Tenable OT Security 3.16 用户指南

上次修订日期：2024 年 4 月 5 日

目录

欢迎使用 Tenable OT Security

Tenable OT Security 功能

Tenable OT Security (OT Security)(原名 Tenable.ot) 可以保护工业网络，使其免受网络威胁、恶意内部人员和人为错误的影响。无论是威胁检测和缓解，还是资产追踪、漏洞管理、配置控制和主动查询检查，OT Security 的 ICS 安全功能都能最大程度提高运营环境的可见性、安全性和可控性。

OT Security 可为 IT 安全人员和 OT 工程师提供全面的安全工具和报告。它可针对融合式 IT/OT 领域和 ICS 活动提供可见性，并助您在单一管理平台中了解所有站点及其各自的 OT 资产(从 Windows 服务器到 PLC 背板) 的态势。

OT Security 具有下主要功能：

- **360 度可见性**：攻击可以在 IT/OT 基础设施中轻易扩散。可以借助单一平台管理和度量 OT 和 IT 系统面临的网络安全风险，以便全方位了解融合攻击面。此外，OT Security 还可在本地与 IT 安全和运营工具相集成，例如安全信息和事件管理 (SIEM) 解决方案、日志管理工具、新一代防火墙以及工单系统。这样便构建了一个生态系统，所有安全产品均可在此系统中作为一个整体协同工作，确保所处环境安全无虞。
- **威胁检测和缓解**：OT Security 利用多元检测引擎查找可能会影响 OT 运营的高风险事件和行为。这些引擎包括策略、行为和基于签名的检测。
- **资产清单和主动检测**：OT Security 利用专利技术，同时在网络级别和设备级别，针对基础设施提供可见性。它使用本机通信协议查询 ICS 环境中的 IT 和 OT 设备，以便识别网络中正在发生的所有活动和操作。
- **基于风险的漏洞管理**：利用全面且详细的 IT 和 OT 资产追踪功能，OT Security 可以使用 ICS 网络中的每项资产的预测优先级分析功能生成漏洞和风险级别。这些报告包括风险评分和详细见解，以及缓解措施建议。
- **配置控制**：OT Security 提供了设备配置随时间变化的完整历史记录，包括特定梯形逻辑段、诊断缓冲区、标签表等细分记录。这使得管理员能够建立带有“上一个经过确认的良好状态”的备份快照，从而加快恢复并遵守业内法规。

提示：《*Tenable OT Security 用户指南*》和 Tenable OT Security 用户界面提供英语、日语、德语、法语和简体中文版本。要更改用户界面语言，请参阅“本地设置”。

有关 Tenable OT Security 的更多信息，请查看以下客户教育材料：

- Tenable OT Security 简介 (Tenable University)

OT Security 技术

OT Security 综合解决方案包含两种核心收集技术：

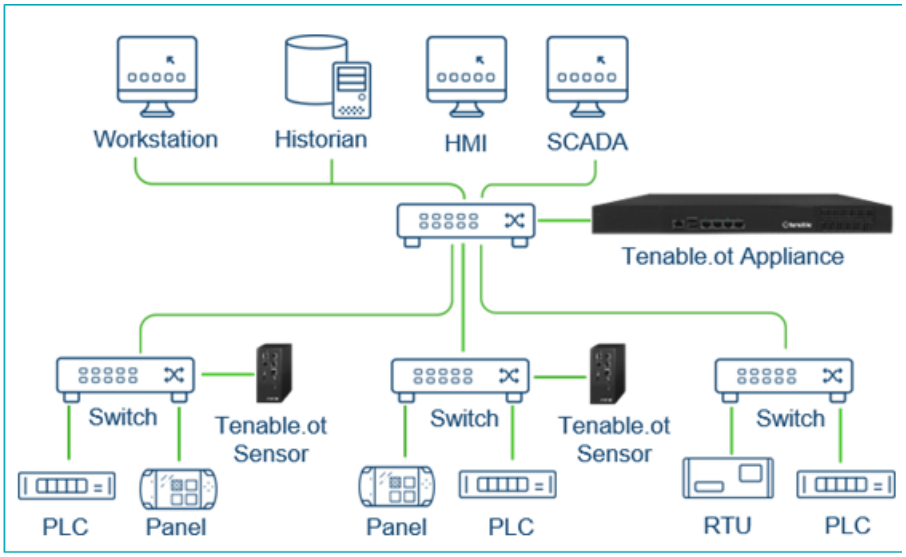
- **网络检测**：OT Security 网络检测技术是一种被动式深度数据包检查引擎，用于应对工业控制系统的独特特性和要求。网络检测可对通过运营网络执行的所有活动提供深入实时可见性，并且侧重于工程活动。相关活动包括通过供应商特定的专有通信协议执行的固件下载/上传、代码更新和配置更改。网络检测可针对可疑/未经授权的活动发出实时警报，并生成包含鉴定数据的综合事件日志。网络检测可以生成三种类型的警报：
  - **基于策略**：可以激活预定义策略或创建自定义策略，此类策略可将指示网络威胁或操作错误的具体精细活动列入允许列表和/或阻止列表，以便触发警报。此外，还可以设置策略来针对预定义情境触发主动查询检查。
  - **行为异常**：系统会检测偏离网络流量基线（基于规定时间范围内的流量模式建立）的情况。它还可以检测表示恶意软件和侦查行为的可疑扫描。
  - **签名检测策略**：这些策略使用基于签名的 OT 和 IT 威胁检测，来识别表示入侵威胁的网络流量。此类检测基于已在 Suricata 威胁引擎中编目的规则。
- **主动查询**：OT Security 的专利查询技术可以通过定期调查 ICS 网络中控制设备的元数据，来监控网络上的设备。此功能强化了 OT Security 自动发现和分类所有 ICS 资产的能力，其中包括 PLC 和 RTU 等较低级别的设备，即使这些资产在网络中未处于活动状态亦是如此。该功能还可识别设备元数据中本地实施的变更（例如固件版本、配置详细信息和状态），以及设备逻辑的每个代码/功能块中的变更。该功能在本机控制器通信协议中使用只读查询，因此不仅安全而且对设备没有影响。可以根据预定义的计划定期运行查询，也可以由用户按需运行。

解决方案架构

OT Security 平台组件

OT Security 解决方案包含这些组件：

- **OT Security**：此组件直接从网络（通过 SPAN 端口或网络分路器）和/或使用 Tenable OT Security 传感器 馈送的数据收集和分析网络流量 (OT Security 传感器)。OT Security 设备可以同时执行网络检测和主动查询功能。
- **OT Security 传感器**：这些是可在相关网段上部署的小型设备，最多可在每个托管的交换机部署一个传感器。传感器的规格有两种：紧凑型机架安装式或 DIN 导轨安装式。OT Security 传感器可以捕获、分析所有流量，然后将信息传送至 OT Security 设备，以确保相关网段的信息完整可见。您可配置传感器版本 3.14 及更高版本，令其向自身所处的网段发送主动查询。



网络组件

OT Security 支持与以下网络组件交互：

- **OT Security 用户（管理）**：您可以创建用户帐户，以便控制对 OT Security 管理控制台的访问权限。您可以借助浏览器 (Google Chrome) 通过安全套接字层身份验证 (HTTPS) 访问管理控制台。

注意：您需要使用最新版本的 Chrome 才能访问 OT Security 用户界面。

- **Active Directory Server**：可以选择使用 LDAP 服务器（例如 Active Directory）分配用户凭据。在这种情况下，可以在 Active Directory 中管理用户特权。
- **SIEM**：使用 Syslog 协议将 OT Security 事件日志发送到 SIEM。
- **SMTP 服务器**：OT Security 可通过 SMTP 服务器以电子邮件形式将事件通知发送给特定的员工组。
- **DNS 服务器**：将 DNS 服务器集成到 OT Security 中，以帮助解析资产名称。
- **第三方应用程序**：外部应用程序可以使用其 REST API 与 OT Security 交互，或使用其他特定集成访问数据[1]。

[1]例如，OT Security 支持与 Palo Alto Networks Next Generation Firewall (NGFW) 和 Aruba ClearPass 集成，从而使 OT Security 能够与这些系统共享资产清单信息。OT Security 还可以与 Tenable Vulnerability Management 和 Tenable Security Center 等其他 Tenable 平台集成。请在“**本地设置**”>“**集成**”下配置集成，详情请参阅“集成”。

系统元素

资产

资产是网络中的控制器、工程站、服务器等硬件组件。OT Security 的自动化资产发现、分类和管理功能可以通过持续跟踪对设备进行的所有更改，来提供准确的资产清单。这简化了维护操作连续性、可靠性和安全性的工作。它还在规划维护项目、确定升级优先级、补丁部署、事件响应和缓解工作中发挥关键作用。

风险评估

OT Security 利用复杂的算法来评估网络上每项资产所面临的风险程度。我们为网络中的每项资产提供了一个风险评分(从 0 到 100) 。风险评分基于以下因素：

- **事件**：网络中发生影响设备的事件(根据事件严重程度和发生时间远近进行衡量) 。

  > **注意**：根据时间远近衡量事件，如此一来，较新事件比较早事件对风险评分的影响更大。

- **漏洞**：影响网络资产的 CVE，以及在网络中发现的其他威胁(例如过时的操作系统、易受攻击协议的使用、易受攻击的已打开的端口等) 。在 OT Security 中，这些漏洞会被检测为针对资产的插件命中。

- **资产重要程度**：设备对系统正常运转重要程度的衡量方式。

  > **注意**：对于连接到背板的 PLC，共享该背板的其他模块的风险分数会影响 PLC 的风险评分。

策略和事件

策略可定义网络中发生的可疑、未授权、异常或值得注意的特定类型的事件。当发生满足特定策略的所有策略定义条件的事件时，OT Security 将生成事件。OT Security 会记录事件，并且会根据为该策略配置的策略操作发出通知。

策略事件有两种类型：

- **基于策略的检测**：在满足由一系列事件描述符定义的策略的精确条件时触发事件。
- **异常检测**：在网络中发现异常或可疑活动时触发事件。

系统具有一组预定义的策略（开箱即用）。此外，系统还提供编辑预定义策略或定义新自定义策略的功能。

基于策略的检测

对于基于策略的检测，您可以为系统中触发事件通知的事件配置特定条件。仅当满足策略的确切条件时，基于策略的事件才会触发。这可确保零误报，因为系统会针对 ICS 网络中发生的实际事件发出警报，同时提供有关“对象”、“事件”、“时间”、“地点”和“方式”的有用的详细信息。策略的制定依据可以是各种事件类型和描述符。

以下是一些可行策略配置的示例：

- **异常或未经授权的 ICS 控制平面活动（工程）**：HMI 不应查询控制器的固件版本（可能表示有攻击者进行了侦查），任何人也不应在运行期间对控制器进行编程（可能表示存在未经授权的潜在恶意活动）。
- **控制器代码变更**：已识别到控制器逻辑发生变更（“快照不匹配”）。
- **异常或未经授权的网络通信**：两个网络资产之间使用了未经允许的通信协议，或两个之前从未发生通信的资产之间发生了通信。
- **资产清单遭到异常或未经授权的更改**：发现了新资产或资产停止在网络中通信。
- **资产属性遭到异常或未经授权的更改**：资产的固件或状态属性发生更改。
- **设定点异常写入**：特定参数遭到更改，导致事件生成。用户可以定义参数的允许范围，并针对范围偏差生成事件。

异常检测

依靠用于检测与“正常”活动的偏差的系统内置功能，异常检测策略可以发现网络中的可疑行为。可用的异常检测策略如下：

- **网络流量基线偏差**：用户根据流量图定义指定时间范围内的“正常”网络流量的基线，并生成基线偏差警报。基线可随时更新。
- **网络流量激增**：检测到网络流量或对话数量急剧增加。
- **潜在的网络侦察/网络攻击活动**：针对指示网络中的侦查或网络攻击活动（例如 IP 冲突、TCP 端口扫描和 ARP 扫描）生成事件。

策略类别

按照以下类别整理策略：

- **配置事件策略**：这些策略与网络中发生的活动有关。配置事件策略有两个子类别：
  - **控制器验证**：这些策略与网络中的控制器发生的变更有关。这可能涉及控制器状态变更，以及固件、资产属性或代码块变更。可以限制策略用于特定计划（例如，工作日期间升级固件）和/或特定控制器。
  - **控制器活动**：这些策略与影响控制器状态和配置的特定工程命令有关。可以定义始终生成事件的特定活动，或指定用于生成事件的一组标准。例如，在某些时间和/或在某些控制器上执行某些活动。支持将资产、活动和计划列入黑名单和白名单。
- **网络事件策略**：这些策略与网络中的资产以及资产之间的通信流有关。这包括添加到网络或从网络删除的资产。它还包括网络的异常流量模式，或已被标记为引起特别关注的流量模式。例如，如果工程站用于与控制器通信的协议不属于预配置协议组（例如，由特定供应商制造的控制器使用的协议），则会触发事件。这些策略可限制用于特定计划和/或特定资产。为方便起见，特定于供应商的协议由供应商整理，而策略定义中可以使用任何协议。
- **SCADA 事件策略**：这些策略会检测设定点值的变更（可能会危害工业过程）。这些变更可能是网络攻击或人为错误所致。
- **网络威胁策略**：这些策略使用基于签名的 OT 和 IT 威胁检测，来识别表示入侵威胁的网络流量。此类检测基于已在 Suricata 威胁引擎中编目的规则。

组

OT Security 中策略定义的一个基本组件是使用组。配置策略时，每个参数均由组指定，这与独立实体相反。这极大地简化了策略配置过程。

事件

当发生满足某项策略的条件的事件时，系统中将生成事件。所有事件都会显示在“事件”屏幕上，也可以通过相关的“清单和策略”屏幕进行访问。系统为每个事件标记了严重程度级别，表明该事件所造成风险的程度。通知可以自动发送到生成事件的策略的策略操作中所指定的电子邮件收件人和 SIEM。

事件可由授权用户标记为“已解决”，并且支持添加注释。

OT Security 许可

本主题详细介绍了作为独立产品的 Tenable OT Security 的许可流程，解释了资产的计数方式，列出了可购买的附加组件，阐述了如何回收许可证，并描述了许可证超额使用或到期时会发生什么。如要了解如何使用 Tenable OT Security，请参阅《Tenable OT Security 用户指南》。

Tenable OT Security 许可

您可以购买订阅版或永久/维护版的 Tenable OT Security。

如要为 Tenable OT Security 申请许可，您需要根据组织的需求和环境详情购买许可证。然后，Tenable OT Security 会将这些许可证分配给您的资产，即所有具有 IP 地址的已检测设备，每个 IP 地址对应一个许可证。

当您的环境扩展时，资产数量也会相应增加，因此您需要购买更多许可证以适应这种变化。Tenable 许可证采用递进定价方式，即购买数量越多，单价就越低。如需了解价格，请联系您的 Tenable 代表。

资产计数方式

在 Tenable OT Security 中，许可证计数基于环境中唯一 IP 地址的数量。资产一旦被检测到即会获得许可。

Tenable OT Security 组件

您可以通过添加组件来自定义 Tenable OT Security 以适应您的使用案例。某些组件是您需要购买的附加组件。

购买随附	附加组件
• 虚拟 Core 设备。 • Tenable Security Center。	• Tenable OT Security Enterprise Manager。 • Tenable OT Security 可配置传感器。 • Tenable OT Security 认证的可配置传感器。 • Tenable OT Security 认证的 Core 平台。 • Tenable OT Security Core 平台。 • Tenable OT Security XL Core 平台。

回收许可证

购买许可证后，在合同有效期内，您的许可证总数保持不变，除非您购买更多许可证。但是，当您的资产数量发生变化时，Tenable OT Security 会实时回收许可证。

Tenable OT Security 会回收以下资产：

- 隐藏的资产
- 处于离线状态超过 30 天的资产
- 您在用户界面中删除或隐藏的资产

超出许可证限制

在 Tenable OT Security 中，除非购买更多许可证，否则您只能使用已分配的许可证数量。

当超出许可证限制时：

- 非管理员无法再访问 Tenable OT Security。
- 用户界面中会出现许可证已超出限制的消息。
- 无法再从 Tenable OT Security 设置中还原资产。
- 无法再更新漏洞插件或 IDS 签名（源更新）。

注意：即使许可证超出限制，Tenable OT Security 仍可检测和添加新资产。

提示：如要更新或重新初始化许可证，请参阅“OT Security 许可证工作流”。

许可证已到期

您购买的 Tenable OT Security 许可证在合同有效期内有效。在许可证到期前 30 天，用户界面中会显示警告。在此续约期间，请与您的 Tenable 代表合作，以添加或移除产品或更改许可证数量。

许可证到期后，Tenable OT Security 将被禁用，您无法再使用。

OT Security 硬件组件

OT Security 设备

组件	描述
电源指示灯	指示 OT Security 设备何时处于打开(绿色)或关闭状态。
控制台端口*	用于服务或本地访问。
USB 端口	用于对离线模式下的设备进行重新映像或升级。
以太网端口	用于连接到管理和运营网络的四个 GbE 端口,具体如下所述: 端口 1:默认情况下,此端口用于管理(用户界面)和作为主动查询端口(与网络资产通信)。可以更改此端口的配置(在安装期间和之后的"设置"页面中),以仅包含查询。这样做是为了将管理接口与控制器的网络分离。 端口 2:镜像端口 - 用作镜像会话 (SPAN) 的目标。此端口可接收网络流量的副本。此端口没有 IP 地址。 端口 3:如果启用了"端口分离"选项,则此端口仅用于管理(用户界面),且可连接到不属于控制器网络的某个网络。 端口 4:保留的端口,由 OT Security 的专业服务人员提供远程或本地支持。

*115200 bps 的传输速率,8N1 配置。

后面板

组件	描述

散热扇	两个散热扇。确保散热扇正常工作。
电源开关	打开/关闭开关。(按住几秒即可关闭电源)
电源端口	交流电接头;100 – 240 V 交流电

包装内容

组件	描述
两根以太网电缆	两根标准 RJ45 以太网电缆。使用这些电缆将 OT Security 设备连接到网络交换机。
电源端口	交流电源接头;100 – 240 V 交流电。
安装支架	2 个 1U 机架安装式支架。

OT Security 传感器

机架安装式传感器

注意:机架安装式传感器即将停产。相反,Tenable 现在会提供适配器套件,以便您能够将可配置传感器型号安装到机架上。

前面板

组件	描述
控制台端口*	用于服务或本地访问。
USB 端口	用于对离线模式下的设备进行重新映像或升级。
以太网端口	用于连接到管理和运营网络的四个 1 GbE 端口,具体如下所述: 端口 1 - 管理端口 - 用于管理设备。 端口 2:镜像端口 - 用作镜像会话 (SPAN) 的目标。此端口可接收网络流量的副本。此端口没有 IP 地址。 端口 3 - 未使用。 端口 4 - 未使用。

*115200 bps 的传输速率，8N1 配置。

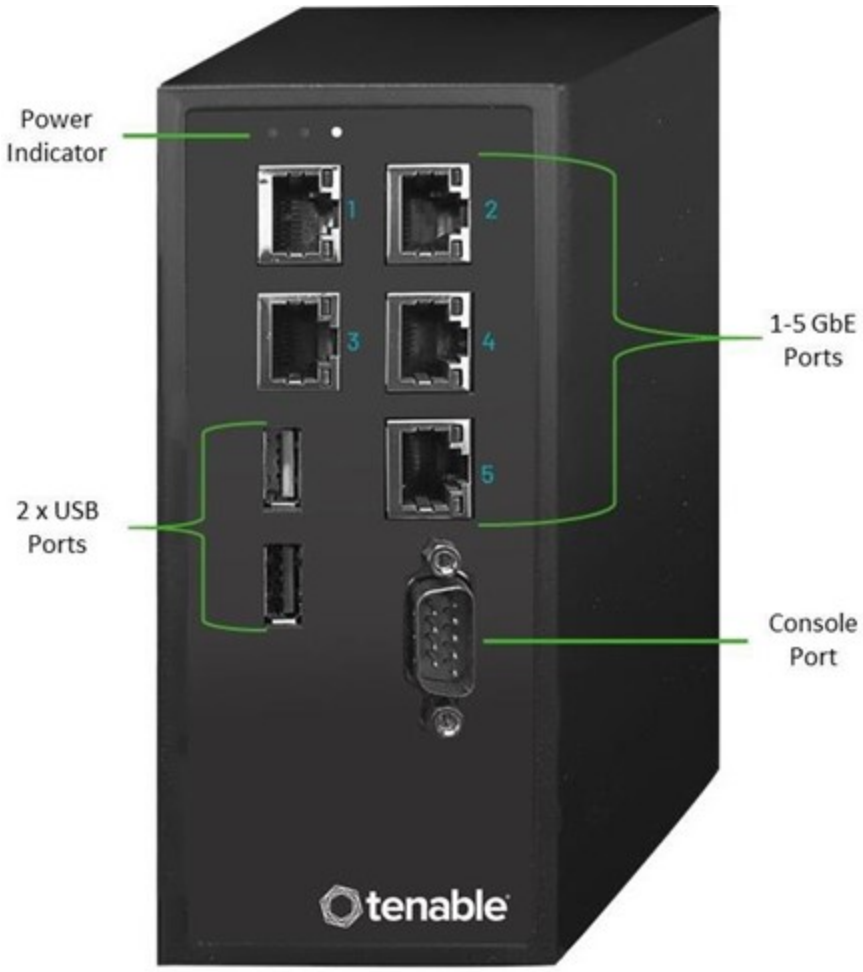
后面板

电源按钮	待机模式下为红色；开机模式下为绿色。
重置按钮	在不关闭电源的情况下重新启动系统。
电源开关	打开/关闭开关。（按住几秒即可关闭电源）
电源端口	交流电接头；100 – 240 V 交流电

包装内容

组件	描述
以太网电缆	一根标准 RJ45 以太网电缆。使用此电缆将传感器连接到网络交换机。
电源线	一根符合当地标准的交流电源线。
电源	60 W 交流电源适配器；100 – 240 V 交流电。
安装支架	2 个 1U L 形机架安装式支架。
螺丝包	

可配置传感器



注意:此型号可安装在 DIN 导轨上或安装机架上(使用适配器套件)。过去,此型号称为 DIN 导轨传感器。

前面板

组件	描述
电源指示灯	指示传感器何时处于打开(绿色)或关闭状态。
控制台端口*	用于服务或本地访问。
USB 端口	用于对离线模式下的设备进行重新映像或升级。

以太网端口	用于连接到管理和运营网络的五个 GbE 端口，具体如下所述： 端口 1 - 管理端口 - 用于管理设备。 端口 2：未使用。 端口 3：镜像端口 - 用作镜像会话 (SPAN) 的目标。此端口可接收网络流量的副本。此端口没有 IP 地址。 端口 4 - 未使用。端口 5：未使用。

*115200 bps 的传输速率，8N1 配置。

包装内容

组件	描述
电源线	一根符合当地标准的交流电源线。
电源	60 W 交流电源适配器；100 – 240 V 交流电。
以太网电缆	一根标准 RJ45 以太网电缆。使用此电缆将传感器连接到网络交换机。
安装式挂耳	2 个 1U L 形机架安装式支架（“挂耳”）。
螺丝包	

配置主动查询的端口

您可以在 Tenable Core 中为主动查询配置传感器端口。

若要更改传感器端口，请执行以下操作：

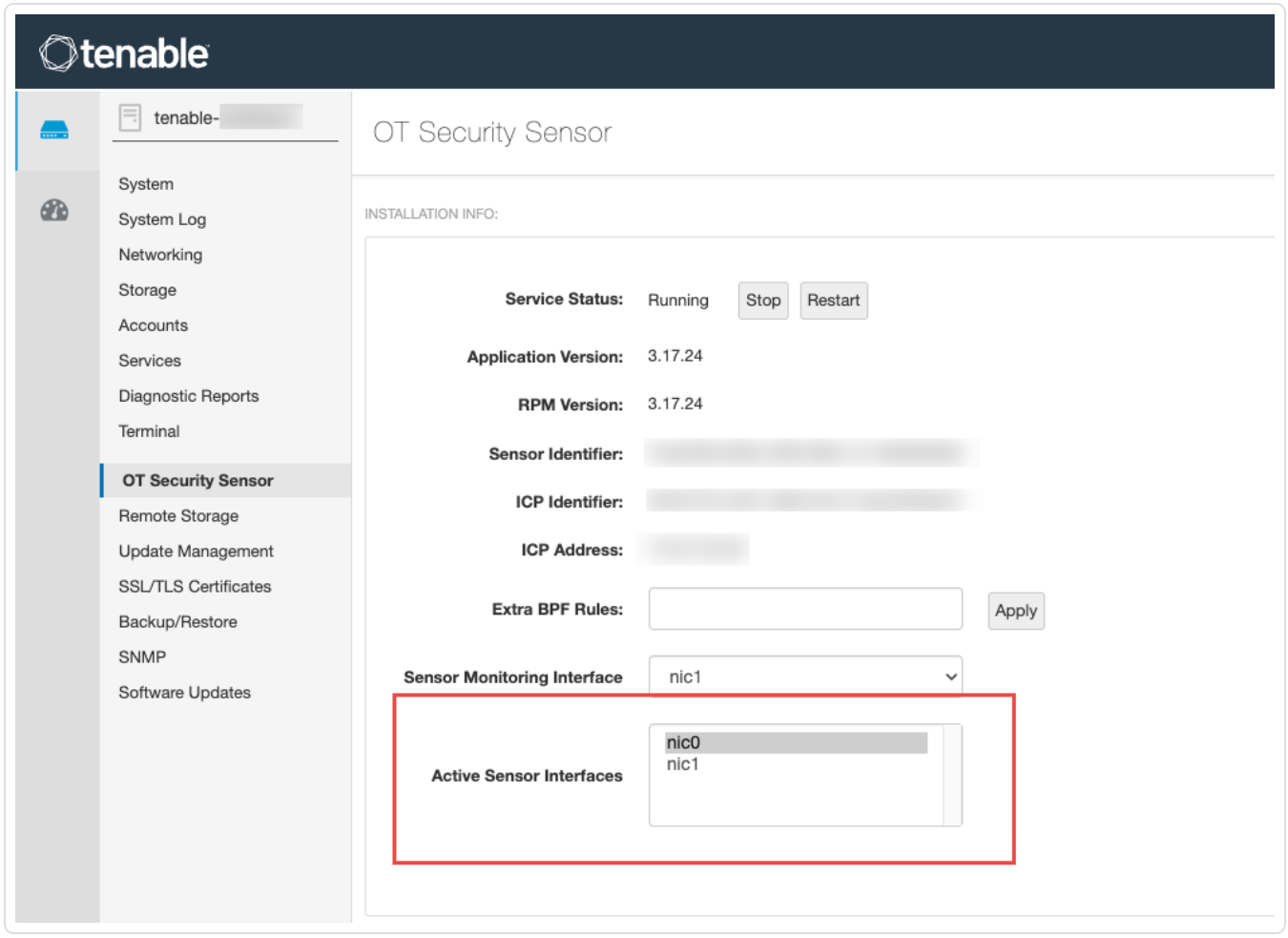
1. 在 Tenable Core 的左侧导航栏中，选择“**OT Security 传感器**”。

   此时会出现“**OT Security 传感器**”页面。

2. 在“**活动传感器接口**”框中，根据需要选择一个或多个端口。默认情况下，会选择“端口 1”。

   > **注意**：您可以在按住 **Ctrl** 键的同时单击以选择多个端口，以使用多个接口进行主动查询。例

如，当传感器连接到同一区域中的多个交换机或不可路由的网络时。



防火墙注意事项

在设置 OT Security 系统时，规划出保持打开状态的端口十分重要，这样做可以确保 Tenable 系统正确运行。下表指出哪些端口应保持打开状态，以与 OT Security Core 平台和 OT Security 传感器配合使用。还有一些表格显示了运行主动查询以及与 Tenable Vulnerability Management 和 Tenable Security Center 集成所需用到的端口。

OT Security Core 平台

以下端口应保持打开状态，以便与 OT Security Core 平台通信。

流向	端口	通信对象	目的
传入	TCP 443 和 TCP 28304	OT 传感器	传感器身份验证、配对和接收传感器信息。
传入	TCP 8000	Tenable Core 的 Web 界面	通过浏览器访问 Tenable Core
传入	TCP 28304	ICP/OT Security	传感器通信
传入	TCP 22	SSH 访问设备	对操作系统或设备执行命令行访问
传出	TCP 443	Tenable Security Center	发送用于集成的数据
传出*	TCP 443	cloud.tenable.com	发送用于集成的数据
传出*	各种工业协议	PLC/控制器	主动查询
传出*	TCP 25 或 587	用于发送警报的电子邮件服务器	SMTP(警报电子邮件、报告)
传出*	UDP 514	Syslog 服务器	发送策略事件警报和 syslog 消息
传出*	UDP 53	DNS 服务器	名称解析
传出*	UDP 123	NTP 服务器	时间服务
传出*	TCP 389 或 636	AD 服务器	AD LDAP 身份验证
传出*	TCP 443	SAML 提供程序	单点登录
传出*	UDP 161	SNMP 服务器	对 Tenable Core 进行 SNMP 监控
传出*	TCP 443	*.tenable.com	自动插件、应用程序和操作系统更新**

*可选服务

**可用的离线程序

OT Security 传感器

以下端口应保持打开状态，以便与 OT Security 传感器通信。

流向	端口	通信对象	目的
传入	TCP 8000	Web 界面	通过浏览器访问用户 GUI
传入	TCP 22	SSH 访问设备	对操作系统或设备执行命令行访问
传出*	TCP 25	用于发送警报的电子邮件服务器	SMTP(警报电子邮件、报告)
传出*	UDP 53	DNS 服务器	名称解析
传出*	UDP 123	NTP 服务器	时间服务
传出*	UDP 161	SNMP 服务器	对 Tenable Core 进行 SNMP 监控
传出	TCP 28303	ICP/OT Security 从传感器发送通信，在 ICP/OT Security 上接收	未经身份验证/仅被动传感器连接
传出	TCP 443 和 TCP 28304	ICP/OT Security 从传感器发送通信，在 ICP/OT Security 上接收	传感器和 ICP 之间经过身份验证/安全的隧道

*可选服务

主动查询

以下端口应保持打开状态，以便使用主动查询功能。

流向	端口	通信对象	目的
传出	TCP 80	OT 设备	HTTP 指纹识别
传出	TCP 102	OT 设备	S7/S7+ 协议
传出	TCP 443	OT 设备	HTTP 指纹识别
传出	TCP 445	OT 设备	WMI 查询
传出	TCP 502	OT 设备	Modbus 协议
传出	TCP 5432	OT 设备	PostgreSQL 查询
传出	TCP 44818	OT 设备	CIP 协议
传出	TCP/UDP 53	OT 设备	DNS
传出	ICMP	OT 设备	资产发现
传出	UDP 161	OT 设备	SNMP 查询
传出	UDP 137	OT 设备	NBNS 查询
传出	UDP 138	OT 设备	NetBIOS 查询

注意：设备使用的端口因供应商和产品线而异。有关确保主动查询成功所需的相关端口和协议的列表，请参阅“识别和详细信息查询”。

OT Security 集成

以下端口应保持打开状态，以便与 Tenable Vulnerability Management 和 Tenable Security Center 集成通信。

流向	端口	通信对象	目的
传出	TCP 443	cloud.tenable.com	Tenable Vulnerability Management 集成
传出	TCP 443	Tenable Security Center	Tenable Security Center 集成

识别和详细信息查询

您可以使用以下端口进行识别和详细信息查询：

注意：您可能需要打开防火墙上的端口，OT Security 或其传感器才能访问您的资产的相关端口。

端口	端口名称
21	FTP
80	HTTP
102	Step-7 / S7+
111	Emerson OVATION
135	WMI
161	SNMP
443	HTTPS
502	MODBUS / MMS
1911	Niagara FOX
2001	Profibus
2222	PCCC_AB-ETH
2404	IEC 60870-5
3500	Bachmann
4000	Emerson ROC
4911	Niagara FOX TLS
5002	Mitsubishi MELSEC
5007	Mitsubishi MELSEC
5432	PSQL / SEL

18245	SRTP
20000	DNP3
20256	PCOM
44818	EthernetIP / CIP
47808	BACNET (udp)
48898	ADS
55553	Honeywell CEE
55565	Honeywell FTE

安装 OT Security 设备

第 1 步：设置 OT Security 设备

您可以将 OT Security 设备安装在机架上，也可以直接将其放在平面上，例如桌面。

机架安装

若要将 OT Security 设备安装到标准（19 英寸）机架上，请执行以下操作：

1. 将服务器单元插入机架中可用的 1U 插槽。

   注意：
   - 确保机架接地。
   - 确保散热扇进风口（位于后面板上）和换气孔（位于顶板上）未被堵塞。

2. 使用适当的机架安装用螺丝（未提供），将机架安装式支架（已提供）固定到机架上，以便将装置安装到机架上。
3. 将提供的交流电源线插入后面板中的电源端口，然后将插头插入交流电源。

平面

若要在平面上安装 OT Security 设备，请执行以下操作：

1. 将设备放在干燥且平坦的表面（如桌面）上。

   注意：
   - 确保桌面平坦干燥。
   - 确保散热扇进风口（位于后面板上）和换气孔（位于顶板上）未被堵塞。
   - 如果将设备置于多个其他电子设备中，请确保散热扇（位于后面板上）后面有足够的空间，以便正常换气和散热。

2. 将提供的交流电源线插入后面板中的电源端口，然后将插头插入交流电源。

第 2 步：将 OT Security 连接到网络

OT Security 可同时用于网络监控和主动查询。

- **网络监控**：将设备连接到网络交换机上的镜像端口，该端口已连接到相应的控制器/PLC。
- **主动查询**：将设备连接到网络交换机上带 IP 地址的常规端口，且该端口已连接到相应的控制器/PLC。

在默认配置中，主动查询和管理控制台使用设备上的相同端口（端口 1）。但是，在初始设置后，您可以通过在端口 3 上配置管理，将管理端口与主动查询端口分离。完成此配置后，您可以将设备上的端口 3 连接到交换机上的常规端口，以执行 第 7 步：连接单独的管理端口（用于“端口分离”选项） 中所述的管理。

对于初始设置，将端口 1 连接到网络交换机上的常规端口，并将端口 2 连接到镜像端口。

若要将 OT Security 设备连接到网络，请执行以下操作：

1. 在 OT Security 设备上，将以太网电缆（已提供）连接到端口 1。
2. 将电缆连接到网络交换机上的常规端口。
3. 在设备上，将另一根以太网电缆（已提供）连接到端口 2。
4. 将电缆连接到网络交换机上的镜像端口。

第 3 步:登录管理控制台

若要登录管理控制台,

1. 请执行下列操作之一:

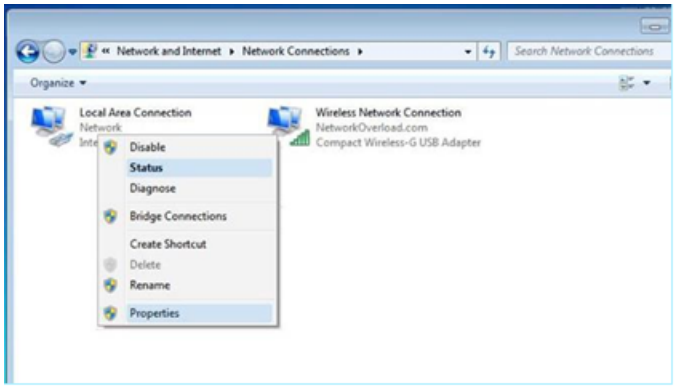
   - 使用以太网电缆将管理控制台工作站(例如 PC、笔记本电脑等)直接连接到 OT Security 设备的端口 1。
   - 将管理控制台工作站连接到网络交换机。

   注意:确保管理控制台工作站与 OT Security 设备(即 192.168.1.0/24)属于同一子网或可路由至此设备。

2. 若要设置静态 IP 以连接 OT Security 设备,请执行以下操作:

   a. 转至"**网络和 Internet**">"**网络和共享中心**">"**更改适配器设置**"。

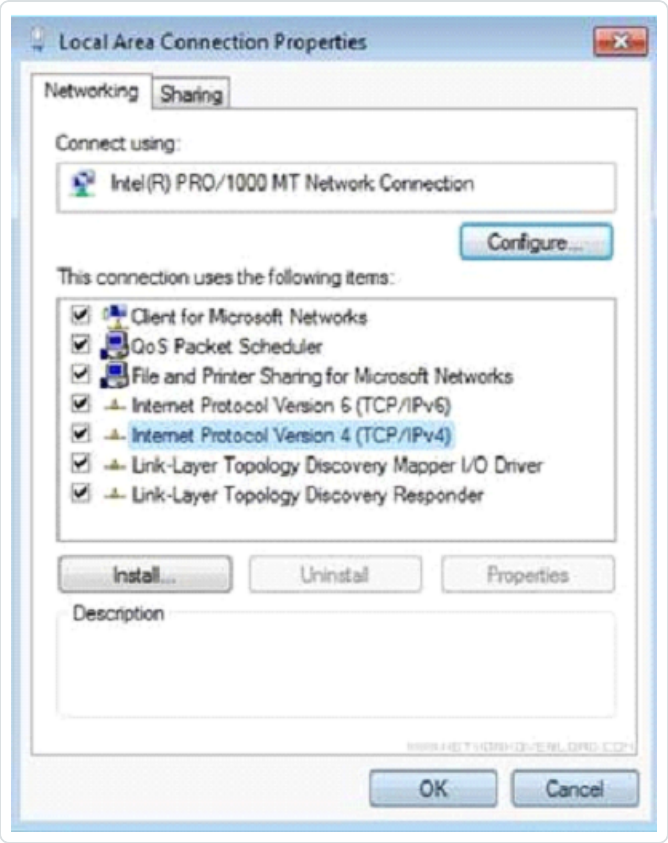
   此时会显示"**网络连接**"屏幕。

   注意:导航可能因 Windows 版本不同而略有差异。

   b. 右键单击"**本地连接**"并选择"**属性**"。

   此时会显示"**本地连接**"窗口。



c. 选择“**Internet 协议版本 4 (TCP/IPv4)**”，然后单击“**属性**”。

此时会显示“**Internet 协议版本 4 (TCP/IPv4) 属性**”窗口。

d. 选择“**使用下列 IP 地址**”。

e. 在“**IP 地址**”框中，输入“192.168.1.10”。

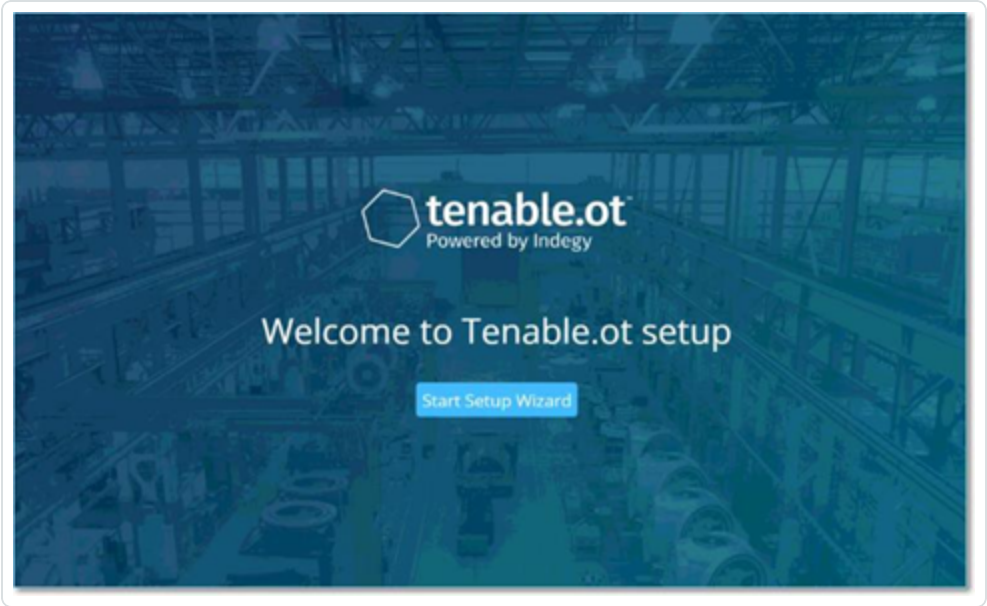
f. 在“**子网掩码**”框中，输入“255.255.255.0”。

g. 点击“**确定**”。

OT Security 会应用新设置。

3. 在 Chrome 浏览器中，导航至 https://192.168.1.5。

此时会打开安装向导的“**欢迎**”屏幕。



注意:您需要使用最新版本的 Chrome 才能访问用户界面。

4. 单击"**启动安装向导**"。

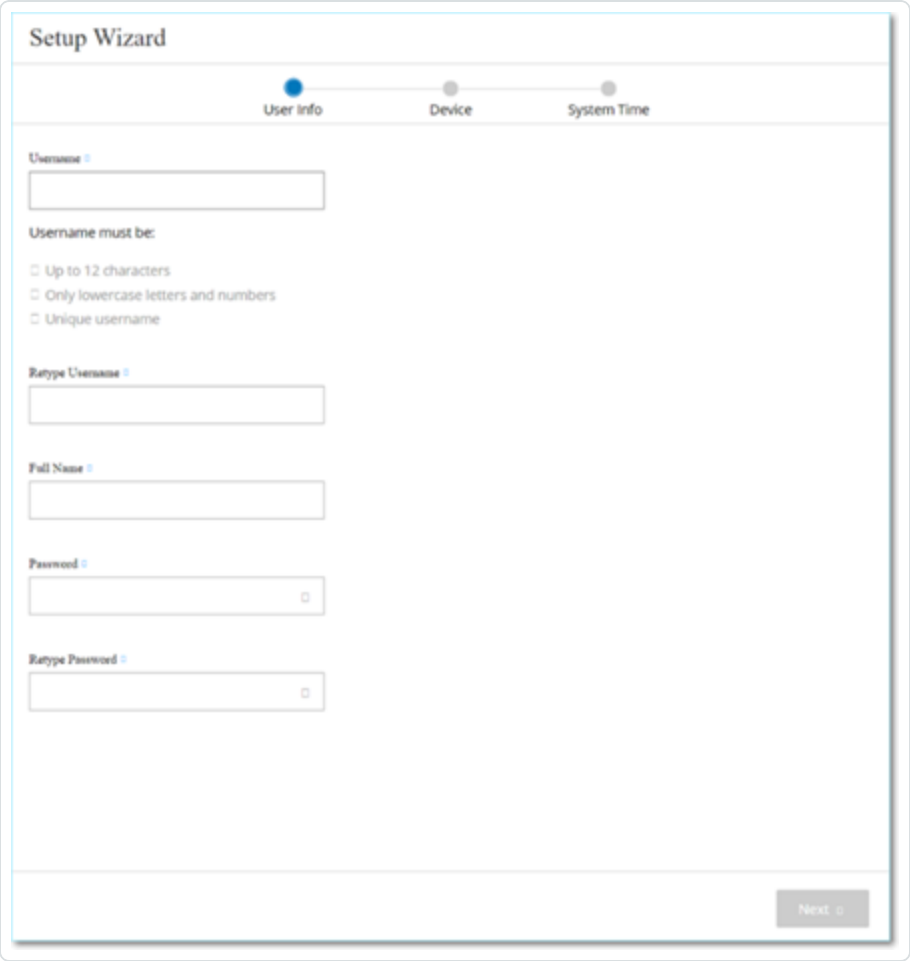
   安装向导打开,显示"**用户信息**"页。

第 4 步:安装向导

OT Security 安装向导将引导您完成配置基本系统设置的过程。

注意:如有必要,您后期可以在管理控制台(用户界面)的"**设置**"屏幕中更改配置。

用户信息



在"**用户信息**"页面上,填写您的用户帐户信息。

注意:在安装向导中,您需要配置管理员帐户的凭据。登录用户界面后,您可以创建其他用户帐户。有关用户帐户的更多信息,请参阅"用户和角色"部分。

1. 在“**用户名**”框中，输入用于登录系统的用户名。

   用户名最多可包含 12 个字符，且只能包含小写字母和数字。

2. 在“**重新输入用户名**”框中，重新输入用户名。
3. 在“**全名**”部分，输入完整的“**名字及姓氏**”。

   > **注意**：用户名将在系统的标题栏和活动日志中显示。

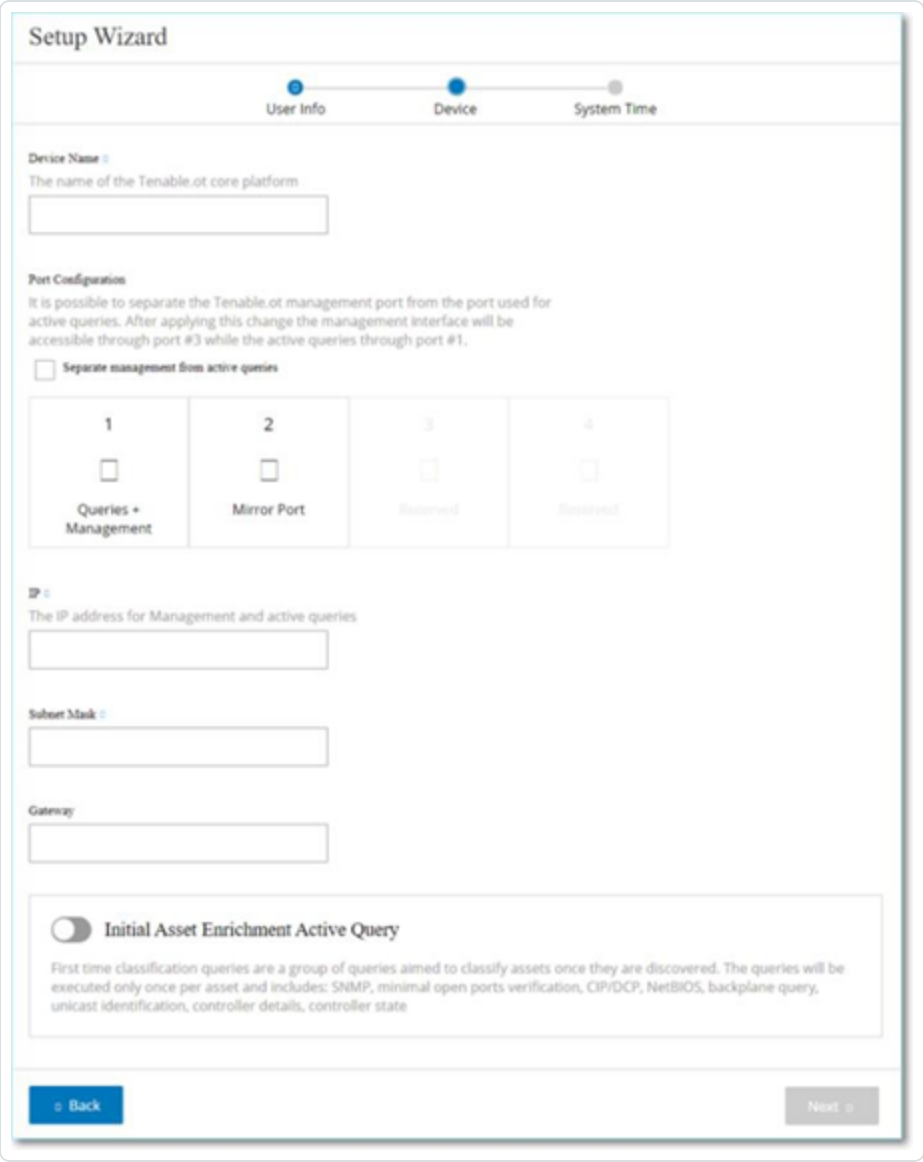
4. 在“**密码**”框中，输入用于登录系统的密码。该密码必须至少包含：

   - 12 个字符
   - 一个大写字母
   - 一个小写字母
   - 一个数字
   - 一个特殊字符

5. 在“**重新输入密码**”框中，重新输入相同的密码。
6. 单击“**下一步**”。

   此时会打开安装向导的“**设备**”页。

设备



在"**设备**"页面上，提供有关 OT Security 平台的信息：

1. 在"**设备名称**"框中，输入 OT Security 平台的唯一标识符。
2. 在"**端口配置**"部分，执行下列操作之一：

   - **端口分离**：您若希望将一个端口用于管理，并将另一个单独的端口用于查询，请选中"**管理端口与主动查询端口分离**"复选框。选择此选项会将端口 1 配置为仅查询端口并将端口 3 配置为仅管理端口。

     注意：在某些系统上，"端口分离"选项可能不可用。请联系支持代理获取帮助。

- **无分离**：若您希望在相同端口中维护查询和管理端口，请勿选中“**管理端口与主动查询端口分离**”复选框。在这种情况下，您可以跳过此程序的第 3-5 条说明，继续进行第 6 条说明。

3. 如果选择“**端口分离**”选项：

   a. 在“**主动查询 IP**”框中，输入设备查询端口的 IP 地址。

      此端口将连接到网络交换机上的常规端口，该端口可与控制器通信（即可路由至控制器）。由于 OT Security 会连接至控制器，因此需要用到网络子网内的 IP 地址。

   b. 在“**主动查询子网掩码**”框中，输入查询端口的子网掩码。

   c. 在“**主动查询网关**”框（可选）中，输入操作网络中网关的 IP 地址。

4. 在“**管理 IP**”框中，输入应用于 OT Security 平台的 IP 地址（在网络子网内）。

   该地址将成为 OT Security 管理 IP 地址。如果端口之间未分离，则此 IP 地址也会成为“查询”地址。

5. 在“**管理子网掩码**”框中，输入网络的子网掩码。

6. （可选）如果要设置网关，请在“**管理网关**”框中。输入网络的网关 IP。

   > **注意**：如果不提供管理网关 IP，OT Security 无法与电子邮件服务器、syslog 服务器等子网之外的外部组件通信。

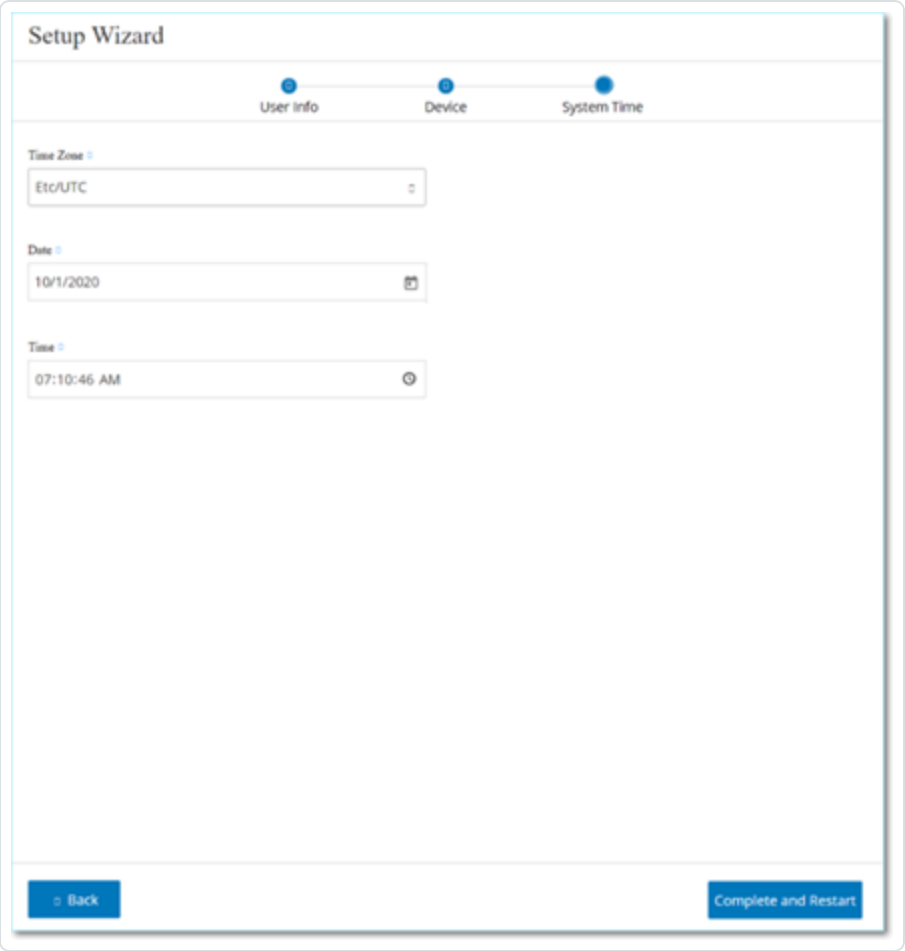
7. **初始资产扩充主动查询** 包含对系统中检测到的每项资产运行的一系列查询。

   这样做有助于 OT Security 对资产分类。若要对 OT Security 发现的每项新资产运行这些查询，请启用“**初始资产扩充主动查询**”切换开关。

8. 单击“**下一步**”。

   此时会打开安装向导的“**系统时间**”页。

系统时间

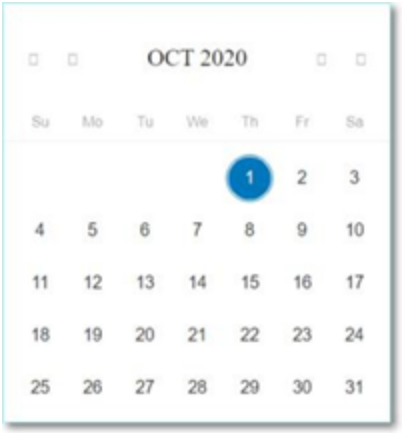


注意:设置正确的日期和时间对于准确记录日志和警报而言至关重要。

"**系统时间**"页会自动出现正确的时间和日期。如果不是,请执行以下操作:

1. 在"**时区**"下拉框中,选择站点位置的本地时区。
2. 在"**日期**"框中,单击日历图标 。

   随后会出现一个弹出式日历。



3. 选择当前日期。
4. 在“**时间**”框中，分别选择“小时”、“分钟”和“秒”、“上午/下午”，然后使用键盘或上下箭头输入正确的数字。

   > **注意**：如果您要编辑任何先前的安装向导页面，请单击“**返回**”。单击“**完成**并**重新启动**”后，将无法返回安装向导。但是，您可以在用户界面的“**设置**”页面更改配置设置。

5. 如要完成安装程序，请单击“**完成并重新启动**”。

   重新启动完成后，OT Security 会将您重定向至“**许可**”窗口。

第 5 步：许可

您必须激活 OT Security 许可证后才能激活系统。有关激活许可证的信息，请参阅“OT Security 许可证工作流”。

第 6 步：启用 OT Security 系统

完成许可证激活后，OT Security 将显示“**启用**”按钮。

您必须启用 OT Security 才能激活系统的核心功能，例如：

- 识别网络中的资产。
- 收集和监控所有网络流量。
- 记录网络中的“对话”。

您可以在用户界面的这些功能中查看编译的所有数据和分析。

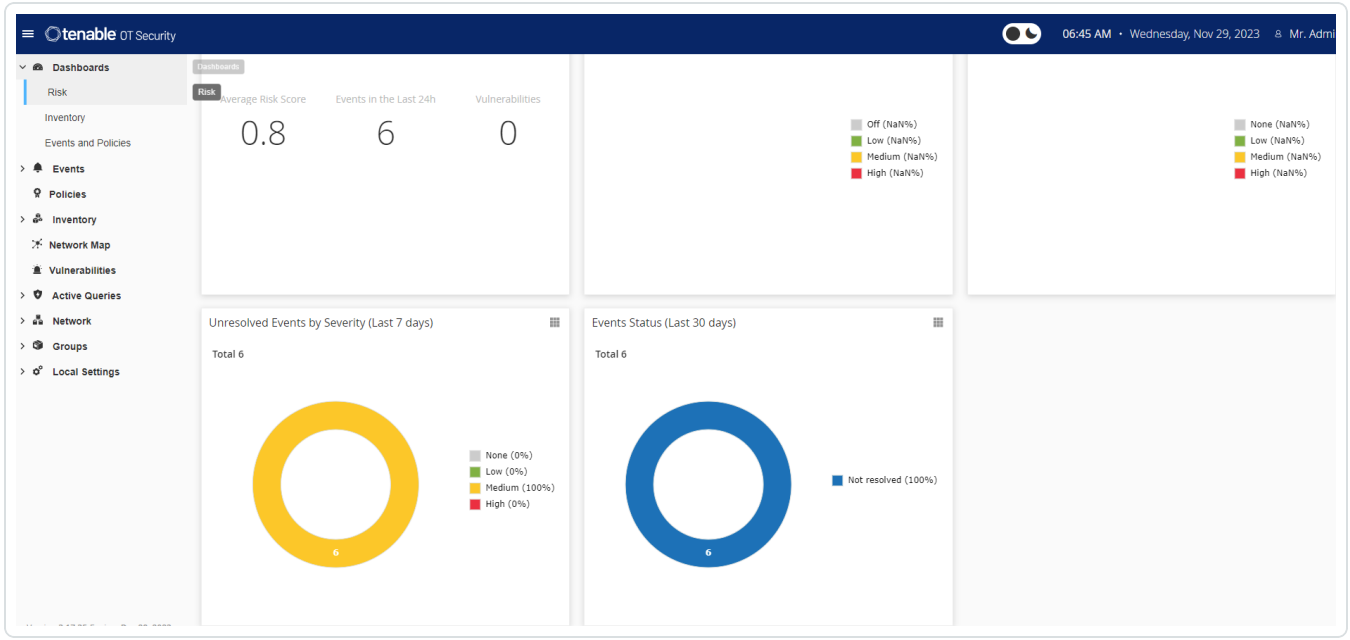
> **注意**：这些进程会持续进行，因此用户界面可能需要一些时间才能显示完全更新后的结果。

您可以在管理控制台（用户界面）的“**本地设置**”窗口上配置和激活“主动查询”等其他功能，详情请参阅“Active Queries”。

若要启用 OT Security，请执行以下操作：

1. 点击“**启用**”。

   OT Security 会启用系统并显示“**仪表盘**”>“**风险**”窗口。



注意:系统识别您的资产需要花几分钟的时间。您可能需要刷新页面才能让数据开始显示。

第 7 步:连接单独的管理端口(用于"端口分离"选项)

如果您已选择端口分离选项(以将"查询"与"管理"分离),则必须将 OT Security 设备上的端口 3(现为管理端口)连接到网络交换机上的端口。该交换机可以是不同类型的网络交换机,例如 IT 网络的网络交换机。

若要连接管理端口,请执行以下操作:

1. 在 OT Security 设备上,将以太网电缆(已提供)连接到端口 3。
2. 将电缆连接到网络交换机上的端口。

安装 OT Security 传感器

将传感器与 ICP 配对

注意：下一节会介绍配置传感器 3.14 及更高版本的步骤。如要配置较早型号的传感器，请按照 附录 1: 安装传感器(3.13 及更低版本) 中所述的程序进行操作。

要将传感器与 Industrial Core Platform (ICP) 配对，请同时使用 ICP 管理控制台和传感器的 Tenable Core 用户界面。

您可以选择启用自动批准传入的配对请求，或禁用自动批准，并允许对每个新的传感器配对请求仅进行手动批准。

开始之前

确保满足以下条件：

- 传感器硬件已正确安装(请参阅“设置传感器”) 。
- 传感器已连接到网络交换机(请参阅“将传感器连接到网络”) 。
- 传感器有专属的静态 IPv4 地址(请参阅“访问传感器安装向导”) 。
- 传感器已连接到 Tenable Core 平台，并且您已设置用于登录 Core 用户界面的用户名和密码。有关使用 Tenable Core 用户界面的更多信息，请参阅 https://docs.tenable.com/tenable-core/OT-security/Content/TenableCore/Introduction_OT.htm。
- ICP 控制台中的证书处于有效状态(请参阅证书) 。

注意：Tenable 建议创建拥有管理员权限的专用 ICP 用户来负责传感器配对过程，以防连接中断(请参阅“添加本地用户”) 。您可以添加新的管理员用户以与多个传感器配对。

注意：有关为 Tenable Core 计算机应用离线更新的信息，请参阅离线更新 Tenable Core。

将传感器配对

若要将 3.14 或更高版本的传感器与 ICP 配对，请执行以下操作：

1. 在 ICP 管理控制台(用户界面)中,导航至"**本地设置**">"**传感器**"窗口。

2. 如果要启用自动批准传感器配对请求,请确保将屏幕顶部的"**自动批准传入的传感器配对请求**"开关切换为"**打开**"。否则,所有配对请求都需要手动批准。

3. 打开新选项卡,让 ICP 选项卡处于打开状态,然后通过输入"**<Sensor IP>:8000**"来访问传感器的 Tenable Core 用户界面。

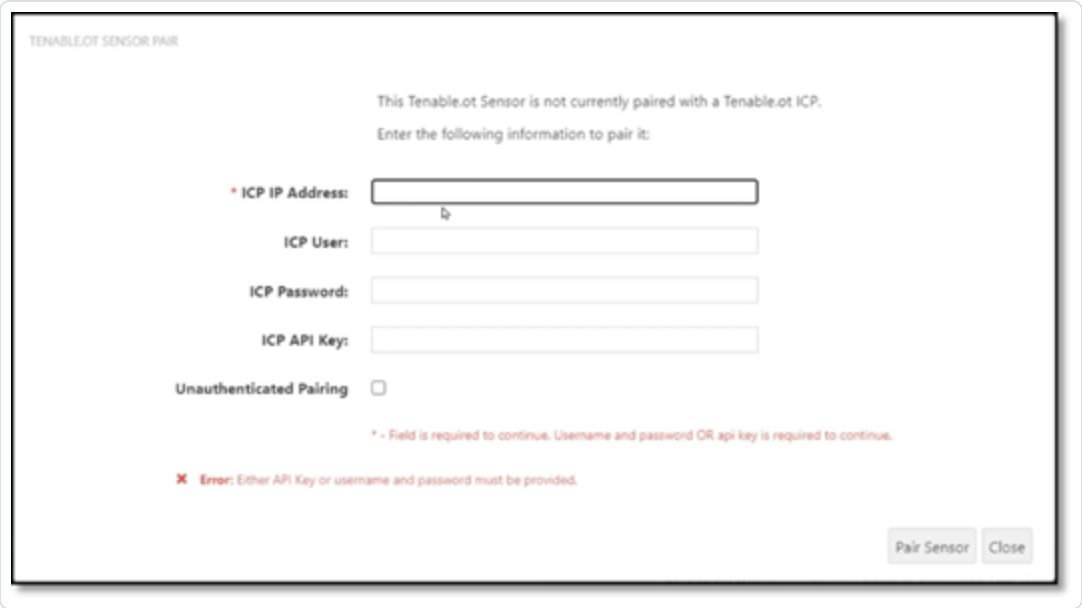
   注意:您需要使用最新版本的 Chrome 才能访问 Tenable Core 用户界面。

4. 在 Tenable Core 控制台登录窗口中,输入您的"**用户名**"和"**密码**",选中"**对特权任务重复使用密码**"复选框,然后单击"**登录**"。

   注意:如果您不选择"**对特权任务重复使用密码**",则无法重新启动传感器服务。

5. 在"导航"菜单栏中,单击"**OT Security 传感器**"。

   此时会出现"**OT Security 传感器配对**"窗口。



注意:"**Tenable OT Security 传感器配对**"窗口仅在首次加载页面时出现。要在此之后打开窗口,请单击 **Tenable Core** 控制台"**配对信息**"部分中的 按钮。

6. 在"**ICP IP 地址**"框中,输入要与此传感器配对的 ICP 的 IPv4 地址。
7. 若要使用未经身份验证(未加密)的配对,请选择"**未经身份验证的配对**"复选框并跳至第 8 步。

注意:使用**未经身份验证的配对**的传感器不仅只能被动扫描其网段,而且不能由 ICP 管理,所以无法发送主动查询。

8. 若要完成配对身份验证,请执行下列操作之一:
   - 在"**ICP 用户**"框中输入 ICP 用户名,在"**ICP 密码**"框中输入 ICP 密码。
   - 在"**ICP API 密钥**"框中,输入 ICP 的 API 密钥。

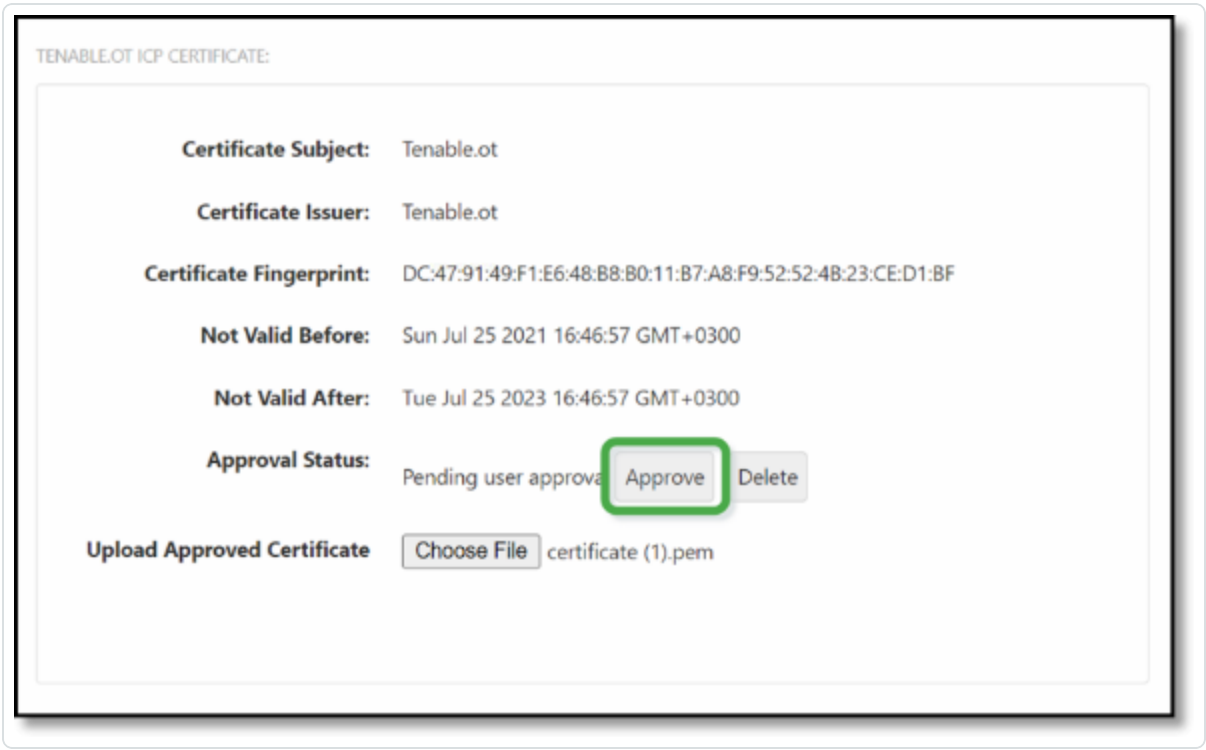
注意:Tenable 建议创建专用 ICP 用户来负责传感器配对,以确保在配对过程中不会发生连接中断(请参阅"添加本地用户")。

注意:使用用户名和密码的身份验证方法具有不会显示凭据的优点,这与 API 密钥不同,API 密钥最终会过期。

9. 单击"**配对传感器**"。

10. 如要使用 ICP 提供的证书，请执行以下操作：

    a. 在 **Tenable Core** 的“**Tenable ICP 证书**”部分的“**批准状态**”下，等待证书信息加载。



    b. 点击“**批准**”以批准该证书。

    c. 在“**确认接受 Tenable OT Security 服务器证书**”弹出窗口中，单击“**接受此证书**”。

    如果喜欢手动上传证书，请执行以下操作：

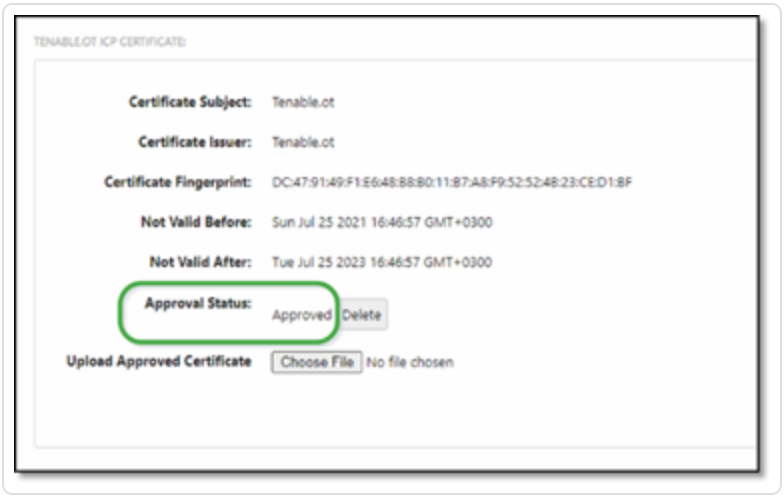
    a. 在 **Tenable ICP**控制台中，请按“生成 HTTPS 证书”中所述的步骤操作。

    b. 在 **Tenable Core** 的“**Tenable ICP 证书**”部分，单击“**上传已批准的证书**”下的“**选择文件**”。

    c. 导航到要上传的 `.pem` 证书文件。

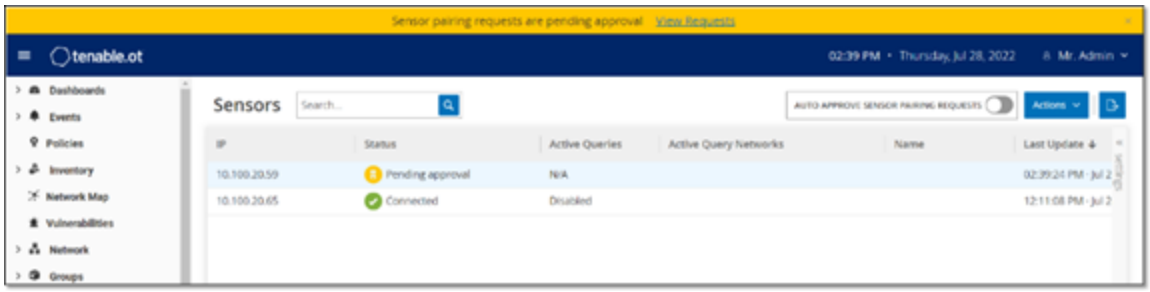
    正确接受有效的证书后，其在“**OT Security ICP 证书**”表中的“**批准状态**”会显示

为“**已批准**”。

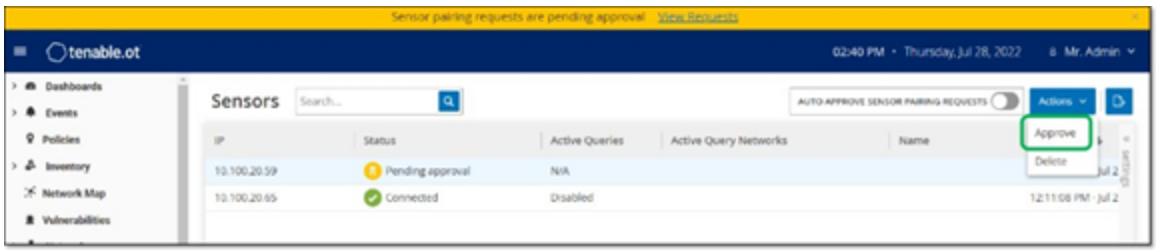


11. 在 ICP 用户界面中，导航至“**本地设置**”>“**系统配置**”>“**传感器**”。

    OT Security 会在表中显示新的传感器，**状态**为“**待批准**”。



12. 单击传感器行，然后单击“**操作**”（或右键单击该行）并选择“**批准**”。



如果**状态**切换为“**已连接**”，则表示配对成功。其他可能的状态包括：

- **已连接（未经身份验证）**：传感器处于已连接模式，但未经身份验证。传感器只能执行被动网络检测。
- **已暂停**：传感器已正确连接，但已暂停。

- **断开连接**：传感器未连接。对于经过身份验证的传感器，可能是因为配对过程中发生错误所致。例如，通道错误和 API 问题。
- **已连接（通道错误）**：配对成功，但通道上的通信不可操作。检查端口 28304 从传感器到 ICP 的连接。有关更多信息，请参阅“防火墙注意事项”。

13. 当 OT Security 将经过身份验证的传感器完成配对后，您便可以配置要在此传感器上运行的主动查询。请参阅“配置主动查询”。

    > **注意**：配对完成后，Tenable 建议您仅使用 ICP 页面而不是 Tenable Core 用户界面来管理传感器。

设置传感器

如“OT Security 传感器”部分所述，传感器有两种型号：机架安装式传感器和可配置传感器。机架安装式传感器可安装到标准的 19 英寸机架上，也可以放在平面上。可配置传感器可安装在 DIN 导轨上，或安装在标准的 19 英寸机架上（使用“安装式挂耳”适配器套件）。

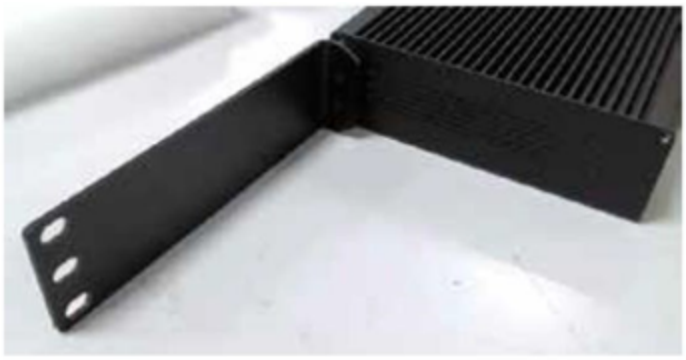
设置机架安装式传感器

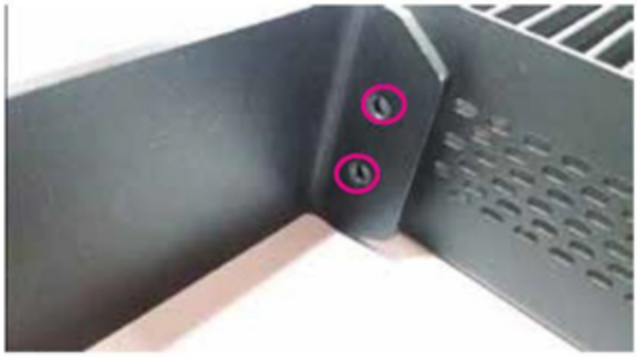
您可将传感器安装在标准的 19 英寸机架上，也可以将其放在平面（如桌面）上。

机架安装（适用于机架安装型号）

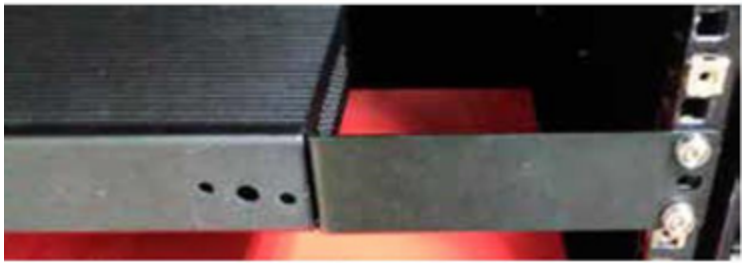
若要将 OT Security 传感器安装到标准（19 英寸）机架上，请执行以下操作：

1. 如下图所示，将 L 形支架连接到传感器两侧的螺钉孔。





2. 在每侧插入两颗螺钉，然后使用螺丝刀将其固定到位。
3. 将配备支架的传感器插入机架中提供的 1U 插槽中。
4. 使用适当的机架安装用螺丝（未提供），将提供的机架安装式支架固定到机架上，以便将装置安装到机架上。



重要说明:

- 确保机架接地。
- 确保散热扇进风口(位于后面板上)和换气孔(位于顶板上)未被堵塞。

5. 将交流电源线(已提供)插入后面板中的电源端口,然后将插头插入交流电源。

平面

若要在平面上安装 OT Security 传感器,请执行以下操作:

1. 将传感器放在干燥、平坦、水平的表面上(如桌面)。

重要说明:

- 确保桌面平坦干燥。
- 确保散热扇进风口(位于后面板上)和换气孔(位于顶板上)未被堵塞。

2. 如果将设备置于多个其他电子设备中,请确保散热扇(位于后面板上)后面有足够的空

间，以便正常换气和散热。

3. 将交流电源线（已提供）插入后面板中的电源端口，然后将插头插入交流电源。

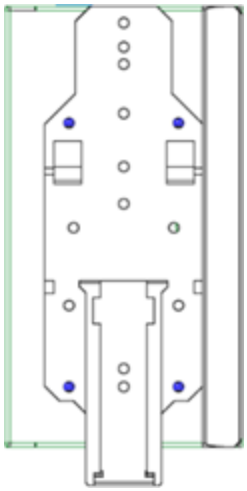
设置可配置传感器

您可将可配置传感器安装在 DIN 导轨上，或安装在标准的 19 英寸安装机架上（使用“安装挂耳”适配器套件）。

DIN 导轨安装

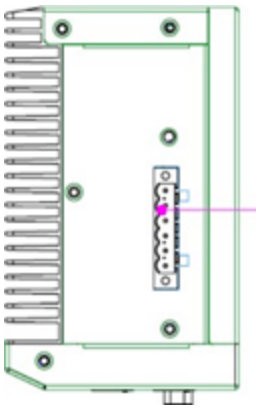
要在标准 DIN 导轨上安装 OT Security 可配置传感器，请执行以下操作：

1. 使用位于传感器背面的支架，将传感器安装到 DIN 轨道上。



2. 使用以下方法之一连接电源：

   - **直流电源**：将 12-36V 直流 6 针 Phoenix Contact 连接器插入传感器设备的侧边，并拧紧连接器顶部和底部的嵌入式螺钉，从而将直流电源线连接到传感器。然后，将电源线的另一端连接到直流电源。



- **交流电源**：将 12-36V 直流 6 针 Phoenix Contact 连接器插入传感器设备的侧边，并拧紧连接器顶部和底部的嵌入式螺钉，从而将交流电源线连接到传感器。

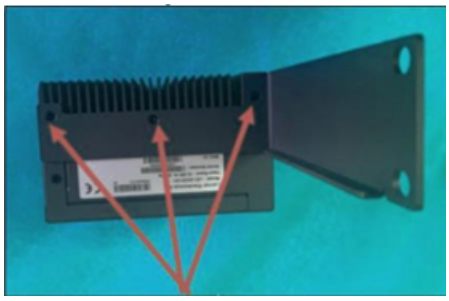
然后，将交流电源线（已提供）插入电源装置，并将另一端插入交流电源插座。

机架安装（适用于可配置型号）

可以使用提供的“安装挂耳”将可配置传感器连接到安装支架。

若要将可配置传感器安装到标准（19 英寸）机架上，请执行以下操作：

1. 准备设备以进行机架安装：
    a. 卸下设备每侧的 3 个螺钉。
    b. 使用新螺钉（已提供）在设备两侧安装“安装挂耳”。



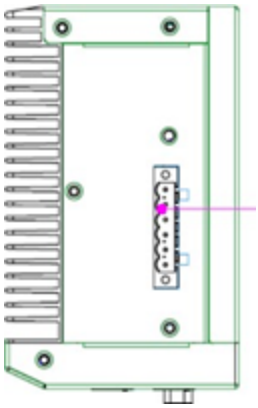
2. 将服务器单元插入机架中可用的 1U 插槽。

注意：

- 确保机架接地。
- 确保散热扇进风口(位于后面板上)和换气孔(位于顶板上)未被堵塞。

3. 使用安装螺钉(已提供)将"安装吊耳"固定到机架框架上，从而将设备固定到机架上。
4. 使用以下方法之一连接电源：

   - **直流电源**：将 12-36V 直流 6 针 Phoenix Contact 连接器插入传感器设备的侧边，并拧紧连接器顶部和底部的嵌入式螺钉，从而将直流电源线连接到传感器。然后，将电源线的另一端连接到直流电源。



   - **交流电源**：将 12-36V 直流 6 针 Phoenix Contact 连接器插入传感器设备的侧边，并拧紧连接器顶部和底部的嵌入式螺钉，从而将交流电源线连接到传感器。

   然后，将交流电源线(已提供)插入电源装置，并将另一端插入交流电源插座。

将传感器连接到网络

OT Security 传感器用于收集网络流量并将其转发到 OT Security 设备。若要执行网络监控，您需要将设备连接到网络交换机上的镜像端口，该端口已连接到相关的控制器/PLC。

如要管理传感器，请将设备连接到网络。可以是与用于执行网络监控的网络不同的网络。

若要将 OT Security 机架安装传感器连接到网络，请执行以下操作：

1. 在 OT Security 传感器上，将以太网电缆（已提供）连接到**端口 1**。
2. 将电缆连接到网络交换机上的常规端口。
3. 在设备上，将另一根以太网电缆（已提供）连接到**端口 2**。
4. 将电缆连接到网络交换机上的镜像端口。

若要将 OT Security 可配置传感器连接到网络，请执行以下操作：

1. 在 OT Security 传感器上，将以太网电缆（已提供）连接到**端口 1**。
2. 将电缆连接到网络交换机上的常规端口。
3. 在设备上，将另一根以太网电缆（已提供）连接到**端口 3**。
4. 将电缆连接到网络交换机上的镜像端口。

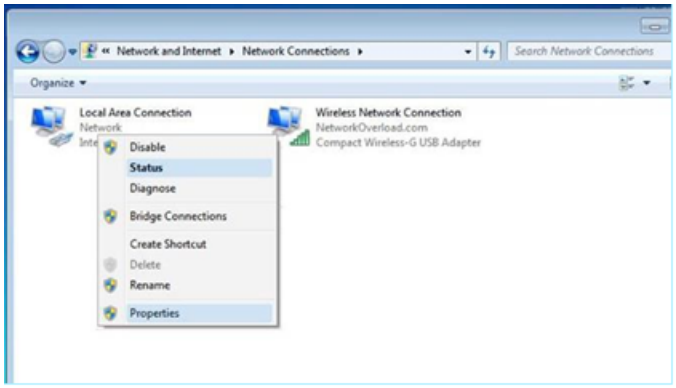
访问传感器设置向导

若要登录管理控制台，

1. 请执行下列操作之一：
   - 使用以太网电缆将管理控制台工作站（例如 PC、笔记本电脑等）直接连接到 OT Security 传感器的端口 1。
   - 将管理控制台工作站连接到网络交换机。
2. 确保管理控制台工作站与 OT Security 传感器（即 192.168.1.5）属于同一子网，或可路由至该装置。
3. 使用以下程序设置静态 IP（必须设置静态 IP，才能连接到 OT Security 传感器）：
   a. 转至“**网络和 Internet**”>“**网络和共享中心**”>“**更改适配器设置**”。

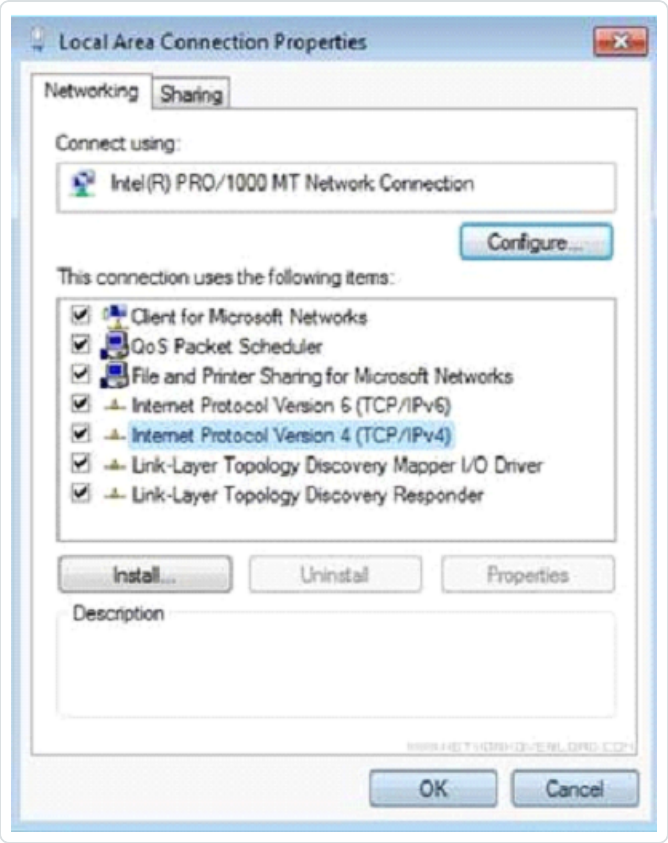
   > **注意**：导航可能因 Windows 版本不同而略有差异。

   此时会显示“**网络连接**”窗口。

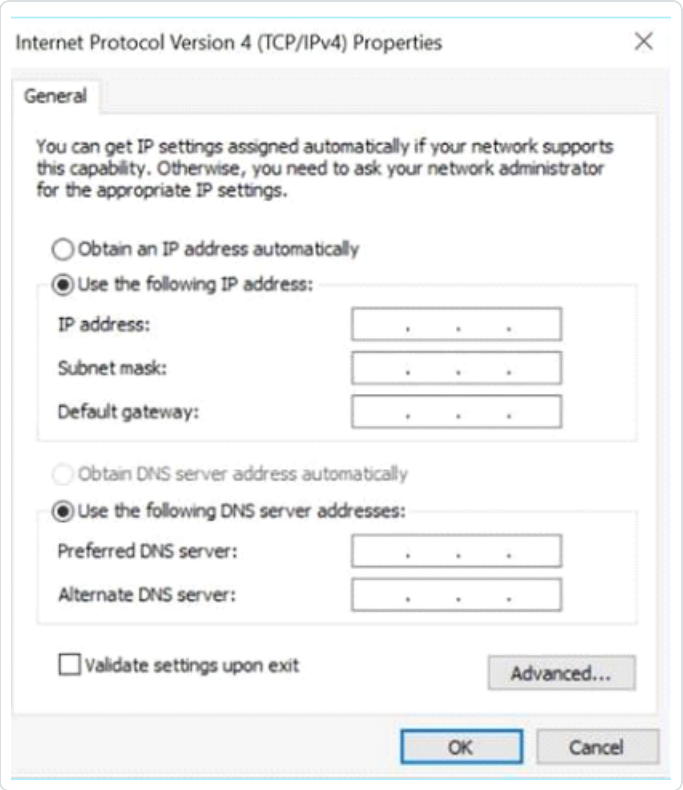
   b. 右键单击“**本地连接**”并选择“**属性**”。

   此时会显示“**本地连接**”窗口。



c. 选择“**Internet 协议版本 4 (TCP/IPv4)**”，然后单击“**属性**”。

此时会显示“**Internet 协议版本 4 (TCP/IPv4) 属性**”窗口。



d. 选择“**使用下列 IP 地址**”。

e. 在“IP 地址”框中，输入“**192.168.1.10**”。

f. 在“**子网掩码**”框中，输入“255.255.255.0”

g. 点击“**确定**”。

OT Security 会应用新设置。

4. 在 Chrome 浏览器中，导航至 https://192.168.1.5:8000。

> **注意**：只能通过 Chrome 浏览器访问 UI，使用最新版本的 Chrome。

5. 将传感器配对。

OT Security 许可证工作流

可以根据系统中唯一 IP 的数量计算 Tenable 帐户的许可证。每个 IP 都需要使用单独的许可证。例如，即使有多个设备共享相同的 IP 地址（如多个设备连接到共享相同的三个 IP 的相同背板），许可证仍将基于 IP 数量。在这种情况下，您需要有 3 个许可证，无需考虑设备数量。

安装 OT Security 设备后，下一步是激活许可证。

注意：若需要更新或重新初始化 OT Security 许可证，请联系 Tenable 客户经理。在您的 Tenable 客户经理更新许可证后，您可以更新或重新初始化许可证。

有关为 Tenable One 部署 Tenable OT Security 和申请相关许可的信息，请参阅《Tenable One 部署指南》。

开始之前

- 安装 OT Security 设备。
- 确保您拥有订购设备时从 Tenable 收到的许可证代码（由 20 个字符的字母/数字组成）。
- 确保您拥有 Internet 的访问权限。如果 OT Security 设备未连接到 Internet，您可通过任何 PC 注册许可证。
- 确保您有权访问 Tenable 配置门户。如需访问权限，请联系 Tenable Customer Success Manager。

激活 OT Security 许可证

您可以激活 OT Security 许可证，并使用 Tenable 配置门户创建新站点以管理您的资产。

若要激活 OT Security 许可证，请执行以下操作：

1. 使用社区帐户登录 Tenable 配置门户。

   此时会出现“**配置**”页面，其中包含您具有许可证的产品。

2. 在左窗格中，选择“**Tenable OT Security**”。

   此时会出现 OT Security 许可证，其中包含购买日期、到期日期以及许可 IP 和站点的数量等详细信息。

3. 从“**代码**”列中，复制 20 位 OT Security 许可证代码。

4. 在 OT Security 中生成激活证书：

   a. 前往 OT Security“**许可证激活**”页面。

   b. 第 1 步，单击“**输入新的许可证代码**”。

      此时右侧会出现“**输入新的许可证代码**”面板。

   c. 在“**许可证代码**”框中，粘贴您从配置门户复制的代码。

   d. 单击“**验证**”。

      OT Security 启用“**生成激活证书**”部分。

   e. 单击“**生成证书**”。

      此时右侧会出现“**生成证书**”面板。

   f. 单击“**将文本复制到剪贴板**”，然后单击“**完成**”。

      OT Security 会生成证书，您必须在 Tenable 配置门户中提供该证书才能添加站点。

5. In the Tenable Provisioning portal, navigate to the **Tenable OT Security Provisioning** page and click ⊕**Add Site**.

   The **Add New Tenable OT Security Site** window appears.

   a. (Optional) In the **Label** box, type a name for the site.

   b. In the **IPs** box, type the number of IP addresses you want to assign to this site.Use the **+** and **-** buttons to increase or decrease the value.

      > **Tip**: To adjust the number of IP addresses assigned to the license, you can also use the slider located under the **IPs** box.

   c. In the **Activation Certificate** box, paste the certificate that you copied from OT Security.See step f.

   d. Click **Create**.

      A dialog box appears with an activation code.This is a one-time generated code that you must copy to the OT Security instance.

   e. Click the ⧉ button, then click **Confirm**.

6. 导航回到 OT Security 实例，第 3 步：在“**输入激活代码**”部分，点击“**输入激活代码**”。

   此时右侧会出现“**输入激活代码**”面板。

7. 在“**激活代码**”框中，粘贴您从“**Tenable OT Security 配置**”网页复制的一次性生成代码。请参阅步骤 e。

8. 点击“**激活**”。

   OT Security 显示一条确认消息，表示系统已成功激活，并出现 OT Security 界面。

9. 点击“**启用**”。

   OT Security 现已启用并可以使用。

10. 导航回到 Tenable 配置门户，在“一次性生成的激活代码”对话框中，单击“**我已保存此证书信息或将其复制到 Tenable.ot 中用于激活**”复选框。

11. 点击“**确认**”。

    新添加的站点会显示在 OT Security 的“**配置**”页面中。

更新许可证

如要提高资产限制、延长许可证期限或更改许可证类型，您可以更新许可证。

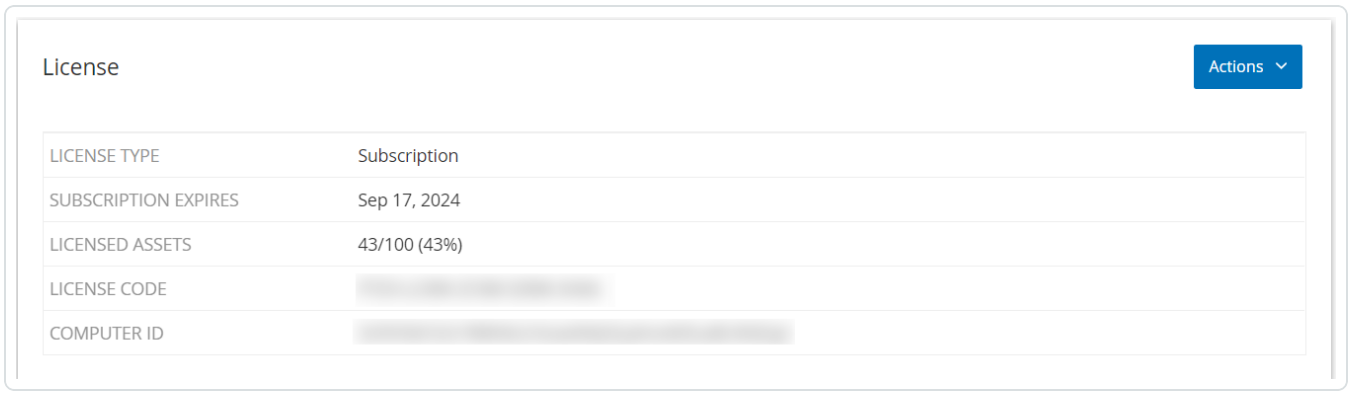
开始之前

- Tenable 客户经理必须已在其系统中更新许可证信息，您才能更新新的许可证。
- 需要 Internet 的访问权限。如果 OT Security 设备未连接到 Internet，您可通过任何 PC 注册许可证。

如要更新许可证，请执行以下步骤：

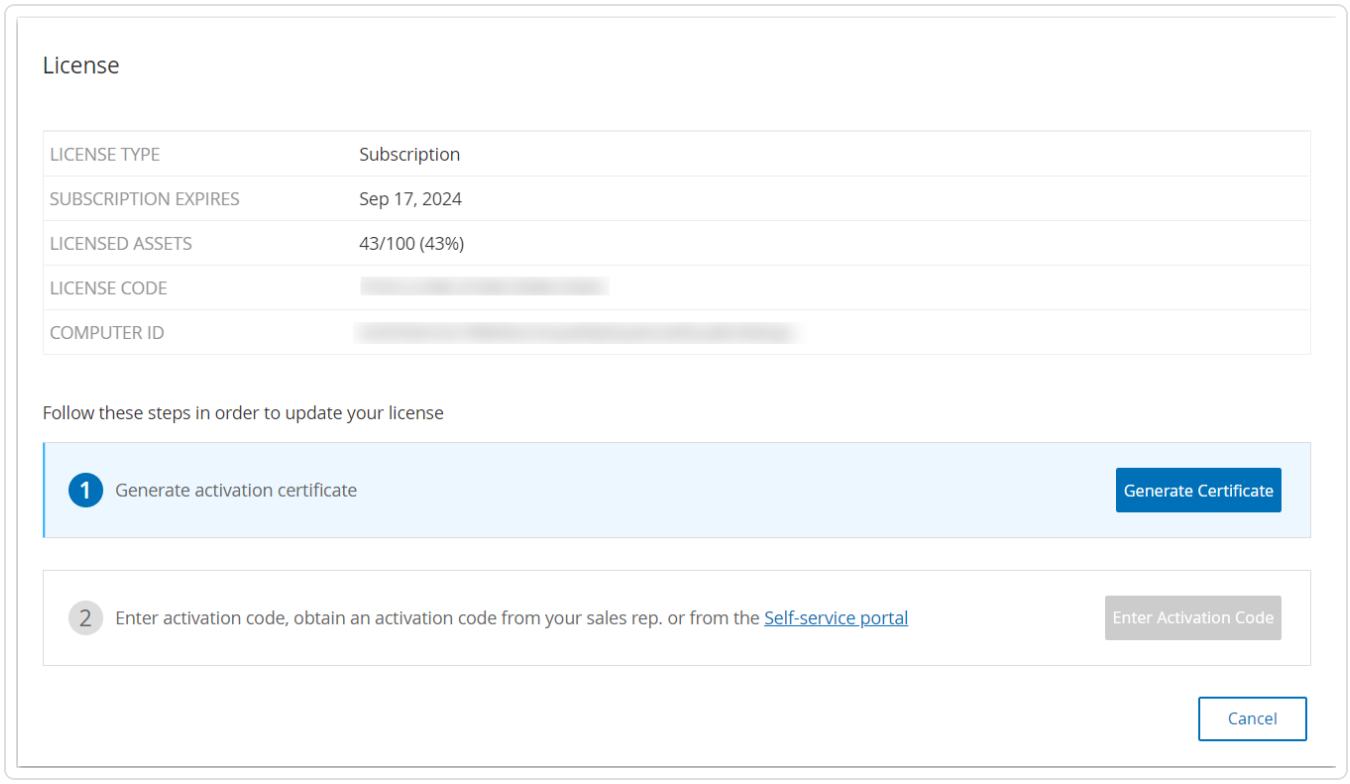
1. 转至“**本地设置**”>“**系统配置**”>“**许可证**”。

   此时会出现“**许可证**”窗口。



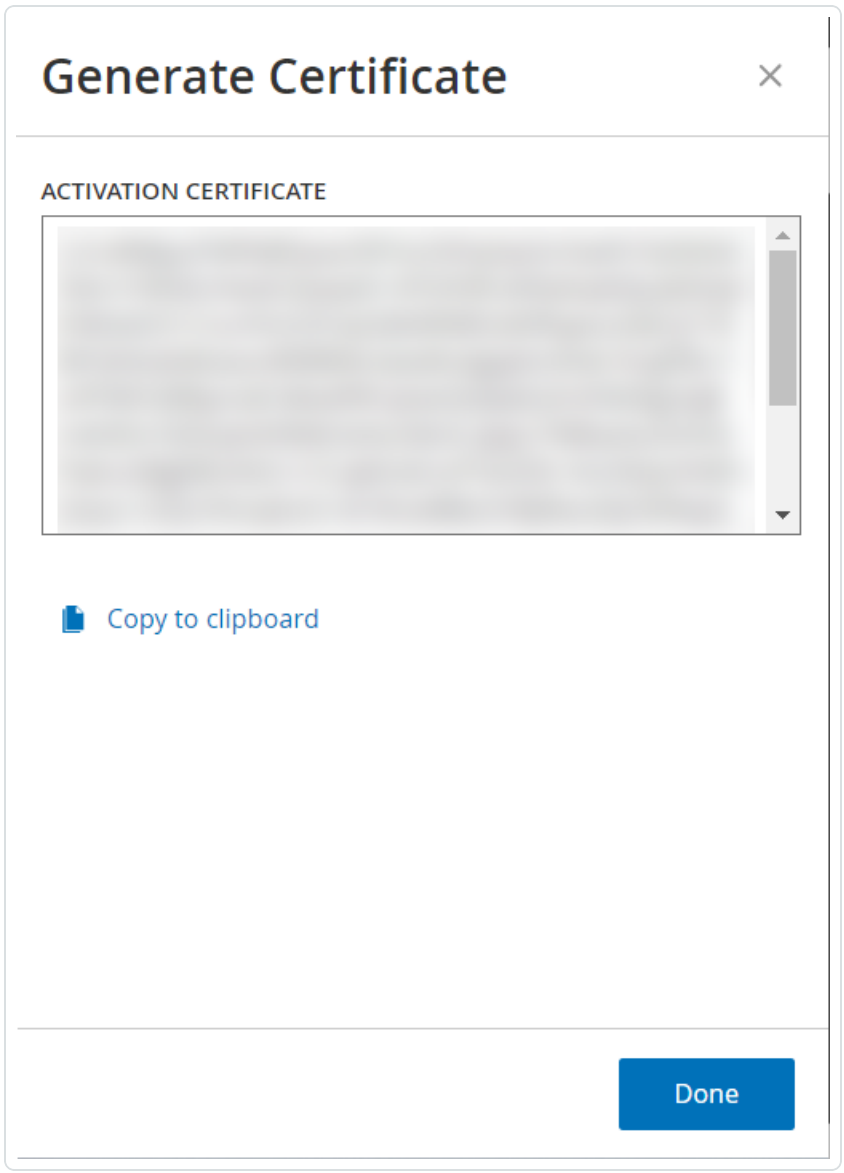
2. 在“**操作**”菜单中，选择“**更新许可证**”。

   此时会显示“**生成证书**”和“**输入激活代码**”步骤。



3. 在“**(1) 生成激活证书**”框中，单击“**生成证书**”。

   此时“**生成证书**”面板将与**激活证书**一起显示。



4. 单击“**将文本复制到剪贴板**”，然后单击“**完成**”。

   此时，侧面板会关闭。

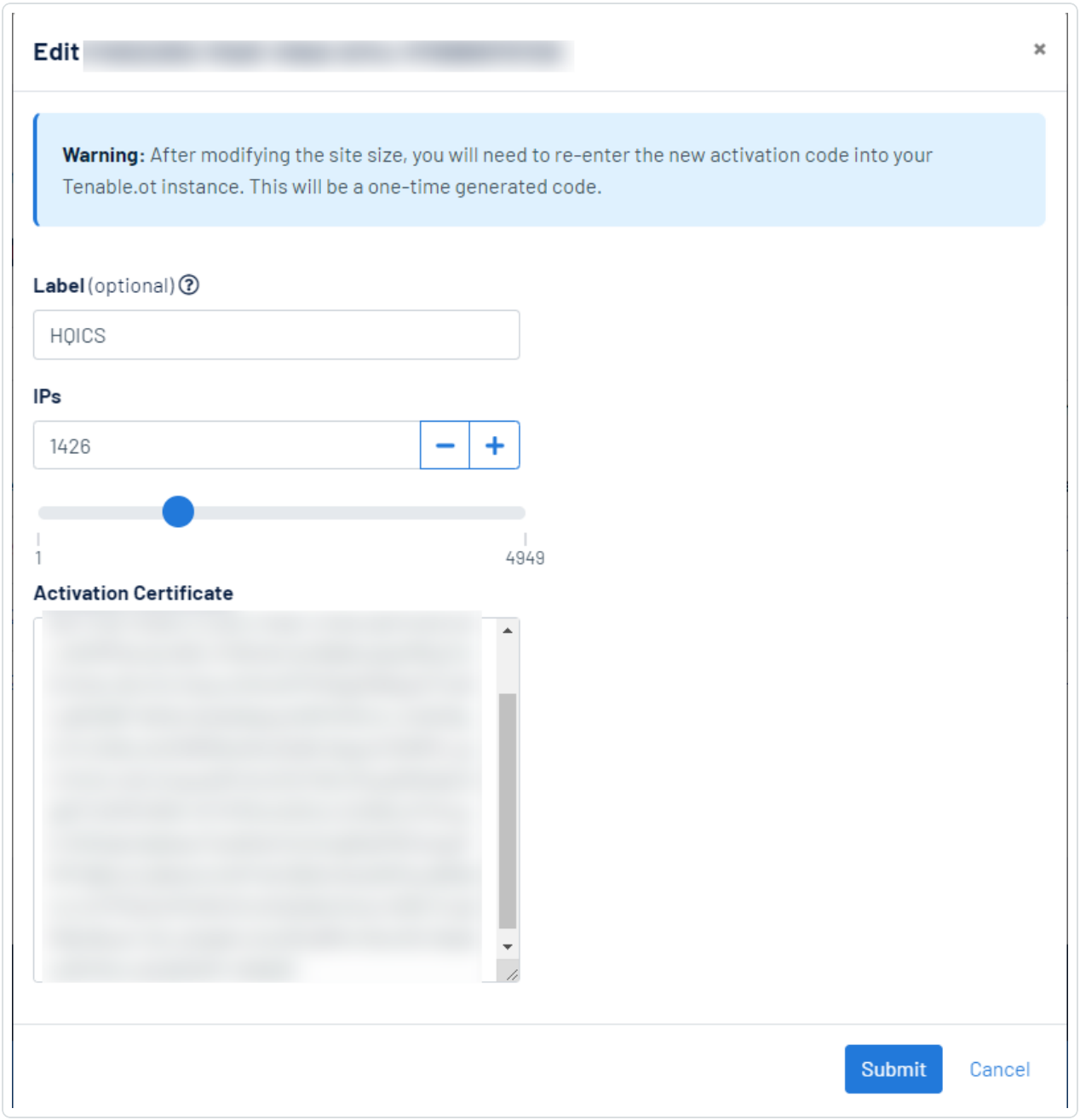
5. 编辑 Tenable 配置门户中的站点详细信息：

   a. 在 Tenable 配置门户中，导航至“**Tenable OT Security 配置**”页面，然后在您要更新的站点行中单击“⋯”按钮。

      此时会出现菜单。

   b. 点击“**编辑网站**”。

此时会出现该站点的编辑窗口。



c. 根据需要调整详细信息。

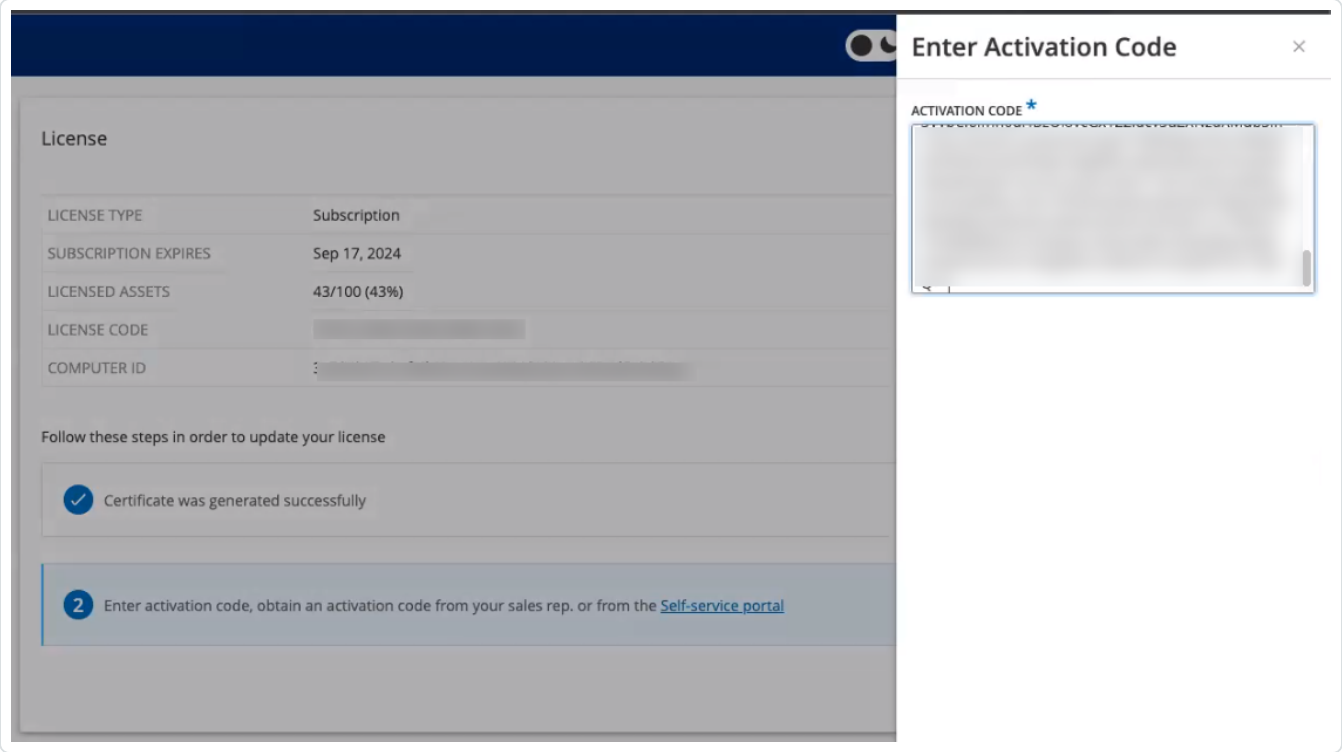
d. 在“**激活证书**”框中，粘贴您从 OT Security 的“**生成证书**”窗口中复制的证书。

e. 点击“**提交**”。

门户网站会显示包含激活代码的对话框。这是一次性生成的代码，必须将其复制到 OT Security 实例。

f. 点击 按钮，然后点击“**确认**”。

6. 导航回 OT Security 实例。
7. 在 (2)“**输入激活代码**”框中，点击“**输入激活代码**”。
8. 在“**激活代码**”框中，粘贴您从“**Tenable OT Security 配置**”网页复制的一次性生成代码。

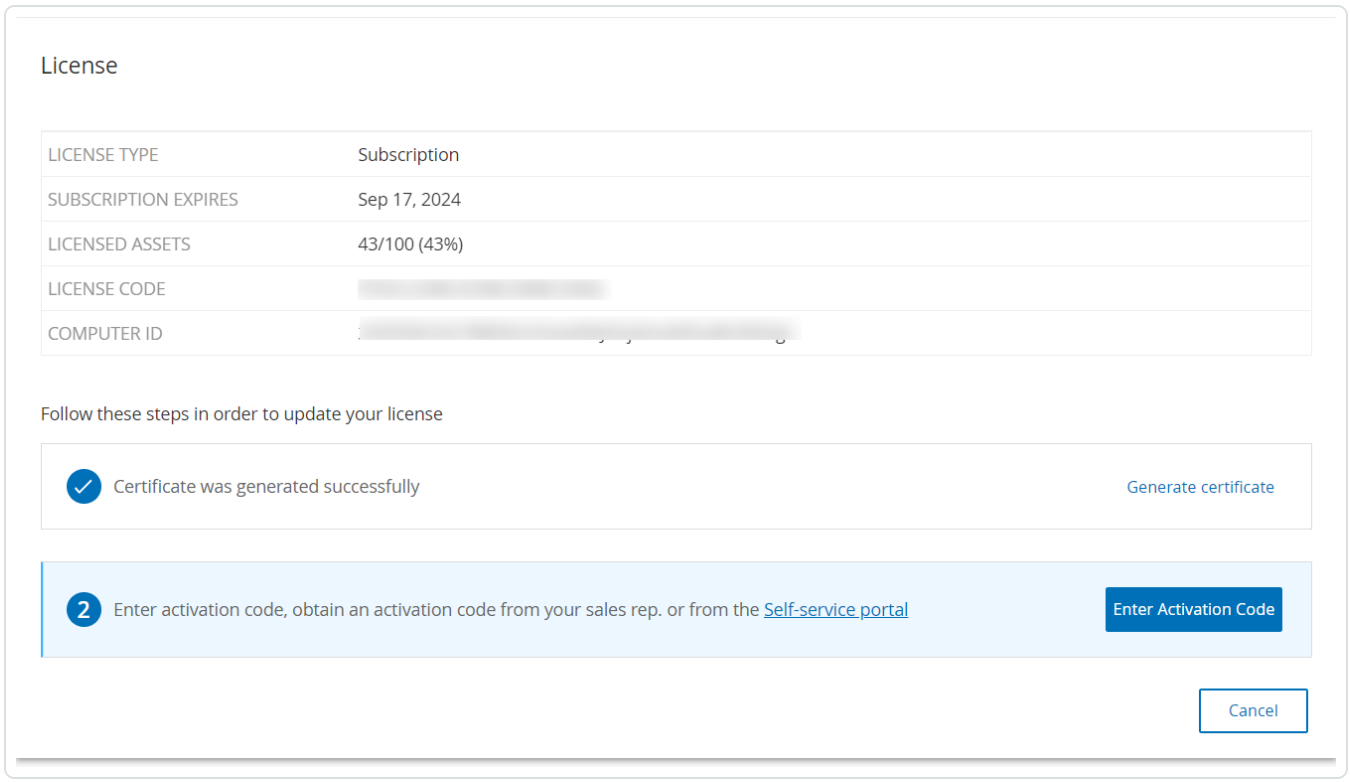


9. 点击“**激活**”。

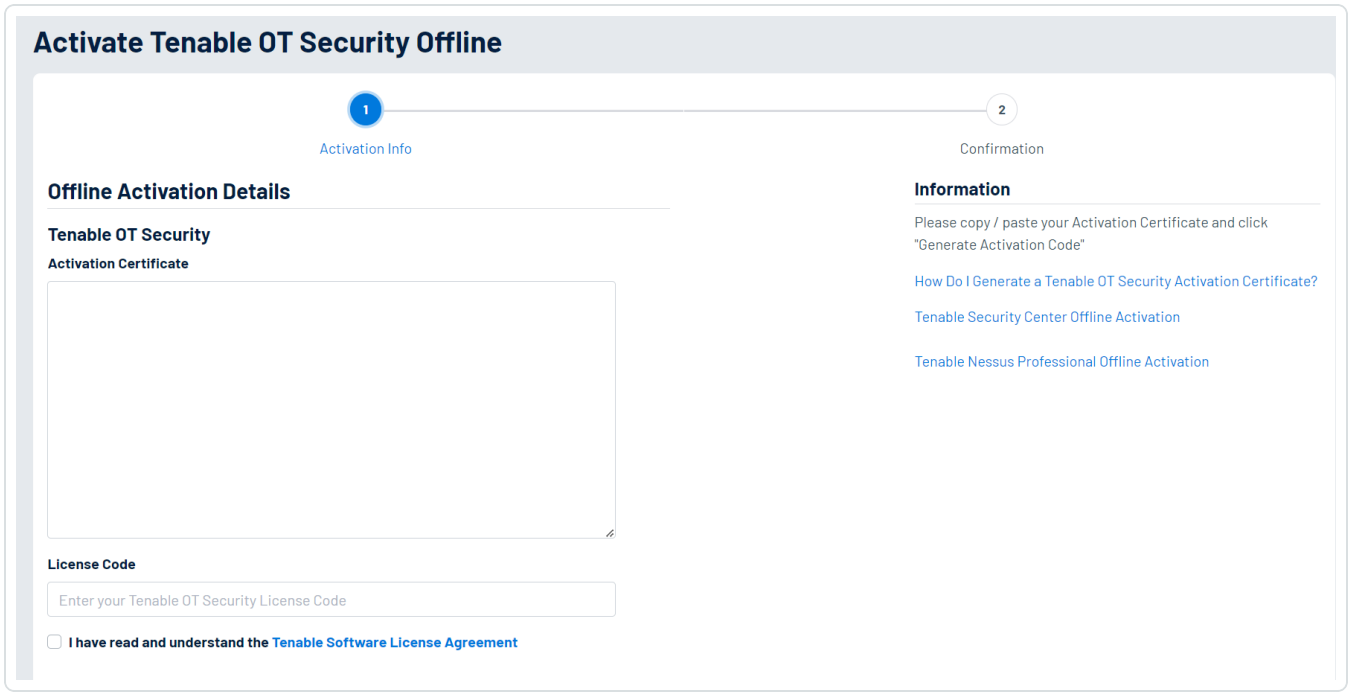
OT Security 会显示系统已成功激活的确认消息，并且“**许可证**”页面会显示更新后的许可证详细信息。

在离线模式下更新许可证

1. 执行“更新许可证”部分中所述的步骤 1 至 4。
2. 在 (2)“**输入激活代码**”框中，单击“自助服务门户”链接。



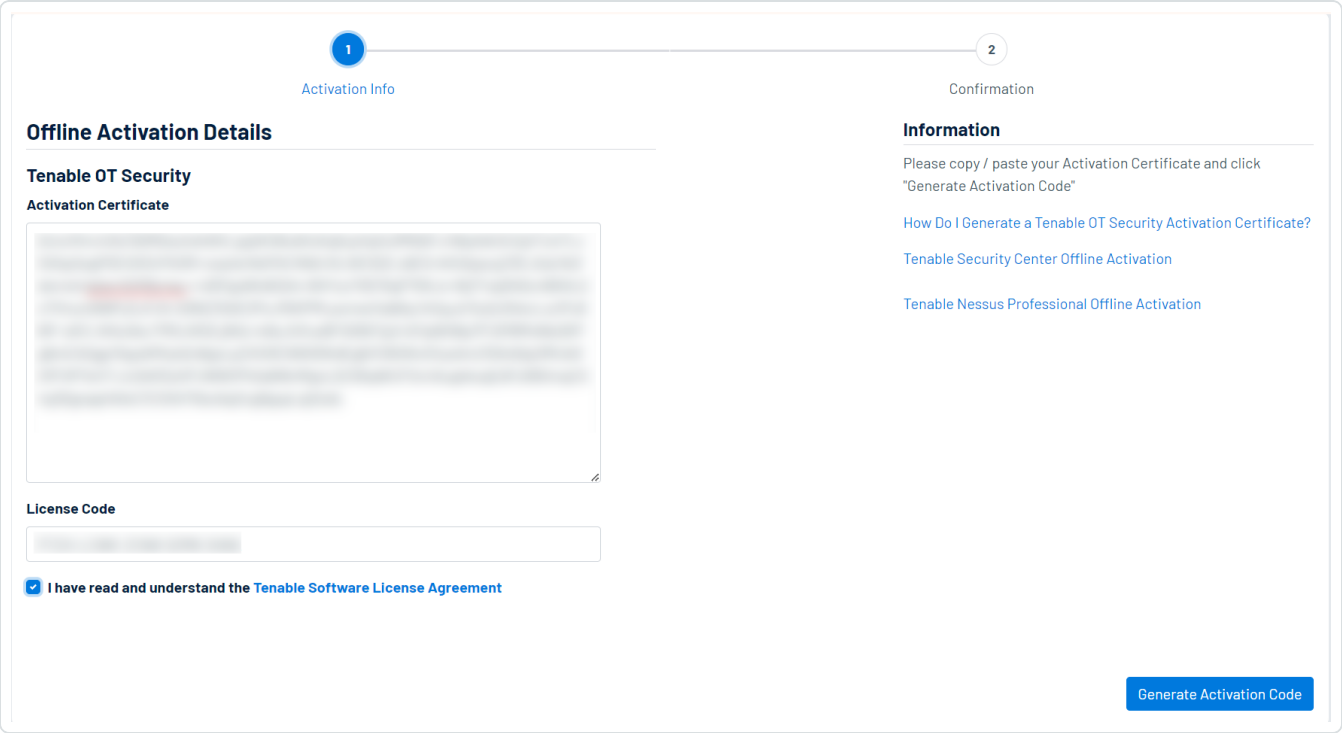
“离线激活 OT Security”窗口会在新选项卡中打开。



注意：您可以在已连接 Internet 的设备上输入以下 URL 以访问“离线激活 OT Security”屏幕：https://provisioning.tenable.com/activate/offline/tenable-ot。

注意：如果您未登录 tenable.com，您可以使用电子邮件地址和密码进行登录。请使用接收**许可证代码**的电子邮件帐户。如果没有登录凭据，您可以单击“**忘记密码**”（并按照提示进行操作）或联系 Tenable 客户经理。

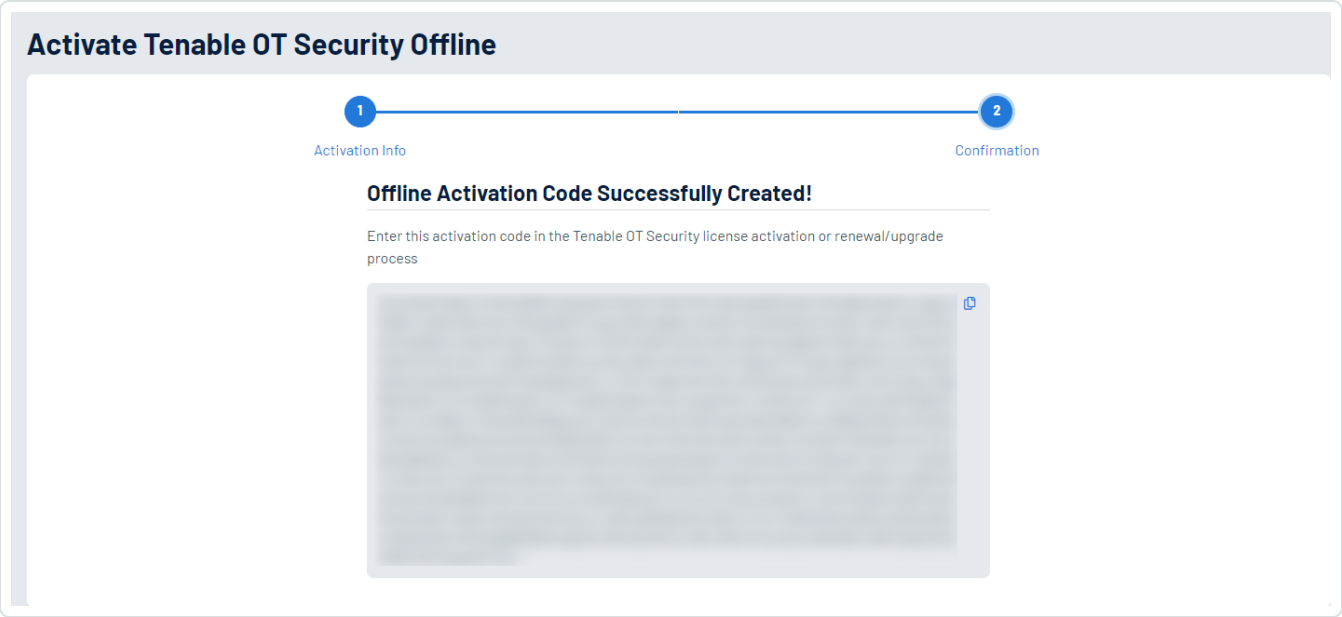
3. 在“**激活证书**”框中，粘贴**激活证书**。
4. 在“**许可证代码**”框中，输入 20 个字符的“**许可证代码**”（可从“**许可证**”屏幕复制粘贴）。
5. 单击“**我已阅读并理解 Tenable 软件许可证协议**”复选框。



注意：如要查看许可证协议，请单击“**Tenable 软件许可证协议**”链接。

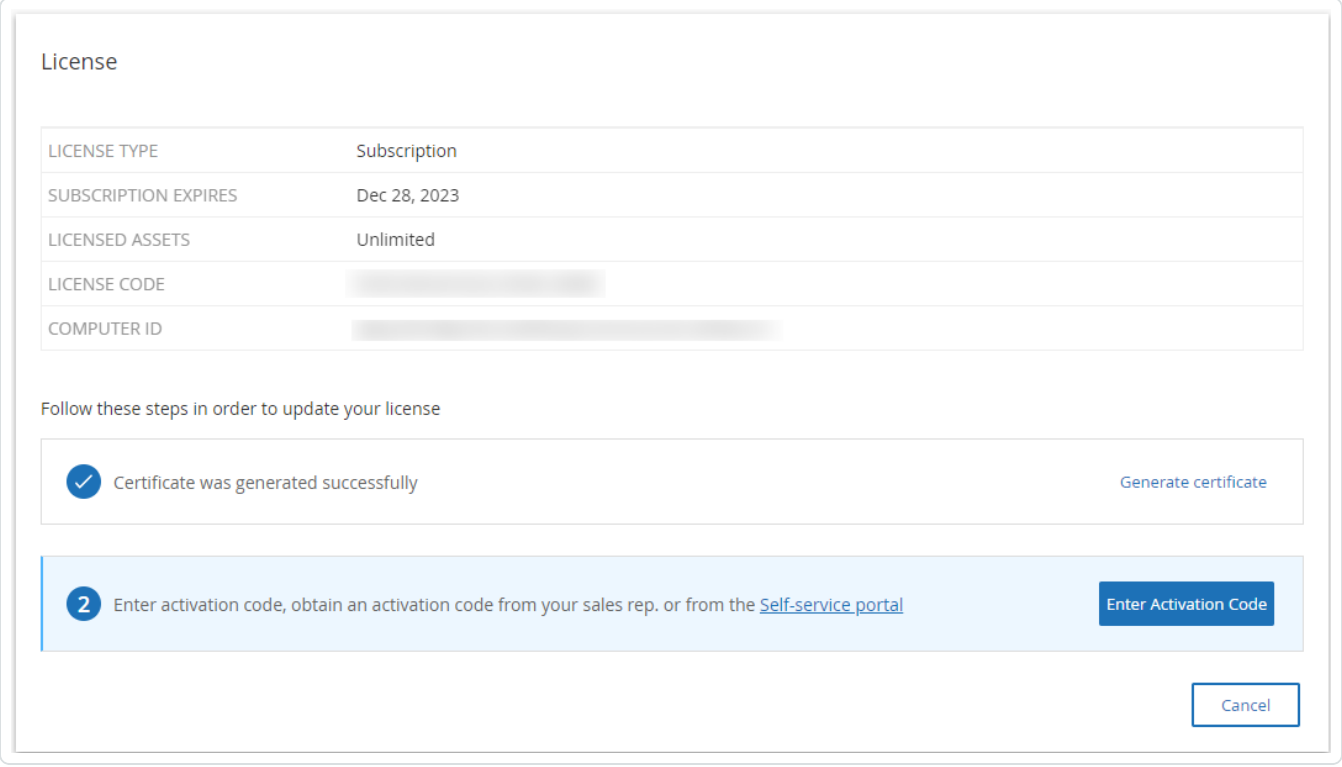
6. 单击“**生成激活代码**”。

   此时将出现“**离线激活代码已成功创建！**”窗口。



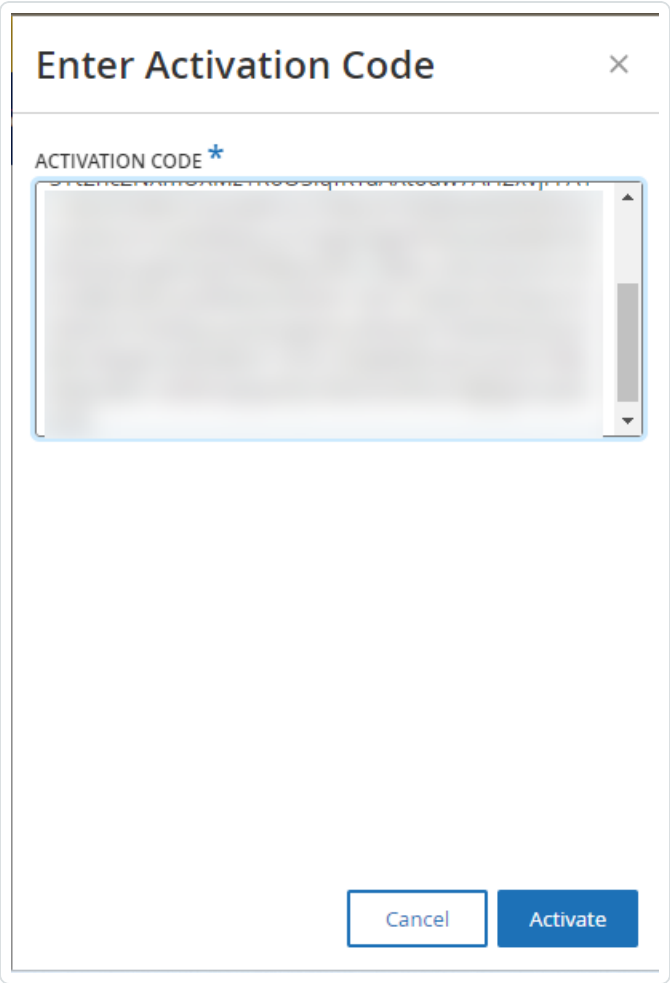
7. 单击 按钮。

8. 导航回到“**许可证**”选项卡，然后单击“**输入激活代码**”。



此时将出现“**输入激活代码**”侧面板。

9. 在“**激活代码**”框中，粘贴激活代码，然后单击“**激活**”。



侧面板关闭即表示 OT Security 已更新许可证。

重新初始化许可证

重新初始化许可证将从系统中删除当前许可证并激活新的许可证，此操作与在系统启动期间激活许可证类似。如果需要重新初始化许可证（即若向您颁发新的许可证），请遵循以下程序。

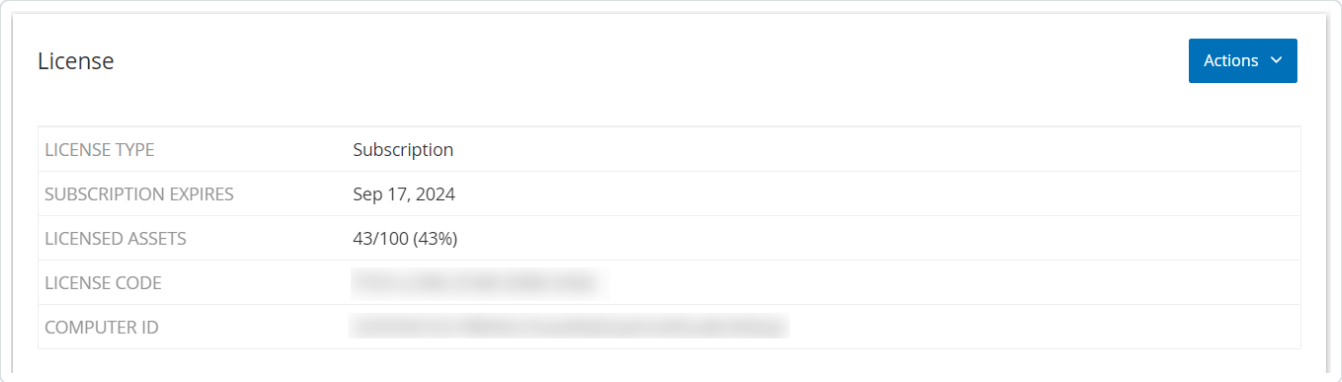
开始之前

- Tenable 客户经理必须已在其系统中颁发新许可证，并提供许可证代码（20 个字符的字母/数字）。

- 需要 Internet 的访问权限。如果 OT Security 设备未连接到 Internet，则可通过任何 PC 注册许可证。

若要重新初始化许可证，请执行以下操作：

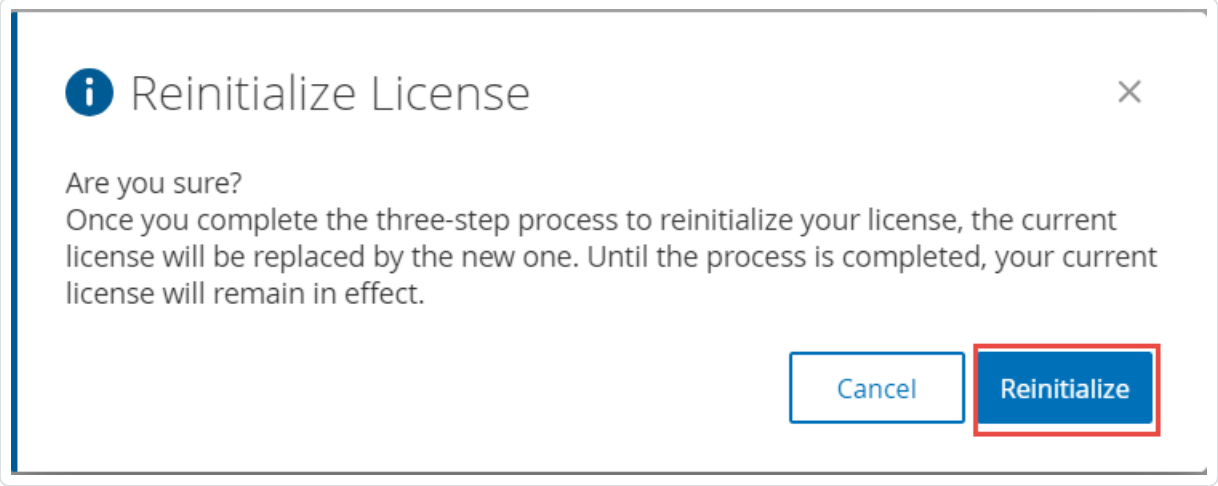
1. 转至“**本地设置**”>“**系统配置**”>“**许可证**”。



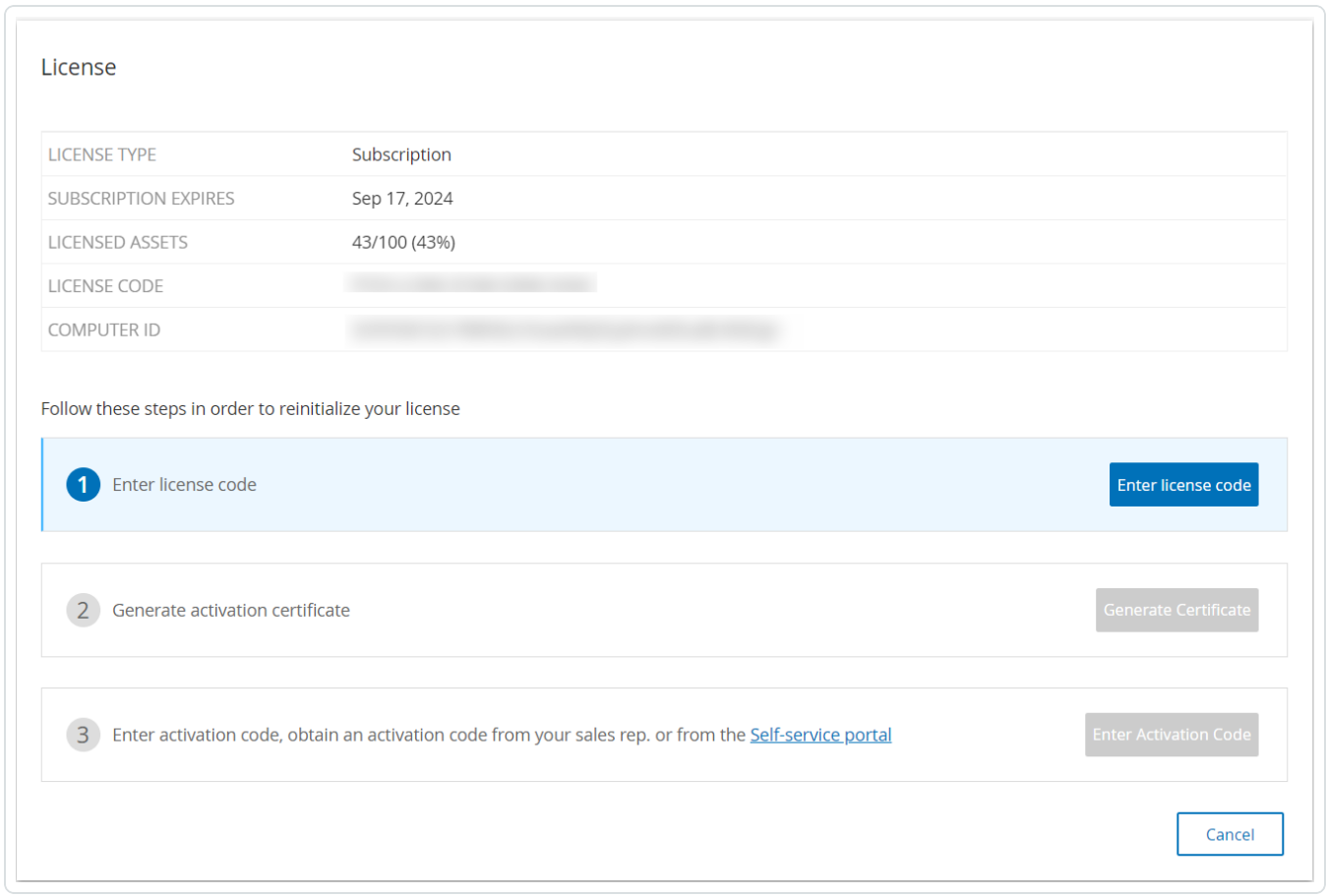
2. 在“**操作**”菜单中，选择“**重新初始化许可证**”。

   此时会出现“确认”窗口。

3. 单击“**重新初始化**”。



   此时会显示“**许可证**”窗口，其中包含三个重新初始化步骤。



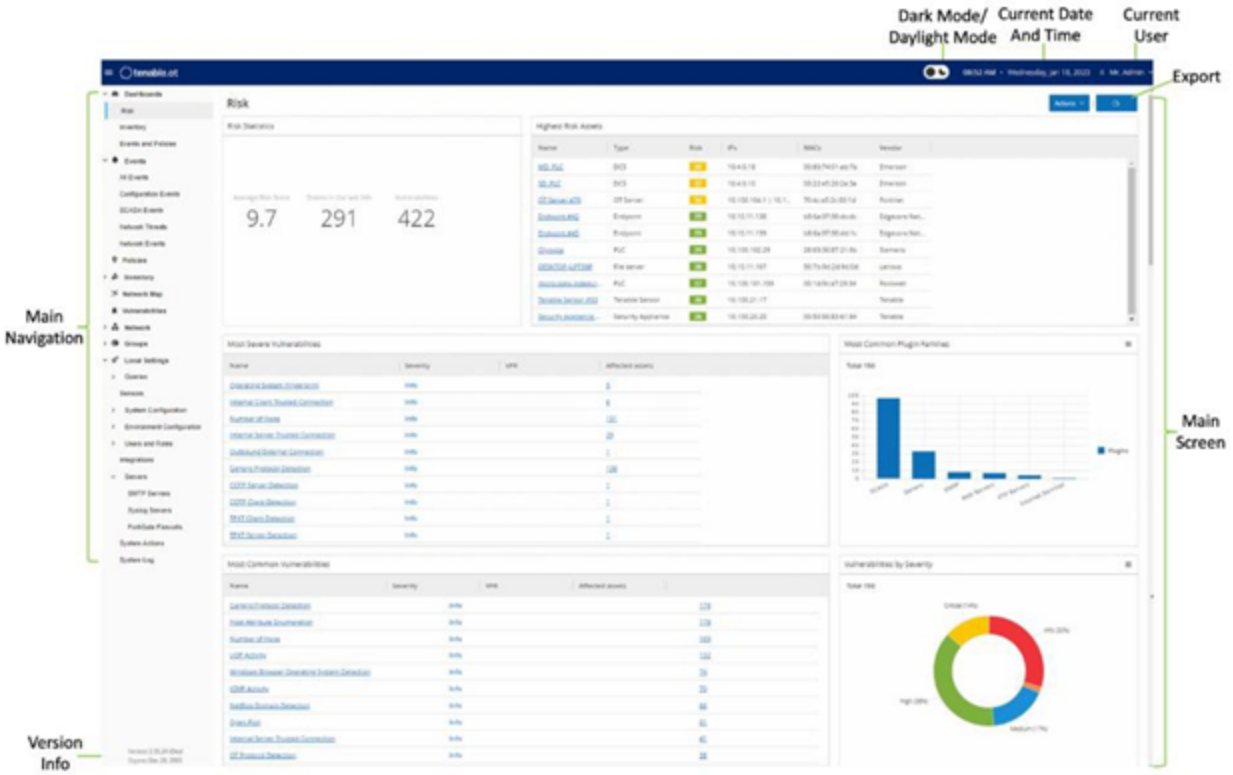
4. 按照系统启动步骤激活许可证。请参阅"激活许可证"。

   提供**激活代码**后，新的许可证将替换当前的许可证。

管理控制台用户界面元素

管理控制台用户界面有助于轻松访问 OT Security 发现的与资产管理、网络活动和安全事件相关的重要数据。您可以根据需要使用用户界面配置 OT Security 平台功能。

主要用户界面元素



下表介绍了主要的用户界面元素。

用户界面元素	描述
主导航	主导航菜单。单击 ☰ 图标可显示/隐藏主导航菜单。
当前日期和时间	显示系统中注册的当前日期和时间。
当前用户名	显示当前登录到系统的用户的名称。单击选择菜单的向下箭头。菜单选项为“**关于**”(显示软件信息) 和“**注销**”。
许可证信息	显示 OT Security 软件版本和许可证到期日期。
主屏幕	显示您在主导航中选择的屏幕。
夜间模式/日间模式	将显示颜色方案更改为夜间式或日间模式。

导出	下载仪表盘的 PDF 文件。

启用或禁用夜间模式

您可通过启用"夜间模式"切换开关在所有屏幕上使用**夜间模式**颜色方案。

要启用或禁用夜间模式：

1. 单击窗口顶部的  (夜间模式)切换开关。

   OT Security 将所选设置应用到所有屏幕。

2. 要恢复日间模式设置，请单击  (日间模式)切换开关。

检查当前软件版本

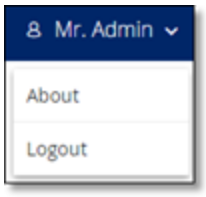
您可以使用标题栏右上方的用户配置文件图标来检查软件的版本。

若要显示当前软件版本，请执行以下操作：

1. 在主标题栏中，单击右上角的  图标即可打开菜单。

   OT Security 会显示用户菜单。

2. 点击"**关于**"。

OT Security 会显示当前软件版本。

浏览 OT Security

您可以从左侧导航面板访问以下主页：

- **仪表盘**：包含图形和表格的视图小组件，可针对网络清单和安全状态提供概览。风险、清单、事件和策略均有单独的仪表盘。请参阅“仪表盘”。
- **事件**：显示由于策略违规而发生的所有事件。有一个显示“所有事件”的屏幕，并且每种特定事件类型都具有单独的屏幕。例如：配置事件、SCADA 事件、网络威胁或网络事件。请参阅“事件”。
- **策略**：查看、编辑和激活系统中的策略。请参阅“策略”。
- **清单**：显示所有已发现资产的清单，允许进行全面的资产管理、监控每项资产的状态并查看其相关事件。有一个显示“所有资产”的屏幕，并且特定类型资产（控制器和模块、网络资产和 IoT）都具有单独的屏幕。请参阅“资产”。
- **网络映射**：以可视化方式显示网络资产及其连接。
- **漏洞**：显示网络中 OT Security 插件检测到的所有威胁的详细列表，并提供建议的修复步骤。本部分包括网络中的 CVE 以及其他资产威胁。例如过时的操作系统、易受攻击协议的使用、易受攻击的已打开端口等。
- **网络**：通过显示网络中各项资产之间随时间推移发生的对话的相关数据，提供网络流量的全面视图。请参阅“网络”。OT Security 在三个单独的窗口中显示此信息：
  - **网络汇总**：显示网络流量概览。
  - **数据包捕获**：显示网络流量的完整数据包捕获。
  - **对话**：显示在网络中检测到的所有对话的列表，其中包含与对话发生时间、所涉资产等内容相关的详细信息。
- **组**：查看、创建和编辑策略配置中使用的组。请参阅“组”。
- **本地设置**：查看和配置系统设置。请参阅“本地设置”。

自定义表格

OT Security 页面以表格格式显示数据以及每个项目的列表。这些表格具有标准化的自定义功能，便于您轻松访问相关信息。

注意:此处的示例针对"**所有事件**"和"**所有资产**"页面,但大多数页面都会提供类似功能。可以随时通过单击"**设置**">"**将表格重置为默认设置**"来恢复为默认显示设置。

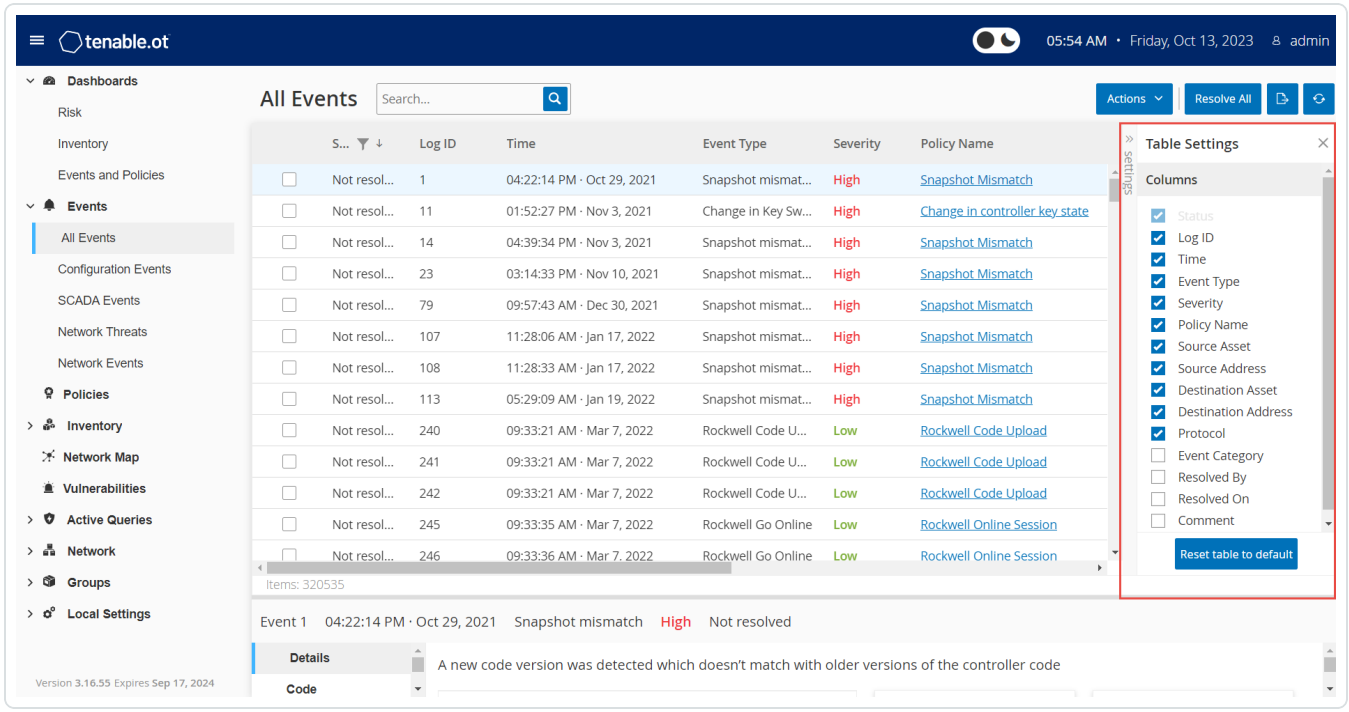
自定义列显示

可以自定义要显示的列及其组织方式。

若要指定显示哪些列，请执行以下操作：

1. 在表格右侧，单击“**设置**”。

   此时会出现“**表格设置**”面板，其中显示了“**列**”部分。



2. 在“**列**”部分，选中要显示的列旁边的复选框。
3. 取消选中要隐藏的列旁边的复选框。

   OT Security 仅会显示选中的列。
4. 单击“**x**”(或“**设置**”选项卡) 即可关闭“**表格设置**”窗口。

若要调整列的显示顺序，请执行以下操作：

1. 单击列标题并将其拖动到所需位置。

按类别对列表分组

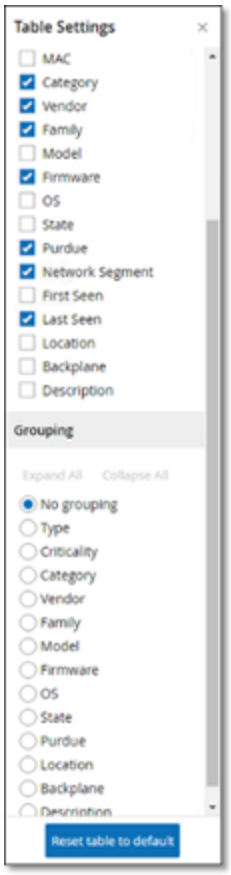
对于“**库存**”页面，您可以按照与该特定屏幕相关的各种参数对列表分组。

若要对列表进行分组，请执行以下操作：

1. 单击表格右边缘的“**设置**”选项卡。

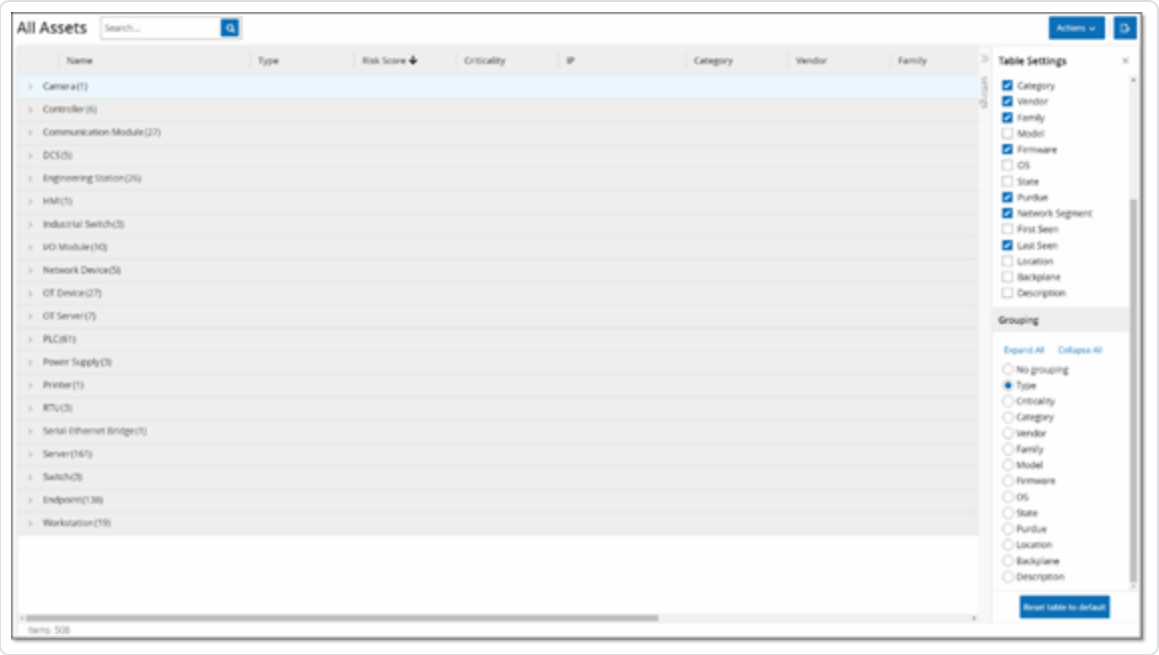
   此时右侧会出现“**表格设置**”窗格以及“**列**”和“**分组**”部分。

2. 向下滚动至“**分组**”部分。



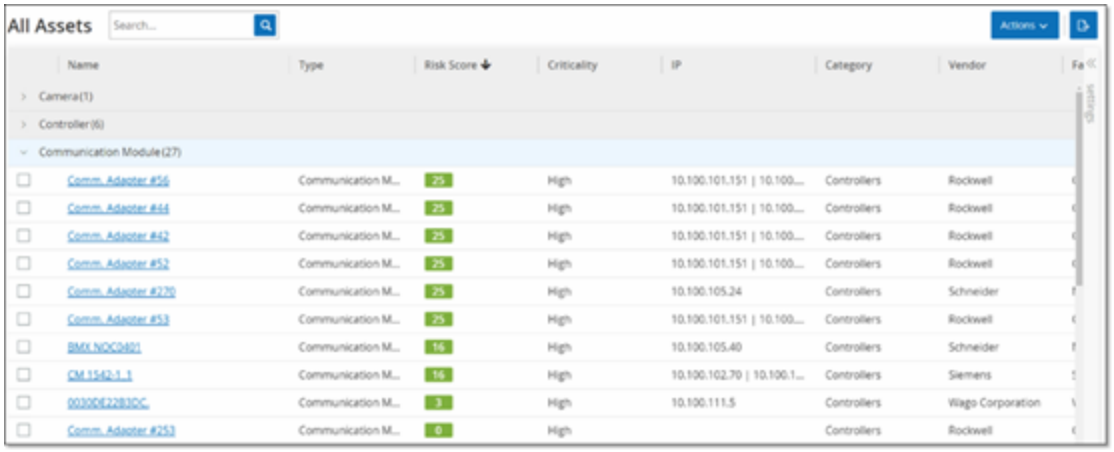
3. 选择列表分组的依据。例如，“**类型**”。

   OT Security 显示已分组的类别。



4. 单击“**x**”(或“**设置**”选项卡) 即可关闭“**表格设置**”窗口。

5. 单击类别旁边的箭头可显示该类别的所有实例。



对列进行排序

若要对列表进行排序，请执行以下操作：

1. 单击列标题即可按该参数对资产进行排序。例如，单击“**名称**”标题可按名称的字母顺序显示资产。
2. 如想反转显示顺序（即 A→Z、Z→A），请再次单击该列标题。

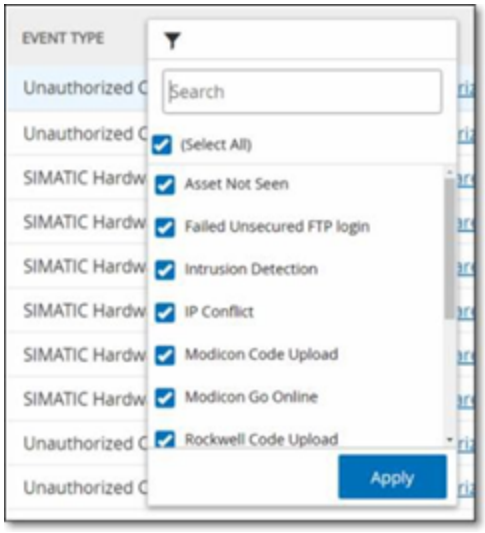
筛选列

您可以为一个或多个列标题设置筛选条件。筛选条件是累积的，因此只显示符合所有筛选条件的列表。筛选选项仅针对每个列标题。每个屏幕都会提供一系列的相关筛选条件。例如，在“**控制器清单**”窗口上，您可以按“**名称**”、“**地址**”、“**类型**”、“**背板**”、“**供应商**”条件等进行筛选。

若要筛选列表，请执行以下操作：

1. 将鼠标悬停在列标题上，可显示筛选图标 ▼。
2. 单击筛选图标 ▼。

   此时将出现筛选选项的列表。选项特定于每个参数。



3. 选择要显示的元素，并取消选中要隐藏的元素旁边的复选框。

   注意：您可以先取消选择“**全选**”复选框，然后选择要显示的复选框。

4. 您可以在列表中搜索筛选条件，然后进行选择或取消选择。
5. 单击“**应用**”。

   OT Security 会按照指定方式筛选列表。

列标题旁边的筛选器 ▼ 按钮表示正在按该参数筛选结果。

若要删除筛选条件，请执行以下操作：

1. 单击筛选器 ▼ 按钮。
2. 单击“**全选**”复选框以清除所有选择。
3. 再次单击“**全选**”复选框以选择所有元素。
4. 单击“**应用**”。

搜索

在每页上，您都可以搜索特定记录。

若要搜索列表，请执行以下操作：

1. 在“**搜索**”框中输入搜索文本。
2. 单击  按钮。
3. 如要清除搜索文本，请单击“**x**”。

导出数据

您可以将 OT Security UI 中显示的任何列表中的数据(例如事件、库存等)以 CSV 文件格式导出。

注意:导出的文件包括该页面的所有数据,即使已针对当前显示内容应用筛选条件亦可导出。

若要导出数据,请执行以下操作:

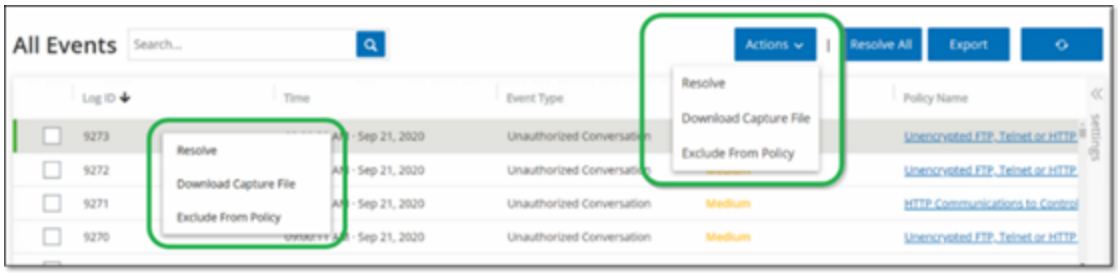
1. 转至要导出数据的屏幕。
2. 在标题栏中,单击"**导出**"。

操作菜单

每个屏幕上都有一系列可用于该屏幕上元素的操作。例如，在“**策略**”屏幕上，您可以**查看**、**编辑**、**复制**或**删除**策略；在“**事件**”屏幕上，您可以**解析**或**下载事件的捕获文件**等。

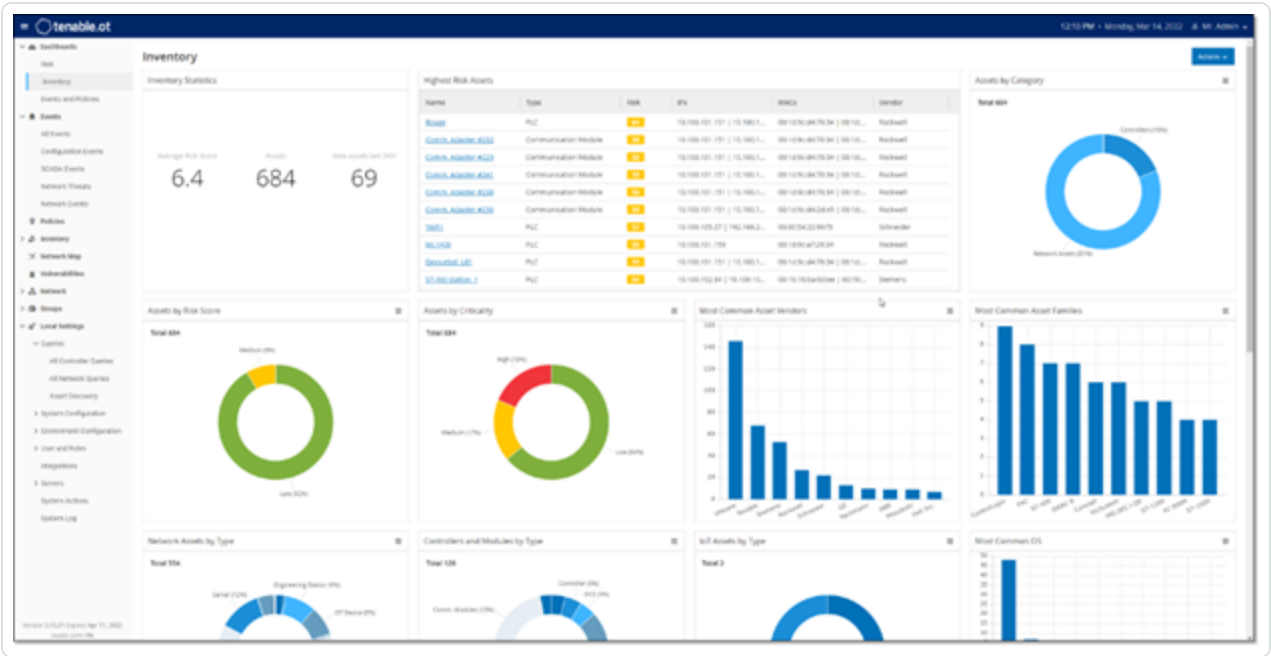
若要访问“**操作**”菜单，请执行下列操作之一：

- 选择一个元素，然后单击标题栏中的“**操作**”按钮。
- 右键点击该元素，然后选择“**操作**”。



仪表盘

共有三个仪表盘：“**风险**”、“**清单**”以及“**事件和策略**”。仪表盘包含可针对网络清单和安全状态提供概览的小组件。



若要选择仪表盘，请执行以下操作：

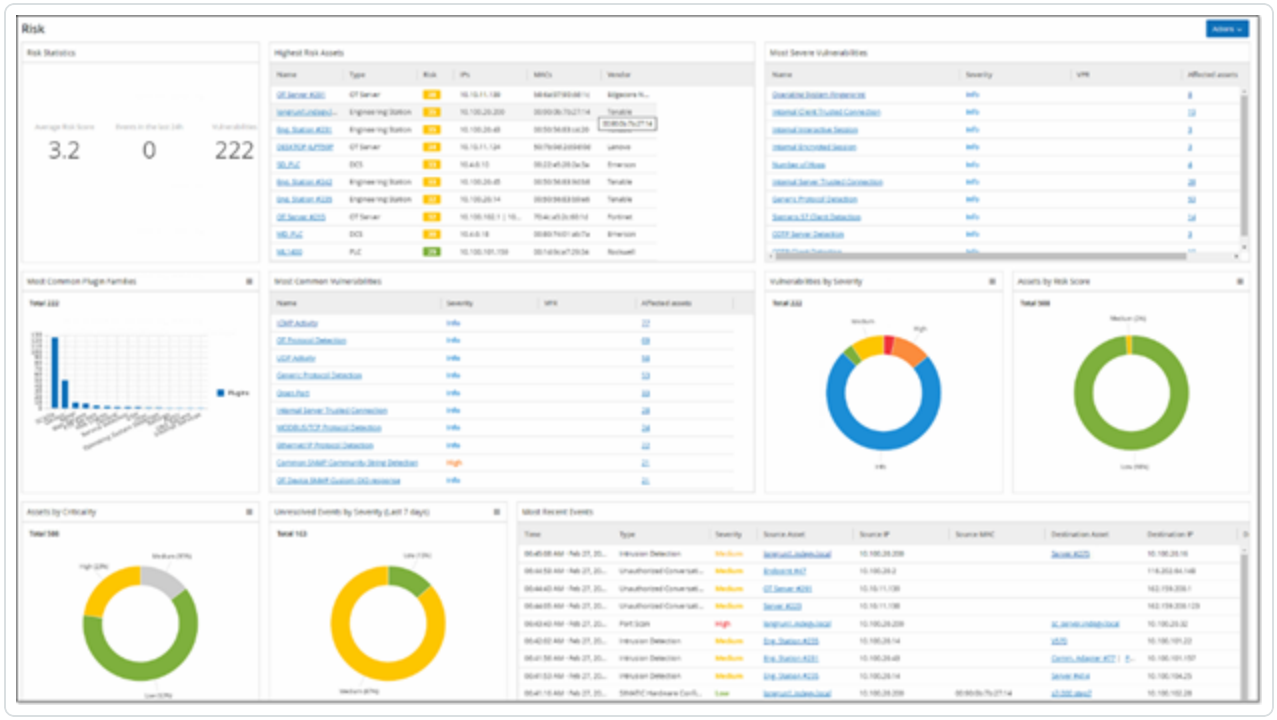
- 在主导航菜单中，点击“**仪表盘**”图标。

“**风险**”仪表盘采用初始默认视图；但是，可以将默认视图更改为其他仪表盘。

可以通过调整显示设置和设置筛选条件来与仪表盘交互，请参阅“与仪表盘交互”。

“风险”仪表盘

“**风险**”仪表盘通过搜集资产风险评分和漏洞管理指标，提供有关网络风险暴露情况的见解。

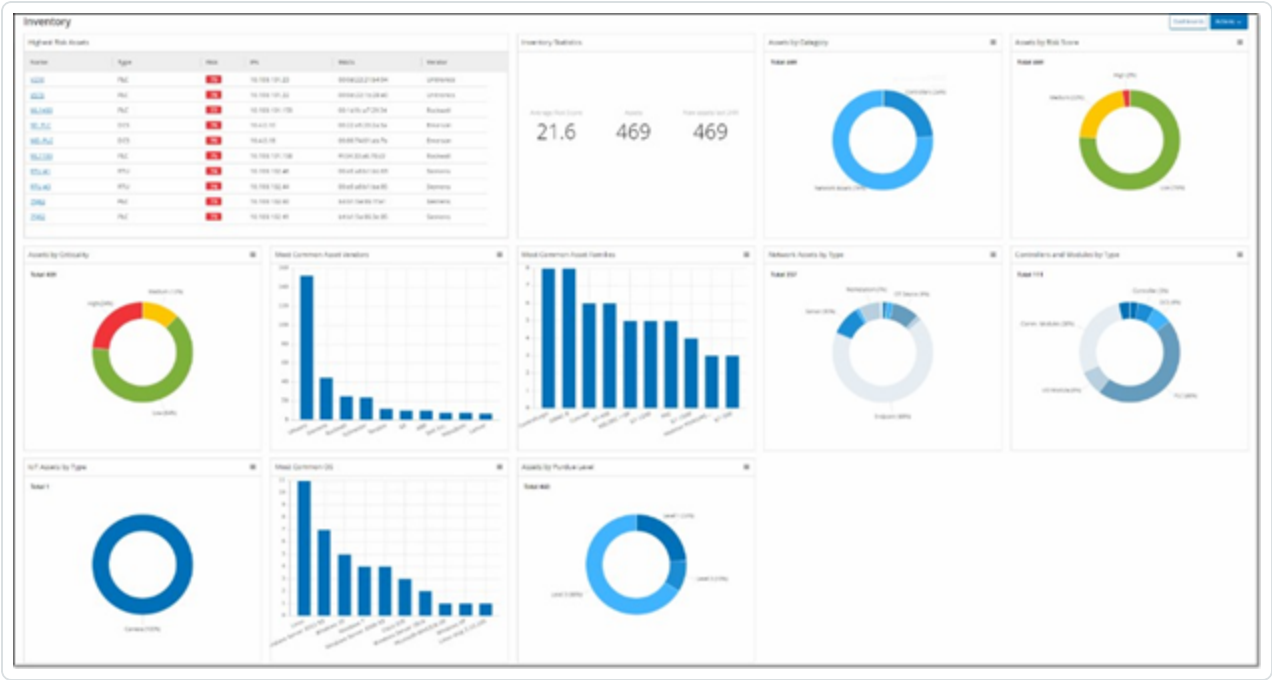


“**风险**”仪表盘显示小组件，例如：风险统计数据、按风险评分分类的资产、按重要程度分类的资产、按严重程度分类的事件、最常见的漏洞等。

单击某个资产或漏洞链接可分别前往“**清单**”或“**漏洞**”屏幕上的相应元素。

“清单”仪表盘

“**清单**”仪表盘便于查看资产清单，有助于资产管理和跟踪。

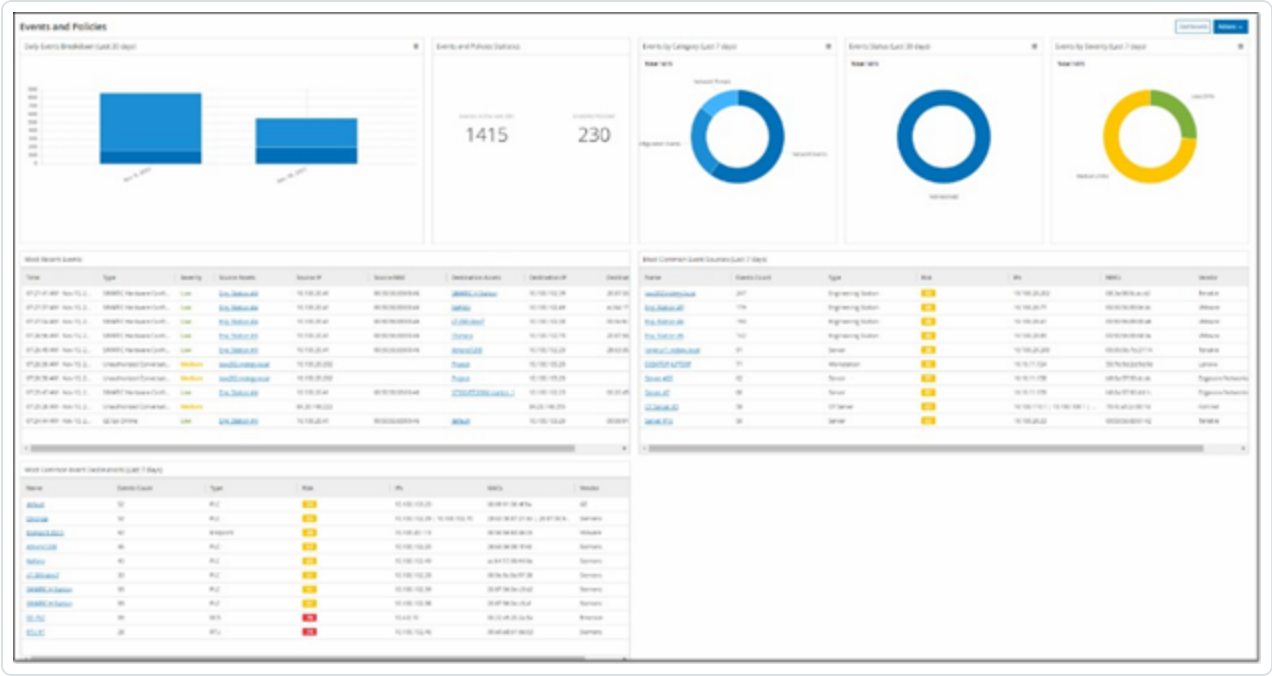


“**清单**”仪表盘显示小组件，例如：最高风险资产、清单统计数据、按风险分类的资产、按类型分类的控制器和模块、按普渡层分类的资产等。

单击资产链接可前往“**清单**”屏幕上的相应资产。

“事件和策略”仪表盘

“**事件和策略**”仪表盘提供了一种通过监控已识别事件及其生成的策略违规来检测网络威胁的方法。



“**事件和策略**”仪表盘显示小组件，例如：每日事件明细、事件和策略统计数据、事件状态、最常见的事件目标等。

单击某个资产或事件链接可分别前往“**清单**”或“**事件**”屏幕上的相应元素。

与仪表盘交互

可以通过与小组件交互来调整仪表盘显示。仪表盘上有两种数据显示模式:图形模式和表格模式。一些小组件具有固定的显示模式,而另外一些则可在模式之间来回切换。您可以在图形模式或表格模式下查看在右上角带有符号的小组件。单击表格/图形符号即可在模式之间切换。

注意:您只能在表格模式下应用筛选条件。设置筛选条件后,该筛选条件将在图形模式中应用。

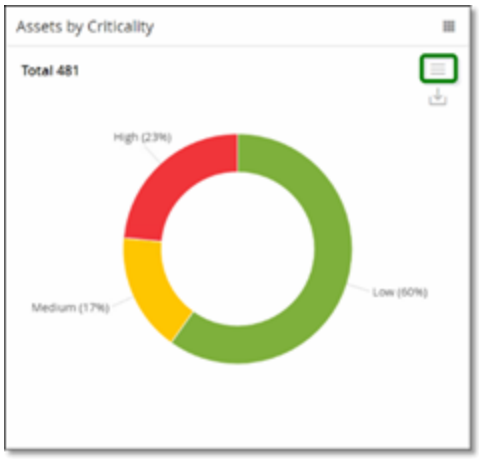
图形模式

图形模式可以图形方式显示小组件数据。

可以通过以下方式与小组件交互:

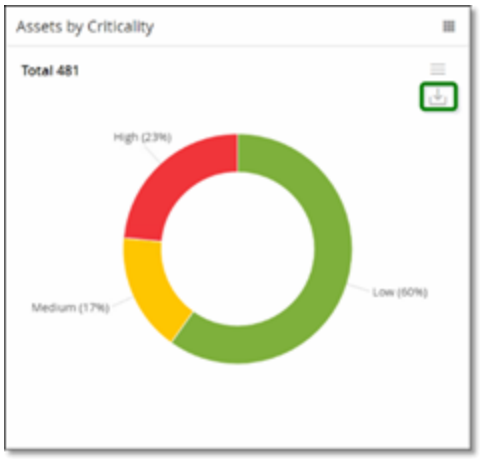
- 将鼠标悬停在图表上的某个点会显示一个窗口,该窗口中包含特定于图表中该区段的数据。

- 您可以通过单击右上角的"**设置**"按钮来调整用于显示的图表类型。

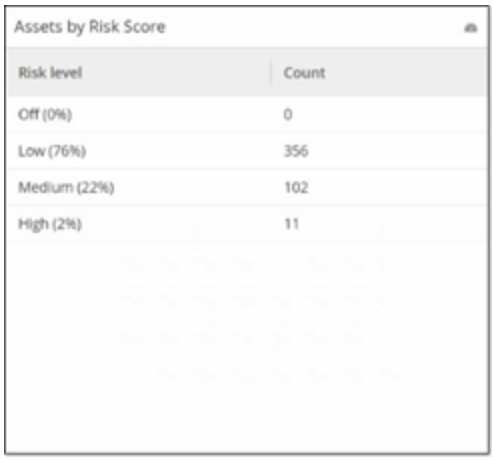


- 然后，您可以从"**设置**"菜单中选择其他一种图表类型。

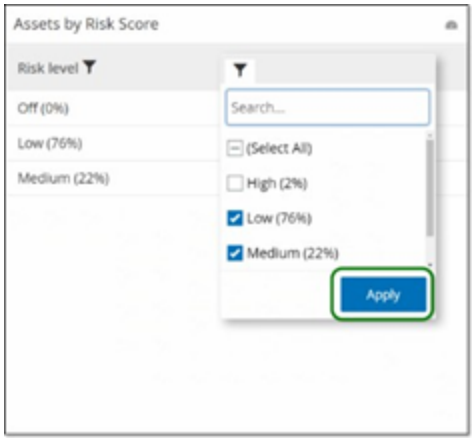
- 在图表模式下查看小组件时，可通过将鼠标悬停在小组件上并单击"**下载**"图标来下载图形图像。



表格模式



在表格模式下查看小组件时，可以将鼠标悬停在列标题上，单击筛选条件图标，选择筛选条件，然后单击"**应用**"来筛选各列。如果切换到图形模式，筛选条件也将应用于图形。



更改默认仪表盘

风险仪表盘是管理控制台的初始默认视图。可以指定一个不同的仪表盘作为默认视图。

若要更改默认仪表盘视图，请执行以下操作：

1. 导航到要用为默认视图的仪表盘。

2. 单击“**操作**”>“**设为默认**”。

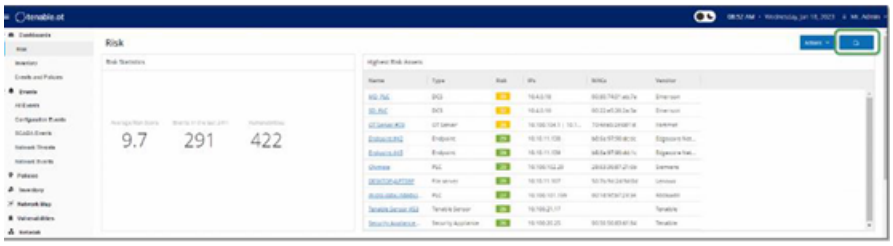
OT Security 会更新默认仪表盘，并在您下次访问管理控制台时显示

导出仪表盘

使用仪表盘屏幕上的“**导出**”按钮，您可以在单独的页面上导出带有每个仪表盘小组件的 PDF 文件。

若要导出仪表盘，请执行以下操作：

1. 单击仪表盘右上角的“**导出**”按钮。



PDF 文件会自动下载到默认的下载文件夹中。

> **注意**：确保浏览器中的仪表盘选项卡在下载 PDF 文件的过程中保持打开状态（2-3 秒）。

2. 文件下载完成后，导航至下载的文件以进行查看或共享。

策略

OT Security 包含用于定义网络中发生的可疑、未授权、异常或值得注意的特定事件类型的策略。当发生满足特定策略的所有策略定义条件的事件时，系统将生成事件。系统会记录事件，并且会根据为该策略配置的策略操作发出通知。

- **基于策略的检测**：会在满足由一系列事件描述符定义的策略的精确条件时触发事件。
- **异常检测**：当 OT Security 在网络中发现异常或可疑活动时触发事件。

OT Security 具有一组预定义的策略（开箱即用）。此外，您可以编辑预定义策略或定义新自定义策略。

> **注意**：默认情况下，大多数策略处于开启状态。如要打开/关闭策略，请参阅"启用或禁用策略"。

策略配置

每个策略都包含一系列定义网络中特定行为类型的条件。这包括活动、涉及的资产和事件的时间安排等考虑因素。只有符合策略中设置的所有参数的事件才会触发该策略的事件。每个策略都有一个指定的策略操作配置，用于定义事件的严重程度、通知方法和日志记录。

组

OT Security 中策略定义的一个基本组件是使用组。配置策略时，每个策略参数均属于组，这与独立实体相反。这可以简化策略配置过程。例如，如果在一天中的特定时间（例如工作时间）在控制器上执行固件更新的活动被视为可疑活动，则不必为网络中的每个控制器创建单独的策略，创建适用于资产组控制器的单一策略即可。

策略配置使用以下类型的组：

- **资产组**：系统随附基于资产类型的预定义资产组。可以根据位置、部门、重要程度等其他因素添加自定义组。
- **网段**：系统根据资产类型和 IP 范围创建自动生成的网段。您可以创建自定义网段，定义任何具有类似通信模式的资产组。
- **电子邮件组**：对接收特定事件的电子邮件通知的多个电子邮件帐户进行分组。例如，按角色、部门等进行分组。
- **端口组**：以类似方式使用的组端口。例如，在 Rockwell 控制器上开放的端口。
- **协议组**：按照协议类型（例如 Modbus）、制造商（例如 Rockwell 允许的协议）等对通信协议进行分组。
- **计划组**：将多个时间范围划分为一个具有某个共同特征的计划组。例如，工作时间、周末等。
- **标签组**：对各种控制器中包含类似操作数据的标签进行分组。例如，控制熔炉温度的标签。
- **规则组**：与组相关的规则，可通过其 Suricata 签名 ID（SID）进行标识。这些组可以用作定义入侵检测策略的策略条件。

只能使用系统中已经配置的组来定义策略。系统提供一组预定义的组。您可以编辑这些组并添加专属组，详情请参阅“组”

注意:只能使用组设置策略参数,即使希望将某个策略应用于单个实体,也必须配置仅包含该实体的组。

严重程度级别

每个策略都分配有特定的严重程度级别,而该级别指示触发事件的情况所造成的风险程度。下表介绍了各种严重程度:

严重程度	描述
无	该事件无需关注。
低	没有立即予以关注。应在方便时检查。
中	适度关注,已发生潜在危害活动。应在方便时予以处理。
高	高度关注,已发生潜在危害活动。应立即处理。

事件通知

当发生满足某项策略的条件的事件时,系统中将生成事件。"**事件**"部分显示"**所有事件**"。"**策略**"页面在触发事件的策略下列出事件,"**清单**"页面在受影响的资产下列出事件。此外,您可将策略配置为使用 Syslog 协议向外部 SIEM 和/或向指定电子邮件收件人发送事件通知。

- **Syslog 通知**:Syslog 消息使用包含标准密钥和自定义密钥(经过配置,可与 OT Security 一起使用)的 CEF 协议。有关如何解释 Syslog 通知的说明,请参阅"OT Security Syslog 集成指南"。
- **电子邮件通知**:电子邮件消息包含有关生成通知的事件的详细信息,以及缓解威胁的步骤。

策略类别和子类别

OT Security 按照以下类别整理策略:

- **配置事件**:这些策略与网络中发生的活动有关。共有两个子类别:
  - **控制器验证**:这些策略与网络中的控制器发生的变更有关。这可能涉及控制器状态变更,以及固件、资产属性或代码块变更。可以限制策略用于特定计划(例如,工作日期间升级固件)和/或特定控制器。
  - **控制器活动**:这些策略与影响控制器状态和配置的特定工程命令有关。可以定义始终生成事件的特定活动,或指定用于生成事件的一组标准。例如,在某些时间和/或在某些控制器上执行某些活动。支持将资产、活动和计划列入屏蔽列表和允许列表。
- **网络事件**:这些策略与网络中的资产以及资产之间的通信流有关。这包括添加到网络或从网络删除的资产。它还包括网络的异常流量模式,或已被标记为引起关注的流量模式。例如,如果工程站用于与控制器通信的协议不属于预配置协议组(例如,由特定供应商制造的控制器使用的协议),则会触发事件。这些策略可限制用于特定计划和/或特定资产。为方便起见,供应商会整理特定于供应商的协议,同时您可以在策略定义中使用任何协议。
- **SCADA 事件策略**:这些策略会检测设定点值的变更(可能会危害工业过程)。这些变更可能是网络攻击或人为错误所致。
- **网络威胁策略**:这些策略使用基于签名的 OT 和 IT 威胁检测,来识别表示入侵威胁的网络流量。此类检测基于已在 Suricata 威胁引擎中编目的规则。

策略类型

每个类别和子类别内都包含一系列不同的策略类型。OT Security 包括每种类型的预定义策略。您还可以针对每种类型创建专属自定义策略。下表说明了按类别分组的各种策略类型。

配置事件:控制器活动事件类型

控制器活动与网络中发生的活动相关。即在网络中的资产之间实施的"命令"。有许多不同类型的控制器活动事件。发生活动的控制器的类型以及特定活动定义了控制器活动类型。例如,Rockwell PLC 停止、SIMATIC 代码下载、Modicon 在线会话等。

适用于控制器活动事件的"策略定义"参数(即策略条件)为"源资产"、"目标资产"和"计划"。

配置事件:控制器验证活动事件类型

下表介绍了各种类型的控制器验证事件。

注意:可以通过选择"资产组"或"网段"来指定与受影响的资产、源或目标相关的策略条件。

事件类型	策略条件	描述
密钥开关变更	受影响的资产、计划	通过调整物理密钥位置对控制器状态进行了更改。目前仅支持 Rockwell 控制器。
状态变更	受影响的资产、计划	控制器从一种操作状态变为另一种。例如运行、停止、测试等。
固件版本变更	受影响的资产、计划	对控制器上运行的固件进行了更改。
模块未出现	受影响的资产、计划	检测已从背板中去除的之前识别的模块。
发现新模块	受影响的资产、计划	检测添加到现有背板的新模块。
快照不匹配	受影响的资产、计划	控制器的最新快照(捕获控制器上部署的程序的当前状态)与该控制器之前的快照不同。

网络事件类型

下表介绍了各种类型的网络事件。

注意:可以通过选择"资产组"或"网段"来指定与受影响的资产、源或目标相关的策略条件。

事件类型	策略条件	描述
资产未出现	未出现,受影响的资产、计划	检测之前在指定时间范围内从网络中删除的"受影响资产"组中识别的资产。
USB 配置变更	受影响的资产、计划	检测 USB 设备何时连接到基于 Windows 的工作站或从其中删除。该策略适用于指定时间范围内受影响资产组中的资产变更。
IP 冲突	计划	使用相同的 IP 地址检测网络中的多项资产。这可能表示存在网络攻击,也可能是指由网络管理不当所致。该策略适用于在指定时间范围内 OT Security 发现的 IP 冲突。
网络基线偏差	源、目标、协议、计划	检测网络基线采样期间未相互通信的资产之间的新连接。只有在系统中设置了网络基线之后,此选项才可用。如要设置初始网络基线或更新网络基线,请参阅"设置网络基线"。该策略适用于在指定时间范围内,使用"协议"组中的协议从"源"资产组中的资产到"目标"资产组中的资产的通信。
发现新资产	受影响的资产、计划	检测指定时间范围内网络中显示的"源"资产组中指定类型的新资产。
已打开的端口	受影响的资	检测网络中的新已打开的端口。未使用的已打开的端口会招致安全风险。该策略适用于受影响资产组中的资产,以及端口组中的

	产、端口	端口。
网络流量激增	时间窗口、敏感度等级、计划	检测网络流量中的异常峰值。该策略适用于与指定时间窗口相关且基于指定敏感度等级的峰值。该策略也仅限于指定时间范围。
对话中的峰值	时间窗口、敏感度等级、计划	检测网络中对话数量的异常峰值。该策略适用于与指定时间窗口相关且基于指定敏感度等级的峰值。该策略也仅限于指定时间范围。
RDP 连接(经过身份验证)	源、目标、计划	已使用身份验证凭据在网络中建立 RDP(远程桌面连接)。该策略适用于在指定时间范围内,连接到"目标"资产组中的"源"资产组中的资产。
RDP 连接(未经身份验证)	源、目标、计划	未使用身份验证凭据在网络中建立 RDP(远程桌面连接)。该策略适用于在指定时间范围内,连接到"目标"资产组中的"源"资产组中的资产。
未经授权的对话	源、目标、协议、计划	检测网络中各个资产之间发送的通信。该策略适用于在指定时间范围内,"源"资产组中的资产使用"协议"组中的协议发送到"目标"资产组中的资产的通信。
不安全的 FTP 登录成功	源、目标、计划	OT Security 将 FTP 视为不安全协议。此策略检测使用 FTP 的成功登录。
不安全的 FTP 登录失败	源、目标、计划	OT Security 将 FTP 视为不安全协议。此策略检测使用 FTP 失败的登录尝试。
不安全的 Telnet 登	源、目标、计	OT Security 将 Telnet 视为不安全协议。此策略检测使用 Telnet 的成功登录。

录成功	划	
不安全的 Telnet 登录失败	源、目标、计划	OT Security 将 Telnet 视为不安全协议。此策略检测使用 Telnet 失败的登录尝试。
不安全的 Telnet 登录尝试	源、目标、计划	OT Security 将 Telnet 视为不安全协议。此策略检测使用 Telnet 的登录尝试(未检测到其结果状态) 。

网络威胁事件类型

下表介绍了各种类型的网络威胁事件。

注意:可以通过选择"资产组"或"网段"来指定与受影响的资产、源或目标相关的策略条件。

事件类型	策略条件	描述
入侵检测	源、受影响的资产、规则组、计划	入侵检测策略使用基于签名的 OT 和 IT 威胁检测, 来识别表示入侵威胁的网络流量。此类检测基于已在 Suricata 威胁引擎中编目的规则。这些规则被划分为类别(例如 ICS 攻击、拒绝服务、恶意软件等) 和子类别(例如 ICS 攻击 - Stuxnet、ICS 攻击 - BlackEnergy 等) 。系统提供一系列相关规则的预定义组。您还可以为各种规则配置专属的自定义分组。 **注意**:您无法编辑入侵检测系统 (IDS) 事件的"**源**"和"**目标**"资产组。
ARP 扫描	受影响的资产、计划	检测网络中运行的 ARP 扫描(网络侦查活动) 。该策略适用于在指定时间范围内受影响资产组中的广播扫描。
端口扫描	源资产、目标资	检测网络中运行的 SYN 扫描(网络侦查活动) , 以检测开放(易受攻击) 端口。该策略适用于在指定时间范围内, 从"源"资产组中的资产到"目标"资产组中的资产的通信。

	产、计划	

SCADA 事件类型

下表介绍了各种类型的 SCADA 事件类型。

注意:可以通过选择"资产组"或"网段"来指定与受影响的资产、源或目标相关的策略条件。

事件类型	策略条件	描述
Modbus 非法数据地址	源资产、目标资产、计划	检测 Modbus 协议中的"非法数据地址"错误代码。该策略适用于在指定时间范围内，从"源"资产组中的资产到"目标"资产组中的资产的通信。
Modbus 非法数据值	源资产、目标资产、计划	检测 Modbus 协议中的"非法数据值"错误代码。该策略适用于在指定时间范围内，从"源"资产组中的资产到"目标"资产组中的资产的通信。
Modbus 非法函数	源资产、目标资产、计划	检测 Modbus 协议中的"非法函数"错误代码。该策略适用于在指定时间范围内，从"源"资产组中的资产到"目标"资产组中的资产的通信。
未经授权的写入	源资产、标签组、标签值、计划	检测未经授权写入指定"源"资产组中的控制器（目前支持 Rockwell 和 S7 控制器）上的指定标签的情况。您可以配置策略以检测任何新的写入、指定值变更或指定范围之外的值。该策略仅在指定时间范围内适用。

ABB - 未经授权的写入	源资产、目标资产、计划	检测通过 MMS 发送到 ABB 800xA 控制器且超出允许范围的写入命令。
IEC 60870-5-104 命令(开始/停止数据传输、质询命令、计数器质询命令、时钟同步命令、重置进程命令、带时间标签的测试命令)	源资产、目标资产、计划	检测发送到被认为有风险的 IEC-104 父设备或子设备的特定命令。
DNP3 命令	源资产、目标资产、计划	检测使用 DNP3 协议发送的所有主要命令。例如,“选择”、“操作”、“热/冷重新启动”等。还可检测源自内部指示符的错误,例如不受支持的函数代码和参数错误。

启用或禁用策略

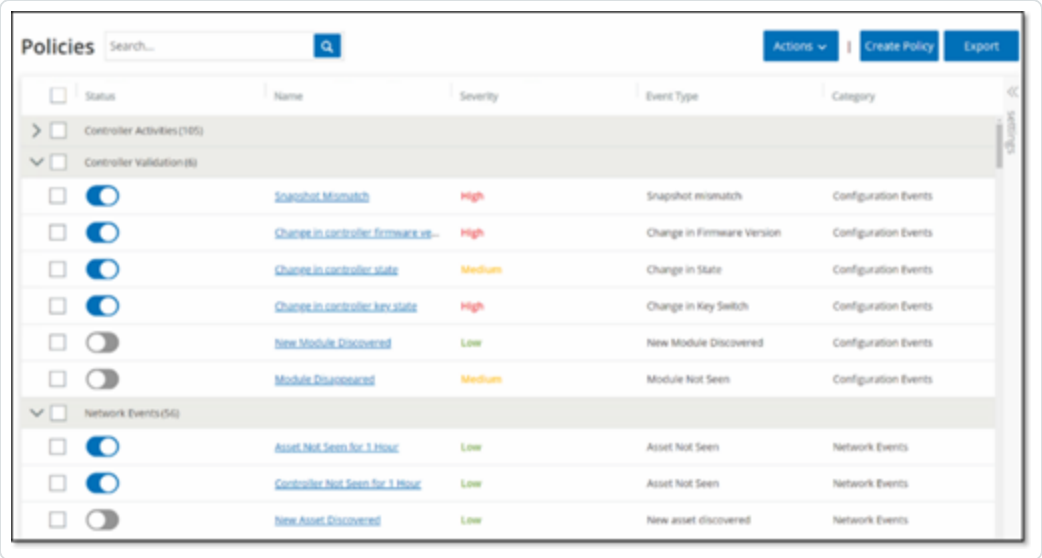
您可以启用或禁用系统中任何已配置的策略(预配置和用户定义)。您可以打开和关闭单个策略,也可以选择多个策略以在批量进程中打开/关闭。

注意:许多策略依赖查询来收集数据。如果禁用部分或所有查询功能,则相关策略将失效。您可以从**主动查询**激活查询,详情请参阅"主动查询"。

若要启用或禁用策略,请执行以下操作:

1. 转至"**策略**"。

   该页面列出了系统中配置的所有策略,并按策略类别分组。

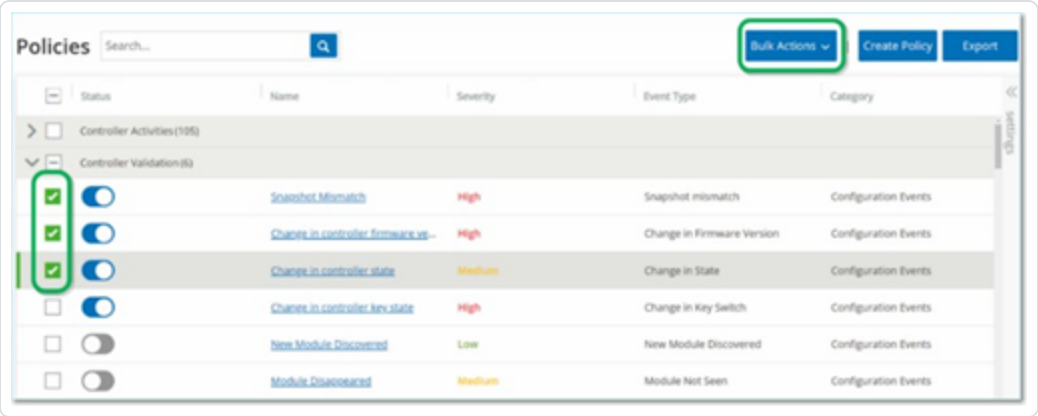


2. 若要启用或禁用该策略,请单击相关策略旁边的"**状态**"切换开关。

若要打开/关闭多种策略,请执行以下操作:

1. 转至"**策略**"。

   该页面列出了系统中配置的所有策略,并按策略类别分组。



2. 选中要打开/关闭的每个策略旁边的复选框。请使用下列选择方法中的一种：

   - **选择单个策略**：单击特定策略旁的复选框。
   - **选择策略类型**：单击策略类型标题旁的复选框。
   - **选择所有策略**：单击表顶部标题栏中的复选框。

3. 从“**批量操作**”下拉框中选择所需的操作（“**启用**”或“**禁用**”）。

   OT Security 启用或禁用所选策略。

查看策略

"**策略**"屏幕列出了系统中的所有已配置的策略。在每个策略类别的单独选项卡下对这些列表进行了分组。此页面上同时列出了预配置的策略和用户定义的策略。每个策略均包含一个显示策略当前状态的切换开关，以及指示策略配置的多个参数。

可以显示/隐藏列，并对资产列表进行排序和筛选，同时搜索关键字。有关定制列表的信息，请参阅"管理控制台用户界面元素"。

下表中介绍了策略参数：

参数	描述
状态	显示策略是打开还是关闭。如果系统由于生成过多事件而自动禁用该策略，则会在切换开关旁边显示一个警告图标。切换状态开关，以打开/关闭某个策略。
策略 ID	系统中策略的唯一标识符。策略 ID 按类别分组，每个类别都具有不同的前缀。例如，P1 代表控制器活动，P2 代表网络事件，等等。
名称	策略的名称。
严重程度	事件的严重程度。可能的值为：无、低危、中危或高危。有关严重程度级别的说明，请参阅严重程度级别部分。
事件类型	触发此事件策略的特定事件类型。
类别	触发此事件策略的事件类型的常规类别。可能的值为：配置、SCADA、网络威胁或网络事件。有关各种类别的说明，请参阅"策略类别和子类别"。
源	策略条件。应用策略的源资产组/网段（即发起活动的资产）。
目标资产/受影响的资产	策略条件。应用策略的目标资产组/网络区段（即收到活动的资产）。对于涉及单一资产（无源和目标）的策略，此参数会显示受事件影响的资产。
计划	策略条件。策略适用的时间范围。
Syslog	记录此策略的事件的 Syslog 服务器 (SIEM)。
电子邮件	电子邮件组向此策略发送事件通知。

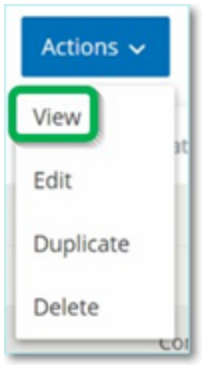
子类别	事件的子类别。“配置事件”类别包含子类别“控制器活动”和“控制器验证”。如需了解关于不同子类别的信息，请参阅“查看策略”。
每个策略的事件数量	列出每个策略生成的事件数量。您可以点击该列，对列表进行排序，以便重点关注违规/事件最多的策略。
排除项	列出添加到每个策略的排除项的数量。有关更多信息，请参阅“事件”。

查看策略详细信息

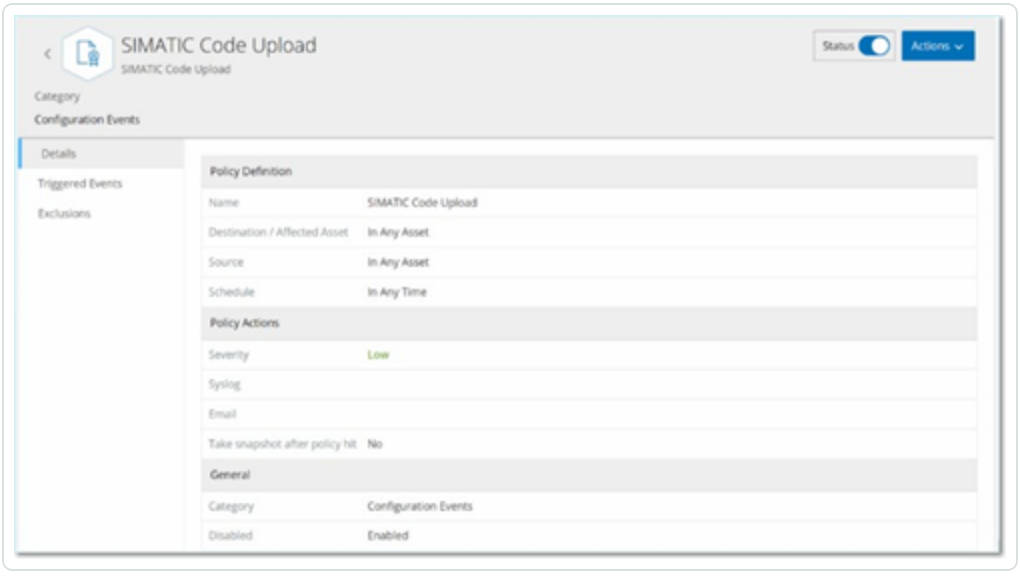
策略的"**策略详细信息**"页面显示关于该策略的更多详细信息。此页面列出了该策略触发的所有策略条件和事件。

若要打开特定策略的"**策略详细信息**"屏幕，请执行以下操作：

1. 在"**策略**"页面上，选择所需的策略。
2. 从"**操作**"下拉框中选择"**查看**"。



此时会显示所选策略的"策略详细信息"屏幕。



注意：您还可以通过右键单击相关策略访问"操作"菜单。

"策略详细信息"页面包含以下元素：

- **标题栏**：显示策略的名称、类型和类别。此页面还有一个用于启用/禁用策略的切换开关，以及一个可用**操作**（“**编辑**”、“**复制**”和“**删除**”）的下拉列表。
- **“详细信息”选项卡**：显示这些部分中有关策略配置的详细信息：
  - **策略定义**：显示所有策略条件。根据策略类型，这包括所有相关字段。
  - **策略操作**：显示事件通知的严重程度级别和目标（Syslog、电子邮件）。此外还会显示“**在策略命中后生成快照**”功能是否已激活。
  - **常规**：显示策略的类别和状态。
- **触发的事件**：显示此策略触发的事件的列表。它还显示有关事件中涉及的资产和事件性质的详细信息。此选项卡中显示的信息与“**事件**”页面上显示的信息相同，只不过此选项卡仅显示指定策略的事件。有关事件信息的说明，请参阅“查看事件”。

  “**排除项**”选项卡：如果某项策略针对不造成安全威胁的特定情况生成事件，则可以从该策略中排除这些情况（即停止针对这些特定情况生成事件）。您可以在“**事件**”页面添加排除项，详情请参阅“事件”。“**排除项**”选项卡显示应用到此策略的所有排除项，并针对每个排除项显示特定的排除条件。您可以通过此选项卡删除排除项，以便系统能够针对指定条件重新生成事件。

创建策略

您可以根据 ICS 网络的特定注意事项创建自定义策略。您可以准确确定必须提请工作人员注意的事件类型以及发送通知的方式。您可以完全灵活地确定要为每个策略提供的定义的具体程度或广泛程度。

> **注意**：可以使用系统中配置的组来定义策略。如果某个参数的下拉列表未出现要应用策略的特定分组，则可以根据需要创建新组，详情请参阅“组”。

创建新策略时，首先选择要创建的策略的“类别”和“类型”。“创建策略”向导将指导您完成设置过程。每个策略类型都有其专属相关策略条件参数集。“创建策略”向导会显示所选策略类型的相关策略条件参数。

对于“源”、“目标”和“计划”参数，可以指定将指定的组列入允许列表还是阻止列表。

- 选择“**位于其中**”，以将指定的组列入允许列表（即将其包含在策略中），或
- 选择“**不在其中**”，以将指定的组列入阻止列表（即将其排除在策略之外）。

对于“资产组”和“网段”参数（即“源”、“目标”和“受影响的资产”），可以使用逻辑运算符（与/或）将策略应用于预定义组的各种组合或子集。例如，若要将策略应用到 ICS 设备或 ICS 服务器，则选择“ICS 设备”或“ICS 服务器”。若要将策略仅应用到控制器（位于工厂 A 内），则选择“控制器”和“工厂 A 设备”。

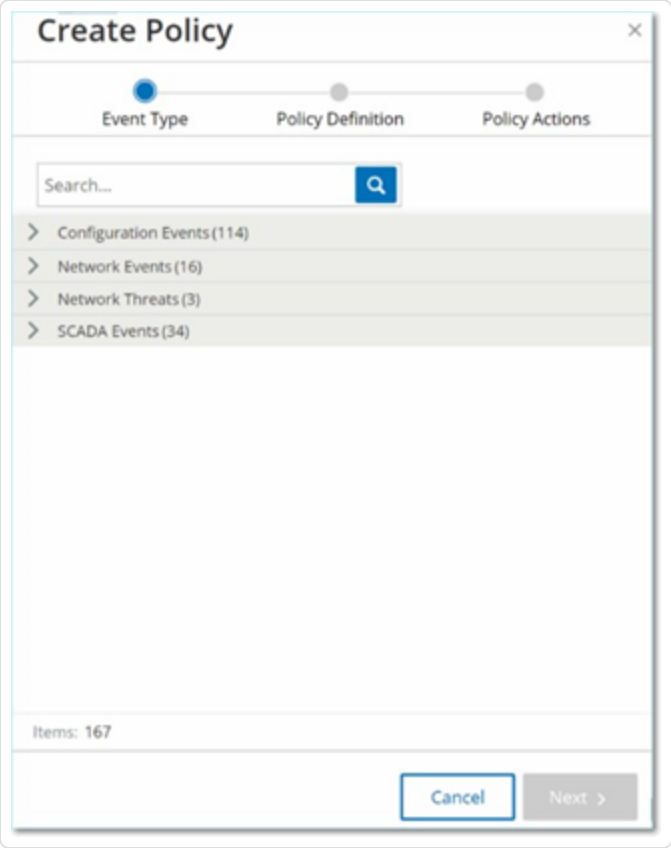
如果要使用与现有策略类似的参数创建新策略，您可以复制原始策略并进行必要的更改，详情请参阅“创建策略”部分。

注意：在创建策略后，如果发现该策略为无需关注的情况生成事件，则可从策略中排除特定情况，详情请参阅“事件”。

若要创建新策略，请执行以下操作：

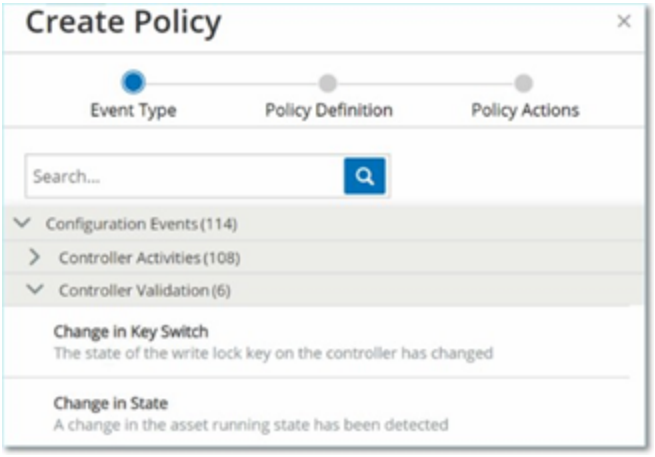
1. 在“**策略**”屏幕上，单击“**创建策略**”。

   此时会打开“**创建策略**”向导。

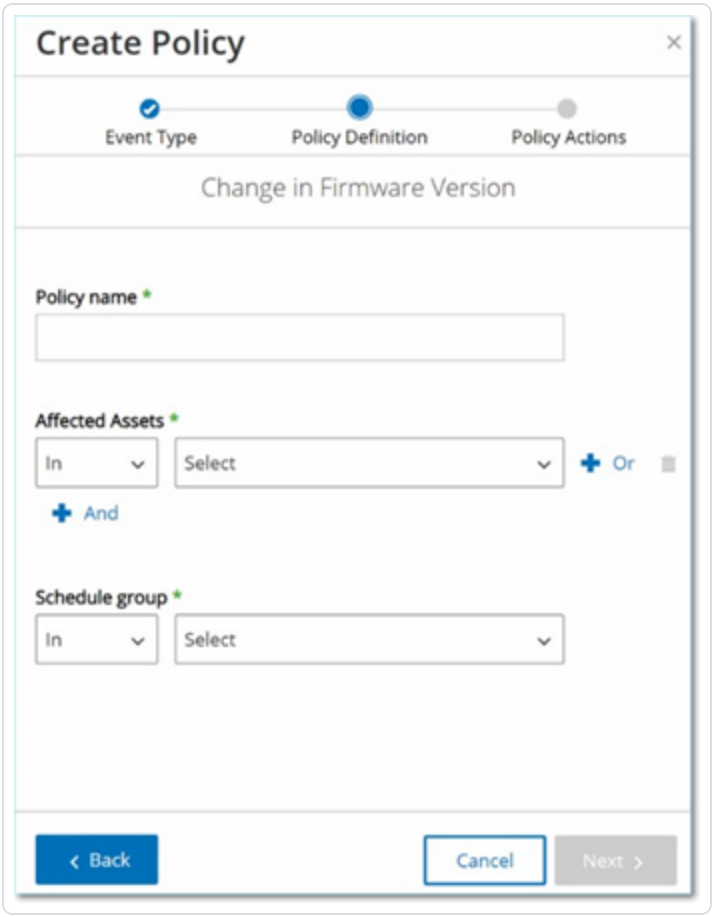


2. 单击“**策略类别**”以显示子类别和/或策略类型。

   此时会显示该类别中包含的所有子类别和/或类型的列表。



3. 选择策略类型。



4. 单击“**下一步**”。

   此时会显示一系列用于定义策略的参数。其中包括适用于所选策略类型的所有相关策略条件。

5. 在“**策略名称**”字段中，为此策略输入一个名称。

   > **注意**：选择一个可以说明策略计划检测的事件类型的特定性质的名称。

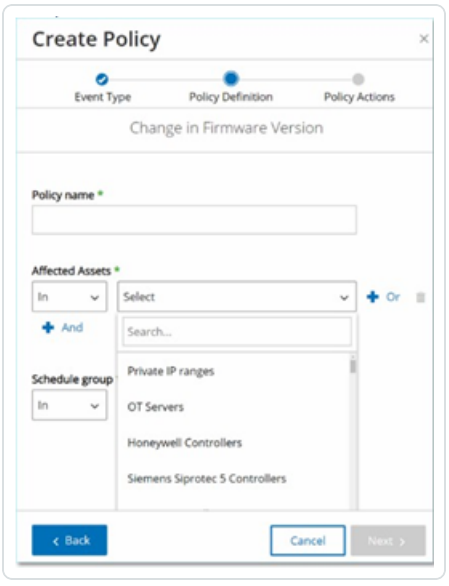
6. 对于每个参数：

   > **重要提示**：您无法编辑入侵检测系统 (IDS) 事件的“**源**”和“**目标**”资产组。

   a. 如果相关，则选择“**位于其中**”（默认），以将所选元素列入允许列表，或选择“不在其中”，以将所选元素列入阻止列表。

   b. 单击“**选择**”。

      此时会显示相关元素（例如资产组、网络区段、端口组、计划组等）的下拉列表。



   c. 选择所需的元素。

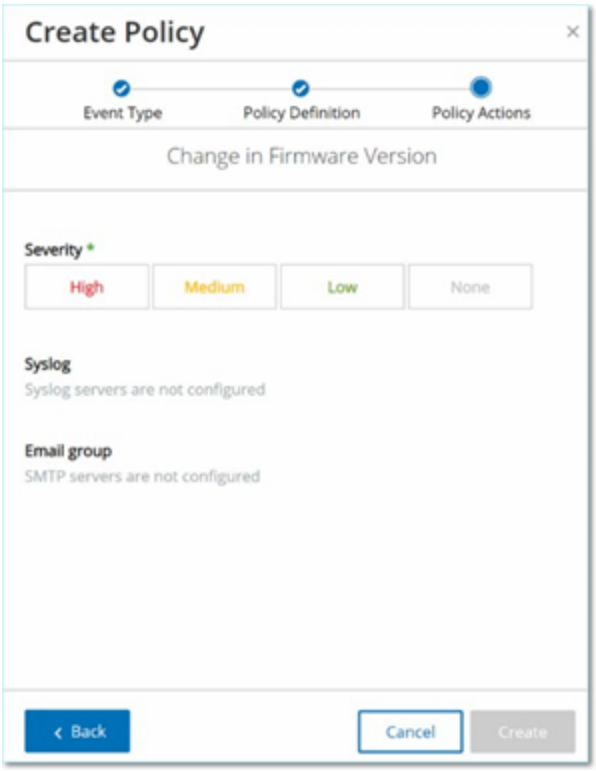
   > **注意**：如果要应用策略的精确分组不存在，则可以根据需要创建新组，详情请参阅“组”。

d. 对于“资产”参数(即“源”、“目标”和“受影响的资产”) , 若想添加具有“或”条件的其他资产组/网段 , 请单击该字段旁的蓝色“**+ 或**”按钮并选择另一个资产组/网段。

e. 对于“资产”参数(即“源”、“目标”和“受影响的资产”) , 若想添加具有“与”条件的其他资产组/网段 , 请单击该字段旁的蓝色“**+ 与**”按钮并选择另一个资产组/网段。

7. 单击“**下一步**”。

此时会显示一系列“策略操作”参数(即发生策略命中时系统采取的操作) 。



8. 在**严重程度**部分 , 单击此策略所需的严重程度级别。

9. 若想将事件日志发送到一个或多个 Syslog 服务器 , 请在 **Syslog** 部分选中要向其发送事件日志的每个服务器旁边的复选框。

> **注意** : 如要添加 Syslog 服务器 , 请参阅“Syslog 服务器”。

10. 如果要发送事件的电子邮件通知 , 请在“电子邮件组”字段的下拉列表中选择接收通知的电子邮件组。

> **注意** : 如要添加 SMTP 服务器 , 请参阅“SMTP 服务器”。

11. 在指定操作与之相关的“**其他操作**”部分中：

    - 如果要在首次发生策略命中后禁用该策略，请选中“**在第一次命中后禁用策略**”复选框。（此操作与某些类型的网络事件策略和某些类型的 SCADA 事件策略相关。）
    - 如果要在检测到策略命中时启动受影响资产的自动快照，请选择“**策略命中后生成快照**”复选框。（此操作与某些类型的配置事件策略相关。）

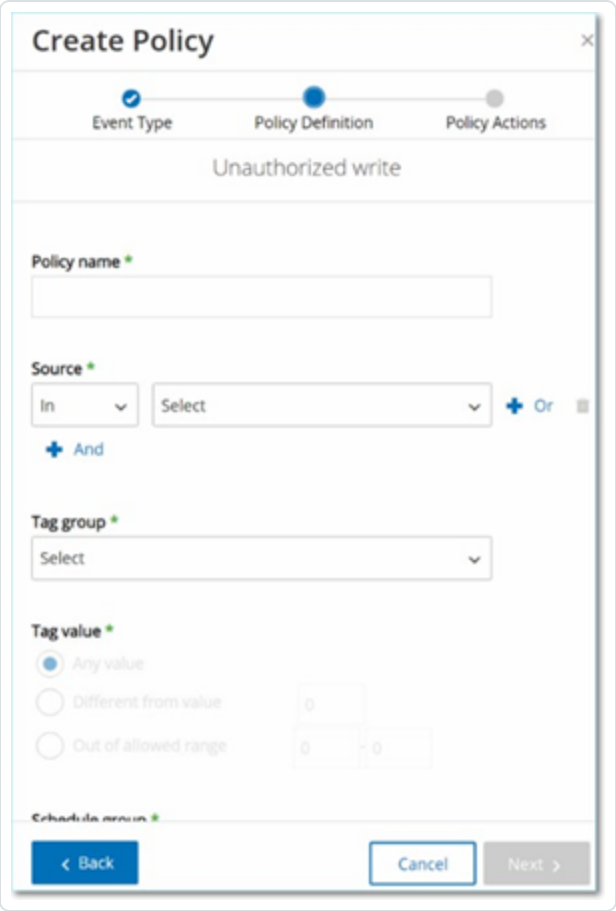
12. 点击“**创建**”。新策略已创建并会自动激活。该策略显示在“策略”屏幕的列表中。

创建未经授权的写入策略

此类策略可检测对控制器标记未经授权的写入。策略定义涉及指定相关标签组和生成策略命中的写入类型。

若要设置未授权写入策略的策略定义，请执行以下操作：

1. 按照“创建策略”中的说明创建新的未经授权的写入策略。



2. 在“策略定义”部分的“**标签组**”字段中，选择要应用此策略的标签组。
3. 在“**标签值**”部分，单击单选按钮并填写必填字段即可选择所需选项。选项包括：
   - **任意值**：选择此选项可检测对标签值的任何更改。
   - **不同于值**：选择此选项可检测指定值以外的任何值。在此选项旁的字段中输入指定值。

- **超出允许范围**:选择此选项可检测超出指定范围的任何值。在此选项旁的相应字段中输入允许范围的下限和上限。

> **注意**:"不同于值"和"超出允许范围"选项仅可用于标准标签类型(例如整数、布尔值等),但不可用于自定义标签或字符串。

4. 完成"创建策略"中所述的策略创建过程。

有关策略的其他操作

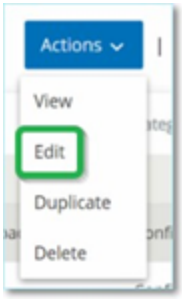
编辑策略

可以编辑预定义策略和用户定义的策略的配置。对于大多数策略，可以调整“**策略定义**”参数（策略条件）和“**策略操作**”参数。对于**入侵检测策略**，只能调整“**策略操作**”参数。

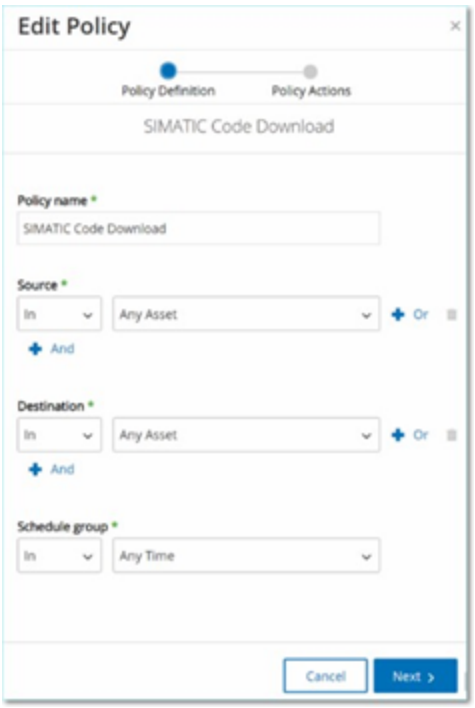
还可以通过批量操作编辑多项策略的“**策略操作**”参数。

若要编辑策略，请执行以下操作：

1. 在“**策略**”窗口中，选中所需策略旁边的复选框。
2. 从“**操作**”下拉框中选择“**编辑**”。



3. 此时会出现“**编辑策略**”窗口，其中包含当前配置。



4. 根据需要调整“**策略定义**”参数。

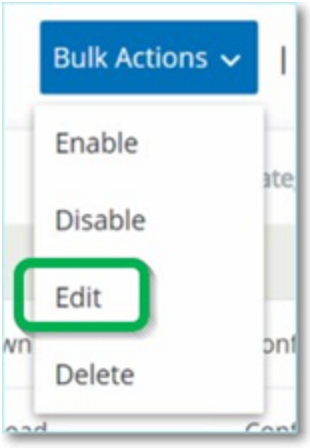
   注意：您无法编辑入侵检测系统 (IDS) 事件的“**源**”和“**目标**”资产组。

5. 单击“**下一步**”。
6. 根据需要调整“**策略操作**”参数。
7. 单击“**保存**”。

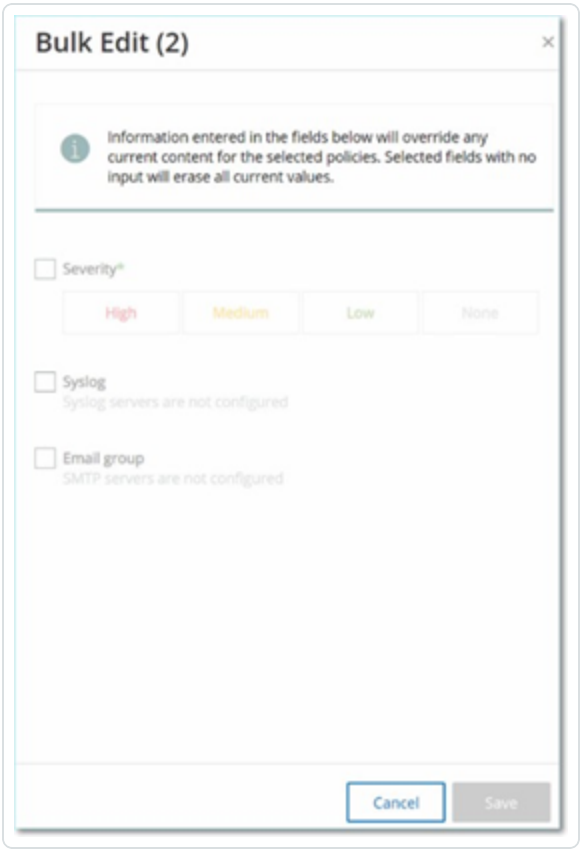
   OT Security 将策略与新配置一起保存。

若要编辑多个策略（批量处理），请执行以下操作：

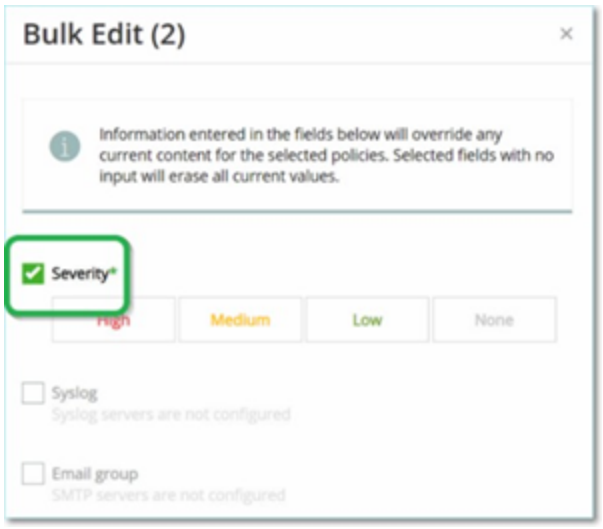
1. 在“**策略**”窗口中，选中两个或更多策略旁边的复选框。
2. 从“**批量操作**”下拉框中选择“**编辑**”。



3. 此时会显示“**批量编辑**”窗口，其中包含可用于批量编辑的策略操作。



4. 选中要编辑的每个参数旁边的复选框：“**严重性**”、“**Syslog**”、“**电子邮件组**”。



5. 根据需要设置每个参数。

> **注意**:在"**批量编辑**"窗口中输入的信息将覆盖选定策略的任何当前内容。如果选中参数旁的复选框但未输入选项,则该参数的当前值将被删除。

6. 单击"**保存**"。

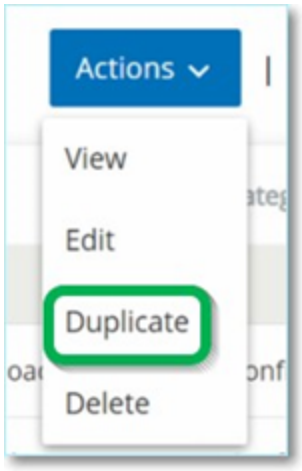
   OT Security 将策略与新配置一起保存。

复制策略

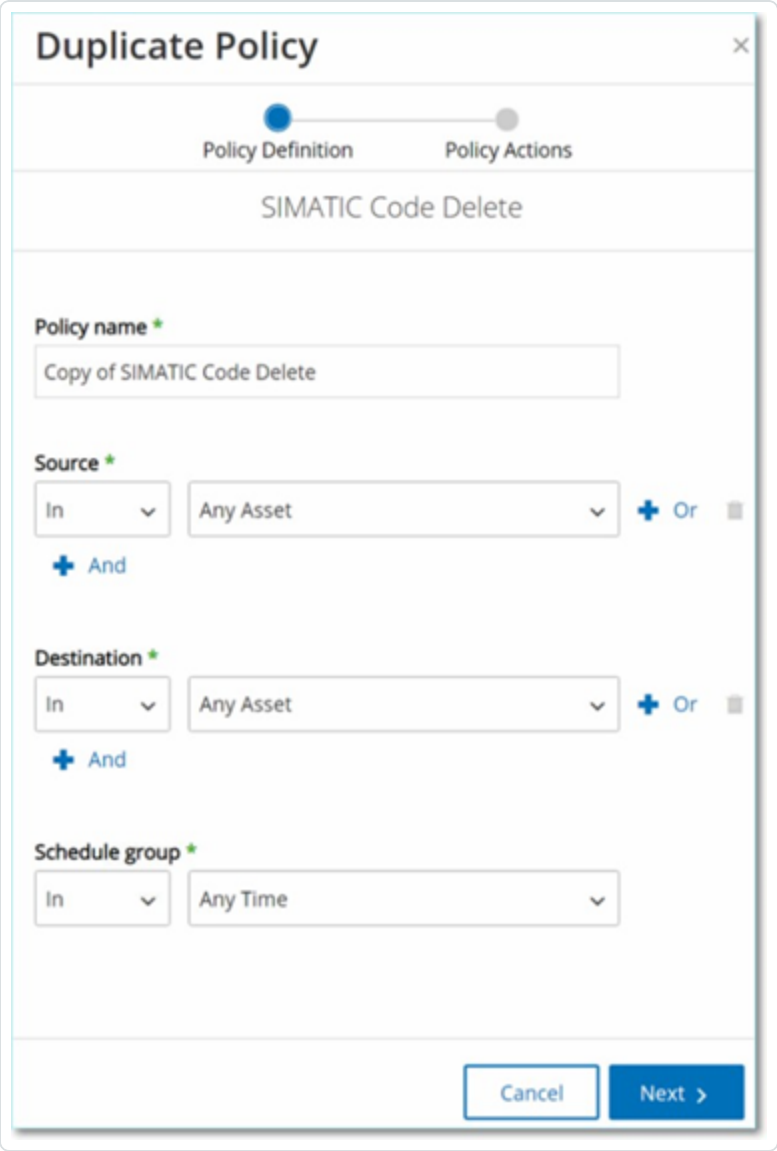
通过复制原始策略并根据需要进行调整，可创建与现有策略类似的新策略。您可以复制预定义和用户定义的策略(**入侵检测策略**除外)。

若要复制策略，请执行以下操作：

1. 在"**策略**"窗口中，选中所需策略旁边的复选框。
2. 从"**操作**"下拉框中选择"**复制**"。



3. "**复制策略**"窗口会显示当前配置，名称默认设置为"*<原始策略名称>的副本*"。



4. 根据需要调整“**策略定义**”参数。
5. 单击“**下一步**”。
6. 根据需要调整“**策略操作**”参数。
7. 单击“**保存**”。

   OT Security 将策略与新配置一起保存。

删除策略

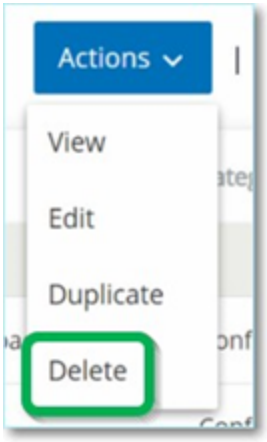
您可以从系统中删除策略。您可以同时删除预定义策略和用户定义的策略(无法删除的**入侵检测策略**除外)。

还可以通过批量操作删除多个策略。

注意:策略从系统中删除后,将无法重新激活。另一种选择是将状态切换为"**关闭**"以暂时将其停用,同时保留以后重新激活它的选项。

若要删除策略,请执行以下操作:

1. 在"**策略**"窗口中,选中所需策略旁边的复选框。
2. 从"**操作**"下拉框中选择"**删除**"。



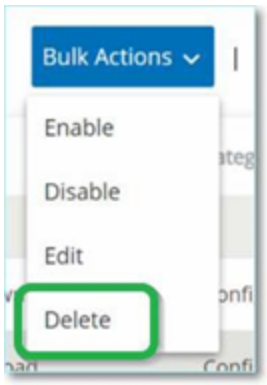
此时会出现"确认"窗口。

3. 点击"**删除**"。

OT Security 会将策略从系统中删除。

若要删除多个策略(批量操作),请执行以下操作:

1. 在"**策略**"窗口中,选中每个所需策略旁边的复选框。
2. 从"**批量操作**"下拉框中选择"**删除**"。



此时会出现"确认"窗口。

3. 点击"**删除**"。

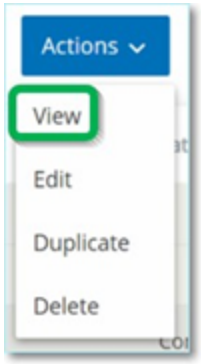
   OT Security 会将策略从系统中删除。

删除策略排除项

如果要删除已应用到特定策略的排除项，可在**策略**窗口中执行此操作。

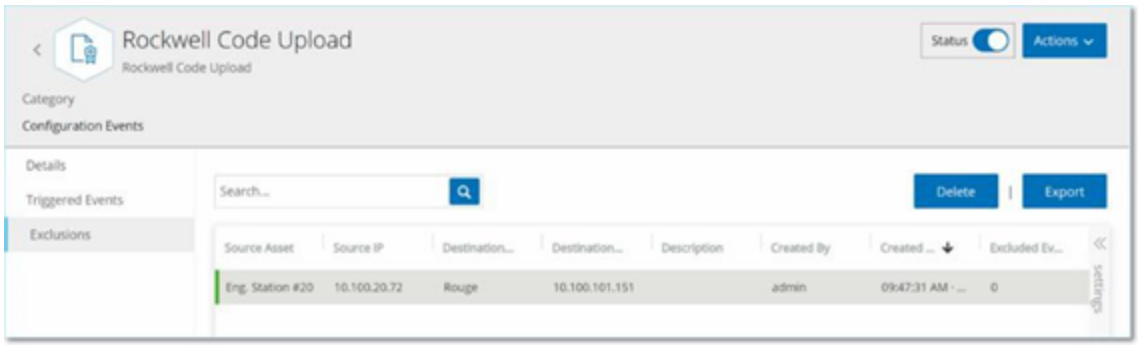
若要删除策略排除项，请执行以下操作：

1. 在"**策略**"窗口中，选择所需策略。
2. 从"**操作**"下拉框中选择"**查看**"。



> **注意**：您还可以通过右键单击相关策略访问"操作"菜单。

3. 单击"**排除项**"选项卡。



此时将出现排除项列表。

4. 选择要删除的策略排除项。
5. 点击“**删除**”。

   此时会出现“确认”窗口。
6. 在确认窗口中，单击“**删除**”。

   OT Security 会将排除项从系统中删除。

组

组是用于构建策略的基本构建块。配置策略时，您可以使用组而不是单个实体来设置每个策略条件。OT Security 提供一些预定义的组。您也可以创建自己的用户定义组。因此，为了简化策略的编辑和创建过程，Tenable 建议提前配置所需组。

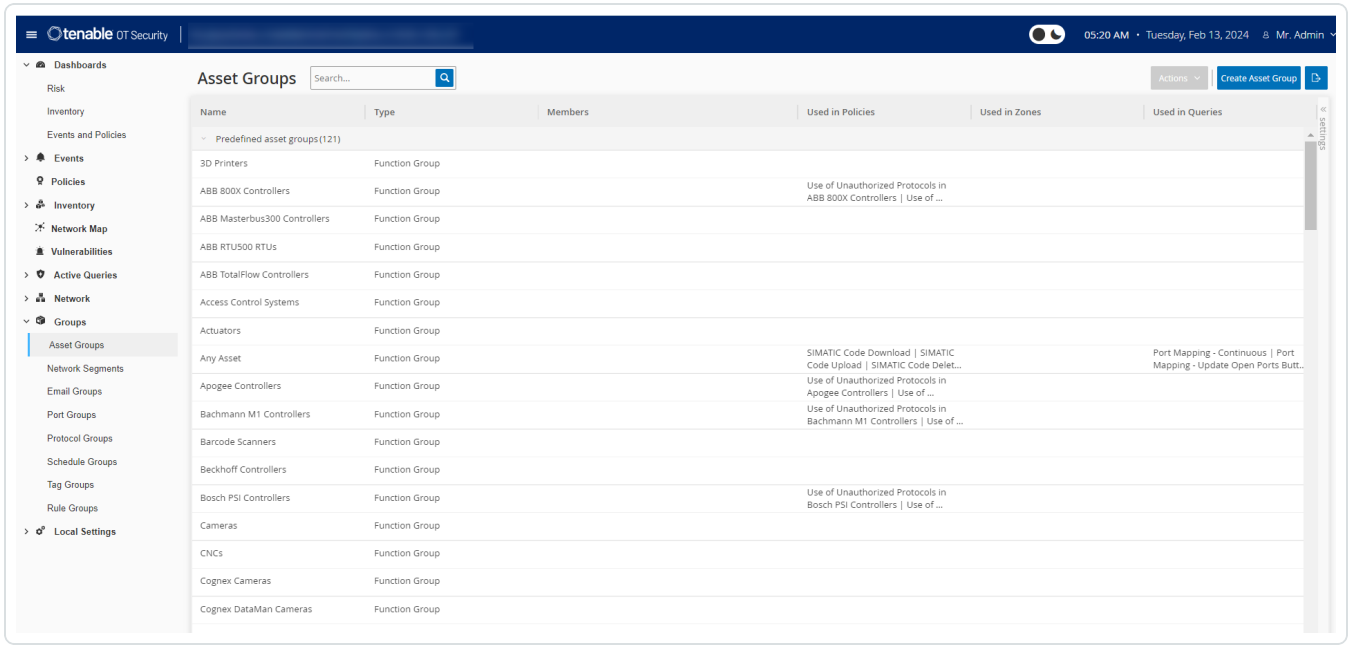
注意：您只能使用“组”设置策略参数。即使希望将某个策略应用于单个实体，也必须配置仅包含该实体的组。

查看组

要查看组：

1. 在左侧导航栏中，单击“**组**”。

   “**组**”部分随即展开，并显示组类型。



在“**组**”下，您可以查看系统中已配置的所有组。组分为以下两类：

- **预定义的组**：经过预先配置，无法编辑。
- **用户定义的组**：您可以创建和编辑这些组。

存在多种不同类型的组，每种类型均可用于配置各种策略类型。每个组类型都显示在“组”下的单独屏幕上。组类型包括：

- **资产组**：资产是网络中的硬件实体。资产组可用作多种策略类型的策略条件。
- **网段**：网段是一种用于创建相关网络资产组的方法，以帮助在逻辑上将一个资产组与另一个资产组隔离。
- **电子邮件组**：发生策略事件时收到通知的电子邮件组。适用于所有策略类型。
- **端口组**：网络中的资产使用的端口组。用于识别已打开的端口的策略。

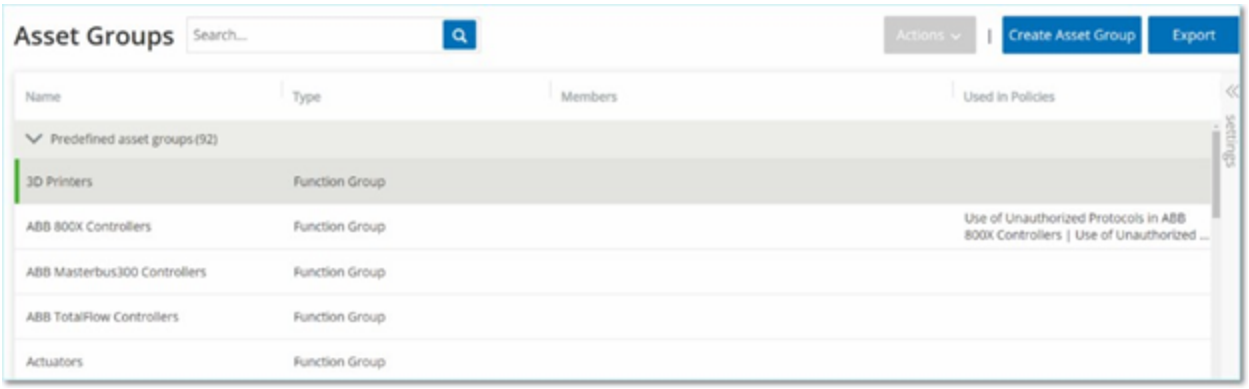
- **协议组**：在网络中的资产之间进行对话所依据的协议组。用作**网络事件**的策略条件。
- **计划组**：计划组定义的是用于配置指定事件必须在什么时间发生才能满足策略条件的时间范围。
- **标签组**：标签是控制器中包含特定操作数据的参数。标签组可用作 SCADA 事件的策略条件。
- **规则组**：规则组由一组相关的规则组成，可以通过其 Suricata 签名 ID (SID) 进行标识。这些组可以用作定义入侵检测策略的策略条件。

以下各节说明了创建每种类型的组的过程。此外，您还可以查看、编辑、复制或删除现有组，详情请参阅“组操作”。

资产组

资产是网络中的硬件实体。将类似的资产划分为同组有助于创建应用于组内所有资产的策略。例如，可以使用资产组“控制器”创建策略，以针对任何控制器的固件变更发出警报。资产组可用作多种策略类型的策略条件。资产组可用于指定各种策略类型的“源”资产、“目标”资产或“受影响的资产”。

查看资产组



“**资产组**”屏幕显示系统中当前配置的所有资产组。“**预定义资产组**”选项卡包含内置于系统中您无法编辑、复制或删除的组。“**用户定义的资产组**”选项卡包含用户创建的自定义组。您可以编辑、复制或删除这些组。

“资产组”表格显示以下信息：

参数	描述
状态	显示策略是打开还是关闭。如果系统由于生成过多事件而自动禁用该策略，则会显示一个警告图标。切换状态开关，以打开/关闭某个策略。
名称	策略的名称。
严重程度	事件的严重程度。可能的值为：无、低危、中危或高危。请参阅“严重程度级别”部分了解更多信息。
事件类型	触发此事件策略的事件类型。
类别	触发此事件策略的事件类别。可能的值为：配置、SCADA、网络威胁或网络事件。

	有关各种类别的说明，请参阅“策略类别和子类别”。
源	策略条件。应用策略的源资产组。资产组是指发起活动的资产。
名称	用于识别组的名称。
类型	组类型。选项包括： • **功能**：为实现特定功能而创建的预定义资产组。 • **资产列表**：组内包含的特定资产。 • **IP 列表**：具有指定 IP 地址的资产。 • **IP 范围**：指定 IP 地址范围内的资产。
成员	显示包含在此组中的资产列表。未出现功能组的值。 **注意**：如果没有空间可以显示此行中的所有资产，则单击“**表格操作**”>“**查看**”>“**成员**”选项卡。
已在以下策略中使用	显示在其配置中使用此资产组的每个策略的名称。 **注意**：如要查看有关使用该组的策略的更多详情，请单击“**表格操作**”>“**查看**”>“**已在以下策略中使用**”选项卡。
在查询中使用	显示使用此资产组的查询的名称。

下一节介绍了创建各种类型的资产组的过程。此外，您还可以查看、编辑、复制或删除现有组，详情请参阅“组操作”。

创建资产组

您可以创建要在策略配置时使用的自定义资产组。将类似的资产划分为同组有助于创建应用于组内所有资产的策略。

存在三种类型的用户定义资产组：

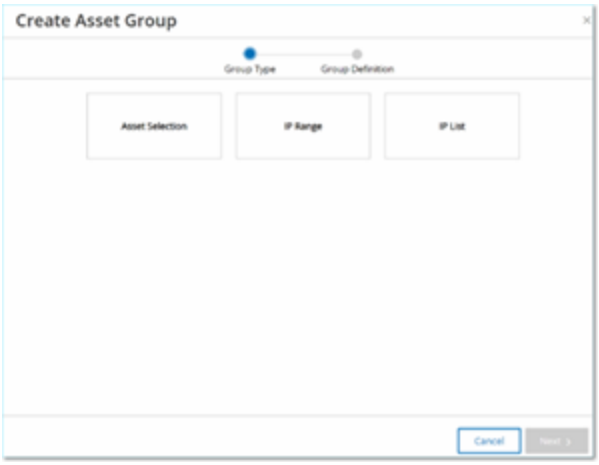
- **资产列表**：指定组内包含的特定资产。
- **IP 列表**：指定组内包含的资产的 IP 地址。
- **IP 范围**：指定组内包含的资产的 IP 地址的范围。

每种类型的资产组都有不同的创建过程。

若要创建资产选择类型资产组，请执行以下操作：

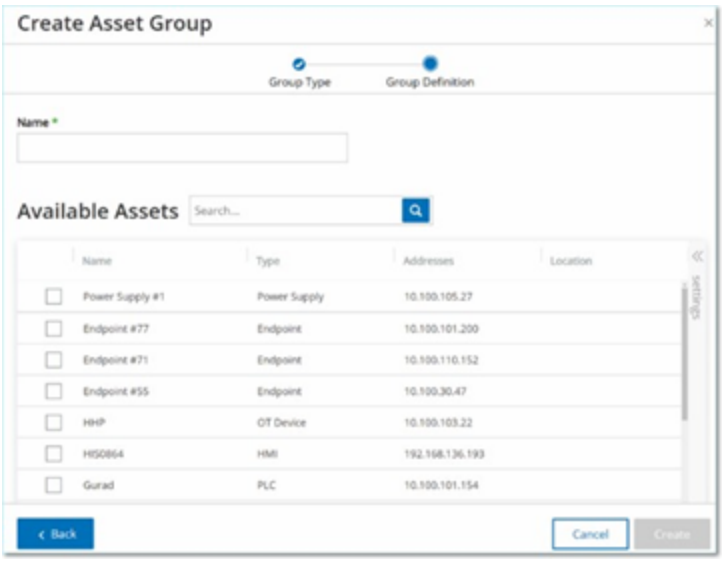
1. 转至“**组**”>“**资产组**”。
2. 单击“**创建资产组**”。

   此时会出现“**创建资产组**”面板。



3. 单击“**资产选择**”。
4. 单击“**下一步**”。

   此时会显示“**可用资产**”列表。



5. 在"**名称**"框中，输入组名称。

   选择一个说明通用元素的名称，该元素用于对组中包含的资产进行分类。

6. 选中要包括在组中的每个资产旁边的复选框。

7. 点击"**创建**"。

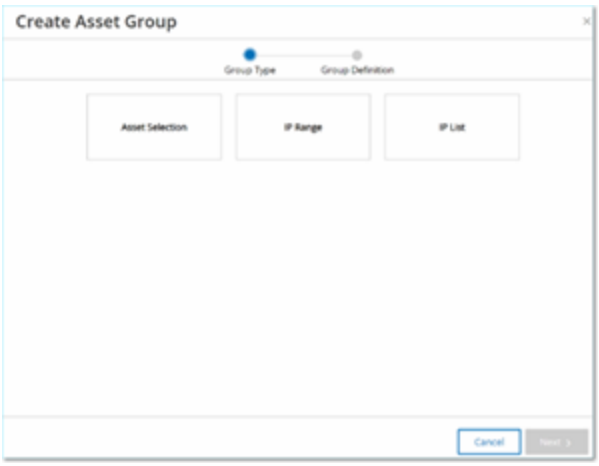
   OT Security 会创建新的资产组并在"**资产组**"屏幕上显示。现在便可在配置策略时使用此组。

若要创建 IP 范围类型资产组，请执行以下操作：

1. 转至"**组**">"**资产组**"。

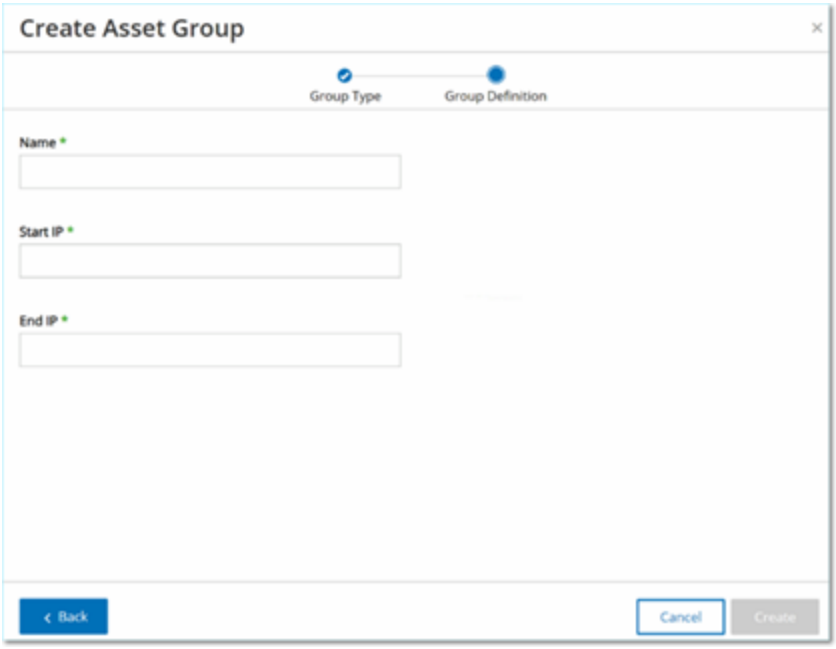
2. 单击"**创建资产组**"。

   此时会出现"**创建资产组**"面板。



3. 单击“**IP 范围**”。
4. 单击“**下一步**”。

   此时会出现“IP 范围选择”面板。



5. 在“**名称**”框中，输入组名称。

   选择一个说明通用元素的名称，该元素用于对组中包含的资产进行分类。
6. 在“**起始 IP**”框中，输入要包括的范围开头的 IP 地址。
7. 在“**结束 IP**”框中，输入要包括的范围结束的 IP 地址。

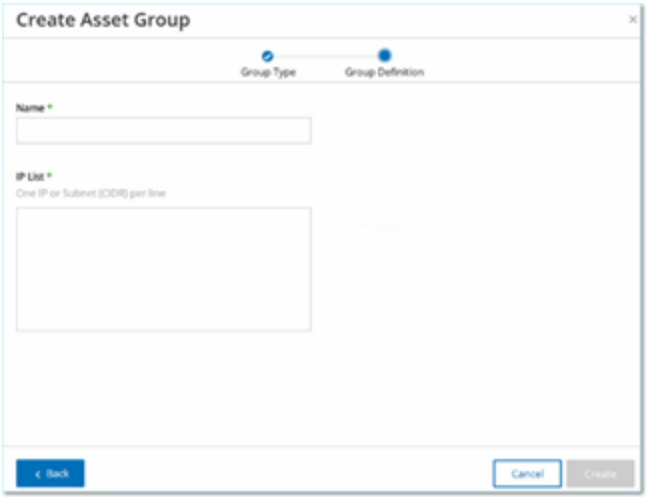
8. 点击“**创建**”。

   OT Security 会创建新的资产组并在“**资产组**”屏幕上显示。现在便可在配置策略时使用此组。

若要创建 IP 列表类型资产组，请执行以下操作：

1. 转至“**组**”>“**资产组**”。
2. 单击“**创建资产组**”。

   此时会出现“**创建资产组**”面板。



3. 单击“**IP 列表**”。
4. 单击“**下一步**”。

   此时会出现“**IP 列表**”面板。

5. 在“**名称**”框中，输入组名称。

   选择一个说明通用元素的名称，该元素用于对组中包含的资产进行分类。

6. 在“**IP 列表**”框中，输入要包含在组中的 IP 地址或子网。
7. 要向组添加更多资产，请在单独的行内输入各个其他 IP 地址或子网。
8. 点击“**创建**”。

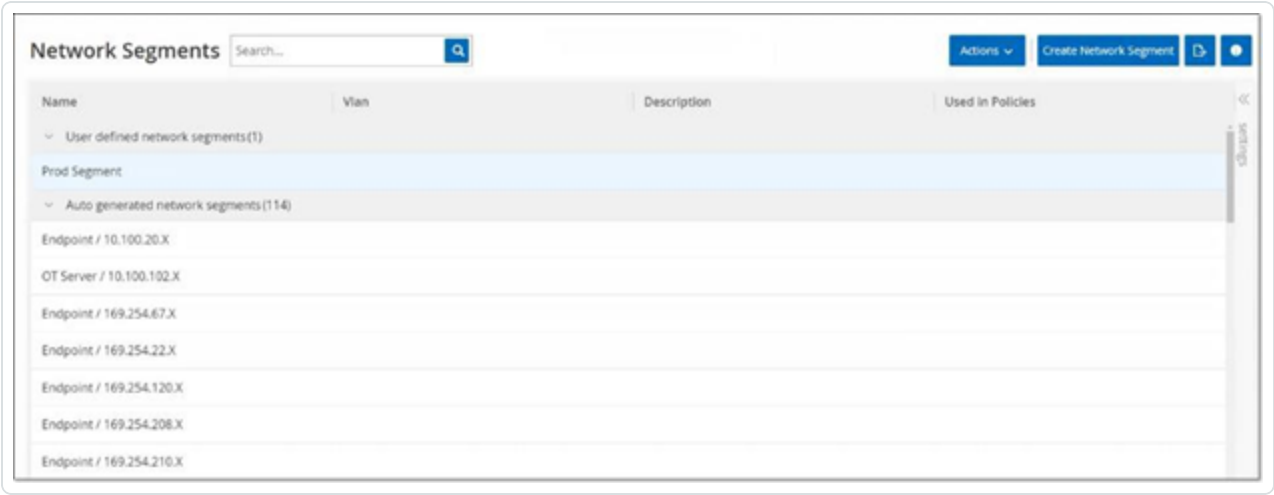
   OT Security 会创建新的资产组并在“**资产组**”屏幕上显示。现在便可在配置策略时使用此组。

网段

借助网段，您可以创建相关网络资产组，从而在逻辑上将一个资产组与另一个资产组隔离。OT Security 会自动将与网络中某项资产关联的每个 IP 地址分配给一个网段。对于具有多个 IP 地址的资产，每个 IP 都与一个网段相关联。每个自动生成的段都包括具有相同 C 类网络地址（即 IP 具有相同的前 24 位）IP 的特定类别（控制器、OT 服务器、网络设备等）的所有资产。

可以创建用户定义的网段，并指定将哪些资产分配给该段。“**清单**”屏幕上某一列会显示每项资产的网段，便于轻松按照网段对资产进行排序和筛选。

查看网段



“**网段**”屏幕显示系统中当前配置的所有网段。“**自动生成**”选项卡包含系统自动生成的网段。“**用户定义**”选项卡包含用户创建的网段。

“网段”表显示以下详细信息：

参数	描述
名称	用于识别网段的名称。
VLAN	网段的 VLAN 编号。（可选）
描述	网段的说明。（可选）
已在以下策略中使用	显示适用于此网段的策略名称。

	注意：如要查看有关使用该网段的策略的更多详情，请单击“**操作**”>“**查看**”>“**已在以下策略中使用**”选项卡。

您可以查看、编辑、复制或删除现有网段。有关更多信息，请参阅“组操作”。

创建网段

可以创建要在策略配置中使用的网段。通过将相关网络资产组合在一起，可以创建为该段中的资产定义可接受的网络流量的策略。

若要创建网段，请执行以下操作：

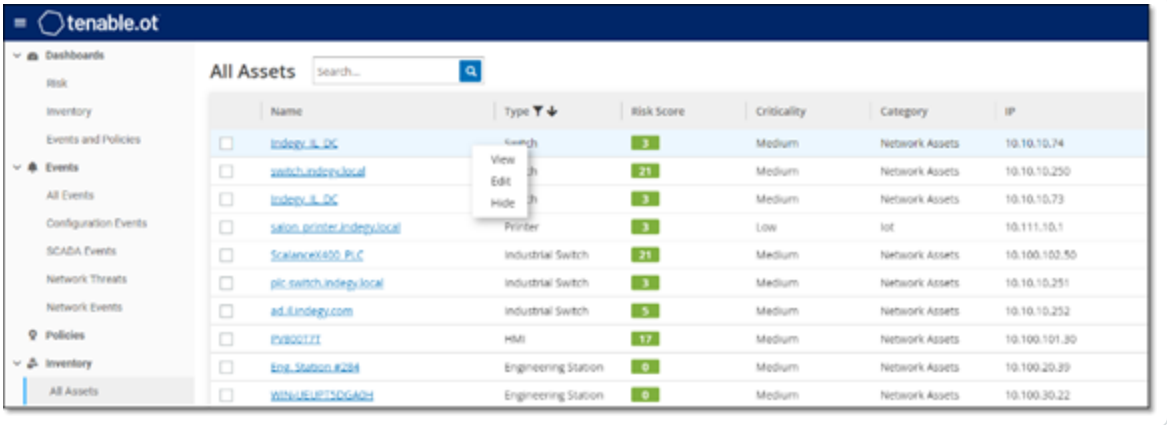
1. 转至“**组**”>“**网段**”。
2. 单击“**创建网段**”。

   此时会出现“**创建网段**”面板。

3. 在“**名称**”框中，为该网段输入一个名称。
4. （可选）在“**VLAN**”框中，为该网段输入一个 VLAN 编号。
5. （可选）在“**说明**”框中，输入网段说明。
6. 点击“**创建**”。

   OT Security 会创建新的网段并在网段列表中显示该网段。
7. 若要将资产分配给新创建的网段，请执行以下操作：
   a. 转至“**清单**”>“**所有资产**”。
   b. 请执行下列操作之一：

- 右键单击要分配给新建网段的资产，然后选择“**编辑**”。
- 将鼠标悬停在要分配的资产上，然后从“**操作**”菜单中选择“**编辑**”。



此时会打开“**编辑资产详细信息**”窗口。

8. 在“**网段**”下拉框中，选择所需的网段。

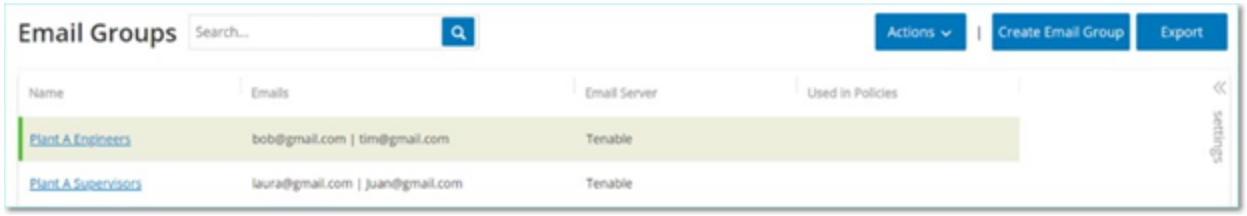
注意：部分资产具有多个关联的 IP 地址，可以为每个地址选择需要的网段。

OT Security 将网段应用到资产并在“**网段**”列中显示该网段。现在便可在配置策略时使用此网段。

电子邮件组

电子邮件组是相关方的电子邮件组。电子邮件组用于指定由特定策略触发的事件通知的收件人。例如，按角色、部门等分组便于将特定策略事件的通知发送给相关方。

查看电子邮件组



"**电子邮件组**"屏幕显示系统中当前配置的所有电子邮件组。

"电子邮件组"表格显示以下信息：

注意：您可以通过选择组并单击"**操作**">"**查看**"，来查看关于某个特定组的更多详细信息。

参数	描述
名称	用于识别组的名称。
电子邮件地址	组中包含的电子邮件列表。 **注意**：如果没有空间可以显示组的所有成员，请单击"**操作**">"**查看**">"**成员**"选项卡。
电子邮件服务器	用于向组发送电子邮件的 SMTP 服务器的名称。
已在以下策略中使用	显示通知已发送至此组的策略名称。 **注意**：如要查看有关使用该组的策略的更多详情，请单击"**操作**">"**查看**">"**已在以下策略中使用**"选项卡。

此外，您还可以查看、编辑、复制或删除现有组。有关更多信息，请参阅"组操作"。

创建电子邮件组

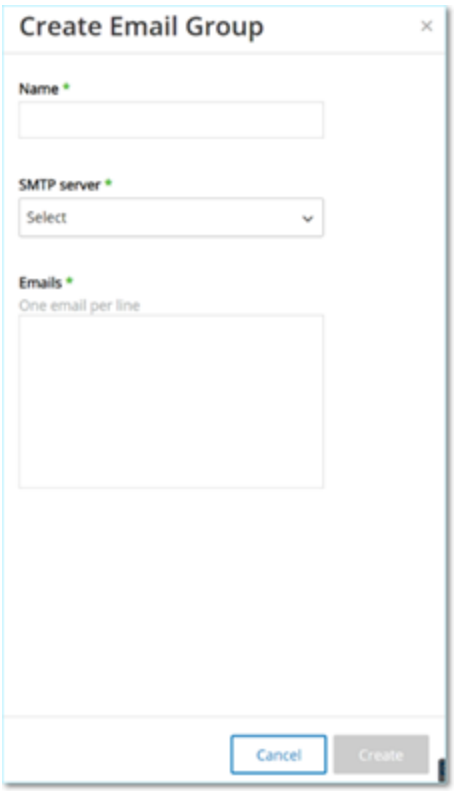
可以创建要在策略配置中使用的电子邮件组。通过对相关电子邮件进行分组，可以设置要发送给所有相关人员的策略事件通知。

注意：您只能为每个策略分配一个电子邮件组。因此，创建广泛的、包容性的组以及特定的、受限组非常有用，如此便可为每个策略分配适当的组。

若要创建电子邮件组，请执行以下操作：

1. 转至“**组**”>“**电子邮件组**”。
2. 单击“**创建电子邮件组**”。

   此时会出现“**创建电子邮件组**”面板。



3. 在“**名称**”框中，输入组名称。
4. 在“**SMTP 服务器**”下拉框中，选择用于发送电子邮件通知的服务器。

   注意：如果系统中未配置 SMTP 服务器，则必须首先配置服务器，才能创建电子邮件组，详情请参阅“SMTP 服务器”。

5. 在“**电子邮件**”框中，在单独的行中输入组内每个成员的电子邮件。

6. 点击“**创建**”。

   OT Security 会创建新的电子邮件组并在“**电子邮件组**”页面上显示该组。现在便可在配置策略时使用此组。

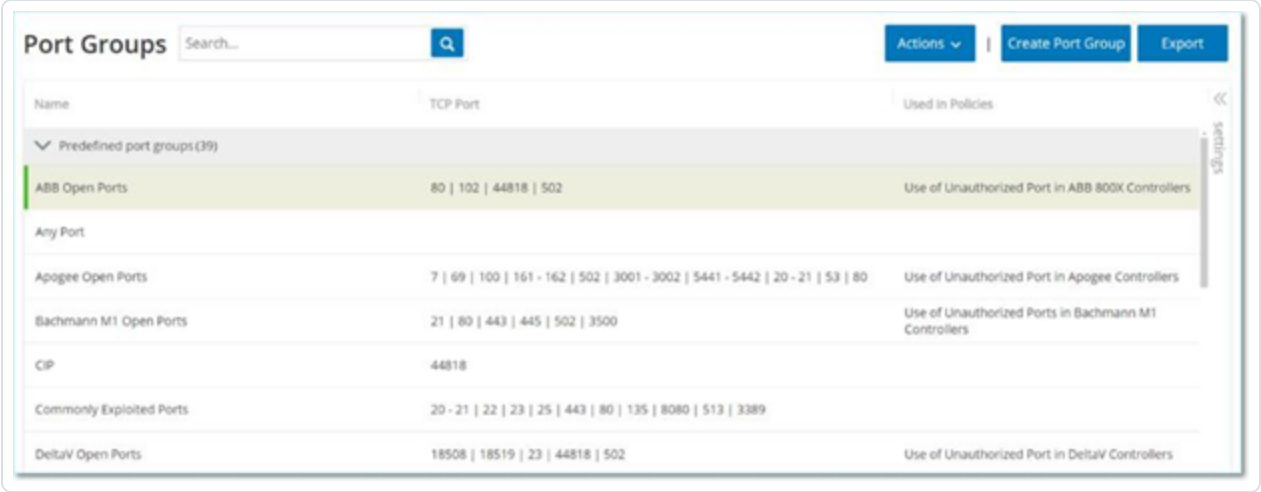
端口组

端口组是网络中的资产使用的端口组。端口组用作定义“**已打开的端口**”网络事件策略的策略条件，可检测网络中的已打开的端口。

“**预定义**”选项卡可显示系统中预定义的端口组。这些组包含预期在特定供应商的控制器上开放的端口。例如，Group Siemens PLC 已打开的端口包括：20、21、80、102、443 和 502。这可配置用于检测预期不会针对该供应商的控制器开放的已打开的端口的策略。这些组无法编辑或删除，但可以复制。

“**用户定义**”选项卡包含用户创建的自定义组。您可以编辑、复制或删除这些组。

查看端口组



“查看端口组”表格包含以下详细信息：

参数	描述
名称	用于识别组的名称。
TCP 端口	组中包含的端口列表和/或端口范围。 **注意**：如果表格未显示组的所有成员，请单击“**操作**”>“**查看**”>“**成员**”选项卡以查看所有成员。
已在以下策略	显示在其配置中使用此端口组的每个策略的名称。

中使用	**注意**：如要查看有关使用此组的策略的其他信息，请单击“**操作**”>“**查看**”>“**已在以下策略中使用**”选项卡。

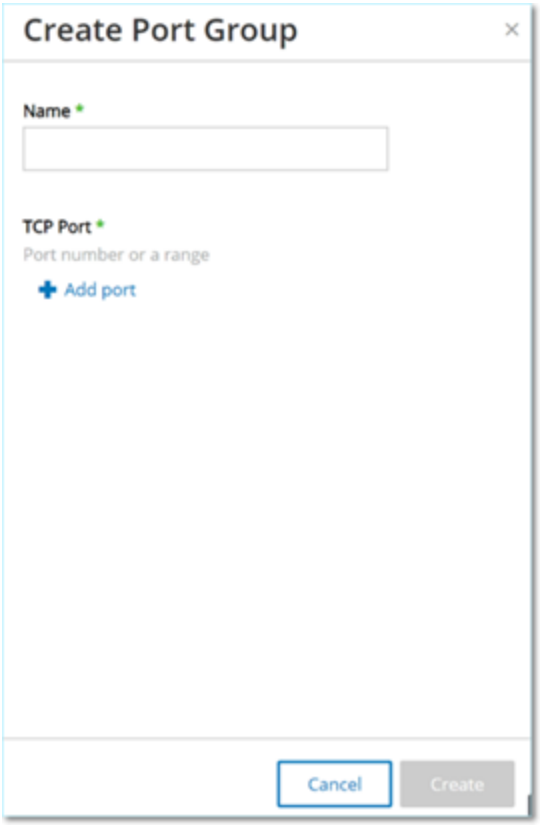
创建端口组

您可以创建要在策略配置中使用的用户定义的端口组。将类似的端口分为同组有助于创建针对造成特定安全风险的已打开的端口发出警报的策略。

若要创建端口组，请执行以下操作：

1. 转至“**组**”>“**端口组**”。
2. 单击“**创建端口组**”。

   此时会出现“**创建端口组**”面板。



3. 在“**名称**”框中，输入组名称。
4. 在“**TCP 端口**”框中，输入要包含在组中的单个端口或一系列端口。

5. 若要向组添加其他端口，请执行以下操作：

   a. 单击“**+ 添加端口**”。

      此时会出现一个新的“端口选择”框。

   b. 在新的“**端口号**”框中，输入要包含在组中的单个端口或一系列端口。

6. 点击“**创建**”。

   OT Security 会创建新的端口组并在“端口组”列表中显示端口组。现在便可在配置策略时使用此组。

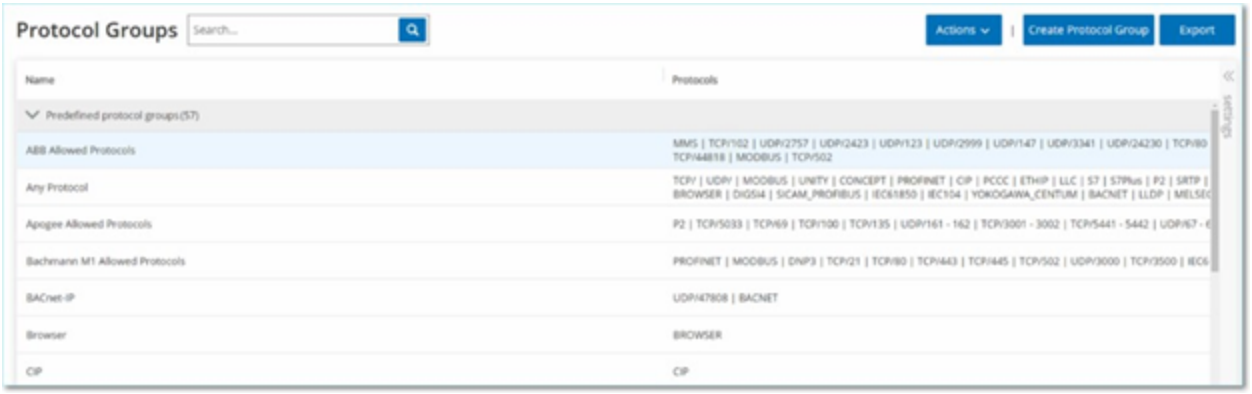
协议组

协议组是在网络中的资产之间进行对话所依据的一组协议。协议组用作网络策略的策略条件，可以定义特定资产之间使用哪项协议触发策略。

OT Security 随附了一组包含相关协议的预定义协议组。这些组可用于策略。您无法编辑或删除这些组。您可以按照特定供应商允许的协议对协议进行分组。

例如，Schneider 允许的协议包括：TCP:80 (HTTP)、TCP:21 (FTP)、Modbus、Modbus_UMAS、Modbus_MODICON、TCP:44818 (CIP)、UDP:69 (TFTP)、UDP:161 (SNMP)、UDP :162 (SNMP)、UDP:44818、UDP:67-68 (DHCP)。您也可以按照协议类型(如 Modbus、PROFINET、CIP 等) 对其进行分组。您还可以创建专属的用户定义的协议组。

查看协议组



“**协议组**”屏幕显示系统中当前配置的所有协议组。“**预定义**”选项卡可显示内置于系统当中的组。您无法编辑或删除这些组，但您可以复制它们。“**用户定义**”选项卡会显示您创建的自定义组。您可以编辑、复制或删除这些组。

“协议组”表格显示以下详细信息：

参数	描述
名称	用于识别组的名称。
协议	组中包含的协议的列表。 **注意**：如果您无法查看组的所有成员，请单击“**操作**”>“**查看**”>“**成员**”选项卡。

已在以下策略中使用	显示在其配置中使用此协议组的每个策略的名称。 **注意**:如要查看有关使用此组的策略的其他详细信息,请单击"**操作**">"**查看**">"**已在以下策略中使用**"选项卡。

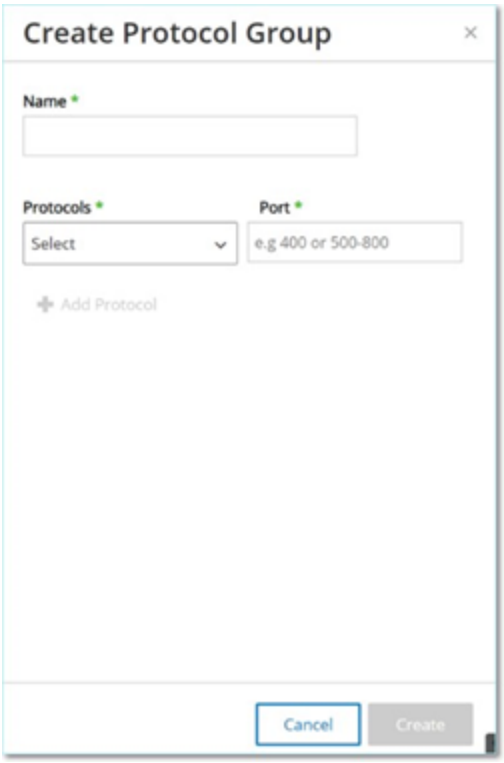
创建协议组

您可以创建要在策略配置中使用的自定义协议组。通过将类似的协议分为同组,您可以创建定义哪些协议可疑的策略。

若要创建协议组,请执行以下操作:

1. 转至"**组**">"**协议组**"。
2. 单击"**创建协议组**"。

   此时会出现"**创建协议组**"。



3. 在"**名称**"框中,输入组名称。
4. 在"**协议**"下拉框中,选择协议类型。

5. 如果所选协议为 TCP 或 UDP，则在“**端口**”框中输入端口号或端口范围。

   对于其他协议类型，您无需在“**端口**”框中输入任何值。

6. 若要向组添加其他协议，请执行以下操作：

   a. 单击“**+ 添加协议**”。

      此时会出现一个新的“**协议选择**”框。

   b. 按照步骤 4-5 中所述的方式填写新的**协议选择**。

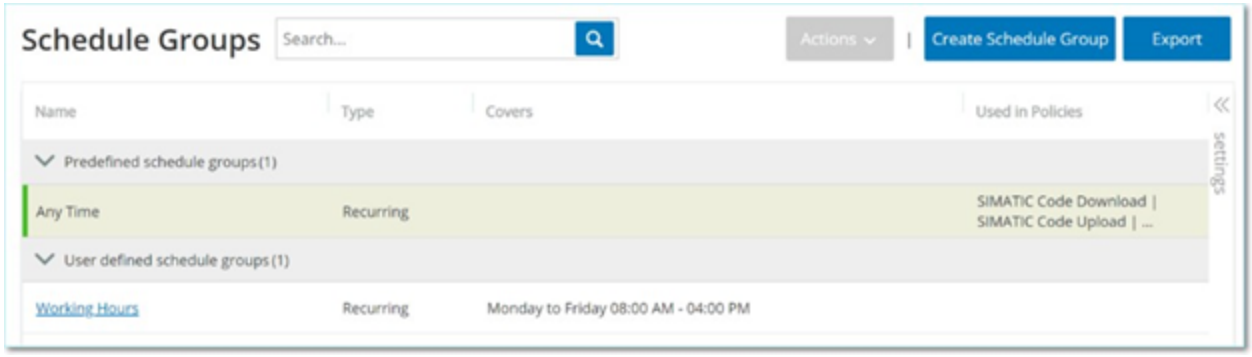
7. 点击“**创建**”。

   OT Security 会创建新的协议组并在“协议组”列表中显示这些组。现在便可在配置策略时使用此组。

计划组

计划组定义了一个或一组时间范围，这些时间范围组具有特定特征，使得在该时间期间发生的活动值得关注。例如，某些活动预计在工作时间内发生，而其他活动预计在停机时间发生。

查看计划组



“**计划组**”屏幕显示系统中当前配置的所有计划组。“**预定义计划组**”选项卡包含内置于系统当中的组。您无法编辑、复制或删除这些组。“**用户定义计划组**”选项卡会显示您创建的自定义组。您可以编辑、复制或删除这些组。

“计划组”表格显示以下详细信息：

参数	描述
名称	用于识别组的名称。
类型	组类型。选项包括： • **功能**：为实现特定功能而创建的预定义计划组。 • **反复**：每日或每周重复的计划。例如，可将工作时间计划定义为星期一至星期五的上午 9 点至下午 5 点。 • **间隔**：在特定日期或日期范围发生的计划。例如，可以按照 6 月 1 日至 8 月 15 日的时间期限制定工厂翻新计划。
时间范围	计划设置的摘要。 **注意**：如果您无法查看组的所有成员，请单击“**操作**”>“**查看**”>“**成员**”选项卡。

已在以下策略中使用	显示在其配置中使用此计划组的每个策略的策略 ID。 **注意**：如要查看有关使用此组的策略的其他详细信息，请单击“**操作**”>“**查看**”>“**已在以下策略中使用**”选项卡。

创建计划组

可以创建要在策略配置中使用的自定义计划组。指定一个或一组共享某些特征的时间范围，以强调在该时间期间发生的事件。

计划组类型包含两种：

- **反复**：每周重复发生的计划。例如，可将工作时间计划定义为星期一至星期五的上午 9 点至下午 5 点。
- **一次性**：在特定日期或日期范围发生的计划。例如，可以按照 6 月 1 日至 8 月 15 日的时间期限制定工厂翻新计划。每种类型的计划组都有不同的创建过程。

每种类型的计划组都有不同的创建过程。

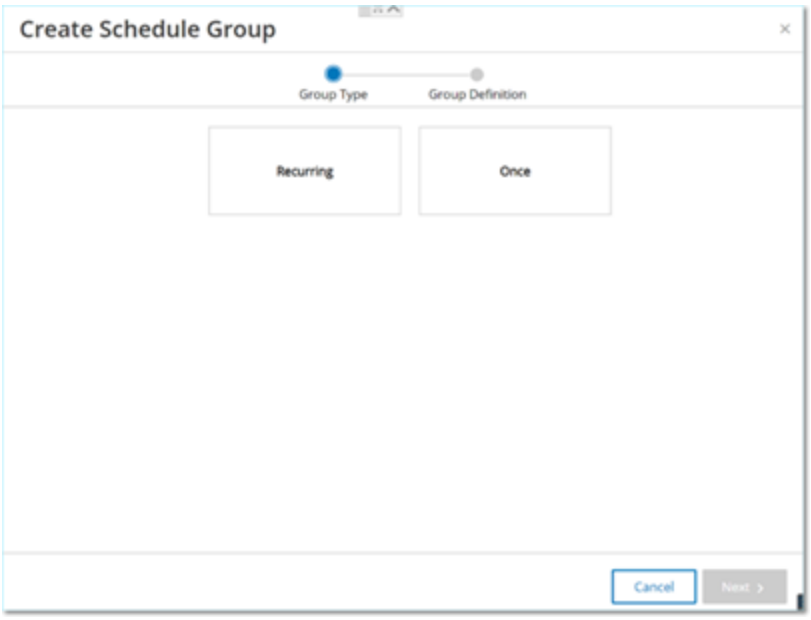
若要创建反复类型计划组，请执行以下操作：

1. 转至“**组**”>“**计划组**”。

   此时会出现“**计划组**”页面。

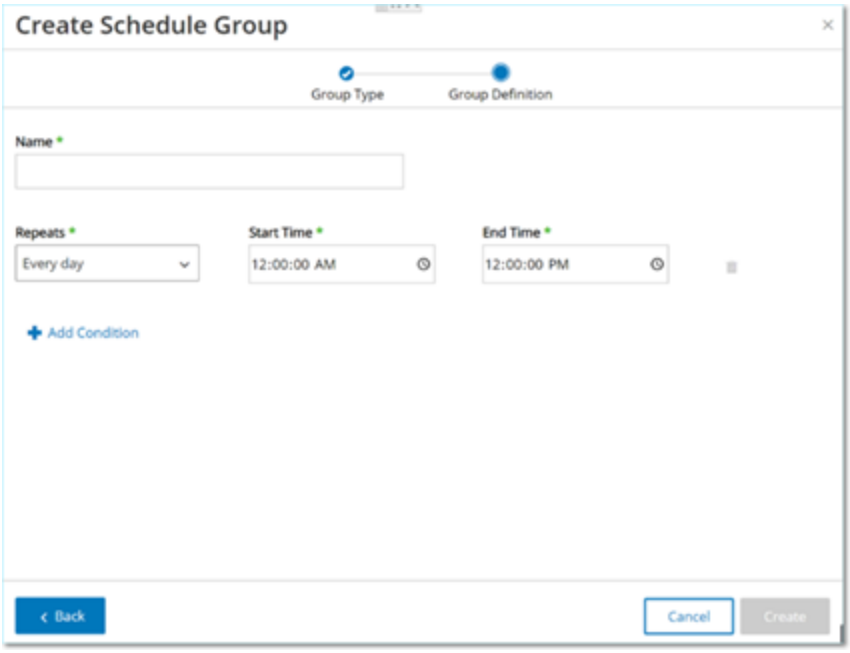
2. 单击“**创建计划组**”。

   此时会出现“**创建计划组**”面板。



3. 单击“**反复**”。
4. 单击“**下一步**”。

   此时会显示用于定义反复计划组的参数。



5. 在“**名称**”框中，输入组名称。
6. 在“**重复**”框中，选择一周中的哪些天包括在计划组中。

   选项包括“每天”、“星期一至星期五”或一周中的特定日期。

注意:如果您要包括一周中的特定日期,例如星期一和星期三,则需要为每一天添加一个单独条件。

7. 在"**开始时间**"框中,输入计划组中所含时间范围的开始时间(HH:MM:SS AM/PM)。
8. 在"**结束时间**"框中,输入计划组中所含时间范围的结束时间(HH:MM:SS AM/PM)。
9. 若要向计划组添加其他条件(即其他时间范围),请执行以下操作:
   a. 单击"**+ 添加条件**"。

      此时会出现一行新的计划选择参数。

   b. 按照上述步骤 5-7 所述填写计划字段。
10. 点击"**创建**"。

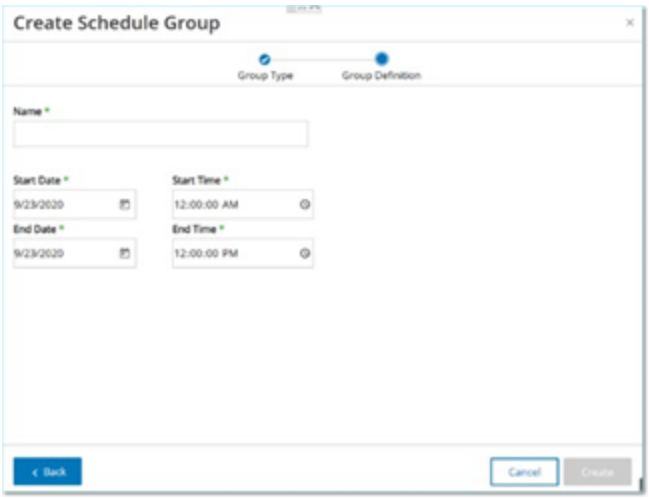
    OT Security 会创建新的计划组并在"计划组"列表中显示这些组。现在便可在配置策略时使用此组。

若要创建一次性计划组,请执行以下操作:

1. 转至"**组**">"**计划组**"。
2. 单击"**创建计划组**"。

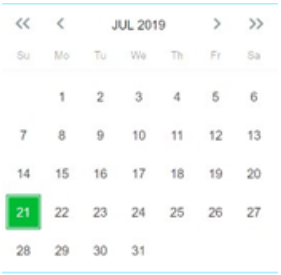
   此时会出现"**创建计划组**"向导。
3. 选择"**时间范围**"。
4. 单击"**下一步**"。

   此时会显示用于定义时间范围计划组的参数。



5. 在“**名称**”框中，输入组名称。
6. 在“**开始日期**”框中，单击日历图标 。

   此时日历窗口打开。



7. 选择计划组开始的日期。默认：当前日期。
8. 在“**开始时间**”框中，输入计划组中所含时间范围的开始时间 (HH:MM:SS AM/PM)。
9. 在“**结束日期**”框中，单击日历图标 。

   此时日历窗口打开。

10. 选择计划组结束的日期。(默认：当前日期)
11. 在“**结束时间**”框中，输入计划组中所含时间范围的结束时间 (HH:MM:SS AM/PM)。
12. 点击“**创建**”。

    OT Security 会创建新的计划组并在“计划组”列表中显示该组。现在便可在配置策略时使用此组。

标签组

标签是包含特定操作数据的控制器中的参数。标签组可用作 **SCADA 事件策略**的策略条件。通过将角色相似的标签分为同组，您可以创建策略来检测对指定参数的可疑更改。例如，通过将控制熔炉温度的标签分为同组，可以创建一个策略来检测可能对熔炉造成危害的温度变化。

查看标签组

"**标签组**"屏幕显示系统中当前配置的所有标签组。

"标签组"表格显示以下详细信息：

参数	描述
名称	用于识别组的名称。
类型	标签的数据类型。可能的值包括 Bool、Dint、Float、Int、Long、Short、Unknown（针对 OT Security 无法识别的标签类型）或任意类型（可包括不同类型的标签）。
控制器	正在监控标签的控制器。
标签	显示组中包含的每个标签，及其所在控制器的名称。 **注意**：如果您无法查看此行中的所有标签，请单击"**操作**">"**查看**">"**成员**"选项卡。
已在以下策略中使用	显示在其配置中使用此计划组的每个策略的策略 ID。 **注意**：如要查看有关使用此组的策略的其他详细信息，请单击"**操作**">"**查看**">"**已在以下策略中使用**"选项卡。

您可以查看、编辑、复制或删除现有组，详情请参阅"组操作"。

创建标签组

可以创建在策略配置中使用的自定义标签组。将类似的标签划分为同组有助于创建应用于组内所有标签的策略。选择类型相似的标签，并为其提供可以代表标签通用元素的名称。

还可以通过选择“**任意类型**”选项来创建包含不同类型标签的组。在这种情况下，应用于此组的策略只能检测对指定标签的“**任何值**”进行的更改，但不能设置为检测特定值。

您可以编辑、复制或删除标签组。

若要创建新标签组，请执行以下操作：

1. 转至“**组**”>“**标签组**”。
2. 单击“**创建标签组**”。

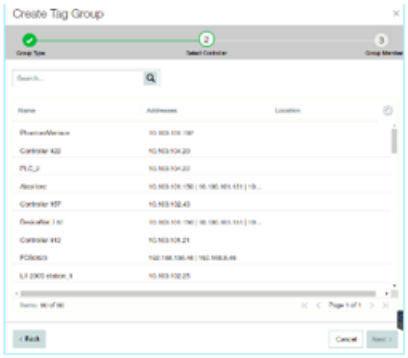
   此时会出现“**创建标签组**”面板。

3. 选择一种标签类型。

   选项包括 Bool、Dint、Float、Int、Long、Short 或任意类型(可包含不同类型的标签)。

4. 单击“**下一步**”。

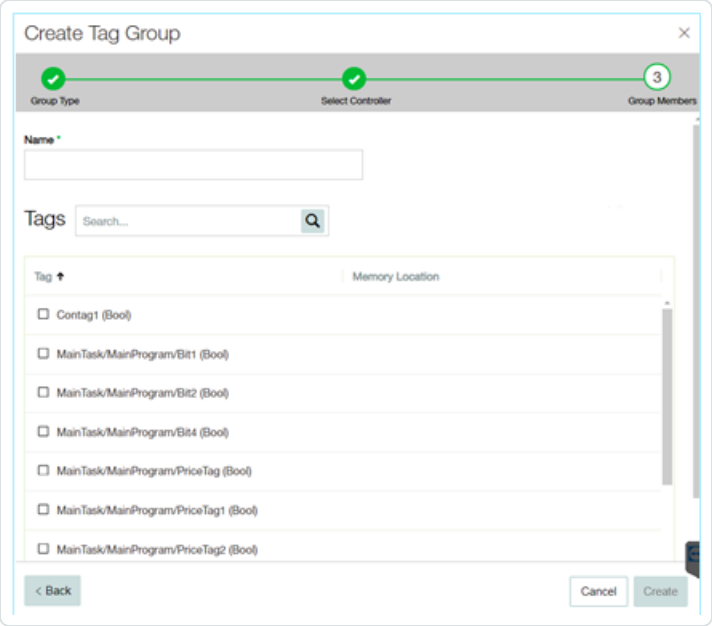
   此时会显示网络中的控制器列表。



5. 选择要在组中包含标签的控制器。

6. 单击“**下一步**”。

   此时会显示指定控制器上指定类型的标签列表。



7. 在“**名称**”框中，输入组名称。
8. 选中要包括在组中的每个标签旁边的复选框。
9. 点击“**创建**”。

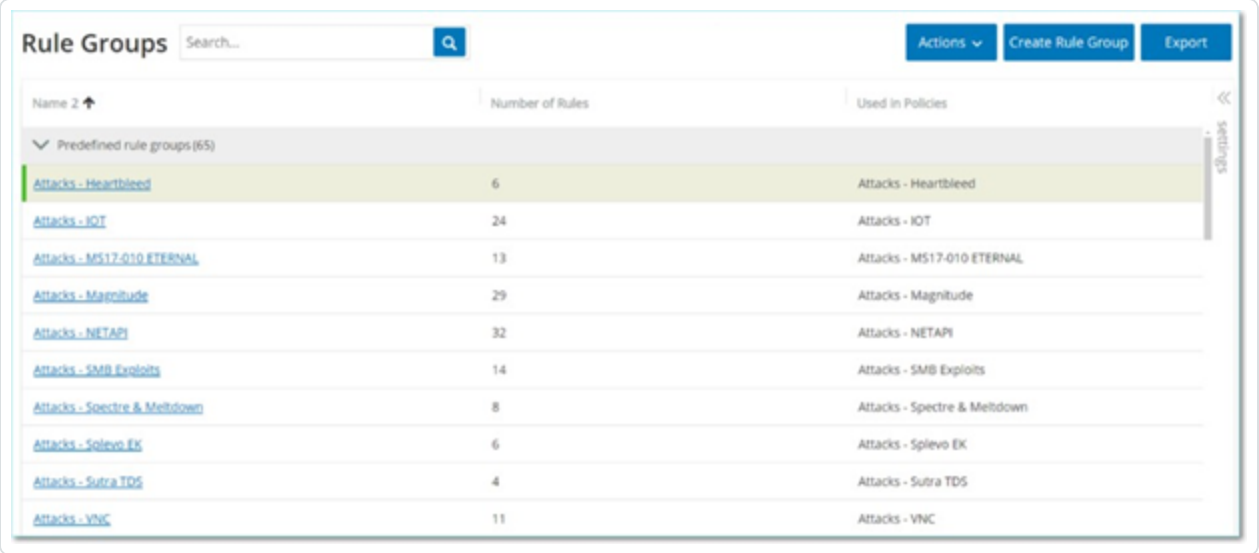
   OT Security 会创建新的标签组并在“标签组”列表中显示这些组。现在便可在配置 SCADA 事件策略时使用此组。

规则组

规则组由一组相关的规则组成，可以通过其 Suricata 签名 ID (SID) 进行标识。这些组可以用作定义入侵检测策略的策略条件。

OT Security 可以提供一系列包含相关漏洞的预定义组。此外，您可以从我们的漏洞库中选择各个规则并创建自己的自定义规则组。

查看规则组



“**规则组**”屏幕显示系统中当前配置的所有规则组。“预定义”选项卡包含内置于系统当中的组。您无法编辑、复制或删除这些组。“**用户定义**”选项卡会显示用户创建的自定义组。您可以编辑、复制或删除这些组。

“规则组”表格显示以下详细信息：

参数	描述
名称	用于识别组的名称。
规则数	组成此规则组的规则 (SID) 的数量。
已在以下策略中使用	显示在其配置中使用此规则组的每个策略的策略 ID。 **注意**：如要查看有关使用此组的策略的其他详细信息，请单击“**操作**”>“**查**

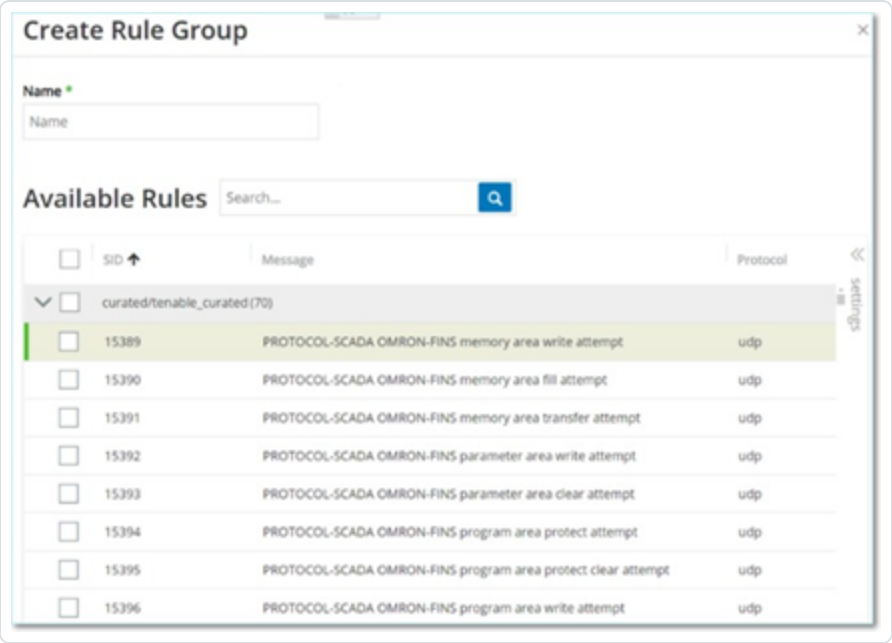
	看">"已在以下策略中使用"选项卡。

创建规则组

若要创建新规则组，请执行以下操作：

1. 转至"**组**">"**规则组**"。
2. 单击"**创建规则组**"。

   此时会出现"**创建规则组**"面板。



3. 在"**名称**"框中，输入组名称。
4. 在"**可用规则**"部分，选中要包括在组中的每个规则旁边的复选框。

   注意：使用搜索框查找所需规则。

5. 点击"**创建**"。

   OT Security 会创建新的规则组并在"规则组"列表中显示该组。现在便可在配置入侵检测策略时使用此组。

组操作

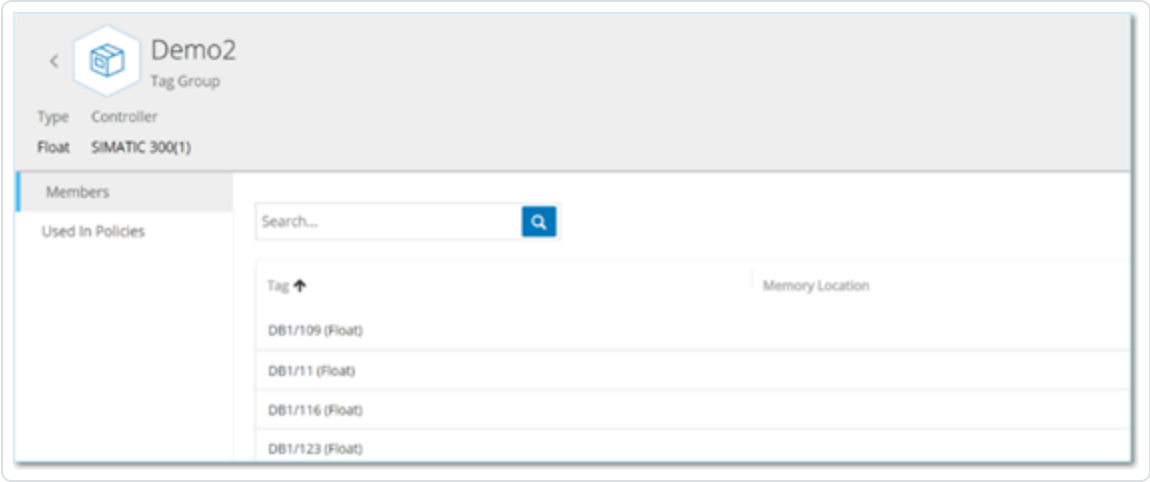
当您在任何“组”屏幕上选择某个组时，您可在屏幕顶部的“**操作**”菜单中执行以下操作：

- **查看**：显示所选组的详细信息，例如该组中包含哪些实体，以及哪些策略使用该组作为策略条件。请参阅“查看组的详细信息”
- **编辑**：编辑组的详细信息。请参阅“编辑组”
- **复制**：使用与指定组类似的配置创建新组。请参阅“复制组”
- **删除**：从系统中删除组。请参阅“删除组”

> **注意**：您无法编辑或删除预定义的组。某些预定义的组也无法复制。您也可通过右键单击“组”来访问“**操作**”菜单。

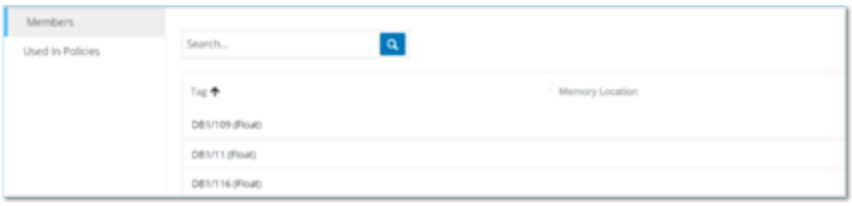
查看组的详细信息

当您在选择某个组并单击“**操作**”>“**查看**”时，系统会显示所选组的“组详细信息”屏幕。



“**组详细信息**”屏幕的标题栏显示了该组的名称和类型。该屏幕还有两个选项卡：

- "**成员**":显示组内所有成员的列表。

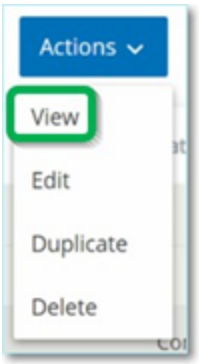


- "**已在以下策略中使用**":显示使用指定组作为策略条件的每个策略的列表。策略列表包含用于打开/关闭策略的切换开关。有关更多信息,请参阅"查看策略"。

若要查看组的详细信息,请执行以下操作:

1. 在"**组**"中,选择所需的组类型。
2. 请执行下列操作之一:
   - 单击"**操作**"。
   - 右键点击所需的组。

     此时会出现菜单。
3. 选择"**查看**"。



此时会出现"组详细信息"屏幕。

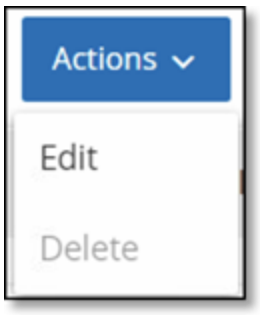
编辑组

可以编辑现有组的详细信息。

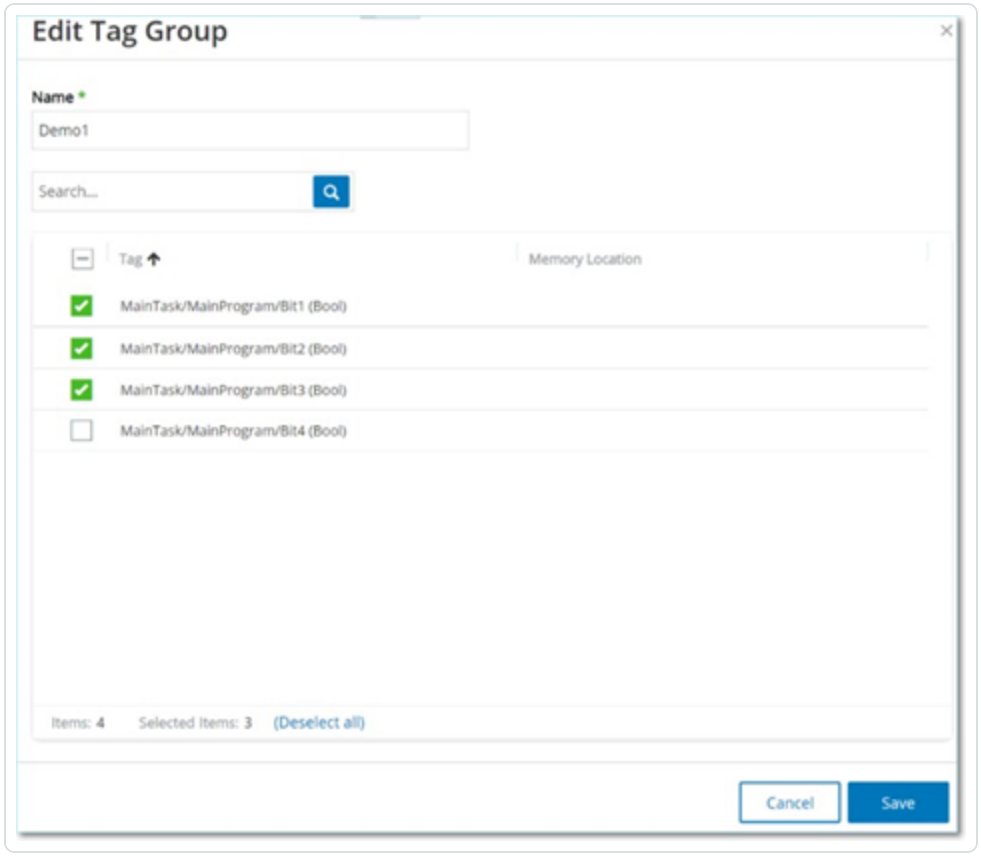
若要编辑组的详细信息,请执行以下操作:

1. 在“**组**”下，选择所需的组类型。
2. 请执行下列操作之一：
   - 单击“**操作**”。
   - 右键点击所需的组。

     此时会出现菜单。
3. 选择“**编辑**”。



4. 此时会显示“**编辑组**”窗口，显示指定组类型的相关参数。



5. 根据需要进行修改。
6. 单击“**保存**”。

   OT Security 将组与新设置一起保存。

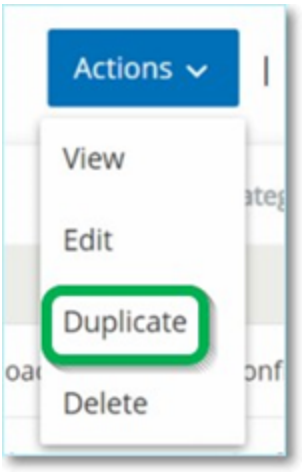
复制组

如要使用与现有组类似的设置创建新组，则可以“复制”现有组。复制组时，除原始组外，也会以新名称保存新组。

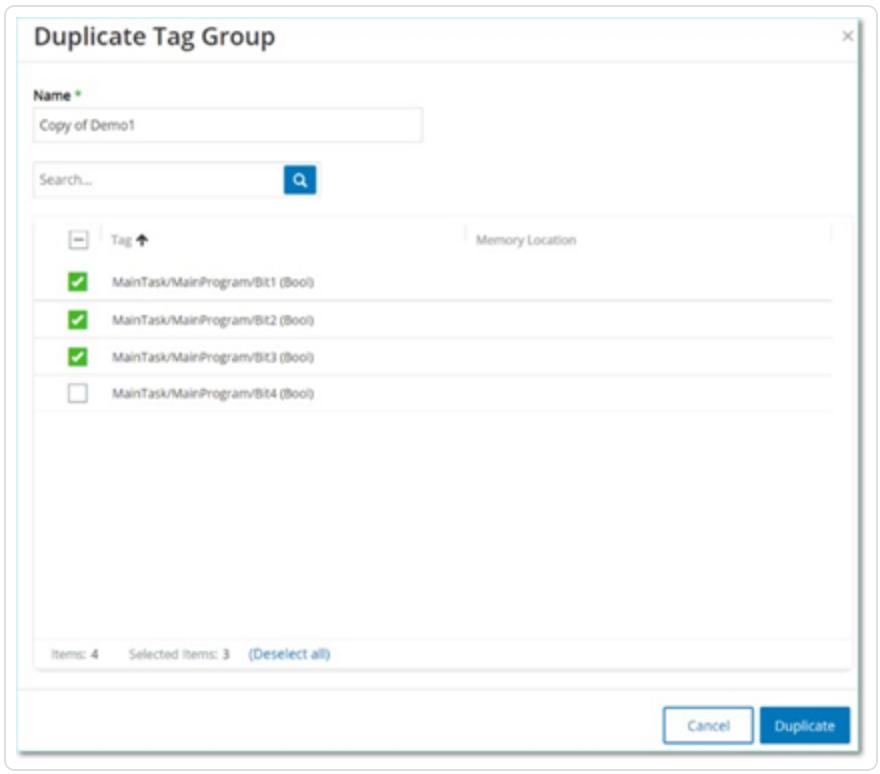
若要复制组，请执行以下操作：

1. 在“**组**”下，选择所需的组类型。
2. 选择要作为新组基础的现有组。
3. 请执行下列操作之一：
   - 单击“**操作**”。
   - 右键点击所需的组。

     此时会出现菜单。
4. 选择“**复制**”。



   此时会显示“**复制组**”窗口，显示指定组类型的相关参数。



5. 在“**名称**”框中，输入新组的名称。默认情况下，新组名为原始组名称的副本，即“Copy of”。
6. 对组设置进行所需的更改。
7. 单击“**复制**”。

   除现有组外，OT Security 会使用新设置保存新组。

删除组

可以删除用户定义的组，但不能删除预定义的组。如果用户定义的组被用作一个或多个策略的策略条件，则无法将其删除。

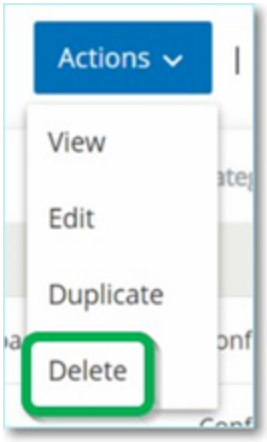
若要删除组，请执行以下操作：

1. 在“**组**”下，选择所需的组类型。
2. 选择要删除的组。
3. 请执行下列操作之一：

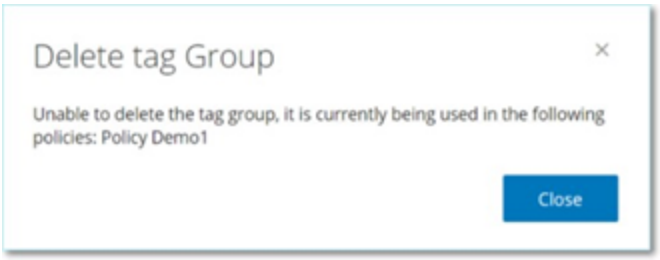
- 单击“**操作**”。
- 右键点击所需的组。

  此时会出现菜单。

4. 选择“**删除**”。



此时会出现“确认”窗口。



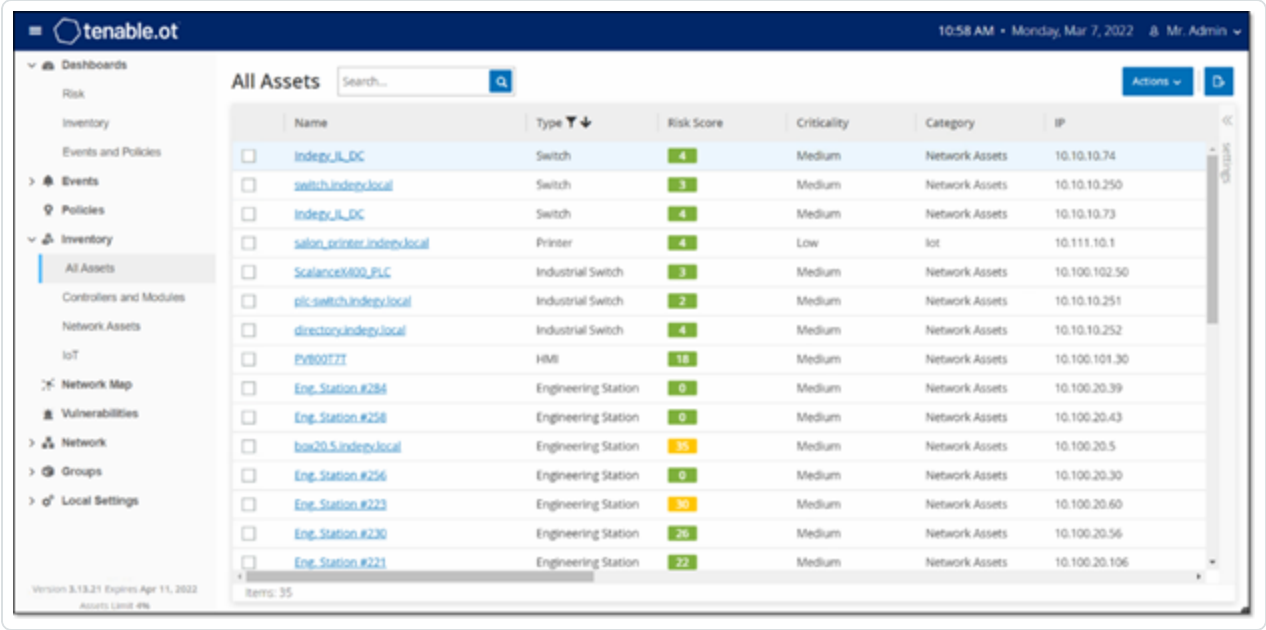
5. 点击“**删除**”。

   OT Security 将该组从系统中永久删除。

资产

OT Security 的自动化资产发现、分类和管理功能可以通过持续跟踪对设备进行的所有更改，来提供准确的最新资产清单。这简化了维护操作连续性、可靠性和安全性的工作。它还在规划维护项目、确定升级优先级、补丁部署、事件响应和缓解工作中发挥关键作用。

查看资产



网络中的所有资产都显示在“清单”屏幕上。显示有关每项资产的详细数据，从而实现全面的资产管理，以及监控每项资产的状态及其相关事件。“清单”屏幕中显示的数据是使用 OT Security 网络检测和主动查询功能收集的。“全部”屏幕显示所有类型资产的数据。此外，以下每种资产类型的特定资产子集会显示在单独屏幕上：“**控制器和模块**”、“**网络资产**”和“**IoT**”。

> **注意**：“网络资产”屏幕包含未包含在“控制器和模块”或“IoT”屏幕中的所有类型的资产。

对于每个资产屏幕（“全部”、“控制器和模块”、“网络资产”和“IoT”），可以通过调整要显示的列以及各列的位置来自定义显示设置。还可以对资产列表进行排序、筛选和搜索。有关自定义功能的说明，请参阅“管理控制台用户界面元素”。

下表介绍了“清单”屏幕上显示的参数。

标有“*”的参数仅显示在“控制器”屏幕上。

参数	描述
名称	网络中资产的名称。单击资产的名称即可查看该资产的“资产详细信息”屏幕（详情请参阅“资产”）。
IP	资产的 IP 地址。

	注意：一项资产可能具有多个 IP 地址。 **注意**：标记为"Direct"的 IP 地址指 Tenable 已与之建立直接连接的 IP 地址。如果未标记，则表示 Tenable 在未建立直接通信的情况下发现了 IP。 **注意**：可按 IP 范围筛选资产。有关筛选的更多信息，请参阅"管理控制台用户界面元素"。
MAC	资产的 MAC 地址。
网段	此资产的 IP 分配到的网段。
类型	资产的类型、控制器、I/O 或通信等。详情请参阅"资产类型"。
背板*	资产连接到的背板装置。"资产详细信息"屏幕会显示有关背板配置的其他详细信息。
插槽*	对于背板上的资产，显示资产所连接的插槽编号。
供应商	资产供应商。
系列*	资产供应商定义的产品的系列名称。
固件	资产上当前安装的固件版本。
位置	用户在 OT Security 资产详细信息中输入的资产的位置。请参阅 资产。
上次出现	OT Security 上次查看设备的时间。这是设备上次连接到网络或执行活动的时间。
操作系统	资产上运行的操作系统。
型号名称	资产的型号名称。
状态*	设备状态。可能的值： • 备份：控制器作为主控制器的备份运行。 • 故障：控制器处于故障模式。 • NoConfig：尚未为控制器设置配置。

	• 运行中:控制器正在运行。 • 已停止:控制器未运行。 • 未知:状态为未知。
描述	资产的简短说明,由用户在 OT Security 资产详细信息中配置。请参阅"资产"。
风险	与此资产相关的风险程度的度量,范围为 0(无风险)到 100(极高风险)。有关如何计算风险评分的说明,请参阅"风险评估"。
重要程度	此资产对系统正常运转重要程度的衡量方式。系统会根据资产类型为每项资产自动分配一个值。可以手动调整该值。
普渡层	资产的普渡层(0 = 物理流程,1 = 智能设备,2 = 控制系统,3 = 制造运营系统,4 = 商业后勤系统)。
自定义字段	可以创建自定义字段以使用相关信息标记资产。自定义字段可以是外部资源的链接。

资产类型

下表介绍了 OT Security 识别的各种资产类型，还显示了 OT Security 管理控制台中代表每种资产类型的图标(例如，在“网络映射”屏幕上)。

类别	默认重要程度/普渡层	描述	子类型	
控制器	高/1	一种工业计算机控制系统，可持续监控输入设备的状态，并根据自定义程序做出决策以控制输出设备的状态。此类别包括所有类型的控制器及其相关组件。		控制器
				PLC
				DCS
				IED
				RTU
				BMS 控制器
				机器人
				通信模块
				I/O 模块
				CNC

				电源
				背板模块
现场设备	高/1	使用工业协议将信息发送到 ICS 系统的工业设备(例如传感器、执行器、电机)。		现场设备
				功率计
				远程 I/O
				中继器
				反相器
				工业传感器
				驱动器
				执行器
OT 设备	中/2	此类别包括所有类型的 OT 设备。		OT 设备

				工业路由器
				工业交换机
				工业网关
				工业网络设备
				工业打印机
OT 服务器	中/2	用于访问工业数据的计算机/设备。此类别包括所有类型的 OT 服务器及其相关组件。		OT 服务器
				Historian
				HMI
				数据记录器
网络设备	中/3	网络设备(例如交换机或路由器) 。此类别包括所有类型的网络设备及其相关组件。		网络设备
				路由器

		
		交换机
		串行以太网桥
		网关
		集线器
		无线接入点
		防火墙
		转换器
		中继器
		无线电

工作站	低/3	连接到网络并用于控制 PLC 的计算机。此类别包括所有类型的工作站及其相关组件。		工作站
				OT 工作站
				工程站
				虚拟工作站
服务器	低/3	此类别包括各种类型的 IT 服务器。		服务器
				文件服务器
				Web 服务器
				虚拟服务器
				安全设备
				TenableICP

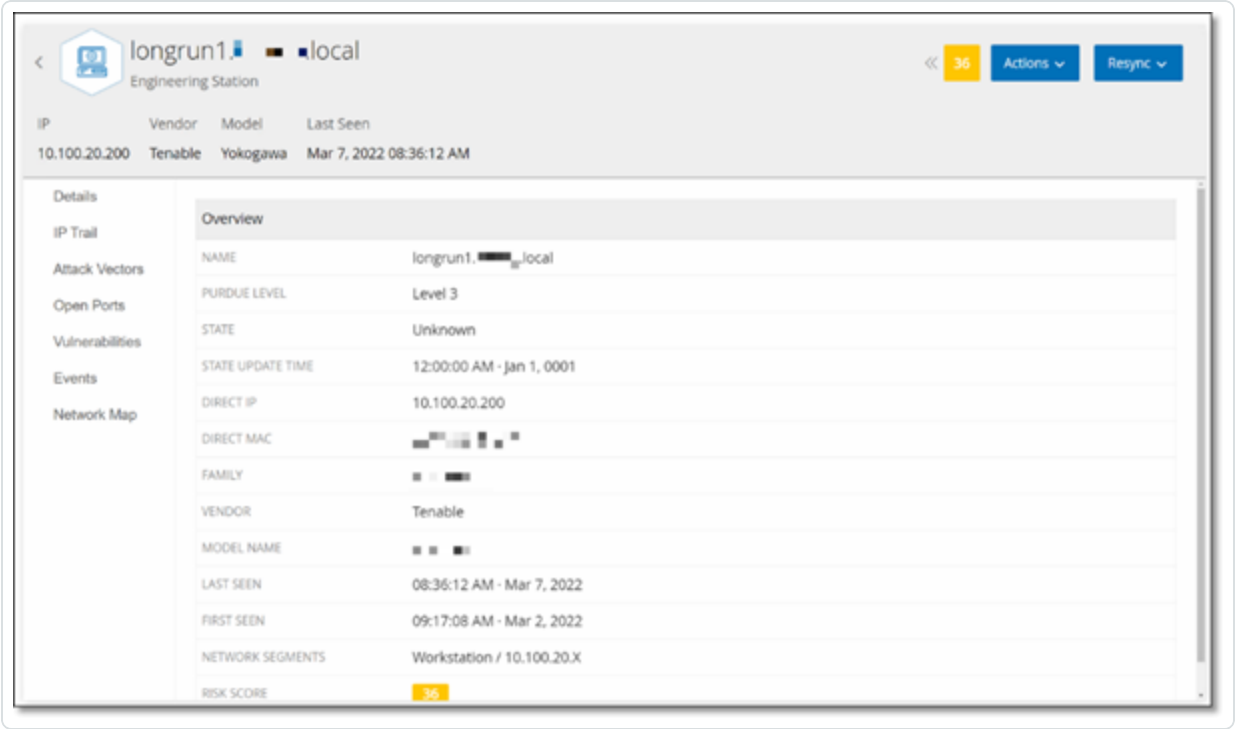
				
				TenableEM
				Tenable 传感器
				域控制器
				IoT
IoT	低/3	此类别包括各种类型的相关设备。		相机
				面板
				投影仪
				VOIP 设备
				3D 打印机

		打印机
		UPS
		IP 电话
		智能传感器
		条码扫描器
		访问控制系统
		照明控制
		空调模块
		智能中心
		智能电视

				医疗设备
				平板电脑
				移动设备
				存储设备
端点	低/3	网络中的不明 IP 地址。		端点

查看资产详细信息

“**资产详细信息**”页面显示有关 OT Security 为所选资产发现的所有数据的全面详细信息。标题栏、一系列选项卡和子部分中会显示详细信息。某些选项卡和子部分仅与特定资产类型相关。



若要访问特定资产的“**资产详细信息**”页面，

1. 请执行下列操作之一：
    - 在资产名称以链接形式显示的任何页面上单击资产名称：“**库存**”、“**事件**”或“**网络**”。
    - 在“**清单**”页面中，单击“**操作**”>“**查看**”。

“**资产详细信息**”窗口包含以下元素（针对相关资产类型）：

- **“标头”窗格**：显示有关资产及其当前状态的基本信息的概述，其中还包含一个“操作”菜单，便于编辑该资产的列表。
- **详细信息**：显示划分为各个子部分的详细信息，其中包含与各种资产类型相关的特定数据。

- **代码修订**(仅适用于控制器):显示由 OT Security"快照"功能发现的当前和以前的代码修订的相关信息。这包括针对代码引入的所有特定更改的详细信息,例如添加、删除或更改的内容(代码块/Rung)。
- **IP 追踪**:显示与资产相关的所有当前和历史 IP。
- **攻击途径**:显示易受攻击的攻击向量,即攻击者可用于获取此资产的路由。可以自动生成攻击途径来显示最重要的攻击途径,也可以通过特定资产手动生成攻击途径。
- **已打开的端口**:显示有关资产上已打开的端口的信息。
- **漏洞**:显示系统发现所选资产存在的漏洞,例如过时的 Windows 操作系统、使用易受攻击的协议和已知对特定类型设备有风险或非必需的开放通信端口,详情请参阅"漏洞"。
- **事件**:网络中涉及资产的事件列表。
- **网络映射**:显示资产网络连接的可视化图形。
- **设备端口**(适用于网络交换机):显示网络交换机上端口的信息。

“标头”窗格

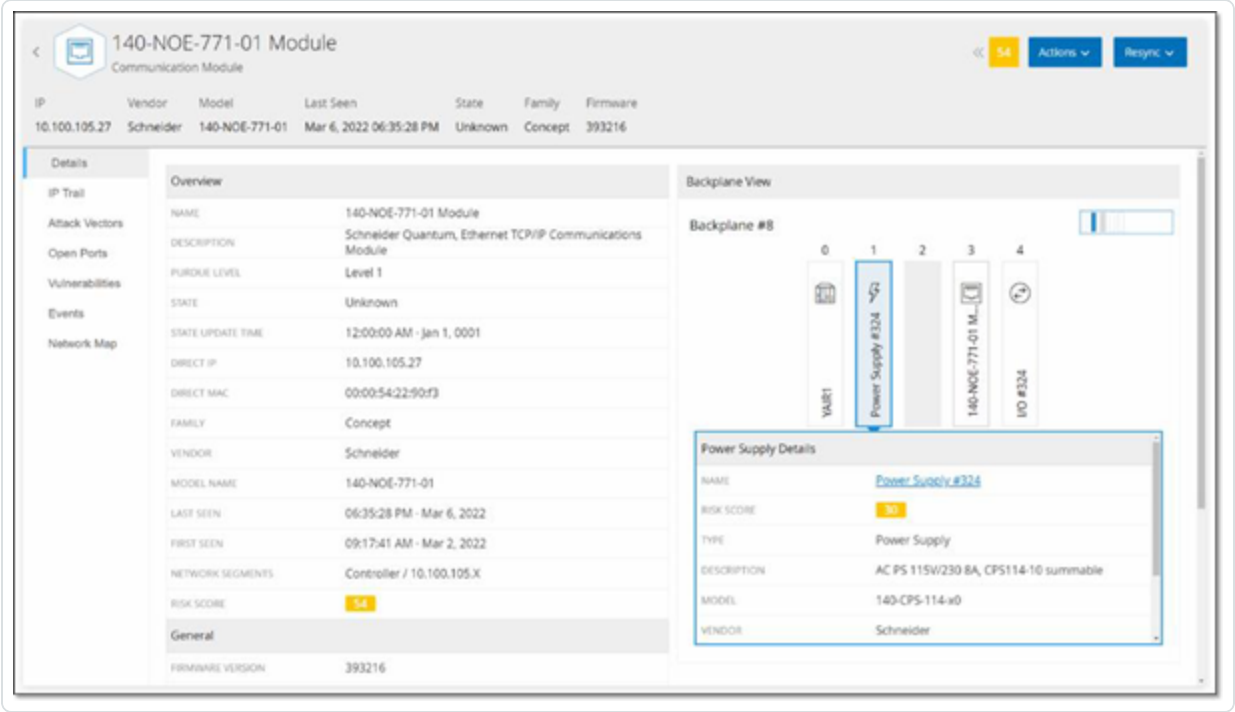
“标头”窗格显示资产当前状态的概览。显示内容包括以下元素：

- **名称**：资产的名称。
- **返回**（链接）：将返回访问此资产屏幕的屏幕。
- **资产类型**：显示资产类型的图标和名称。
- **资产概览**：显示有关资产的基本信息，包括 IP、供应商、系列、型号、固件和上次查看（日期和时间）。
- **风险评分小组件**：显示资产的风险评分。风险评分是对资产所面临威胁的程度进行的评估（从 1 到 100）。有关如何确定该值的说明，请参阅“风险评估”。单击“风险评分”指标可显示一个扩展小组件，其中包含有助于评估风险级别的因素（未解决的事件、漏洞和重要程度）的细分。其中一些元素是指向显示该元素详细信息的相关屏幕的链接。

- **“操作”菜单**：允许编辑资产详细信息或运行 Tenable Nessus 扫描。
- **“重新同步”按钮**：单击此按钮即可手动运行可用于此资产的一个或多个查询。请参阅 “标头”窗格。

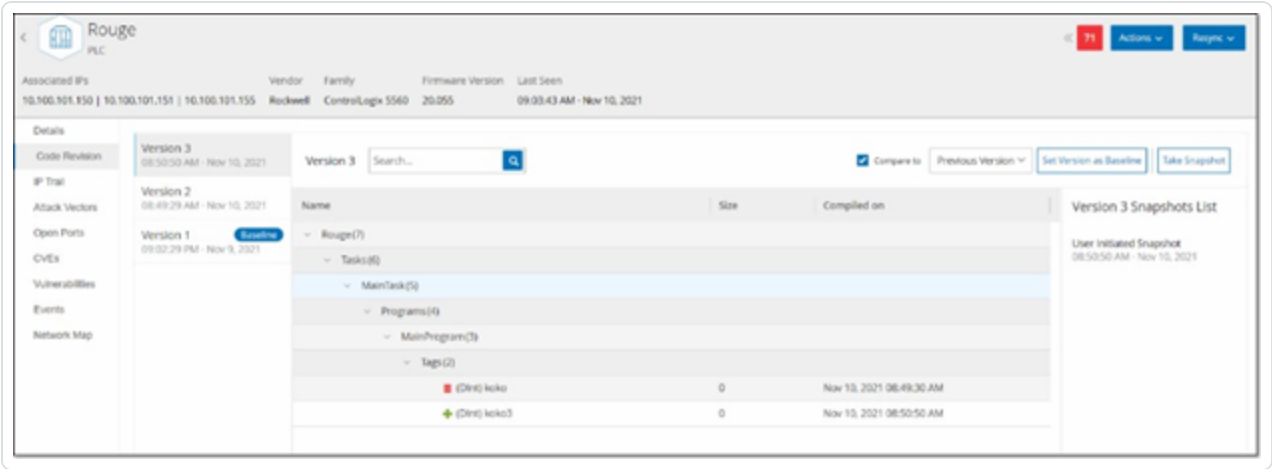
“详细信息”选项卡



“**详细信息**”选项卡显示有关所选资产的其他详细信息。信息被分成若干个部分，以显示指定资产的各种系统类型和配置数据。系统仅显示与指定资产相关的部分。以下是可能针对各种资产显示的所有部分类别的列表：概览、常规、项目、内存、以太网、Profinet、OS、系统、硬件、设备和驱动程序、USB 设备、安装的软件、IEC -61850 和接口状态。

对于连接到背板的资产，还有一个“背板视图”部分，该部分显示背板配置的图形表示，其中包括每个已连接设备的插槽位置。选择一个设备，即可在下方窗格中显示其详细信息。

代码修订



“代码修订”选项卡(仅适用于控制器)显示由 OT Security“快照”捕获的控制器代码的各种版本。每个“快照”版本都包含拍摄“快照”时的代码修订信息,其中包括有关特定部分(代码块/Rung)和标签的详细信息。每当“快照”与该控制器的上一个“快照”不同时,系统就会创建代码修订的新版本。可以在版本之间进行比较,了解对控制器代码进行了哪些更改。

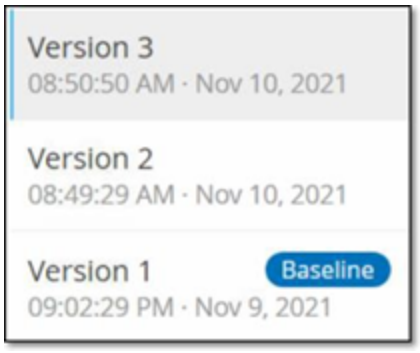
可以通过以下方式触发快照:

- **常规**:根据用户在“系统设置”屏幕中的设置,定期拍摄快照。
- **活动触发**:系统在检测到特定代码活动(例如代码下载)时触发快照。
- **用户发起**:用户可以通过单击特定资产的“拍摄快照”按钮,手动触发快照。

您可以配置“快照不匹配”策略来检测对控制器代码的添加、删除或更改操作,详情请参阅“配置事件:控制器活动事件类型”。

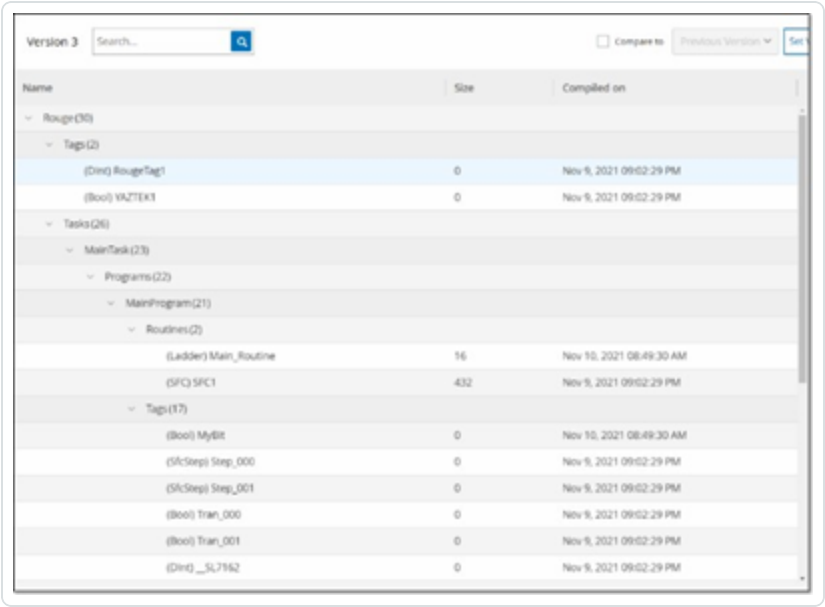
以下部分介绍了代码修订显示的各个部分,以及如何比较不同的“快照”版本。

“版本选择”窗格



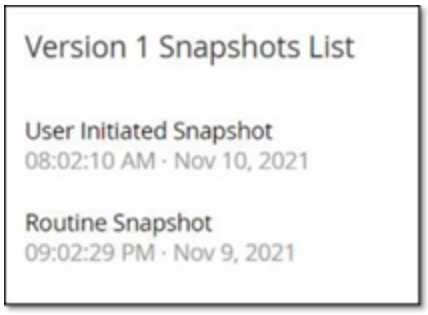
此窗格显示此控制器代码修订的所有可用版本的列表。对于每个版本而言，系统会显示已知版本的开始时间。每次检测到上一个“快照”发生变更时，系统都会创建一个新版本。“基线”标签会指出当前哪个版本被设置为用于比较的基线版本。选择一个版本，以在“快照详细信息”窗格中显示其代码修订。

“快照详细信息”窗格



“详细信息”窗格显示有关所选快照版本的特定代码块、Rung 和标签的详细信息。代码元素会以树状结构显示，并带有用于展开/最小化所显示详细信息的箭头。该窗格会显示每个元素的名称、大小和编译日期。您可以将所选版本与上一版本或“基线”版本进行比较，以查看进行了哪些更改，详情请参阅“比较快照版本”。

“版本历史记录”窗格



此窗格显示有关捕获所选版本的“快照”的详细信息，其中包括启动快照的方法以及捕获快照的日期和时间。

如果快照之间无任何更改，则系统会将多个快照组合为一个版本。该版本的“快照历史记录”窗格中列出了所有相同的快照。

比较快照版本

可以将快照版本与上一版本或基线版本进行比较。运行比较后，“快照详细信息”窗格将显示对两个快照之间的控制器代码做出的更改。

相关更改会以下列方式标出：

✚已添加：在所选版本中添加的新代码。

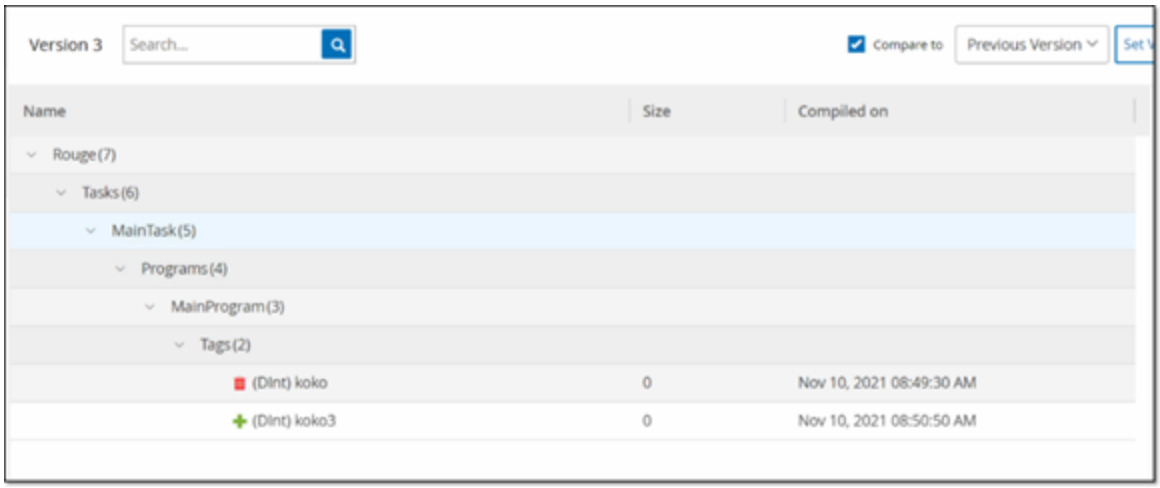
已删除：从所选版本中删除的代码。

已编辑：在所选版本中编辑过的新代码。

若要将快照版本与上一版本进行比较，请执行以下操作：

1. 在“**清单**”>“**控制器**”屏幕上，选择所需的控制器。
2. 单击“**代码修订**”选项卡。
3. 在“**版本选择**”窗格中，选择要分析的版本。
4. 在“**快照详细信息**”窗格顶部的“比较”字段中，从下拉菜单中选择“**上一版本**”。
5. 单击“**比较**”复选框。

   “快照详细信息”窗格会显示两个版本之间的所有差异。对于每次变更，都会有一个图标表示所发生的变更类型。



若要将快照版本与之前的版本进行比较（上一版本除外），请执行以下操作：

1. 在“**清单**”>“**控制器**”屏幕上，选择所需的控制器。
2. 单击“**代码修订**”选项卡。
3. 在“**版本选择**”窗格中，选择要用作比较基线的版本。
4. 在“**快照详细信息**”窗格的顶部，单击“**将版本设置为基线**”。

   显示所选版本的“**基线**”标签，表示其已设置为基线版本。

   > **注意**：将版本设置为基线仅影响使用此屏幕进行的比较，不影响检查快照不匹配的策略。

5. 在“**版本选择**”窗格中，选择要与基线比较的版本。
6. 单击“比较”复选框。在“比较”复选框旁的字段中，从下拉菜单中选择“基线版本”。
7. “快照详细信息”窗格会显示两个版本之间的所有差异。对于每次变更，都会有一个图标表示所发生的变更类型。

创建快照

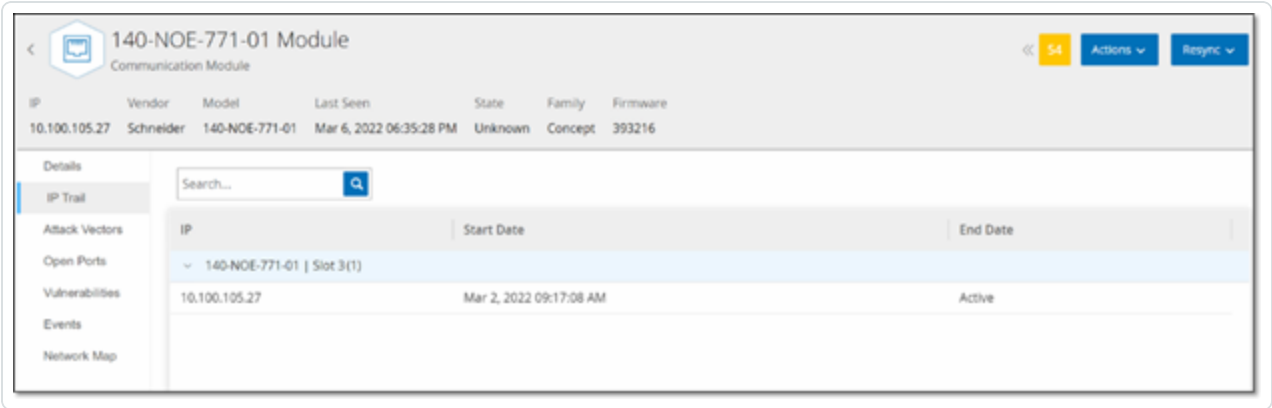
用户可手动发起快照。例如，建议在技术人员维修控制器之前和之后拍摄快照。

若要创建控制器快照，请执行以下操作：

1. 在“**清单**”>“**控制器**”屏幕上，选择所需的控制器。
2. 单击“**代码修订**”选项卡。
3. 在“**快照详细信息**”窗格的右上方，单击“**拍摄快照**”。

   此时用户发起的快照已创建。
4. 如果未发现任何变更，则系统会将新的用户识别快照添加到最新版本的“修订历史记录”窗格。如果发现变更，则系统会创建一个显示代码修订变更的新版本。

IP 追踪



“IP 追踪”选项卡显示与此资产相关的所有 IP。“网卡”列显示此资产使用的网卡列表。单击某个网卡旁边的箭头展开列表，以显示连接到共享背板的所有资产的 IP。

这些列表包括使用 IP 地址的开始和结束日期。“结束日期”的选项包括：

- **活动**：此资产当前正在使用 IP 地址。
- **（日期/时间）**：此资产的 IP 地址上次活动的日期和时间（如果该地址在过去 30 天之内一直处于活动状态）。
- **{日期/时间}（非活动）**：此资产的 IP 地址上次活动的日期和时间（如果该地址在过去 30 天或更长时间内处于非活动状态）。
- **非活动**：IP 地址正被另一项资产使用。

攻击途径

攻击者可利用网络中易受攻击的“弱链接”获取关键资产的访问权限。该重要资产是攻击目标，攻击途径是攻击者用于获取该资产访问权限的途径。

如何确定攻击途径？

指定目标资产后，系统将计算可访问此资产的所有潜在攻击途径，并识别最有可能危害此资产的途径。此预测以多个参数为因素，并使用基于风险的方法来识别最危险的攻击途径。使用的参数包括：

- 资产风险等级
- 途径的长度
- 资产之间的通信方法
- 外部通信（互联网/公司网络）与内部通信

推荐的缓解步骤

要将利用所选途径的潜在攻击的风险降至最低，请执行以下推荐的缓解步骤：

- 降低攻击途径中所含资产的相关风险评分或单独风险评分。
- 最大程度减少或切断对外部网络（互联网或公司网络）的访问
- 检查链上的通信路径，并验证这些路径与流程的相关性。如果这些通信路径并非至关重要，则应删除它们（例如关闭端口或删除服务），以消除潜在攻击途径。

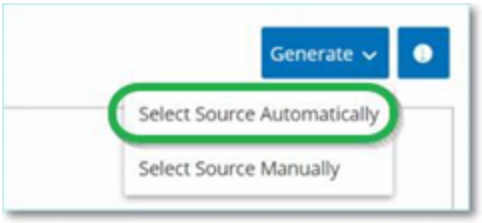
生成攻击途径

需要为每个相关目标资产手动生成攻击途径。可针对所需目标资产的“攻击途径”选项卡完成此操作。生成攻击途径的方法有两种：

- **自动**：OT Security 评估所有潜在攻击途径并识别最易受到攻击的途径。
- **手动**：指定特定源资产后，OT Security 会展示可用于访问目标资产的潜在路径（如有）。

若要生成自动攻击途径，请执行以下操作：

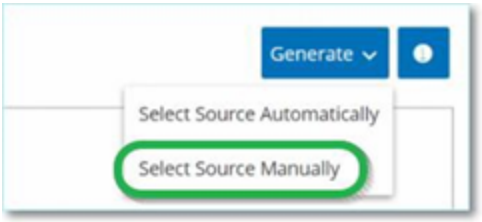
1. 导航至所需目标资产的“**资产详细信息**”页面，然后单击“**攻击途径**”选项卡。
2. 单击“**生成**”，然后从下拉列表中单击“**自动选择源**”。



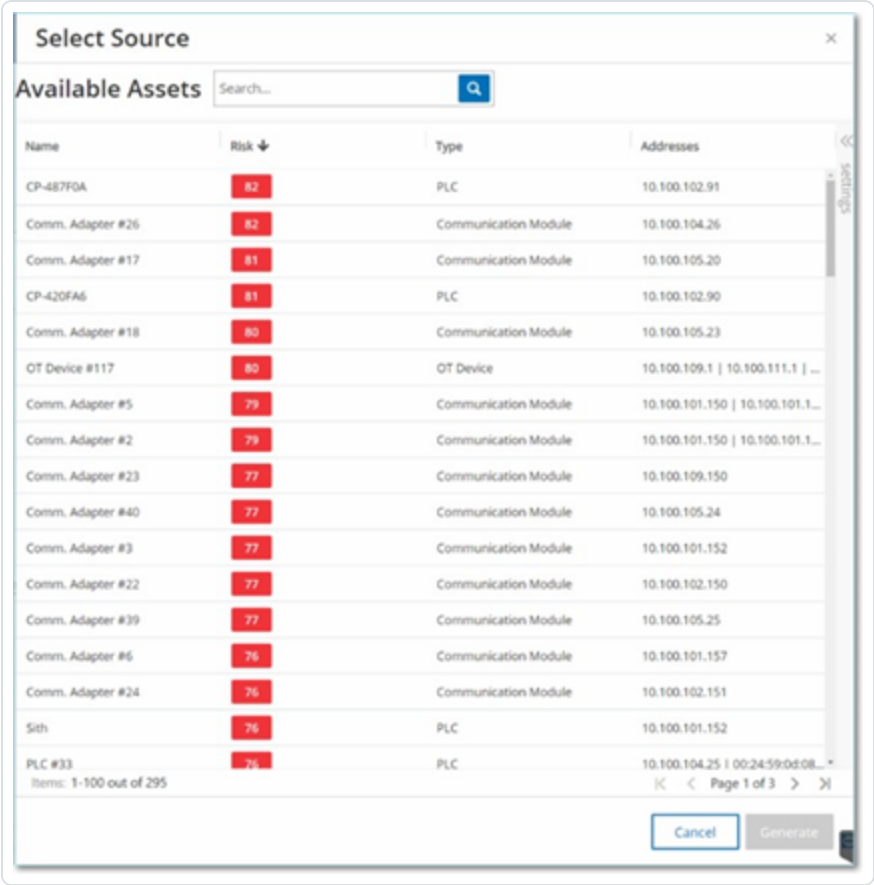
此时攻击途径会自动生成并显示在“**攻击途径**”选项卡中。

若要生成手动攻击途径，请执行以下操作：

1. 导航至所需目标资产的“**资产详细信息**”页面，然后单击“**攻击途径**”选项卡。
2. 单击“**生成**”，然后从下拉列表中单击“**手动选择源**”。



此时会显示“**选择源**”窗口。

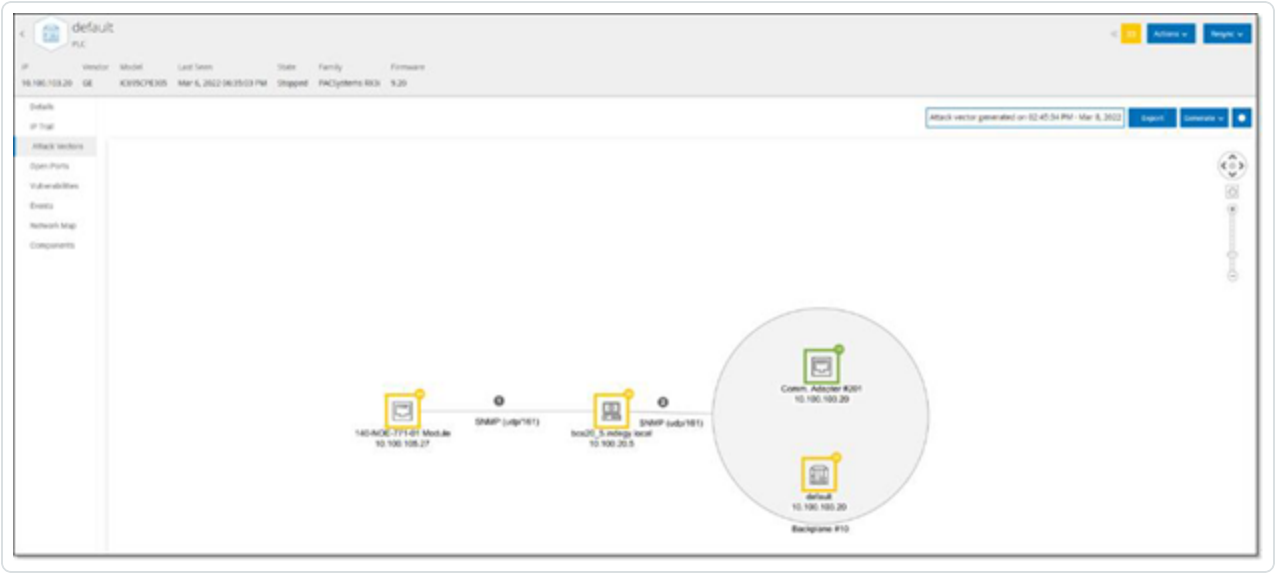


注意:默认情况下,源资产按风险评分排序。可以调整所需资产的显示设置或对其进行搜索。

3. 选择所需的源资产。
4. 单击"**生成**"。

   此时攻击途径会手动生成并显示在"**攻击途径**"选项卡中。

查看攻击途径

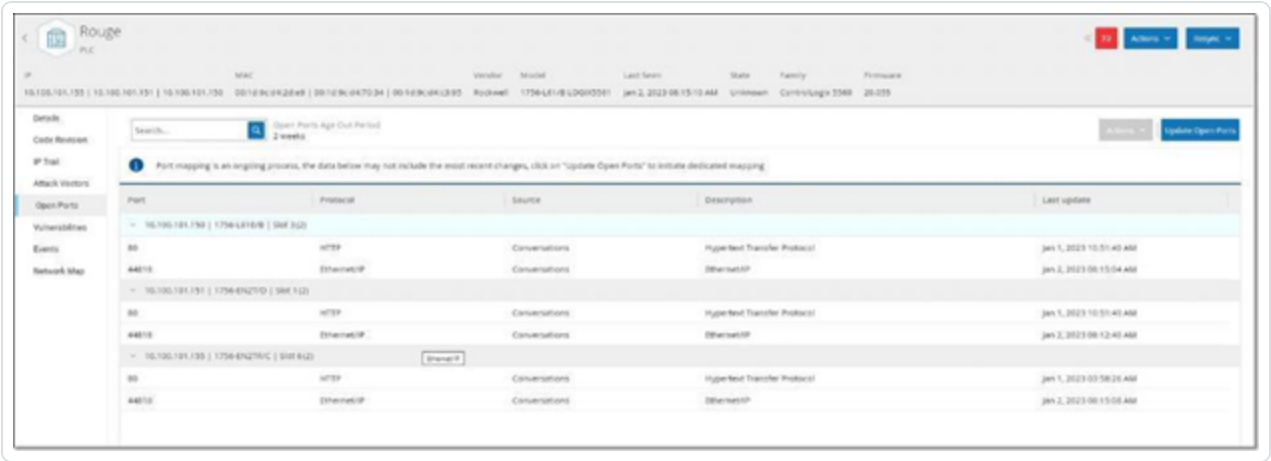


“攻击途径”选项卡显示了最近针对指定目标资产生成的“攻击途径”图表。“生成”按钮旁的方框显示了所示攻击途径的生成日期和时间。“攻击途径”图表包括以下元素：

- 对于攻击途径中包含的每项资产，系统会显示风险级别和 IP 地址。单击“资产”图标即可显示有关其风险因素的更多详细信息。
- 系统显示每个网络连接的通信协议。
- 共享背板的资产均以圆圈圈起。

> **注意**：单击“攻击途径”选项卡右上角的“帮助”按钮，即可获取“攻击途径”功能的说明。

已打开的端口



“**已打开的端口**”选项卡显示此资产上的已打开的端口列表。系统提供关于每个已打开端口的详细信息，包括其使用的协议、其功能说明、上次更新数据的日期和时间以及表明端口已打开的信息来源（主动查询、端口映射、对话、Tenable Nessus Network Monitor 或 Tenable Nessus 扫描）。此外，系统会显示该资产的每个可用 IP 的单独已打开的端口列表（包括通过共享背板访问的端口）。单击 IP 旁的箭头可展开列表，以显示其已打开的端口。

系统自动设定了“**已打开端口的使用期限**”。在此之后，如果没有收到进一步表明该端口仍处于打开状态的指示，已打开端口列表将自动从列表中删除。默认时长为两周。要调整“已打开端口的使用期限”的时长，请参阅设备。

可以在主动查询中配置已打开端口的扫描参数。还可以针对所选资产运行手动查询，以更新已打开的端口的列表。

若要手动更新已打开的端口列表，请执行以下操作：

1. 在“**清单**”>“**控制器/网络资产**”屏幕上，选择所需的资产。

   此时会显示“**资产详细信息**”屏幕。

2. 单击“**已打开的端口**”选项卡。

3. 在“已打开的端口”窗格的右上角单击“**更新已打开的端口**”。

   运行新的扫描，更新为此控制器显示的已打开的端口。

“已打开的端口”选项卡中的其他操作

可以在某个特定资产的“已打开的端口”选项卡中，针对特定已打开的端口采取以下进一步操作。

- 扫描：运行所选端口的扫描。
- 查看：通过访问设备的 Web 界面，显示其他设备的详细信息和诊断。

若要在特定端口上运行扫描，请执行以下操作：

1. 在“**清单**”>“**控制器/网络资产**”屏幕上，选择所需的资产。

   此时会显示“**资产详细信息**”屏幕。
2. 单击“**已打开的端口**”选项卡。
3. 选择一个特定端口。
4. 单击“**操作**”菜单。
5. 从下拉菜单中选择“**扫描**”。

   OT Security 对所选端口运行扫描。

若要查看资产的门户网站，请执行以下操作：

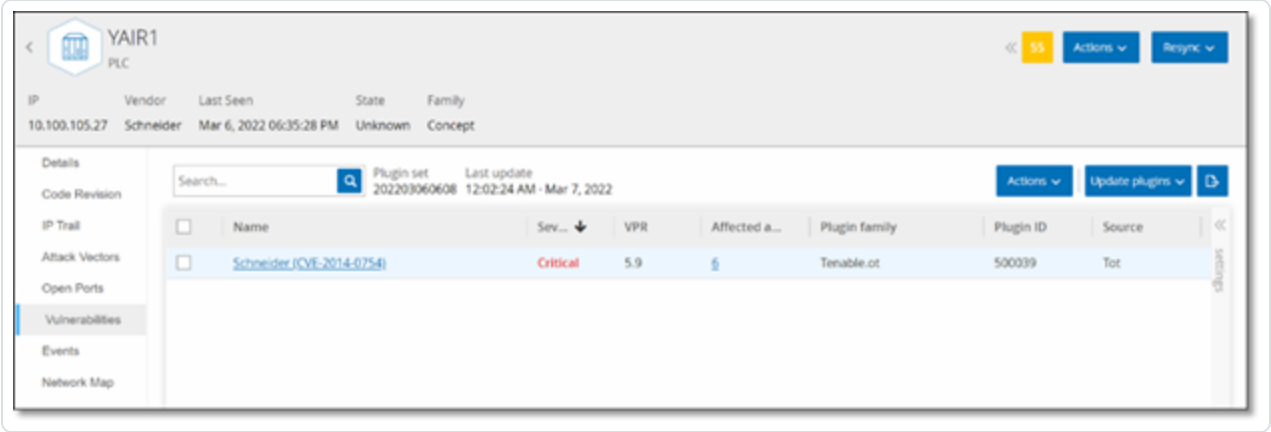
> **注意**：此选项仅在端口 80（用于 Web 访问）属于已打开的端口之一时可用。

1. 在“**清单**”>“**控制器/网络资产**”屏幕上，选择所需的资产。

   此时会显示“**资产详细信息**”屏幕。
2. 单击“**已打开的端口**”选项卡。
3. 选择一个特定端口。
4. 单击“**操作**”菜单。
5. 从下拉菜单中选择“**查看**”。

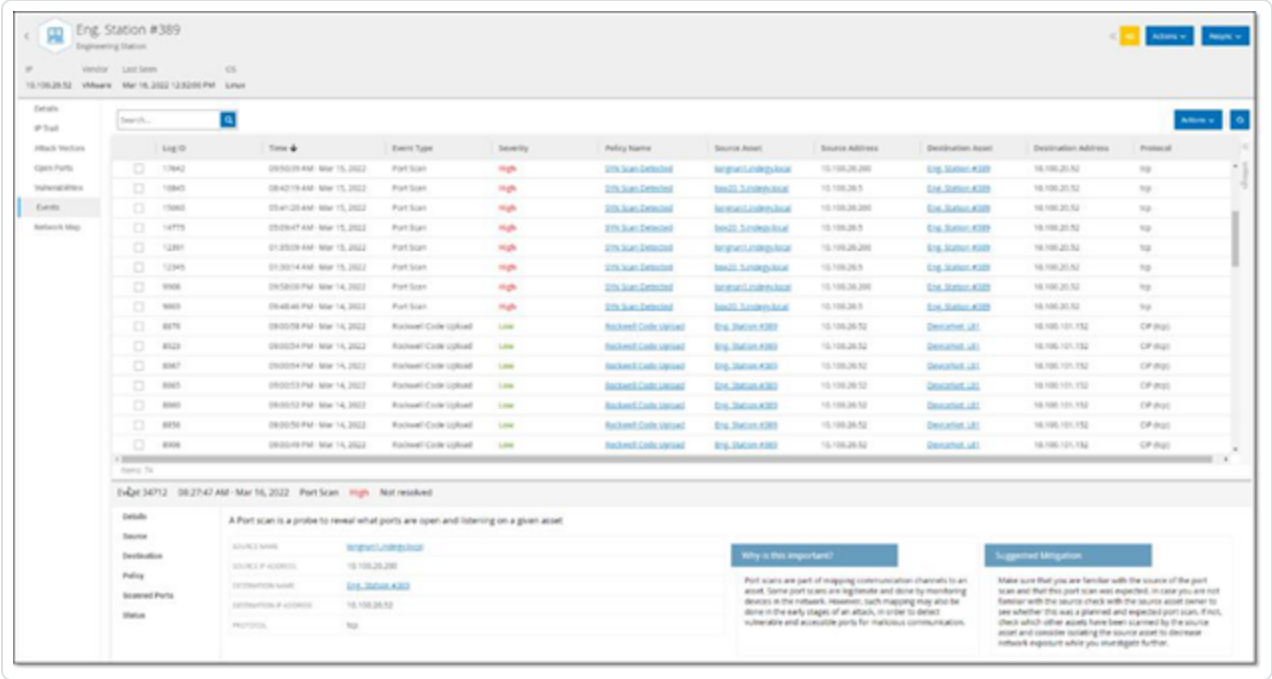
   此时将打开一个新的浏览器选项卡，显示该资产的资产门户。

漏洞



"**漏洞**"选项卡会显示 OT Security 插件检测到的影响指定资产的所有漏洞的列表。系统会识别漏洞，例如过时的 Windows 操作系统、使用易受攻击的协议和已知对特定类型设备有风险或非必需的开放通信端口。每个列表都显示了威胁性质及其严重程度的详细信息。此选项卡中显示的信息与"**风险**" > "**漏洞**"屏幕上显示的信息相同，只有与此处所示特定资产相关的漏洞除外。有关漏洞信息的说明，请参阅"漏洞"。

事件



“**事件**”选项卡显示 OT Security 插件检测到的网络中涉及资产的事件的详细列表。可以通过调整要显示的列以及各列的位置来自定义显示设置。可根据不同类别(例如事件类型、严重程度、策略名称)对事件进行分组。还可以对事件列表进行排序和筛选，也可以搜索文本。有关自定义功能的说明，请参阅“管理控制台用户界面元素”。

屏幕底部显示有关所选事件的详细信息，并分为多个选项卡。系统仅显示与所选事件的事件类型相关的选项卡。有关事件的更多信息，请参阅“事件”。

窗格顶部有一个“**操作**”按钮，该按钮便于针对所选事件执行以下操作：

- 解决：将此事件标记为“已解决”。
- 下载 PCAP：下载此事件的 PCAP 文件。
- 排除：为此事件创建策略排除项。

有关这些操作的详细信息，请参阅“事件”一章。

下表介绍了针对每个事件列表显示的信息：

参数	描述
日志	系统生成的用于参考事件的 ID。

ID	
时间	事件发生的日期和时间。
事件类型	说明触发事件的活动类型。事件由在系统中设置的策略生成。有关各种策略的说明，请参阅“策略类型”。
严重程度	显示事件的严重程度级别。以下是可能值的说明： • 无：无需关注。 • 信息：无需立即关注。应在方便时检查。 • 警告：已发生潜在危害活动，需适度关注。应在方便时予以处理。 • 严重：已发生潜在危害活动，需高度关注。应立即处理。
策略名称	生成事件的策略的名称。该名称是指向策略列表的链接。
源资产	发起事件的资产的名称。此字段是指向资产清单的链接。
源地址	发起事件的资产的 IP 或 MAC。
源地址	发起事件的资产的 IP 或 MAC。
目标资产	受事件影响的资产的名称。此字段是指向资产清单的链接。
目标地址	受事件影响的资产的 IP 或 MAC。
协议	协议会在相关时显示用于生成此事件的对话的协议。
事件类别	显示事件的一般类别。 注意：所有类型的事件会在“所有事件”屏幕上显示。每个特定的“事件”屏幕仅显示指定类别的事件。 以下是事件类别的简要说明（有关更加详细的说明，请参阅“策略类别和子类

	别”）： • 配置事件：这包括两个子类别 • 控制器验证事件：这些策略检测网络中的控制器发生的变更。 • 控制器活动事件：活动策略与网络中发生的活动（即在网络中的资产之间实施的“命令”）相关。 • SCADA 事件：识别控制器数据平面变更的策略。 • 网络威胁事件：这些策略识别表示入侵威胁的网络流量。 • 网络事件：这些策略与网络中的资产以及资产之间的通信流有关。
状态	显示事件是否已被标记为“已解决”。
解决者	对于已解决的事件，显示哪个用户将该事件标记为“已解决”。
解决日期	对于已解决的事件，显示何时将该事件标记为“已解决”。
注释	显示解决事件时添加的任何注释。

网络映射

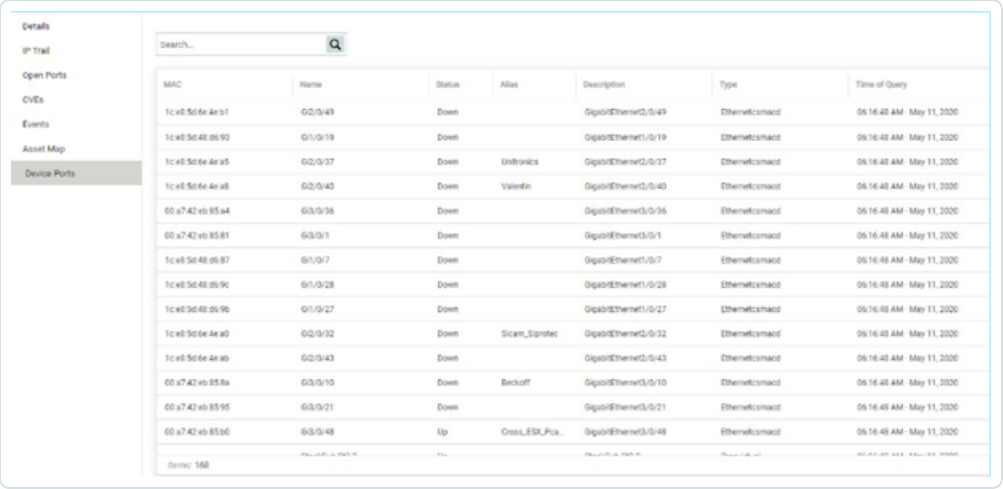
“**网络映射**”选项卡显示资产的网络连接的可视化图形。此视图显示所选资产在过去 30 天内建立的所有连接。

此选项卡中显示的信息与“**网络映射**”屏幕上显示的信息类型，但仅限于涉及此特定资产的连接。此外，此屏幕显示单个资产的连接，不显示与“网络映射”屏幕中所示的资产组的连接。有关此选项卡中所示信息的说明，请参阅“网络映射”。

若要查看所有资产的网络映射，请单击“**转至网络映射**”按钮。单击时，“网络映射”将动态放大并聚焦此资产，并显示其与其他资产组的连接。

单击映射上的任何已连接资产可显示该资产的详细信息，单击资产名称中的链接可前往所选资产的“详细信息”屏幕。

设备端口



系统会为网络交换机显示“设备端口”选项卡，还会显示有关网络交换机上的端口的详细信息。使用对交换机的 SNMP 查询收集此数据。系统会显示每个端口的以下信息：MAC 地址、名称、连接状态（启动或关闭）、别名和说明。

注意：此选项卡仅在针对帐户激活时可用。要激活此功能，请联系支持代理。

编辑资产详细信息

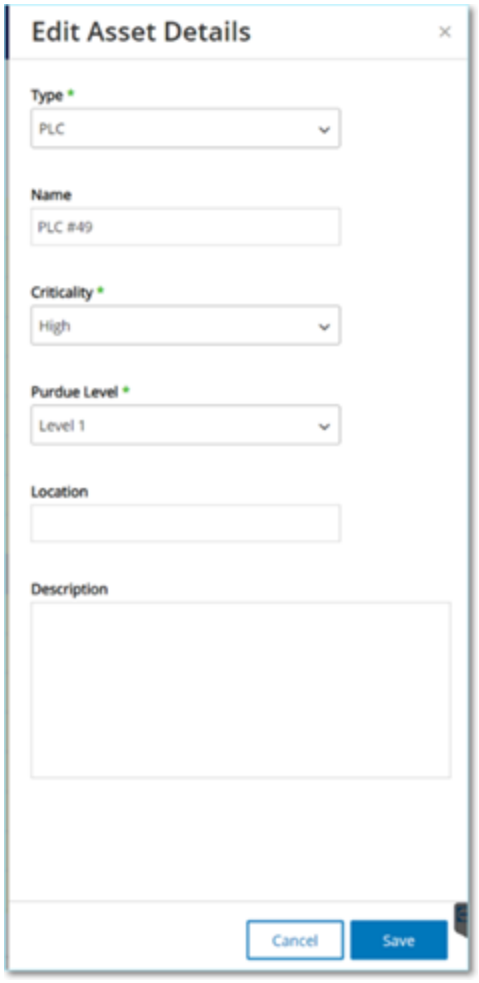
OT Security 会根据其内部数据及其在网络中的活动自动识别资产类型和名称。如果系统无法收集此信息，或者您认为自动识别不准确，则可以直接通过 UI 或上传 CSV 文件来编辑这些参数。还可以添加一般资产说明和装置位置说明。

通过 UI 编辑资产详细信息

若要编辑单个资产的资产详细信息，请执行以下操作：

1. 在“**清单**”下，单击“**控制器**”或“**网络资产**”。
2. 选择所需的源资产。
3. 在标题栏中单击“**操作**”按钮。
4. 从下拉菜单中选择“**编辑**”。

   此时会打开“**编辑资产详细信息**”窗口。



5. 在“**类型**”字段中，从下拉列表中选择资产类型。
6. 在“**名称**”字段中，输入将在 OT Security UI 中识别的资产的名称。
7. 在“**重要程度**”字段中，输入此资产对系统的重要程度。

8. 在“**普渡层**”字段中，根据资产类型输入普渡层。
9. 在“**背板**”字段（适用于控制器）中，输入安装资产的背板的名称。
10. 在“**位置**”字段中，输入资产位置的说明。此字段为选填字段。相关数据显示在资产表中以及此资产的“资产详细信息”屏幕中。
11. 在“**说明**”字段中，输入资产说明。此字段为选填字段。相关数据显示此资产的“资产详细信息”屏幕中。
12. 单击“**保存**”。

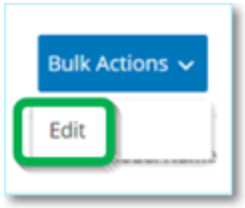
    系统会保存编辑过的资产详细信息。

若要编辑多个资产（批量处理），请执行以下操作：

1. 在“**清单**”下，单击“**控制器**”或“**网络资产**”。
2. 选中每个所需资产旁的复选框。

   注意：您还可以通过在单击每个所需资产的同时按住“Shift”键来选择多个资产。

3. 单击“**批量操作**”菜单，然后从下拉列表中选择“**编辑**”。



   此时会显示“**批量编辑**”屏幕，其中包含可用于批量编辑的参数。

4. 选中要编辑的每个参数旁边的复选框（“类型”、“重要程度”、“普渡层”、“网段”、“位置”和“说明”）。

   注意：批量编辑网段时，请先按类型筛选资产，然后再选择要批量编辑的资产。具有多个 IP 地址的资产不能包含在网段的批量编辑操作中；需要手动编辑每个资产。

5. 根据需要设置每个参数。

   注意：在“批量编辑”字段中输入的信息将覆盖选定资产的任何当前内容。如果选中参数旁的复选框但未输入选项，则该参数的当前值将被删除。

6. 单击“**保存**”。

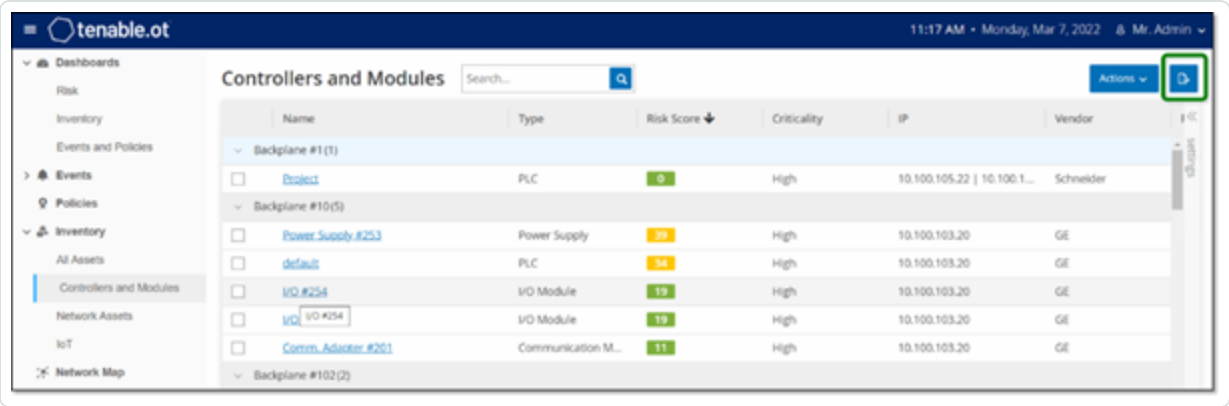
   资产将与新配置一起保存。

通过上传 CSV 编辑资产详细信息

这种编辑资产详细信息的方法支持通过 CSV 文件编辑大量资产，无需在 UI 中手动编辑。可以使用此方法编辑下列详细信息："类型"、"名称"、"重要程度"、"普渡层"、"位置"、"说明"和自定义字段。

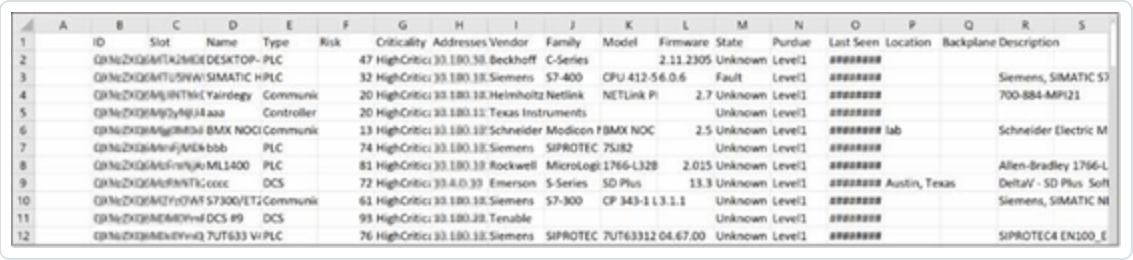
若要通过 CSV 编辑资产详细信息，请执行以下操作：

1. 在"**清单**"下，单击"**所有资产**"、"**控制器**和**模块**"或"**网络资产**"。
2. 单击"**导出**"按钮。



下载清单的 CSV 文件。

3. 导航到刚下载的文件并将其打开。



4. 通过更改单元格内容来编辑允许的参数。（允许的参数包括"类型"、"名称"、"重要程度"、"普渡层"、"位置"、"说明"和自定义字段。）

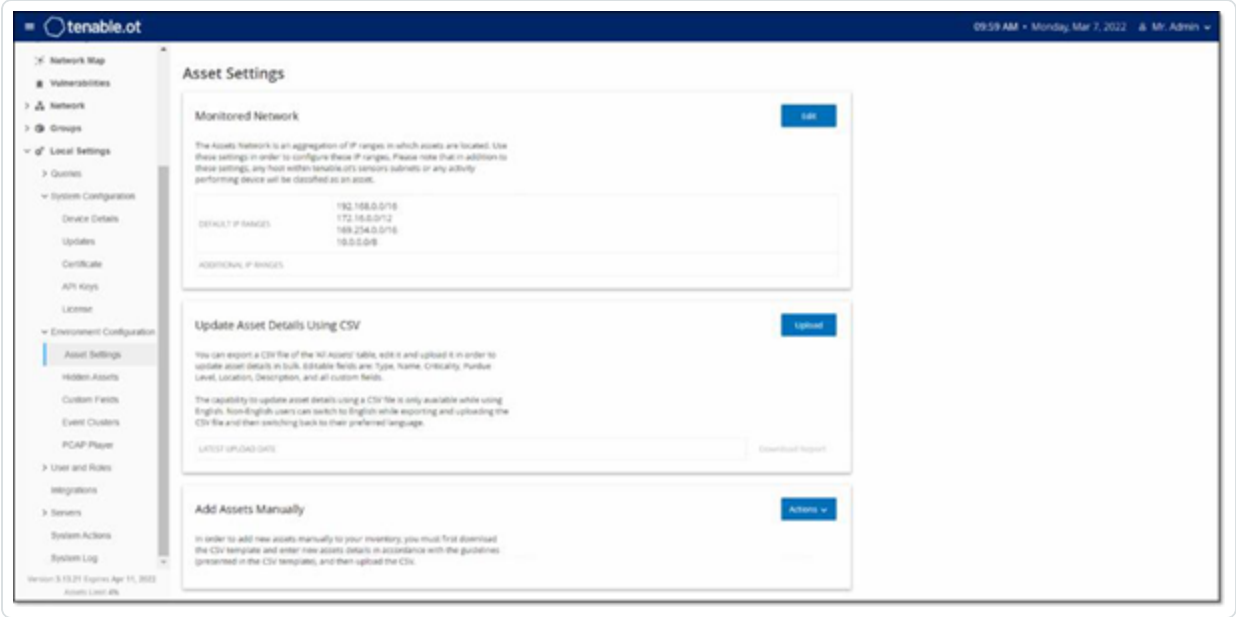
> **注意**：您必须为需要特定选项的参数（例如类型、重要程度、普渡层）输入有效数据。否则，相应的资产将无法更新。

5. 将文件另存为 CSV 文件类型。

注意：只有修改的资产才会在系统中更新。未包含在 CSV 中的资产或未经修改的行在系统中将保持不变。无法使用此方法删除资产。

6. 在“**本地设置**”下，转至“**环境配置**”>“**资产设置**”。

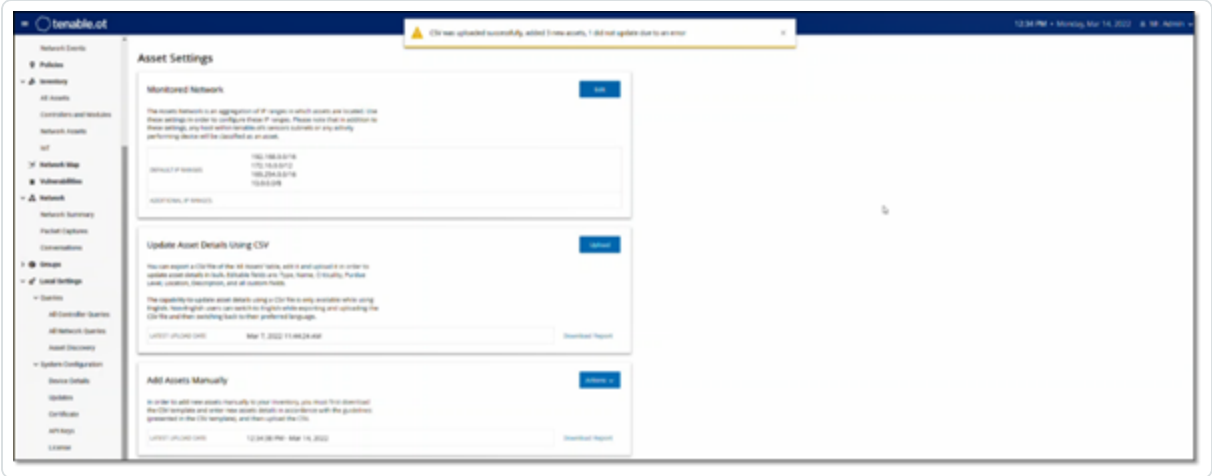
   此时会显示“**资产设置**”屏幕。



7. 在“**使用 CSV 更新资产详细信息**”部分中，单击“**上传**”。

8. 按照设备的导航提示上传刚刚保存的 CSV 文件。

   此时会显示一条确认消息，指出已成功更新的行数。



已更新“使用 CSV 更新资产详细信息”部分中的“最近上传日期”字段。

9. 如需了解有关上传结果的更多信息，请在“**使用 CSV 更新资产详细信息**”部分中单击“**下载报告**”。

   此时将下载一个 CSV 文件，该文件详细说明了已成功更新和更新失败的资产 ID。

隐藏资产

可以隐藏资产清单中的一项或多项资产。已隐藏的资产不会显示在“清单”中，并且会从组中删除。但仍会显示隐藏资产的事件和网络活动。

可以从“**本地设置**”>“**资产**”>“**隐藏资产**”屏幕还原隐藏的资产，详情请参阅“本地设置”。

若要隐藏一项或多项资产，请执行以下操作：

1. 在“**清单**”下，单击“**控制器**”或“**网络资产**”。
2. 选中要删除的一项或多项资产旁边的复选框。
3. 在标题栏中单击“**操作**”按钮。
4. 从下拉菜单中选择“**隐藏资产**”。

   此时会打开“**隐藏资产**”窗口。
5. 可以在“**注释**”字段中添加关于资产的自由文本注释。(可选)

   > **注意**：注释会在已删除资产列表中显示，该列表位于“**本地设置**”>“**资产**”>“**隐藏资产**”屏幕上。
6. 单击“**隐藏**”。

   对于“清单”和“组”而言，资产已隐藏。

执行资产特定 Tenable Nessus 扫描

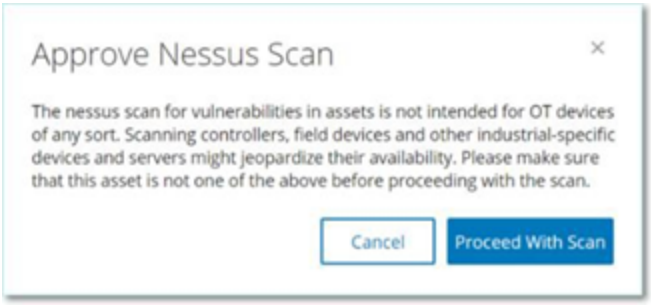
Tenable Nessus 是一款可以扫描 IT 设备以检测漏洞的工具。OT Security 支持针对 OT 网络内的特定 IT 资产运行 Tenable Nessus"基本网络扫描"。这是一种主动式完整系统扫描，可以收集有关服务器和网络设备漏洞的更多信息。此扫描将使用用户提供的 WMI 和 SNMP 凭据。此操作仅适用于基于相关 PC 的计算机。扫描结果会显示在"漏洞"屏幕上。您还可以创建自定义扫描，以在特定的网络资产集上运行一系列特定的 Tenable Nessus 插件，详情请参阅"Tenable Nessus插件扫描"。

注意：Tenable Nessus 是最适合在 IT 环境中使用的侵入式工具。建议不要在 OT 设备上使用，因为它可能会干扰该等设备正常运作。

若要手动运行 Tenable Nessus 扫描，请执行以下操作：

1. 在"**清单**"下，单击"**网络资产**"。
2. 选择所需的源资产。
3. 在标题栏中单击"**操作**"按钮。
4. 从下拉菜单中选择"**Nessus 扫描**"。

   此时会显示"**批准 Nessus 扫描**"确认窗口。



5. 单击"**继续扫描**"。

   Tenable Nessus 扫描正在运行。

执行重新同步

重新同步函数对网络和控制器发起一个或多个查询，以捕获此资产的最新信息。可以运行所有可用查询，或特定查询。

以下是可用于"重新同步"的查询：

- **背板扫描**：发现背板中的模块及其规格。
- **DNS 扫描**：搜索网络资产的 DNS 名称。
- **详细信息查询**：检索控制器的硬件和固件的详细信息。结果会显示在"**资产**">"**控制器和模块**"页面的"**固件**"字段中。
- **识别查询**：使用多种协议以识别资产。
- **NetBIOS 查询**：发送 NetBIOS 单播数据包，该数据包可用于分类并检测网络中的 Windows 计算机。
- **SNMP 查询（适用于启用了 SNMP 的资产）**：检索启用了 SNMP 的资产的配置详细信息。
- **状态**：检测资产的当前状态（**运行中**、**已停止**、**故障**、**未知**和**测试**）。
- **ARP**：检索在网络中检测到的新 IP 的 MAC 地址。结果显示在"**详细信息**">"**概览**"部分。

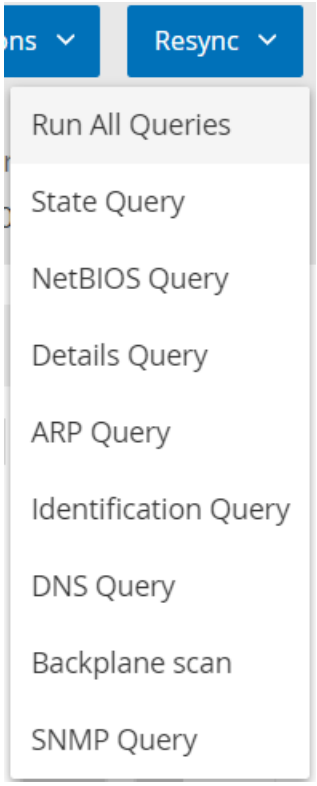
在特定情况下，"**重新同步**"按钮可能会被禁用。可能的原因包括：

- 设备不可访问或缺少可用查询。
- "**主动查询**"页面上配置的权限可能会限制非管理员帐户发起特定查询。
- OT Security 部署中未启用查询。
- "**主动查询**">"**手动**"部分中的所有查询均已禁用。
- 资产缺少可查询的已知 IP 地址。

若要运行重新同步资产数据，请执行以下操作：

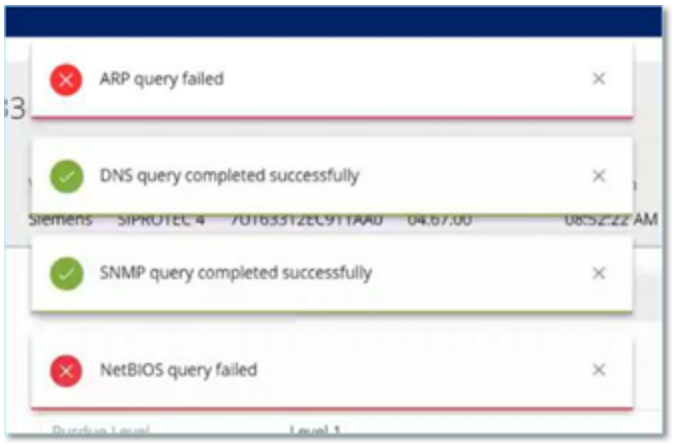
1. 在所需资产的"**资产详细信息**"页面上，点击右上角的"**重新同步**"。

   此时会出现查询的下拉列表。



2. 单击要运行的查询，或单击“**运行所有查询**”以运行所有可用查询。

   每个查询运行时，都出现一则通知，显示查询的状态。



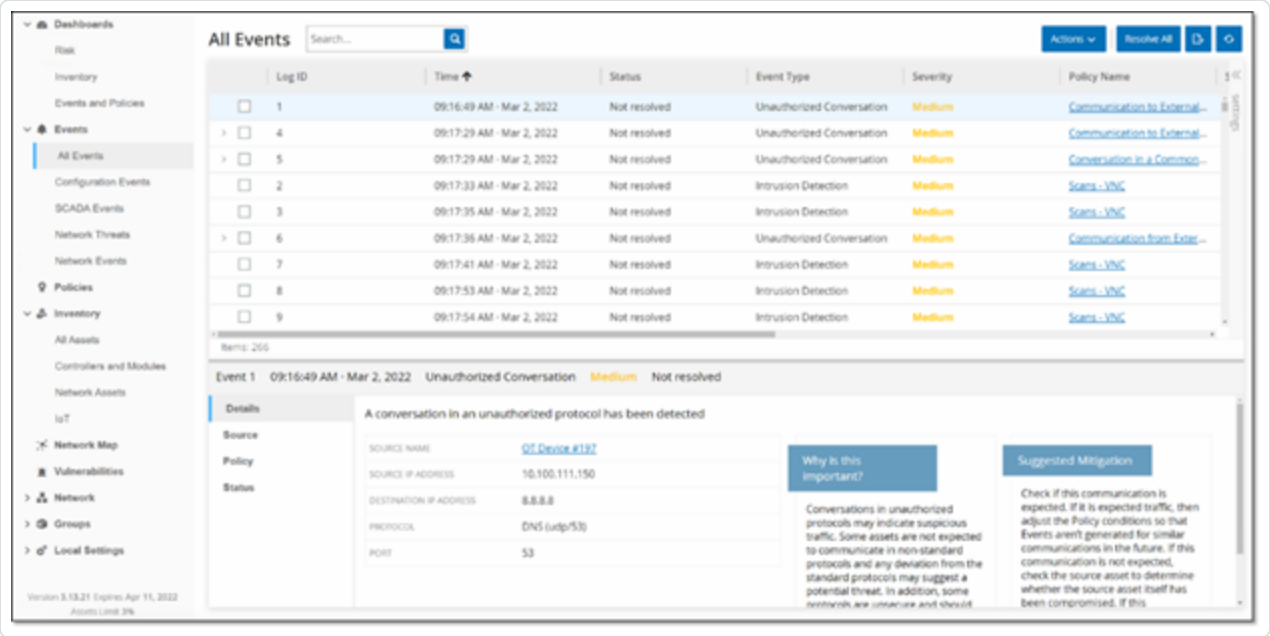
对于每个已完成的查询，OT Security 会根据新数据更新该资产的系统数据。

事件

事件是指系统中生成的通知，用于提醒注意网络中可能有害的活动。在系统中设置的策略会按照以下类别之一生成事件：“配置事件”、“SCADA 事件”、“网络威胁”或“网络事件”。为每个策略分配了一个严重程度级别，目的在于指示事件的严重程度。

策略激活后，系统中符合策略条件的任何事件都将触发事件日志。具有相同特性的多个事件会划分一个群集中。

查看事件



系统中发生的所有事件都会显示在“**所有事件**”屏幕上。事件的特定子集会显示在以下每个事件类别对应的单独屏幕上：“**配置事件**”、“**SCADA 事件**”、“**网络威胁**”和“**网络事件**”。

屏幕顶部显示每个事件的列表。对于每个“事件”屏幕（“配置事件”、“SCADA 事件”、“网络威胁”和“网络事件”），可以通过调整要显示的列以及各列的位置来自定义显示设置。可根据不同类别（例如事件类型、严重程度、策略名称）对事件进行分组。还可以对事件列表进行排序和筛选，也可以搜索文本。有关自定义功能的说明，请参阅“管理控制台用户界面元素”。

标题栏中有一个“**操作**”按钮，该按钮便于针对所选事件执行以下操作：

- 解决：将此事件标记为“已解决”。
- 下载 PCAP：下载此事件的 PCAP 文件。
- 排除：为此事件创建策略排除项。

有关这些操作的详细信息，请参阅以下部分。

屏幕底部显示有关所选事件的详细信息，并分为多个选项卡。系统仅显示与所选事件的事件类型相关的选项卡。系统会显示各种事件的下列选项卡：“详细信息”、“代码”、“源”、“目标”、“策略”、“扫描的端口”和“状态”。

注意：您可以向上或向下拖动面板分隔线，以放大/缩小底部面板显示。

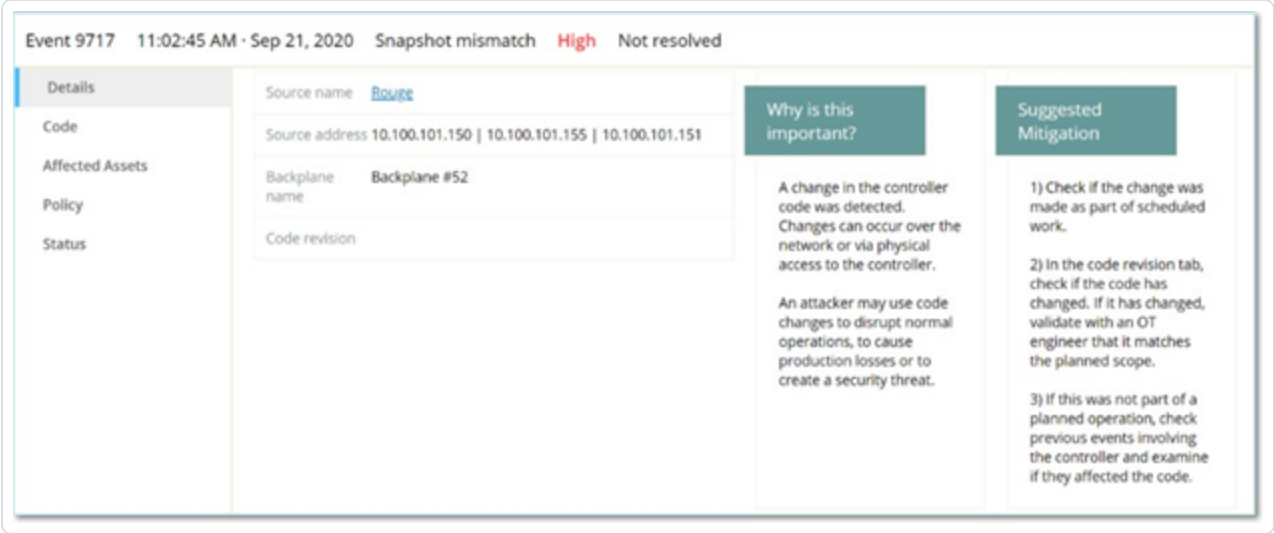
您可以下载与每个事件关联的数据包捕获文件，详情请参阅“网络”。下表介绍了针对每个事件列表显示的信息：

参数	描述
名称	网络中设备的名称。单击资产的名称即可查看该资产的“资产详细信息”屏幕（详情请参阅“资产”）。
地址	资产的 IP 和/或 MAC 地址。 **注意**：一项资产可能具有多个 IP 地址。
类型	资产类型。请参阅“资产类型”，获取有关各种资产类型的说明。
背板	控制器连接到的背板装置。“资产详细信息”屏幕会显示有关背板配置的其他详细信息。
插槽	对于背板上的控制器，显示控制器所连接的插槽编号。
供应商	资产供应商。
系列	控制器供应商定义的产品的系列名称。
固件	控制器上当前安装的固件版本。
位置	用户在 OT Security 资产详细信息中输入的资产的位置。请参阅“资产”。
上次出现	OT Security 上次查看设备的时间。这是设备上次连接到网络或执行活动的时间。
操作系统	资产上运行的操作系统。
日志 ID	系统生成的用于参考事件的 ID。
时间	事件发生的日期和时间。
事件类型	说明触发事件的活动类型。事件由在系统中设置的策略生成。有关各种策略的说明，请参阅“策略类型”。
严重	显示事件的严重程度级别。以下是可能值的说明：

程度	无：无需关注。 信息：无需立即关注。应在方便时检查。 警告：已发生潜在危害活动，需适度关注。应在方便时予以处理。 严重：已发生潜在危害活动，需高度关注。应立即处理。
策略名称	生成事件的策略的名称。该名称是指向策略列表的链接。
源资产	发起事件的资产的名称。此字段是指向资产清单的链接。
源地址	发起事件的资产的 IP 或 MAC。
目标资产	受事件影响的资产的名称。此字段是指向资产清单的链接。
目标地址	受事件影响的资产的 IP 或 MAC。
协议	协议会在相关时显示用于生成此事件的对话的协议。
事件类别	显示事件的一般类别。 **注意**：所有类型的事件会在"所有事件"屏幕上显示。每个特定的"事件"屏幕仅显示指定类别的事件。 以下是事件类别的简要说明（有关更加详细的说明，请参阅"策略类别和子类别"）： • 配置事件：这包括两个子类别 • 控制器验证事件：这些策略检测网络中的控制器发生的变更。 • 控制器活动事件：活动策略与网络中发生的活动（即在网络中的资产之间实施的"命令"）相关。 • SCADA 事件：识别控制器数据平面变更的策略。• 网络威胁事件：这些策略识别表示入侵威胁的网络流量。

	• 网络事件:这些策略与网络中的资产以及资产之间的通信流有关。
状态	显示事件是否已被标记为“已解决”。
解决者	对于已解决的事件,显示哪个用户将该事件标记为“已解决”。
解决日期	对于已解决的事件,显示何时将该事件标记为“已解决”。
注释	显示解决事件时添加的任何注释。

查看事件详细信息

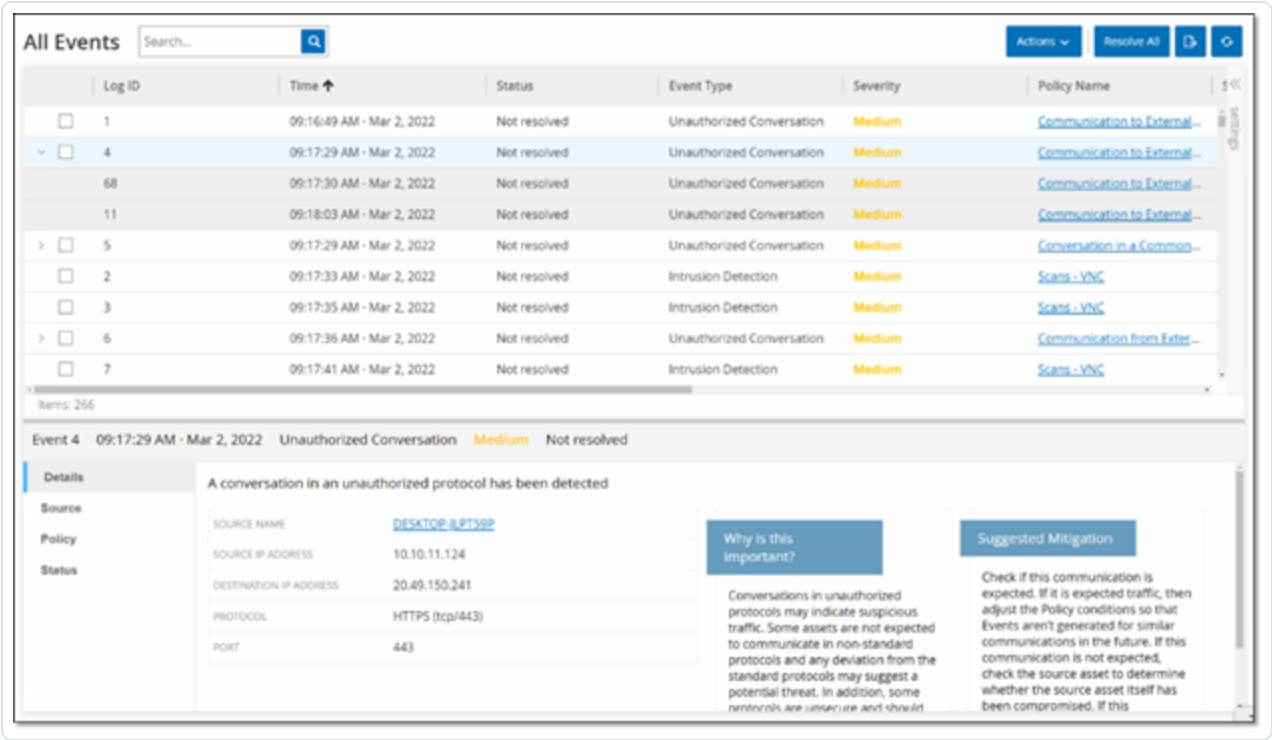


"事件"屏幕底部显示有关所选事件的其他详细信息。该等信息被分成多个选项卡。但系统仅显示与所选事件相关的选项卡。详细信息包括相关实体(源资产、目标资产、策略、组等)的附加信息的链接。

- **标头**:显示有关事件的基本信息的概述。
- **详细信息**:提供事件的简要说明和此类信息如此重要的说明,以及为缓解事件造成的潜在危害应采取的建议措施。此外,它还显示了事件中涉及的源资产和目标资产。
- **规则详细信息**(针对入侵检测事件):显示有关适用于事件的 Suricata 规则的信息。
- **代码**:此选项卡显示与控制器活动相关的信息,例如代码下载和上传、硬件配置和代码删除。它还会显示有关相关代码的详细信息,其中包括特定的代码块、Rung 和标签。代码元素会以树状结构显示,并带有用于展开/最小化所显示详细信息的箭头。
- **源**:显示有关此事件的源资产的详细信息。
- **目标**:显示有关此事件的目标资产的详细信息。
- **受影响的资产**:显示有关受此事件影响的资产的详细信息。
- **已扫描的端口**(适用于端口扫描事件):显示已扫描的端口。
- **已扫描的地址**(适用于 ARP 扫描事件):显示已扫描的地址。
- **策略**:显示与触发事件的策略有关的详细信息。

- **状态**:显示事件是否已被标记为“已解决”。对于已解决的事件,显示与哪个用户将其标记为“已解决”以及何时解决有关的详细信息。

查看事件群集



为了便于监控事件，具有相同特性的多个事件会划分到一个群集中。群集基于事件类型（即共享相同的策略）、源和目标资产，以及事件发生的时间范围。有关配置事件群集的信息，请参阅“事件群集”。

群集事件由日志 ID 旁的箭头指示。要查看群集中的各个事件，请单击记录以展开列表。

解决事件

获得授权的技术人员评估事件并采取必要的措施来解决问题，或者确定无需采取措施之后，应将该事件标记为“**已解决**”。当解决了作为群集一部分的一个事件后，该群集中的所有事件都将被标记为“已解决”。您可以在批处理中选择多个事件并将它们标记为“**已解决**”。也可以同时将所有事件（或特定类别的所有事件）标记为“**已解决**”。

解决单独事件

若要将特定事件标记为"已解决",请执行以下操作:

1. 在相关"**事件**"页面(配置事件、SCADA 事件、网络威胁或网络事件)中,选中要标记为"**已解决**"的一个或多个事件旁边的复选框。
2. 在标题栏中单击"**操作**"。

   此时会出现一个下拉菜单。

   > **注意**:即使将多个事件标记为"**已解决**",也必须单击"**解决**"按钮(而不是"**全部解决**"按钮)才能解决所有所选事件。"**全部解决**"按钮用于解决所有事件,甚至包括未选择的事件。
3. 选择"**解决**"。

   此时将出现"**解决事件**"窗口。

4. 在"**注释**"框中,可以添加说明为解决问题而采取的缓解措施的注释。
5. 单击"**解决**"。

   所选事件的状态标记为"**已解决**"。

解决所有事件

根据当前应用的筛选条件，“**全部解决**”操作将应用于当前页面上的所有事件。例如，如果“**配置事件**”页面打开，则“**全部解决**”将解决“配置事件”，但不会解决“SCADA 事件”等其他事件。对于群集事件，群集中的所有事件都会标记为“已解决”。

若要将所有事件标记为“已解决”，请执行以下操作：

1. 在相关“**事件**”页面（“配置事件”、“SCADA 事件”、“网络威胁”或“网络事件”）的标题栏中，单击“**全部解决**”。

   “**解决所有事件**”窗口会显示要解决的事件数量。

2. （可选）在“**注释**”框中，可以添加关于正在解析的事件组的注释。

3. 单击“**解决**”。

   OT Security 会显示警告消息。

4. 单击“**解决**”。

   OT Security 会将当前显示的所有事件都标记为“**已解决**”。

创建策略排除项

如果某项策略针对不造成安全威胁的特定情况生成事件，则可以从该策略中排除这些情况（即停止针对这些特定情况生成事件）。例如，如果策略检测到 Workday 使用期间发生的控制器状态变更，但确定特定控制器的状态在这些时间段内出现变更是正常的，则可以从策略中排除该控制器。

您可以根据策略生成的事件通过“**事件**”页面创建排除项。您可以指定要从策略中排除的特定事件的条件。

如果要在后期恢复为指定的条件生成事件，则可以删除排除项，请参阅“策略”。

若要创建策略排除项，请执行以下操作：

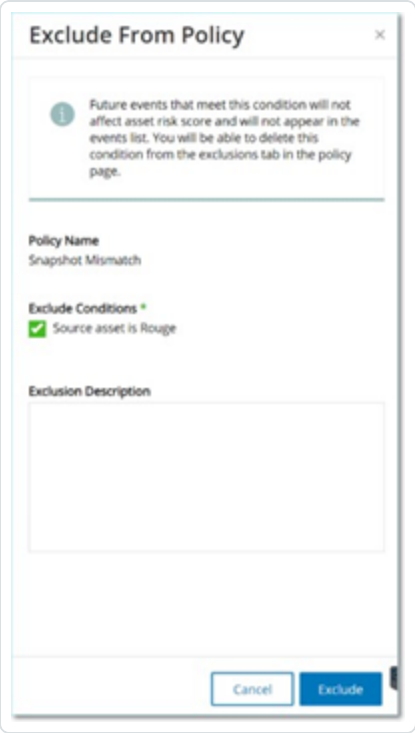
1. 在相关“**事件**”页面（“配置事件”、“SCADA 事件”、“网络威胁”或“网络事件”）中，选择要为其创建排除项的事件。
2. 在标题栏中，单击“**操作**”或右键单击该事件。

   此时会出现“**操作**”菜单。
3. 单击“**从策略中排除**”。

   此时会打开“**从策略中排除**”窗口。
4. 在“**排除条件**”部分中，默认情况下会选择所有条件。

   这会导致具有任何指定条件的事件被排除在策略之外。您可以取消选中要继续为其生成事件的每个条件旁的复选框。

   > **注意**：举例来说，在下面显示的窗口中，如果要从此策略中排除指定的源和目标资产及 IP，但要继续将此策略应用到网络中其他资产之间的 UDP 对话，则应取消选择“协议即 UDP”。



注意:可排除的条件因策略类型而异,具体请参阅下表。

5. 在"**排除项说明**"框中,可以添加关于排除项的注释(可选)。
6. 单击"**排除**"。

   OT Security 会创建排除项。

   下表显示了可用于每种事件类型的排除条件。

策略类别	事件类型	排除条件
控制器活动	配置事件(活动)	• 源资产 • 源 IP • 目标资产 • 目标 IP
控制器验证	密钥状态变更	源资产
	控制器状态变更	源资产

	固件版本变更	源资产
	模块未出现	源资产
	快照不匹配	源资产
网络	资产未出现	源资产
	USB 配置变更	• 源资产 • USB 设备 ID
	IP 冲突	• MAC 地址 • IP 地址
	网络基线偏差	• 源资产 • 源 IP • 目标资产 • 目标 IP • 协议
	已打开的端口	• 源资产 • 源 IP • 端口
	RDP 连接	• 源资产 • 源 IP • 目标资产 • 目标 IP
	未经授权的对话	• 源资产 • 源 IP • 目标资产

		• 目标 IP • 协议
	FTP 登录(失败和成功)	• 源资产 • 源 IP • 目标资产 • 目标 IP
	Telnet 登录(尝试、失败和成功)	• 源资产 • 源 IP • 目标资产 • 目标 IP
网络威胁	入侵检测	• 源资产 • 源 IP • 目标资产 • 目标 IP • SID
	ARP 扫描	• 源资产 • 源 IP
	端口扫描	• 源资产 • 源 IP
SCADA	Modbus 非法数据地址	• 源资产 • 源 IP • 目标资产 • 目标 IP

	Modbus 非法数据值	• 源资产 • 源 IP • 目标资产 • 目标 IP
	Modbus 非法函数	• 源资产 • 源 IP • 目标资产 • 目标 IP
	未经授权的写入	• 源资产 • 目标资产 • 标签名称
	IEC60870-5-104 StartDT IEC60870-5-104 StopDT	• 源资产 • 源 IP • 目标资产 • 目标 IP
	基于 IEC60870-5-104 函数代码的事件	• 源资产 • 源 IP • 目标资产 • 目标 IP • COT
	DNP3 事件	• 源资产 • 源 IP • 目标资产

		• 目标 IP • 源 DNP3 地址 • 目标 DNP3 地址

下载各个捕获文件

OT Security 存储与网络中每个事件关联的数据包捕获数据。将数据存储为可使用网络协议分析工具(例如 Wireshark 等) 下载和分析的 PCAP 文件。您也可以下载整个网络的 PCAP 文件，请参阅“网络”。

注意：PCAP 文件仅在激活数据包捕获功能时可用。您可通过“**本地设置**”>“**系统配置**”>“**数据包捕获**”来激活数据包捕获功能，详情请参阅“数据包捕获”。PCAP 文件仅适用于与网络活动相关的事件，例如控制器活动、网络威胁、SCADA 事件和部分类型的网络事件。

下载 PCAP 文件

若要下载 PCAP 文件，请执行以下操作：

1. 在“**事件**”页面中，选中要下载其 PCAP 文件的事件旁的复选框。
2. 在标题栏中单击“**操作**”。

   此时会出现“**操作**”菜单。
3. 选择“**下载捕获文件**”。

   将压缩的 PCAP 文件下载到本地计算机。

创建 FortiGate 策略

FortiGate 集成允许使用特定的 OT Security 事件，在 FortiGate 新一代防火墙中创建防火墙策略/规则。支持此功能（受支持的事件）的事件类型为基线偏差、未经授权的对话、入侵检测和 RDP 连接（未经授权且未经身份验证）。FortiGate 策略设置为自动应用到 OT Security 事件中涉及的源资产和目标资产。默认情况下，该策略会导致 FortiGate 拒绝（即阻断）指定类型的流量。FortiGate 管理员可以调整 FortiGate 应用程序中的策略设置。

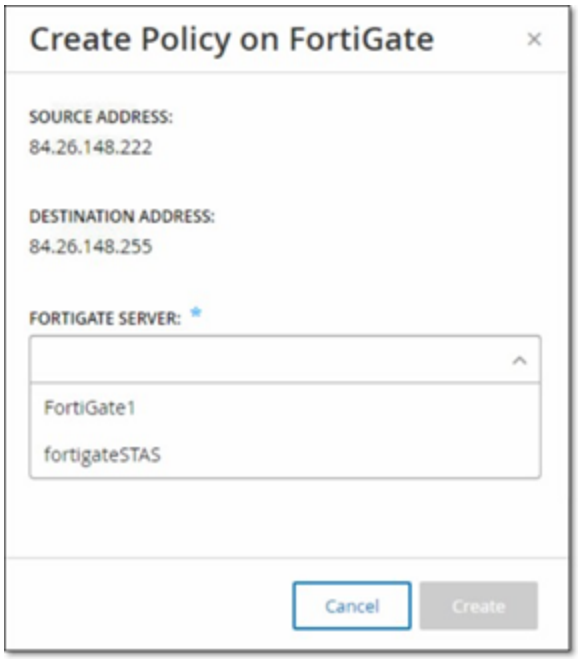
在推荐 FortiGate 策略之前，需要设置 FortiGate 防火墙服务器与 OT Security 的集成。请参阅“FortiGate 防火墙”。

若要推荐 FortiGate 策略，请执行以下操作：

1. 在相关“**事件**”页面（“配置事件”、“SCADA 事件”、“网络威胁”或“网络事件”）中，选择要为其创建 FortiGate 策略的事件。
2. 在标题栏中，单击“**操作**”或右键单击该事件。

   此时会出现一个下拉菜单。
3. 选择“**创建 FortiGate 策略**”。

   FortiGate 面板上的“**创建策略**”打开，其中已填写 OT Security 事件中涉及的资产的“**源地址**”和“**目标地址**”。
4. 在“**FortiGate 服务器**”下拉框中，选择所需的服务器。



5. 点击“**创建**”。

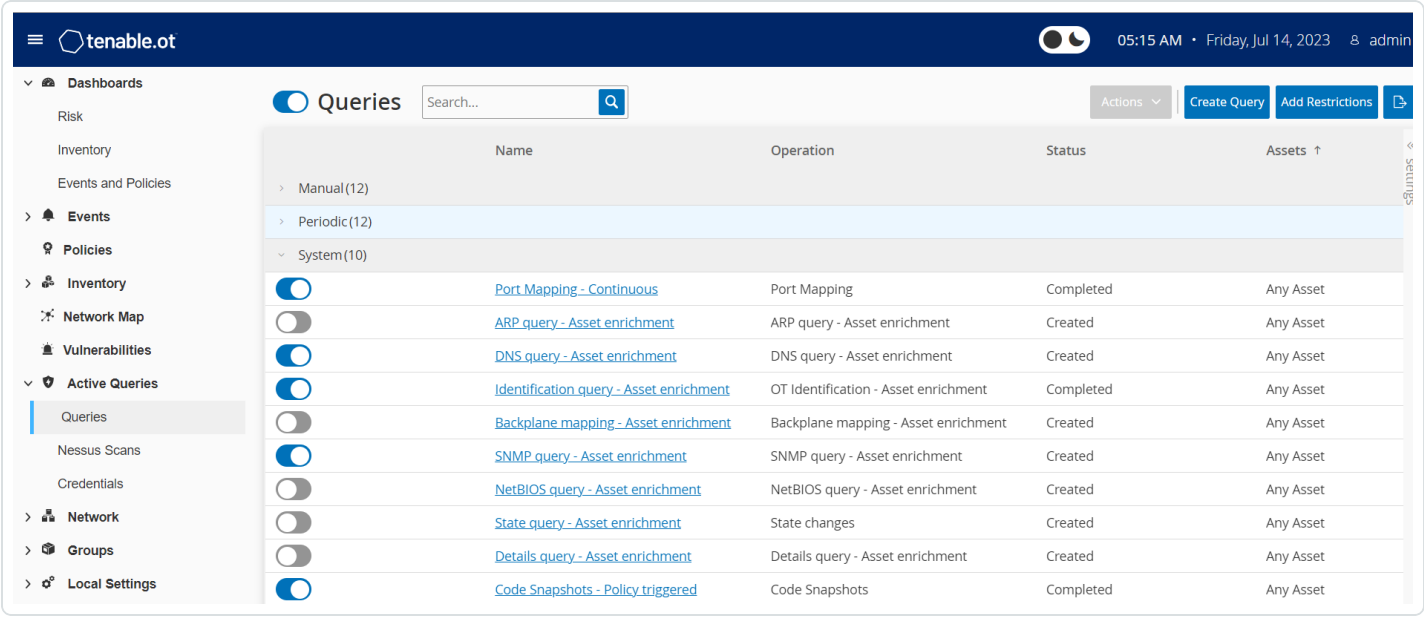
   策略已在 FortiGate 中创建且面板关闭。可以在 FortiGate 应用程序中查看新策略。FortiGate 管理员可根据需要调整设置。

主动查询

OT Security **查询**窗口方便您配置和激活查询功能。有关查询技术的一般说明，请参阅“OT Security 技术”。作为初始设置的一部分，Tenable 建议激活所有查询功能。您可以随时激活/停用任何查询功能，还可以调整查询执行时间和方式的设置。

除定期运行的自动查询之外，您还可以通过单击查询旁的切换按钮来按需启动查询。

注意：关闭查询可能导致资产保持无法识别的状态。OT Security 通过被动监控和主动查询跟踪设备。



您可以通过"**主动查询**">"**查询**"页面激活和配置查询。系统提供三个以精细方式控制主动查询的选项:"**手动**"、"**定期**"和"**系统**"。

手动:在使用单个资产的"**重新同步**"选项查看该资产时,此选项可用于控制可执行的查询。手动查询允许您在查看单个受监控资产时,控制特定查询类型的产品功能。启用重新同步选项后,您可以在查看资产时执行这些查询。有关"**重新同步**"选项的更多信息,请参阅"执行重新同步"。

定期:这是在您设定的固定时间间隔内运行的查询。启用后,查询将根据您在此页面上"**重复**"列中指定的计划执行。您可以右键点击要运行的定期查询并选择"**立即运行**",从而按需运行所有查询。这样做不会影响为下一个查询设置的计划或时间。您手动创建的所有查询都具有周期设置。

系统:OT Security 根据特定标准或条件自动处理的查询。例如,每当 Tenable 首次被动或主动观察到一台设备时,就会发生基于资产扩充的查询。借助资产扩充,OT Security 会在设备出现在网络上后立即对设备进行指纹采样和标识。受策略配置控制,资产扩充功能还可以决定在基于控制器的事件发生时是否启用**策略触发快照**。

> **注意**:如果您使用资产扩充功能,请确保启用这些查询:
>
> - 端口映射 – 持续
> - 识别查询 – 资产扩充

"查询"表格显示以下信息:

列	描述
启用或禁用切换	点击查询名称旁边的切换开关以启用或禁用查询。
名称	查询的名称。
操作	查询类型:“发现”、“定期”或“系统”查询。
状态	查询的状态:“**已创建**”、“**进行中**”、“**准备中**”、“**已完成**”和“**失败**”。
资产	此查询必须轮询的资产组。 **注意**:您可以构建自己的资产组,以在所配置的查询中使用。

创建查询

您可以为不同的项目和功能创建查询，以控制运行哪个查询以及何时运行。

例如，您可以在以下情况下配置自定义查询：

- 工厂不同部分的维护时间不同。
- 不同资产的项目和重要性不同。
- OT 功能和 IT 功能的查询不同。

若要创建查询，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**查询**”窗口。

2. 点击“**创建查询**”。

   此时会出现“**创建查询**”面板。

3. 从下列一个选项中选择所需的查询类型：

   - **发现**：在 OT Security 监控的网络中检测实时资产的查询。
     - **资产发现**利用互联网控制消息协议 (ICMP) 或 ping 来检测实时和响应 IP 地址。
     - **活动资产跟踪**会定期尝试对已知的、受监控的资产进行 ping 操作，以确保资产仍然正常运行且可用。
     - **控制器发现**会向网络发送一组多播数据包，以促使控制器或 ICS 设备直接向 OT Security 回复信息。
   - **IT**：用于从 OT Security 观察到的受监控 IT 类型资产中获取更多数据点的查询。除 NetBIOS 外，这些 IT 类型的查询都需要凭据。
     - **NetBIOS 查询**尝试发现在 OT Security 传感器或 OT Security 本身的广播范围中监听 NetBIOS 的任何设备。此类查询适用于识别附近的 Windows 设备。

- **SNMP 查询**使用 SNMP v2 或 SNMP v3 凭据请求支持 SNMP 的网络基础架构或联网设备，以获取其识别详细信息。OT Security 查询 SNMP 系统描述和其他参数，以帮助添加资产上下文并协助进行指纹识别。
- **WMI 详细信息查询**从基于 Windows 的系统中提取各种重要数据点。这要求被查询系统的 Windows 帐户（本地或域）具备足够的权限来轮询 Windows Management Instrumentation (WMI) 服务。
- **WMI USB 状态**查询确定可移动媒体（如 USB 驱动器或移动硬盘驱动器）是否连接到 Windows 设备，例如工程工作站或服务器。此查询与“**Windows 计算机上 USB 配置变更**”策略密切相关，因为其是此策略正常工作的先决条件。

- **OT**：旨在使用专有协议安全地轮询控制器和嵌入式设备以获取更多信息的查询。OT Security 执行只读查询以收集设备信息。在某些情况下，OT Security 不只查询设备识别详细信息，而且可以显示信息，例如 PLC 运行状态或连接到背板的其他模块。OT Security 尝试查询正在监听 OT Security 支持的专有协议的设备。如需详细了解自定义查询或使用的协议，请参阅文档。

4. 单击“**下一步**”。

   此时会出现“**查询定义**”面板。

5. 在“**名称**”框中，输入查询的名称。
6. 在“**描述**”框中，输入对查询的描述。
7. 在“**资产**”下拉框中，选择资产。

   注意：您也可以使用“**搜索**”框搜索特定资产。

8. 在“**重复频率**”部分，输入一个数字，然后从下拉框中选择“**天**”或“**周**”。对于某些查询，您还可以设置“**分钟**”和“**小时**”。

   如果选择“**周**”，请指明在一周中的哪天运行查询。

9. 在“**精确时间**”框中，单击时钟图标并选择时间或手动输入时间，即可设置要运行查询的时间（采用 HH:MM:SS 的格式）。
10. 点击“**查询状态**”切换开关以启用查询。
11. （仅适用于资产发现）在“**IP 范围**”框中，输入资产的 IP 地址。

12. (仅适用于发现查询)在"**要同时轮询的资产数**"下拉框中,选择资产数量。可用的选项包括:"10 项资产"、"20 项资产"或"30 项资产"。

13. (仅适用于发现查询)在"**发现查询之间的时间间隔**"下拉框中,选择发现查询之间的时间间隔。可用的选项包括:"1 秒"、"2 秒"或"3 秒"。

添加限制

您可以阻止查询在特定资产上运行，例如 IP 范围、OT 服务器、平板电脑、医疗设备、域控制器等。

若要添加限制，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**查询**”窗口。

2. 在“**已屏蔽的资产**”下拉框中，选择要需要屏蔽的资产。

   > **注意**：您可以使用搜索框搜索特定资产。

3. 在“**已限制的客户端**”下拉框中，选择所需的客户端。

4. 在“**限制买卖期**”下拉框中，选择您希望屏蔽资产的时长。可用的选项包括：“**无**”、“**工作时间**”。

5. 单击“**保存**”。

   OT Security 对特定客户端和资产应用限制。

查看查询

若要查看查询的详细信息，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**查询**”窗口。

2. 在要查看的查询所在的行中，执行下列操作之一：

   - 右键点击查询并选择“**查看**”。
   - 选择查询，然后从“**操作**”菜单中选择“**查看**”。

   此时会出现一个窗口，其中包含查询的详细信息。

编辑查询

若要编辑查询详细信息，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**查询**”窗口。

2. 从查询列表中，选择要编辑的查询并执行下列操作之一：

   - 右键点击查询并选择“**编辑**”。
   - 选择查询，然后从“**操作**”菜单中选择“**编辑**”。

   此时会出现“**编辑查询**”面板。

   > **注意**：您也可以从“**查询详细信息**”页面编辑查询。

3. 根据需要修改查询。

4. 单击“**保存**”。

复制查询

注意:您只能为**定期**查询创建重复查询。

1. 转至"**主动查询**">"**查询**"。

   此时会出现"**查询**"窗口。

2. 从查询列表中,选择要创建副本的查询并执行下列操作之一:

   - 右键点击查询并选择"**复制**"。
   - 选择查询,然后从"**操作**"菜单中选择"**复制**"。

   此时会出现"**复制查询**"面板,其中包含查询的详细信息。

   注意:您也可以从"查询详细信息"页面创建查询的副本。

3. 重命名查询并根据需要修改详细信息。

4. 单击"**保存**"。

   OT Security 将查询保存在查询表中。

运行查询

您可以在需要时运行定期查询。

> **注意**:"**立即运行**"选项仅可用于**定期**查询。

若要运行查询,请执行以下操作:

1. 转至"**主动查询**">"**查询**"。

   此时会出现"**查询**"窗口。

2. 从查询列表中,选择要运行的查询并执行下列操作之一:

   - 右键点击查询并选择"**立即运行**"。
   - 选择查询,然后从"**操作**"菜单中选择"**立即运行**"。

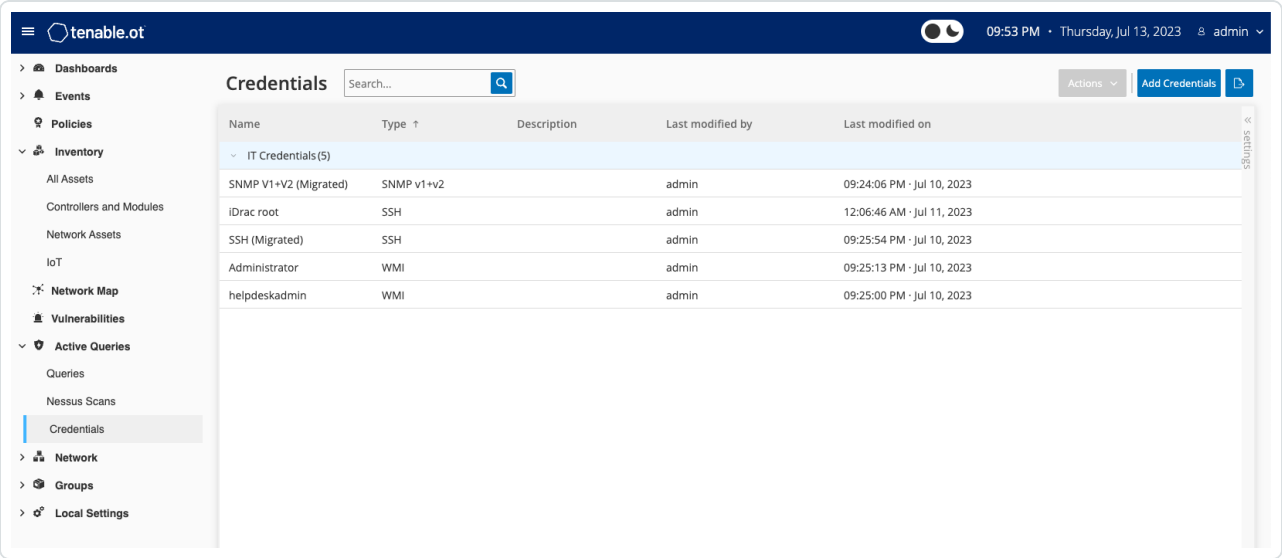
   此时会出现一则要求您确认运行查询的消息。

3. 点击"**确定**"。

   OT Security 会运行所选查询。

凭据

根据需要使用"**凭据**"页面配置设备凭据。在许多情况下，只要您在设备本机网络协议或专有协议中进行通信，该设备就不需要凭据。但是，某些 OT Security 支持的设备可能需要凭据才能执行资产发现。



添加凭据

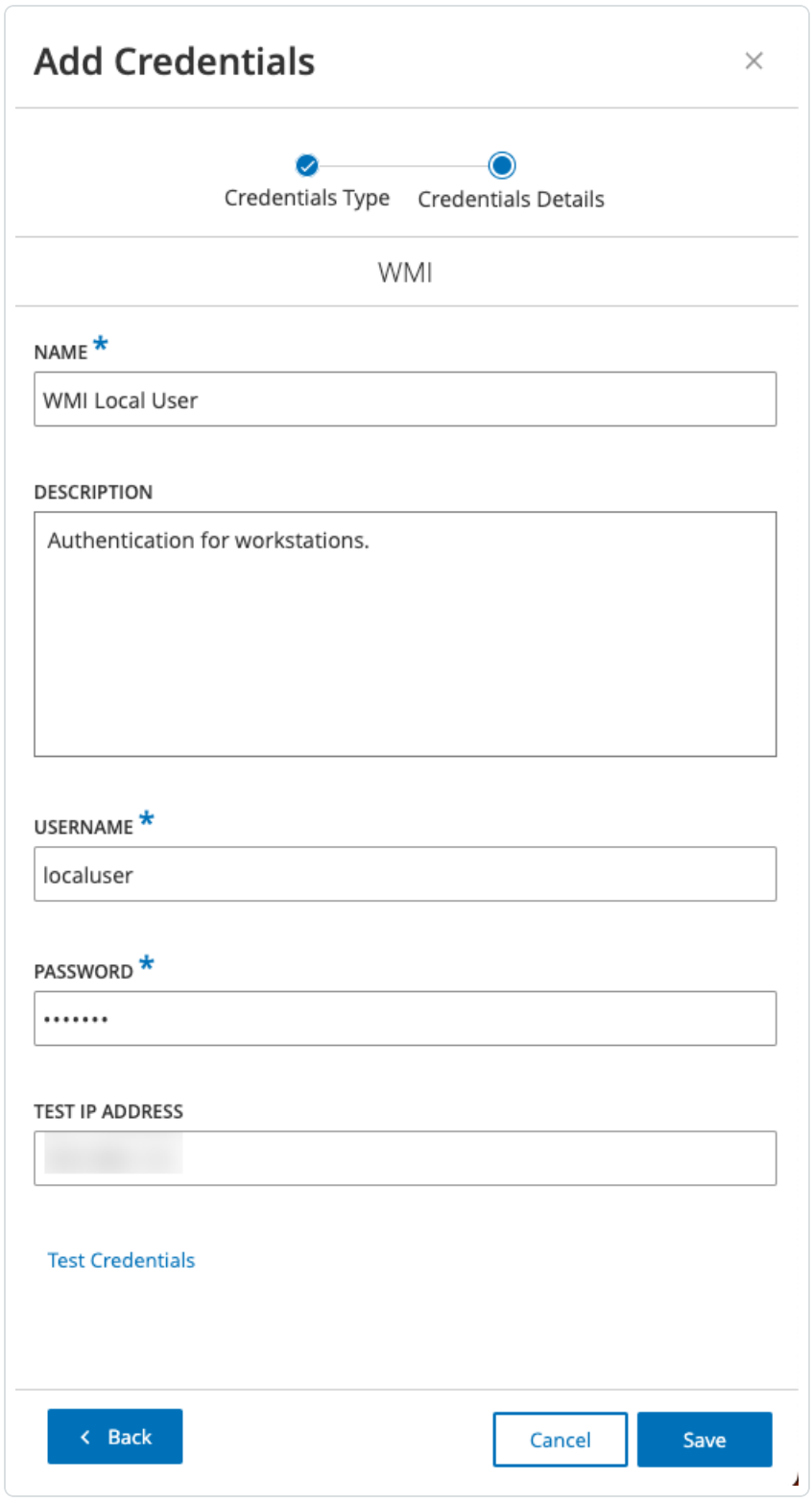
若要添加凭据，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**凭据**”窗口。

2. 点击右上角的“**添加凭据**”。

   此时会出现“**添加凭据**”面板。



3. 点击以选择凭据类型。可用的选项如下：

- ABB RTU 500
- Bachmann
- 概念
- Sel
- SicamA8000
- SIPROTEC 5
- SNMP v1+v2
- SNMP v3
- SSH
- WMI

4. 单击"**下一步**"。

   此时会出现"**凭据详细信息**"面板。

5. 提供以下详细信息:

   - **名称**:凭据的名称。
   - **说明**:对凭据的说明。
   - **用户名**:要使用的用户名。
   - **密码**:凭据的密码。
   - **测试 IP 地址**:用于测试凭据的 IP 地址。

6. 单击"**测试凭据**"以测试凭据是否有效。
7. 单击"**保存**"。

   OT Security 会保存凭据,这些凭据会显示在"**凭据**"页面中。

编辑凭据

您可以编辑凭据详细信息。

若要编辑凭据，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**凭据**”窗口。

2. 请执行下列操作之一：

   - 右键点击所需凭据，然后选择“**编辑**”。
   - 选择所需凭据，然后从“**操作**”菜单中选择“**编辑**”。

   此时会出现“**编辑凭据**”面板。

3. 根据需要修改详细信息。
4. 单击“**保存**”。

删除凭据

您可以删除不再需要的凭据。

如要删除凭据，请执行以下操作：

1. 转至“**主动查询**”>“**查询**”。

   此时会出现“**凭据**”窗口。

2. 请执行下列操作之一：

   - 右键点击所需凭据，然后选择“**删除**”。
   - 选择所需凭据，然后从“**操作**”菜单中选择“**删除**”。

   OT Security 会删除所选凭据。

WMI 帐户

若要启用 OT Security 以执行 Windows Management Instrumentation (WMI) 查询，您可以设置 WMI 帐户。OT Security 依赖 WMI 查询来获取有关 Windows 系统的更多信息。

执行 WMI 查询时，OT Security 依赖与 Tenable Nessus 相同的 WMI 方法。要设置 WMI 帐户进行扫描，请参阅《Tenable Nessus 用户指南》中的"启用 Windows 登录以进行本地和远程审核"部分。

Nessus 插件扫描

Tenable Nessus 插件扫描会根据用户定义的插件列表对 CIDR 和 IP 地址列表中指定的资产启动高级 Nessus 扫描。

OT Security 针对指定 CIDR 内的响应式资产执行扫描。但是，为了保护您的 OT 设备，系统只会扫描给定范围内（非 PLC）的已确认网络资产，而不会扫描"端点"类型的资产。

注意：Tenable Nessus 是最适合在 IT 环境中使用的侵入式工具。建议不要在 OT 设备上使用，因为它可能会干扰该等设备正常运作。

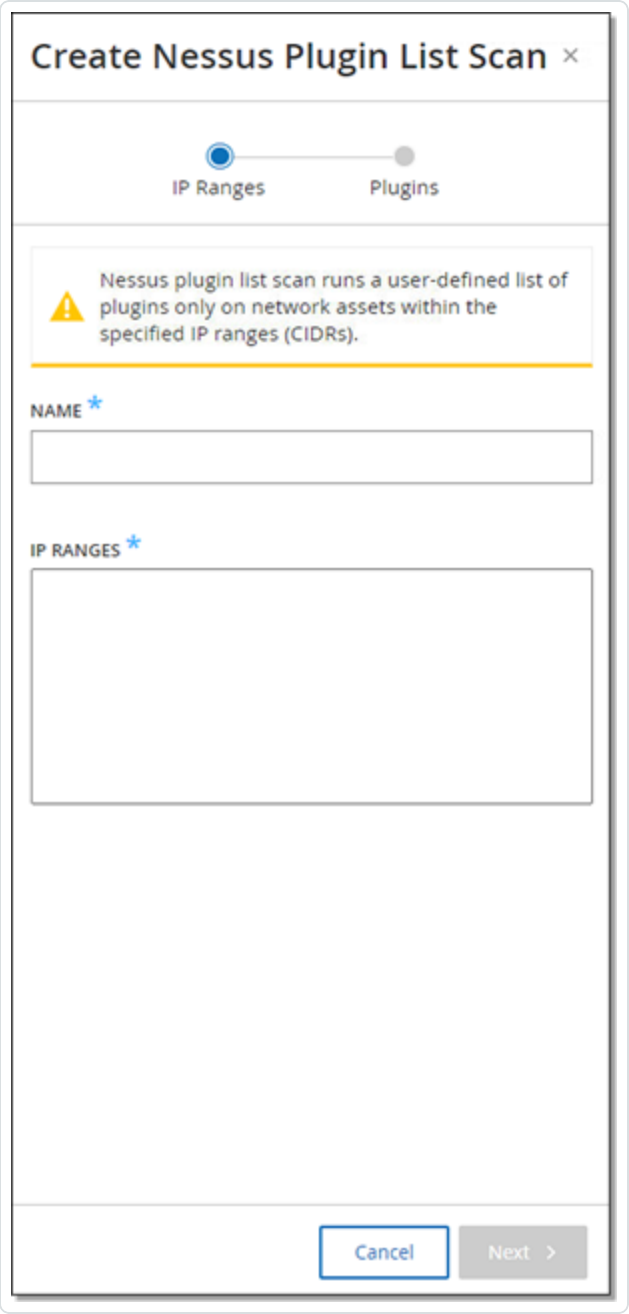
如要对任何一项资产运行基本的 Nessus 扫描，请参阅"资产"。

注意：可对"端点"类型的资产运行基本扫描。

若要创建 Nessus 插件扫描，请执行以下操作：

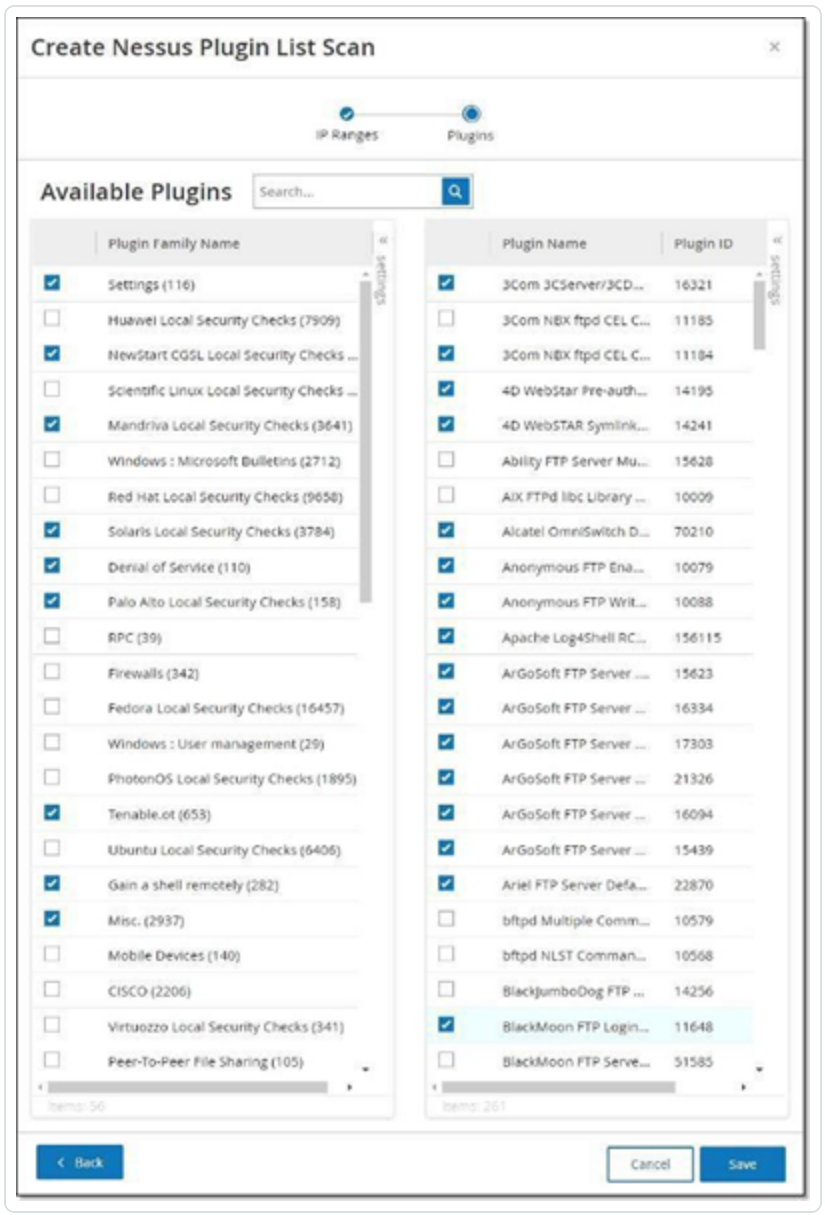
1. 转至"**主动查询**"> "**Nessus 扫描**"。
2. 点击"**创建扫描**"。

   此时会显示"**创建 Nessus 插件列表扫描**"面板。



3. 在“**名称**”框中，为 Nessus 扫描输入一个名称。
4. 在“**IP 范围**”框中，为 IP 或 CIDR 输入范围。
5. 单击“**下一步**”。

   此时会出现“**插件**”窗格。



注意：列出的插件因设备而异。必须使用最新的许可证才能接收新的插件。如要更新许可证，请参阅“许可证”。

6. 根据需要在左列中选择要包含在扫描中的插件系列，并根据需要在右列中取消选择各个插件。

注意：有关 Tenable Nessus 插件系列的更多信息，请参阅 https://zh-cn.tenable.com/plugins/nessus/families。

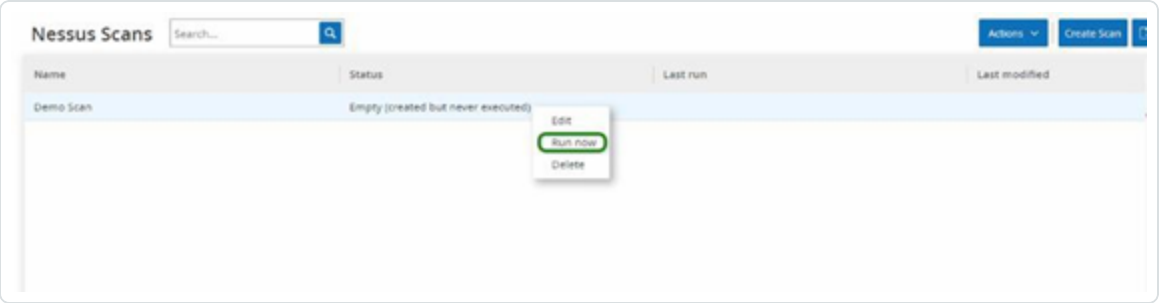
7. 单击“**保存**”。

新的 Nessus 扫描会在“**Nessus 扫描**”屏幕中显示。

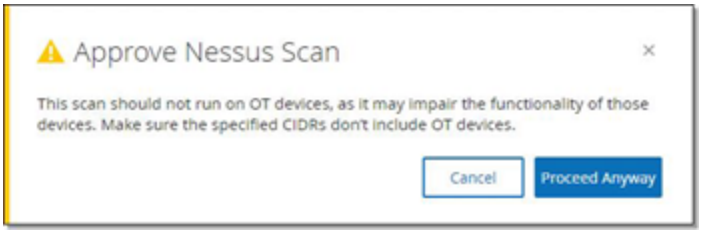
> **注意**：如要编辑或删除现有的 Tenable Nessus 扫描，右键单击所需的扫描行并选择“**编辑**”或“**删除**”。

若要运行 Nessus 插件扫描，请执行以下操作：

1. 在“**Nessus 扫描**”屏幕上，选择所需的扫描行，右键单击并选择“**立即运行**”，或单击“**操作**”>“**立即运行**”。



此时会出现“**批准 Nessus 扫描**”对话框。



2. 如果您知道 OT 设备不在扫描范围内，请单击“**仍然继续**”。

   对话框关闭，扫描已保存。

3. 要运行扫描，再次右键单击扫描行并选择“**立即运行**”。

   随后会再次出现“**批准 Nessus 扫描**”对话框。

4. 单击“**仍然继续**”。

   扫描现在正在运行。扫描可能会暂停/恢复、停止和终止，具体视其当前的状态而定。

网络

OT Security 监控网络中的所有活动并在“**网络**”页面中显示此信息。

OT Security 在三个单独的窗口上显示网络数据。

- **网络汇总**:显示网络活动概览。
- **数据包捕获**:显示系统捕获的 PCAP 文件的列表。
- **对话**:显示在网络中检测到的所有对话的列表,其中包含与对话发生时间、所涉资产等内容相关的详细信息。

网络汇总

“**网络汇总**”屏幕显示汇总网络活动的可视化图表。您可以设置页面显示数据的时间范围。还可以与小组件交互以显示其他详细信息。

该屏幕包括四个小组件：

- **一段时间内的流量和对话**：显示网络中发生的流量（以 GB/MB 为单位）和对话数量的图表。
- **前 5 个来源**：一个条形图，显示发起最多网络活动的 5 个源资产。对于每个源，该图表会显示代表流量的条形图。将光标悬停在图表上时，工具提示中会显示对话数量。
- **前 5 个目标**：一个条形图，显示收到最多网络活动的 5 个目标资产。对于每个目标，该图表会显示代表传入流量的条形图。将光标悬停在图表上时，工具提示中会显示对话数量。
- **协议**：显示网络中使用的通信协议的条形图，相关内容按频率排序。对于每个协议，该图表会显示其使用速率（占总流量的百分比）和流量。

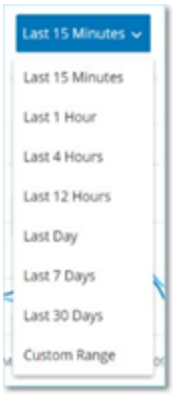
设定时间范围

“**网络**”屏幕上显示的所有数据代表指定时间范围内网络中发生的活动。标题栏显示针对当前数据显示的时间范围。默认时间范围设置为“**过去 15 分钟**”。标题栏会显示所选时间范围的“开始”和“结束”时间。

若要设定时间范围，请执行以下操作：

1. 在标题栏中点击“**时间范围选择**”。默认时间范围设置为“**过去 15 分钟**”。

   下拉框中列出了时间范围选项。

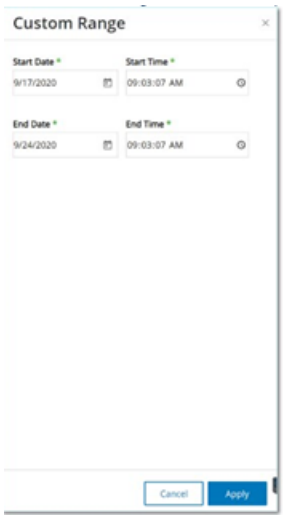
   

2. 使用下列方法之一选择时间范围：

   - 单击所需范围以选择预设时间范围。选项包括“过去 15 分钟”、“过去 1 小时”、“过去 4 小时”、“过去 12 小时”、“过去一天”、“过去 7 天”或“过去 30 天”。
   - 若要设置自定义时间范围，请执行以下操作：

     a. 单击“**自定义**”。

        此时会出现“**自定义范围**”窗口。



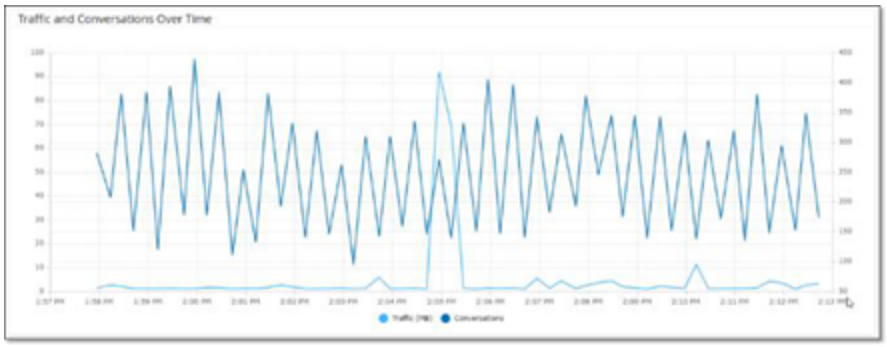
b. 在相应的框中填写“**开始日期**”、“**开始时间**”、“**结束日期**”和“**结束时间**”。

c. 单击“**应用**”。

设置时间范围后，标题栏会在所选时间范围旁显示开始日期/时间和结束日期/时间。OT Security 会刷新屏幕以仅显示所选时间范围内的数据。

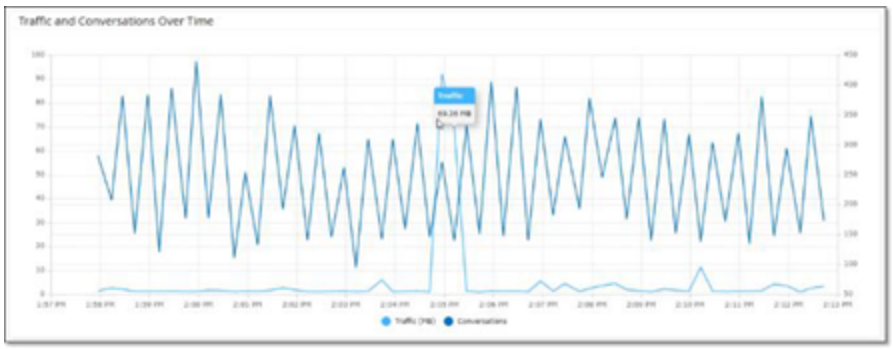
一段时间内的流量和对话

折线图显示了网络中随时间推移发生的流量(以 KB/MB/GB 为单位)和对话数量。图例键显示在图表的顶部。



若要显示特定时间段的数据,请执行以下操作:

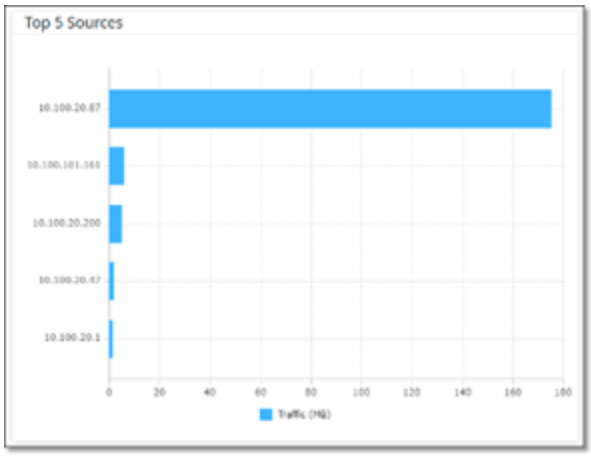
1. 将鼠标悬停在图表上的一个点上即可显示一个弹出窗口,该窗口包含与该时间段内所发生流量和对话相关的特定数据。



注意:时间段长度会根据图表中显示的时间刻度进行调整。例如,对于 15 分钟的时间范围而言,系统会单独显示每分钟的数据,但对于 30 天的时间范围而言,系统则按 6 小时段显示。

前 5 个来源

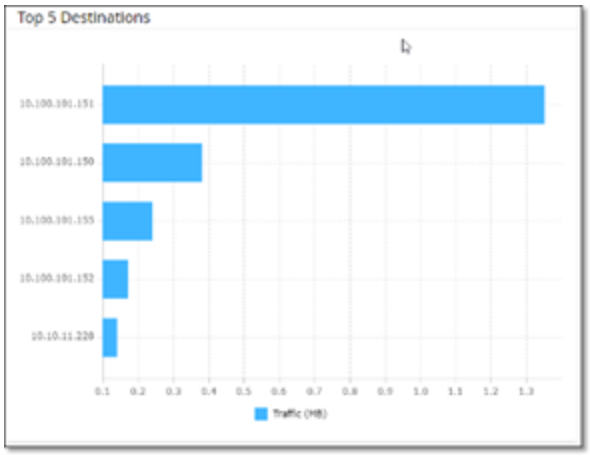
“前 5 个来源”小组件显示在指定时间范围内通过网络发送通信的前 5 个资产中的每个资产的对话数和流量。



可以通过其 IP 地址识别源资产。将鼠标悬停在条形图上会显示从该资产发送的对话数和流量。

前 5 个目标

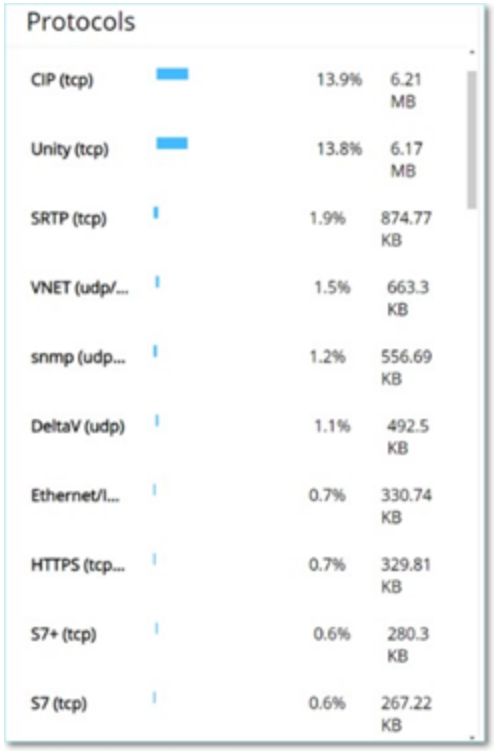
“前 5 个目标”小组件显示在指定时间范围内通过网络收到通信的前 5 个资产中的每个资产的对话数和流量。



可以通过其 IP 地址识别目标资产。将鼠标悬停在条形图上会显示该资产收到的对话数和流量。

协议

“**协议**”小组件显示有关各种网络通信协议在指定时间范围内的使用情况的数据。



协议按最常用(在顶部)到最不使用(在底部)的顺序排列。每个协议都显示以下信息:

- 显示使用率的条形图(完整的条形表示最高使用率,部分条形表示相对于最高使用协议的使用程度)。
- 使用百分比。
- 通信总量。

数据包捕获

系统会存储包含网络中活动的完整网络数据包捕获的文件。将数据存储为可使用网络协议分析工具(例如 Wireshark 等)分析的 PCAP 文件。这支持对关键事件进行深入取证分析。当系统存储容量超过 1.8 TB 时，系统会删除较早的文件。

“**数据包捕获**”屏幕显示系统中的所有数据包捕获文件。“**已完成**”选项卡显示可供下载的每个已完成文件的列表。“正在进行”选项卡显示有关系统中当前正在进行的数据包捕获的详细信息。

“标题栏”显示系统中仍然可用的最旧的捕获文件。它还包含用于下载文件和手动关闭当前数据包捕获的选项。

在文件列表表格中，您可以显示/隐藏列，并对列表进行排序和筛选，同时搜索关键字。有关自定义功能的说明，请参阅“管理控制台用户界面元素”。

注意：您也可以从“**事件**”屏幕下载单个事件的 PCAP 文件，详情请参阅“下载文件”。

数据包捕获参数

数据包捕获列表显示以下详细信息：

参数	描述
开始时间	数据包捕获开始的日期和时间。
结束时间	数据包捕获结束的日期和时间。
状态	捕获的状态。可能的值为“**已完成**”或“**正在进行中**”。
传感器	捕获数据包的 OT Security 传感器。对于 OT Security 设备直接捕获的数据包，其值为“local”。
文件名	文件的名称。
文件大小	文件的大小，以 KB/MB 为单位。

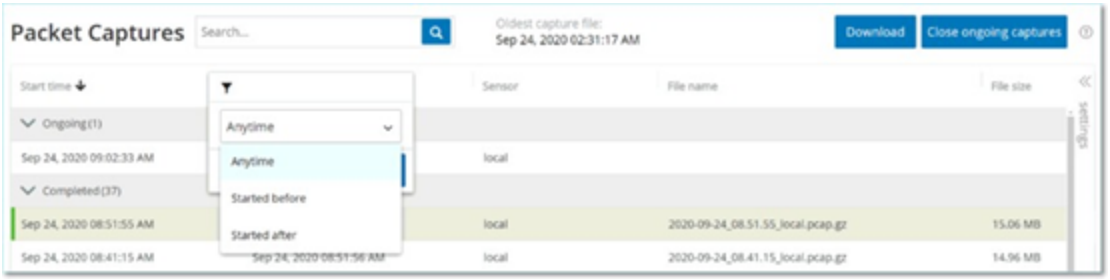
筛选数据包捕获显示

通过输入开始时间和/或结束时间的参数，您可以筛选数据包捕获显示以查找特定 PCAP。

若要筛选数据包捕获，请执行以下操作：

1. 转至“**网络**”>“**数据包捕获**”。
2. 如要按开始时间筛选，请将鼠标悬停在“**开始时间**”上，然后单击出现的 ▽ 图标。

   此时将打开一个下拉菜单。



   按如下所示设置筛选条件：

   a. 选择所需的筛选条件。选项包括“**任何时间**”（**默认**）、“**开始时间早于**”或“**开始时间晚于**”。

   b. 如果选择了“**开始时间早于**”或“**开始时间晚于**”，则将打开一个包含“**日期**”和“**时间**”字段的窗口，以便选择所需的日期和时间。

   c. 单击“**应用**”。

3. 若要按结束时间筛选，请单击“**结束时间**”旁的 ▽ 图标。

   此时将打开一个下拉菜单。按如下所示设置筛选条件：

   a. 选择所需的筛选条件。选项包括“**任何时间**”（**默认**）、“**开始时间早于**”或“**开始时间晚于**”。

   b. 如果选择了“**开始时间早于**”或“**开始时间晚于**”，则将打开一个包含“**日期**”和“**时间**”字段的窗口，以便选择所需的日期和时间。

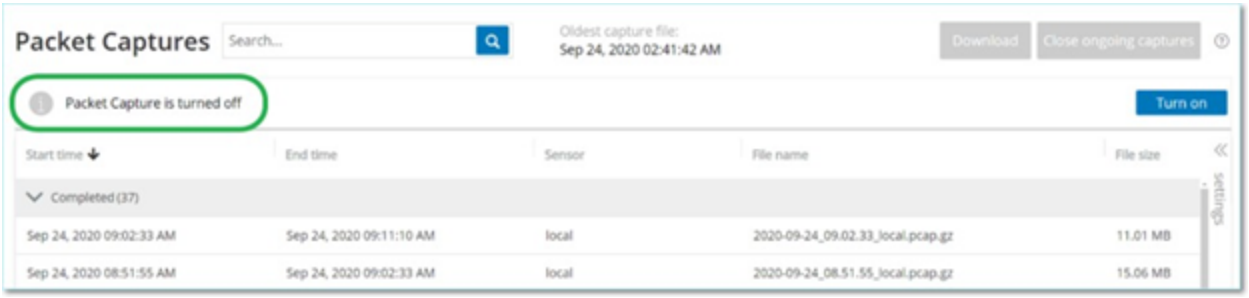
   c. 单击“**应用**”

      OT Security 会应用筛选条件，并且仅显示在所选时间范围内生成的文件。

激活/停用数据包捕获

可在“**本地设置**”>“**系统配置**”>“**设备**”中激活或停用数据包捕获，详情请参阅“数据包捕获”。

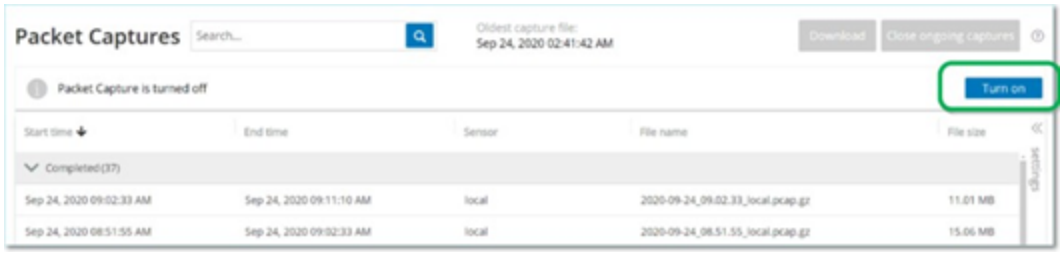
如果“**数据包捕获**”功能已关闭，则“**数据包捕获**”屏幕会显示该功能已关闭的消息通知。



您可以通过“**网络**”>“**数据包捕获**”激活(但不能停用)数据包捕获。

若要从“数据包捕获”屏幕激活数据包捕获，请执行以下操作：

1. 转至“**网络**”>“**数据包捕获**”。
2. 在“**标题**”栏中单击“**打开**”。



系统开始数据包捕获。

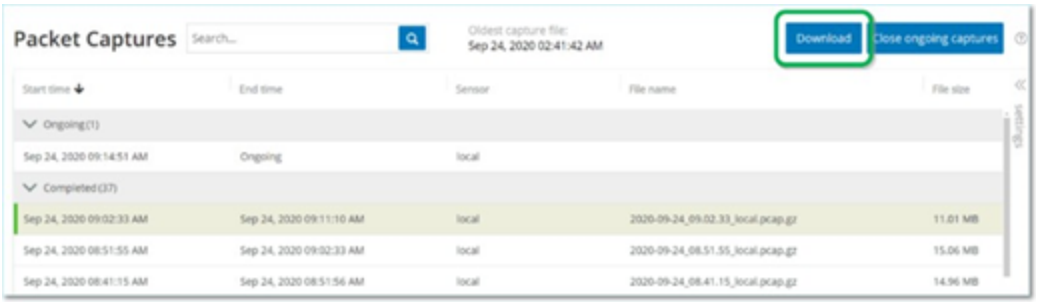
下载文件

可以将任何“**已完成**”的 PCAP 文件下载到本地计算机。随后您可使用网络协议分析工具(例如 Wireshark 等) 分析 PCAP 文件。

仍在进行中的文件捕获尚不可下载。您可以手动关闭正在进行的捕获，以便关闭当前文件并开始捕获新文件的信息。

若要下载已完成的文件，请执行以下操作：

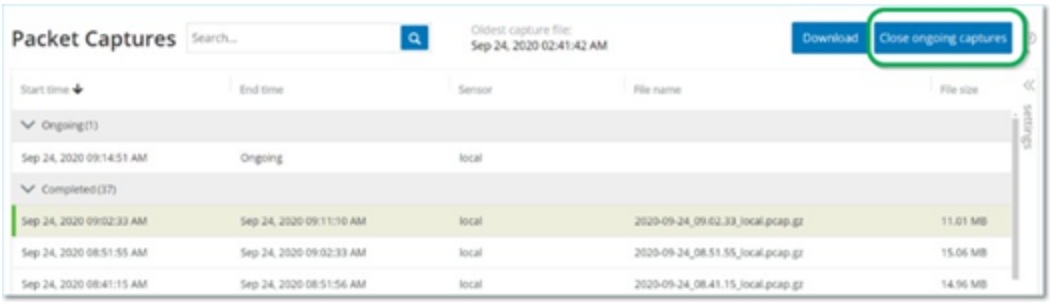
1. 转至“**网络**”>“**数据包捕获**”。
2. 从数据包捕获列表中选择所需文件。
3. 在“**标题**”栏中单击“**下载**”。



OT Security 将压缩的 PCAP 文件下载到本地计算机。

若要手动关闭当前的数据包捕获，请执行以下操作：

1. 转至“**网络**”>“**数据包捕获**”。
2. 在“**标题**”栏中单击“**关闭正在进行的捕获**”。



OT Security 会停止当前捕获，且文件可供下载。系统会自动启动新的数据包捕获。

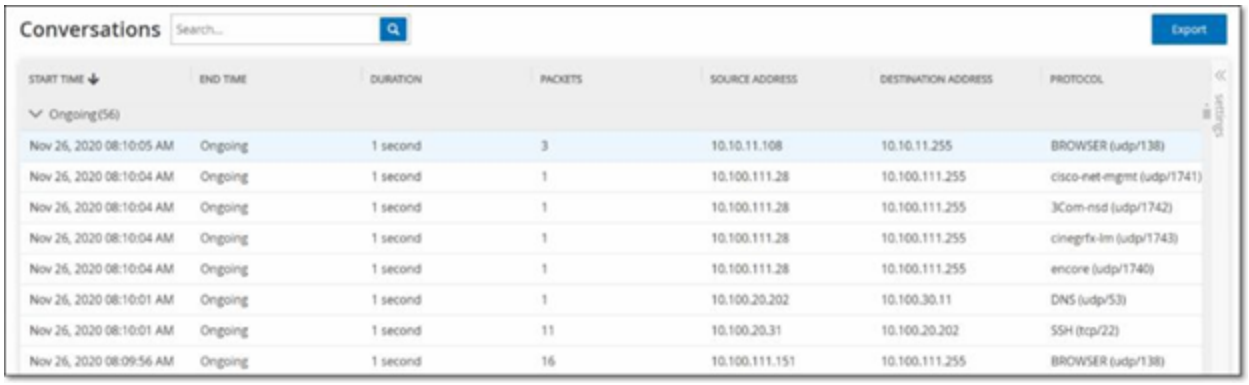
对话

对话是源资产与目标资产之间的网络通信。例如，工程工作站和 PLC 之间的交互，或者两个服务器之间的交互。**对话**屏幕显示当前对话和过去对话的列表，包括有关对话的详细信息。

"**对话**"屏幕具有以下附加功能：

- **搜索**：通过在"**搜索**"框内输入识别信息来搜索特定对话。
- **导出**：单击"**导出**"，将"**对话**"选项卡中的所有数据以 .CSV 文件的格式导出到本地计算机上。

> **注意**：对话表格显示最近的 10,000 个网络对话。

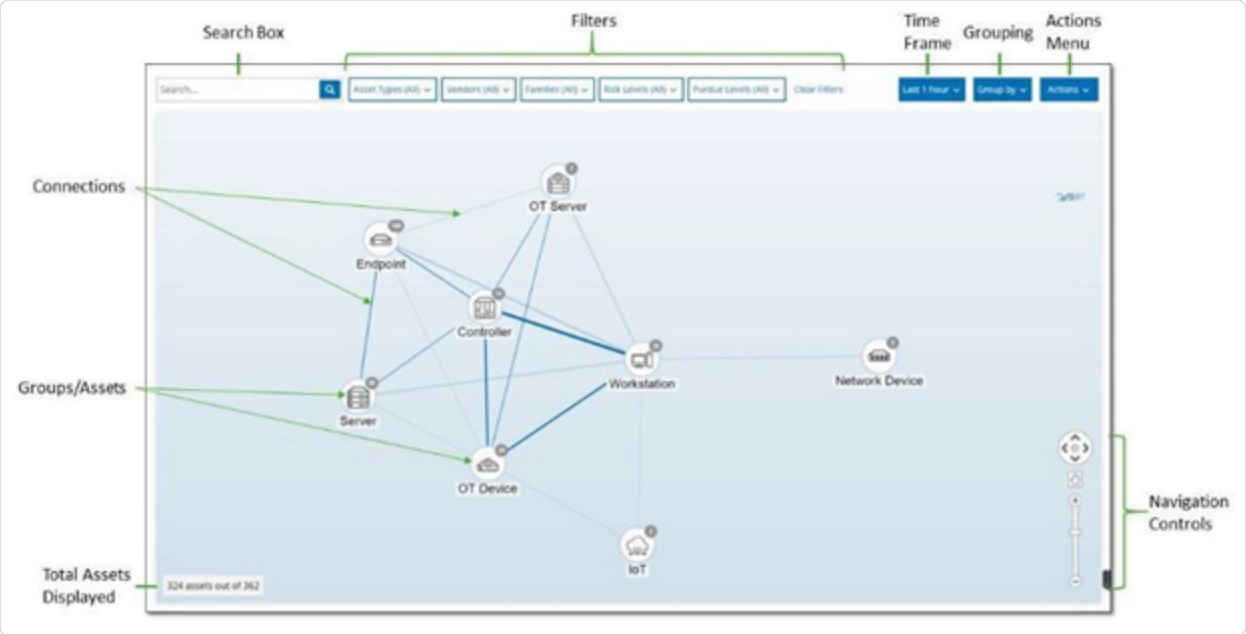


"对话"选项卡显示以下详细信息：

参数	描述
开始时间	对话开始的时间。
结束时间	对话结束的时间。针对仍在进行中的对话显示"**进行中**"。
持续时间	对话正在进行的时间。
数据包	发送的数据包数量。
源地址	发送数据的资产的 IP。
目标地址	接收数据的资产的 IP。
协议	用于通信的协议。

网络映射

“**网络映射**”屏幕提供了 OT Security 的网络检测功能发现的网络资产及其连接随时间推移的可视化表示。网络检测可对通过运营网络执行的所有活动提供深入实时可见性，并且侧重于控制平面工程活动。例如，通过供应商特定的专有协议执行的固件下载或上传、代码更新和配置更改。网络映射可按相关资产组显示资产，也显示单个资产。



“**网络映射**”显示在指定时间范围内 Tenable 发现的所有资产和连接。

“**网络映射**”页面显示以下详细信息：

- **搜索框**：输入搜索文本以搜索显示中的资产。“网络映射”通过突出显示与搜索文本匹配的所有组来显示搜索结果。您可以深入了解每个组以查看相关资产。
- **筛选条件**：可以按一个或多个指定类别筛选映射显示：“**资产类型**”、“**供应商**”、“**系列**”、“**风险级别**”、“**普渡层**”。如要获取有关资产类型的说明，请参阅“资产类型”。
- **时间范围**：“网络映射”显示在指定时间范围内检测到的资产和网络连接。默认时间范围设置为“**过去 30 天**”。在“时间范围”下拉框中，选择其他时间范围。
- **分组**：可以指定在显示中按照哪个类别对资产进行分组。选项包括“**资产类型**”、“**普渡层**”、“**风险级别**”或“**无分组**”。“**折叠所有组**”选项可保留当前分组选项，但折叠所有其他已打开的组。
- **操作**：可以从下拉菜单中选择以下操作：

- **设置为基线**:设置用于检测异常网络活动的基线,详情请参阅"设置网络基线"。
- **自动排列**:自动优化当前所示实体的映射显示。

- **组/资产**:每组资产在映射上以一个图标表示,每种资产类型由不同的图标表示。如"资产类型"中所述。对于组而言,图标顶部的数字表示该组中包含的资产数量。可以进一步显示每个子组的单独图标,直到找到各个资产图标。对于单个资产,资产周围的边框颜色表示其风险级别(红、黄、绿)。

  > **注意**:您可以拖动组和资产并重新排位,以便更好地查看资产及其连接。

- **连接**:资产组和/或单个资产之间的每次通信,基于映射中当前显示的粒度。线条粗细表示通过该连接进行的通信量。
- **显示的资产总数**:根据指定时间范围和资产筛选条件,显示在网络中检测到的资产数量(并在映射中显示)。此数字是相对在网络中检测到的资产总数显示的。
- **导航控件**:您可以使用屏幕控件或标准鼠标控件放大和缩小显示内容,并进行导航以显示所需元素。

资产分组

“**网络映射**”页面可以显示按各种类别分组的资产。该页面会显示资产组之间的连接。您可以单击资产，以深入了解该组中的元素。您还可以同时深入了解多个组。OT Security 包含多个嵌入式组，因此您可通过深入了解来获得包含资产的更精细视图。

以下是可应用到主显示的分组以及该选项的深入了解选项。

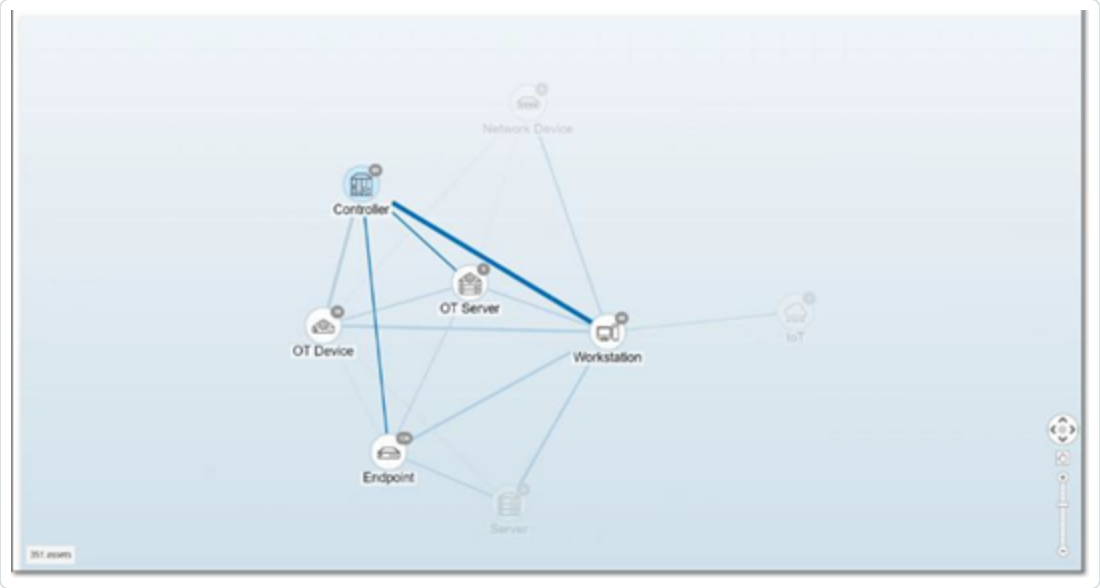
当映射显示按“**资产类型**”（默认）显示分组时，深入了解的层次结构如下：“**资产类型**”>“**供应商**”>“**系列**”>“**单个资产**”。

当映射显示按“**风险级别**”或“**普渡层**”显示分组时，这会在“资产类型”分组之上添加一个额外的级别，因此层次结构为：“**普渡层/风险级别**”>“**资产类型**”>“**供应商**”>“**系列**”>“**单个资产**”。每个级别都由包含的组/资产周围的圆圈表示。

以下示例显示了如何深入了解显示内容：

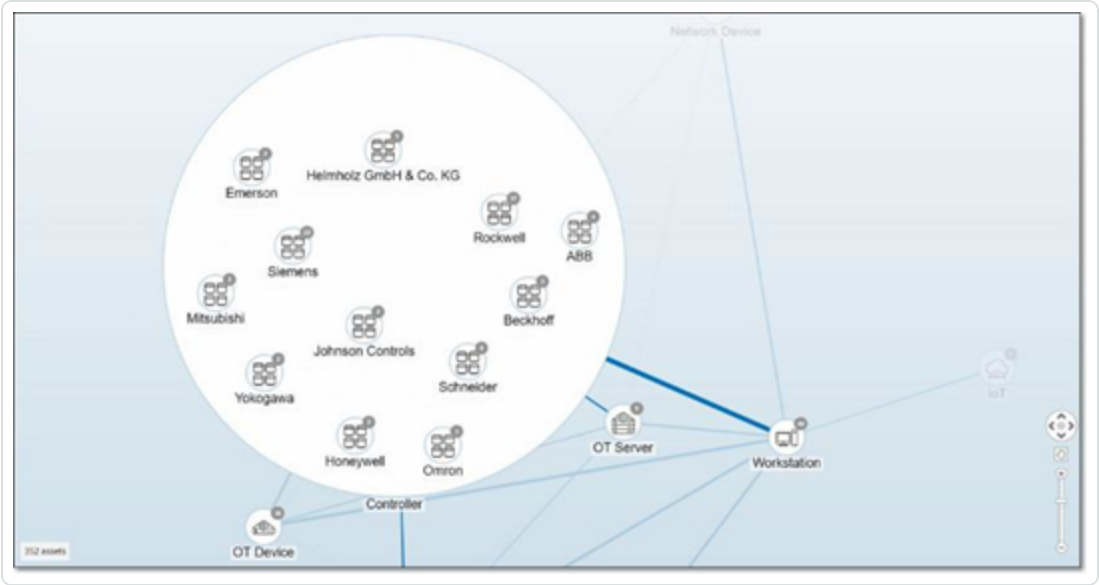
若要深入了解资产类型组，请执行以下操作：

1. 默认情况下，“**网络映射**”屏幕会显示按“资产类型”分组的资产。

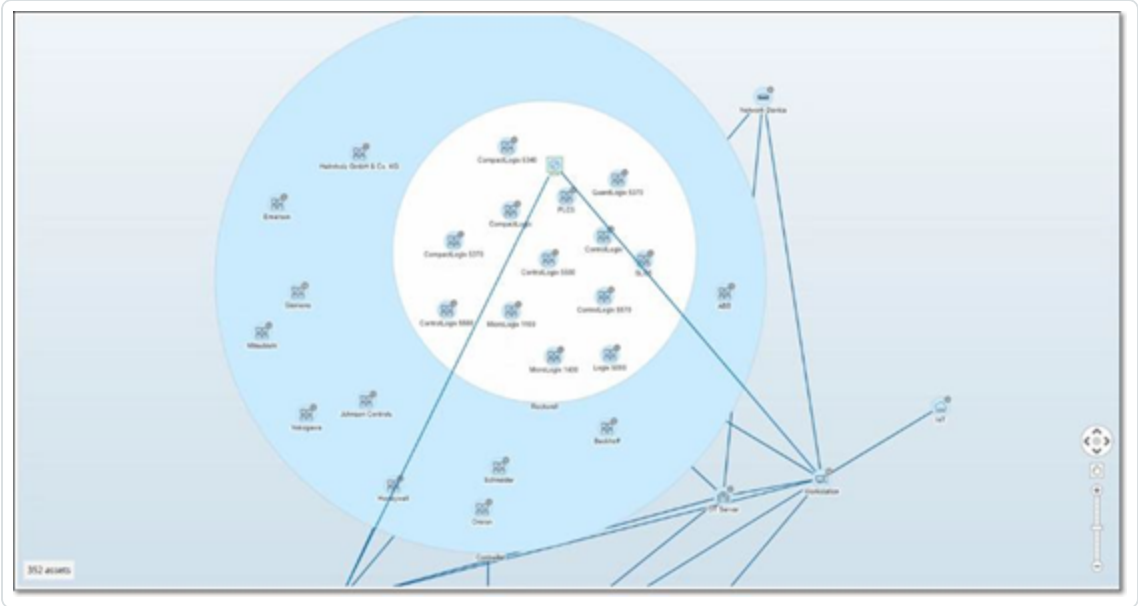


2. 双击您要深入了解的组图标（例如“控制器”）。

   该组已展开，显示该组中的“供应商”组。

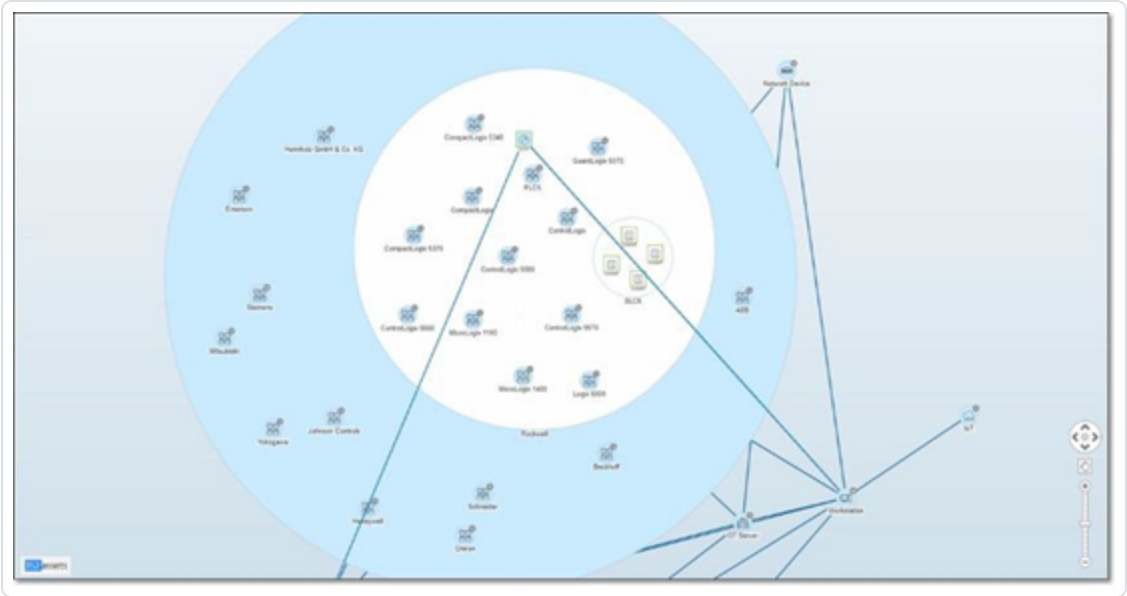


3. 若要深入了解，请单击“供应商”组（例如 Rockwell）。



4. 若要深入了解，请单击“系列”组（例如 SLC5）。

   此时会显示该组内的各个资产。



5. 现在可以单击特定资产以查看该资产及其连接的详细信息，详情请参阅“资产”。

若要折叠显示内容，请执行以下操作：

1. 单击“**分组依据**”。
2. 单击“**折叠所有组**”。

   此时显示内容再次显示顶级组。

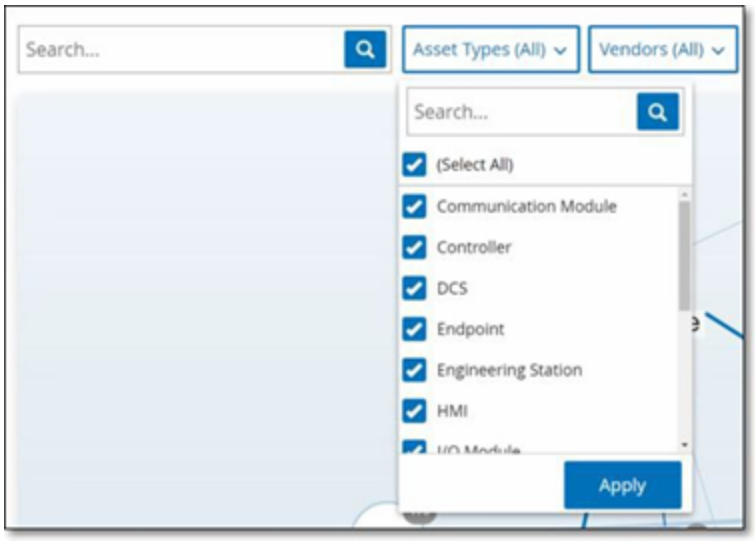
若要删除所有分组，请执行以下操作：

1. 单击“**分组依据**”按钮。
2. 选择“**无分组**”。

   此时映射会显示不含任何分组的所有单一资产。

对映射显示应用筛选条件

您可以按一个或多个指定类别筛选映射显示：“资产类型”、“供应商”、“系列”、“风险级别”、“普渡层”。



若要对映射应用筛选条件，请执行以下操作：

1. 单击所需的筛选条件类别。
2. 选中或取消选中要在显示内容中包括或排除的每个元素的复选框。

   注意：默认情况下，筛选条件包含所有元素。

3. 您可以单击“**全选**”复选框以清除所有值，然后添加所需值。
4. 可以在筛选搜索框中执行搜索，以在筛选窗口中查找特定值。
5. 根据需要，对每个筛选器类别重复此过程。
6. 单击“**应用**”。

   映射仅显示所选元素。

查看资产详细信息

单击特定资产可显示与该资产及其网络活动有关的基本信息，其中包括“风险级别”、“IP 地址”、“资产类型”、“供应商”和“系列”。“映射”显示从所选资产到与之通信的所有其他资产的连接。然后，您可以单击资产名称中的链接，以转到“**资产详细信息**”屏幕，该屏幕显示有关资产的更多详细信息。

设置网络基线

网络基线是指定时间段内网络中的资产之间发生的所有对话的映射。网络基线偏差策略使用网络基线针对网络中的异常对话发出警报，详情请参阅"网络事件类型"。

在基线示例期间未发生交互的资产会针对每个对会触发策略警报(假设对话在指定策略条件范围内)。您必须在"**网络映射**"屏幕上创建初始网络基线，才能创建网络基线偏差策略。您可以通过设置新的网络基线来随时更新网络基线。

若要设置网络基线，请执行以下操作：

1. 在"**网络映射**"屏幕上，使用屏幕顶部的"**时间范围选择**"来选择要包括在网络基线中的对话时间范围。

   此时会显示所选时间范围的"**网络映射**"。

2. 在右上角选择"**操作**">"**设置为基线**"。

   OT Security 会配置新的网络基线，并将其应用于所有网络基线偏差策略。

漏洞

OT Security 可识别影响网络资产的各种威胁。在系统发现新漏洞信息并将其发布到一般公共域时，Tenable 的研究人员会设计程序来支持 Tenable Nessus 对漏洞进行检测。

这些程序名为插件，以 Tenable Nessus 专有脚本语言编写，名为 Tenable Nessus 攻击脚本语言 (NASL)。这些插件会检测网络中的 CVE，以及其他威胁(例如过时的操作系统、易受攻击协议的使用、易受攻击的已打开的端口等)。

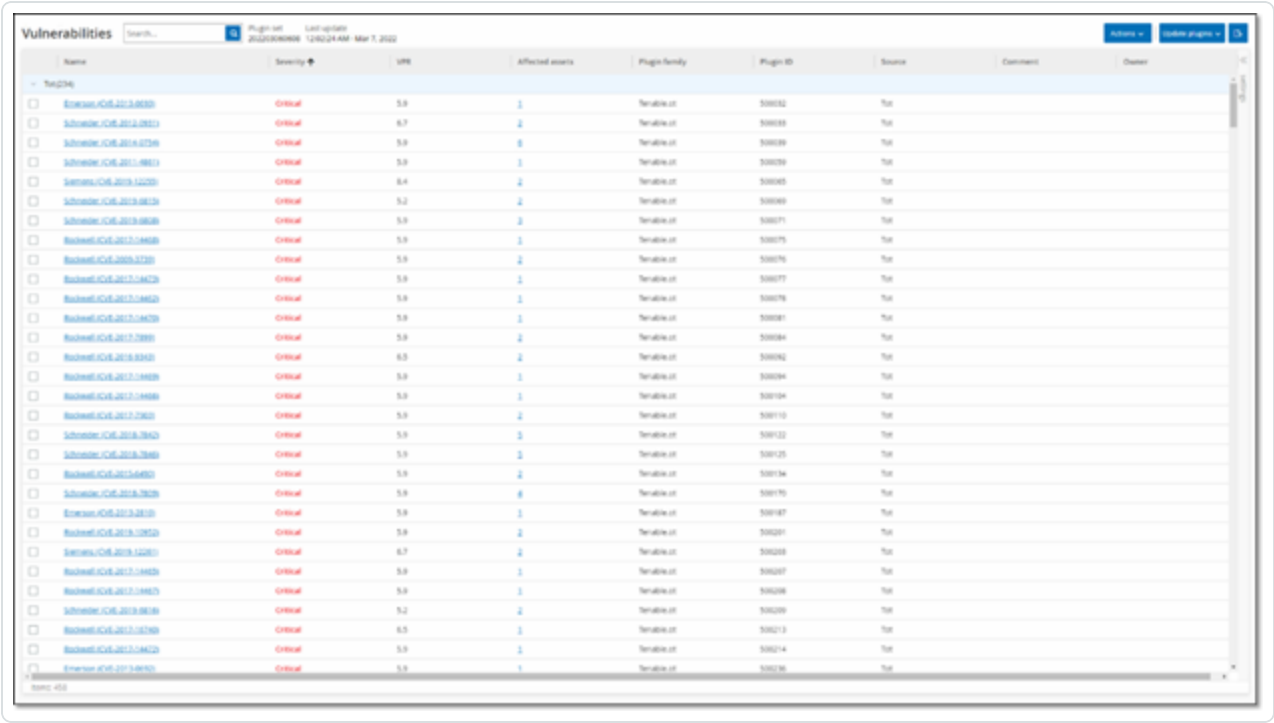
插件包含漏洞信息、一组通用的修复操作，以及用于测试是否存在安全问题的算法。

有关更新插件集的信息，请参阅"环境配置"。

“漏洞”屏幕

“**漏洞**”屏幕显示 Tenable 插件检测到的影响网络和资产的所有漏洞的列表。

可以通过调整要显示的列以及各列的位置来自定义显示设置。有关自定义功能的说明，请参阅“管理控制台用户界面元素”。



“漏洞”页面显示以下详细信息：

参数	描述
名称	漏洞的名称。“名称”是显示完整漏洞列表的链接。
严重程度	此分数表示此插件检测到的威胁的严重程度。可能的值为：“信息”、“低危”、“中危”、“高危”或“严重”。
VPR	漏洞优先级评级 (VPR) 是严重程度级别的动态指标，会根据漏洞的当前利用情况不断更新。作为 Tenable 预测优先级分析的输出，此值由 Tenable 生成，用于评估漏洞所造成的技术影响和威胁。VPR 值的范围为 0.1-10.0，值较高表示被利用的可能性较高。
插件 ID	插件的唯一标识符。

受影响的资产	网络中受此漏洞影响的资产的数量。
插件系列	与此插件关联的系列(组)。
注释	可以添加关于此插件的自由文本注释。

插件详细信息

若要查看插件详细信息，请执行以下操作：

1. 在要查看该漏洞详细信息的漏洞行中，点击漏洞名称。

   此时会出现“漏洞详细信息”窗口。

“漏洞详细信息”窗口显示以下详细信息：

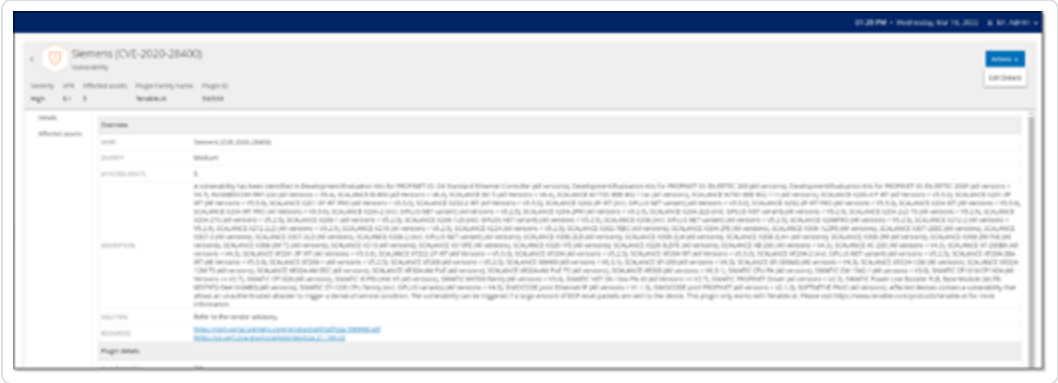
- **标题栏**：显示有关指定漏洞的基本信息。从“**操作**”菜单中选择“**编辑详细信息**”，以编辑漏洞详细信息。请参阅 编辑漏洞详细信息。
- **“详细信息”选项卡**：显示漏洞的完整说明并提供相关资源的链接。
- **“受影响的资产”选项卡**：显示受指定漏洞影响的所有资产的列表。每个列表都包含有关资产的详细信息，以及用于查看该资产的“资产详细信息”窗口的链接。

编辑漏洞详细信息

若要编辑漏洞详细信息，请执行以下操作：

1. 在相关“**漏洞详细信息**”页面，单击右上角的“**操作**”菜单。

   此时会出现“**操作**”菜单。



2. 点击“**编辑详细信息**”。

   此时会出现“**编辑漏洞详细信息”面板**。

3. 在“**注释**”框中输入有关漏洞的注释。
4. 在“**负责人**”框中，输入为解决漏洞而分配的人员的姓名。
5. 单击“**保存**”。

查看插件输出

资产的插件输出提供上下文或说明，以说明为何要报告资产具有特定插件。

若要从“漏洞”页面查看插件输出的详细信息，请执行以下操作：

1. 转至“**漏洞**”。

   此时会出现“**漏洞**”页面。

2. 在漏洞列表中，选择要查看关于哪个漏洞的详细信息，然后执行下列操作之一：

   - 点击漏洞链接。
   - 右键点击漏洞并选择“**查看**”。
   - 从“**操作**”下拉框中选择“**查看**”。

   此时会出现“漏洞详细信息”页面，其中包含“**插件输出**”面板，并显示以下信息：

   - 命中日期
   - 源
   - 端口
   - 插件输出

     > **注意**：并非所有插件都提供插件输出。

若要从“清单”页面查看插件输出的详细信息，请执行以下操作：

1. 转至“**清单**”>“**所有资产**”。

   此时会出现“**清单**”页面。

2. 在资产列表中，选择要查看关于哪个资产的详细信息，然后执行下列操作之一：

   - 点击资产链接。
   - 右键点击资产并选择“**查看**”。
   - 选中资产旁边的复选框，然后从“**操作**”下拉框中选择“**查看**”。

   此时会出现“资产详细信息”页面。

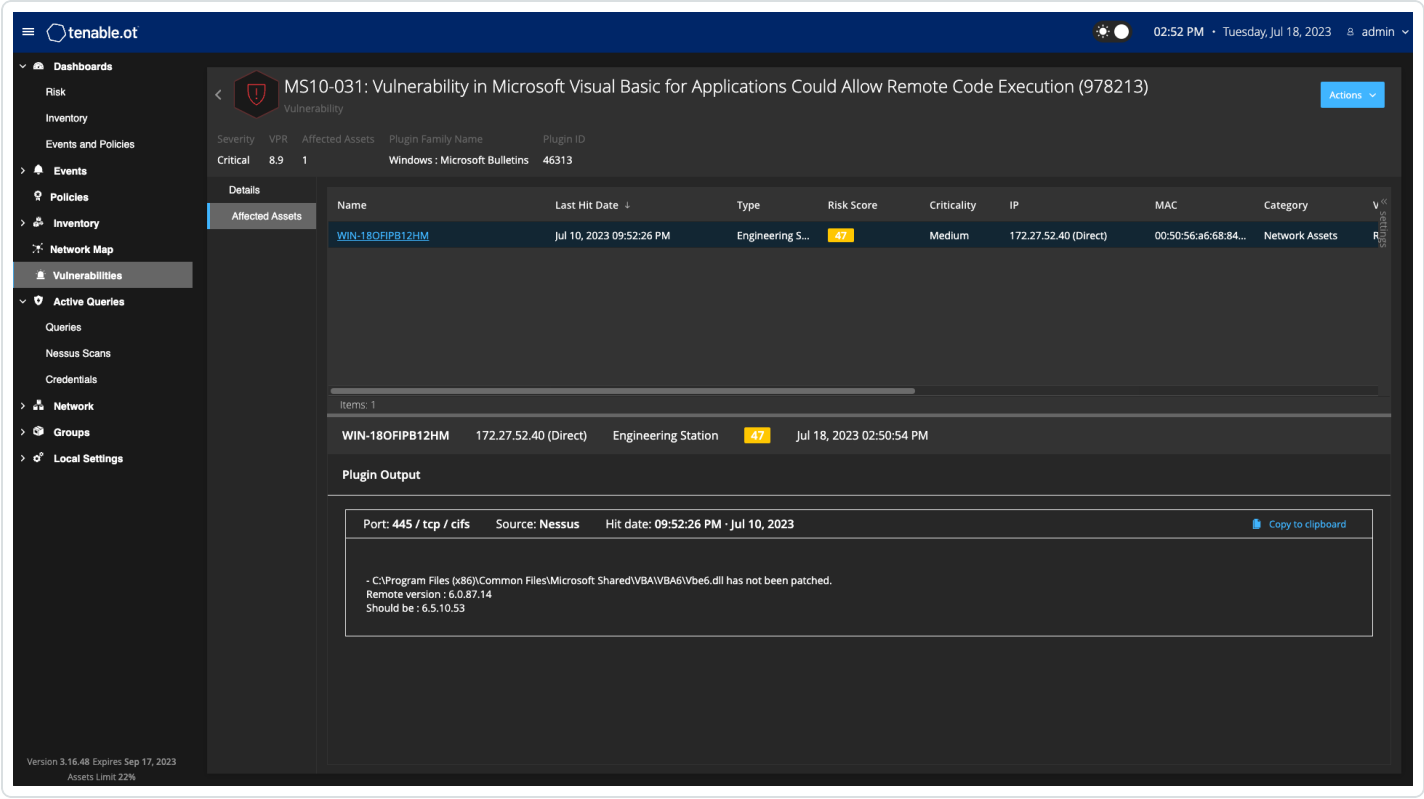
3. 点击“**漏洞**”选项卡。

   此时会出现漏洞列表，其中显示“**插件输出**”面板，以及以下信息：

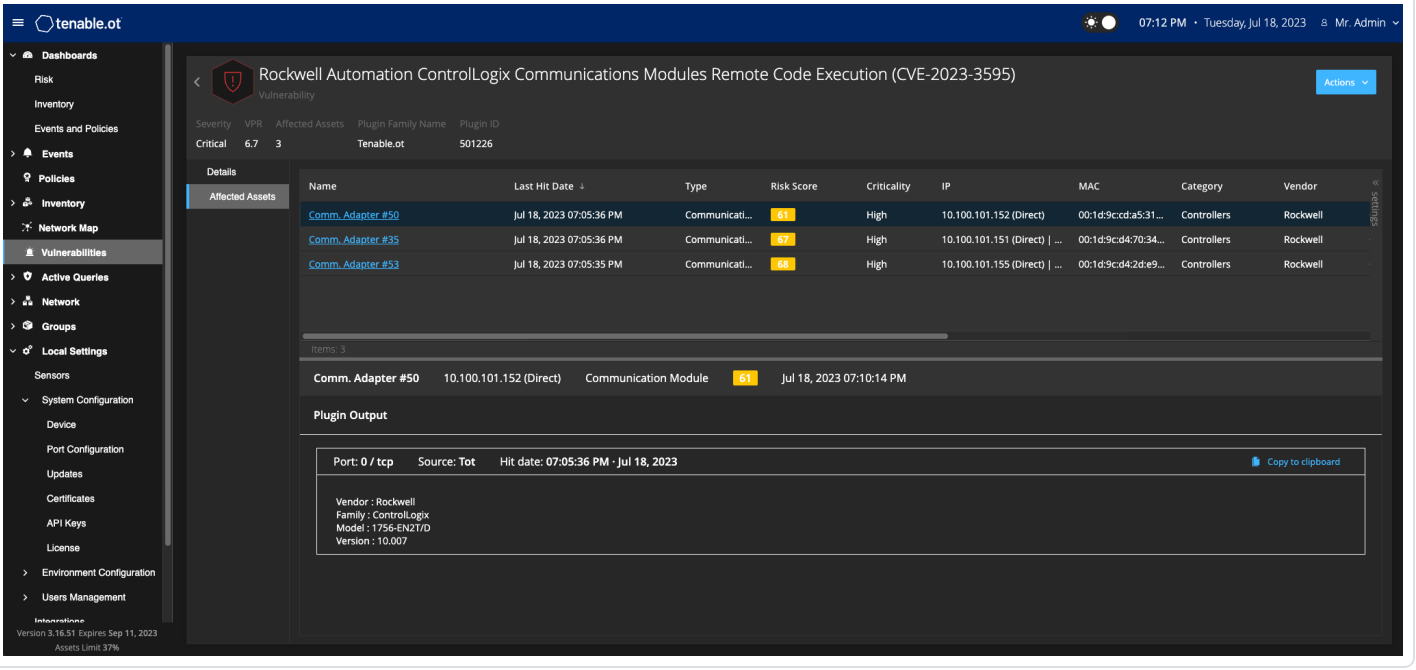
   - 命中日期
   - 源
   - 端口
   - 插件输出

   注意：并非所有插件都提供插件输出。

Tenable Nessus 插件的插件输出示例



OT Security 插件的插件输出示例


tenable.ot
07:12 PM • Tuesday, Jul 18, 2023
Mr. Admin
Dashboards
Risk
Inventory
Events and Policies
Events
Policies
Inventory
Network Map
Vulnerabilities
Active Queries
Network
Groups
Local Settings
Sensors
System Configuration
Device
Port Configuration
Updates
Certificates
API Keys
License
Environment Configuration
Users Management
Version 3.16.51 Expires Sep 11, 2023
Assets Limit 37%
Rockwell Automation ControlLogix Communications Modules Remote Code Execution (CVE-2023-3595)
Vulnerability
Actions
Severity VPR Affected Assets Plugin Family Name Plugin ID
Critical 6.7 3 Tenable.ot 501226
Details
Affected Assets
Name Last Hit Date Type Risk Score Criticality IP MAC Category Vendor
Comm. Adapter #50 Jul 18, 2023 07:05:36 PM Communicati... 61 High 10.100.101.152 (Direct) 00:1d:9c:cd:a5:31... Controllers Rockwell
Comm. Adapter #35 Jul 18, 2023 07:05:36 PM Communicati... 67 High 10.100.101.151 (Direct) | ... 00:1d:9c:d4:70:34... Controllers Rockwell
Comm. Adapter #53 Jul 18, 2023 07:05:35 PM Communicati... 68 High 10.100.101.155 (Direct) | ... 00:1d:9c:d4:2d:e9... Controllers Rockwell
Items: 3
Comm. Adapter #50 10.100.101.152 (Direct) Communication Module 61 Jul 18, 2023 07:10:14 PM
Plugin Output
Port: 0 / tcp Source: Tot Hit date: 07:05:36 PM · Jul 18, 2023
Copy to clipboard
Vendor : Rockwell
Family : ControlLogix
Model : 1756-EN2T/D
Version : 10.007

本地设置

OT Security 中的“**本地设置**”部分包含 OT Security 的大多数配置页面。**本地设置**中包含以下页面：

主动查询：激活/停用查询功能并调整其频率和设置。请查看主动查询。

传感器：查看和管理传感器、批准或删除传入的传感器配对请求、配置传感器执行的主动查询。请参阅“传感器”。

系统配置

- “**设备**”：查看和编辑设备详细信息及网络信息。例如，系统时间、自动注销（即不活动超时）。

  > **注意**：您可以在 Tenable Core 中配置 DNS 服务器。有关更多信息，请参阅《Tenable Core + Tenable OT Security 用户指南》中的“手动配置静态 IP 地址”。

- **端口配置**：查看如何配置设备上的端口。有关端口配置的更多信息，请参阅“安装 OT Security 设备 > 第 4 步：安装向导 > 屏幕 2：设备”。
- **更新**：通过云端或离线方式对插件进行自动或手动更新。
- **证书**：通过在系统中生成新的 HTTPS 证书或上传自己的证书，查看有关 HTTPS 证书的信息并确保连接安全。请参阅“系统配置”。
- **API 密钥**：生成 API 密钥，以便第三方应用程序能够通过 API 访问 OT Security。所有用户均可创建 API 密钥。API 密钥与创建它的用户拥有相同的权限，具体根据其角色而定。API 密钥在第一次生成时只显示一次；您必须将其保存在安全的位置以供以后使用。
- **许可证**：查看、更新和续订许可证。请参阅“许可证”。

环境配置

- **资产设置**
  - **受监控的网络**：查看和编辑系统对资产进行分类的 IP 范围聚合。
  - **使用 CSV 更新资产详细信息**：使用 CSV 模板更新资产的详细信息。
  - **手动添加资产**：使用 CSV 模板将新资产添加到资产列表。

注意：可发送到 Tenable Nessus Network Monitor 的 IP 范围的最大数量为 128，因此 Tenable 建议不要超过此限制。除指定的 IP 范围之外，位于 OT Security 平台子网内的任何主机或任何执行活动的设备都将划分为资产。

- **隐藏的资产**：查看系统中的隐藏资产列表。这些资产是从资产列表中删除的资产，详情请参阅"资产"。您可以从此页面还原隐藏的资产。
- **自定义字段**：创建自定义字段以使用相关信息标记资产。自定义字段可以是纯文本，也可以是外部资源的链接。
- **事件群集**：您可以将指定时间范围内发生的多个类似事件聚集在一起，以对其进行监控。请参阅"事件群集"。
- **PCAP 播放器**：您可以上传包含记录的网络活动的 PCAP 文件，并在 OT Security 上"播放"，从而将数据加载到系统中。请参阅"PCAP 播放器"。

- **用户和角色**：查看、编辑和导出与所有用户帐户有关的信息。
  - **用户设置**：查看和编辑当前登录系统的用户信息（全名、用户名和密码），并更改用户界面中使用的语言（英语、日语、中文、法语或德语）。
  - **本地用户**：管理员用户可以为特定用户创建本地用户帐户并向该帐户分配角色，详情请参阅"用户和角色"。
  - **用户组**：管理员用户可查看、编辑、添加和删除用户组。请参阅"用户和角色"。
  - **身份验证服务器**：可以选择使用 LDAP 服务器（例如 Active Directory）分配用户凭据。在这种情况下，可以在 Active Directory 中管理用户特权。请参阅 用户和角色。
- **集成**：建立与其他平台的集成。OT Security 当前支持与 Palo Alto Networks 新一代防火墙 (NGFW) 和 Aruba ClearPass 以及其他 Tenable 产品（Tenable Security Center 和 Tenable Vulnerability Management）集成。请参阅"集成"。
- **服务器**：查看、创建和编辑系统中配置的服务器。针对以下服务器显示单独的屏幕：
  - **SMTP 服务器**：SMTP 服务器可通过电子邮件发送事件通知。
  - **Syslog 服务器**：Syslog 服务器可将事件日志记录在外部 SIEM 上。
  - **FortiGate 防火墙**：OT Security 与 FortiGate 集成后，用户可以根据 OT Security 网络事件向 FortiGate 防火墙发送防火墙策略建议。

- **系统操作**：显示系统活动的子菜单。子菜单包含下列选项：
  - **系统备份** — Allows you to back up your OT Security appliance (except packet capture data). To restore the system from a backup file, see Manual Restore of a OT Security Backup. During the backup process, OT Security is unavailable to all users.
  - **导出设置**：将 OT Security 平台配置设置作为 **.ndg** 文件导出到本地计算机。此文件用作系统重置时的备份或用于导入新的 OT Security 平台。
  - **导入设置**：将另存为 **.ndg** 文件的 OT Security 平台配置设置导入本地计算机。
  - **下载诊断数据**：在 OT Security 平台上创建包含诊断数据的文件，并将其存储在本地计算机上。
  - **重新启动**：重新启动 OT Security 平台。这是激活某些配置更改所必需的操作。
  - **禁用**：禁用所有监控活动。可以随时重新激活监控活动。
  - **关闭**：关闭 OT Security 平台。若要开机，请按 OT Security 设备上的电源按钮。
  - **恢复出厂设置**：将所有设置恢复为出厂默认设置。警告：

    注意：此操作无法撤消，系统中的所有数据都将丢失。
- **系统日志**：显示系统中发生的所有系统事件的日志。例如，已打开的策略、已编辑的策略、已解决的事件等。可以将该日志作为 CSV 文件导出或将其发送到 Syslog 服务器。请参阅 系统日志。

传感器

使用 Tenable Core 用户界面将传感器配对后，您可使用“**操作**”菜单中的“**编辑**”、“**暂停**”和“**删除**”功能批准新配对、查看和管理传感器。您也可以选择使用“**自动批准传感器配对请求**”切换开关为传感器配对请求启用自动批准。

注意：低于版本 2.214 的传感器型号不会出现在 ICP 传感器页面中。但是，它们仍可在未经身份验证的模式中使用。

注意：您可以通过 ICP 配对无限数量的传感器，但是每个设备的 SPAN(交换端口分析器) 流量总和存在上限。例如，您可以拥有 10 个传感器，每个传感器的传输速率为 10 Mbps 到 20 Mbps，但总流量不

得超过 ICP 的限制。有关更多信息，请参阅 Tenable Core 和 OT Security 用户指南中的“系统和许可证要求”。

查看传感器

“传感器”表显示系统中所有 2.214 及更高版本的传感器的列表。

“传感器”表格包含以下详细信息：

参数	描述
IP	传感器的 IPv4 地址。
状态	传感器的状态包括：**已连接**、**已连接（未经身份验证）**、**待批准**、**已断开连接**或已暂停。
主动查询	传感器发送主动查询的功能包括：**已启用**、**已禁用**、**不适用**。
主动查询网络	获得传感器分配的网段。
名称	传感器在系统中的名称。
上次更新时间	传感器信息上次更新的日期和时间。
传感器标识符	传感器通用唯一标识符 (UUID)，用于唯一标识互联网上的对象或实体的 128 位值。
版本	传感器版本。
吞吐量	测量通过传感器的数据量（单位：KB/s）

手动批准传入的传感器配对请求

如果将“**自动批准传感器配对请求**”设置切换为“**关闭**”，则必须手动批准传入的传感器配对请求才能成功连接。

若要手动批准传感器配对请求，请执行以下操作：

1. 转至“**本地设置**”>“**传感器**”。
2. 单击表中状态为“**待批准**”的行。
3. 单击“**操作**”>“**批准**”，或选择右键单击菜单中的“**批准**”。

注意：如果要删除传感器，请单击“**操作**”>“**删除**”，或右键单击并选择右键单击菜单中的“**删除**”。

配置主动查询

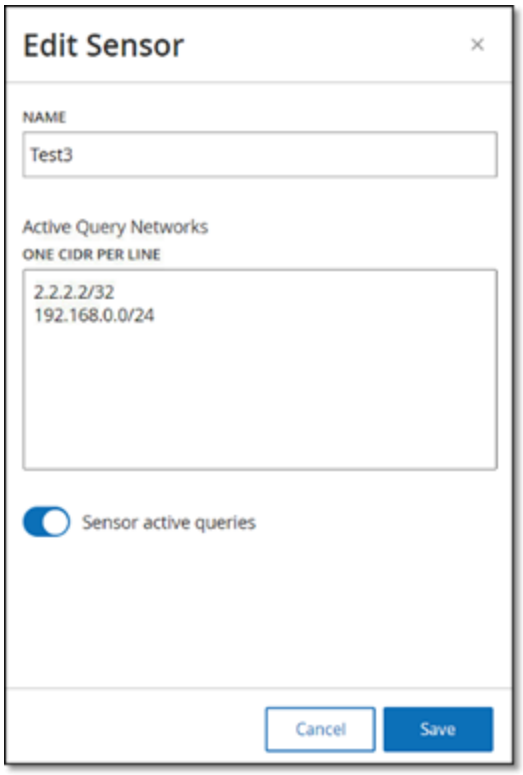
在“经过身份验证”模式下连接并经过配置后，传感器可以在分配的网段中执行主动查询。您需要指定传感器要查询的网段。

注意：传感器可以不按此配置在所有可用网段上执行被动网络检测。

若要配置主动查询，请执行以下操作：

1. 在“**本地设置**”下，转至“**系统配置**”>“**传感器**”。
2. 单击表中状态为“**已连接**”的行。
3. 单击“**操作**”>“**编辑**”，或右键单击并选择“**编辑**”。

   此时会显示“**编辑传感器**”面板。



4. 如要重命名传感器，请编辑“**名称**”框中的文本。

5. 在“**主动查询网络**”框中，通过使用 CIDR 符号并在单独的行上添加每个子网络，可添加或编辑传感器将向其发送主动查询的相关网段。

   > **注意**：只能对包含在受监控网络范围内的 CIDR 执行查询。确保仅添加可通过此传感器访问的 CIDR。若添加不可访问的 CIDR，则可能会干扰 ICP 通过其他方式查询这些分段的能力。

6. 单击“**传感器主动查询**”切换开关以启用主动查询。
7. 单击“**保存**”。

   随后，面板关闭。在“**传感器**”表的“**主动查询**”栏下，已启用的传感器现在会显示“**已启用**”。

更新传感器

从 3.16 版开始，OT Security 传感器会从管理传感器的 ICP 接收软件和安全更新。当传感器经过身份验证进行配对后，就会依赖该站点提供任何必要的操作系统和软件更新。传感器只需联系到 OT Security，即可接收软件更新。OT Security 允许您从“**传感器**”页面集中更新所有传感器。

如果传感器需要更新，您会在以下情况下收到警报：

- 启动。
- 传感器与 ICP 之间的配对完成。
- 定期检查。
- 使用“**检查更新**”选项。

注意：传感器与 OT Security 配对时必须进行身份验证，才能更新远程传感器。有关配对的更多信息，请参阅“使用 ICP 配对传感器”。

若要使用 ICP 更新经过身份验证的传感器版本 3.16 或更高版本，请执行以下操作：

1. 转至“**本地设置**”>“**传感器**”。

   此时会出现“**传感器**”页面。

2. 检查“**版本**”列，查看版本是否为最新，或者是否需要更新。
3. 如果该版本需要更新，请执行下列操作之一：

   更新单个传感器：

   - 右键单击所需传感器，然后选择“**更新**”。
   - 选中所需传感器旁边的复选框，然后从“**操作**”菜单中选择“**更新**”。

   更新多个传感器：

   - 选择一个或多个需要更新的传感器，然后从“**操作**”菜单中选择“**更新**”。

OT Security 会更新所选的传感器。

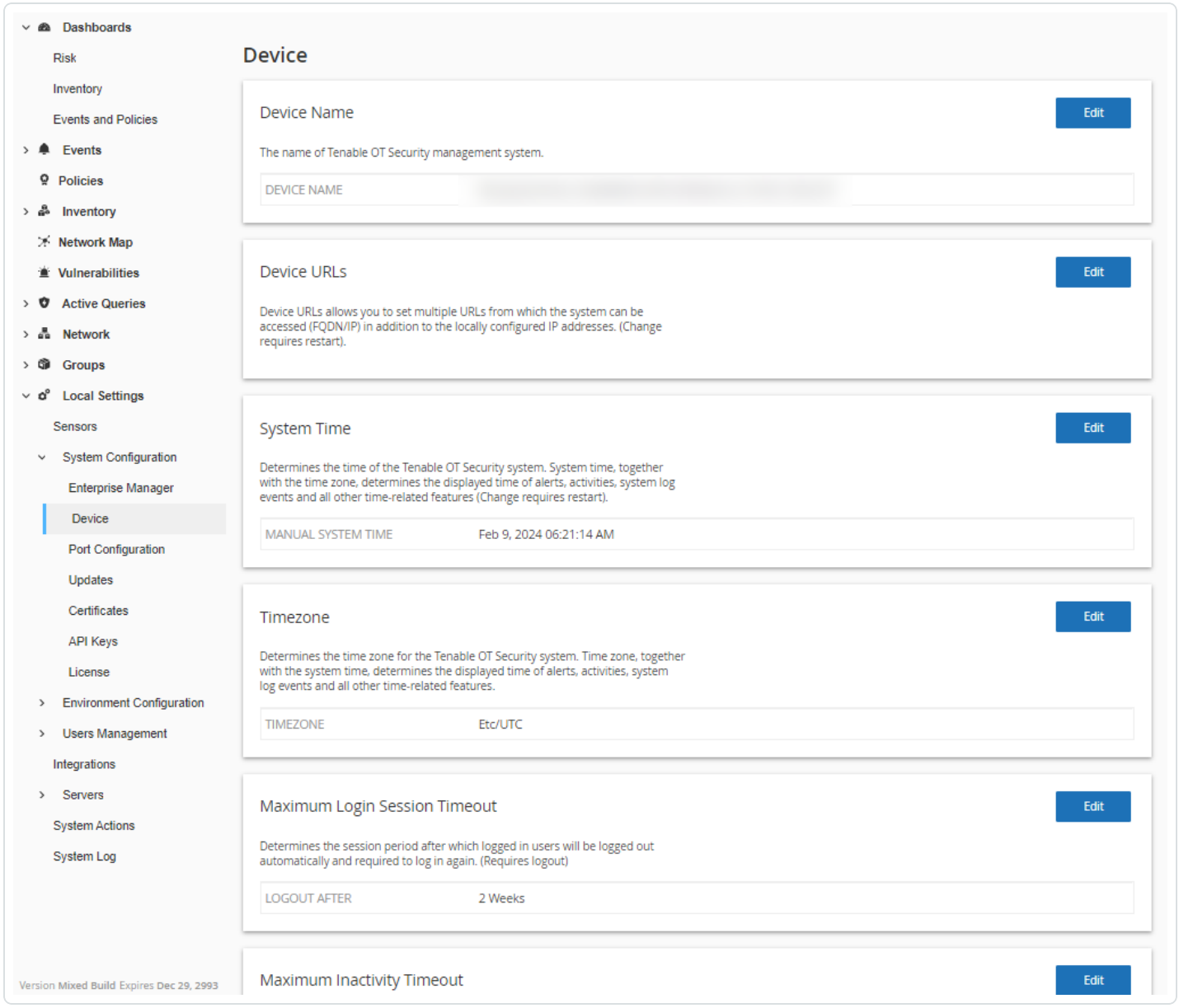
注意：更新期间，传感器可能不可用。

系统配置

OT Security"**系统配置**"页面允许自动配置和手动执行插件更新，以及查看和更新与设备、HTTPS 证书、API 密钥和许可证相关的详细信息。

设备

“**设备**”页面显示有关 OT Security 配置的详细信息。您可以在此页面上查看并编辑配置。



设备名称

OT Security 设备的唯一标识符。

设备 URL

允许您设置可用于访问系统的单个 URL (FQDN)。

要点:编辑设备 URL 是一项重要更改。新的 FQDN 不会再次显示。如果不能准确记录字符串,用户界面将无法访问。请务必验证字符串解析,然后再继续。

系统时间

系统会自动设置正确的时间和日期,但您可以编辑。

注意:设置正确的日期和时间对于准确记录日志和警报而言至关重要。

时区

从下拉列表中选择站点位置的本地时区。要更改时区,请单击"**编辑**"

登录会话最长超时时间

会话时间段,此时间段过后,已登录用户将自动注销并需要重新登录。要更改登录会话超时时间,请单击"**编辑**"。可用的时间段选项包括:2 周、30 分钟、1 小时、4 小时、12 小时、1 天、1 周和 2 周。

最长无效超时时间

无效时间段,此时间段过后,已登录用户将自动注销并需要重新登录。要更改不活动时间,请单击"**编辑**"。

开放端口老化期

确定一个时间段,此段时间过后,如果未收到表明端口仍处于打开状态的进一步说明,开放端口列表便会从各个"**资产详细信息**"屏幕中删除。默认设置为两周。有关更多信息,请参阅"资产"。

Ping 请求

开启 Ping 请求可激活 OT Security 平台对 ping 请求的自动响应。

要激活 Ping 请求,请单击"**Ping 请求**"切换开关以启用 Ping 请求。

数据包捕获

打开完整数据包捕获功能可激活连续记录网络中所有流量的完整数据包捕获的功能。这可实现广泛的故障排除和取证调查功能。当存储容量超过 1.8 TB 时，系统会删除较早的文件。您可以在"**网络**">"**数据包捕获**"页面上查看和下载可用文件，详情请参阅"网络"部分。

要激活数据包捕获，请单击"**数据包捕获**"切换开关以启用数据包捕获。

注意：您可以通过将开关切换为"**关闭**"随时停止数据包捕获功能。

自动批准传感器配对请求

启用"自动批准传入的传感器配对请求"可确保所有传感器配对请求在无需任何其他管理员的情况下即可获得批准。如果未选择此选项，则任何新的传感器都需要经过最终的手动批准后才能连接到网络。

要启用自动批准传入的传感器配对请求，请单击"**自动批准传入的传感器配对请求**"切换开关以启用自动批准。

启用使用情况统计信息

"**启用使用情况统计数据**"选项指定 Tenable 能否收集关于 OT Security 部署的匿名遥测数据。启用后，Tenable 会收集无法归因于特定个人的遥测信息；仅在公司级别收集。这些信息不包含个人数据或个人身份信息 (PII)。遥测信息包括但不限于关于所访问的页面、所使用的报告和仪表盘以及所配置的功能的数据。Tenable 会按照 Tenable 主协议的规定使用这些数据，以改善用户使用新版 OT Security 的体验和用于其他合理的商业目的。此设置默认为启用。

要启用遥测收集，请单击"**启用使用情况统计数据**"。

注意：单击切换开关即可随时禁用使用情况统计数据共享。

GraphQL Playground

浏览器内 GraphQL IDE。启用/禁用此切换开关，允许/禁止使用生产环境中的 Playground 测试 API 查询。

端口配置

“**端口配置**”页面会显示如何配置设备上的端口。有关端口配置的更多信息，请参阅“**安装 OT Security 设备 > 第 4 步：安装向导 > 屏幕 2：设备**”。

更新内容

将插件和 IDS 引擎规则集保持在最新状态可以确保监控资产是否存在所有最新已知漏洞。可通过云自动和手动执行更新，也可离线执行。

注意：您也可以通过单击“**更新插件**”按钮从“**漏洞**”窗口执行更新。

注意：如果用户许可证过期，则下载新更新的选项将被阻止，用户将无法更新其插件。

Tenable Nessus 插件集更新

云更新

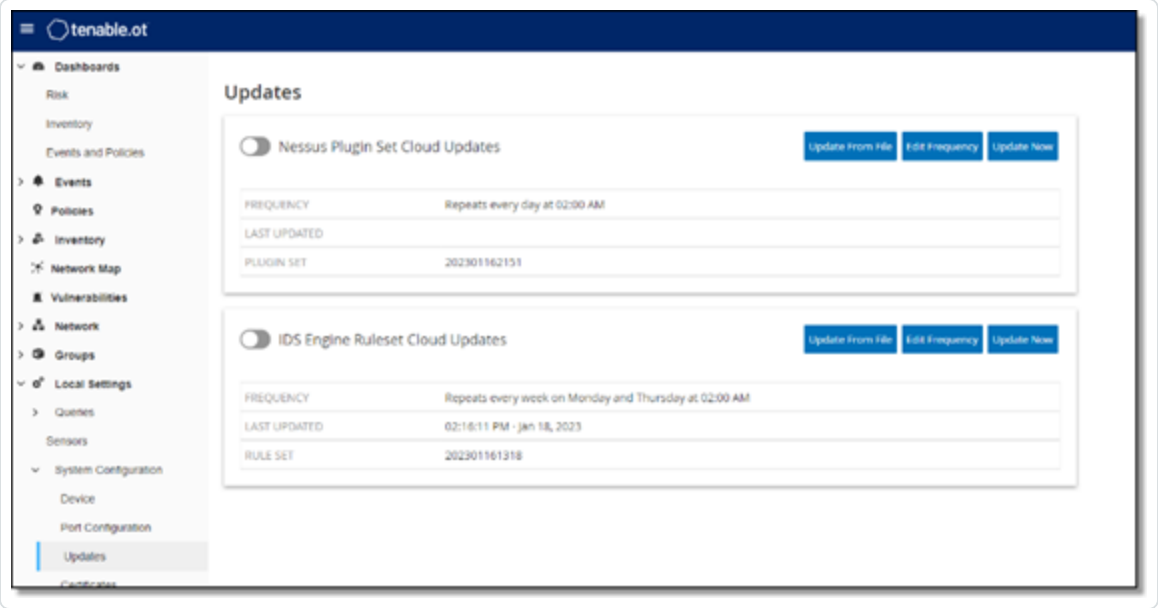
具有 Internet 连接的用户可通过云更新插件。打开自动更新后，插件会按用户设置的时间和频率进行更新（默认设置：每天凌晨 02:00）。

设置通过云自动更新插件

若要启用插件的自动更新功能，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”窗口会显示“**Nessus 插件集云更新**”，其中包含插件集的编号、上次更新时间和更新计划。



2. 点击“**Nessus 插件设置云更新**”切换开关以启用自动更新。

若要编辑插件的自动更新计划，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”窗口会显示“**Nessus 插件集云更新**”，其中包含插件集的编号、上次更新时间和更新计划。

2. 点击“**编辑频率**”。

   此时会出现“**编辑频率**”侧面板。

3. 在“**重复频率**”部分，输入一个数字并从下拉框中选择时间单位（天或周），以此来设置更新插件的时间间隔。

   如果选择“**周**”，请选择要在每周的哪些天对插件执行更新。

4. 在“**精确时间**”部分，单击时钟图标并选择时间或手动输入时间即可设置您希望更新插件的时间（采用 HH:MM:SS 的格式）。

5. 单击“**保存**”。

   此时会出现一条消息，确认 OT Security 已成功更新频率。

手动通过云更新插件

若要手动更新插件，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”页面会显示“**Nessus 插件集云更新**”，其中包含插件集的上次更新版本、上次更新时间和更新计划。

2. 单击“**立即更新**”。

   此时会出现一条消息，确认更新已开始。更新完成后，“**插件集**”将显示当前插件集的编号。

   > **提示**：更新**插件集**的过程中，请确保浏览器窗口保持打开且不要刷新页面。

离线更新

OT Security 设备上无 Internet 连接的用户可通过从 Tenable 客户门户网站下载最新的插件集并上传文件来手动更新其插件。

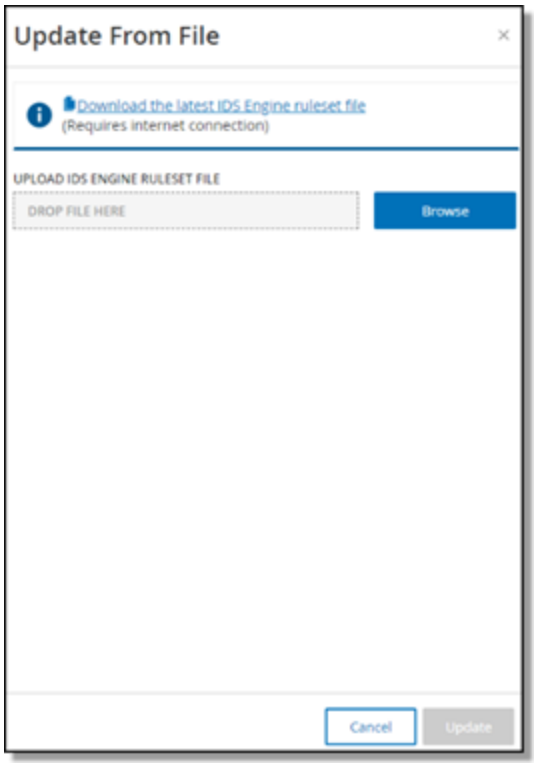
若要离线更新插件，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”页面会显示“**Nessus 插件集云更新**”，其中包含插件集的编号、上次更新时间和更新计划。

2. 点击“**从文件更新**”。

   此时会出现“**从文件更新**”窗口。



3. 如果尚未执行此操作，请单击链接下载最新的插件文件，然后返回“**从文件更新**”窗口。

   注意：只有连接 Internet(例如连接到 Internet 的 PC) 后才能从该链接下载最新的插件文件。

4. 单击“**浏览**”，然后导航至从 OT Security 客户门户网站中下载的插件集文件。

5. 单击“**更新**”。

IDS 引擎规则集更新

云更新

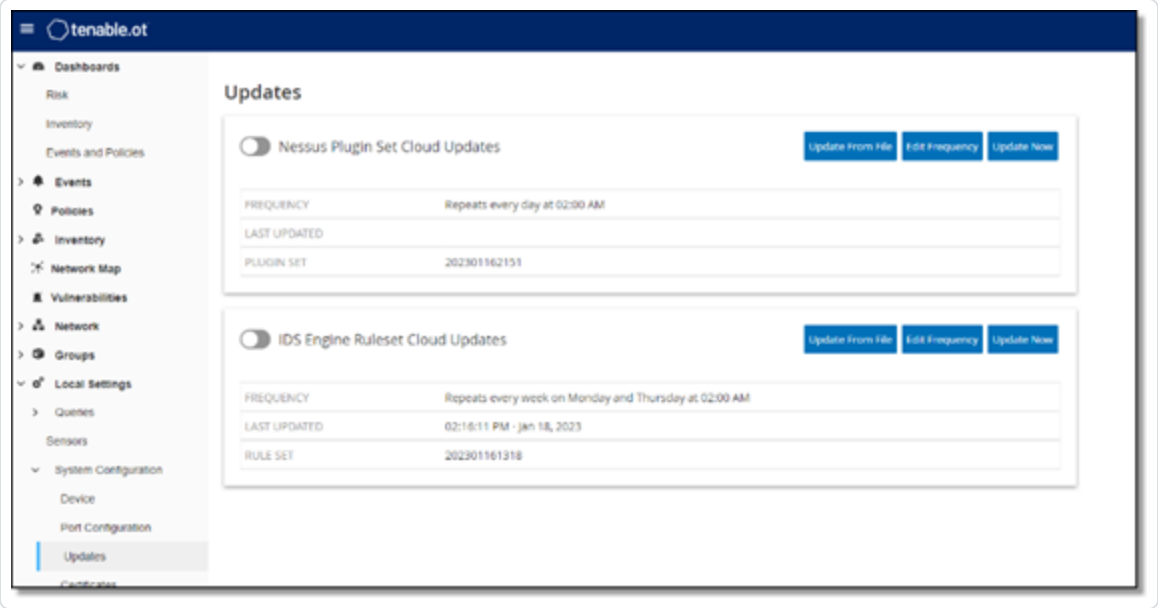
已连接 Internet 的用户可通过云更新其 IDS 引擎规则集。打开自动更新后，IDS 引擎规则集会按用户设置的时间和频率进行更新(默认设置：每周一和周四的凌晨 02:00)。

设置自动通过云更新 IDS 引擎规则集

若要为 IDS 引擎规则集启用自动更新，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”页面会显示“**IDS 引擎规则集云更新**”，其中包含规则集的编号、上次更新时间和更新计划。



2. 点击“**IDS 引擎规则集云更新**”切换开关以启用自动更新。

若要编辑 IDS 引擎规则集的自动更新计划，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”页面会显示“**IDS 引擎规则集云更新**”，其中包含规则集的编号、上次更新时间和更新计划。

2. 点击“**编辑频率**”。

   此时会出现“**编辑频率**”侧面板。

3. 在“**重复频率**”部分，输入一个数字并从下拉框中选择时间单位（天或周），以此来设置更新规则集的时间间隔。

   如果选择“**周**”，请选择要在每周的哪些天对规则集执行更新。

4. 在“**精确时间**”部分，单击时钟图标并选择时间或手动输入时间即可设置您希望更新 IDS 引擎规则集的时间（采用 HH:MM:SS 的格式）。

5. 单击“**保存**”。

   此时会出现一条消息，确认频率已成功更新。

对 IDS 引擎规则集执行手动云更新

若要手动更新 IDS 引擎规则集，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”页面会显示“**IDS 引擎规则集云更新**”，其中包含规则集的编号、上次更新时间和更新计划。

2. 单击“**立即更新**”按钮。

   此时会显示一个对话框，告知更新已开始。更新完成后，“**规则集**”字段将显示当前 IDS 引擎规则集的编号。

离线更新

OT Security 设备上无 Internet 连接的用户可通过从 Tenable 客户门户网站下载最新的规则集并上传文件来手动更新其 IDS 引擎规则集。

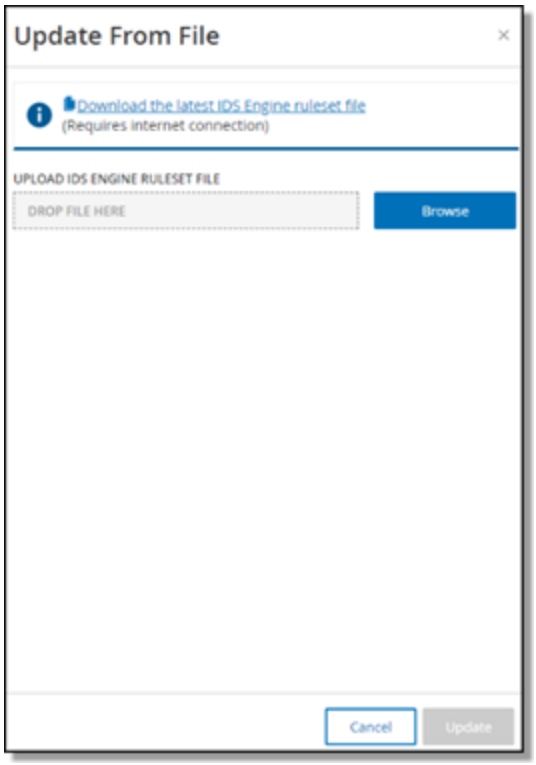
若要离线更新 IDS 引擎规则集，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**更新**”。

   “**更新**”屏幕会显示“**IDS 引擎规则集云更新**”，其中包含规则集的编号、上次更新时间和更新计划。

2. 点击“**从文件更新**”。

   此时会出现“**从文件更新**”窗口。



3. 如果您尚未完成此操作，请单击链接下载最新的 IDS 引擎规则集文件。

> **注意**：只有连接 Internet(例如连接到 Internet 的 PC) 后才能从该链接下载最新的 IDS 引擎规则集文件。

4. 单击“**浏览**”，然后导航至从 OT Security 客户门户网站中下载的 IDS 引擎规则集文件。
5. 单击“**更新**”。

证书

生成 HTTPS 证书

HTTPS 证书确保系统使用安全的 OT Security 设备和服务器连接。初始证书会在两年后到期。可以随时生成新的自签名证书。新证书的有效期为一年。

注意:生成新证书将覆盖当前证书。

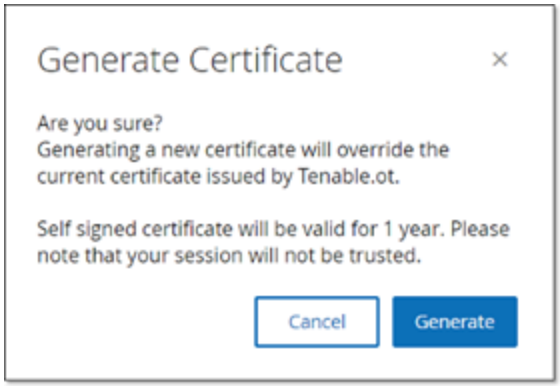
若要生成自签名证书,请执行以下操作:

1. 转至"**本地设置**">"**系统配置**">"**证书**"。

   此时会出现"**证书**"窗口。

2. 在"**操作**"菜单中,选择"**生成自签名证书**"。

   此时会出现"生成证书"确认窗口。



3. 单击"**生成**"。

   OT Security 会生成自签名证书,您可在"**本地设置**">"**系统配置**">"**证书**"页面中查看。

上传 HTTPS 证书

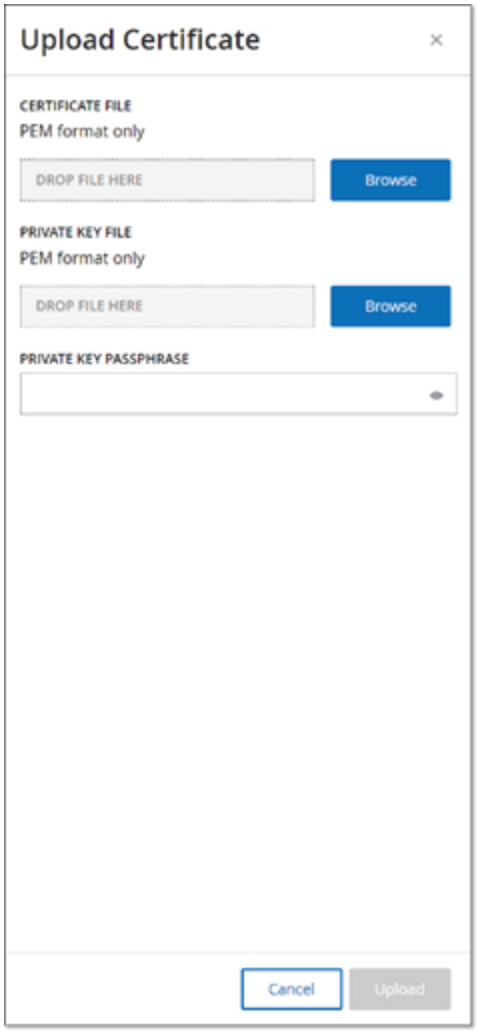
若要上传 HTTPS 证书，请执行以下操作：

1. 转至“**本地设置**”>“**系统配置**”>“**证书**”。

   此时会出现“**证书**”窗口。

2. 在“**操作**”菜单中，选择“**上传证书**”。

此时会显示“**上传证书**”侧面板。



3. 在“**证书文件**”部分中，单击“**浏览**”并导航至要上传的证书文件。
4. 在“**私钥文件**”部分中，单击“**浏览**”并导航至要上传的私钥文件。
5. 在“**私钥密码**”框中输入私钥密码。
6. 单击“**上传**”以上传文件。

   此时会关闭侧面板。

> **注意**：替换证书后，Tenable 建议您重新加载浏览器选项卡，以确保 HTTP 证书更新成功。如果上传失败，OT Security 会显示警告消息。

许可证

若需要更新或重新初始化 OT Security 许可证，请联系 Tenable 客户经理。在您的 Tenable 客户经理更新许可证后，您可以更新或重新初始化许可证。有关更多信息，请参阅 OT Security 许可证工作流。

环境配置

手动添加资产

为了跟踪清单，即使 OT Security 尚未检测到这些资产，您也可能希望查看这些资产。可以通过下载并编辑 CSV 文件，然后将该文件上传到系统来手动将这些资产添加到清单中。您只能上传其 IP 未被系统中现有资产所使用的资产。如果系统检测到具有相同 IP 的网络通信资产，则系统将使用检索到的有关已检测到资产的信息并覆盖之前上传的信息。当检测到在网络中通信时，系统会开始将该资产作为常规资产进行处理。

已上传资产的 IP 地址会计入系统许可。

在 OT Security 检测到上传的资产之前，其风险评分为 0。

注意：手动添加资产后，OT Security 在检测到这些资产在网络中发生通信后才会检测与之相关的事件。

若要手动添加资产，请执行以下操作：

1. 转至“**本地设置**”>“**环境配置**”>“**资产设置**”。

   此时会出现“**资产设置**”屏幕。

2. 打开“**手动添加资产**”，在“**操作**”菜单中选择“**下载 CSV 模板**”。

   OT Security 会下载 tot_Assets 模板文档。

3. 打开 tot_Assets 模板文档。

4. 根据文件中的说明精确编辑 tot_Assets 模板，仅保留列标题（名称、类型等）和输入的值。

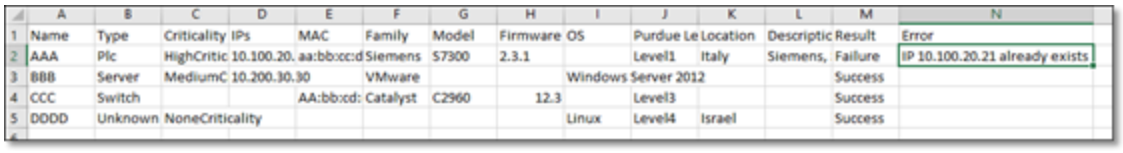
5. 保存已编辑的文件。

6. 返回“**资产设置**”屏幕。

7. 在“**操作**”菜单中，选择“**上传 CSV**”，然后导航至要上传的 CSV 文件并打开文件。

8. 在“**手动添加资产**”中，单击“**下载报告**”。

   此时会显示一个包含报告的 CSV 文件，“结果”列中会显示成功和失败。错误的详细信息会显示在“错误”列中。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Name	Type	Criticality	IPs	MAC	Family	Model	Firmware	OS	Purdue Le	Location	Descriptic	Result	Error
2	AAA	Plc	HighCritic	10.100.20.	aa:bb:cc:d	Siemens	S7300	2.3.1		Level1	Italy	Siemens,	Failure	IP 10.100.20.21 already exists
3	BBB	Server	MediumC	10.200.30.	30	VMware			Windows	Server 2012			Success	
4	CCC	Switch			AA:bb:cd:	Catalyst	C2960	12.3		Level3			Success	
5	DDDD	Unknown	NoneCriticality						Linux	Level4	Israel		Success	

事件群集

为了便于监控事件，具有相同特性的多个事件会划分到一个群集中。群集基于事件类型（即共享相同策略的事件）、源和目标资产等。

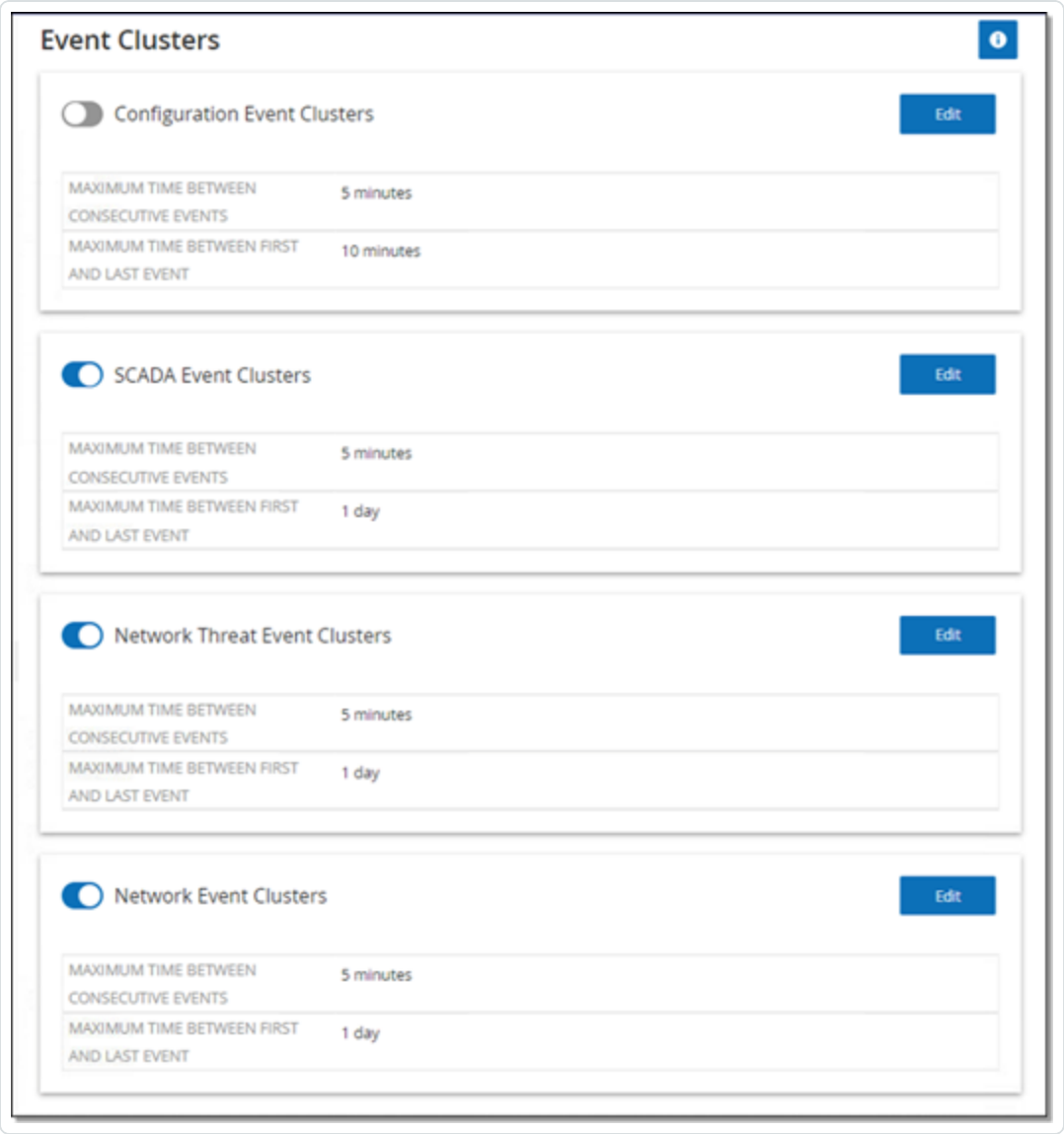
必须在以下已配置时间间隔内生成要划分到一个群集的事件：

- **连续事件之间的最长时间间隔**：设置事件之间的最长时间间隔。如果超过此时间，连续事件则不会划分到一个群集中。
- **第一个和最后一个事件之间的最长时间间隔**：设置所有事件显示为一个群集的最长时间间隔。在此时间间隔之后生成的事件将不是群集的一部分。

若要启用群集，请执行以下操作：

1. 转至“**本地设置**”，然后转至“**环境配置**”>“**事件群集**”。

   此时会出现“**事件群集**”屏幕。

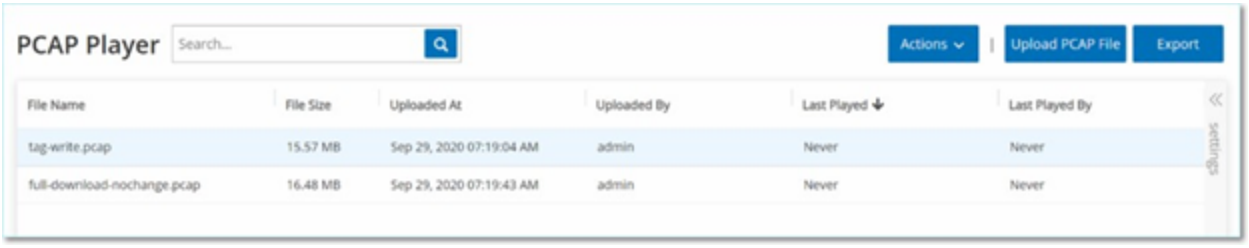


2. 单击切换开关以启用所需的群集类别。
3. 如要配置某个类别的时间间隔，请单击“**编辑**”。

   此时会出现“**编辑配置**”窗口。
4. 在数字框中输入所需的数值，并使用下拉框选择时间单位。

   注意：有关群集和时间间隔的更多信息，请单击 按钮。
5. 单击“**保存**”。

PCAP 播放器



OT Security 支持上传包含记录的网络活动的 PCAP(数据包捕获) 文件，并在 OT Security 上“播放”。在“播放”PCAP 文件时，OT Security 会监控网络流量，并记录有关检测到的资产、网络活动和漏洞的所有信息，如同流量出现在您的网络中一样。此功能可用于模拟目的，或分析在 OT Security 监控的网络之外发生的流量。例如，远程工厂。

注意：PCAP 播放器支持这些文件类型：`.pcap`、`.pcapng`、`.pcap.gz`、`.pcapng.gz`。可以使用由 OT Security 的实例或其他网络监控工具记录的文件。

上传 PCAP 文件

若要上传 PCAP 文件，请执行以下操作：

1. 转至“**本地设置**”>“**环境配置**”>“**PCAP 播放器**”。
2. 单击“**上传 PCAP 文件**”。

   此时会打开**文件资源管理器**。
3. 选择所需的 PCAP 记录。
4. 单击“**打开**”。

   OT Security 将 PCAP 文件上传到系统。

播放 PCAP 文件

若要播放 PCAP 文件，请执行以下操作：

1. 转至“**本地设置**”>“**环境配置**”>“**PCAP 播放器**”。
2. 选择要播放的 PCAP 录音。
3. 单击“**操作**”>“**播放**”。

   此时会出现“**播放 PCAP**”向导。
4. 在“**播放速度**”下拉框中，选择您希望系统播放文件的速度。

   选项为：“1X”、“2X”、“4X”、“8X”或“16X”。

   > **注意**：播放 PCAP 文件会将数据注入到系统中，此操作在执行后无法撤消或停止。
5. 单击“**播放**”。

   系统播放 PCAP 文件。PCAP 文件中的所有网络活动都会在系统中注册，并且系统识别的资产会添加到资产清单中。

   > **注意**：当某个文件仍在播放时，不能播放另一个 PCAP 文件。

用户和角色

OT Security 控制台的访问权限由指定该用户可用权限的用户帐户控制。用户的权限由为其分配的用户组确定。为每个用户组分配有一个角色，该角色定义了其成员可用的一组权限。因此，例如，如果"站点操作员"用户组具有"站点操作员"角色，则分配到该组的所有用户都将拥有与"站点操作员"角色关联的一组权限。

系统随附一组与每个可用角色对应的预定义用户组，即**管理员用户组 > 管理员角色**、**站点操作员用户组 > 站点操作员角色**等。还可以创建自定义用户组并指定其角色。

有三种在系统中创建用户的方法：

- **添加本地用户**：创建用户帐户以授权单个用户访问系统。将用户分配到定义其角色的用户组。
- **身份验证服务器**：使用组织的身份验证服务器（例如 Active Directory、LDAP）授予用户系统访问权限。可以根据 Active Directory 中的现有组分配 OT Security 角色。
- **SAML**：建立与身份提供程序（例如 Microsoft Entra ID）的集成并将用户分配给 OT Security 应用程序。

本地用户

用户组

用户角色

身份验证服务器

SAML

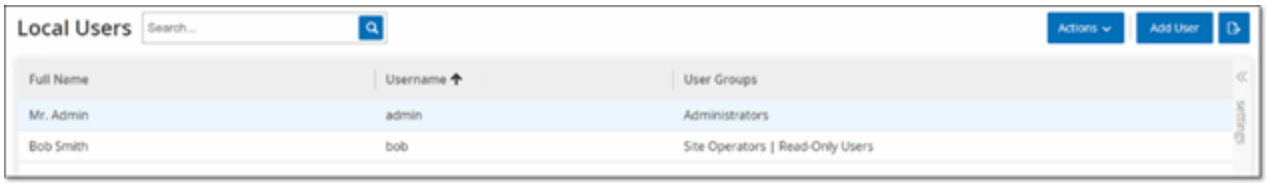
本地用户

管理员用户可以创建新的用户帐户和编辑现有帐户。将每个用户分配到一个或多个用户组，这些用户组确定了分配给该用户的角色。

注意：您可以在创建/编辑用户帐户或用户组期间将用户添加到用户组。

查看本地用户

“**本地用户**”窗口显示系统中所有本地用户的列表。



“**本地用户**”窗口显示以下详细信息：

参数	描述
全名	用户的全名。
用户名	用户用于登录的用户名。
用户组	为用户分配的用户组。

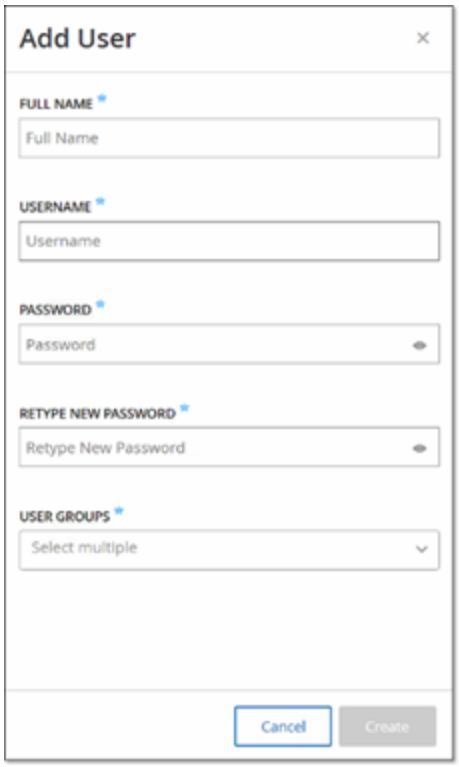
添加本地用户

可以创建用户帐户以授权单个用户访问系统。必须为每个用户分配一个或多个用户组。

若要创建用户帐户，请执行以下操作：

1. 转至“**本地设置**”>“**用户管理**”>“**本地用户**”。
2. 单击“**添加用户**”。

   此时会出现“**添加用户**”窗格。



3. 在“**全名**”框中，输入名字及姓氏。

   > **注意**：用户登录时，标题栏中会显示您输入的名称。

4. 在“**用户名**”框中，输入用于登录系统的用户名。
5. 在“**密码**”框中，输入密码。
6. 在“**重新输入密码**”框中，输入相同的密码。

注意:这是用户会用于初始登录的密码。登录系统后,用户可在"**设置**"窗口中更改密码。

7. 在"**用户组**"下拉框中,选择您要为此用户分配的每个用户组的复选框。

   注意:系统随附一组与每个可用角色对应的预定义用户组,即**管理员用户组** > **管理员角色**、**站点操作员用户组** > **站点操作员角色**等。有关可用角色的说明,请参阅"本地用户"。

8. 点击"**创建**"。

   OT Security 会在系统中创建新用户帐户,并添加到"**本地用户**"的用户列表中。

针对用户帐户的其他操作

编辑用户帐户

可以将用户分配到其他用户组或从某组中删除该用户。

若要更改用户的用户组，请执行以下操作：

1. 转至“**本地设置**”>“**用户管理**”>“**本地用户**”。

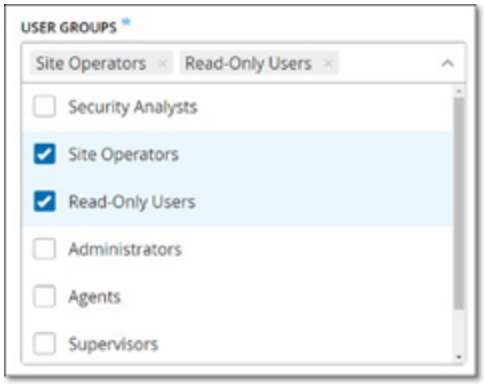
   此时会出现“**本地用户**”屏幕。

2. 右键单击所需用户，然后选择“**编辑用户**”。

   > **注意**：您还可以选择一个用户，然后在“**操作**”菜单中选择“**编辑用户**”。

3. 此时会显示“**编辑用户**”窗格，其中显示了用户分配到的用户组。

4. 在“**用户组**”下拉框中，选择或清除所需的用户组。



5. 单击“**保存**”。

更改用户的密码

注意:管理员用户可使用此程序更改系统中任何帐户的密码。任何用户都可以通过转至"**本地设置**">"**用户**"来更改自己的密码。

若要更改用户的密码,请执行以下操作:

1. 转至"**本地设置**">"**用户管理**">"**本地用户**"。

   此时会出现"**本地用户**"屏幕。

2. 右键单击所需用户,然后选择"**重置密码**"。

   注意:您还可以选择一个用户,然后在"**操作**"菜单中选择"**重置密码**"。

   此时会出现"**重置密码**"窗口。

3. 在"**新密码**"框中,输入新密码。
4. 在"**重新输入新密码**"框中,重新输入新密码。
5. 单击"**重置**"。

   此时,OT Security 会将新密码应用到指定的用户帐户。

删除本地用户

若要删除用户帐户,请执行以下操作:

1. 转至“**本地设置**”>“**用户管理**”>“**本地用户**”。

   此时会出现“**本地用户**”屏幕。

2. 右键单击所需用户，然后选择“**删除用户**”。

   注意：您还可以选择一个用户，然后在“**操作**”菜单中选择“**删除用户**”。

   此时会出现“确认”窗口。

3. 点击“**删除**”。

   OT Security 将用户帐户从系统中删除。

用户组

管理员用户可以创建新的用户组和编辑现有组。将每个用户分配到一个或多个用户组，这些用户组确定了分配给该用户的角色。

系统随附一组与每个可用角色对应的预定义用户组，即管理员用户组 > 管理员角色、站点操作员用户组 > 站点操作员角色等。有关可用角色的说明，请参阅“用户角色”。

查看用户组

“用户组”页面显示系统中所有用户组的列表。

“用户组”页面包含以下详细信息：

参数	描述
名称	用户组的名称。
成员	分配给该组的所有成员的列表。
角色	授予此组的角色。有关与每个角色关联的权限的说明，请参阅“用户角色表”。

添加用户组

可以创建新的用户组并将用户分配到该组。

若要创建用户组，请执行以下操作：

1. 转至“**本地设置**”>“**用户管理**”>“**用户组**”。

   此时会出现“**用户组**”屏幕。

2. 单击“**用户组**”。

   此时会出现“**创建用户组**”窗格。

3. 在“**名称**”框中，输入组名称。

4. 在“**角色**”下拉框中，从下拉列表中选择要分配给此组的角色。可用的角色包括：

- 只读
- 安全分析员
- 安全管理员
- 站点操作员
- 主管

5. In the **Users** drop-down box, select one or more users that you want to assign to this group.
6. 点击“**创建**”。

   OT Security 会创建新用户组，并添加到“**本地用户**”屏幕中显示的组列表中。

针对用户组的其他操作

编辑用户组

可以通过编辑组来编辑设置，以及向现有用户组添加成员或删除现有用户组的成员。

注意：您还可以选择一个用户，然后在“**操作**”菜单中选择“**删除用户**”。

若要编辑用户组，请执行以下操作：

1. 转至“**本地设置**”>“**用户管理**”>“**用户组**”。

   此时会出现“**用户组**”屏幕。

2. 请执行下列操作之一：

   - 右键单击所需用户组，然后选择“**编辑**”。
   - 选择您要编辑的用户组。此时会出现“**操作**”菜单。选择“**操作**”>“**编辑**”。

   此时会显示“**编辑用户组**”面板，其中显示了该组的设置。

3. 单击“**保存**”。

删除用户组

注意：您只能删除当前未向其分配用户的用户组。如果已将用户分配到组，则需要先从组中删除用户，然后才能删除该组。

若要删除用户组，请执行以下操作：

1. 转至“**本地设置**”>“**用户管理**”>“**用户组**”。

   此时会出现“**用户组**”屏幕。

2. 请执行下列操作之一：

   - 右键单击所需用户组，然后选择“**删除**”。
   - 选择您要删除的用户组。此时会出现“**操作**”菜单。选择“**操作**”>“**删除**”。

   此时会出现“确认”窗口。

3. 点击“**删除**”。

   OT Security 会删除**用户组**。

用户角色

可用的角色如下：

- **管理员**：拥有在系统中执行所有运营任务和管理任务（包括创建新的用户帐户）的最高特权。
- **只读**：可以查看数据（资产清单、事件和网络流量），但无法在系统中执行操作。
- **安全分析师**：可以在系统中查看数据以及解决安全事件。
- **安全经理**：可以管理与安全相关的功能，包括配置策略、在系统中查看数据以及解决事件。
- **站点操作员**：可以在系统中查看数据以及管理资产清单。
- **主管**：拥有在系统中执行所有运营任务和有限的管理任务（不包括创建新用户及其他敏感活动）的完全特权。

用户角色表

下表提供了为每个角色启用的权限的详细分类。

权限	管理员（本地）	管理员（外部/AD）	主管	安全管理员	安全分析员	站点操作员	只读
事件							
查看事件	✓	✓	✓	✓	✓	✓	✓
解决	✓	✓	✓	✓	✓	✗	✗
下载捕获文件	✓	✓	✓	✓	✓	✓	✓
从策略中排除	✓	✓	✓	✓	✗	✗	✗
全部解决	✓	✓	✓	✓	✓	✗	✗
导出	✓	✓	✓	✓	✓	✓	✓
在 FortiGate 上创建策略	✓	✓	✓	✓	✗	✗	✗
刷新	✓	✓	✓	✓	✓	✓	✓
策略							
查看策略	✓	✓	✓	✓	✓	✓	✓
启用/禁用	✓	✓	✓	✓	✗	✗	✗
查看操作	✓	✓	✓	✓	✓	✓	✓
编辑	✓	✓	✓	✓	✗	✗	✗
复制	✓	✓	✓	✓	✗	✗	✗
删除	✓	✓	✓	✓	✗	✗	✗

创建策略	✓	✓	✓	✓	✗	✗	✗
导出	✓	✓	✓	✓	✓	✓	✓
资产							
查看资产	✓	✓	✓	✓	✓	✓	✓
查看操作	✓	✓	✓	✓	✓	✓	✓
编辑	✓	✓	✓	✗	✗	✓	✗
删除	✓	✓	✓	✗	✗	✓	✗
导入(通过 CSV 上传新资产)	✓	✓	✓	✗	✗	✓	✗
隐藏	✓	✓	✓	✗	✗	✓	✗
导出	✓	✓	✓	✓	✓	✓	✓
重新同步	✓	✓	✓	✓	✓	✓	✗
Nessus 扫描	✓	✓	✓	✓	✓	✓	✗
生成快照(单一资产)	✓	✓	✓	✓	✓	✓	✗
更新已打开的端口(单一资产)	✓	✓	✓	✓	✓	✗	✗
更新端口状态(单一资产)	✓	✓	✓	✓	✓	✗	✗
在浏览器中查看(单一资产)	✓	✓	✓	✓	✓	✓	✓

在主资产映射中查看(单一资产)	✓	✓	✓	✓	✓	✓	✓
生成攻击途径(单一资产)	✓	✓	✓	✓	✓	✓	✓
漏洞(插件)							
查看插件命中率	✓	✓	✓	✓	✓	✓	✓
查看操作	✓	✓	✓	✓	✓	✓	✓
编辑注释	✓	✓	✓	✓	✓	✗	✗
更新插件集	✓	✓	✓	✓	✗	✗	✗
导出	✓	✓	✓	✓	✓	✓	✓
网络							
打开数据包捕获	✓	✓	✓	✗	✗	✗	✗
关闭正在进行的捕获	✓	✓	✓	✓	✓	✓	✗
下载 PCAP 文件	✓	✓	✓	✓	✓	✓	✓
导出对话表	✓	✓	✓	✓	✓	✓	✓
设置为基线	✓	✓	✓	✓	✗	✗	✗
生成映射	✓	✓	✓	✓	✓	✓	✓
刷新映射	✓	✓	✓	✓	✓	✓	✓
组							

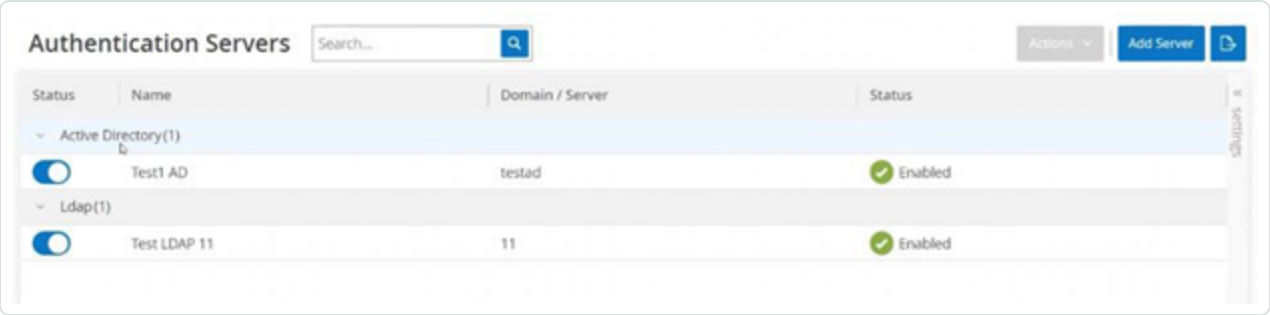
查看组	✓	✓	✓	✓	✓	✓	✓
查看操作	✓	✓	✓	✓	✓	✓	✓
编辑	✓	✓	✓	✓	✗	✗	✗
复制	✓	✓	✓	✓	✗	✗	✗
删除	✓	✓	✓	✓	✗	✗	✗
创建组	✓	✓	✓	✓	✗	✗	✗
导出	✓	✓	✓	✓	✓	✓	✓
报告							
查看报告	✓	✓	✓	✓	✓	✓	✓
生成	✓	✓	✓	✓	✓	✓	✓
下载	✓	✓	✓	✓	✓	✓	✓
导出	✓	✓	✓	✓	✓	✓	✓
网段							
查看网段	✓	✓	✓	✓	✓	✓	✓
编辑	✓	✓	✓	✓	✗	✗	✗
删除	✓	✓	✓	✓	✗	✗	✗
创建	✓	✓	✓	✓	✗	✗	✗
导出	✓	✓	✓	✓	✓	✓	✓
了解更多	✓	✓	✓	✓	✓	✓	✓
本地设置							
查询	✓	✓	✓	✗	✗	✗	✗
系统配置:设备详细信息	✓	✓	✓	✗	✗	✗	✗

系统配置:传感器	✓	✓	✓	✓(无操作)	✓(无操作)	✓(无操作)	✓(无操作)
系统配置:端口配置	✓	✓	✓	✗	✗	✗	✗
系统配置:更新	✓	✓	✓	✗	✗	✗	✗
系统配置:证书 (HTTPS)	✓	✓	✗	✗	✗	✗	✗
系统配置:API 密钥	✓	✗	✓(仅限本地用户)	✓(仅限本地用户)	✓(仅限本地用户)	✓(仅限本地用户)	✓(仅限本地用户)
系统配置:许可证	✓	✓	✗	✗	✗	✗	✗
环境配置:资产设置	✓	✓	✓	✗	✗	✗	✗
环境配置:隐藏资产	✓	✓	✓	✓-无还原	✓-无还原	✓	✓-无还原
环境配置:自定义字段	✓	✓	✓	✗	✗	✗	✗
环境配置:事件群集	✓	✓	✓	✗	✗	✗	✗
环境配置:PACP 播放器	✓	✓	✓	✗	✗	✗	✗
用户和角色:用户设置	✓	✓	✓	✗	✗	✗	✗
用户和角色:本地用户	✓	✗	✗	✗	✗	✗	✗

用户和角色：用户组	✓	✗	✗	✗	✗	✗	✗
用户和角色：Active Directory	✓	✗	✗	✗	✗	✗	✗
集成	✓	✓	✗	✗	✗	✗	✗
服务器	✓	✓	✓	✓（无操作）	✓（无操作）	✓（无操作）	✓（无操作）
系统操作	✓	✓无恢复出厂设置	✓仅备份和诊断	✓仅诊断	✗	✗	✗
系统日志	✓	✓	✓	✓	✓	✓	✓无系统日志
启用（设置时和禁用后）	✓	✓	✗	✗	✗	✗	✗
删除资产	✓	✓	✓	✗	✗	✗	✗

身份验证服务器

“**身份验证服务器**”页面显示与身份验证服务器的现有集成。单击“**添加服务器**”按钮即可添加服务器。



Active Directory

您可以将 OT Security 与贵组织的 Active Directory (AD) 集成。这将使用户可以使用其 Active Directory 凭据登录 OT Security。配置涉及建立集成，然后将 AD 中的组映射到 OT Security 中的用户组。

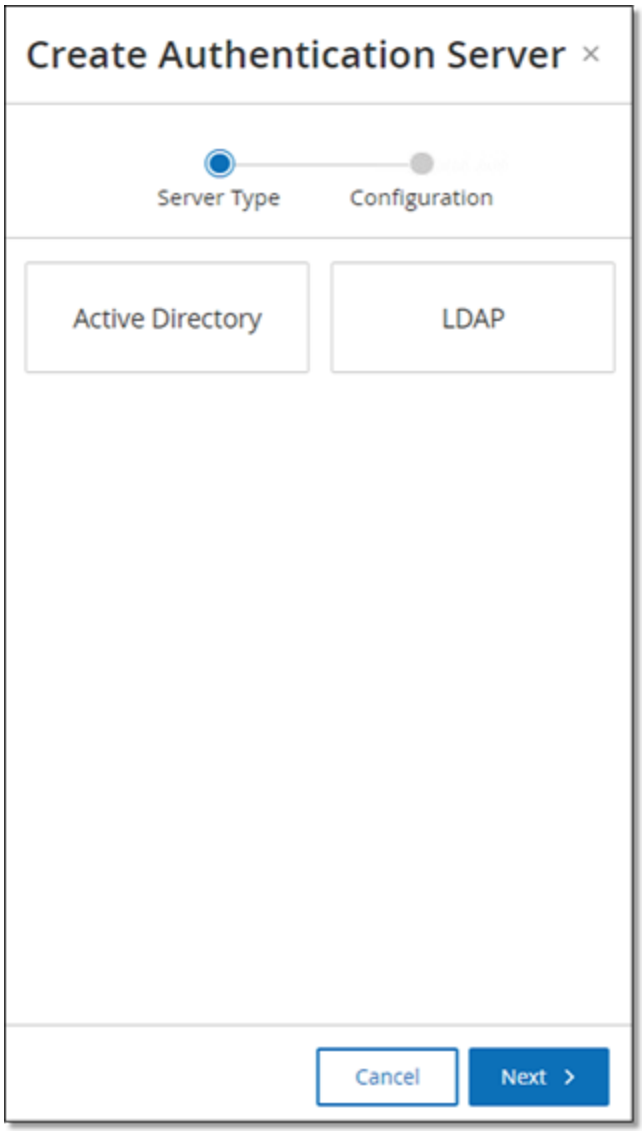
注意：系统随附一组与每个可用角色对应的预定义用户组，即**管理员用户组 > 管理员角色**、**站点操作员用户组 > 站点操作员角色**等。有关可用角色的说明，请参阅"身份验证服务器"。

若要配置 Active Directory，请执行以下操作：

1. 或者，从组织的 CA 或网络管理员处获取 CA 证书，并将其加载到本地计算机上。
2. 转至"**本地设置**">"**用户管理**">"**身份验证服务器**"。

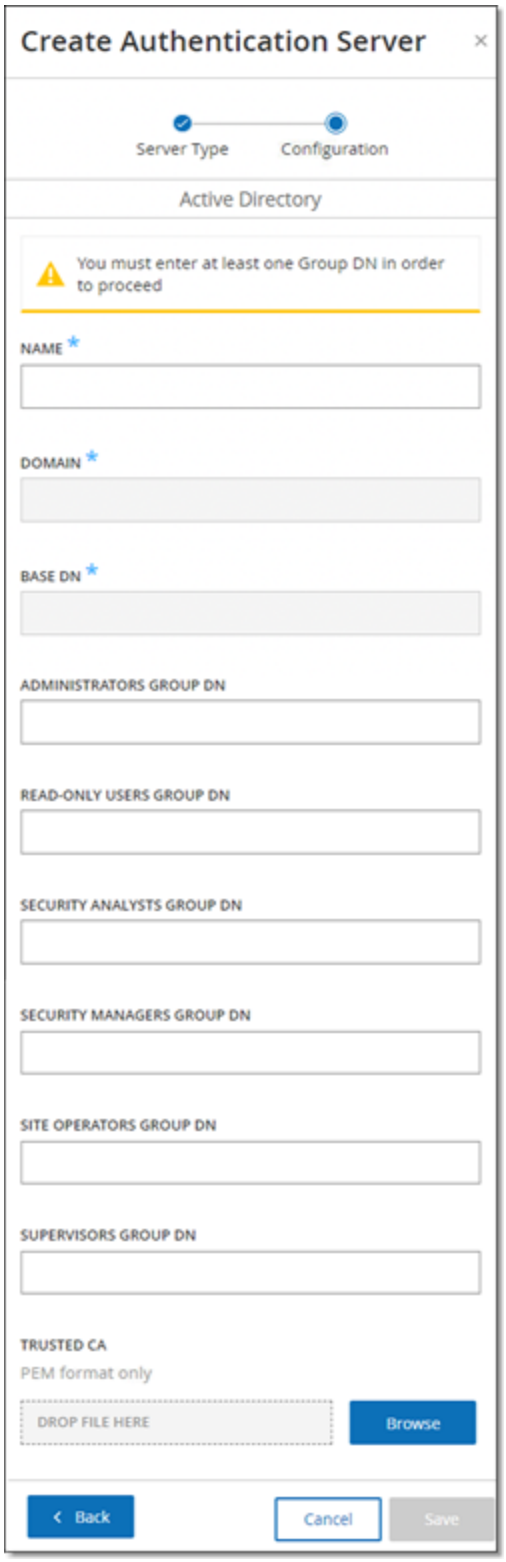
   此时会出现"**身份验证服务器**"窗口。
3. 单击"**添加服务器**"。

   此时会出现"**创建身份验证服务器**"面板，并显示"**服务器类型**"。



4. 点击“**Active Directory**”，然后点击“**下一步**”。

   此时会显示“**Active Directory**”配置窗格。



5. 在“**名称**”框中，输入要在登录屏幕中使用的名称。
6. 在“**域名**”框中，输入组织域名的 FQDN(例如 company.com) 。

注意：如果您不知道自己的域是什么，可通过在 Windows CMD 或命令行中输入"set"命令来查找。"USERDNSDOMAIN"属性的给定值即为域名。

7. 在"**基本 DN**"框中，输入域的可分辨名。此值的格式为"DC={second-level domain},DC={top-level domain}"(例如 DC=company,DC=com) 。

8. 对于要从 AD 组映射到 OT Security 用户组的每个组而言，在相应的方框中输入该 AD 组的 DN。

   例如，要向管理员用户组分配一组用户，请在"**管理员组 DN**"框中输入要为其分配管理员特权的 Active Directory 组的 DN。

   注意：如果不知道要为其分配 OT Security 特权的组的 DN，可通过在 Windows CMD 或命令行中输入命令"`dsquery group -name Users*`"，来查看在包含用户的 Active Directory 中配置的所有组的列表。应以与显示的格式相同的格式输入要分配的组名称(例如"CN=IT_Admins,OU=Groups,DC=Company,DC=Com") 。每个 DN 的结尾还必须包含基本 DN。

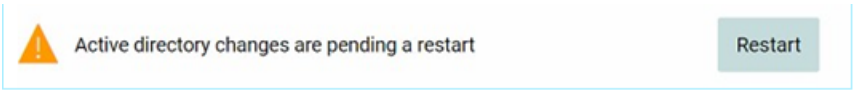
   注意：这些字段为可选字段。如果字段为空，则不会向该用户组分配 AD 用户。您可以设置不映射任何组的集成，但在这种情况下，除非添加至少一个组映射，否则任何用户都无法访问系统。

9. (可选) 在"**受信任的 CA**"部分，单击"**浏览**"并导航至包含贵组织的 CA 证书(从 CA 或网络管理员处获得) 的文件。

10. 选中"**启用 Active Directory**"复选框。

11. 单击"**保存**"。

    此时会出现一则信息，提示您需要重新启动设备才能激活 Active Directory。



12. 单击"**重新启动**"。

    设备会重新启动。重新启动时，OT Security 会激活 Active Directory 设置。分配到指定组的任何用户均可使用其组织凭据访问 OT Security 平台。

    注意：若要使用 Active Directory 登录，必须在登录页面输入用户主体名称 (UPN)。在某些情况下，这意味着只需在用户名后面加上 @<domain>.com 即可。

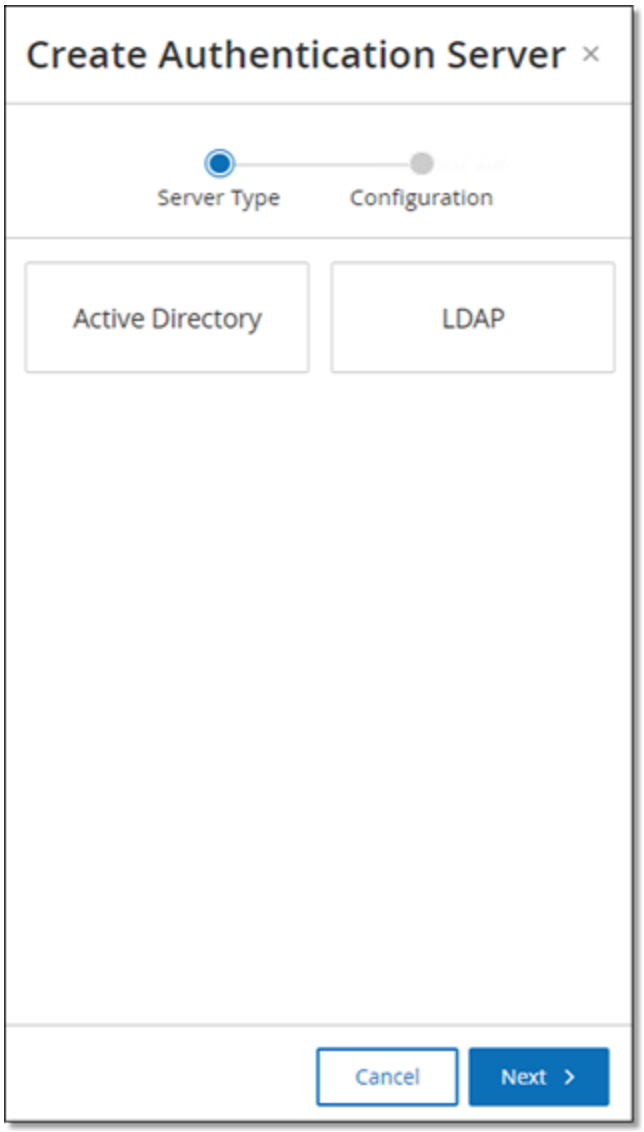
LDAP

您可以将 OT Security 与贵组织的 LDAP 集成。这使得用户可以使用 LDAP 凭据登录 OT Security。配置涉及建立集成，然后将 AD 中的组映射到 OT Security 中的用户组。

若要配置 LDAP，请执行以下操作：

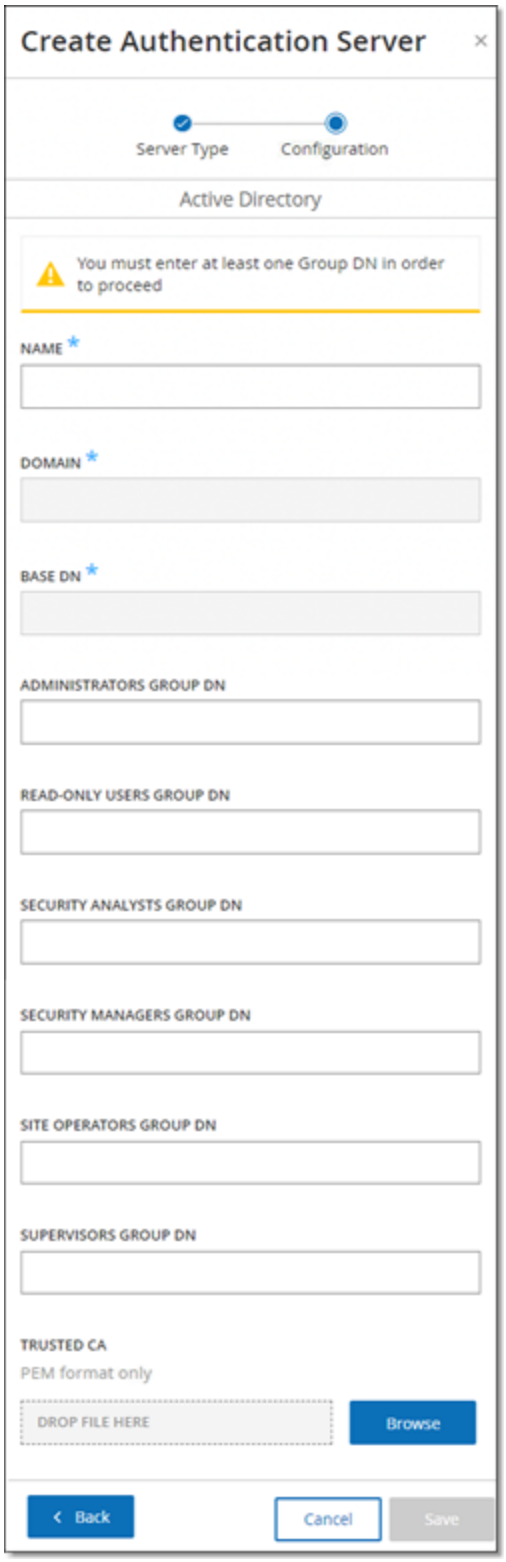
1. 转至“**本地设置**”>“**用户管理**”>“**身份验证服务器**”。
2. 单击“**添加服务器**”。

   此时会出现“**添加身份验证服务器**”面板，并显示“**服务器类型**”。



3. 选择“**LDAP**”，然后点击“**下一步**”。

   此时会出现“**LDAP 配置**”窗格。



4. 在“**名称**”框中，输入要在登录屏幕中使用的名称。

注意：登录名必须与众不同，并凸显其 LDAP 用途。如果同时配置了 LDAP 和 Active Directory，则只有通过登录名才能区分登录屏幕上的不同配置。

5. 在"**服务器**"框中，输入 FQDN 或登录地址。

   注意：如果使用安全连接，Tenable 建议使用 FQDN 而不是 IP 地址，以确保提供的安全证书得到验证。

   注意：如果使用主机名，其必须在 OT Security 系统的 DNS 服务器列表中。请参阅"系统配置">"设备"。

6. 在"**端口**"框中，输入 389 以使用非安全连接，或输入 636 以使用安全 SSL 连接。

   注意：如果选择端口 636，则需要提供证书才能完成集成。

7. 在"**用户 DN**"框中，以 DN 格式输入带参数的 DN(例如，服务器名称可以为 AD_1.qa.com，用户 DN 可以为 CN=Administrator,CN=Users,DC=qa,DC=com) 。

8. 在"**密码**"框中，输入用户 DN 的密码。

   注意：只有当前的用户 DN 密码有效时，针对 LDAP 的 OT Security 配置才能继续正常发挥作用。因此，如果用户 DN 密码更改或过期，还必须更新 OT Security 配置。

9. 在"**用户基本 DN**"框中，输入 DN 格式的基本域名。例如，DC=qa,DC=com。

10. 在"**组基本 DN**"框中，输入 DN 格式的组基本域名。

11. 在"**域附加**"框中，输入在用户未应用其所属域时将附加到身份验证请求的默认域。

12. 在相关组名称框中，输入供用户为 LDAP 配置使用的 Tenable 组名称。

13. 如果要针对配置使用端口 636，请单击"**受信任的 CA**"下的"**浏览**"，然后导航至有效的 PEM 证书文件。

14. 单击"**保存**"。

    OT Security 以**禁用**模式启动服务器。

15. 要应用配置，单击切换开关至"**打开**"。

    此时会出现"**系统重新启动**"对话框。

16. 单击“**立即重新启动**”以立即重新启动并应用配置，或单击“**稍后重新启动**”以在没有新配置的情况下暂时继续使用系统。

> **注意**：系统重新启动后，LDAP 配置才能完成启用/禁用。如果不立即重新启动系统，请在做好重新启动准备时单击屏幕顶部标题栏上的“**重新启动**”按钮。

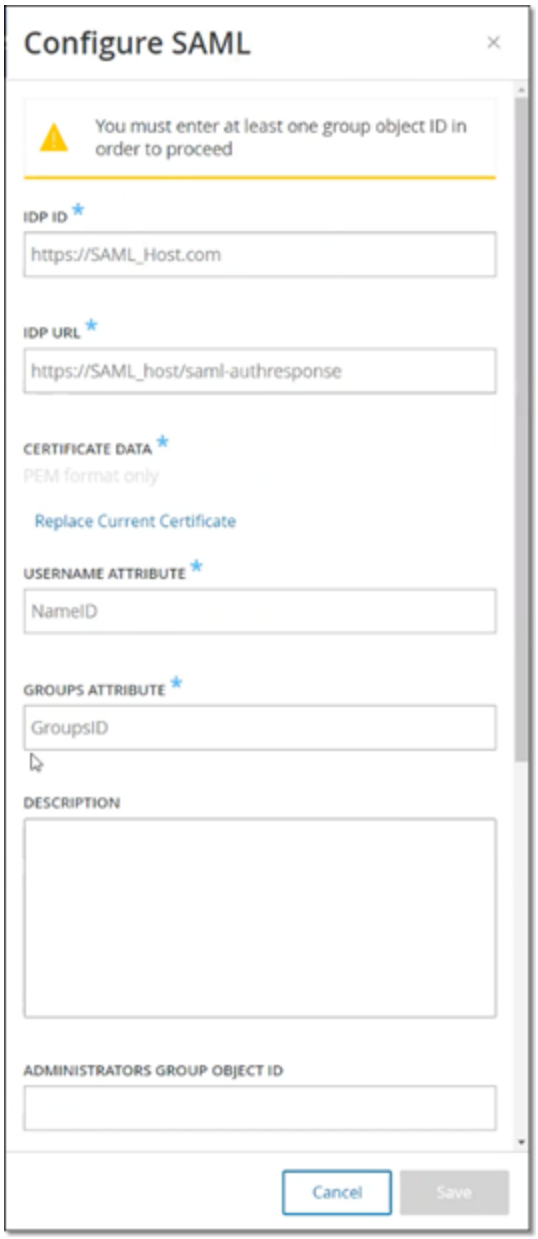
SAML

您可以将 OT Security 与组织的身份提供程序(例如 Microsoft Azure) 集成，以便用户能够使用其身份提供程序进行身份验证。配置涉及以下操作：通过在身份提供程序内创建 OT Security 应用程序来建立集成、输入有关所创建的 OT Security 应用程序的信息、将身份提供程序的证书上传到 OT Security **SAML** 页面，以及将身份提供程序中的组映射到 OT Security 中的用户组。有关将 OT Security 与 Microsoft Azure 集成的详细教程，请参阅"附录 2：Microsoft Entra ID 的 SAML 集成"

若要配置 SAML，请执行以下操作：

1. 转至"**本地设置**">"**用户管理**">"**SAML**"。
2. 单击"**配置**"。

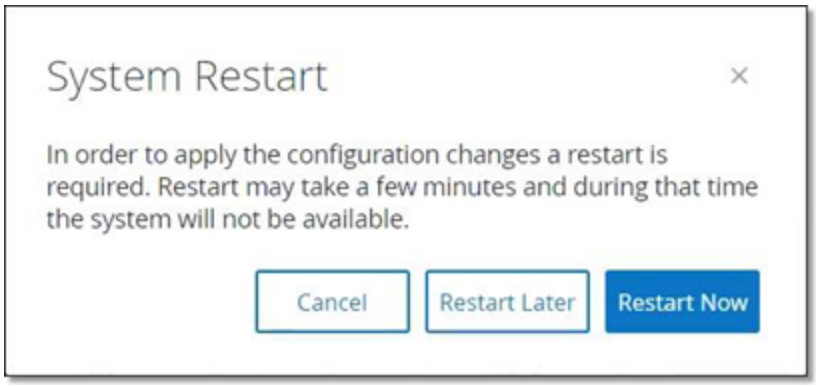
   此时会出现"**配置 SAML**"面板。



3. 在“**IDP ID**”框中，输入 OT Security 应用程序的身份提供程序 ID。
4. 在“**IDP URL**”框中，输入 OT Security 应用程序的身份提供程序 URL。
5. 在“**证书数据**”中，单击“**将文件拖放至此处**”，导航至您下载的用于 OT Security 应用程序的“身份提供程序的证书”文件并将其打开。
6. 在“**用户名属性**”框中，输入身份提供程序为 OT Security 应用程序提供的用户名属性。
7. 在“**组属性**”框中，输入身份提供程序为 OT Security 应用程序提供的组属性。

8. (可选)在"**描述**"框中,输入对查询的描述。
9. 对于要配置的每个组映射,访问身份提供程序为用户组提供的**组对象 ID**,并将其输入到所需的"**组对象 ID**"字段中,以将其映射到所需的 OT Security 用户组。
10. 单击"**保存**"以保存操作并关闭侧面板。
11. 在"**SAML**"窗口中,单击"**SAML 单点登录**"切换开关以启用单点登录。

    此时会显示"**系统重新启动**"通知窗口。



12. 单击"**立即重新启动**"以重新启动系统并立即应用 SAML 配置,或单击"**稍后重新启动**"以将应用 SAML 配置延迟到下次系统重新启动时。如果您选择稍后重新启动,OT Security 会在重新启动完成之前一直显示标题栏:

    重新启动后,设置将被激活,分配到指定组的任何用户都可以使用其身份提供程序凭据访问 OT Security 平台。

集成

您可以与其他受支持的平台建立集成，以便 OT Security 与其他网络安全平台同步。

Tenable 产品

您可以将 OT Security 与 Tenable Security Center 和 Tenable Vulnerability Management 集成。OT Security 通过这些集成与其他平台共享数据。同步后的数据包括 OT 漏洞，以及从 OT Security 启动的 IT 类型 Tenable Nessus 扫描发现的数据。

注意：OT Security 不会通过集成将"**隐藏**"资产的数据发送到 Tenable Security Center 和 Tenable Vulnerability Management。

注意：若要集成平台，OT Security 必须能够通过端口 443 访问 Tenable Security Center 和/或 Tenable Vulnerability Management。Tenable 建议您在 Tenable Security Center 和/或 Tenable Vulnerability Management 上创建特定用户以用作 OT Security 的集成用户。

Tenable Security Center

要集成 Tenable Security Center，请在 Tenable Security Center 中创建“**通用存储库**”，以存储 OT Security 数据并记录存储库 ID。有关更多信息，请参阅“通用存储库”。

注意：Tenable 建议在 Tenable Security Center 上创建特定用户，用于与 OT Security 集成。用户应拥有安全管理员/安全分析师或漏洞分析师角色，并被分配到“完全访问权限”组。

要集成 Tenable Security Center，请执行以下操作：

1. 转到“**本地设置**”>“**集成**”。

   将出现“**集成**”页面。

2. 单击右上角的“**添加集成模块**”。

   将出现“**添加集成模块**”面板。

3. 在“**模块类型**”部分中，选择 Tenable Security Center。

4. 单击“**下一步**”。

   包含相关字段的“**模块定义**”面板随即出现。

5. 在“**主机名/IP**”框中，输入 Tenable Security Center 的主机名或 IP。

6. 在“**用户名**”框中，输入帐户用户 ID。

7. 在“**密码**”框中，输入帐户密码。

8. 在“**存储库 ID**”中，提供通用存储库 ID。

9. 在“**同步频率**”下拉框中，设置同步数据的频率。

10. 单击“**保存**”。

    OT Security 创建集成并在“集成”页面上显示新的集成。

11. 右键单击新的集成，然后单击“**同步**”。

Tenable Vulnerability Management

注意：您需要先在 Tenable Vulnerability Management 控制台中生成一个 API 密钥（“**设置**”>“**我的帐户**”>“**API 密钥**”>“**生成**”）。系统会提供一个**访问密钥**和一个**密钥**，请在配置集成时将其输入 OT Security 控制台。

要集成 Tenable Vulnerability Management，请执行以下操作：

1. 转到“**本地设置**”>“**集成**”。

   将出现“**集成**”页面。

2. 单击右上角的“**添加集成模块**”。

   将出现“**添加集成模块**”面板。

3. 在“**模块类型**”部分中，选择 Tenable Vulnerability Management。

4. 单击“**下一步**”。

   包含相关字段的“**模块定义**”面板随即出现。

5. 在“**访问密钥**”框中，提供访问密钥。

6. 在“**密钥**”框中，提供密钥。

7. 在“**同步频率**”下拉框中，选择同步数据的频率。

Palo Alto Networks：新一代防火墙

可以与 Palo Alto 系统共享 OT Security 发现的资产清单信息。

若要将 OT Security 与 Palo Alto Networks 新一代防火墙 (NGFW) 集成，请执行以下操作：

1. 转到“**本地设置**”>“**集成**”。

   将出现“**集成**”页面。

2. 单击右上角的“**添加集成模块**”。

   将出现“**添加集成模块**”面板。

3. 在“**模块类型**”部分中，选择 Palo Alto Networks NGFW。

4. 单击“**下一步**”。

5. 在“**主机名/IP**”框中，输入 Palo Alto NGFW 帐户的主机名或 IP 地址。

6. 在“**用户名**”框中，输入 NGFW 帐户的用户名。

7. 在“**密码**”框中，输入 NGFW 帐户的密码。

8. 单击“**保存**”。

   OT Security 会保存集成。

Aruba: ClearPass 策略管理器

可以与 Aruba 系统共享 OT Security 发现的资产清单信息。

若要将 OT Security 与 Aruba ClearPass 帐户集成，请执行以下操作：

1. 转到"**本地设置**">"**集成**"。

   将出现"**集成**"页面。

2. 单击右上角的"**添加集成模块**"。

   将出现"**添加集成模块**"面板。

3. 在"**模块类型**"部分中，选择 Aruba Networks ClearPass。

4. 单击"**下一步**"。

5. 在"**主机名/IP**"框中，输入 Aruba Networks ClearPass 帐户的主机名或 IP 地址。

6. 在"**用户名**"框中，输入 Aruba Networks ClearPass 帐户的用户名。

7. 在"**密码**"框中，输入 Aruba Networks ClearPass 帐户的密码。

8. 在"**客户端 ID**"框中，输入 Aruba Networks ClearPass 帐户的客户端 ID。

9. 在"**API 客户端密钥**"框中，输入 Aruba ClearPass 帐户的 API 客户端密钥。

10. 单击"**保存**"。

    OT Security 会保存集成。

服务器

您可以在系统中设置 SMTP 服务器和 Syslog 服务器，以启用要通过电子邮件发送和/或在 SIEM 上记录的事件通知。您也可以设置 FortiGate 防火墙，以根据 OT Security 网络事件向 FortiGate 发送防火墙策略建议。

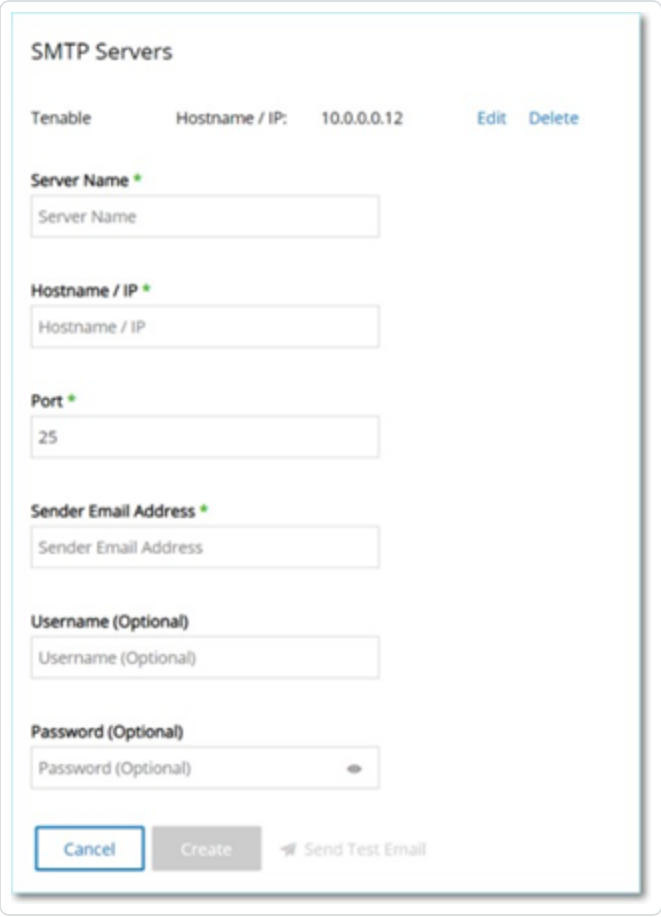
SMTP 服务器

为了能够通过电子邮件向相关方发送事件通知，需要在系统中设置 SMTP 服务器。如果不设置 SMTP 服务器，那么无论事件何时生成，系统都无法发出电子邮件通知。在任何情况下都可以在管理控制台（用户界面）的“**事件**”屏幕上查看所有事件。

若要设置 SMTP 服务器，请执行以下操作：

1. 转至“**本地设置**”>“**服务器**”>“**SMTP 服务器**”。
2. 单击“**添加 SMTP 服务器**”。

   此时会出现“**SMTP 服务器**”配置窗口。



3. 在“**服务器名称**”框中，输入要用于发送电子邮件通知的 SMTP 服务器的名称。
4. 在“**主机名\IP**”框中，输入 SMTP 服务器的主机名或 IP 地址。

5. 在“**端口**”框中，输入 SMTP 服务器将在其上监听事件的端口号（默认值：25）。
6. 在“**发件人电子邮件地址**”框中，输入显示为事件通知电子邮件发件人的电子邮件地址。
7. （可选）在“**用户名**”和“**密码**”框中，输入将用于访问 SMTP 服务器的用户名和密码。
8. 如要发送测试电子邮件以验证配置是否成功，请点击“**发送测试电子邮件**”，然后输入要发送到的电子邮件地址，并检查收件箱是否收到了电子邮件。如果电子邮件未送达，则故障排除以发现问题的原因并予以修正。
9. 单击“**保存**”。

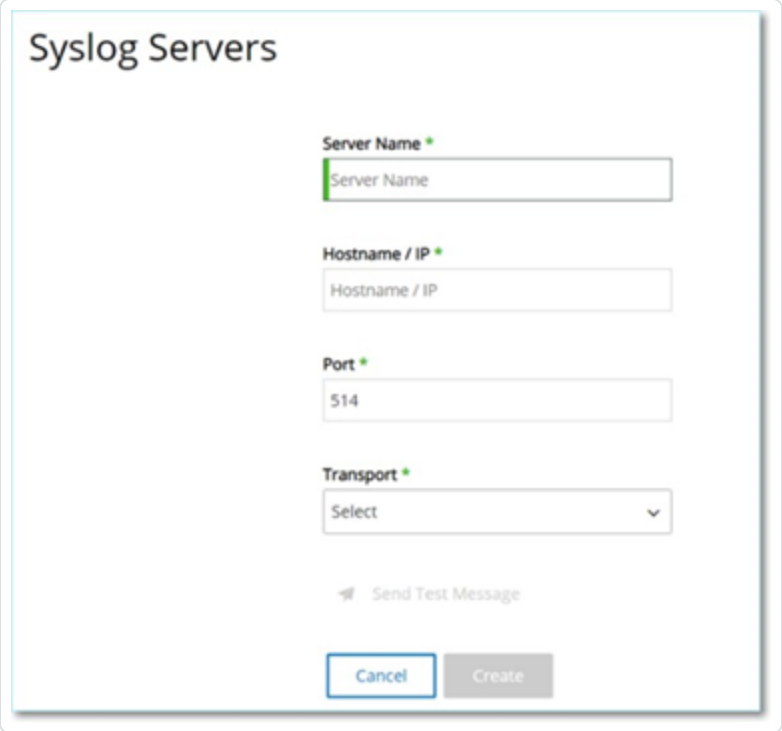
   您可以通过重复此过程来设置其他 SMTP 服务器。

Syslog 服务器

为了在外部服务器上启用日志事件收集，您需要在系统中设置 Syslog 服务器。如果不想设置 Syslog 服务器，则事件日志将仅保存在 OT Security 平台上。

若要设置 Syslog 服务器，请执行以下操作：

1. 转至“**本地设置**”>“**服务器**”>“**Syslog 服务器**”。
2. 单击“**+ 添加 Syslog 服务器**”。此时会出现“**Syslog 服务器**”配置窗口。



3. 在“**服务器名称**”框中，输入要用于记录系统事件的 Syslog 服务器的名称。
4. 在“**主机名\IP**”框中，输入 Syslog 服务器的主机名或 IP 地址。
5. 在“**端口**”框中，输入要向该 Syslog 服务器发送事件的服务器上的端口号。默认：514
6. 在“**传输**”下拉框中，选择要使用的传输协议。选项为 TCP 或 UDP。
7. 如要发送测试消息以验证配置是否成功，请单击“**发送测试消息**”，然后检查消息是否送达。如果消息未送达，则故障排除以发现问题的原因并予以修正。

8. 单击“**保存**”。

   您可以通过重复此过程来设置其他 Syslog 服务器。

FortiGate 防火墙

若要设置 FortiGate 服务器，请执行以下操作：

1. 前往“**本地设置**”>“**服务器**”>“**FortiGate 防火墙**”。
2. 点击“**添加防火墙**”。

   此时会显示“**添加 FortiGate 防火墙**”配置窗口。

3. 在“**服务器名称**”框中，输入要使用的 FortiGate 服务器的名称。
4. 在“**主机名\IP**”框中，输入 FortiGate 服务器的主机名或 IP 地址。
5. 在“**API 密钥**”框中，输入从 FortiGate 生成的“API 标记”。

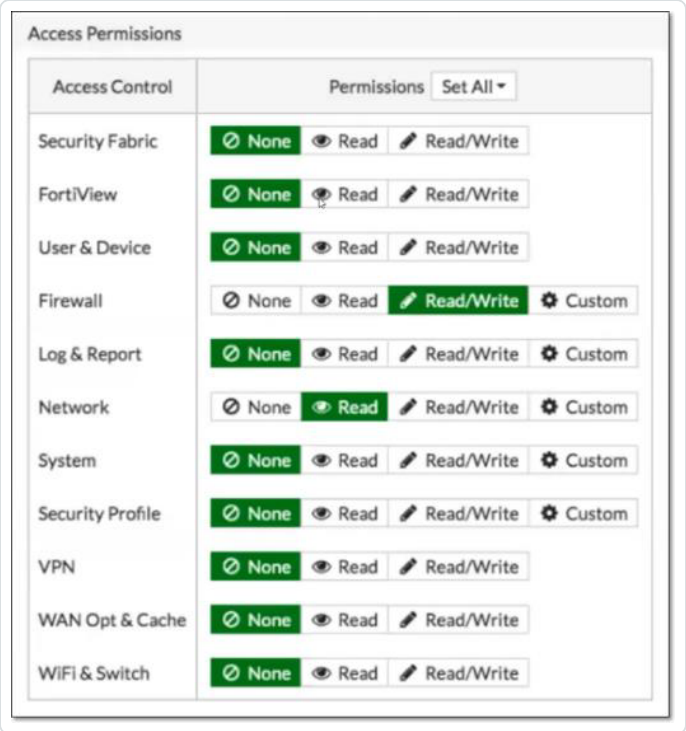
   注意：有关生成 FortiGate API 标记的说明，请参阅以下页面：https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token。

6. 单击“**添加**”。

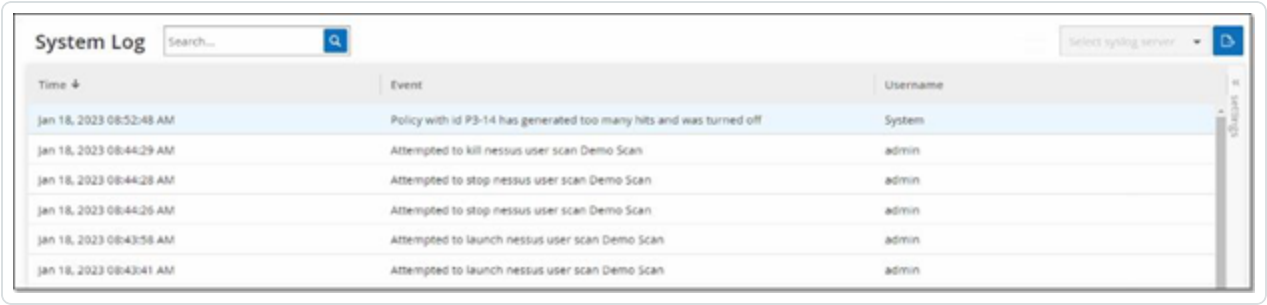
   OT Security 会创建 FortiGate 防火墙服务器。

注意:对于源地址(确保仅可通过受信任的主机使用 API 标记所需的地址),请使用 OT Security 装置 IP 地址。

为 OT Security 创建管理员配置文件时,确保根据以下设置应用访问权限:



系统日志



"**系统日志**"屏幕显示系统中发生的所有系统事件(例如策略已打开、策略已编辑、事件已解析等)的列表。此日志既包括用户发起的事件,也包括自动发生的系统事件(例如由于点击次数过多,导致策略自动关闭)。此日志不包括"**事件**"屏幕上显示的策略生成的事件。您可以将日志作为 CSV 文件导出。还可以配置系统以将系统日志事件发送到 Syslog 服务器。

每个记录的事件都包含以下详细信息:

参数	描述
时间	事件发生的时间和日期。
事件	所发生事件的简短说明。
用户名	发起事件的用户的名称。对于自动发生的事件,不提供用户名。

将系统日志发送到 Syslog 服务器

若要将系统配置为向 Syslog 服务器发送系统事件，请执行以下操作：

1. 转至“**本地设置**”>“**系统日志**”。
2. 点击右上角的下拉框以显示服务器列表。

   注意：如要添加 Syslog 服务器，请参阅“Syslog 服务器”。

3. 选择所需的服务器。

   OT Security 将系统日志事件发送到指定的 Syslog 服务器。

附录 1：安装传感器（3.13 及更低版本）

以下程序说明了配置传感器 3.13 及更低版本的完整流程。一些初始步骤同样适用于新的传感器。但是，安装向导已被传感器配对中所述的配对程序所取代。

第 1 步：设置传感器

安装传感器硬件。有关设置传感器的说明，请参阅“设置传感器”。

第 2 步：将传感器连接到网络

将传感器连接到网络交换机。有关将传感器连接到网络的说明，请参阅“将传感器连接到网络”。

第 3 步：访问传感器设置向导

使用传感器自身的静态 IPv4 地址访问传感器。有关如何设置静态 IP 的说明，请参阅“访问传感器设置向导”。

第 4 步:传感器安装向导

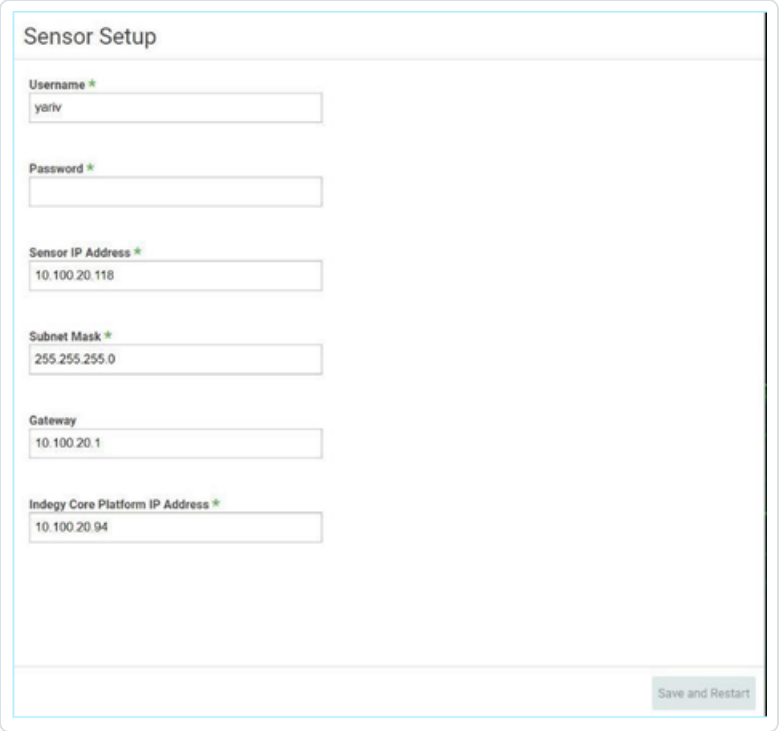
OT Security 安装向导将引导您完成配置基本系统设置的过程。

注意:若想稍后更改配置,可以在管理控制台 (UI) 的"**设置**"屏幕上执行此操作。

若要设置传感器,请执行以下操作:

1. 在欢迎屏幕上,单击"**开始设置**"。

   此时会显示"设置"屏幕。

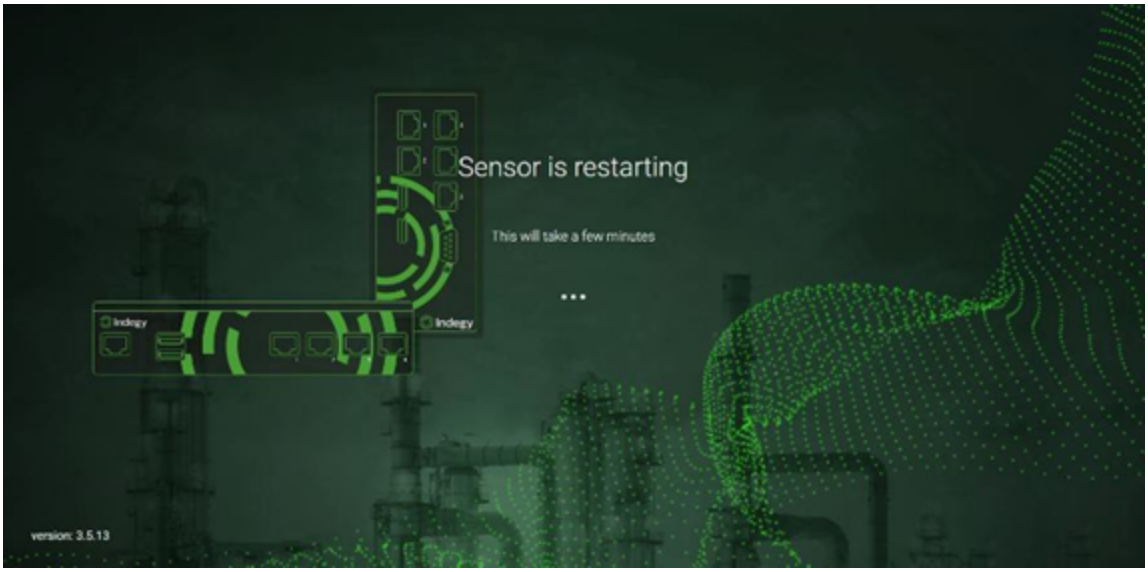


2. 在"**用户名**"字段中,输入用于登录系统的用户名。用户名最多可包含 12 个字符,且只能包含小写字母和数字。
3. 在"**密码**"字段中,输入用于登录系统的密码。该密码必须至少包含:
   - 12 个字符
   - 一个大写字母
   - 一个小写字母

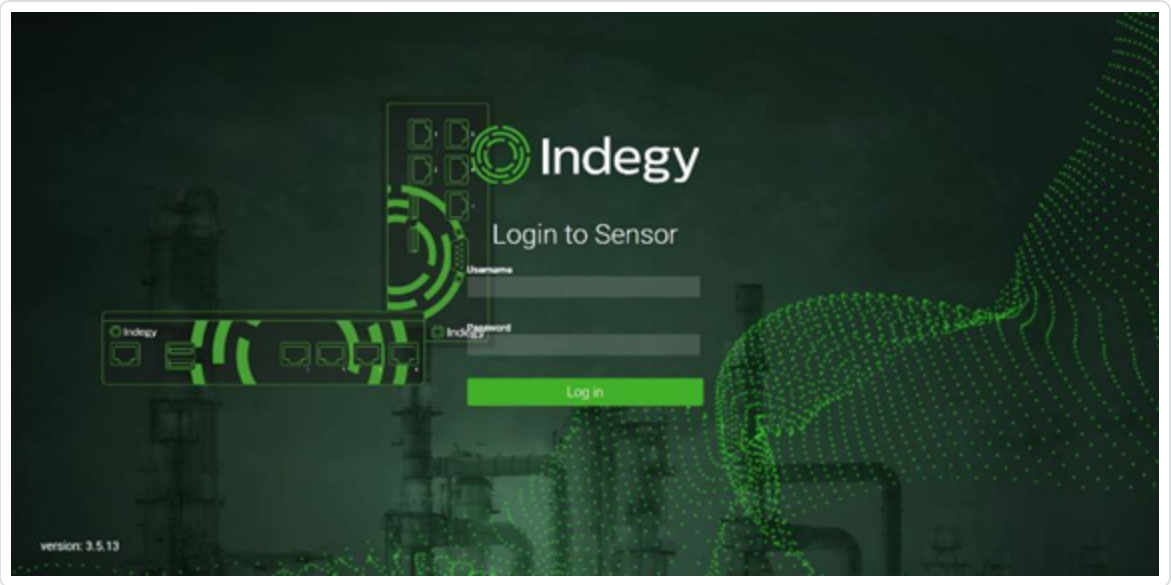
- 一个数字
- 一个特殊字符

4. 在“**重新输入密码**”字段中，重新输入相同的密码。
5. 在“**传感器 IP 地址**”字段中，输入应用于 OT Security 传感器 传感器的 IP 地址（在网络子网内）。强烈建议更改默认 IP 地址。
6. 在“**子网掩码**”字段中，输入网络的子网掩码。
7. 如果要设置网关（可选），请在“**网关**”字段中输入网络的网关 IP。
8. 在“**IP 地址**”字段中，输入 OT Security 平台的 IP 地址。
9. 单击“**保存并重新启动**”。

   传感器将执行重新启动：



10. 在重新启动过程之后，系统会将网络流量转发到 OT Security 平台。若要修改配置，可使用已配置的 IP 地址和已配置的凭据登录传感器：



附录 2：Microsoft Entra ID 的 SAML 集成

OT Security 支持按照 SAML 协议与 Microsoft Entra ID 集成。因此，分配到 OT Security 的 Azure 用户能够通过 SSO 登录 OT Security。您可以根据用户在 Azure 中被分配到的组使用组映射在 OT Security 中分配角色。

建立集成

此部分说明针对 OT Security 与 Microsoft Entra ID 的集成设置单点登录 (SSO) 的完整流程。配置涉及以下操作：通过在身份提供程序内在 Microsoft Entra ID 中创建 OT Security 应用程序来建立集成、输入有关所创建的 OT Security 应用程序的信息、将身份提供程序的证书上传到 OT Security SAML 页面，以及将身份提供程序中的组映射到 OT Security 中的用户组。

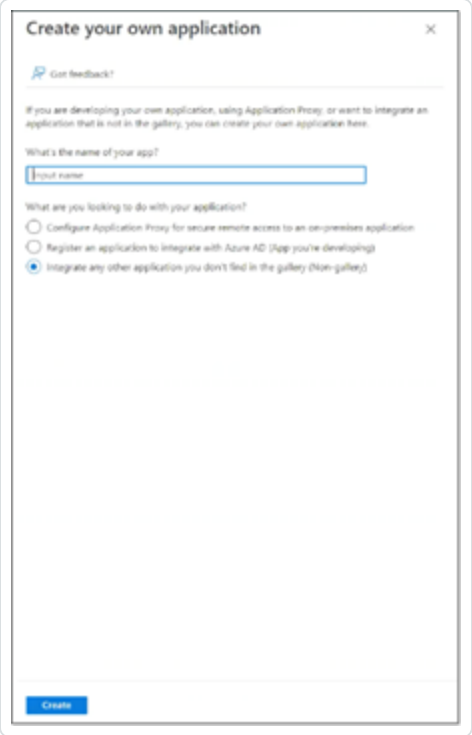
要设置配置，需要以管理员用户的身份登录 Microsoft Entra ID 和 OT Security。

第 1 步：在 Microsoft Entra ID 中创建 Tenable 应用程序

若要在 Microsoft Entra ID 中创建 Tenable 应用程序，请执行以下操作：

1. 在 Microsoft Entra ID 中，转至“Microsoft Entra ID”>“**Enterprise 应用程序**”，单击“**+ 新建应用程序**”会显示“**浏览 Microsoft Entra ID Gallery**”，然后单击“**+ 创建专属应用程序**”。

   随后将显示“**创建专属应用程序**”侧面板。

2. 在“**应用程序的名称是什么？**”字段中，输入应用程序的名称（例如 Tenable_OT）并选择“**集成库中未找到的任何其他应用程序（非库）**”（默认选中），然后单击“**创建**”以添加应用程序。

第 2 步：初始配置

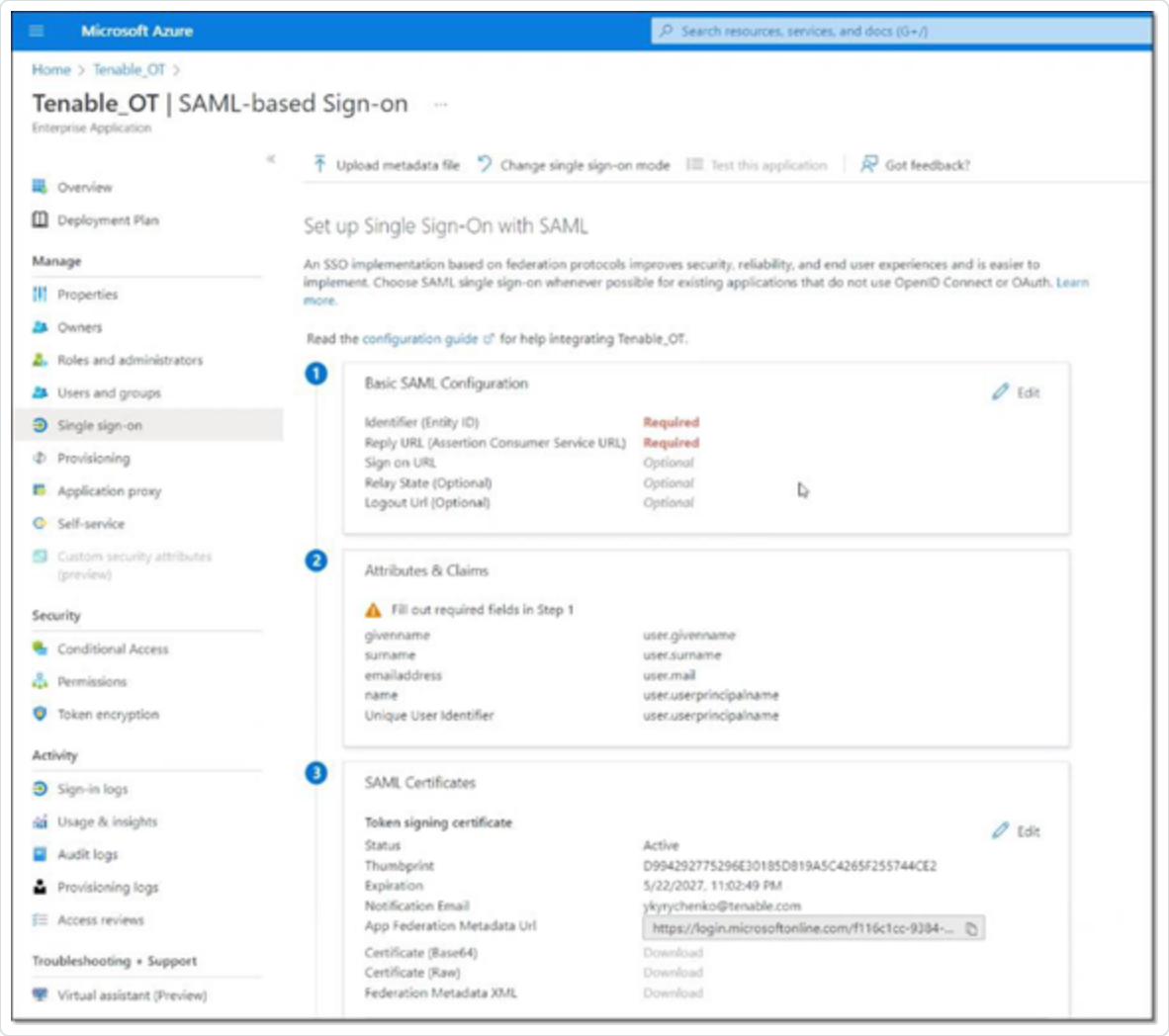
此步骤是在 Azure 中完成 OT Security 应用程序的初始配置，包括为基本 SAML 配置值标识符和回复 URL 创建临时值，以便下载所需证书。

注意：仅此程序中的指定字段为必须配置的内容。其他字段可保留其默认值。

若要进行初始配置，请执行以下操作：

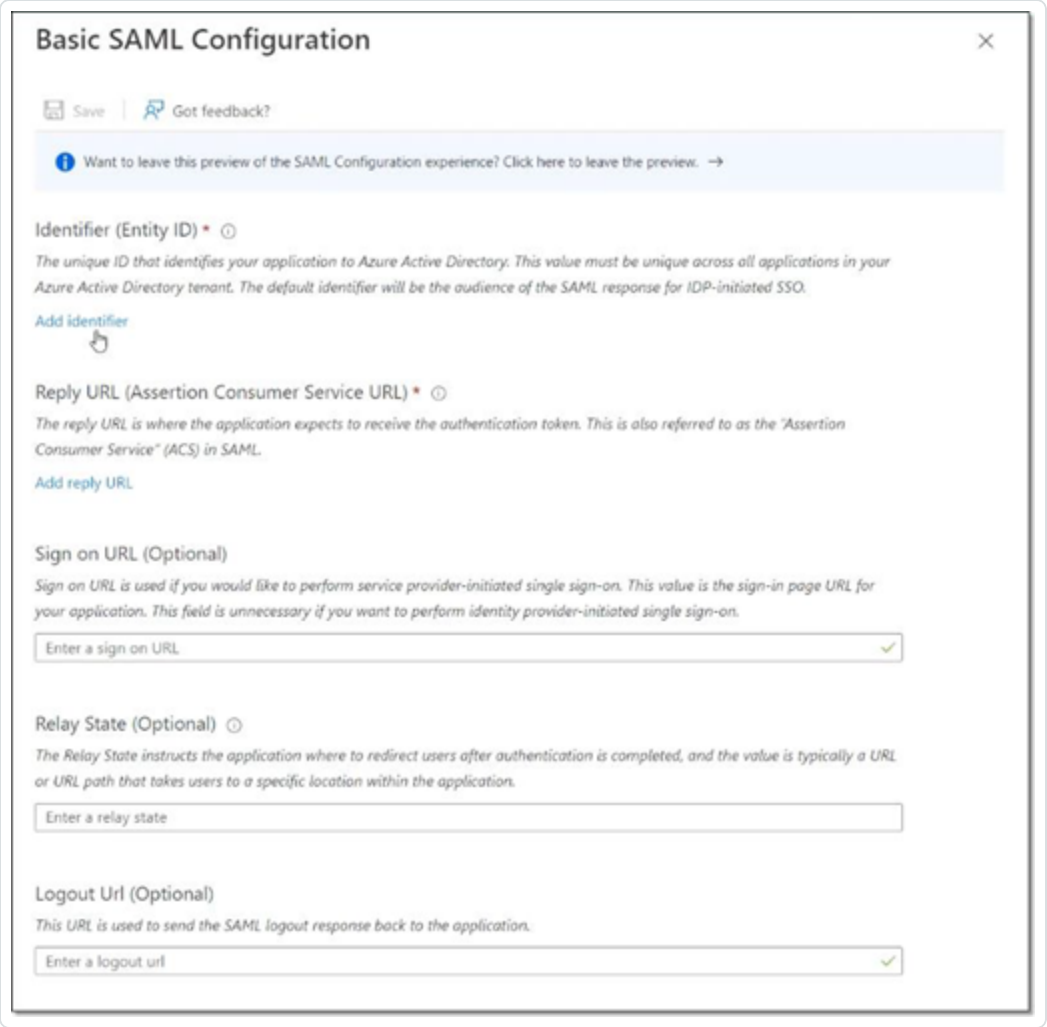
1. 在“Microsoft Entra ID”导航菜单中，单击“**单点登录**”，然后选择“SAML”作为单点登录方法。

   此时会显示“**基于 SAML 的登录**”屏幕。



2. 在第 1 部分(**基本 SAML 配置**) 中，单击编辑 。

   此时会显示“**基本 SAML 配置**”侧面板。



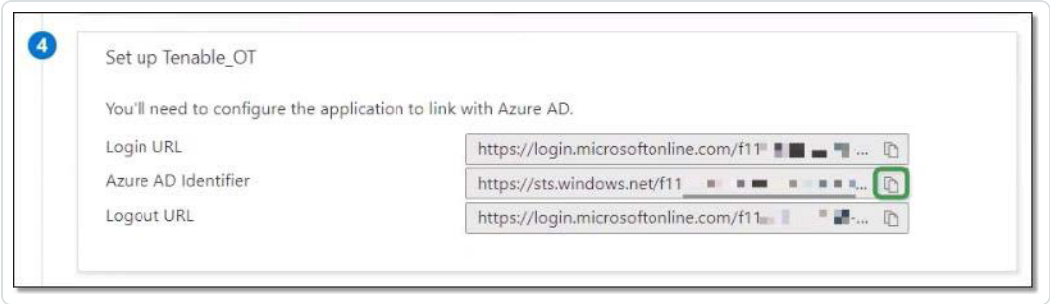
3. 在“**标识符(实体 ID)**”字段中，输入 Tenable 应用程序的临时 ID(例如，tenable_ot) 。

4. 在“**回复 URL(断言消费者服务 URL)**”字段中，输入有效的 URL(例如，https://OT Security) 。

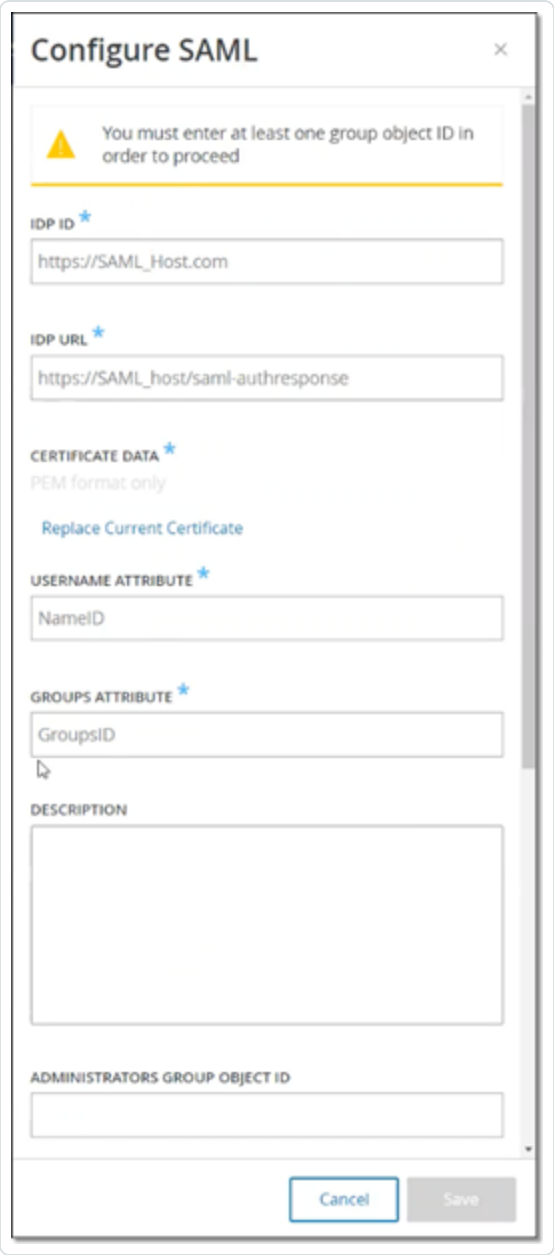
   > **注意**：标识符和回复 URL 将在稍后的配置过程中发生更改。

5. 单击“**保存**”以保存临时值并关闭“**基本 SAML 配置**”侧面板。

6. 在第 4 部分(**设置**) ，单击“**复制**”图标以复制 **Microsoft Entra ID 标识符**。

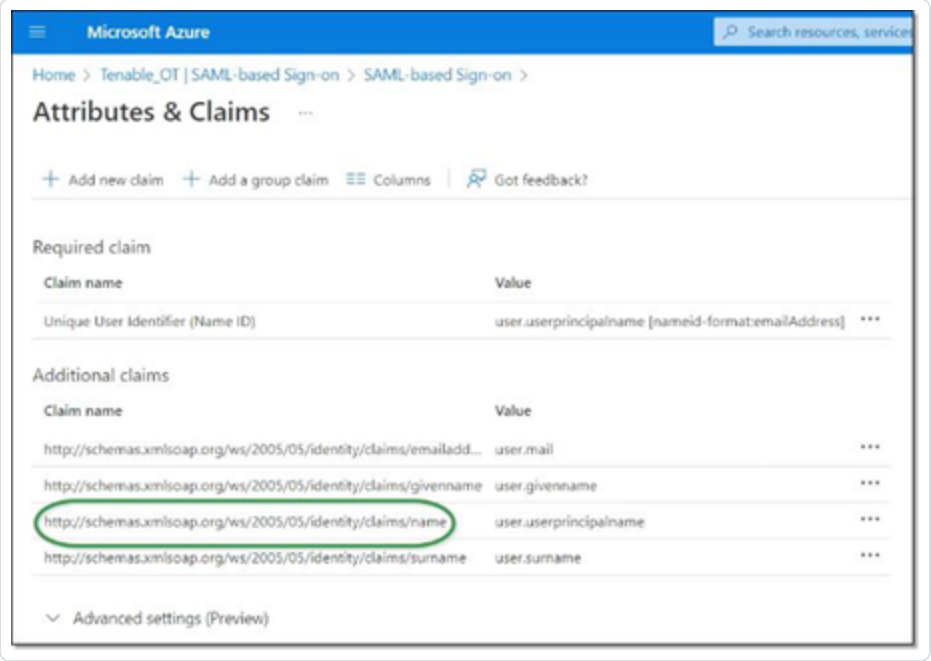


7. 切换到 OT Security 控制台，然后转至“**用户和角色**”>“**SAML**”。
8. 单击“**配置**”以显示“**配置 SAML**”侧面板，并将复制的值粘贴到“**IDP ID**”字段中。



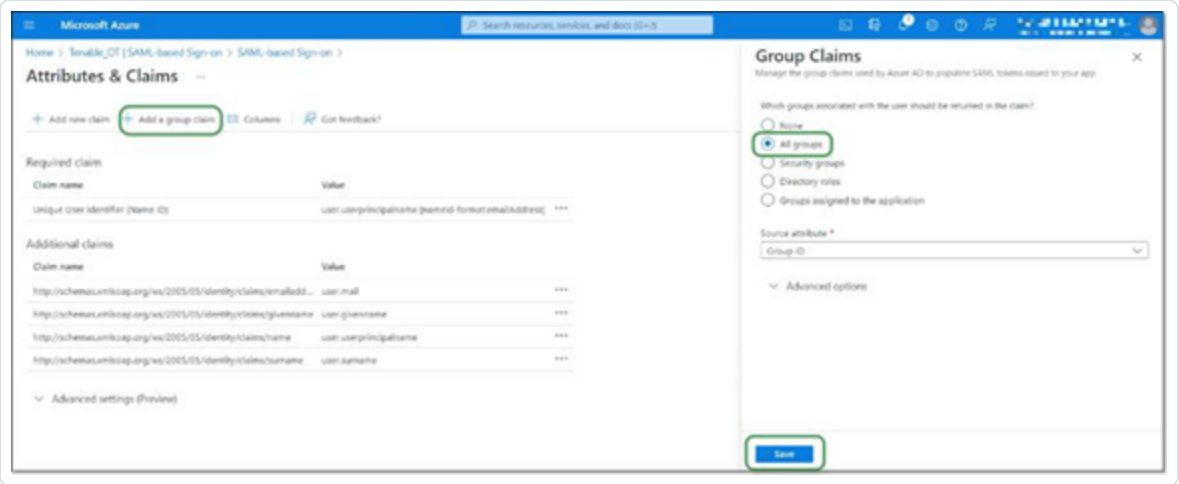
9. 在 **Azure** 控制台中，单击图标以复制**登录 URL**。
10. 返回 **OT Security** 控制台并将复制的值粘贴到“**IDP URL**”字段中。
11. 在 **Azure** 控制台的第 3 部分（**SAML 证书**）中，对于**证书 (Base64)**，单击“**下载**”。
12. 返回 **OT Security** 控制台，在“**证书数据**”下，单击“**浏览**”，导航至安全证书文件并选中。
13. 在 **Azure** 控制台的第 2 部分（**属性和声明**）中，单击“ **编辑**”。

14. 在“**其他声明**”下，选择并复制与值 **user.userprincipalname** 对应的**声明名称** URL。



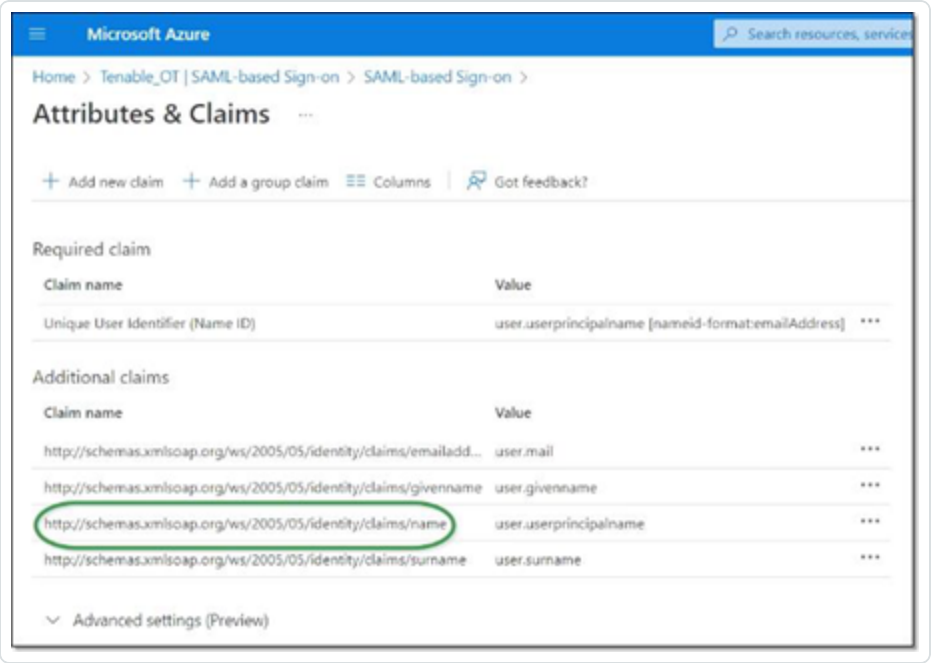
15. 返回 **Tenable** 控制台并将此 URL 粘贴到“**用户名属性**”字段中。

16. 在 Azure 控制台中，单击“**+ 添加组声明**”以显示“**组声明**”侧面板，然后在“**声明中应返回哪些与此用户关联的组？**”下，选择“**所有组**”并单击“**保存**”。



注意：如果在 Microsoft Azure 中启用了组设置，可选择“分配给应用程序的组”而不是“所有组”，并且 Azure 仅会提供分配给应用程序的用户组。

17. 在“**其他声明**”下，突出显示并复制与值 user.groups [All] 关联的**声明名称** URL。



18. 返回 **Tenable** 控制台并将复制的 URL 粘贴到“**组属性**”字段中。
19. 如果要添加关于 SAML 配置的说明，请在“**说明**”字段中输入。

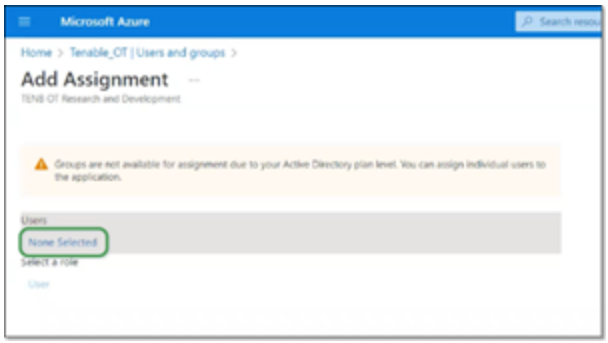
第 3 步：将 Azure 用户映射到 Tenable 组

在此步骤中，Microsoft Entra ID 用户会被分配到 OT Security 应用程序。如需对可授予每个用户的权限作出指定，请在用户分配到的 Azure 组与预定义的 OT Security 用户组（拥有关联的角色和一组权限）之间进行映射操作。OT Security 预定义的用户组为：管理员、只读用户、安全分析师、安全经理、站点操作员和主管。有关更多信息，请参阅“用户和角色”。必须为每个 Azure 用户至少分配一个映射至 OT Security 用户组的组。

注意：通过 SAML 登录的管理员用户被视为管理员（外部）用户，且未被授予本地管理员的所有权限。分配到多个用户组的用户可能被授予最高的组权限。

若要将 Azure 用户映射到 OT Security，请执行以下操作：

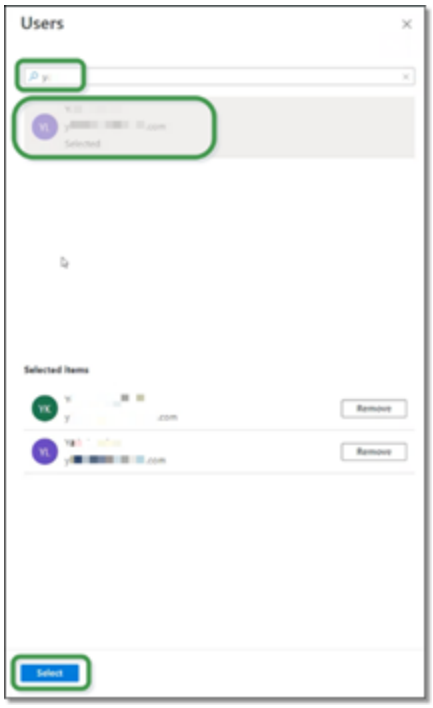
1. 在 **Microsoft Azure**中，导航至“**用户和组**”页面，然后单击“**+ 添加用户/组**”。
2. 在“**添加分配**”屏幕的“**用户**”下，单击“**未选择**”。



此时会出现“用户”侧面板。

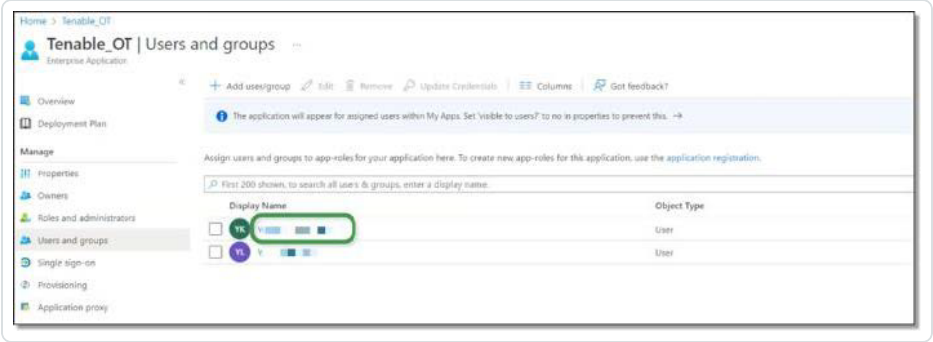
注意：如果在 Microsoft Azure 中启用了组设置并在之前选择了“**分配给应用程序的组**”而不是“所有组”，则可以选择分配组而不是单个用户。

3. 搜索并单击所有所需用户，然后单击“**选择**”，再单击“**分配**”以将其分配至应用程序。



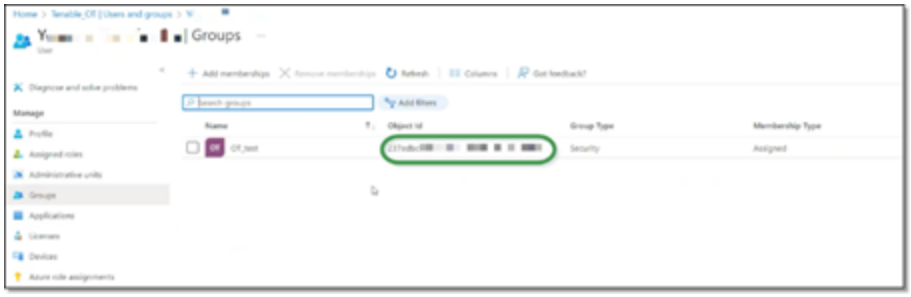
此时会出现“**用户和组**”页面。

4. 单击用户(或组)的“**显示名称**”可显示该用户(或组)的配置文件。

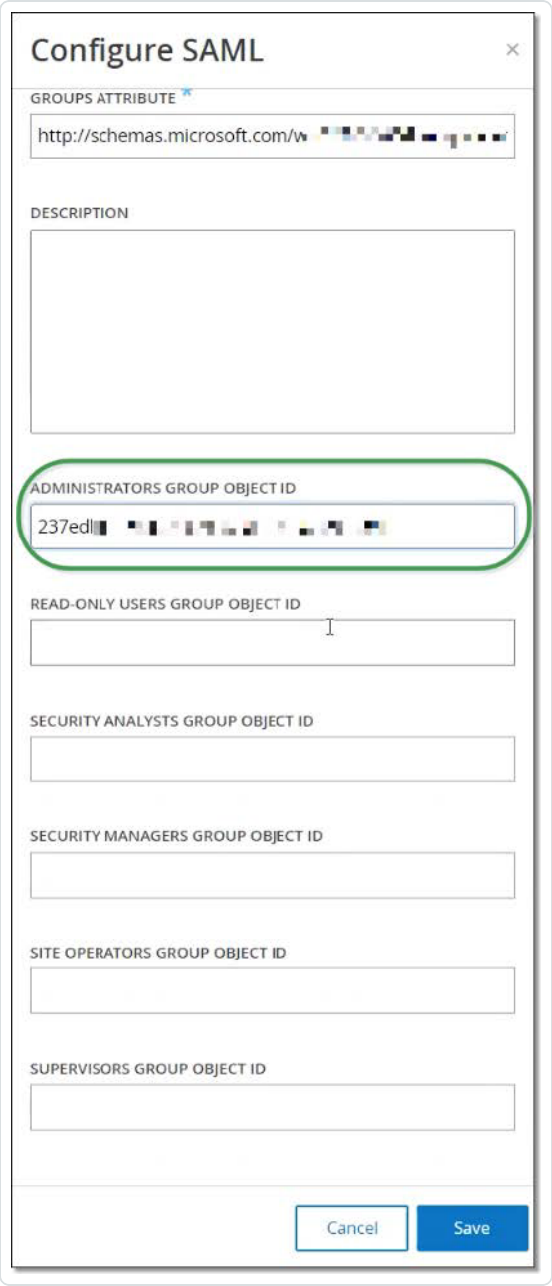


5. 在“**配置文件**”屏幕的左侧导航栏中,选择“**组**”以显示“**组**”屏幕。

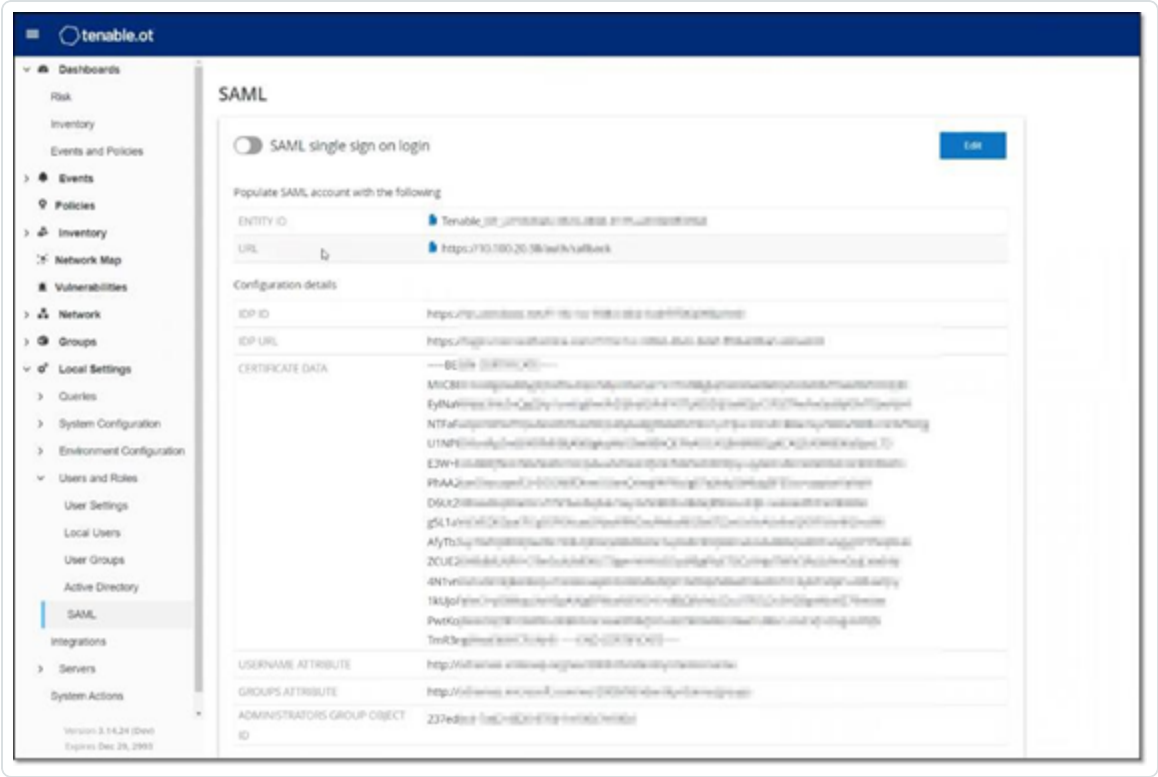
6. 在“**对象 ID**”下,突出显示并复制将映射到 Tenable 的组的值。



7. 返回 **OT Security** 控制台并将复制的值粘贴到所需的**组对象 ID** 字段(例如，管理员组对象 ID) 。
8. 对要映射到 OT Security 中不同用户组的每个组重复步骤 1-7。
9. 单击"**保存**"以保存操作并关闭侧面板。



SAML 屏幕将显示在 OT Security 控制台中，并包含已配置的信息。


tenable.ot
Dashboards
Risk
Inventory
Events and Policies
Events
Policies
Inventory
Network Map
Vulnerabilities
Network
Groups
Local Settings
Queries
System Configuration
Environment Configuration
Users and Roles
User Settings
Local Users
User Groups
Active Directory
SAML
Integrations
Servers
System Actions
SAML
SAML single sign on login
Edit
Populate SAML account with the following
ENTITY ID
URL
Configuration details
IDP ID
IDP URL
CERTIFICATE DATA
USERNAME ATTRIBUTE
GROUPS ATTRIBUTE
ADMINISTRATORS GROUP OBJECT ID

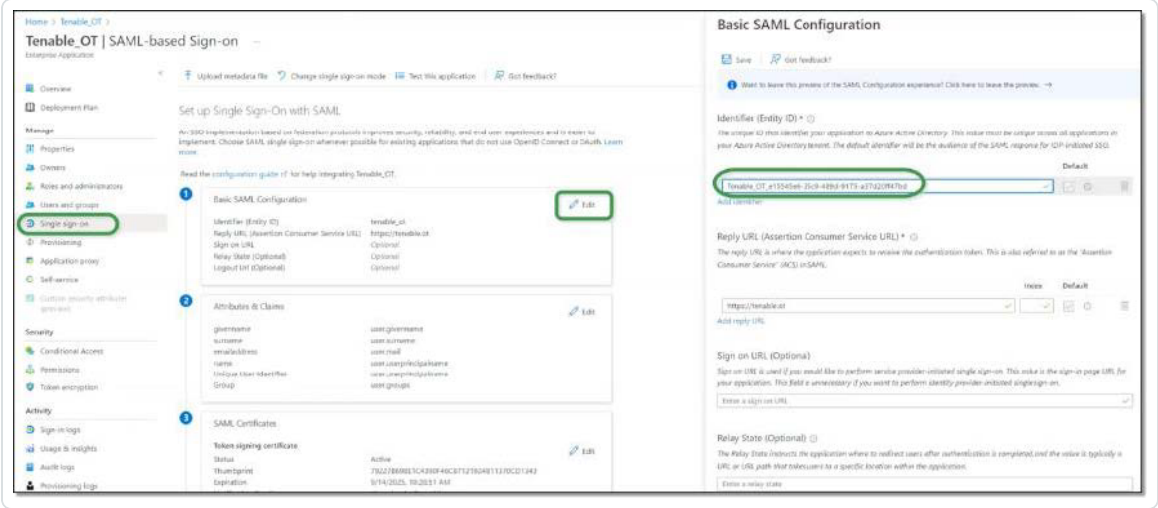
第 4 步：完成 Azure 中的配置

若要完成 Azure 中的配置，请执行以下操作：

1. 在 OT Security **SAML** 屏幕中，单击“**实体 ID**”下的复制图标。

2. 切换到“**Azure**”屏幕，然后单击左侧导航菜单中的“**单点登录**”以打开“**基于 SAML 的登录**”页面。

3. 在第 1 部分（**基本 SAML 配置**）中，单击“**编辑**”，然后将复制的值粘贴到“**标识符（实体 ID）**”字段中，以替换之前输入的临时值。



4. 返回“OT Security **SAML**”屏幕，单击“**URL**”下的复制图标。

5. 在 **Azure** 控制台和“**基本 SAML 配置**”侧面板中，将复制的 URL 粘贴到“**回复 URL（断言消费者服务 URL）**”下方，以替换之前输入的临时 URL。

6. 单击“**保存**”以保存配置并关闭侧面板。

   配置完成，“**Azure Enterprise 应用程序**”屏幕即会显示连接情况。

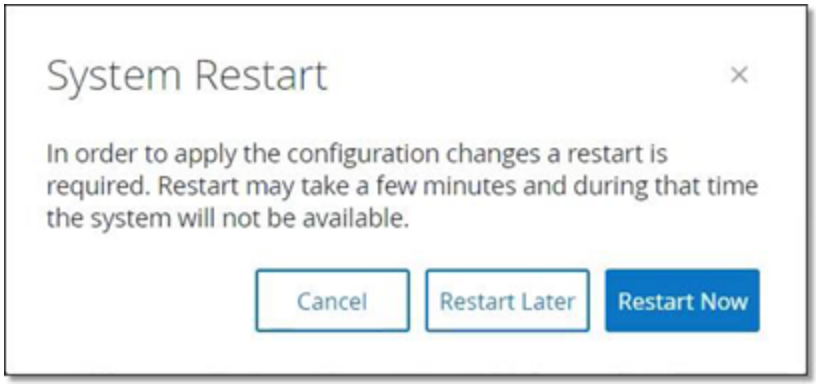
第 5 步:激活集成

若要激活 SAML 集成,则必须重新启动 OT Security。用户可立即重新启动系统或选择稍后重新启动。

若要激活集成,请执行以下操作:

1. 在 OT Security 控制台的"**SAML**"屏幕上,单击以将"**SAML 单点登录**"按钮切换为"**打开**"。

   此时会显示"**系统重新启动**"通知窗口。



2. 单击"**立即重新启动**"以重新启动系统并立即应用 SAML 配置,或单击"**稍后重新启动**"以将应用 SAML 配置延迟到下次系统重新启动时。如果您选择稍后重新启动,以下标题栏会在重新启动完成之前一直显示:

使用 SSO 登录

重新启动后，**OT Security** 登录窗口的"登录"按钮下方会出现一个新的"**通过 SSO 登录**"链接。分配至 OT Security 的 Azure 用户可以使用 Azure 帐户登录 OT Security。

若要使用 SSO 登录，请执行以下操作：

1. 在 **OT Security** 登录屏幕上，单击"**通过 SSO 登录**"链接。

如果已登录 Azure，则会直接进入 OT Security 控制台，否则会重定向至 Azure 登录页面。

拥有多个帐户的用户将被重定向至 Microsoft"**选择帐户**"页面，以便选择所需的帐户进行登录。

修订历史记录

产品版本：OT Security 文档修订历史记录：

文档修订号	日期	描述
1.0	2018 年 10 月 8 日	为《用户指南》创建了第一个版本，即版本 2.5
1.1	2019 年 1 月 28 日	对版本 2.7 进行了更新
1.2	2019 年 8 月 20 日	对版本 3.1 进行了更新
1.3	2019 年 10 月 10 日	对当前支持的功能进行了修订
1.4	2019 年 1 月 12 日	对版本 3.3 进行了更新
1.5	2020 年 3 月 24 日	对版本 3.4 进行了更新
1.6	2020 年 4 月 6 日	对版本 3.5 进行了更新
1.7	2020 年 4 月 27 日	添加了传感器文档
1.8	2020 年 6 月 3 日	对版本 3.6 进行了更新
1.9	2020 年 8 月 8 日	对版本 3.7 进行了更新
2.0	2020 年 10 月 11 日	对版本 3.8 进行了更新
2.1	2020 年 12 月 2 日	对版本 3.9 进行了更新
2.2	2021 年 4 月 6 日	对版本 3.10 进行了更新
2.3	2021 年 6 月 30 日	对版本 3.11 进行了更新
2.4	2021 年 12 月 12 日	对版本 3.12 进行了更新
2.5	2022 年 3 月 25 日	对版本 3.13 进行了更新
2.6	2022 年 8 月 22 日	对版本 3.14 进行了更新
2.7	2022 年 9 月 25 日	添加了 SAML 集成 (SP1)
2.8	2023 年 1 月 31 日	对版本 3.15 进行了更新
2.9	2023 年 7 月 25 日	对版本 3.16 进行了更新

3.0	2023 年 9 月 11 日	对版本 3.17 进行了更新
3.1	2024 年 3 月 15 日	对版本 3.18 进行了更新