 以具有所有者权限的用户身份登录 IoT Security 门户。
2. 选择 **Policy Sets**（策略集） > **Settings**（设置）并打开开关 **Control newly onboarded low-confidence devices through firewall policy rules**（通过防火墙策略规则控制新加入的低置信度设备）。
3. （可选）如果身份置信度分数低于 90，更改 IoT Security 将设备归类为加入设备的时间段。默认加入期限为 7 天。没有最大和最小限制。您还可以从有限的时间期限切换到无限的时间长度。

   启用此功能并为加入期限设置时间长度后，如果有任何设备的加入期限即将到期，IoT Security 会显示每日系统警报。警报会在到期前几天显示，并包含指向 **Assets**（资产） > **Devices**（设备）页面的链接（已应用过滤器），以便仅显示这些设备的页面。
4. 要查看哪些设备属于“加入设备”类别，请选择 **Assets**（资产） > **Devices**（设备），并在必要时显示“设备”表中的 **Onboarding Device**（加入设备）列。

   如有必要，还要显示 ***First Seen***（首次出现）列，然后按此排序，根据 *IoT Security* 首次在网络上发现设备的顺序来组织设备显示方式。

支持隔离网段

隔离网段是专用网络的一部分，它允许在网段中的设备与任何其他本地网段或公共网络中的设备之间建立极其有限的连接集。因为 IoT Security 是基于云的应用程序，依赖网络流量日志来提供服务，所以需要有一种在不影响隔离网段安全性的情况下将日志送到 IoT Security 的方法。为此，您可以将新一代防火墙配置为安全遥测网关（在 PAN-OS Web 界面中称为代理），以将流量日志从隔离网段通过非隔离网段转发到 Palo Alto Networks 日志记录服务，其中 IoT Security 可以访问该服务。此外，对于加入 IoT Security 和支持 Device-ID 所需的数据和文件，安全遥测网关还可以转发来自隔离防火墙的请求：许可证、证书、IP 地址到设备的映射、安全策略规则建议和字典文件下载。

此数据路径仅通过安全遥测网关出现，只有新一代防火墙生成的请求和网络流量日志，而不是来自受保护设备的实际数据，才会通过安全遥测网关链发送到此路径上。

重要的是，隔离网段中的设备与云之间没有直接连接，安全遥测网关到云的连接状态(上行或下行)对受保护设备的操作以及新一代防火墙功能(如策略实施和威胁检测与防范)没有影响。即使上游安全遥测连接中断，所有受保护的设备和防火墙操作将继续运行。

您可以使用单个安全遥测网关或由两个或多个安全遥测网关组成的链进行额外的安全分层。通过这种方式，Palo Alto Networks 可以为具有隔离 OT 网络的行业提供 IoT Security 服务，例如在电力公用事业和油气公司中很常见。这些网络通常由两个网段组成：IT 网络和 OT 网络。利用现有的新一代防火墙或部署新的防火墙，您可以配置两个防火墙作为安全遥测网关，其中一个位于 OT 和 IT 网络之间的边界，另一个位于 IT 和公共网络之间的边界。OT 网络中的防火墙会将流量日志发送到 OT 安全遥测网关，再由网关转发给IT安全遥测网关，再由网关转发给 Palo Alto Networks 日志记录服务。在这样的安全遥测网关链中设置新一代防火墙会增加逻辑网段边界的深度，因为 IT 安全遥测网关会阻止到 OT 安全遥测网关的入站连接。

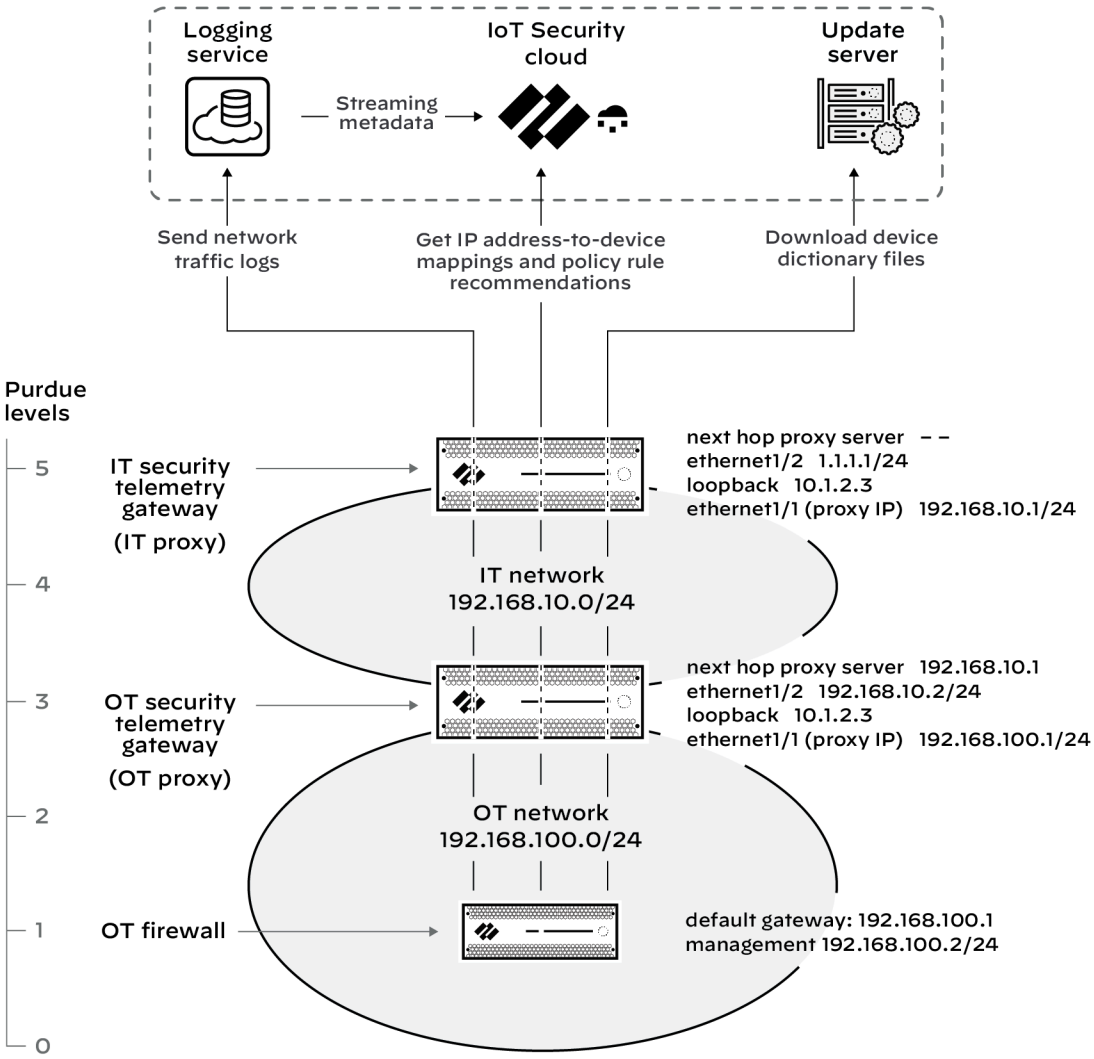
以下新一代防火墙支持安全遥测网关功能：

- 物理防火墙：PA-1400 系列、PA-3400 系列、PA-5400 系列（PA-5450 除外）
- VM-300、VM-500、VM-700

防火墙必须运行 PAN-OS 11.0.1-h2 或更高版本。

为包含隔离的 OT 网段的网络部署防火墙时，请从 IT 外围(IT 安全遥测网关)向 OT 网络最深处依次设置安全遥测网关：IT 安全遥测网关，然后是 OT 安全遥测网关，最后是 OT 防火墙。通过按此顺序部署它们，您将在完成一个部署后获得部署下一个部署所需的信息。而且，随着每个防火墙上线，下一个防火墙需要到达公共网络时，该防火墙或多个防火墙将已经上线并可到达。

下图显示了安全遥测网关链中新一代防火墙的逻辑关系，以及随后的配置说明中用作示例的 IP 地址和子网。如这里所示，OT 防火墙通过 OT 和 IT 安全遥测网关发起到日志记录服务、IoT Security 云和更新服务器的所有出站连接。



尽管在 *OT* 安全遥测网关前设置 *IT* 安全遥测网关可让您在 *OT* 网络外围阻止到防火墙的入站连接，但不需要多个级联网关。如果您在 *OT* 网络周边使用单个安全遥测网关，它将成为外部网络中 *OT* 防火墙和 *Palo Alto Networks* 云服务之间的代理，而不是通过 *IT* 安全遥测网关跳跃。

配置 IT 安全遥测网关

IT 安全遥测网关是新一代防火墙，它将流量日志和从 OT 安全遥测网关收到的请求转发到日志记录服务、IoT Security 和更新服务器。它通常部署在网络外围。

STEP 1 | 配置新一代防火墙作为 IT 安全遥测网关。

1. 以超级用户或设备管理员身份访问 CLI,然后输入以下命令使防火墙能够用作安全遥测网关(代理)：

   ```
   set system setting paloalto-networks-service-proxy on
   ```

2. 重启防火墙。

   使用 *Panorama* 管理防火墙时，请在 *Panorama CLI* 中输入上述命令，然后重新启动 *Panorama*。

3. 以超级用户或设备管理员身份登录到防火墙 Web 界面，并配置两个第 3 层接口 — 一个在 IT 网络上，另一个在外部网络上。例如，为 IT 网络配置 IP 地址为 192.168.10.1/24 的 ethernet1/1，为外部网络配置 IP 地址为 1.1.1.1/24 的 ethernet1/2。
4. 使用与其他两个网络不同的子网中的 IP 地址创建环回接口。例如，如果 IT 网络的子网是 192.168.10.0/24，而外部网络的子网是 1.1.1.0/24，则对环回接口使用不在这两个子网中的 IP 地址，如 10.1.2.3。
5. 为所有三个接口创建一个虚拟路由器，并将其添加到其中（例如，**vr1**）。如果外部网络接口是静态 IP 地址，则添加一条默认路由到外部网络子网中的网关作为下一跳。
6. 为 **IT**、**external**（外部）和 **Loop**（环路）等每个接口创建区域。
7. 选择 **Network**（网络） > **DNS Proxy**（**DNS** 代理），为外部区域的接口配置 DNS 代理。例如，创建一个名为 **dns-proxy** 的配置，在 **8.8.8.8** 的 DNS 服务器上从 **ethernet1/2** 进行 DNS 查找。
8. 选择 **Objects**（对象） > **URL Category**（**URL** 类别）并创建以下 URL 组：

   名称：为 URL 列表命名；例如，**iot_cloud_traffic**。

   URL List（**URL** 列表）：将以下 URL（和 IP 地址）添加到 URL 列表中。这些是必须允许代理流量访问的唯一目标。

   - *.paloaltonetworks.com/
   - *.panservicetest.com/
   - ocsp.godaddy.com/
   - certificates.godaddy.com/
   - *.gpcloudservice.com/
   - *.lencr.org/
   - 34.122.191.141

   使用 *Panorama* 管理防火墙时，请将 *URL* 类别创建为“共享”。

9. 选择 **Policies**（策略） > **Security**（安全），并创建一个通用策略规则，允许 **iot_cloud_traffic** URL 类别中的目标从 IT 区域到外部区域的任何应用程序，并将其置于其他策略规则之上。
10. 选择 **Policies**（策略） > **NAT**，然后创建策略，将 IT 和环路区域中设备和接口的源地址转换为外部区域中出口接口的 IP 地址。在我们的示例中，这将是 1.1.1.1，即以太网 1/2 的 IP 地址。

11. 选择 **Network**（网络） > **Proxy**（代理），单击代理启用的设置图标，选择 **Palo Alto Networks Service Proxy**（**Palo Alto Networks** 服务代理），然后单击 **OK**（确定）。
12. 单击 Palo Alto Networks 服务代理配置的设置图标，然后输入以下内容：

    Connect Timeout（连接超时）：**5**（默认）

    Listening（侦听）：输入 IT 网络接口的名称；例如，**ethernet1/1**.

    Upstream interface（上游接口）：**loopback.1**

    Proxy IP（代理 **IP**）：输入 IT 区域中接口的 IP 地址；例如 **192.168.10.1**。

    DNS-Proxy（**DNS** 代理）：输入您以前定义的 DNS 代理的名称；例如 **dns-proxy**.

    Allowed URL Category（允许的 **URL** 类别）：输入之前定义的允许 URL 组的名称，例如 **iot_cloud_traffic**。

    Next Hop Proxy Server（下一跳代理服务器）：留空。

    Next Hop Proxy Port（下一跳代理端口）：留空。

STEP 2 | 可选）要在 IT 网络中使用 IoT Security 进行设备识别、风险评估和漏洞检测，请将充当 IT 安全遥测网关的防火墙订阅到 IoT Security。

如果您不希望作为 *IT* 安全遥测网关的防火墙在 *IT* 网络中使用 *IoT Security* 服务，则没有必要订阅 *IoT Security*，您可以跳过此步骤。

1. IT 安全遥测网关上的 加入 IoT Security。
2. 在 IT 安全遥测网关上安装日志记录服务和 IoT Security 的许可证，并将设备证书下载到 IT 安全遥测网关，以验证其与日志记录服务和 IoT Security 的连接。
3. 配置 IT 安全遥测网关以支持 Device-ID 并使用 IoT Security。

配置 OT 安全遥测网关

IT 安全遥测网关配置就绪后，您可以接下来配置 OT 安全遥测网关。OT 安全遥测网关是新一代防火墙，它将从 OT 防火墙收到的流量日志转发到IT安全遥测网关，IT 安全遥测网关再将其转发到日志记录服务。它还会将来自 OT 防火墙的 IP 地址到设备映射请求、策略规则建议和字典文件转发到 IoT Security 和更新服务器。它通常部署在 OT 网络的边缘。

STEP 1 | 配置新一代防火墙作为 OT 安全遥测网关。

1. 以超级用户或设备管理员身份访问 CLI，然后输入以下命令，使防火墙能够用作安全遥测网关（在 PAN-OS 中称为代理）：

   ```
   set system setting paloalto-networks-service-proxy on
   ```

2. 重启防火墙。

   使用 *Panorama* 管理防火墙时，请在 *Panorama CLI* 中输入上述命令，然后重新启动 *Panorama*。

3. 配置两个第 3 层接口 — 一个在 OT 网络上，另一个在 IT 网络上。例如，为 OT 网络配置 IP 地址为 192.168.100.1 的以太网 1/1，为IT网络配置 IP 地址为 192.168.10.2 的以太网 1/2。
4. 使用与其他两个网络不同的子网中的 IP 地址创建环回接口。由于它仅用于内部路由，您甚至可以使用与IT安全遥测网关上的环回接口相同的 IP 地址—例如 10.2.3.4。
5. 为所有三个接口创建一个虚拟路由器并将其添加到其中（例如，**vr1**），然后添加一条默认路由，将以太网 1/2 作为出口接口，将 IT 安全遥测网关接口上以太网 1/1 的 IP 地址 192.168.10.1 作为下一跳。
6. 为每个接口创建一个区域，如 **OT**、**IT** 和 **Loop**（环路）。
7. 如果下一跳安全遥测网关服务器是主机名，请选择 **Network**（网络）> **DNS Proxy**（DNS 代理）并为 IT 区域中的 OT 安全遥测网关的接口配置 DNS 代理。例如，创建一个名为 **dns-**

proxy 的配置，在 OT 安全遥测网关可以从 ethernet1/2 连接到的本地 DNS 服务器上执行 DNS 查找。

如果下一跳安全遥测网关服务器是 *IP* 地址，则无需配置 *DNS* 代理，可以跳过此步骤。

8. 选择 **Objects**（对象） > **URL Category**（**URL** 类别）并创建以下 URL 组：

   名称：为 URL 列表命名；例如，**iot_cloud_traffic**。

   URL List（**URL** 列表）：将以下 URL（和 IP 地址）添加到 URL 列表中。这些是必须允许代理流量访问的唯一目标。

   - *.paloaltonetworks.com/
   - *.panservicetest.com/
   - ocsp.godaddy.com/
   - certificates.godaddy.com/
   - *.gpcloudservice.com/
   - *.lencr.org/
   - 34.122.191.141

   使用 *Panorama* 管理防火墙时，请将 *URL* 类别创建为“共享”。

9. 选择 **Policies**（策略） > **Security**（安全），并创建一个通用策略规则，允许 **iot_cloud_traffic** URL 类别中的目标从 OT 区域到 IT 区域的任何应用程序，并将其置于其他策略规则之上。

   添加拒绝来自 *OT* 网络的所有其他出站连接和到 *OT* 网络的所有入站连接的安全策略规则，并将其放置在允许到 *iot_cloud_traffic URL* 列表中目标的出站连接的规则下方。

10. 选择 **Network**（网络） > **Proxy**（代理），单击代理启用的设置图标，选择 **Palo Alto Networks Service Proxy**（**Palo Alto Networks** 服务代理），然后单击 **OK**（确定)。

11. 单击 Palo Alto Networks 服务代理配置的设置图标，然后输入以下内容：

    Connect Timeout（连接超时）：**5**（默认）

    Listening（侦听）：输入 0T 网络接口的名称；例如，**ethernet1/1**.

    Upstream interface（上游接口）：**loopback.1**

    Proxy IP（代理 **IP**）：输入 OT 区域中接口的 IP 地址，例如 **192.168.100.1**。

    DNS-Proxy（**DNS** 代理）：输入您以前定义的 DNS 代理的名称；例如 **dns-proxy**.

    Allowed URL Category（允许的 **URL** 类别）：输入之前定义的允许 URL 组的名称，例如 **iot_cloud_traffic**。

    Next Hop Proxy Server（下一跳代理服务器）：在 IT 安全遥测网关接口上输入 ethernet1/1 的 IP 地址；在我们的示例中为 **192.168.10.1**。

    Next Hop Proxy Port（下一跳代理端口）：**8080**

STEP 2 | （可选）要从 OT 安全遥测网关以及 OT 防火墙转发 OT 网络的网络流量日志，请将 OT 安全遥测网关订阅到 IoT Security。

如果您不希望作为 *OT* 安全遥测网关的防火墙在 *OT* 网络中使用 *IoT Security* 服务，则没有必要订阅 *IoT Security*，您可以跳过此步骤。

1. OT 安全遥测网关上的 加入 IoT Security
2. 在 OT 安全遥测网关上安装日志记录服务和 IoT Security 的许可证，并将设备证书下载到 IT 安全遥测网关，以验证其与日志记录服务和 IoT Security 的连接。
3. 配置 OT 安全遥测网关以支持 Device-ID 并使用 IoT Security。

配置 OT 防火墙

配置了 IT 和 OT 安全遥测网关后，您可以设置 OT 防火墙以使用安全遥测网关链访问支持 IoT Security 所需的 Palo Alto Networks 云服务：

- 日志记录服务 — OT 防火墙将 EAL 和流量日志转发到日志记录服务，日志记录服务将元数据流式传输到 IoT Security 进行分析，以识别设备、评估风险和检测设备漏洞。
- **IoT Security** — OT 防火墙从 IoT Security 检索 IP 地址到设备的映射，以执行 Device-ID 安全策略规则。OT 防火墙还会从 IoT Security 检索策略规则建议。
- 更新服务器 — OT 防火墙定期下载设备字典文件，其中包含定期更新的设备属性列表，用作 Device-ID 安全策略规则中的组件。
- **License server**（许可证服务器）— OT 防火墙从许可证服务器下载激活的日志记录服务和 IoT Security 许可证。
- **Certificate Server**（证书服务器）— 防火墙从 certificate.paloaltonetworks.com 获取新的设备证书，并使用其现有的设备证书（过期但仍有效）从 certificatetrusted.paloaltonetworks.com 获取续订的证书。
- **Customer Service Portal**（客户服务门户）和 **Hub** — 防火墙连接到客户服务门户以验证管理员用户，然后连接到 Hub 以获取其角色分配。

STEP 1 | 配置新一代防火墙作为 OT 防火墙。

1. 选择 **Device**（设备） > **Setup**（设置） > **Interfaces**（接口） > **Management**（管理），在 OT 网络上使用 IP 地址配置 MGT 接口，并在 OT 区域输入 OT 安全遥测网关接口的 IP 地址作为其默认网关；例如：

   IP Type（**IP**类型）：**Static**（静态）

   IP Address（**IP** 地址）：**192.168.100.2**

   Netmask（网络掩码）：**255.255.255.0**

   Default Gateway（默认网关）：**192.168.100.1**

   OT 防火墙使用管理界面加入 IoT Security 并获取证书和许可证，将各种流量日志转发到日志记录服务，从 IoT Security 请求 IP 地址到设备的映射和策略规则建议，以及从更新服务器下载字典文件。

   您还可以将 *OT* 防火墙配置为在通过安全遥测网关链发起连接时使用其以太网接口之一。如果是，则必须配置服务路由以指示防火墙使用此接口而不是管理接口。在服务路由配置中，选择 *Palo Alto Networks* 服务、数据服务和 *IoT*。

2. 根据需要配置接口、安全区域和安全策略规则，以收集网络流量元数据来供 IoT Security 分析。PAN-OS 提供了各种选项，您需要使用适合您的网络拓扑的任何方法；例如：

   虚拟线路捕获 **OT** 流量 — 创建一个虚拟线路区域和一个连接两个虚拟线路接口的虚拟线路对象。添加允许同一区域内设备之间通信的区域内或通用策略规则，并在该规则上启用日志记录和日志转发。考虑在 OT 网络上的某个 OT Purdue 级别 (0-3) 放置具有此配置的一个或多个 OT 防火墙，以捕获此级别的网络流量并将流量日志转发到 OT 安全遥测网关。

   Tap 接口来收集下游交换机的流量 — 创建具有 Tap 接口的 Tap 区域，以从下游交换机上的镜像端口接收流量。这将捕获未到达 OT 防火墙的其他 Purdue 级别的流量，然后这些流量可以转发到日志记录服务。

   第 **3** 层接口用于从下游交换机上的 ERSPAN 端口收集流量 — 在 OT 防火墙上创建具有第 3 层接口的第 3 层区域。将交换机配置为使用封装远程交换端口分析器 (ERSPAN) 通过通用路由封装 (GRE) 隧道向 OT 安全遥测网关上的 OT 网络接口的 IP 地址发送镜像流量。OT 安全遥测网关在对流量进行解封装后，生成各种流量类型的日志并将其转发到 IT 安全遥测

网关，IT 安全遥测网关再将其转发到日志记录服务，IoT Security 可以访问这些日志进行分析。

3. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务），在“代理服务器”部分输入以下设置，其他设置保留默认值：

   代理服务器

   - **Server**（服务器）：输入 OT 区域中 OT 安全遥测网关接口的 IP 地址；例如 192.168.100.1,这是 OT 安全遥测网关以太网 1/1 接口的 IP 地址。
   - **Port**（端口）：**8080**
   - **Use proxy to send logs to** （使用代理将日志发送到）**Strata Logging Service**：（选择）

4. 选择 **Policies**（策略） > **Security**（安全），并创建一个通用策略规则，允许以下应用程序从 OT 网络区域到任何区域，并将其置于其他策略规则之上：

   google-base

   paloalto-device-telemetry

   paloalto-iot-security

   paloalto-logging-service

   paloalto-shared-services

STEP 2 | 将 OT 防火墙订阅到 IoT Security。

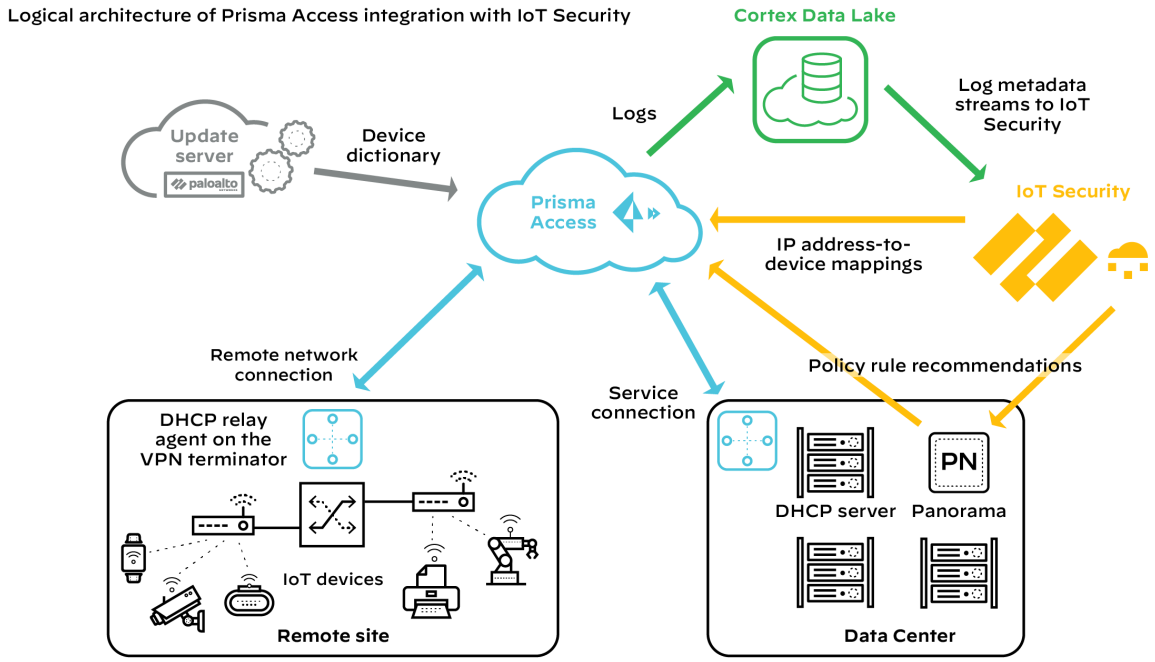
1. OT 防火墙上的 加入 IoT Security
2. 在 OT 防火墙上安装日志记录服务和 IoT Security 的许可证，并将设备证书下载到 OT 防火墙以验证其与日志记录服务和 IoT Security 的连接。
3. 将 OT 防火墙配置为支持 Device-ID 并使用 IoT Security。

IoT Security 与 Prisma Access 集成

Prisma Access 使用基于云的基础设施，可让您避免设置防火墙大小和计算资源分配的挑战，同时保护远程网络和移动用户的安全。为了识别远程站点的 IT 和 IoT 设备，检测 IoT 设备漏洞，并发现这些设备和网络面临的威胁，Prisma Access 可以通过购买的附加组件与 IoT Security 集成。此外，IoT Security 还通过 Panorama 向 Prisma Access 提供策略规则建议，以便只允许可接受的网络行为并阻止来自 IoT 设备的异常行为。

为了让 IoT Security 识别 IT 和 IoT 设备，分析风险级别并检测 IoT 设备上的安全警报，必须能够访问网络流量元数据。它需要处理的数据越多，就越准确和快速。因此，关键是要做两件事来收集尽可能多的流量元数据。首先，从战略性高度设计您的网络，让 Prisma Access 看到来自远程站点的所有流量，包括 DHCP 流量。然后对尽可能多的流量应用策略规则，并在这些规则上启用日志记录和日志转发，以向 Strata Logging Service 发送流量元数据。

DHCP 流量对 IoT Security 尤为重要。它为 IoT Security 提供了有用的数据，包括每个 DHCP 客户端的 IP 地址到 MAC 地址的映射，这是用于设备标识的 IP 地址到设备映射的关键要素。要获取此数据，请确保 DHCP 服务器位于您的数据中心或类似的集中站点，DHCP 中继代理位于每个站点终止远程网络连接的客户本地设备 (CPE) 上。每个中继代理通过Prisma Access服务基础设施将其从 DHCP 客户端收到的 DHCP 消息转发到 DHCP 服务器的 IP 地址。在允许从远程站点到 DHCP 服务器的 DHCP 流量的策略规则上，请确保已启用日志记录和日志转发，以便 Prisma Access 向 Strata Logging Service 发送 DHCP 流量日志。实际上，如果您尚未在所有策略规则上启用日志记录和日志转发功能，请启用此功能。启用日志转发后，Prisma Access 会通过 Strata Logging Service 发送其日志，然后将元数据流式传输到 IoT Security 以进行分析。



对于源和目标都位于同一站点的第 2 层流量或第 3 层流量，*Prisma Access* 无法将日志转发到的 *IoT Security*，因为这些流量永远无法到达。如果没有 *ARP* 和 *DHCP* 流量元数据，*IoT Security* 识别设备时可能需要更多时间，而且其置信度可能低于其他方法。要应对这种情况，请考虑在远程站点部署 *SD-WAN ION* 设备，它们可以记录这些类型的流量，并将其日志转发到 *Strata Logging Service* 以供 *IoT Security* 访问。通过将 IoT Security 集成到 Prisma Access 和 SD-WAN 中，*IoT Security* 可以获得站点和互联网之间流动的流量以及停留在站点内的流量的可见性。

在 IoT Security 获得足够的信息，可以从设备网络行为中识别设备后，它会向 Prisma Access 提供 IP 地址到设备的映射，向 Panorama 提供策略建议，Panorama 管理员可以导入这些建议，然后将其推送到 Prisma Access，以便对 IoT 设备流量实施策略。此外，Prisma Access 还会从更新服务器下载设备字典文件。设备字典列出了 Panorama 管理员可以用来构造安全策略规则的各种设备属性。IP 地址到设备的映射、策略建议和设备字典文件的组合构成 PAN-OS 10.0 中引入的 Device-ID 功能的要素。

所需的 **Panorama** 配置

检查您是否在日志转发配置文件上启用了增强型应用程序日志。

1. 登录 Panorama 并选择 **Remote_Network_Device_Group** 设备组或父设备组下的 **Objects**（对象） > **Log Forwarding**（日志转发）。
2. 打开日志转发配置文件，并确保为 Strata Logging Service 选中 **Enable enhanced application logging to**（启用增强型应用程序日志记录）。

使用具有 **Prisma Access** 的 **IoT Security** 的要求

要将 IoT Security 附加组件与 Prisma Access 一起使用，请检查您的部署是否满足以下要求：

1. Prisma Access 正在运行 Prisma Access 2.0-Innovation 或更高版本。
2. 您已购买并激活 Strata Logging Service 的许可证，以及 Prisma Access 的 IoT Security 附加组件。

   如果您是截至 2022 年 8 月的新 Panorama 管理 Prisma Access 的客户，请通过 Prisma SASE 平台激活新的 Prisma Access 许可证。

   如果您是 2022 年 8 月之前现有 Panorama 管理 Prisma Access 的客户，您的 Prisma Access 租户将从 Hub 过渡到 Prisma SASE 平台。完成过渡后，在 Hub 上将无法再看到 Prisma Access 应用标题。但是，在 Hub 上会有一个按钮，可以导航到sase.paloaltonetworks.com，从而通过 Prisma SASE 平台激活新的 Prisma Access 许可证。在此之前，继续像以前一样管理部署。
3. 在特定区域部署 Prisma Access 要求与其配合的 Strata Logging Service 实例和 IoT Security 应用程序也位于特定位置。下表显示了不同区域的 Prisma Access 部署 与 Strata Logging Service 和 IoT Security 位置的关系。

	Prisma Access	Strata Logging Service	IoT Security
美洲	加拿大	加拿大	加拿大
	美国	美国	美国
欧盟	法国	法国	德国

	Prisma Access	Strata Logging Service	IoT Security
	德国	德国	德国
	意大利	意大利	德国
	波兰	波兰	德国
	西班牙	西班牙	德国
	荷兰	荷兰	德国
	瑞士	瑞士	瑞士
	英国	英国	英国
亚太地区	澳大利亚	澳大利亚	澳大利亚
	中国	中国	新加坡
	印度	印度	新加坡
	印度尼西亚	印度尼西亚	新加坡
	日本	日本	日本
	新加坡	新加坡	新加坡

4. 您使用 Panorama 10.0 或更高版本来管理 Prisma Access。

   通过 *Prisma Access* 和本地部署的新一代防火墙的混合部署，您必须使用相同的 *Panorama* 管理系统来管理它们，并使用相同的 *IoT Security* 租户来管理它们。

5. DHCP 正在从数据中心或其他一些中心站点提供服务。
6. Prisma Access 基础架构提供从远程站点到数据中心资源的路由，其中包括 DHCP 服务器。
7. 所有远程站点 VPN 终端上的 DHCP 中继代理都指向数据中心 DHCP 服务器的 IP 地址。
8. Prisma Access 中的安全策略规则控制到 Internet、数据中心和其他远程站点的流量。在这些策略上启用日志记录，Prisma Access 会将日志记录数据转发给 Strata Logging Service，后者将其流式传输到 IoT Security。

   IoT Security 使用增强型应用程序日志 *(EAL)*、流量日志（包括 *DHCP* 流量）、威胁日志和 *Wildfire* 日志。确保您的策略规则已启用日志记录，并且正在将 *EAL* 和流量日志转发到 *Strata Logging Service*。虽然 *IoT Security* 运行不需要后两种日志类型，但我们建议获取威胁防御和 *Wildfire* 的许可证并转发其日志，因为它们有助于改进风险评估和恶意软件检测。

满足这些要求后，使用 IoT Security 监控流量元数据、识别 IoT 设备、检测漏洞、发现威胁并准备策略规则建议。将策略规则建议从 IoT Security 导入 Panorama 或直接在 Panorama 中配置 Device-ID 策略规则，然后将其推送到 Prisma Access 以对 IoT 设备流量实施策略。

IoT Security 许可证

当 IoT Security 订阅的许可证或第三方集成附加组件过期时，您可以使用多个选项。如果您不再希望防火墙订阅 IoT Security 服务或与第三方系统集成，可以让许可证过期。如果您确实想继续使用这些服务或集成，可以延长试用期和评估许可证、续订付费许可证，甚至将许可证从一种类型转换为另一种类型。

许可证延期

购买 IoT Security 前，您可以先试用并进行评估。试用或评估许可证的初始期限为 60 天，可以以 30 天为增量延长。要延长试用或评估期限，请通过 Palo Alto Networks 销售代表或销售工程师申请延长 30 天。

许可证续订

当付费许可证即将到期时，您可以进行续订，这样服务就不会中断，下一个许可证将在当前许可证结束后立即开始。您可以续订以下许可证：

- IoT Security 订阅实验室许可证
- IoT Security 订阅 Prod（生产）许可证
- IoT Security，不需要数据湖 (DRDL) 订阅实验室许可证
- IoT Security、DRDL 订阅 Prod 许可证
- IoT Security 基本第三方集成附加许可证
- IoT Security 高级第三方集成附加许可证

要续订任何这些许可证，请联系您的 Palo Alto Networks 销售代表。

许可证转换

许可证转换是指从一种许可证类型转变为另一种许可证类型。许可证可以是 IoT Security 订阅的或第三方集成附加组件的。

您可以将防火墙上的 *IoT Security* 转换从试用版转换为生产版，但不能从评估版转换为生产版。评估许可证适用于评估防火墙，该许可证属于 *Palo Alto Networks* 财产，仅租借以供临时之用。但是，如果您在评估防火墙上创建一个评估许可证的 *IoT Security* 租户 *URL*，然后将其替换为生产防火墙上的生产许可证，则可以继续使用相同的 *IoT Security* 租户 *URL*。

Palo Alto Networks 支持以下转换：

IoT Security 许可证转换

- 试用 > 生产
- IoT Security 订阅 > IoT Security — 不需要数据湖 (DRDL) 订阅
- IoT Security、DRDL 订阅 > IoT Security 订阅

从不需要数据湖的订阅转换为需要数据湖的订阅之前，请激活 *Strata Logging Service* 实例。

IoT Security 第三方集成附加组件许可证转换

- 基础 > 高级
- 高级 > 基本

所有转换都可以在当前许可证到期后进行，但只有被视为升级的转换才允许在中期进行。中期转换会立即进行，并用新期限取代前一个期限。以下转换属于升级：

IoT Security 许可证升级

- 任何类型的试用版许可证 > 任何类型的生产版许可证
- IoT Security 订阅 > IoT Security、DRDL 订阅

IoT Security 第三方集成附加组件许可证升级

- 任何类型的附加组件的试用版 > 任何类型的附加组件的生产版
- 基础 > 高级

将 *IoT Security* 许可证从试用版转换为生产版会生成一个新的购买订单，并带有指向新加入工作流程的链接。在加入过程中，您可以选择之前用于试用目的现有 *IoT Security* 租户。其余加入工作流程遵循在防火墙上激活生产许可证的机制，与激活试用许可证的机制相同。

要转换任何许可证，请联系您的 Palo Alto Networks 销售代表。

撤销 IoT Security 订阅

从防火墙上脱离IoT Security 服务有三种方式：

- 停用防火墙上的IoT Security 许可证，并可选择将其传输到其他防火墙
- 将防火墙从一个客户支持门户 (CSP) 帐户转移到另一个帐户
- 让订阅过期

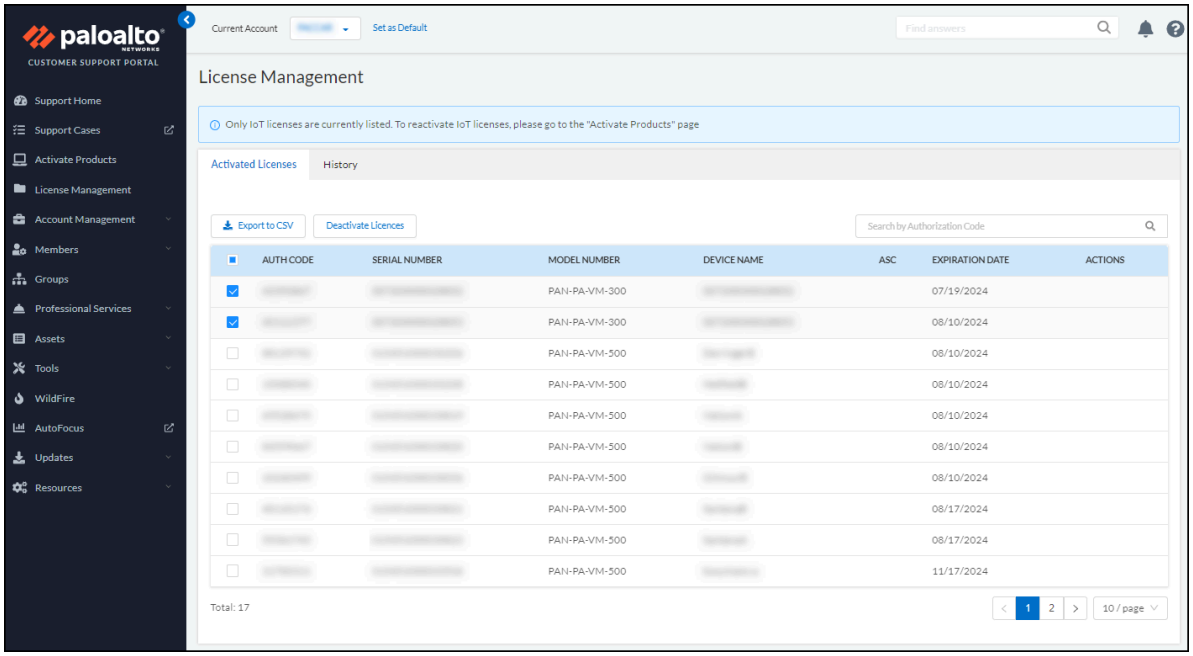
停用防火墙和传输许可证

如果您想从防火墙中删除 IoT Security 许可证 — 或许然后在另一个防火墙上使用该许可证 — 您可以在客户支持门户上执行此操作。

STEP 1 | 登录您的客户支持门户帐户。

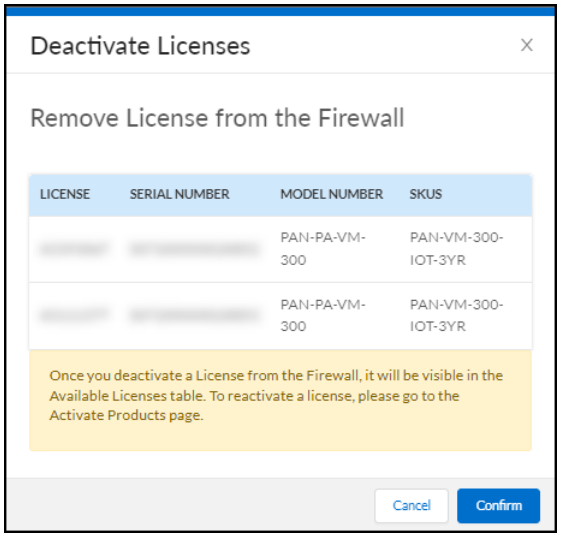
STEP 2 | 将 IoT Security 许可证与一个或多个防火墙解除关联。

1. 选择 **License Management**（许可证管理） > **Activated Licenses**（激活的许可证），根据防火墙序列号选择要切断的许可证与防火墙关联，然后 **Deactivate Licenses**（停用许可证）。



2. **Confirm**（确认）停用。

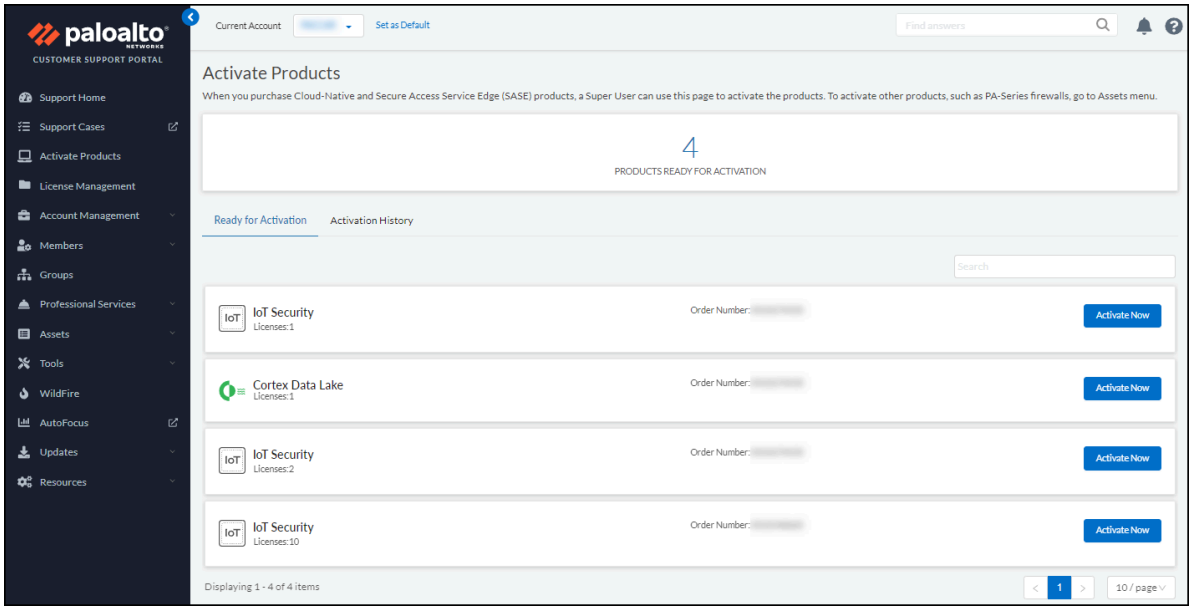
如果要将停用的许可证应用于其他防火墙，并且您有多个*IoT Security* 许可证采购订单，请在确认停用之前记下激活产品页面上订单中的可用许可证数量。然后，当您停用许可证后返回此页面时，您可以知道它们是返回到哪个顺序的，因为许可证号会增加。



这会将选定的 IoT Security 许可证与防火墙序列号分离，并按照激活产品页面上的原始顺序将其返回到可用许可证池中。

STEP 3 | 将许可证与其他防火墙关联，或将其与相同的防火墙重新关联。

1. 选择 **Activate Products**（激活产品） > **Ready for Activation**（准备激活），然后单击 **Activate Now**（立即激活）以获得要激活的许可证的订单。



2. 按照加入 IoT Security中所述的工作流程操作。

   当您在加入工作流中选择了防火墙订阅 IoT Security 时，您可以在购买期限下拉列表中看到每个许可证的剩余时间长度。如果您想将刚才停用的许可证应用到其他防火墙上，您会发现

其未使用的剩余时间将比其他尚未投入使用的许可证短。例如，如果原始订单包含有效期为三年的许可证，并且您在停用许可证之前使用了一年，则您可以轻松地发现它，因为其剩余有效期将是唯一列为仅两年的许可证。

CSP 帐户之间的传输防火墙

如果您有两个 CSP 帐户，或者是一个管理多个帐户的 MSSP，您可以将防火墙从一个帐户转移到另一个帐户，这可能是因为您将防火墙移动到由不同团队使用自己的帐户管理的不同位置。当您传输防火墙时，其所有许可证都将随之传输。为此，请登录 CSP 并单击 **Devices**（设备）。找到要转移的设备，单击其序列号为其打开设备详细信息窗格，然后单击 **Transfer Ownership**（转移所有权）。在出现的“设备传输”对话框中，输入您要向其传输防火墙的帐户所有者的目标电子邮件地址。

让 IoT Security 订阅过期

当防火墙不再有 IoT Security 订阅，因为它已过期(并且没有待续许可证),该防火墙的 IoT Security 服务将停止，并且 IoT Security 与防火墙之间的连接将终止。IoT Security 退订防火墙日志源。因此，它停止接收和处理来自该防火墙的日志。防火墙停止接收新的策略建议和 IP 地址到设备的映射，并在 200 分钟（约 3 小时）后清除缓存的映射。此时，使用 Device-ID 的基于设备的策略规则都不会起作用，应从策略集中删除。删除它们的有效方法是检查 **Policies**（策略） > **Security**（安全）页面上的"源设备"和"目标设备"列，并删除这两个列中的任何一个列中具有条目的所有规则。

IoT Security 概述

了解 IoT Security 的基础知识，它的作用及其工作原理。

- IoT Security 简介
- IoT Security 与新一代防火墙集成
- IoT Security 门户
- 垂直主题门户
- 设备到站点映射
- 站点和站点组
- 网络
- 网络可视化
- 创建可视化地图
- 在可视化地图中查看数据
- 报告
- IoT Security 与防火墙的集成状态
- 具有 Prisma Access 的 IoT Security 集成状态
- 数据质量诊断
- 授权按需 PCAP
- IoT Security 与第三方产品的集成
- IoT Security 和 FedRAMP

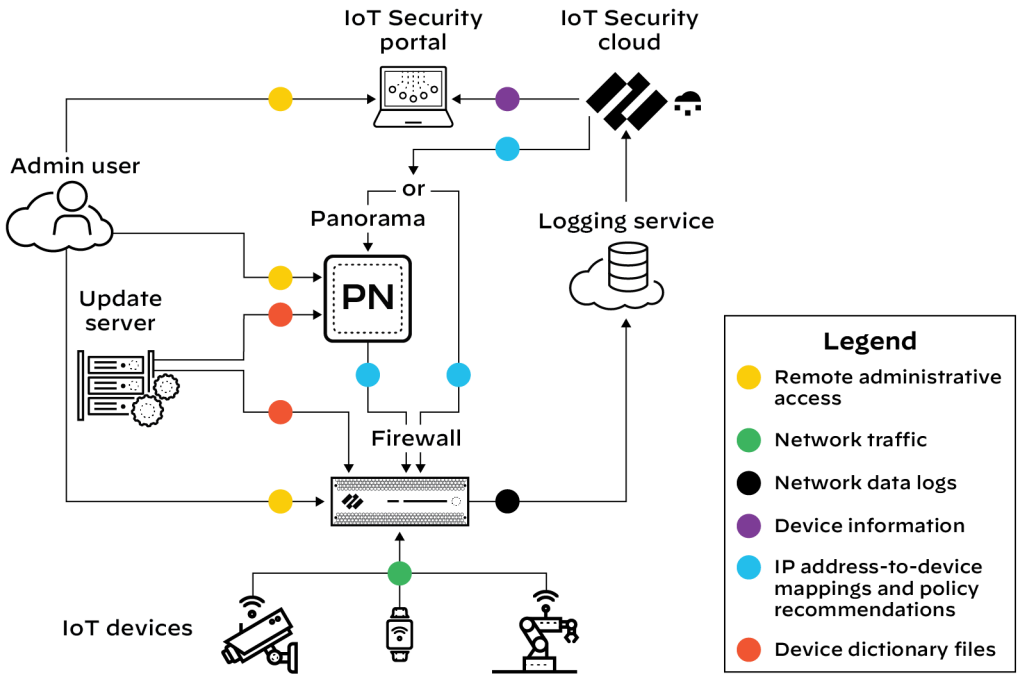
IoT Security 简介

IoT Security 是一种按需云订阅服务，旨在发现和保护网络上越来越多的联网“事物”。与执行各种任务的 IT 设备（例如笔记本电脑）不同，IoT 设备往往是专门构建的，并且具有一组狭义的功能。因此，IoT 设备会生成独特而可识别的网络行为模式。凭借机器学习和 AI，IoT Security 可以识别这些行为并识别网络上的每一台设备，从而创建动态维护并始终保持丰富且可感知上下文的最新清单。

在识别设备并建立正常网络活动的基线后，IoT Security 会继续监控网络活动，以便检测任何表明攻击或违规的异常行为。如果它检测到此类行为，IoT Security 会通过门户中的安全警报通知管理员，并根据每个管理员的通知设置，通过电子邮件和短信通知通知管理员。

IoT Security 还使用这些行为和设备标识自动生成安全策略规则建议，允许 IoT 设备继续进行正常的网络活动，并阻止它们执行任何异常操作。然后，Panorama 或新一代防火墙可以导入这些策略规则并强制执行它们。

对于具有需要 *Strata Logging Service* 的 *IoT Security* 订阅的 *Panorama* 托管防火墙 — 在用于将托管防火墙加入 Strata Logging Service 时，*Panorama* 才能导入策略规则建议。

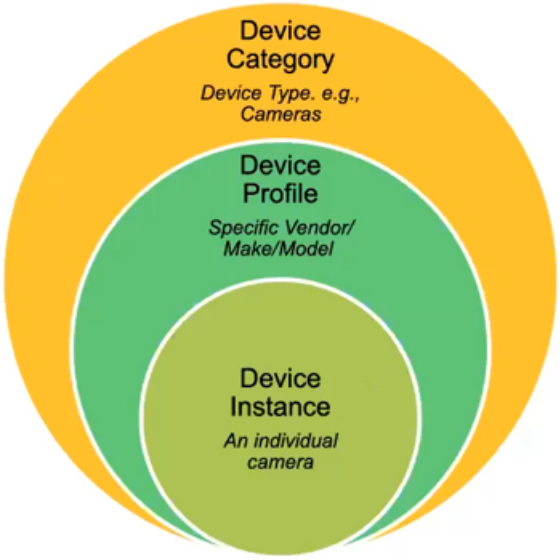


防火墙从 IoT 设备的网络流量中收集元数据，生成增强型应用程序日志 (EAL)，并将其转发到日志记录服务。然后，IoT Security 云从这些日志中提取元数据进行分析，并采用 AI 和机器学习算法，使用其获得专利的三层深度学习引擎来检测和识别 IoT 设备：

第 **1** 层：设备类别 — IoT Security 首先确定 IoT 设备所属的类别。例如，它可能会识别所有安全相机常见的网络行为。

第 **2** 层：设备配置文件 — 接着，IoT Security 会构建设备的配置文件，了解其供应商、品牌和型号。例如，它可能会发现通过相机的行为方式即可唯一识别它，比如说检查特定服务器的软件更新。

第 **3** 层：设备实例 — IoT Security 会继续进行分析，直到它辨别出已识别安全相机的特定实例所特有的行为。



IoT Security 查看网络流量元数据中的 200 多个参数，包括 DHCP 选项 55 参数列表、HTTP 用户代理 ID、协议、协议标头以及许多其他参数。它将新设备的网络流量模式与先前识别设备的网络流量模式进行匹配，以识别相同或类似类型的设备，甚至包括首次遇到的设备。

根据各种因素，例如 IoT 设备产生的网络流量以及其行为模式的差异程度，IoT Security 通常在开始从日志记录服务访问元数据的第一天，以高置信度识别大多数 IoT 设备。然后，IoT Security 继续增加确定识别的设备数量，直到识别出所有或几乎所有设备。在此期间，您可以登录 IoT Security 门户，用于检查是否正在填充设备清单并监视其进度。

置信度分数表示 *IoT Security* 在其设备标识中的置信度水平。根据计算出的置信度分数，*IoT Security* 有三个置信度级别：高 *(90-100%)*、中 *(70-89%)* 和低 *(0-69%)*。

除了使用机器学习 (ML) 来观察网络流量，并提取各种属性来识别设备和检测异常行为外，IoT Security 还采用基于 ML 的模型来检查注入到 HTTP URL 中的 SQL 内容，这是 SQL 漏洞利用中常见的技术。通过使用基于 ML 的模型而不是基于规则的模型，IoT Security 即使没有特定的签名，也可以找到注入的 SQL 内容的某些模式。

IoT Security 与新一代防火墙集成

IoT Security 解决方案涉及集成三个关键架构组件来处理网络数据：

- **Palo Alto Networks** 新一代防火墙收集设备数据并将其发送到日志记录服务。
- 日志记录服务使用基于云的日志转发过程将日志从防火墙定向到目标，例如 IoT Security 和 Strata Logging Service根据 IoT Security 订阅的类型，日志记录服务会将元数据流式传输到您的 IoT Security 帐户和 Strata Logging Service 实例，或仅传输到您的 IoT Security 帐户。
- **IoT Security** 是一个在基于云的平台上运行的应用程序，其中机器学习、人工智能和威胁情报用于发现、分类和保护网络上的 IoT 设备。该应用引入包含网络流量数据的防火墙日志，并提供安全策略建议和到防火墙的 IP 地址到设备的映射，以便在安全策略规则中使用。管理员可以通过 IoT Security 门户访问动态扩充的 IoT 设备清单、检测到的设备漏洞、安全警报和建议的策略集。

IoT Security 应用程序通过 Device-ID 与新一代防火墙集成，Device-ID 是一种使用设备身份作为应用策略的结构。集成使用三种机制。

- 设备字典 — 这是一个 XML 文件，由 IoT Security 生成并可供 Panorama 和防火墙导入。字典文件为 Panorama 和防火墙管理员提供了设备属性列表，以便在从 IoT Security 中导入推荐的安全策略规则和创建规则时时进行选择。这些属性包括配置文件、类别、供应商、型号、操作系统系列和操作系统版本，适用于 IoT 和传统 IT 设备。虽然无法下载设备字典文件，但您可以查看发行说明，其中总结了添加到防火墙已导入的文件的新内容。为此，请登录 PAN-OS Web 门户，选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后单击您要了解的设备字典文件的 **Release Notes**（发行说明）。
- 策略规则建议 — 在 IoT Security 管理员根据同一设备配置文件中来自 IoT 设备的流量创建一组安全策略规则，防火墙管理员可以将它们导入为建议，以便在其策略集中使用。
- **IP** 地址到设备的映射 — 这些映射告诉防火墙具有特定 IP 地址的设备具有哪些属性。当进出该 IP 地址的流量到达防火墙时，它会检查其某个属性是否与策略匹配，如果匹配，防火墙将应用该策略。如果设备标识的置信度分数较高（90-100%），并且它们在过去一小时内发送或接收过流量，IoT Security 会将 IP 地址到设备的映射发送到 IoT 和 IT 设备的防火墙。

Device-ID 的目标是利用 IoT Security 的情报来在 IoT 设备上实施防火墙策略。

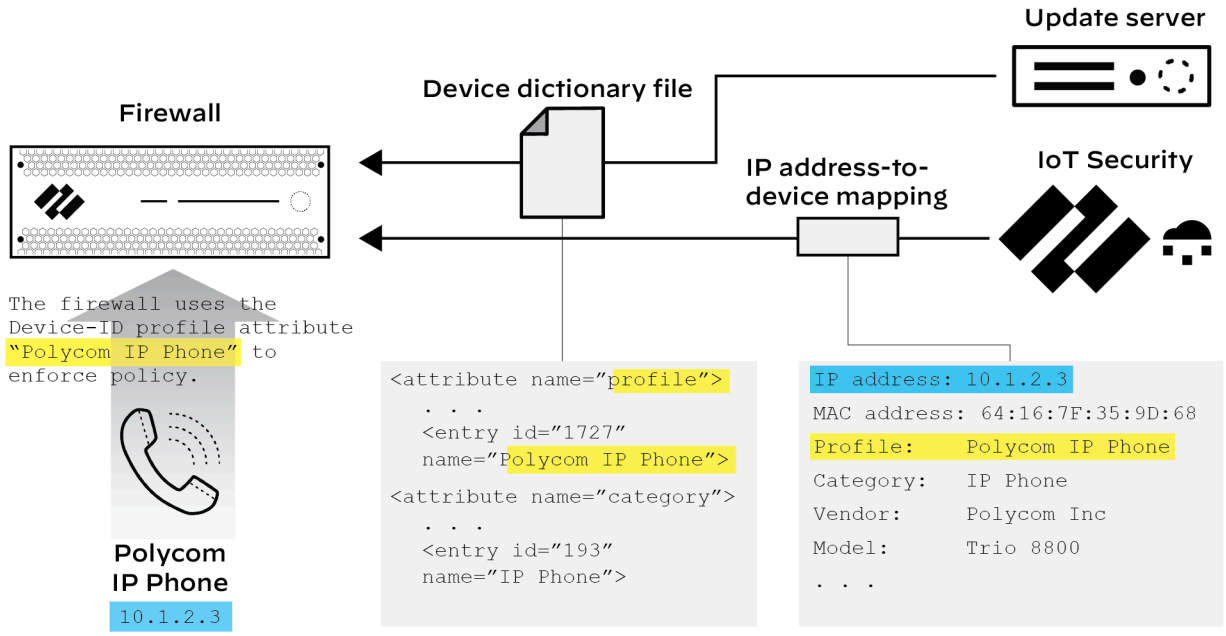
设备 ID

PAN-OS 10.0 引入了新的策略实施概念：Device-ID。Device-ID 是一种根据设备属性强制执行策略规则的方法。IoT Security 为防火墙提供一个设备字典文件，其中包含设备属性列表，例如配置文件、类别、供应商和型号。对于字典文件中的各种属性，它列出了一组条目。例如，配置文件属性的三个条目可能是 Advidia Camera、BK Medical UltraSound Machine 和 Carefusion Infusion Pump Base Station。

目前，*multi-vsys* 防火墙不支持 *Device-ID*。

配置安全策略规则时，防火墙管理员可以选择从设备字典中选择设备属性。如果他们选择 **Profile**（配置文件），则可以选择其中一个配置文件条目：例如，**Polycom IP Phone**（**Polycom IP** 电话）。然后，策略规则将应用于与此配置文件匹配的所有设备。但是，防火墙如何知道设备的配置文件是什么呢？它从 IP 地址到设备的映射中了解配置文件，IoT Security 也会向防火墙提供

该配置文件。这些映射标识每个设备的属性。当来自映射到策略规则中指定的设备属性的 IP 地址的流量到达防火墙时，策略规则查找将找到与此规则的匹配项，并应用它强制执行的任何操作。



防火墙从更新服务器下载设备字典文件。字典文件填充配置文件、类别、供应商等的所有 Device-ID 属性列表中的条目。然后，这些属性条目可用作策略规则配置元素。防火墙管理员接下来使用配置文件属性“Polycom IP 电话”配置防火墙策略规则。Polycom Trio 8800 设备加入网络后，然后 IoT Security 会识别它，IoT Security 为防火墙提供 IP 地址到设备的映射。此示例的映射中的两个关键元素是其设备配置文件（Polycom IP 电话配置文件，以黄色突出显示）和其 IP 地址（10.1.2.3，以蓝色突出显示）。当来自 10.1.2.3 的 Polycom Trio 8800 设备的流量到达防火墙时，它会执行 Device-ID 策略规则查找，发现此 IP 地址处设备的配置文件与策略规则中指定的配置文件匹配，然后应用该规则。

如果防火墙从 *IoT Security* 断开连接，防火墙将保留其 *IP* 地址到设备的映射，并继续对它们执行 *Device-ID* 策略规则，直到重新建立连接。

每个新一代防火墙型号都具有相同的最多 1000 个唯一 Device-ID 对象。

Device-ID 对象的最大数量为 1000 个，这与 IP 地址到设备映射的最大数量不同。IP 地址到设备映射的最大数量因防火墙型号而异，与“产品选择”页面上每种防火墙型号的“+ 显示更多”部分中列出的 User-ID 最大值相同。

有关 Device-ID 功能的详细信息，请参阅《PAN-OS 管理员指南》。

设备目录

设备字典是防火墙在安全策略规则中使用的 XML 文件。它包含以下设备属性的条目：配置文件、类别、供应商、型号、操作系统系列和操作系统版本。这些条目来自所有 IoT Security 租户的设备，并定期完全刷新，并作为新文件发布到更新服务器上。如果字典条目有任何更改，则会在更新服务器上发布修订后的文件，以便 Panorama 和防火墙在下次检查更新服务器时自动下载并安装该文件，每两个小时自动执行此操作。

IP 地址到设备的映射

在 IoT Security 识别设备后，它会捆绑有关它的以下一组标识特征：

- IP 地址
- MAC 地址
- 主机名
- 设备类型
- 设备类别
- 设备配置文件
- 供应商
- 模型
- OS 系列
- OS 版本
- 风险评分
- 风险程度

防火墙轮询 IoT Security 这些 IP 地址到设备的映射，以用于策略实施。防火墙每秒轮询一次新的或修改的映射，并且 IoT Security 会返回它已识别出的具有高置信度（置信度分数为 90-100%）的映射，这些映射适用于过去一小时内处于活动状态的设备。对于防火墙接收的每个 IP 地址到设备映射，防火墙会在其主机信息配置文件 (HIP) 匹配日志中生成一个条目。

如果 IoT Security 发现重复的 IP 地址到设备的映射（即，有两个 IP 地址映射到同一设备的 MAC 地址），它会将其解析为具有最新网络活动的 MAC 地址。

防火墙保留 IP 地址到设备映射的时间没有时间限制。只有当缓存填满时，它才会开始删除它们，从最早的开始删除。

策略规则建议

您可以根据同一设备配置文件中 IoT 设备的正常、可接受的网络行为生成安全策略规则建议，并手动将其导入防火墙以进行实施。PAN-OS 8.1 及更高版本支持导入 IoT Security 策略规则建议.

对于具有需要 *Strata Logging Service* 的 *IoT Security* 订阅的 *Panorama* 托管防火墙 — 在用于将托管防火墙加入 Strata Logging Service 时，*Panorama* 才能导入策略规则建议。

与 **IoT Security** 相关的防火墙和 **Panorama** 通信

来自没有 Panorama 管理的防火墙的 IoT Security 通信：

- 防火墙在 TCP 端口 443 上从 updates.paloaltonetworks.com 更新服务器下载设备字典文件。
- 防火墙将日志转发到 TCP 端口 443（用于增强型应用程序日志）和 3978（用于所有其他防火墙日志）上的日志记录服务。

有关新一代防火墙与日志记录服务通信所需的端口和 *FQDN* 的详细信息，请参阅 Strata Logging Service 入门。

- 防火墙在 TCP 端口 443 上从 IoT Security 中检索 IP 地址到设备的映射和策略建议。根据其所在区域，他们使用以下边缘服务 URL 之一：
  - 美国：iot.services-edge.paloaltonetworks.com
  - 加拿大：ca.iot.services-edge.paloaltonetworks.com
  - 欧盟：eu.iot.services-edge.paloaltonetworks.com
  - 瑞士：ch.iot.services-edge.paloaltonetworks.com
  - 英国：uk.iot.services-edge.paloaltonetworks.com
  - APAC：apac.iot.services-edge.paloaltonetworks.com
  - 日本：jp.iot.services-edge.paloaltonetworks.com
  - 澳大利亚：au.iot.services-edge.paloaltonetworks.com

  下表总结了不同数据湖区域/提取区域与 IoT Security 应用区域之间的关系：

	数据湖区域/提取区域	IoT Security 应用区域
美洲	加拿大	加拿大、美国*
	美国	美国
	FedRAMP	FedRAMP
欧盟	法国	德国
	德国	德国
	意大利	德国
	荷兰	德国
	波兰	德国
	西班牙	德国
	瑞士	瑞士、德国*
	英国	英国、德国*
亚太地区	澳大利亚	澳大利亚、新加坡*
	印度	新加坡
	印度尼西亚	新加坡
	日本	日本

	数据湖区域/提取区域	IoT Security 应用区域
	新加坡	新加坡

*已将瑞士和英国添加为 2023 年 7 月 31 日的 IoT Security 应用程序区域。在此日期之后，将 IoT Security 加入在它之前建立的现有防火墙部署时，防火墙将继续使用 **Germany**（德国）作为 IoT Security 应用程序区域。对于 2023 年 7 月 31 日之后，将 IoT Security 加入在瑞士或英国建立的新部署时，防火墙将为每个国家/地区使用本地 IoT Security 应用程序区域。

加拿大也是类似的情况，该国家继续使用 **United States – Americas**（美国 - 美洲）作为 2023 年 1 月 25 日之前存在的部署的 IoT Security 应用程序区域，对于此日期之后的新部署，则使用 **Canada**（加拿大）。同样，澳大利亚在 2022 年 10 月 25 日之前存在的部署仍使用 **Singapore**（新加坡） 的 IoT Security 应用程序，而在此日期之后的新部署则使用 **Australia**（澳大利亚）。

- 在防火墙和 IoT Security 云前面的边缘服务器之间进行证书交换期间，它们会验证彼此的证书。防火墙通过检查以下站点来验证它收到的证书：
  - o.lencr.org
  - c.lencr.org

  与这些站点的通信通过 TCP 端口 80 上的 HTTP 进行。

来自 Panorama 的 IoT Security 通信：

- Panorama 管理服务器通过上面列出的防火墙使用的相同 URL 从 IoT Security 中导入策略建议。在验证边缘服务器提供的证书时，Panorama 会检查上面列出的防火墙检查的相同站点。

  Panorama 管理下的防火墙仍使用 *IP* 地址到设备的映射的区域边缘服务 *URL* 联系 *IoT Security*，它们仍从更新服务器下载设备字典，并且仍将日志转发到日志记录服务。
- Panorama 管理服务器将日志查询发送到 TCP 端口 444 上的日志记录服务。

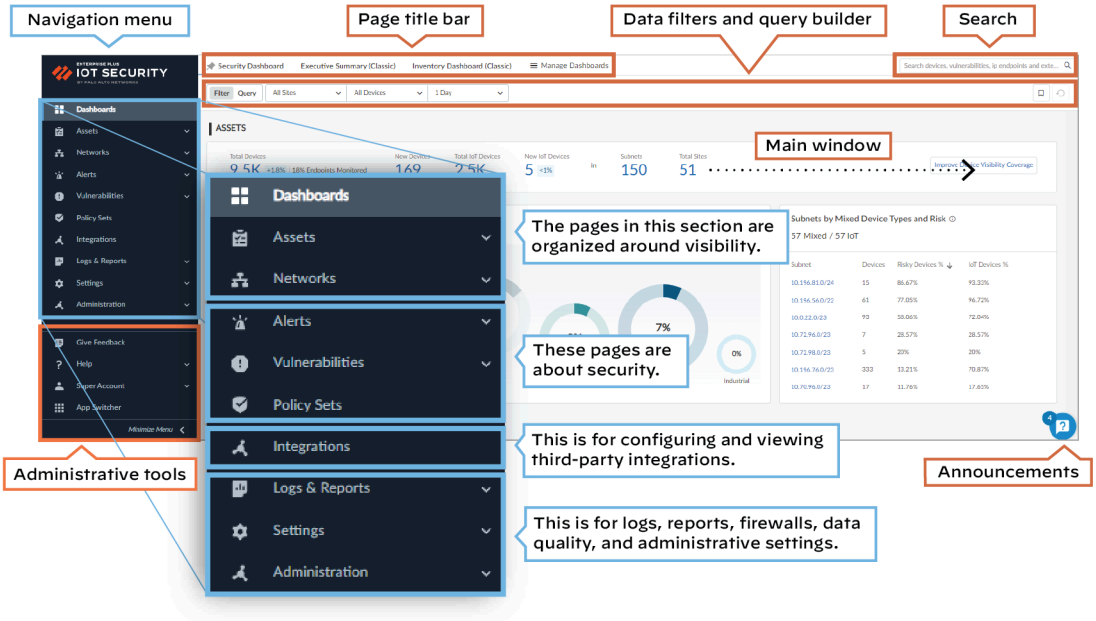
IoT Security 门户

加入 IoT Security 后，请在防火墙上激活 IoT Security 许可证，并部署它们，以便它们能够将数据提供给日志记录服务，这样，您就可以访问 IoT Security 门户并开始使用它了。使用 Palo Alto Networks 客户服务门户帐户凭证登录。

IoT Security 使用单点登录 (SSO) 来验证您的登录。

IoT Security 门户完全支持 *Google Chrome* 并部分支持 *Microsoft Edge*，这意味着该门户预计可用，但可能看起来不完全符合设计。它没有提供对 *Microsoft Internet Explorer*、*Apple Safari* 或任何其他类型浏览器的正式支持。

门户界面分为几个部分。



导航 — 左侧导航菜单中的项目大致分为四个部分。第一部分围绕可见性进行组织：指示板、资产和网络。下一部分与安全相关：警报、漏洞和策略集。第三部分是配置和检查将 IoT Security 与第三方产品集成相关的设置：集成。最后，在最后一部分，您可以检查日志、报告、防火墙和数据质量，并对管理设置进行管理：日志和报告、设置和管理。

使用左侧导航菜单导航至 IoT Security 门户。当页面顶部有数据过滤器时，使用它们来控制按站点、设备类型和时间段显示在页面上的数据。

导航菜单下是一组管理工具：

- 提供反馈 — 向 IoT Security 开发人员提供反馈。
- 帮助 — 打开客户支持门户。
- 用户名（用户联系信息中的名字和姓氏）— 单击姓名时，将显示以下选项：
  - 首选项 — 修改您的联系信息、时区、空闲会话超时时间、警报声音（即控制在 IoT Security 检测到新的安全警报时是否发出声音）、以及短信和电子邮件通知设置。
  - 资源中心 — 查看有关防火墙日志的状态通知，并通过推荐的资源和有用的链接了解 IoT Security
  - 深色主题/浅色主题 — 切换深色和浅色 UI 显示主题。
  - 注销 — 注销您的管理会话。
- 应用程序切换器 — 通过 Hub 快捷方式访问其他 Palo Alto Networks 应用程序。

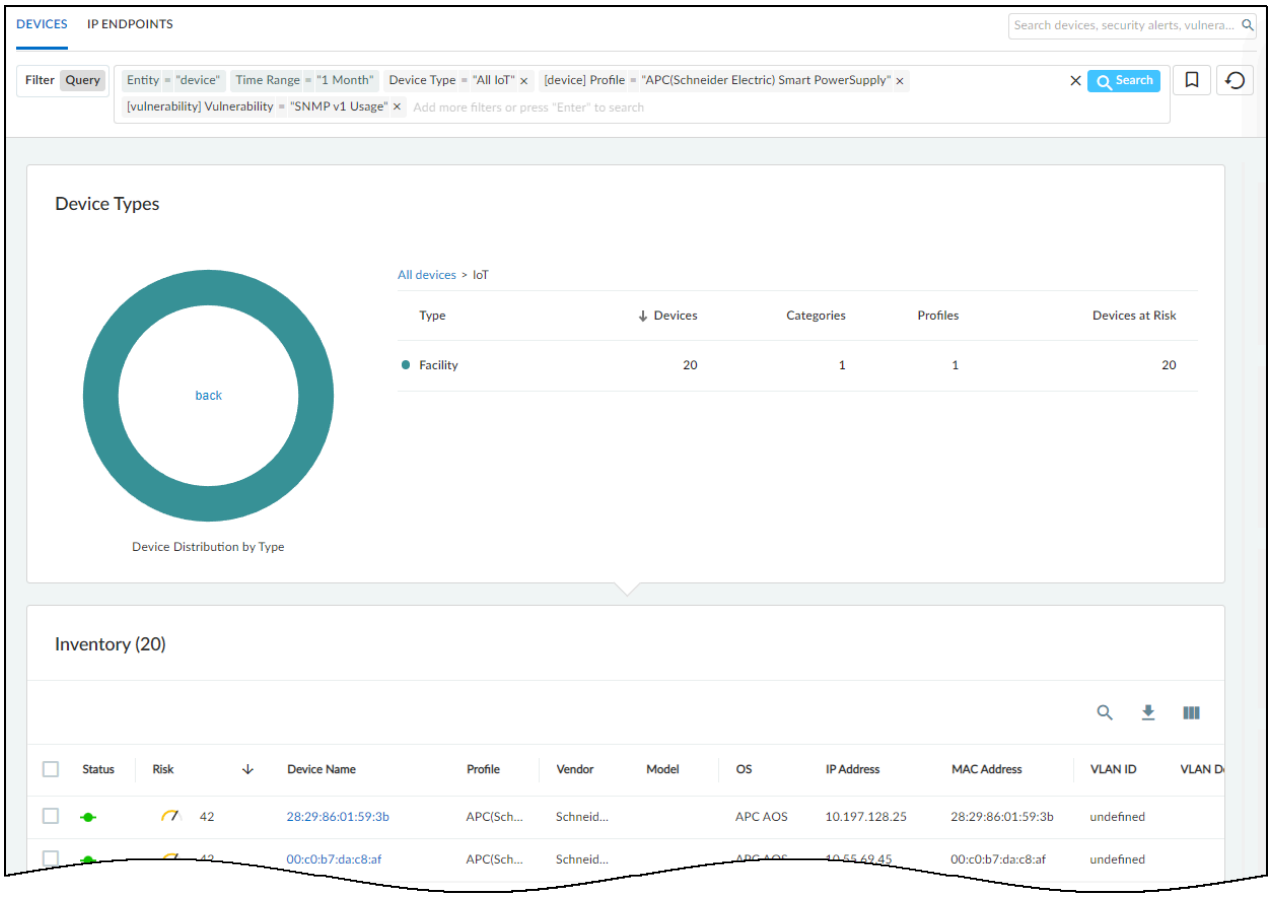
搜索 — 页面顶部标题栏右侧有一个搜索字段，您可以在其中输入关键字来搜索设备、警报、漏洞和外部目标，从而查找数据。

数据过滤器 — 许多页面的标题栏和搜索栏下方是一组过滤器，用于在每个页面上控制 IoT Security 门户的显示。过滤系统由全局过滤器和本地页面特定过滤器组成。当您在不同页面之间导航时，全局过滤器设置会保持不变，并且每个页面会根据需要出现各种过滤器。例如，漏洞页面上没有时间过滤器，设备和安全警报页面上有附加过滤器，而用户帐户页面上根本没有过滤器。全局过滤器有默认值，但也可以自定义。修改和添加的过滤器在 UI 中显示为蓝色而不是黑色，因此您可以轻松地将它们与默认过滤器区分开来。如果页面具有默认的本地过滤器，它将出现在页面顶部的其他全局过滤器中。例如，“安全警报”页面默认应用“活动警报”过滤器，因此每当您打开“安全警报”页面时，此本地过滤器就会自动出现在全局过滤器中。此外，还有仅适用于特定页面上的数据的页面过滤器。当您向下滚动页面时，全局过滤器和页面过滤器仍会保留在标题栏右上方的视图中。

查询生成器 — 数据过滤器旁边是查询生成器。通过构建各种组件的查询，使用它来查找有关设备、警报和漏洞的信息。单个查询可以结合设备和安全警报或设备和漏洞。例如，您可以查询特定供应商发出特定警报的所有 IoT 设备，或者查询特定配置文件中具有特定漏洞的所有 IoT 设备。例如，此查询显示 APC (Schneider Electric) 智能电源设备配置文件中的设备是否支持 SNMPv1：

```
entity = device, Time Range = “month”, Device Type = “All IoT”,
 [device] Profile = “APC(Schneider Electric) Smart PowerSupply”
 [vulnerability] Vulnerability = “SNMPv1 Usage”
```

查询结果显示有 20 个 IoT 设备支持 SNMPv1，以及它们分别是哪些。



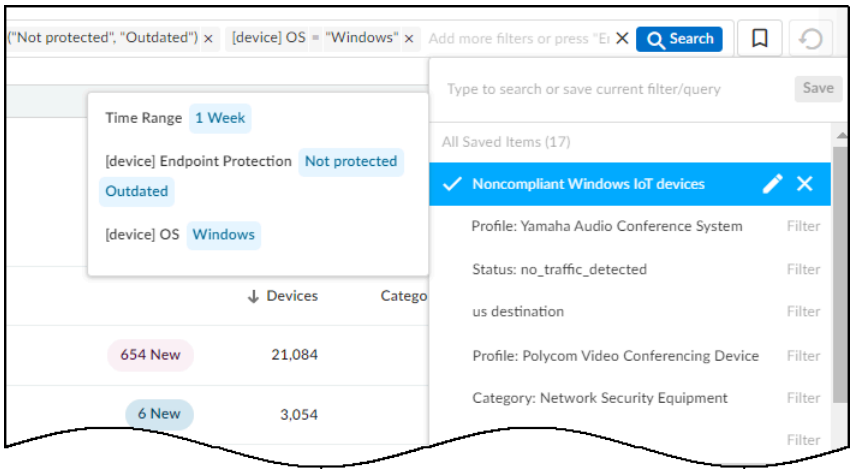
该查询工具使用运算符 =（等于）、 !=（不等于）和 IN（包含），并在表达式之间使用逻辑运算符“AND”。例如，以下查询用于获取数据，其中 Time Range = “week” **AND** Device Type = “All IoT” **AND** [vulnerability] Severity IN (“High”, “Critical”)：

```
entity = device, Time Range = “week”, Device Type = “All IoT”,
 [vulnerability] Severity IN (“High”, “Critical”)
```

您可以保存查询，这样就不必重新创建重复使用的查询。要保存查询，请单击查询字段右侧的功能区书签图标，然后为其命名。例如，如果您定期检查过去一周内在网络上活跃且没有端点保护或保护已过期的运行 Windows 操作系统的 IoT 设备的数量，请创建此查询并使用诸如“不合规的 Windows IoT 设备”之类的名称保存它：

```
entity = device, Time Range = “week”, Device Type = “All IoT”,
 [device] Endpoint Protection IN (“Not protected”, “Outdated”),
 [device] OS = “Windows”
```

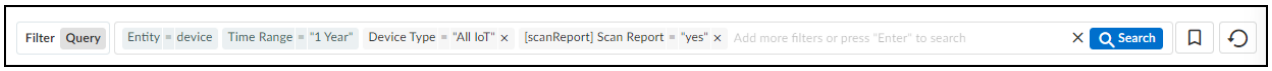
当您想要再次使用该查询时，只需单击书签图标，然后单击先前保存的查询和过滤器列表中的名称。您还可以编辑此列表中的条目并删除它们。



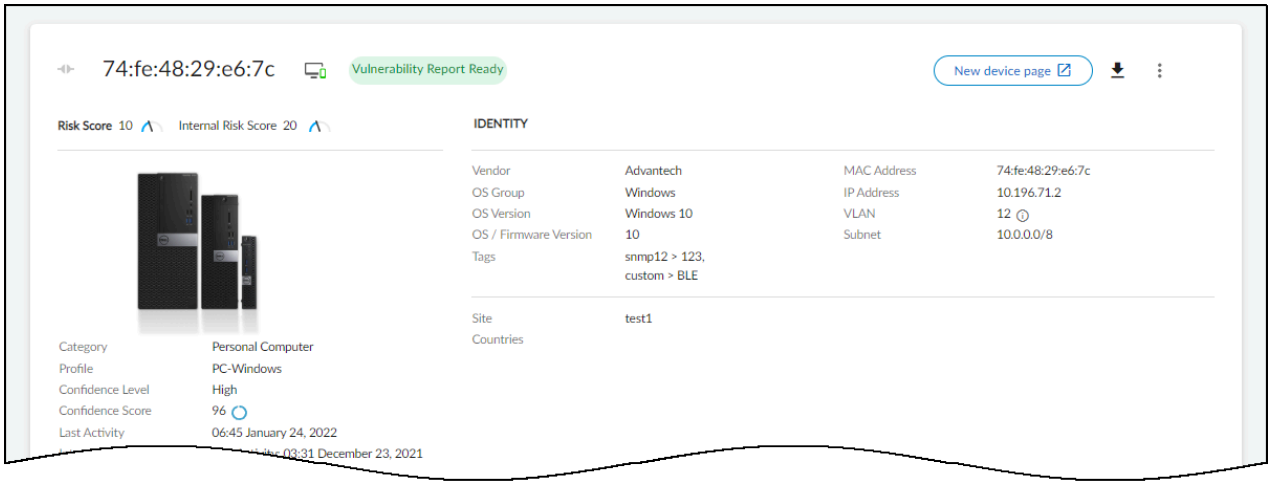
您无法保存任何指示板的查询，例如执行摘要。

查询工具具有许多参数，您可以使用它们来查找所需的任何数据。例如，输入以下查询可检查哪些设备在漏洞扫描报告中：

```
Entity = device, Time Range = “1 Year”, Device Type = “All IoT”,
 [scanReport] Scan Report = “yes”
```

通过查看查询结果中的设备“设备详细信息”页面并单击 **Vulnerability Report Ready**（漏洞报告就绪），您可以将报告以 PDF 格式下载到您的系统中，以便在其中保存和阅读。



为了帮助您开始使用查询生成器，IoT Security 提供常见查询的示例模板集合。研究这些预配置的查询以了解查询生成器的功能，按原样使用它们，或将它们用作构建您自己的类似查询的模型。

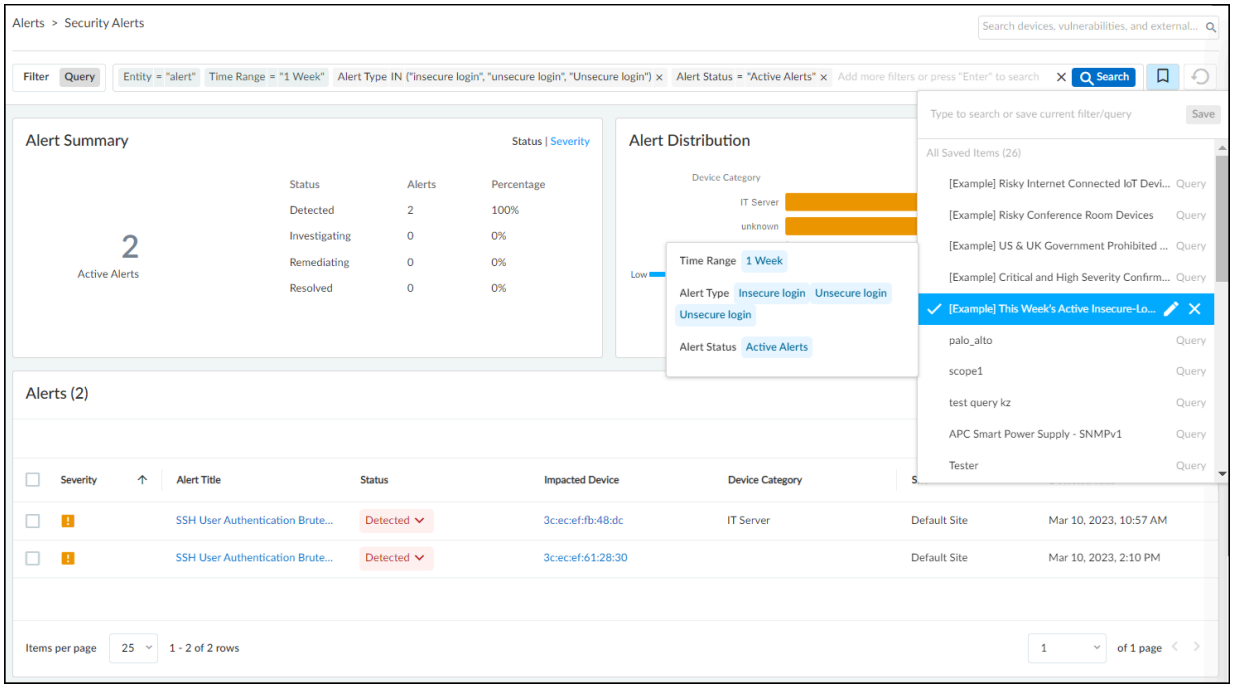
要查看预配置的示例查询，请单击页面标题栏下的 **Query**（查询），然后单击 **Query Bookmarks**（查询书签）图标。

根据 IoT Security 门户上活动的垂直主题，预配置的模板会有所不同。每个垂直主题有五个示例模板。下面是每个主题的示例：

Enterprise IoT Security Plus

- 名称：[示例] 本周的活动不安全登录警报
- 查询：Entity=”alert”, Time Range=”1 Week”, Alert Status=”Active Alerts”, Alert Type IN (“insecure login”, “unsecure login”, “Unsecure login”)

- 摘要：这会查询 IoT Security 针对过去一周内与不安全登录相关的所有活动警报。



Industrial IoT Security

- 名称：[示例] 关键风险联网工业设备
- 查询：Entity="device", Time Range="1 Year", Device Type="Industrial", [device] Risk = "Critical", [device] Internet Access="yes"
- 摘要：这会查询 IoT Security 以显示过去一年内所有具有关键风险等级且可以访问互联网的 Industrial IoT 设备。

Medical IoT Security

- 名称：[示例] 存在风险的联网 IoT 设备
- 查询：Entity="device", Time Range="1 Year", Device Type="All IoT", [device] Risk IN ("High", "Critical"), [device] Internet Access="yes"
- 摘要：这会查询 IoT Security 以显示过去一年内所有具有高或关键风险级别，并且可以访问互联网的 IoT 设备。

您可以编辑构成查询模板的表达式和模板名称，或许可以使用新名称保存修改后的查询以供以后重复使用。您也可以删除示例模板。

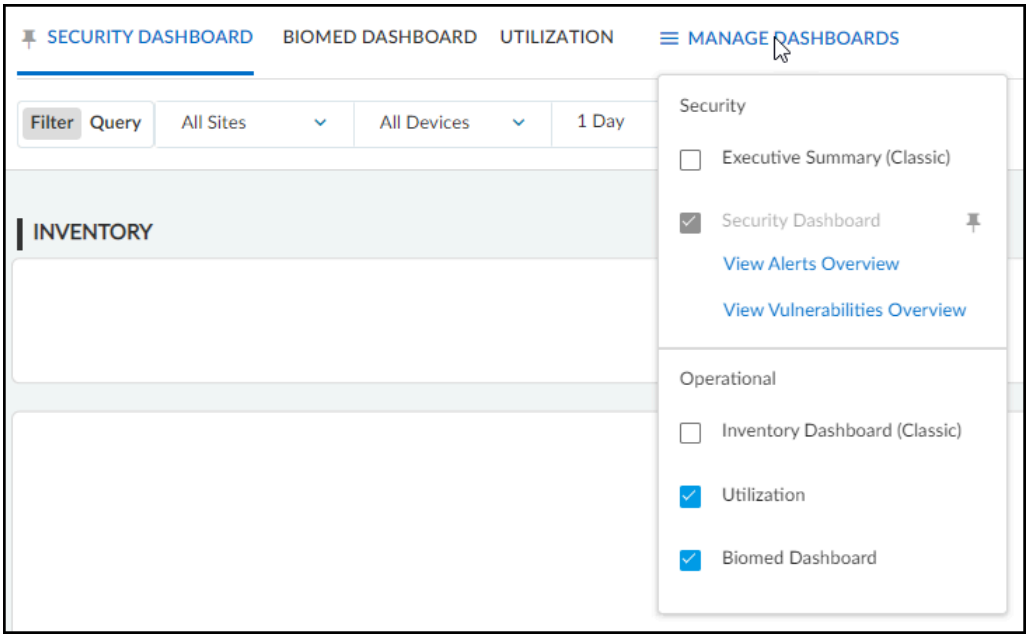
公告 — 打开和关闭用户界面右侧的垂直面板，其中包含有关最新功能发布和重要安全公告的信息。

管理指示板 — 当您的门户主题有多个指示板时，例如Medical IoT Security，您可以控制哪一个是默认的，哪些可以在相邻的选项卡中快速访问，哪些是隐藏的。认识到 IoT Security 门户的用户在不同角色中发挥作用，IoT Security 让您以最适合自己需求的方式设置偏好，从而提高效率和生产力。

1. 要管理各种指示板的显示，请选择 **Dashboards**（指示板） > **Manage Dashboards**（管理指示板）。

2. 在 **Manage Dashboards**（管理指示板）下拉菜单中，选中您想要显示为选项卡式指示板以便更快访问的指示板的复选框。清除您不想显示为选项卡式指示板的复选框。

   主窗口中显示的选项卡式指示板的从左到右顺序与下拉菜单中列出的指示板的从上到下顺序相对应，其中固定（首选）指示板显示在最左侧。



3. 要设置在左侧导航面板中导航到 **Dashboards**（指示板）时首先显示的默认指示板，请单击 **Manage Dashboards**（管理指示板）下拉菜单中指示板名称旁边的图钉图标。

   如果您将门户主题更改为不包含固定指示板的垂直主题，则该垂直主题的默认指示板将成为新的固定指示板。

4. 要打开显示安全警报和漏洞的新浏览器选项卡或窗口，请单击 **View Alerts Overview**（查看警报概述）和 **View Vulnerabilities Overview**（查看漏洞概述）。

垂直主题门户

IoT Security 门户进行了更改，以更好地为不同行业的用户提供服务。给定 IoT Security 租户中的用户看到的门户主题取决于两个选择：

- 购买时选择的 IoT Security 产品
- IoT Security 租户所有者选择的主题

门户主题

IoT Security 为企业、工业和医疗垂直领域提供四种不同主题的门户：

- Enterprise IoT Security Plus
- Enterprise IoT Security
- Industrial IoT Security
- Medical IoT Security

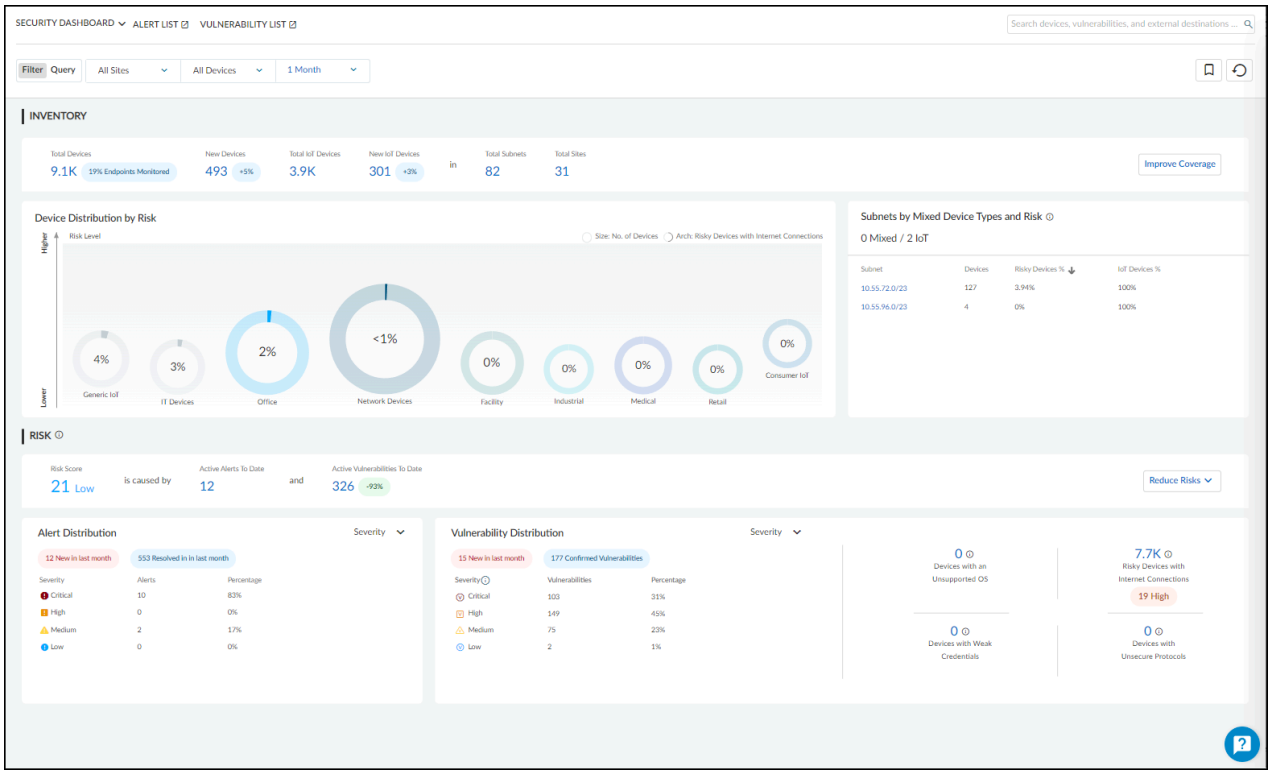
Enterprise 版

IoT Security 为企业 IoT 提供两种产品：Enterprise IoT Security Plus 和 Enterprise IoT Security。

Enterprise IoT Security Plus 是适用于商业企业和政府组织的解决方案。它使您可以查看和保护企业组织中的每台 IoT 设备，以符合 NIST 指南。它还有助于防止您的 IoT 设备成为网络攻击的目标。使用 Enterprise IoT Security Plus，您可以执行以下操作：

- 自动对具有 50 多个设备属性的设备进行分类
- 查看、编辑、确认和重新分类设备
- 添加具有静态 IP 地址的设备
- 查看您的 IP 地址结构和设备分布
- 查看防火墙和设备网站
- 为设备、网络行为和安全风险生成报告
- 与多个第三方产品集成
- 查看设备使用的应用程序
- 将策略规则建议导入防火墙
- 获取异常网络活动的安全警报
- 评估风险和设备漏洞
- （可选）保留流量日志

安全控制面板可让您快速访问有关设备清单、警报和风险的信息，如下所示。它出现在 Enterprise IoT Security Plus 门户以及 Industrial IoT Security 和 Medical IoT Security 门户中。

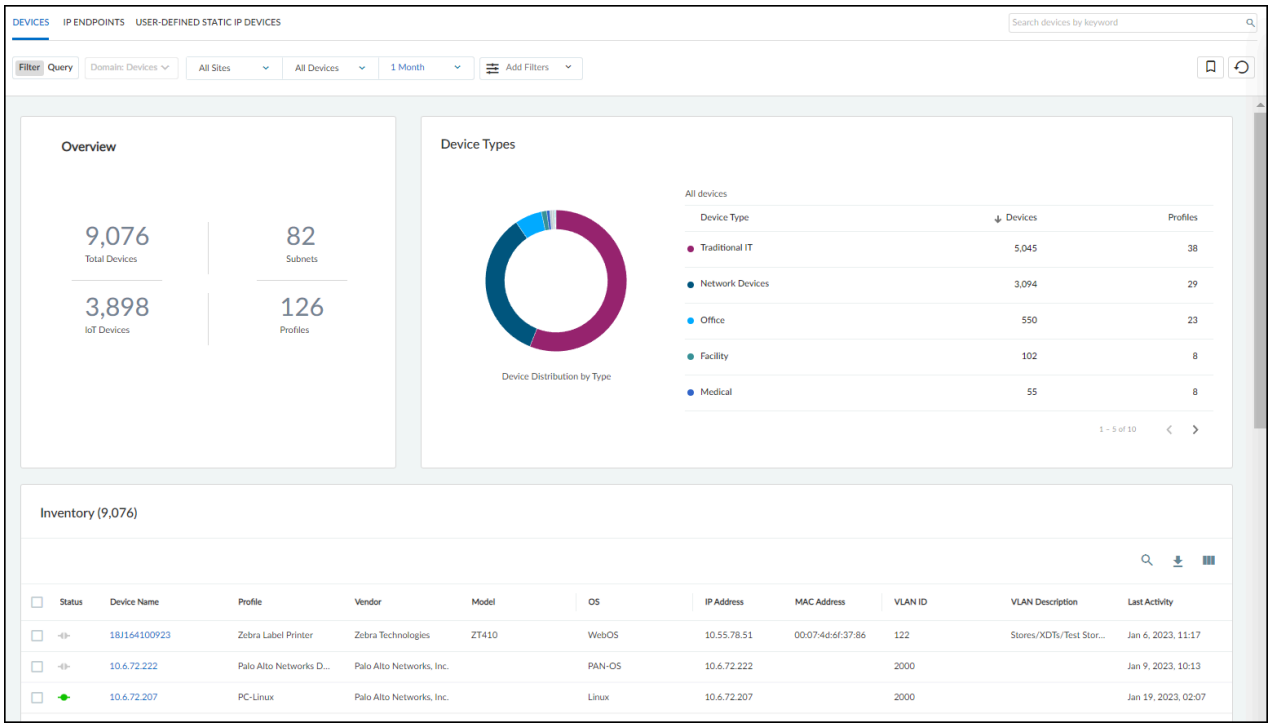


对于在 *2022* 年 *12* 月 *15* 日之立建立 租户 的 *IoT Security* 客户，您可以在有限的时间内继续使用现有的执行摘要和清单控制面板。他们最终将退役并被替换。

Enterprise IoT Security 识别企业网络中的设备并创建动态设备清单。它不包括 Enterprise IoT Security Plus、Industrial OT Security 和 Medical IoT Security 中可用的安全功能和第三方集成。Enterprise IoT Security 允许您执行以下操作：

- 自动对具有 12 个设备属性的设备进行分类
- 查看、编辑、确认和重新分类设备
- 添加具有静态 IP 地址的设备
- 查看您的 IP 地址结构和设备分布
- 查看防火墙和设备网站
- 生成设备报告

设备页面如下所示，是登录 Enterprise IoT Security 门户后的默认登录页面。与其他以垂直为主题的产品门户不同，它不包含指示板。



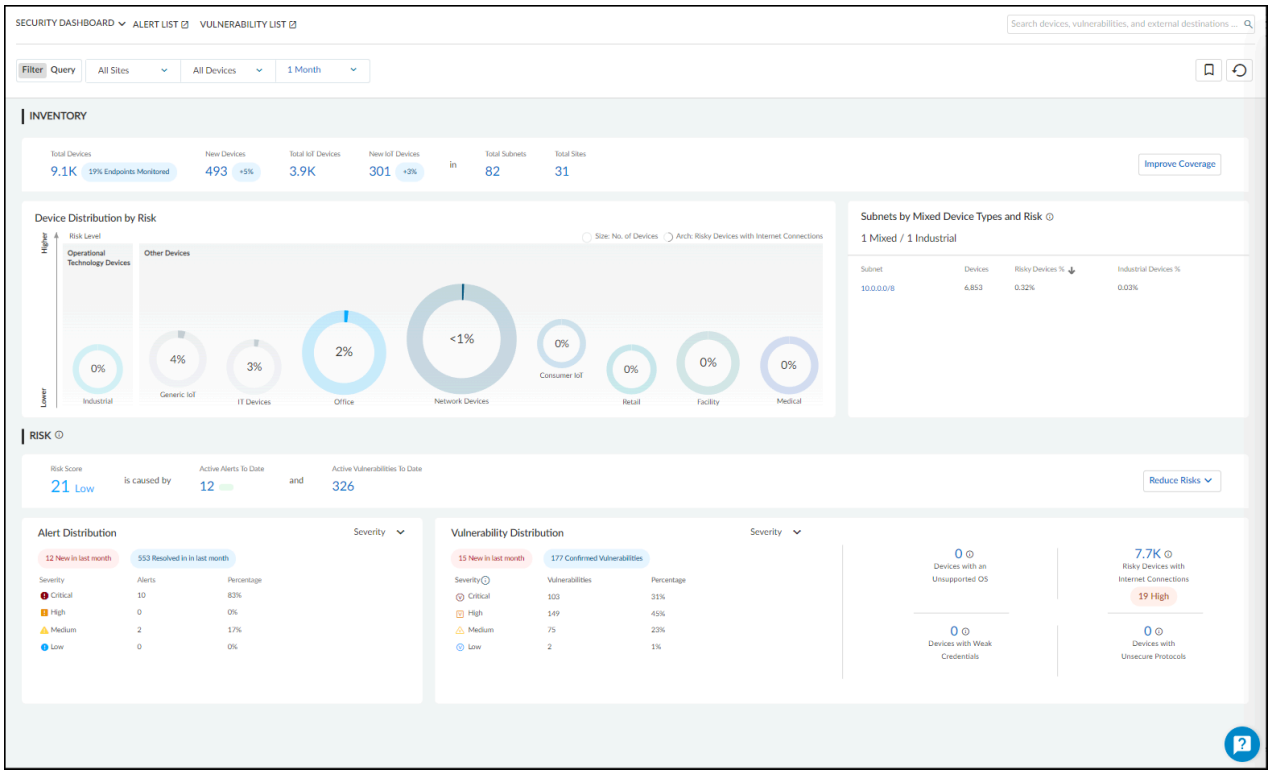
有关更多信息，请参阅 Enterprise IoT Security管理员指南。

工业

Industrial IoT Security 是工业企业的解决方案。它使您可以查看和保护每台设备，包括专业操作技术 (OT) 设备，因此您可以随时保持运营正常运行并达到 NIST 和 ISA/IEC 合规性。您可以使用 Industrial IoT Security 执行以下操作：

- 获得 Enterprise IoT Security Plus 中的所有功能
- 检测 OT 设备异常
- 使用 Purdue 等级进行设备建模和可视化（参阅网络可视化）
- 为流程完整性创建自定义规则（参阅创建警报规则）

与 Enterprise IoT Security Plus 门户一样，Industrial IoT Security 门户还包括安全控制面板。



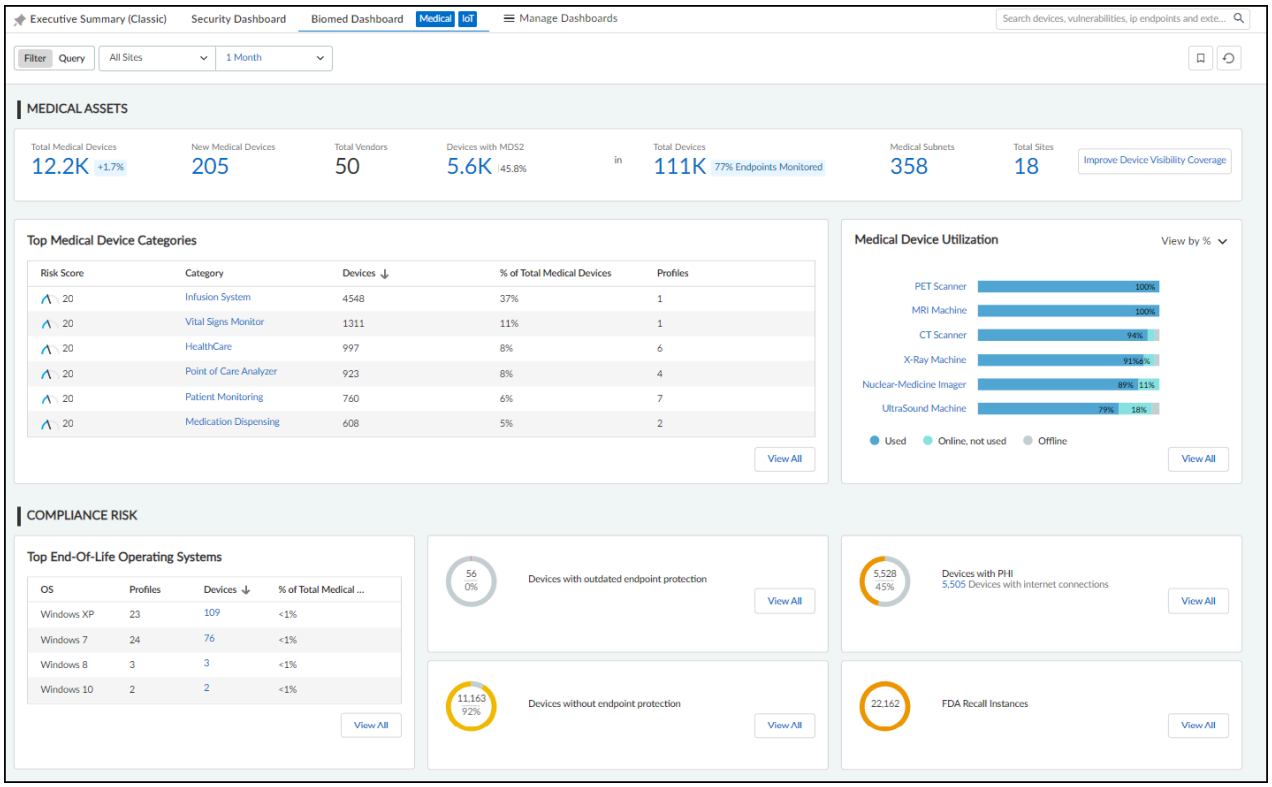
工业网络包含一个或多个气隙分段的情况并不少见。这些网络区域不允许在气隙网络分段中的设备与任何其他私有网段或公共网络中的设备之间进行入口或出口连接。通过使用配置为安全遥测网关的新一代防火墙，您可以为此类网络中的设备提供 IoT Security 服务。

Medical

Medical IoT Security 是医疗保健提供者的解决方案。它使您可以查看和保护网络上的所有设备，包括专业医疗设备，因此您可以提供高质量的患者护理并达到 HIPAA 合规性。使用 Medical IoT Security 执行以下操作：

- 获得 Enterprise IoT Security Plus 中的所有功能
- 检测医疗设备异常
- 利用 FDA 召回、PHI 识别和 MDS2 评估医疗设备风险
- 追踪医疗设备使用情况

Medical IoT Security 门户显示两个仅与Medical IoT 相关的页面，并且仅在激活 Medical IoT Security 主题时出现。一个用于食品药品监督管理局 (FDA) 召回，另一个用于医疗设备安全制造商披露声明 (MDS2) 表格。使用 Medical IoT Security 主题时，该门户还包括两个指示板，其中包含有关医疗 IoT 设备的数据：利用率指示板和生物医学指示板，如下所示。

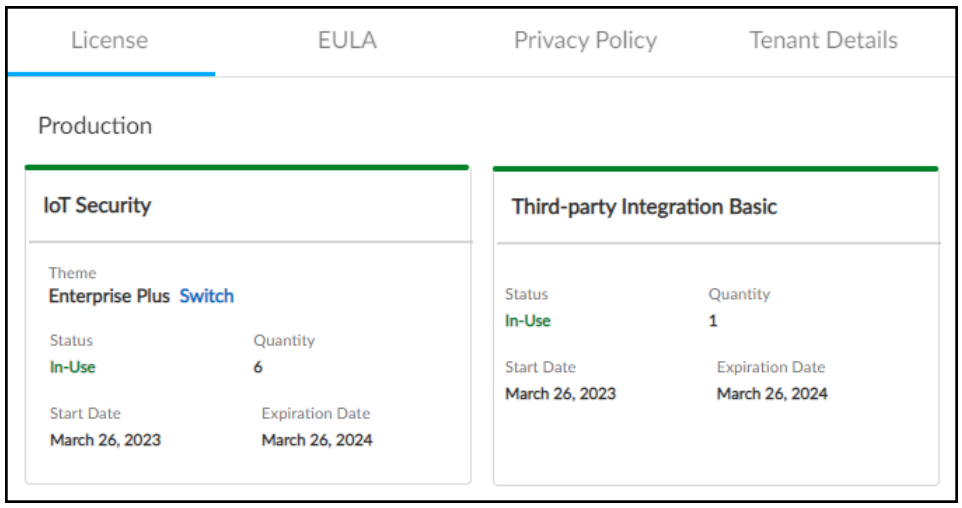


有关详细信息，请参阅Medical IoT。

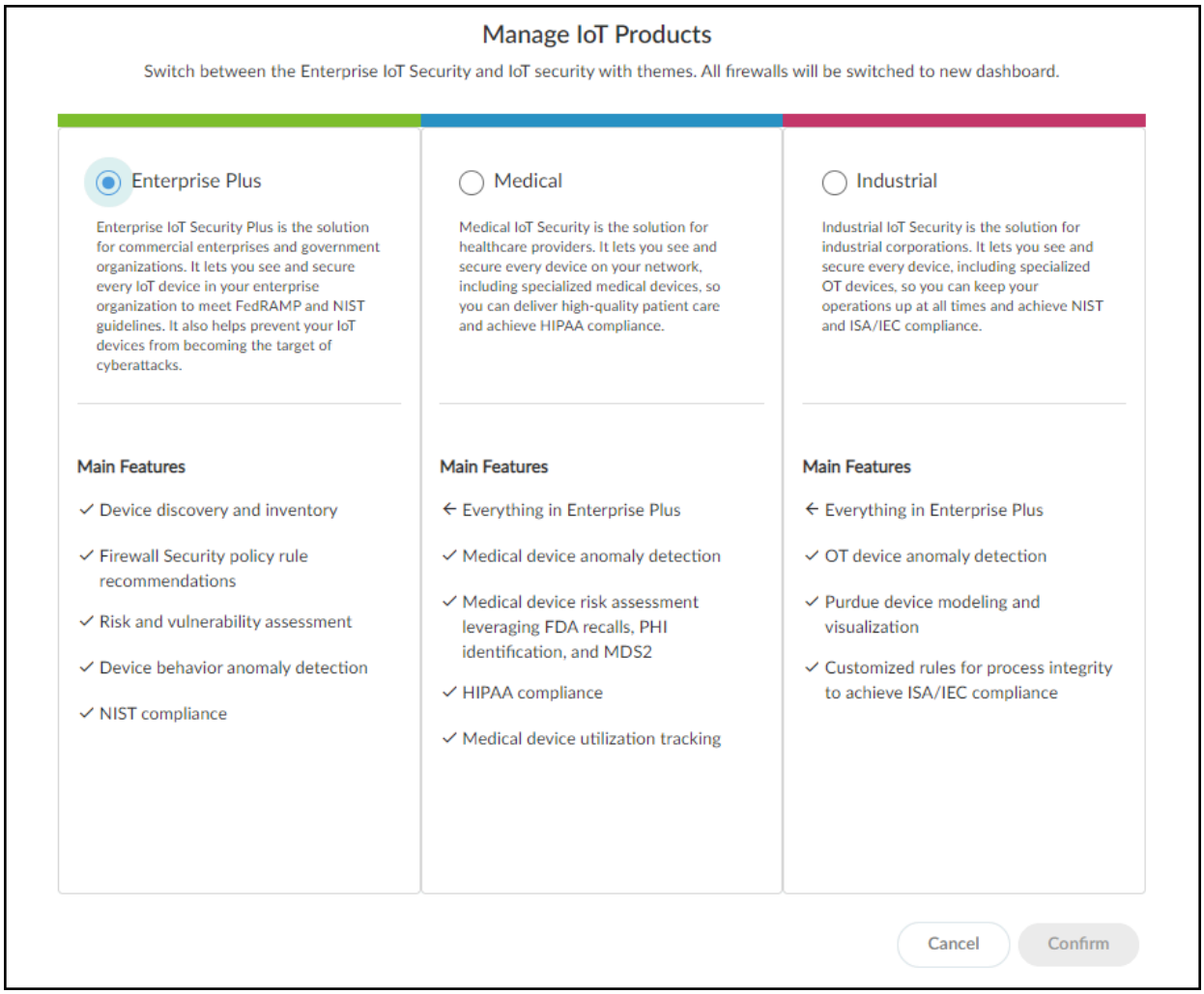
切换门户主题

租户一次只能为 IoT Security 租户设置一个主题；但是，租户所有者可以切换主题。当用户首次登录租户，并且订购的 IoT Security 产品已定义主题时，默认情况下会自动加载该主题。但是，如果您购买了多个具有不同主题的 IoT Security 产品（或者您是在 2022 年 12 月 15 日之前购买的 IoT Security 产品），则 IoT Security 会在所有者首次登录门户时提示他们选择一个主题。如果所有者未做出选择，则 IoT Security 显示 Enterprise IoT Security Plus 主题，并继续提示所有者在每次登录时选择一个主题，直到其中一个人做出选择。做出选择后，同一租户中的所有其他用户在访问门户时也将看到相同的主题。

要切换垂直主题，请以具有所有者权限的用户身份登录，选择 **Administration**（管理） > **About**（关于） > **License**（许可证）。状态表示当前正在使用哪个主题。（您还可以在此处查看订阅的防火墙数量以及许可证的开始和到期日期。）单击当前正在使用的主题名称旁边的 **Switch**（切换）。



选择一个新主题，然后单击 **Confirm**（确认）。



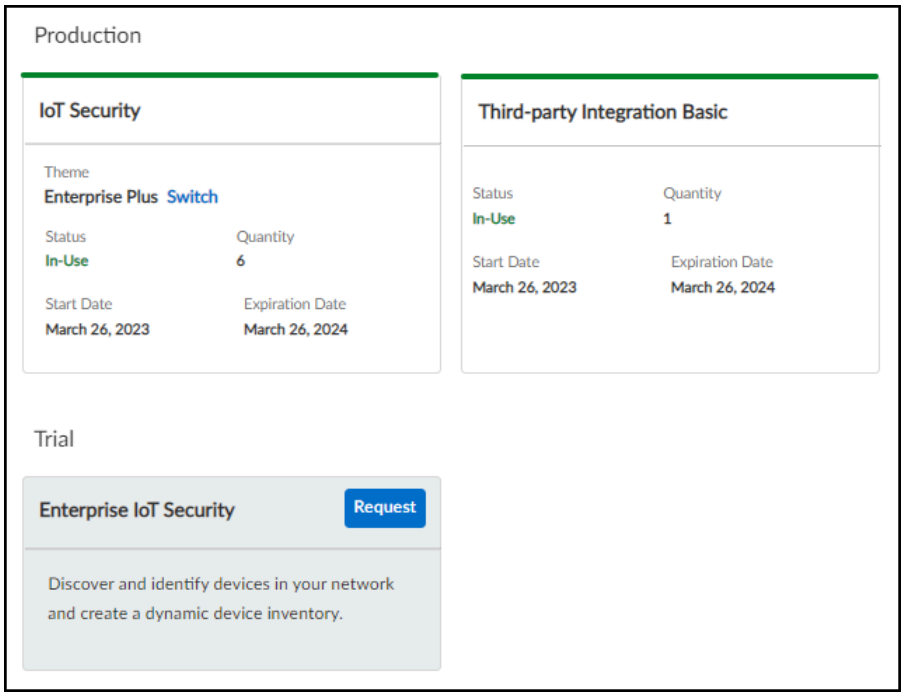
作为所有者，您可以根据需要多次为租户切换主题。

创建试用 Enterprise IoT Security 租户

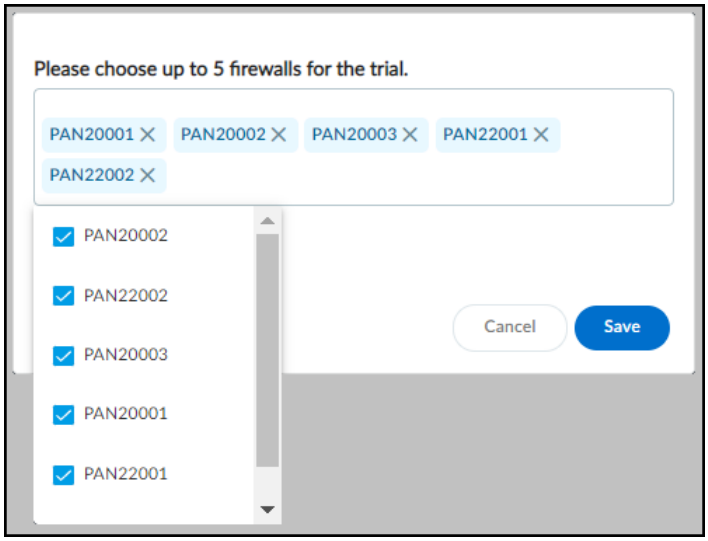
如果您拥有 Enterprise IoT Security Plus、Industrial IoT Security Medical IoT Security 的生产许可证，并想了解 Enterprise IoT Security，则可以创建一个一次性试用租户，并为其分配最多五个防火墙。试用有效期为 30 天。在此期间，生产租户和试用租户都会使用分配给试用租户的防火墙发送给日志记录服务的日志数据。当试用期结束且试用租户被自动删除时，仅生产 IoT Security 租户将继续使用来自防火墙的日志数据。

1. 要启动试用版，请使用具有所有者权限的用户帐户登录 IoT Security 门户。

2. 选择 **Administration**（管理） > **About**（关于） > **License**（许可证），然后在“试用”部分单击 Enterprise IoT Security 旁边的 **Request**（请求）。



3. 最多选择五个要用于试用的防火墙，然后 **Save**（保存）。

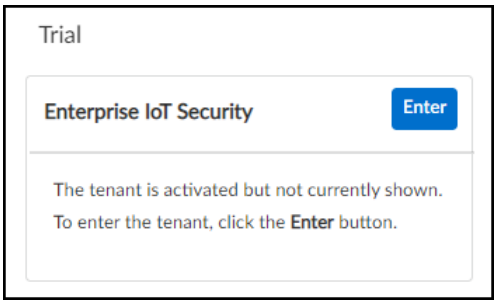


将显示一条消息，说明正在创建 Enterprise IoT Security 的试用租户，所选的防火墙将与之关联，整个过程通常需要大约十分钟。

该过程完成后，会出现另一条消息，指出试用租户已创建，所选防火墙已与之关联。此消息还包括试用租户的名称。

试用租户的创建和防火墙分配也记录在 **Logs & Reports**（日志和报告） > **Audit Log**（审核日志）中。

4. 在 **Administration**（管理） > **About**（关于） > **License**（许可证）上，Enterprise IoT Security 的“试用”部分旁的按钮从 **Request**（请求）变成 **Enter**。要访问试用租户门户，请单击 **Enter**。

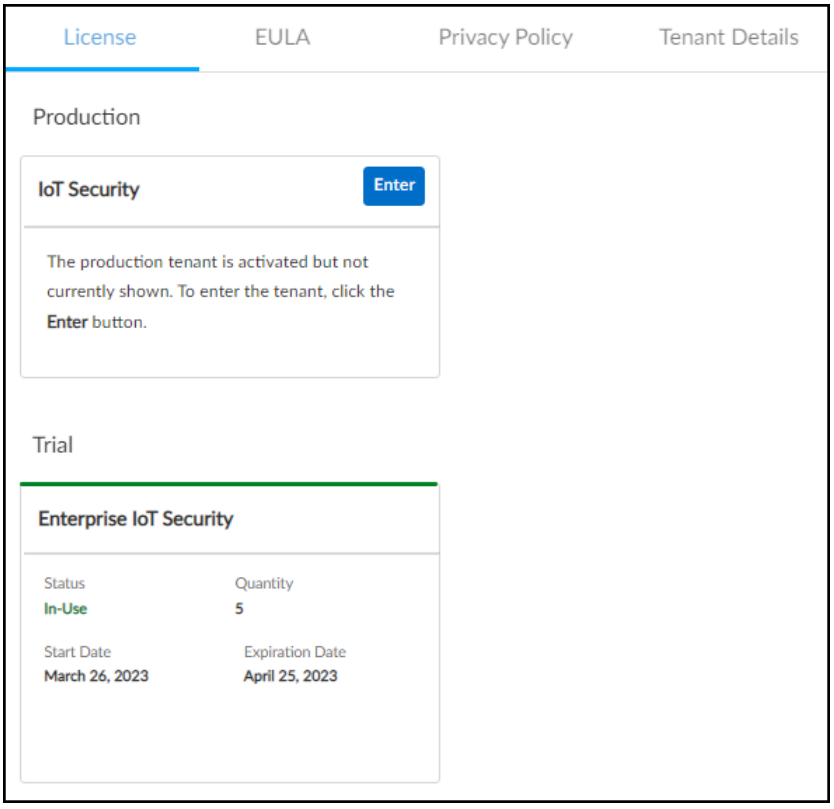


在新的浏览器窗口中会显示试用租户的登录提示。

5. 使用登录生产 IoT Security 租户时使用的相同凭据登录。

Enterprise IoT Security 门户将打开资源中心，可供试用租户使用。在 30 天试用期内，IoT Security 租户和Enterprise IoT Security 试用租户都将使用分配给试用租户的防火墙中的日志。您可以登录两个租户并比较每个租户的功能。

6. 要退出试用租户并返回生产租户，请导航至 **Administration**（管理） > **About**（关于） > **License**（许可证），然后在“生产”部分单击 IoT Security旁边的 **Enter**。



试用版租户浏览器窗口保持打开状态，而生产租户在新浏览器窗口中打开。

试用结束后，试用租户将自动删除，同时生产租户继续使用来自防火墙的日志数据。

如果您拥有 *IoT Security* 的试用许可证，并且想要试用 *Enterprise IoT Security* 产品，请使用具有所有者权限的用户帐户登录 *IoT Security* 门户，选择 ***Administration***（管理）***> About***（关于）***> License***（许可证），然后单击 ***Manage Trial***（管理试用版）。选择 ***Enterprise***（***Enterprise*** 版），然后 ***Confirm***（确认）您的决定。要返回 *IoT Security* 产品，请返回许可证页面，再次单击 ***Manage Trial***（管理试用版），选择 ***Enterprise Plus***，然后单击 ***Confirm***（确认）。

设备到站点映射

从 2022 年 3 月起，IoT Security 为现有租户提供了两种将设备链接到站点的方式：

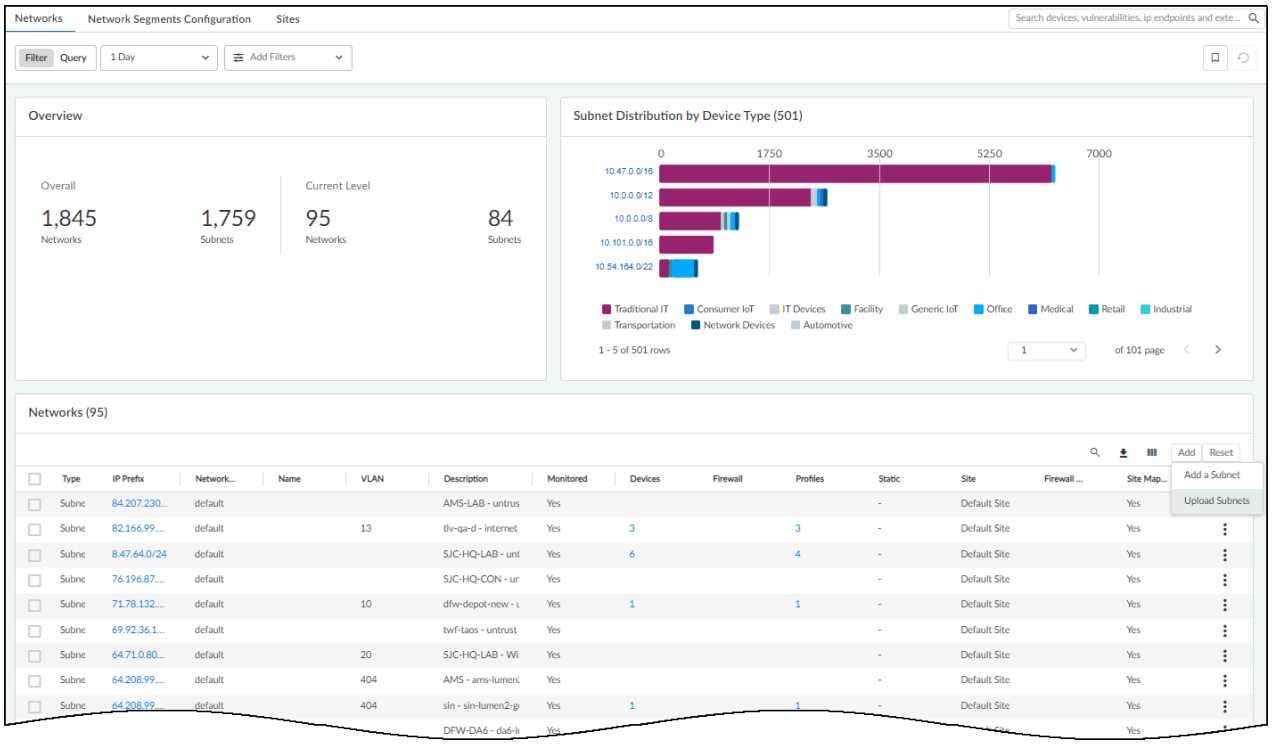
- 基于 IP 地址的站点分配 — IoT Security 根据设备 IP 地址将设备分配给站点。这种方法于 2022 年 3 月推出。现有 IoT Security 租户可切换到这种方法，也是新租户（截至 2022 年 3 月）可以使用的唯一选项。
- 基于防火墙的站点分配 — IoT Security 根据向其发送日志的防火墙的位置将设备分配给站点。在 2022 年 3 月之前，这是 IoT Security 提供的唯一方法。

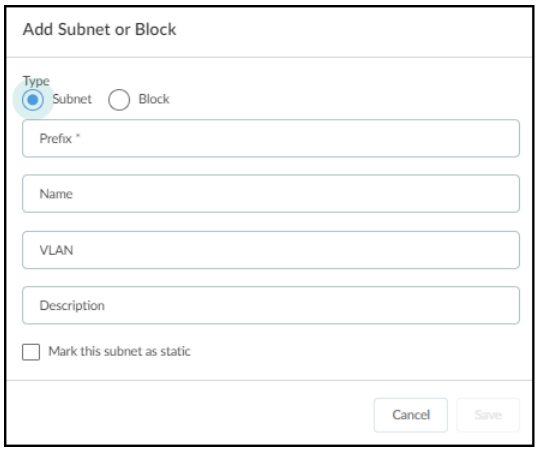
对于第一种方法，您必须为 **Network**（网络） > **Subnets**（子网）中的每个站点定义一个或多个无类域间路由 (CIDR) 块或子网。对于第二种方法，您必须在 **Administration**（管理） > **Sites and Firewalls**（站点和防火墙） > **Firewalls**（防火墙）处为每个防火墙分配一个站点。基于防火墙的站点分配适用于较小的单站点部署。但是，当两个站点有多个站点和设备相互通信时，可能会出现问题。当出现这种情况时，两个站点的防火墙都会观察涉及相同两台设备的会话，并在日志中将其报告给 IoT Security，后者无法判断每台设备的实际位置。IoT Security 根据 IP 地址为站点分配设备时不会出现此问题，这是首选方法。

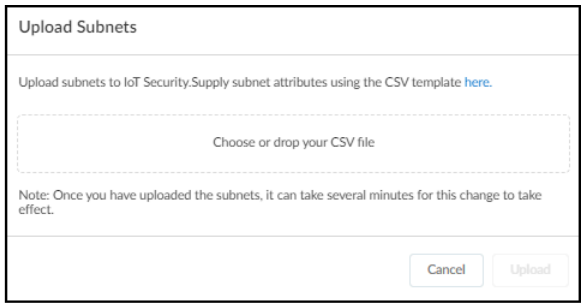
基于 IP 地址的站点分配

这种将设备映射到站点的方法使用 IP 地址，从 2022 年 3 月开始，这是向新的 IoT Security 租户提供的唯一站点映射方法。

如果您没有这样做，请在 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）上的 CIDR 标记中输入或上传您网站的 IP 地址组的 CSV 文件。（CIDR 表示法示例：10.55.0.0/16 和 10.197.0.0/16。）然后单击 **Add**（添加） > **Add a Subnet**（添加子网），然后以 CIDR 符号和说明输入网络地址，或者单击 **Add**（添加） > **Upload Subnets**（上传子网），然后使用提供的模板上传多个子网。

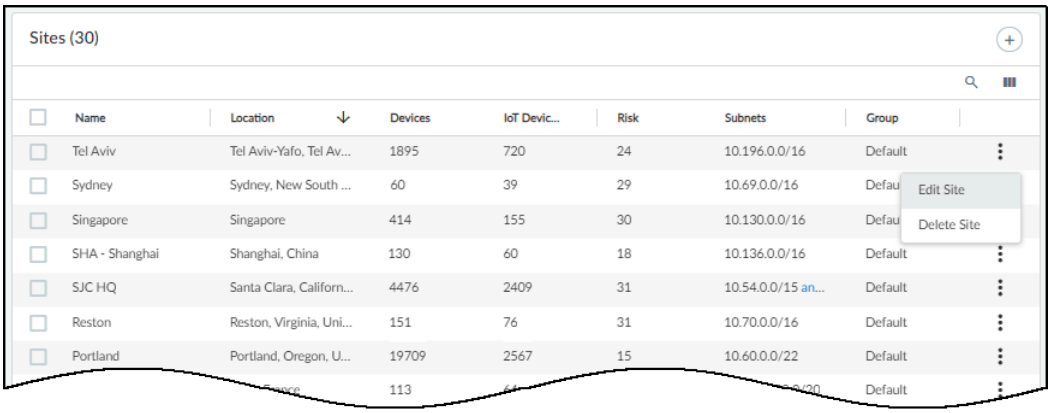






站点映射不需要使用属于某个站点的所有子网。它会选择最大的子网（*IP* 地址组）进行站点分配。例如，一个站点可能有多个子网，如 *10.55.10.0/24*、*10.5.28.0/24* 和 *10.55.121.0/24*，它们都位于 *10.55.0.0/16* 的单个 *IP* 组内。在这种情况下，请使用 *10.55.0.0/16* 进行站点映射。*IoT Security* 会自动将站点映射 *IP* 组中的较小子网分配给同一站点，并将每个子网中的设备分配给与其子网相同的站点。

添加或上传子网后，将其分配给 **Networks**（网络） > **Networks and Sites and Firewalls**（网络、站点和防火墙） > **Sites**（站点）上的站点。单击"站点"表右上角的 **Create Site**（创建站点） **(+)** 图标，或单击之前创建的站点所在行最右侧的三个垂直点图标，然后单击 **Edit Site**（编辑站点）。

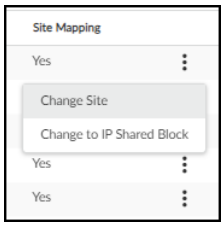


选择您在 **Networks**（网络） > **Networks and Sites and Firewalls**（网络、站点和防火墙） > **Networks**（网络）上添加或上传的子网。

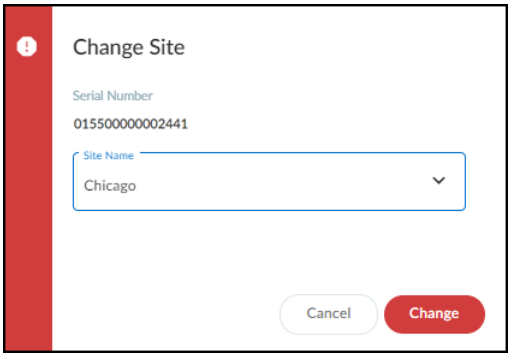
如果您没有添加子网，IoT Security 无法将子网中的设备链接到站点。发生这种情况时，它会将此子网中的设备分配给默认站点，所有私有 IP 范围（10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16）都分配给默认站点，以便捕获任何未分配的子网。

基于防火墙的站点分配

对于在 2022 年 3 月之前加入的 IoT Security 租户，IoT Security 使用基于防火墙的站点分配。防火墙加入后，它会显示在分配给默认站点的 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）页面上。要将其重新分配到另一个站点，请单击其最右侧行中的三个垂直点图标，然后单击 **Change Site**（更改站点）。



在站点名称列表中选择一个站点，然后单击 **Change**（更改）。



IoT Security 将流量元数据出现在日志中的设备从此防火墙映射到此站点。

有关创建站点的信息，请参阅站点和站点组。

如果不为站点分配防火墙，IoT Security 将无法将流量出现在日志中的设备从此防火墙链接到站点。出现这种情况时，它会将这些设备分配给默认站点。

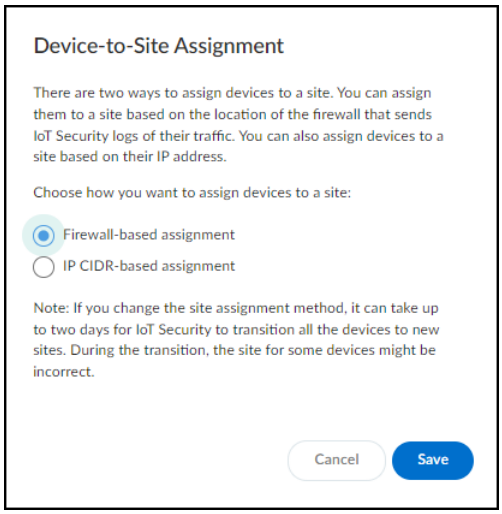
将站点分配从防火墙更改为 IP 地址

只有拥有所有者权限的用户才能从基于防火墙的站点分配更改为基于 *IP* 地址的站点分配。

对于将设备映射到基于防火墙的站点的 IoT Security 租户，IoT Security 提供了切换到基于 IP 地址的方法的选项。这是一次性更改。切换到基于 IP 地址的站点分配后，您不能切换回基于防火墙的方法。

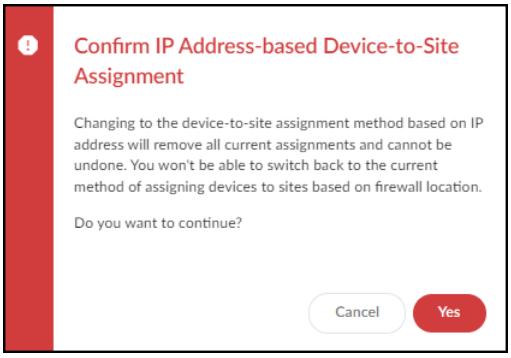
选择 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点），然后单击站点面板右上角的齿轮图标 ( )。

从 **Firewall-based assignment**（基于防火墙的分配）切换到 **IP CIDR-based assignment**（基于 **IP CIDR** 的分配），然后 **Save**（保存）。



如对话框中的说明所述，IoT Security 可能需要两天时间才能将所有设备过渡到新站点，在此期间，某些设备的站点分配可能不正确。

阅读出现的确认消息，该消息旨在提醒您稍后不能撤消此开关，准备好后，请单击 **Yes**（是）以继续。



在为站点映射设置完 IP CIDR 块后，新的基于 IP 地址的站点分配方法还有几天时间建立设备到站点的分配，您可以检查 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）以验证配置，并在必要时进行任何调整。

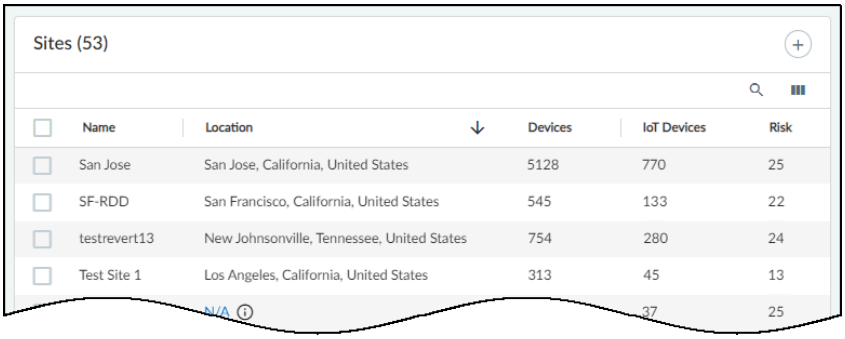
特别感兴趣的是站点映射列。当子网链接到站点时，其站点映射列中的条目为 **Yes**（是），表示子网已手动映射到站点。当子网链接到站点，但其在站点映射列中的条目为 **No**（否）时，表示该子网是映射到站点的较大 IP 地址块的一部分，并且此子网继承了其站点映射。

将设备到站点的映射从防火墙切换到 *IP* 地址后，*IoT Security* 将删除 ***All connected sites***（所有连接站点）和 ***All disconnected sites***（所有断开站点）的过滤器。这些过滤器基于站点的防火墙活动状态，切换后，*IoT Security* 不再将防火墙链接到站点。

站点和站点组

只有具有所有者权限的用户才能创建和管理站点，将站点组织成组，并将对站点和站点组的访问权限分配给其他用户。

以具有所有者权限的用户身份登录，然后选择 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点）。您可以在此处添加、查看、编辑和删除设备受 IoT Security 保护的站点。

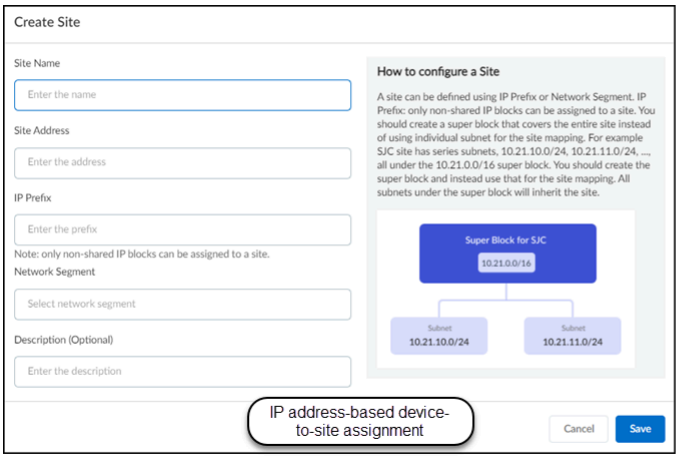


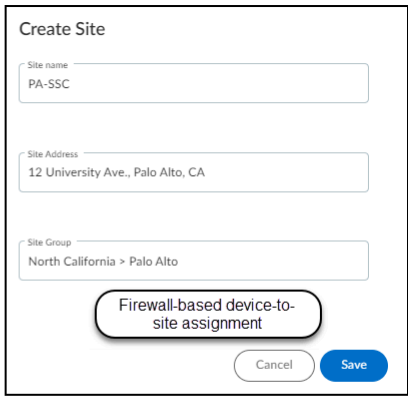
“站点”页面上有三个部分：

- 顶部是标题栏，上面有“网络”、“网络分段配置”和“站点”选项卡的标题。还有一个全局过滤器，可以按网站和时间范围控制页面上显示的内容。
- 组织部分显示组织中站点的分层结构。
- 站点部分是一张表格，其中包含有关各个站点的有用信息。

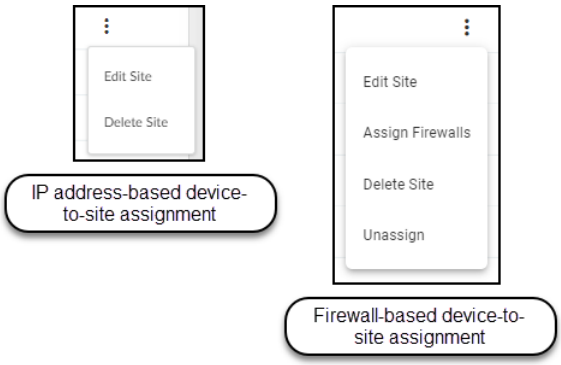
默认站点是 IoT Security 最初分配防火墙的地方。稍后您可以将它们重新分配给用户定义的站点。

要添加新站点，请单击表格上方的 **+**。根据正在使用的设备到站点分配方法，有不同的设置。在按 IP 地址将设备分配给站点时，输入站点名称，可以选择输入站点地址和描述，选择非共享 IP 块或先前定义的网段的 IP 前缀，然后 **Save**（保存）。通过防火墙将设备分配给站点时，输入站点名称，（可选）输入该站点的地址，然后（如果您要将站点分组）选择一个站点组，然后选择 **Save**（保存）。





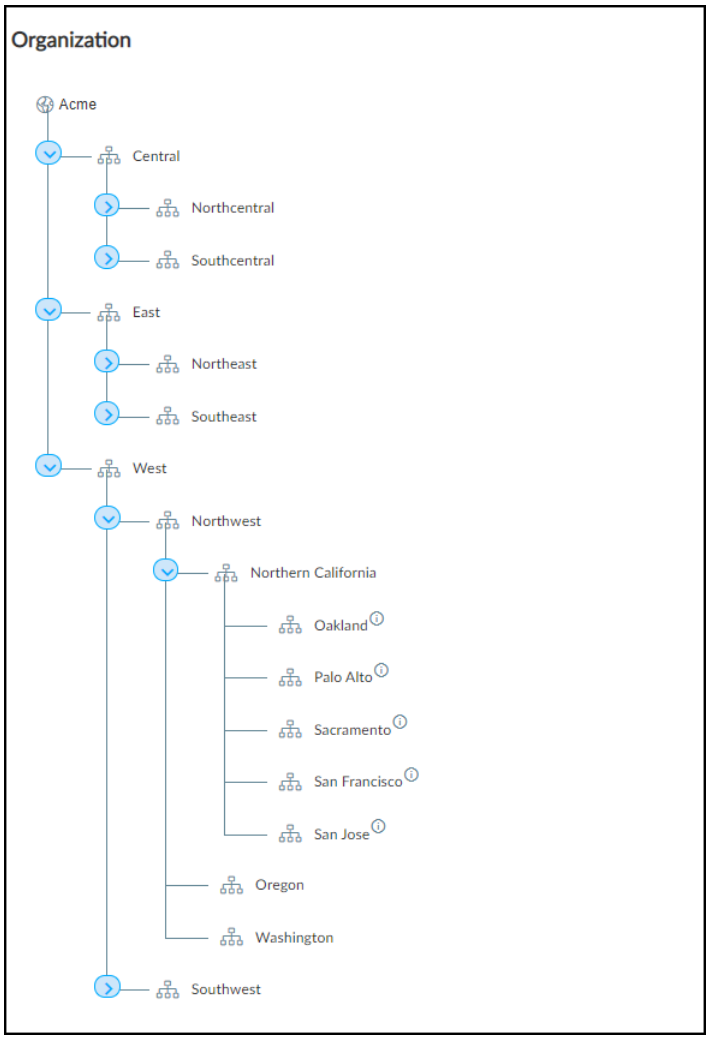
要编辑或删除网站，请单击站点行最右边的三个垂直点，然后单击出现的其中一个操作。在根据防火墙将设备分配给站点时，还有两个附加选项。您可以为站点分配一个或多个防火墙，也可以从群组中取消分配站点。



在删除站点之前，必须先移除其中的所有防火墙或将其重新分配给不同的站点。

将网站分组

您可以选择在分层结构中将站点组织成组，然后在结构内的不同级别设置控件，以定义管理用户的查看和操作。例如，在下图所示的树结构中，您可以授予用户访问单个站点级别、城市、州或更广泛区域内所有站点的数据的访问权限。



您不必将网站分组。实际上，默认情况下，**Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点）页面上的“组织”面板处于隐藏状态。如果需要，可以在不使用站点组的情况下为每个站点分配用户访问权限。但是，如果您想查看“组织”面板并使用此功能，请单击 **Show Organization**（显示组织），然后单击 **Organize Sites**（组织站点）。

向树中添加群组并将站点添加到群组

只有拥有所有者权限的用户才能添加、编辑和删除群组以及向群组添加站点。

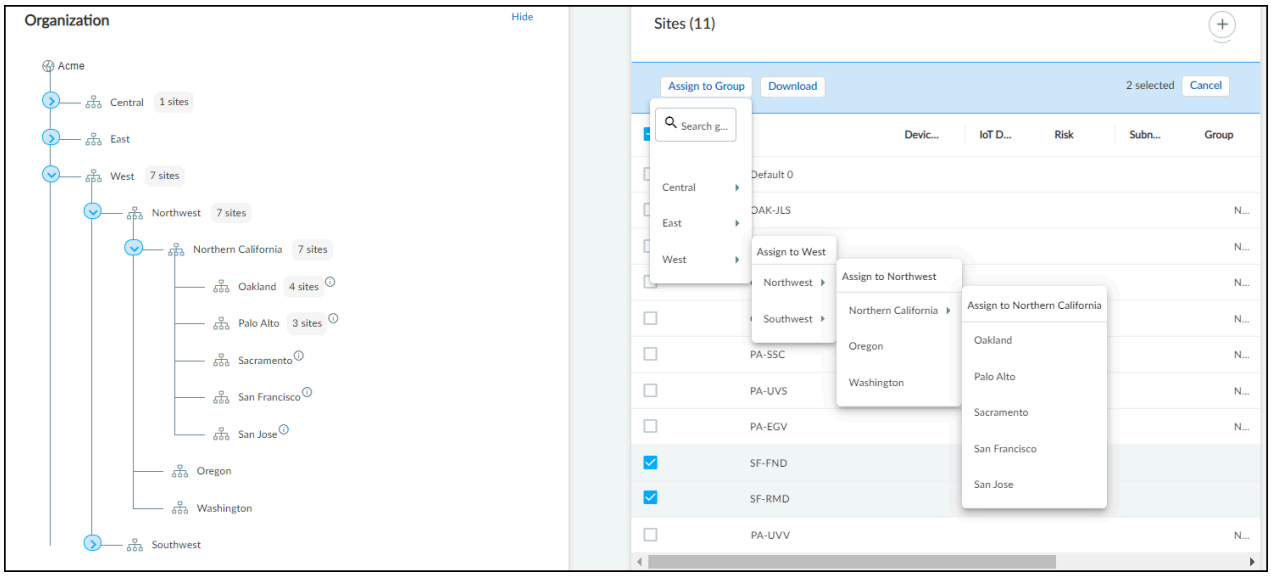
一个组层次结构中可以有五个级别。根节点构成顶级组（此处的示例中为“Acme”），默认情况下是所有站点所属的组。默认情况下，它是租户帐户的名称，无法删除，但可以重命名。根目录下的所有其他群组完全由所有者定义。

要向组织添加群组，请将光标悬停在现有群组上，单击 **Add group**（添加群组）图标，然后输入新名称。要更改其名称，请单击“添加群组”图标旁边的三个点 **(...)**，然后单击 **Rename**（重命名）。

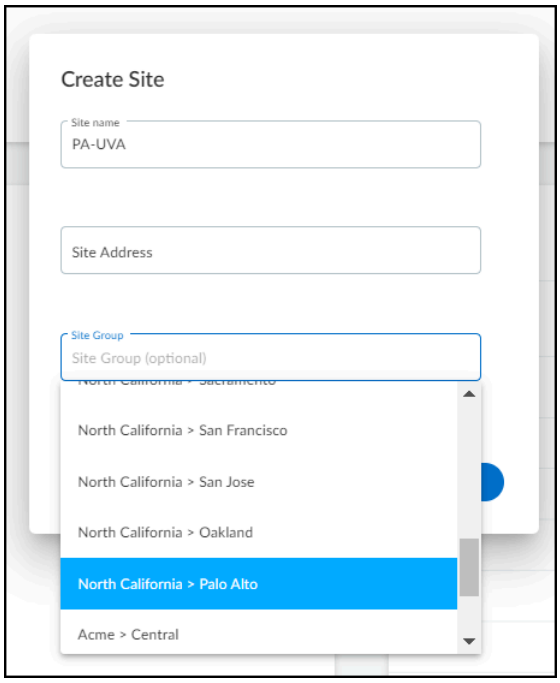
全局过滤器优先于页面级过滤器。创建树结构时，请确保将页面顶部的全局过滤器设置为 ***All Sites***（所有站点）。如果将其设置为其他任何内容，则组织面板将继续折叠以仅显示在全局过滤器中选择的一个或多个站点。

根据需要添加群组和子组，以反映您的组织结构。添加所需群组后，向其添加站点。在“站点”面板中选中一个或多个站点的复选框，单击 **Assign to Group**（分配到群组），然后选择要将它们放入的群组。

您可以通过在“分配给群组”下拉菜单顶部的搜索组字段中键入群组名称来搜索群组。



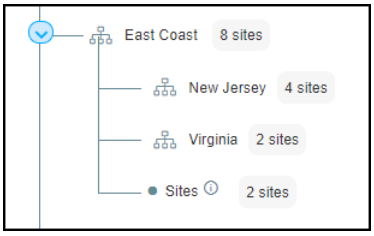
除了将现有站点添加到群组外，您还可以向群组中添加新站点。创建新站点 [**Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点） > **+**]时，“站点组”选项允许您将站点分配给现有组，从而将站点创建和群组分配合并为一个方便的单步过程。



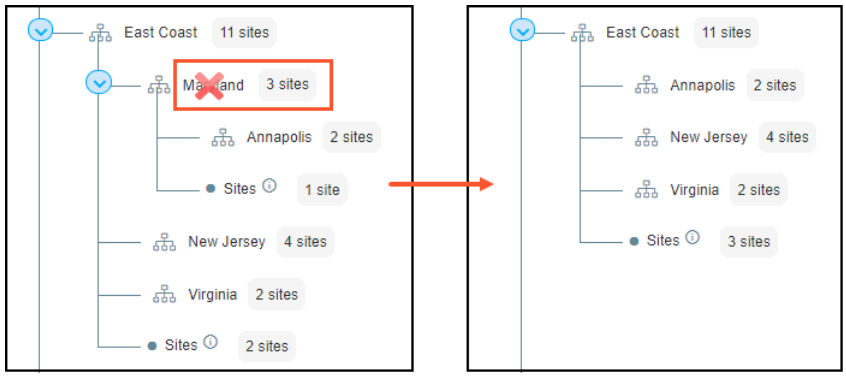
重新分配站点和删除群组

如果以后要将站点从一个组重新分配给另一个组，请使用相同的过程将其添加到组中，但要从列表中选择另一个组。

当您将站点分配给一个也有子组的组时，一个标记为“站点”的节点会出现在树中其分配的组下方，该节点与子组处于同一级别。例如，请注意名为 East Coast 的群组有两个子组（新泽西州和弗吉尼亚州），而且它还有一个名为 Sites 的节点，用于分配给东海岸组的两个站点。



如果您删除某个群组，IoT Security 会将其所有站点和子组重新分配给其父组。例如，看看删除马里兰州群组后会发生什么。属于马里兰州的遗址现在属于东海岸，其子团体安纳波利斯变成了东海岸的儿童团体。

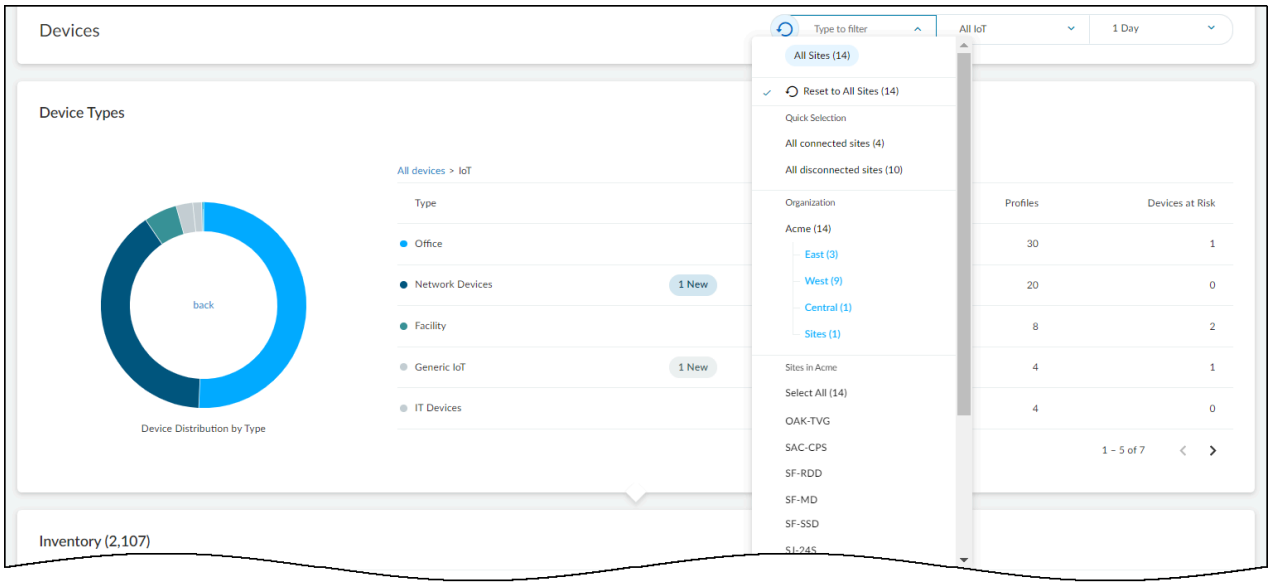


为避免 IoT Security 在删除站点群组时自动重新分配该站点，或者只是将其从群组中移除，请在“站点”面板中单击该行最右边的三个垂直点，然后单击 **Edit Site**（编辑站点）以将其重新分配给另一个群组，或单击 **Unassign**（取消分配）以将其从当前群组中移除并放入根节点。

使用群组过滤和控制对数据的访问权限

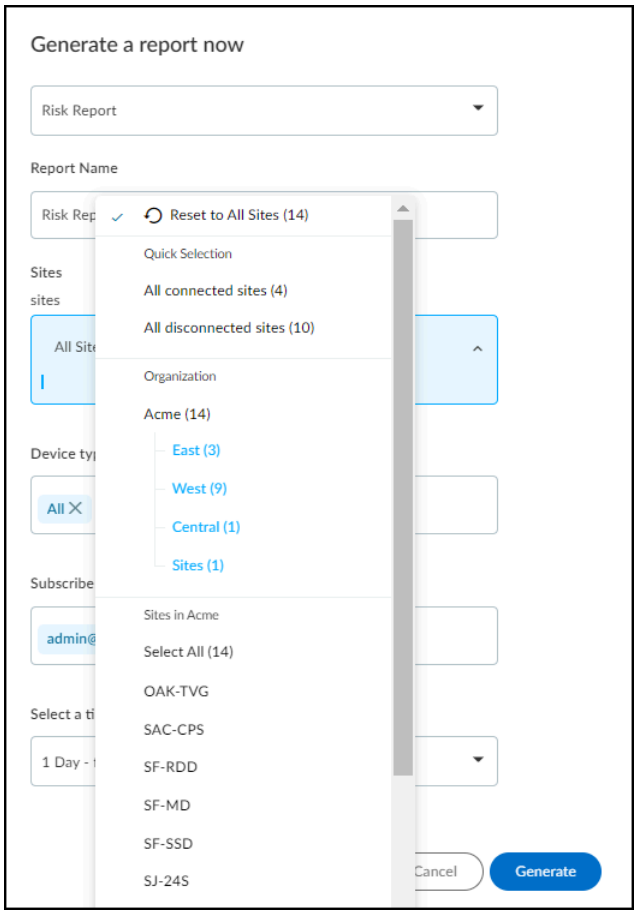
创建完组织结构并将站点分配给群组后，您可以使用树来过滤要在“站点”页面上显示的内容。单击树中的任意群组名称，即可在右侧的“站点”面板中显示属于该群组的站点。显示的站点要么直接属于该组，要么属于其子组之一。（要删除过滤器，请单击“站点”表格顶部其名称右侧的 **X**。）

您不仅可以使用群组来过滤 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点）页面上显示的站点，还可以在 **Devices**（设备）页面上按群组进行过滤。

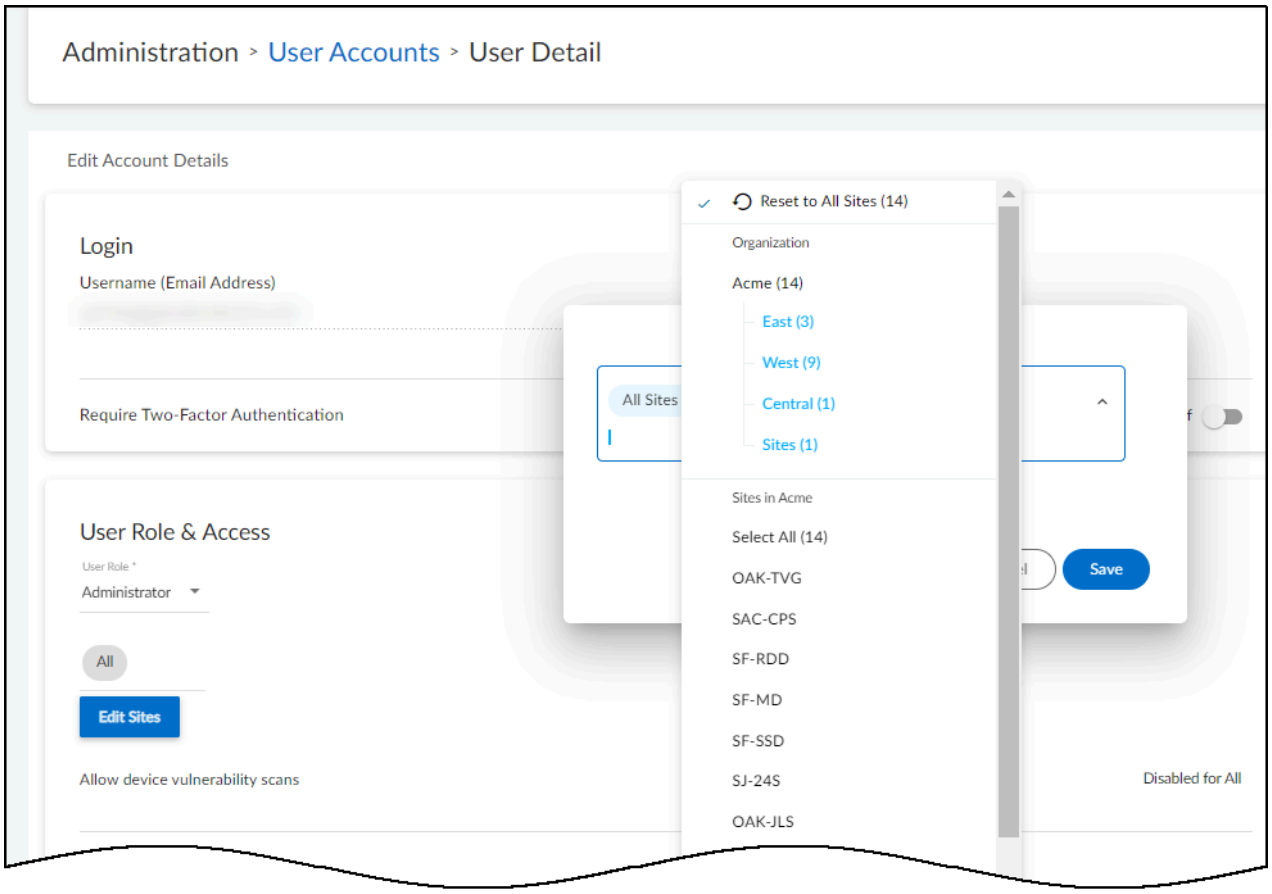


在站点全局过滤器的下拉列表中，单击群组名称（蓝色），然后单击 **Select All**（全选）以查看所选组中所有站点的设备，或单击特定站点仅查看该站点上的设备。

在 **Reports**（报告） > **Files and Settings**（文件和设置） > **+** 中定义报告的范围，并单击 **Generate a report now**（立即生成报告）或 **Schedule a report for later**（安排稍后生成报告）。



以具有所有者权限的用户身份登录时，您可以使用群组来控制允许其他用户访问的站点。通过单击 **Administration**（管理） **> User Accounts**（用户帐户） **>** *username*（用户名），在用户的用户帐户设置的“用户角色和访问权限”部分中执行此操作。



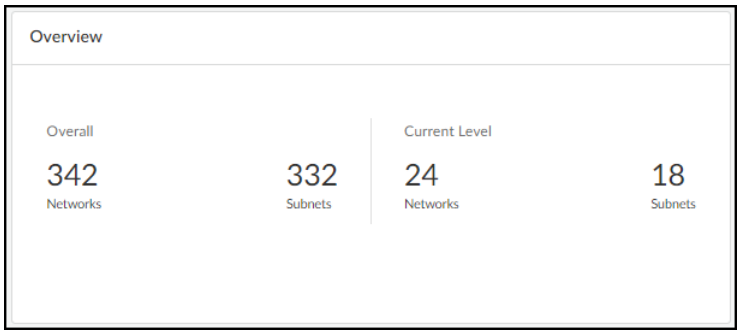
默认情况下，所有用户都可以访问所有群组和站点。但是，在具有所有者权限的用户向其他用户授予访问一个站点或群组的权限之后，他们只能访问这些站点或群组。如果该站点或群组被删除，这些用户将无法恢复对所有内容的默认访问权限。相反，他们将无法访问任何东西；也就是说，直到他们获得访问其他内容的权限。另一方面，具有所有者权限的用户始终可以访问其帐户中的所有群组和网站。

网络

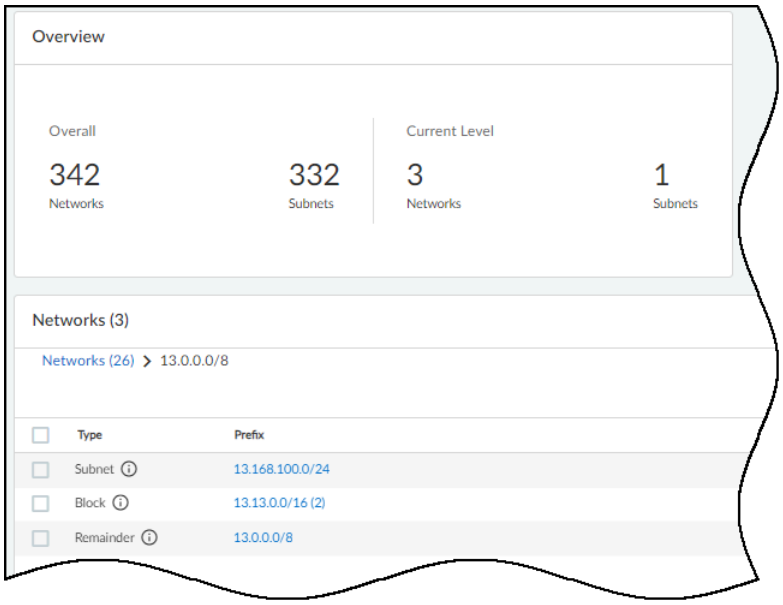
IoT Security 通过多种方式了解网络上的寻址方案。您可以手动添加子网和无类域间路由 (CIDR) 块，甚至指定子网是否包含具有静态 IP 地址的设备。IoT Security 可以通过观察 DHCP 客户端和服务器之间的交换来发现子网。通过使用 SNMP 进行网络发现，IoT Security 可以通过与网络交换机的第三方集成来了解子网。它还可以通过与 BlueCat 和 Infoblox 的 IP 地址管理 (IPAM) 集成来了解子网和 CIDR 块。

当 IoT Security 收集网络信息时，它按层次结构组织这些信息，并在 **Networks**（网络）页面 [**Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）] 上显示子网和块。块是 IP 地址空间的逻辑分区，可作为管理地址的组织工具。较大的“父”块可以包含较小的“子”块和子网，设备就位于其中。另一个概念分组是“剩余”。这些是块内的 IP 地址集，不属于子网或子块。

网络页面顶部有两个面板，提供网络的高级视图以及不同类型的设备在网络中的分布情况。概览面板分为两部分。左边是“网络”的总数，它实际上是网络中的所有网络元素（块、子网和剩余部分）的集合，以及网络中子网的总数。概览面板的右侧是特定级别的网络元素的总数。如果您没有选择网络表中某个块的前缀列中的条目，则当前级别将显示根级别的块和子网的总数。例如，下面的概览面板显示有 342 个网络（各种块、子网和剩余部分），其中 332 个是子网。在当前（根）级别，有 24 个网络（块和子网），由 18 个子网和 6 个块 (24-18) 组成。



如果通过单击网络表中前缀列中的条目来选择其中一个块，则总数保持不变，但当前级别的总数会发生变化，以显示所选块内的子网、子块和剩余部分。



要查看子块中的元素，请选择前缀列中的条目。要返回根级别，请单击网络表上方痕迹导航中的 **Networks (number) [**网络（数字）**]**。

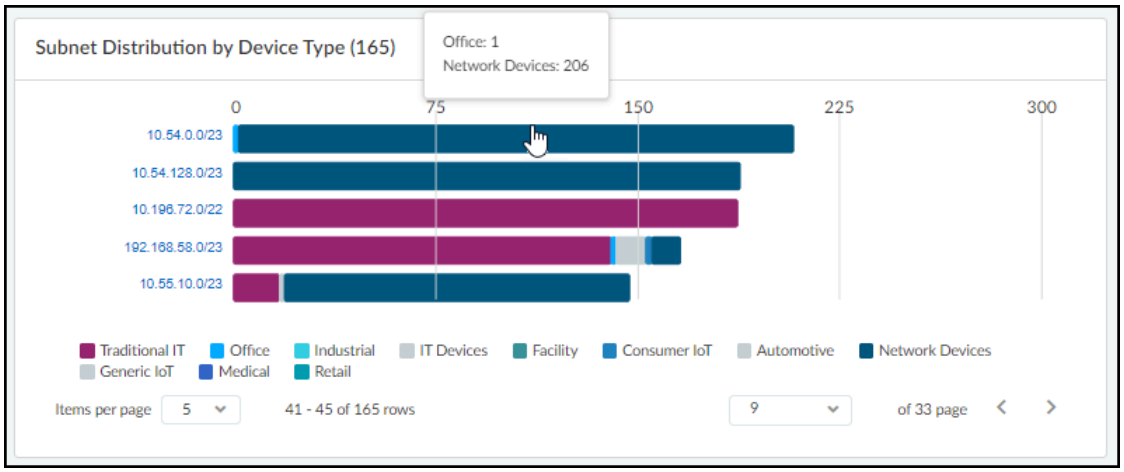
网络页面顶部的另一个面板包含一个条形图，显示每个子网中设备类型的分布。

“按设备类型划分的子网分布”后面括号内的数字是页面上方过滤器所设置的时间段内活跃设备的子网总数。无论 IoT Security 是否检测其中的设备活动，左侧面板中的子网总数都是所有子网的数量。IoT Security 可以通过各种方式了解子网而无需检测设备活动：

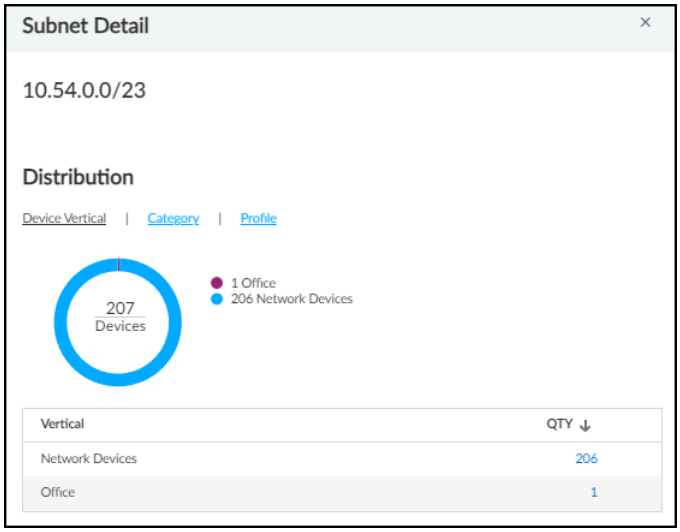
- IoT Security 门户中用户配置的子网
- .csv 文件中用户发起的子网配置上传
- 使用 SNMP 进行网络发现的第三方集成
- 与 BlueCat 或 Infoblox 的 IP 地址管理 (IPAM) 解决方案的第三方集成
- 检测 IP 端点但不检测子网中的设备
- 检测在网络页面上设置的较短时间段内处于非活动状态的子网中过去的设备活动

如果 IoT Security 检测其所知的每个子网中的设备活动，则两个面板中的子网总数可能相同，但大多数情况下总数很可能不同。

将光标悬停在其中一个栏上，即可看到一个信息弹出窗口，其中列出了该子网中的设备类型。例如，下面显示的 10.54.0.0/23 子网在仅由网络设备组成的子网中有一个办公设备。这立即表明办公设备可能在网络上放错了地方。

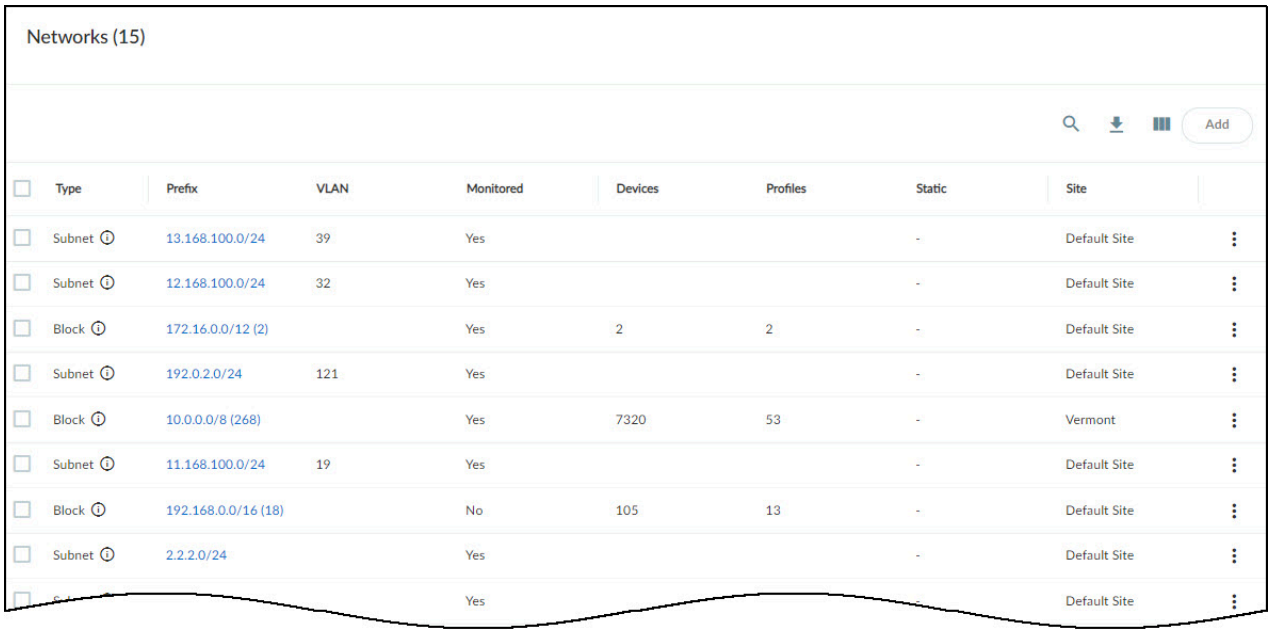


单击条形图左侧的子网以查看子网详细信息面板。默认情况下，显示设备类型。要查看设备类别和设备配置文件，请单击 **Category**（类别）和 **Profile**（配置文件）选项卡。

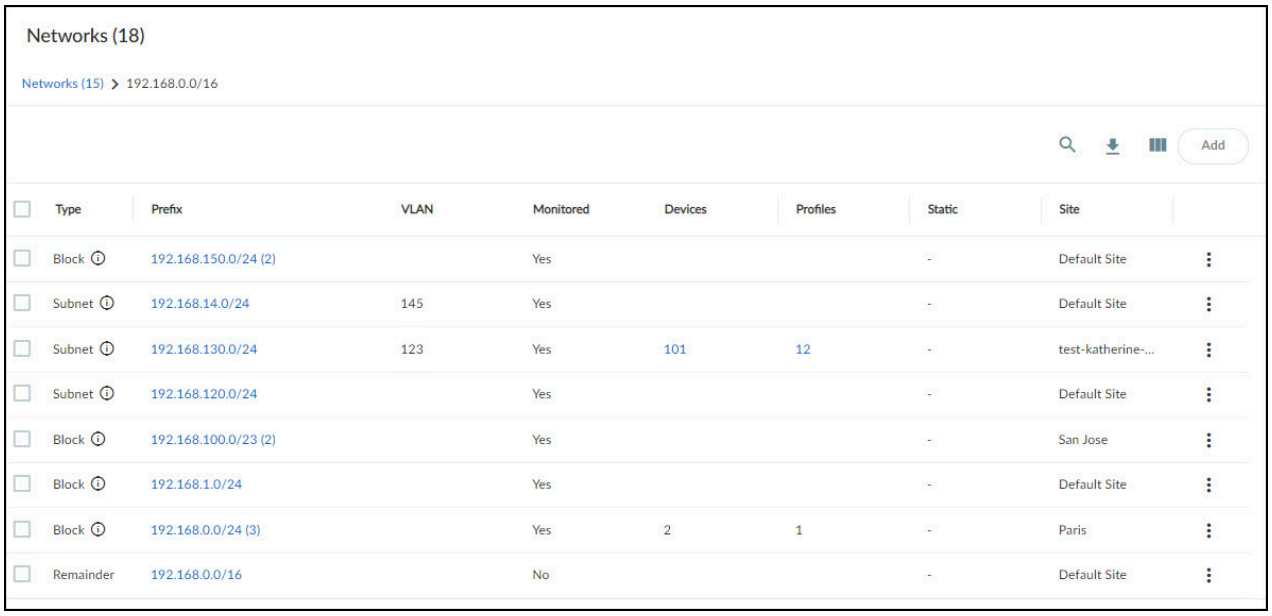


要查看子网中某一类设备的详细信息（例如一台办公设备），请单击 **QTY**（数量）列中的数字。IoT Security 将打开 **Assets**（资产） > **Devices**（设备） 页面，并进行过滤以显示所选的设备。然后单击特定设备的名称以查看其 **Device Details**（设备详细信息）页面。

在网络表中，IoT Security 在网络页面上显示已配置、发现和通过第三方集成学习到的所有块和子网。当“父”块下方嵌套其他块和子网时，其“子”块的数量会以括号显示。要查看这些块，请单击包含该块的前缀。

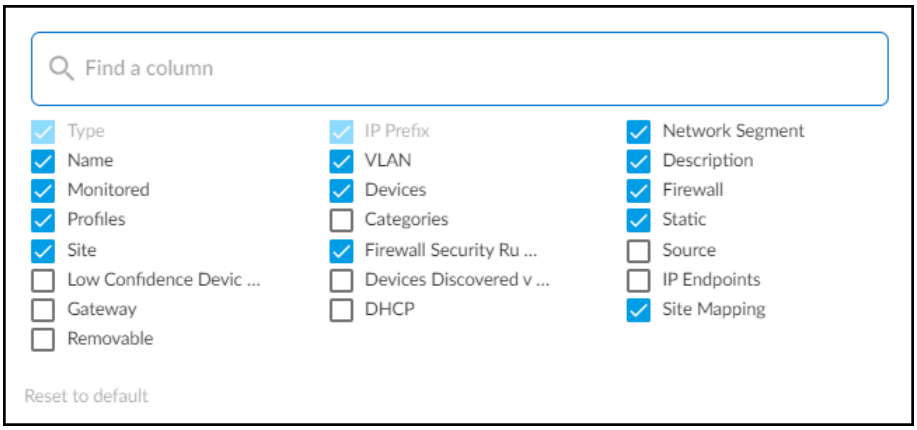


例如，如果您单击上面屏幕截图中的 **192.168.0.0/16** 块，IoT Security 会显示其中的块和子网的列表。



请注意它包含 18 个块和子网，并且一些块后面有括号内的数字，表示它们下面还有其他较小的块和子网。您可以通过单击后面带有括号数字的任何块的前缀继续向下移动到层次结构中的较低级别。要向上移动，请单击页面顶部的痕迹路径中的更高级别。

网络页面主要由一个表格组成，该表格显示了您的网络的层次视图以及构成网络的块和子网的属性。



Type（类型）：网络分组类别有以下几种类型：

- **Subnet**（子网）— 具有广播域和网关的网络部分。
- **IP Block**（IP 块）— IP 地址空间的一个分区，在逻辑上可以包含其他块和子网。

  Shared IP Block（共享 IP 块）— 其空间被划分为至少一个子网的 IP 块，可在不同的共享网络段中重复使用。这会导致同一网络上的设备 IP 地址重叠。例如，您可能在整个网络的多个网段中使用同一个子网来处理来宾流量。在这种情况下，您首先需要列出防火墙及其在网络上的位置，可能是在同一站点，也可能在不同的站点。接下来，您将计划如何将防火墙分组到不同的网络段，并将每个防火墙和站点分配到特定的段。最后，您将包含来宾子网的 IP 块定义为共享 IP 块。IoT Security 现在可以根据共享的 IP 块和发送包含该地址的日志的防火墙自动检测 IP 地址来自哪个网段。

  Non-shared IP Block（非共享 IP 块）— 其空间被划分为网络中唯一的较小块和子网的 IP 块。非共享 IP 块中的 IP 地址仅在您的网络的一个网段中使用。
- **Remainder**（剩余部分）— 不包含在更大的超集块内的更具体的 IP 块或子网中的所有 IP 地址。
- **Network Segment**（网络段）— 一个或多个防火墙加上一个 IP 块的逻辑分组。当防火墙发送流量日志时，IoT Security 通过设备 IP 地址所在的 IP 块 + 发送日志的防火墙来识别设备属于哪个网段。这样，即使每个设备使用与不同网段中的另一台设备相同的 IP 地址，日志也能唯一地标识每个设备。

Name（名称）、**VLAN** 和 **Description**（描述）：在 IoT Security 门户中手动添加块和子网时，您可以包含名称和说明，以及子网的 VLAN。IoT Security 还可以通过第三方集成了解这些属性。BlueCat IPAM 集成可以为块或子网提供名称。SNMP 和 Infoblox IPAM 集成可以为子网提供 VLAN。Infoblox IPAM 集成可以提供描述。

您稍后可以修改 *VLAN* 和描述，但不能修改名称。

Monitored（监控）：**Yes**（是）或 **No**（否）分别表示网络内有 IoT Security 正在监控/没有监控的网络活动。

Categories（类别）和 **Profiles**（配置文件）：子网中的设备类别（例如个人计算机或 IP 电话）的数量和设备配置文件（例如 PC-Windows 和 Poly IP 电话）。

源：有几种方法可以将块或子网添加到 IoT Security。此列显示每个块或子网的来源。以下是可能的来源：

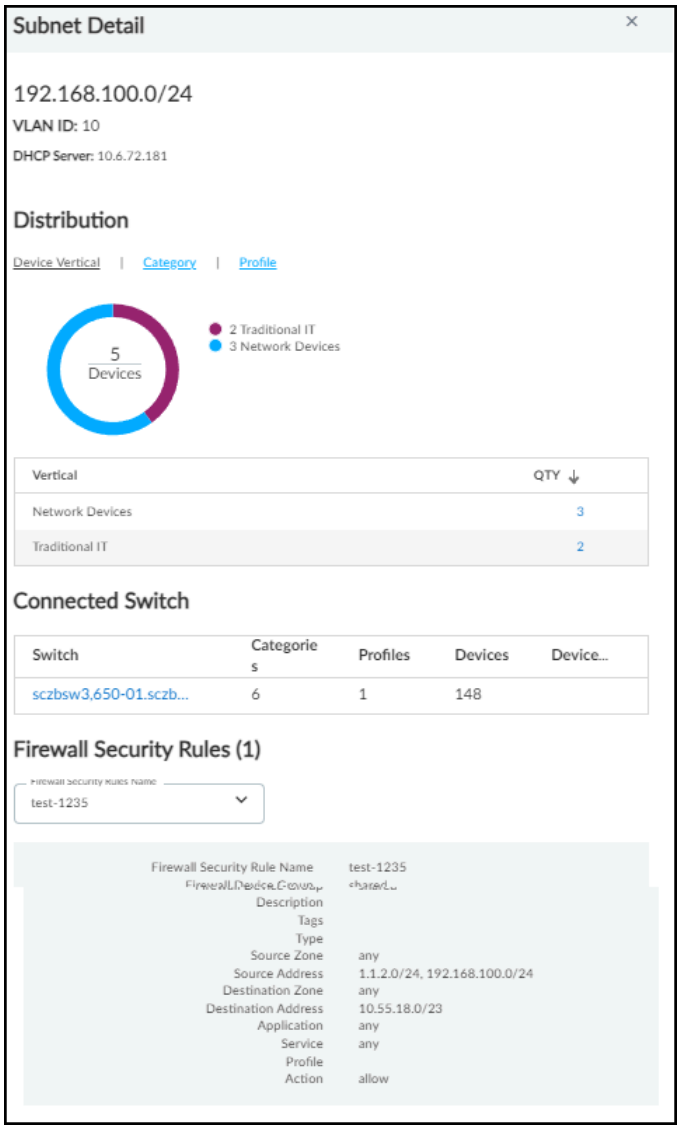
- **Discovered**（已发现） — IoT Security 通过观察网络流量发现的子网。
- **Config**（配置） — 用户手动配置了 IP 块或子网。
- **Preconfig**（预配置） — IP 块由 IoT Security 预配置且无法删除。例如 10.0.0.0/8 A 类私有块。
- **BlueCat IPAM** — IoT Security 通过与 BlueCat IPAM 集成了解了 IP 块或子网。
- **Infoblox IPAM** — IoT Security 通过与 Infoblox IPAM 集成了解了 IP 块或子网。
- **Network Discovery SNMP**（网络发现 **SNMP**） — IoT Security 通过使用 SNMP 从交换机发现网络信息，了解了 IP 块或子网。

IP Endpoints（**IP** 端点）：IP 端点 是 IoT Security 了解其 IP 地址，但不知道它们的 MAC 地址的设备。此外，它们的行为还不够稳定，IoT Security 自信地推断它们的地址是静态定义的。IoT Security 显示子网中的 IP 端点数量。单击该数字即可下载包含逗号分隔值格式的 IP 端点报告的 .zip 文件。

DHCP 和 **Gateway**（网关）：当 IoT Security 与使用 SNMP 进行网络发现的交换机集成，并了解子网的 DHCP 服务器和网关的 IP 地址时，它会将其显示在这些列中。BlueCat IPAM 集成还为子网提供网关。

Prefix（前缀）：CIDR 块或子网的 IP 地址的网络部分。如果您单击某个块的前缀列中的条目，IoT Security 会显示其中的块、子网和剩余部分。

如果单击子网条目，IoT Security 会打开页面右侧的子网详细信息面板。该面板包括有关子网的各种详细信息，例如 VLAN ID；DHCP 服务器 IP 地址；每个设备类型、类别和配置文件的设备数量；子网连接的交换机的名称和详细信息；以及防火墙安全规则详细信息（如果通过 Cortex XSOAR 与 Panorama 的集成了解到此子网的规则）。



并非每个子网详细信息面板都包含连接的交换机和防火墙安全规则部分。例如，*IoT Security* 仅从与 *Cisco Prime*、*DNA Center* 或 *Meraki* 的第三方集成，或从使用 *SNMP* 进行网络发现的集成中了解连接的交换机。

Devices（设备）：IoT Security 已在子网中发现并通过第三方集成了解的设备数量。

Static（静态）：如果子网定义为具有静态 IP 地址，则此列中会显示 **Yes**（是）。否则，此处会出现一个短横线 **(-)**，表示 IoT Security 没有足够的数据来确定子网是否具有静态 IP 地址。

防火墙安全规则：（需要 IoT Security 第三方集成附加组件许可证或通过功能齐全的 Cortex XSOAR 服务器进行集成）配置 IoT Security 后，通过 Cortex XSOAR 与 Panorama 通信时，它可以获取引用子网作为源或目标的任何防火墙安全规则。应用于子网的规则数量显示在防火墙安全规则列中。当您单击前缀列中的子网条目时，您可以在出现的子网详细信息面板中看到规则本身。

当防火墙安全规则列中出现 ***0*** 时，表示引用该子网的先前规则已被删除，现在没有其他规则适用于它。

Low-confidence Devices（低置信度设备）：这是 IoT Security 无法自信识别其标识的设备数量。单击子网的编号可打开“设备”页面，其中应用了过滤器，仅显示该子网中置信度较低的设备；即计算出的置信度分数为 0-69% 的设备。

置信度分数表示 *IoT Security* 在其设备标识中的置信度水平。根据计算出的置信度分数，*IoT Security* 有三个置信度级别：高 *(90-100%)*、中 *(70-89%)* 和低 *(0-69%)*。

Site Mapping（站点映射）：嵌套在其他块中的子网和块将继承其集合中最顶层块的站点。例如，如果名为“NYC”的站点处有一个 10.1.0.0/16 块，并且它包含一个 10.1.1.0/24 子网或块，那么该子网或块也会继承“NYC”作为其站点。**Yes**（是）或 **No**（否）表示子网或块是否以这种方式继承其站点。

Site（站点）：可以手动定义块或子网所属的站点（参阅 设备到站点映射，或通过与 Infoblox IPAM 集成来了解。

Devices Discovered via Integration（通过集成发现的设备）：通过与第三方系统集成了解的设备数量。

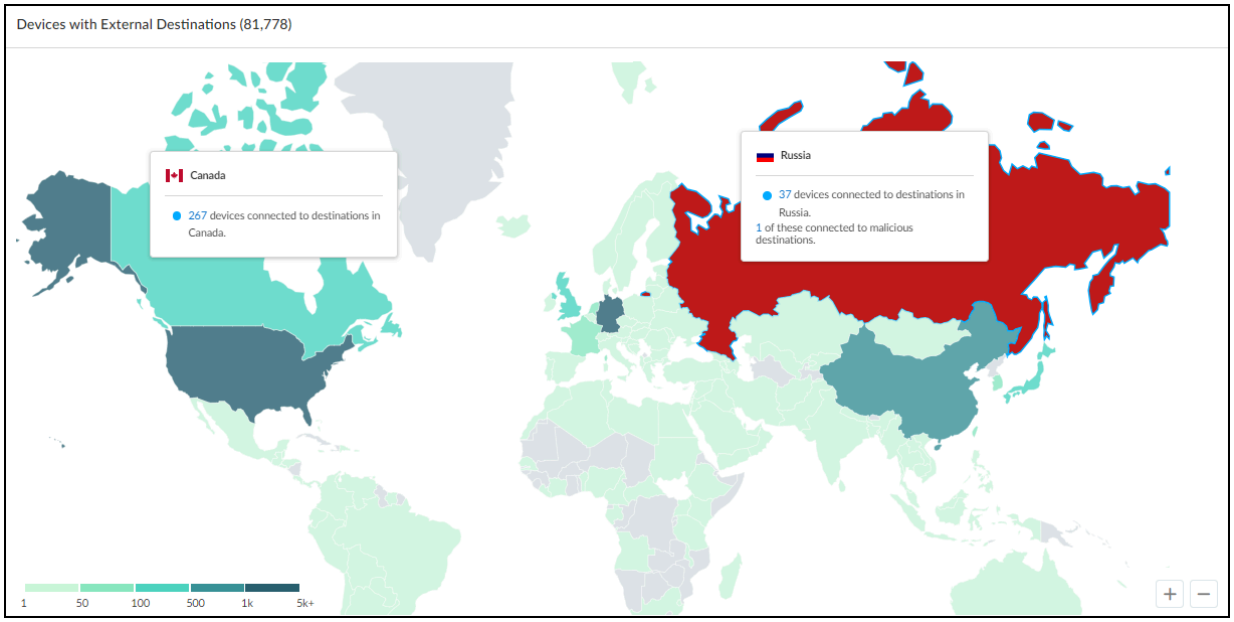
Removable（可移除）：指示是否可以删除子网或块。预配置的块（例如 10.0.0.0/8）以及当前用于站点映射的块无法被删除。

单击前缀列中的子网条目将打开子网详细信息面板，您可以在其中查看有关它的更多信息。

网络表下方是一张地图，显示了与外部目标（即本地网络之外的目标）建立连接的设备数量。设备所连接的国家/地区的颜色表示有多少设备与其建立了连接，以及是否有任何目标是恶意的。

- 灰色表示没有与该国家/地区连接的设备。
- 绿色表示设备连接到某个国家/地区的安全目标。绿色越深，连接到该目标的设备越多。（请参阅图例中的数字。）将光标悬停在某个国家/地区上，即可在页面顶部看到一个信息弹出窗口，其中显示在时间段过滤器内连接到该国家/地区目标的设备数量。如果您单击某个国家，信息弹出窗口将一直保留在视图中，直到您再次单击该国家将其关闭。这样，您就可以单击两个或多个国家/地区，并轻松比较每个国家/地区的连接数。单击弹出窗口中的数字以打开 **Assets**（资产） > **Devices**（设备）页面，其中设置过滤器以显示连接到该国家/地区的设备。

- 红色表示至少有一个设备连接到那里的恶意目标。



单击并拖动光标来移动地图。使用鼠标滚轮或地图右下角的 **+/-** 工具可放大或缩小。

网络可视化

IoT Security 监控并分析网络流量，以提供数据丰富、动态更新的网络设备清单。通过对网络活动的广泛监控和分析，IoT Security 还可以通过在用户定义的网络可视化图中可视化感兴趣的设备之间的通信模式。通过关注不同的设备组和网络的不同方面，可以在设备通信的可视化中以及设备与其运行的网络段之间的关系中，或者对于运营技术 (OT) 设备而言，在 OT 设备与其被分配到的 Purdue 级别之间的关系中会出现趋势、模式和异常。

IoT Security 提供了多种方法对设备进行分组以实现可视化：按设备属性（例如子网、VLAN、供应商、类别和配置文件）以及按 Purdue 级别。它还提供了创建具有一层或两层可视化地图的选项。也就是说，您首先根据特定属性（例如设备所在的 VLAN）将设备组织到群组中。这将产生一组按 VLAN 组织的设备组，让您可以查看网络中不同 VLAN 之间的设备分布情况。到目前为止，这是一张单层地图。但是，如果您愿意，您也可以通过其他属性（例如设备配置文件）来组织每个 VLAN 内的设备。然后，通过深入研究不同的 VLAN，您可以进入地图的第二层，并按配置文件查看每个 VLAN 内的设备分布。

创建可视化地图

STEP 1 | 选择 **Networks**（网络） > **Network Visualizations**（网络可视化）。

在创建第一个网络可视化地图之前，“网络可视化”页面会显示一张世界地图。任何已定义位置的现有站点都会出现在地图上的相应位置。没有明确位置的站点会出现在地图左下角的未知站点列表中。要定义站点的位置，请选择 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点），单击“位置”列中的 **N/A**（不适用）[或单击行右端的三个垂直点图标，然后单击 **Edit Site**（编辑站点）]，在“站点地址”中输入城市名称，然后单击 **Save**（保存）。

添加并保存可视化地图后，它将出现在此页面上，以便您稍后可以通过单击 **View Map**（查看地图）即可返回来查看该地图。

STEP 2 | 创建网络可视化地图。

您可以创建的可视化地图数量没有上限，但一个地图最多可以显示 *500* 个节点（子网、配置文件、设备等）。如果节点数超过 *500* 个，*IoT Security* 会隐藏地图并仅以表格格式显示信息。

1. 选择 **Networks**（网络） > **Network Visualizations**（网络可视化） > **+ Create Map**（+创建地图），选择一个或多个站点，然后 **Add to Scope**（添加到范围）。
2. 设置站点范围后，单击 **Next**（下一步）。
3. 单击 **Device Grouping**（设备分组），根据您的需要配置在地图上对设备进行分组的方法。您可以稍后更改。

   您选择的设备分组决定了您创建的地图类型。首先，根据以下属性之一对设备进行分组：**Category**（类别）、**Profile**（配置文件）、**Vendor**（供应商）、**Subnet**（子

网）、**VLAN ID** 或 **Purdue Level**（**Purdue** 级别）。然后，根据您使用的属性，可选地在第一层的每个组中按照第二层中的另一种类型的属性来组织它们：

第一组	第二组（可选）
类别	–
配置文件	–
供应商	风险等级
子网	类别或配置文件
VLAN ID	类别或配置文件
Purdue 等级*	类别或配置文件

* 在创建基于 Purdue 级别的设备可视化地图之前，必须首先指明各种设备所属的 Purdue 级别。您可以通过定义将 Purdue 级别自动应用于设备的自定义属性规则来实现这一点。这涉及以下过程：

1. 列出网络上所有 Purdue 0-3 级 OT 设备的设备属性，例如配置文件。或者，列出与 OT 分开且处于 4-5 级的所有其他 IT 和 IoT 设备的子网列表。
2. 在设备页面上创建六个过滤器，每个过滤器列出特定 Purdue 级别的设备的一组配置文件或子网。有关过滤器的详细信息，请参阅IoT Security 设备页面。
3. 使用 Purdue 级别 0-5 的六个预定义值来创建自定义属性规则，以根据您创建的过滤器将 Purdue 级别分配给设备（默认过滤器用于根据类别将 Purdue 级别分配给设备）。IoT Security 将任何不符合这些规则的设备分配到“未知”级别。

例如，如果将第一组设置为 **Subnet**（子网），将第二组设置为 **Category**（类别），那么您将创建一个地图，该地图首先显示组织到各个子网中的设备。然后，如果您通过单击其中一个子网导航到地图的第二层，将看到按设备类别分组的设备。

4. 通过输入更多参数来定义可视化地图的范围，继续细化地图范围，然后单击 **Update**（更新）。

IoT Security 根据您定义的范围显示可视化效果。范围必须包括设备在网络上活跃的时间范围（过去一天、一周或一个月）。范围通常还包含至少一个站点；但是，也可以制作不指定任何特定站点的地图，在这种情况下，地图将包含所有站点。除了时间范围和站点之外，您

还可以选择添加多个过滤器来进一步缩小地图范围。这样做可以让您更轻松地找到所需的设备类型，同时还可以减少地图显示的节点数量。

5. 查看可视化效果，如有必要，继续调整范围和设备分组，直到地图显示您想要查看的数据。
6. 当您对可视化地图的内容满意后，单击 **Build Map**（构建地图），然后输入以下内容：

   Name（名称）：输入可视化地图的名称

   Description（说明）：可选择输入可视化地图的描述，以供日后参考。

   Scope（范围）：查看定义地图参数的过滤器。由于地图最多可包含 500 个节点，因此定义一个保持在此范围内的范围。您可以通过按类型以及各种设备、警报和漏洞属性过滤设备来缩小范围。这种过滤的行为与查询生成器非常相似。

   Device Grouping（设备分组）：查看地图的设备分组。您可以在此处以及查看已保存的地图时编辑分组方法。
7. 单击 **Confirm**（确认）。

   该地图可立即在网络可视化页面上查看。

STEP 3 | Purdue 级别可以如有必要，单独手动重新分配设备。

设置过滤器并让规则自动将设备分配到 Purdue 级别后，定期对重要设备进行抽查，以确保它们在可视化地图上被分配到正确的 Purdue 级别。如果任何设备未正确分配，请记下其 IP 和 MAC 地址，以便通过 Device-ID 在 IoT Security 清单中查找。然后在“设备详细信息”页面上手动将其重新分配到正确的级别。

在可视化地图中查看数据

导航可视化地图和查看其数据的选项适用于两种类型的可视化方法：设备属性和 Purdue 级别。

节点（组和设备）

地图每层上的节点被描绘成圆形，节点之间的虚线表示网络连接。节点可以是一组对象，如子网、VLAN-ID、设备类别、设备配置文件、供应商或风险级别，也可以是这些组中的单个设备。圆圈内显示的数字表示其中有多少设备。有些组在其圆圈边缘周围有彩色线段。这些表示其中具有特定风险严重性的设备的比例。关键为红色，高为橙色，中为黄色。低风险级别是包围圈子的剩余灰色。（在 IoT Security 门户的其他部分，蓝色代表低严重级别；但是，由于蓝色用于突出显示可视化地图中的节点，因此此处不用于表示低风险级别。）一个组的圆圈大小表示其中的设备相对于地图上其他组的比例。

突出显示

位于可视化地图顶部的突出显示工具可帮助您查找具有某些特性的设备。要使用它，请使用查询语言输入一个或多个过滤器，然后单击 **Highlight**（突出显示）。IoT Security 会突出显示(带有蓝色环或部分环)与过滤器匹配的所有组和设备。环的长度表示组中与突出显示定义匹配的项目的比例。然后，您可以向下钻取匹配过滤器的高亮设备。

交互

- 悬停：将光标悬停在一组设备上，可看到一个弹出面板，其中包含组和设备的相关信息。您可以将光标悬停在包含其他组的组上，以查看所有组内设备的信息，也可以将光标悬停在其中一个内组上，以查看有关该组的信息。将鼠标悬停在设备上会显示一个弹出面板，其中包含有关该设备的信息。

- 单击一次：单击某个组或设备后，该组或设备将处于焦点位置，并在地图右侧显示有关该组或设备的信息面板。单击设备信息面板顶部的 **External Link**（外部链接）图标将打开设备的设备详细信息页面，您可以在其中看到相关信息。
- 单击两次：单击组两次(双击或单击已聚焦的组或设备)可深入查看其内容以及其内容与其他组的网络连接。单击设备两次可显示其与其他设备的网络连接。
- 重新定位节点：您还可以拖动组和设备在地图上重新定位它们。此功能仅适用于主地图显示。双击特定组时，焦点中的新组始终显示在地图上居中。
- 使用表格和痕迹：使用表格中的链接在地图层中导航，方法是单击表格列中的链接以深入地图，然后单击表格上方痕迹中的链接以向上移动到较高层。
- 使用返回按钮：除了单击表格上方的痕迹移回更高的地图层，您还可以单击页面顶部 IoT Security 标识和地图名称之间的 **Back**（返回）按钮。当您已经处于地图顶层时，单击 **Back**（返回）按钮将退出当前地图并返回到可视化登录页面。

地图名称和总计

各种总计的摘要显示在页面左上角的地图名称下方。

例如，第一个数字可能是子网数，第二个可能是类别数，第三个可能是地图上的设备数。如果作用域包含超过 500 个节点，请考虑缩小作用域，以便地图显示它们。

创建地图并使用地图后，您可能会做一些更改和调整，并决定要保存编辑的地图。为此，请单击地图名称旁边的 **Edit Map**（编辑地图）图标。IoT Security 将显示“更新网络可视化地图”面板，您可以在其中更改地图名称、描述、可视化方法和范围，然后 **Confirm**（确认）更改。更新网络可视化地图面板中的另一个选项是地图生成器。单击 **Map Builder**（地图生成器）以查看地图并对可视化方法（设备分组）和范围进行编辑。通过向作用域添加或删除过滤器后单击 **Update**（更新），您可以看到您的更改如何影响地图内容。完成后，单击 **Update Map**（更新映射），这将返回更新网络可视化映射。查看您修改的设置，如果满意，请 **Confirm**（确认）更改。如果您还不满意，请再次单击 **Map Builder**（地图生成器）以返回地图，然后根据需要继续进行调整。

图例

可视化地图的左边是放大 (+) 和缩小 (-) 图标，以及一个信息图标，打开一个颜色和图标含义的图例。单击以展开它。

基本

- 查看单个设备时，其风险级别由圆圈上一点处的颜色表示。
- 查看设备组时，设备组内设备的风险级别以圆形边缘周围的红色、橙色和黄色表示。每种颜色的数量是处于该风险级别的设备与组中设备总数的比例。
- 使用突出显示工具查找具有特定属性的设备时，一个蓝色环(或环的段)出现在组的边缘，其长度表示组中具有突出显示属性的设备的比例。蓝色线段越长，按比例突出显示的设备越多。

风险等级

- 标识每个风险级别的颜色。

图标

- 绿色地球表示组中的一台或多台设备连接到正常的 Internet 站点。
- 红色地球表示一个或多个设备已连接到恶意互联网网站。

- 三边形的黄色图标表示存在一个或多个到地图外设备的连接；也就是说，连接到本地网络上但不在此可视化地图定义的范围内的设备。
- 笔记本电脑图标表示一个或多个设备连接到本地网络上的 IP 端点。IP 端点是 IoT Security 已获知 IP 地址但未获知 MAC 地址的网络连接的源或目标。

地图管理

在地图管理部分，您可以控制在地图上显示哪些类型的设备和连接。通过选中并清除它们的复选框，您可以切换地图上的图标。

- **Inner Connection**（内部连接）：选中或清除复选框以显示或隐藏内部连接，这些连接是同一设备组内的连接。因为组之间的连接通常更受关注，所以默认情况下会关闭。要查看内部连接（同一组中设备之间的连接），请切换内部连接。
- 设备可视化地图有时包括 **IP Endpoints**（**IP** 端点）、**Off-map Devices**（地图外设备）和 **Internet Connections**（互联网连接） [**Normal**（正常）和 **Malicious**（恶意）]，只要需要显示可视化地图范围内定义的设备与该范围外目标之间的连接。非映射设备(深黄色阴影圈)和 IP 端点(灰色阴影圈)位于本地专用网络中，互联网地址是外部公共网络中的站点（绿色阴影圈表示正常站点，红色阴影表示恶意站点）。IP 端点是 IoT Security 知道 IP 地址的设备。范围外设备是指 IoT Security 同时知道 IP 地址和 MAC 地址但在映射范围之外的设备。与其他设备组一样，您还可以钻取范围外的设备和端点以及 Internet 地址的组。单击该组一次，将其置于焦点并打开一个信息面板。单击两次可放大并查看其内容。

报告

您可以在报告部分 [**Logs & Reports**（日志和报告） > **Reports**（报告）] 查看和下载各种类型的报告：

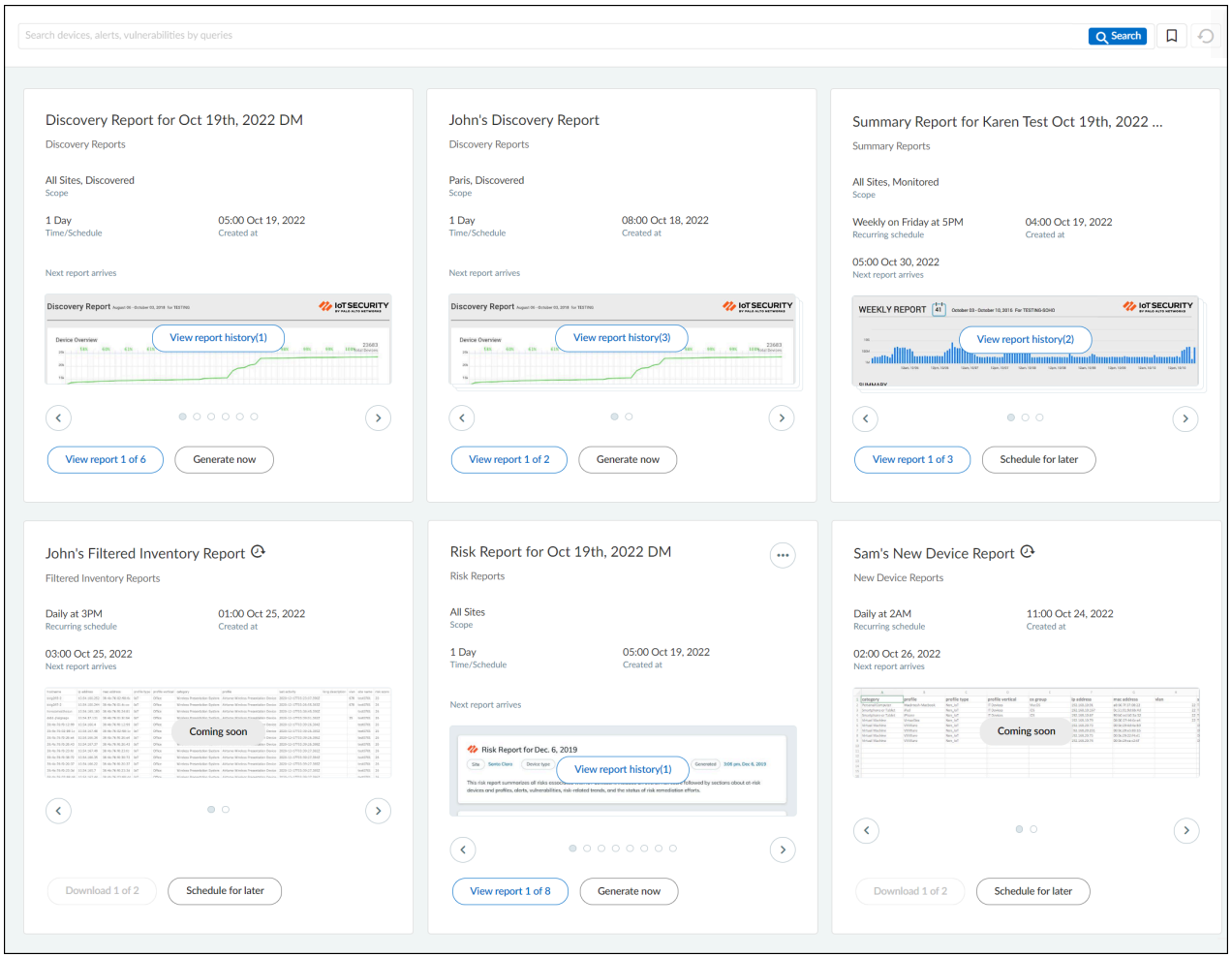
- 摘要部分提供了设备清单、风险评估和警报的摘要。
- 发现部分提供 IoT Security 在您的网络上发现的设备的视图，它们在不同的子网/VLAN 中的分布以及具有高风险分数和待处理警报的设备。
- 新设备部分报告自上次报告以来，在您的网络上检测到的所有新设备。IoT Security 可以按日、周或月生成报告。
- 风险部分总结与 IoT 设备相关的所有风险。它报告总体风险评分、风险设备、警报、漏洞、风险相关趋势以及风险补救措施的状态。
- 清单缺口（当 IoT Security 与 CMMS 集成时）部分显示由 IoT Security 发现的设备，您的 CMMS（计算机化维护管理系统）清单中的设备，以及两组设备重叠和不重叠的地方。
- 利用率部分提供有关医疗 IoT 设备操作和使用情况的数据可视化。
- 过滤清单部分使用您在“设备”页面中选择的先前定义的过滤器来准备设备清单报告。

生成报告有两种方式：立即生成和按计划生成。计划报告可以生成一次，也可以定期生成。

- 发现报告只能立即生成
- 所有其他报告类型都必须安排
- 风险报告和利用率报告可以双向生成

配置报告

您可以将报告配置为按需生成或安排在稍后生成。



立即生成报告

您只能立即生成发现、利用率和风险报告；所有其他报告都必须安排。要立即生成报告，请单击报告页面右上角的 **+** 图标，然后选择 **Generate a report now**（立即生成报告）。提供或选择所需的详细信息，然后单击 **Generate**（生成）。

- **Report type**（报告类型）：从下拉列表中选择报告类型。
- **Report Name**（报告名称）：输入报告的名称。
- 站点：您可以选择所有站点、单个站点或者（如果您将站点排列在分层组中）一组站点。
- **Alert Severity**（警报严重性）和 **Risk Level**（风险级别）：对于发现报告，警报严重性针对的是安全警报，风险级别针对的是漏洞。您可以选择一、二或三个严重性和风险级

别。IoT Security 将根据您的选择过滤发现报告中包括的设备。如果将这些内容留空，则警报严重性和风险级别将不会用于过滤要包含在报告中的设备。

- **Device type**（风险类型）：风险报告可选；选择所有设备类型或一种或多种单独的类型（汽车、工业、医疗等）。对于发现报告，请从已发现或已监控中进行选择。“已发现”的设备是 IoT Security 知道在内部网络上，但没有受到监控和保护的设备。“受监控”的设备也位于内部网络上，并且 IoT Security 正在监控它们的网络活动以进行设备分析、行为分析和风险监控。
- **Device Category**（设备类别）：对于利用率报告，清单报告的设备类别字段仅限于输液系统和图像扫描程序（X 射线机、超声波机、MRI 机、CT 扫描程序和 PET 扫描程序）。
- **Subscribe**（订阅）：选择您要向其发送报告的电子邮件地址。
- **Select a time range**（选择时间范围）：从可用的时间范围中选择或创建您想要生成报告的自定义时间范围。

报告将在几分钟内生成并可在报告页面上查看。

安排稍后报告

计划报告可以生成一次或定期生成。除发现报告和利用率报告外，所有报告均可安排。要安排以后日期的报告，请单击报告页面右上角的 **+** 号，然后选择 **Schedule a report for later**（安排以后的报告）。请提供或选择所需的详细信息，然后单击 **Schedule**（计划）。

除了上一节中介绍的字段之外，下面还介绍了特定于计划报告的字段。

- **Scope**（范围）：对于摘要报告，这决定了报告将包含的内容，并且可以设置为站点或设备类型（汽车、工业、医疗等）。选择全部则不会过滤站点或设备类型。
- **Saved Filters/Queries**（已保存的过滤器/查询）（可选）：对于已过滤的清单报告，请从下拉菜单中选择已保存的过滤器。
- **Set a recurring schedule**（设置重复执行计划）：您可以安排报告按日、周、月或自定义时间运行。
  - 摘要报告：每周、每月第一天
  - 风险报告：每日、每周、每月第一天、自定义时间表（设置为一周中的任何一天和时间）
  - 新设备和过滤清单报告：每日、每周、每月第一天

  首次生成计划报告时，它将包含 IoT Security 在报告配置中设置的时间段内收集的数据。例如，如果您在 10 月 27 日创建每月定期新设备报告，并从当月第一天开始，IoT Security 将于 11 月 1 日生成第一份报告，其中包含自 10 月 1 日起 31 天的新设备数据。对于每日和每周的定期报告也是如此。最初生成计划报告后，IoT Security 继续按照指定的时间间隔生成报告，每份新报告中都会包含自上一份报告以来收集的数据。

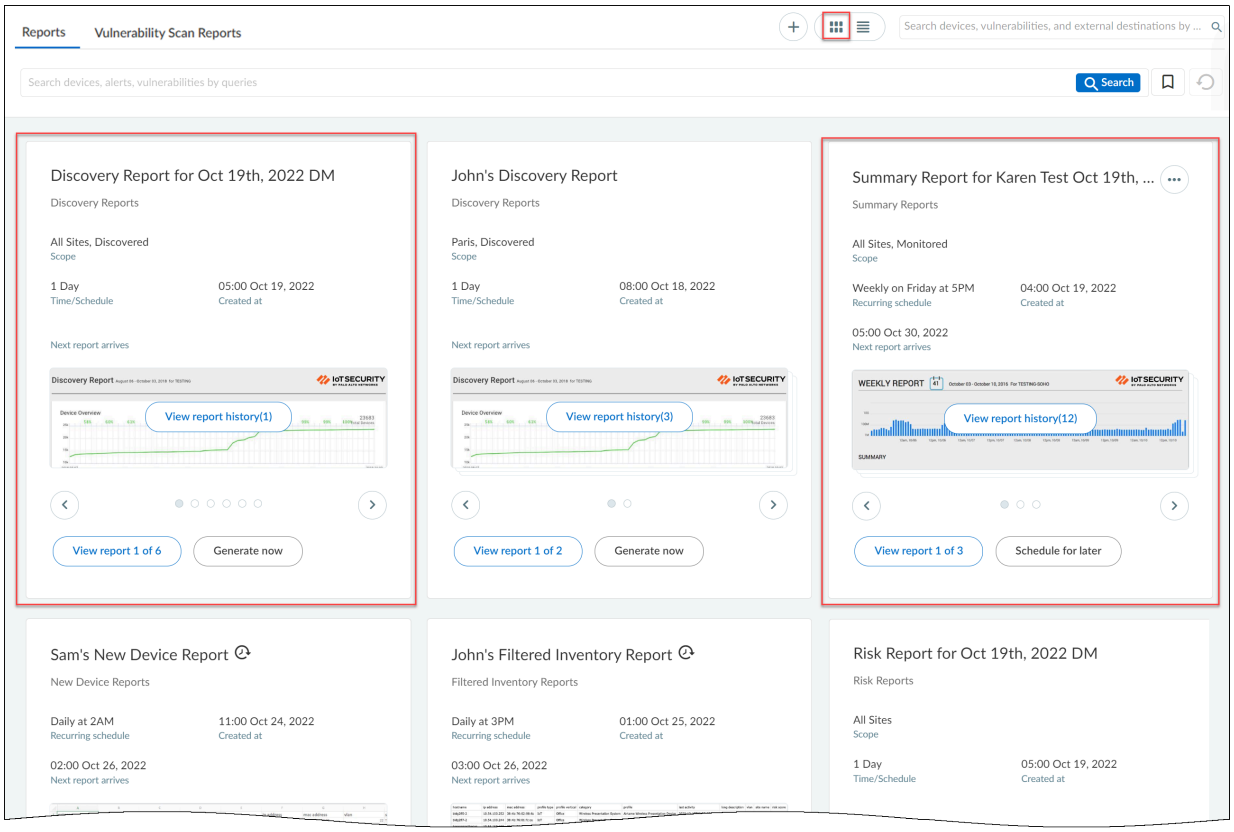
该报告现在计划在您选择的时间生成。与即时报告类似，此报告也可在报告页面上找到。

查看报告

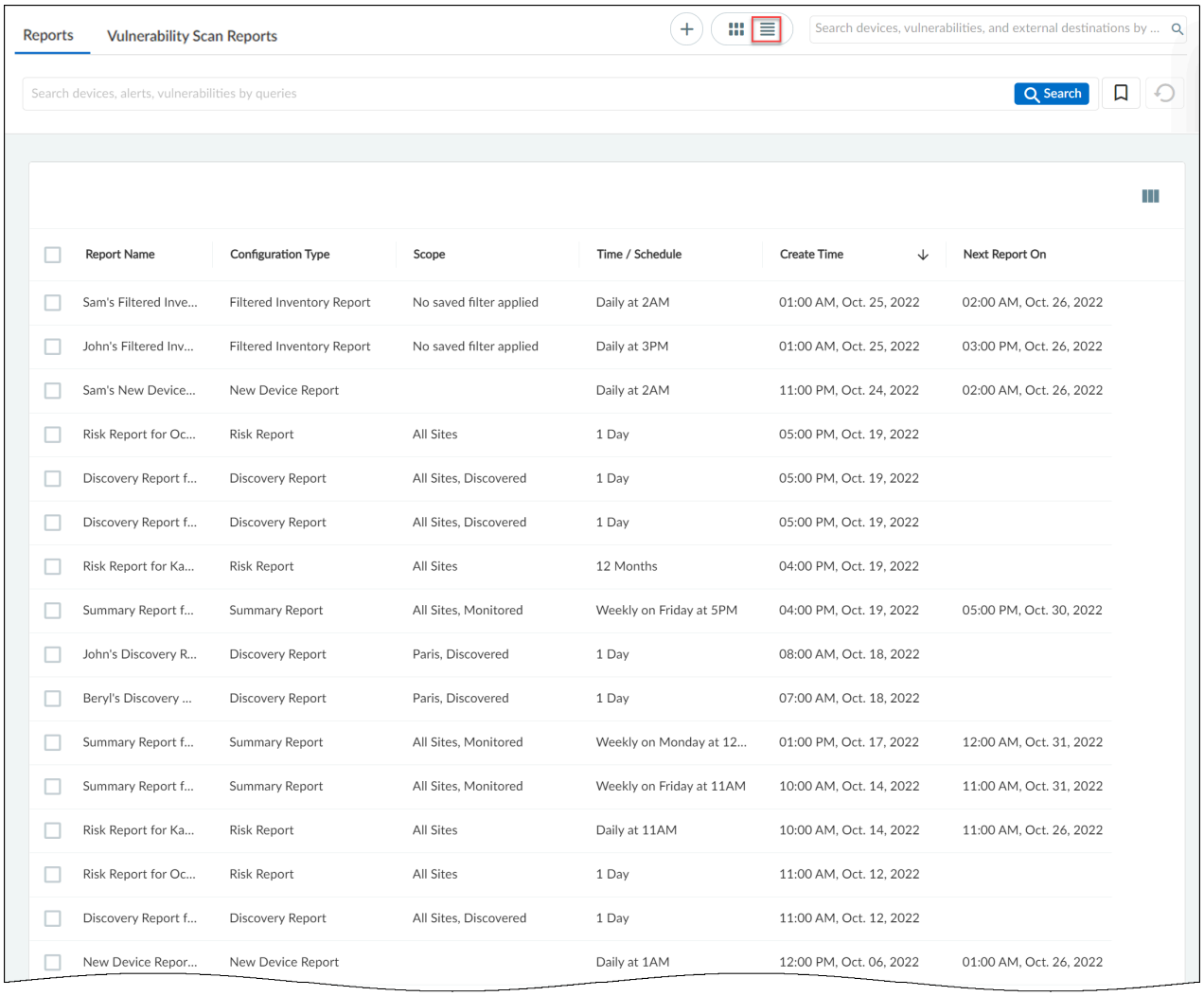
您可以在卡片视图或列表视图中查看报告。视图设置位于报告页面的右上角的 **+** 图标和搜索字段之间。

报告页面上的卡片视图显示分组在卡片内的类似报告。卡片按三个参数分组：报告类型、范围和时间表。例如：

- 所有范围设置为“所有站点，已发现”且时间安排设置为 1 天的发现报告均分组到一张卡片下。
- 所有范围设置为“所有站点，受监控”且时间表设置为“每周五下午 5 点”的摘要报告都分组在另一张卡片下。



报告页面上的列表视图以列表格式显示所有报告。您可以根据报告名称、配置、范围等对报告进行排序。您只能在列表视图中删除报告。



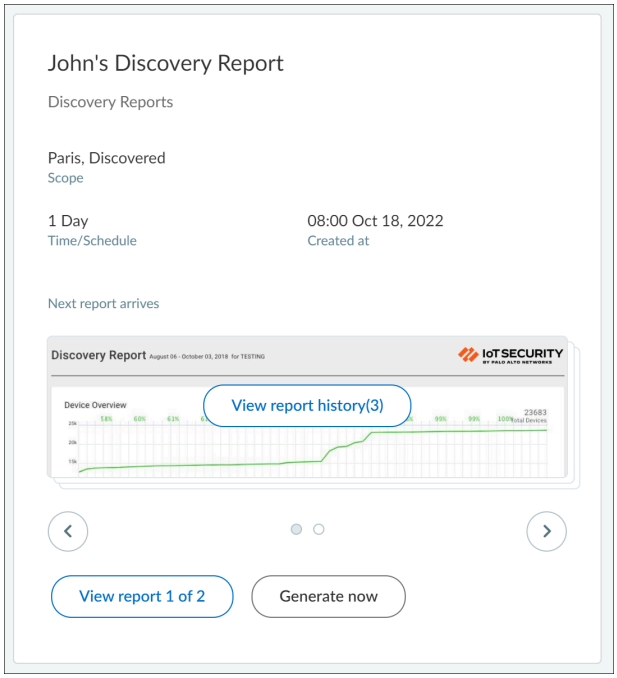
Report Name	Configuration Type	Scope	Time / Schedule	Create Time	Next Report On
Sam's Filtered Inve...	Filtered Inventory Report	No saved filter applied	Daily at 2AM	01:00 AM, Oct. 25, 2022	02:00 AM, Oct. 26, 2022
John's Filtered Inv...	Filtered Inventory Report	No saved filter applied	Daily at 3PM	01:00 AM, Oct. 25, 2022	03:00 PM, Oct. 26, 2022
Sam's New Device...	New Device Report		Daily at 2AM	11:00 PM, Oct. 24, 2022	02:00 AM, Oct. 26, 2022
Risk Report for Oc...	Risk Report	All Sites	1 Day	05:00 PM, Oct. 19, 2022	
Discovery Report f...	Discovery Report	All Sites, Discovered	1 Day	05:00 PM, Oct. 19, 2022	
Discovery Report f...	Discovery Report	All Sites, Discovered	1 Day	05:00 PM, Oct. 19, 2022	
Risk Report for Ka...	Risk Report	All Sites	12 Months	04:00 PM, Oct. 19, 2022	
Summary Report f...	Summary Report	All Sites, Monitored	Weekly on Friday at 5PM	04:00 PM, Oct. 19, 2022	05:00 PM, Oct. 30, 2022
John's Discovery R...	Discovery Report	Paris, Discovered	1 Day	08:00 AM, Oct. 18, 2022	
Beryl's Discovery ...	Discovery Report	Paris, Discovered	1 Day	07:00 AM, Oct. 18, 2022	
Summary Report f...	Summary Report	All Sites, Monitored	Weekly on Monday at 12...	01:00 PM, Oct. 17, 2022	12:00 AM, Oct. 31, 2022
Summary Report f...	Summary Report	All Sites, Monitored	Weekly on Friday at 11AM	10:00 AM, Oct. 14, 2022	11:00 AM, Oct. 31, 2022
Risk Report for Ka...	Risk Report	All Sites	Daily at 11AM	10:00 AM, Oct. 14, 2022	11:00 AM, Oct. 26, 2022
Risk Report for Oc...	Risk Report	All Sites	1 Day	11:00 AM, Oct. 12, 2022	
Discovery Report f...	Discovery Report	All Sites, Discovered	1 Day	11:00 AM, Oct. 12, 2022	
New Device Repor...	New Device Report		Daily at 1AM	12:00 PM, Oct. 06, 2022	01:00 AM, Oct. 26, 2022

多个用户的类似报告在卡片视图中分组到一张卡片下。可以通过在列表视图中排序来查看多个用户的类似报告。用户生成的报告可以有多个版本。

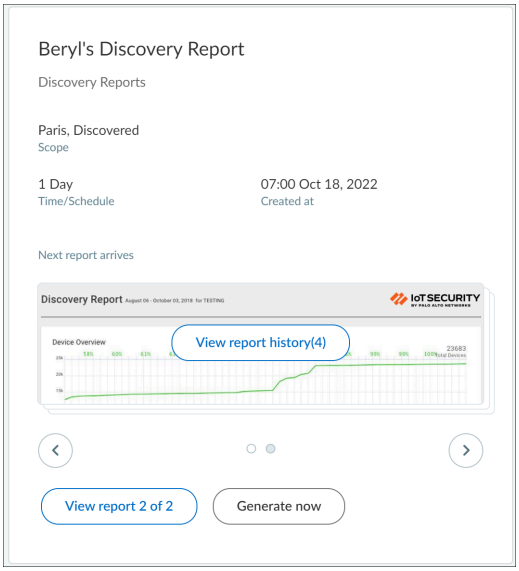
查看报告历史记录 **(*n*)** 和查看 **(*m*)/(*n*)** 份报告

View report history（查看报告历史记录） **(*n*)** 与 查看 **(*m*) / (*n*)** 份报告不同，通过以下示例使用案例即可看出：

John 和 Beryl 生成相同的报告：发现报告的范围设置为“巴黎，已发现”，时间设置为 1 天。两份报告都放在一张卡片内。每次 John 单击 **Generate now**（立即生成）来生成报告时，**View report history**（查看报告历史记录）**(n)** 就会逐步增加。例如，当您看到 John 的报告的查看报告历史记录 (3) 时，这意味着 John 已生成了三次报告。因此，**View report history**（查看报告历史记录）显示的是同一用户对同一份报告的不同版本。底部的 **View report 1 of 2**（查看报告 **1**（共 **2** 份）表示此报告（也是最新报告）是由 John 生成的，并且还有另一份类似类型的发现报告由其他用户生成。

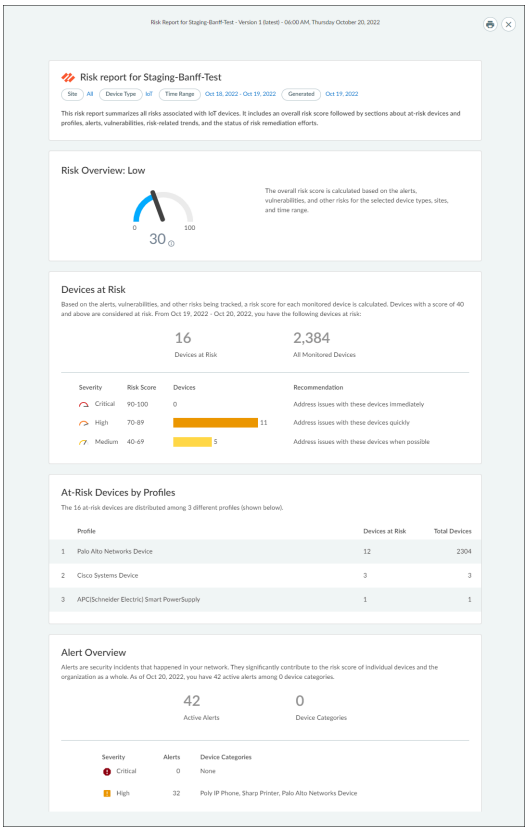


要查看第二个用户的报告，请单击卡片底部的 **>**，数字现在变为 **View report 2 of 2**（查看报告 **2**，共 **2** 份（见下图）。报告 2 由 Beryl 生成。Beryl 生成了四次报告，因此我们现在看到 **View report history**（查看报告历史记录）**(4)**。



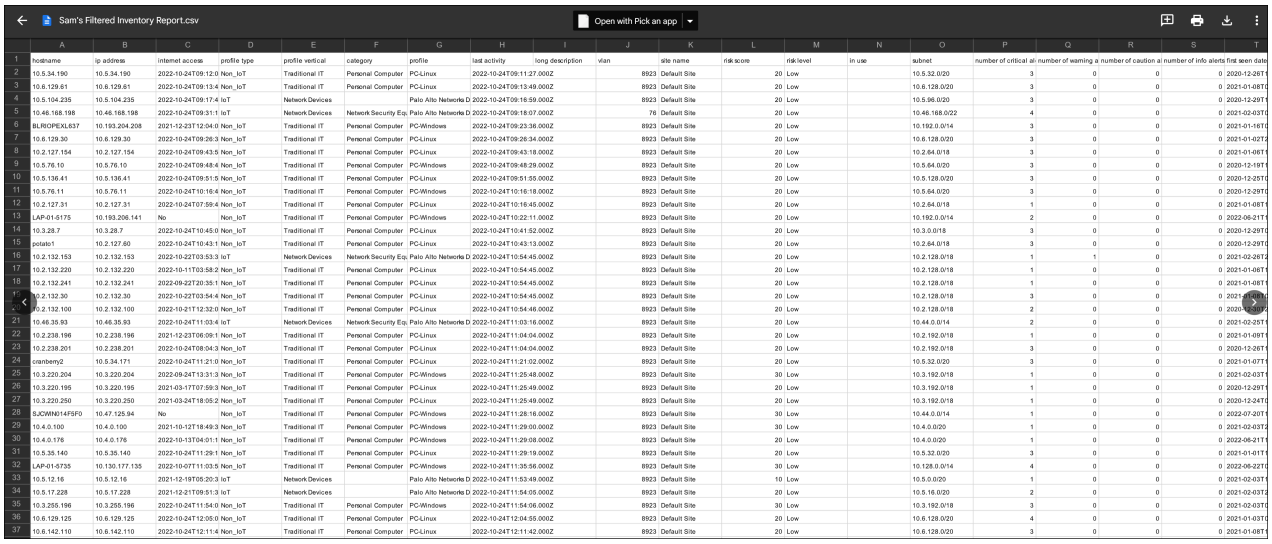
在浏览器中查看报告

由于摘要、连接、发现、风险、清单和利用率报告都是以 HTML 格式生成的，因此可以在浏览器中查看它们。要查看您的报告，请单击报告上的 **View Report History**（查看报告历史记录）**(n)**或 **View Report (m) of (n)**（查看报告 **m**，共 **n** 份）。您还可以将其打印并下载为 PDF 文件。



下载报告以供查看

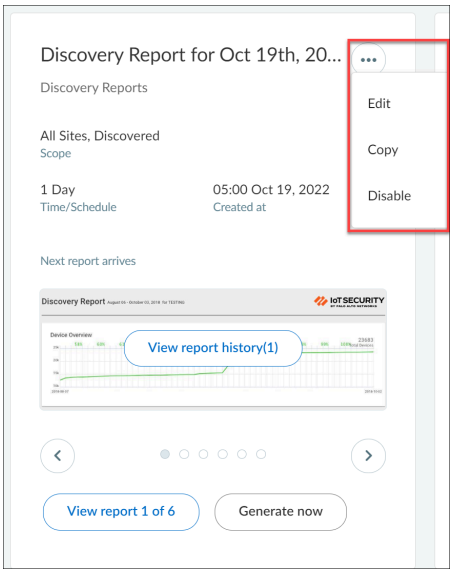
由于新设备报告和过滤清单报告以 .csv 文件形式生成，因此只能在下载后在电子表格阅读器或编辑器中查看。要下载报告，请单击报告上的 **View Report History**（查看报告历史记录）**(n)** 或 **View Report (m) of (n)**（查看报告 **m**，共 **n** 份）。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	hostname	ip address	internet access	profile type	profile vertical	category	profile	last activity	long description	vlan	site name	risk score	risk level	in use	subnet	number of critical al	number of warning a	number of caution a	number of info alerts	first seen date
2	10.5.34.190	10.5.34.190	2022-10-24T09:12:0	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T09:11:27.000Z		8923	Default Site	20	Low		10.5.32.0/20	3	0	0	0	2020-12-28T
3	10.6.129.61	10.6.129.61	2022-10-24T09:13:4	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T09:13:49.000Z		8923	Default Site	20	Low		10.6.128.0/20	3	0	0	0	2021-01-08T
4	10.5.104.235	10.5.104.235	2022-10-24T09:17:4	IoT	Network Devices		Palo Alto Networks D	2022-10-24T09:18:59.000Z		8923	Default Site	20	Low		10.5.96.0/20	3	0	0	0	2020-12-29T
5	10.46.168.198	10.46.168.198	2022-10-24T09:31:1	IoT	Network Devices	Network Security Eq	Palo Alto Networks D	2022-10-24T09:18:07.000Z		76	Default Site	20	Low		10.46.168.0/22	4	0	0	0	2021-02-03T
6	BLRIOPEXL637	10.193.204.208	2021-12-23T12:04:0	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T09:23:36.000Z		8923	Default Site	20	Low		10.192.0.0/14	3	0	0	0	2021-01-16T
7	10.6.129.30	10.6.129.30	2022-10-24T09:26:3	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T09:26:34.000Z		8923	Default Site	20	Low		10.6.128.0/20	3	0	0	0	2021-01-02T
8	10.2.127.154	10.2.127.154	2022-10-24T09:43:5	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T09:43:18.000Z		8923	Default Site	20	Low		10.2.64.0/18	3	0	0	0	2021-01-06T
9	10.5.76.10	10.5.76.10	2022-10-24T09:48:4	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T09:48:29.000Z		8923	Default Site	20	Low		10.5.64.0/20	3	0	0	0	2020-12-19T
10	10.5.136.41	10.5.136.41	2022-10-24T09:51:5	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T09:51:55.000Z		8923	Default Site	20	Low		10.5.128.0/20	3	0	0	0	2020-12-25T
11	10.5.76.11	10.5.76.11	2022-10-24T10:16:4	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T10:16:18.000Z		8923	Default Site	20	Low		10.5.64.0/20	3	0	0	0	2020-12-29T
12	10.2.127.31	10.2.127.31	2022-10-24T07:59:4	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:16:45.000Z		8923	Default Site	20	Low		10.2.64.0/18	1	0	0	0	2021-01-08T
13	LAP-01-5175	10.193.206.141	No	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T10:22:11.000Z		8923	Default Site	20	Low		10.192.0.0/14	2	0	0	0	2022-06-21T
14	10.3.28.7	10.3.28.7	2022-10-24T10:45:0	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:41:52.000Z		8923	Default Site	20	Low		10.3.0.0/18	3	0	0	0	2020-12-29T
15	potato1	10.2.127.60	2022-10-24T10:43:1	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:43:13.000Z		8923	Default Site	20	Low		10.2.64.0/18	3	0	0	0	2020-12-29T
16	10.2.132.153	10.2.132.153	2022-10-22T03:53:3	IoT	Network Devices	Network Security Eq	Palo Alto Networks D	2022-10-24T10:54:45.000Z		8923	Default Site	20	Low		10.2.128.0/18	1	1	0	0	2021-02-26T
17	10.2.132.220	10.2.132.220	2022-10-11T03:58:2	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:54:45.000Z		8923	Default Site	20	Low		10.2.128.0/18	1	0	0	0	2021-01-06T
18	10.2.132.241	10.2.132.241	2022-09-22T20:35:1	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:54:45.000Z		8923	Default Site	20	Low		10.2.128.0/18	1	0	0	0	2021-01-08T
19	10.2.132.30	10.2.132.30	2022-10-22T03:54:4	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:54:45.000Z		8923	Default Site	20	Low		10.2.128.0/18	3	0	0	0	2021-01-08T
20	10.2.132.100	10.2.132.100	2022-10-21T12:32:0	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T10:54:46.000Z		8923	Default Site	20	Low		10.2.128.0/18	2	0	0	0	2020-12-29T
21	10.46.35.93	10.46.35.93	2022-10-24T11:03:4	IoT	Network Devices	Network Security Eq	Palo Alto Networks D	2022-10-24T11:03:16.000Z		8923	Default Site	20	Low		10.44.0.0/14	2	0	0	0	2021-02-25T
22	10.2.238.196	10.2.238.196	2021-12-23T06:09:1	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T11:04:04.000Z		8923	Default Site	20	Low		10.2.192.0/18	1	0	0	0	2021-01-09T
23	10.2.238.201	10.2.238.201	2022-10-24T08:04:3	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T11:04:04.000Z		8923	Default Site	20	Low		10.2.192.0/18	3	0	0	0	2020-12-26T
24	cranberry2	10.5.34.171	2022-10-24T11:21:0	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T11:21:02.000Z		8923	Default Site	20	Low		10.5.32.0/20	3	0	0	0	2021-01-07T
25	10.3.220.204	10.3.220.204	2022-09-24T13:31:3	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T11:25:48.000Z		8923	Default Site	30	Low		10.3.192.0/18	1	0	0	0	2021-02-03T
26	10.3.220.195	10.3.220.195	2021-03-17T07:59:3	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T11:25:49.000Z		8923	Default Site	20	Low		10.3.192.0/18	1	0	0	0	2020-12-29T
27	10.3.220.250	10.3.220.250	2021-03-24T18:05:2	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T11:25:49.000Z		8923	Default Site	20	Low		10.3.192.0/18	1	0	0	0	2020-12-24T
28	SJCWN0114F5F0	10.47.125.94	No	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T11:28:16.000Z		8923	Default Site	30	Low		10.44.0.0/14	1	0	0	0	2022-07-20T
29	10.4.0.100	10.4.0.100	2021-10-12T18:49:3	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T11:29:00.000Z		8923	Default Site	30	Low		10.4.0.0/20	1	0	0	0	2021-02-03T
30	10.4.0.176	10.4.0.176	2022-10-13T04:01:1	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T11:29:08.000Z		8923	Default Site	20	Low		10.4.0.0/20	1	0	0	0	2022-06-21T
31	10.5.35.140	10.5.35.140	2022-10-24T11:29:1	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T11:29:19.000Z		8923	Default Site	20	Low		10.5.32.0/20	3	0	0	0	2021-01-01T
32	LAP-01-5735	10.130.177.135	2022-10-07T11:03:5	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T11:35:56.000Z		8923	Default Site	30	Low		10.128.0.0/14	4	0	0	0	2022-06-22T
33	10.5.12.16	10.5.12.16	2021-12-19T05:20:3	IoT	Network Devices		Palo Alto Networks D	2022-10-24T11:53:49.000Z		8923	Default Site	10	Low		10.5.0.0/20	1	0	0	0	2021-02-03T
34	10.5.17.228	10.5.17.228	2021-12-21T09:51:3	IoT	Network Devices		Palo Alto Networks D	2022-10-24T11:54:05.000Z		8923	Default Site	20	Low		10.5.16.0/20	2	0	0	0	2021-02-03T
35	10.3.255.196	10.3.255.196	2022-10-24T11:54:0	Non_IoT	Traditional IT	Personal Computer	PC-Windows	2022-10-24T11:54:06.000Z		8923	Default Site	30	Low		10.3.192.0/18	3	0	0	0	2021-02-03T
36	10.6.129.125	10.6.129.125	2022-10-24T12:05:0	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T12:04:55.000Z		8923	Default Site	20	Low		10.6.128.0/20	4	0	0	0	2021-01-03T
37	10.6.142.110	10.6.142.110	2022-10-24T12:11:4	Non_IoT	Traditional IT	Personal Computer	PC-Linux	2022-10-24T12:11:42.000Z		8923	Default Site	20	Low		10.6.128.0/20	3	0	0	0	2021-01-08T

编辑、复制和禁用报告

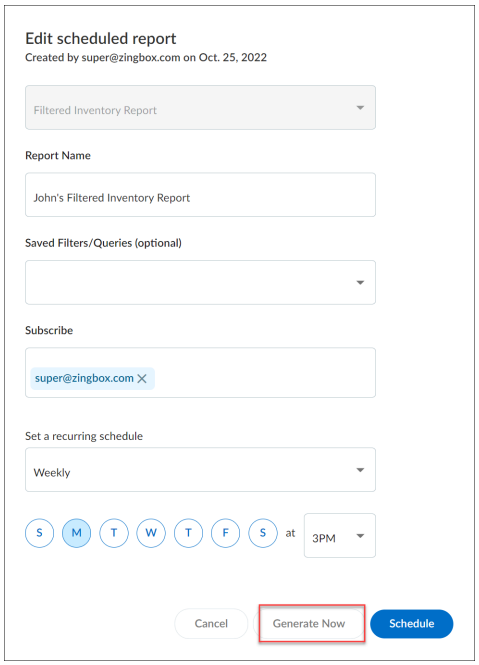
单击报告上的操作菜单图标 **(...)** 来编辑、复制和禁用它。



编辑报告

编辑报告以调整设置。例如，您可能想要增加或减少计划报告的频率，或者添加或删除订阅的电子邮件地址。

您还可以根据需要生成计划报告，而不必等待计划的时间。当您单击 **Edit**（编辑） > **Generate Now**（立即生成）以生成计划报告时，IoT Security 根据配置中设置的时间段（每日、每周或每月）生成报告，从您单击 **Generate Now**（立即生成）时回溯一天、一周或一个月，并生成到该时刻的报告。例如，如果您计划在每周一凌晨 3:00 生成一份“新设备”报告，而您在周三上午 10:00 单击 **Generate Now**（立即生成），那么您将获得从上周三上午 10:00 到您单击 **Generate Now**（立即生成）那一刻为止的整整一周（7 天）的报告。



复制报告

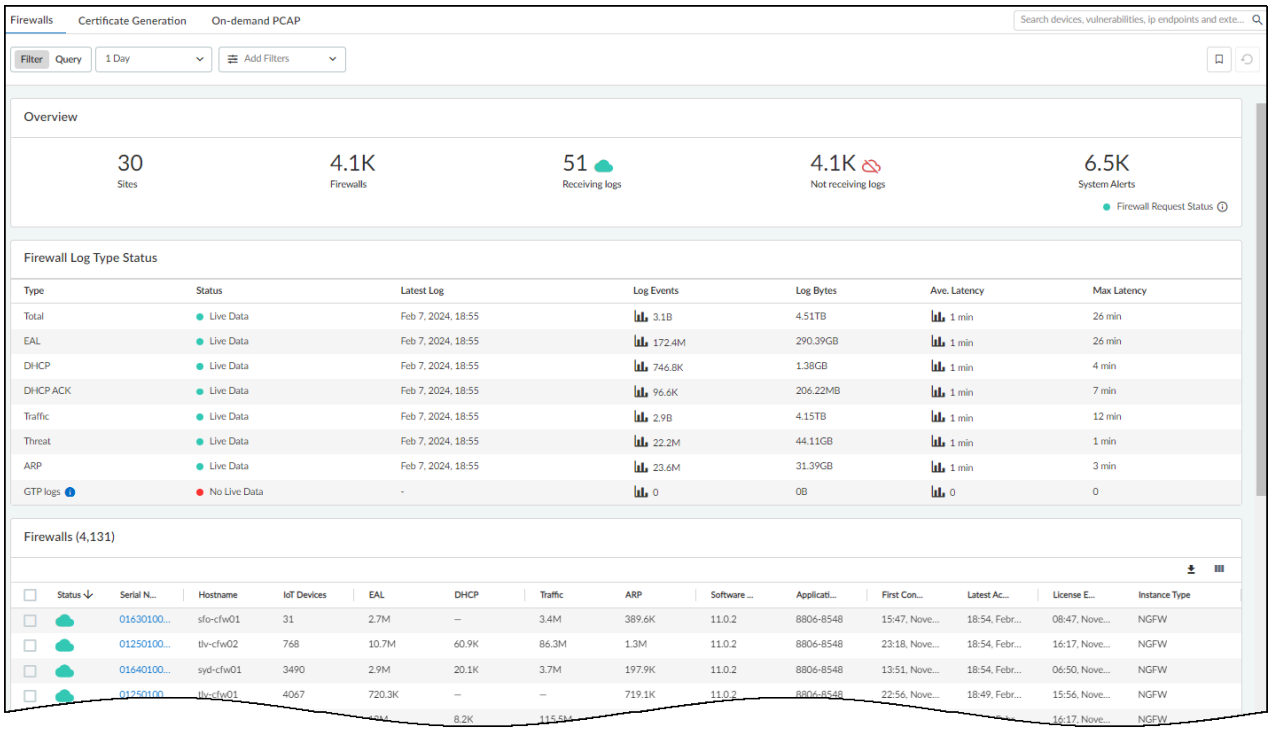
复制一份报告以保留原始报告，但在此基础上创建另一份报告并进行一些更改；例如，您可能希望定期生成两份新设备报告 - 每天一份报告用于每日健全性检查，每月一份报告用于每月团队报告。

禁用报告

禁用报告以暂停其预定的生成，可能是在预定的网络维护期间。不过，在禁用该功能后您仍然可以查看现有报告。当您稍后想要恢复使用该报告时，可以再次启用它。

IoT Security 与防火墙的集成状态

“防火墙”页面 [**Administration**（管理） > **Firewalls**（防火墙） > **Firewalls**（防火墙）] 概述了防火墙连接和活动、防火墙发送的日志状态、它们对策略规则建议和 IP 地址到设备映射的请求，以及各个防火墙的详细信息。



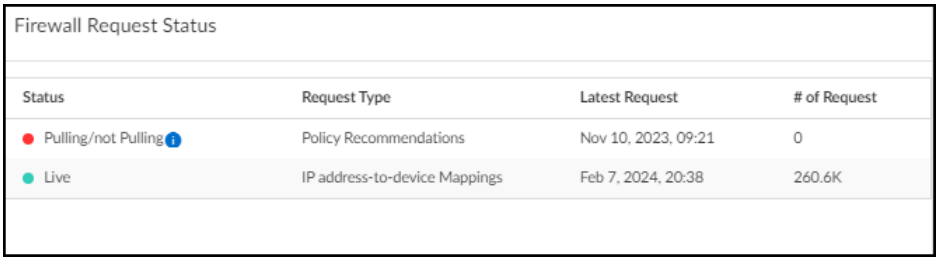
页面顶部的概览显示了 IoT Security 管理下有多少个站点，订阅了多少个防火墙到 IoT Security，有多少个防火墙处于活动状态，IoT Security 正在从多少个防火墙接收日志，IoT Security

没有从多少个防火墙接收日志，以及有多少个系统警报。单击系统警报编号可查看位于 **Administration**（管理） > **System Events**（系统事件）中的警报列表。

如果防火墙在过去 30 分钟内收到来自它的日志，则 IoT Security 认为防火墙处于活动状态，如果在此期间未收到日志，则认为防火墙处于活动状态，它将自动生成警报。“防火墙”页面还显示防火墙在过去 7 天、24 小时或一小时（取决于您设置的时间过滤器）发送到 IoT Security 的日志事件数，收到最后一条日志的时间，以及防火墙的连接状态。

IoT Security 协调从同一站点的所有防火墙接收的数据。并非每个防火墙都需要像其他防火墙一样将日志发送到 *IoT Security*，并且其日志会从您希望 *IoT Security* 进行监控的所有 *IoT* 设备捕获网络流量数据。

将光标悬停在 **Firewall Request Status**（防火墙请求状态）图标上课查看 IoT Security 是否正在接收来自防火墙的有关策略建议和 IP 地址到设备映射的请求。



当 IoT Security 在过去 30 分钟内收到过其中一个请求时，状态图标为绿色。否则为红色。

对于在过去 30 分钟内已将日志事件发送到 IoT Security 的主动/被动 HA 对中的防火墙，活动防火墙的状态显示为 **Receiving logs**（正在接收日志）。除了重新启动后的 30-60 分钟，被动防火墙的状态通常显示为 **Not receiving logs**（未收到日志）。在此期间，其状态将更改为 **Receiving logs**（正在接收日志），然后恢复 **Not receiving logs**（未收到日志）状态。对于具有物理接口的被动防火墙和具有未配置链路聚合控制协议 (LACP) 被动预协商的聚合接口的被动防火墙，都是如此。如果被动防火墙具有配置了 LACP 被动预协商的聚合接口，则它始终显示为 **Receiving logs**（正在接收日志），因为它不断将学习的 ARP 条目发送到 IoT Security

如果您将防火墙从 *PAN-OS 9.x* 升级到 *10.0* 或更高版本，并且发现 *HA* 对中之前在 *IoT Security* 中显示为“活动”的被动防火墙对现在显示为“非活动”，请检查它们是否具有聚合接口，以及它们是否配置了 *LACP* 被动预协商。

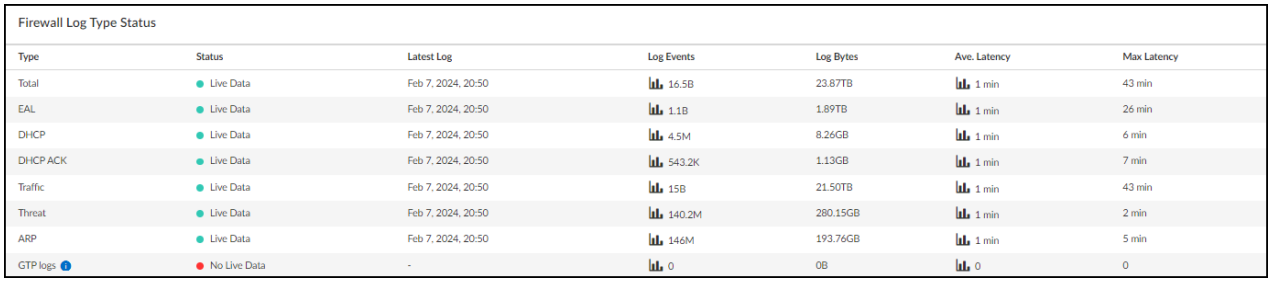
防火墙将日志事件发送到日志记录服务，该服务将日志事件流式传输到 IoT Security 来进行分析，并且，根据您的 IoT Security 订阅类型，将它们发送到 Strata Logging Service 来进行存储。然后，IoT Security 会处理和分析从日志记录服务接收的原始元数据，并将分析生成的数据保留以下时间长度：

- 针对设备网络流量行为的数据保留一个月

- 以下数据保留一年：
  - 设备标识
  - 安全警报、风险和漏洞
  - （Medical IoT）设备利用率

上述保留期限适用于 *IoT Security*。有关 *IoT Security* 数据保留的更多信息，请参阅 IoT Security 隐私表。有关 *Strata Logging Service* 数据保留的信息，请参阅 Strata Logging Service 隐私表。

“防火墙日志类型状态”部分显示 IoT Security 是否在过去 30 分钟内从日志记录服务收到 EAL、DHCP、DHCP ACK、ARP、流量和威胁日志的日志事件。如果有，则状态为 **Live Data**（实时数据）。如果没有，则状态为 **No Live Data**（无实时数据）。

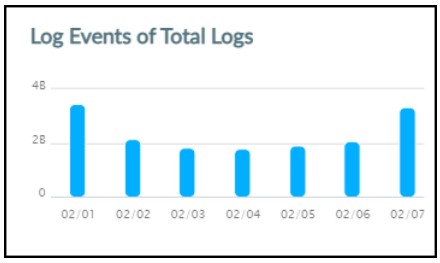

Firewall Log Type Status

Type	Status	Latest Log	Log Events	Log Bytes	Ave. Latency	Max Latency
Total	Live Data	Feb 7, 2024, 20:50	16.5B	23.87TB	1 min	43 min
EAL	Live Data	Feb 7, 2024, 20:50	1.1B	1.89TB	1 min	26 min
DHCP	Live Data	Feb 7, 2024, 20:50	4.5M	8.26GB	1 min	6 min
DHCP ACK	Live Data	Feb 7, 2024, 20:50	543.2K	1.13GB	1 min	7 min
Traffic	Live Data	Feb 7, 2024, 20:50	15B	21.50TB	1 min	43 min
Threat	Live Data	Feb 7, 2024, 20:50	140.2M	280.15GB	1 min	2 min
ARP	Live Data	Feb 7, 2024, 20:50	146M	193.76GB	1 min	5 min
GTP logs	No Live Data	-	0	0B	0	0

当状态为 **Live Data**（实时数据）时，这并不意味着所有活动防火墙都在过去 30 分钟内向日志记录服务发送了日志事件。尽管这是可能的，但您只能安全地推断出至少有一个活动防火墙已执行此操作，并且日志记录服务随后已将其接收到的任何日志事件流式传输到 IoT Security但是，如果状态为 **No Live Data**（无实时数据），则可以有把握地得出结论，在过去 30 分钟内，日志记录服务未收到来自任何防火墙的日志事件。

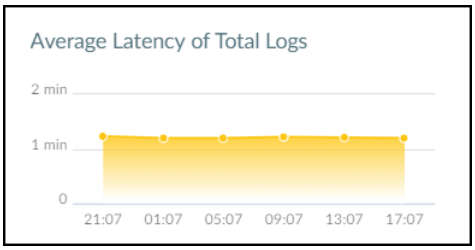
如果概述部分的防火墙状态为 ***Active***（活动）或 ***Inactive***（非活动），则不是实时数据。它每 *30* 分钟更新一次，以小时和半小时为单位。另一方面，防火墙日志类型状态接近实时。每次刷新页面时，“防火墙日志类型状态”都会显示这四种日志类型的当前状态。因此，两个状态指示器之间有时会出现暂时的不匹配。

将光标悬停在“日志事件”列中的图形图标上，可看到一个弹出的面板，其中包含有关每种类型日志的信息。



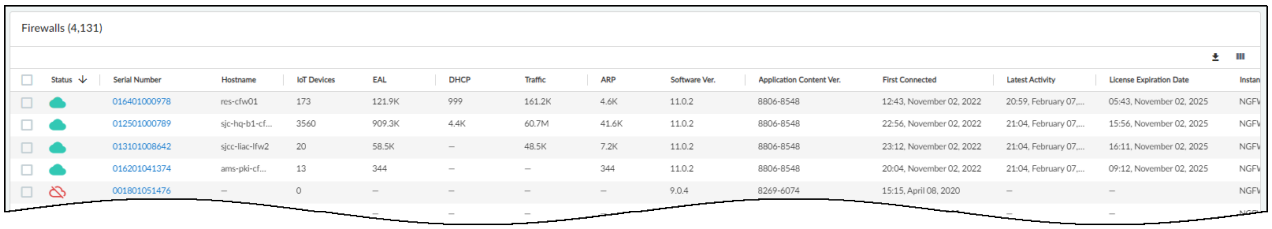
该面板包含一个图表，该图表显示 IoT Security 收到的日志事件。当您将页面顶部的时间过滤器设置为 **1 Week**（**1** 周）时，数据以 7 个 24 小时为间隔显示，涵盖过去 7 天。当您将过滤器设置为 **1 Day**（**1** 天）时，数据以 6 个 4 小时为间隔显示，涵盖过去 24 小时。当您将其设置为 **1 Hour**（**1** 小时）时，数据以 6 个 10 分钟为间隔显示，涵盖过去 60 分钟。将光标悬停在各个数据点上，可查看包含有关数据点的更多信息的工具提示。

将光标悬停在“平均延迟”列中的图形图标上，可看到一个弹出面板，其中包含有关防火墙将日志上传到日志记录服务的时间与 IoT Security 接收它们的时间之间的延迟信息。



当您将页面顶部的时间过滤器设置为 **1 Week**（**1** 周）时，则显示过去 7 天每天的平均延迟。当您将过滤器设置为 **1 Day**（**1** 天）时，平均延迟以 6 个 4 小时为间隔显示，涵盖过去 24 小时。当您将其设置为 **1 Hour**（**1** 小时）时，则过去 60 分钟内的平均延迟以 6 个 10 分钟的间隔显示。将光标悬停在各个数据点上，可查看包含有关数据点的更多信息的工具提示。

“防火墙”页面的其余部分包含一个表，其中包含订阅 IoT Security 服务的所有防火墙。您可以使用列控制工具（显示在表格上方的带有三个灰色条的图标）来自定义表格中显示的数据。除了防火墙的状态、主机名、序列号、IP 地址（默认情况下不可见）以及在其上运行的 PAN-OS 版本外，该表还显示其他几个数据点。有针对 IoT 字典版本、App-ID 的应用程序内容版本和防火墙许可证类型 [Prod（生产）、Eval（评估）或 Lab] 的列。首次连接 IoT Security 时，您还可以查看每个防火墙、它所在的站点（默认情况下不可见）的不同类型日志事件的数量，以及它上次处于活动状态的时间。



默认情况下，“IoT 字典版本”列在表中可见。如果未显示在表格中，请单击列可见性图标（三条垂直线），然后选择 **IoT Dictionary Ver**（**IoT** 词典版本）。此列显示每个防火墙上字典文件的版本号。新版本每两周发布一次，内部版本号在各个版本之间逐渐增加。例如，版本是 1-218，然后在两周后（以及两个内部版本之后）发布版本 2-221。

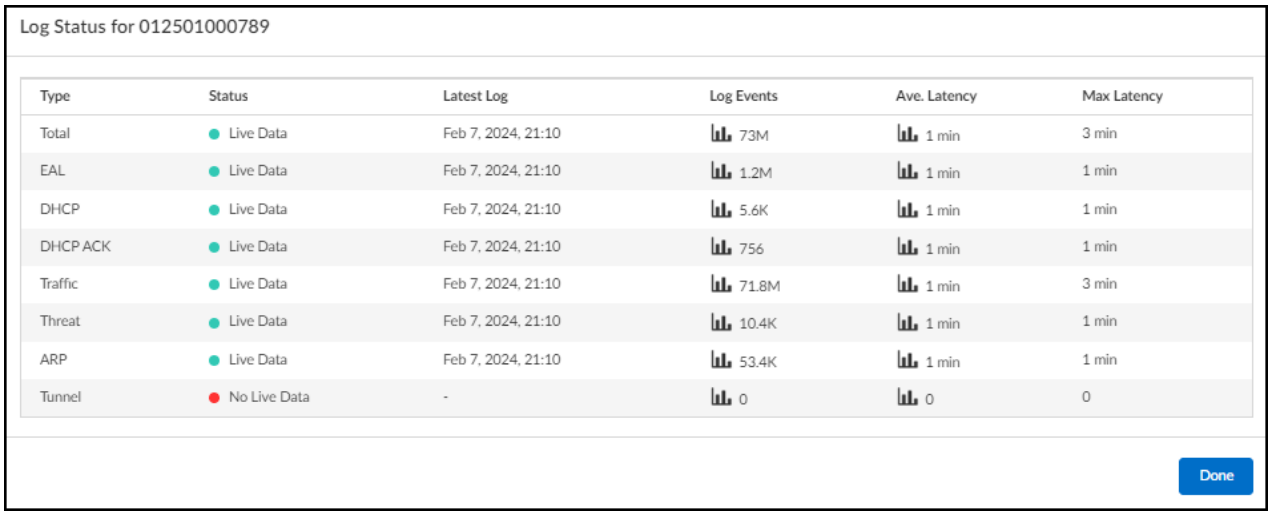
所有防火墙都应具有相同的 IoT 字典版本；即最新版本。如果防火墙使用过时的字典（很可能是因为它无法访问更新服务器），则它无法使用 Device-ID 完全准确地执行安全策略规则。采取措施恢复其与更新服务器的连接，以便下次防火墙自动检查其 IoT 字典版本与服务器上的版本（每两小时检查一次）时，它将检测到新版本并下载它。

只有运行 *PAN-OS* 版本 *10.0* 或更高版本的防火墙才支持 *Device-ID* 和 *IoT* 字典。对于运行早期版本的 *PAN-OS* 的防火墙，此列中会显示一个短划线。

应用程序内容版本决定了防火墙发送到 IoT Security 的日志中的协议数据类型。低版本可能不会生成 IoT Security 需要的 IoT 协议日志。

最右边的列提供了将防火墙从一个站点移动到另一个站点的选项。

如果单击防火墙序列号，则会出现一个弹出面板，其中包含有关此防火墙的日志的信息。您可以查看 IoT Security 当前是否正在接收实时数据、最新日志的时间戳、接收的事件数、平均延迟以及为“防火墙”页面指定的时间过滤器 [**1 Week**（**1** 周）、**1 Day**（**1** 天）或 **1 Hour**（**1** 小时）] 内的最大延迟。


Log Status for 012501000789

Type	Status	Latest Log	Log Events	Ave. Latency	Max Latency
Total	Live Data	Feb 7, 2024, 21:10	73M	1 min	3 min
EAL	Live Data	Feb 7, 2024, 21:10	1.2M	1 min	1 min
DHCP	Live Data	Feb 7, 2024, 21:10	5.6K	1 min	1 min
DHCP ACK	Live Data	Feb 7, 2024, 21:10	756	1 min	1 min
Traffic	Live Data	Feb 7, 2024, 21:10	71.8M	1 min	3 min
Threat	Live Data	Feb 7, 2024, 21:10	10.4K	1 min	1 min
ARP	Live Data	Feb 7, 2024, 21:10	53.4K	1 min	1 min
Tunnel	No Live Data	-	0	0	0

Done

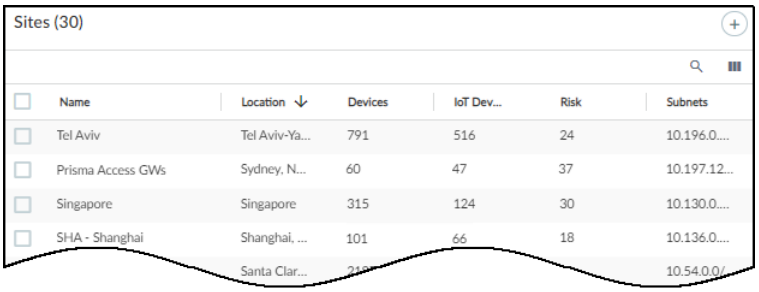
具有 Prisma Access 的 IoT Security 集成状态

在 IoT Security 门户中，站点和防火墙页面提供了具有活动 IoT Security 订阅的新一代防火墙。它们显示每个站点的防火墙总数、每个防火墙的连接状态、它们转发到日志记录服务的日志事件总数以及它们发送的日志类型。然而，当 Prisma Access 通过 IoT Security 附加组件订阅 IoT Security 时，这些页面上显示的信息与新一代防火墙所显示的信息不同。

站点

当 Prisma Access 使用 IoT Security 附加组件时，它在 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点）页面上的站点名称是 Prisma Access。无论单个 Prisma Access 实例是保护一个或一百个远程站点，IoT Security 都不知道它们的数量。从 IoT Security 的角度来看，设备和 IoT 设备的数量来自单个 Prisma Access 实体，与保护的远程站点数量无关。

以下屏幕截图显示 Prisma Access 以及几个拥有内部新一代防火墙的站点的混合部署，以供比较。



站点页面包含 Prisma Access 的以下类型的信息：

状态：绿色云表示 IoT Security 已连接到 Prisma Access 且正在接收日志。带有一条线的红色云表示 IoT Security 未检测到从 Prisma Access 转发到 Strata Logging Service 的日志。

名称：Prisma Access

Location（位置）：如果先前定义了位置，那么这就是站点位置。

设备：这是 IoT Security 在 Prisma Access 保护下的所有远程站点中识别的设备总数量。

IoT 设备：这是 Prisma Access 在所有远程站点上识别的 IoT 设备总数量。这是“设备”列中显示的总数量的一个子集。

风险：这是针对 Prisma Access 保护的所有 IoT 设备计算出的总体风险评分。

子网：这些是跨所有 Prisma Access 远程站点的子网。因为 IoT Security 无法了解 Prisma Access 正在保护多少个站点，这可能来自具有单个子网的单个站点、具有多个子网的单个站点、每个站点具有单个唯一子网的多个站点、具有多个子网的多个站点，或者这些场景的任意组合。

群组：这表示站点在分层站点组织中位于哪个组。

源：如果 IoT Security 与 BlueCat IPAM 或 Infoblox IPAM 有第三方集成，并从该处了解站点名称，则集成的名称显示在此处。当第三方集成不是 IoT Security 了解到的网站时，这里会显示一个短横线。

防火墙

本页 [**Administration**（管理） > **Firewalls**（防火墙） > **Firewalls**（防火墙）] 不适用于 Prisma Access。如果您正在将 IoT Security 专门与 Prisma Access 搭配使用，则页面顶部会显示两个站点，一个用于 Prisma Access一个用于默认站点，即 IoT Security 最初分配内部防火墙的站点。活跃和非活跃状态分别为 1 或 0，具体取决于 IoT Security 检测到的在过去 30 分钟内从 Prisma Access 发送到 Strata Logging Service 的任何日志。

IoT Security 显示与 Prisma Access 相关的系统警报数量。这些是针对策略建议和 IP 地址到设备的映射，接收的来自 Prisma Access 的请求。例如：

`IoT Security` 在过去 `30` 分钟内未收到任何策略建议请求。

`IoT Security` 正在再次接收 `IP` 地址到设备映射的请求。

单击防火墙页面顶部的系统警报数量，打开 **Administration**（管理） > **System Events**（系统事件），以便查看它们。Prisma Access 系统警报的来源始终是 `All firewalls`。

防火墙页面的其余部分没有任何与 Prisma Access 相关的数据。

如果您的部署包括 Prisma Access 以及本地新一代防火墙的混合，则本页面包含 Prisma Access 的上述信息，以及有关防火墙及其提供的日志的更多信息。

数据质量诊断

防火墙处理并转发到日志记录服务的网络数据的质量会直接影响 IoT Security 可以执行的分析的质量。在 **Administration**（管理） > **Data Quality**（数据质量）页面上，您可以查看 IoT Security 必须使用的数据的质量。两个关键因素是 IP 端点和低置信度设备。

IP 端点是没有唯一标识符的设备，因此随着时间的推移它们无法被追踪。如果 IoT Security 无法为设备找到唯一的设备标识符，则将其归类为 IP 端点。当 IoT Security 通过 DHCP 或 ARP 了解设备的 IP 地址，但不知道其 MAC 地址时，以及当 IoT Security 了解设备的 IP 地址，但其设备配置文件不够稳定，无法将其归类为静态 IP 设备时，通常会发生这种情况。在第一种情况下，MAC 地址是 DHCP 客户端的唯一标识符。在第二种情况下，如果静态 IP 设备的配置文件足够稳定，表明 IP 地址不会在不同的 DHCP 客户端之间转移，则该 IP 地址是静态 IP 设备的唯一标识符。

低置信度设备是指 IoT Security 可以使用低于 70% 的置信度进行识别的设备。IoT Security 提供识别网络连接设备并为其分配设备配置文件的基础服务之一。在整个过程中，它会考虑多种因素，并为每次识别创建一个置信度分数。该分数在 0 至 100 之间，其中 100 表示最高置信度。置信度水平很重要，因为 IoT Security 仅在设备身份的置信度得分较高 (90-100%)，并且在过去一小时内发送或接收了流量时，才会向防火墙发送 IP 地址到设备的映射。

置信度分数表示 *IoT Security* 在其设备标识中的置信度水平。根据计算出的置信度分数，*IoT Security* 有三个置信度级别：高 *(90-100%)*、中 *(70-89%)* 和低 *(0-69%)*。

当防火墙向日志记录服务转发较少的数据日志，以便 IoT Security 进行分析时，它往往无法准确识别设备。另一方面，当防火墙将更多日志转发到日志记录服务时，IoT Security 可以识别设备，并且能够更彻底地确定其行为基准。这会带来更高的设备身份置信度分数。

此页面显示网络上的 IP 端点和低置信度设备的数量，以及属于这两类的设备占网络上设备总数的百分比。通过这些数字，您可以推断出 IoT Security 正在接收的设备数据的质量，这些数字是过去 30 天内从所有设备获取的。

每个部署都有其独特的特点，您使用 IoT Security 的理由将确定网络上 IP 端点和低置信度设备的可接受百分比。例如，如果您的目标是发现、识别和保护 IoT 设备，则可能只能使用附近有一到两个防火墙的 IoT Security。在这种情况下，可接受的 IP 端点和低置信度设备的百分比将非常接近网络上非 IoT 设备的百分比。简而言之，考虑一下您的目标是什么，并使用这里的数据来查看您距离目标还有多远。如果您的网络上 IP 端点和低置信度设备的数量超出预期，请考虑页面上提供的建议并遵循您认为可以减少这些数量的建议。

在部署后的前几个月，最好每周检查一次数据质量诊断，以确保 *IoT Security* 正在获取识别设备所需的数据，如果没有，则根据需要进行调整。在您满意之后，请定期返回进行抽查，并在网络发生变化时进行跟进。

授权按需 PCAP

新一代防火墙的按需数据包捕获 (PCAP) 功能允许您授权 IoT Security 研究团队执行数据包捕获，并自动将捕获的数据包文件上传到 IoT Security 来进行离线分析。IoT Security 研究团队仅在必要时进行数据包捕获，例如，当您的网络上出现未知设备或未知应用程序且无法通过其他方式获取评估情况所需的信息时。此类数据包捕获的范围受到限制，因此它们不会影响正常的防火墙操作。

PCAP 文件会安全存储，只有 IoT Security 研究团队成员才能访问。在分析完成后，您可以手动删除这些文件，也可以等到 30 天后让它自动删除。

为了让 IoT Security 研究团队使用 PCAP 从防火墙收集网络流量元数据，您必须首先授予防火墙允许捕获数据包的权限。

要在防火墙上支持 *PCAP*，它们必须正在运行：

- *PAN-OS 11.0.4* 或更高的 *11.0* 版本
- *PAN-OS 11.1.0* 或更高版本

STEP 1 | 登录 PAN-OS 并安装 openconfig 附加组件。

1. 选择 **Device**（设备） > **Plugins**（附加组件）并搜索 `openconfig`。
2. 下载版本 2.1.0 或更高版本，然后进行 **Install**（安装）。

STEP 2 | 使用具有管理员或所有者权限的用户帐户登录 IoT Security 门户。

STEP 3 | 在一个或多个防火墙上授权 PCAP。

1. 选择 **Administration**（管理） > **Firewalls**（防火墙） > **On-demand PCAP**（按需 **PCAP**），然后单击 **Add**（添加） **(+)** 图标。
2. 通过序列号或序列号和名称的串联来选择防火墙。
3. 设置在防火墙上授权 PCAP 的时间段，可以是 1 个月、3 个月，也可以是无限期。

   当授权期限到期时，PCAP 将失去在防火墙上获得的授权。如果需要，可以对其重新授权 PCAP。然后，您可以在授权防火墙列表中看到新的 PCAP 授权期限。
4. **Confirm**（确认）授权。
5. 要在其他防火墙上授权 PCAP，请重复这些步骤。

STEP 4 | 在一个或多个防火墙上取消授权 PCAP。

当您想在防火墙上取消对 PCAP 的授权时。

1. 在“授权防火墙”列表中选择一个或多个防火墙。
2. **Unauthorize**（取消授权）所选防火墙。

   如果您只想在一个防火墙上取消对 *PCAP* 的授权，您也可以单击 ***Reauthorize***（重新授权）图标。

IoT Security 与第三方产品的集成

在 IoT Security 识别您网络上的 IoT 设备并发现它们是否构成任何安全威胁后，它会与新一代防火墙以及 Prisma Access 配合使用，以保护您的设备和网络。此外，您还可以将 IoT Security 与第三方产品集成，以扩展其特定功能的使用范围，将 IoT 纳入其中。例如，当网络访问控制 (NAC) 解决方案与 IoT Security 集成时，它可以允许或拒绝其身份原本无法获知的 IoT 设备的网络访问。IoT Security 用户还可以发送 NAC 系统或无线局域网控制器命令来隔离存在漏洞或有安全警报的 IoT 设备。有时集成是朝一个方向进行的，即 IoT Security 与第三方产品共享其设备信息，有时集成是朝另一个方向进行的，即 IoT Security 从第三方产品学习设备信息。其他集成增强了 IoT Security 功能，例如与第三方漏洞扫描程序的集成。

有两种选项可以将 IoT Security 与第三方系统集成，第三种选项是通过其 API 将 Cortex XSOAR 与 IoT Security 集成：

- 具有共同托管、功能有限的 Cortex XSOAR 实例的 IoT Security 公共云（需要购买 IoT Security 第三方集成附加组件，该附加组件附带自动生成的共同托管 XSOAR 实例，无需额外付费）

  IoT Security 第三方集成附加组件不需要购买完整的 *Cortex XSOAR* 产品。启用该附加组件后，*IoT Security* 会自动生成一个功能有限的云托管 *XSOAR* 实例（与完整的 *Cortex XSOAR* 产品不同），以协助 *IoT Security* 实现其支持的集成。
- 使用本地、功能齐全的 Cortex XSOAR 服务器实现 IoT Security
- 功能齐全的 Cortex XSOAR 实例，可访问 IoT Security API

有关 IoT Security 支持的第三方集成的信息，请参阅 IoT Security 集成指南。

IoT Security 和 FedRAMP

联邦风险和授权管理计划 (FedRAMP) 是美国政府的一项计划，旨在促进联邦政府使用安全的云服务。根据 FIPS 出版物 199 安全分类，归类为中等安全影响级别的云计算系统被授权存储和处理政府数据。Palo Alto Networks IoT Security 云已获得 FedRAMP Moderate 授权。

IoT Security FedRAMP Moderate 解决方案旨在供需要采用标准化方法来评估、授权和持续监视云产品和服务的美国政府机构使用。它还旨在供与美国政府有业务往来的商业实体使用。IoT Security FedRAMP Moderate 解决方案作为一个独立的实体运营。

IoT Security 商业解决方案和 IoT Security FedRAMP Moderate 解决方案存在以下差异：

- 您必须购买额外的 SKU 才能获得 IoT Security FedRAMP Moderate 解决方案。
- IoT Security FedRAMP Moderate 解决方案仅允许 FedRAMP 授权的人员访问数据。
- 由于 Palo Alto Networks 对 FedRAMP 租户强制执行严格的传入安全策略规则，因此必须为访问您的 IoT Security 门户的管理用户提供 Palo Alto Networks 客户服务以及一个 IP 地址列表。当流向门户的用户流量通过外围防火墙、边缘路由器或 VPN 网关上的 NAT 设备时，请提供 NAT 将用户的原始 IP 地址转换为的 IP 地址。在您提交包含这些地址的支持票证后，客户服务将为您提供的地址创建一个允许列表，该列表将允许用户从这些地址登录并访问门户。
- 与第三方产品集成时，请使用完整的本地 Cortex XSOAR 服务器。FedRAMP 建议使用供应商批准 FIPS 版本（符合 FIPS 140-2 标准）的本地组件运行解决方案的本地组件。

> 为不需要购买 *IoT Security* 第三方集成附加组件许可证的 *IoT Security* 第三方 集成使用本地 *Cortex XSOAR* 服务器。

对于 Prisma Access 和 FIPS 模式下的新一代防火墙，IoT Security 支持安全策略规则建议和基于 Device-ID 的自动化零信任实施。使用 CLI 配置 PAN-OS Edge 服务以检索 Device-ID 判定和 IoT Security 策略建议。

```
fw> configure fw# set deviceconfig setting iot edge address \
 iot.services-edge.pubsec-cloud.paloaltonetworks.com fw# commit
 fw# quit fw> debug software restart process icd
```

有关 Palo Alto Networks IoT Security FedRAMP 授权的更多信息，请访问以下网站：

- FedRAMP 的官方网站
- FedRAMP Marketplace 上的 Palo Alto Networks 解决方案
- FedRAMP 授权服务 Palo Alto Networks 网站

发现 IoT 设备并创建清单

IoT Security 使用多种方法来发现 IoT 设备并创建动态清单。

- IoT 设备发现
- IoT Security 设备页面
- IoT Security 设备详细信息页面
- 创建多接口设备
- 具有静态 IP 地址的设备
- 上传静态 IP 设备列表
- 添加静态 IP 设备配置
- 上传只有静态 IP 地址的子网列表
- 添加只有静态 IP 地址的子网
- IP 端点
- 发现移动设备属性
- 自定义属性
- 标签管理

IoT 设备发现

与通常是多用途硬件的 IT 资产不同，IoT 设备是专门构建的系统。这些设备旨在以重复方式执行一些任务，并且 IoT Security 解决方案提供对正常和可疑网络行为的深入可见性。

每个 IoT 设备在网络上都表现出独特的特性。当未知设备加入网络时，一个或多个 Palo Alto Networks 防火墙会记录其网络流量，然后将日志发送到日志记录服务。这些日志包括会话日志（包含有关流量流的元数据）和增强的应用程序日志（包含来自数据包有效负载的数据）。IoT Security 从日志记录服务访问数据，并使用其先进的机器学习算法和三层分析系统来分析网络行为并为设备构建基线。然后，它将该基线与其他已知设备的行为进行比较（有关详细信息，请参阅 IoT Security 概述。这样，它就可以确定设备的独特性，并为其创建一个配置文件，包括设备类型、类别、供应商、型号、操作系统等等。IoT Security 自动为设备构建行为配置文件，包括可接受行为的基线以及与其他设备的通信模式。

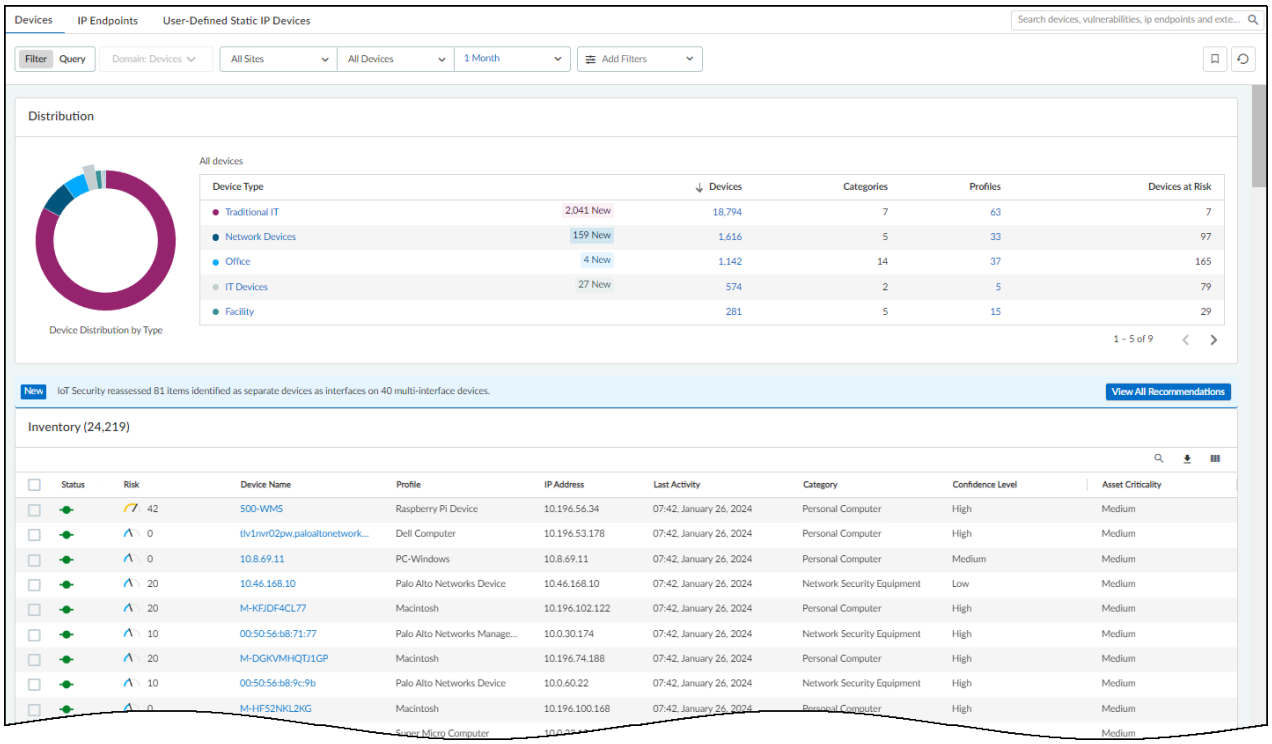
IoT Security 持续学习并维护设备行为的滚动基线。构建初始配置文件所需的时间取决于几个因素：

- 设备在网络上的活跃程度如何？IoT Security 对产生大量流量的设备的分析比产生少量流量的设备更快，因为它有更多的数据要分析。
- 网络上有多少个相同类型的设备？相同类型的设备越多，分析工作速度就越快，因为它可以同时聚合从多个设备学到的知识。
- 单个设备的行为有多复杂？例如，IoT Security 学习联网恒温器的行为比学习医院手术机器人的速度快得多。

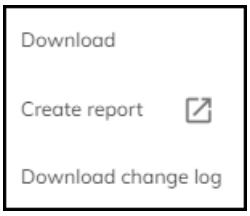
IoT Security 在网络上发现和识别的设备显示在 IoT Security 门户的“设备”页面上。

IoT Security 设备页面

在此页面 [**Assets**（资产） > **Devices**（设备）] 中，您可以查看已发现或正在监控的所有设备的清单以及应用于它们的设备配置文件。此页面有三个部分：用于控制其上显示的数据的过滤器、网络上设备的高级摘要以及设备清单表。



页面顶部是过滤器，用于控制按站点、监控状态（监控的设备或发现的设备）、设备类型和时间段显示的数据。同一组全局过滤器位于设备页面和指示板的顶部。当您导航至另一个部分时，在一个部分中设置的任何全局过滤器都会保留下来。这些过滤器控制显示什么和下载什么。单击 **Download**（下载）图标 ( )> **Download**（下载）。对于报告中的每个设备，IoT Security 包括所有清单表列的所有数据，无论它们在下载时是否可见。



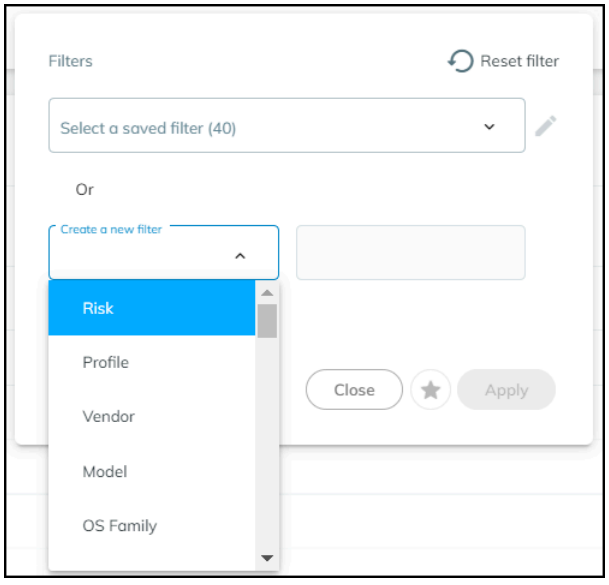
下载菜单中还有另外两个选项。单击 **Create report**（创建报告）将打开一个新的浏览器窗口或选项卡，您可以在其中配置以下类型的计划报告之一：摘要、风险、新设备和过滤清单。单击 **Download change log**（下载更改日志）并选择两个日期将生成一个 CSV 格式的文件，用于比较您选择的两个日期的设备清单变化。IoT Security 会检查并报告类别、配置文件、配置文件垂直、操作系统组、设备型号、IP 地址和子网等数据字段的变化。

单击饼图或单击表格中的内容可以查看多个粒度级别的设备数据。

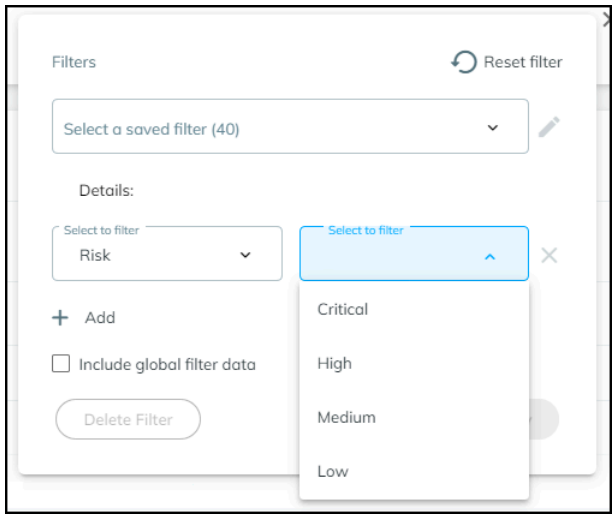
清单表的顶部是一个搜索工具，可让您搜索设备名称。您可以搜索全部或部分匹配。如果您采用一种命名约定，通过功能、位置或其他特征来识别所有设备，则可以通过特定分组中所有设备共享的名称部分进行搜索。

还有一个用于创建自定义过滤器的工具，可以控制 IoT Security 在清单表中显示的内容。要创建并应用新过滤器或应用之前创建的过滤器，请单击 **Filter**（过滤器）图标 ( )。

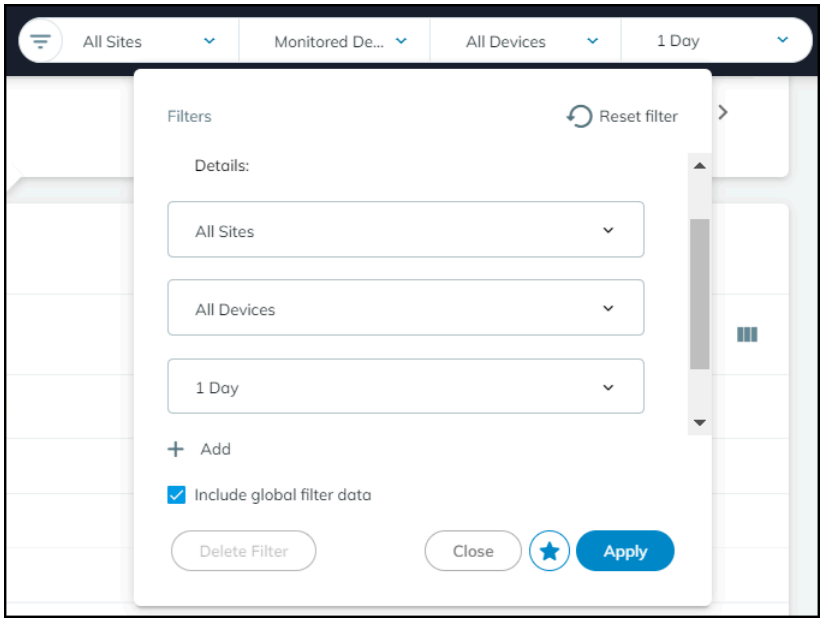
在出现的过滤器对话框中，选择之前定义并保存的过滤器，或者单击 **Create a new filter**（创建新过滤器）字段，然后选择要用于过滤设备的设备特征。



输入想要用于过滤设备的特征值。



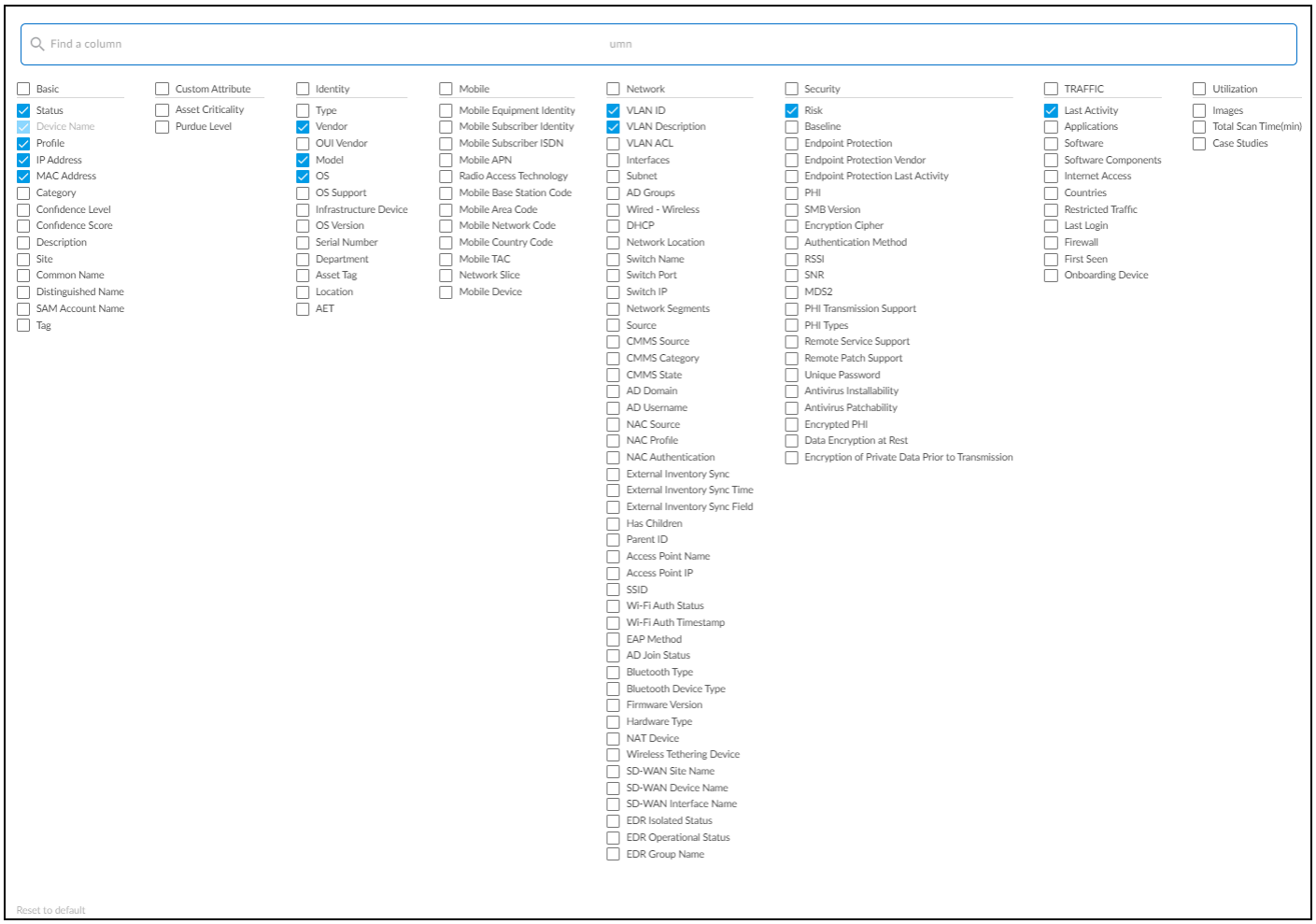
决定是否要在自定义过滤器中包含全局过滤器。当您选择 **Include global filter data**（包括全局过滤器数据）时，您可以在应用所定义的自定义过滤器时控制站点、设备类型和时间的全局过滤器。您的自定义过滤器可以使用当前全局过滤器，或者如果您在设置中修改它们，则可以使用修改后的全局过滤器。如果您未选择 **Include global filter data**（包含全局过滤数据），则您的自定义过滤器将使用您应用它时有效的任何全局过滤器。



单击星形图标可以保存过滤器以供将来使用。单击 **Apply**（应用）即可使用它来过滤清单表的内容。

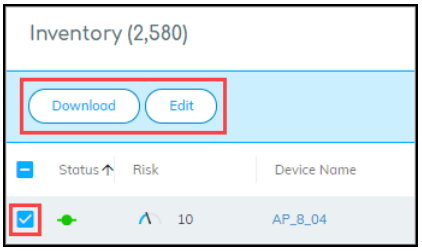
您可以通过单击并拖动列标题到不同的位置来重新排列设备清单表中的列。

您还可以更改表中显示的列。单击 **Columns**（列）图标（三条垂直线），选择要查看的列的名称，然后清除要隐藏的列。选中复选框的列会显示，清除复选框的列则会隐藏。使用搜索工具快速找到列标题。



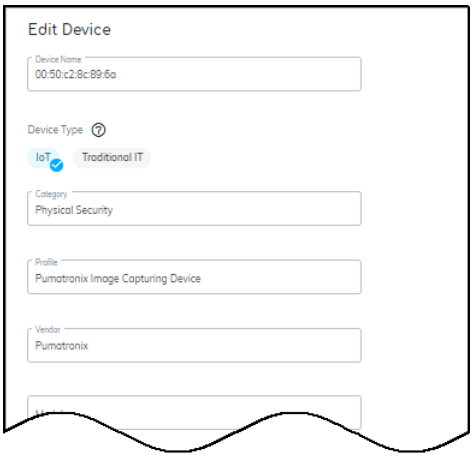
要返回默认的列集，请 **Reset to default**（重置为默认值）。

如果选中一个或多个设备的复选框，则会出现“下载”和“编辑”按钮。



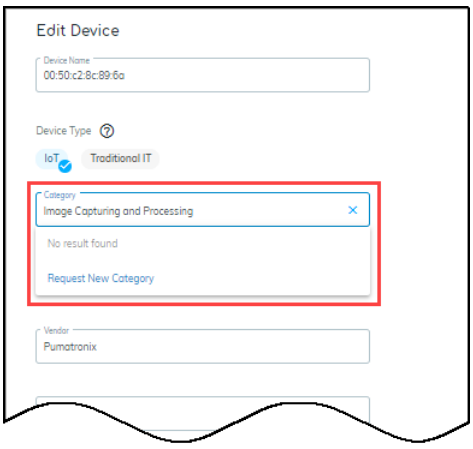
单击 **Edit**（编辑）时，将打开一个对话框，您可以在其中更改 IoT 和传统 IT 之间的设备类型并定义其他设备特征：类别、配置文件、供应商、型号、操作系统系列、操作系统版本、位置、资产标签、序列号、用户标签和描述。

当您手动编辑设备并更改其任何属性时，您的更改将被视为最终更改，并且不会被覆盖。因此，手动编辑设备时要小心，因为您正在锁定您的编辑。

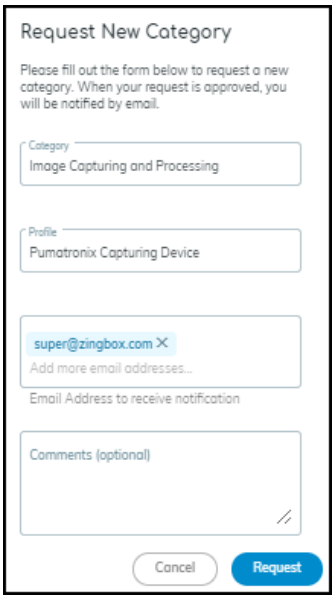


每当您手动编辑设备时，修改都会被输入到机器学习中。如果 IoT Security 确定输入有效后，它会使用添加或修改的数据重新训练其模型，并将结果传播给所有客户。然后，IoT Security 会将其修改后的模型应用于所有客户环境中同一类型的其他设备。

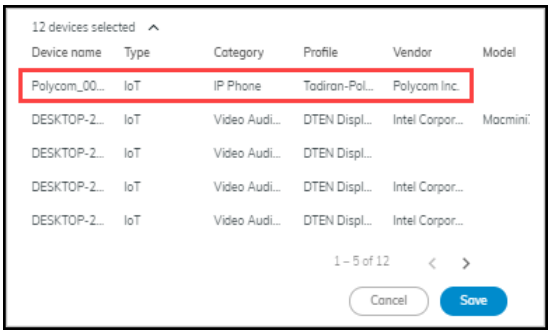
如果您在类别字段中输入内容，但不存在现有类别，则会出现“请求新类别”选项。



使用此选项请求 IoT Security 为该设备创建一个新类别。如果请求得到验证，则将添加该类别 — 不仅适用于提出请求的人，也适用于所有 IoT Security 客户。



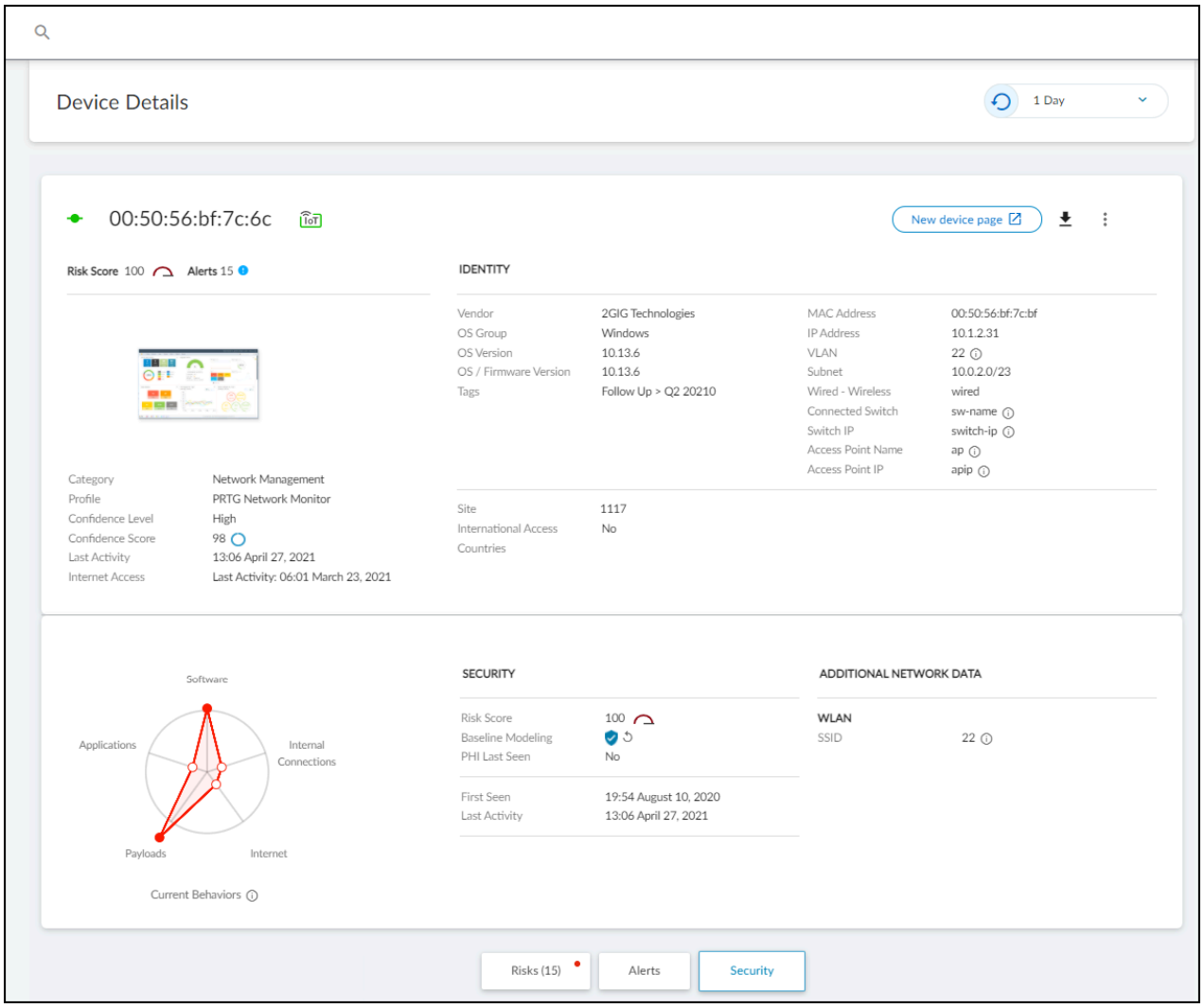
当您选择多个设备进行编辑时，对话框底部会出现一个表格以方便您编辑。其中显示您选择的当前值。如果您错误地选择了不想要的，可以在这里发现它。



IoT Security 设备详细信息页面

要查看有关设备的详细信息，请单击设备名称。然后，IoT Security 门户会显示设备详细信息页面，内容分为以下几个部分：

- 标识
- Active Directory 属性（启用 Cloud Identity Engine 集成时显示）
- 安全（摘要）
- 风险
- 警报
- 安全
  - 网络流量
  - 应用程序
  - 软件组件
  - 网络使用情况
- MDS2（用于医疗 IoT 设备）



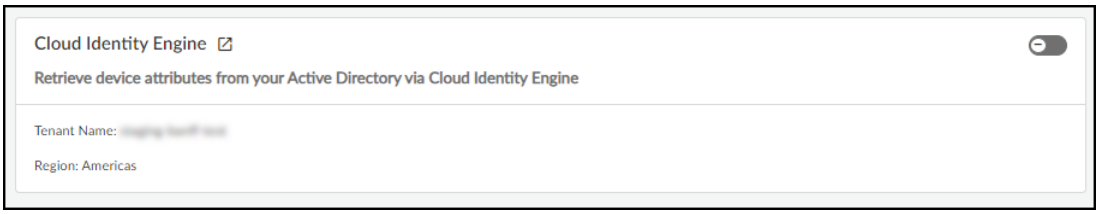
：页面顶部的身份部分提供识别数据，例如设备的类别和配置文件、其供应商和型号、其操作系统以及各种特定于网络的详细信息。

IoT Security 门户仅显示具有值的字段。根据 *IoT Security* 的信息量，您可能会看到比此处显示的更多或更少的详细信息。

Active Directory 属性（启用 Cloud Identity Engine 集成时显示）

如果您已将本地 Active Directory (AD) 与 Cloud Identity Engine (CIE) 同步，并且 CIE 租户与您的 IoT Security 租户位于同一租户服务组 (TSG) 中，您可以将 IoT Security 与 CIE 集成。通过此集成，您可以识别 IoT Security 发现的设备 — 它是您的 AD 的一部分，并收集一些 AD 属性以显示在设备详细信息页面上。要仅查看 Active Directory 中的设备，您可以根据设备的 AD 加入状态来过滤和搜索清单中的设备。

要将 IoT Security 集成 CIE 集成，请以具有所有者权限的用户身份登录 IoT Security 门户，选择 **Integrations**（集成） > **Cloud Identity Engine Integration**（云身份引擎集成），然后打开集成。切换按钮位于页面的右上角。



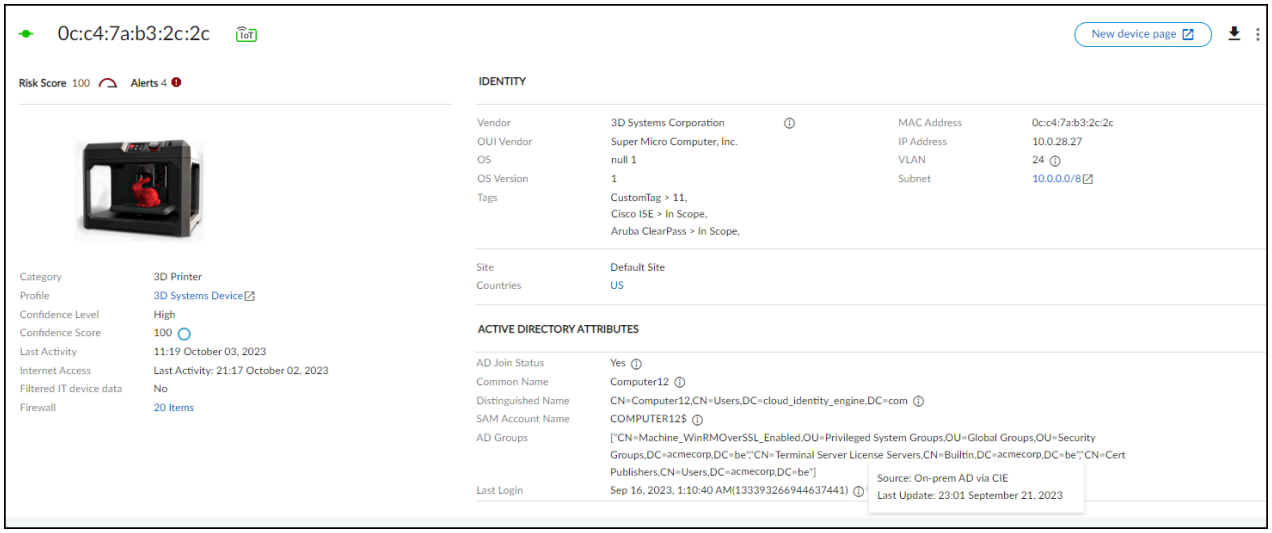
外部链接图标 (⧉) 会打开您的 *CIE* 租户的门户。

因为 IoT Security 从 Hub 了解 CIE 租户是否是其 TSG 的一部分，它将允许您启用集成，如果 IoT Security 和 CIE 都是同一个 TSG 中的租户，如果不是，则切换将无法操作。假设您可以启用集成，IoT Security 仅在第一次或上次同步超过 24 小时后才会立即检索 Active Directory 属性，然后每 24 小时进行一次每日检索。（如果距离上一次同步少于 24 小时，则关闭并重新打开集成不会触发新的同步。）当您启用切换按钮时，IoT Security 会连接您的 CIE，并开始根据 CIE/AD 数据库匹配设备，以识别哪些设备在您的 AD 中。匹配过程使用 AD 中的通用名称对 IoT Security 中的设备名称进行比较。对于 AD 中的设备，IoT Security 还检索以下属性以显示在设备详细信息页面上：

从 *Active Directory* 中获知的设备属性	
AD 域	OS
通用名称（IoT Security 在与 IoT Security 中的名称匹配的 Active Directory 中查找与设备名称匹配的通用名称。当找到匹配项时，IoT Security 随后从 Active Directory 检索设备属性。	操作系统版本
专有名称	OS 服务包

安全帐户管理器 (SAM) 帐户名称	序列号
AD 组	上次登录（这是设备最后一次向 AD 进行身份验证的时间。它来自 AD lastLogon 属性。）

启用 CIE 集成后，这些属性将显示在 **Assets**（资产） > **Devices**（设备）页面的列中以及设备详细信息页面的 Active Directory 属性部分中。IoT Security 将通过 CIE 集成（作为通过 **CIE** 的本地 **AD**）显示从 Active Directory 中了解的属性来源。



对于大多数设备属性，IoT Security 使用它所了解的最新值，无论它是通过网络流量还是通过集成发现。但是，通过网络流量了解到的值有八个属性具有优先权，即使 IoT Security 后来通过集成了解到了不同的值：

通过网络流量获知的设备属性值优先于稍后通过集成获知的值。	
模型	固件
供应商	序列号
OS 群组	有线或无线
OS 版本	vlan

如果 IoT Security 了解到其中一个属性的冲突值，它首先优先考虑通过网络流量了解到的值，然后才是通过集成（包括 CIE 集成）了解到的值。基本逻辑如下：

- 通过网络流量了解到的任何新值都会取代以前通过任何方式了解到的值。
- 通过集成了解的新值将取代通过相同类型的集成了解的先前了解的值。它不会取代通过网络流量或其他类型的集成了解的值。

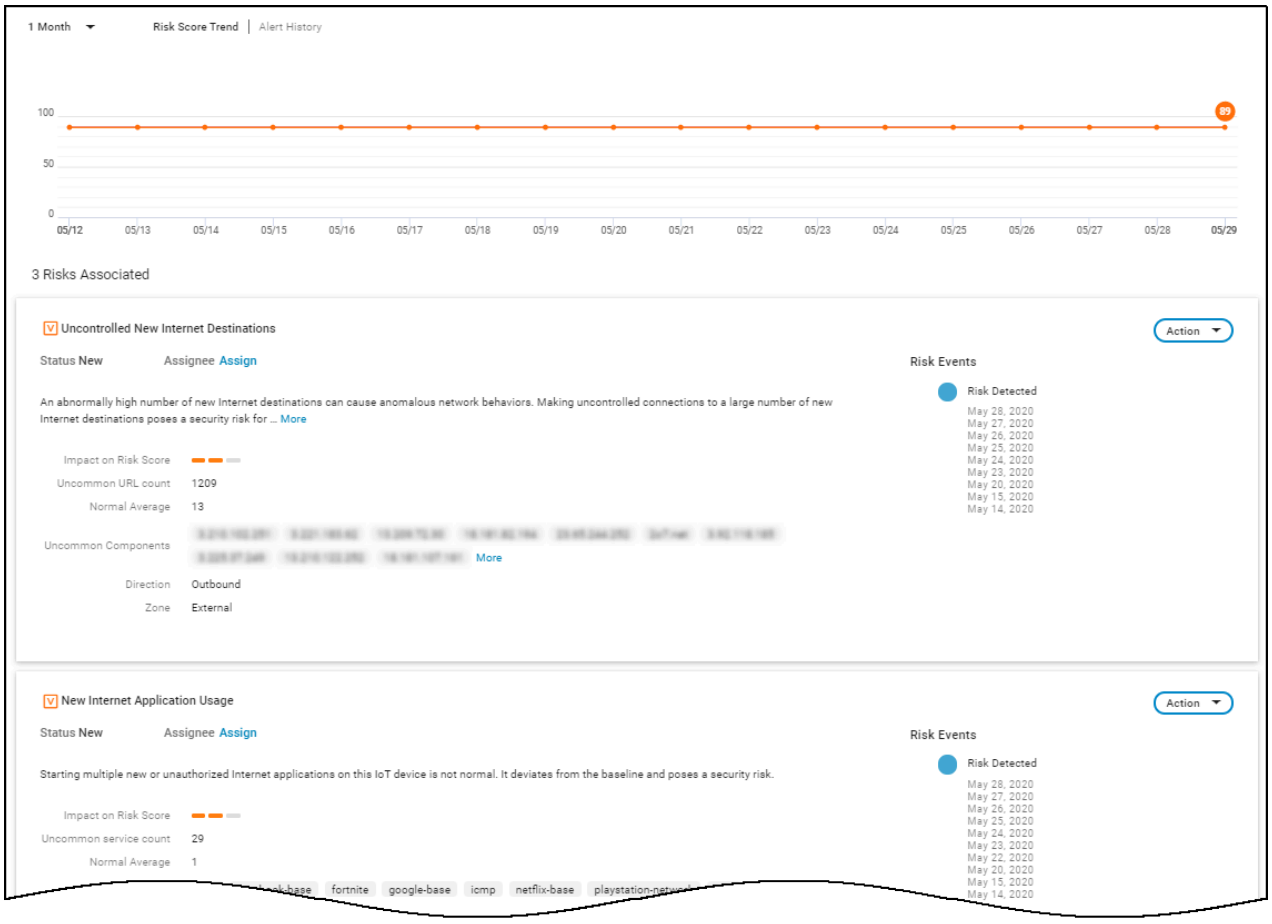
安全性（摘要）：下一节中的信息与安全性有关，包括设备的单独风险评分以及基线建模是否完成或仍在进行中。当前行为图显示了对五种行为类型的评估，从正常（靠近中心）到异常（靠近或超出边缘）。

当设备详细信息页面针对的是医疗设备时，IoT Security 有一个 MDS2 文件，它显示从文件中了解到的设备功能和操作状态的信息，例如：

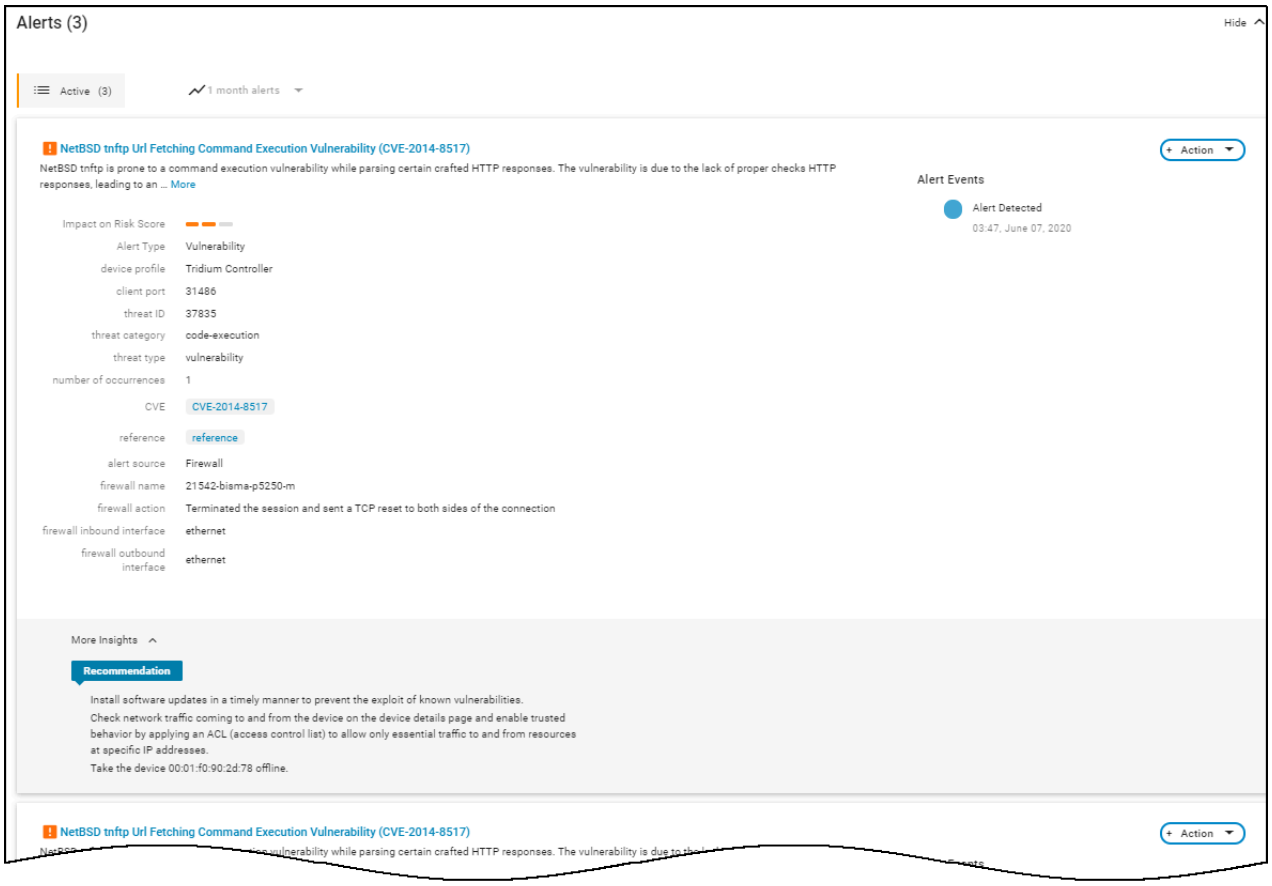
- 远程服务和补丁支持
- 个人健康信息 (PHI) 类型和传输支持
- 防病毒可安装性和可修补性
- 数据存储和加密
- 是否禁用了不必要的应用程序和端口
- 本地网络内外的设备通信
- 支持外部用户身份验证

IoT Security 使用 MDS2 文件中列出的属性来调整设备的基线风险级别。基于 MDS2 属性的风险因素构成了整体设备风险评分的一部分。

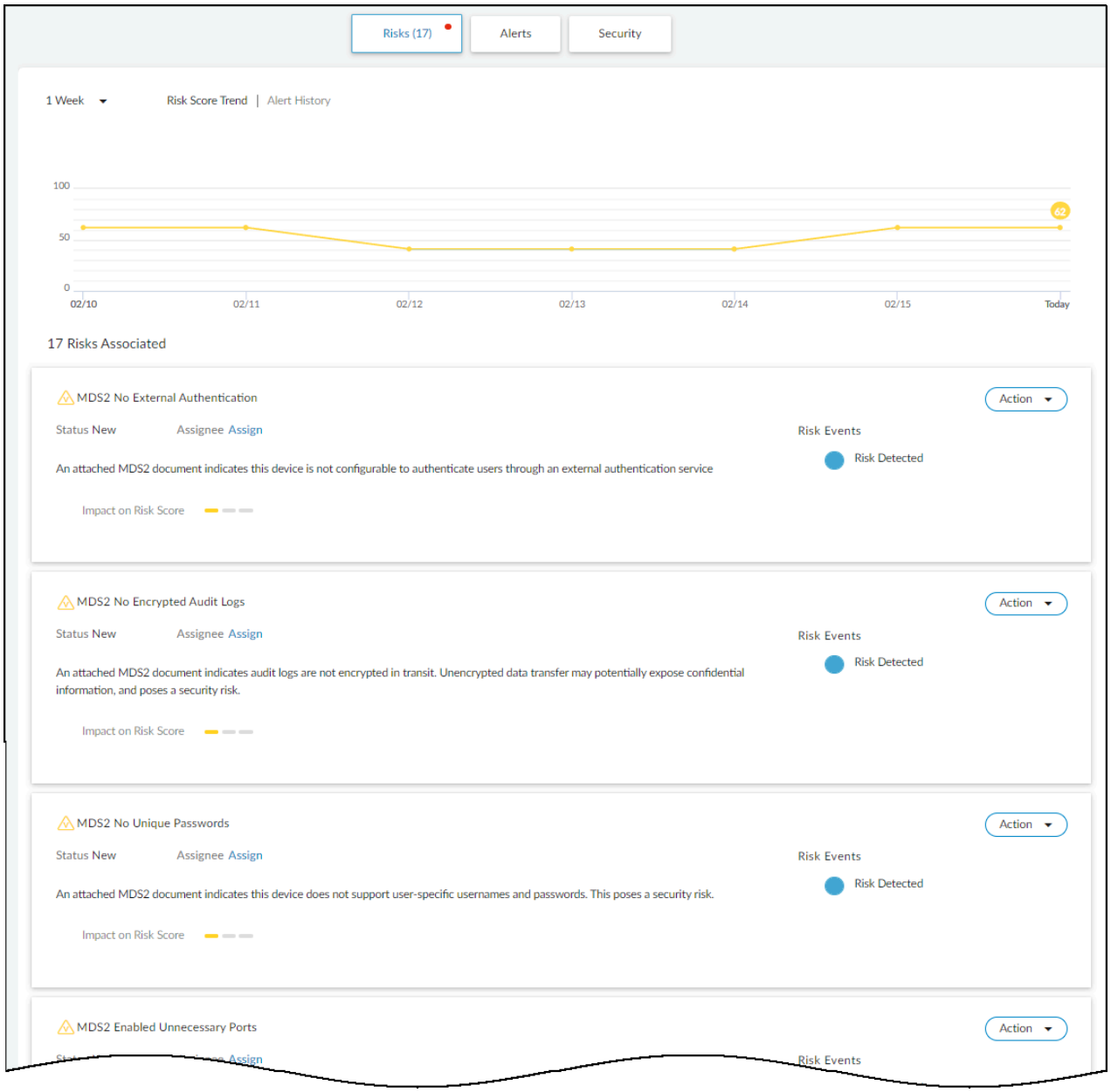
风险：风险部分包含页面顶部设置的时间范围内设备发生的警报、漏洞和异常。事件按时间线显示，并以列表形式显示，其中包含每个事件的详细信息。



当 IoT Security 对应对风险有建议时，它会显示更多见解。单击以展开该部分，并阅读有关风险对设备和网络的影响以及如何解决它的更多信息。



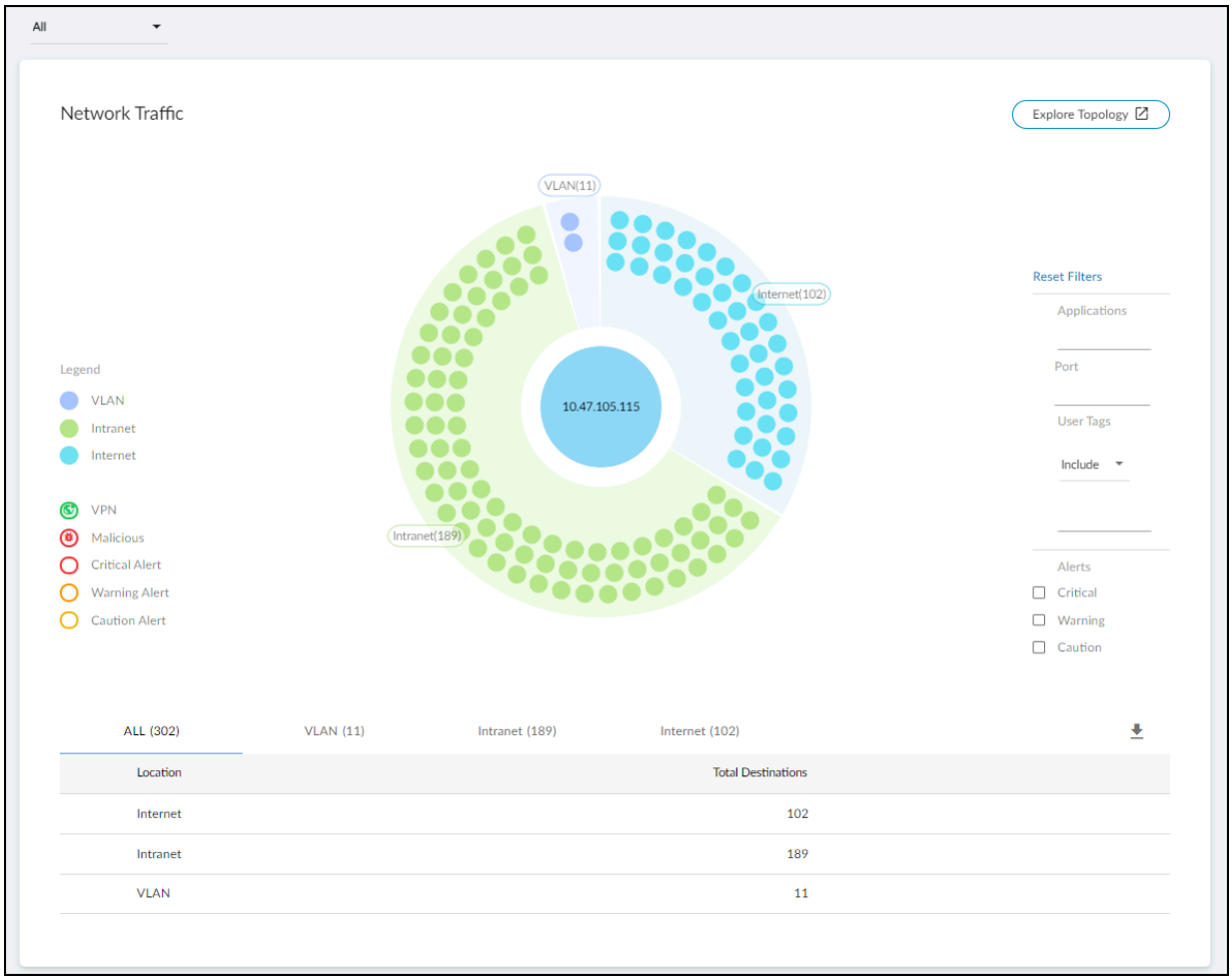
对于页面顶部附近总结的具有 MDS2 风险的医疗 IoT 设备，这里也列出了这些风险以及更多详细信息。IoT Security 在检测到任何其他漏洞之后显示它们。



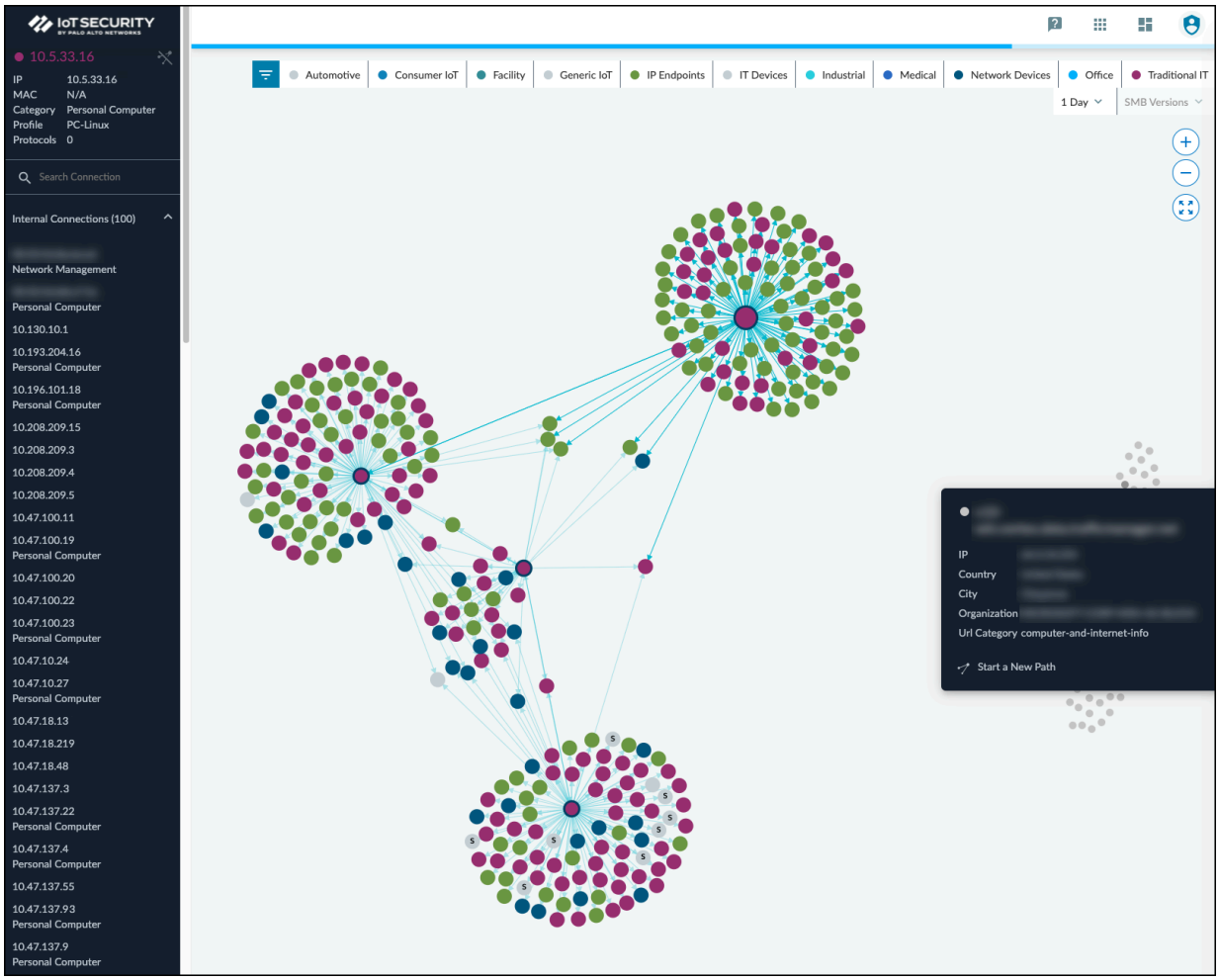
警报：此部分仅包含设备在指定时间范围内发出的警报。警报是风险的一部分，并且 IoT Security 在检测到与警报规则匹配的异常行为和活动时就会生成它们。您可以查看时间线上警报的发生时间、阅读有关警报的详细信息并采取措施解决警报。

安全：安全部分包含三个小节，展示设备如何连接到网络上的其他设备以及它正在使用哪些应用程序。

- 流量：查看概念网络拓扑，其中显示设备已形成连接的节点。使用过滤器显示入站或出站连接；具有各种警报级别的节点；到同一 VLAN、同一内联网或 Internet 中的节点的连接；等等。



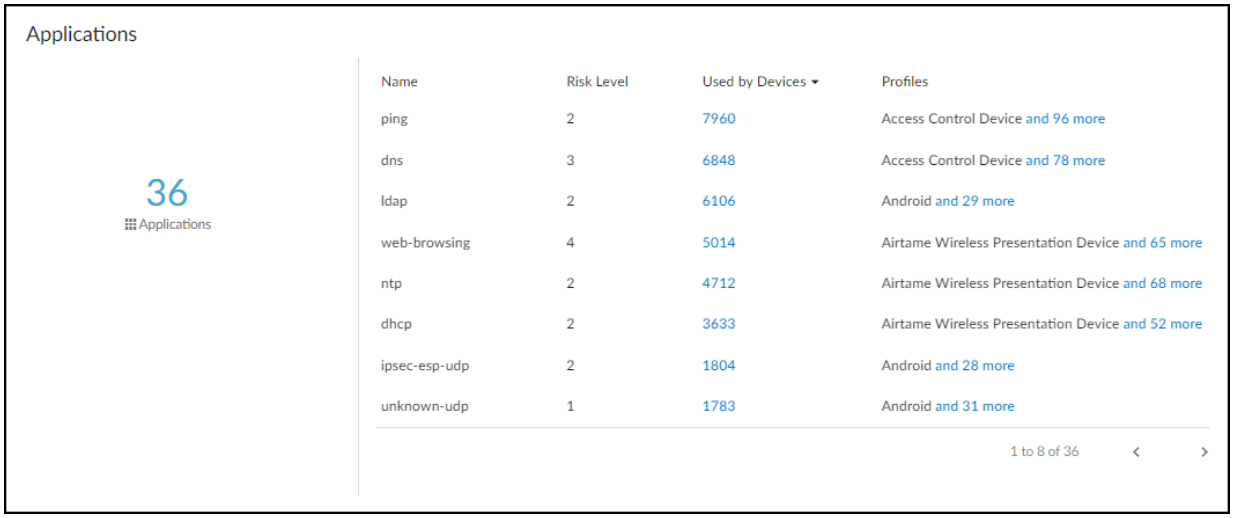
如果单击浏览拓扑结构，则会打开一个新的浏览器窗口，其中显示焦点设备的内部和外部连接的信息。您可以与信息进行交互，查看有关每个节点的详细信息，并单击不同的节点以聚焦它们并查看它们的连接。



任何带有“S”的节点都是服务器。

要了解更多信息，请观看拓扑浏览器的一对视频说明。第 1 部分涵盖导航、信息弹出窗口、缩放、设备类别过滤器和 SMB 过滤器。第 2 部分介绍信息面板、如何浏览拓扑结构以及如何开始新路径。每个视频大约两到三分钟长。

- 应用程序：此部分显示设备使用的应用程序、其风险级别（1-5 的等级，数字越接近 5 表示风险越高）以及有多少其他设备和设备配置文件使用相同的应用程序。单击“设备所用”列中的数字可打开“设备”页面，其内容按相应的应用程序进行过滤。将光标悬停在“配置文件”列中条目的蓝色文本上将显示使用该应用程序的所有配置文件的列表。



- 软件组件：大多数软件都使用各种第三方软件组件，例如库、模块、二进制文件、编译器、可执行文件、文件和源代码。在国家电信和信息管理局主导以及众多制造商参与的软件组件透明度倡议的推动下，这些组件的详细信息越来越多地被记录在软件材料清单中。软件材料清单 (SBOM) 是一种全面的记录，详细说明系统或设备内的所有软件部分及其相互关系。它本质上是软件组件和子组件的嵌套清单，包括固件和嵌入式软件。它通常还包括许可、作者和版本信息以及其他元数据。目的是尽可能提高设备上运行的软件内容的透明度，以便我们更好地保护它们免受攻击。

  一些漏洞专门利用了透明度的缺乏以及针对 Spring4Shell、Urgent/11、Ripple20 和 Log4j 2 等软件组件中出现的漏洞。了解设备上有哪些软件组件可以加快漏洞检测、风险分析和补救工作。例如，Log4j 2 漏洞影响 Apache Log4j 2 Java 日志库的特定版本，该库是一个基于 Java 的开源日志框架，被世界各地的 Java 应用程序使用。攻击者可以利用此漏洞发起拒绝服务攻击或

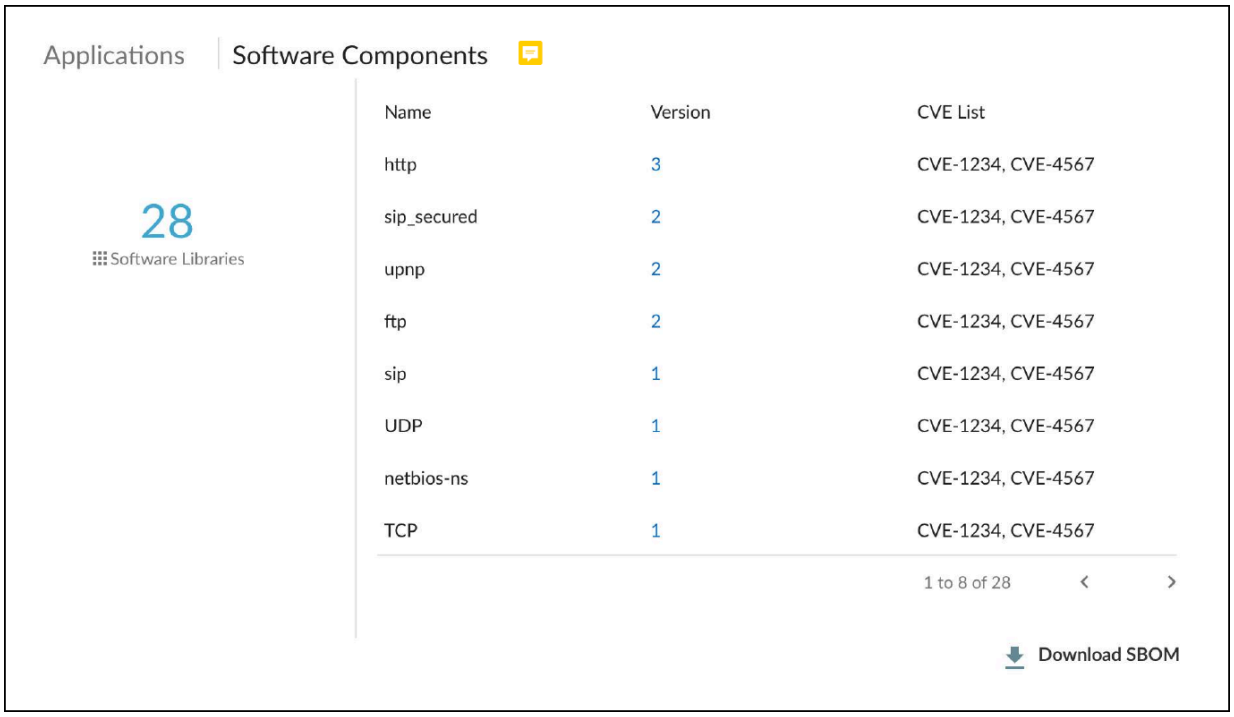
获取目标设备的远程控制权。应对此威胁的第一步是确定哪些设备使用 Log4j 2 Java 日志库，如果是，则确定它是否是易受攻击的版本。凭借 IoT Security，您只需花几秒钟的时间就可以在清单中搜索使用此特定库和版本的设备，或搜索易受一个或多个相关 CVE 攻击的设备，从而节省几天甚至几周的响应时间。

IoT Security 主要从流量检查（例如 HTTP 标头中的用户代理字段）中了解 SBOM 信息，并在较小程度上从其他来源（如 FTP 横幅和 HTTP URL 信息）中了解。然后，它会在“设备”页面

的“软件组件”列中显示设备 SBOM 中标识的软件组件和版本号。IoT Security 还会在“设备详细信息”页面的“软件组件”部分中显示软件组件名称、版本号和任何相关的 CVE。

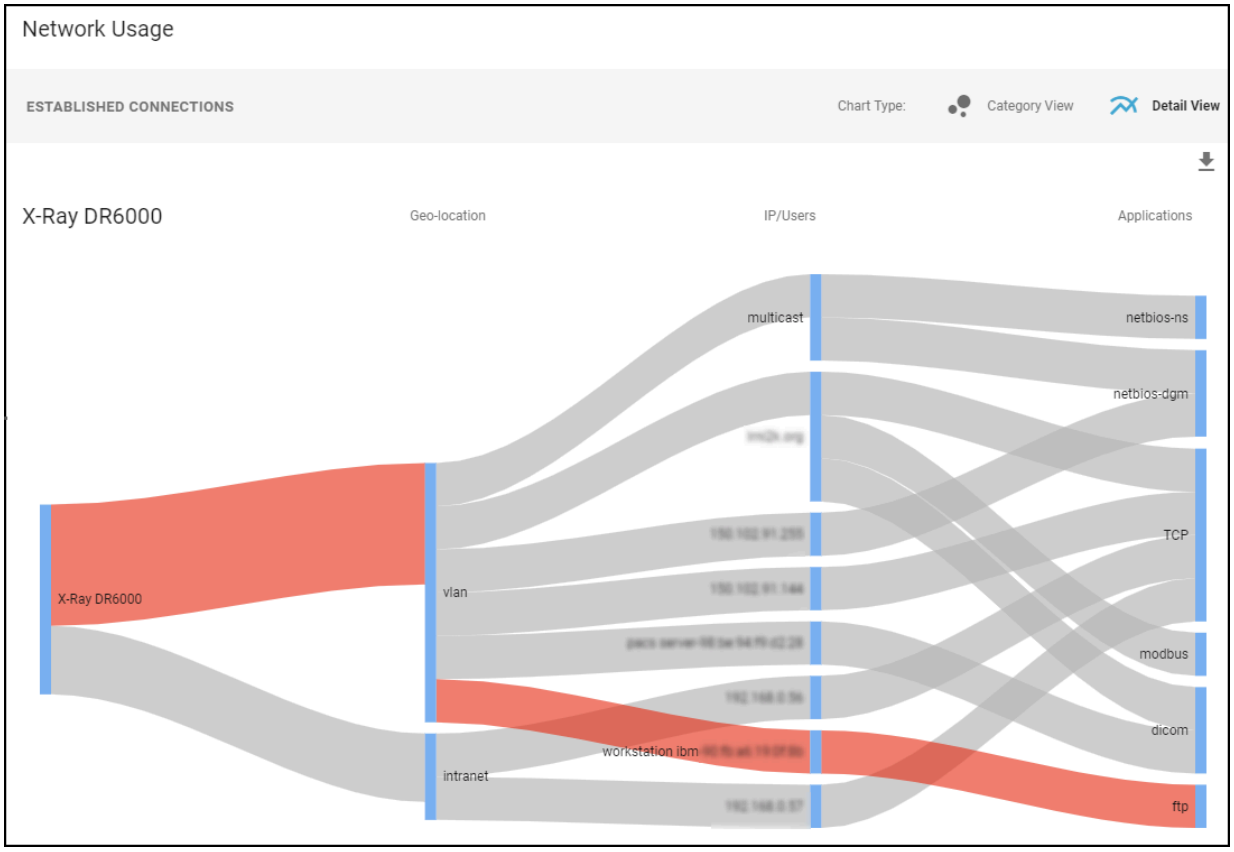
您可以从设备页面下载设备清单报告。该报告包含 IoT Security 检测到的所有设备的软件组件名称和版本号列表。

您还可以使用软件包数据交换 (SPDX) 格式下载单个设备的软件库详细信息，这是捕获 SBOM 数据的最常见数据标准之一。要下载 SPDX 文件，请单击软件组件部分底部的 **Download SBOM**（下载 **SBOM**）。然后，您可以使用任何标准文本编辑器打开并读取 SPDX 文件。



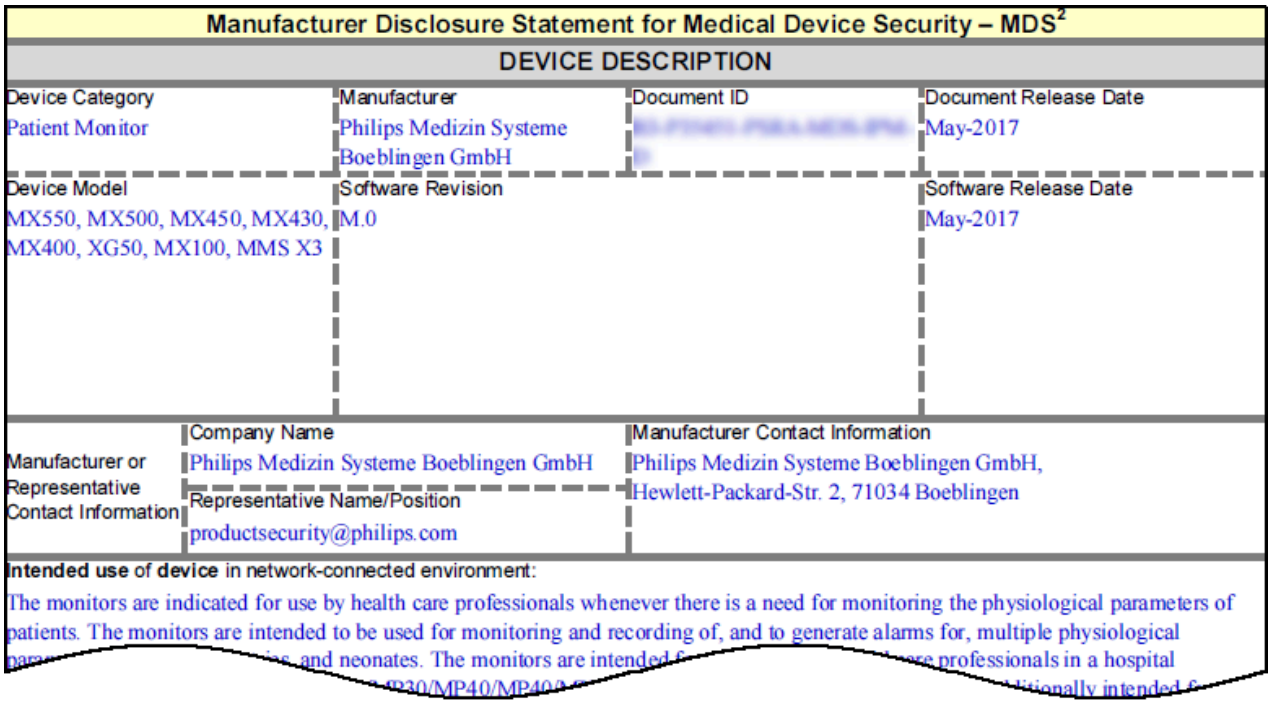
IoT Security 了解的数据量仅限于设备通过网络发送的 *SBOM* 信息以及可从网络流量中提取的信息。

- 网络使用情况：最后部分展示了一个桑基图，其中的线条表示网络连接。红线表示它涉及高严重性警报。单击其中一个蓝色条，然后单击出现的 **Create Policy**（创建策略）选项以创建一个策略，其中策略编辑器中会自动填充以下字段：(“Group #1” = source, and “Group #2 = destination)。



MDS2（用于医疗 IoT 设备）

医疗设备供应商通常会在医疗设备安全制造商披露声明 (MDS2) 中列出其产品的安全相关特性，并与客户分享。供应商为每个版本的医疗设备发布这些 MDS2 文档，其中包含有价值的信息，例如设备是否处理 PHI（个人健康信息）；是否存储 PHI；如果是，是否加密；以及设备上是否安装了防病毒软件。



Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Patient Monitor	Philips Medizin Systeme Boeblingen GmbH	[redacted]	May-2017

Device Model	Software Revision	Software Release Date
MX550, MX500, MX450, MX430, MX400, XG50, MX100, MMS X3	M.0	May-2017

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information	Philips Medizin Systeme Boeblingen GmbH	Philips Medizin Systeme Boeblingen GmbH, Hewlett-Packard-Str. 2, 71034 Boeblingen
	Representative Name/Position productsecurity@philips.com	

Intended use of device in network-connected environment:

The monitors are indicated for use by health care professionals whenever there is a need for monitoring the physiological parameters of patients. The monitors are intended to be used for monitoring and recording of, and to generate alarms for, multiple physiological [illegible] and neonates. The monitors are intended f[illegible] professionals in a hospital [illegible]P30/MP40/MP40 [illegible] additionally intended f[illegible]

[illegible]s are only [illegible] home use. The[illegible] prescription use only.

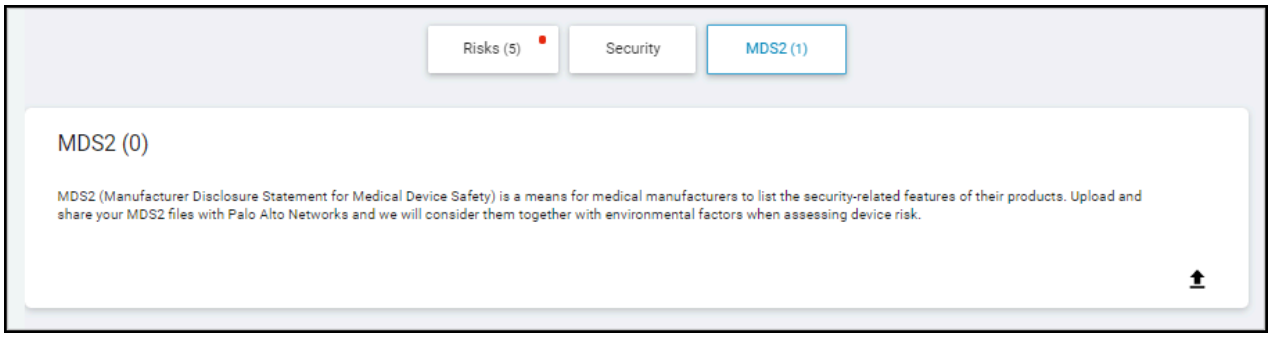
MANAGEMENT OF PRIVATE DATA

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?	[redacted]	
B	Types of **private data** elements that can be maintained by the **device**:		
B.1	Demographic (e.g., name, address, location, unique identification number)?	[redacted]	
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	[redacted]	
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	[redacted]	
B.4	Open, unstructured text entered by **device user/operator**?	[redacted]	1
B.5	**Biometric data**?	[redacted]	
B.6	Personal financial information?	[redacted]	
C	[illegible]ata - Can the **device**:		
	[illegible]arily in volatile mem[illegible]	[redacted]	

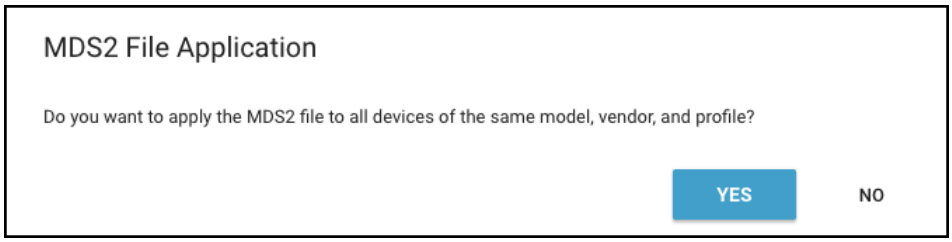
随着时间的推移，医疗保健提供者可以收集数千种医疗设备的数千份 MDS2 文档。按照预期使用时，MDS2 文档可以极大地增强您的安全态势和事件响应 (IR)。然而，从这些文档中获取有关在其连接的设备上运行的软件的特定版本的详细信息是一项艰巨的任务。因此，MDS2 文件经常被闲置。

IoT Security 简化您拥有的 MDS2 文件的管理和使用。如果您将设备的 MDS2 文件上传到 IoT Security，然后，它会在评估设备风险时将这些数据与其他环境因素一起纳入其中。例如，如果 MDS2 文件中指定的设备的软件版本存在已知漏洞，IoT Security 可以更准确地将其识别为一个漏洞，而不仅仅是一个潜在的漏洞。IoT Security 支持 2004、2008、2013 和 2019 格式的 MDS2 文件。

要上传您的某个医疗设备的 MDS2 文件，请单击设备详细信息页面上的 MDS2 按钮，单击右下角的上传图标，然后导航到您的 MDS2 文档（其格式必须为 PDF）并上传。

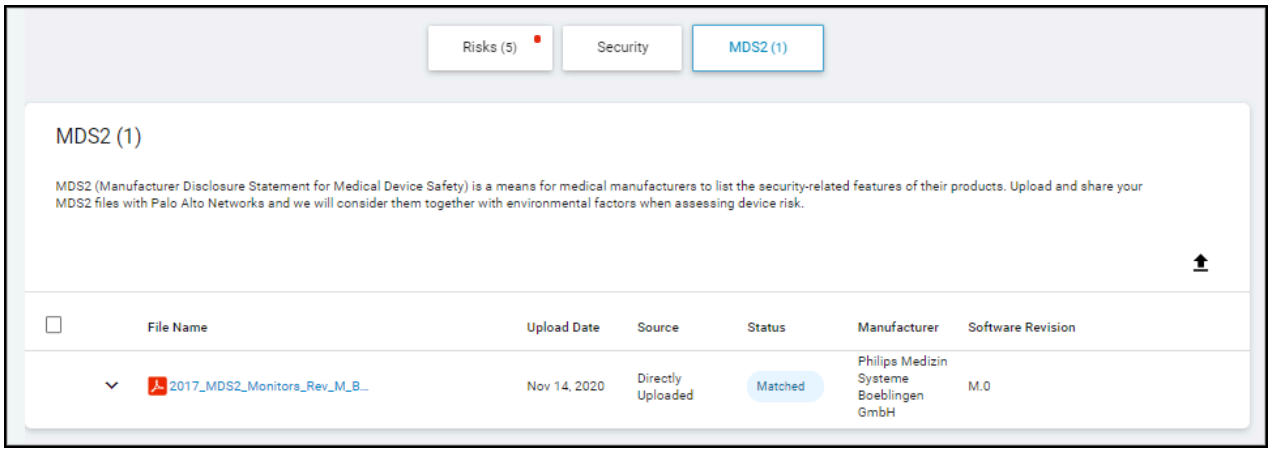


随即会出现提示，将 MDS2 文件应用于所有共享相同型号、供应商和配置文件的设备。要将 MDS2 文件应用到所有具有相同属性的设备，请单击 **Yes**（是）。要将其仅应用于此特定设备，请单击 **No**（否）。



要上传 *MDS2* 文件并自动将其应用于具有匹配型号、供应商和配置文件属性的所有设备，请使用 ***Administration***（管理）> ***MDS2*** 上的上传选项。有关详细信息，请参阅MDS2。

上传的 MDS2 文件的条目会出现在“设备详细信息”页面的 MDS2 部分，其中包含一些上传详细信息、设备制造商名称和软件修订号（如果有）。此外，如果在提示您将 MDS2 文件应用到具有相同型号、供应商和配置文件的其他设备时选择 **Yes**（是），并且存在这样的设备，则 IoT Security 会将上传的 MDS2 文件也应用于它们。



上传日期显示此文件已上传至 IoT Security。

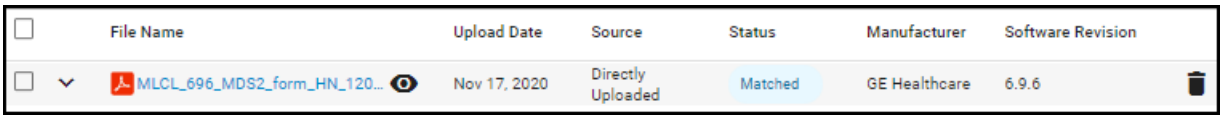
时间戳使用“首选项”页面中指定的时区（ > 首选项）。

上传的 MDS2 文件的来源始终是 **Directly Uploaded**（直接上传的），这意味着用户手动将文件上传到 IoT Security。

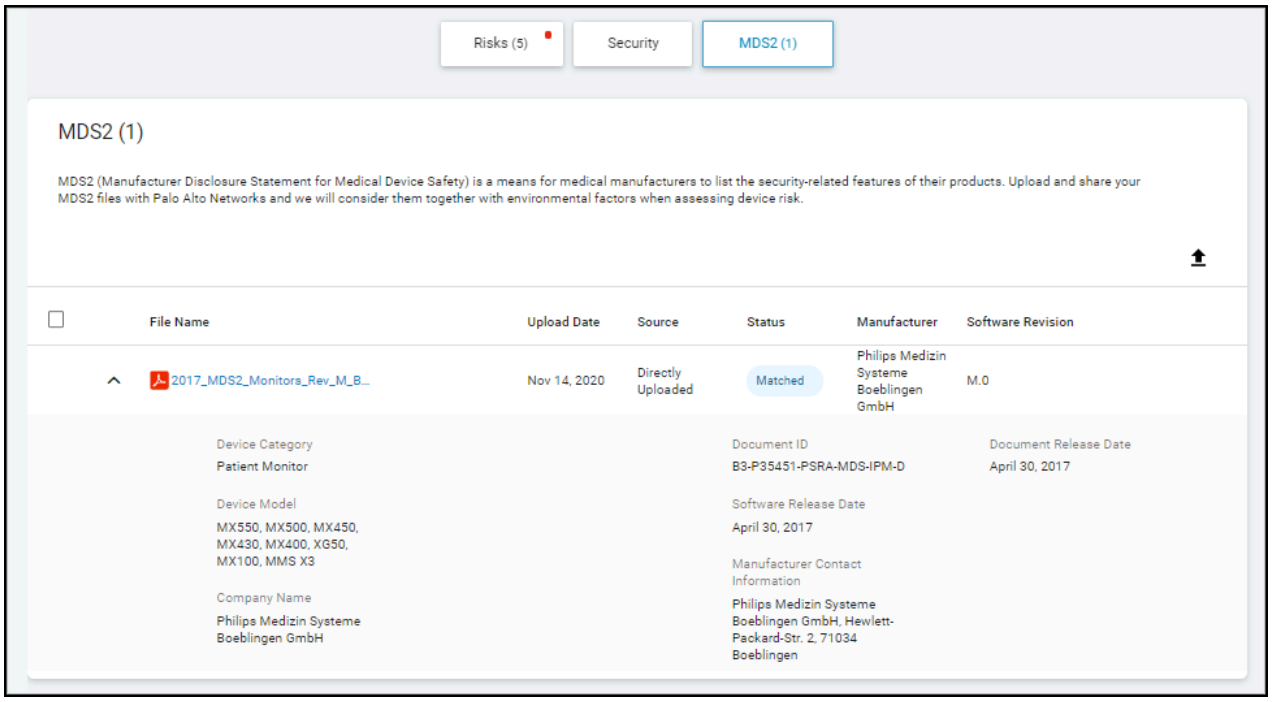
已上传文件的状态指示以下状态之一：

- **Matched**（匹配） — 上传的文件是包含正确格式字段的 PDF
- **Cannot Extract Data**（无法提取数据） — 该文件是 PDF，字段格式不正确
- **Unsupported File Type**（不支持的文件类型） — 上传的文件不是 PDF

如果文件状态为最后两种状态之一，请将光标悬停在包含 MDS2 文件的表格行上，然后单击最右侧显示的删除图标 ( )。

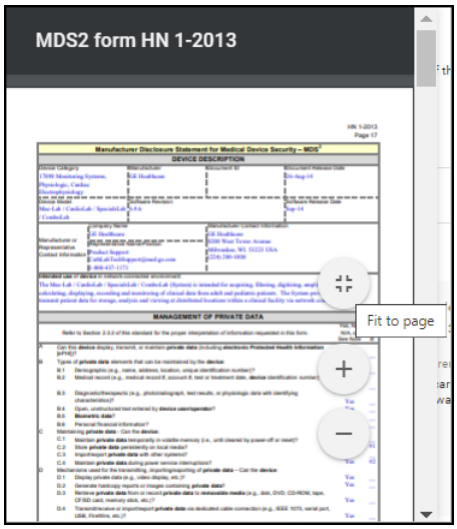


要查看有关设备和 MDS2 文件的更多详细信息，请展开该行。



制造商可能会发布更新的 MDS2，也许是为了在设备型号列表中添加更多型号、更改其制造商联系信息，或者出于其他原因。如果是，请删除第一个 MDS2 文件，然后上传新文件。

要查看 MDS2 文件的预览，请将光标悬停在其表格行上，随即会出现预览图标 ( )。单击该图标或将光标悬停在它上面即可在弹出预览窗口中查看该文件。



使用查看选项滚动浏览文件并放大和缩小。

要查看文件本身，请单击文件名。IoT Security 会下载 PDF 文件，以便您可以在本地打开并查看。

IoT Security 使用 MDS2 表单中的几个字段进行风险检测：

- 该设备可以显示、传输或维护私人数据吗？
- 设备可以维护哪些类型的私有数据元素？
- 可以远程安装安全补丁或其他软件吗？

这些问题的措辞在 *MDS2* 的不同版本中有所不同。

这些信息可以帮助 IoT Security 评估风险。例如，如果 MDS2 文件指出某台设备不支持远程服务，并且 IoT Security 检测到来自外部源的入站连接，它会将其标记为异常行为并生成安全警报。类似地，如果 MDS2 文件指出设备无法进行远程修补，则任何从外部位置尝试的入站文件传输也将被视为异常并触发警报。

创建多接口设备

某些设备有多个网络接口。这些设备可以是具有多个网络端口的 L3 交换机和防火墙等网络和安全设备，也可以是可以同时连接到有线网络和无线网络的物理终端设备（如打印机）。

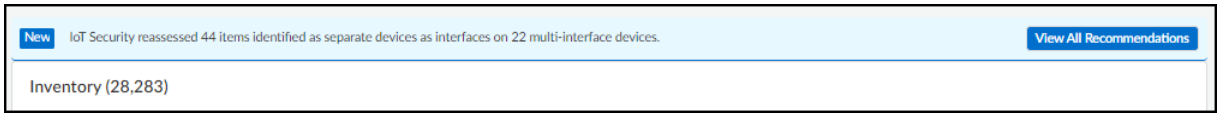
由于多接口设备上的每个接口都有自己的 MAC 地址和 IP 地址，IoT Security 最初将每个接口视为单独的单接口设备。这可能导致资产清单中出现重复设备和重复漏洞。当 IoT Security 检测到具有共同属性（如主机名或序列号）的两个或多个设备时，它会建议您将它们分组为同一多接口设备上的不同接口。除了按原样接受建议外，您还可以修改或忽略建议，而合并其他设备。合并过程包括分配一个“设备”作为主接口，并将其他设备作为辅助接口。执行此操作时，IoT Security 会将主接口的设备级属性应用于整个多接口设备，同时保留每个接口的网络级属性。

设备级属性最初从分配为主接口的设备学习，然后应用到所有合并接口	最初在每个以前未合并的设备上学习并为合并设备上的接口保留的网络级别属性
类别	IP 地址
设备名称	MAC 地址
端点保护（供应商）	OUI 供应商（NIC 供应商）
模型	站点
OS 群组	状态（网络连接）
操作系统组合（操作系统组 + 操作系统版本）	子网
患者健康信息支持（仅限Medical IoT）	切换
配置文件	标记
风险程度	无线接入点
风险评分	vlan
序列号	除了 CMMS（计算机化维护管理系统）、EDR（端点检测和响应）和外部清单之外的所有网络属性
类型	除以下各项外的所有通信属性：软件、软件组件和受限流量。
供应商	–

在单个设备合并成为单个设备上的接口时，这些属性会分配给多接口设备。合并后，它们可以根据 IoT Security 观察到的网络行为继续更改。IoT Security 还会合并漏洞、安全警报、风险评分和以前分离的设备的报告，因为它们成为一台设备上的接口。

将设备合并为多接口设备

您可以根据 IoT Security 的建议，将一个或多个设备合并为单个多接口设备，或创建自己的多接口设备（无需建议）。IoT Security 具有建议时，它会在 **Assets**（资产） > **Devices**（设备）页面上的“清单”表上方显示一条通知。



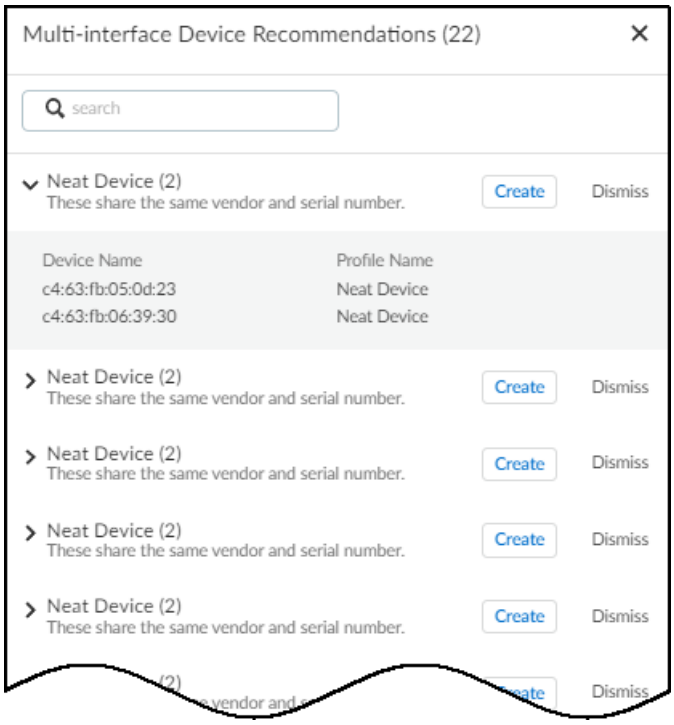
STEP 1 | 查看 IoT Security 建议合并为多接口设备的两个或多个单接口设备的组。

1. 要查看列表，请单击清单表上方的 **View All Recommendations**（查看所有建议）。

   设备页面右侧将打开一个面板，显示 IoT Security 建议合并在一起的所有设备以及每个建议的原因。

2. 单击建议左侧的箭头以查看要合并的各个设备。

   IoT Security 显示建议合并为一个多接口设备的每个单接口设备的名称和配置文件。

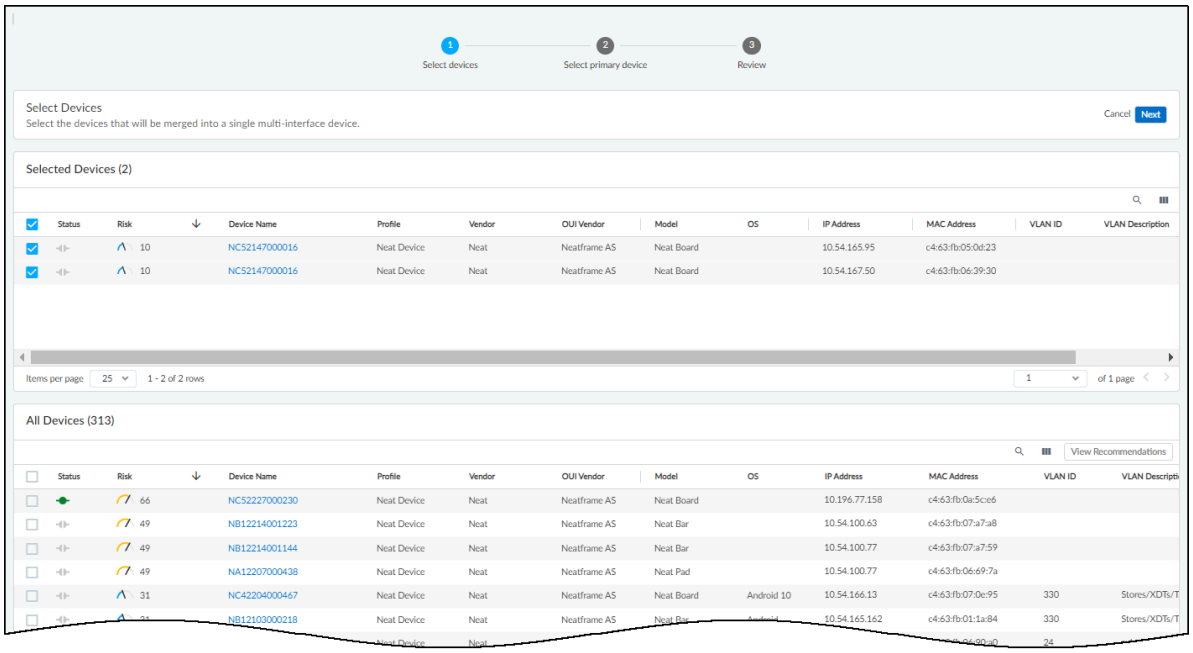


单击 **Create**（创建）可启动合并过程。单击 **Dismiss**（解除）将永久解除建议。但是，如果被驳回的建议发生更改（将设备添加到原始建议中或从中删除）IoT Security 将提出修订建议。

STEP 2 | 将单个设备合并为单个多接口设备。

1. 对于要创建的多接口设备，单击 **Create**（创建）。

   这将启动一个三步过程，第一步是选择要合并的设备。IoT Security 选择的设备显示在"所有设备"部分中其他设备上方的"已选设备"部分。

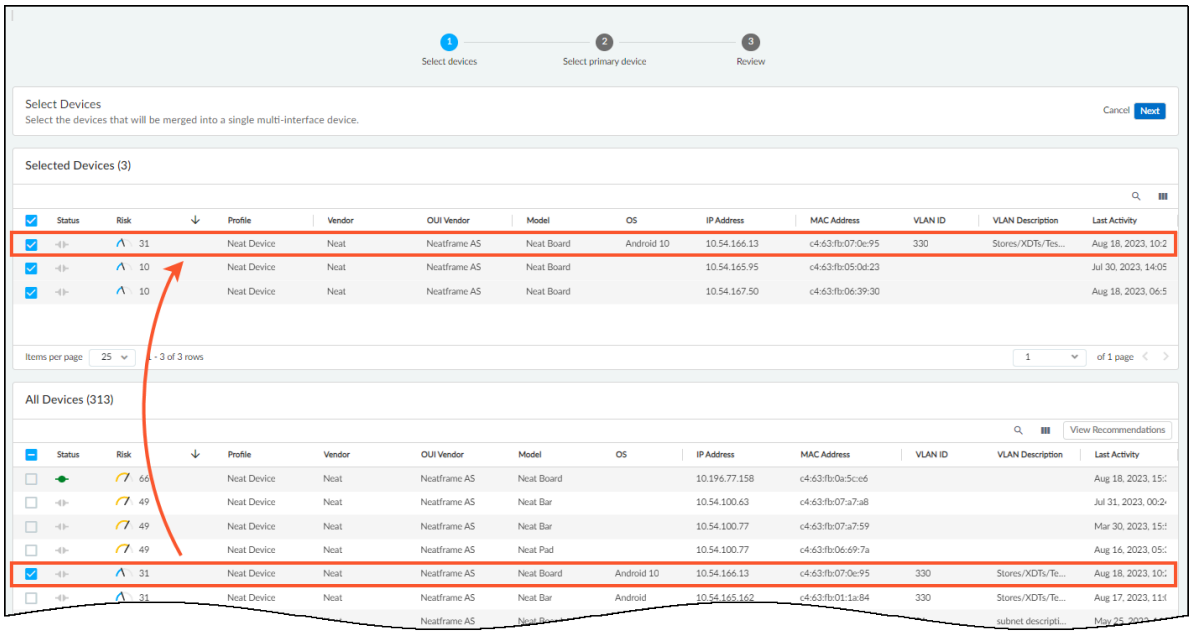


2. 如果要将 IoT Security 推荐的设备包括在多接口设备中，请保持选中状态，清除任何要排除的设备，如果认为还应包括这些设备，请从"所有设备"表中添加更多设备。

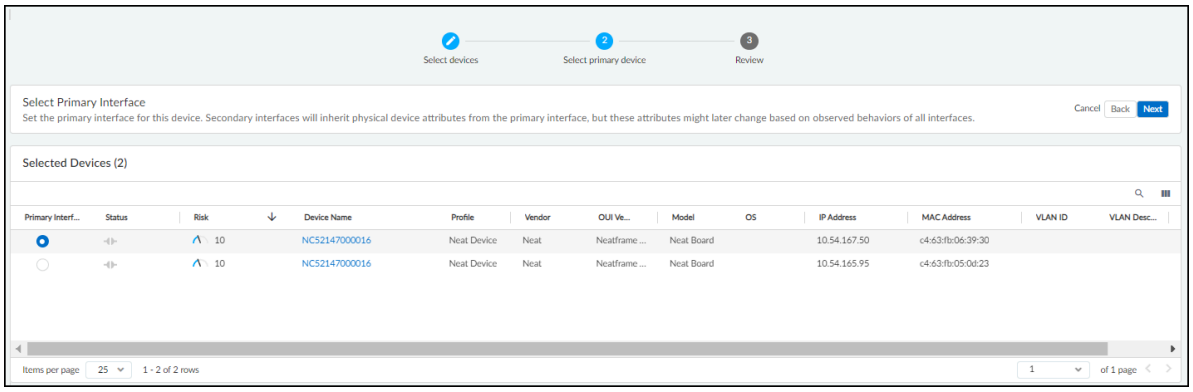
   您在“所有设备”中选择的任何设备也会显示在“已选设备”中。

   您不能将以前合并的多接口设备添加到另一个多接口设备。



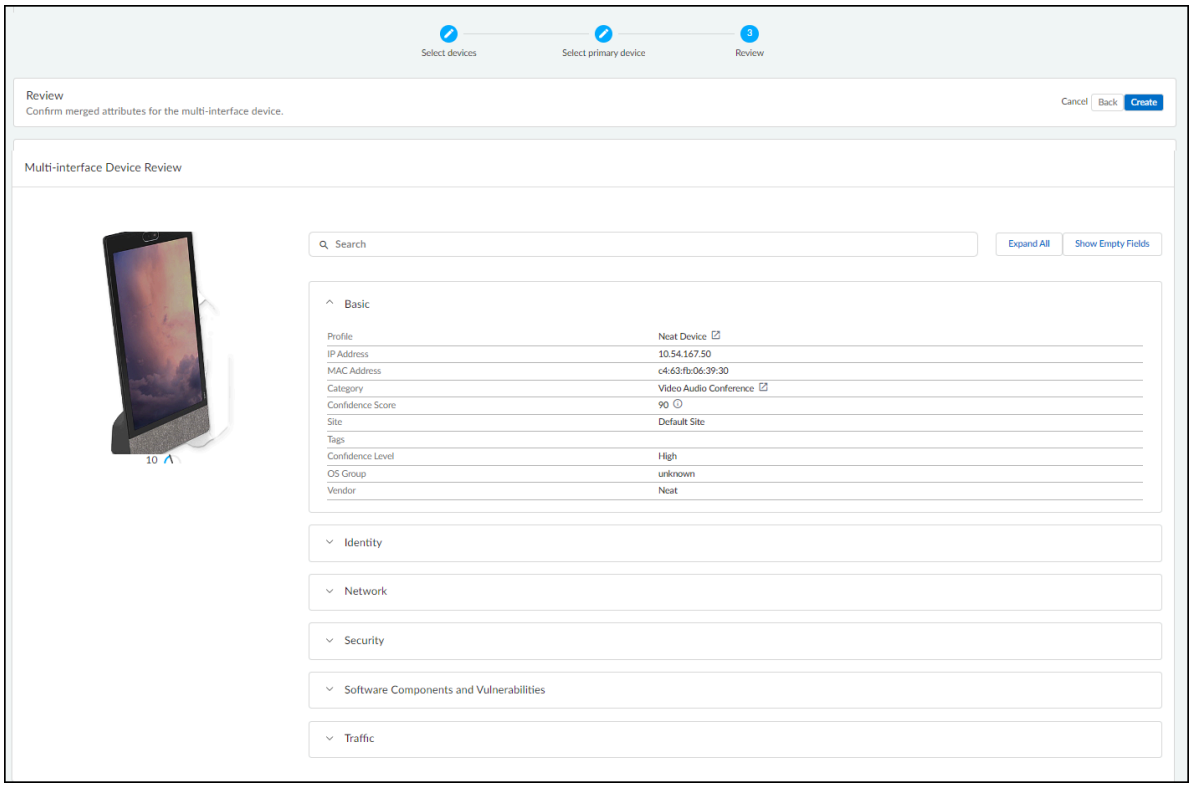
3. 当您满意后，单击 **Next**（下一步）。
4. 选择多接口设备的主接口。



虽然所有接口都保留其特定于网络的属性（IP 地址、MAC 地址、子网和 VLAN），但合并的设备将使用主接口的物理设备属性。您可以考虑选择处理最多流量的接口，因为 IoT

Security 最有可能拥有来自此接口的最多数据，因此设备识别和风险分析也最准确。如果您的网络上有专用的管理子网和 VLAN,则另一个选项是选择该子网和 VLAN 中的接口。

5. 选择设备的主要接口后，单击 **Next**（下一步），然后展开不同的部分以查看合并的属性。



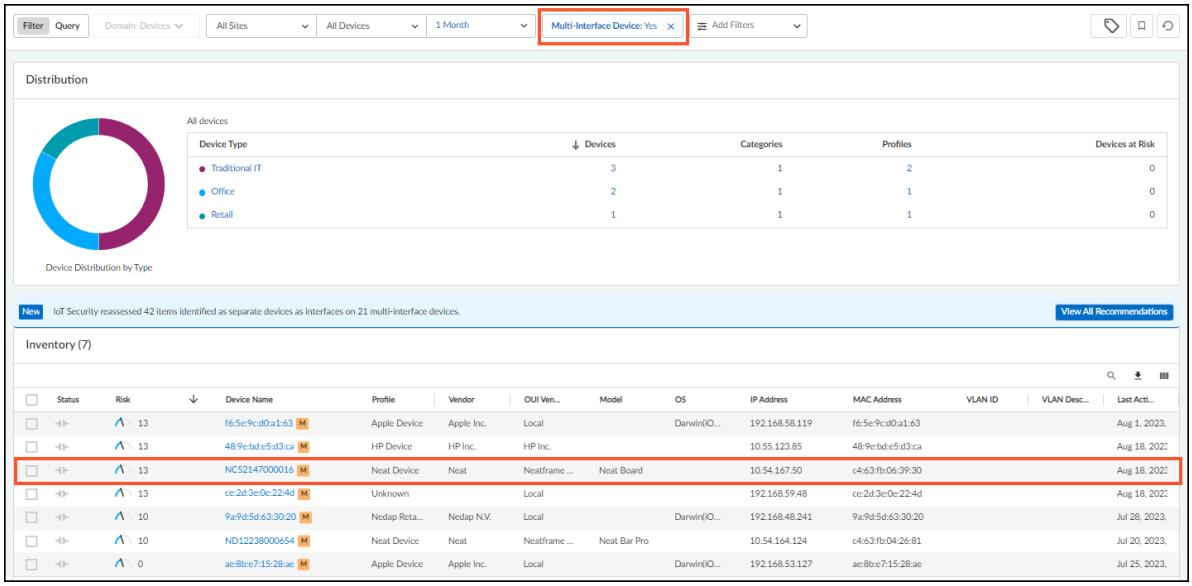
您可以单击 **Expand All**（全部展开）以同时查看所有六组属性，然后单击 **Collapse All**（全部折叠）以将其一起关闭。您可以通过单击 **Hide Empty Fields**（隐藏空字段）来降低展开

部分的高度。要查看所有字段，包括有数据的字段和无数据的字段，请 **click Show Empty Fields**（单击显示空字段）。

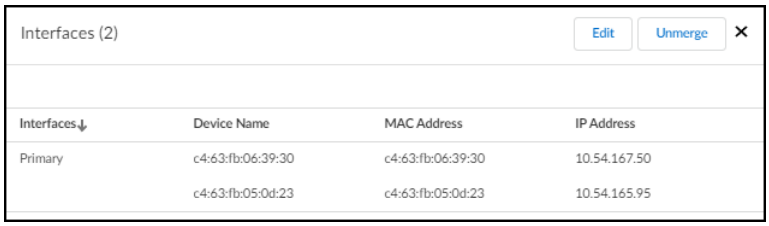
创建多接口设备后，您还可以在 ***Device Details***（设备详细信息） ***> New device page***（新设备页面）的属性部分看到此信息。

6. 当您满意并希望完成合并过程时，请单击 **Create**（创建）。
7. 要在资产 **>** 设备页面上查看合并的设备，请添加过滤器以显示多接口设备。

   新创建的多接口显示在清单表中，其设备名称后带有多接口设备图标 (M)。



8. 单击多接口设备图标 (M) 以查看其接口（在顶部标识主接口），并访问 **Edit**（编辑）和 **Unmerge**（取消合并）选项。



STEP 3 | （可选）编辑多接口设备。

创建多接口设备后，您可以稍后更改主接口、将更多设备作为接口合并到其中、从中移除一个或多个接口或取消合并所有接口。

要更改多接口设备上的主接口，请执行以下操作：

1. 选择 **Assets**（资产） > **Devices**（设备），单击多接口图标 (M) 以打开要更改其主接口设备的接口面板，然后 **Edit**（编辑）。
2. 单击 **Next**（下一步），进入选择主接口的步骤。
3. 选择要创建新主接口的接口，然后单击 **Next**（下一步）。
4. 检查设置，确保新的主接口是您想要的接口，然后单击 **Create**（创建）。

要向现有多接口设备添加一个或多个接口，请执行以下操作：

1. 选择 **Assets**（资产） > **Devices**（设备），单击多接口图标 (M) 以打开要将一个或多个单接口设备合并成接口的设备的接口面板，然后 **Edit**（编辑）。
2. 在“所有设备”表中选择要从单个独立设备转换为多接口设备上的接口的一个或多个设备，然后单击 **Next**（下一步）。
3. 保留先前选择的主接口，或者根据需要将另一个接口设为主接口，然后单击 **Next**（下一步）。
4. **Create**（创建）。

要删除一个或多个接口(但不是全部),并将它们作为单个单接口设备返回清单，同时保留多接口设备：

1. 选择 **Assets**（资产） > **Devices**（设备），单击多接口图标 (M) 以打开要删除其接口设备的接口面板，然后 **Edit**（编辑）。
2. 清除要从多接口设备中删除的接口的选择，然后单击 **Next**（下一步）。
3. 保留先前选择的主接口，或者根据需要将另一个接口设为主接口，然后单击 **Next**（下一步）。
4. **Create**（创建）。

要取消合并所有接口，请执行以下操作：

1. 选择 **Assets**（资产） > **Devices**（设备），单击多接口图标 (M) 以打开要取消合并其接口设备的接口面板，然后 **Edit**（编辑）。
2. **Confirm**（确认）取消合并操作并将每个接口返回到单个单接口设备。

具有静态 IP 地址的设备

虽然大多数联网设备通过 DHCP 动态接收 IP 地址，但通常会保留部分网络地址空间以用作路由器、打印机、FTP 服务器和 DHCP 服务器等设备的静态 IP 地址。除了这种常见做法外，还有一些行业和设施主要使用静态 IP 地址；例如，制造业、公用事业、石油和天然气、仓库、订单履行中心以及处理和配送中心。由于大多数自动化和控制应用程序直接在其程序中使用 IP 地址，因此装配线和加工中心的机器人设备以及控制器必须具有静态 IP 地址，这就是这些领域普遍使用静态寻址的原因。

IoT Security 可以部署在 DHCP 动态为设备分配 IP 地址，网络管理员使用静态 IP 地址手动配置设备以及两者相结合的网络中。IoT Security 使用多种技术来检测和监控网络活动并将其与单个设备相关联。通过检查防火墙提供的 DHCP 流量日志，它将动态分配的 IP 地址与设备 MAC 地址关联起来，并将这些设备添加到清单中。通过查看 ARP 日志，IoT Security 还可以了解 IP 地址到 MAC 地址的映射，并将具有静态 IP 地址的设备添加到清单中，否则这些设备可能无法通过 DHCP 发现。但是，由于 ARP 广播的本质，这仅适用于与报告防火墙位于同一第 2 层广播域内的设备。对于静态 IP 地址超出第 2 层边界的设备，IoT Security 使用机器学习来发现表明此类设备可能存在的网络活动模式。您还可以选择通过静态 IP 设备和子网配置手动为 IoT Security 提供静态 IP 地址分配。

仅为 *IoT Security* 提供静态 *IP* 地址配置不足以将设备添加到清单中。*IoT Security* 还必须检测进出具有已配置静态 *IP* 地址的设备的网络流量。然后，它会将设备添加到清单中。

使用以下方法之一向 IoT Security 清单中添加静态 IP 设备和子网：

- 上传静态 IP 设备列表
- 添加静态 IP 设备配置
- 上传只有静态 IP 地址的子网列表
- 添加只有静态 IP 地址的子网

随后，IoT Security 使用这些设备的 IP 地址（而不是 MAC 地址）来识别和跟踪它们。

上传静态 IP 设备列表

如果您有设备的静态 IP 地址列表，请在 CSV（逗号分隔的值）文件中输入这些地址并将其上传到 IoT Security。

每个上传的 *CSV* 文件有 *10,000* 个静态 *IP* 设备的限制。如果需要上传超过 *10,000* 个，请上传多个 *CSV* 文件。

STEP 1 | 导航到“用户定义的静态 IP 设备”页面，路径为 **Assets**（资产） > **Devices**（设备） > **User-Defined Static IP Devices**（用户定义的静态 **IP** 地址），然后单击 **Add**（添加） > **Upload Static IP Devices**（上传静态 **IP** 设备）。

STEP 2 | 单击链接下载 CSV 模板。

STEP 3 | 使用静态 IP 设备信息填写模板，或以与模板相同的格式创建新文件并填写。

输入要上传的每个设备的静态 IP 地址。（可选）在模板中指示的列中输入其 MAC 地址、供应商和型号。IoT Security 接受以下任何 MAC 地址格式：

aa:bb:cc:00:11:22	**AA:BB:CC:00:11:22**
aa.bb.cc.00.11.22	**AA.BB.CC.00.11.22**
aa-bb-cc-00-11-22	**AA-BB-CC-00-11-22**
aa bb cc 00 11 22	**AA BB CC 00 11 22**
aabbcc001122	**AABBCC001122**

IoT Security 使用 IP 地址而不是MAC地址来识别和跟踪静态IP设备。在稍后参考“用户定义的静态 IP 设备”页面上的条目时，附加的用户配置属性提供了额外的信息。但是，只有上传的 IP 地址和（如果提供）MAC 地址才会出现在“设备”和“设备详细信息”页面上。

STEP 4 | 返回到“用户定义的静态 IP 设备”页面，单击 **Add**（添加） > **Upload Static IP Devices**（上传静态 **IP** 设备），将完成的 CSV 文件选择或拖到对话框中的空白处，然后 **Upload**（上传）。

如果 IoT Security 先前从上传的 IP 地址之一检测到网络活动，则视为匹配。页面顶部的设备匹配计数器递增，“匹配”将显示在此 IP 地址的结果列中。然后，IoT Security 将静态 IP 设备添加到其清单中，并在“设备”和“设备详细信息”页面上显示它。IoT Security 需要几分钟的时间来检查与现有数据的潜在匹配，然后相应地更新清单和静态 IP 设备列表。

如果 IoT Security 尚未检测到某个上传 IP 地址的网络活动，则认为“未找到”。在这种情况下，“未找到的设备”计数器递增，“结果”列中出现短横线。如果 IoT Security 后来发现此 IP 地址的网络活动，它会将其从“未找到”移至“匹配”，将静态 IP 设备添加到其清单中，并开始在“设备”和“设备详细信息”页面上显示。

如果用户定义的 *MAC* 地址与 *IoT Security* 在网络上检测到的 *MAC* 地址不同，检测到的 *MAC* 地址将覆盖用户定义的 *MAC* 地址。

添加静态 IP 设备配置

无需上传包含静态 IP 设备列表的 CSV 文件（参阅上传静态 IP 设备列表），您可以单独添加。

STEP 1 | 导航到用户定义的静态 IP 设备页面，路径为 **Assets**（资产） > **Devices**（设备） > **User-Defined Static IP Devices**（用户定义的静态 **IP** 设备），然后单击 **Add**（添加） > **Manually Add a Static IP Device**（手动添加静态 **IP** 设备）。

STEP 2 | 定义静态 IP 设备，然后单击 **Add**（添加）。

IP 地址：输入您要添加到清单的设备的静态 IP 地址。IP 地址是 IoT Security 用于跟踪用户定义的静态 IP 设备的地址。

MAC 地址（可选）：如果需要，可以使用十六进制形式添加设备的 MAC 地址。IoT Security 接受以下 MAC 地址格式：

aa:bb:cc:00:11:22	**AA:BB:CC:00:11:22**
aa.bb.cc.00.11.22	**AA.BB.CC.00.11.22**
aa-bb-cc-00-11-22	**AA-BB-CC-00-11-22**
aa bb cc 00 11 22	**AA BB CC 00 11 22**
aabbcc001122	**AABBCC001122**

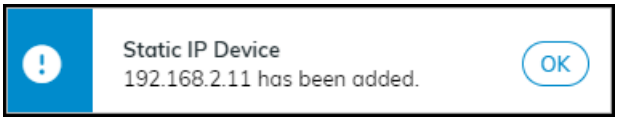
如果用户定义的 *MAC* 地址与 *IoT Security* 在网络上检测到的 *MAC* 地址不同，则检测到的 *MAC* 地址将覆盖用户定义的 *MAC* 地址。如果 *IoT Security* 未检测到 *MAC* 地址，则用户定义的 *MAC* 地址会出现在“设备和设备详细信息”页面上。

供应商（可选）：输入该设备的供应商。

型号（可选）：输入设备型号。

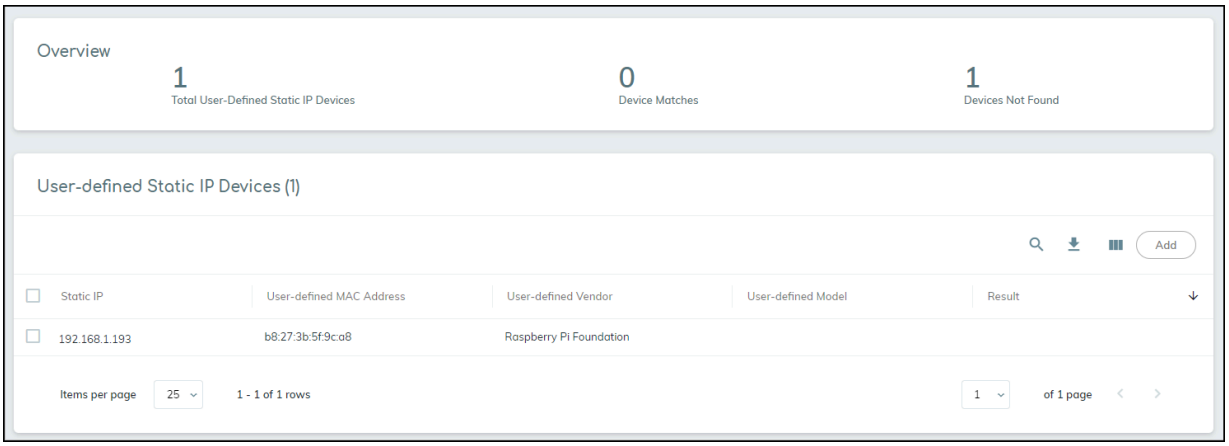
稍后引用用户定义的静态 IP 设备页面上的条目时，供应商和型号属性可以提供额外的信息。但是，它们不会出现在“设备和设备详细信息”页面上。

STEP 3 | 单击 **Add**（添加），将配置添加到 IoT Security然后单击 **OK**（确定）以关闭出现的确认消息。



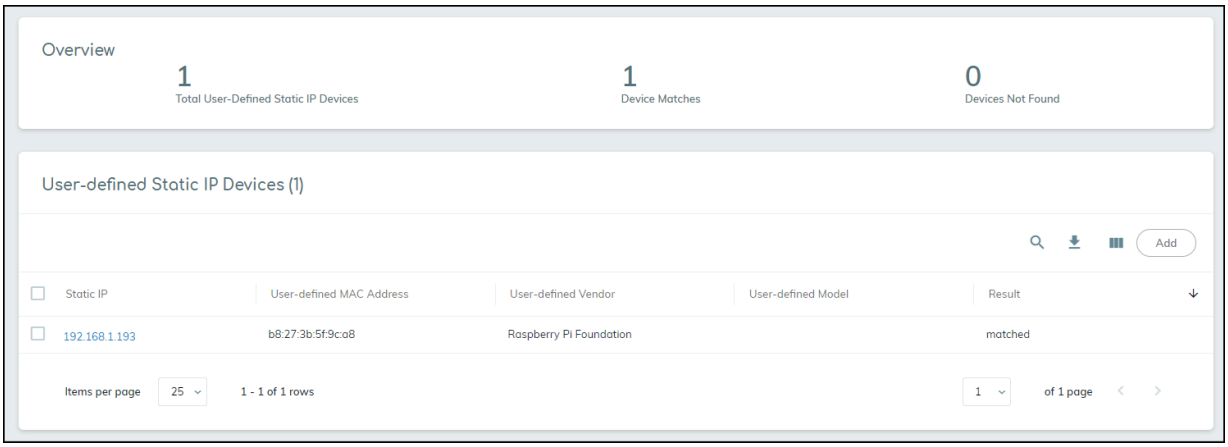
添加静态 IP 设备后，IoT Security 最初将其视为“未找到”。它会逐步将“用户定义的静态 IP 设备总数”计数器加一，并将“未找到的设备”计数器加一。虽然它在用户定义的静态 IP 设备

列表中添加了一个条目，但结果列仍然是空的 — 没有“匹配”的条目，这表明 IoT Security 检测到此 IP 地址的网络活动；或者显示一个短横线，表示未检测到此类活动。



IoT Security 会定期将用户定义的静态 IP 设备列表中的条目与其清单中的条目及其所检测到 IP 地址（不附带 MAC 地址）的内部数据库中的条目进行比较，因此，该页面可以在初始状态保持几分钟。

如果找到匹配项，则”设备匹配计数器“加一，而“未找到设备计数器”减一。此外，“匹配项”现在会显示在结果列中。



如果 IoT Security 没有找到匹配项，它最终会在结果列中显示一个短横线。

您可能需要重新加载用户定义的静态 *IP* 设备页面才能查看更新的数据。

上传只有静态 IP 地址的子网列表

如果整个子网由静态 IP 地址组成，则添加子网并将其定义为具有静态 IP 地址比单独添加多个静态 IP 设备更高效。当您有多个具有静态 IP 地址的子网时，您可以一次将所有子网上传到一个 CSV 文件中。

每个上传的 *CSV* 文件有 *10,000* 个子网的限制。如果需要上传超过 *10,000* 个，请上传多个 *CSV* 文件。

在为 IoT Security 提供子网配置并指定其具有静态 IP 地址，然后 IoT Security 检测到来自该子网中某个设备的流量后，会将该设备视为静态 IP 设备。使用 IP 地址作为 Device-ID（而不是 MAC 地址），它将设备添加到其清单中。IoT Security 仅对未通过其他检测机制（如 ARP 日志）发现的设备以这种方式将静态 IP 设备添加到其清单中。

如果在 *IoT Security* 将此子网的静态 *IP* 设备添加到其清单后删除某个静态 *IP* 子网，则 *IoT Security* 会反转此操作并自动将其从清单中删除。

STEP 1 | 导航到网络页面，路径为 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络），然后单击 **Add**（添加） > **Upload Subnets**（上传子网）。

STEP 2 | 单击链接下载 CSV 模板。

STEP 3 | 使用子网信息填写模板。

为要上传的每个子网输入以下内容：

prefix：以点十进制表示法输入子网的 IP 地址，以 CIDR 表示法输入其网络掩码（例如，10.1.1.0/24）。这将出现在“子网”页面中，对于此子网中的设备，子网和网络掩码将显示在“设备”和“设备详细信息”页面中。

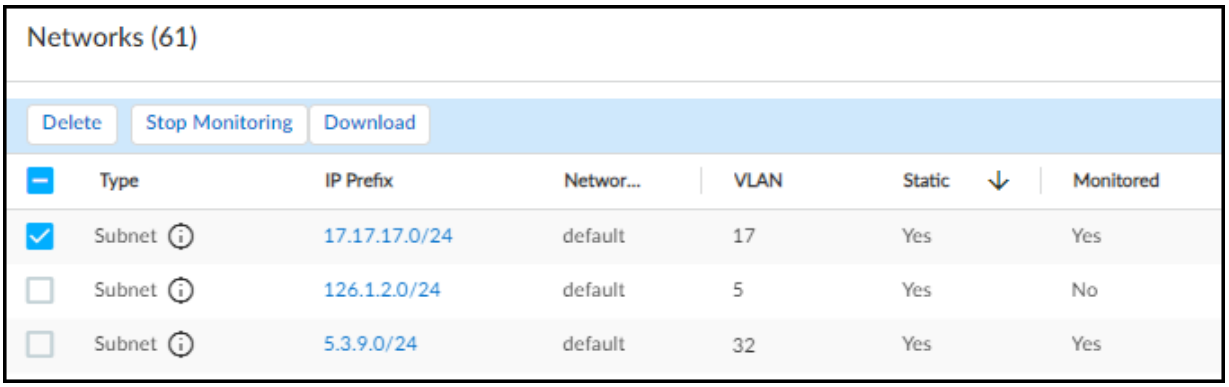
vlan：（可选）输入 VLAN ID。如果输入，它也会显示在“子网”页面上，对于此子网中的设备，它会显示在“设备”和“设备详细信息”页面上。

description：（可选）输入子网/VLAN 的描述，也许注意它所针对的设备类型。描述字段中不允许使用以下特殊字符：~ ` ! # $ % ^ & * + = { } [ ] | \ < > ?此说明仅显示在“子网”页面上。

static：输入 **yes** 将其定义为包含静态 IP 地址的子网。当 IoT Security 从与防火墙不同的 L2 域中用户配置的静态 IP 子网中发现设备并将其添加到其清单中时，“设备”页面上的“源”列将显示 **User-Configured** 的设备。（如果不希望子网是静态的，请留空）。

monitored：如果您希望 IoT Security 提供此子网中设备的设备分析、行为分析和风险监控，请输入 **yes**。如果只想让 IoT Security 检测子网中的设备并执行简化的设备身份分析，请将其留空。基于此字段，在 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）上的“网络”表中，IoT Security 门户会在 **Monitored**（监控）列中显示 **Yes** 或 **No**，并提供相应级别的设备监视、分析和保护。

Add a subnet（添加子网）选项不提供将子网指定为已监视或未监视的选项。*IoT Security* 会自动将添加的子网分类为已监视。但是，您可以在添加子网后更改其分类，方法是选择子网并单击网络表上方的 ***Stop Monitoring***（停止监视）。您还可以进行多项选择以停止同时监视多个子网。稍后，您可以选择未监视的子网，然后单击表上方的 ***Start Monitoring***（开始监视）。



STEP 4 | 上传 CSV 文件。

在“网络”页面上，单击 **Add**（添加） > **Upload Subnets**（上传子网），选择或拖拽完成的 CSV 文件到对话框中的空白处，然后单击 **Upload**（上传）。

如果 IoT Security 以前从一个上传的子网中的 IP 地址检测到网络活动，则现在会将其视为静态 IP 地址，并自动将静态 IP 设备添加到“设备”页面上的清单中。同样，如果 IoT Security 稍后检测到来自其中一个子网中的 IP 地址的流量，它会自动在当时将条目添加到清单中。

新条目可能需要几分钟才能显示在“设备”页面上。

添加只有静态 IP 地址的子网

不要上传包含静态 IP 子网列表的 CSV 文件（参阅上传只有静态 IP 地址的子网列表），您可以单独添加静态 IP 子网。

STEP 1 | 导航到“网络”页面，路径为 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络），然后单击 **Add**（添加） > **Add a Subnet**（添加子网）。

STEP 2 | 定义子网，然后 **Save**（保存）。

Type（类型）：选择 **Subnet**（子网）。

Prefix（前缀）：输入要添加的子网的 IP 地址/网络掩码。以点十进制表示法输入子网的 IP 地址，以 CIDR 表示法输入其网络掩码（例如，10.1.1.0/24）。

Name（名字）（可选）：输入子网的名称

VLAN ID（可选）：输入子网的 VLAN ID。

Description（描述）（可选）：输入 VLAN/子网的描述，例如它所针对的设备类型。描述字段中不允许使用以下特殊字符：~ ` ! # $ % ^ & * + = { } [ ] | \ < > ?

Mark this subnet as static（将此子网标记为静态）：选择：

新条目可能需要几分钟时间才能显示在“网络”页面上。您可能需要重新加载页面才能看到更新的数据。

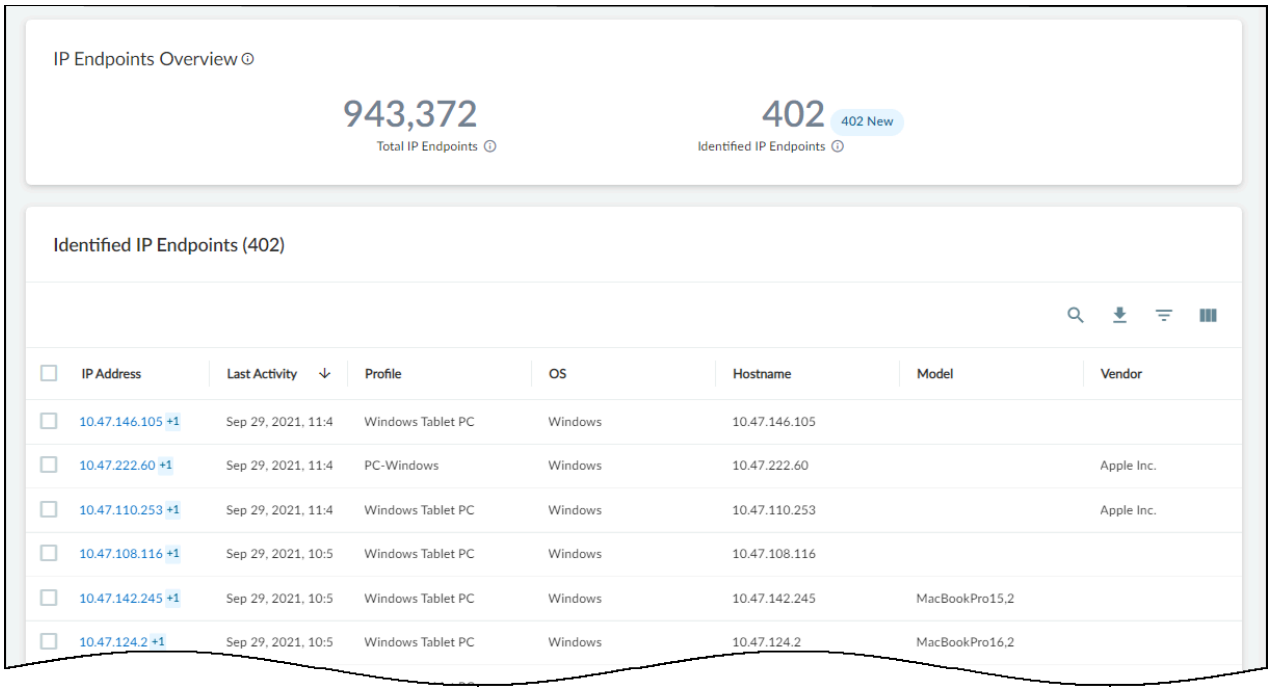
IP 端点

当 IoT Security 接收到足够的网络流量元数据时，它使用人工智能和机器学习来识别产生流量的设备。然而，有时它接收的信息不足以唯一地识别设备。例如，IoT Security 可能知道有往返于特定 IP 地址的流量，但是，由于该设备与记录网络流量元数据的防火墙位于不同的第 3 层域中，因此它永远不会了解其 MAC 地址。该设备可能位于路由器、NAT 设备或无线网络共享设备后面，因此防火墙只能获取其 IP 地址。如果 DHCP 为网络设备提供网络设置，则不同的设备可能会在不同时间使用相同的 IP 地址。因此，随着不同类型的设备轮流使用 IP 地址，与 IP 地址相关的网络行为将不断变化。当 IoT Security 知道流量的来源和目标的 IP 地址，但不知道其 MAC 地址，并且网络行为不够稳定时，无法推断出它是静态分配的 IP 地址，IoT Security 会将其归类为 IP 端点。

IoT Security 了解 IP 端点的另一种方式是通过第三方集成。IoT Security 可以通过与网络管理或资产管理解决方案集成并使用 SNMP 向网络交换机查询与其连接的设备来接收设备数据。

如果 IoT Security 观察到与 IP 端点相关的稳定流量模式，并且其主要设备属性在七天内没有任何变化，它会将其移动到设备页面。IoT Security 主要监视八个主要设备属性的变化：设备配置文件、类别、供应商、型号、操作系统、主机名、序列号和站点 ID。任何一个属性的改变都表明使用该 IP 地址的设备已经改变，因此如果它们在七天内都保持不变，那么可以合理地假设设备身份是稳定的。

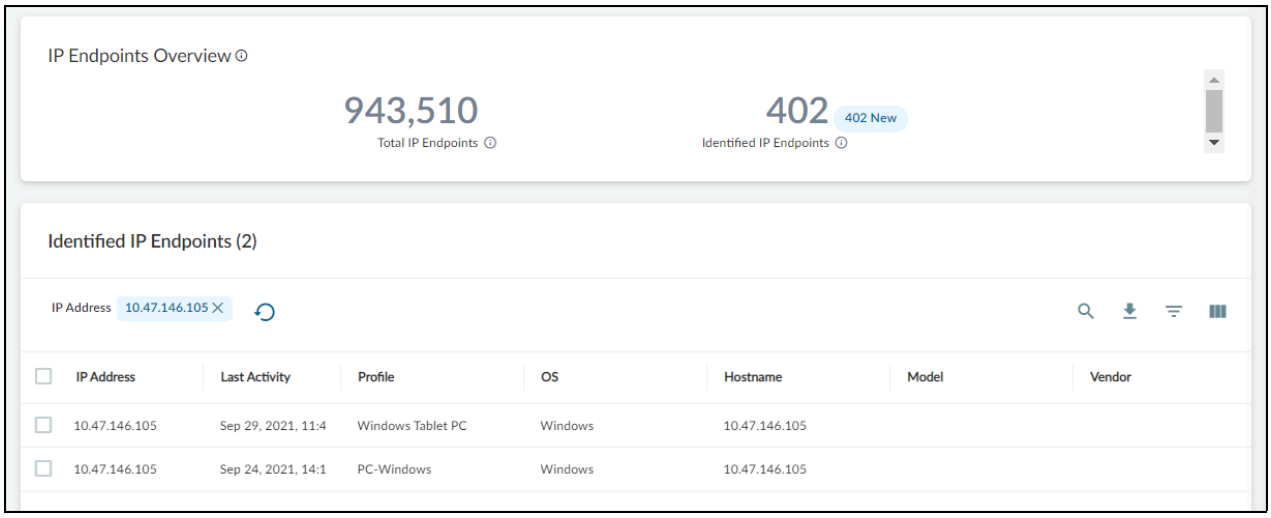
将 IP 端点添加到设备页面后，IoT Security 会继续每天追踪其属性。如果之后设备的任何属性发生改变，IoT Security 会立即将其移动到已识别的 IP 端点表，并在那里继续跟踪这些属性。您可以查看在网络上发现的或从集成的第三方产品中了解到的所有 IP 端点的总数，以及在 **Assets**（资产）> **Devices**（设备）> **IP Endpoints**（IP 端点）上所有已识别的 IP 端点的总数和列表。



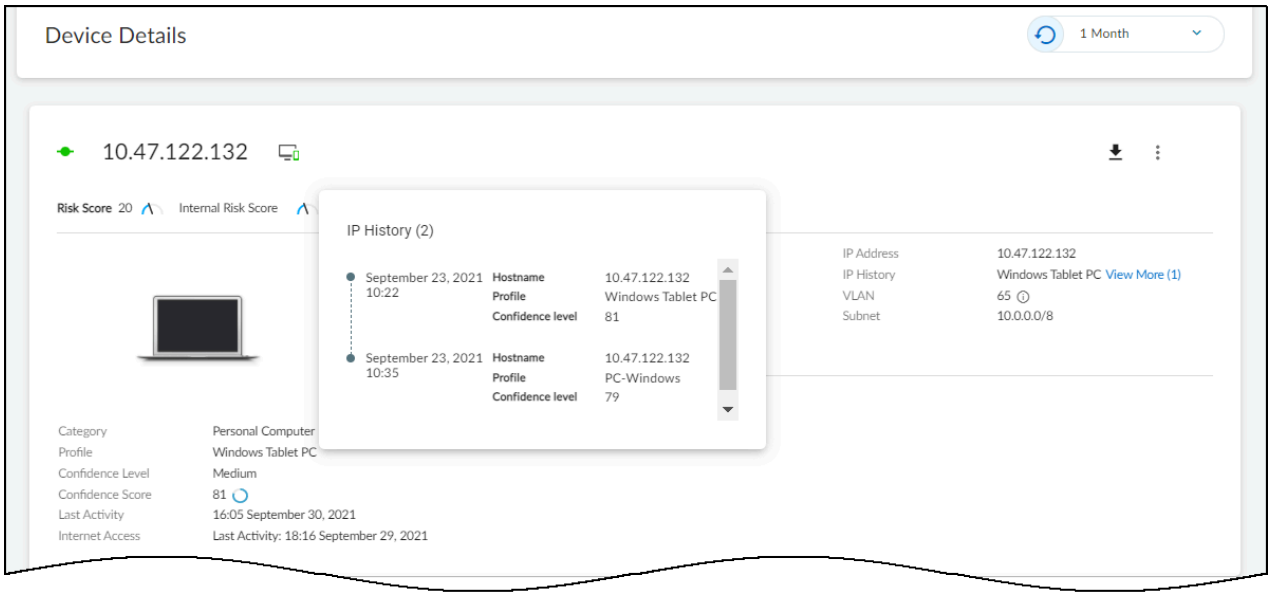
页面顶部是站点、设备类型和时间段（1 天、1 周和 1 个月）的数据过滤器。站点过滤器控制每个站点、每个站点组或所有站点的 IP 端点和已识别的 IP 端点显示的数据。设备类型过滤器可控制按工业、医疗、办公、传统 IT、所有 IoT 和所有设备等类型显示的数据显示。时间过滤器显示 IoT Security 在过去一天、一周或一个月内发现或了解到的数据。

您可能想知道为什么设备类型过滤器会影响 IP 端点的总数。毕竟，IoT Security 还无法识别 IP 端点是什么类型的设备。然而，对于其中一些设备来说，它已经有一个大概的概念 — 例如，足以区分 IT 设备和 IoT 设备。这就是为什么当过滤器为 **All Devices**（所有设备）和 **All IoT**（所有 **IoT**）时，您可能会看到不同的 IP 端点总数。

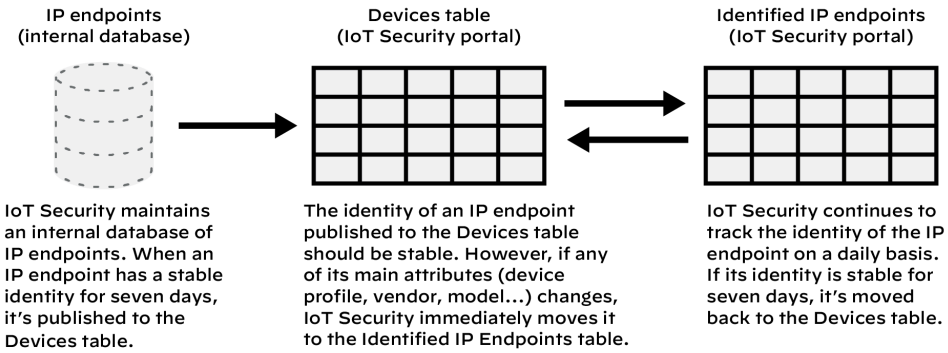
要查看已识别 IP 端点的历史记录，请单击其 IP 地址。例如，下面的历史显示 IoT Security 最初将此 IP 端点识别为 Windows PC，然后将其修改为 Windows 平板电脑。IoT Security 保留过去 30 天内最多 10 条更改的历史记录。



如果已识别 IP 端点的行为最终再次稳定下来，并且其主要设备属性连续七天没有进一步变化，IoT Security 会将其移回至设备页面。您还可以在设备详细信息页面上查看最近十次更改的历史记录。



IP 端点内部数据库、设备表和已识别的 IP 端点表之间的关系如下所示。



发现移动设备属性

IoT Security 可以了解移动（蜂窝）设备属性，将设备添加到其清单中，并通过 IMEI 号码对其进行跟踪。然后，您可以在 **Assets**（资产） > **Devices**（设备）和 **Device Details**（设备详细信息）页面上查看它们的各种移动设备属性。您还可以在创建自定义警报时使用移动设备属性。但是，由于将其归类为传统 IT 设施，因此，IoT Security 不会为移动设备提出策略规则建议或发送防火墙 IP 地址到设备的映射。

将 IoT Security 设置为发送 PAN-OS 移动设备属性

这假设 *IoT Security* 已加入您的防火墙，它有所需的许可证和证书，并且已启用日志记录。

STEP 1 | 在防火墙上启用 GTP Security。

1. 登录 PAN-OS，选择 **Device**（设备） > **Setup**（设置） > **Management**（管理），然后单击常规设置中的 **Edit**（编辑）（齿轮图标）。
2. 选择 **GTP Security**，然后单击 **OK**（确定）。
3. **Commit**（提交）您的更改，然后选择 **Device**（设备） > **Operations**（操作） > **Reboot Device**（重新引导设备）。

STEP 2 | 创建包含 GTP 日志记录的日志转发配置文件。

1. 重新登录并选择 **Objects**（对象） > **Log Forwarding**（日志转发） > **Add**（添加）。
2. 输入日志转发配置文件的名称，如 `Mobile Device Logging`，选择 **Enable enhanced application logging to Strata Logging Service**（启用 **Strata** 日志记录服务的增强型应用日志记录），然后单击 **OK**（确定）。

STEP 3 | 为网络上的移动设备类型创建移动网络保护配置文件。

下面是建议的设置，用于启用不同移动设备的 User-ID 和 Device-ID 与用户设备 IP 地址 (UEIP) 的关联。有关每个设置的详细信息，请参阅 PAN-OS 中的移动网络保护配置文件帮助。

- 支持 **RADIUS** 的 **5G** 移动设备
  1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Mobile Device Protection**（移动设备保护），然后单击 **Add**（添加）。
  2. 输入配置文件的名称，如 `RADIUS Correlation`，单击 **Correlation**（关联），然后输入以下内容：

     UEIP Correlation（**UEIP** 关联）：（选择）

     Mode（模式）：释放

     User Plane with GTP-U encapsulation（采用 **GTP-U** 封装的用户面板）：（清除）

     Source（源）：**RADIUS**

     Log At Ueip Start（在 **Ueip** 开始时记录）：（选择）

     Log At Ueip End（在 **Ueip** 结束时记录）：（选择）
  3. 单击 **GTP Inspection**（**GTP** 检查） > **GTP-U**，然后输入以下内容来对 GTP 标头中的信息元素 (IE) 执行有效性检查，并在发现任何异常时生成警报：

     Alert（警报）：（选择）

     Reserved IE（保留 **IE**）：（选择）

     Order of IE（**IE** 的顺序）：（选择）

     Length of IE（**IE** 的长度）：（选择）

     Spare Flag in Header（标头中有备用标志）：（选择）

     Unsupported message type（不支持的消息类型）：（选择）

     GTP-in-GTP：警报
- 具有数据包转发控制协议 **(PFCP)** 的 **5G** 移动设备
  1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Mobile Device Protection**（移动设备保护），然后单击 **Add**（添加）。
  2. 输入配置文件的名称，如 `PFCP-5G Correlation`，单击 **Correlation**（关联），然后输入以下内容：

     UEIP Correlation（**UEIP** 关联）：（选择）

     Mode（模式）：释放

     User Plane with GTP-U encapsulation（采用 **GTP-U** 封装的用户面板）：（清除）

     Source（源）：**PFCP**

     Log At Ueip Start（在 **Ueip** 开始时记录）：（选择）

     Log At Ueip End（在 **Ueip** 结束时记录）：（选择）

3. 单击 **GTP Inspection**（**GTP** 检查） > **GTP-U**，然后输入以下内容来对 GTP 标头中的 IE 执行有效性检查，如果发现任何不正常情况，将生成警报：

   Alert（警报）：（选择）

   Reserved IE（保留 **IE**）：（选择）

   Order of IE（**IE** 的顺序）：（选择）

   Length of IE（**IE** 的长度）：（选择）

   Spare Flag in Header（标头中有备用标志）：（选择）

   Unsupported message type（不支持的消息类型）：（选择）

   GTP-in-GTP：警报

- 支持 **GTP-C** 的 **3G** 和 **4G** 移动设备

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Mobile Device Protection**（移动设备保护），然后单击 **Add**（添加）。
2. 输入配置文件的名称，如 `GTP-C-3G4G Correlation`，然后在 **GTP-C** 选项卡中输入以下内容以使用状态检查，对 GTP 标头中的 IE 执行有效性检查，并在发现异常时生成警报：

   GTPv1-C

   Stateful Inspection（有状态检查）：（选择）

   Alert（警报）：（选择）

   Reserved IE（保留 **IE**）：（选择）

   Order of IE（**IE** 的顺序）：（选择）

   Length of IE（**IE** 的长度）：（选择）

   Spare Flag in Header（标头中有备用标志）：（选择）

   Unsupported message type（不支持的消息类型）：（选择）

   GTPv2-C：

   Stateful Inspection（有状态检查）：（选择）

   Alert（警报）：（选择）

   Reserved IE（保留 **IE**）：（选择）

   Length of IE（**IE** 的长度）：（选择）

   Spare Flag in Header（标头中有备用标志）：（选择）

   Unsupported message type（不支持的消息类型）：（选择）
3. 单击 **GTP-U**，然后输入以下内容：

   Alert（警报）：（选择）

   Reserved IE（保留 **IE**）：（选择）

   Order of IE（**IE** 的顺序）：（选择）

Length of IE（**IE** 的长度）：（选择）

Spare Flag in Header（标头中有备用标志）：（选择）

Unsupported message type（不支持的消息类型）：（选择）

GTP-in-GTP：警报

Log at GTP-U session start（在 **GTP-U** 会话开始时记录）：（选择）

Log at GTP-U session end（在 **GTP-U** 会话结束时记录）：（选择）

GTP-U Content Inspection（**GTP-U** 内容检测）：（选择）

STEP 4 | 创建安全策略规则以记录移动设备流量，并将日志转发到日志记录服务。

创建安全策略规则以记录移动设备流量，并将日志转发到日志记录服务以供 IoT Security 分析。您创建的规则取决于网络上移动设备的生成，以及网络是使用 RADIUS 还是 PFCP。

- 支持 **RADIUS** 的 **5G** 移动设备
  1. 选择 **Policys**（策略） > **Security**（安全），然后单击 **Add**（添加）。
  2. 使用以下设置创建通用安全策略规则：

     允许将 **Radius** 作为从任何源到任何目标的应用程序。

     在“操作”选项卡中，选择 **Profiles**（配置文件）作为配置文件类型，选择您以前为 RADIUS 关联创建的移动网络保护配置文件，选择 **Log at Session Start**（在会话开始时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

     单击 **OK**（确定）。
  3. 单击 **Add**（添加），然后使用以下设置创建通用安全策略规则：

     在“操作”选项卡中，选择 **None**（无）作为配置文件类型，选择 **Log at Session Start**（在会话开始时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

     允许从任何源到任何目标的任何应用程序。

     单击 **OK**（确定）。
  4. 如有必要，在规则集中将第一条规则的位置调整到第二条规则之上。
- 采用 **PFCP** 的 **5G** 移动设备
  1. 选择 **Policies**（策略） > **Security**（安全），然后单击 **Add**（添加）。
  2. 使用以下设置创建通用安全策略规则：

     允许将 **pfcp** 作为从任何源到任何目标的应用程序。

     在“操作”选项卡中，选择 **Profiles**（配置文件）作为配置文件类型，选择您以前为 PFCP 5G 关联创建的移动网络保护配置文件，选择 **Log at Session Start**（在会话开始时记

录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

单击 **OK**（确定）。

3. 单击 **Add**（添加），然后使用以下设置创建通用安全策略规则：

   允许将 **gtp-u** 从任何源到任何目标的应用程序。

   在“操作”选项卡中，选择 **Profiles**（配置文件）作为配置文件类型，选择您以前为 PFCP 5G 关联创建的移动网络保护配置文件，选择 **Log at Session Start**（在会话开始时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

   单击 **OK**（确定）。

4. 单击 **Add**（添加），然后使用以下设置创建通用安全策略规则：

   允许从任何源到任何目标的任何应用程序。

   在“操作”选项卡中，选择 **None**（无）作为配置文件类型，选择 **Log at Session Start**（在会话开始时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

   单击 **OK**（确定）。

5. 如有必要，请调整规则位置，让第一条和第二条规则排在规则集中的第三条规则之上。

- 支持 **GTP-C** 的 **3G** 和 **4G** 移动设备

1. 选择 **Policies**（策略） > **Security**（安全），然后单击 **Add**（添加）。
2. 使用以下设置创建通用安全策略规则：

   允许将 **gtpv1-c** 和 **gtpv2-c** 作为从任何源到任何目标的应用程序。

   在“操作”选项卡中，选择 **Profiles**（配置文件）作为配置文件类型，选择您以前为 GTP-C 3G 和 4G 关联创建的移动网络保护配置文件，选择 **Log at Session Start**（在会话开始时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

   单击 **OK**（确定）。

3. 单击 **Add**（添加），然后使用以下设置创建通用安全策略规则：

   允许将 **gtp-u** 从任何源到任何目标的应用程序。

   在“操作”选项卡中，选择 **Profiles**（配置文件）作为配置文件类型，选择您以前为 GTP-C 3G 和 4G 关联创建的移动网络保护配置文件，选择 **Log at Session Start**（在会话开始

时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

单击 **OK**（确定）。

4. 单击 **Add**（添加），然后使用以下设置创建通用安全策略规则：

   允许从任何源到任何目标的任何应用程序。

   在“操作”选项卡中，选择 **None**（无）作为配置文件类型，选择 **Log at Session Start**（在会话开始时记录）和 **Log at Session End**（在会话结束时记录），然后选择您以前创建的日志转发配置文件。

   单击 **OK**（确定）。

5. 如有必要，请调整规则位置，让第一条和第二条规则排在规则集中的第三条规则之上。

STEP 5 | **Commit**（提交）配置

在 IoT Security 中查看移动设备属性

在防火墙开始记录移动设备流量后，它会将 GTP 日志中的流量元数据转发到日志记录服务，再由日志记录服务将其流式传输到 IoT Security。要检查 GTP 日志的状态，请登录 IoT Security 门户，然后选择 **Administration**（管理） > **Firewalls**（防火墙）。这里可以看到 IoT Security 是否正在接收 GTP 日志，最新日志的时间，以及它接收了多少 GTP 日志事件和字节数。

要在 Devices（设备）页面上的设备清单中查看移动设备属性，请选择 **Assets**（资产） > **Devices**（设备）。移动设备列在默认情况下是隐藏的，所以请单击带有三个竖条的图标以打开列选择面板，然后选择所有要查看的列。显示移动设备属性的所有列均可在移动部分获得：

- 移动设备标识 — 分配给每个移动设备的 15 至 17 位代码，用于唯一标识它国际移动设备标识 (IMEI)
- 移动用户身份 — 在用户身份模块 (SIM) 卡上发布的唯一标识符。在 2G、3G 和 4G 网络中，此标识符称为国际移动用户标识 (IMSI)。在 5G 网络中，则称为订阅永久标识符 (SUPI)。
- 移动用户 **ISDN** — 综合业务数字网络号码是蜂窝电话号码到移动用户的映射
- 移动 **APN**（接入点名称）— 用于标识移动设备通过 2G、3G 或 4G 蜂窝网络连接的外部分组数据网络 (PDN) 的术语。在 5G 网络中，它是指数据网络名称 (DNN)。
- 无线电接入技术 — 移动设备用于无线无线通信的基础连接方法；例如，蓝牙、Wi-Fi、UMTS、LTE 或 5G NR
- 移动基站代码 — 唯一标识蜂窝基站的标识号
- 移动区号 — 用户所在位置的区号
- 移动网络代码 (MNC) — 识别移动用户公共陆地移动网络 (PLMN) 的两位（欧洲标准）或三位（北美标准）号码
- 移动国家/地区代码 (MCC) — 识别移动用户所在国家/地区的三位数字
- 移动 **TAC**（类型分配代码）— 识别移动设备制造商的八位数字
- 网络切片 — 在公共基础架构上运行的网络的逻辑离散部分
- 移动设备 — 在无线网络上运行的最终用户设备

除了在清单表中显示具有这些属性的列外，您还可以在设备页面顶部的过滤器和查询中使用它们。它们显示在移动设备的设备详细信息页面上，可在自定义警报规则时使用。

自定义属性

IoT Security 为发现和了解的设备提供大量属性。其中一些是设备型号、供应商、操作系统、VLAN ID、风险级别和位置。有关完整列表，请参阅“设备”页面上清单表的列。在查看清单中的设备时，您可以按这些设备属性进行排序和过滤，从而更轻松地查找和跟踪感兴趣的设备。但是，如果这些属性不能满足所有需求，您可以创建更符合您使用的设备属性的自定义属性。IoT Security 允许为每个租户创建 50 个自定义属性。

创建自定义属性并自动应用

您可以使用条件语句配置自定义属性，以便在满足条件时，让 IoT Security 自动应用值。

在开始之前，请确保您已在 **Devices**（设备）页面 [**Assets**（资产） > **Devices**（设备）] 上创建和保存一个或多个数据过滤器。您将在每个 IF/THEN 语句的“IF”子句中使用过滤器，指示 IoT Security 将“THEN”子句中的值应用于设备。

通过使用简单的 IF/THEN 语句自动分配自定义属性，为其应用程序提供了一种有效的方法。例如，当设备由组织中的不同部门管理时，自定义属性可以指示哪个部门管理哪个设备。为此，首先创建一个数据过滤器，将特定部门管理的所有设备配置文件组合在一起。然后，为另一个部门管理的所有设备配置文件创建另一个数据过滤器。根据需要继续操作，直到所有设备按配置文件在管理它们的各个部门之间划分。然后使用条件语句创建一个自定义属性，这些语句表示如果设备匹配 <filter-1>，则对其应用 <name of department-1>；如果另一个设备匹配 <filter-2>，则应用 <name of department-2> 等等。完成后，您可以在“设备”页面上按管理它们的部门对清单中的设备进行排序。

STEP 1 | （可选）创建要在属性中使用的过滤器。

如果您还没有要在自定义属性中使用的过滤器，请登录 IoT Security 门户，然后选择 **Devices**（设备）。定义数据过滤器，然后保存。

STEP 2 | 创建一个自定义属性，IoT Security 将会自动将其应用到设备。

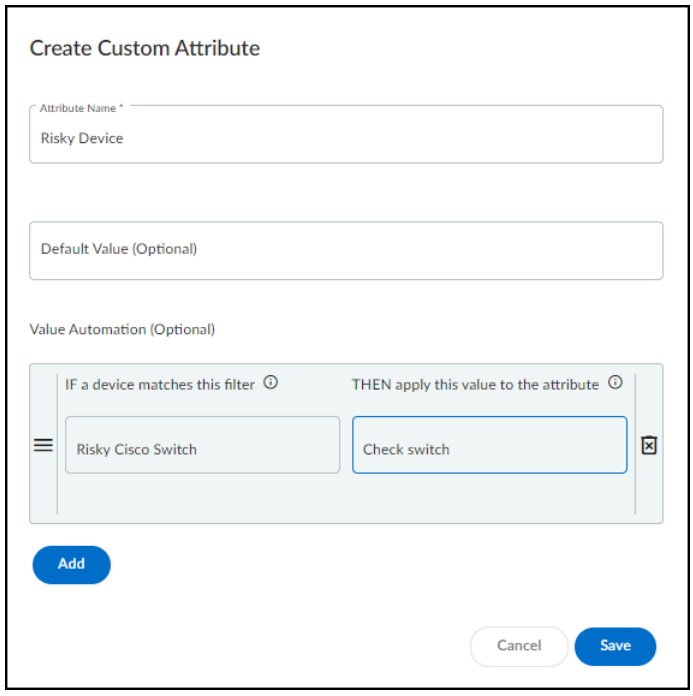
1. 选择 **Settings**（设置） > **Custom Attributes**（自定义属性） > **+**（创建自定义属性）。
2. 在出现的“创建自定义属性”弹出面板中输入以下内容：

   Attribute Name（属性名称）：输入自定义属性的名称。该名称不能包含特殊字符，并且不能超过 50 个字符。

   Default Value (Optional) [默认值（可选）]：输入一个 IoT Security 默认应用到清单中所有设备的值。如果不包含默认值，IoT Security 会在此属性的字段中输入 N/A。

   Value Automation (Optional) [价值自动化（可选）]：**Add**（添加）一个 IF/THEN 条件语句，用于确定何时将值应用于设备属性。为 **IF a device matches this filter**（如果设备与此过滤器匹配）字段选择之前定义的过滤器，然后在 **THEN apply this value to the attribute**（则将此值应用于属性）字段中输入一个值。您可以添加更多 IF/THEN 语句（最多 5 个）。它

们之间的逻辑关系是“或”，而且它们的顺序很重要，因为 IoT Security 从上到下检查条件，并将应用找到的第一个匹配项的值。



STEP 3 | **Save**（保存）自定义属性配置。

IoT Security 在“值自动化”部分搜索其清单中匹配条件（或几个可能条件之一）的任何设备，然后应用规定的值。此搜索可能需要几分钟才能完成。然后，IoT Security 将该值应用于其条件与属性配置中的条件匹配的任何设备。

手动将自定义属性值应用于设备

除了创建自定义属性之外，IoT Security 会根据指定条件将值自动应用于设备，您可以创建自定义属性并自行为每个设备手动应用值。

STEP 1 | 创建一个自定义属性，由您手动将其值应用于设备。

1. 登录 IoT Security 门户，然后选择 **Settings**（设置） > **Custom Attributes**（自定义属性） > **+**（创建自定义属性）。
2. 在出现的“创建自定义属性”弹出面板中输入以下内容：

   Attribute Name（属性名称）：输入自定义属性的名称。该名称不能包含特殊字符，并且不能超过 50 个字符。

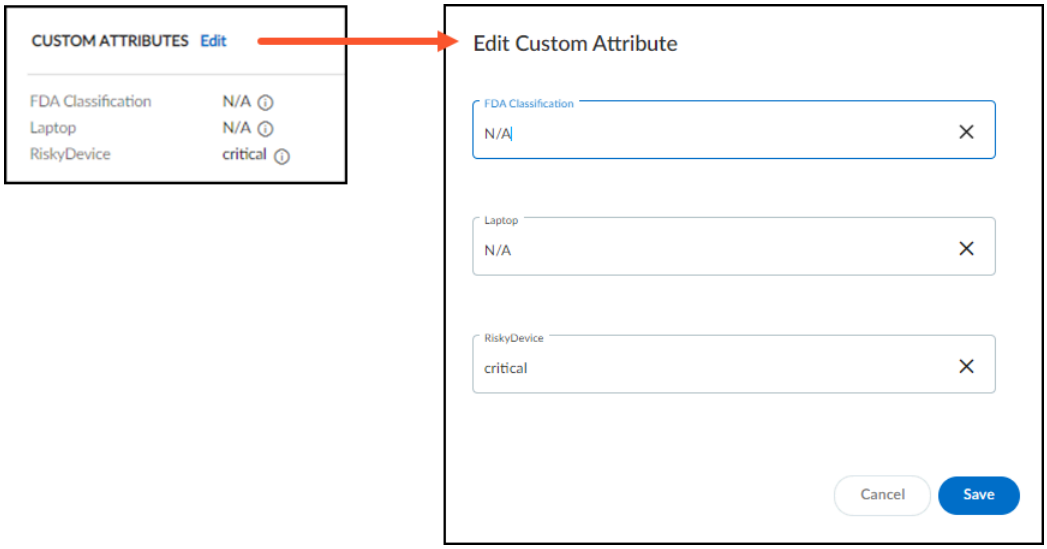
   Default Value (Optional) [默认值（可选）**]**：输入一个 IoT Security 默认应用到清单中所有设备的值。如果不包含默认值，IoT Security 会在此属性的字段中输入 `N/A`。

   Value Automation (Optional) [价值自动化（可选）**]**：请勿配置此部分。

STEP 2 | **Save**（保存）自定义属性配置。

STEP 3 | 将自定义属性应用于设备。

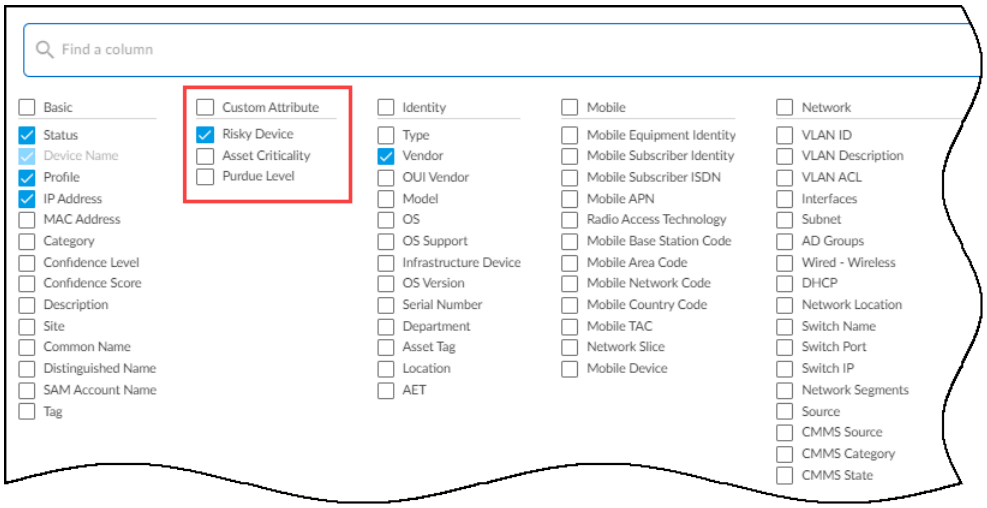
1. 选择 **Assets**（资产） > **Devices**（设备），然后使用“搜索”、“过滤”和“排序”工具显示清单中要应用刚才所创建属性的设备。
2. 单击设备名称，这将打开“设备详细信息”页面。
3. 单击“自定义属性”旁的 **Edit**（编辑）。
4. 删除您不想应用于设备的任何值，然后编辑或添加您想应用的任何值。



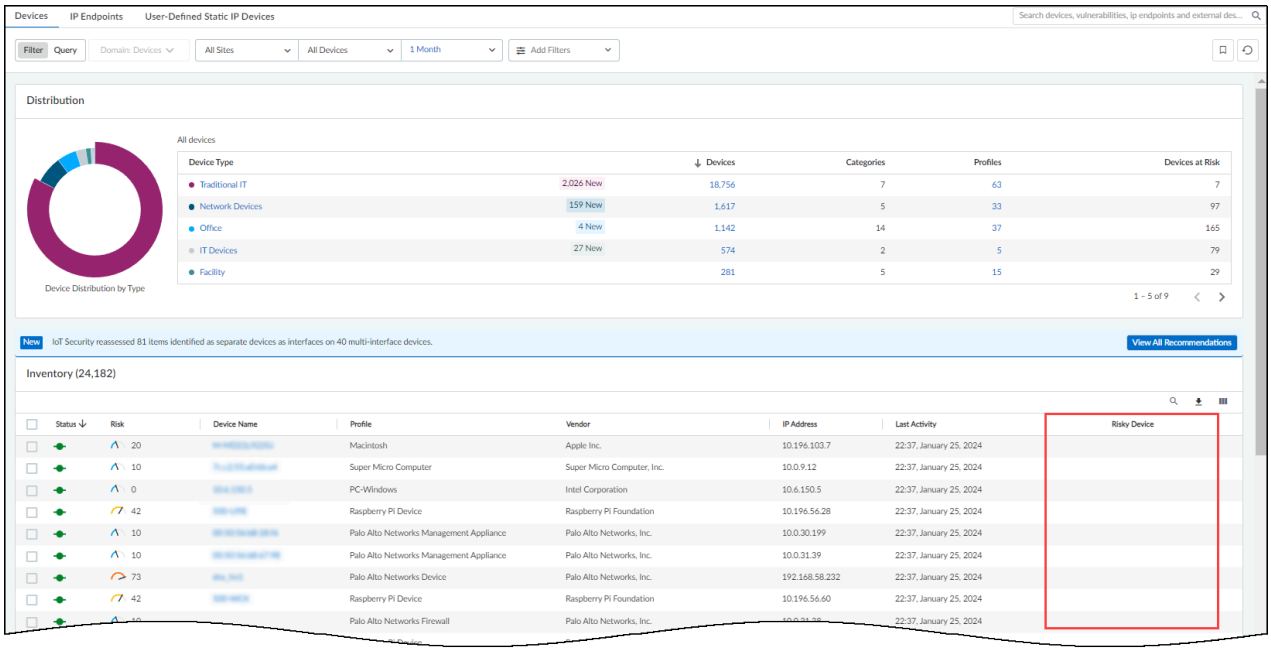
5. **Save**（保存）您的配置更改。

按自定义属性查看设备

将自定义属性应用于设备后，您可以在“设备”页面上显示自定义属性列。单击列图标 (▮▮▮)，然后选择一个或多个要在页面上显示其列的自定义属性。



所选列将显示在“设备”页面的“清单”部分。



要隐藏该列，请再次单击该列图标，并清除您不想再看到的自定义属性的复选框。

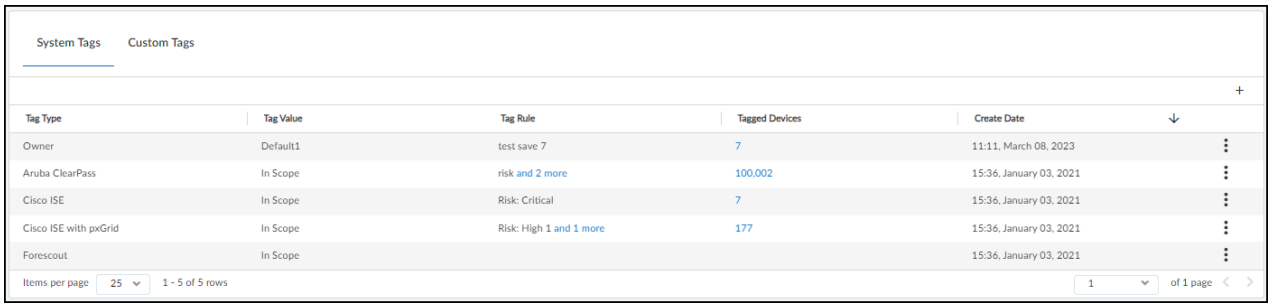
编辑自定义属性并将其从设备中删除

要编辑或删除自定义属性，请选择 **Settings**（设置） > **Custom Attributes**（自定义属性），单击“自定义属性”最右侧的三个垂直点，然后单击 **Delete**（删除）或 **Edit**（编辑）。

标签管理

Settings（设置） > **Tag Management**（标记管理）页面包含可应用于清单中设备的所有标记的列表。此页面上有两个选项卡：具有预定义系统标记的 **System Tags**（系统标记）和具有用户自定义标记的 **Custom Tags**（自定义标记）。

您可以创建自己的自定义标签，并使用它们向设备添加有意义的标签。IoT Security 会根据环境中检测到的设备类型创建系统定义的标签。例如，如果找到制造设备，则它会为 Purdue 级别 1 到 5 创建系统标记。



按照以下步骤管理设备标记：

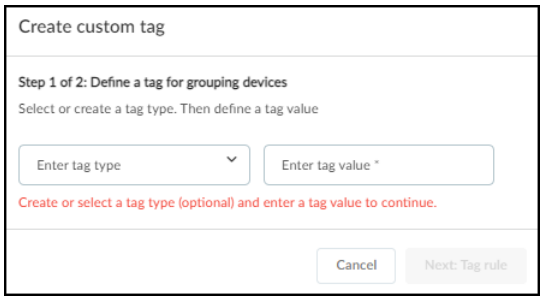
- 创建自定义标记并自动应用
- 手动将标记应用于一个或多个设备
- 手动将标记应用于单个设备
- 从设备中删除标记

创建自定义标记并自动应用

STEP 1 | 定义标记。

要创建自定义标记，请单击自定义标记选项卡右上角的 **+** 图标。

创建自定义标记窗口打开，其中包含标记类型和标记值的字段。类型是可选的，值是必需的。

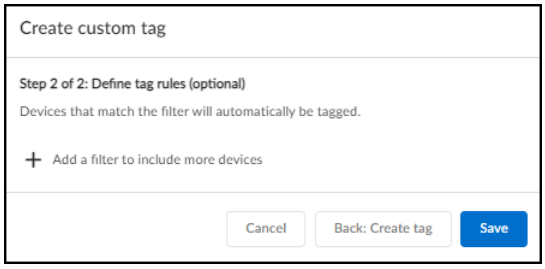


（可选）选择或创建标记类型，定义标记值，然后单击 **Next:Tag Rule**（下一步：标记规则）

STEP 2 | 可选地定义标记规则以自动应用标记。

标记规则定义了应用标记的条件。当设备匹配标记规则中的一个或多个过滤器时，IoT Security 会自动应用指定的标记。IoT Security 不仅在您最初定义标记规则时这样做，而且在以后发现新的匹配设备时也会应用标记。相反，如果某个设备不再匹配过滤器，IoT Security 会自动从其中删除标记。

如果要在设备匹配过滤器时应用标记，请从列表中选择以前保存的过滤器。您还可以添加一个或多个过滤器以将标记应用于多个设备。如果有多个过滤器，则 IoT Security 会将标记应用到设备，如果它匹配其中任何一个。



如果要在“设备”页面上手动或单独在“设备详细信息”页面上将标记应用于一个或多个设备，而不是通过标记规则自动应用，请不要选择或添加任何过滤器。

完成后，**Save**（保存）标记。

您最多可以创建 *1000* 个唯一标记，并手动将其应用于最多 *100,000* 个设备。单个设备最多可以应用 *100* 个标签。

手动将标记应用于一个或多个设备

有两种将标记应用于设备的方法：

- 手动将标记应用于 **Devices**（设备）页面上的一个或多个设备，或 **Device Details**（设备详细信息）页面上的单个设备

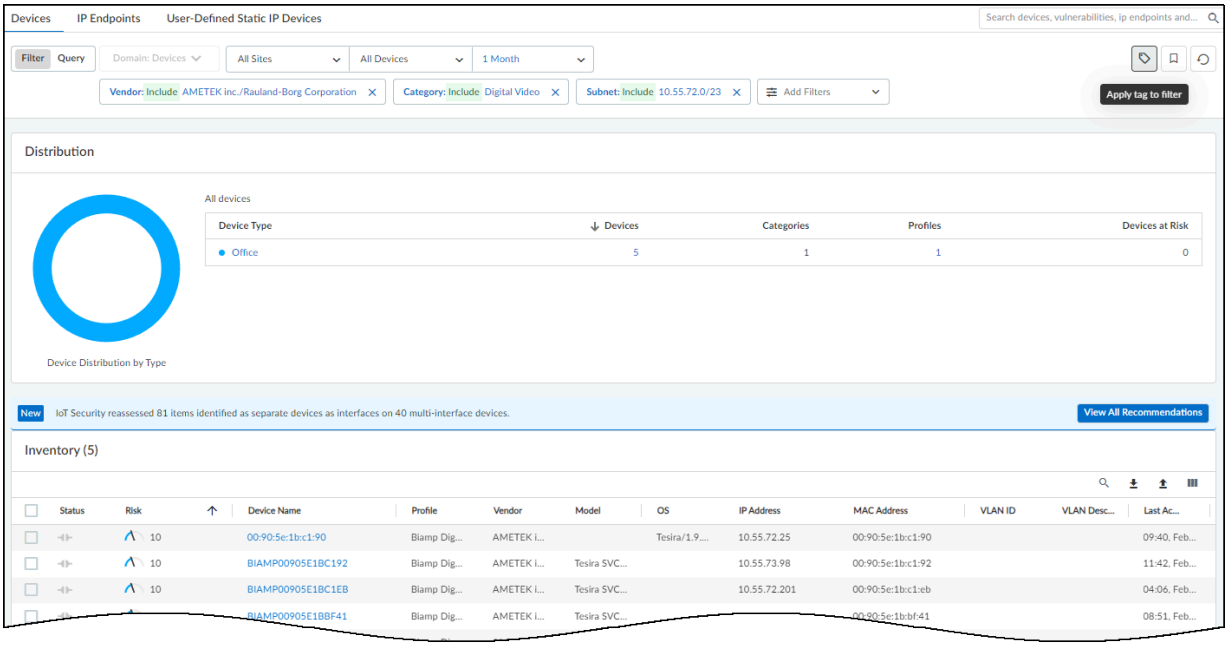
- 通过在 **Settings**（设置） > **Tag Management**（标记管理）页面上使用称为标签规则的特殊过滤器自动应用标签

标记设备的最快方法是通过 **Devices**（设备）页面上的设备清单手动标记。

STEP 1 | 过滤要标记的设备。

打开 **Assets**（资产） > **Devices**（设备）页面，使用过滤工具细化列表中的设备。

列出正确的设备后，单击 **Tag**（标记）图标 ( ) 标记过滤的设备。事实上，您不仅标记这组过滤设备，而且标记过滤器本身。如果 IoT Security 在将来检测到与此过滤器匹配的设备，它也会标记它们。

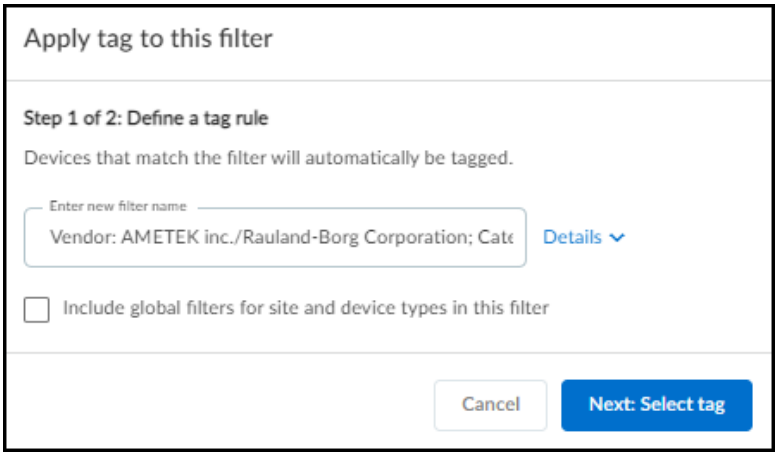


STEP 2 | 应用标记前确认过滤参数。

检查过滤器是否是您要使用的过滤器。如果没有，请在标记设备之前 **Cancel**（取消）并修改过滤器。

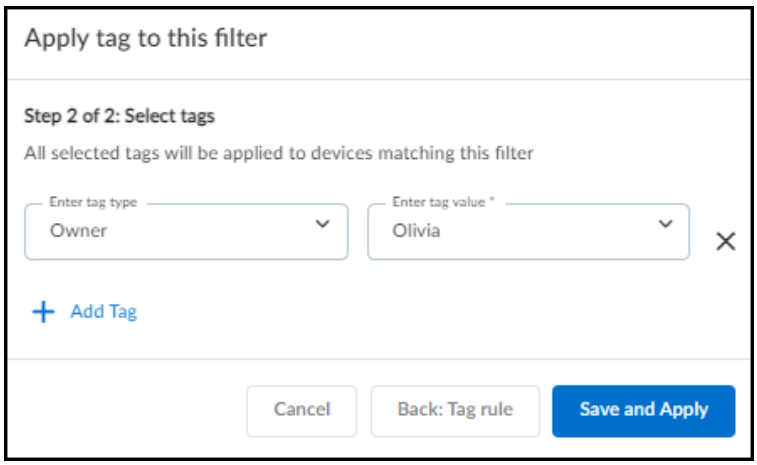
要在“设备”页顶部包含站点和设备类型的全局过滤器，请选择**Include global filters for site and device type in this filter**（在此过滤器中包含站点和设备类型的全局过滤器）。清除该复选框以排除站点和设备类型的全局过滤器。

完成后，请单击 **Next:Select tag**（下一步：选择标记）。



STEP 3 | 选择一个或多个标记并应用它们。

将标记应用于此过滤器窗口打开，其中包含标记类型和标记值的字段。类型是可选的，值是必需的。



可选择或创建标记类型，并选择或创建标记值。

要应用多个标记，请单击 **+ Add Tag**（+添加标记）。

完成后，**Save and Apply**（保存并应用）。

IoT Security 标记过滤的设备，如果将来检测到与您的过滤器匹配的新设备，它也会自动标记它们。同样，如果任何已标记的设备不再匹配过滤器，IoT Security 将自动从其中删除标记。

初始标记过程可能需要几分钟才能完成，具体取决于 *IoT Security* 必须标记多少设备。

手动将标记应用于单个设备

除了在“设备”页面上标记设备外，您还可以从其“设备详细信息”页标记单个设备。

STEP 1 | 打开单个设备的管理标签窗口。

在“设备”页面中，单击某个设备名称以打开此设备的“设备详细信息”页面。

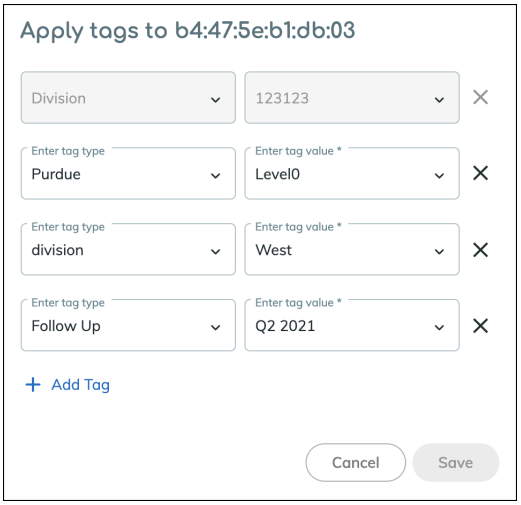
单击页面右上角的操作菜单图标 (⋮)，然后单击 **Manage Tags**（管理标签）。

STEP 2 | 将一个或多个标记应用于设备。

可选择或创建标记类型并选择或创建标记值。

要应用其他标记，请单击 **+ Add Tag**（+添加标记）。单个设备最多可应用 100 个标签。

完成后 **Save**（保存）。



从设备中删除标记

可以从单个设备和 IoT Security 系统中移除标签。

要从单个设备中删除手动应用的标记，请执行以下操作：

1. 导航到设备详细信息页面。
2. 单击操作菜单图标 (⋮)，然后单击 **Manage Tags**（管理标签）。
3. 单击标记条目旁边的 **X** 将其删除，然后 **Save**（保存）。

您只能从单个设备中删除手动应用的标记，因为 *IoT Security* 会重新分配根据标记规则自动分配的任何已删除标记。要删除自动分配的标记，您必须将其从系统中完全删除。

要从整个 IoT Security 系统中删除标记，请执行以下操作：

1. 选择 **Settings**（设置） > **Tag Management**（标记管理）。
2. 单击最右侧列中的操作菜单图标 (⋮)，然后单击 **Delete Tag**（删除标记）。

   在“标记管理”页面上删除标记时，IoT Security 会将其从所有设备中删除。此操作无法撤消，因此，请谨慎删除标记。

了解 IoT 设备应用

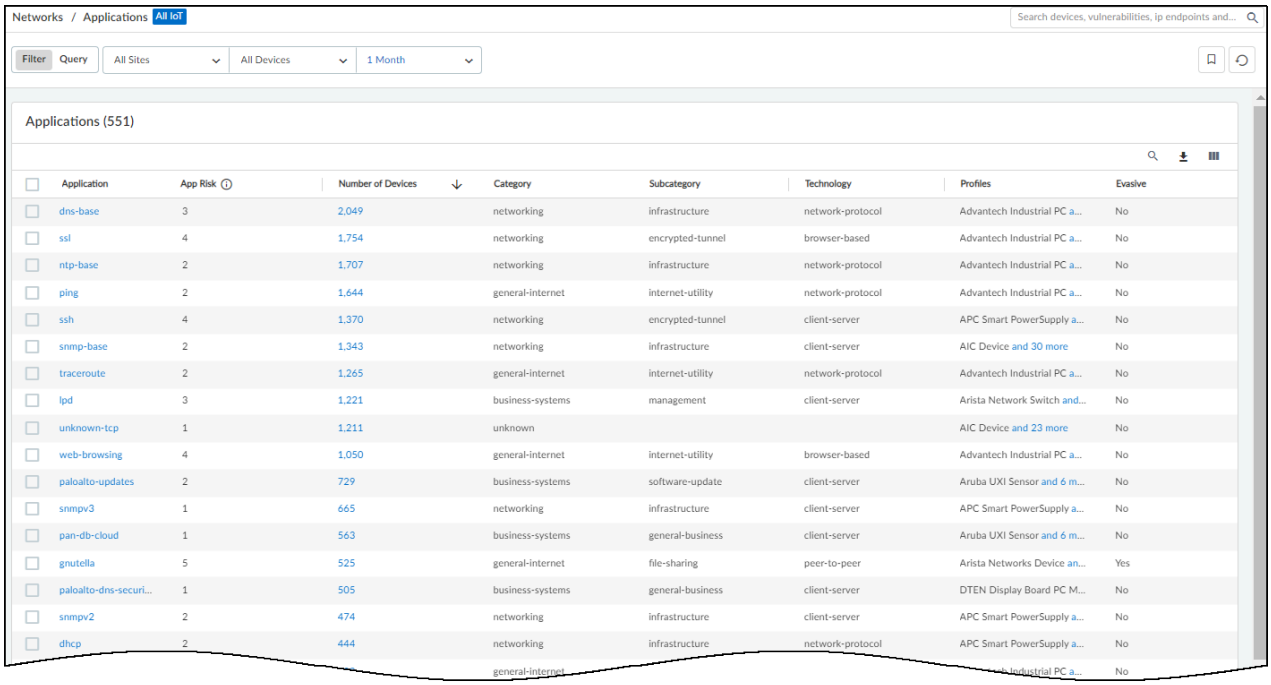
IoT Security 使用机器学习发现网络上的 IoT 设备使用的应用程序。

- IoT 设备应用发现

IoT 设备应用发现

您的网络连接的 IoT 设备使用哪些应用程序？有多少设备使用它们？了解这些信息非常有用，尤其是在防御潜在威胁时。例如，如果您知道一个广泛使用的应用程序最近遭到入侵，您可以检查哪些设备在使用它，并根据应用程序的重要性做出相应的响应。如果它对业务来说不是必需的，您可以为防火墙创建策略建议以阻止该应用程序。如果它是必需的，并且有新版本，则可以为操作分配任务以升级使用它的所有设备。如果它是必需的，并且还没有新版本，请对使用它的所有设备进行细分，并对他们的访问权限进行限制，确保只有必需使用该应用程序才能正常工作的人员和资源才能访问。通过了解网络上的应用程序，您可以在危险来临时迅速采取行动保护资产。

在 **Networks**（网络） > **Applications**（应用程序）页面上，IoT Security 会显示网络上的 IoT 设备正在使用的所有应用程序。



Application	App Risk	Number of Devices	Category	Subcategory	Technology	Profiles	Evasive
dns-base	3	2,049	networking	infrastructure	network-protocol	Advantech Industrial PC a...	No
ssl	4	1,754	networking	encrypted-tunnel	browser-based	Advantech Industrial PC a...	No
ntp-base	2	1,707	networking	infrastructure	network-protocol	Advantech Industrial PC a...	No
ping	2	1,644	general-internet	internet-utility	network-protocol	Advantech Industrial PC a...	No
ssh	4	1,370	networking	encrypted-tunnel	client-server	APC Smart PowerSupply a...	No
snmp-base	2	1,343	networking	infrastructure	client-server	AIC Device and 30 more	No
traceroute	2	1,265	general-internet	internet-utility	network-protocol	Advantech Industrial PC a...	No
lpd	3	1,221	business-systems	management	client-server	Arista Network Switch and...	No
unknown-tcp	1	1,211	unknown			AIC Device and 23 more	No
web-browsing	4	1,050	general-internet	internet-utility	browser-based	Advantech Industrial PC a...	No
paloalto-updates	2	729	business-systems	software-update	client-server	Aruba UXI Sensor and 6 m...	No
snmpv3	1	665	networking	infrastructure	client-server	APC Smart PowerSupply a...	No
pan-db-cloud	1	563	business-systems	general-business	client-server	Aruba UXI Sensor and 6 m...	No
gnutella	5	525	general-internet	file-sharing	peer-to-peer	Arista Networks Device an...	Yes
paloalto-dns-securi...	1	505	business-systems	general-business	client-server	DTEN Display Board PC M...	No
snmpv2	2	474	networking	infrastructure	client-server	APC Smart PowerSupply a...	No
dhcp	2	444	networking	infrastructure	network-protocol	APC Smart PowerSupply a...	No
			general-internet			Industrial PC a...	No

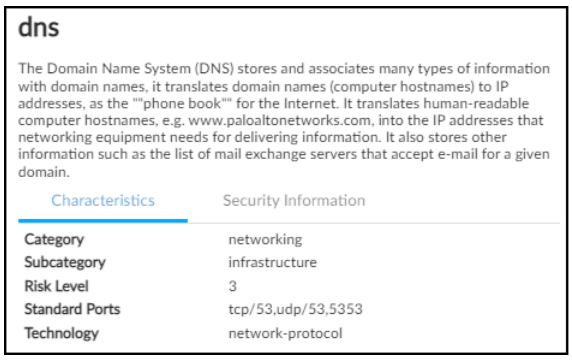
“应用程序”页面显示与页面顶部设置的站点和时间范围过滤器匹配的 IoT 设备检测到的唯一应用程序总数。

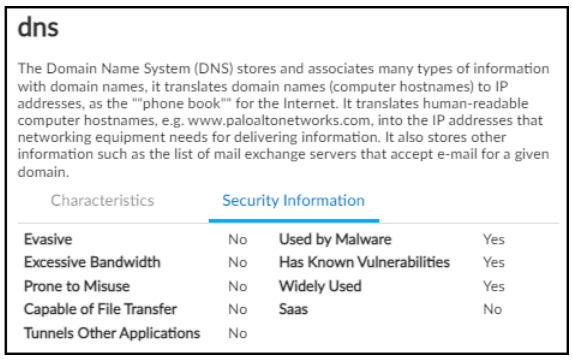
IoT Security 门户会忽略此页面上的设备类型过滤器，并始终显示“所有 *IoT*”设备的应用程序，如页面顶部的蓝色图标所示。

IoT Security 一旦发现并识别设备和网络，就会显示它们，但它会收集一天内有关检测到的应用程序的数据，然后编制一个列表。然后，它会在“应用程序”页面上显示该列表，直到编译在网络上检测到的下一个每日应用程序列表。开始使用 IoT Security 时，您可能会发现，它先在“设备和网络”页面上显示数据，然后在“应用程序”页面上显示内容。这可能是因为 IoT Security 尚未生成应用程序列表。这样，它此后每天都会继续这样做。

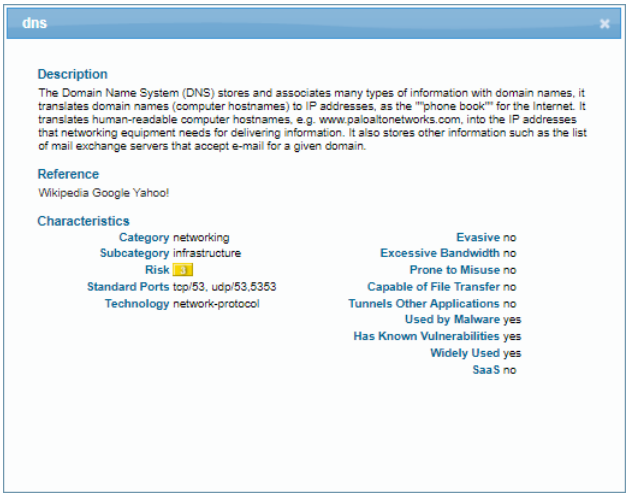
如果将时间范围过滤器设置为 **1 Day**（**1** 天）、**1 Week**（**1** 周）或 **1 Month**（**1** 个月），则“应用程序”页面会显示您设置的时间范围的数字。然而，因为 IoT Security 将其检测到的应用程序组织到每日列表中，因此，**1 Hour**（**1** 小时）过滤器与 **1 Day**（**1** 天）过滤器显示同一组唯一应用程序，这是您可以看到的最小的应用程序列表。另外，IoT Security 不会将应用程序详细信息保留超过一个月。因此，**1 Year**（**1** 年）时间范围过滤器与 **1 Month**（**1** 月）过滤器显示同一组唯一应用程序，这是您可以看到的最大的应用程序列表。

有关监视的每个应用程序，IoT Security 会提供来自 Applipedia 的数据。当出现新的应用程序时，您可以使用此数据来确定它是否符合预期，并查看它给您的网络带来的风险级别。例如，对于 DNS，下面会显示 IoT Security 从 Applipedia 检索的应用程序描述、特征和安全信息：





下面是 Applipedia 中提供的有关 DNS 的相同信息：



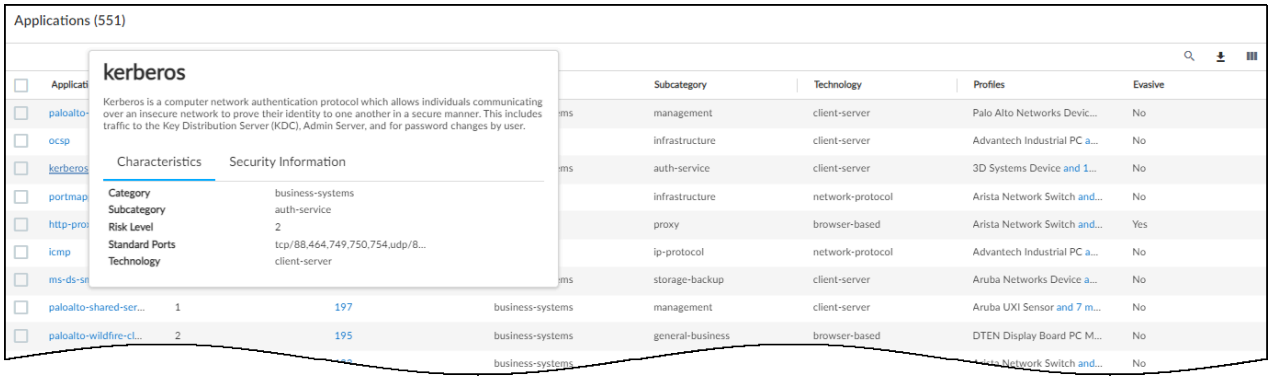
下面总结了安全信息的不同特征和类型，其中 IoT Security 从 Applipedia 检索并显示每个应用程序。

应用程序特征	
类别	单个应用程序所属的广泛应用程序类型
子类别	针对单个应用程序的更具体的应用程序类型
风险等级	应用程序固有的风险级别，由下表中列出的特征确定，风险等级从 1 到 5
标准端口	应用程序使用的协议和标准服务端口号
技术	应用程序的功能：网络协议、客户端-服务器、点对点或基于浏览器

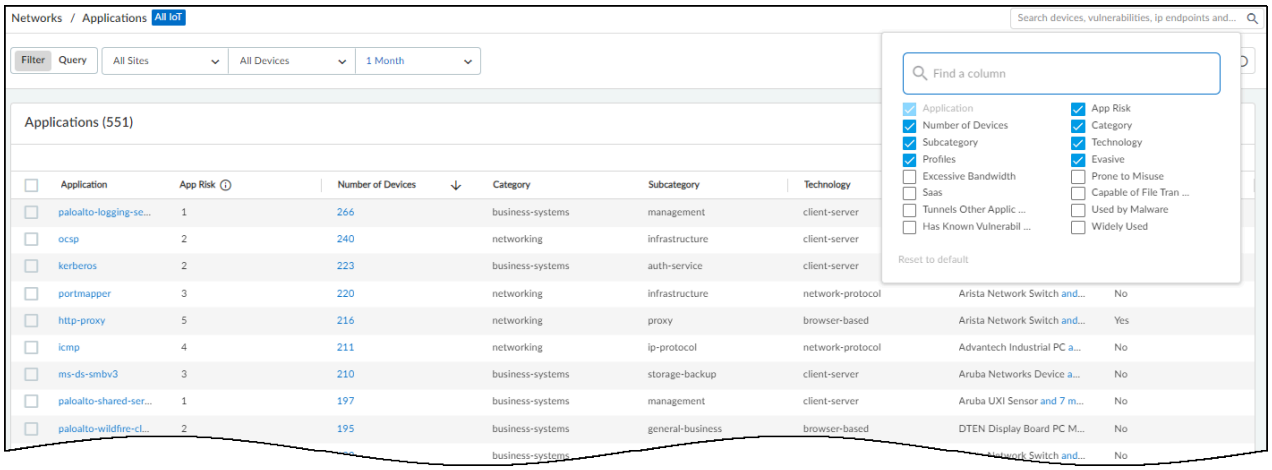
应用程序安全信息	
回避	是 = 应用程序将端口或协议用于其最初预期目的以外的其他目的，目的是逃避防火墙策略实施。
过多带宽	是 = 应用程序在正常使用期间定期消耗至少 1 Mbps。
易误用	是 = 该应用程序通常用于恶意目的，或者很容易设置为暴露超出用户预期的内容。
能够传输文件	是 = 应用程序能够通过网络将文件从一个系统传输到另一个系统。
其他隧道应用程序	是 = 应用程序可以在其协议内传输其他应用程序。
由恶意软件使用	是 = 已知恶意软件使用应用程序进行传播、攻击或数据盗窃，或者应用程序已与恶意软件一起分发。
有已知漏洞	是 = 应用程序至少有一个公开报告的漏洞。（基于 Web 的应用程序始终设置为“是”，因为 HTTP 始终存在漏洞。
广泛使用	是 = 应用程序可能有超过 1,000,000 个用户。
SaaS	是 = 应用程序基于云的，并通过软件即服务 (SaaS) 提供。否 = 应用程序托管在本地。

其中许多解释来自知识库文章“如何确定应用程序、间谍软件和防病毒软件的风险级别”。这里可以阅读有关 *Applipedia* 提供的信息以及如何计算风险评分的更多信息。

要在“应用程序”页面上查看 Applipedia 中有关应用程序的数据，请单击或将光标悬停在应用程序名称上，以查看一个弹出窗口，其中包含直接从 Applipedia 获取的应用程序信息。

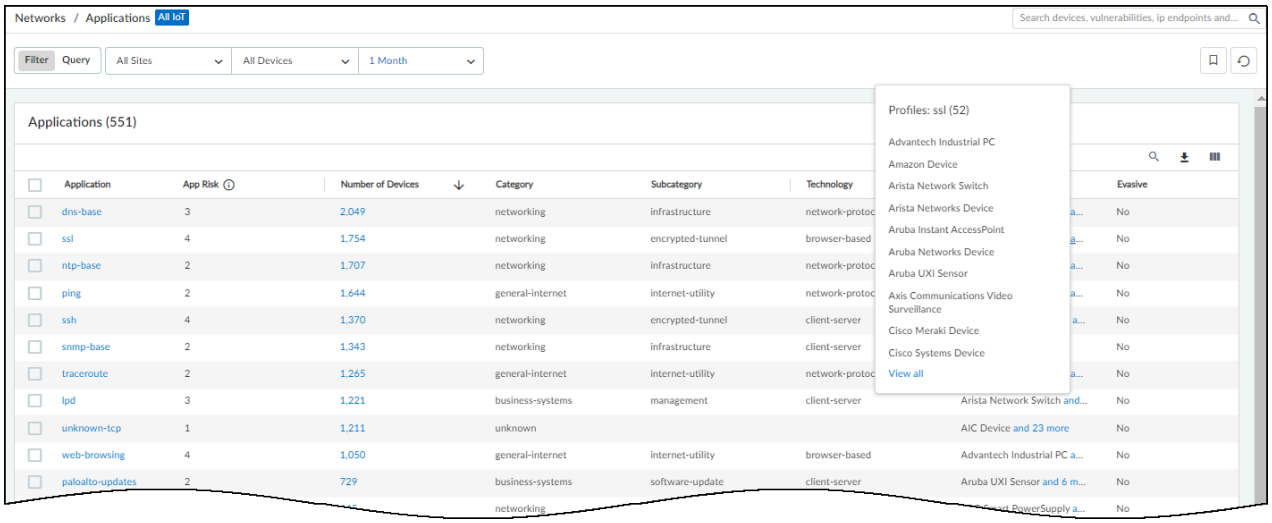


此外，使用列选取器在“应用程序”页面的列中显示来自 Applipedia 的信息。



单击“设备数量”列中的数字以打开应用了过滤器的“设备”页，以仅显示使用相应应用程序的设备。

单击光标或将光标悬停在“配置文件”列中条目的蓝色文本上，将显示使用该应用程序的所有配置文件的列表。



检测 IoT 设备漏洞

IoT Security 使用机器学习来检测漏洞和评估风险。它基于 IoT 设备的网络流量行为和动态更新的威胁馈送进行检测和评估。

- IoT 设备漏洞检测
- 漏洞概述指示板
- 漏洞页面
- 漏洞详细信息页面
- IoT 风险评估

IoT 设备漏洞检测

漏洞是指内置于设备的软件或硬件中的固有缺陷，通常是众所周知的，可以以某种方式利用。另一方面，风险除了考虑一个或多个潜在漏洞外，还考虑环境、配置、行为和安全策略相关因素。这种区别很重要，因为有些风险会出现在设备详细信息页面中，但不会出现在漏洞页面上，它们可能会影响 IoT Security 分配给漏洞的严重级别。

IoT Security 认为，当漏洞适用于特定设备类型、型号和版本号，并且一个或多个设备与指定的设备类型匹配，但其型号和/或版本号未知时，该漏洞是潜在的。同样，出于相同的原因，设备也被认为可能有漏洞。

如果漏洞仅适用于具有某些序列号的设备，并且存在序列号未知但在所有其他方面与漏洞描述匹配的设备，则也可以将漏洞视为潜在漏洞。

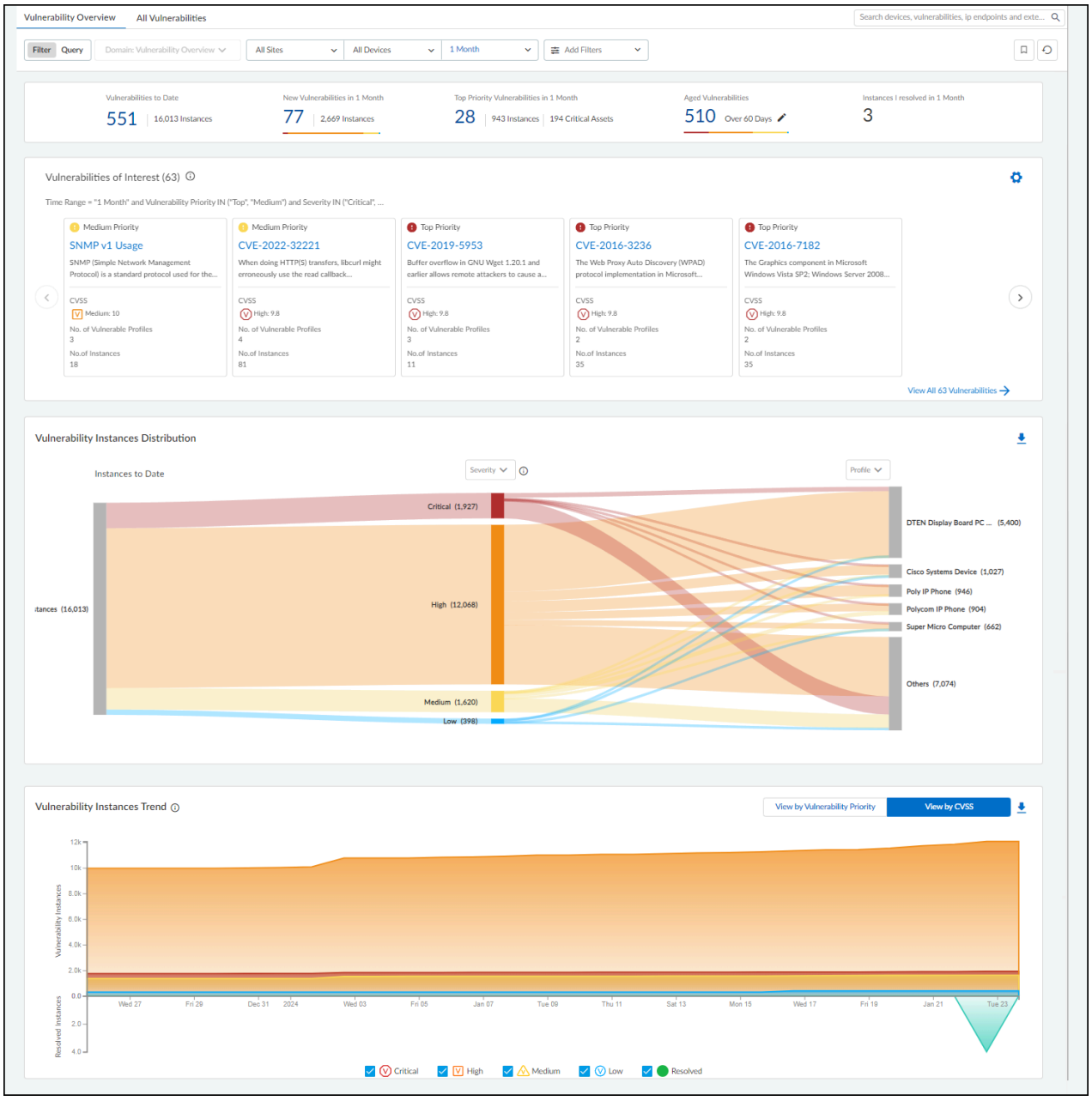
IoT Security 应用程序仅检测 *IoT* 设备的漏洞。它不为 *IT* 设备提供漏洞检测、警报、策略建议和网络行为分析。对于 *IT* 设备，*IoT Security* 应用程序仅提供设备标识。

漏洞概述指示板

漏洞概述指示板 [**Vulnerabilities**（漏洞） > **Vulnerability Overview**（漏洞概述）] 允许您自定义有关漏洞和漏洞实例的信息的显示方式，以便您可以从不同角度查看它们对设备的影响。通过设置过滤器，您可以确定显示信息的范围，通过定义查询和设置，您可以控制漏洞类型和要查看的设备类型。

您在页面顶部设置的过滤器不会影响“感兴趣的漏洞”部分。此处显示的漏洞由您在该部分内部配置的设置决定。

该指示板包括四个主要部分，可帮助您轻松查看关键统计数据、识别感兴趣的主要漏洞、深入了解这些漏洞在不同设备组之间的分布以及跟踪漏洞实例趋势。



页面顶部是站点、设备类别和时间范围的过滤器定义参数内的关键漏洞统计信息的摘要。

- **Vulnerabilities to Date**（目前的漏洞）— 这是自您开始使用 IoT Security 租户以来检测到的漏洞总数。

  虽然 IoT Security 在其数据库中保留安全警报一年，但并未对漏洞设置此时间限制。如果您使用 IoT Security 超过一年，它将继续显示一年多前检测到的漏洞。

- <time range> 内的 **New Vulnerabilities**（新漏洞）— 这是页面顶部数据过滤器中指定的时间范围内检测到的漏洞总数。

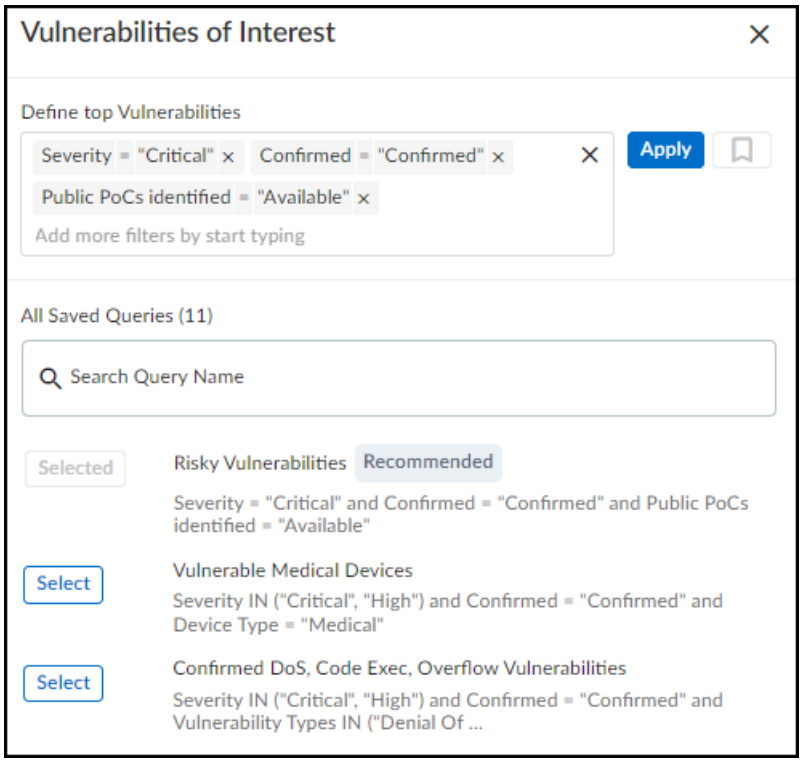
- <time range>内的 **Top Priority Vulnerabilities in**（高优先级漏洞）— 这是 IoT Security 列为“Top”的漏洞总数。（也有"中"和"低"优先级。）然后是这些漏洞的实例数及其影响的关键资产数。如果单击此处的链接之一，IoT Security 将打开应用了过滤器的 **All Vulnerabilities**（所有漏洞）页面，仅显示 **Vulnerabilities Dashboard**（漏洞指示板）上设置的站点、设备类型和时间范围内的最高优先级漏洞。

- **Aged Vulnerabilities**（过时漏洞）— 这是超过指定时间范围（30、60、90 或 180 天）仍未解决的所有漏洞的总和。

- <time range> 内的 **Instances I resolved**（我解决的实例）— 这是分配给当前登录的人员并在页面顶部数据过滤器中指定的时间范围内解决的漏洞实例总数。

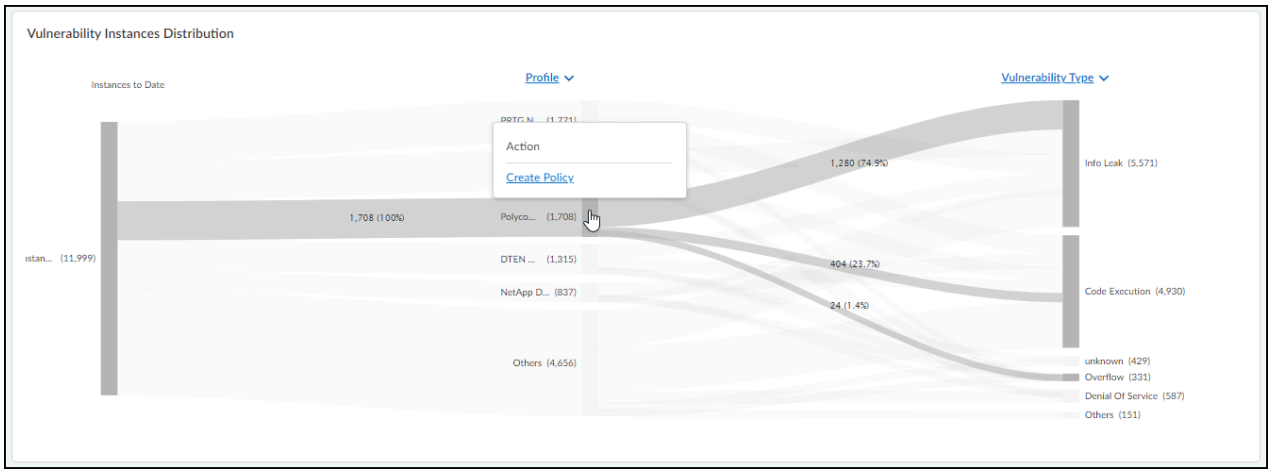
Vulnerabilities of Interest（感兴趣的漏洞）— 定义对您最重要的漏洞标准。然后，IoT Security 将显示响应您查询的 CVSS 得分最高的前十个漏洞，以及影响首先显示的设备配置文件最多的漏洞。例如，如果您想查看最近一周内检测到的特定供应商或配置文件的漏洞，请单击齿轮图标 (⚙)，然后配置查询以显示您感兴趣的漏洞。IoT Security 将显示与您的条件匹配的十个影响最广泛的最严重漏洞。

默认情况下，IoT Security 使用预定义的“风险漏洞”查询来搜索已确认的公开提供概念证明 (PoC) 的关键漏洞。您可以编辑此查询以定义其他感兴趣的属性，然后单击书签图标 (🔖) 将其保存以供重复使用。



Vulnerability Instances Distribution（漏洞实例分布）— 桑基图表允许您查看漏洞实例在不同设备组中的分布。从左到右阅读图表，您将从左侧开始，在页面顶部找到与站点和设备类别过滤器匹配的所有漏洞实例。（无论为页面设置的时间范围过滤器如何，此图表均显示迄今为止的所有漏洞实例。）然后，图表将这些实例与中间的分组类型关联起来，并再次将这些实例与右侧的另一种分组类型关联起来。这些分组的选项包括 **Severity**（严重性）、**Vulnerability Type**（漏洞类型）、**Status**（状态）、**Device Type**（设备类型）、**Device Category**（设备类别）、**Profile**（配置文件）、**Vendor**（供应商）、**Exploit Status**（漏洞利用状态）、**Attack Vector**（攻击途径）（CVE 中定义的利用漏洞所需的访问类型）和 **Vulnerability Priority**（漏洞优先级）（高、中、低）。漏洞实例在图表中按严重性（当选择严重性组时）、优先级（当选择漏洞优先级时）或实例计数（对于所有其他类型）垂直分布。严重性最高、优先级最高或实例最多的组位于图表的顶部。当有五个以上的分组时，桑基控制图会显示前五个，然后将其他所有内容收集到“其他”组中。将光标悬停在 **Others**（其他）上以查看接下来的 10 个分组的列表，然后单击 **View all**（查看全部）以查看包含完整列表的弹出面板。

当您使用 **Profile**（配置文件）对实例进行分组，然后将光标悬停在特定配置文件的柱子上的某个区域上时，IoT Security 将显示一个操作弹出面板，允许您创建以该配置文件为源的一组recommended policy rules（建议策略规则）。



单击 **Create Policy**（创建策略）后，IoT Security 将打开 **Assets**（资产） > **Devices**（设备） > *profile-name* > **Create New Policy Set**（新建策略集）。从这里可以根据需要修改自动生成的策略集，保存它，然后激活它以供防火墙导入。

例如，要查看不同设备配置文件和不同漏洞类型之间的漏洞实例比率，请为中间柱子选择 **Profile**（配置文件），为右侧柱子选择 **Vulnerability Type**（漏洞类型）。左后和中间之间的灰色带显示有多少实例属于前五个设备配置文件中的每一个，中间柱子和右侧柱子之间的灰色带显示每个配置文件中有多少实例属于不同的漏洞类型。每个带都有标签，并显示每个配置文件的漏洞实例总数（左侧），以及该配置文件的每个漏洞类型（右侧）。带的宽度可让您一目了然地看到漏洞实例的相对数量。将光标悬停在柱子的某个部分上会显示相邻波段的实例百分比。

颜色仅表示表示漏洞严重级别的含义：红色 = 关键，橙色 = 高，黄色 = 中，蓝色 = 低。对于其他类型的分组，半透明的灰色阴影仅用于区分一个波段与另一个波段。

要从桑基图表中下载您的记录或报告的数据，请单击图表右上角的下载图标 ()。IoT Security 将其另存为 .xlsx 文件，第一张工作表上有漏洞实例分布信息，第二张工作表上有漏洞实例的完整列表。

Vulnerability Instances Trend（漏洞实例趋势）— 实例趋势图显示指定时间段内漏洞实例的累积计数和已解决实例的每日非累积计数。这将直观地显示漏洞实例趋势，以帮助漏洞管理团队查看漏洞实例的数量是否随时间而增加或减少。您可以查看按漏洞优先级（最高、中、低优先级）或

CVSS 分数（关键、高、中、低）显示的数据。使用图表上方右侧的切换键在两个视图之间切换。使用 CVSS 分数视图时，图表还会显示已解决漏洞实例的数据，这有助于团队衡量其在漏洞解决方面的进展。将光标悬停在图表的不同点上，可查看具有不同优先级的漏洞实例数或不同日期的 CVSS 分数。

要从报告或记录的实例趋势图下载数据，请单击图表右上角的下载图标 ()。IoT Security 将其另存为 .xlsx 文件，其中包含指定时间段内迄今为止的漏洞实例数和已解决实例数。

漏洞页面

漏洞页面 [**Vulnerabilities**（漏洞） > **Vulnerability Overview**（漏洞概述） > **All Vulnerabilities**（所有漏洞）] 列出 IoT Security 已检测到或通过第三方集成了解到的漏洞。

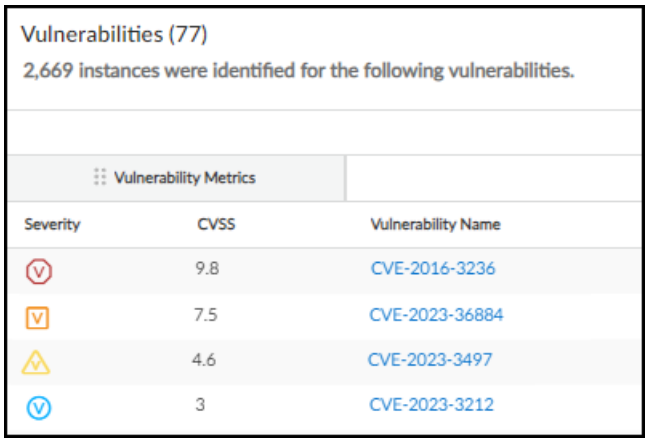
您可以在任意列中搜索文本字符串，下载漏洞列表，创建过滤器以仅显示您想要看到的漏洞，并控制您想要显示和隐藏的列。

尽管表中的“严重性”列仅显示图标，但您仍然可以通过严重性级别字词“关键”、“高”、“中”和“低”进行搜索。

您还可以设置每页显示的行数（从 5 到 200）并在多页之间导航。

CVSS 分数范围	严重性级别
9.0 — 10.0	关键
7.0 — 8.9	高
4.0 — 6.9	中
< 4.0	低

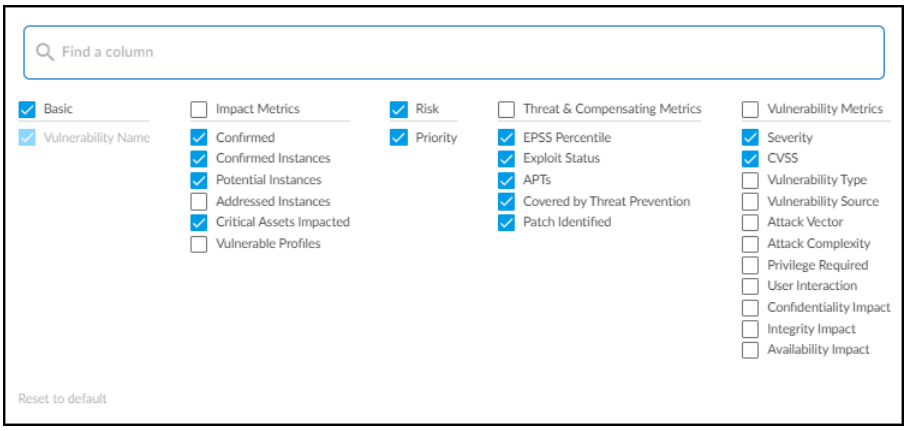
虽然 IoT Security 系统中的严重性级别反映了通用漏洞评分系统 (CVSS) 分数，但两者之间并不总是存在直接关联。例如，设备中的硬编码密码的 CVSS 分数可能是 10.0，但 IoT Security 严重性级别为“高”，而不是“关键”。当没有证据证明该设备可以通过互联网或未经授权的用户访问时，就会发生这种情况。虽然美国国家标准与技术研究院 (NIST) 通常为漏洞分配 CVSS 分数，但 IoT Security 根据每个案例的具体情况，为漏洞分配“风险严重性”级别。



例如，虽然第一个漏洞的 CVSS 评分为 9.8，但其风险严重性为“高”，而不是“关键”。IoT Security 严重性不仅基于 CVSS 评分，还基于其他决定性风险因素。

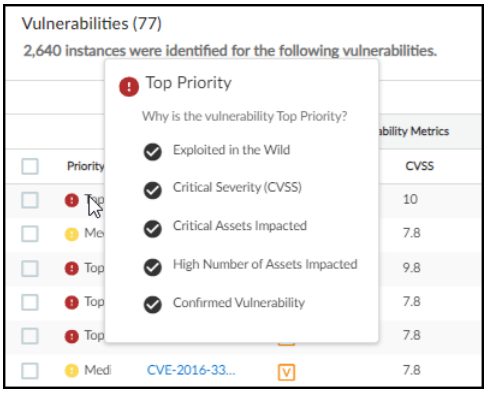
漏洞表的列分为五类：风险、基础、漏洞指标、威胁指标和影响指标。虽然风险和基本类别各自包含一列，但三个指标类别各自包含一组列。您可以单击并拖动列以在各自的组内重新排列它们，或者单击并拖动组以在表格上重新排列它们的顺序。但是，启用分组后，您无法单击并拖动组外的列。要禁用分组，请单击右侧表格上方的三个垂直点图标，然后单击 **Ungroup columns**（取消列分组）。取消分组后，您可以重新定位它们，以便它们与之前分成其他组的列混合在一起。

与 IoT Security 门户上的其他表格相似，您可以控制显示哪些列。单击右侧表格上方的三个垂直点，单击 **Edit columns**（编辑列），然后选择要查看的列并清除要隐藏的列。



风险 — 风险是对漏洞带来的潜在危险的一种排名。它是多种因素共同作用的结果，这些因素结合起来可以帮助您确定需要关注和解决的漏洞的优先次序。

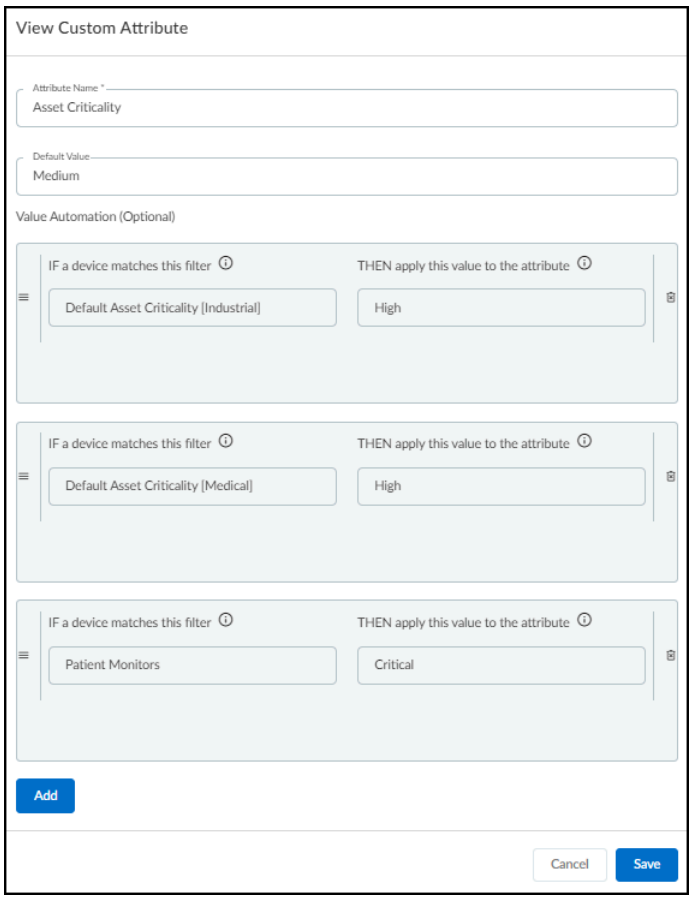
- 优先事项 — IoT Security 通过权衡各种因素来计算发生攻击的可能性及其对您的资源造成的影响，从而确定最高、中、低的排名。将光标悬停在优先级上可以查看影响其排名的风险指标摘要。



当此处显示 ***Processing...***（正在处理…）时，表示 *IoT Security* 仍在确定漏洞的优先级。因为 *IoT Security* 每天运行一项服务来确定优先级，最多可能需要 *24* 小时才能确定设备的优先级。

IoT Security 自动默认为工业和Medical设备分配高资产关键性级别，为所有其他设备分配中等资产关键性级别。它通过系统定义的资产关键性属性实现此目的，您可以在 **Settings**（设置） > **Custom Attributes**（自定义属性）中看到该属性。您还可以在 **Assets**（资产） > **Devices**（设备）上定义过滤器并将其添加到资产关键性属性，以根据设备类别、配置文件或供应商等属

性为设备分配不同的资产关键性级别。例如，您可能首先在 **Assets**（资产） > **Devices**（设备）上定义一个病人监护配置文件过滤器，然后向系统定义的资产关键性属性添加一条规则，该规则规定，如果设备与病人监护配置文件过滤器匹配，则 IoT Security 将对其应用“关键”资产关键性级别。



您还可以在 ***Device Details***（设备详细信息）页面上编辑单个设备的资产关键性。单击自定义属性部分中的 ***Edit***（编辑），然后将资产关键性字段更改为所需的级别。

基本 — 这是漏洞的名称。

- 漏洞名称 — 漏洞的名称或常见漏洞暴露 (CVE) 编号。这会链接到漏洞详细信息页面。

漏洞指标 — 这些指标与漏洞以及利用漏洞的攻击有关

- 严重性 — 漏洞的严重性级别：关键、高、中或低。
- **CVSS** — 漏洞的 CVSS（通用漏洞评分系统）分数。
- 漏洞类型 —（默认不显示）这标识了漏洞的类型，例如信息泄露、溢出或代码执行。
- 漏洞来源 —（默认不显示）识别设备漏洞的来源：IoT Security、第三方集成（Rapid7、Qualys、Tenable）或 IoT Security 设备软件库。

- 攻击媒介 — （默认不显示）也称为“访问媒介”，这是攻击者利用漏洞所必须拥有的访问类型。度量值在 CVE 中定义。漏洞分数会随着与目标的可能距离的增加而增加：
  - **Physical**（物理） — 攻击者必须物理接触或控制易受攻击的设备。
  - **Local**（本地）— 攻击者必须在本地发起攻击，或者使用社会工程学欺骗用户帮助发起攻击。
  - **Adjacent**（相邻）— 攻击者必须能够访问与易受攻击的设备相同的物理或逻辑网络。
  - **Network**（网络） — 攻击者可以从网络上任何可以访问易受攻击设备的地方远程发起攻击。

  当攻击媒介未定义时，它被归类为“未知”。
- 攻击复杂性 — （默认不显示）表示利用漏洞所需的复杂性级别“低”或“高”。
- 所需权限 — （默认情况下不显示）表示执行漏洞利用所需的管理权限级别，可以是“无”、“低”或“高”。
- 用户交互 — （默认不显示）除威胁行为者之外的用户是否必须以某种方式参与利用漏洞。此处显示的值是“无”或“必需”。
- 机密性影响 — （默认不显示）攻击者是否可以利用漏洞访问敏感信息以及可能泄露的敏感程度。值为“无”、“低”和“高”。
- 完整性影响 — （默认不显示）受保护的信息是否可能以任何方式被更改。值包括“无”（不丢失数据完整性）、“低”（可以修改少量数据）和“高”（可以修改任意或所有数据）。
- 可用性影响 — （默认不显示）利用漏洞是否会导致数据或设备无法访问。其值为“无”（无可用性损失）、“低”（性能较差或偶尔丢失可访问性）和“高”（完全丢失可访问性）。

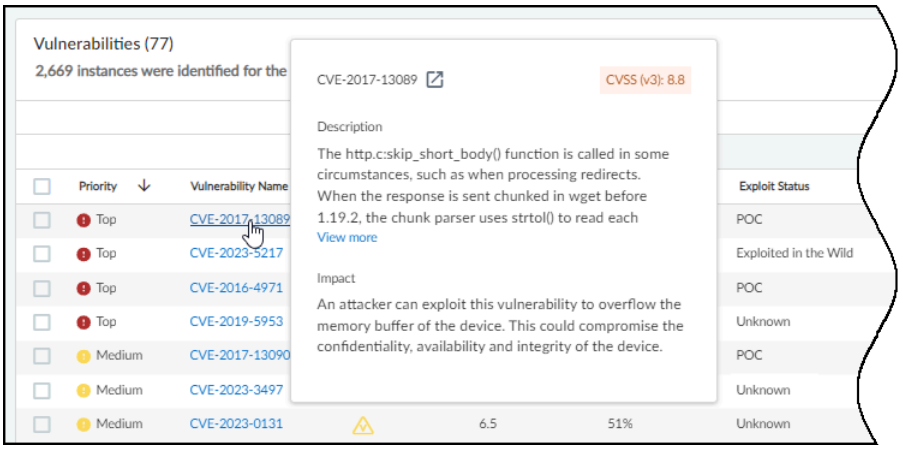
威胁指标 — 这些指标主要关注漏洞对网络及其设备的安全造成的威胁。

- **EPSS** — 漏洞预测评分系统 (EPSS) 每天估计未来 30 天内漏洞被利用的概率。要了解有关 EPSS 的更多信息，请参阅 EPSS 模型。
- 漏洞状态 — （默认不显示）显示是否已确定漏洞的概念证明 (POC) 或尚未确定（“未知”）。
- **APT** — （默认不显示）显示是否存在任何已知的高级持续性威胁 (APT) 漏洞利用。值为“是”或“否”。
- 威胁防护涵盖 — （默认情况下不显示）表示漏洞是否被 Palo Alto Networks 威胁防护应用程序涵盖（“是”）或不涵盖（“否”）。

影响指标 — 这些指标深入了解了利用漏洞所造成的影响的广泛性和严重性。

- 已确认 — 表示是否确认漏洞适用于一个或多个设备。空字段表示这是一个潜在的漏洞。
- 已确认实例 — 已确认存在漏洞的设备数量。此数字链接到漏洞详细信息页面。
- 潜在实例 — 可能存在漏洞但尚未确认的设备数量。此数字还链接到漏洞详细信息页面。
- 已解决的实例 — （默认不显示）已解决的漏洞实例数。
- 受影响的关键资产 — 被归类为受漏洞影响的关键资产的数量。
- 易受攻击的配置文件 — 已确认或潜在漏洞适用的设备配置文件的数量。

当您将光标悬停在“漏洞”列中的条目上时，会弹出一个面板，显示其描述和影响。



单击漏洞条目的名称将打开“漏洞详细信息”页面。

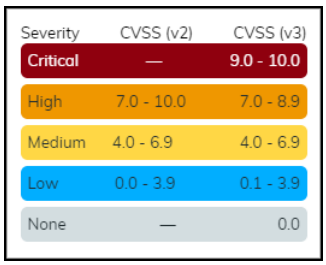
漏洞详细信息页面

单击“漏洞”列中的 CVE（常见漏洞和暴露）链接或“漏洞”页面上“已确认的实例”或“潜在实例”列中的数字，将打开该漏洞的“漏洞详细信息”页面 [**Vulnerabilities**（漏洞） > **Vulnerability Overview**（漏洞概述） > **Vulnerabilitiy Details**（漏洞详细信息）]。在这里，您可以阅读漏洞的描述，查看漏洞的详细信息，并了解它会影响哪些设备配置文件。您还可以查看漏洞影响或可能影响哪些设备。

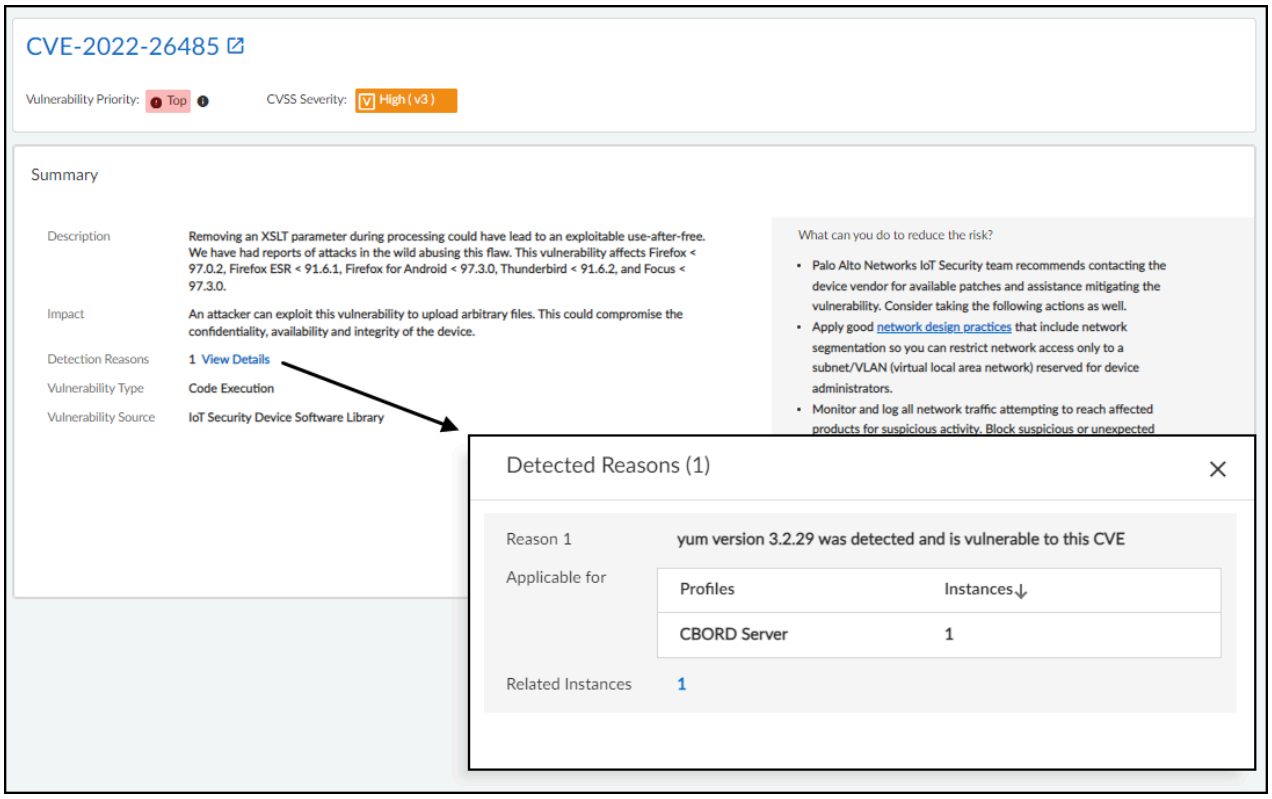
漏洞详细信息页面的顶部有几个重要属性：

- CVE ID 链接到美国国家标准与技术研究所 (NIST) 数据库中有关该漏洞的页面。例如，单击 CVE-2022-4436 会打开 https://nvd.nist.gov/vuln/detail/CVE-2022-4436。

- CVSS（通用漏洞评分系统）分数以 0-10 的等级对漏洞进行排名，其中 0 表示最不严重，10 表示最严重。
- 基于 CVSS 的 IoT Security 评级系统将漏洞分数分为几个严重性级别之一。共有两个 CVSS 版本，都会显示：



接下来是描述漏洞是什么、如何检测漏洞以及发现漏洞来源的章节。它还解释了漏洞被利用可能造成的影响，以及您可以采取哪些措施来修复该漏洞。最后，还有一张图表显示了按配置文件分组的受影响设备的总数以及每组的相对大小。



摘要

- **Description**（描述）部分总结了漏洞。
- **Impact**（影响）部分解释了攻击者如何利用漏洞及其构成的威胁。
- **Detection Reasons**（检测原因）解释了如何检测到已确认的漏洞实例。当您单击 **View Details**（查看详细信息）时，页面右侧会出现一个面板，显示每个检测原因、其适用的设备配置文件以及针对不同配置文件检测到的漏洞实例的数量。（未显示检测潜在漏洞的原因。）
- **Vulnerability Type**（漏洞类型）标识漏洞的类别，例如代码执行、信息泄漏、溢出和拒绝服务。

- **Vulnerability Source**（漏洞来源）确定漏洞的检测位置。基于固件、型号和操作系统等设备属性时，检测来源之一是 IoT Security。当检测基于设备上运行的软件和应用程序时，另一个来源是 IoT Security 设备软件库。另一个来源是 IoT Security 集成的以下内容的第三方漏洞扫描程序：Qualys、Rapid7 或 Tenable。
- IoT Security 列出了所有已识别的可以修复漏洞的软件补丁。

  我们建议您在安全或漏洞管理团队或产品供应商对设备进行认证以确保不会出现任何意外结果或副作用之前，不要将由 *IoT Security* 识别的补丁更新应用到设备上。
- 摘要部分的右侧是建议列表。它通常包括您可以采取的各种选项，以降低漏洞构成的风险，甚至修复问题。

Vulnerability Metrics（漏洞指标）— 在本节中，您可以查看 CVE 子指标分数，这些分数可以进一步了解漏洞严重性级别，帮助您确定补救工作的优先顺序。例如，即使其他漏洞的 CVSS 分数更高，可以远程利用的漏洞也可能需要比其他漏洞更紧急的响应。

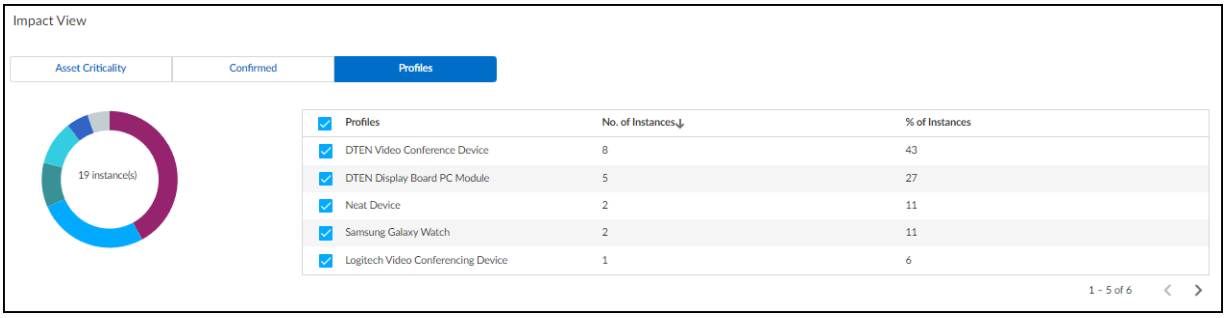
- 漏洞利用率指标包括攻击向量（网络、邻近、本地或物理）、攻击复杂度（高或低）、发起攻击所需的权限，以及漏洞期间是否需要除攻击者之外的人为操作。
- 影响指标表明漏洞可能影响哪些领域（机密性、完整性和可用性）以及这些领域的影响 — 无、低或高。
- 范围指标表明已利用漏洞的影响是仅限于受影响的组件（未更改），还是可以扩展到其他组件（已更改）。

Threat & Compensating Metrics（威胁和弥补指标）— 在本节中，您可以查看有关漏洞被利用的可能性、已知发生的漏洞类型以及是否有办法通过 Palo Alto Networks 威胁防御应用程序弥补威胁的信息。

- 漏洞预测评分系统 (EPSS) 百分位数是对未来 30 天内漏洞被利用概率的每日估算值。要了解有关 EPSS 的更多信息，请参阅 EPSS 模型。
- 漏洞利用状态可以是以下之一：
  - **Unknown**（未知）— 没有已知或武器化的恶意软件利用此漏洞。
  - **POC** — 有已知的代码可以利用该漏洞来证明安全漏洞。
  - **Weaponized**（武器化）— 有一个已知的恶意漏洞或持续攻击目标。
  - **Exploited in the Wild**（外部利用）— 威胁行为者或已知已利用漏洞 (KEV) 目录公开报告了在外部利用的该漏洞。
- 通过单击已识别漏洞的 **View Details**（查看详细信息），您可以看到已知的 POC 和武器化漏洞列表（但不能查看任何状态为 “未知”或“外部利用”的漏洞）。对于每个漏洞，都有一个 URL（来源），您可以在其中了解更多信息、漏洞利用状态和漏洞发布日期。
- 高级持续威胁 (APT) 指示 APT 是否已知使用了任何漏洞。通过单击 **View Details**（查看详细信息），您可以看到 APT 列表。每一个都有 APT 的名称、对它的描述、它们所针对的国家、它们利用的已知 CVE 以及它们采用的策略和技术。
- 威胁防御覆盖范围指明漏洞是否受到 Palo Alto Networks 威胁防御应用程序的保护。通过单击 **View Details**（查看详细信息），您可以查看漏洞的名称、其唯一威胁 ID 号、支持该漏洞的最低 PAN-OS 版本、其首次发布和最新更新的日期，以及可以了解更多信息的 URL（参考）。

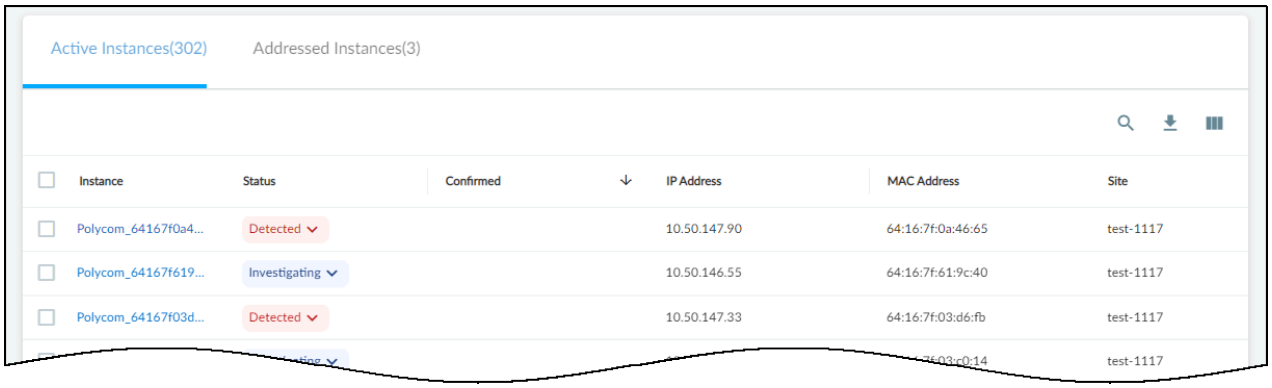
Impact View（影响视图）— 在本节中，您可以看到漏洞影响的设备数量及其各种严重性：关键、高、中、低。严重性可以帮助您评估您的组织在遭到入侵时将受到的影响程度。

- **Asset Criticality**（资产重要性）— 在“资产重要性”选项卡中，图表和随附的表格显示了受漏洞影响的资产（实例）总数以及每个重要程度级别的受影响资产的数量和百分比。该图表以数字形式直观地显示了表中包含的数据。通过选中并清除表格中的“关键”、“高”、“中”和“低”复选框，可以在图表中显示和隐藏相应的区段。
- **Confirmed**（已确认）— 在“已确认”选项卡中，图表和表格显示了已确认易受攻击的资产总数以及可能存在漏洞但尚未确认的资产总数。除总数外，它们还显示了已确认和未经证实的脆弱资产的百分比。您可以选中并清除每行的复选框以在图表中显示或隐藏相应的分段。
- **Profiles**（配置文件）— 在“配置文件”选项卡中，图表显示了按配置文件分组的受影响设备的总数以及每组的相对大小。当您将光标悬停在图表中的某个部分上时，会出现一个弹出窗口，标识该配置文件及其中的设备数量。当漏洞影响大量设备配置文件时，这尤其有用。

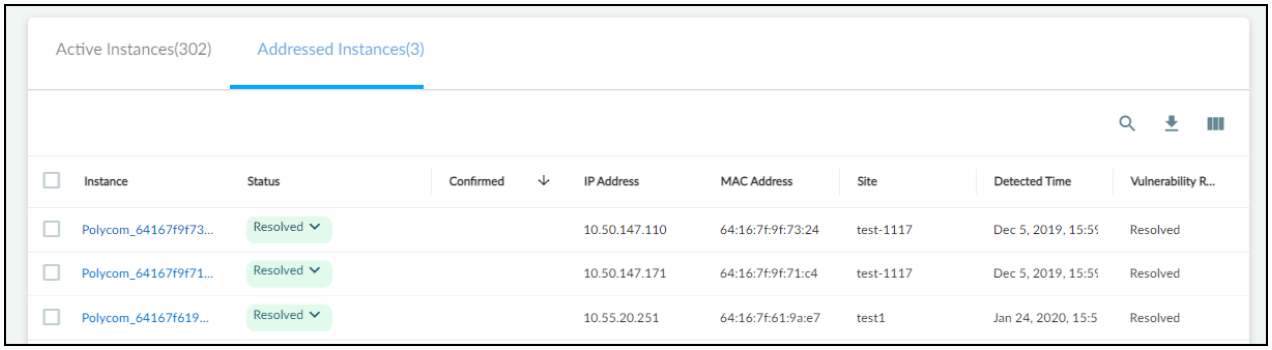


漏洞详细信息页面的底部有两个选项卡：活动实例和已寻址实例。每个选项卡上都有一个表格显示所有易受攻击和可能存在漏洞的设备，这些设备被称为实例。以下示例说明了这两种设备之间的区别。如果漏洞仅影响运行特定软件版本的设备，而 IoT Security 将一台设备上运行的版本识别为存在此漏洞，但无法识别另一台设备上的哪个软件版本，则第一台设备被视为存在已确认的漏洞，但不会将第二台设备视为存在已确认的漏洞。（如果“已确认”列中出现 **Yes**（是），则确认设备存在漏洞。如果“已确认”列为空，则设备可能存在漏洞，但尚未得到确认。）

漏洞实例最初显示在“活动实例”选项卡中。



将漏洞实例的状态更改为 **Resolved**（已解决）后，IoT Security 会将其从“活动实例”选项卡移至“已解决实例”选项卡。



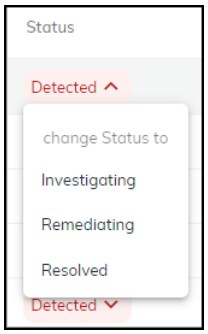
如果您稍后将已解析的实例更改为 **Detected**（已检测），它将自动移回“活动实例”选项卡。

要查看有关设备的更多信息，请单击“实例”列中的设备名称，在新的浏览器窗口或选项卡中打开设备的“设备详细信息”页面。

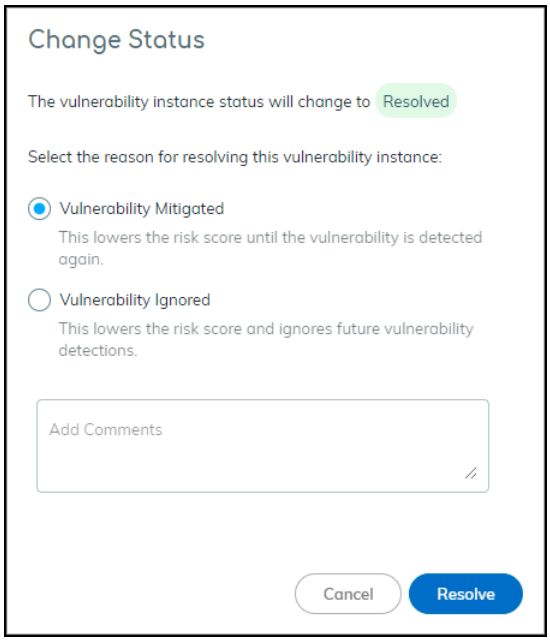
漏洞实例的状态从“已检测”状态开始。您可以将其保留在原处，也可以将其设置为其他状态以反映其在修复过程中的位置：

- 已检测：这是新检测到的漏洞实例的状态。如果未采取任何措施来调查、修正或解决它，则将其保持在此状态是有意义的。
- 正在调查：在漏洞实例的初步工作已经开始，经过验证、研究和影响分析之后，可以考虑将其设置为这种状态。
- 正在修正：在采取措施修复实例但尚未完成时，可以考虑将实例设置为这种状态。
- 已解决：要么缓解问题，要么忽略并接受该问题，实例就会得到解决。

要更改漏洞实例的状态，请单击“状态”列中的条目并选择其他状态。

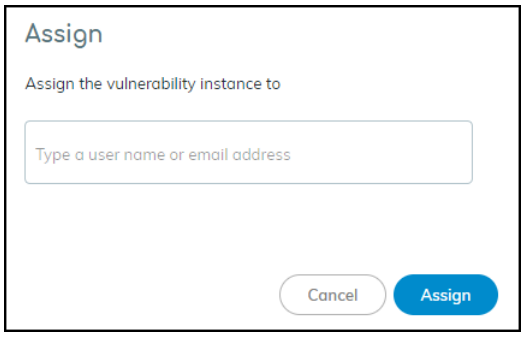


当您解决漏洞实例时，IoT Security 会提示您提供解决该漏洞的理由。



要将漏洞实例分配给某人进行处理，请选中该实例的复选框，然后单击 **More**（更多） > **Assign**（分配）。输入用户的用户名或电子邮件地址，然后单击 **Assign**（分配）。

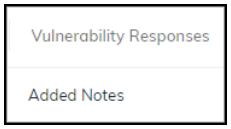
您向其分配漏洞实例的人员必须拥有 *IoT Security* 用户帐户，这样才能向相应的电子邮件地址发送消息。



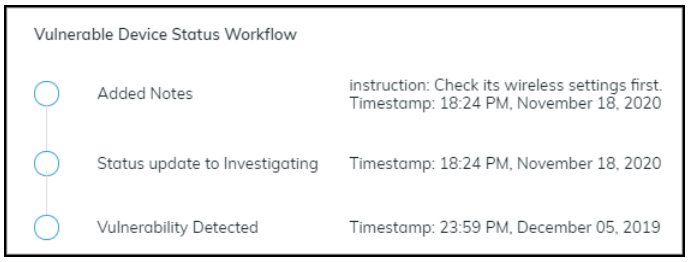
然后，用户会收到一封电子邮件，说明漏洞已分配给他或她，并提供漏洞链接以供调查。

要添加有关漏洞实例或正在进行的工作的备注，请选中该实例的复选框，然后单击 **More**（更多）**> Add notes**（添加备注）。输入备注，然后单击 **Add**（添加）。

漏洞响应列显示已添加的备注。



要阅读备注和之前所做的任何状态更改，请将光标悬停在“添加的备注”上。有关漏洞实例响应的历史记录显示在弹出窗口中。



IoT 风险评估

评估风险是一个发现漏洞和检测威胁的持续过程。在这个持续的过程中，IoT Security 衡量风险并根据观察到的风险量分配分数。实际上，IoT Security 从四个层面衡量和评分风险，从单个 IoT 设备开始，范围扩展到设备配置文件、站点，最后是组织。不同的分数提供了一种简单的方法来检查网络各个点和区域所存在的风险。

在评估风险时，IoT Security 同时使用静态和动态因素。静态风险形成基线并包括以下内容：

- 所有 MDS2 风险（针对医疗设备）
- 特定于配置文件的内在风险因素，例如操作系统、应用程序、角色、环境
- 难以缓解的趋势威胁
- 特定于配置文件或设备的使用行为

动态风险是在基线风险之上添加的：

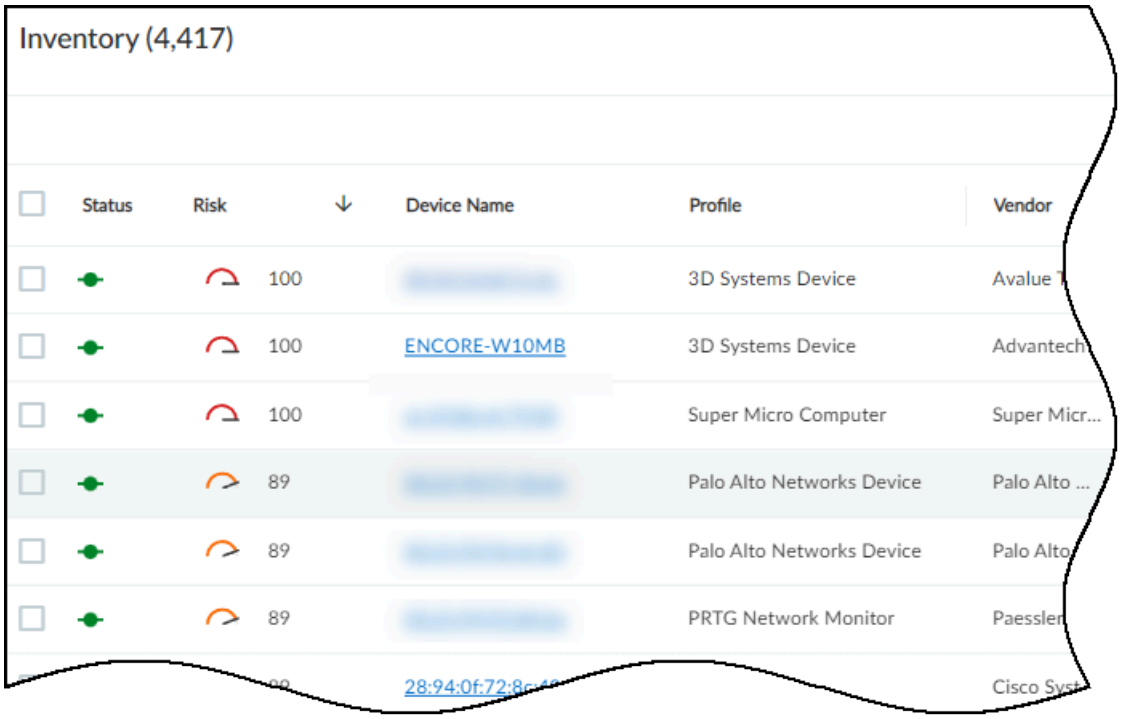
- 实时检测到的威胁（例如：警报）
- 行为风险（异常、用户实践问题）也会触发警报
- 漏洞，通过被动分析和检测以及使用集成的第三方漏洞扫描引擎（如 Qualys 和 Rapid7）进行漏洞扫描发现

通过收集和建模数据并分析漏洞和威胁，IoT Security 每天计算风险。它生成的风险评分包括警报、漏洞、行为异常和威胁情报。在计算设备配置文件、站点和组织的风险评分时，IoT Security 不仅考虑特定组内各个设备的得分，还考虑组中所有设备中存在风险的设备的百分比。

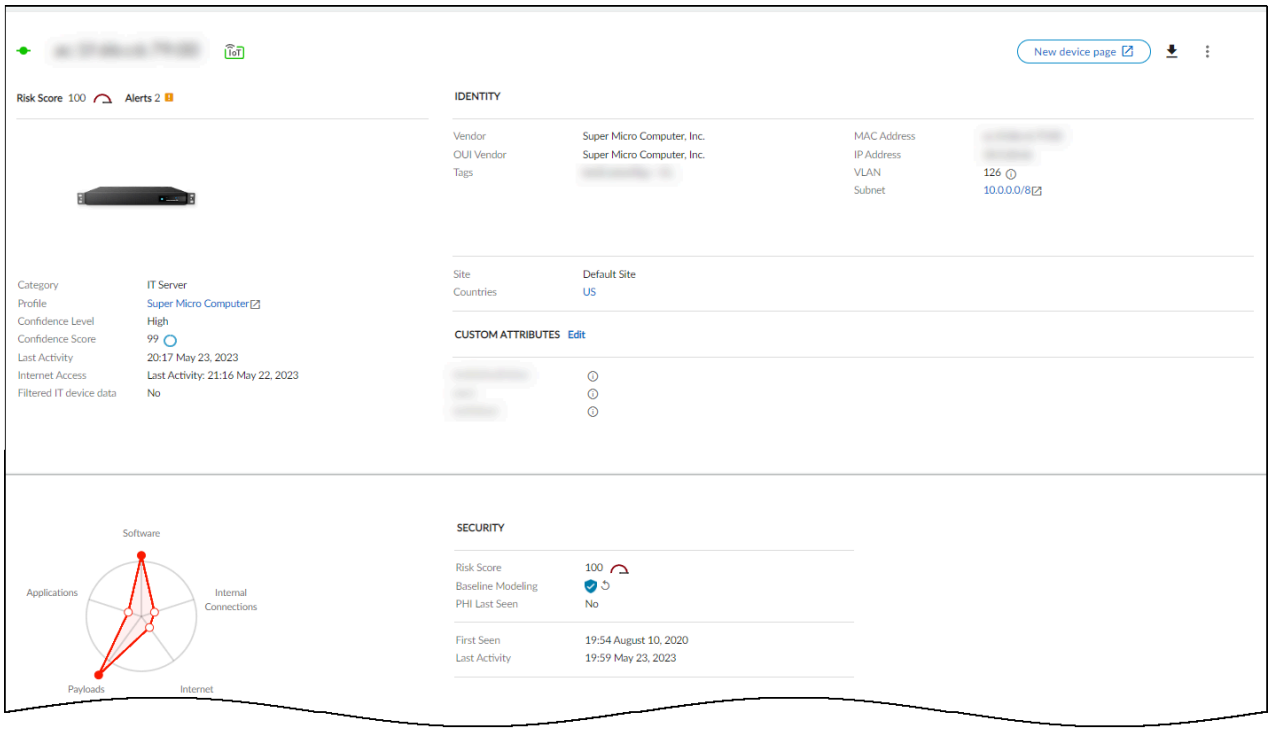
以下部分提供了有关 IoT Security 为这四个级别生成的风险评分的更多信息：设备、设备配置文件、站点和组织。

设备风险

IoT Security 在设备页面 [**Assets**（资产） > **Devices**（设备）] 的风险列中显示每个设备的风险评分。它每天会为设备生成风险评分。

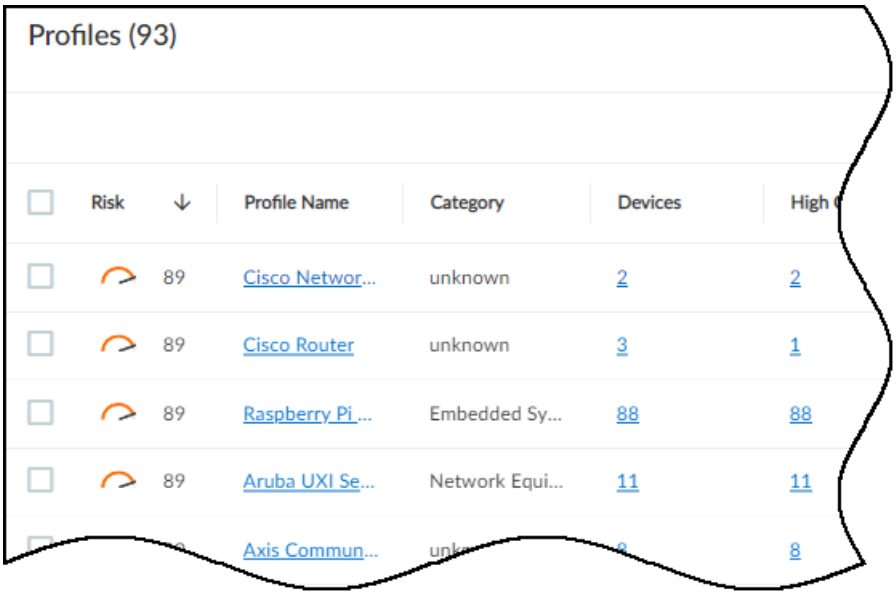


另请参阅 **Device Details**（设备详细信息）页面 [**Assets**（资产） > **Devices**（设备） > *device-name* > **Device Details**（设备详细信息）]，其中设备风险评分列出了两次 — 在顶部和安全摘要部分。风险部分包括一个图表，该图表显示了指定时间段内风险评分的变化：一天、一周、一个月、一年或迄今为止的所有时间段。通过该图表您可以看到风险评分随时间的变化趋势。将光标悬停在线上的标记上，即可查看该时间点的警报列表。单击标记即可查看图表下方的警报列表。



设备配置文件风险

IoT Security 在配置文件页面 [资产（**Assets**） > **Profiles**（配置文件）] 的风险列中显示设备配置文件的风险评分。



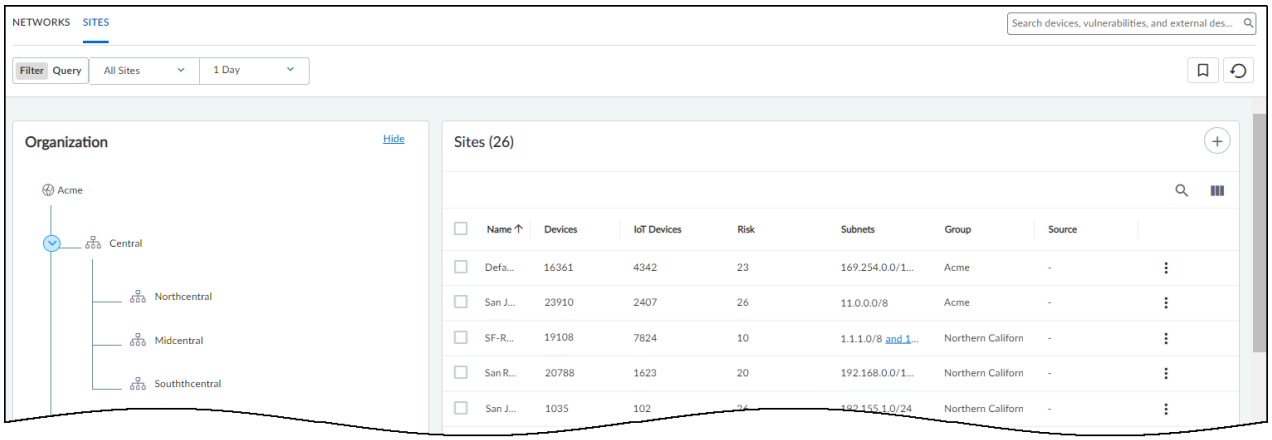
IoT Security 使用同一配置文件中各个存在风险的设备（即风险评分为 40 或更高）的分数来计算整个设备配置文件的风险评分。然而，这并不像对配置文件中所有设备的风险评分求平均值那么简单。计算时还考虑了其他因素，例如配置文件中的危险设备的数量。

例如，如果同一配置文件中的五台设备的单独风险评分为 42，IoT Security 会计算出该配置文件的风险评分为 89。在这种情况下，由于配置文件中的所有设备都处于危险之中，配置文件分数会高于您最初预期的分数。

考虑另一个例子，同样有五个设备在同一个配置文件中。一台设备风险较高，评分为 98。其他四台设备的风险等级为正常，得分均为 30。在这种情况下，IoT Security 计算出它们的配置文件的风险评分为 64。在如此小的集合中，一台高风险设备对配置文件分数的影响比更多设备的分数参与计算时的影响要大得多。

站点风险

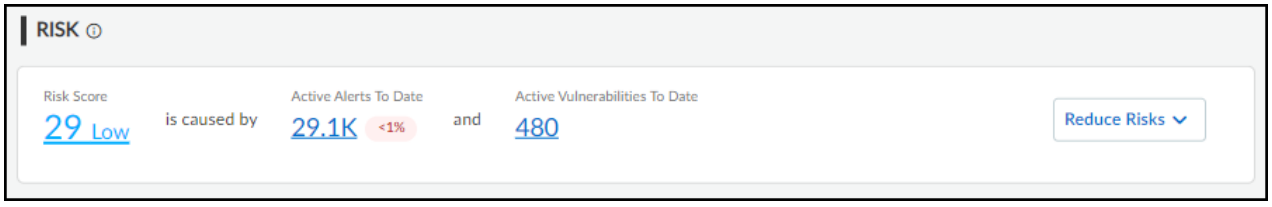
请参阅站点页面 [**Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点）] 上风险列中的风险评分列。



IoT Security 用于计算站点风险评分的公式使用设备配置文件风险评分的加权平均值，每个配置文件的权重由配置文件中的设备数量和配置文件风险级别决定。

组织风险

在 **Dashboards**（指示板） > **Security Dashboard**（安全指示板）上查看风险面板中的风险评分。



IoT Security 使用与站点相同的方法计算组织的风险评分。

风险评分和严重性

以下解释了风险评分的严重性如何排序：

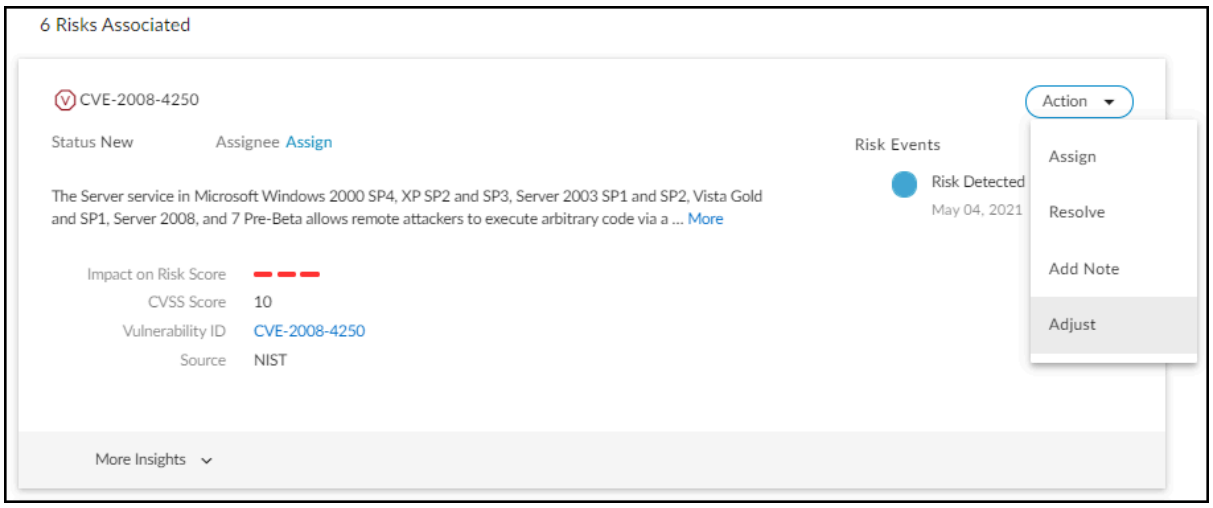
风险评分	风险严重性	注意
< 40	低	这是正常的风险水平。
40-69	中	可能存在少量异常网络行为、中级别警报、CVSS（通用漏洞评分系统）评分在 4.0 到 6.9 之间的漏洞。
70-89	高	可能存在多个高度异常行为、高级别警报和 CVSS 分数在 7.0 到 8.9 之间的漏洞。
90-100	关键	可能存在多个极其异常的行为、关键严重性警报（例如恶意软件攻击）以及 CVSS 评分最高为 10 的漏洞。

调整设备风险评分

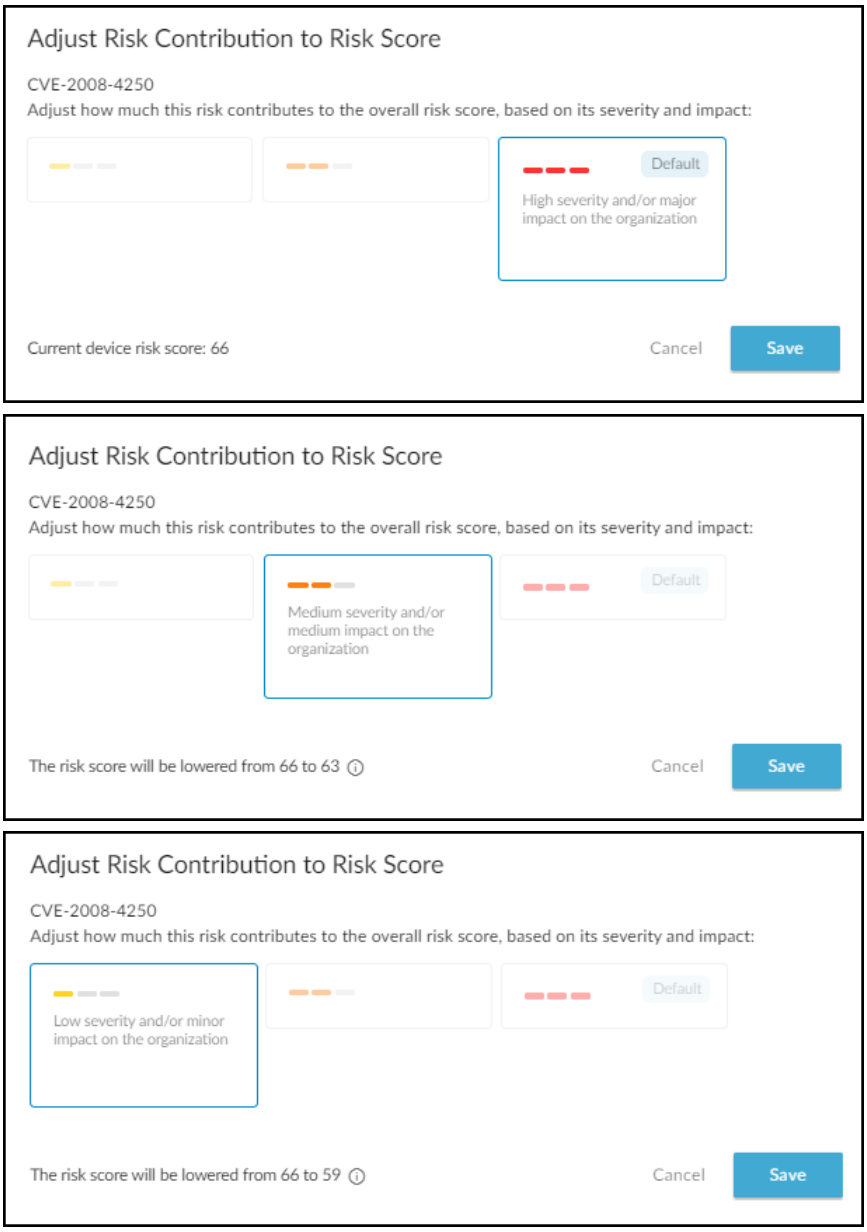
可以调整单个风险对设备整体风险评分的贡献程度。在 **Vulnerabilities**（漏洞） > **Vulnerability Overview**（漏洞概述） > **All Vulnerabilities**（所有漏洞）页面上，单击已确认实例或潜在实例列中的数字可查看漏洞的详细信息，包括该漏洞影响或可能影响哪些设备。然后单击“实例”列中的设备名称以打开该设备的详细信息页面。

IoT Security 根据 CVE 风险的来源，对其进行不同分类。当 IoT Security 通过其内部漏洞匹配逻辑（源 = IoT Security 设备软件库）或漏洞扫描的结果发现它们，并将其分类为漏洞。当防火墙应用威胁防护并将其报告给 IoT Security（警报来源 = 防火墙）时，IoT Security 将其归类为警报。“调整”选项仅出现在漏洞的“操作”菜单中；或者换句话说，仅出现在未被归类为警报的风险的“操作”菜单中。

在漏洞部分，展开漏洞的操作菜单，然后单击 **Adjust**（调整）。



考虑到此风险的严重性及其对组织的影响，并调整您认为它对设备整体风险评分的贡献程度。选择其贡献是低、中还是高。



请注意，您所做的更改对总体分数的影响取决于其他风险因素的数量和严重性。如果存在很多风险，调整单一风险对评分的贡献程度可能不会产生太大影响。另一方面，如果只有少数风险，调整其中一个风险的贡献就可以显著改变分数。

风险评分变化警报

当风险评分的增加导致其超过将一个风险级别与另一个风险级别分开的阈值时，IoT Security 生成风险变化警报。（由于风险降低而超过风险级别阈值不会触发警报。）风险增加会触发不同严重性的警报，具体取决于风险的新严重性：

- 当风险等级从高升至关键时发出警告

- 当风险等级从中等升至高时需谨慎

为了减少生成的警报总数，当风险级别从低增加到中时不会触发警报。

除了风险评分因手动调整风险因素而发生变化外，风险评分还可能因以下原因而发生变化：

风险增加

- 每日风险更新会发现新的漏洞或增加的 CVSS 风险评分。

降低风险

- 用户解决了一个风险因素。
- 每日风险更新可发现漏洞减少、CVSS 分数降低或风险减轻。

解决风险

您可以通过内置到 IoT Security 门户的工作流解决漏洞和安全警报。本质上，您可以通过减轻或忽略漏洞或警报来解决这些问题。因此，设备风险评分可能会根据其他影响因素（例如风险的严重性以及其他风险的数量和严重性）降低。解决设备上的漏洞或警报可能会同样影响其配置文件、站点和组织风险评分，具体取决于该变化相对于同一组中其他设备的数量和风险级别的影响有多大。有关解决漏洞和安全警报的信息，请参阅漏洞详细信息页面和根据安全警报采取行动。

回应 IoT Security 警报

了解 IoT Security 与安全警报相关的门户，以及如何在检测警报和响应警报时有效使用它们。

- 安全警报概述
- 创建警报规则
- 了解安全警报
- 根据安全警报采取行动
- 常规安全警报管理

安全警报概述

所有安全警报 IoT Security 生成基于以下机制之一：

- 机器学习算法，可自动学习正常设备行为，因此可以检测异常行为。
- 检测特定流量模式 - 无需使用机器学习算法。例如，如果设备连接到站点信誉服务已与恶意软件关联的网站，则 IoT Security 会生成警报。
- 用户定义的安全警报规则指定生成一个或多个已配置操作的活动或状态 — 安全警报、用户通知、设备隔离。例如，当观察到特定活动时，或者当未观察到特定活动时，或者当设备或设备组脱机两小时时。（此时间段不可配置。）
- Palo Alto Networks 新一代防火墙检测到的 IoT 设备上的威胁将在威胁日志中报告给 IoT Security。

IoT Security 实时检查网络流量，分析来自网络上每个设备的通信以及与网络上每个设备的通信。如果检测到与策略规则匹配的异常行为或活动，它会生成警报。

IoT Security 仅为 *IoT* 设备生成警报。它不为 *IT* 设备提供警报、漏洞检测、策略建议和网络行为分析。对于 *IT* 设备，*IoT Security* 仅提供设备标识。

IoT Security 门户中的“警报”和“警报详细信息”页面提供所有生成的警报的概述以及有关各个警报的详细信息，以便进行分析和跟进。IoT Security 将安全警报保留最多一年。

安全警报与设备设置和网络行为有关，这些设置和网络行为指示可能的安全漏洞：

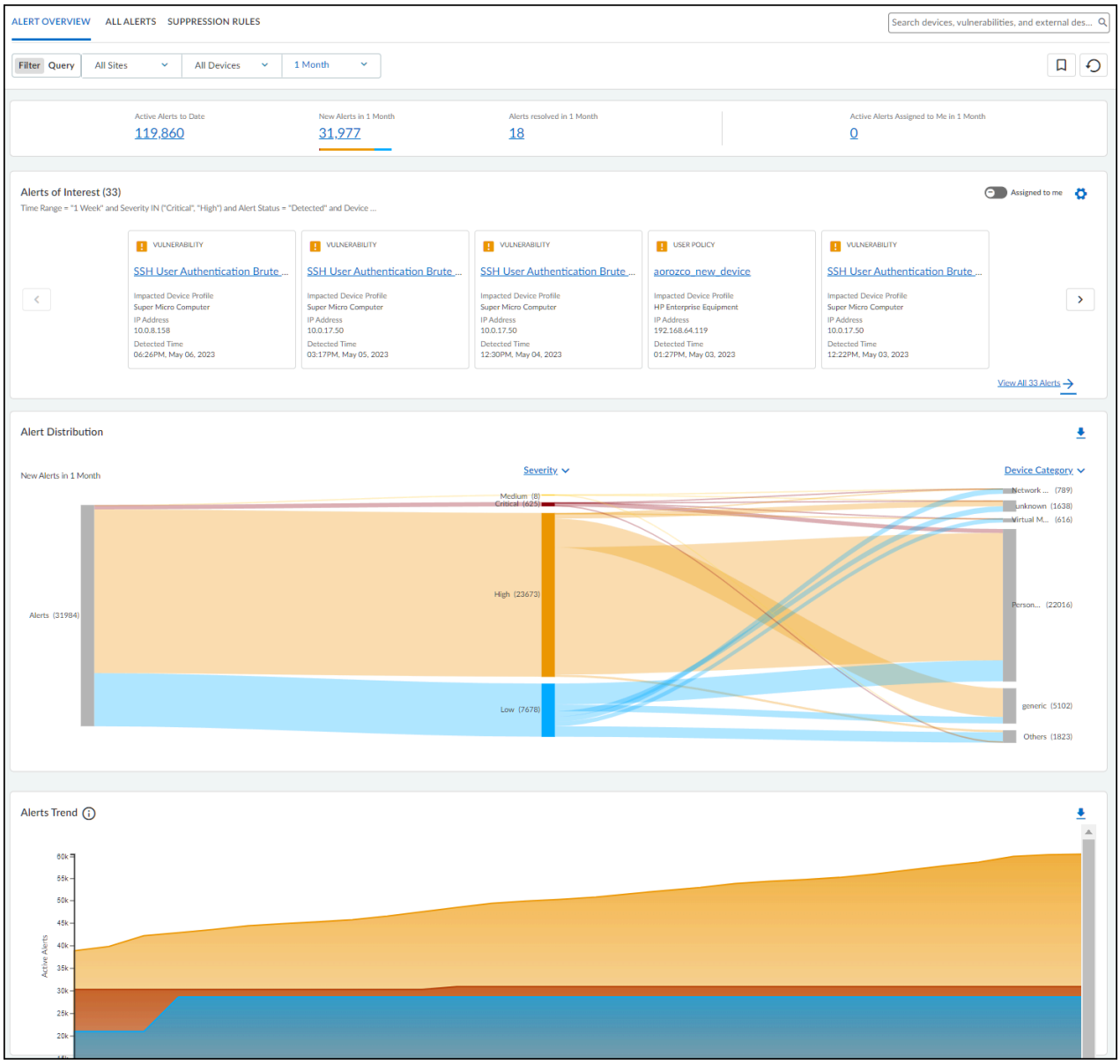
- 不安全的设备设置（例如：使用默认用户名和密码的设备）
- 可疑行为（例如：过多的 DNS 查找失败）
- 侦查或漏洞利用（例如：端口扫描和 EternalBlue SMB 漏洞利用尝试）

“安全警报”部分 [**Alerts**（警报） > **Security Alerts**（安全警报）] 由三个页面组成：

- **Alert Overview**（警报概述）— 这是一个指示板，您可以在其中查看与您最相关的警报，分析 IoT 设备和网络上的风险，并观察和报警报报趋势。
- **All Alerts**（所有警报）— 此页面按顺序显示警报表，其中包含可自定义的分页、列和列顺序。您可以通过单击“过滤器”图标 ( )。
- **Suppression Rules**（禁止规则）— 此页面是用户定义的规则列表，这些规则是为禁止将来检测警报而创建的。有关信息，请参阅根据安全警报采取行动。

警报概述

“警报概述”页是一个指示板，其中包含四个主要部分，旨在帮助您识别优先级最高的警报、分析风险并轻松报告 IoT 设备的警报趋势。



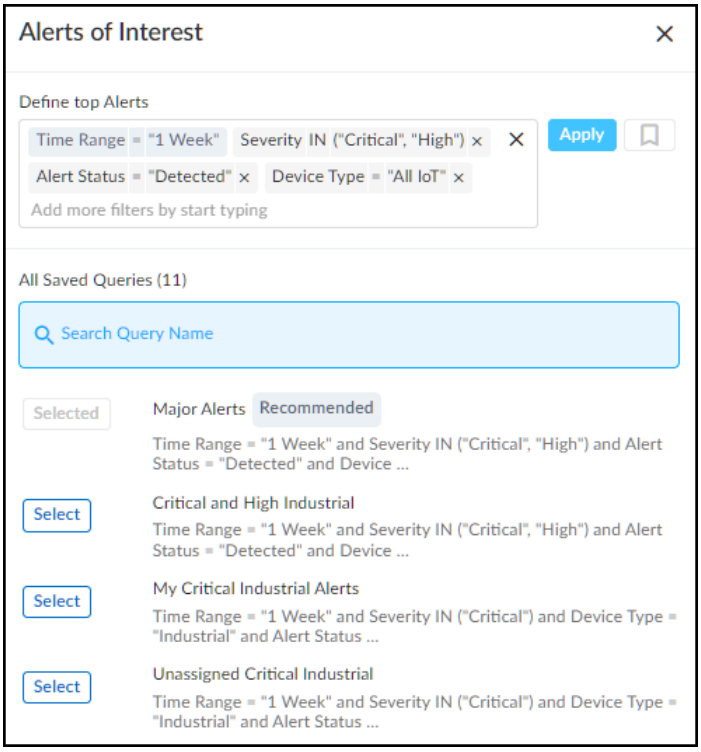
页面顶部是一个警报摘要，其中包含与为站点、设备类别和时间范围设置的过滤器匹配的警报的警报信息。

- **Active Alerts to Date**（目前的活动警报）— 是打开的警报的总数。警报可以处于以下四种状态之一：已检测到、正在调查、正在修正和已解决。处于前三种状态之一的任何警报（即，除“已解决”以外的任何状态）都被视为打开或活动，并包含在此计数中。

  IoT Security 在其数据库中保留安全警报长达一年。如果您使用 *IoT Security* 超过该期限，请记住，此计数不包括一年多前发现的任何警报。
- **New Alerts in**（新警报） <time range>— 这是在页面顶部的数据过滤器中指定的时间范围内检测到的所有打开警报的总和。
- **Alerts resolved in**（警报已解决）<time range> — 这是在页面顶部的数据过滤器中指定的时间范围内解决的所有警报的总和。
- **Active Alerts Assigned to Me in**（分配给我的活动警报） <time range> — 这是在页面顶部的数据过滤器中指定的时间范围内分配给当前登录人员的未打开警报的总数。

Alerts of Interest（感兴趣的警报）— 定义对您最重要的警报的条件。IoT Security 随后将显示响应查询的前十个警报，并首先显示更严重和较新的警报。例如，如果您想要查看上周内检测到的特定供应商或配置文件的警报，请单击齿轮图标 (⚙) 并配置查询以显示您感兴趣的警报。IoT Security 随后显示与您的术语匹配的 10 个最新和最严重的警报。

默认情况下，IoT Security 使用预定义的“主要警报”查询来搜索过去一周内检测到的所有 IoT 设备的关键警报和高严重性警报。您可以编辑此查询以定义其他感兴趣的属性，然后单击书签图标 (🔖) 进行保存，以供重复使用。



您也可以 **Assigned to me**（分配给我），从而让 IoT Security 仅显示分配给您的前 10 个警报。如果警报超过 10 个，请单击 **View All**（查看全部） <number> **Alerts**（警报）以查看符合您条件的

所有警报。IoT Security 在“所有警报”页面上显示这些内容。单击警报名称以打开该警报的“警报详细信息”页面。

Alert Distribution（警报分发）— 桑基图可让您查看活动警报在不同设备分组中的分布。从左到右阅读图表，从左侧开始，页面顶部显示与站点、设备类别和时间范围过滤器匹配的所有活动警报。然后，该图表将这些警报与中间的一种设备分组相关联，并再次将这些警报与右侧的另一种类型的分组相关联。这些分组的选项包括 **Severity**（严重性）、**Profile**（配置文件）、**Device Category**（设备类别）、**Vendor**（供应商）、**Status**（状态）、**Device Type**（设备类型）和 **Alert Type**（警报类型）。警报在图表中按计数垂直分布，警报最多的分组位于图表顶部。当有五个以上的分组时，桑基控制图会显示前五个，然后将其他所有内容收集到“其他”组中。将光标悬停在 **Others**（其他）上以查看接下来的 10 个分组的列表，然后单击 **View all**（查看全部）以查看包含完整列表的弹出面板。

例如，要查看不同设备类别中关键、高、中、低严重性警报的比率，对于中间柱子，请选择 **Severity**（严重性），对于右侧柱子，请选择 **Device Category**（设备类别）。左侧和中间柱子之间的彩色条带表示有多少活动警报是关键、高、中和低，中间和右侧柱子之间的彩色条带表示不同设备类别中的设备在每个严重性级别触发的警报数。每个波段都带有标签，并显示其严重性（左侧）和每个设备类别（右侧）的严重性的活动警报总数。通过波段的宽度，您可以一目了然地看到警报的严重性所划分的相对数量。将光标悬停在柱子的一部分上可显示相邻波段的警报百分比。

颜色仅传达表示警报严重性级别的含义：红色 = 关键，橙色 = 高，黄色 = 中等，蓝色 = 低。对于其他类型的分组，半透明的灰色阴影仅用于区分一个波段与另一个波段。

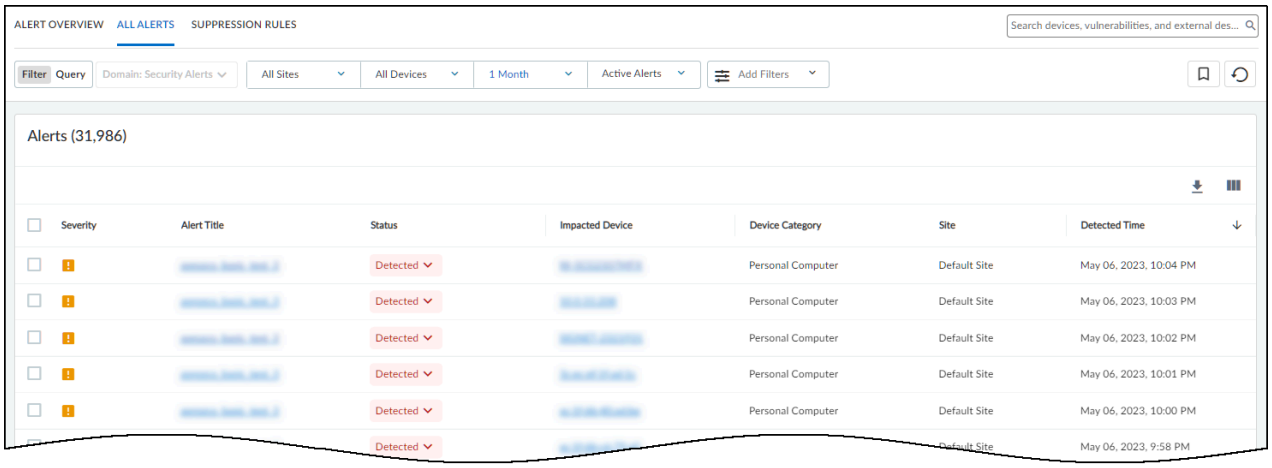
要从桑基图表中下载记录或报告的数据，请单击下载图标 (⬇) 在图表的右上角。IoT Security 将其另存为 .xlsx 文件，第一个工作表上是警报分发信息，第二个工作表上是活动警报的完整列表。

Alert Trend（警报趋势）— 警报趋势图表显示指定时间段内活动警报的累积计数和已解决警报的每日非累积计数。这直观地显示警报趋势，以帮助 SOC 和管理团队查看活动警报的数量是否随着时间的推移而增加或减少。它还显示已解决警报的数据，这可以帮助团队衡量他们在警报解决方面的进度。将光标悬停在图表上的不同点上，可查看不同日期的关键、高、中、低和已解决警报的数量。

要从报告或记录的警报趋势图表中下载数据，请单击下载图标 (⬇) 在图表的右上角。IoT Security 将其另存为 .xlsx 文件，其中包含迄今为止的活动警报数和指定时间段内已解决的警报数。

所有警报

“所有警报”页面显示所有警报，或者按日期组织到前一天的警报实例数，这是 IoT Security 具有完整的警报列表的最后一天。在页面顶部定义过滤器，以控制要显示的警报。有针对站点、设备类别、时间范围和响应状态（活动警报、已解决、已分配、未分配、已检测到和所有）的过滤器。您也可以添加更多过滤器。



警报的状态从“已检测到”状态开始。您可以将其保留在那里，也可以将其设置为不同的状态，以反映它在修正过程中的位置：

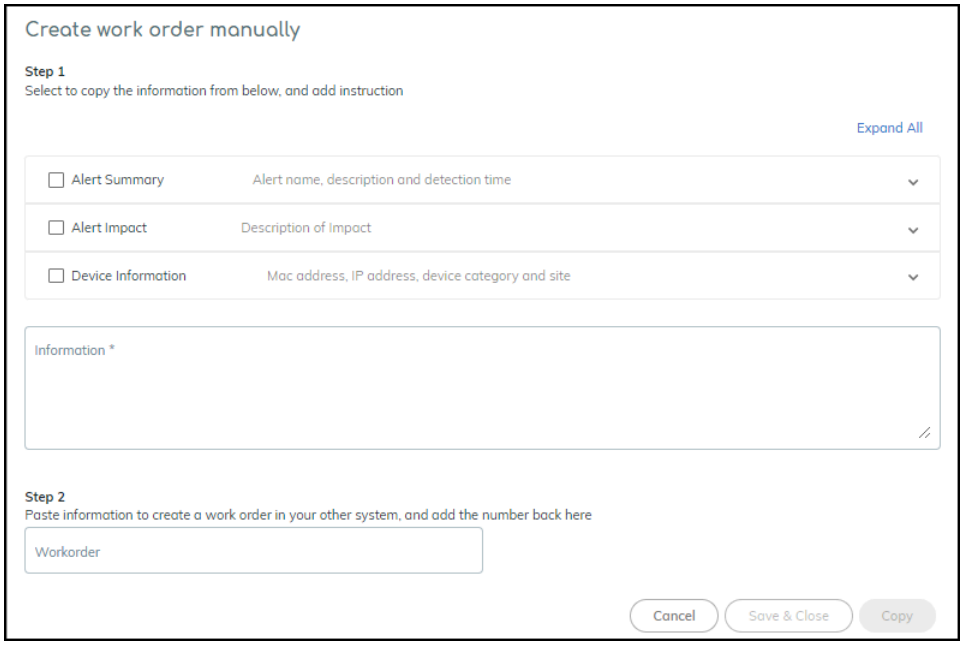
- 已检测：这是新检测到的警报实例的状态。如果未采取任何措施来调查、修正或解决它，则将其保持在此状态是有意义的。
- 正在调查：请考虑在开始对其进行初步工作并对其进行验证、研究并分析其影响后，将警报实例设置为此状态。
- 正在修正：请考虑将警报实例设置为此状态，同时正在采取措施进行修正，但尚未完成。
- 已解决：警报实例可以通过缓解问题或忽略并接受问题来解决。

要更改警报实例的状态，请单击“状态”列中的条目，然后选择其他状态。当您解决它时，IoT Security 提示您提供解决该问题的原因。

要将警报实例分配给要处理的人员，请选中该实例的复选框，然后单击 **More**（更多） > **Assign**（分配）。输入用户的用户名或电子邮件地址，然后单击 **Assign**（分配）。然后，用户会收到一封电子邮件，指出已为他或她分配了警报，并在 IoT Security 门户中提供了用于调查的警报链接。

向其分配警报实例的人员必须具有 *IoT Security* 用户帐户，以便它可以向适当的电子邮件地址发送消息。

IoT Security 提供用于复制警报实例详细信息和创建用于资产管理系统的工作订单的选项。选中实例的复选框，然后单击 **More**（更多） > **Copy Alert Information**（复制警报信息）。选择要包含在工作订单中的警报描述部分，在“信息”字段中添加其他说明或相关信息，然后单击 **Copy**（复制）以复制这些部分中的文本。



将复制的内容粘贴到资产管理控制台的描述字段中，同时在其中手动创建工作订单。然后，您可以从资产管理控制台复制工作订单编号，并在 IoT Security 中将其粘贴回手动创建工作订单对话框中的工作订单字段，然后单击 **Save & Close**（保存并关闭）。

要添加有关警报实例或对其执行的工作的备注，请选中该实例的复选框，然后单击 **More**（更多） > **Add notes**（添加备注）。输入备注，然后单击 **Add**（添加）。

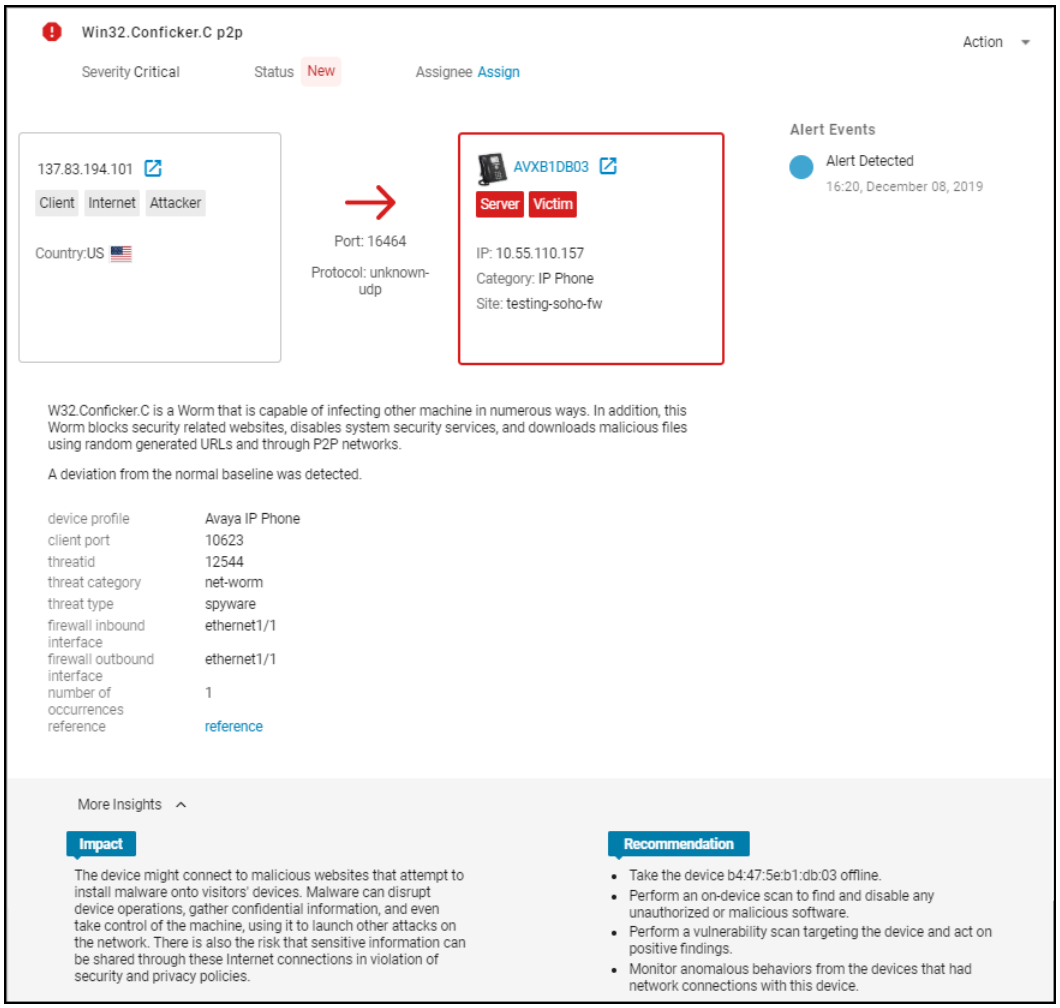
要查看以前添加的备注以及以前对警报实例所做的任何状态更改，请单击或将光标悬停在“上次操作”列中的条目上。有关实例响应的历史记录将显示在弹出窗口中。

您可以设置希望在每个页面上看到的行数（从 5 到 200），并在多个页面之间导航。

“安全警报详细信息”页面

单击安全警报实例的名称将打开“设备详细信息”页面。

“警报详细信息”页面分为三个主要部分。顶部是有关事件本身的信息。客户端始终显示在左侧，服务器显示在右侧，两者之间有一个向右的指向箭头 - 如果它们形成了连接，则为实线，如果只是尝试连接，则为虚线。连接（或尝试的连接）中使用的一个或多个协议列在箭头下方。发出警报的设备显示在一个框内，该框采用颜色编码以匹配警报的严重性。通过这种方式，您可以轻松查看设备角色和警报发生的位置。



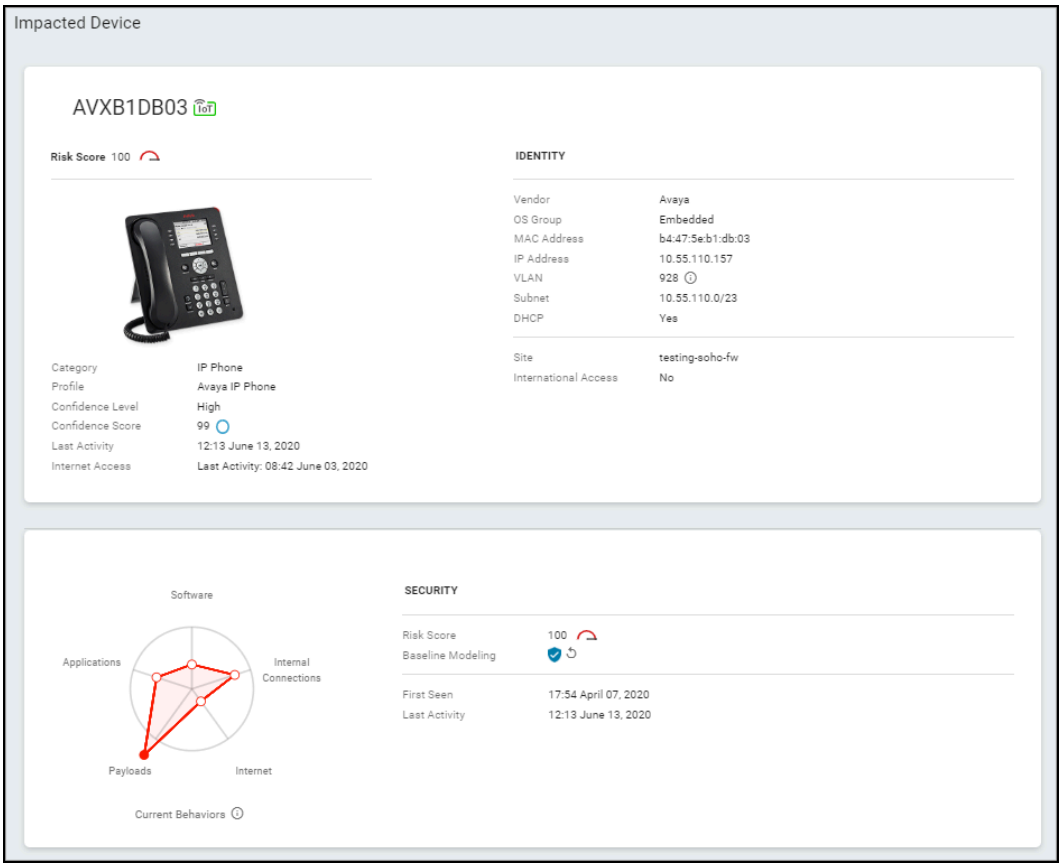
左侧的客户端与右侧服务器角色中的 Avaya IP 电话形成 UDP 连接。IP 电话是发出警报的设备。

设备名称旁边的蓝色图标（指向框外的箭头）将打开一个新的浏览器选项卡，其中显示动态拓扑查看器，该设备处于焦点状态（参阅IoT Security 设备详细信息页面。在此处可以看到它与多少其他设备通信以及它们是什么。这在调查受感染的设备时非常有用，因为它可以揭示参与攻击的远程设备的位置以及可能成为受害者发起的进一步攻击目标的本地设备。

该参考链接到有关 Conficker 蠕虫的 Palo Alto Networks 知识库文章。

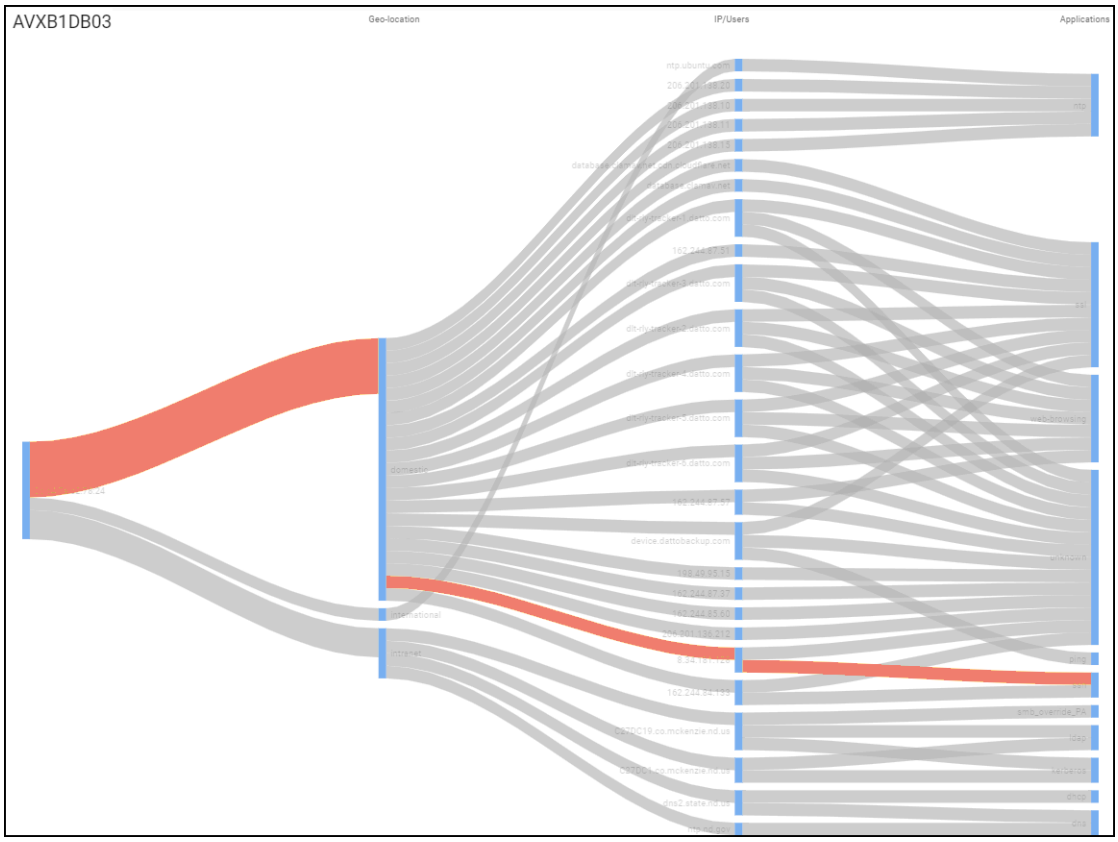
“影响”部分说明了该问题如何影响用户、设备或网络的安全性。（并非所有警报都有“影响”部分。）“建议”部分列出了解决此问题的选项。

“警报详细信息”页面的第二个主要部分检查受影响的设备并总结其安全状态。



您可以了解受影响设备的身份和活动、其物理位置（站点）及其在网络上的逻辑位置。在“当前行为”图中，将光标悬停在五个红色小圆圈或信息图标上的任何一个上，以查看更多信息。“安全”部分提供有关设备的安全相关信息。

“警报详细信息”页面上的第三个主要部分以桑基图的形式显示受影响设备的网络流量快照。该图包括其他端点的 IP 地址及其通信中使用的应用程序。这些线表示各种网络连接。红色表示高严重性警报中涉及的连接。



如果设备有多个警报，则所有相关线条都会根据每个警报的严重性进行着色。

创建警报规则

IoT Security 使用 AI 和机器学习算法根据异常网络行为自动生成安全警报，并在设备属性与已发布的漏洞数据库（例如 nvd.nist.gov 和 www.cisa.gov 的漏洞数据库）中的属性匹配时检测漏洞，以及由其安全专家团队添加到 IoT Security 数据库的漏洞。有了这些内置于系统中的自动检测机制，IoT Security 将持续监控您的网络，并通知您安全威胁，而无需您配置和启用规则或设置即可执行此操作。但是，如果要检测特定网络事件（如新设备发现或使用特定应用程序的特定设备），则可以定义一些条件来识别这些事件并触发安全警报和执行操作。为此，您可以创建自定义规则，并将其添加到已实施的内部规则集中。

IoT Security 中定义的指定规则可以基于单个更改事件（例如发现新设备）触发。它也可以由指定的流量模式触发，例如特定的应用程序命令或一段时间内的流量累积。它甚至可以由两者的组合触发。规则每天仅为每个设备触发一次操作，以避免产生过多的噪声。要查看观察到的条件与规则匹配的次数，请查看 **Alerts**（警报） > **Custom Alert Rules**（自定义警报规则）页面上的“匹配计数”列。

以下列表显示您可能定义的几种类型的条件：

- 一台设备与另一台设备通信
- 设备出现在特定的 VLAN 或网段上，连接到特定的无线接入点或网络交换机，或者出现在特定的新一代防火墙区域中
- 设备的子网或 IP 地址发生更改
- 有风险的设备与 Internet 通信
- 设备的风险级别发生变化
- 设备传输一定的网络流量
- 设备使用特定应用程序或使用特定应用程序以外的其他内容
- 设备使用特定应用程序命令或命令中的特定值

如果检测到，这些条件将触发 IoT Security 执行一项或多项配置的操作，例如生成警报、通知用户、隔离相关设备等。

尽管为简单起见，上述条件使用单数形式“设备”，但规则条件也可以应用于多个单独的设备、一种或多种类型的设备（设备配置文件）或一个或多个设备组（由用户标记、*Purdue* 级别或类别定义）。

规则引擎位于 **Alerts**（警报） > **Custom Alert Rules**（自定义警报规则）且包含三个部分：基本信息、规则详细信息和规则预览。

为了帮助您开始使用规则引擎，IoT Security 提供了常用规则的示例模板集合。研究这些预配置规则以熟悉规则引擎功能，按原样启用和使用它们，或者将它们用作构建自己的类似规则的模型。

默认情况下，预定义的规则处于禁用状态，因此它们不会触发不需要的警报。

要查看预配置的示例规则，请选择 **Alerts**（警报） > **Custom Alert Rules**（自定义警报规则）。

根据 IoT Security 门户上活动的垂直主题，预配置的模板会有所不同。每个垂直主题都有两个或三个示例规则模板。下面是每个主题的示例：

Enterprise IoT Security Plus

- 规则名称：[示例] 可疑打印机通信
- 说明：每当打印机使用不在允许列表中的应用程序与任何其他端点通信时，都会发出关键警报。
- 规则：WHEN category = “Printer”, application =!Dhcp, dns, dns-base, ldap, netbios-ns, ntp-base, smtp-base, snmp-base, snmpv1, ssl, ws-discovery ; DO Publish “Critical” alert
- 操作：发出关键严重性警报

Industrial IoT Security

- 规则名称：[示例] 工业设备脱机
- 说明：当工业控制器或远程终端单元 (RTU) 在工作时间内离线时，会发出高严重性警报。
- 规则：WHEN category IN (“Industrial Controller”, “Industrial RTU”), Offline Device; DO Publish “High” alert
- 操作：引发高严重性警报

Medical IoT Security

- 规则名称：[示例] 发现新的摄像机资产
- 说明：每当在网络上检测到新的 IP 摄像机时，会发出关键严重性警报。
- 规则：WHEN: category = “Camera”, New Device Discovery; DO Publish Alert
- 操作：发出关键严重性警报

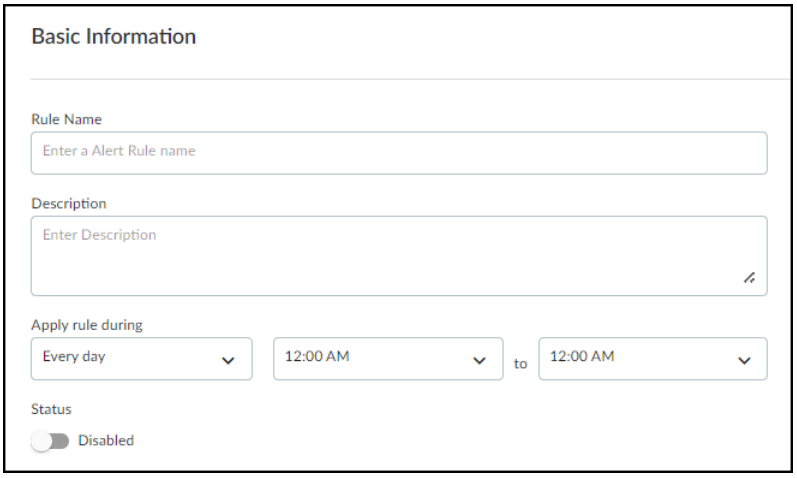
如果您想尝试某个规则，请打开规则引擎编辑器，并将状态从 **Disabled**（禁用）切换到 **Active**（活动），即可启用该规则。在 **Alerts**（警报） > **Custom Alert Rules**（自定义警报规则）页面上，您可以使用“操作”列中的选项编辑、克隆和删除示例模板。

STEP 1 | 确定您的网络问题以及您希望 IoT Security 监控并通知您的事件。

STEP 2 | 从一些基本信息开始，创建一个规则来解决您的问题。

在“基本信息”部分中，输入规则的名称和描述以及您希望何时强制执行该规则。

- **Rule Name**（规则名称）：输入规则的唯一名称。
- **Description**（说明）：（可选）输入规则的描述，例如其总体意图，以供将来参考。
- **Apply rule during**（应用规则的时间期限）：您想要 IoT Security 强制执行规则的日期以及一天内执行的次数。默认情况下，规则始终处于强制执行状态；也就是说，每天整天执行。
- **Status**（状态）：如果您想要让 IoT Security 监控规则条件，请将其状态切换为 **Active**（活动）。如果您不想让 IoT Security 应用规则，请将其状态切换为 **Disabled**（禁用）。



STEP 3 | 定义规则的条件。

在“规则详细信息”部分，定义触发 IoT Security 将执行的操作所需的条件。

- **All(AND) [**全部（和）**]**或**ANY(OR) [**任何（或）**]**：如果您希望满足所有条件，以便让 IoT Security 执行定义的操作时，请选择 **All(AND) [**全部（和）**]**。如果您希望有任何一个条件触发它时，请选择 **ANY(OR) [**任何（或）**]**。
- **Add Condition**（添加条件）：选择 **Traffic Pattern**（流量模式），以根据网络流量行为定义条件。选择 **Change Event**（更改事件），以根据设备的更改定义条件，例如设备更改其 IP 地址或脱机，或者新设备进入网络。

  如果选择“流量模式”，IoT Security 会显示目标设备的两个字段以及流量和应用程序使用情况的额外条件选项。

  - **Add Target Devices**（添加目标设备）：在第一个目标设备字段中，确定要应用规则的一个或多个设备。您可以通过选择最多 10 个属性来执行此操作。这些可以是设备的 IP 地址和名称、它们所属的子网和 VLAN、以前定义的标记和自定义属性、设备类别和配置文件、设备访问网络的交换机和无线接入点以及流量目标（ISO 3166-1 标准中定义的国家和地区的双字符代码）。您可以指定目标设备是否有 **(=)** 或没有 **(!=)** 某个特定属性，或者如果它们在一组属性中是否有 **(IN)** 或没有 **(NOT IN)** 任何一个属性。构建目标设备条件的工作方式类似于查询生成器。
  - **Target Devices (optional) [**目标设备（可选）**]**：如果要定义两个特定设备或设备类型之间的流量模式，请使用第二个目标设备字段来标识通信的另一端。如果您未在此处输入任何内容，它将被视为“任何目标”（这可以是内部设备或外部网址）。

- **Show Extra Criteria**（显示额外条件）：您可以通过选择 **Traffic Volume**（流量）和 **App Usage**（应用使用情况）以及设置参数来设置额外条件（可以选择一个或两个条件）。

  配置这些设置需要深入了解流量，并了解应用程序设置及其适当的值。

  如果选择 **Traffic Volume**（流量），然后输入流量和流量发生的时间段，作为触发规则的条件。您可能希望使用此选项来观察流量的意外激增，尤其是前往不寻常目标的流量。

  如果选择 **App Usage**（应用使用情况），然后选择 **Application: is**（应用：是），然后，您可以选择单个 OT 或 IoT/IT 应用程序，并输入网络流量中必须存在的任何命令、参数和值才能触发操作。如果您选择 **Application:not**（应用：否），您可以选择一个必须不存在的应用程序来触发操作。如果要创建应用于多个应用程序的条件，请选择 **Application:in**（应用：在）或 **Application:not in**（应用：不在）。

  命令、参数和值的其他选择器字段仅在选择 ***Application: is***（应用：是）后可用。

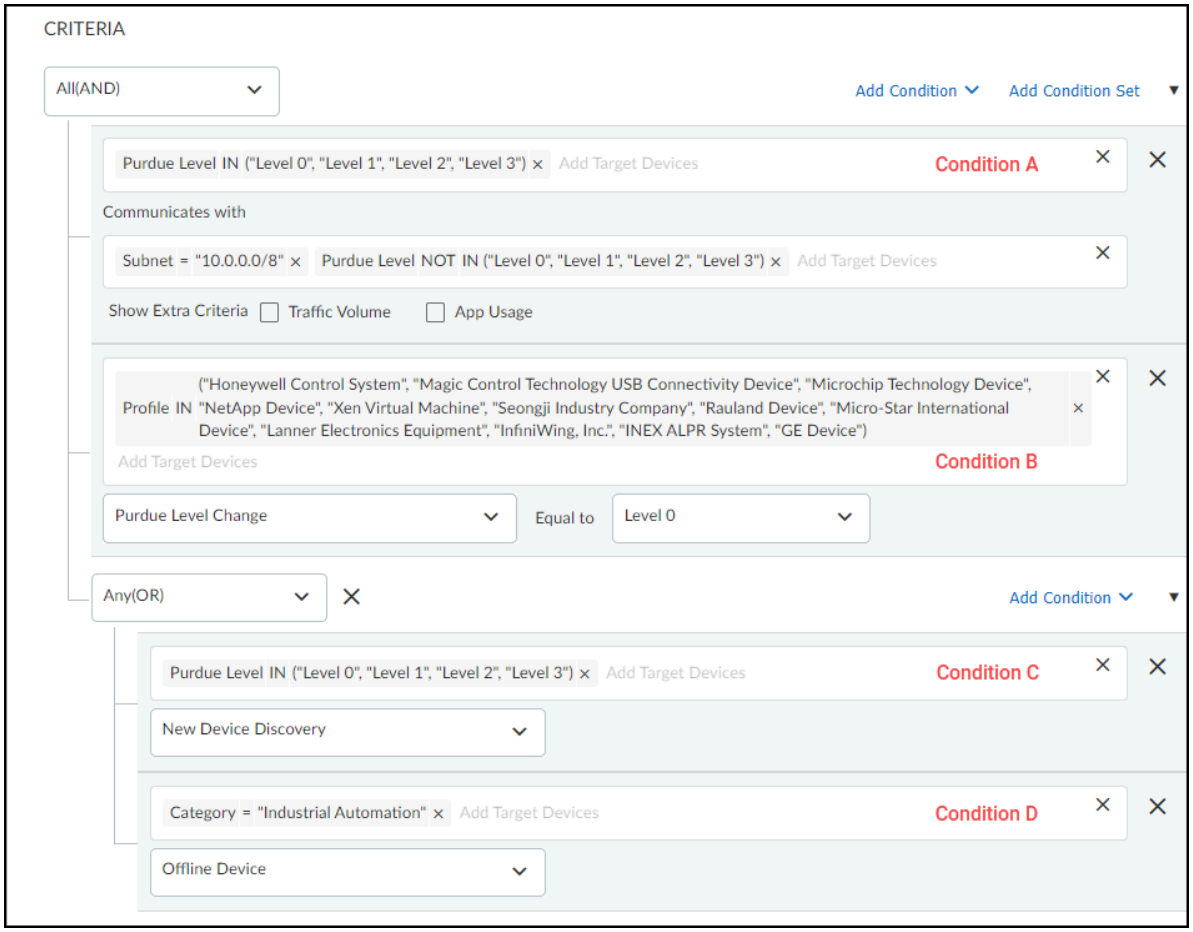
如果您选择 **Change Event**（更改事件），IoT Security 显示与在 **Traffic Pattern**（流量模式）中所选择的相同的“目标设备”字段，再加上一个 **Event**（事件）下拉列表。您可以选择以下事件来触发操作：

- IP 更改
- 新设备发现
- 新漏洞发现（包括已确认的实例和潜在的实例）
- 离线设备
- Purdue 级别更改（您还必须选择 Purdue级别。）
- 风险级别更改（您必须选择 **Any**（任何）或特定的风险级别。

- 子网更改

Add Condition Set（添加条件集）：通过添加条件集，您可以使用自己的 All(AND)或 ANY(OR) 运算符创建条件子组。它可用于在主要条件集下链接多个条件。

例如，以下条件有四个条件，逻辑为 Condition A **AND** Condition B **AND** { Condition C **OR** Condition D }。要应用操作，必须满足条件 A 和 B 以及 C 或 D。



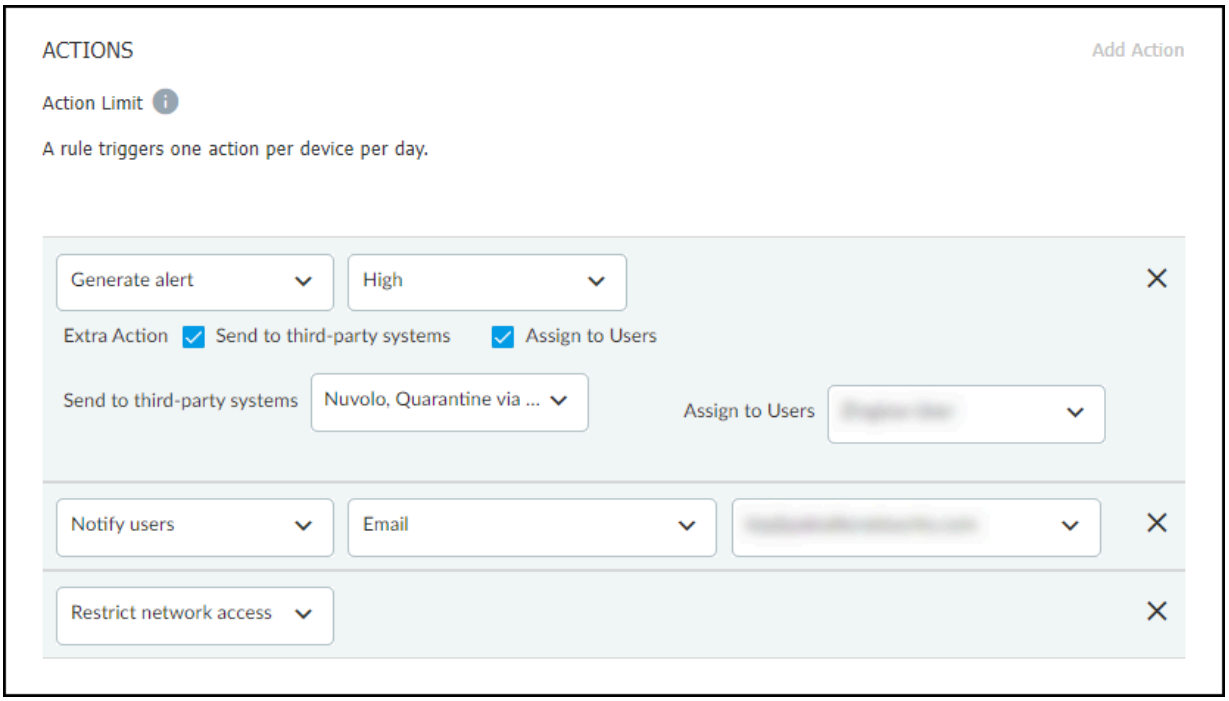
STEP 4 | 设置在满足定义的条件时 IoT Security 执行的操作。

为避免规则产生过多噪声，IoT Security 对每个设备每天仅触发一次指定操作。您可以将 IoT Security 配置为最多执行以下操作中的三项：

Generate alert（生成警报） + 其他操作 [**Send to third-party systems**（发送到第三方系统）和 **Assign to Users**（分配给用户）] — 当满足规则条件时，IoT Security 生成安全警报，并将其显示在“警报 > 安全警报”页面上。另外，IoT Security 可以自动将警报推送到第三方系统，从而触发第三方系统的其他操作，例如启动 NAC 隔离或触发工作订单。它还可以将警报分配给一个或多个用户，以调查补救措施。

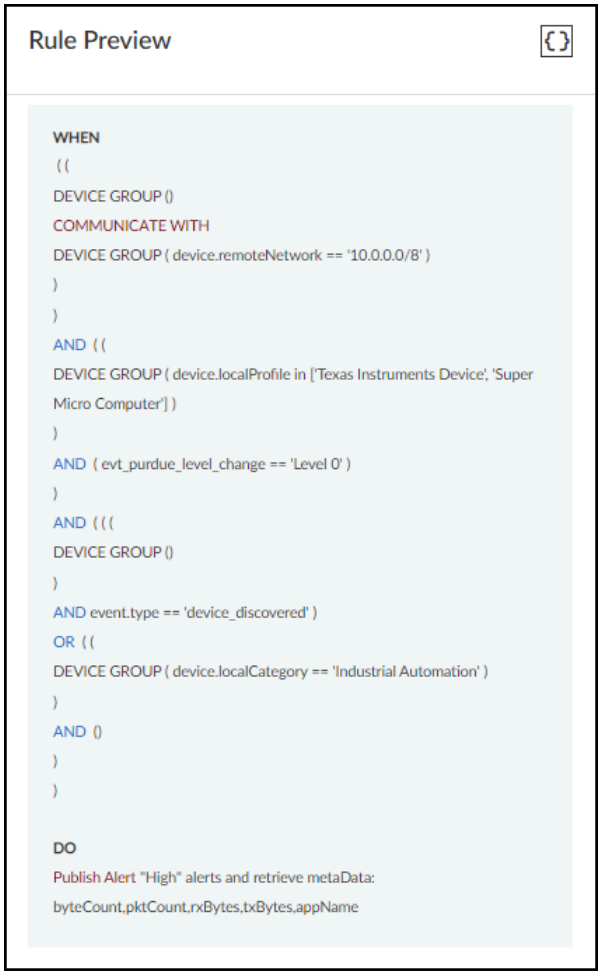
Notify users（通知用户）— 设置 IoT Security 以通过电子邮件通知多个用户或通过短信通知您。[要接收短信通知，您必须输入您的手机号码并在 *User-Name*（用户名） > **Preferences**（首选项）中启用短信通知。]

Restrict network access（限制网络访问权限）—对于行为与触发操作所需条件相符的设备，通知 Palo Alto Networks 新一代防火墙限制网络访问权限。



STEP 5 | 检查规则预览中的设置。

查看以类似 SQL 的可读格式显示的规则。这是“条件”和“操作”部分的高级快照，可用于检查规则中设置的逻辑关系。以后对这些部分中的设置进行的任何更改都将更新规则预览。

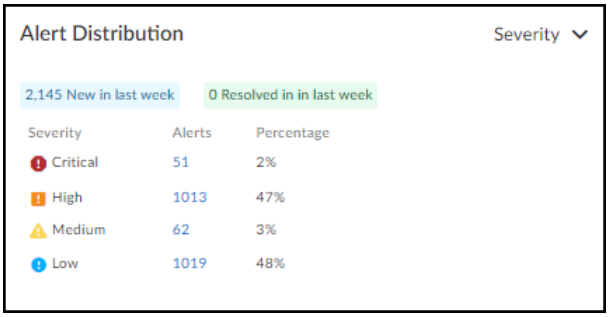


了解安全警报

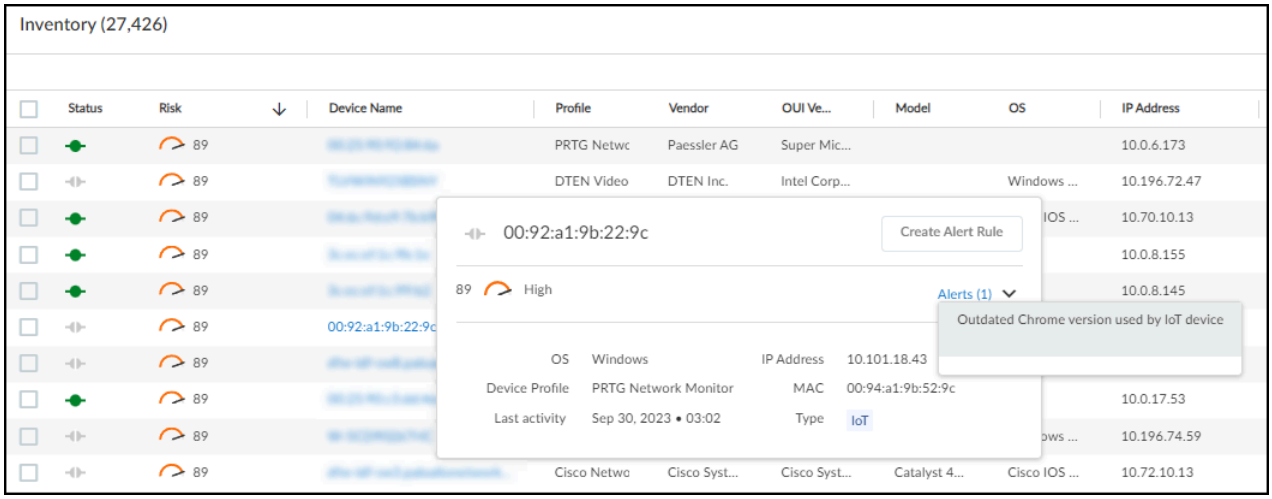
有几种方法可以了解安全警报。IoT Security 可以自动通过短信和电子邮件通知您，具体取决于您在帐户首选项中启用的方法。即使未启用警报通知，当其他用户为您分配要调查的警报时，您仍可能收到通知。

通过检查“安全指示板”上的“警报”部分，将鼠标悬停在“设备”页面上的设备名称上，以及查看“安全警报”页面，您还可以在 IoT Security 门户中解警报。

一种了解 IoT Security 门户中警报的方式是查看“安全指示板”的“警报”部分。您可以按严重性（低、中、高、关键）、状态（已检测到、正在调查、正在修复、已解决）、设备类别（例如：音频流、IT 服务器、销售点系统）或警报类型（例如：安全风险、不安全协议、用户策略）来组织显示的警报。按严重性查看时，“警报”列中的数字是可单击的。单击其中一个将打开 **Alerts**（警报）> **Security Alerts**（安全警报）> **All Alerts**（所有警报）页面，该页面上行应用了过滤器，仅显示与您单击的项目匹配的警报。



当您将光标悬停在“设备”页面上的设备名称上时，IoT Security 门户会显示一个弹出面板，其中包含有关设备的信息，包括警报列表（如果有）。单击其中一个警报名称将打开其“警报详细信息”页面。



单击警报的名称以在新的浏览器窗口中打开“警报详细信息”页面。

安全警报及系统警报通知

除了在 IoT Security 门户或通知调查警报时可以查看安全警报外，IoT Security 还会在事件触发时自动发送电子邮件和文本通知。它针对两种类型的警报执行此操作：

- 安全警报 — 这些警报与 IoT Security 正在监视的设备相关，并由指示潜在攻击的行为更改触发。下面是安全警报通知的示例：

  ```
  Palo Alto Networks 针对 Super Micro Computer 设备的 IoT 策略警报：（警告）SSH 用户身份验证暴力破解。此事件表示通过多次登录 SSH 服务器而遭到暴力攻击。
  ```

- 系统警报 — 这些警报与新一代防火墙有关。目前，只有过时的应用程序内容包会触发系统警报通知。

在具有所有者权限的用户将其发送给全部所有者（默认启用），或在 **Administration**（管理） > **Notification Management**（通知管理）上将用户添加到列表以接收通知后，IoT Security 会发送这些通知。

所有者可以通过从显示的下拉列表中选择现有管理员用户来添加这些用户。这些用户通过电子邮件和/或文本接收通知，具体取决于他们的用户偏好。所有者还可以输入其电子邮件地址与其中一个所有者共享同一域的用户的单个电子邮件地址或分发列表。（IoT Security 拒绝任何具有未由所有者共享的域的地址。这些用户通过电子邮件接收通知。如果所有者禁用 **Send to all the owners**（发送给所有所有者），则只有电子邮件列表中的用户才会收到通知。

根据安全警报采取行动

了解安全警报后，第一步是阅读详细信息并确认的确发生了触发该警报的事件，方法可能是检查防火墙事件日志条目。确认警报后，您必须快速评估其重要性和紧迫性，确定受影响的设备类型，然后决定如何应对以及与谁接触。响应者可能是 IT 安全部门、临床工程部门、第三方网络安全服务提供商，也可能是设备供应商或制造商。找到责任方并就警报与他们联系。

出现安全警报时采取行动

有很多方法可以响应安全警报。您采取的措施取决于该情况的补救要求：

- 如果设备感染了恶意软件或病毒，请立即拔下设备的电源。如果必须继续使用该设备，请与 IT 安全部门合作，将其与网络的其余部分隔离开。您可能需要修改防火墙的安全策略，仅允许设备运行必需的流量，并在制定解决方案时阻止其他所有内容。
- 该解决方案可能需要软件补丁，有时您可能还需要让设备供应商参与打补丁。如果您必须继续使用设备，请在补丁可用之前强制执行严格的零信任策略。
- 如果警报是由安全策略违规生成的，则可以向防火墙发送策略建议，使其仅允许正常设备行为产生的流量。
- 为了帮助您进行分析，IoT Security 提供警报日志文件（采用 .csv 和 .log 格式），其中包含触发警报的设备在数天内建立的网络连接。您还可以下载 IoT Security 以桑基图表形式显示的网络流量数据，并以电子表格 (.xls) 形式查看。

分配和跟踪安全警报

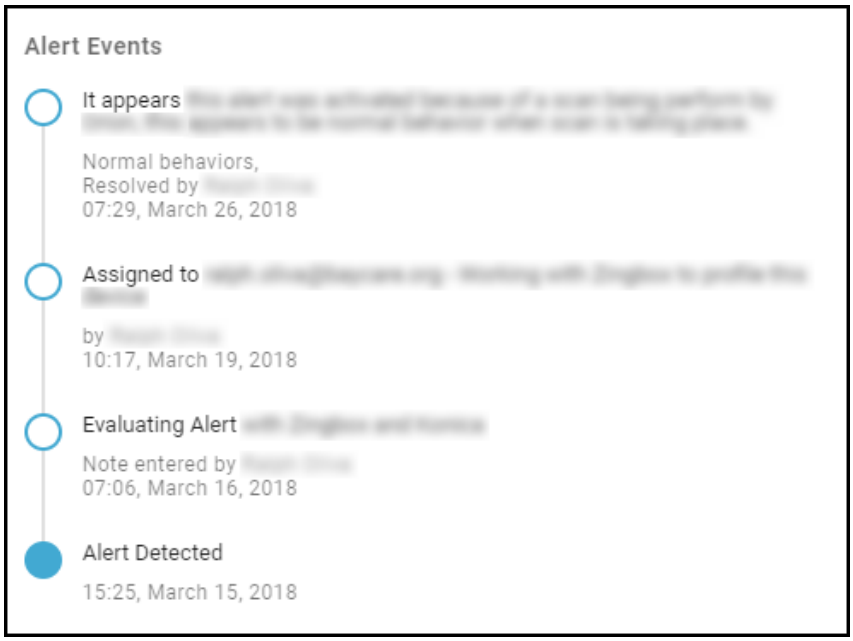
在“警报和警报详细信息”页面中，您可以将安全警报分配给一个或多个人员进行调查。在 **Alerts**（警报） > **Security Alerts**（安全警报） > **All Alerts**（所有警报）上选择警报时，警报表格顶部会显示一组操作。

要将警报分配给他人进行调查，请单击 **More**（更多） > **Assign**（分配）。输入电子邮件地址和备注，然后单击 **Assign**（分配）。

如果您向外部用户（即没有 *Palo Alto Networks* 用户帐户且无法登录 *IoT Security* 门户的用户）分配警报，则包含警报详细信息的 *PDF* 将附在电子邮件中。

通过单击 **Action**（操作） > **Assign**（分配），您还可以从“警报详细信息”页面分配显示的警报。导航路径为：**Alerts**（警报） > **Security Alerts**（安全警报） > **All Alerts**（所有警报） > *alert_title*。

您也可以在警报中添加备注，这是您和团队跟踪高级警报调查进度的一种便捷方式。在“警报”页面中，选择一个警报，然后单击 **More**（更多） > **Add notes**（添加备注）。在“警报详细信息”页面上，单击 **Action**（操作） > **Add Notes**（添加备注）。备注显示在“警报详细信息”页面的“警报事件”列表中。



解决并重新激活安全警报

要解决安全警报，要么接受该警报，要么以某种方式解决问题，可以将其分配给网络安全管理员进行调查和修复。

Resolve 工具可用于显示每周或每月报告中已解决的警报数量。

如果您认为一个或多个警报是可以接受的，例如严重性级别较低的警报，则可以解决这些警报。没必要单独解决每个警报事件。您可以选中警报组名称旁边的复选框，然后单击“警报”列表顶部的 **Resolve**（解决）。

单击 **Resolve**（解决）后，将出现“解决警报”对话框。选择解决原因，添加备注，然后单击 **Resolve**（解决）。

如果您后来决定重新激活之前标记为“已解决”的一个或多个警报，则可以将警报列表上方的过滤器设置为 **Resolved**（已解决），选择警报，然后单击 **Unresolve**（未解决）来实现。在“更改状态”对话框中，输入备注，然后单击 **Change**（更改）。

抑制安全警报

如果 IoT Security 针对预期事件发出安全警报，则可以抑制将出现的警报，这样就无需在这些警报上花费更多资源。您可以仅抑制触发警报的设备，也可以抑制共享相同设备配置文件、类别或设备类型的所有设备，从而抑制未来的警报检测。您可以无限期抑制警报，也可以抑制警报一段有限的时间。除了抑制将来的警报检测外，您还可以将当前警报事件标记为“已解决”。

要抑制警报，请以具有管理员或所有者权限的用户身份登录 IoT Security，然后选择 **Alerts**（警报） > **Security Alerts**（安全警报） > **All Alerts**（所有警报）。选择要抑制的警报，然后单击 **More**（更多） > **Suppress Alerts**（抑制警报）。

如果警报类型相同（警报名称相同），则可以选择多个警报实例。当选择不同的警报类型时，“抑制”选项将不可用。

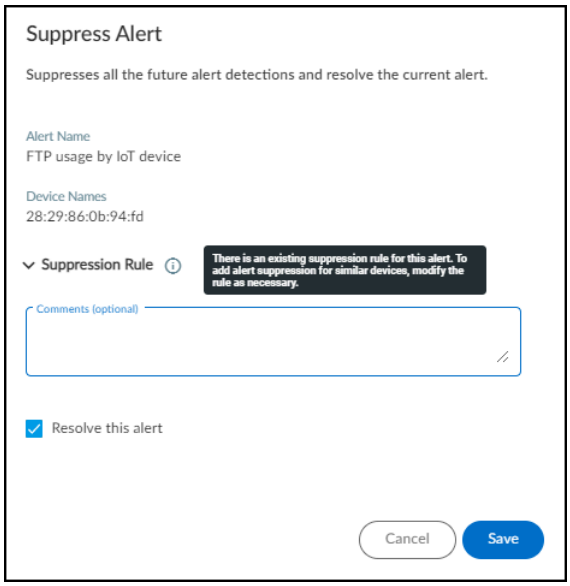
对于触发警报的一台或多台设备，要抑制未来检测到的所有警报，请添加备注，选中 **Resolve this alert**（解决此警报），然后单击 **Save**（保存）。

要抑制未来在其他设备以及该特定设备上检测到的警报，请展开 **Suppression Rule**（抑制规则），在“标签”、“类别”、“配置文件”和“设备类型”字段中选择一个或多个属性，设置警报抑制时长，添加备注，然后单击 **Save**（保存）。如果有任何选定的属性匹配，Cortex XSOAR 将在指定的时间段内抑制未来设备上出现的警报。

创建抑制规则后，IoT Security 约需 30 分钟才能将其应用到整个清单中的所有设备上。IoT Security 还会将其添加到 **Alerts**（警报） > **Security Alerts**（安全警报） > **Suppression Rules**（抑制规则）表中。

单击规则名称将打开“抑制警报”配置面板，您可以在其中查看和编辑详细信息。状态列表示两种状态。规则在创建或修改后的初始 30 分钟申请期内处于“处理中”状态。之后，状态更改为“成功”，表示 IoT Security 已将该规则应用到清单中的所有目标设备。

创建规则后，您可以随时修改规则，使其包括更多设备，方法是修改规则以涵盖更多设备。实际上，每当您要抑制设备上的警报时，IoT Security 都会提示您执行此操作，并且已经有针对此类警报的抑制规则，但它不适用于该特定设备。它会显示一个信息图标，当您将光标悬停在其上方时，该图标会展开为弹出消息。



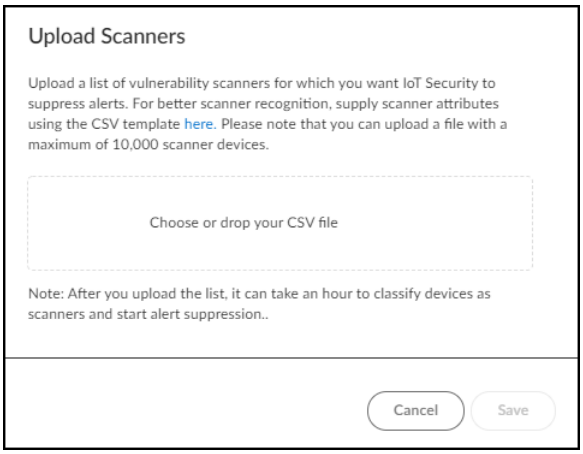
要仅将此设备添加到现有规则，可以选择添加备注并选中 **Resolve this alert**（解决此警报），然后单击 **Save**（保存）。要将抑制规则应用于此设备和其他类似设备，请展开 **View targeted devices**（查看目标设备），修改原始规则，使其包括适用于此设备和类似设备的配置文件、类别或设备类型，然后单击 **Save**（保存）。

要停止警报抑制，请以具有管理员或所有者权限的用户身份登录 IoT Security，然后选择 **Alerts**（警报） > **Security Alerts**（安全警报） > **Suppression Rules**（抑制规则）。在表中选择一行或多行，然后单击 **Release Suppression**（释放抑制）。

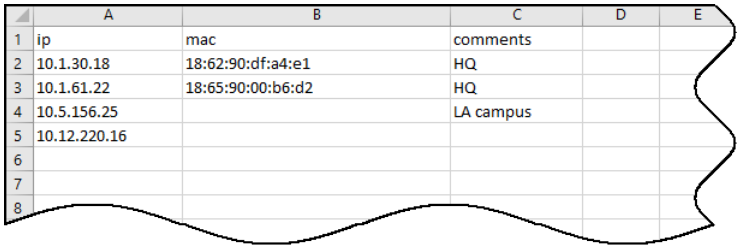
由于漏洞扫描程序生成的流量会触发大量警报，因此您很可能希望抑制对它们发出的警报。如果您有 IoT Security 第三方集成附加组件许可证或功能齐全的 Cortex XSOAR 服务器，则可能已经通过 Cortex XSOAR 为 IoT Security 集成了 Qualys、Rapid7 或 Tenable 漏洞扫描程序。如果是这样，IoT Security 会自动从集成产品中导入所有扫描引擎的名称和 IP 地址，以及所有站点和漏洞扫描模板的名称，并将其添加到 **Settings**（设置） > **Scanners**（扫描程序）的扫描程序列表中。来源列通过显示集成产品名称，表明扫描程序是自动导入的：**Qualys**、**Rapid7** 或 **Tenable**。如果您不想自动将此信息导入扫描程序列表，请在以下 Cortex XSOAR 作业之一中禁用 **Automatically**

Synchronize Scanners with IoT Security（自动同步扫描程序与 **IoT Security**），具体取决于您使用的集成：PANW IoT 获取 Qualys 扫描程序和配置文件，PANW IoT 获取 Rapid7 扫描程序和配置文件，或者 PANW IoT 获取 Tenable 扫描程序和配置文件。禁用此设置不会自动将先前导入的扫描程序从 IoT Security 门户的列表中移除。您必须手动将其删除，方法是在列表中选定相应的扫描程序，单击 **Remove from Scanner List**（从扫描程序列表中移除），然后根据提示单击 **Continue**（继续）。

如果您想抑制由网络上未集成 IoT Security 的漏洞扫描程序触发的警报，请创建扫描程序 IP 地址列表并将其上传到 IoT Security。单击 **Settings**（设置） > **Scanners**（扫描程序），单击 **Add Scanners**（添加扫描程序），然后下载 CSV 模板。



对于每个扫描程序，添加其 IP 地址，还可以选择添加其 MAC 地址和备注。

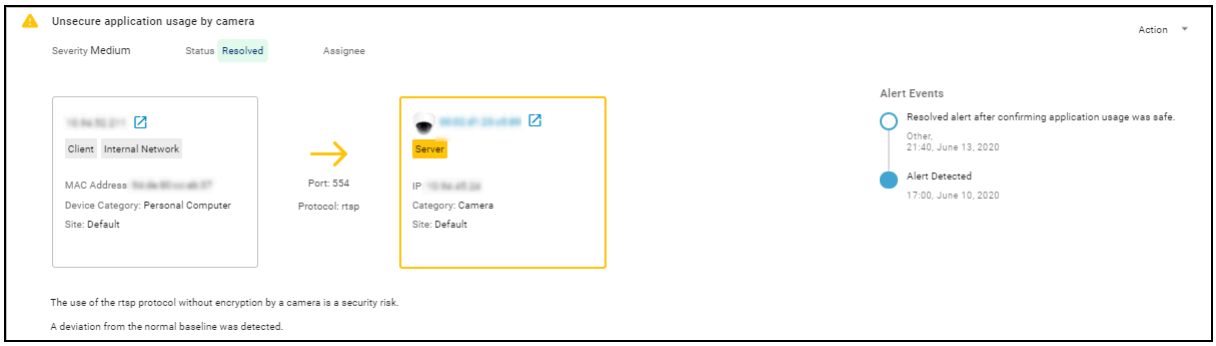


	A	B	C	D	E
1	ip	mac	comments		
2	10.1.30.18	18:62:90:df:a4:e1	HQ		
3	10.1.61.22	18:65:90:00:b6:d2	HQ		
4	10.5.156.25		LA campus		
5	10.12.220.16				
6					
7					
8					

将文件上传到 IoT Security。如果 CSV 文件中的 IP 地址与设备清单中的 IP 地址相匹配，IoT Security 会将其添加到扫描程序列表中，并开始抑制针对它们的警报。（上传后最多可能需要一个小时才能开始抑制警报。）“扫描程序”表中的“来源”列通过显示 **User**（用户）来表示扫描程序是手动上传的。如果 IP 地址对 IoT Security 来说是新的，则会将其添加到扫描程序列表中，并在检测到它们的网络流量后，将其作为扫描程序添加到清单中。如果有重复的条目，IoT Security 在上传过程中会将其跳过。最后，如果上传的扫描程序的 IP 和 Mac 地址的配对与清单中设备的配对不相符，则 IoT Security 不会上传。

常规安全警报管理

定期监控添加到警报事件列表中的备注，以了解您正在跟踪的高级安全警报。这是团队成员协调工作和检查状态的有效方式。



每天查看低严重性警报。选择您认为可以接受的问题，然后单击几下即可解决所有问题，如上一节所述。

每周或每月下载所有警报和所有已解决的警报。使用那里的数据制作状态报告，以显示您的团队的所作所为。

除了对已经出现的警报做出反应外，您还可以在攻击发生之前主动修复漏洞。在 **Dashboards**（指示板） **> Security Dashboard**（安全指示板）上，查看“风险”面板中的“目前的活跃漏洞”条目。

单击 **Active Vulnerabilities to Date**（目前的活跃漏洞）以打开 **Vulnerabilities**（漏洞） **> All Vulnerabilities**（所有漏洞）页面。

默认情况下，IoT Security 门户按严重性对漏洞进行排序，首先显示最严重的漏洞。当您单击漏洞名称时，会打开其漏洞详细信息页面。您可以在此处查看哪些设备易受攻击，因此您可以采取措施在漏洞被攻击之前将其删除。

推荐安全策略

IoT Security 使用机器学习根据同一设备配置文件中的 IoT 设备的正常、可接受的网络行为自动生成策略规则建议。

- 策略规则建议
- 设备配置文件概述
- 设备配置文件行为
- 设备配置文件策略
- 在 IoT Security 中创建策略集
- 将策略集导入 Panorama
- 限制网络访问权限

策略规则建议

IoT Security 使用机器学习根据同一设备配置文件中 IoT 设备的正常、可接受的网络行为自动生成安全策略规则建议。然后，它为新一代防火墙控制 IoT 设备流量提供这些建议。

IoT Security 从它在 IoT 设备生成的流量中观察到的网络行为得出建议，这些 IoT 设备位于跨多个 IoT Security 租户的同一配置文件中。它将观察到的行为中的应用程序分为三组：

- 未在本地观察到的常用应用程序 — 多个 IoT Security 租户环境（不包括您自己的）中的设备配置文件中设备常用的应用程序。
- 本地观察到底常用应用程序 — 多个 IoT Security 租户环境（包括您自己的）中的设备配置文件中的设备常用的应用程序
- 唯一应用程序 — 此设备配置文件中的设备不常用的应用程序，仅您的环境中的设备在使用中观察到的应用程序

目前，*multi-vsys* 防火墙不支持策略规则建议。您必须手动创建。

从 *PAN-OS 11.1* 开始，向新一代防火墙推荐安全策略规则采用与此处介绍的不同的过程。以下工作流程仍然适用于运行 *PAN-OS 11.1* 之前的 *PAN-OS* 版本的防火墙。

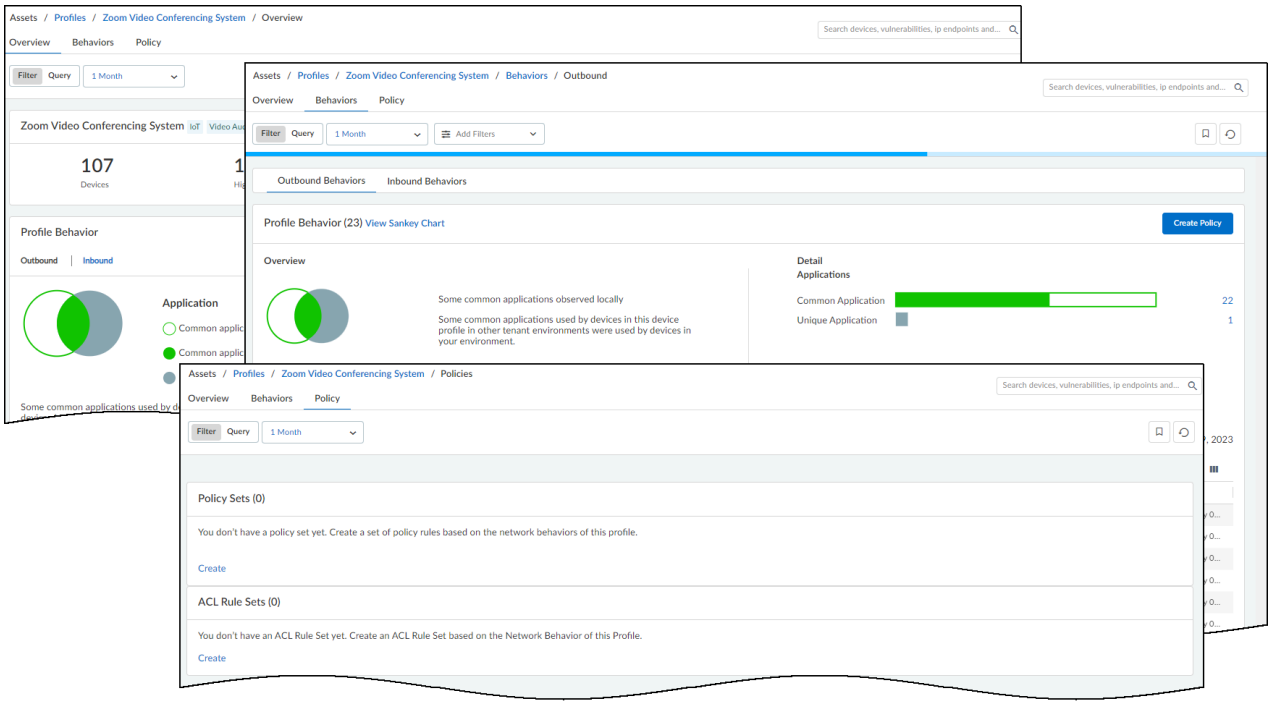
然后，IoT Security 会制定一套策略规则建议。这些规则允许此设备配置文件中的设备继续执行多个租户环境中常见的网络行为以及您特有的网络行为。前提是这些行为是属于此设备配置文件的设备运行所必需的。您可以接受所有这些建议，也可以禁用或修改单个规则，以满足网络的安全要求。当您对策略集感到满意时，请将其保存并激活。一旦激活，防火墙就可以通过 Panorama 或直接导入，然后添加到规则集中。

Panorama 或防火墙管理员从 IoT Security 导入一组安全策略规则时，导入操作会自动在建议的规则中从源配置文件和目标配置文件创建设备对象，并在其构造的安全策略规则中使用这些对象。为了让防火墙识别要将其策略规则应用于哪些 IoT 设备，它使用 IoT Security 通过 Device-ID 提供的 IP 地址到设备的映射。防火墙从映射中获取 IoT 设备的设备配置文件，并应用以匹配的设备对象为源的规则。

IoT Security 应用仅针对高度自信（置信度得分为 *90-100 %*）的 *IoT* 设备提出策略规则建议。它不考虑中低置信度 *IoT* 设备的网络行为（*0-69%* 和 *70-89%* 得分）。此外，*IoT Security* 不为 *IT* 设备提供策略规则建议、警报和漏洞检测以及网络行为分析，*IT* 设备不是为特定任务而构建的设备，例如个人电脑、智能手机和平板电脑。对于 *IT* 设备，*IoT Security* 应用仅提供设备标识。

让 IoT Security 有足够的时间在配置文件中收集 IoT 设备的全部行为之后，您就准备好了为其创建策略规则建议。

要开始，请登录 IoT Security 门户，导航到 **Assets**（资产） > **Profiles**（配置文件），然后单击配置文件名称。

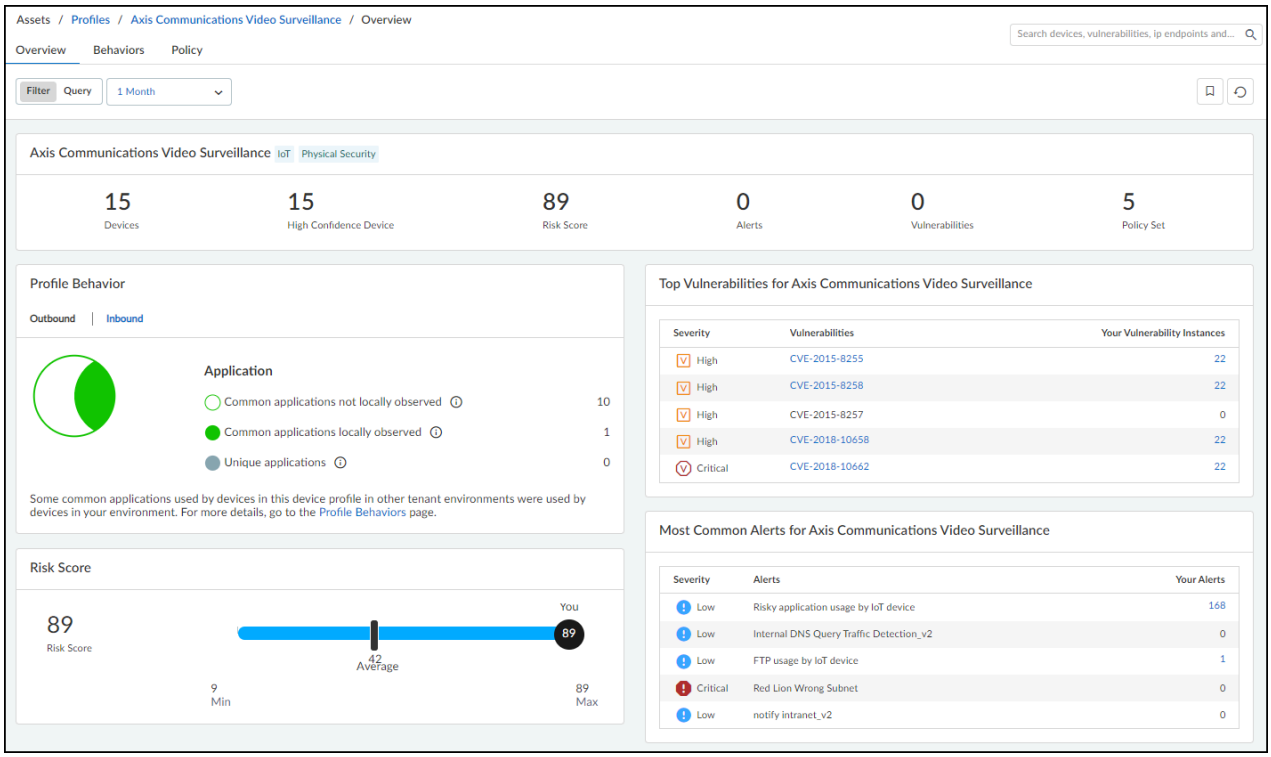


IoT Security 显示三个配置文件详细信息页面：

- **Overview**（概述）— 查看此配置文件中高置信度 IoT 设备及其在过去一天、一周或一个月的相关风险因素的摘要。请参阅设备配置文件概述。
- **Behaviors**（行为）— 查看本地网络环境中和其他 IoT Security 租户环境中属于此配置文件的高置信度 IoT 设备的行为。同时根据这些观察到的行为为新一代防火墙创建安全策略规则集。请参阅设备配置文件行为。
- **Policy**（策略）— 查看以前为新一代防火墙创建的安全策略规则集和与 Cisco ISE 集成的 ACL 规则集。IoT Security 会根据在本地网络环境中该配置文件的高置信度 IoT 设备和在其他 IoT Security 租户环境中观察到的网络行为生成这两种类型的规则集。请参阅设备配置文件策略。

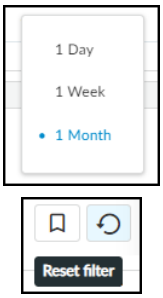
设备配置文件概述

要访问设备配置文件的“概述”页面，请选择 **Assets**（资产） > **Profiles**（配置文件） > *profile_name* > **Overview**（概述）。



概述页面显示有关此配置文件中设备的数据。数据仅从置信度分数高达 90-100% 的 IoT 设备中提取；即 IoT Security 识别为高置信度的设备。如果高置信度设备的数量低于 50%，请考虑使用数据质量诊断页面 [**Administration**（管理） > **Data Quality**（数据质量）] 上提供的建议来增加配置文件中高置信度设备的数量。

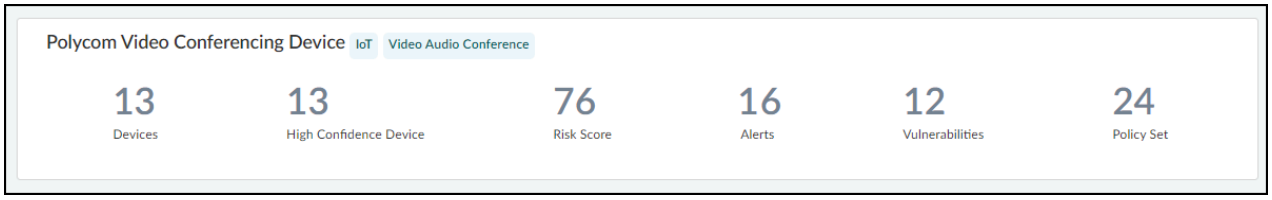
时间过滤器 — 时间过滤器通过配置文件中在过去 1 天（到现在为止的过去 24 小时）、过去 1 周或过去 1 个月内在网络上处于活动状态的高置信度设备数量来控制“概览”页面上显示的数据。单击 **Reset filter**（重置过滤条件）图标 ( )，将其设置为 **1 Day**（**1** 天）。



时间过滤器仅影响本地网络中高置信度设备的显示，不影响所有设备的显示。

摘要栏 — 概述页面顶部的配置文件摘要简单提供了有关配置文件中设备的重要信息：设备总数、高置信度设备的数量、该设备配置文件的风险评分（有关风险评估的详细信息，请参阅IoT 风险评估）、高置信度设备的警报和漏洞数量，以及为此配置文件配置的策略集的数量。

您可以为同一个配置文件配置多个策略集，但一次只能激活其中一个策略集。



摘要下方是有关设备配置文件关键方面和相关风险因素的几个部分。IoT Security 通过使用机器学习来观察和分析配置文件中所有高可信设备的网络活动，从而生成这些信息。然后，它将有关您的设备的信息与其他 IoT Security 租户网络中相同设备配置文件中的信息进行比较，从而使您了解您的设备行为和风险水平如何与其他租户网络相匹配。

配置文件行为 — 这显示了高置信度设备的不同类型的出站和入站行为。单击 **Outbound**（出站）和 **Inbound**（入站），在这两种行为之间切换。

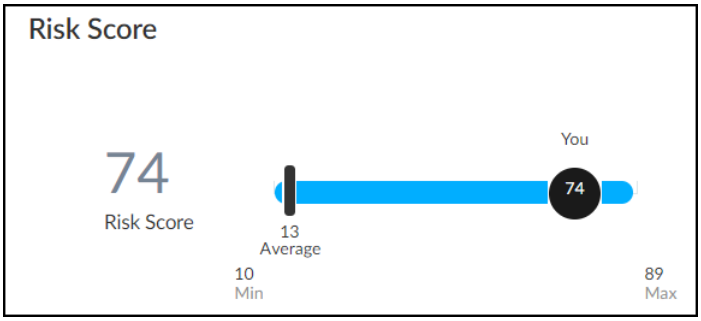
IoT Security 将此配置文件中的高置信度设备在页面顶部设置的时间范围内使用的应用程序与同一配置文件中的设备在其他 IoT Security 租户中使用的应用程序进行比较。时间过滤器为 1 天、1 周或 1 个月。然后，它仅显示在其他租户的环境（常用，不是本地观察到的）、您和其他租户的环境（常用、本地观察到的）以及仅在您的环境（独特的应用程序）中观察到的应用程序数量。

profile_name 的最常见警报 — 这列出该设备配置文件中设备针对多个 IoT Security 租户及其严重性级别发出的多达五个最常见的安全警报。您的设备发出的警报数量也显示在标签为“您的提醒”的列中。

profile_name 的主要漏洞 — 这列出最多五个影响该设备配置文件中多个 IoT Security 租户的设备的主要漏洞及其严重性级别。您的网络环境中的漏洞实例数量也显示在标签为“您的漏洞实例”的列中。

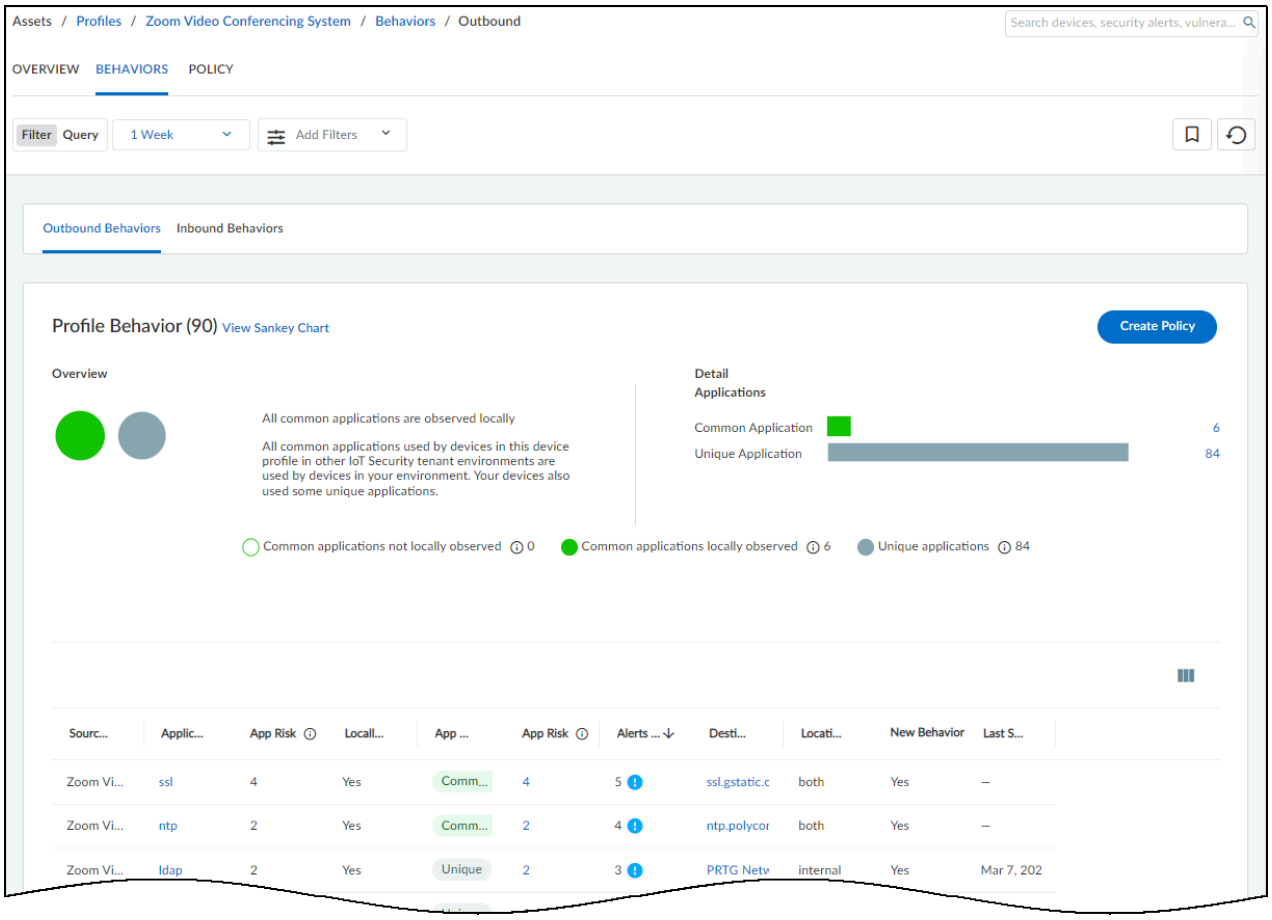
风险分数 — 显示设备配置文件相对于总体范围的风险分数以及与具有相同配置文件的所有 IoT Security 租户的平均值相关的风险分数。这可以帮助您查看设备相对于其他 IoT Security 租户平均水平的风险级别。

在以下屏幕截图中，范围为 10 到 89，这是该设备配置文件在所有 IoT Security 租户中最低和最高的风险分数，平均风险评分为 13。本地风险评分为 74 时，您可以考虑应对一些威胁以降低风险，并将分数降至远离该范围的高端。



设备配置文件行为

要访问设备配置文件的概述页面，请选择 **Assets**（资产） > **Profiles**（配置文件）> *profile_name* > **Behaviors**（行为）。

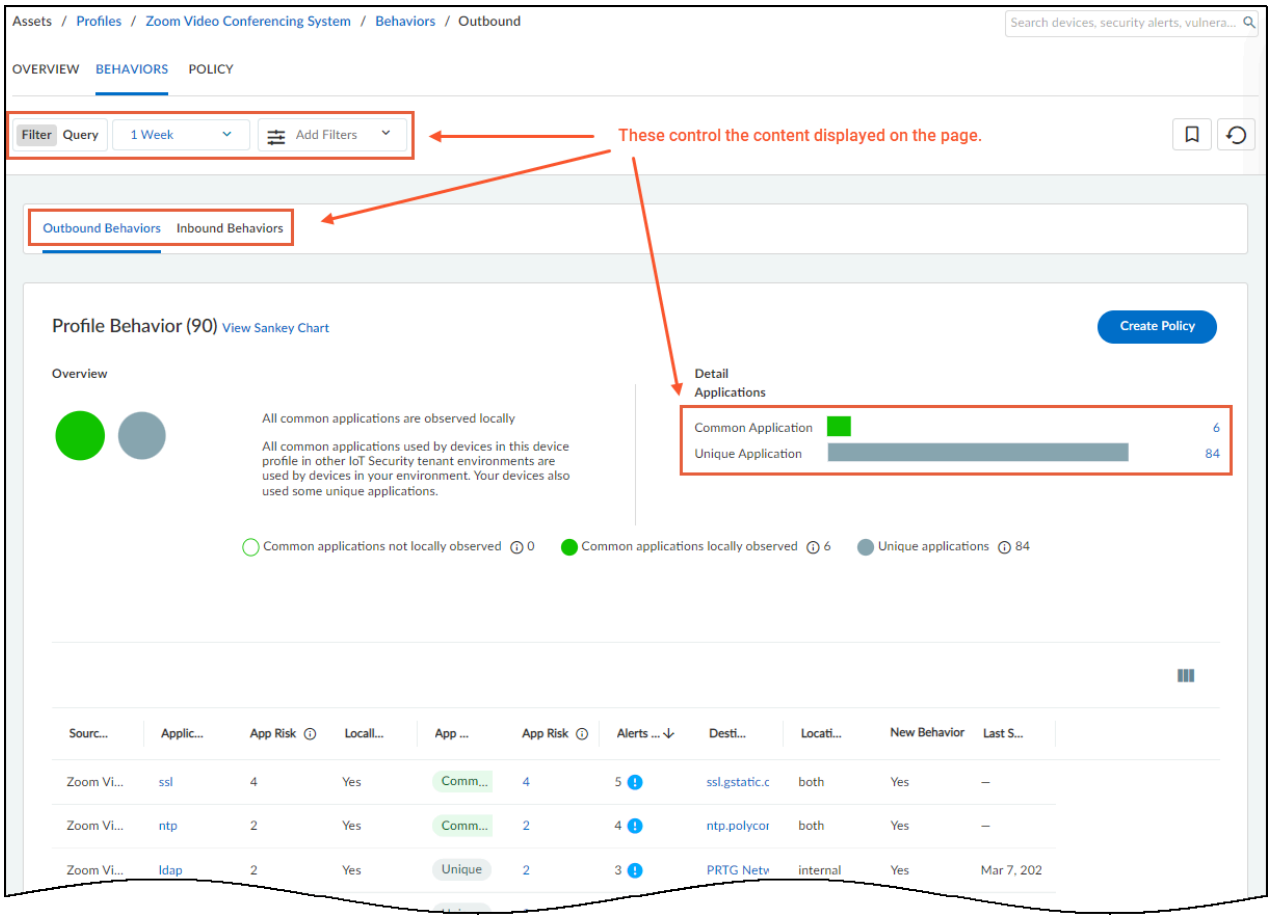


行为页面显示此配置文件中高置信度 IoT 设备的行为。这些是 IoT Security 已识别为高度可信，并计算出置信度得分为 90-100% 的 IoT 设备。这些行为属于其他 IoT Security 租户的同一配置文件的 IoT 设备在您的本地网络环境和其他网络环境中的行为。

置信度分数表示 *IoT Security* 在其设备标识中的置信度水平。根据计算出的置信度分数，*IoT Security* 有三个置信度级别：高 *(90-100%)*、中 *(70-89%)* 和低 *(0-69%)*。

过滤显示的内容

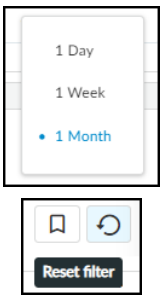
此页面和相关桑基图中显示的行为由页面顶部的过滤器控制；显示出站或入站行为的选项；以及在“配置文件行为”部分中的“应用程序”下显示常见应用程序、唯一应用程序或两者（默认）的选项。



时间过滤器还决定显示哪些出站或入站行为。

您只能为出站行为创建策略规则集；也就是说，当行为的来源是设备配置文件中的 *IoT* 设备时。*IoT Security* 不会针对入站行为（即 *IoT* 设备作为目标的情况）生成策略规则建议。

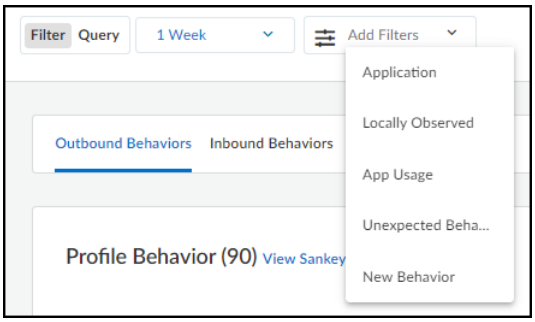
时间过滤器 — 时间过滤器根据过去 1 天（截至目前的过去 24 小时）、过去 1 周或过去 1 个月内在网络上观察到的每个行为来控制“行为”页面上显示的行为。单击 **Reset filter**（重置过滤器）图标 ( ) 将时间设置为 1 天，并删除您可能设置的任何其他过滤器。



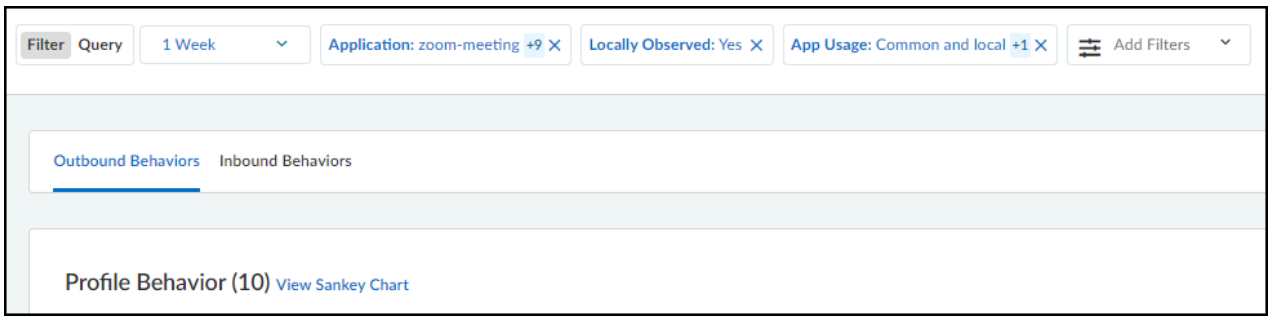
Add Filters（添加过滤器） — 添加过滤器以显示特定类型的行为。选择以下一项或多项：

- **Applications**（应用程序） — 选择要在页面上显示的一个或多个应用程序。列出的应用程序是在时间过滤器设置的时间段内，在网络上观察到的高置信度 IoT 设备行为的一部分。
- **Local Observed**（本地观察） — 选定并选择 **Yes**（是）以显示在网络中本地观察到的行为，或选择 **No**（否）以隐藏本地观察到的行为。
- **App Usage**（应用使用情况） — 根据观察到的行为的位置选择并确定要显示的内容：
  - **Common only**（仅常见）是在其他 IoT Security 租户环境中观察到，但不是在您的环境中观察到的行为。
  - **Common and local**（常见和本地）行为是在其他租户环境和您的环境中都观察到的行为。
  - **Local only**（仅限本地）是在您的环境中观察到的行为，而不是在任何其他租户的环境中观察到的行为。
- **Unexpected behavior**（意外行为） — 选定并选择 **Yes**（是）以显示在激活策略集时明确不允许，但随后出现在网络上的行为。选择 **No**（否）以隐藏意外行为。
- 新行为 — 选定并选择 **Yes**（是）以显示上次激活策略集后在网络上发现的行为。选择 **No**（否）以隐藏新行为。

这些过滤器和时间过滤器都无法决定在您可能创建的任何策略集中包含哪些行为。它们仅决定在行为页面上显示什么。然而，一旦您开始创建策略集，*IoT Security* 会显示一组类似的过滤器，以供在策略创建过程中使用。



当您添加和删除过滤器时，“配置文件行为”旁边括号中的数字也会相应变化。请参阅此处以快速了解过滤器如何影响过滤器生效期间页面上出现的行为数量。



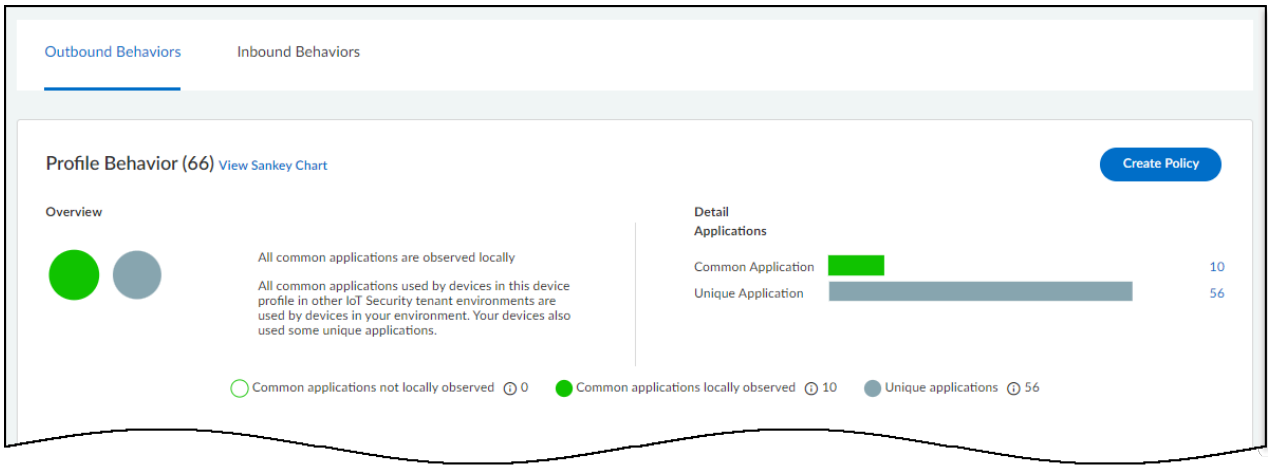
Outbound Behaviors（出站行为）和 **Inbound Behaviors**（入站行为） — 默认情况下显示出站行为。这些行为中，该设备配置文件是网络活动的来源。

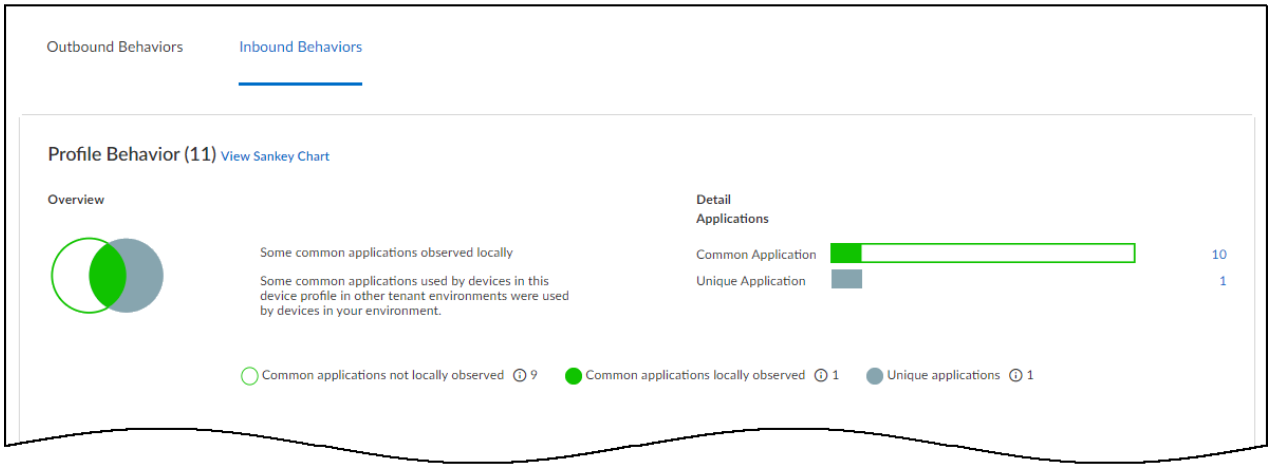
在下面两个的上面屏幕截图中，有 66 个出站行为：

- 10 个出站行为包括在您和其他租户的环境中观察到的常见应用程序。这些在维恩图和条形图中以绿色填充表示。
- 56 包括适合您的环境的独特应用程序。这些以灰色表示。

在下面的屏幕截图中，有 11 个入站行为，这些行为是此设备配置文件作为网络活动目标的行为：

- 9 个入站行为包括在其他租户的环境中观察到但在您的环境中未观察到的常见应用程序。这些在维恩图和条形图中以绿色轮廓表示。
- 1 包括在您和其他租户的环境中观察到的常见应用程序。这以绿色实心圆表示。
- 1 包括仅在您的环境中观察到的独特应用程序。这以灰色表示。





您选择的方向（出站或入站）控制“行为”页面底部列表和桑基图中显示的内容。您的选择还会显示或隐藏 **Create Policy**（创建策略）按钮，仅在 **Outbound Behaviors**（出站行为）处于活动状态时显示该按钮。单击条形图右侧的数字还可以控制是否在页面和桑基图中显示常见或独特的应用程序。要通过单击任一数字撤消应用的过滤器，请在页面顶部旁边单击位于时间过滤器旁的 **Reset filter**（重置过滤器）图标 ( )。

创建策略集

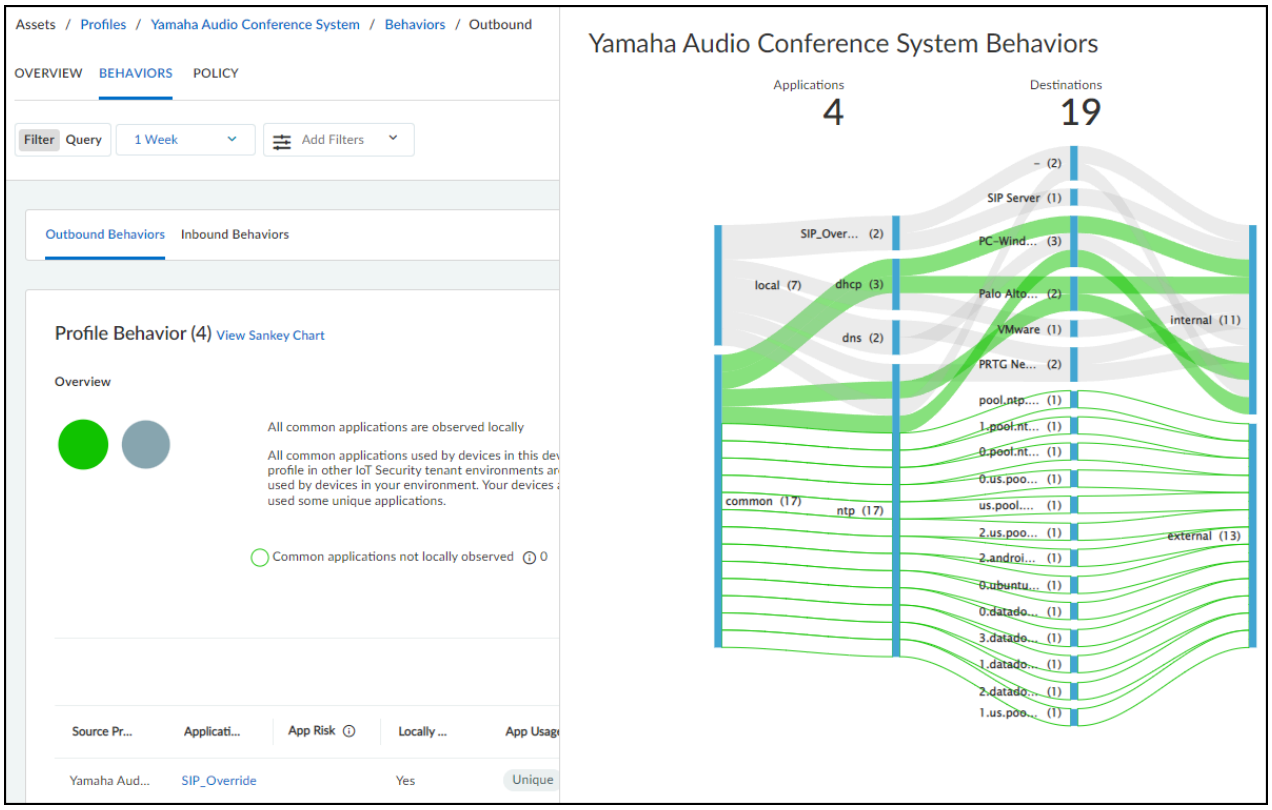
使用 IoT Security 根据在同一设备配置文件中观察到的 IoT 设备的网络行为来创建策略规则集的建议。有关创建策略集的说明，请参阅 在 IoT Security 中创建策略集。

从 *PAN-OS 11.1* 开始，向新一代防火墙推荐安全策略规则采用与此处介绍的不同的过程。以下工作流程仍然适用于运行 *PAN-OS 11.1* 之前的 *PAN-OS* 版本的防火墙。

查看桑基图

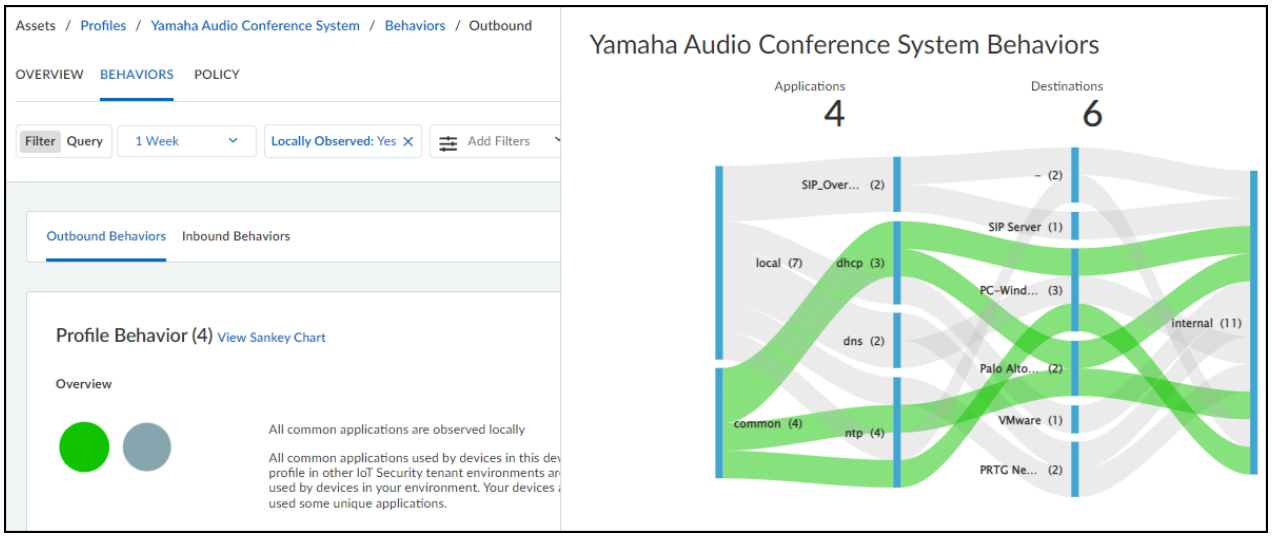
桑基图是一种用线表示连接的图表。单击 **View Sankey Chart**（查看桑基图）以打开右侧面板，显示应用程序从源（出站行为中的当前设备配置文件）到目标以及目标位置（内部或外部）的流程。这些线条按上述颜色编码，并分为以下三组：

- 灰色适用于独特的本地应用程序
- 绿色实心圆表示本地观察到的常见应用
- 绿色空心圆表示未在本地观察到的常见应用

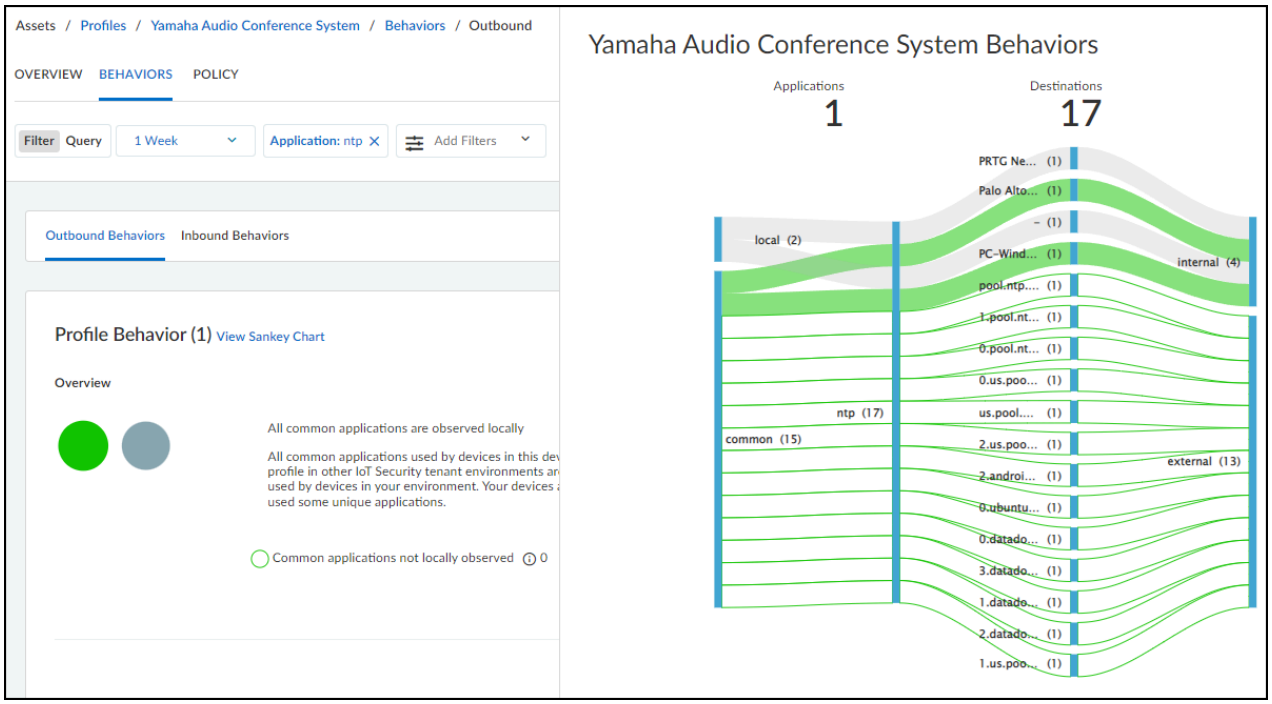


当目标的设备配置文件未知时，内部目标会显示短横线。目标后的数字表示目标配置文件（对于内部目标）或域名后面（对于外部目标）的不同 *IP* 地址的数量。

由于桑基图在包含大量线条时会变得难以理解，因此您可以应用过滤器来减少线条的数量。例如，应用仅显示本地观察到的应用程序的过滤器会将上图中的线数从 24 减少到 11，同时增加线宽。请参阅下面的图表。



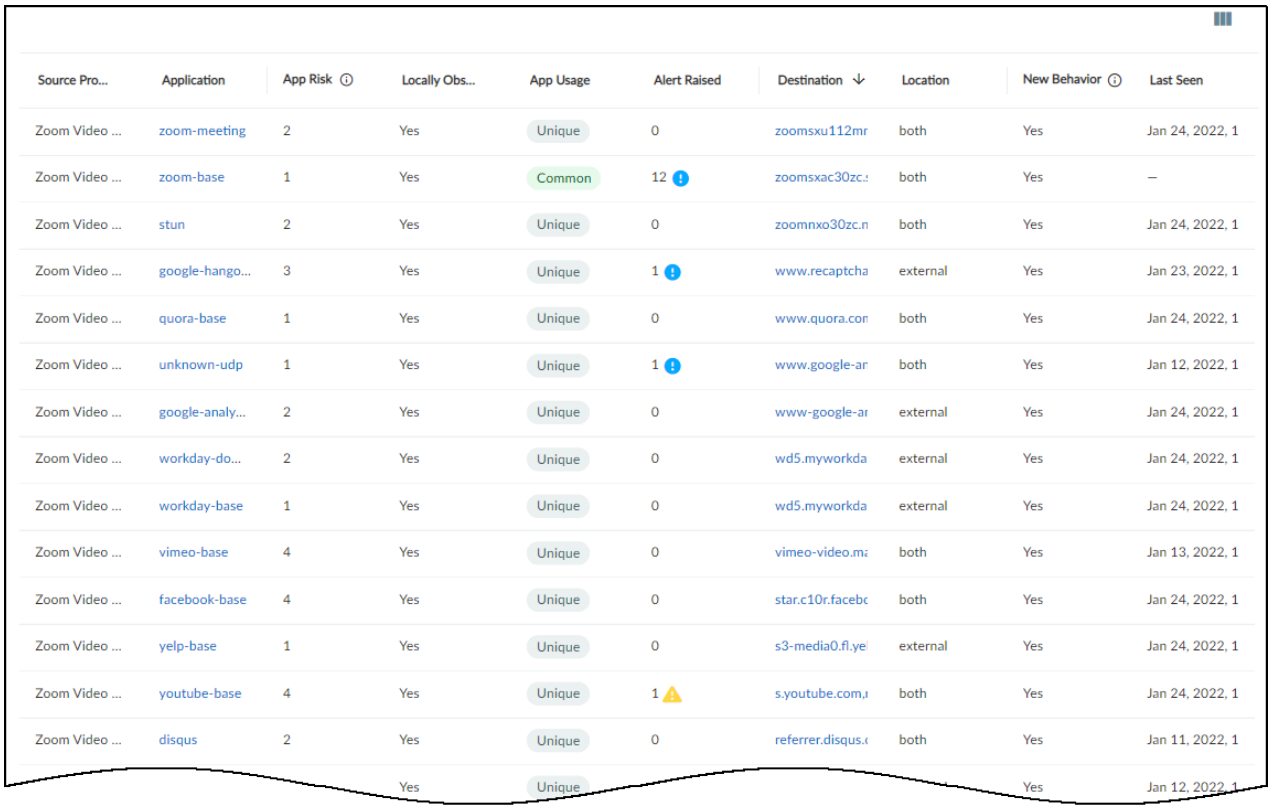
您还可以应用应用程序过滤器。例如，如果有一个应用程序令您感兴趣，那么您可以仅显示包含该应用程序的行为。您还可以按多个应用程序进行过滤。以下屏幕截图显示了仅针对 NTP 的出站行为。



该图表的另一个特点是您可以将光标悬停在线条和蓝条上以查看信息弹出窗口。在上面的屏幕截图中，光标悬停在目标栏上，其中一种常见行为与目标栏交叉，显示一个弹出窗口，标识其特定目标。这对于查看图表中缩写的完整目标配置文件名称和域名很有用。

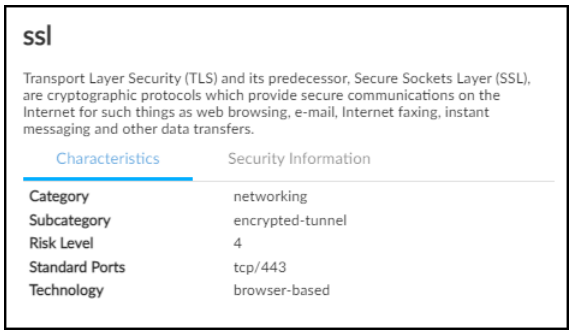
查看行为表

“行为”页面的底部是一个表格，列出了此配置文件与已设置的过滤器匹配的所有行为：靠近页面顶部的时间过滤器和附加过滤器、出站或入站行为切换，以及详细应用程序下的通用或唯一应用程序编号。表中的数据是按应用程序分组的行为汇总的。

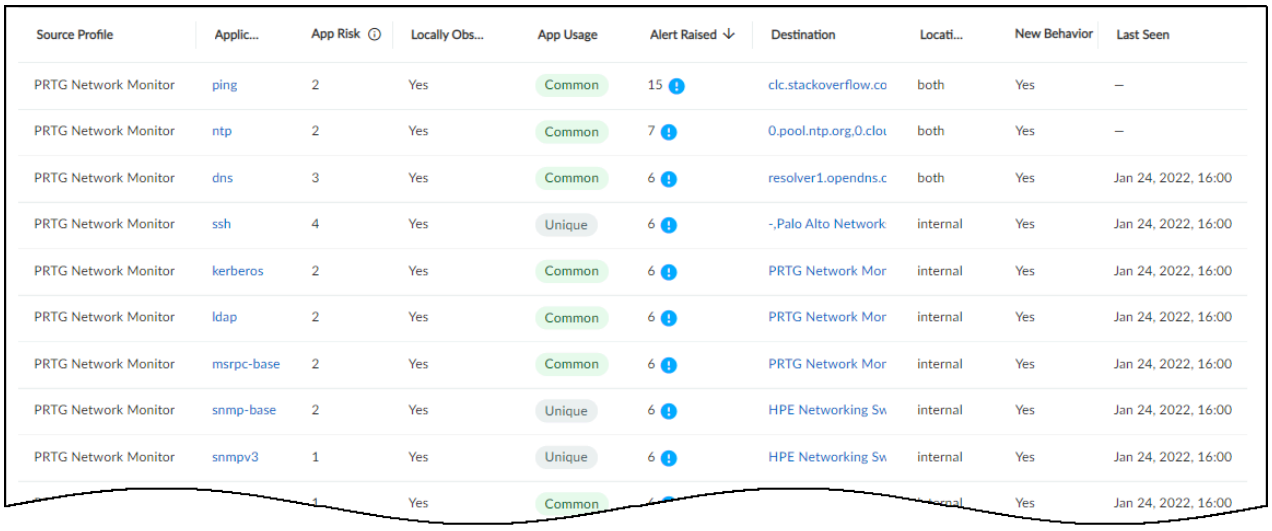


Source Pro...	Application	App Risk	Locally Obs...	App Usage	Alert Raised	Destination	Location	New Behavior	Last Seen
Zoom Video ...	zoom-meeting	2	Yes	Unique	0	zoomsxu112mr	both	Yes	Jan 24, 2022, 1
Zoom Video ...	zoom-base	1	Yes	Common	12	zoomsxac30zc.:	both	Yes	–
Zoom Video ...	stun	2	Yes	Unique	0	zoomnxo30zc.n	both	Yes	Jan 24, 2022, 1
Zoom Video ...	google-hango...	3	Yes	Unique	1	www.recaptcha	external	Yes	Jan 23, 2022, 1
Zoom Video ...	quora-base	1	Yes	Unique	0	www.quora.cor	both	Yes	Jan 24, 2022, 1
Zoom Video ...	unknown-udp	1	Yes	Unique	1	www.google-ar	both	Yes	Jan 12, 2022, 1
Zoom Video ...	google-analy...	2	Yes	Unique	0	www-google-ar	external	Yes	Jan 24, 2022, 1
Zoom Video ...	workday-do...	2	Yes	Unique	0	wd5.myworkda	external	Yes	Jan 24, 2022, 1
Zoom Video ...	workday-base	1	Yes	Unique	0	wd5.myworkda	external	Yes	Jan 24, 2022, 1
Zoom Video ...	vimeo-base	4	Yes	Unique	0	vimeo-video.ma	both	Yes	Jan 13, 2022, 1
Zoom Video ...	facebook-base	4	Yes	Unique	0	star.c10r.facebc	both	Yes	Jan 24, 2022, 1
Zoom Video ...	yelp-base	1	Yes	Unique	0	s3-media0.fl.ye	external	Yes	Jan 24, 2022, 1
Zoom Video ...	youtube-base	4	Yes	Unique	1	s.youtube.com,r	both	Yes	Jan 24, 2022, 1
Zoom Video ...	disqus	2	Yes	Unique	0	referrer.disqus.c	both	Yes	Jan 11, 2022, 1
			Yes	Unique				Yes	Jan 12, 2022, 1

应用程序风险列包含 Applipedia 中定义的此应用程序的风险级别。风险等级分为 1 至 5 级，数字越接近 5，风险就越大。将光标悬停在应用程序名称上将显示一个弹出面板，其中包含从 Applipedia 检索的有关该应用程序的信息。有关此信息的解释，请参阅IoT 设备应用发现。

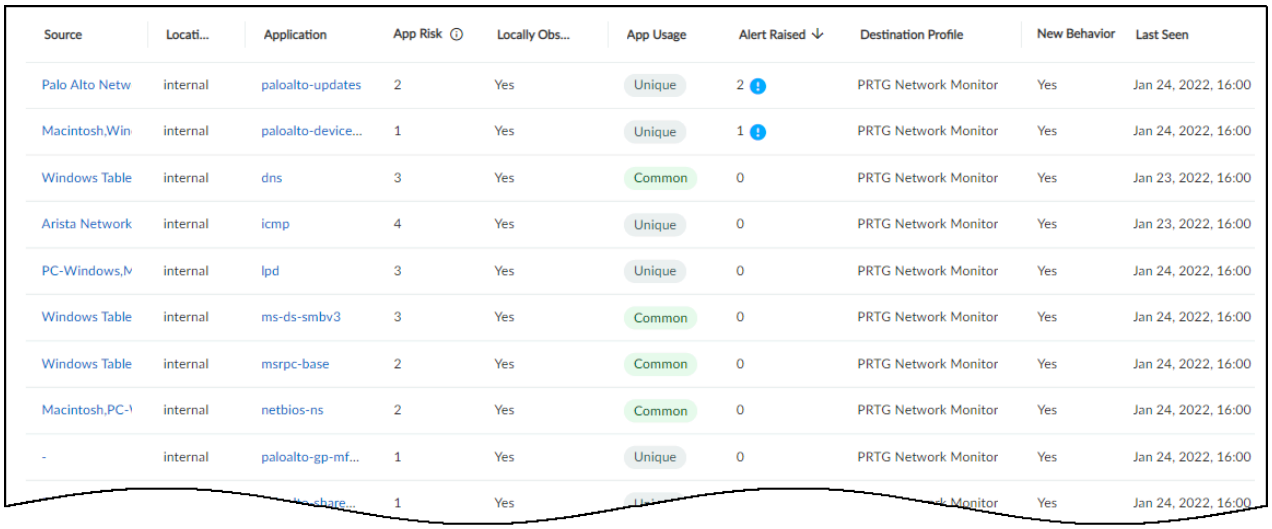


安全警报实例的数量及其严重性级别显示在“引发的警报”列中。对于出站行为，您可以在每行中看到应用程序源配置文件中设备上发生的警报实例数。



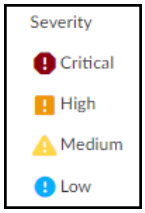
Source Profile	Applic...	App Risk	Locally Obs...	App Usage	Alert Raised	Destination	Locati...	New Behavior	Last Seen
PRTG Network Monitor	ping	2	Yes	Common	15	clc.stackoverflow.co	both	Yes	–
PRTG Network Monitor	ntp	2	Yes	Common	7	0.pool.ntp.org,0.clou	both	Yes	–
PRTG Network Monitor	dns	3	Yes	Common	6	resolver1.opendns.c	both	Yes	Jan 24, 2022, 16:00
PRTG Network Monitor	ssh	4	Yes	Unique	6	-,Palo Alto Network	internal	Yes	Jan 24, 2022, 16:00
PRTG Network Monitor	kerberos	2	Yes	Common	6	PRTG Network Mor	internal	Yes	Jan 24, 2022, 16:00
PRTG Network Monitor	ldap	2	Yes	Common	6	PRTG Network Mor	internal	Yes	Jan 24, 2022, 16:00
PRTG Network Monitor	msrpc-base	2	Yes	Common	6	PRTG Network Mor	internal	Yes	Jan 24, 2022, 16:00
PRTG Network Monitor	snmp-base	2	Yes	Unique	6	HPE Networking Sw	internal	Yes	Jan 24, 2022, 16:00
PRTG Network Monitor	snmpv3	1	Yes	Unique	6	HPE Networking Sw	internal	Yes	Jan 24, 2022, 16:00
		1	Yes	Common	6			Yes	Jan 24, 2022, 16:00

对于入站行为，“引发的警报”列显示应用程序目标配置文件中的设备上发生的警报实例的数量。

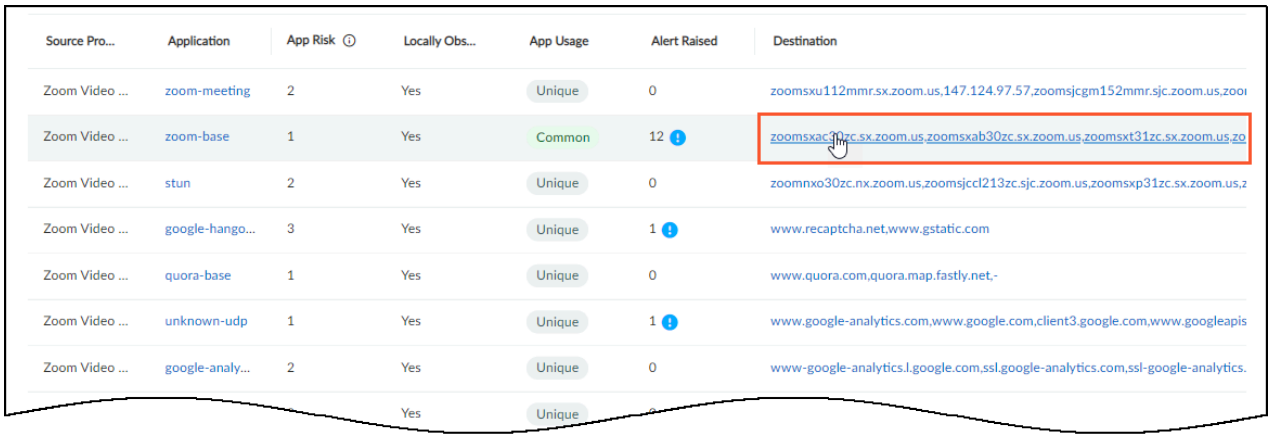


Source	Locati...	Application	App Risk	Locally Obs...	App Usage	Alert Raised	Destination Profile	New Behavior	Last Seen
Palo Alto Netw	internal	paloalto-updates	2	Yes	Unique	2	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
Macintosh,Win	internal	paloalto-device...	1	Yes	Unique	1	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
Windows Table	internal	dns	3	Yes	Common	0	PRTG Network Monitor	Yes	Jan 23, 2022, 16:00
Arista Network	internal	icmp	4	Yes	Unique	0	PRTG Network Monitor	Yes	Jan 23, 2022, 16:00
PC-Windows,M	internal	lpd	3	Yes	Unique	0	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
Windows Table	internal	ms-ds-smbv3	3	Yes	Common	0	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
Windows Table	internal	msrpc-base	2	Yes	Common	0	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
Macintosh,PC-I	internal	netbios-ns	2	Yes	Common	0	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
-	internal	paloalto-gp-mf...	1	Yes	Unique	0	PRTG Network Monitor	Yes	Jan 24, 2022, 16:00
			1	Yes				Yes	Jan 24, 2022, 16:00

“引发的警报”列中的警报实例总数按其严重性级别分组：关键、高、中和低。以下图标表示这四个级别：

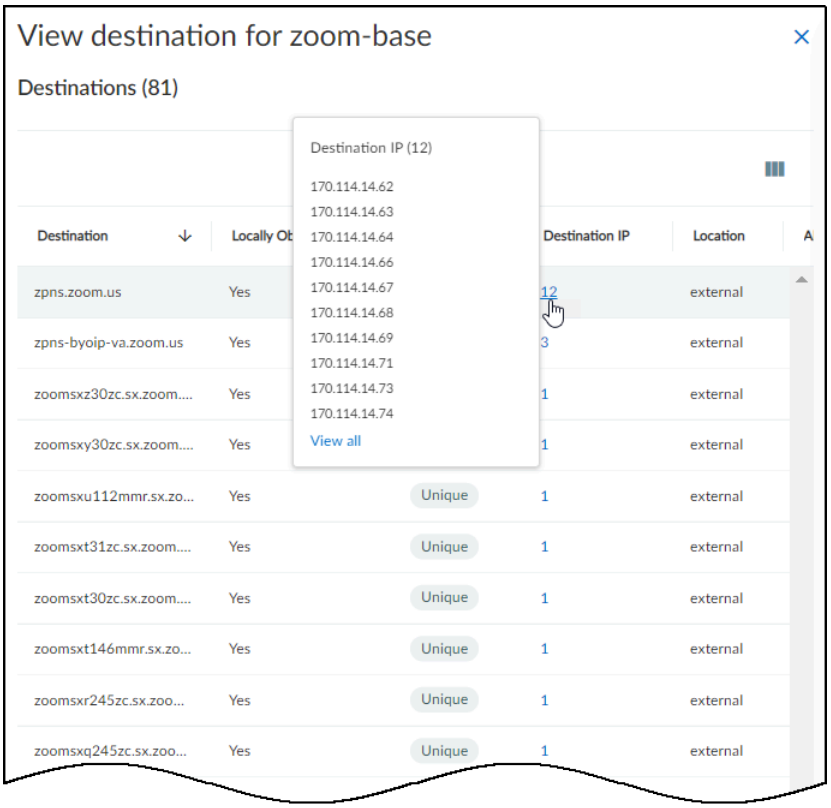


源设备配置文件和应用程序的行为可能有多个目标。您可以拖动目标列来加宽它，但这仍然可能不足以看到所有内容。要打开包含详细信息的面板，请单击目标字段中的任意位置。

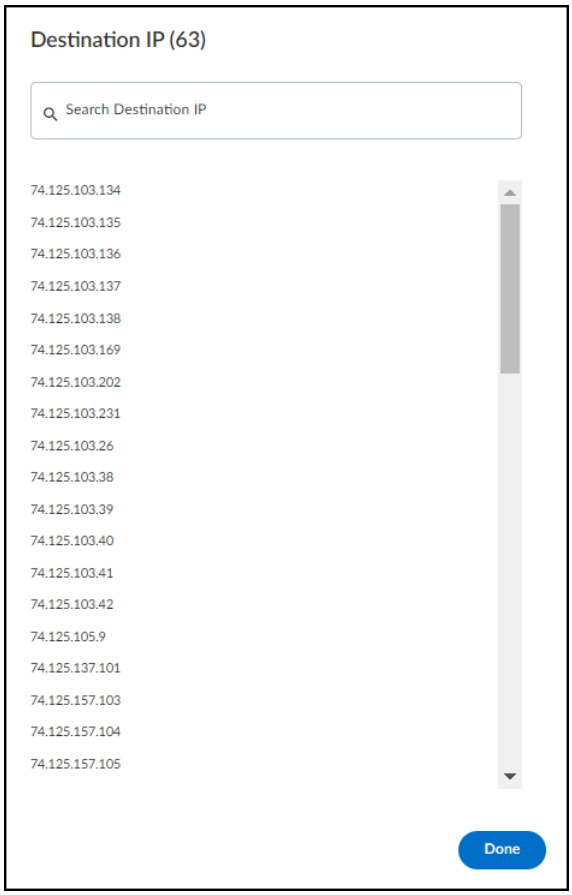


Source Pro...	Application	App Risk	Locally Obs...	App Usage	Alert Raised	Destination
Zoom Video ...	zoom-meeting	2	Yes	Unique	0	zoomsxu112mmr.sx.zoom.us,147.124.97.57,zoomsjcgm152mmr.sjc.zoom.us,zoo
Zoom Video ...	zoom-base	1	Yes	Common	12	zoomsxac30zc.sx.zoom.us,zoomsxab30zc.sx.zoom.us,zoomsxt31zc.sx.zoom.us,zo
Zoom Video ...	stun	2	Yes	Unique	0	zoomnxo30zc.nx.zoom.us,zoomsjccl213zc.sjc.zoom.us,zoomsxp31zc.sx.zoom.us,z
Zoom Video ...	google-hango...	3	Yes	Unique	1	www.recaptcha.net,www.gstatic.com
Zoom Video ...	quora-base	1	Yes	Unique	0	www.quora.com,quora.map.fastly.net,-
Zoom Video ...	unknown-udp	1	Yes	Unique	1	www.google-analytics.com,www.google.com,client3.google.com,www.googleapis
Zoom Video ...	google-analy...	2	Yes	Unique	0	www-google-analytics.l.google.com,ssl.google-analytics.com,ssl-google-analytics.
			Yes	Unique		

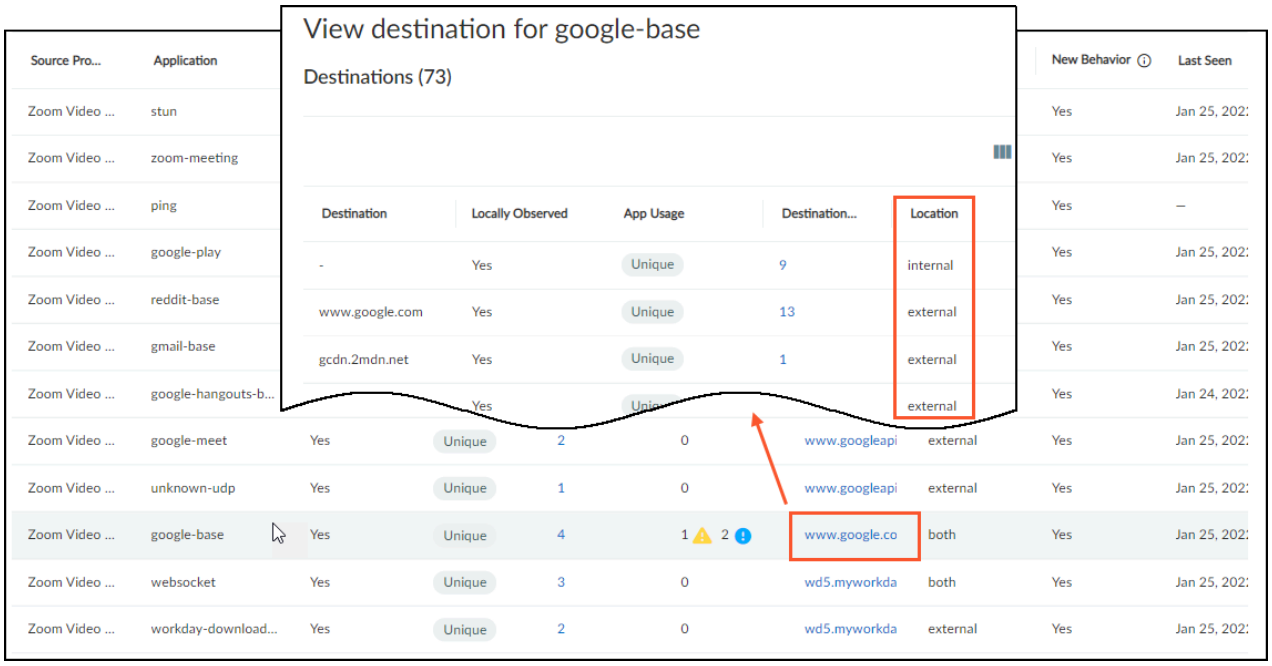
application_name 的“查看目标”面板提供了自己的表，其中每行代表源设备配置文件中的设备向其发送特定应用程序的每个单独目标。将光标悬停在目标 IP 列中的数字上，即可看到包含 IP 地址列表的弹出窗口。



如果您正在寻找特定的目标 IP 地址，并且地址列表太长以至于“目标 IP”弹出窗口无法全部显示，请单击“目标 IP”列中的数字，然后会出现一个带有搜索选项的对话框。



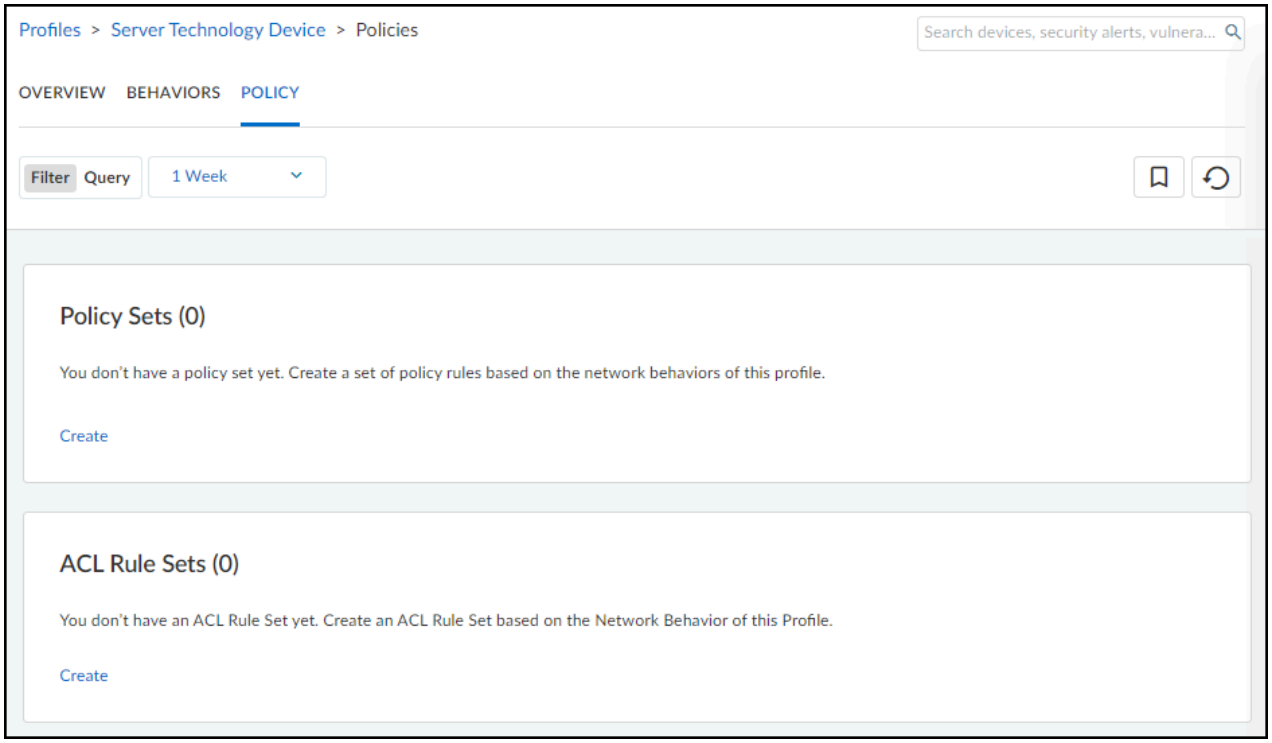
在行为表中，位置列表示行为的目标在哪里。如果所有目标都在本地网络中，则该位置为内部。如果所有目标都在本地网络之外，则该目标为外部。如果一些目标是内部的，一些是外部的，则该位置就是两者兼有。在这种情况下，您可以通过单击“行为”表中的“目标”列并查看“查看 *application_name* 的目标”面板中的“位置”列来查看各个目标的位置。



设备配置文件策略

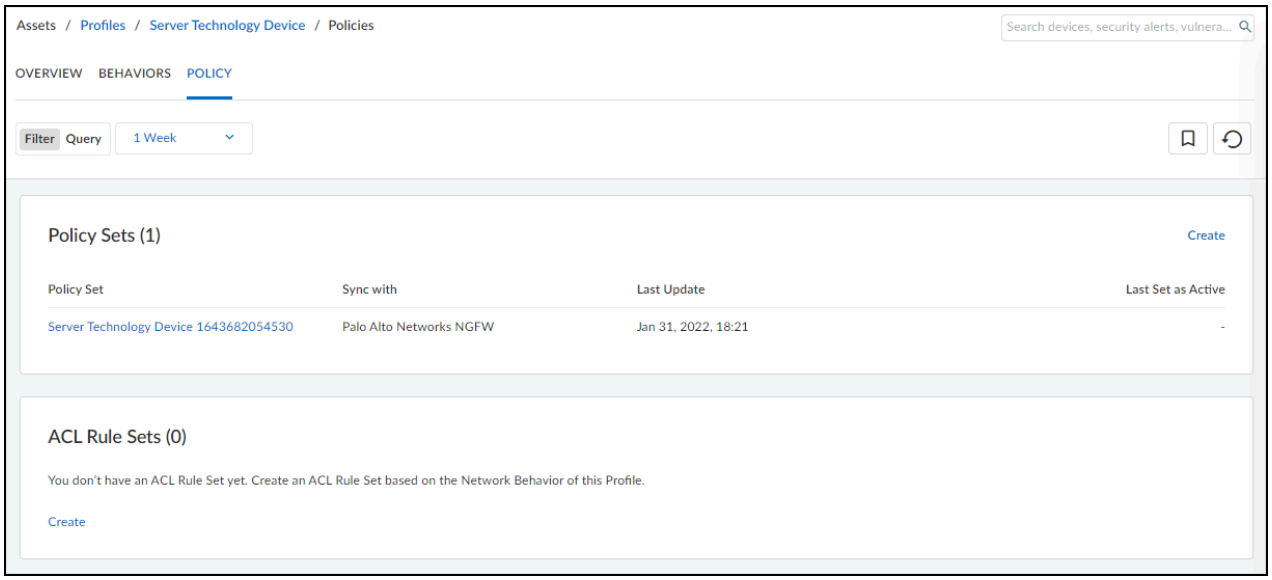
从 *PAN-OS 11.1* 开始，向新一代防火墙推荐安全策略规则采用与此处介绍的不同的过程。以下工作流程仍然适用于运行 *PAN-OS 11.1* 之前的 *PAN-OS* 版本的防火墙。

要访问设备配置文件的策略页面，请选择 **Profiles**（配置文件）> *profile_name* > **Policy**（策略）。

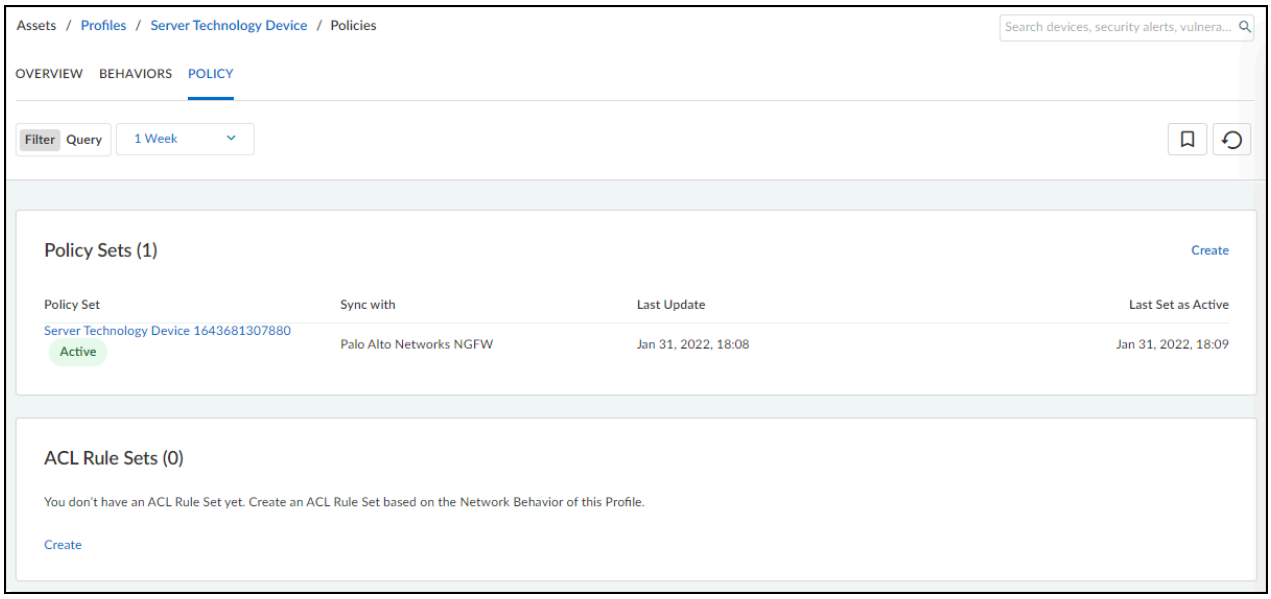


此页面列出为设备配置文件创建的所有策略集，它们上次更新的时间，是否已激活，以及如果已激活，是在何时激活的。当设备配置文件没有策略集时，策略页面为空。

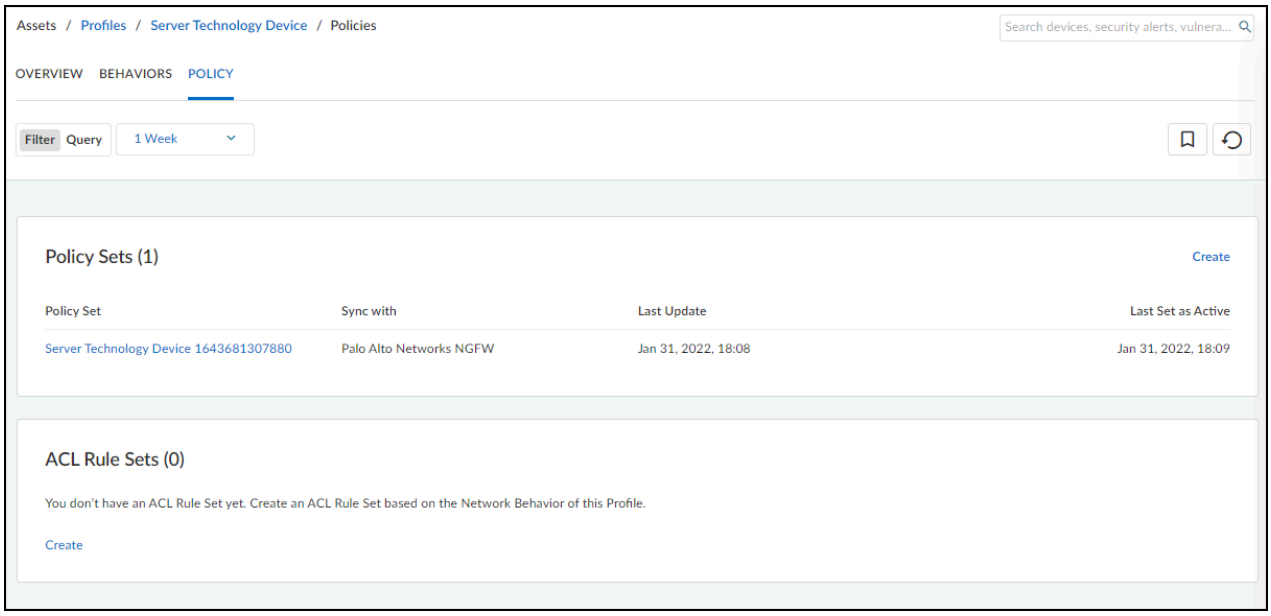
如果您为设备配置文件创建策略集并保存，但不将其激活，则会将其添加到策略页面。在这种情况下，“上次设置为活动”列中有一个短横线。



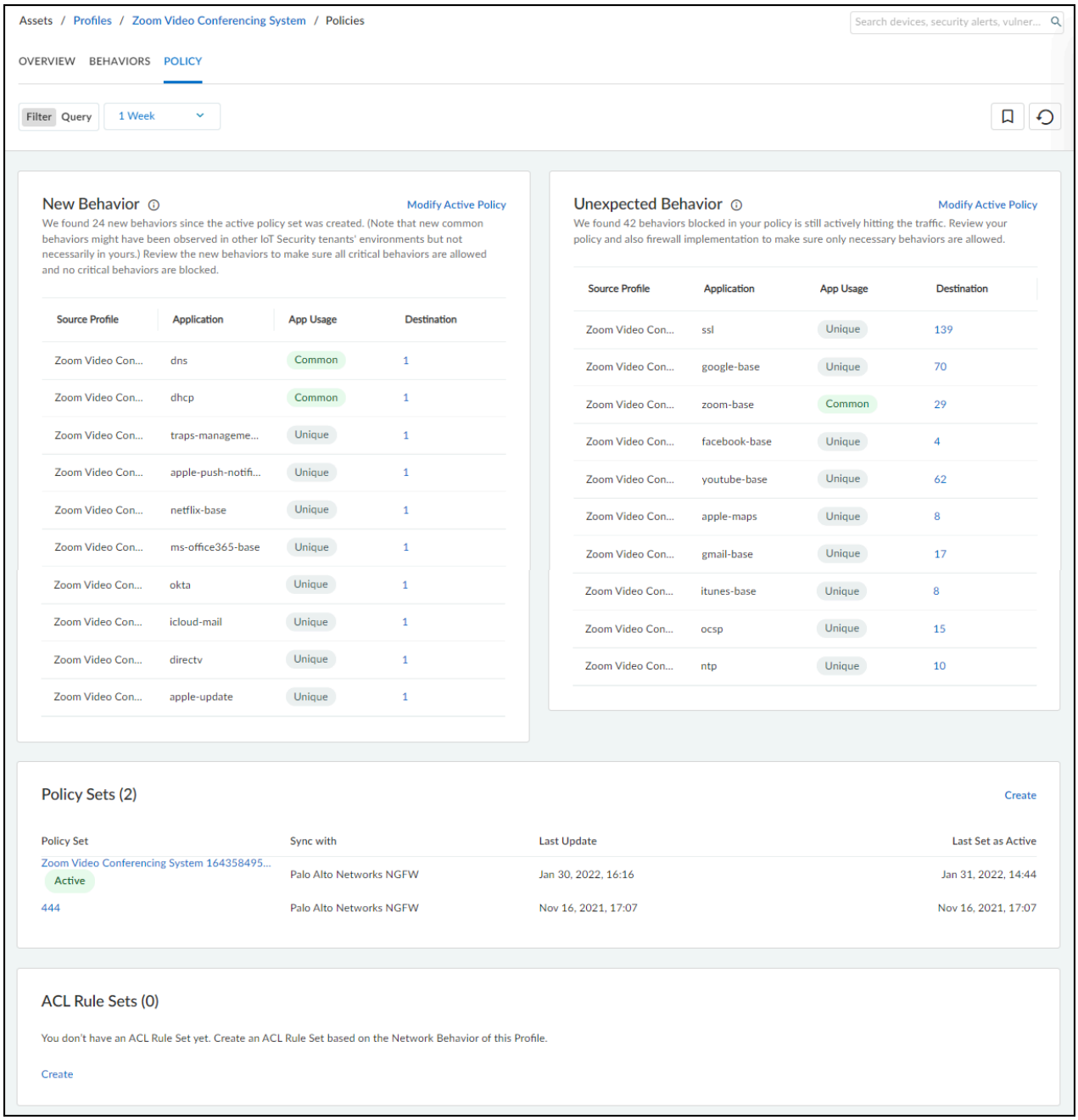
激活策略集后，会将其标记为“活动”标签，并且 IoT Security 在“上次设置为活动”列中添加时间戳。



如果您稍后停用该策略集，则会删除“活动”标签。但仍会保留“上次设置为活动”列中的时间戳，指示它曾经处于活动状态以及何时处于活动状态。



新行为是在活动策略集激活，或者上次更新后在网络上发现的行为。意外行为是在策略集激活，或者上次更新时明确不允许，但后来出现在网络上的行为，这意味着新一代防火墙中实施的强制措施缺少这些行为。在策略集首次激活后，如果经过一段时间，IoT Security 检测到网络上的新行为或意外行为，它会将它们列在 **Assets**（资产） > **Profiles**（配置文件） > *profile_name* > **Policy**（策略）页面上，并为您提供修改活动策略集以解释这些行为的机会。



将 IoT Security 与 Cisco ISE 集成时，您可以向 IoT 设备发送 ISE 自动生成的 ACL 规则集。有关为 ISE 提供 IoT 设备访问控制列表的信息，请参阅通过 Cisco ISE 应用访问控制列表。

在 IoT Security 中创建策略集

IoT Security 提供自动生成的策略规则建议来控制 IoT 设备流量。这些建议基于您本地网络环境中同一设备配置文件的所有高置信度 IoT 设备的网络行为，以及其他 IoT Security 租户环境中同一配置文件的设备网络行为。

高置信度设备是指 *IoT Security* 对其身份非常有信心，并计算出置信度得分为 *90-100%* 的设备。根据计算出的置信度分数，*IoT Security* 有三个置信度级别：高 *(90-100%)*、中 *(70-89%)* 和低 *(0-69%)*。

IoT Security 在配置文件中收集 IoT 设备的全部行为达到足够的时间后，您可以为其创建一组策略规则建议。

从 *PAN-OS 11.1* 开始，向新一代防火墙推荐安全策略规则采用与此处介绍的不同的过程。以下工作流程仍然适用于运行 *PAN-OS 11.1* 之前的 *PAN-OS* 版本的防火墙。

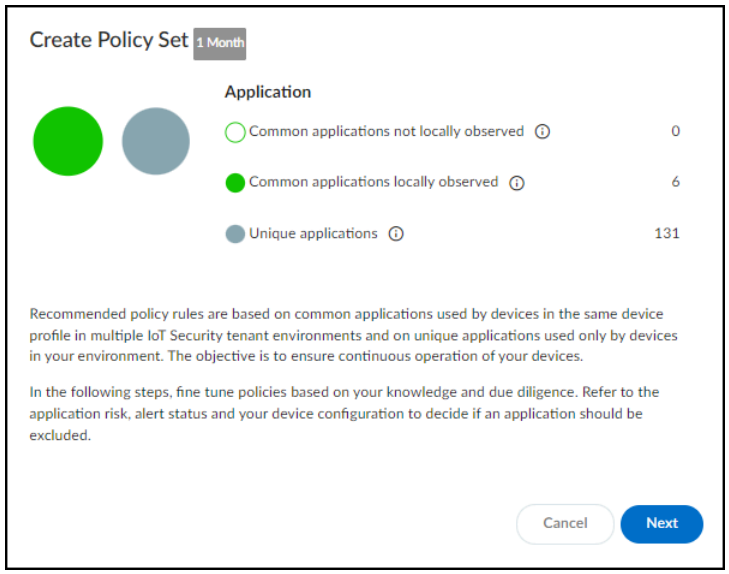
STEP 1 | 登录 IoT Security 门户并选择 **Assets**（资产） > **Profiles**（配置文件） > *profile_name* > **Behaviors**（行为）。

STEP 2 | 查看“行为”页面上的数据，选择 **Outbound Behaviors**（出站行为），然后单击 **Create Policy**（创建策略）。

有关设备配置文件的行为页面内容的描述，请参阅设备配置文件行为。

您还可以导航至“配置文件”页面，将光标悬停在配置文件名称上，然后单击出现的信息弹出窗口中的 ***Create Policy Set***（创建策略集）来创建策略集。

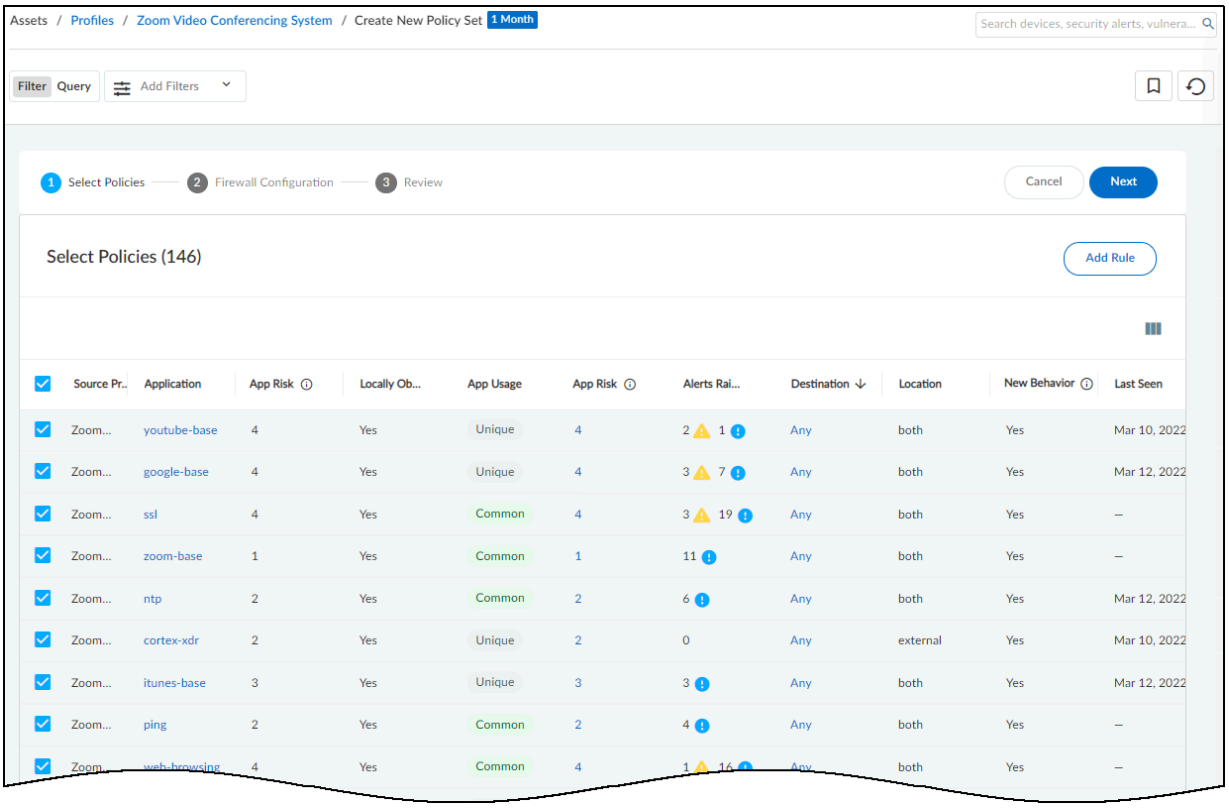
STEP 3 | 阅读有关 IoT Security 可以推荐给新一代防火墙的创建安全策略规则集的介绍，然后单击 **Next**（下一步）。



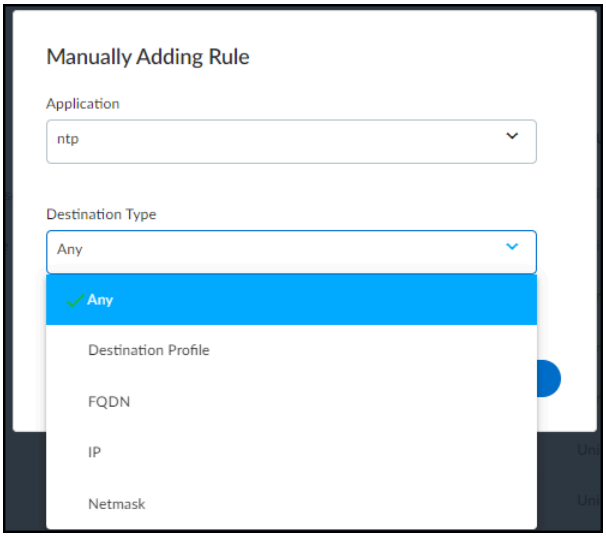
STEP 4 | 选择要包含在策略集中的推荐策略规则。

IoT Security 自动生成策略规则建议列表。这些基于多个 IoT Security 租户环境下同一设备配置文件中的设备使用的共同应用程序，以及基于仅您的环境中的设备上个月使用过的独特应用程

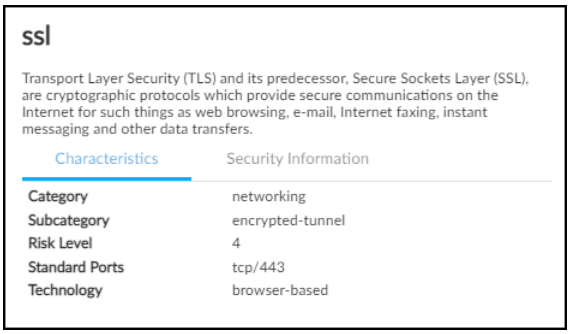
序（注意页面顶部的痕迹导航右侧的 **1** 个月 标签）。规则建议按应用程序组织，默认选择所有规则。根据您组织的策略和实践以及所提供的信息，清除任何您不想使用的内容。



除了 IoT Security 根据观察到的同一配置文件中设备的网络行为生成的自动策略规则外，您可以手动将其他规则添加到集合中。在策略集创建工作流中，单击 **Add Rule**（添加规则），然后设置应用程序和目标。默认情况下，**Any**（任何）都会出现在“应用程序”和“目标类型”字段中。要更改应用程序，请删除 **Any**（任何）并开始键入要为其创建规则的应用程序，直到自动补全功能提供足够的字母来选择它。要设置目标，请先选择目标类型：目标配置文件（用于内部目标）、FQDN、IP 或网络掩码。然后从列表中选择一个或多个目标配置文件，或者输入一个或多个 FQDN、IPv4、IPv6 地址或网络掩码。完成后，**Create**（创建）规则。



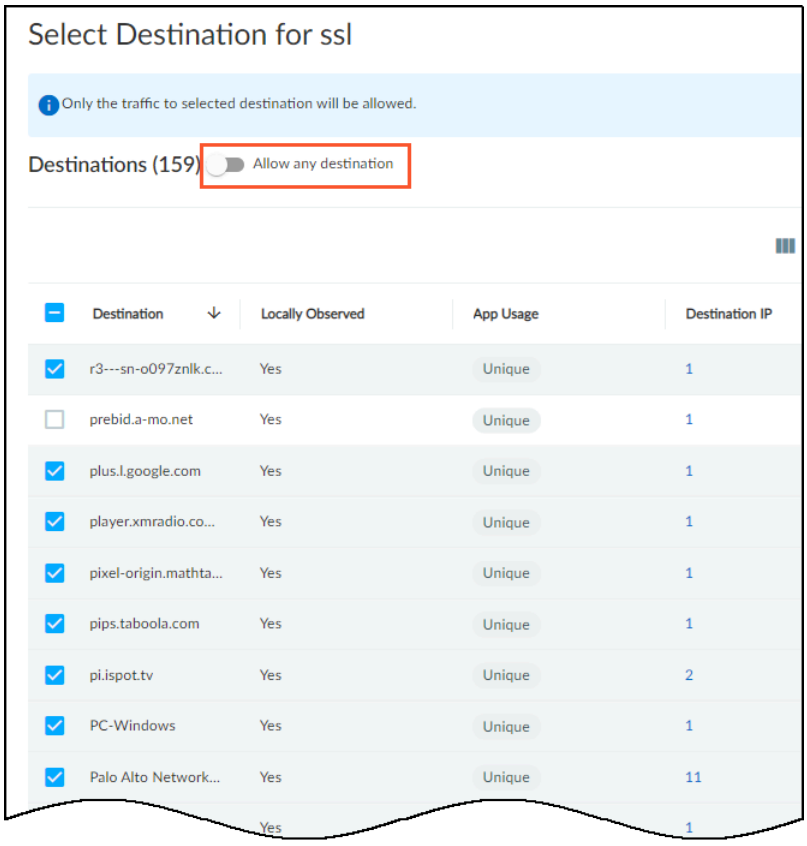
应用程序风险列包含 Applipedia 中定义的此应用程序的风险级别。风险等级分为 1 至 5 级，数字越接近 5，风险就越大。将光标悬停在应用程序名称上将显示一个弹出面板，其中包含从 Applipedia 检索的有关该应用程序的信息。有关此信息的解释，请参阅IoT 设备应用发现。



“已引发警报”列提供了源配置文件中的设备上发生的涉及每个应用程序的警报实例数。在决定是否将推荐的行为纳入一组策略规则时，此信息很有用。例如，如果您注意到某种行为与大量警报相关，则您可能会延迟添加允许此行为的规则，直到您调查出警报的严重性。如果它们都是低严重性警报，您可能会认为它们是可以接受的。另一方面，如果它们是高严重性警报或关键严重性警报，您可能会决定先解决它们，然后再继续。

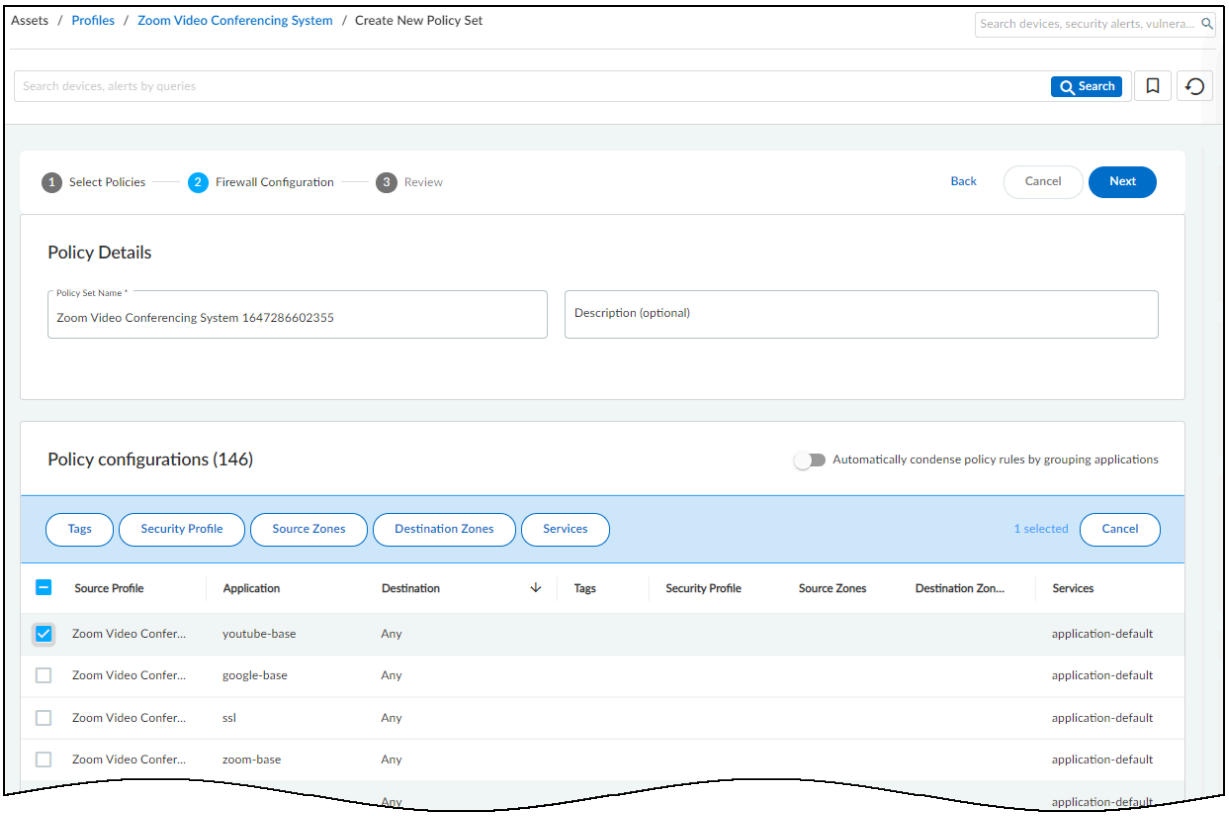
默认情况下，IoT Security 建议允许源配置文件中的 IoT 设备使用在观察到的网络流量中检测到的所有目标的应用程序。这由目标列中的任意 (Any) 表示。如果您不想允许某些目标，请单击

Any（任何），关闭 **Allow any destination**（允许任何目标），从列表中清除这些目标，然后关闭“选择目标”面板。

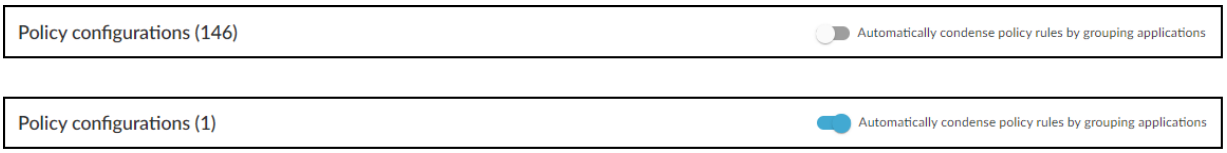


STEP 5 | 使用自动生成的策略规则配置或根据需要进行修改。

使用默认策略集名称或输入您自己的策略集名称。可选择添加描述以供将来参考。



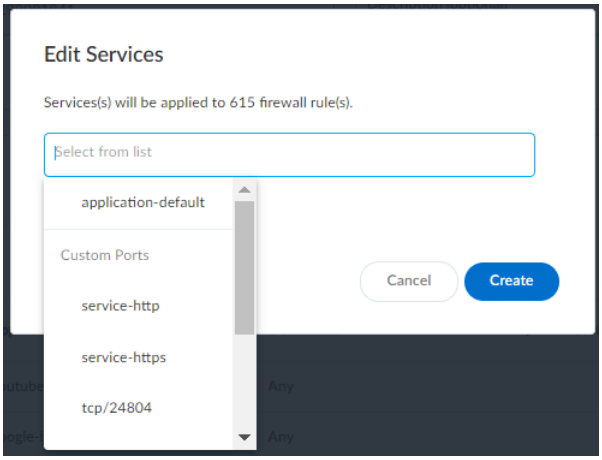
如果您想减少 IoT Security 生成的策略规则的数量，请启用 **Automatically condense policy rules by grouping applications**（通过分组应用程序自动压缩策略规则）。当多条规则具有不同的应用，但其他所有内容均相同（相同的目标或目标集，以及如果已配置，还具有相同的标签、安全配置文件、源和目标区域和服务）时，IoT Security 会将其全部收集到一条规则中，并将之前作为规则中唯一区分元素的所有应用程序放入一个应用程序列表中。例如，如果未启用此选项（其默认状态），并且有十个不同的应用程序位于同一个目标位置，IoT Security 会创建十条规则。但是，如果您启用此选项，则 IoT Security 只会创建一条包含十个应用程序的规则。



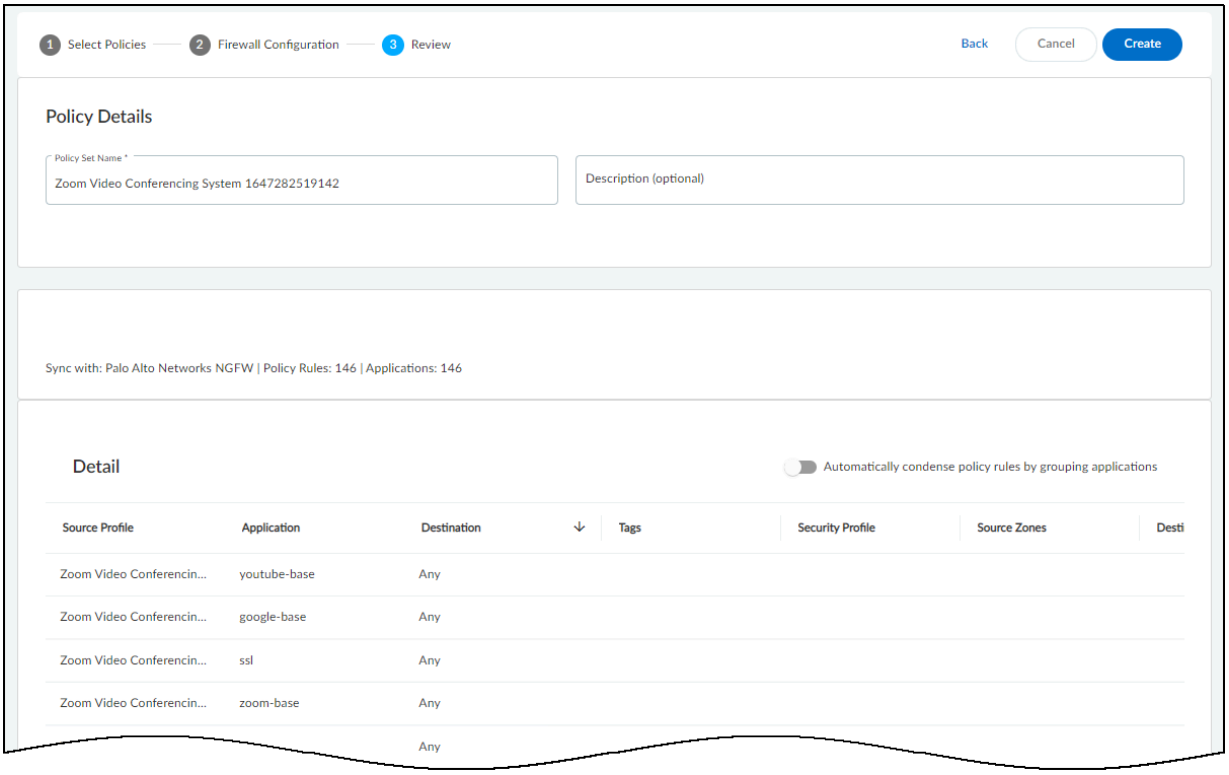
IoT Security 会始终将目标组合在一起以减少推荐的策略规则的数量。与应用程序组选项不同，它不需要您启用。

可选择应用标签、安全配置文件、源区域和目标区域以及服务，以便当 Panorama 或防火墙管理员导入时，它们可以成为策略规则的一部分。这使管理员无需编辑导入的规则即可稍后应用。选择您想要将其应用到的规则，然后单击页面顶部的 **Tags**（标记）、**Security Profile**（安全配置文件）、**Source Zones**（安全区域）、**Destination Zones**（目标区域）或 **Services**（服务），以便查看您的选择。创建或选择之前定义的选项，然后单击 **Apply**（应用）或 **Create**（创建）。您可以将一个或多个标签、源区域、目标区域和服务应用于同一个应用程序。

默认情况下，应用程序使用其标准端口并在服务列中显示 application-default。编辑服务时，“编辑服务”对话框会显示 IoT Security 观察到应用程序使用的任何非标准端口，以及 service-http 和 service-https 这两个选项。选择规则中要使用的服务，然后单击 **Create**（创建）。



STEP 6 | 仔细检查规则集，如果觉得满意，则 **Create**（创建）推荐的策略规则集。

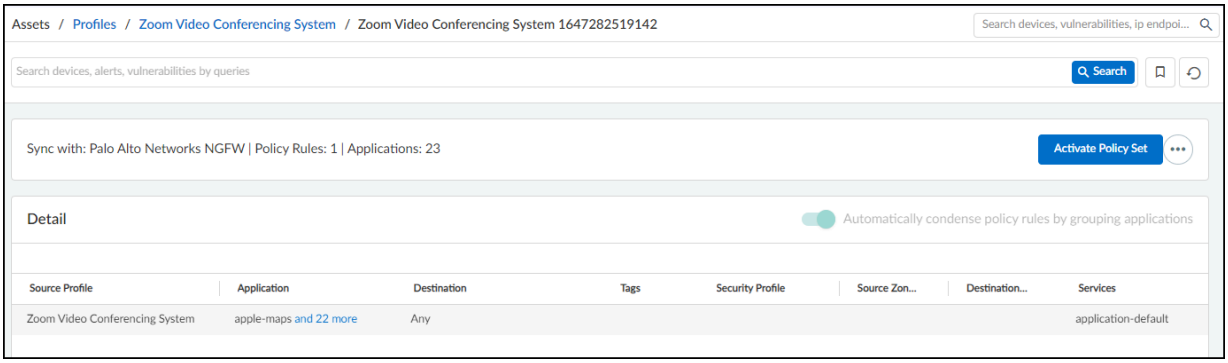


在检查策略集时，请注意 IoT Security 会显示许多允许的应用程序的默认服务端口。这些是所选应用程序过去一个月内在网络上使用的服务端口。如果超过一个月没有观察到应用程序，它的服务端口将不再出现在列表中。

IoT Security 通过观察网络流量来了解应用程序的服务端口。确保有足够的时间来收集所需的会话数据，请记住，IoT Security 不常使用的应用程序需要更多时间。

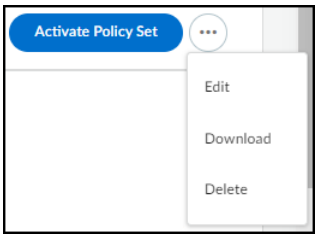
单击“创建”后，IoT Security 会创建并保存策略集。您可以在策略页面上查看为设备配置文件创建的所有策略集，IoT Security 还会提示您激活策略集，为了让 Panorama 和各个防火墙可以导入，这是必要的。

STEP 7 | 要激活策略集以使其可供 Panorama 和各个防火墙导入，请单击 **Activate Policy Set**（激活策略集）。



一个设备配置文件一次只能有一个活动策略集。

如果在激活策略集之前看到任何想要更改的内容，请单击 **More Actions**（更多操作）图标 (⋯)，然后单击 **Edit**（编辑）。IoT Security 会返回第一页（选择策略），以便您进行更改。



从相同的更多操作菜单中，您可以将策略集下载为电子表格，并将其删除。

要保存策略集而不将其激活，请导航至 IoT Security 门户。

将策略集导入 Panorama

目前，*multi-vsys* 防火墙不支持策略规则建议。您必须手动创建。

STEP 1 | 登录 Panorama 管理服务器并导航至 **Panorama** > **Policy Recommendation**（策略建议） > **IoT**。

这样，Panorama 就可以从 IoT Security 云中获取最新的活动建议。如果您在激活 IoT Security 中的策略集时已打开“策略建议”页面，或者修改或停用现有的活动策略集，则必须刷新页面才能看到更改。Panorama 或防火墙都不会缓存任何策略建议。

STEP 2 | 单击 **Import**（导入）并将策略规则建议导入到前规则库或后规则库，然后选择要放在导入规则后的规则。

前规则写在 *Panorama* 中，这些规则在防火墙本地定义的规则之前添加。后规则写在 *Panorama* 中，这些规则在防火墙上定义规则后添加。

如果您不选择规则，Panorama 会将导入的策略建议置于规则库的顶部。

为了确保针对与推荐规则相同的设备的任何其他安全策略规则不会遮挡它们，请将推荐规则放在规则库中其他规则之前。

STEP 3 | 单击 **OK**（确定）。

导入操作会自动创建策略规则所需的支持对象（设备对象、服务对象、地址对象），然后创建策略规则。

您可以手动将日志转发配置文件应用于每个策略规则，或者在导入规则建议之前创建一个日志转发配置文件，并将其命名为“默认”以自动应用。请参阅为 IoT Security 准备好您的防火墙和配置日志转发策略中有关日志转发配置文件的部分。

STEP 4 | 提交配置更改。

有关将策略集导入到 *Panorama*（并直接导入防火墙），请参阅配置 Device-ID。

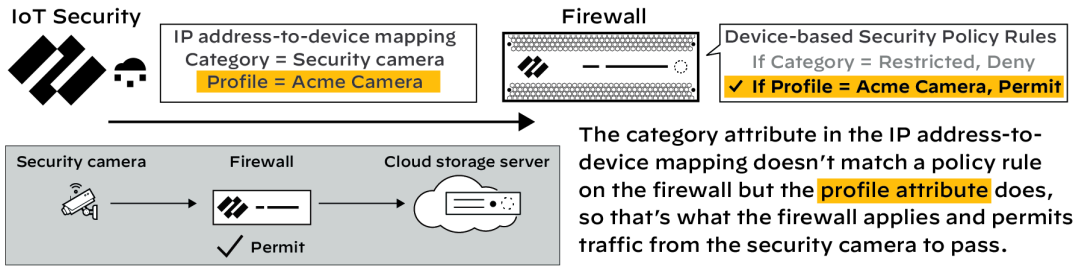
限制网络访问权限

虽然策略建议强制实施 IoT 设备的可信行为，但仅在设备行为发生变化时才生效。但是，如果 IoT Security 检测到设备上的风险升高，可能是由运行过时操作系统的关键业务设备引起的，并且您希望在发起利用漏洞之前采取预防措施，则需要采用不同于基于行为的策略规则的方法。

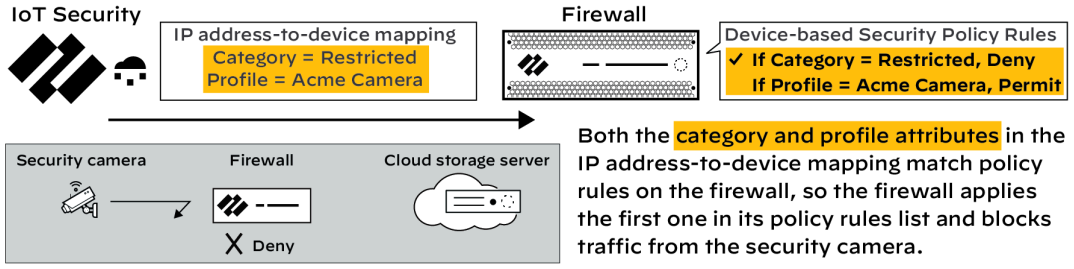
IoT Security 提供了另一个选项，可让您限制对存在相同问题的特定 IoT 设备或 IoT 设备组的网络访问，例如容易受到或怀疑受到危害的设备。

为此，首先创建一个安全策略规则，其中“源设备”是类别为“受限”的任何设备，规则中的操作为“拒绝”。将此规则置于规则列表中所有其他基于设备的规则之上。否则，基于配置文件属性或其他属性的规则可能会将其遮挡。同样，确保“受限”规则高于任何可能遮挡的规则，即使是那些不使用 Device-ID 的规则。

然后在 IoT Security 门户中启用网络流量限制功能，但暂时不要使用此功能限制访问。请注意，防火墙不会应用新规则，因为没有一个 IP 地址到设备的映射具有与“受限”匹配的类别属性。



当您限制一个或多个设备的网络访问时，IoT Security 会立即将其类别属性从真实设备类别更改为“受限”，并向防火墙发送新的 IP 地址到设备的映射。当流量从具有“受限”类别属性的设备到达防火墙时，它会应用您创建的安全规则，拒绝其访问网络。



虽然附图显示了防火墙如何强制执行“*category=Restricted*”规则，而不是其他基于设备的安全策略规则，但其他规则不必基于设备。即使防火墙基于源 *IP* 地址、服务、应用或任何其他因素或因素组合允许访问，您也可以限制 *IoT* 设备的网络访问。

稍后，在安全问题解决后，您解除对设备的限制，这会将设备的 IP 地址到设备的映射返回到其以前的类别。因此，它们的类别属性不再符合“受限”规则，设备将被允许访问其他规则所确定的网络。

注意：

- 要支持 Device-ID 和 IP 地址到设备的映射，防火墙必须运行 PAN-OS 10.0 或更高版本。要支持流量限制功能，防火墙必须具有设备字典文件 16-253 或更高版本。PAN-OS 软件版本和设备字典版本都出现在 PAN-OS Web 界面指示板的“常规信息”部分。
- 流量限制仅适用于身份置信度得分为 90 或以上的设备。

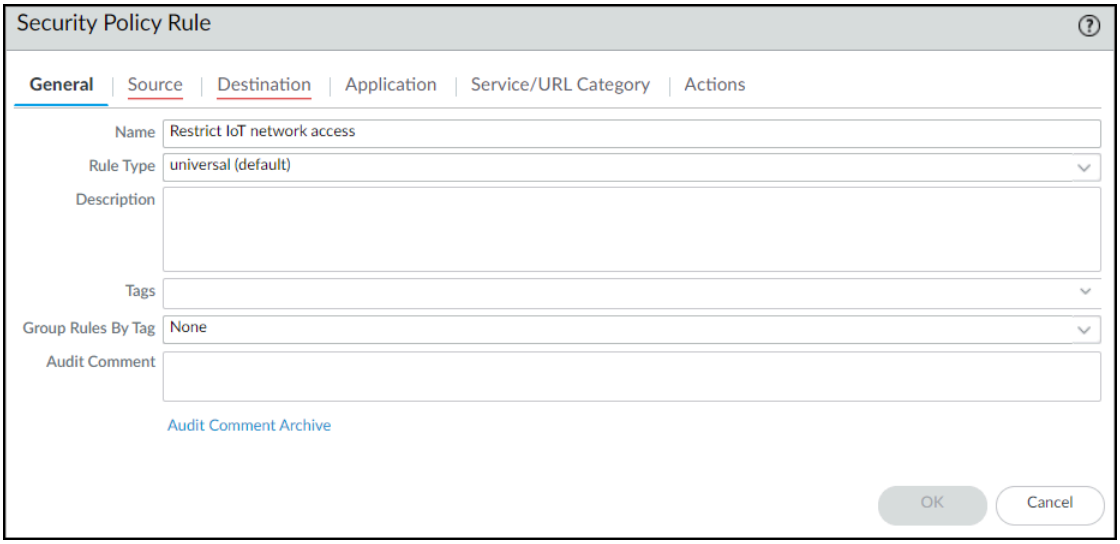
  

  置信度分数表示 *IoT Security* 在其设备标识中的置信度水平。根据计算出的置信度分数，*IoT Security* 有三个置信度级别：高 *(90-100%)*、中 *(70-89%)* 和低 *(0-69%)*。
- 此功能可限制网络访问，但不能完全隔离设备。根据网络设计，受限设备仍然可以访问其可以到达的网络部分，而无需穿越防火墙。
- 只有拥有所有者权限的 IoT Security 用户才能启用和禁用该功能。

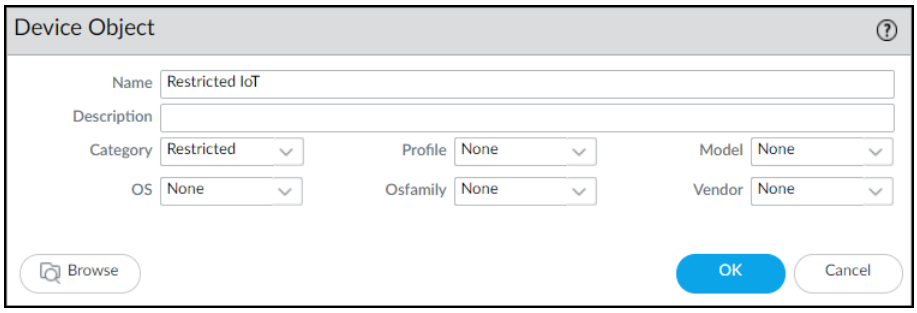
STEP 1 | 配置安全策略规则，拒绝来自任何设备的流量，该设备的类别 Device-ID 属性为“受限”。

这些说明解释了如何在 *PAN-OS Web UI* 中配置安全策略规则。您还可以通过 *Panorama* 进行配置。

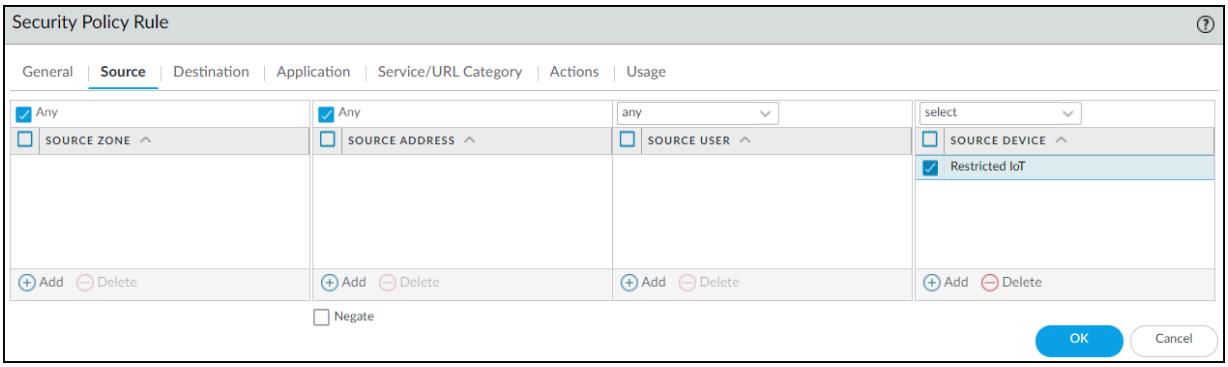
登录防火墙上的 Web UI，单击**Policies**（策略） > **Security**（安全），然后单击 **Add**（添加）以创建新的安全策略规则。在常规选项卡上，输入规则的名称，如 **`Restrict IoT network access`**。



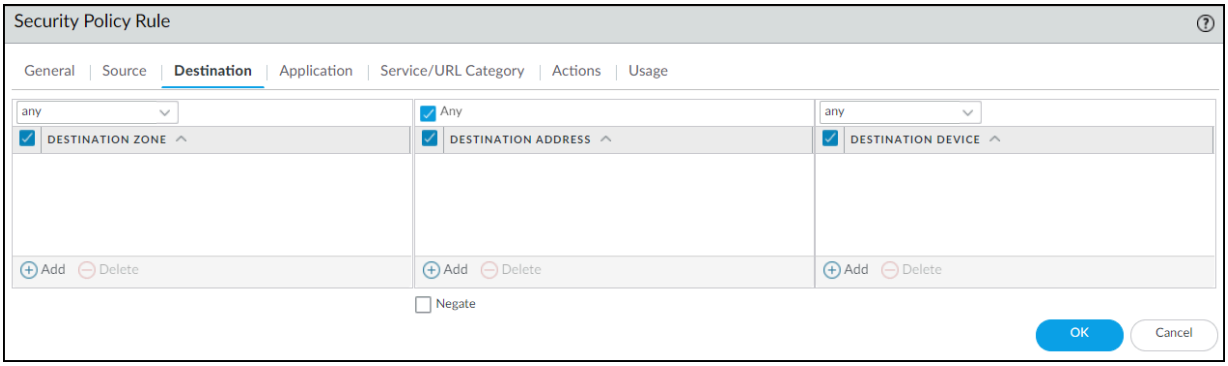
在源选项卡上，单击源设备部分中的 **Add**（添加），然后单击 **Device**（设备）。在出现的“设备对象”对话框中，输入名称，为类别选择 **Restricted**（限制），然后单击 **OK**（确定）。



选择您刚才创建的设备对象作为源设备，并为源区域和地址选择 **Any**（任意）。

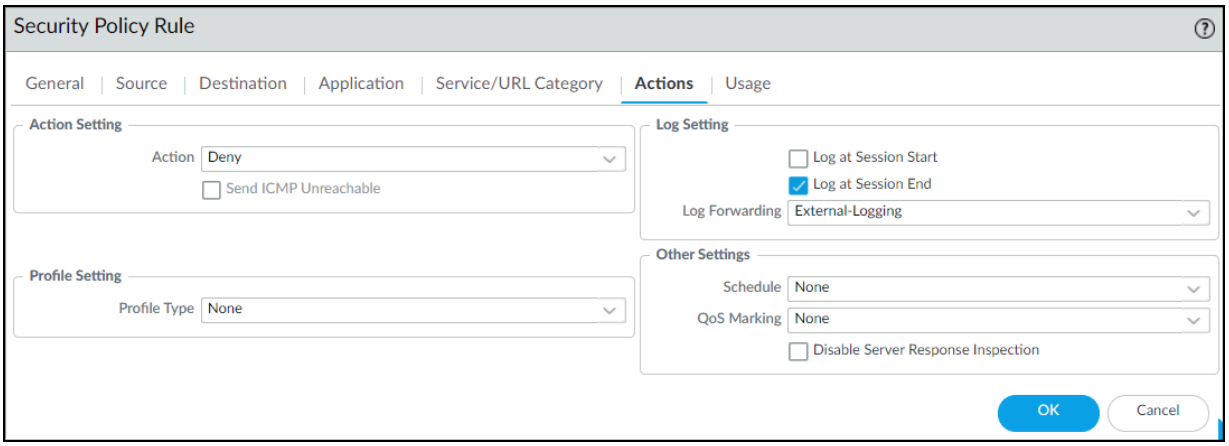


在“目标”选项卡上，为目标区域、地址和设备选择 **Any**（任意）。

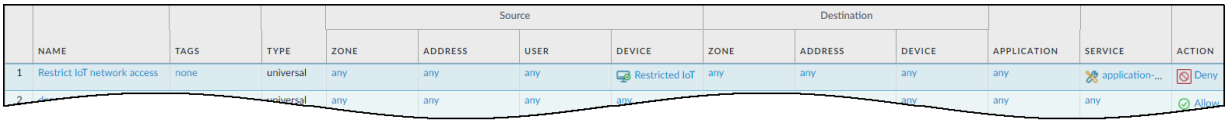


在“操作”选项卡上，选择 **Deny**（拒绝）作为操作。如果防火墙将日志转发到 Strata Logging Service、Panorama 或其他外部日志记录服务器，请选择日志转发配置文件。即使对于拒绝

流量的规则，日志也能提供受限设备尝试连接内容的可见性，在补救期间非常有用。单击 **OK**（确定）以保存安全策略规则配置。



将规则移到其他策略规则之上。

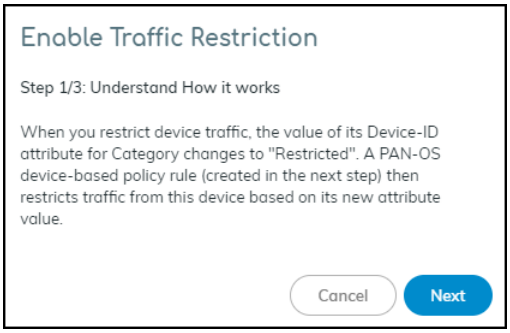


STEP 2 | 在 IoT Security 门户中启用流量限制。

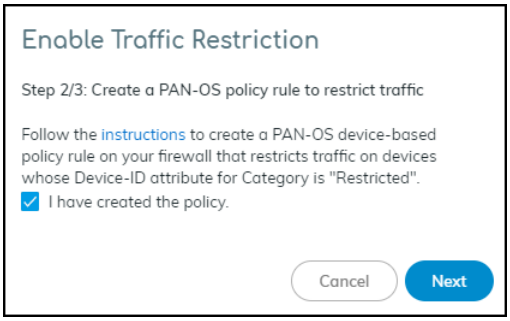
使用所有者权限登录 IoT Security 门户，单击 **Policy Sets**（策略集） > **Settings**（设置），然后切换 **Restrict device traffic via firewall policy**（通过防火墙策略限制设备流量）。

以下用户角色*IoT Security*具有所有者权限：帐户管理员、应用管理员、实例管理员和所有者。

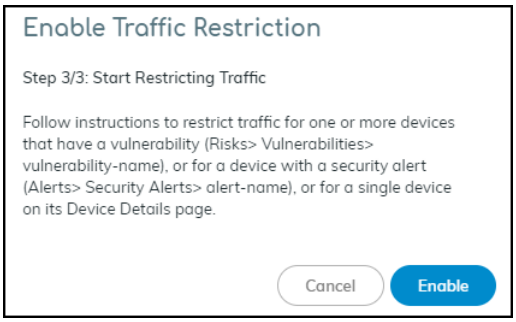
此时会出现一个弹出面板。阅读流量限制的工作原理，然后单击 **Next**（下一步）。



选择 **I have created the policy**（我已创建策略），然后单击 **Next**（下一步）。



阅读 IoT Security 门户中限制流量的位置，然后单击 **Enable**（启用）。



STEP 3 | 限制 IoT 设备。

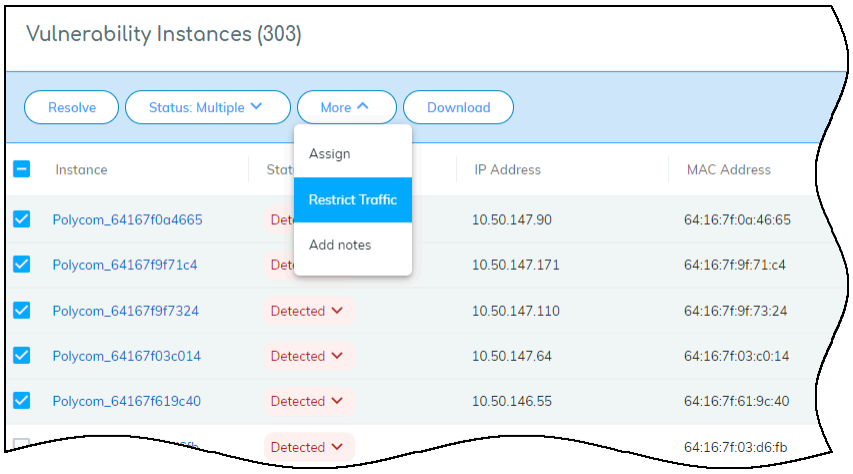
如启用流量限制面板的步骤 3/3 中所述，在 IoT Security 门户中有三个位置可以限制网络流量：漏洞详细信息页、安全警报详细信息页和设备详细信息页面上的漏洞实例。每个地方或限制点说明如下。

虽然只有所有者可以启用和禁用限制网络流量的功能，但所有者或管理员都可以使用该功能对设备施加限制或解除设备限制。有关用户角色的更多信息，请参阅创建 IoT Security 用户。

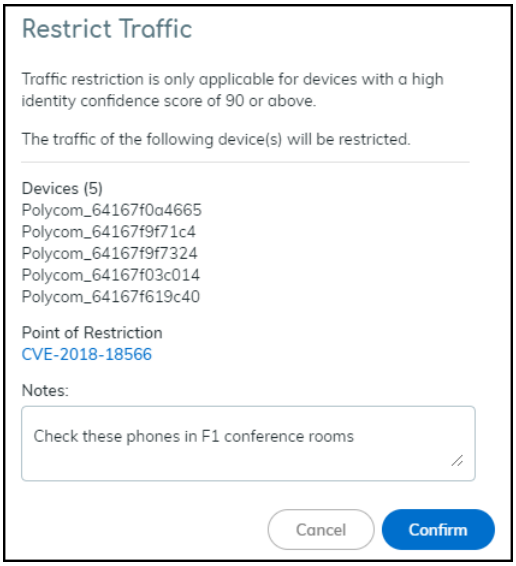
漏洞实例作为限制点

要在“漏洞详细信息”页面上限制一个或多个 IoT 设备，请单击 **Risks**（风险） > **Vulnerabilities**（漏洞），然后单击漏洞名称。

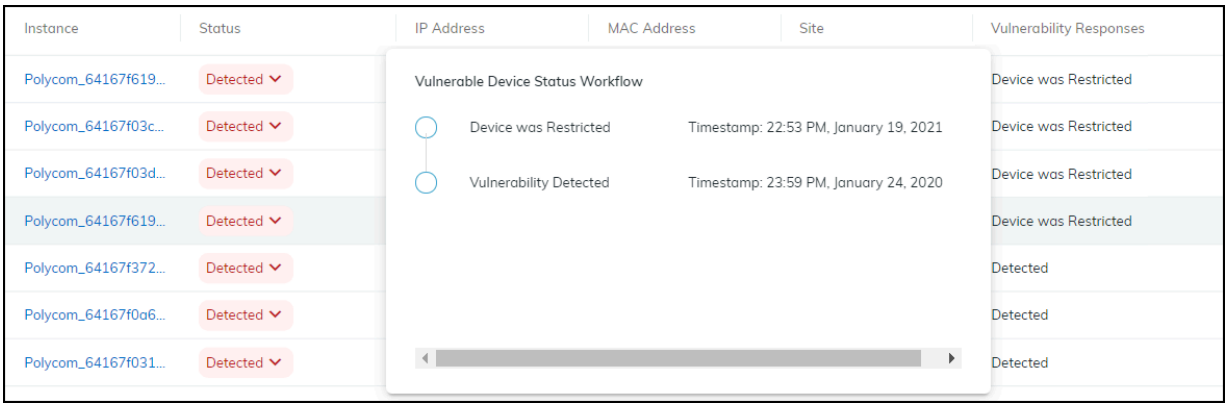
如果“置信水平”列被隐藏，请单击"列"图标 (▮▮▮) 并将其选中。选择置信度得分为 90 或以上的一个或多个漏洞实例，然后单击**More**（更多） > **Restrict Traffic**（限制流量）。



查看流量将受到限制的易受攻击或潜在易受攻击设备的列表，可选地添加备注以供将来参考，然后单击 **Confirm**（确认）。

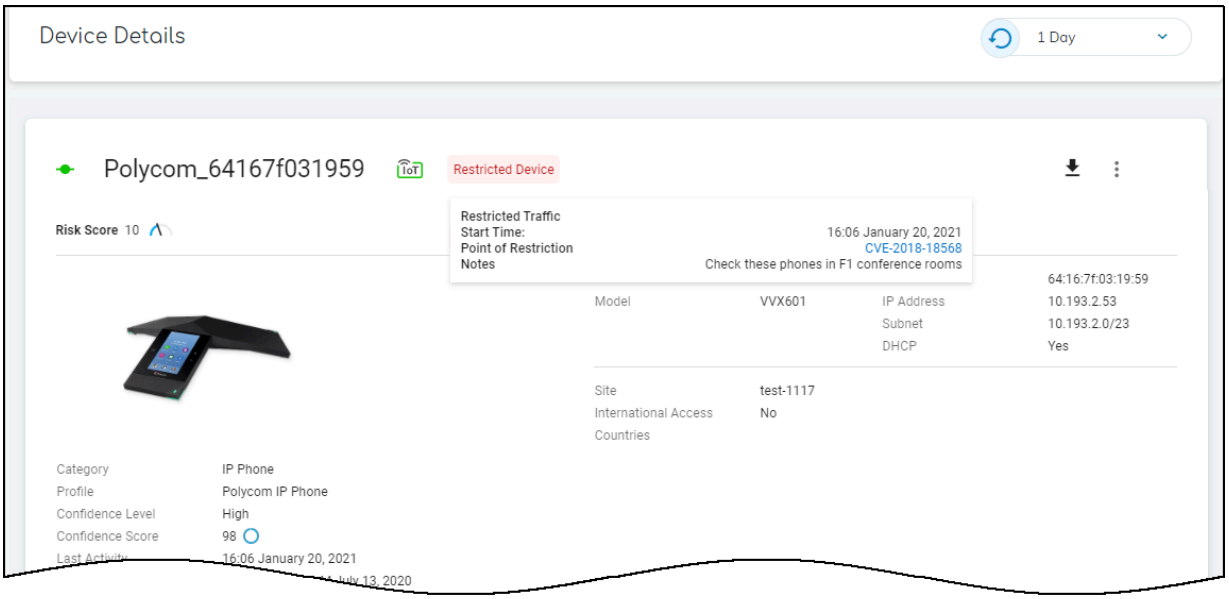


限制流量列中该设备的条目从 No更改为 Yes，表示其流量正在受到限制。如果您没有看到限制流量列，请单击列图标 (▮▮▮) 并选择**Restricted Traffic**（限制流量）。漏洞响应列中将显示一个新条目。将光标悬停在条目上可查看所执行操作的历史记录。



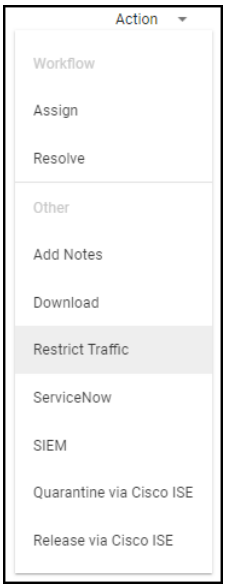
流量限制设备的“设备详细信息”页面会在设备名称旁边添加 *Restricted Traffic*（限制设备）标签。如果您将光标悬停在标签上，则会出现一个弹出窗口，其中包含限制的时间点以及指向漏

洞、安全警报或设备详细信息页面的链接。在这种情况下，它将是指向漏洞详细信息页面的链接。弹出窗口还包括您所做的任何笔记。

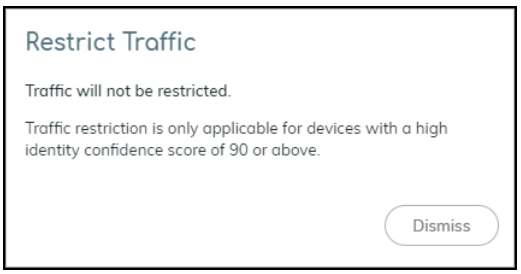


作为限制点的安全警报

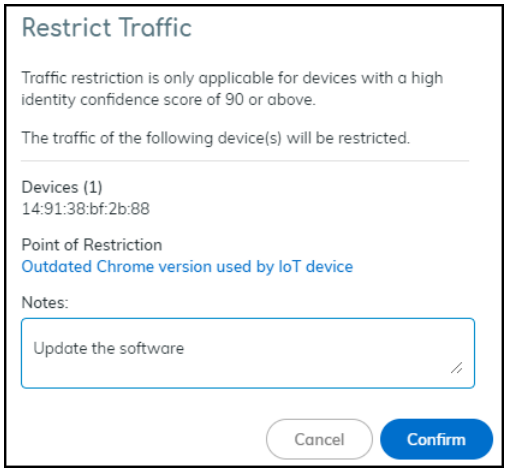
要使用特定的安全警报限制 IoT 设备，请单击 **Alerts**（警报） > **Security Alerts**（安全警报），然后单击警报名称。在警报详细信息页面上，单击 **Action**（操作） > **Restrict Traffic**（限制流量）。



如果受影响设备的置信度得分低于 90,则会显示以下消息。置信度得分显示在“警报详细信息”页面的“受影响设备”部分。

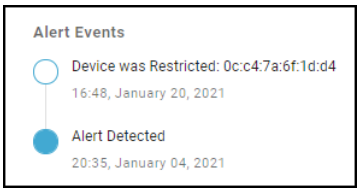


如果置信度得分为 90 或以上，则会显示“限制流量”对话框。



查看其流量将受到限制的设备，可选地添加备注以供将来参考，然后单击 **Confirm**（确认）。

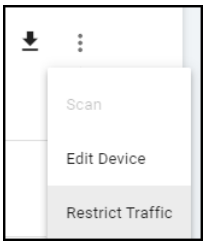
警报详细信息页面的顶部会出现一个新标签，说明 `Traffic Restricted Yes`，警报事件列中会出现一个新条目。



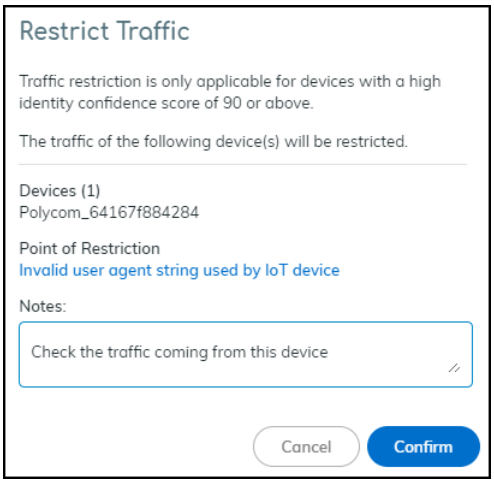
流量限制设备的“设备详细信息”页面会在设备名称旁边添加 *Restricted Traffic*（限制设备）标签。将光标悬停在标签上时，将出现一个弹出窗口，上面显示您开始限制流量的时间；指向限制点的链接，在本例中是指向安全警报详细信息页面；以及您所做的任何笔记。

IoT 设备详细信息作为限制点

要在“设备详细信息”页面上限制单个 IoT 设备，请单击 **Devices**（设备），然后单击清单表中某个设备的名称。在设备详细信息页面顶部的身份部分，单击 **Action**（操作）图标（三个垂直点） > **Restrict Traffic**（限制流量）。



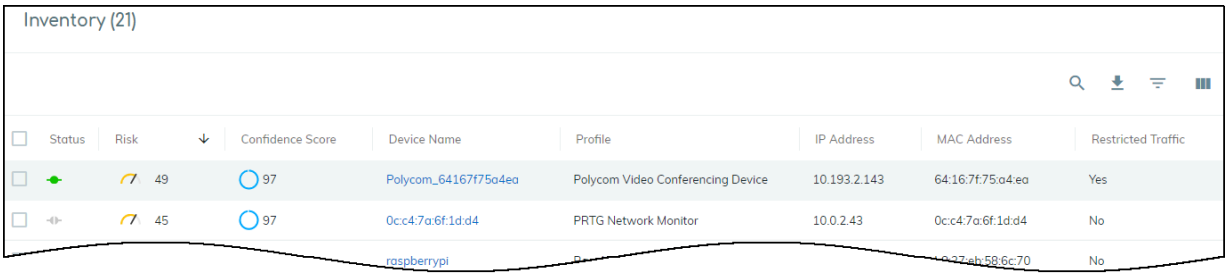
检查将限制其流量的设备是否正确，可选地添加备注以供将来参考，然后单击 **Confirm**（确认）。



IoT Security 门户会在设备详细信息页面的设备名称旁边添加一个 *Restricted Device*（受限设备）标签。当您将光标悬停在标签上时，将出现一个弹出式窗口，上面显示您开始限制流量的

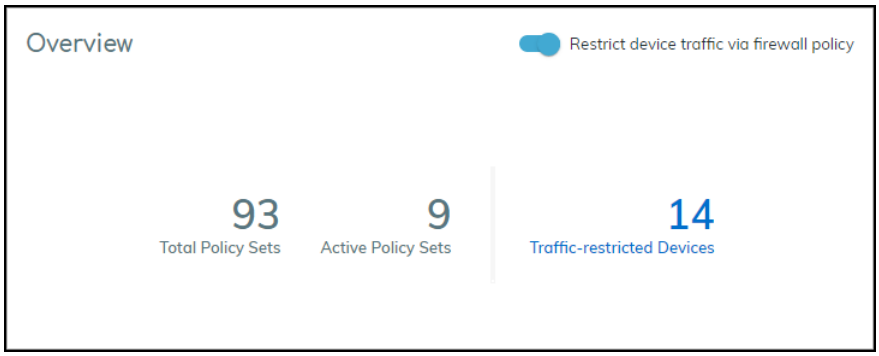
时间；指向限制点的链接，在本例中，该链接指向您已经在使用的同一设备详细信息页面；以及您所做的任何笔记。

在“设备”页面上，此设备在“限制流量”列中的条目从 **No** 更改为 **Yes**，表明其流量正在受到限制。如果您没有看到限制流量列，请单击列图标 (▮▮▮)，然后在流量部分选择 **Restricted Traffic**（限制流量）。

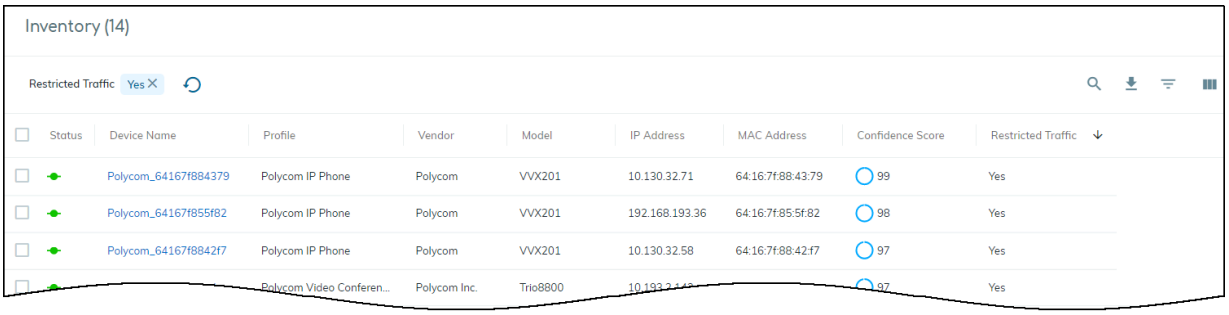


STEP 4 | 查看所有受限设备。

在“策略集”页面上，单击“概述”面板中显示的受限设备数量。



设备页面打开，应用了一个过滤器，仅显示清单表中受限的设备。



STEP 5 | 在调查和修正流量限制设备后，解除对其流量的限制。

要取消限制设备的流量，请重复与限制流量相同的过程，但单击 **Derestrict Traffic**（取消限制流量）。

您可以批量解除对多个漏洞实例的限制。在漏洞详细信息页面上选择一个或多个实例，然后单击 **More**（更多） > **Derestrict Traffic**（限制流量）。

对于其他流量限制设备，请在应用了限制流量过滤器的“设备”页面上查看清单。接着逐个单击设备名称，打开每个设备的设备详细信息页面，然后单击 **Action**（操作）图标（三个垂直点） > **Derestrict Traffic**（限制流量）。

要完全禁用该功能，请单击 ***Policy Sets***（策略集），关闭 ***Restrict device traffic via firewall policy***（通过防火墙策略限制设备流量），然后 ***Confirm***（确认）操作。此时，*IoT Security* 会取消所有现有的设备流量限制。它还将这些设备的漏洞响应列（风险 > 漏洞 > *vulnerability_name*）和最后操作列（警报 > 安全警报）中的条目更改为 *`Device was derestricted`*。

Medical IoT

IoT Security 提供了一种方法来监控其 支持的医疗 IoT 成像设备和输液系统类别的使用情况，以及供应商是否召回了您网络中的医疗设备。它还支持上传 MDS2 文件，用于发现漏洞并发出医疗 IoT 设备的安全警报。

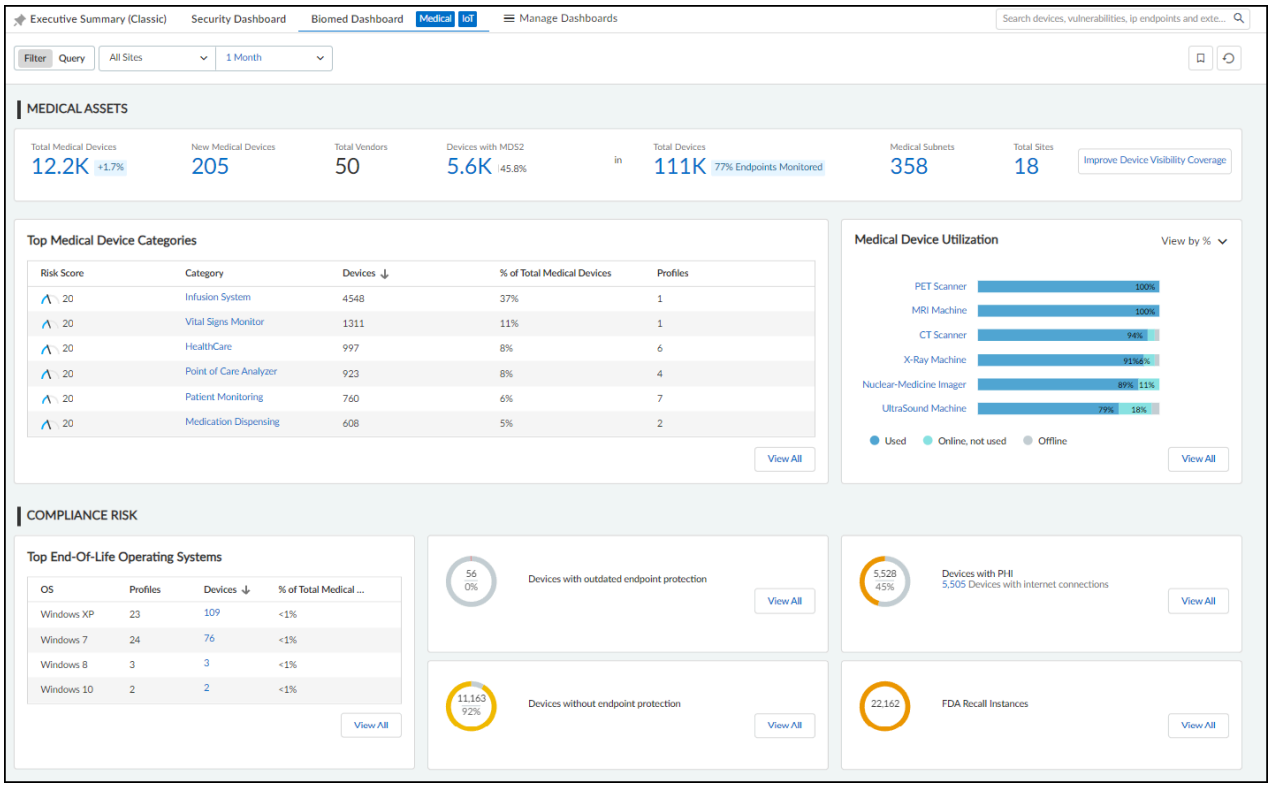
当 IoT Security 门户主题为医疗 IoT Security 时，才会显示利用率和生物医学指示板以及 MDS2 页面。它仅在您清单中的设备被召回时显示召回页面。

- 生物医学指示板
- 利用率指示板
- 利用率指示板过滤器
- 使用信息面板
- MDS2
- MDS2 社区
- 召回

生物医学指示板

IoT Security 收集有关正在监控的医疗 IoT 设备的统计信息，评估其风险，并在生物医疗指示板上显示发现结果。您可以利用这些数据来跟踪医疗设备的清单和利用率，以及评估和解决医疗 IoT 设备的风险。

要查看生物医学指示板，请确保 **Medical IoT Security** 是门户中已激活的垂直主题，选择 **Dashboard**（指示板），然后从 **Manage Dashboards**（管理指示板）下拉列表中选择 **Biomed**（生物医学）。



指示板分为三个主要部分。顶部是一组站点和时间范围过滤器。紧接着是“医疗资产”部分，该部分具有医疗设备信息的高级摘要和两个面板，显示顶级医疗设备类别和医疗设备利用率。指示板底部是“合规风险”部分，其中有几个面板显示可能存在风险的医疗设备类型。

医疗资产

在“医疗资产”部分的顶部是所有医疗 IoT 设备、新的医疗 IoT 设备、其供应商以及具有 MDS2 表单的医疗 IoT 设备的总数列表。为了提供这些数字的上下文，还提供了网络中所有设备、子网和站点的总数。

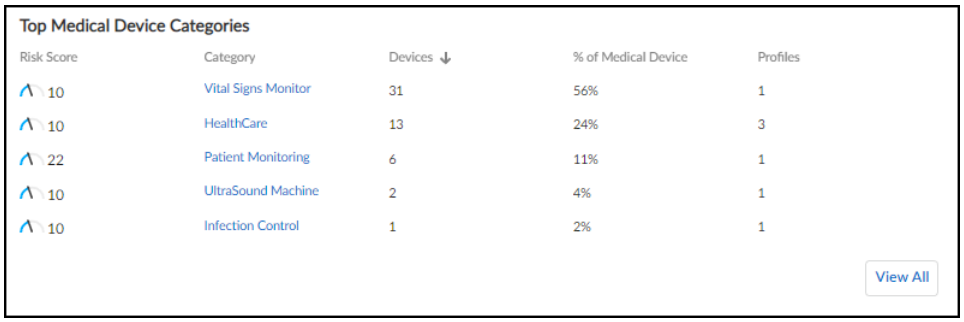
更详细地说，高级摘要包含以下设备统计信息：

- **Total Medical Devices**（医疗设备总数）：这是在生物医学指示板上设置的时间范围内，在网络、站点和时间范围内检测到流量的医疗 IoT 设备的总数。单击总数将打开 **Assets**（资产） > **Devices**（设备）页面，以显示在定义的站点和时间范围过滤器内检测到的所有医疗设备的条目。
- **New Medical Devices**（新医疗设备数量）：这是 IoT Security 在指定站点发现，并在指定时间范围内（而不是之前）发现的医疗设备的数量。单击总数将打开 **Assets**（资产） > **Devices**（设备）页面，仅显示在定义的站点发现内且符合时间范围过滤条件的医疗设备的条目。
- **Total Vendors**（供应商总数）：这是“医疗设备总数”中引用的医疗设备供应商数量。
- **Devices with MDS2**（具有 **MDS2** 的设备）：这是 IoT Security 具有 MDS2 表单的医疗设备的数量。
- **Total Devices**（设备总数）：这显示网络上的设备总数，由生物医学指示板上设置的站点和时间范围过滤器以及在另一个页面（如“设备”）上设置的设备类型的全局过滤器确定。单击该数字将打开 **Assets**（资产） > **Devices**（设备）页面，以显示与站点、设备类型和定义的时间范围过滤器匹配的设备条目。
- **Medical Subnets**（医疗子网）：这是包含医疗设备的子网总数，由生物医学指示板上设置的站点和时间范围过滤器以及在另一个页面（如“设备”）上设置的设备类型的全局过滤器确定。单击该数字将打开 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Networks**（网络）页面。
- 站点总数：这是租户的绝对站点总数，无论在生物医学指示板上设置的当前站点和时间范围过滤器如何，以及在另一个页面上设置的设备类型的全局过滤器如何。单击该数字将打开 **Networks**（网络） > **Networks and Sites**（网络和站点） > **Sites**（站点）页面。
- 提高设备可见性覆盖率：此按钮打开 数据质量诊断 页面，导航路径为 **Administration**（管理） > **Data Quality**（数据质量）。您可以看到 IoT Security 正在接收的数据的质量。特别是，该页面重点关注 IP 端点和低置信度设备、它们如何降低数据质量，以及通过提高网络覆盖范围来减少其数量的方法。

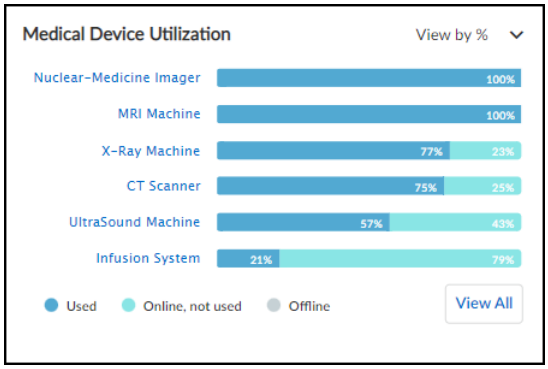
“医疗资产”部分中的两个面板包含有关医疗 IoT 设备的主要类别及其使用情况的信息：

- **Top Medical Device Categories**（主要医疗设备类别）：此面板列出了医疗设备类别，并按设备数量对它们进行排名，包含最多医疗设备的类别位于顶部。单击类别名称将打开一个新的浏览器窗口，其中显示经过过滤的 **Assets**（资产） > **Devices**（设备）页面，仅显示与此

类别匹配的条目。单击右下角的 **View All**（查看全部），打开经过过滤的 **Assets**（资产） > **Devices**（设备）页面，以显示所有医疗设备。



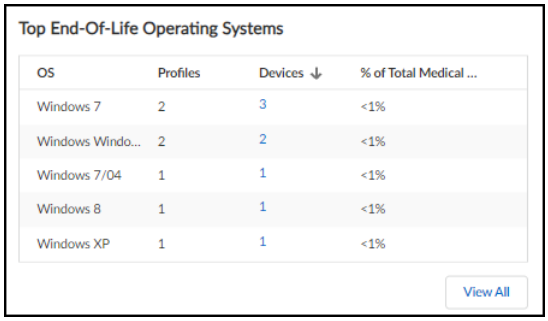
- **Medical Device Utilization**（医疗设备利用率）：此面板显示所有医疗 IoT 类别以及每个类别中设备的使用情况。条形图显示检测到的正在使用、在线但未正在使用，以及离线的设备所占的时间百分比。将光标悬停在条形图上可以看到一个弹出窗口，其中包含每种利用率的数字。单击医疗设备类别，在新的浏览器标签或窗口中打开 **Assets**（资产） > **Devices**（设备）页面。将对页面进行过滤，以显示所选类别中的设备。



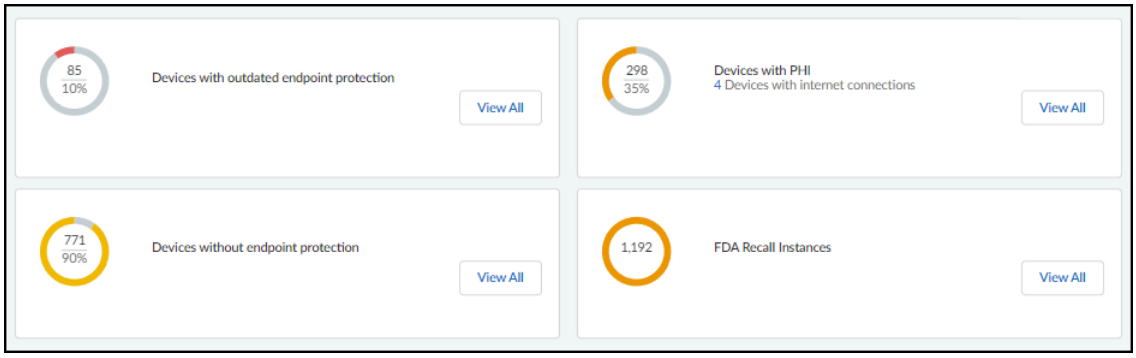
合规风险

指示板的此部分显示有关影响其风险暴露的医疗 IoT 设备的信息。

- **Top End-of-Life Operating Systems**（生命周期终止的主要操作系统）：供应商不再为这些设备运行的操作系统版本提供补丁更新，因而更容易遭受攻击。该表显示了有多少设备配置文件具有生命周期终止的操作系统，以及受影响的医疗设备相对于所有医疗设备的百分比。单击“设备”列中的数字将打开经过过滤的 **Assets**（资产） > **Devices**（设备）页面，仅显示运行此操作系统和版本的设备。



- 列出具有各种风险因素的设备。每一个都会显示具有此风险的设备总数及其相对于所有医疗 IoT 设备的百分比。对于前三个，单击 **View All**（查看全部）将打开带过滤器的 **Assets**（资产） > **Devices**（设备）页面，以便仅显示这些设备。对于具有 FDA 召回的设备，单击 **View All**（查看全部），将打开 **Vulnerabilities**（漏洞） > **Recalls**（召回）页面。



Devices with outdated endpoint protection（具有过时端点保护的设备）：这些设备具有端点保护（例如防病毒保护），但它们尚未与供应商通信，并且一个多月未进行更新。这会使它们容易受到上次更新后发布的新型攻击。

Devices without endpoint protection（没有端点保护的设备）：这些设备上未安装任何端点保护。

Devices with PHI（具有 **PHI** 的设备）：这些设备包含个人健康信息 (PHI)。

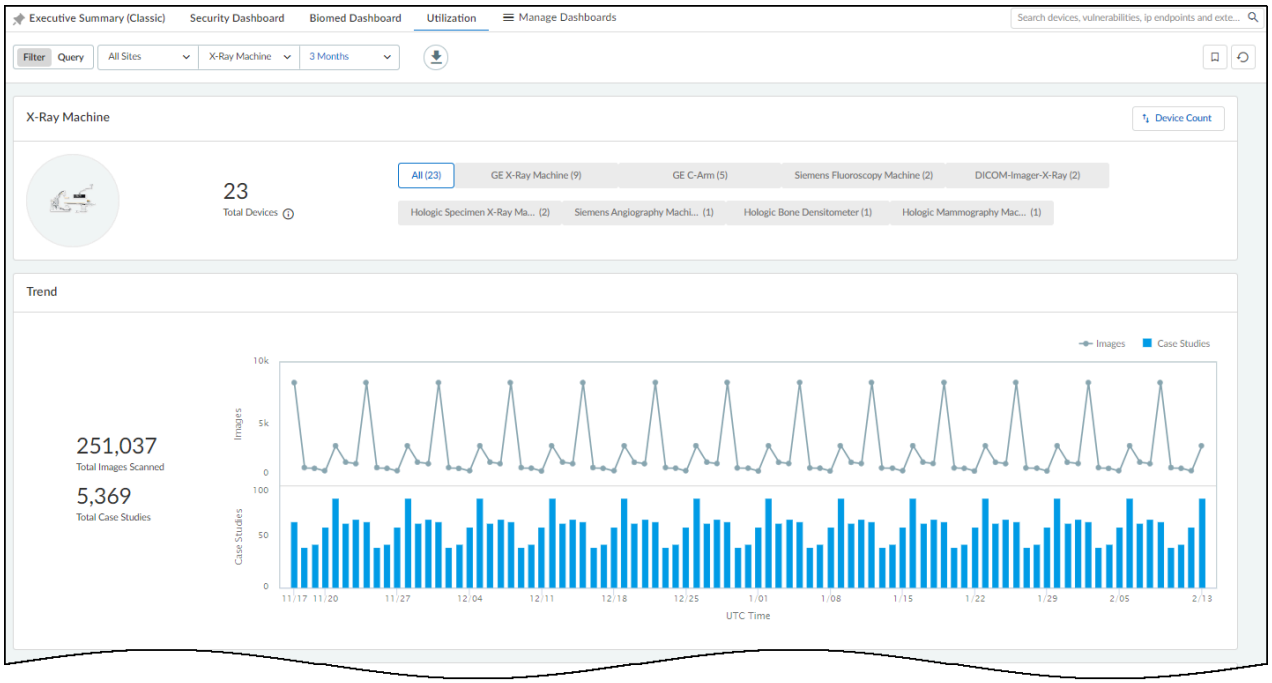
FDA Recall Instances（**FDA** 召回实例）：这里显示因为产品有影响安全的缺陷而需要修理或更换，导致美国食品和药物管理局 (FDA) 发出召回令的设备总数。

利用率指示板

当IoT Security门户主题为医疗 IoT Security 时，您可以看到利用率指示板。IoT Security 收集有关其监控的医疗 IoT 设备的利用率统计数据和指标，并将其显示在此指示板上。然后，您可以利用这些数据来最大限度地减少设备停机时间、降低总体拥有成本 (TCO)，并通过更好的资本规划来增加收入。除了最大限度地减少停机时间和维护之外，您还可以使用收集的数据来识别未使用的资产（可能是损坏或放错位置的），并确保在 IoT 设备生命周期结束时安全可靠地处置设备。

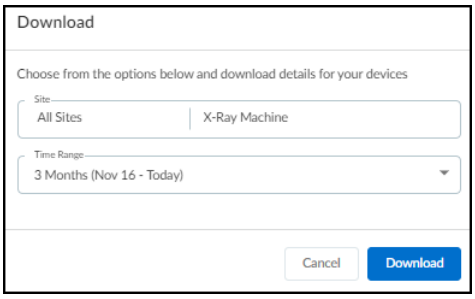
确保防火墙上的应用程序内容版本 为 *8367-6513* 或更高版本；也就是说，主版本（由前四位数字标识）为 *8367* 或更高版本（*8368*、*8369*、*8370* 等），从 *8367-6513* 开始。这些版本包括医疗保健专用应用程序，允许 *IoT Security* 发现医疗设备并提供使用数据。他们还允许防火墙安全策略规则包含医疗保健特定的应用程序。

要查看“利用率”指示板，请选择 **Dashboards**（指示板），然后从 **Manage Dashboards**（管理指示板）下拉列表中选择 **Utilization**（利用率）。



指示板分为两大部分。顶部是一组针对站点、医疗 IoT 设备类别和时间范围的过滤器，用于控制页面上显示的内容。过滤器下方是信息面板，显示有关如何使用医疗 IoT 设备的各种类型的信息。

在 IoT Security 门户中除了查看指示板之外，您可以将其数据下载为 Excel 电子表格。单击顶部过滤器右侧的 **Download**（下载）图标，设置过滤器以包含要保存的数据，然后单击 **Download**（下载）。

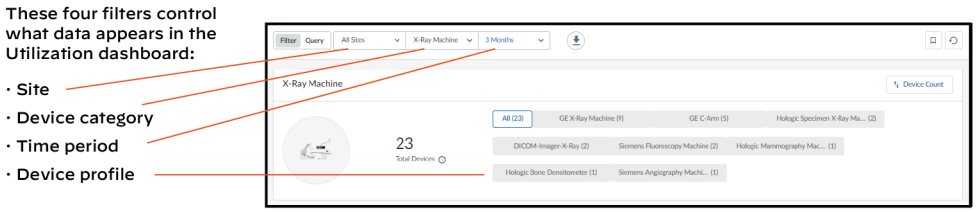


IoT Security 创建一个包含您在多个选项卡上指定的详细信息的 Excel 文件，并使该文件可供下载。

	A	B	C	D	E	F	G	H
1	**site name**	**mac address**	**ip address**	**hostname**	**category**	**profile**	**last activity**	**currently in use**
2	Healthcare	90:1b:0e:26:ff:fa	10.163.23.10	XP1028101323459	X-Ray Machine	Siemens Fluoroscopy Machine	2024-02-14T16:34:18.743Z	yes
3	Healthcare	e4:02:9b:80:48:96	10.23.176.126	WISP-	X-Ray Machine	GE C-Arm	2024-02-11T16:33:06.889Z	yes
4	Healthcare	b0:b9:8a:6d:06:5b	10.44.178.26	LOGIQe	UltraSound Machine	GE UltraSound Machine	2024-02-14T16:34:18.743Z	
5	Healthcare	04:92:26:8a:77:22	10.44.178.145	DESKTOP-7KGV839	X-Ray Machine	DICOM-Imager-X-Ray	2024-02-11T16:33:06.889Z	
6	Healthcare	04:f0:21:0c:28:f6	10.23.176.105	SJHSXRM2333	X-Ray Machine	GE X-Ray Machine	2024-02-14T16:34:18.743Z	yes
7	Healthcare	04:f0:21:4b:76:f1	10.23.182.64	SJS_GEOPTIMA_82	X-Ray Machine	GE X-Ray Machine	2024-02-14T16:34:18.743Z	yes
8	Healthcare	00:25:90:f3:44:7c	10.163.23.192	TOMO01_SJHS	X-Ray Machine	Hologic Mammography Machine	2024-02-14T16:34:18.743Z	yes
9	Healthcare	90:1b:0e:17:5f:d7	10.163.23.11	10502200-60404	X-Ray Machine	Siemens Fluoroscopy Machine	2024-02-14T16:34:18.743Z	yes
10	Healthcare	00:90:fb:65:90:f0	10.163.23.65	WISP-	X-Ray Machine	GE C-Arm	2024-02-11T16:33:06.889Z	yes
11	Healthcare	04:f0:21:85:5f:f3	10.23.176.107	SJS_GEOPTIMA_84	X-Ray Machine	GE X-Ray Machine	2024-02-14T16:34:18.743Z	
12	Healthcare	c8:d3:ff:ba:4c:00	10.160.214.200	minint-3f2eelg	MRI Machine	Siemens MRI Machine	2024-02-14T16:34:18.743Z	yes
13	Healthcare	88:b1:11:d6:06:14	10.23.176.125	WISP-	X-Ray Machine	GE C-Arm	2024-02-14T16:34:18.743Z	yes
14	Healthcare	3c:52:82:6f:c2:25	10.163.23.24	minint-43mgoop	MRI Machine	Siemens MRI Machine	2024-02-14T16:34:18.743Z	yes
15	Default Site	d4:85:64:b9:9b:00	10.10.37.224	X-Ray DR6000	X-Ray Machine	GE X-Ray Machine	2024-02-14T16:34:18.743Z	
16	Healthcare	c8:d3:ff:bc:2d:ff	10.163.23.189	Admin-PC	X-Ray Machine	Hologic Bone Densitometer	2024-02-14T16:34:18.743Z	yes
17	Healthcare	00:0e:8e:63:23:9d	10.23.180.62	SURGERY-2LTAIII	X-Ray Machine	GE C-Arm	2024-02-14T16:34:18.743Z	yes
18	Healthcare	18:60:24:ae:81:22	10.163.23.81	SJS_XR646_81	X-Ray Machine	GE X-Ray Machine	2024-02-14T16:34:18.743Z	yes
19	Healthcare	f0:03:8c:99:bd:fc	10.23.178.100	SJHSUSM2353	UltraSound Machine	GE UltraSound Machine	2024-02-14T16:34:18.743Z	
20	Healthcare	00:0b:ab:c2:f6:42	10.163.23.53	SJHSUSM2353	UltraSound Machine	GE UltraSound Machine	2024-02-14T16:34:18.743Z	yes
21	Healthcare	a0:42:3f:29:e9:2a	10.163.23.136	minint-g34bt9l	X-Ray Machine	Siemens Angiography Machine	2024-02-14T16:34:18.743Z	yes
22	Healthcare	48:0f:cf:4b:fb:9f	10.163.23.74	SJSD63074	Nuclear-Medicine Imager	GE Nuclear-Medicine Imager	2024-02-14T16:34:18.743Z	yes
23	Healthcare	ac:1f:6b:1e:47:57	10.163.23.70	SJS_VOL_03	UltraSound Machine	Volcano UltraSound Machine	2024-02-14T16:34:18.743Z	
24	Healthcare	00:19:99:ec:d9:46	10.163.23.102	CTAWP66611	CT Scanner	Siemens CT Scanner	2024-02-14T16:34:18.743Z	
25	Healthcare	3c:52:82:5f:3f:7a	10.163.23.101	minint-g20usvj	MRI Machine	Siemens MRI Machine	2024-02-14T16:34:18.743Z	yes
26	Default Site	d4:85:64:b9:9b:81	10.10.37.224	X-Ray DR6000	X-Ray Machine	GE X-Ray Machine	2024-02-14T16:34:18.743Z	yes
27	Healthcare	90:1b:0e:ea:12:c2	10.163.23.28	SJHSCT28	CT Scanner	Siemens CT Scanner	2024-02-14T16:34:18.743Z	yes
28	Healthcare	00:13:95:25:9a:fd	10.163.23.107	LS81709157S4	UltraSound Machine	GE UltraSound Machine	2024-02-14T16:34:18.743Z	yes

利用率指示板过滤器

指示板顶部是站点过滤器、医疗 IoT 设备类别、时间范围（1 周、1 个月或 3 个月）和设备配置文件。过滤器决定显示在整个指示板上的数据。



站点：网站过滤器的选择包括 **All Sites**（所有站点）以及一个或多个单个站点。IoT Security 网站过滤器允许您组合多个选项，从而提供了极大的灵活性。

医疗 **IoT** 设备类别：此列表的内容由在您的网络上发现的设备动态确定，并按字母顺序列出。当您最初导航到使用率指示板时，它会按字母顺序对排在第一位的设备类别使用过滤器。如果您更改类别过滤器，导航离开，然后返回到利用率指示板，它会记住您之前选择的过滤条件并继续使用它。

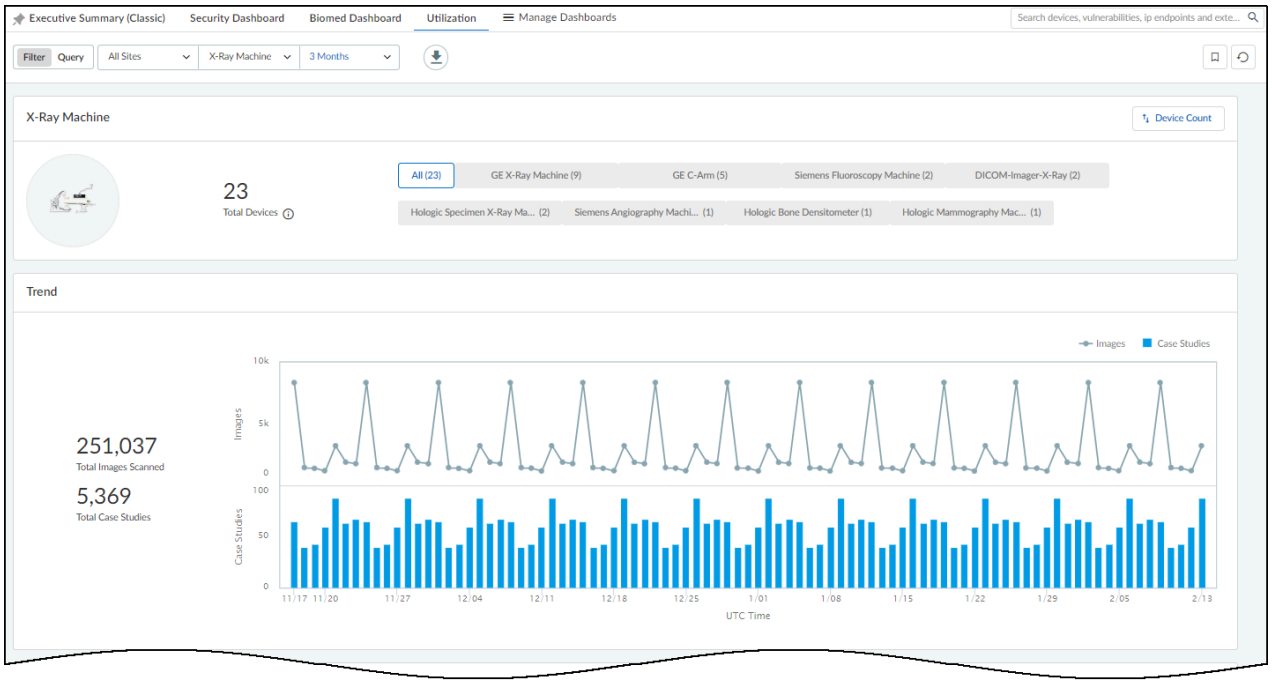
以下是支持的医疗 IoT 设备类别，根据您的网络中是否存在此类设备，这些设备可以显示为过滤器：

- CT 扫描程序
- 输液系统
- 核磁共振机
- 核医学成像仪
- PET 扫描程序
- 超声波机
- X 射线机

时间范围：利用率控制面板的时间范围过滤器包括 1 周、1 个月和 3 个月，指的是最近 7 天、最近 30 天或最近 90 天。当您最初导航到利用率指示板时，它会继承在其他页面或指示板上设置的时间过滤器。如果时间过滤条件不是 1 周、1 个月或 3 个月，则继承的过滤条件仍会显示，但指示板上的内容设置为 1 个月。

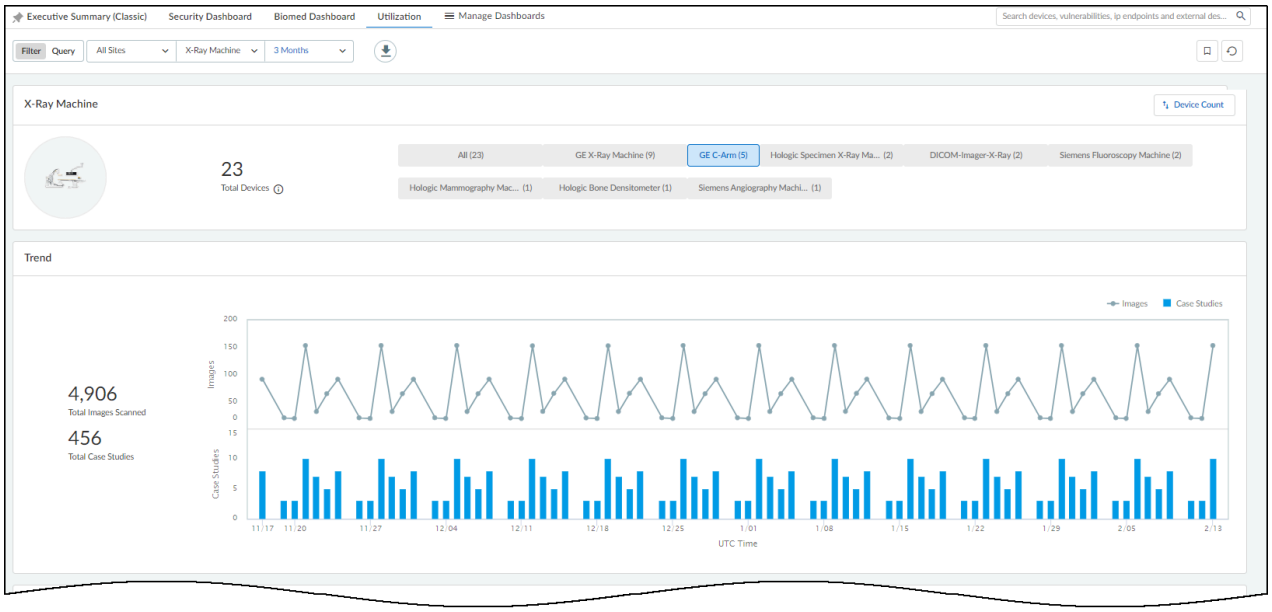
时间过滤器与站点和医疗 IoT 设备类别的过滤器一起，决定了信息面板中数据的范围。但是，无论时间范围过滤器如何，设备配置文件过滤器中显示的设备总数始终是过去一年的设备总数。

设备配置文件：页面标题和顶部过滤栏下方是一个面板，其中显示了过去一年中选定设备类别中的医疗 IoT 设备总数以及该类别中设备所属的设备配置文件。这些配置文件是额外的过滤器，允许您从更广泛的设备类别级别放大到单个设备配置文件中的使用率详细信息。



默认情况下，利用率指示板按设备最多的设备配置文件到设备最少的顺序显示设备配置文件。要按字母顺序列出它们，请单击 **Device Count**（设备计数） > **Profile Name**（配置文件名称）。

此外，默认情况下，利用率指示板显示该类别中所有设备配置文件的数据。要进一步过滤，请选择设备配置文件。



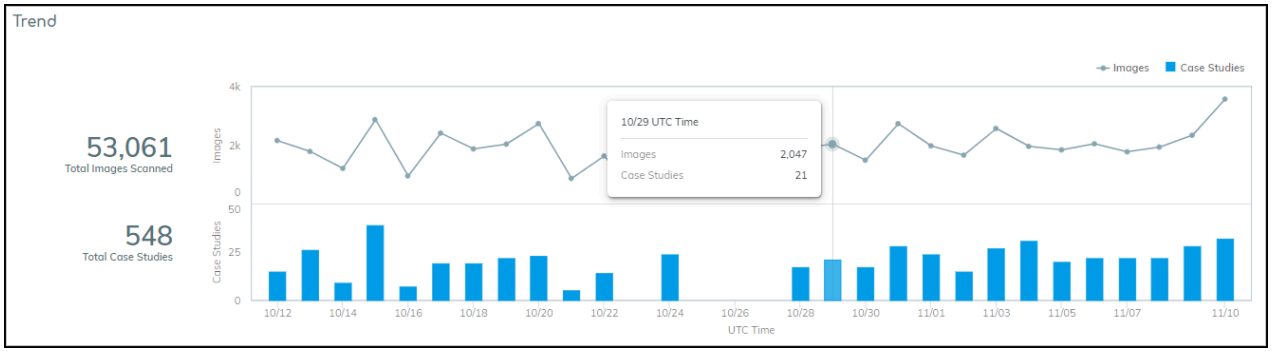
使用信息面板

利用率指示板包含各种信息面板。根据您选择的医疗 IoT 设备类别过滤器，面板的类型会有所不同。

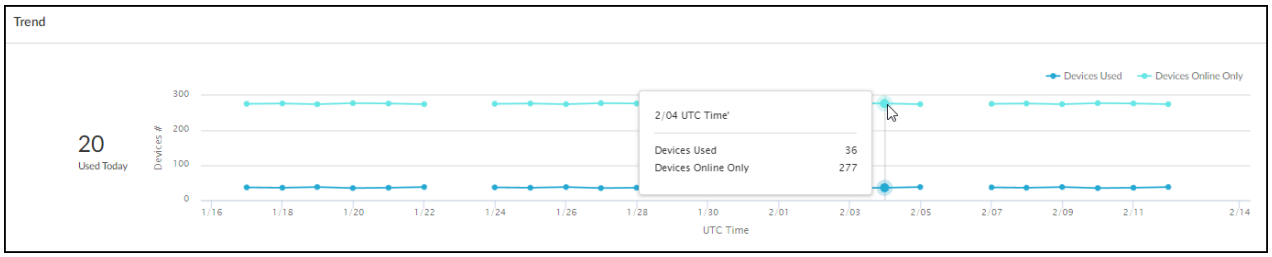
数据不会立即显示在“利用率”指示板中。至少需要 *24* 小时才能收集足够的数据，以便在信息面板中填充有意义的数据。

趋势 — 趋势信息面板显示图表，可帮助您发现设备使用方式的趋势。

对于医疗成像设备，“趋势”面板显示两张图表。折线图显示了在设置为时间过滤器的整个时间段内每隔一段时间拍摄的图像数量。条形图显示了同期创建的案例研究总数。一目了然，您可以看到活动模式以及任何时期的平静和高峰。将光标悬停在数据点上方会显示该点的图像数量和案例研究。如果您只想查看一个或另一个图表，请单击“趋势”面板右上角的 **Images**（图像）或 **Case Studies**（案例研究），以便显示或隐藏它们。如果您想将注意力集中在一张图表上，但不想完全隐藏另一张图表，请将光标悬停在 **Images**（映像）或 **Case Studies**（案例研究）上，使另一张图表逐渐消失。



对于输液系统，趋势面板显示折线图，以跟踪正在使用的系统数量以及连接到网络（在线）但不一定在使用的数量。如果所有连接的输液系统都已连接且正在使用，则这两条线路似乎是一条线，因为它们的所有数据点都对齐。但是，如果将光标悬停在“趋势”面板右上角的 **Devices Used**（已用设备）或 **Devices Online Only(**仅限在线设备**)**上，则可以显示或隐藏一行或另一行。将光标悬停在数据点上方，查看已使用的设备数量和当时连接的设备数量。



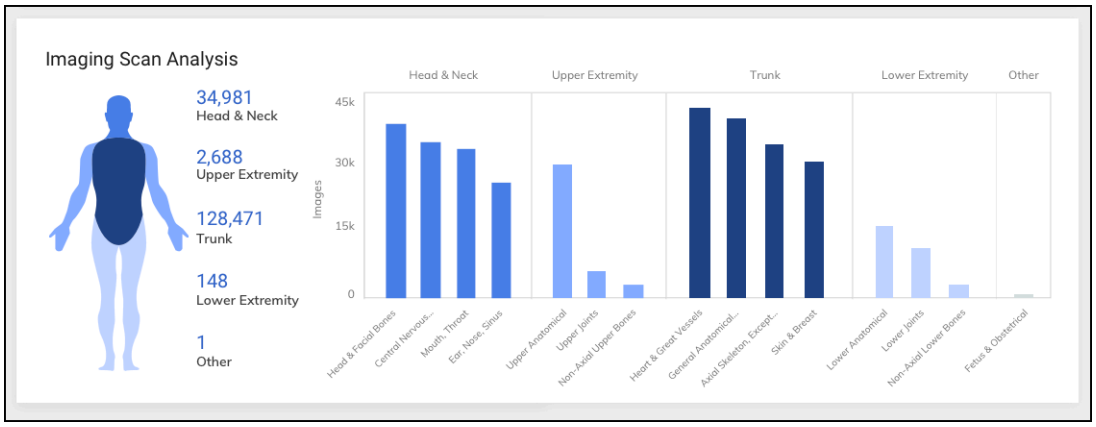
图表左侧显示的数字不是总数。它使用可以计算总数的最新时间，显示当今使用了多少个输液系统。

成像扫描分析 — 该面板总结了成像设备扫描的人体部分。除超声设备外，所有DICOM设备均显示该信息，超声波设备无法识别交通中扫描的身体部位。

该面板分为两个部分。左边是一个由四个主要解剖区域组成的人物图形：

- 头颈
- 上肢
- 躯干
- 下肢

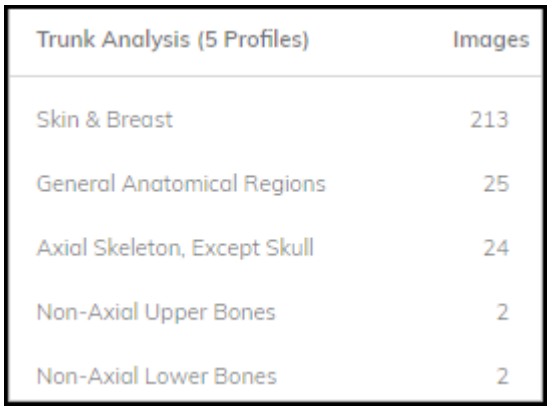
还有第五组叫做“其他”。这适用于无法识别的扫描。



身体每个区域的颜色代表对其进行的扫描量。区域越暗表示该区域的扫描次数越多。

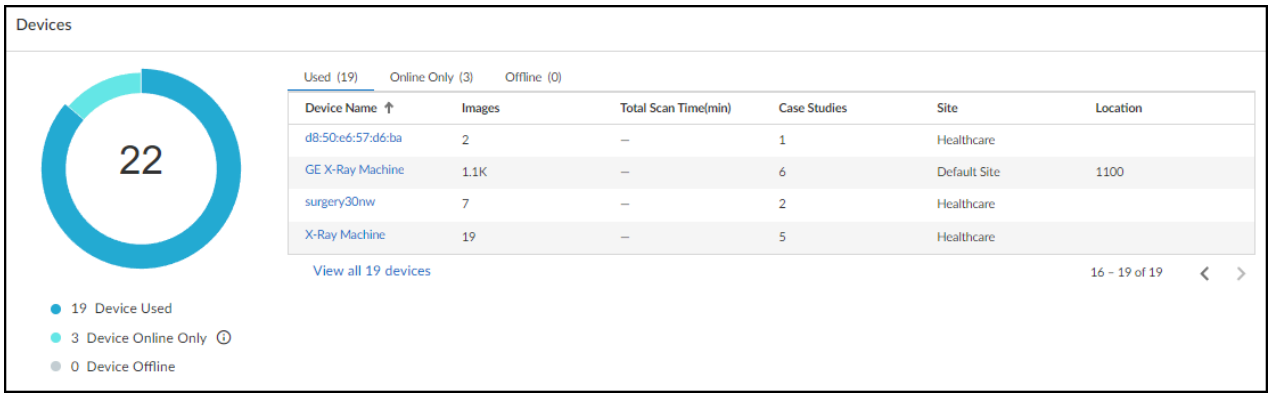
右边是五张条形图，每个条形图代表四个主要解剖区域，第五个条形图代表其他分组。以这种方式对数据进行分块可以更轻松地查看成像设备的使用情况。每张图表中的条形表示对更具体身体部位的扫描次数（例如，更具体的口腔和喉咙的条形图位于头部和颈部的条形图中）。这些图表包括扫

描次数最多的区域的条形图。要查看完整列表，请将光标悬停在其中一个主要部分上，将出现一个弹出窗口。



设备 — 此信息面板显示过去一年中网络上的设备总数，以及在过滤的时间范围内连接到网络并使用、连接但未使用（仅限在线）和断开连接（离线）的设备数量。

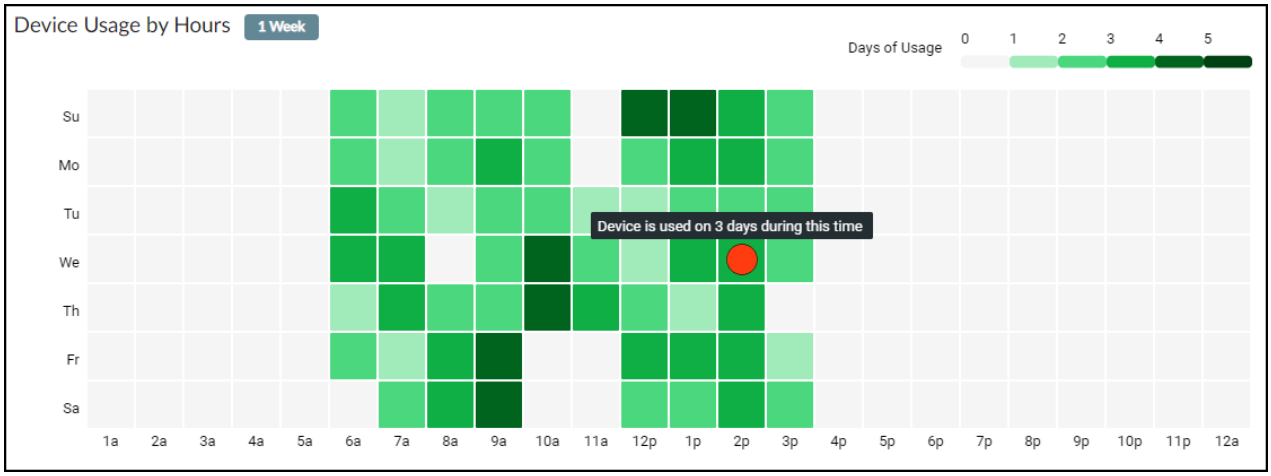
- 已使用 — 这些设备符合所有过滤器，不仅在网络上，而且通过协议发送流量，表明正在使用这些设备。
- 仅限在线 — 这些设备符合所有过滤器并在网络上被检测到，但未发送表明正在使用的流量。
- 离线 — 这些设备是过去一年内 IoT Security 在网络上检测到的，但在时间过滤器中设定的时间范围内未检测到的。



单击甜甜圈图形的某一部分或选项卡标题可切换列表。单击 **View all**（查看所有）**<number>Devices**（设备），打开“设备”页面，过滤器设置为仅显示活动列表中的设备。单击特定的设备名称以查看其设备详细信息。

当您单击“设备名称”列中的某个条目时，将打开该条目的“设备详细信息”页面。在查看“设备详细信息”页面时，单击 **Utilization**（使用率）以查看更多详细信息。

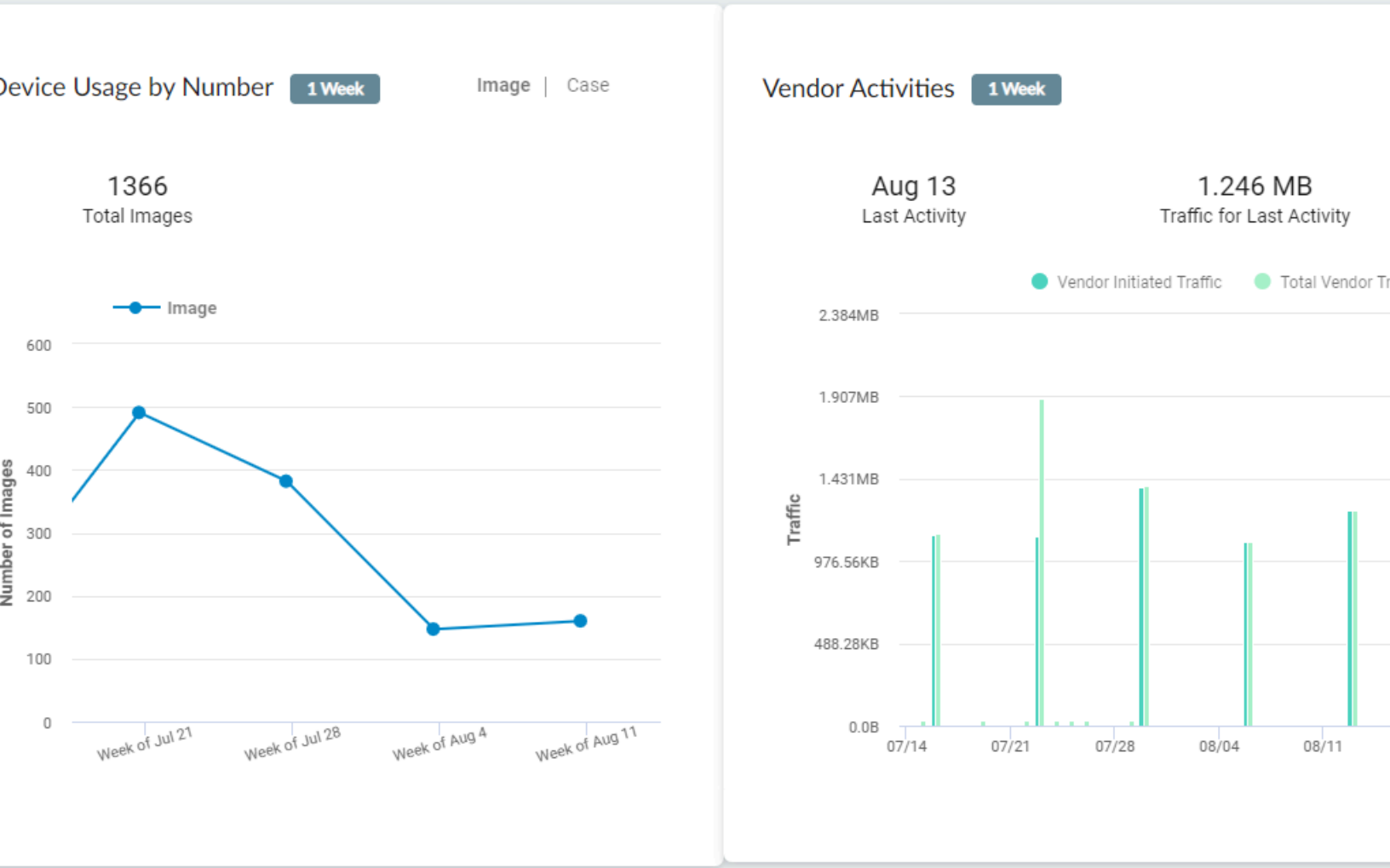
任何成像设备（例如超声波机、X 射线机或 CT 扫描程序）的“设备详细信息”页面上的“使用率”部分会显示该设备何时使用和未使用、如何使用以及何时与设备供应商通信。例如，在设备详细信息页面顶部将时间过滤器设置为 1 个月时，“按小时划分的设备使用情况”信息面板显示设备在过去一个月中的使用时间。



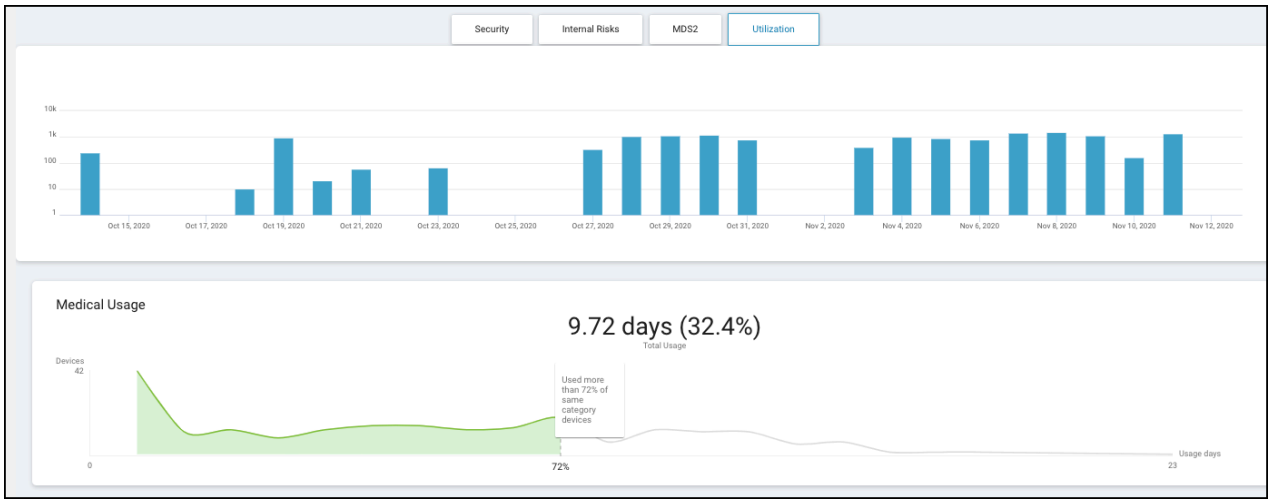
右上角的图例解释了颜色如何表示设备每小时的使用量。绿色越深，使用的次数越多。您也可以将光标悬停在正方形上方，查看解释当时设备使用频率的工具提示。例如，在上图中，该设备在周三下午 2:00 使用了三次。

根据您选择的时间范围，图例是动态的：*1* 周为 *0-1*，*1* 个月为 *1-5*，*1* 年为 *0-40+*。

在“按数量列出的设备使用情况”中，您可以查看设备拍摄的图像数量，或者单击“大小写”，查看设备拍摄图像的 **Case**（案例）数量。在“供应商活动”中，您可以看到设备何时与其供应商通信，对于许多设备而言，这是一种自动获取软件和安全更新的方式。您可以看到供应商发起的流量和供应商总流量，这是设备与供应商之间所有通信的超集，无论是哪一方发起的。



在输液系统的“设备详细信息”页面上查看使用率部分时，IoT Security 门户会显示以下信息。

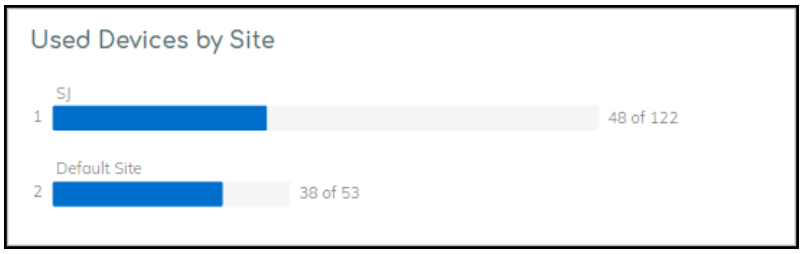


上方图表中的蓝条显示设备使用了多长时间。在 1 周、1 天或 2 小时内，每个蓝条表示设备在过去 168、24 或 2 小时内每小时的使用分钟数（最多 60 分钟）。在 1 个月或 1 年内，它显示设备在过去 30 或 365 天内每天使用的分钟数（最多 1440 分钟）。

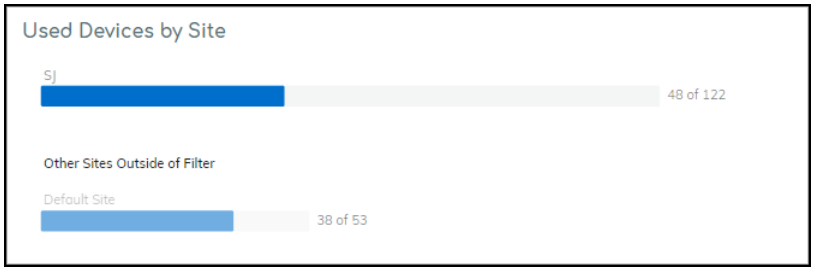
下方的图表显示了该设备与同一设备类别中的其他设备的比较。您可以看到它使用了多长时间以及它在设定的时间范围中所占的积极使用时间百分比。在上面的示例中，它使用了 9.72 天除以 30 天或 32.4% 的时间。折线图显示，在同一类别的 42 台设备中，该设备的使用率超过其他设备的 72#（向左显示为绿色），少于其余 28#（向右显示为白色）。

以下特定于站点的信息面板仅在您为多个站点使用 *IoT Security* 时出现。

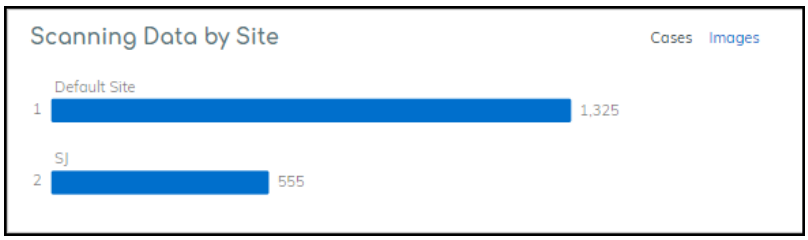
按站点划分的已使用设备 — 这些条形图显示了每个站点在过滤器参数范围内使用了多少医疗 IoT 设备。显示在过滤时间范围内使用的设备数量与过去一年中每个站点的设备总数的关系。



如果您过滤指示板以显示单个站点的数据，则此面板不仅会显示该站点使用的设备，还会显示具有活动设备的其他站点，以提供比较参考。



按站点扫描数据 — 当医疗 IoT 设备类别针对成像设备时，此信息面板显示每个带有活动设备的站点的扫描图像和案例数量。单击 **Cases**（案例）或 **Images**（图片）可在它们之间切换。



如果您过滤指示板以显示单个站点的数据，则此面板不仅会显示该站点的扫描数据，还会显示具有扫描数据的其他站点，以提供比较参考。

按站点划分的平均使用量 — 当您将 **Infusion System** 设置为医疗 IoT 设备类别过滤器时，此信息面板显示每个站点的平均设备使用情况。平均值的计算方法是将某个站点设备在过滤器期间（1 周、1 个月或 3 个月）的总使用时长除以该站点在同一时间内使用的设备总数。在此期间未使用的任何设备都不包括在计算范围内。简而言之，使用时间/使用中的设备 = 平均使用量。

如果您过滤指示板以显示单个站点的数据，则该面板不仅会显示该站点输液系统的平均使用情况，还会显示其他具有主动输液系统的站点的平均使用情况，以提供比较参考。

MDS2

注意：仅当门户主题为 *Medical IoT Security* 时，才会显示 ***Vulnerabilities***（漏洞） > ***MDS2***页面。

医疗设备供应商通常会在医疗设备安全制造商披露声明 (MDS2) 中列出其产品的安全相关特性，并与客户分享。供应商为每个版本的医疗设备发布这些 MDS2 文档，其中包含有价值的信息，例如设备是否处理 PHI（个人健康信息）；是否存储 PHI；如果是，是否加密；以及设备上是否安装了防病毒软件。

随着时间的推移，医疗保健提供者可以收集数千种医疗设备的数千份 MDS2 文档。按照预期使用时，MDS2 文档可以极大地增强您的安全态势和事件响应 (IR)。然而，从这些文档中获取有关在其连接的设备上运行的软件的特定版本的详细信息是一项艰巨的任务。因此，MDS2 文件经常被闲置。

IoT Security 简化您拥有的 MDS2 文件的管理和使用。如果您将设备的 MDS2 文件上传到 IoT Security，然后，它会在评估设备风险时将这些数据与其他环境因素一起纳入其中。例如，如果 MDS2 文件中指定的设备的软件版本存在已知漏洞，IoT Security 可以更准确地将其识别为一个漏洞，而不仅仅是一个潜在的漏洞。IoT Security 支持 2004、2008、2013 和 2019 格式的 MDS2 文件。

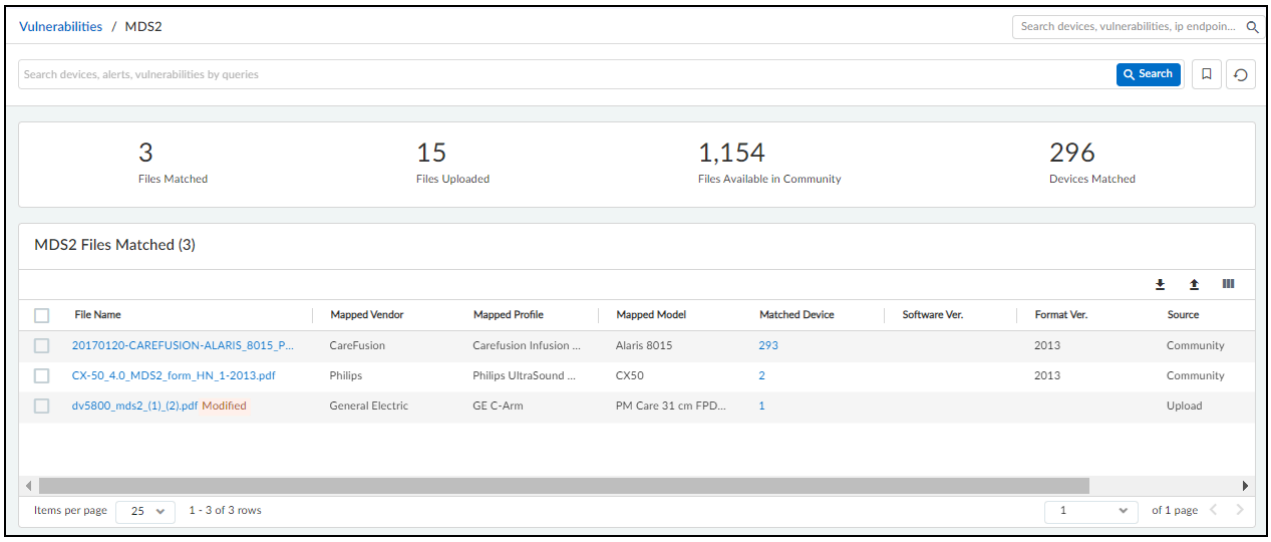
您可以将 MDS2 文件上传至 IoT Security并使用其他 IoT Security 用户通过 MDS2 社区共享的文件。要加入，请选择 **Vulnerabilities**（漏洞） > **MDS2**，单击 **Learn More**（了解更多），阅读有关 MDS2 社区如何运作的信息，然后单击 **Join Now**（立即加入）。之后，IoT Security 会扫描社区并显示与您的设备匹配的其他社区成员先前上传的 MDS2 文件。同时，Palo Alto Networks 安全工程师会审查您已上传的任何 MDS2 文件。如果获得批准，IoT Security 随后会与其他社区成员共享您的文件。本着这种合作精神，每位用户都能从彼此共享的文件中受益。

如果成员上传重复的 MDS2 文件（即多个文件适用于同一供应商、配置文件和型号），IoT Security 会使用以下逻辑按从上到下的顺序排列优先次序并自动将其应用到您的设备：

- 如果排除 MDS2 文件，请不要使用它。
- 使用手动选择的 MDS2 文件而不是自动选择的文件。
- 使用您上传的 MDS2 文件。
- 使用社区中共享的 MDS2 文件。
- 使用低于其他版本的 MDS2 文件版本。
- 使用 MDS2 文件的较新格式版本，而不是较早格式；例如，使用 2017 MDS2 文件，而不是 2013 格式版本。

当您加入 MDS2 社区后选择 **Vulnerabilities**（漏洞） > **MDS2** 时，IoT Security 会显示 MDS2 文件匹配页面。这会列出 IoT Security 清单中与医疗 IoT 设备匹配的 MDS2 文件。您可以从这里导航到包含您之前上传的 MDS2 文件的页面，这是包含其他 IoT Security 客户上传的文件的页面，以及此处列出与 MDS2 文件匹配的医疗 IoT 设备的页面。

在 **Vulnerabilities**（漏洞） > **MDS2**上，您可以查看清单中与医疗 IoT 设备匹配的文件，下载这些文件，如果您不希望 IoT Security 将其应用到您的医疗 IoT 设备中，则将其排除。您还可以下载所有已上传的 MDS2 文件的完整列表或一个或多个选定文件的列表。



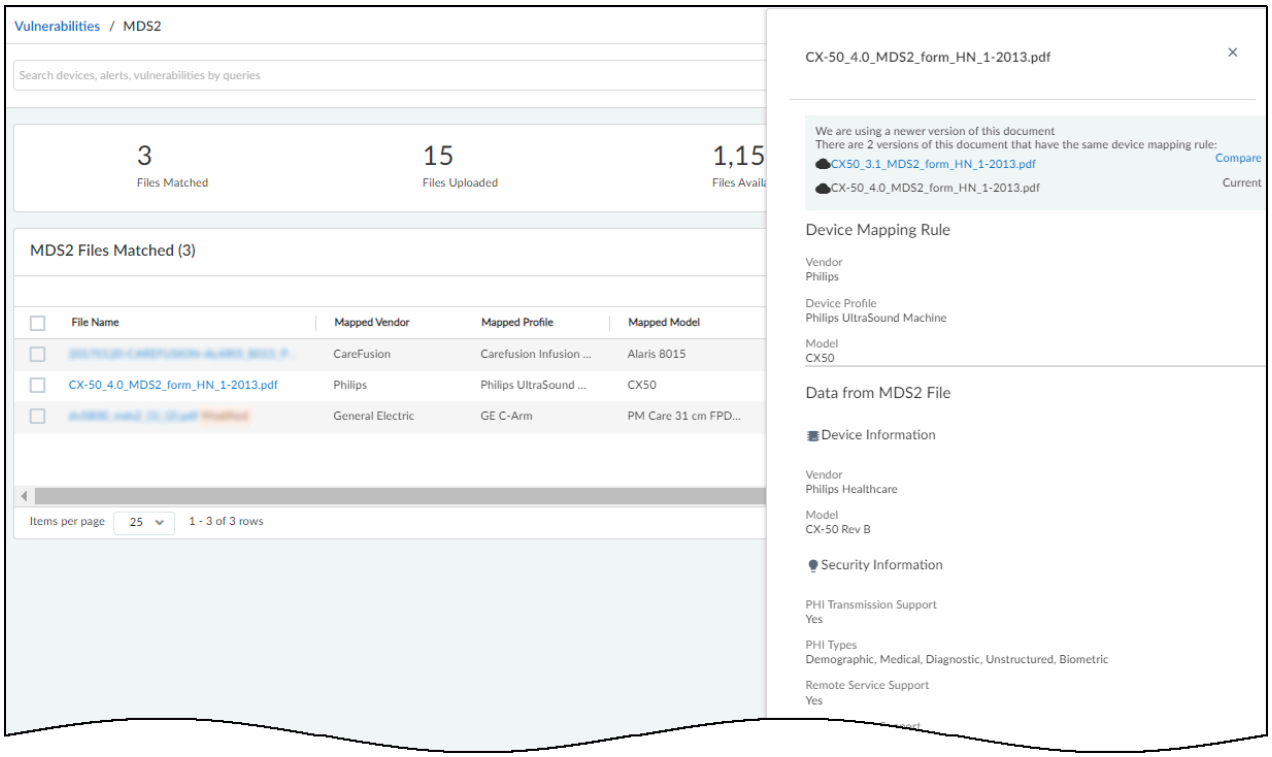
要上传文件，请单击 **Upload**（上传）图标 (⬆)，找到一个 PDF 格式的 MDS2 文件，然后选择并上传。

IoT Security 将上传的 MDS2 文件与文件中指定的具有相同型号、供应商和配置文件的设备进行匹配。虽然您可以在 “设备详细信息”页面上传 MDS2 文件，IoT Security 仅将 MDS2 文件应用于该单个设备。另一方面，如果您在 MDS2 页面上上传 MDS2 文件，IoT Security 会在其清单中搜索具有相同型号、供应商和配置文件属性的所有设备，并将 MDS2 文件应用于所有匹配的设备。此外，如果以后有新设备添加到清单中，IoT Security 会将 MDS2 文件也应用于这些设备。

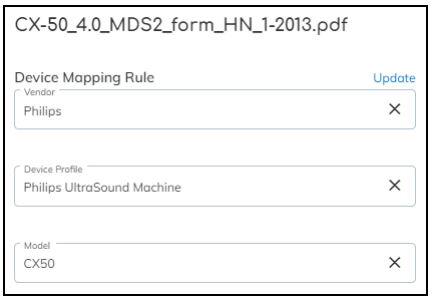
单击“匹配的设备”列中的数字将打开“设备”页面，其中会应用过滤器仅显示与 MDS2 文件匹配的设备。

MDS2 页面上“匹配的设备”列中的数字是所有站点的总数。如果您对站点子集的设备数据具有管理访问权限，则“设备”页面上匹配的设备数量可能小于 *MDS2* 页面上的数量。

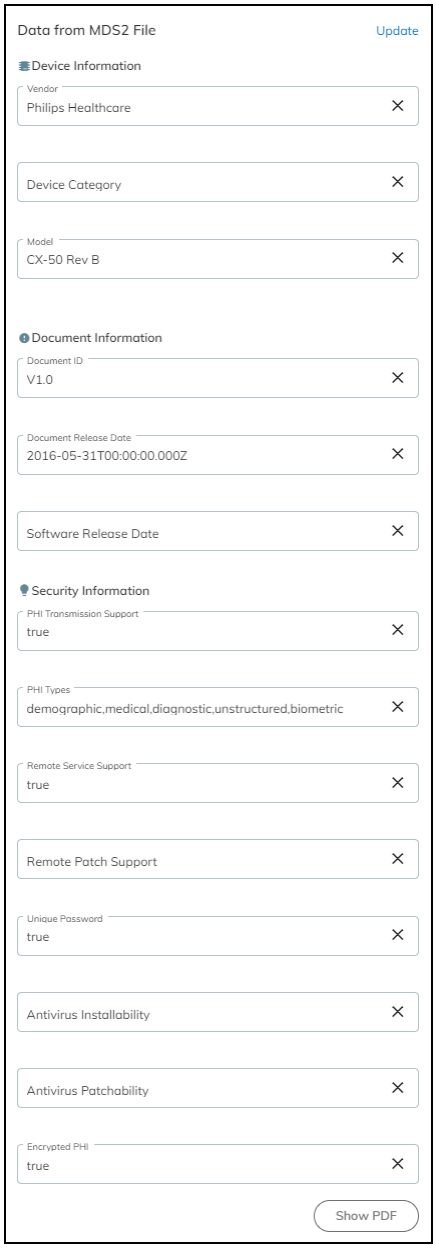
要查看有关 MDS2 文件的一些详细信息，请单击“文件名”列中的条目。主窗口右侧会滑动打开一个信息面板，其中列出了 IoT Security 用于将 MDS2 文件映射到设备的三个属性。下面列出了有关设备、文档和安全的几个要点。



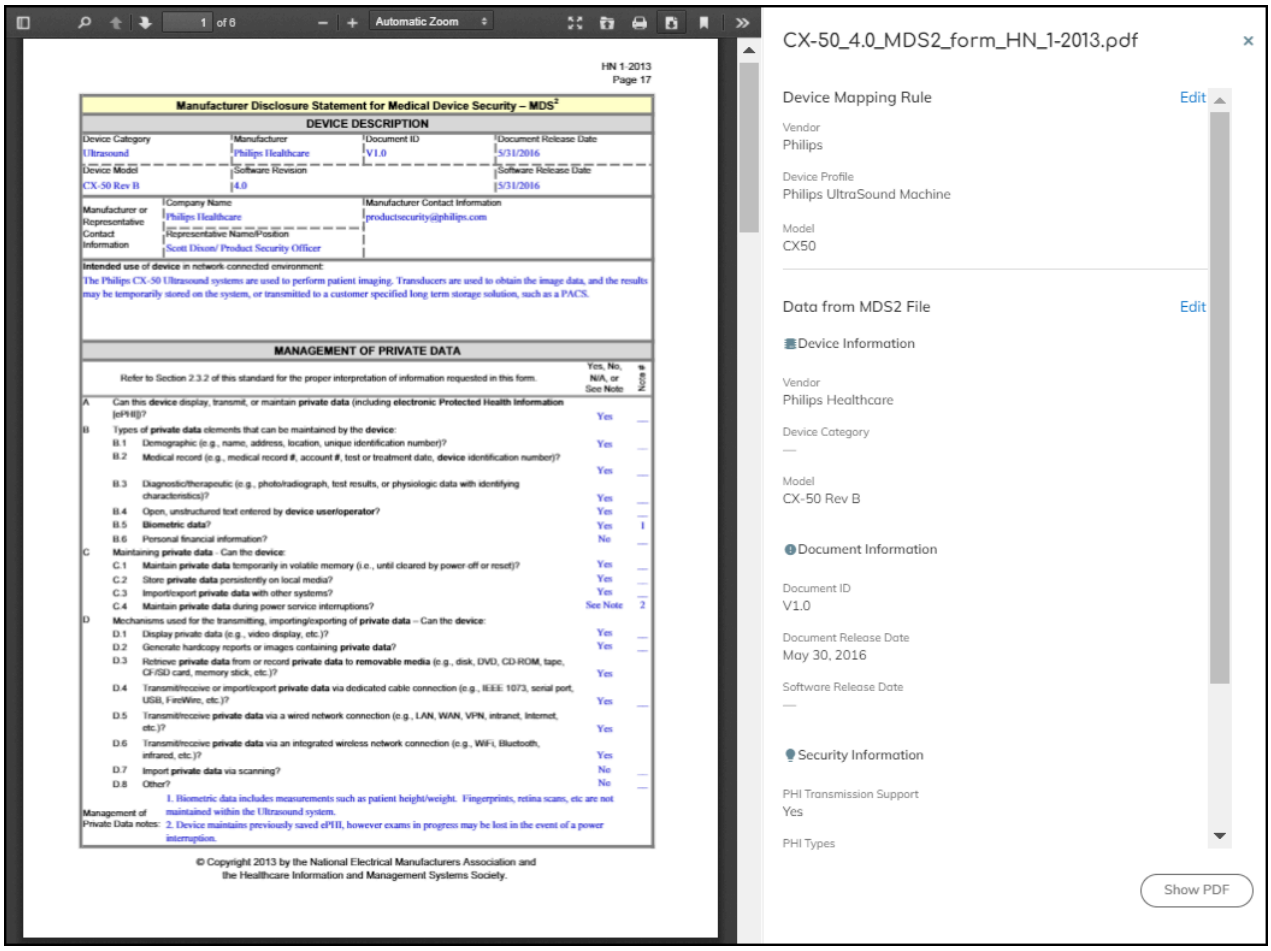
上传 MDS2 文件时，请检查设备映射规则值是否存在不准确之处。PDF 中的文本对齐问题可能会导致字符解析不正确。如果发生这种情况，IoT Security 无法将 MDS2 文件与设备匹配。在这种情况下，单击“设备映射规则”右侧的 **Edit**（编辑），根据需要修改文本，然后单击 **Update**（更新）。



除了设备映射规则中的值之外，如果 MDS2 文件中的其他属性解析不正确，您还可以编辑它们。每当您单击 **Update**（更新）时（无论是对设备映射规则还是对来自 MDS2 文件的数据的更改），IoT Security 都会立即删除 MDS2 文档的所有先前匹配项并再次运行匹配过程。



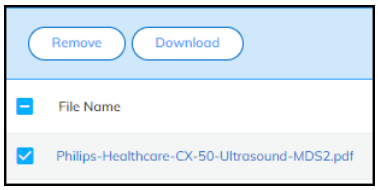
要以 PDF 格式查看整个 MDS2 文件，请单击信息面板中的 **Show PDF**（显示 **PDF**）。



要下载 PDF，请单击位于 PDF 查看器顶部的 **Download**（下载）图标 ( )。

要关闭信息面板（和 PDF 查看器，如果也打开的话），请单击右上角的 **X** 或再次单击文件名。

要下载 .csv 文件中所有已上传 MDS2 文件的列表，请单击位于 MDS2 表上方的 **Download**（下载）图标 ( )。要以 .csv 文件形式下载一个或多个 MDS2 文件的列表，请选中要下载的文件的复选框，然后单击 **Download**（下载）。



要删除一个或多个先前上传的 MDS2 文件，请选中要删除的文件的复选框，然后单击 **Remove**（移除）。

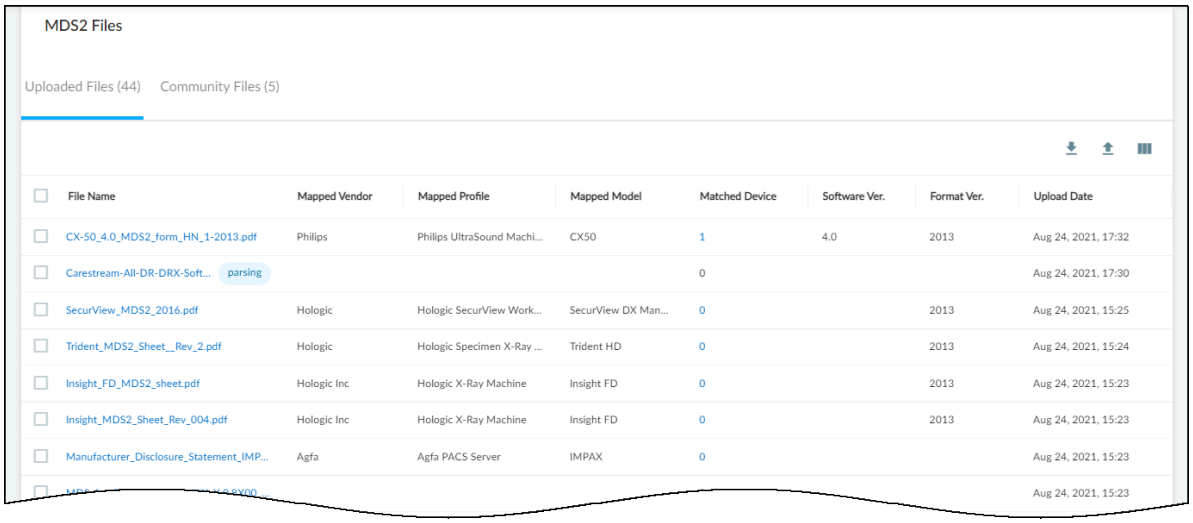
MDS2 社区

如果您愿意，可以覆盖自动 MDS2 文件选择并应用您选择的其他文件。请参阅下面最后一步的说明。

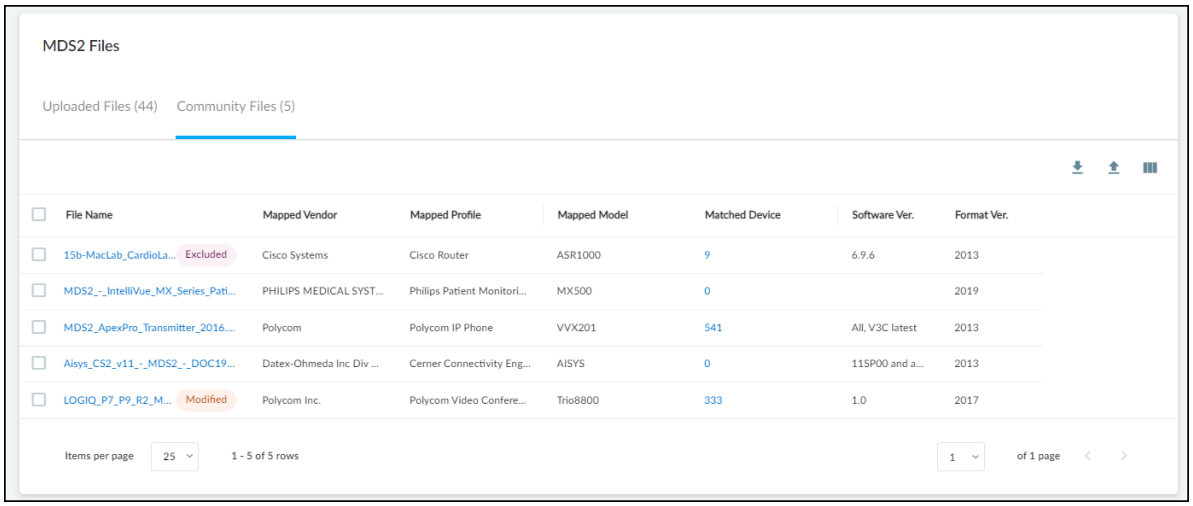
STEP 1 | 查看您上传的 MDS2 文件和共享的社区文件。

1. 在 **Vulnerabilities**（漏洞） > **MDS2** 页面上，单击 <number>**Files Available in Community**（社区中可用的文件）。

   Vulnerabilities（漏洞） > **MDS2** > **MDS2 Files**（**MDS2** 文件）页面打开时有两个选项卡：一个用于您上传的文件 **[Uploaded Files(**已上传的文件**)]**，一个用于在社区中共享的文件 **[Community Files**（社区文件）]。



该表提供了有关 MDS2 文件的关键详细信息：它适用的供应商、配置文件、型号和软件版本；它匹配的清单设备数量；MDS2 文件的格式版本；以及它上传到 IoT Security 的时间。



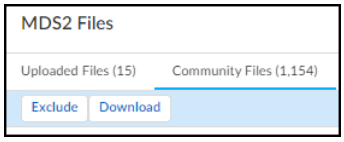
社区文件页面上的表格提供的信息几乎与上传的文件页面上的信息相同，但文件上传日期除外。

STEP 2 | 如果有您不想要 IoT Security 应用于您的设备的共享 MDS2 文件，请将其排除。

也许因为某种原因，您更喜欢不同的版本，您可能不想要 IoT Security 将一个或多个社区文件应用到您的医疗 IoT 设备。在这种情况下，您可以将它们排除在自动选择过程之外。

1. 选择 **Vulnerabilities**（漏洞） > **MDS2** > **MDS2 Files**（**MDS2** 文件） > **Community Files**（社区文件），选中要从自动选择过程中排除的 MDS2 文件的复选框。

   表格上方的 **Exclude**（排除）并 **Download**（下载）按钮。



2. 单击 **Exclude**（排除）。

   如果您改变主意，请重复这些步骤，但要单击 ***Include***（包括）而不是 ***Exclude***（排除）。*IoT Security* 会为先前排除的 *MDS2* 文件显示 ***Include***（包含）按钮。

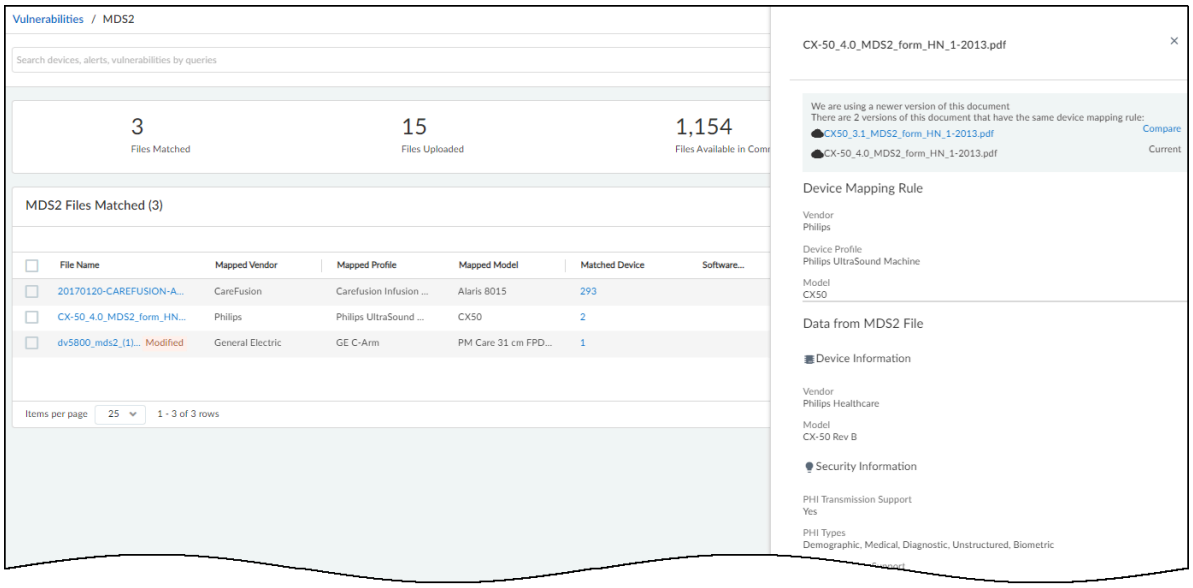
STEP 3 | 如果有重复的 MDS2 文件，并且您想使用与 IoT Security 自动选择的文件不同的文件，则手动覆盖选择。

当多个 MDS2 文件适用于同一供应商、配置文件和型号时，您可能需要 IoT Security 应用除自动选择的 MDS2 文件之外的其他 MDS2 文件。例如，如果您的医疗 IoT 设备运行的是早期软件

版本，那么您可以选择早期格式的版本，并且此 MDS2 文件比更高版本的文件更准确地适用于它们。

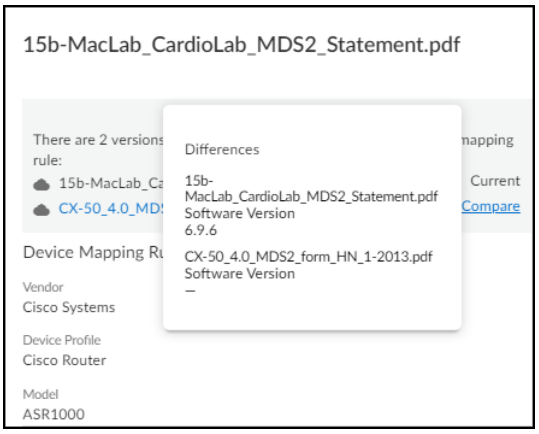
1. 单击 **Vulnerabilities**（漏洞） > **MDS2** 页面上的 MDS2 文件名。

   页面右侧打开的信息面板按优先级顺序列出重复的 MDS2 文件。

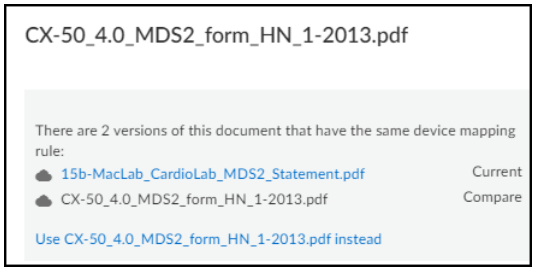


您上传的文件的信息面板包含 ***Edit***（编辑）选项，但社区共享文件的面板则没有。

2. 要比较两个重复文件，请单击或将光标悬停在 **Compare**（比较）上。IoT Security 会将其与当前应用的文件进行比较。在这里显示的示例中，您可以看到第一个 MDS2 文件被优先考虑，因为它具有软件版本，而第二个文件没有。



3. 要使用其他文件，请单击其名称，然后单击 **Use** <file-name> **instead**（改为使用 **<file-name>**）。



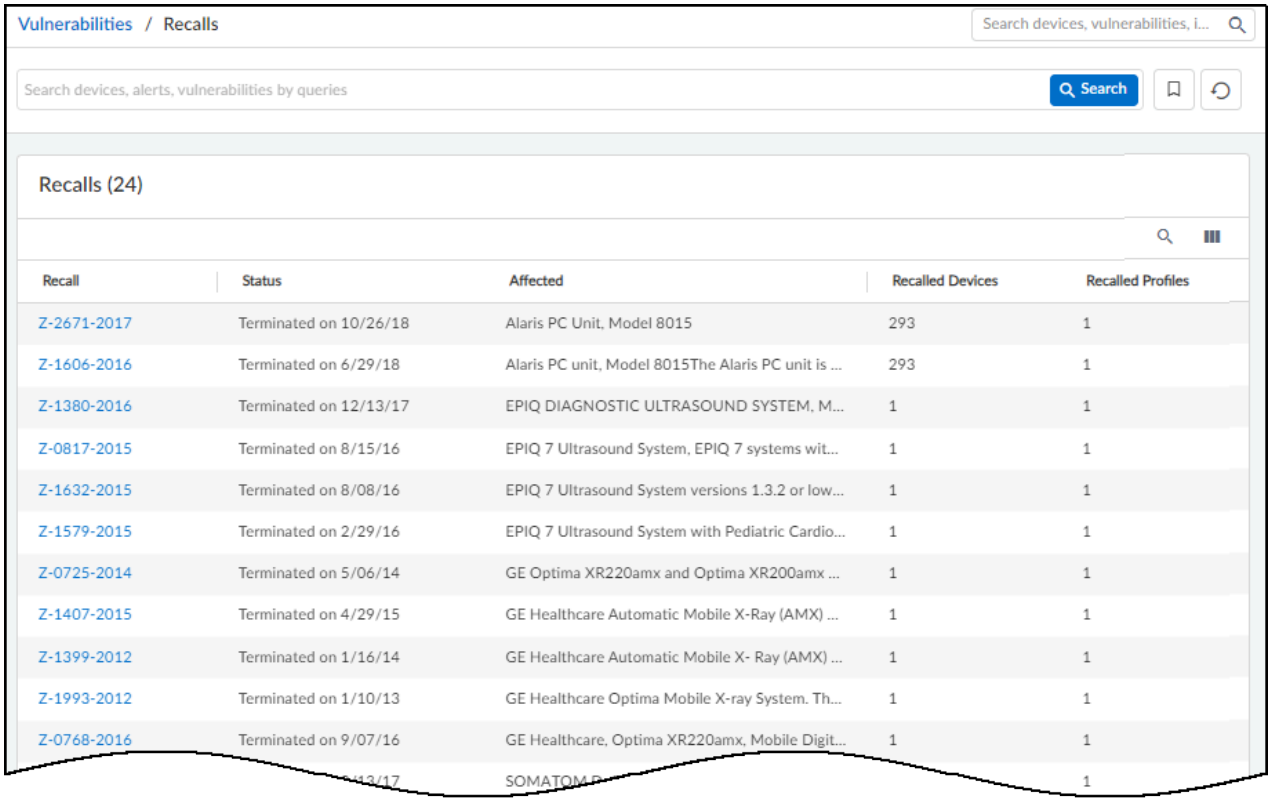
您选择的文件的名称现在出现在文件名列中，并在信息面板中显示为 *Current*（当前）。

召回

Vulnerabilities（漏洞） > **Recalls**（召回）页面在您的网络上列出美国食品药品监督管理局 (FDA) 召回的设备。

仅在主题为“医疗 *IoT Security*”并检测到网络上至少有一个医疗 *IoT* 设备已被召回时，*IoT Security* 门户才会显示“召回”页面。防火墙上的程序内容版本必须为 *8367-6513* 或更高版本，才能检测特定于医疗保健的应用程序并将其包含在安全策略规则中。

Recalled Devices（已召回设备）列显示网络中已召回的设备数量，如果状态为开放，则制造商仍接受设备退货。



每个召回标识符都链接到美国 URL。美国食品和药物管理局网站上有关于召回的信息。例如，单击上面显示的“召回”列中的 **Z-1380-2016** 将打开网页。

Class 2 Device Recall EPIQ DIAGNOSTIC ULTRASOUND SYSTEM

See Related Information

Date Initiated by Firm	March 28, 2016
Create Date	April 13, 2016
Recall Status[1]	Terminated [3] on December 13, 2017
Recall Number	Z-1380-2016
Recall Event ID	73865
510(K)Number	K132304
Product Classification	System, imaging, pulsed doppler, ultrasonic - **Product Code** IYN
Product	EPIQ DIAGNOSTIC ULTRASOUND SYSTEM, Model EPIQ 5C, EPIC 5G, EPIQ 5W, EPIQ 7C, EPIC 7GC, and EPIQ 7W. Diagnostic Ultrasound System for ultrasound imaging in abdominal, cardiac adult, cardiac other (fetal), cardiac pediatric, cerebral vascular, cephalic (adult), cephalic (neonatal), fetal/obstetric, gynecological, intraoperative (vascular), intraoperative (cardiac), musculoskeletal (conventional), musculoskeletal (superficial), other: urology, pediatric, peripheral vessel, small organ (breast, thyroid, testicle), transesophageal (cardiac), trans rectal, transvaginal.
Code Information	All Serial numbers
Recalling Firm/ Manufacturer	Philips Ultrasound, Inc. 22100 Bothell Everett Hwy Bothell WA 98021-8431
For Additional Information Contact	Philips Customer Service 800-722-9377
Manufacturer Reason for Recall	The fasteners securing the control panel assembly to the base of the Philips EPIQ Ultrasound System may loosen over time, which could subsequently lead to the detachment of the entire assembly from the ultrasound system.
FDA Determined Cause [2]	Device Design
Action	The firm, Philips, sent an "Urgent-Medical Device Correction" Philips EPIQ Ultrasound System (MDC 79500381/2), letter dated 2016 MAR 23 to consignees on 3/28/16. The letter describes the product, problem and actions to be taken. The customers were instructed to review the information with all members of your staff who need to be aware of the contents of this communication. If, at any time, the control panel assembly on your ultrasound system wobbles or feels loose, stop using your system immediately and contact your local Philips representative or Philips Customer Service at 1-800-722-9377. Otherwise, you may continue to use your system. Philips will contact all EPIQ customers to arrange for service to replace the fasteners connecting the control panel assembly to the system with fasteners less likely to loosen with repeated handling. This service will be performed free of charge. If you need any further information or support concerning this issue, please contact your local Philips representative or Philips Customer Service at 1-800-722-9377.
Quantity in Commerce	11,085 units total (4909 units in the US and 6176 units outside the US)
Distribution	Worldwide Distribution: US (nationwide) including Washington, D.C., and countries of: Algeria, Argentina, Armenia, Australia, Austria, Bahrain, Bangladesh, Belgium, Bermuda, Bolivia, Brazil, Brunei Darussalam, Bulgaria, Canada, Chile, China, Colombia, Costa Rica, Croatia, Cuba, Czech Republic, Denmark, Ecuador, Egypt, Estonia, Finland, France, French Guiana, French Polynesia, Georgia, Germany, Greece, Guadeloupe, Guatemala, Hong Kong, Hungary, India, Indonesia, Iran, Ireland, Israel, Italy, Japan, Jersey, Jordan, Kazakhstan, Kenya, Korea, Republic of, Kuwait, Latvia, Lebanon, Libya, Lithuania, Luxembourg, Macedonia, Malaysia, Malta, Martinique, Mayotte, Mexico, Monaco, Mongolia, Morocco, Myanmar, Netherlands, New Caledonia, New Zealand, Nicaragua, Norway, Oman, Pakistan, Palestine, State of, Panama, Peru, Philippines, Poland, Portugal, Puerto Rico, Qatar, R¿¿union, Romania, Russia , Russian Federation, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Tanzania, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, Uzbekistan, and Viet Nam.
Total Product Life Cycle	TPLC Device Report

无论您是否在产品召回时收到制造商的说明，您都可以打开召回 URL 以获取被召回设备的批号、序列号或版本号等识别信息，并了解制造商的联系信息。然后，您可以使用这些号码来定位设备，并致电或写信给制造商。

管理 IoT Security 用户

利用基于角色的访问控制 (RBAC) 管理 IoT Security 用户。

- 创建 IoT Security 用户
- IoT Security 的用户角色

创建 IoT Security 用户

用户使用单点登录 (SSO) 登录 IoT Security 门户时，需要经过一个两步流程。在步骤 1 中，SSO 身份提供程序 (IdP) 通过验证用户的凭据对其进行身份验证。在步骤 2 中，用户被授权并被赋予访问 IoT Security 的角色。

用户使用 Palo Alto Networks SSO 登录 IoT Security 门户时，将对照客户服务门户 (CSP) 中的用户帐户验证其凭据。然后根据 Hub 的身份和访问部分分配其用户角色。用户角色决定了他们可以在门户中看到什么和做什么。这些用户角色称为“外部管理用户角色”，而“内部管理用户角色”在 IoT Security 门户中分配，将在后面的章节中介绍。

此外，IoT Security 还提供了通过 SSO 针对 Active Directory (AD) 身份验证系统验证用户的选项。在这种情况下，用户帐户在 Active Directory 中，Active Directory 代表 IoT Security 验证用户凭据。您可以通过两种不同的方式来管理给定用户的角色，类似于 Palo Alto Networks SSO：(1) 由 IoT Security 在内部管理或 (2) 由 Active Directory 在外部管理。

外部角色在 *AD* 中管理，而不是像在 *Palo Alto Networks SSO* 选项中一样在 *Hub* 中管理。

由于可以在两个不同的地方管理用户角色，因此当用户通过 SSO 登录时，IoT Security 可能会发现自己的外部角色与内部角色不同。在这种情况下，较高的角色优先。

使用 Palo Alto Networks SSO 对用户进行身份验证并管理 Hub 中的用户角色

IoT Security 通过应用程序管理员、实例管理员、所有者、管理员和只读角色支持基于角色的访问控制 (RBAC)。为 IoT Security 应用程序创建用户涉及三个步骤：

- 在客户支持门户中创建用户帐户
- 在 Hub 中分配用户角色
- （对于管理员和只读用户）允许访问所有站点或站点子集

STEP 1 | 使用超级用户权限登录到客户支持门户，这允许您创建新的用户帐户。

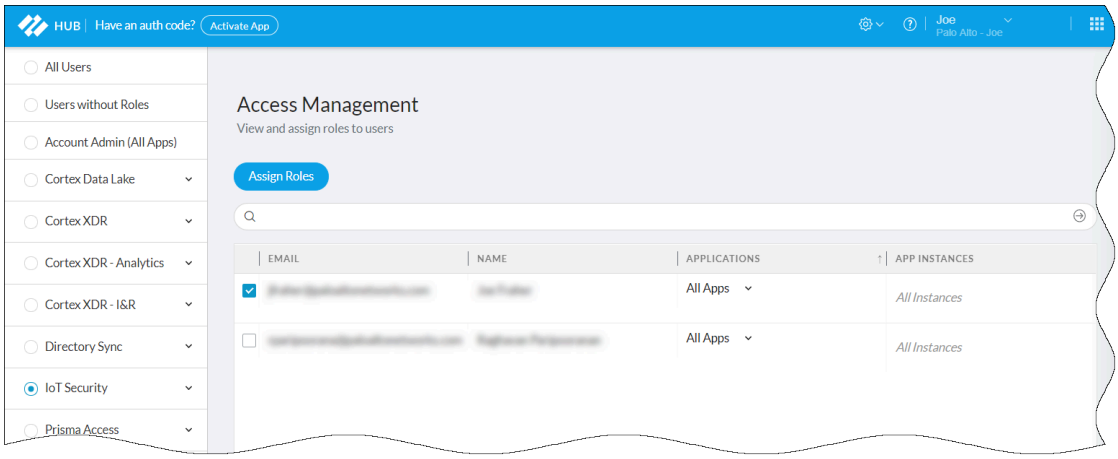
STEP 2 | 单击 **Members**（成员） > **Create New User**（新建用户），输入所需信息，然后 **Submit**（提交）。

将创建一个新的用户帐户并将其作为成员添加到帐户中。将向具有登录凭据的新用户发送电子邮件通知。

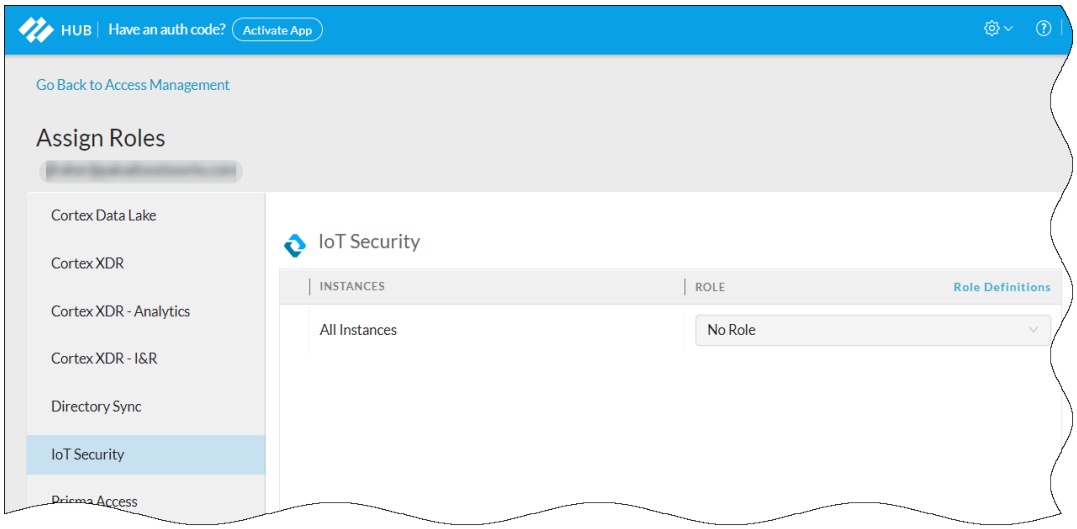
STEP 3 | 登录到 Hub。

STEP 4 | 单击 Hub 登录页右上角的齿轮图标，然后单击 **Access Management**（访问管理）。

STEP 5 | 展开左侧面板中的 IoT Security 部分，选择要向用户分配的 IoT Security 实例，选中刚才创建的用户帐户的复选框，然后 **Assign Roles**（分配角色）。



STEP 6 | 选择左侧面板中的 **IoT Security**，在主面板中显示 IoT Security 角色分配窗口。



STEP 7 | 从角色下拉列表中选择以下角色之一：

应用程序管理员

实例管理员

所有者

管理员

只读

STEP 8 | 有关这些用户角色的信息，请单击 **Role Definitions**（角色定义）。

要了解有关应用程序管理员和实例管理员角色的详细信息，这两个角色是所有 Palo Alto Networks 应用程序的常见角色，并在 IoT Security 中提供与所有者相同的权限，请参阅可用角色。要了解有关所有者、管理员和只读角色（特定于 IoT Security的详细信息，请参阅IoT Security 的用户角色。

使用 Active Directory SSO 验证用户并管理 Active Directory 中的用户角色

STEP 1 | 准备身份验证系统。

配置 IoT Security 之前，请准备 Active Directory 与之通信，并导出 IoT Security 需要与 IdP 通信的身份提供程序 (IdP) 元数据文件。

1. 使用以下 URL 配置 IdP，将 `tenant-id` 变量替换为自己的租户 ID，这是 IoT Security 门户 URL 的第一部分：

   ```
   https://tenant-id.iot.paloaltonetworks.com/login
   ```

   根据配置 IdP 的方式，将其指向 IoT Security 元数据 URL 以检索所有必要的数据，或者单独输入信息。

   - **Assertion Consumer Service (ACS)** — 这是 IdP 发送身份验证断言以响应用户身份验证请求的目的。

     ```
     https://tenant-id.iot.paloaltonetworks.com/v0.3/zauth/saml2_sso/acs
     ```

   - **Entity ID**（实体 **ID**）— 这是唯一标识 Zingbox SP 的 URL。

     ```
     https://tenant-id.iot.paloaltonetworks.com/v0.3/zauth/saml2_sso/metadata
     ```

   - **Palo Alto Networks Metadata**（**Palo Alto Networks** 元数据）— 此文件包括 ACS URL 和实体 ID 以及其他参数，如公共 Security Assertion Markup Language (SAML) 2.0 加密密钥。

     ```
     https://tenant-id.iot.paloaltonetworks.com/v0.3/zauth/saml2_sso/metadata
     ```

   要查看包含特定租户 *ID* 的 *URL*，请执行下一节中的步骤 *1-2*，然后复制服务提供商 *(SP)* 配置详细信息部分中的 *URL*。

2. 复制并保存 IoT Security 可以从您的 SSO 身份验证系统导入 IdP 元数据文件的网址，或者下载该文件并将其保存为 XML 格式。您稍后会将其导入IoT Security 门户。

STEP 2 | 准备 IoT Security 以使用外部管理的 SSO。

1. 以所有者身份登录 IoT Security 门户，导航至 **Administration**（管理） > **User Accounts**（用户帐户），然后 **Manage SSO**（管理 **SSO**）。

   Palo Alto Networks 是默认的 SSO 身份提供程序 (IdP)，用于验证访问 IoT Security 门户的用户并为其分配用户角色。

2. 要添加用户配置的 SSO，请**Add New SSO**（添加新的 **SSO**），然后在出现的单一登录配置对话框中输入以下内容：

   Name（名称）：输入 SSO 的名称。最多可包含 16 个字符。此名称将显示在登录页面上，如下面的预览所示。

   Logo (Optional) [徽标（可选）**]**：上传一个显示在登录页面的 SSO 名称旁的图像文件，如预览所示。图像文件最大可达 2 MB，并且必须为 .bmp、.jpg 或 .png 格式。

   IdP Metadata（**IdP** 元数据）：输入之前复制并保存的 IdP 元数据文件的 URL，或者单击 **Choose file**（选择文件），导航至从身份验证系统导出的 XML 文件，然后选择该文件。

3. 验证 **IdP** 元数据 **URL** 或上传的文件。

   验证 IdP 元数据 URL 将激活 **Save**（保存）和 **Test**（测试）按钮。

4. 配置以下设置以标识要让 Active Directory 授权其用户的 AD 用户组。如果将其留空，IoT Security 会在本地对其授权。

   Attribute to get AD Groups（获取 **AD** 组的属性）：在 SAML 2.0 响应中输入标识 Active Directory 中的用户组的属性。

   AD Group Format（**AD** 组格式）：选择属性的格式为 **Plain Text**（纯文本）或 **Regular Expression**（正则表达式）。这些是IoT Security如何将 AD 用户组映射到 IoT Security 用户角色。

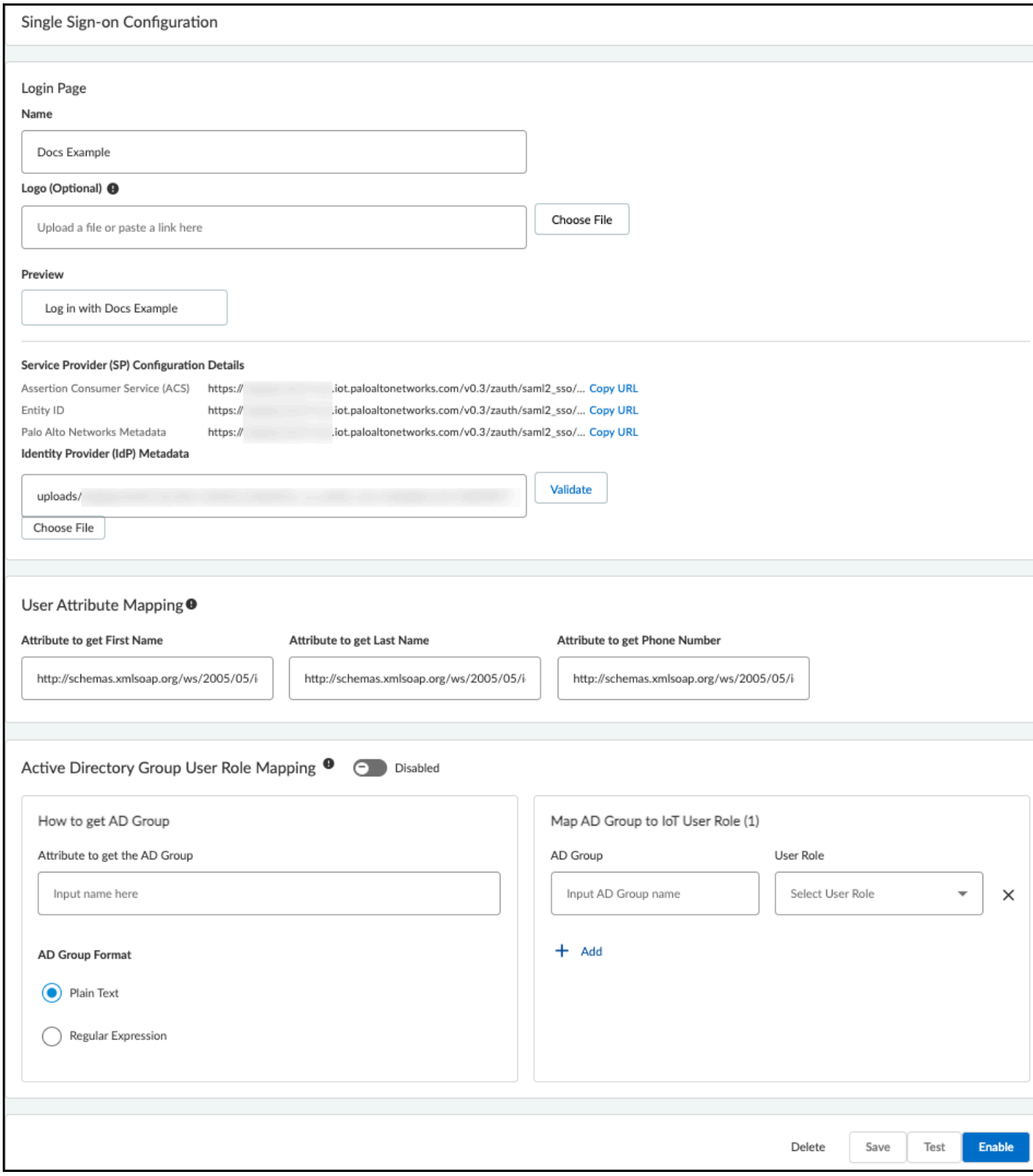
   Plain Text（纯文本）使用在 **Attribute to get AD Groups**（获取 **AD** 组的属性）中指定的精确值。例如，如果 **AD Group Format**（**AD** 组格式）为 **Plain Text**（纯文本），而 **AD Group**（**AD** 组）为 医院管理员，则IoT Security仅将名为医院管理员 的 AD 组中的用户映射到指定的 IoT Security 角色。

   Regular Expression（正则表达式）标识包含 **Attribute to get AD Groups**（获取 **AD** 组的属性）中指定的值的任何用户组。例如，如果 **AD Group Format**（**AD** 组格式）为 **Regular Expression**（正则表达式），而 **AD Group**（**AD** 组）为 **`OUI=Hospital*`**，则IoT Security将组织单位标识符 (OUI) 包括 **`Hospital`** 的任何 AD 组中的用户（如 **`OUI=Hospital Administrator`** 和 **`OUI=Hospital NetSec`**）映射到一个或多个指定的 IoT Security 角色。

   AD Group（**AD** 组）和 **User Role**（用户角色）：输入 Active Directory 组的名称，然后选择要将其映射到的 IoT Security 用户角色：**Owner**（所有者）、**Administrator**（管理员）或 **Read Only**（只读）。单击 **+** 以添加更多 AD 组到用户角色映射。您最多可以创建 50 个映

射。单个 AD 组无法映射到多个 IoT Security 用户角色，但多个 AD 组可以映射到同一个 IoT Security 用户角色。

有关 *IoT Security* 用户角色的信息，请参阅IoT Security 的用户角色。



5. **Save**（保存）SSO 配置。
6. **Test**（测试）SSO 配置。

   IoT Security 会打开一个小窗口，使用身份验证系统登录。
7. 测试完成后，单击 **Confirm**（确认）。
8. **Enable**（启用）SSO 配置。
9. 启用配置后，**Enable**（启用）按钮将更改为 **Disable and Edit**（禁用和编辑）。

使用任何 SSO 对用户进行身份验证，并在 IoT Security 门户中管理用户角色

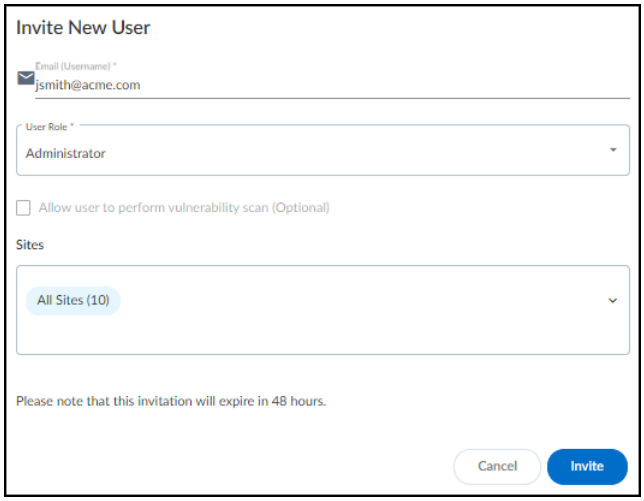
为外部 SSO 身份验证系统中的用户帐户（Palo Alto Network SSO 和客户管理的 SSO）设置用户角色，但您也可以使用所有者权限登录 IoT Security 门户，并为管理员和只读用户设置其他角色。如果外部管理角色和内部管理角色不同，IoT Security 会分配两者中权限较高者。因此，在 IoT Security 上，只能在内部设置高于外部所设置权限的用户角色；否则，将永远不会分配内部角色。按照从高到低的权限顺序，角色依次是所有者、管理员、只读用户。

如果外部 SSO 中的用户帐户未定义任何外部管理角色，则在具有所有者权限的本地用户为其设置内部管理角色并邀请其登录 IoT Security 之前，这些用户将无法登录 IoT Security。

STEP 1 | 邀请在外部 SSO 上拥有帐户但没有外部管理角色的用户访问 IoT Security。

如果用户具有映射到 *IoT Security* 中角色的外部管理角色，则跳过此步骤。

1. 以拥有所有者权限的用户身份登录 IoT Security，选择 **Administration**（管理） > **User Accounts**（用户帐户），然后单击用户帐户表上方的 **Invite New User**（邀请新用户）图标 **(+)**。
2. 输入电子邮件地址，选择角色，包括 **Owner**（所有者）、**Administrator**（管理员）或 **Read only**（只读），指定用户可以访问的网站，然后 **Invite**（邀请）用户。



IoT Security 会自动生成带有登录链接的电子邮件并将其发送给用户。

邀请发送后 *48* 小时内有效。

当电子邮件收件人单击电子邮件中的链接时，他/她将被引导至登录页面。用户单击 **Log in with <sso-name>**（使用 **h <sso-name>** 登录）按钮即可通过 SSO 登录。用户登录后，IoT Security 将授予他/她使用您指定的本地角色的访问权限。

3. 如果要邀请更多用户，请对每个用户重复前面的步骤。

STEP 2 | 查看用户、其外部管理角色、角色提供程序和内部管理角色以及他们可以访问的站点。

您可以在 Hub 的访问管理页面上查看用户及其角色的列表，如果您以所有者权限登录，则可以在 IoT Security 门户的用户帐户页面 [**Administration**（管理） > **User Accounts**（用户帐户）]上看到用户及其角色的列表。

Externally Managed Role（外部托管角色）和 **Role Provider**（角色提供程序）：如果 IoT Security 应用在外部 SSO 身份验证系统上设置的用户角色，则该角色将显示在“外部托管角

色”列中，SSO 名称将显示在“角色提供程序”列中。如果 IoT Security 具有与其外部管理角色相同或更高的用户内部管理角色，则应用内部管理角色。在这种情况下，这两列为空。

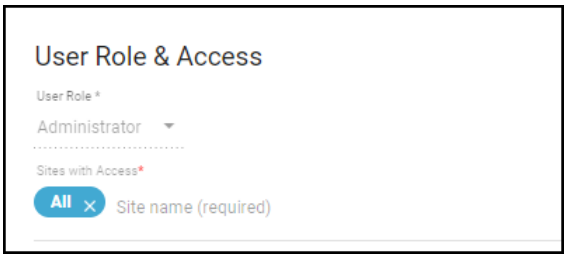
Internally Managed Role（内部管理角色）：此列列出在 IoT Security 中定义的用户角色。只有在内部没有定义角色时才为空。

在客户支持门户和 *Hub* 中创建用户帐户后，在用户登录 *IoT Security* 门户之前，该帐户不会显示在 *IoT Security* 门户中的 ***Administration***（管理）***> User Accounts***（用户帐户）页面上。

STEP 3 | 分配具有内部管理角色的用户。

1. 以所有者权限登录 IoT Security 门户时，单击 **Administration**（管理）**> User Accounts**（用户帐户），然后单击电子邮件（用户名）列中的管理员或只读用户条目。

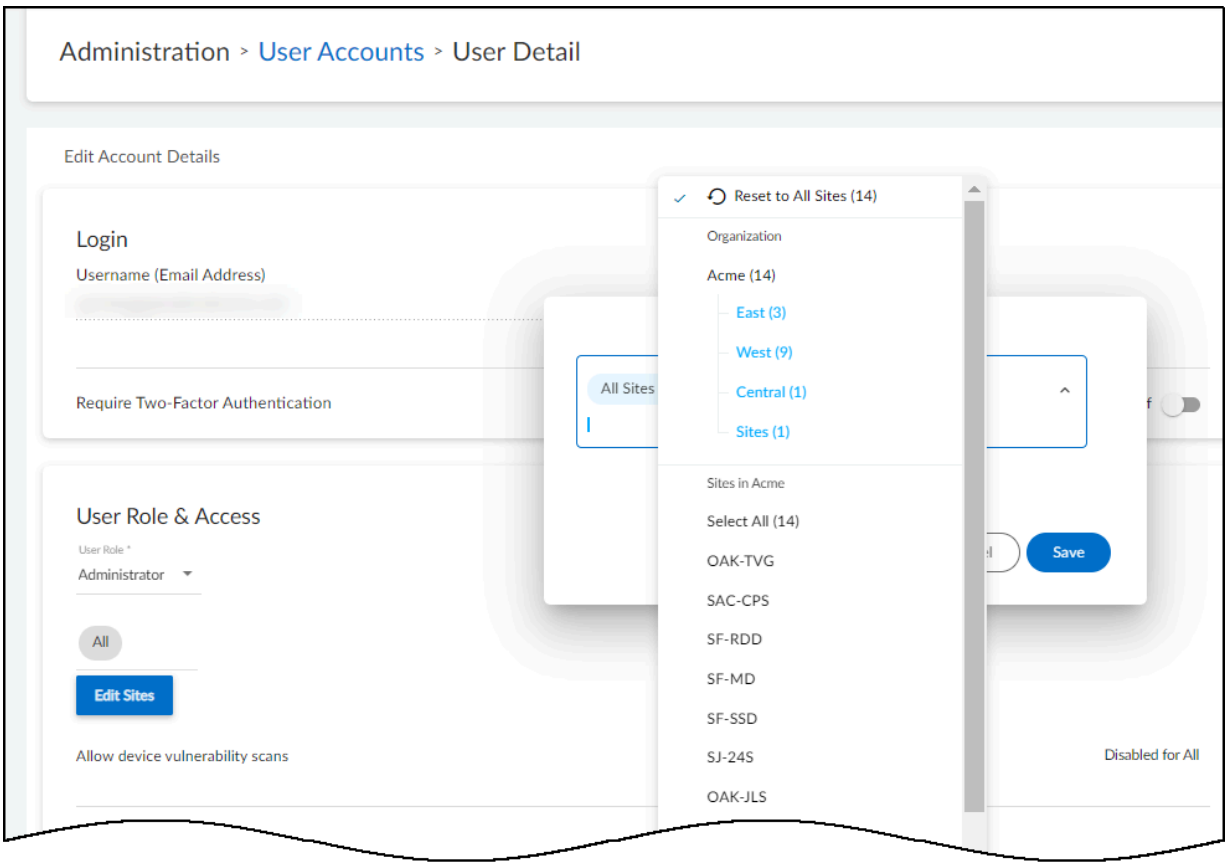
   此时将打开“用户角色和访问权限”对话框。



2. 从“用户角色”下拉列表中选择其他角色。当同一用户有不同的外部和内部管理角色时，IoT Security 将应用具有更高权限的角色。因此，在设置内部角色时，请选择高于外部 SSO 身份验证系统分配的角色。

STEP 4 | 确定管理员或只读用户可以访问哪些站点。

默认情况下，所有用户都可以访问所有站点。要授予用户访问站点子集的权限，请单击“全部”标签中的 **x**，然后选择要允许访问的站点或站点组的名称。



有关站点组以及如何使用它们控制用户可以访问哪些数据的信息，请参阅站点和站点组。

STEP 5 | 完成后，**Save**（保存）配置更改。

用户下次登录时，将仅具有内部管理角色的权限以及访问选定站点的设备和数据的权限。

IoT Security 的用户角色

基于角色的访问控制 (RBAC) 使您能够通过角色分配为管理用户分配特权和访问权限。您可以在客户支持门户 (CSP) 中创建用户帐户，在 Hub 为他们分配角色，并限制他们可以在 IoT Security 门户中通过站点访问的数据。有关为 IoT Security 创建用户的分步说明，请参阅创建 IoT Security 用户。

IoT Security 支持以下用户角色：

- 应用程序管理员
- 实例管理员
- 所有者
- 管理员
- 只读

应用程序管理员和实例管理员是每个 Palo Alto Networks 产品应用程序可用的常见角色。为 IoT Security，它们提供与所有者相同的权限。要了解有关它们的更多信息，请参阅可用角色.

专门针对 IoT Security 门户的三个用户角色是“所有者”、“管理员”和“只读”。

用户角色	角色定义	存取控制
所有者 （兼任应用管理员和实例管理员）	访问 IoT Security 门户	作为管理员的所有读/写权限以及： • 设置全局空闲超时 • 将设备到站点分配方法从基于防火墙位置的方法更改为基于 IP 地址的方法 • 查看所有用户的审核日志 • 为每个管理员帐户设置扫描权限 • 控制具有管理员和只读权限的用户可以访问哪些网站 • 控制谁会接收安全警报和系统警报的通知
管理员	访问 IoT Security 门户	创建、编辑和删除 IoT Security 配置并管理自己的帐户首选项： • 查看他们自己的用户角色和他们可以访问的网站列表

用户角色	角色定义	存取控制
		• 创建、下载和删除 API 访问密钥 • 更新联系信息 • 如果访问多个部署，请修改其登录首选项 • 缩短空闲超时 • 启用和禁用警报声音 • 启用和禁用通过短信和电子邮件发送的警报通知 • 管理自己的用户帐户首选项 • 请参阅他们自己的活动的审核日志
只读	只能查看 IoT Security 门户	• 查看可访问的网站的 IoT Security 数据 • 管理自己的用户帐户首选项 • 请参阅他们自己的活动的审核日志

对于具有 Panorama 管理的 Prisma Access 租户，该租户具有 IoT Security 附加许可证，添加以下类型的用户，以授予他们对 Prisma Access 和 IoT Security 的访问权限：

Prisma SASE 平台用户角色	**IoT Security** 用户角色
超级用户、MSP 超级用户	所有者
不适用	管理员*
仅查看管理员	只读

* *Prisma SASE* 中没有映射到 *IoT Security* 中 *Administrator* 角色的用户角色。

对于截至 2022 年 8 月由 Panorama 管理的 Prisma Access 的新客户，或已将 Prisma Access 实例过渡到 Prisma SASE 平台的现有 Panorama 管理的 Prisma Access 客户，请使用用于管理用户访问权限、角色和服务帐户的常用服务：身份与访问权限。

对于现有的 Panorama 托管 Prisma Access 客户，其 Prisma Access 实例尚未过渡到 Prisma SASE 平台，您可以继续使用创建管理用户的现有流程，直到过渡完成。