Tenable OT Security User Guide

Version 3.14

Revision History

Product version: Tenable.ot 3.14

Document revision history:

Document Revision	Date	Description
1.0	October 8, 2018	Created first version of User Guide for Version 2.5
1.1	January 28, 2019	Updated for version 2.7
1.2	August 20, 2019	Updated for version 3.1
1.3	October 10, 2019	Revised for currently supported features
1.4	January 12, 2019	Updated for version 3.3
1.5	March 24, 2020	Updated for version 3.4
1.6	April 6, 2020	Updated for version 3.5
1.7	April 27, 2020	Added documentation of Sensors
1.8	June 3, 2020	Updated for version 3.6
1.9	August 8, 2020	Updated for version 3.7
2.0	October 11, 2020	Updated for version 3.8
2.1	December 2, 2020	Updated for version 3.9
2.2	April 6, 2021	Updated for version 3.10
2.3	June 30, 2021	Updated for version 3.11
2.4	December 12, 2021	Updated for version 3.12
2.5	March 25, 2022	Updated for version 3.13
2.6	August 22, 2022	Updated for version 3.14
2.7	September 25, 2022	Added SAML integration (SP1)

Table of Contents

Introduction

Tenable.ot protects industrial networks from cyber threats, malicious insiders and human error. From threat detection and mitigation to asset tracking, vulnerability management, configuration control and Active Query checks, Tenable.ot's ICS security capabilities maximize your operational environments visibility, security and control.

Tenable.ot offers comprehensive security tools and reports for IT security personnel and OT engineers. It provides unmatched visibility into converged IT/OT segments and ICS activity, and delivers crystal-clear situational awareness across all sites and their respective OT assets—from Windows Servers to PLC backplanes—in a single pane of glass.

Tenable.ot has the following key features:

- 360-Degree Visibility - Attacks can easily propagate in an IT/OT infrastructure. With a single platform to manage and measure cyber risk across your OT and IT systems, you have complete visibility into your converged attack surface. Tenable.ot also natively integrates with leading IT security and operational tools, such as your Security Information and Event Management (SIEM) solution, log management tools, next-generation firewalls, and ticketing systems. Together, this builds an ecosystem of trust where all of your security products can work together as one to keep your environment secure.
- Threat Detection and Mitigation - Tenable.ot leverages a multi-detection engine to find high-risk events and behaviors that can impact OT operations. These engines include policy, behavioral and signature-based detection.
- Asset Inventory and Active Detection - Leveraging groundbreaking patented technology, Tenable.ot provides unparalleled visibility into your infrastructure—not only at the network level, but down to the device level. It uses native communication protocols to actively query both IT and OT devices in your ICS environment in order to identify all of the activities and actions occurring across your network.
- Risk-Based Vulnerability Management - Drawing on comprehensive and detailed IT and OT asset tracking capabilities, Tenable.ot generates vulnerability and risk levels using Predictive Prioritization for each asset in your ICS network. These reports include risk-scoring and detailed insights, along with mitigation suggestions.
- Configuration Control – Tenable.ot provides a full granular history of device configuration changes over time, including specific ladder logic segments, diagnostic buffers, tag tables and more. This enables administrators to establish a backup snapshot with the "last known good state" for faster recovery and compliance with industry regulations.

Tenable.ot Technologies

The Tenable.ot comprehensive solution comprises two core collection technologies:

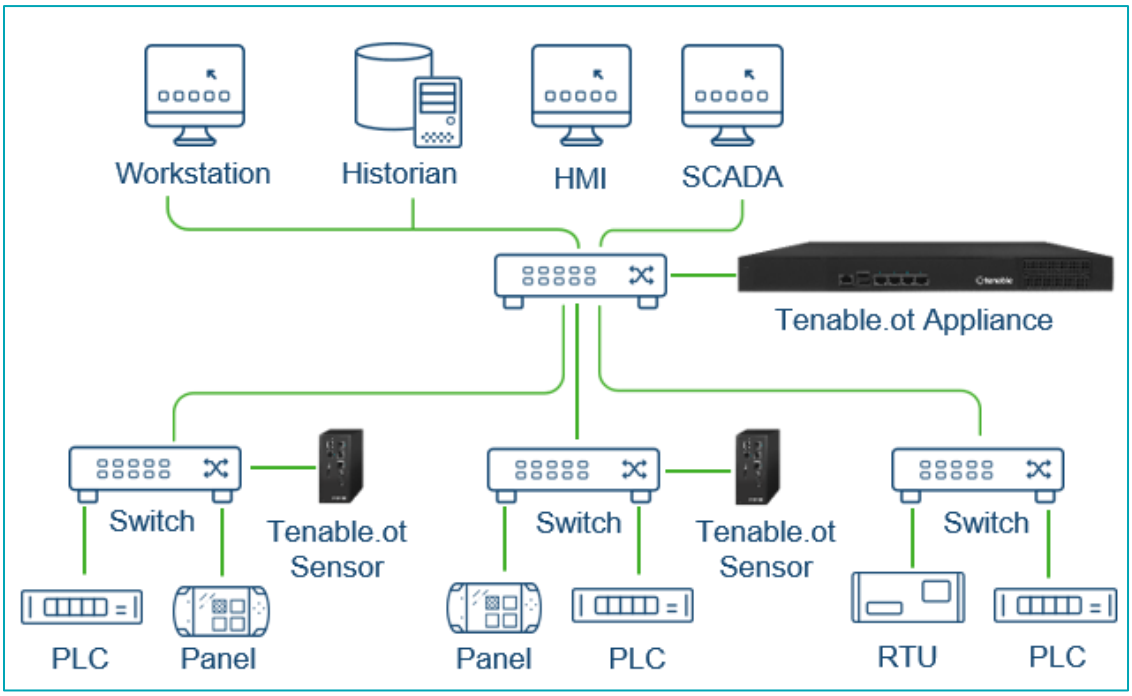
- Network Detection – Tenable.ot network detection technology is a passive deep-packet inspection engine specifically designed to address the unique characteristics and requirements of industrial control systems. Network Detection provides in depth, real time visibility into all activities performed over the operational network, with a unique focus on engineering activities. This includes firmware downloads/uploads, code updates and configuration changes performed over proprietary, vendor specific communication protocols. Network detection alerts in real-time for suspicious/unauthorized activities and produces a comprehensive event log with forensic data. Network Detection generates three types of alerts:
    - Policy Based – You can activate predefined policies or create custom policies which whitelist and/or blacklist specific granular activities indicative of cyber threats or operational mistakes to trigger alerts. Policies can also be set to trigger Active Query checks for predefined situations.
    - Behavioral Anomalies – The system detects deviations from a network traffic baseline, which was established based on traffic patterns during a specified time range. It also detects suspicious scans that are indicative of malware and reconnaissance behaviors.
    - Signature Detection Policies – these policies use signature-based OT and IT threat detection to identify network traffic that is indicative of intrusion threats. The detection is based on rules that have been catalogued in Suricata's Threats engine.
- Active Query – Tenable.ot's patented querying technology monitors devices that are on the network by periodically surveying the metadata of control devices in the ICS network. This capability enhances Tenable.ot's ability to automatically discover and classify all the ICS assets, including lower-level devices such as PLCs and RTUs, even when they aren't active in the network. It also identifies locally implemented changes in the device's metadata (e.g. firmware version, configuration details and state) as well as changes in each code/function block of the device's logic. Since it uses read only queries in the native controller communication protocols, it is completely safe and has no impact on the devices. Queries can be run periodically based on a predefined schedule or on-demand by the user.

Solution Architecture

Tenable.ot Platform Components

The Tenable.ot solution is comprised of two components:

- Tenable.ot Appliance – this component collects and analyses the network traffic directly from the network (via a span port or network tap) and/or using a data feed from the Tenable.ot Sensors. The Tenable.ot appliance executes both the Network Detection and Active Query functions.
- Tenable.ot Sensors - small devices that can be deployed on network segments that are of interest, up to one sensor per managed switch. The sensors are available in 2 form factors: compact rack mount or DIN-Rail mount. Tenable.ot sensors provide full visibility into these network segments by capturing all the traffic, analyzing it and then communicating the information to the Tenable.ot appliance. Sensors version 3.14 and above can also be configured to send out active queries to the network segments on which they are deployed.



Network deployment of Tenable.ot appliance and Sensors

Network Components

Tenable.ot supports interaction with the following network components:

- Tenable.ot user (management) – Users accounts are created to control access to the Tenable.ot Management Console. The Management Console is accessed through a web browser (Google Chrome) via a secure socket-layer authentication (HTTPS).

The UI can only be accessed from a Chrome browser. You also need to be using the latest version of Chrome.

- Active Directory Server – User credentials can optionally be assigned using an LDAP server, such as Active Directory. In this case, user privileges are managed on the Active Directory.
- SIEM – Tenable.ot Event logs can be sent to a SIEM using Syslog protocol.
- SMTP Server – Tenable.ot Event notifications can be sent by email to specific groups of employees via an SMTP server.
- DNS Server – DNS servers can be integrated into Tenable.ot to help in resolving asset names.
- Third party applications – External applications can interact with Tenable.ot using its REST API or access data using other specific integrations[1].

System Elements

Assets

Assets are the hardware components in your network such as controllers, engineering stations, servers etc. Tenable.ot's automated asset discovery, classification and management provides an accurate asset inventory by continuously tracking all changes to devices. This simplifies sustaining of operational continuity, reliability and safety. It also plays a key role in planning maintenance projects, prioritizing upgrades, patch deployments, incident response and mitigation efforts.

Risk Assessment

Tenable.ot applies sophisticated algorithms to assess the degree of risk posed to each asset on the network. A *Risk Score* (from 1 to 100) is given for each Asset in the network. The Risk score is based on the following factors:

- Events - that occurred in the network that affected the device (weighted based on Event severity and how recently the Event occurred).

[1] For example, Tenable.ot supports integration with Palo Alto Networks Next Generation Firewall (NGFW) and Aruba ClearPass, enabling Tenable.ot to share asset inventory info with these systems. Tenable.ot can also integrate with other Tenable platforms such as Tenable.io and Tenable.sc. Integrations are configured under **Local Settings** > **Integrations**, see **Local Settings.**

Events are weighted according to currency, so that more recent Events have a greater impact on the Risk score than older Events.

- Vulnerabilities –CVEs that affect assets in your network, as well as other threats identified in your network (e.g. obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, etc.). In the Tenable.ot, these are detected as plugin hits on your assets.
- Asset Criticality – a measure of the importance of the device to the proper functioning of the system.

For PLC's that are connected to a backplane, the Risk score of other modules that share the backplane affect the PLC's Risk score.

Policies and Events

Policies are used to define specific types of events that are suspicious, unauthorized, anomalous or otherwise noteworthy that take place in the network. When an event occurs that meets all the *Policy Definition* conditions for a particular Policy, an Event is generated in the system. The Event is logged in the system and notifications are sent out in accordance with the *Policy Actions* configured for the Policy.

There are two types of policy events:

- Policy-based Detection – which triggers Events when the precise conditions of the Policy, as defined by a series of event descriptors, are met.
- Anomaly Detection –which trigger Events when anomalous or suspicious activity is identified in the network.

The system features a set of predefined policies (out-of-the-box). In addition, the system offers the ability to edit the predefined policies or define new custom policies.

Policy-Based Detection

For Policy-based detection, you configure the specific conditions for what events in the system trigger Event notifications. Policy-based Events are triggered only when the precise conditions of the policy are met. This ensures zero false positives, as the system alerts for actual events that take place in the ICS network, while providing meaningful detailed information about the 'who', 'what', 'when', 'where' and 'how'. The policies can be based on various Event types and descriptors. The following, are some examples of possible policy configurations:

- Anomalous or unauthorized ICS control-plane activity (engineering): for example, an HMI should not query the firmware version of a controller (may indicate reconnaissance), and a controller should not be programmed during operational hours (may indicate unauthorized, potentially malicious activity).
- Change to controller's code – a change to the controller logic was identified ("Snapshot mismatch").

- Anomalous or unauthorized network communications: for example, an un-allowed communication protocol was used between two network assets or a communication took place between two assets that have never communicated before.
- Anomalous or unauthorized changes to the asset inventory: for example, a new asset was discovered or an asset stopped communicating in the network.
- Anomalous or unauthorized changes in asset properties: for example, the asset firmware or state has changed.
- Abnormal writes of set-points: Events are generated for changes made to specific parameters. The user can define the allowed ranges for a parameter and generate Events for deviations from that range.

Anomaly Detection

Anomaly Detection policies discover suspicious behavior in the network based on the system's built-in capabilities for detecting deviations from 'normal' activity. The following anomaly detection policies are available.

- Deviations from a network traffic baseline: the user defines a baseline of 'normal' network traffic based on the traffic map during a specified time range and generates alerts for deviations from the baseline. The baseline can be updated at any time.
- Spike in Network Traffic: a dramatic increase in the volume of network traffic or number of conversations is detected.
- Potential network reconnaissance/cyber-attack activity: Events are generated for activities indicative of reconnaissance or cyber-attack activity in the network, such as IP conflicts, TCP port scans and ARP scans.

Policy Categories

The Policies are organized by the following categories:

- Configuration Event Policies – these Policies relate to the activities that take place in the network. There are two sub-categories of Configuration Event Policies:
    - Controller Validation - these Policies relate to changes that take place in the controllers in the network. This can involve changes in the state of a controller as well as changes to the firmware, asset properties or code blocks. The Policies can be limited to specific schedules (e.g. firmware upgrade during a work day), and/or specific controller/s.
    - Controller Activities – these policies relate to specific engineering commands that impact controllers' state and configuration. It is possible to define specific activities that always generate Events or to designate a set of criteria for generating Events. For example, if certain activities are performed at certain times and/or on certain controllers. Both black listing and white listing of assets, activities and schedules are supported.
- Network Events Policies – these Policies relate to the assets in the network and the communication streams between assets. This includes assets that were added to or removed from the network. It also includes traffic patterns that are anomalous for the network or that have been flagged as raising particular cause for concern. For example, if an engineering station communicates with a controller using a protocol that is not part of a pre-configured set of protocols (e.g. protocols that are used by controllers manufactured by a specific vendor), an

Event is triggered. These policies can be limited to specific schedules and/or specific assets. Vendor specific protocols are organized by vendor for convenience, while any protocol can be used in a policy definition.

- SCADA Event Policies – these Policies detect changes in set-point values which can harm the industrial process. These changes may result from a cyber-attack or human error.
- Network Threats Policies – these Policies use signature-based OT and IT threat detection to identify network traffic that is indicative of intrusion threats. The detection is based on rules that have been catalogued in Suricata's Threats engine.

Groups

An essential component in the definition of Policies in Tenable.ot is the use of *Groups*. When configuring a Policy each of the parameters is designated by a Group as opposed to individual entities. This greatly streamlines the Policy configuration process.

Events

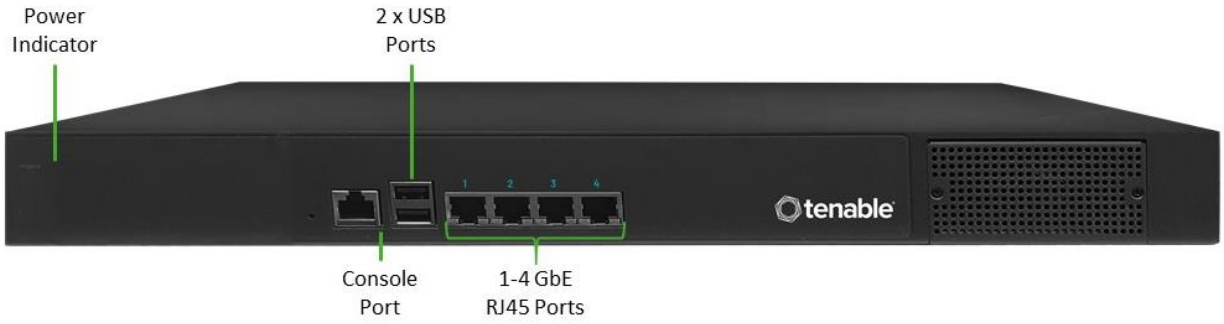
When an event occurs that matches the conditions of a Policy, an Event is generated in the system. All Events are displayed on the Events screen and can also be accessed through the relevant Inventory and Policy screens. Each Event is marked with a severity level, indicating the degree of risk posed by the Event. Notifications can be automatically sent out to email recipients and SIEMs as specified in the Policy Actions of the Policy that generated the Event.

An Event can be marked as resolved by an authorized user and a comment can be added.

Tenable.ot Hardware Components

Tenable.ot Appliance

Front Panel



Component	Description
Power Indicator	Indicates when the Tenable.ot appliance is turned on (Green) or off.
Console Port	Not in use
USB Ports	Not in use
Ethernet Ports	Four GbE ports used to connect to management and operational networks as follows: Port 1 – by default, this port is used for both Management (User Interface) and as the Active Query port (that communicates with the network assets). This port configuration could be changed (both during the set up and later in the Settings page) to include just the Queries. This is done in order to separate the management interface from the controllers' network. Port 2 – Mirror port - used as the destination of the mirroring session (SPAN). This port receives a copy of the network traffic. This port has no IP address. Port 3 – if the port separation option is enabled, this port is used for management (UI) only and can be connected to a network that is not part of the controller's network. Port 4 - Reserved port, used by Tenable.ot's Professional Services for remote or local support.

Rear Panel

Component	Description
Cooling Fans	Two cooling fans. Make sure that the fans are not obstructed.
Power Switch	ON/OFF switch. (Press and hold for a few seconds to turn power off.)
Power Supply Port	AC power connector; 100 – 240 V AC

Package Contents

Component	Description
Two Ethernet Cables	Two standard RJ45 Ethernet cables. Use these cables to connect the Tenable.ot appliance to the network switch.
Power Supply Port	AC power connector; 100 – 240 V AC.
Mount Brackets	2 x 1U rack mount brackets.

Tenable.ot Sensor

Rack Mount Sensor

The Rack Mount sensor is being discontinued. Instead, we now offer an adapter kit that enables you to attach the Configurable Sensor model to a rack mount.

Front Panel

Component	Description
Console Port	Not in use
USB Ports	Not in use
Ethernet Ports	Four 1GbE ports used to connect to management and operational networks as follows: Port 1 – Management port – used for managing the device. Port 2 – Mirror port - used as the destination of the mirroring session (SPAN). This port receives a copy of the network traffic. This port has no IP address. Port 3 – Not in use. Port 4 – Not in use.

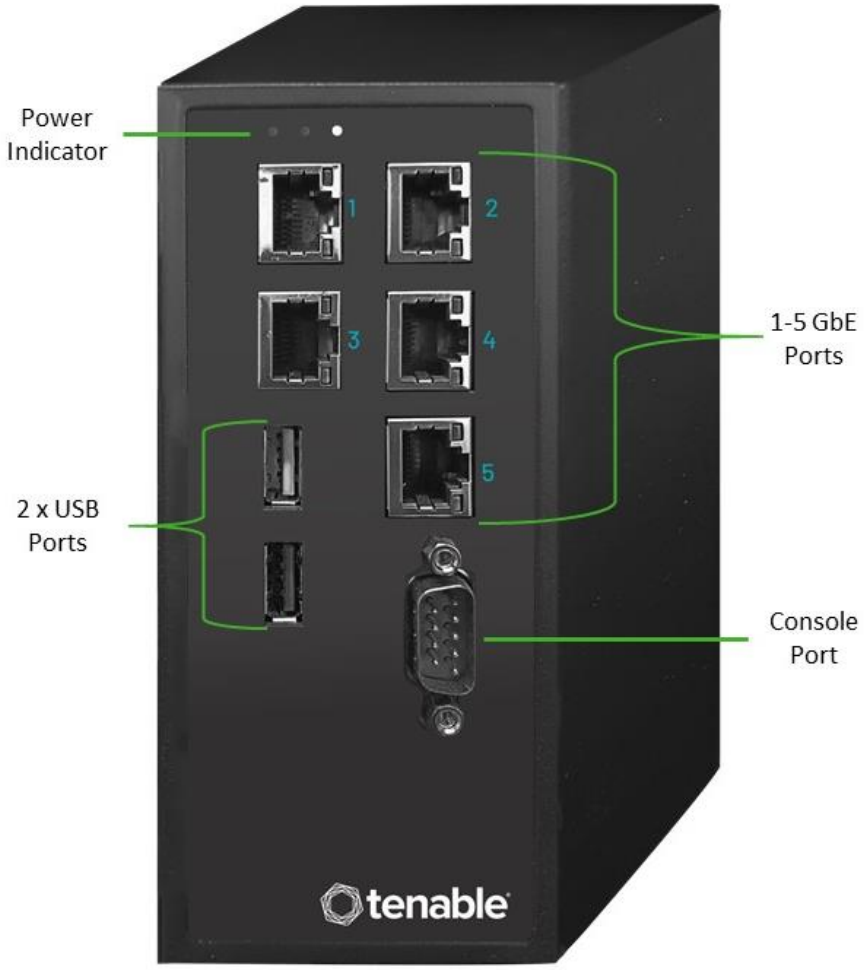
Rear Panel

Component	Description
Power Button	Stand-by mode in red; Power-on mode in green.
Reset Button	Reboots the system without turning off the power.
Power Switch	ON/OFF switch. (Press and hold for a few seconds to turn power off.)
Power Supply Port	AC power connector; 100 – 240 V AC

Package Contents

Component	Description
Ethernet Cable	A standard RJ45 Ethernet cable. Use this cable to connect the sensor to the network switch.
Power Cable	A standard US power cable.
Power Supply	60W AC power adaptor; 100 – 240 V AC.
Mount Brackets	2 x 1U L-shaped rack mount brackets.
Screws Pack	

Configurable Sensor



This model can be mounted either on a DIN rail, or on a mounting rack (using the adapter kit). In the past, this model was referred to as the DIN Rail Sensor.

Front Panel

Component	Description
Power Indicator	Indicates when the sensor is turned on (Green) or off.
Console Port	Not in use

Component	Description
USB Ports	Not in use
Ethernet Ports	Five GbE ports used to connect to management and operational networks as follows: Port 1 – Management port – used for managing the device. Port 2 – Not in use. Port 3 – Mirror port - used as the destination of the mirroring session (SPAN). This port receives a copy of the network traffic. This port has no IP address. Port 4 – Not in use. Port 5 - Not in use.

Package Contents

Component	Description
Power Cable	A standard US power cable.
Power Supply	60W AC power adaptor; 100 – 240 V AC.
Ethernet Cable	A standard RJ45 Ethernet cable. Use this cable to connect the sensor to the network switch.
Mounting Ears	2 x 1U L-shaped rack mount brackets (“Ears”).
Screws Pack	

Installing the Tenable.ot Appliance

Step 1 – Setting up the Tenable.ot Appliance

The Tenable.ot appliance can be either rack mounted, or simply rested on top of a flat surface (such as a desktop).

Rack Mounting

➡ **To mount the Tenable.ot appliance on a standard (19-inch) rack:**

1. Insert the server unit into an available 1U slot in the rack.

Make sure that the rack is electrically grounded. Make sure that the cooling fan air intake (located in the back panel) and the air ventilation holes (on the top panel) are not obstructed.

2. Secure the unit to the rack by fastening the rack-mount brackets (supplied) to the rack frame, using the appropriate screws for rack mounting (not supplied).
3. Plug in the AC power supply cable (supplied) to the power supply port in the rear panel, then plug the cable to the AC power supply (mains).

Flat Surface

➡ **To install the Tenable.ot appliance on a flat surface:**

1. Place the appliance unit on a dry, flat, leveled surface (such as a desktop).

Make sure that the tabletop is flat and dry.
Make sure that the cooling fan air intake (located in the back panel) and the air ventilation holes (on the top panel) are not obstructed.

2. If the unit is placed within a stack of other electrical appliances, make sure there is ample space behind the cooling fan (located in the back panel) to allow proper ventilation and cooling.
3. Plug in the AC power supply cable (supplied) to the power supply port in the rear panel, then plug the cable to the AC power supply (mains).

Step 2 – Connecting Tenable.ot to the Network

Tenable.ot is used for both Network Monitoring and Active Query.

- To perform Network Monitoring - you will need to connect the unit to a mirroring port on the network switch, which is connected to the controllers/PLCs of interest.
- To perform Active Query - you will need to connect the unit to a regular port that has an IP address on the network switch, which is connected to the controllers/PLCs of interest.

By default, the Active Query and the Management Console are configured to use the same port on the unit (Port 1), however after the initial setup it is possible to separate the Management port from the Active Query port, by configuring the management on Port 3. After this configuration, you will need to connect Port 3 on the unit to a regular port on the switch to perform the management as described in **Step 7 – Connecting the Separate Management Port (for Port Separation Option)**.

For the initial setup you will connect Port 1 to a regular port on the network switch and connect Port 2 to a mirroring port.

➡ **To Connect the Tenable.ot appliance to the network:**

1. On the Tenable.ot appliance, connect the Ethernet cable (supplied) to **Port 1**.
2. Connect the cable to a regular port on the network switch.
3. On the unit, connect another Ethernet cable (supplied) to **Port 2**.
4. Connect the cable to a mirroring port on the network switch.

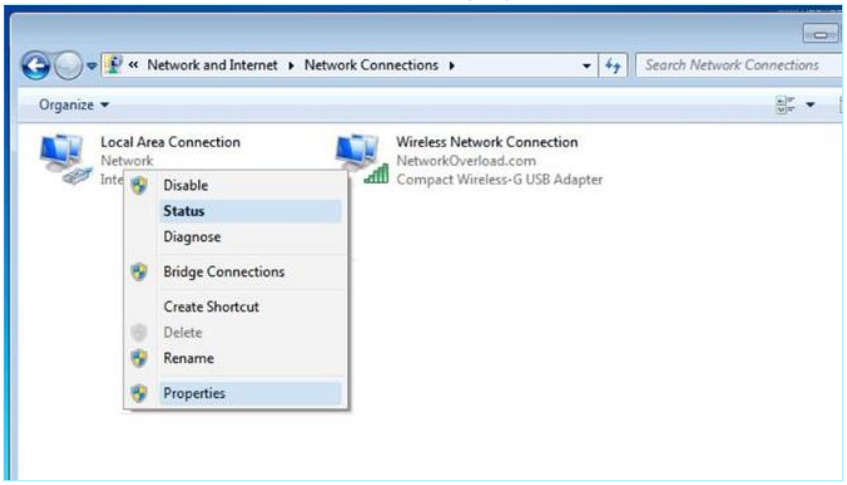
Step 3 – Logging in to the Management Console

➡ **To Log in to the Management Console.**

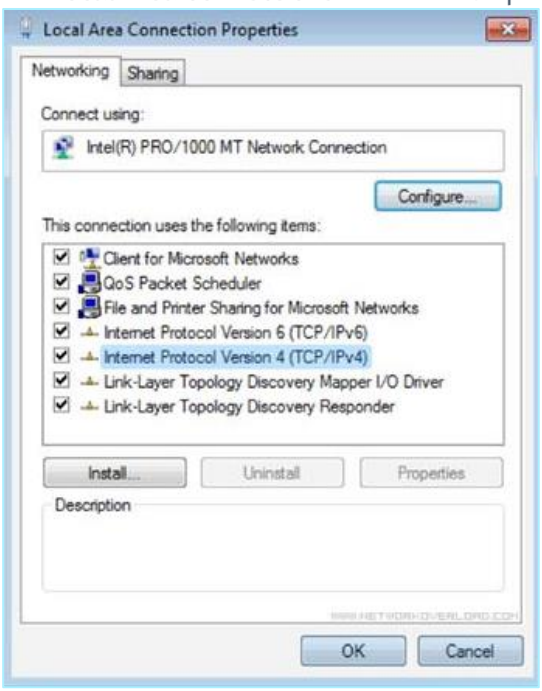
1. Do one of the following:
   - Connect the Management Console workstation (e.g. PC, laptop etc.) directly to Port 1 of the Tenable.ot appliance using the Ethernet cable, OR
   - Connect the Management Console workstation to the network switch.
2. Ensure that the Management Console workstation is part of the same subnet as the Tenable.ot appliance (which is 192.168. 1.0/24) or is routable to the unit.
3. Use the following procedure to set up a static IP (you must set up a static IP in order to connect to the Tenable.ot appliance):
   a. Go to **Network and Internet** > **Network and Sharing Center** > **Change adapter settings**.

	Navigation may vary slightly for different versions of Windows.

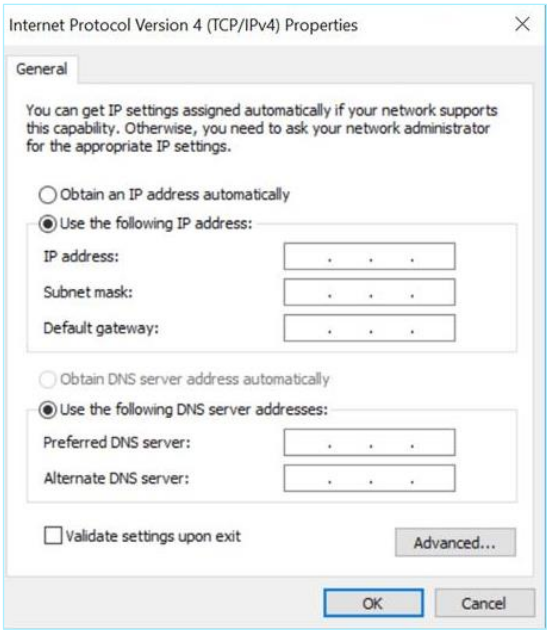
b. The Network Connections screen is displayed.



c. Right click on **Local Area Connections** and select **Properties**.
The **Local Area Connections** window is displayed.



d. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
The Internet Protocol Version 4 (TCP/IPv4) Properties window is displayed.



e. Select Use the Following IP address.
f. In the IP address field, enter *192.168.1.10*
g. In the Subnet mask field, enter *255.255.255.0*.
h. Click **OK**.
The new settings are applied.

4. From your Chrome web browser, navigate to https://192.168.1.5.
The Welcome screen of the setup wizard opens.

The UI can only be accessed from a Chrome browser. You also need to be using the latest version of Chrome.

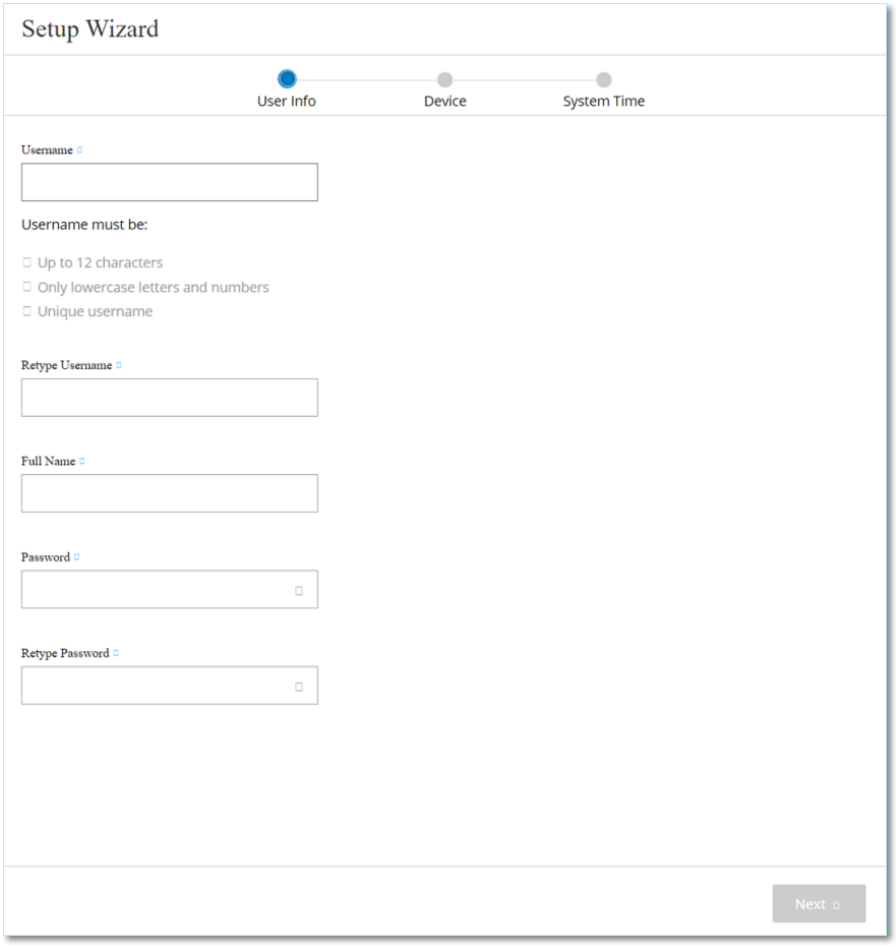
5. Click **Start Setup Wizard**.
   The setup wizard opens, showing the **User Info** page.

Step 4 – Setup Wizard

The Tenable.ot setup wizard takes you through the process of configuring the basic system settings.

If you would like to change the configuration later, you will be able to do so on the Settings screen in the Management Console (UI).

Screen 1 - User Info



➡ **On the User Info page, fill in your user account information as follows.**

In the setup wizard you configure the credentials for an Administrator account. After logging in to the UI you can create additional user accounts. For more information about user accounts see section **USERS AND ROLES**.

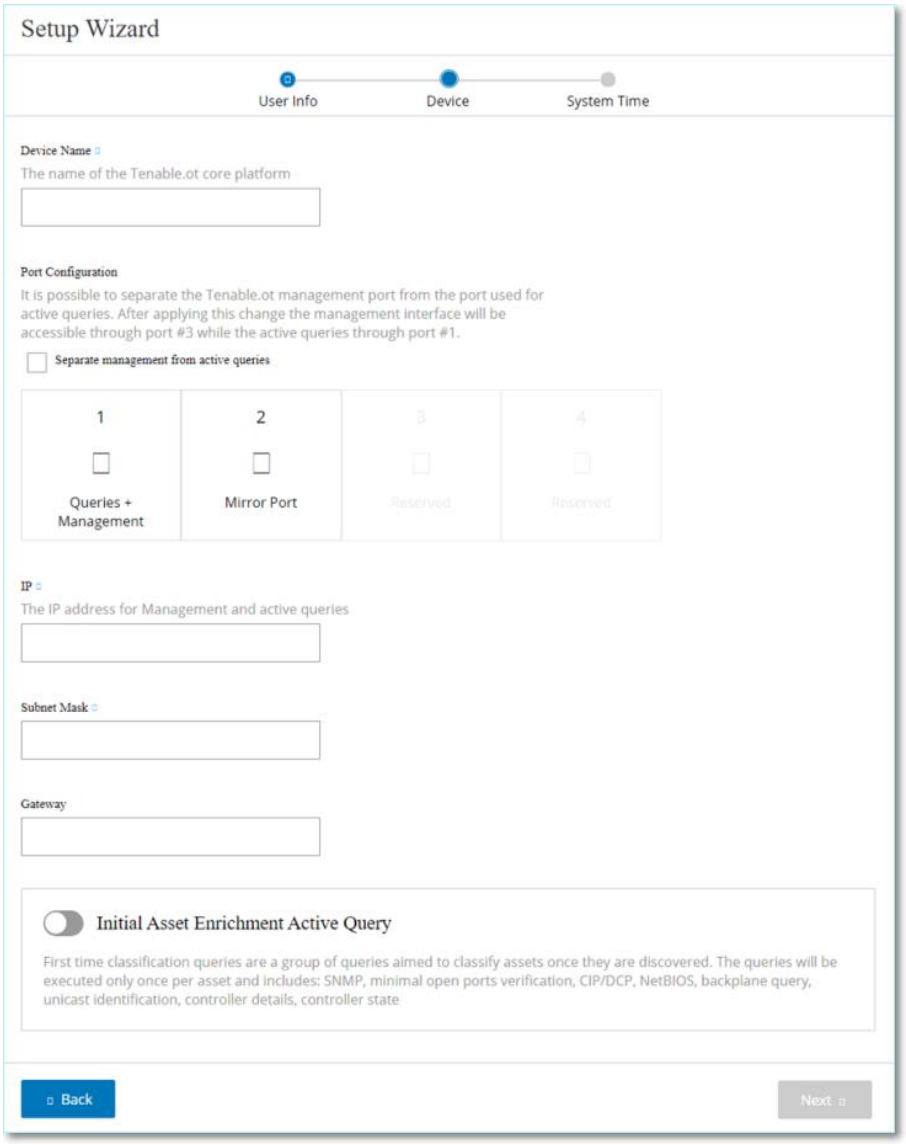
1. In the **Username** field, enter a username to be used for logging into the system. The username can have up to 12 characters and must include only lowercase letters and numbers.

2. In the **Retype Username** field, re-enter the identical username.
3. In the **Full Name** section, enter your complete **First and Last Name**.

This is the name that will appear in the header bar and on logs of your activity in the system.

4. In the **Password** field, enter a password to be used for logging into the system. The passwords must contain at least:
   - 12 characters
   - One uppercase letter
   - One lowercase letter
   - One digit
   - One special character
5. In the **Retype Password** field, re-enter the identical password.
6. Click **Next**.
   The **Device** page of the setup wizard opens.

Screen 2 – Device



➡ **On the Device page, fill in the information about the Tenable.ot platform as follows:**

1. In the **Device Name** field, enter a unique identifier for the Tenable.ot platform.
2. In the **Port Configuration** section, do one of the following:
   - **Port separation** - If you wish to use one port for management and a separate port for Queries, select the **Separate management from active queries** checkbox. Selecting this option will configure *Port 1* as the Queries *only* port and *Port 3* as the Management *only* port.

On some systems, the Port separation option may not be available. Contact your support agent for assistance.

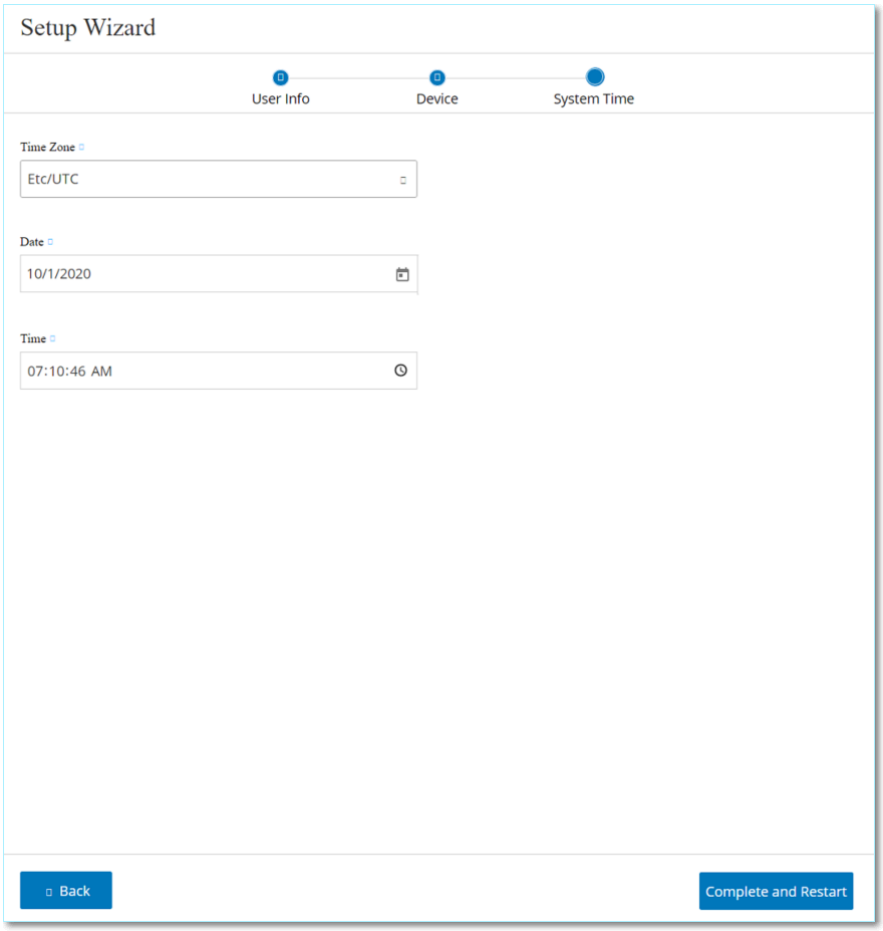
- **No separation** – if you wish to maintain the Queries and Management in the same port, don't select the **Separate management from active queries** checkbox. In this case, you can skip instructions number 3-5 of this procedure and proceed to **number 6.**

3. If you have selected the **port separation** option, in the **Active Queries IP** field, enter the IP address of the unit's *Queries port*. This port will be connected to a regular port in the network switch, which can communicate with (i.e. is routable to) the controllers. And, since Tenable.ot will actively connect to the controllers, it will need an IP address within the network subnet.
4. If you have selected the **port separation** option, in the **Active Queries Subnet Mask** field, enter the Subnet Mask of the *Queries port*.
5. If you have selected the **port separation** option, in the **Active Queries Gateway** field (optional), enter the IP address of the gateway in the operations network.
6. In the **Management IP** field, enter an IP address (within the network subnet) to be applied to the Tenable.ot platform. This becomes the Tenable.ot management IP address. (It is also the *Queries* address if there is no separation between the ports.)
7. In the **Management Subnet Mask** field, enter the Subnet Mask of the network.
8. If you would like to set up a Gateway (optional), enter the Gateway IP for the network in the **Management Gateway** field.

If you do not fill in this field then Tenable.ot will not be able to communicate with external components outside of the subnet (e.g. email servers, syslog servers etc.).

9. *Initial Asset Enrichment Active Query* is a series of queries that are run on each asset that is discovered in the system. This helps Tenable.ot to classify the assets. If you would like to run these queries on each new asset that is discovered, turn **on** the toggle switch in the bottom box.
10. Click **Next**.
    The **System Time** page of the setup wizard opens.

Screen 3 – System Time



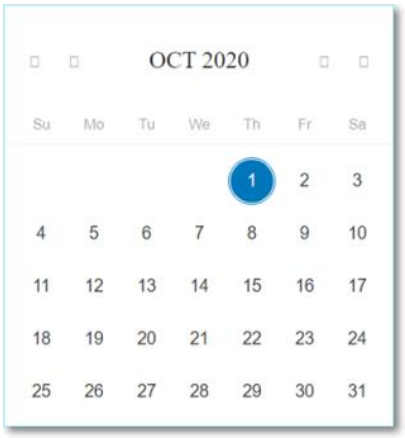
On the System Time page, the correct time and date are generally set automatically.

Setting the correct date and time is essential for accurate recording of logs and alerts.

➡ **If the correct date and time are not set, fill in the information as follows.**

1. In the **Time Zone** field, select from the dropdown list the local time zone at the site location.

2. In the **Date** field, click the calendar icon .
   A pop-up calendar appears.



3. Select the current date.
4. In the **Time** field, select **hours**, **minutes** and **seconds AM/PM** respectively and enter the correct number using either the keyboard or the up and down arrows.

If you would like to edit any of the previous pages of the setup wizard, click Back. After clicking Complete and Restart you won't be able to return to the setup wizard. However, you can change the configuration settings on the Settings page of the UI.

5. To complete the setup procedure, click **Complete and Restart**.
   Once the restart is complete, you are redirected to the Licensing screen.

Step 5 – Licensing

Before you can activate the system, you need to register your Tenable.ot license.

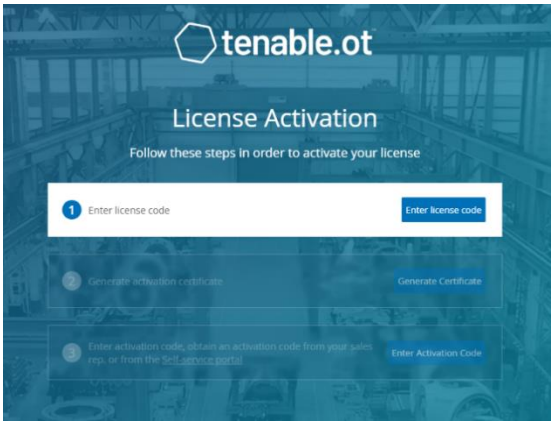
Prerequisites

- The License Code (20 characters letter/numbers) which you received from Tenable when you ordered your device.
- You need access to the Internet. If your Tenable.ot device is not connected to the Internet, you can register the license from any PC.

Activating your License

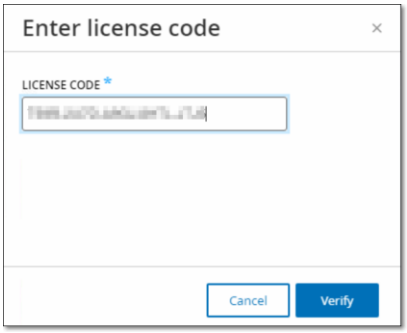
➡ **To Activate Your License:**

1. On the **License Activation** screen, in step 1**, Enter license code** field, click the **Enter license code** button.



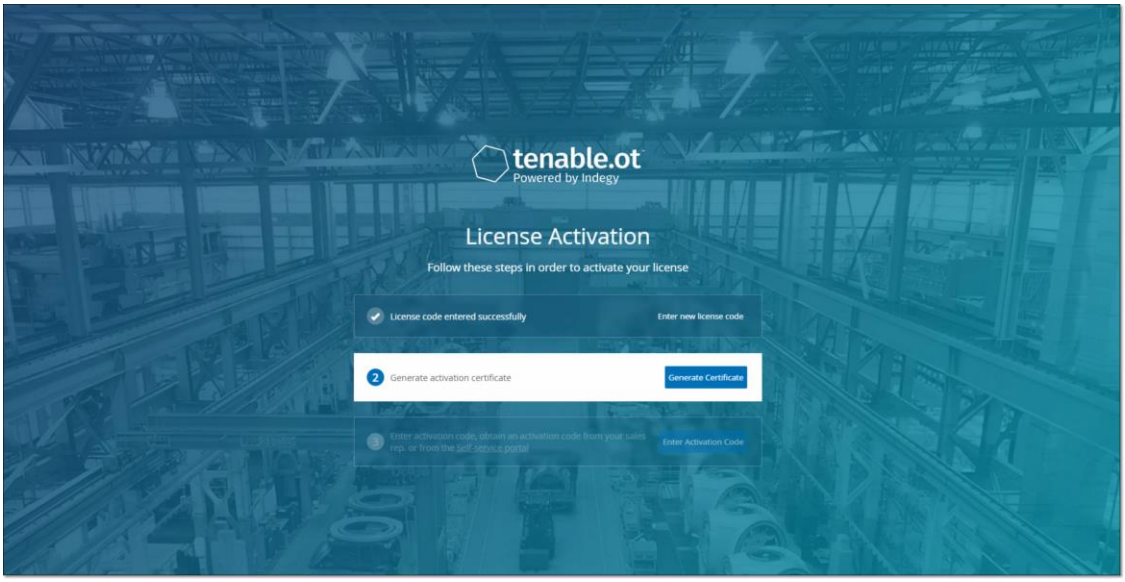
The **Enter license code** side panel is shown on the right side.

2. In the **License Code** field, enter your license code and click **Verify**.



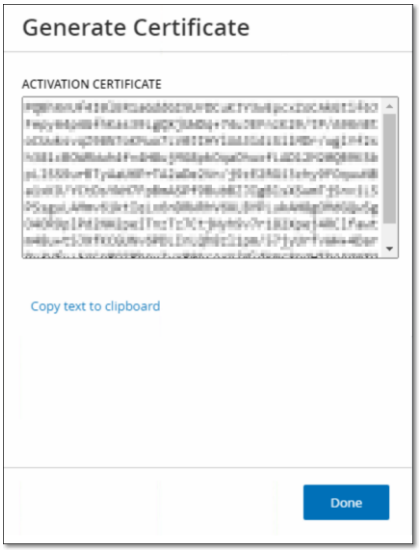
The side panel closes.

3. In step 2, **Generate activation certificate** field, click the **Generate Certificate** button.



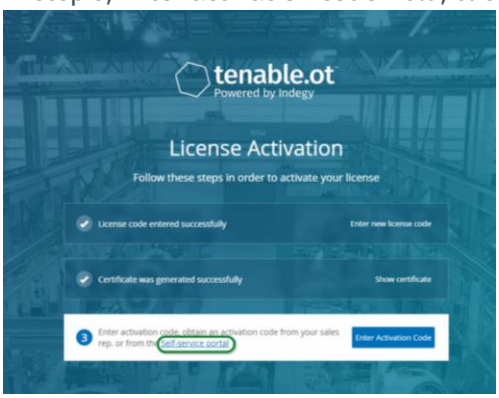
The **Generate Certificate** side panel is shown with the Activation Certificate.

4. Click the **Copy text to clipboard** button, and then click **Done**.

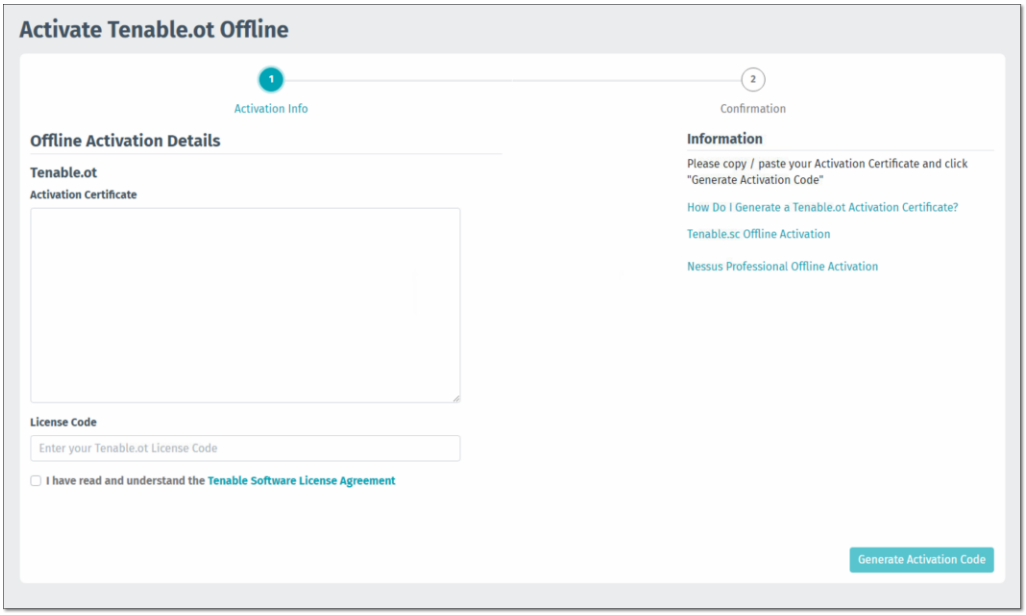


The side panel closes.

5. In step 3, **Enter activation code** field, click the **Self-service portal** link.



The **Activate Tenable.ot Offline** screen opens in a new tab.



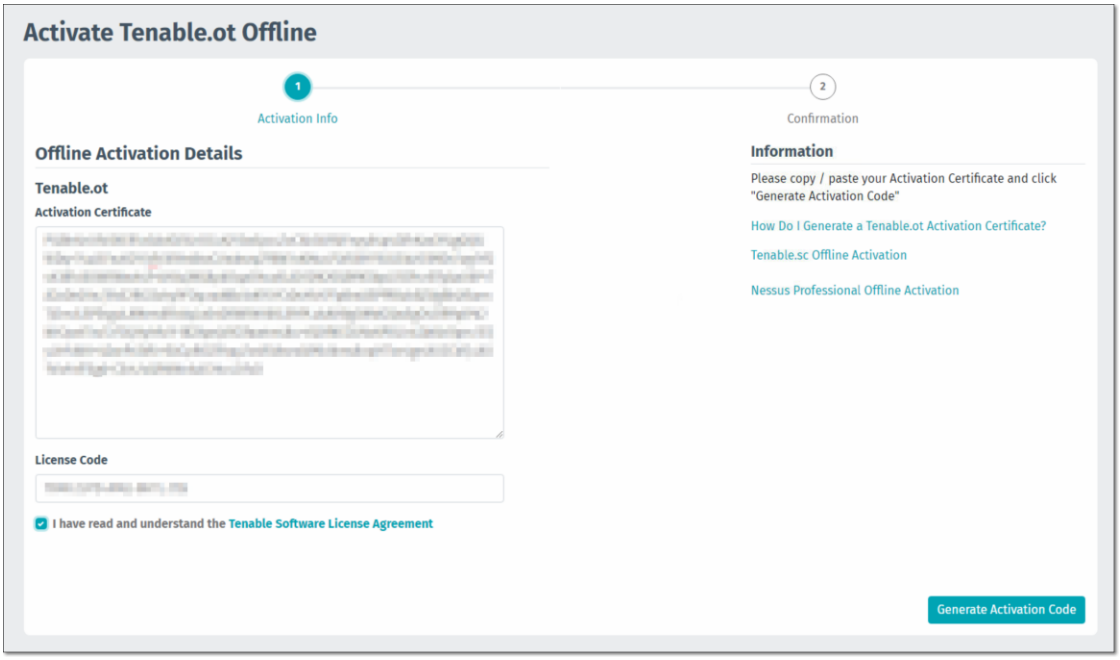
If your Tenable.ot device is not connected to the Internet, you will need to access the Activate Tenable.ot Offline screen from an Internet-connected device using the following URL: https://provisioning.tenable.com/activate/offline/tenable-ot.

If you are not currently logged in to tenable.com, you will need to log in using your email address and password. You must use the email account where you received your License Code.

If you don't have login credentials, you can either click on **Don't remember your password** (and follow the prompts) or reach out to your Tenable account manager .

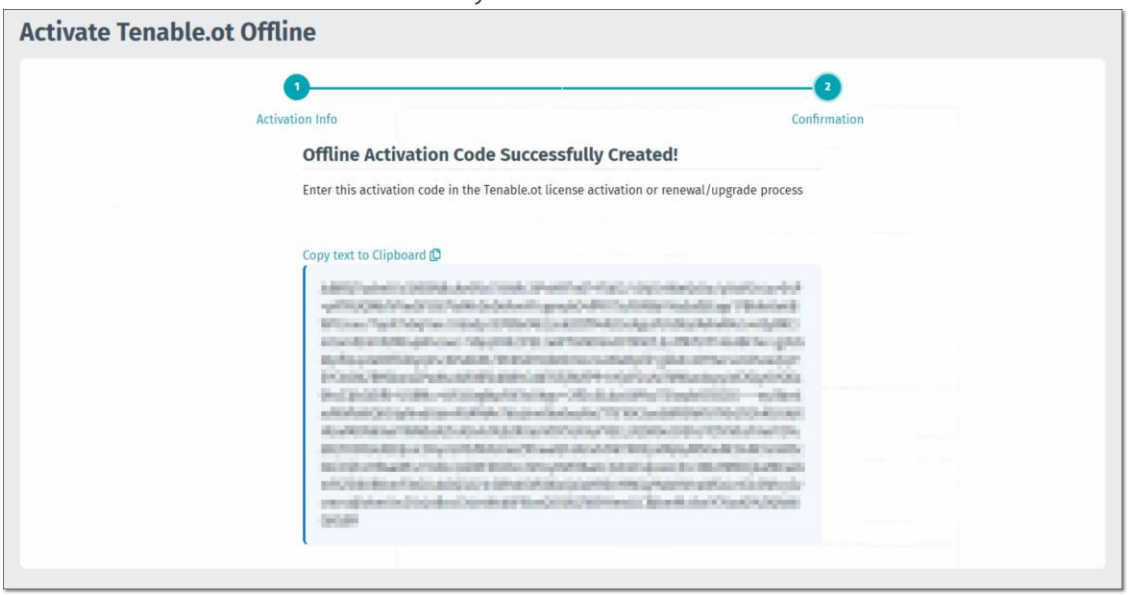
6. In the Activation Certificate field, enter the Activation Certificate.
7. In the **License Code** field, enter the same 20-character **license code** you entered in Step 2 of this procedure.

8. Click the I have read and understand the Tenable Software License Agreement checkbox.



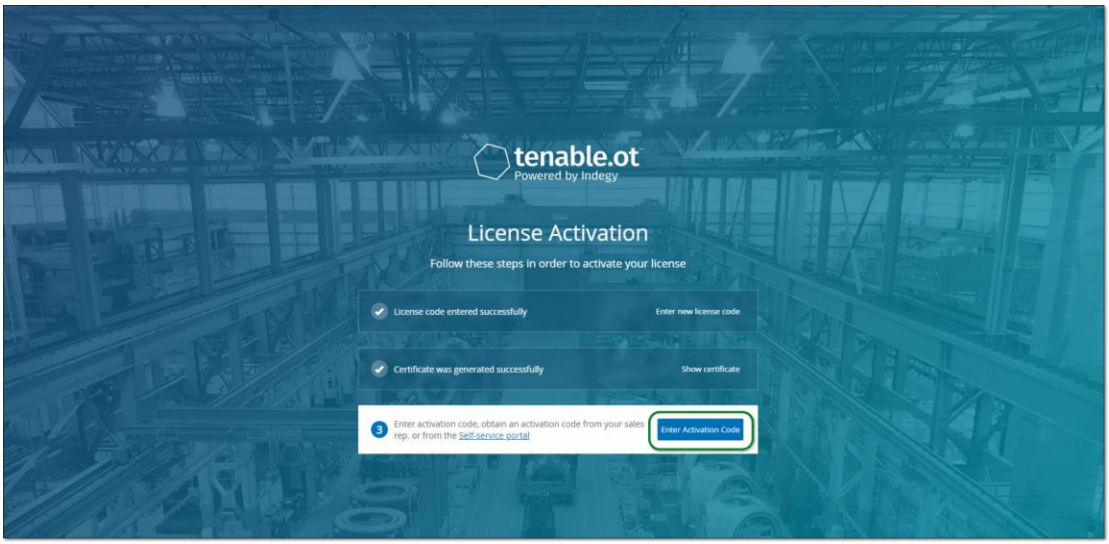
To view the license agreement, click on the **Tenable Software License Agreement** link.

9. Click the Generate Activation Code button.
   The Offline Activation Code Successfully Created! screen is shown.



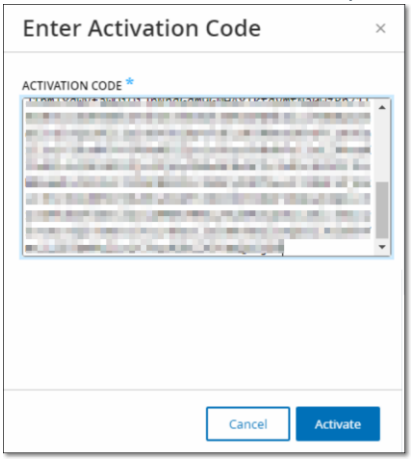
10. Click Copy text to Clipboard.

11. Navigate back to the **License Activation** screen on your Tenable.ot device, and click the **Enter Activation Code** button.



The **Enter Activation Code** side panel is shown.

12. In the **Activation Code** field, paste your activation code and click the **Activate** button.



The side panel closes, and the Tenable.ot home screen is shown. The Enable button is displayed.

For information about updating your license, see **Updating the License**.

Step 6 - Enabling the System

After completing the license activation, the *Enable* button is displayed.

You need to enable the system in order to activate the system's core functionality.

The following functionalities are activated when the system is enabled:

- Identifying Assets in the network
- Collection and monitoring of all network traffic
- Logging 'Conversations' on the network

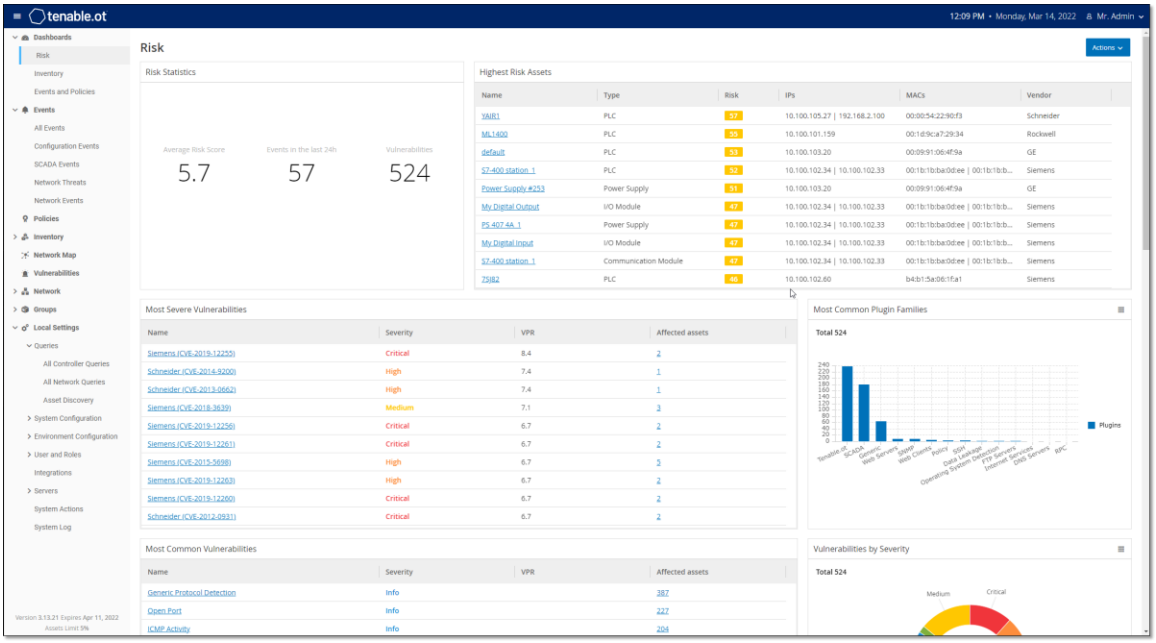
All compiled data and analysis from the above functionalities can be viewed in the Management Console (UI).

These are ongoing processes that continue over time, it will take some time until the results shown in the UI are fully updated.

Additional functions such as Active Queries can be configured and activated on the Local Settings screen in the Management Console (UI), see **QUERIES**.

➡ **To enable the system.**

1. Click the **Enable** button.
   The system is enabled. The UI opens, showing the **Dashboard** > **Risk** screen.



It will take a few minutes for the system to identify your assets. You may need to refresh the page in order to start showing the data.

Step 7 – Connecting the Separate Management Port (for Port Separation Option)

If you have selected the port separation option (to separate Queries from the Management), you must connect Port 3 on the Tenable.ot appliance, which is now the management port, to a port in a network switch. This can be a different network switch, such as a network switch of the IT network.

➡ **To Connect the Management Port:**

1. On the Tenable.ot appliance, connect an Ethernet cable (supplied) to Port 3.
2. Connect the cable to a port on a network switch.

Installing a Tenable.ot Sensor

Pairing Sensors with the ICP

The following section describes the procedure for configuring a Sensor version 3.14 and above. To configure an earlier model sensor, use the procedure described in **Appendix 1 – Installing a Sensor (Version 3.13 and Below).**

Pairing Sensors with the ICP is done using both the ICP Management Console and the Sensor's Tenable Core UI.

You may choose to enable automatic approval of incoming pairing requests, or disable automatic approval in order to require manual approval for each new Sensor pairing request.

Prerequisites

- The Sensor hardware is properly installed (see **Step 1 - Setting up the Sensor**).
- The Sensor is connected to your network switch (see **Step 2 – Connecting the Sensor to the Network**).
- The Sensor has its own static IPv4 address (see **Step 3 – Accessing the Sensor Setup Wizard**).
- The Sensor is connected to Tenable Core platform and you have a username and password for logging into the Core User Interface. For more information on using the Tenable Core User Interface, see https://docs.tenable.com/tenablecore/Tenableot/Content/TenableCore/Introduction_OT.htm.
- Verify you have a valid Certificate in the ICP console (see **Certificate**).
- It is recommended to create a dedicated ICP user with admin role for the process of pairing Sensors, in order to prevent disruptions in connectivity (see **Adding Local Users**). One new admin user may be used to pair multiple Sensors.

Pairing the Sensor

➡ **To pair a Sensor v.3.14 or above with the ICP:**

1. In the ICP Management Console (UI), navigate to the **Local Settings** > **System Configuration** > **Sensors** screen.

2. If you would like to enable automatic approval of Sensor Pairing, ensure that the **Auto Approve Incoming Sensor Pairing Requests** switch at the top of the screen is toggled to **ON**. If not selected, all pairing requests must be manually approved.

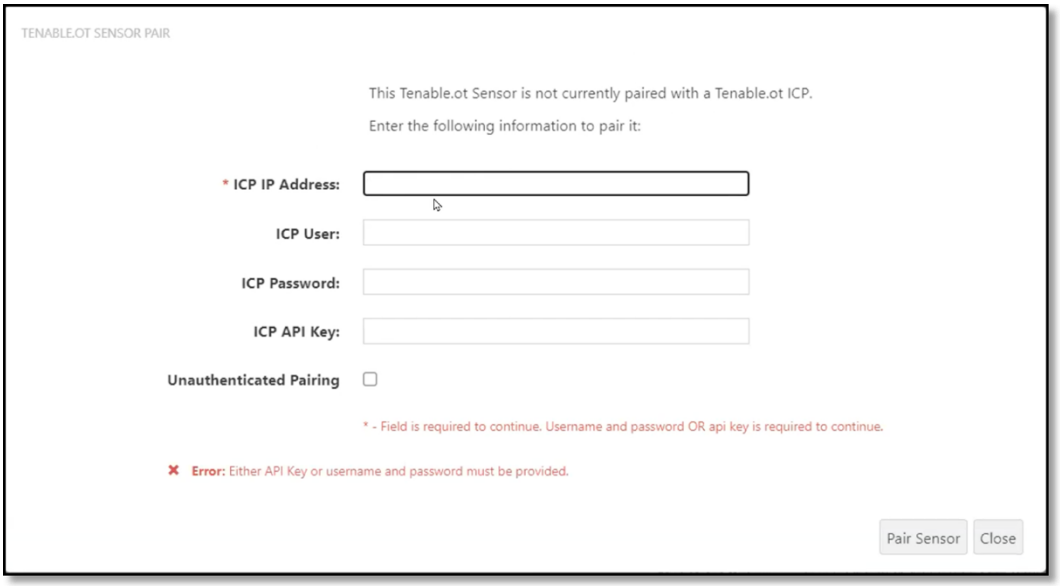
3. Open a new tab, leaving the ICP tab open, and access the Sensor's Tenable Core User Interface by entering **<Sensor IP>:8000**.

> The UI can only be accessed from a Chrome browser. You also need to be using the latest version of Chrome.

4. In the Tenable Core console login window, enter your **User name** and **Password**, select the **Reuse my password for privileged tasks** checkbox, and click **Log In**.

> If the **Reuse my password for privileged tasks** checkbox is not selected upon login, the user will not be able to restart the Sensor service.

5. In the Navigation menu bar, click **Tenable.ot Sensor**.
The **Tenable.ot Sensor Pair** window is displayed.



The **Tenable.ot Sensor Pair** window only pops up the first time the page is loaded. To open the window after this, click on the button in the **Pairing Info** section of the **Tenable Core** console.

6. In the **ICP IP Address** field, enter the IPv4 address for the ICP with which you would like to pair this Sensor.
7. If you would like to use unauthenticated (unencrypted) pairing, click the **Unauthenticated Pairing** checkbox and skip to step 8.

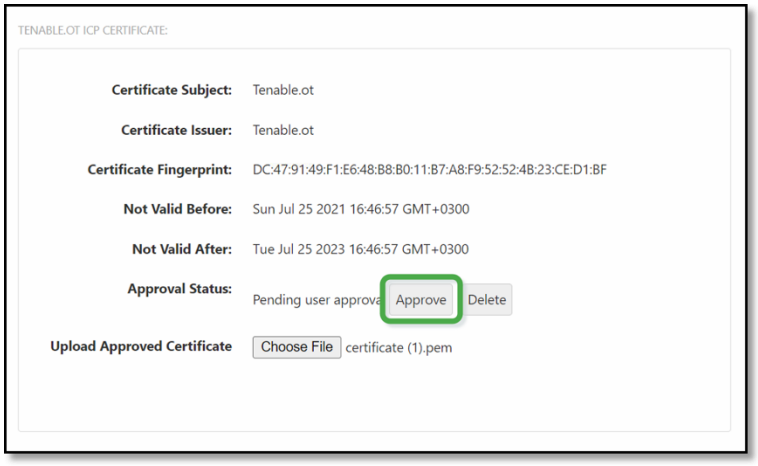
Sensors that use Unauthenticated Pairing will only be able to passively scan their network segments and cannot be managed by the ICP in order to send Active Queries.

8. To authenticate the pairing, do one of the following:
   - Enter the ICP username in the **ICP User** field and the ICP password in the **ICP Password** field, OR
   - Enter an API Key for the ICP in the **ICP API Key** field.

It is recommended to create a dedicated ICP user for pairing Sensors in order to ensure connectivity during the pairing process (see **ADDING LOCAL USERS**).

The method of authentication via username and password has the advantage that the credentials don't expire, as opposed to an API Key that will expire.

9. Click **Pair Sensor**.
10. If you wish to use a Certificate offered by the ICP:
    a. In the **Tenable Core** console, in the **Tenable ICP Certificate** section, under **Approval Status**, wait for the Certificate information to load, then click **Approve** to approve the Certificate.



b. In the **Confirm Accept Tenable.ot Server Certificate** pop-up window, click **Accept This Certificate**.

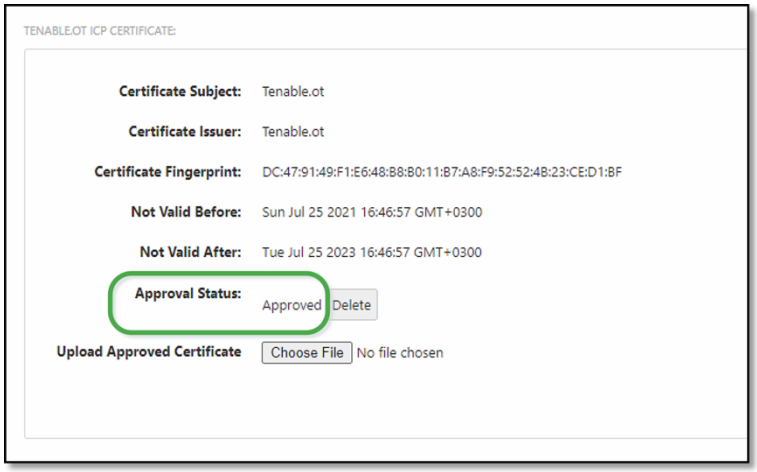
If you prefer to manually upload a Certificate:

a. In the **Tenable ICP** console, follow the procedure described **IN GENERATING AN HTTPS CERTIFICATE.**

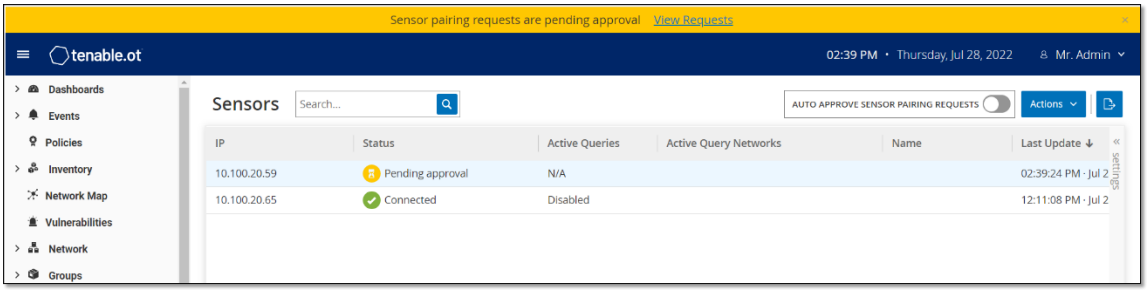
b. In the **Tenable Core** console, in the **Tenable ICP Certificate** section, under **Upload Approved Certificate,** click **Choose File**.

c. Navigate to the .pem Certificate file to upload.

Once a valid Certificate is accepted, its **Approval Status** in the **Tenable.ot ICP Certificate** table is displayed as **Approved**.

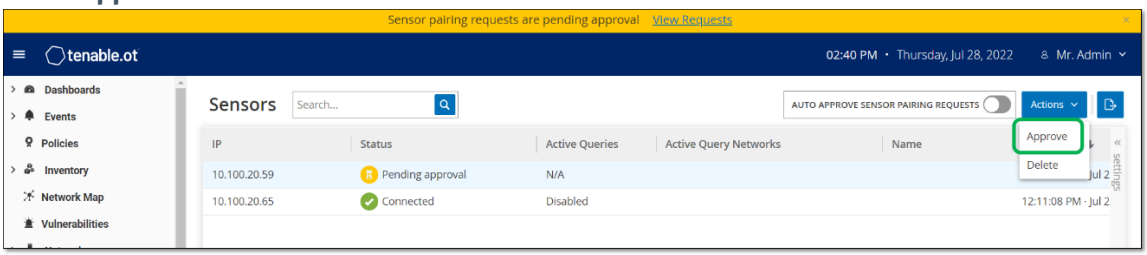


11. In the ICP UI, return to the **Local Settings > System Configuration > Sensors** screen.



The new Sensor is displayed in the table, the Status should be *Pending Approval*.

12. Click on the Sensor's row, then click on the **Actions** button (or right-click on the row) and select **Approve**.



13. The Status should switch to *Connected*, indicating that the pairing was successful. Other possible Statuses are:

- *Connected (Unauthenticated)* – The Sensor is connected in unauthenticated mode. The Sensor can only execute passive network detection.
- *Paused* – The Sensor is connected properly, but has been paused.

- *Disconnected* – The Sensor is not connected. For an authenticated Sesnsor, this may result from an error in the pairing process (e.g. tunnel error, API issue).

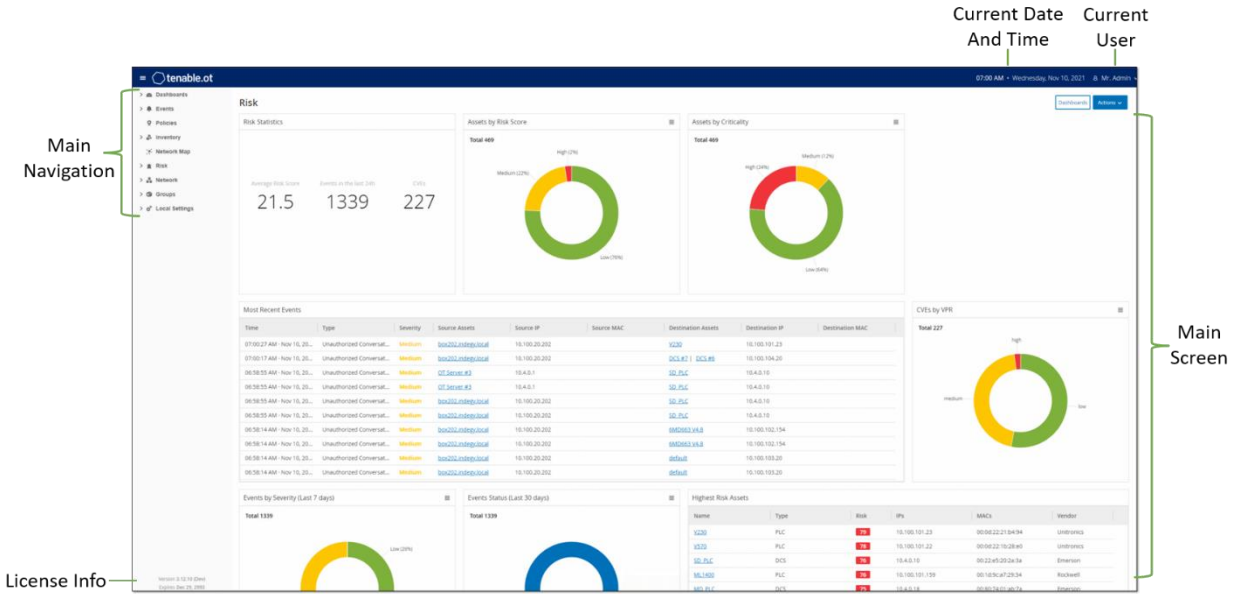
14. Once the pairing has been completed for an Authenticated Sensor, you can configure Active Queries to run on that Sensor. See **Configuring Active Queries**.

Once the pairing has been completed, it is recommended to use only the ICP page to manage the Sensor, and not the Tenable Core UI.

Management Console UI Elements

The Management Console UI provides easy access to important data discovered by Tenable.ot relating to asset management, network activity and security events. You can use the UI to configure the Tenable.ot platform functionality according to your needs. This chapter gives a brief overview of the UI elements. Details about specific UI functionality are provided in the following chapters.

Main UI Elements



The following table describes the Main UI elements which are always shown.

UI Element	Description
Main Navigation	Main navigation menu. Click on the icon to show/hide the navigation menu.
Current Date and Time	Shows the current date and time as registered in the system.
Current User Name	Shows the name of the user who is currently logged into the system. Click on the down arrow for a selection menu. Menu options are About or Logout.
License Info	Shows the Tenable.ot software version and the license expiration date.
Main Screen	Displays the screen that was selected in the Main Navigation.

Main Screens

The UI has several main screens that can be accessed from the Main Navigation. The following is a brief description of the various screens. Each one we will be explained more fully in the following chapters.

- Dashboards - view widgets containing graphs and tables that give an at-a-glance view of your network's inventory and security posture. There are separate dashboards for *Risk*, *Inventory*, and *Events and Policies*. See Chapter **DASHBOARDS**.
- Events - shows all Events that have occurred, as a result of Policy hits, in the system. There is a screen for viewing *All Events* as well as separate screens for viewing Events of each specific type (Configuration Events, SCADA Events, Network Threats or Network Events). See Chapter **EVENTS**.
- Policies - view, edit and activate Policies in the system. See Chapter **POLICIES**.
- Inventory - displays an inventory of all the discovered assets, allowing comprehensive asset management, monitoring of the status of each asset, and viewing their related Events. There is a screen for viewing *All* assets as well as separate screens for viewing assets of specific types (*Controllers and Modules*, *Network Assets* and *IoT*). See Chapter **INVENTORY**.
- Network Map - shows a visual representation of the network assets and their connections.
- Vulnerabilities - shows a detailed list all the threats in the network detected by Tenable.ot Plugins, and provides recommended remediation steps. This section includes CVEs as well as other threats to the assets in your network (e.g. obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, etc.).
- Network - provides a comprehensive view of the network traffic by showing data about conversations that took place between assets in the network over time. See Chapter **NETWORK.** The information is shown on three separate screens:
    - Network Summary - shows an overview of network traffic
    - Packet Captures - shows full-packet captures of network traffic
    - Conversations – shows a list of all conversations detected in the network, with details about the time that it occurred, involved assets etc.
- Groups - view, create and edit Groups, which are used in Policy configuration. See Chapter **GROUPS**.
- Local Settings – view and configure the system settings. See Chapter **LOCAL SETTINGS**.

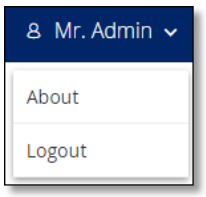
Checking Current Software Version

The user can check the version of his software using the username button in the top-right corner of the header bar.

➡ **To display the current software verision:**

1. In the main header bar, click on the username button in the top-right corner to open the menu.

The user menu is displayed.



2. In the menu, click **About**.
   The current software version is displayed.

Working with Lists

The various Tenable.ot screens display the data relevant to that screen in table format with a list for each item. These tables have standardized customization features, enabling the user to easily access the relevant information. The following sections describe the customization features.

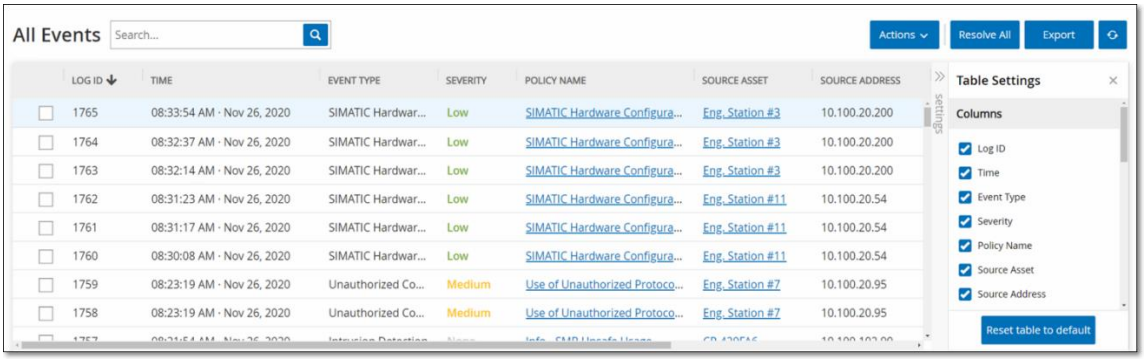
> Examples are shown for the All Events and All Assets screens, but similar functionality is available for most screens in the UI.
>
> You can revert to the default display settings at any time by clicking Settings > Reset table to default.

Customizing the Column Display

You can customize which columns are displayed and how they are organized.

To select which columns are displayed:

1. Click the **Settings** tab along the right edge of the table.
   The **Table Settings** pane is displayed on the right side of the screen, showing the **Columns** section.



2. In the **Columns** section, select the checkbox next to each column that you would like to show.
3. Deselect the checkbox next to each column that you would like to hide.
   Only the selected columns are displayed.
4. Click on the '**x**' (or on the **Settings** tab) to close the *Table Settings* window.

To adjust the order in which the columns are displayed:

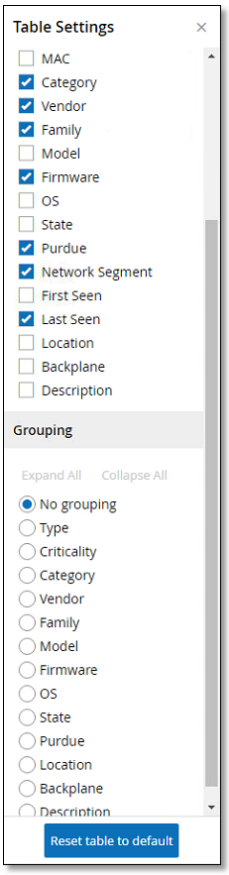
1. Click on a column and drag it to the desired position.

Grouping

For each of the Inventory screens, you can group the lists by various parameters that are relevant to that particular screen.

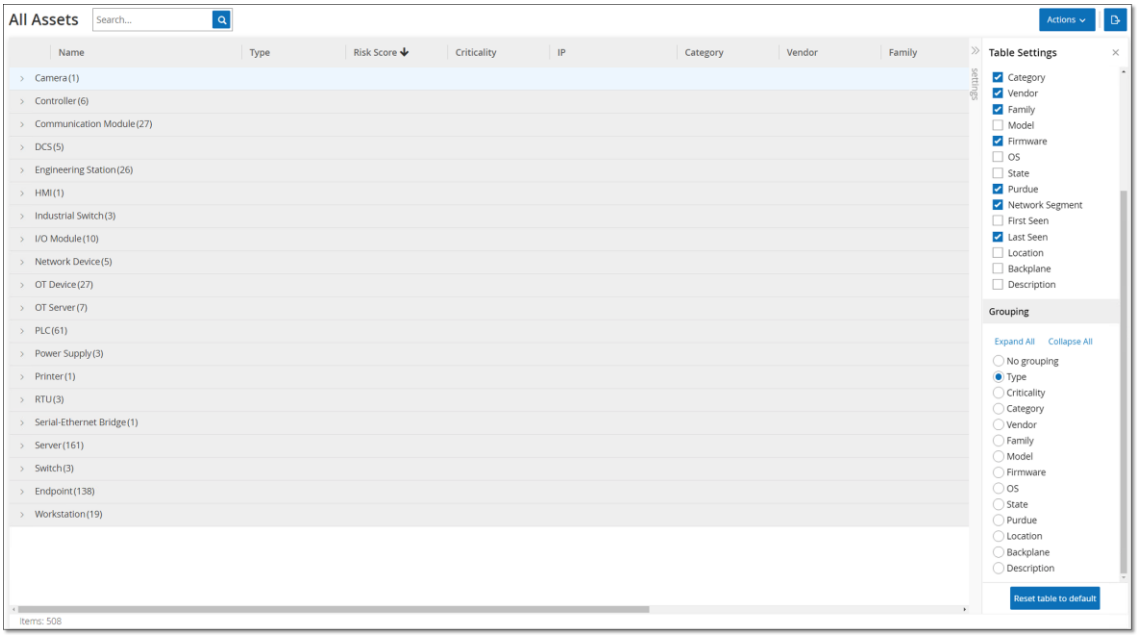
➡ **To group the lists:**

1. Click the **Settings** tab along the right edge of the table.
   The **Table Settings** pane is displayed on the right side of the screen, showing the **Columns** and **Grouping** sections.
2. Scroll down to the **Grouping** section.

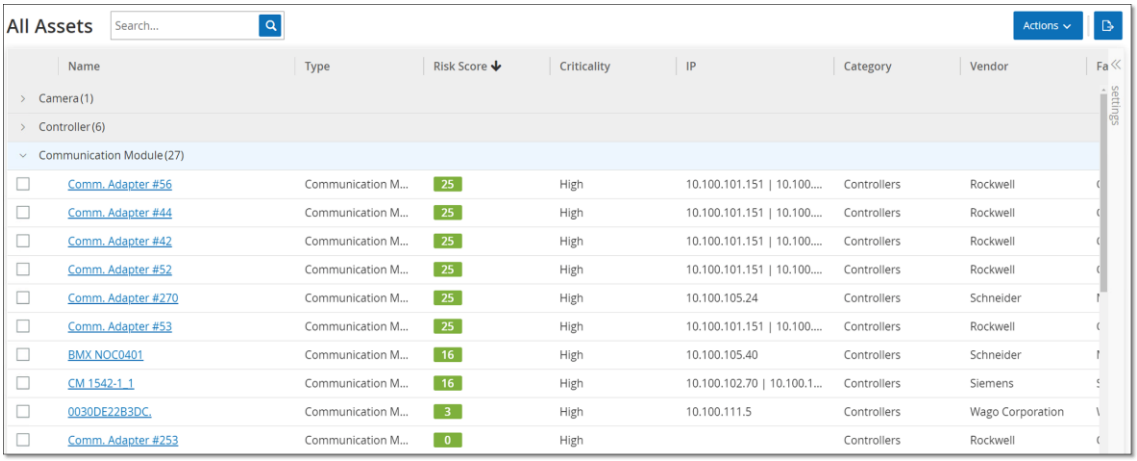


3. Select the radio button next to the parameter by which you would like to group the lists (e.g. Type).

The group categories are displayed in the main window.



4. Click on the '**x**' (or on the **Settings** tab) to close the *Table Settings* window.
5. Click on the arrow next to a category to show all instances for that category.



Sorting

➡ **To sort the lists:**

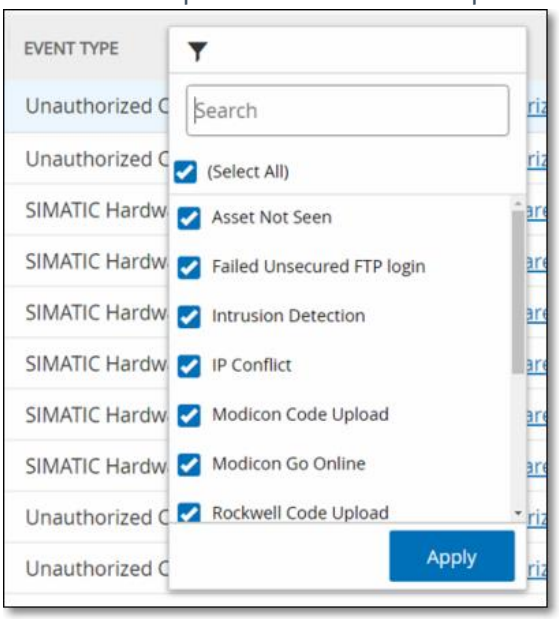
1. Click on a column heading to sort the assets by that parameter (e.g. click on the **Name** heading to display the assets in alphabetical order by Name).
2. Click on the column heading a second time if you would like to reverse the display order (i.e. A→Z, Z→A).

Filtering

You can set filters for one or more column headings. The filters are cumulative so that only lists that fit all the filter criteria are displayed. The filter options are specific to each column heading. Each screen offers a selection of relevant filters. For example, on the Controllers Inventory screen you can filter by *Name*, *Addresses*, *Type*, *Backplane*, *Vendor* etc.

To filter the lists:

1. Hover over a column heading to show the filter icon .
2. Click on the filter icon .
   A list of filter options are shown. The options are specific to each parameter.



3. Select the elements that you would like to display and deselect the ones that you would like to hide.

> You can start by deselecting the **Select All** checkbox and then select the ones that you would like to show.

4. You can search the list for filters and select or deselect them.
5. Click **Apply**.
   The lists are filtered as specified.
6. The filter icon next to the column heading indicates that the results are being filtered by that parameter.

To remove the filters:

1. Click on the filter icon .
2. Click on the *Select All* checkbox to clear all selections.
3. Click **a second time** on the *Select All* checkbox to select all elements.
4. Click **Apply**.

Searching

On each screen, you can search for specific records.

To search the lists:

1. Enter the search text in the Search box.
2. Click on the icon.
3. To clear the search text, click on the '**x**'.

Exporting Data

You can export data from any of the lists shown in the Tenable.ot UI (e.g. Events, Inventory etc.) as a CSV file.

> The exported file includes all data for that page, even if filters have been applied to the current display.

To export data:

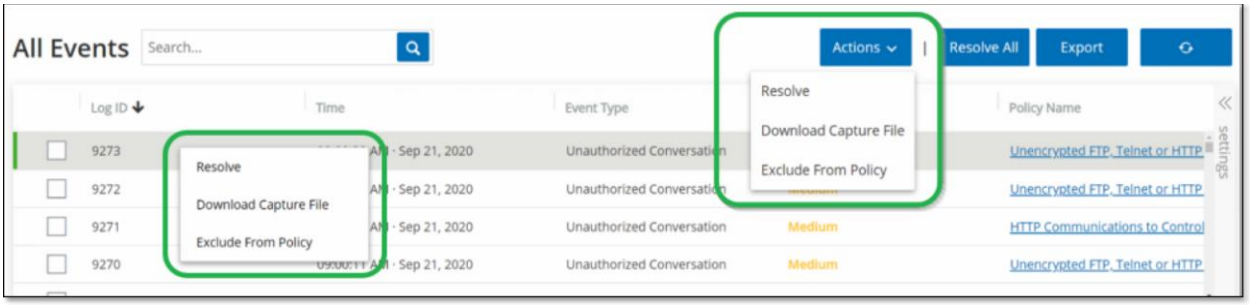
1. Go to the screen for which you want to export data.
2. In the Header Bar, click **Export**.

Actions Menus

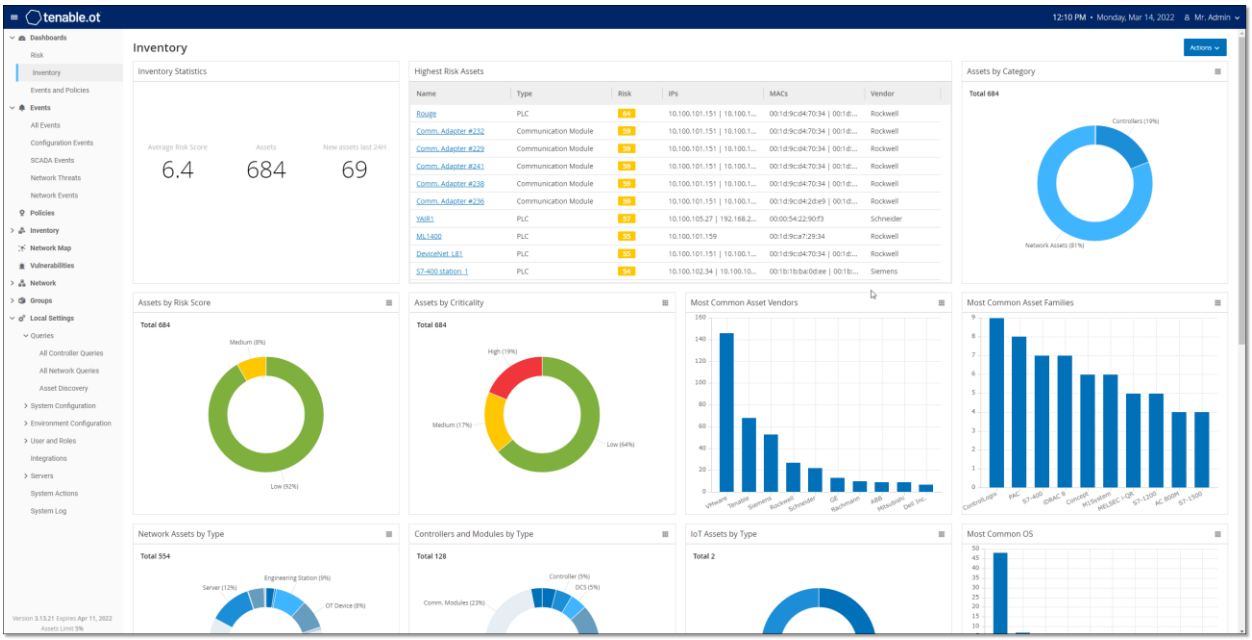
Each screen has a series of Actions that can be taken for the elements listed on that screen. For example, on the Policies screen you can *View*, *Edit*, *Duplicate* or *Delete* a Policy; on the Events screen, you can *Resolve* or *Download Capture File* for an Event etc.

There are two ways of accessing the Actions menu:

- Select an element and then click on the Actions button in the Header bar, OR
- Right-click on the element



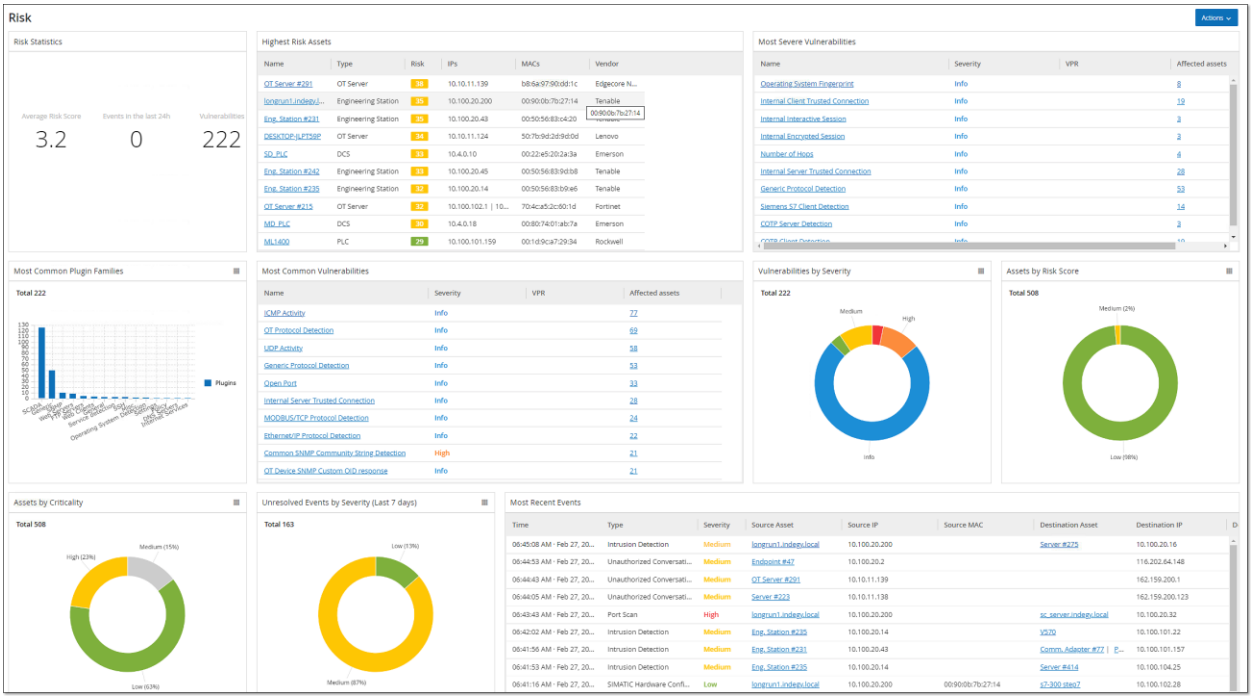
Dashboards



There are three dashboards: *Risk*, *Inventory*, and *Events and Policies*. The dashboards contain widgets that offer an at-a-glance view of your network's inventory and security posture. You can choose a dashboard from the Main Navigation or by clicking on the **Dashboards** button in the upper-right corner, and selecting one from the menu that is shown. The *Risk* dashboard is the initial default view; however, you can change the default view to a different dashboard.

You can interact with dashboards by adjusting the display settings and setting filters, see **Interacting with Dashboards**.

Risk Dashboard

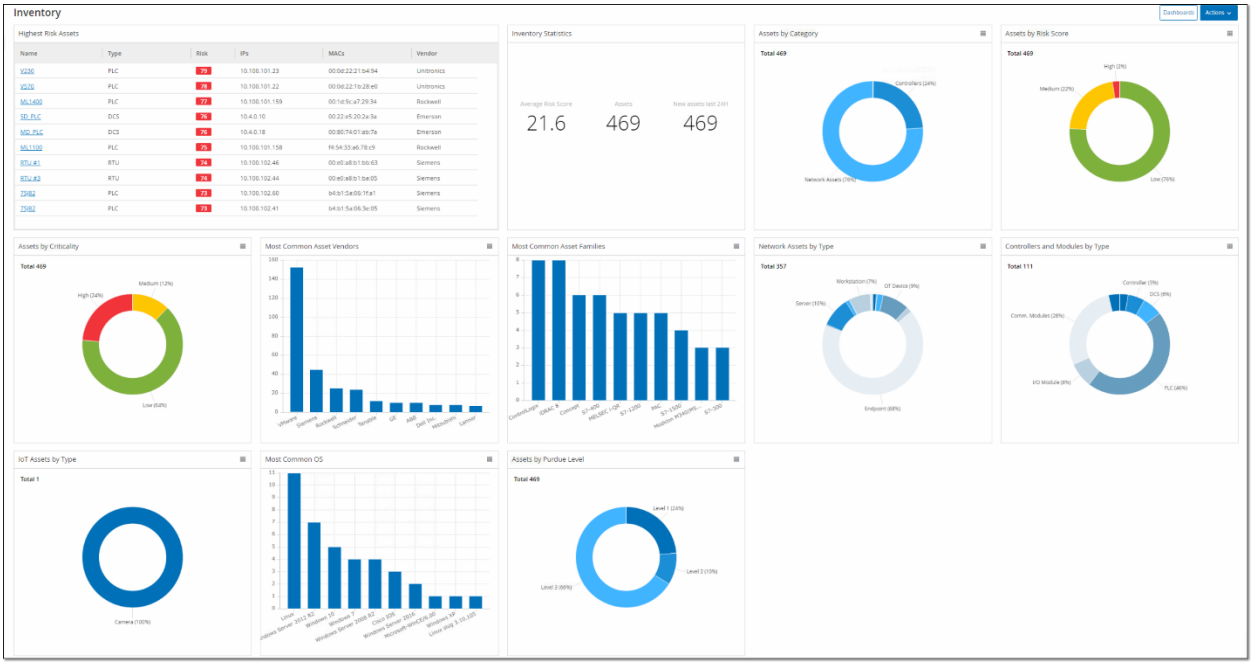


The **Risk** dashboard provides insights on the network's cyber exposure by looking into asset risk scores and vulnerability management metrics.

The **Risk** dashboard shows widgets such as: Risk Statistics, Assets by Risk Score, Assets by Criticality, Events by Severity, Most Common Vulnerabilities, etc.

Clicking on an asset or Vulnerability link takes you to the corresponding element on the Inventory or Vulnerabilities screen, respectively.

Inventory Dashboard

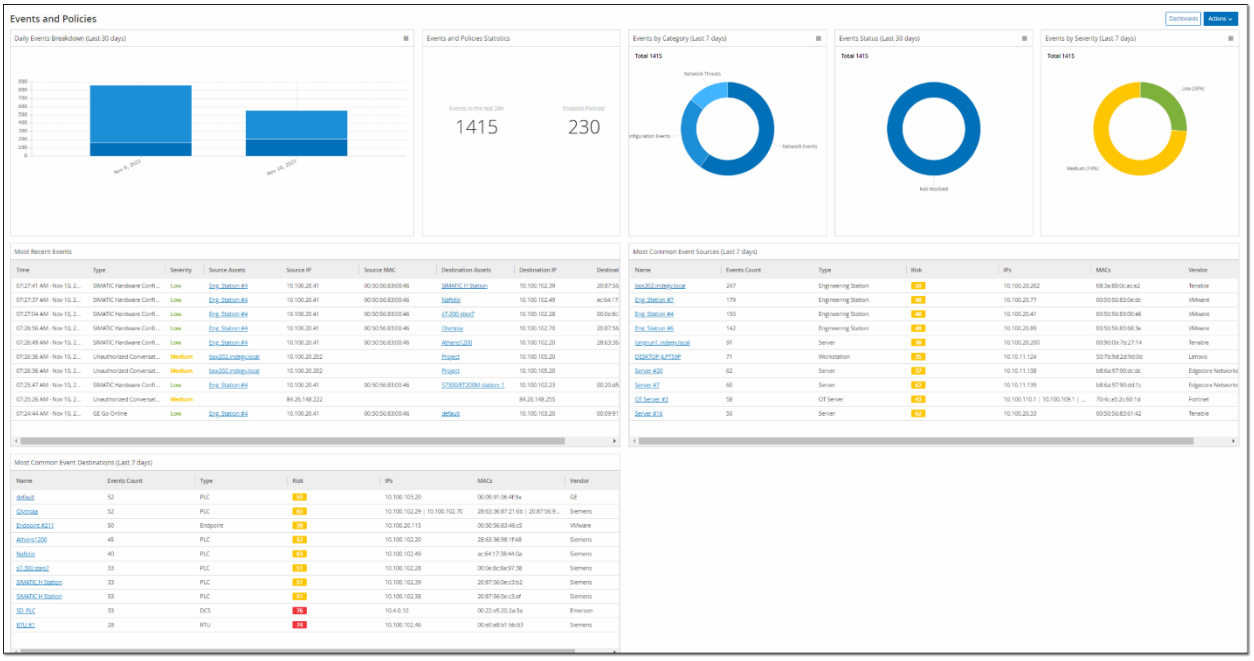


The **Inventory** dashboard provides visibility into the asset inventory, facilitating asset management and tracking.

The **Inventory** dashboard shows widgets such as: Highest Risk Assets, Inventory Statistics, Assets by Risk, Controllers and Modules by Type, Assets by Purdue Level etc.

Clicking on an asset link takes you to the corresponding asset on the Inventory screen.

Events and Policies Dashboard



The **Events and Policies** dashboard provides a means to detect network threats by monitoring the identified events and the policies violations that they generate.

The **Events and Policies** dashboard shows widgets such as: Daily Events Breakdown, Events and Policies Statistics, Events Status, Most Common Event Destinations etc.

Clicking on an asset or event link takes you to the corresponding element in the Inventory or Events screens respectively.

Interacting with Dashboards

You can adjust the dashboard display by interacting with widgets. There are two modes for showing data on the dashboards, graph mode and table mode. Some widgets have a fixed display mode, and some can be toggled back and forth between modes. Widgets with a symbol in the upper-right corner can be viewed in graph mode or table mode. Click on the table/graph symbol to toggle between modes.

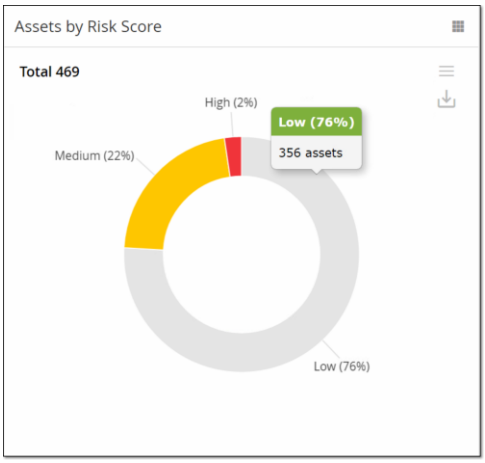
Filters can only be set in table mode. Once a filter is set, it is applied also in graph mode.

Graph mode

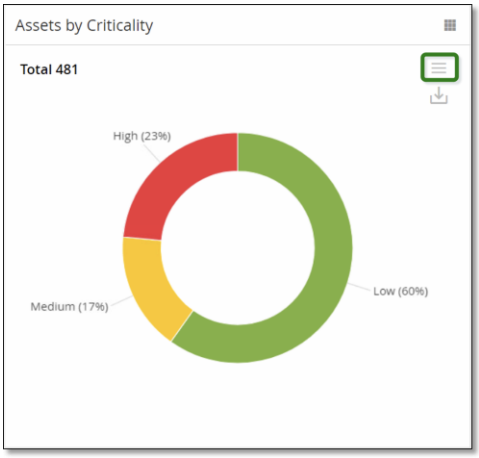
Graph mode shows a graphic visualization of the widget data.

You can interact with the widgets in the following ways:

- Hovering over a point on the graph displays a pop-out window with data specific to that segment of the graph.



You can adjust the type of chart used for the display by clicking on the **Settings** button in the top right corner.



You can then select one of the other chart types from the **Settings** menu.

- When viewing a widget in graph mode, you can download an image of the graph by hovering over the widget and clicking the **Download** icon.

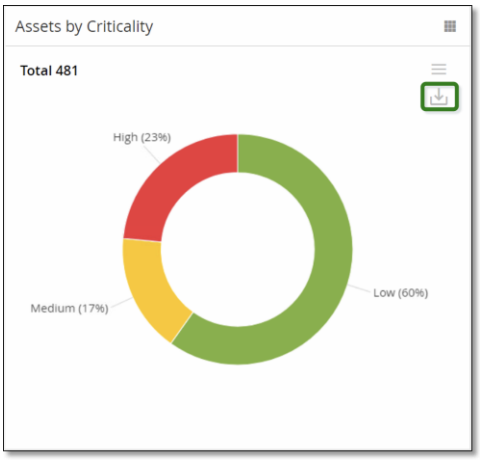
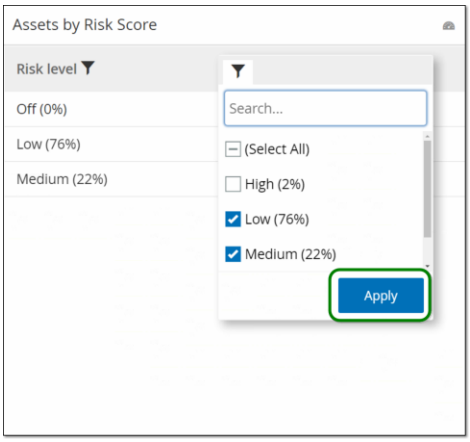


Table mode

When viewing a widget in table mode you can filter each column by hovering over the column header, clicking on the filter icon, choosing your filters, and clicking **Apply**. The filters will also apply to the graph if you switch to graph mode.

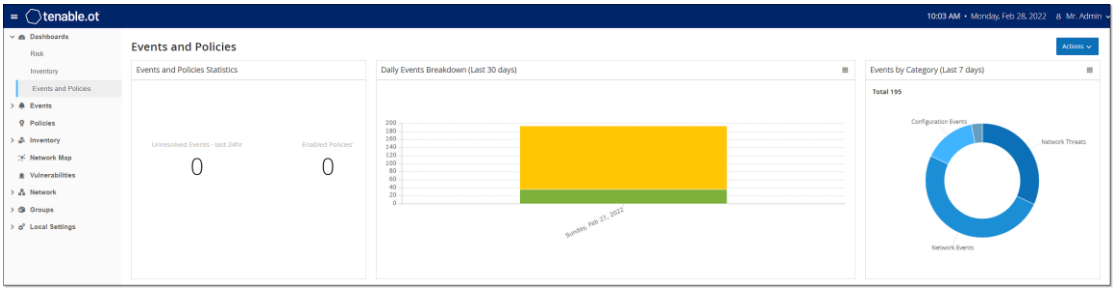


Changing the Default Dashboard

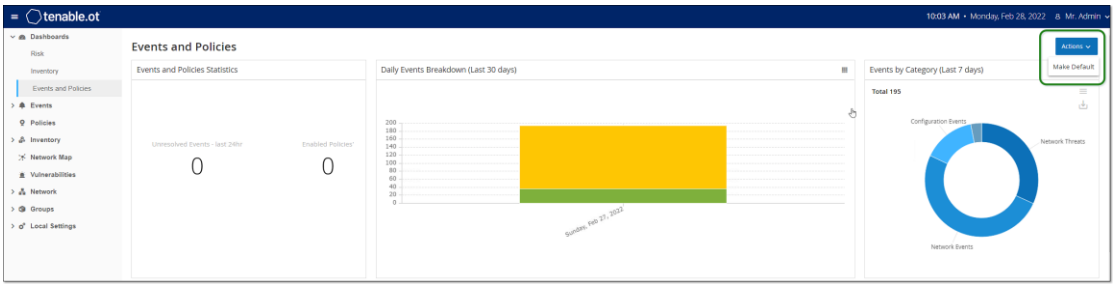
The Risk dashboard is the initial default view of the Management Console. You can designate a different dashboard to be shown as the default view.

To change the default dashboard view:

1. Navigate to the dashboard you wish to set as the default view.



2. Click **Actions** > **Make default**.



The default dashboard is updated. The next time you access the Management Console, this dashboard will be shown.

Policies

Policies are used to define specific types of events that are suspicious, unauthorized, anomalous or otherwise noteworthy that take place in the network. When an event occurs that meets all of the *Policy Definition* conditions for a particular Policy, an Event is generated in the system. The Event is logged in the system and notifications are sent out in accordance with the *Policy Actions* configured for the Policy.

There are two types of policy Events:

- Policy-based Detection – which triggers an Event when the precise conditions of the Policy, as defined by a series of event descriptors, are met.
- Anomaly Detection –which triggers an Event when anomalous or suspicious activity is identified in the network.

The system features a set of predefined policies (out-of-the-box). In addition, the system offers the ability to edit the predefined policies or define new custom policies.

By default, *most* policies are turned on. To turn Policies on/off see **Turning Policies On and Off**.

Policy Configuration

Each Policy consists of a series of conditions that define a specific type of behavior in the network. This includes considerations such as the activity, the assets involved and the timing of the event. Only an event that conforms to **all** the parameters set in the Policy will trigger an Event for that Policy. Each Policy has a designated Policy Actions configuration which defines the severity, notification methods, and logging of the Event.

Groups

An essential component in the definition of Policies in Tenable.ot is the use of *Groups*. When configuring a Policy each of the parameters is designated by a Group as opposed to individual entities. This greatly streamlines the Policy configuration process. For example, if the Activity *Firmware update* is considered a suspicious activity when it is performed on a controller during certain hours of the day (e.g. during work hours), instead of creating a separate Policy for each controller in your network you can create a single Policy that applies to the Asset Group *Controllers*.

The following types of Groups are used as part of the Policy configuration:

- Asset Groups –the system comes with predefined Asset Groups based on asset type. You can add custom groups based on other factors such as location, department, criticality etc.
- Network Segments – the system creates auto-generated Network Segments based on asset type and IP range. You can create custom Network Segments defining any group of assets that should have similar communication patterns.
- Email Groups - you can group multiple email accounts that will receive email notifications for specific Events. For example, grouping by role, department, etc.

- Port Groups – ports that are used in a similar manner can be grouped together. For example, ports that are generally open on Rockwell controllers.
- Protocol Groups – communication protocols can be grouped by the type of protocol (e.g. Modbus), the manufacturer (e.g. Rockwell allowed protocols), etc.
- Schedule Groups – several time ranges can be grouped as a schedule group that has a certain common characteristic. For example, work hours, weekend etc.
- Tag Groups – you can group tags that contain similar operational data in various controllers. For example, tags that control furnace temperature.
- Rule Groups - Rule Groups are comprised of a group of related rules, which are identified by their Suricata Signature IDs (SIDs). These groups are used as a Policy condition for defining Intrusion Detection Policies.

Policies can only be defined using Groups that have been configured in your system. The system comes with a set of predefined Groups. You can edit these Groups and add your own Groups, see Chapter **GROUPS**.

Policy parameters can only be set using Groups, even if you want a Policy to apply to an individual entity you must configure a Group that includes only that entity.

Severity Levels

Each Policy has a specific Severity level assigned to it which indicates the degree of risk posed by the situation that triggered the Event. The meaning of the different Event levels is described in the following table.

Severity	Description
None	The Event is not cause for concern.
Low	No immediate reason for concern. Should be checked out when convenient.
Medium	Moderate concern that potentially harmful activity has occurred. Should be dealt with when convenient.
High	Severe concern that potentially harmful activity has occurred. Should be dealt with immediately.

Event Notifications

When an event occurs that matches the conditions of the policy, an Event is triggered. All Events are displayed in the Events. (Each Event is also listed under the Policy that triggered the Event in the Policies screen and under the Asset that was affected by the Event in the Inventory screen.) In addition, Policies can be configured to send notification of Events to an external SIEM using Syslog protocol and/or to designated email recipients.

- Syslog Notification – Syslog messages use CEF protocol with both Standard Keys and Custom Keys (which are configured for use with Tenable.ot). For an explanation of how to interpret Syslog notifications see **TENABLE.OT SYSLOG INTEGRATION GUIDE**.
- Email Notifications – Email messages include details about the Event that generated the notification as well as suggestions of steps that should be taken to mitigate the threat.

Policy Categories and Sub-Categories

The Policies are organized by the following categories:

- Configuration Event Policies – these Policies relate to the activities that take place in the network. There are two sub-categories of Configuration Event Policies:
    - Controller Validation - these Policies relate to changes that take place in the controllers in the network. This can involve changes in the state of a controller as well as changes to the firmware, asset properties or code blocks. The Policies can be limited to specific schedules (e.g. firmware upgrade during a work day), and/or specific controller/s.
    - Controller Activities – these policies relate to specific engineering commands that impact controllers' state and configuration. It is possible to define specific activities that always generate Events or to designate a set of criteria for generating Events. For example, if certain activities are performed at certain times and/or on certain controllers. Both black lists and white lists of assets, activities and schedules are supported.
- Network Events Policies – these Policies relate to the assets in the network and the communication streams between assets. This includes assets that were added to or removed from the network. It also includes traffic patterns that are anomalous for the network or that have been flagged as raising cause for concern. For example, if an engineering station communicates with a controller using a protocol that is not part of a pre-configured set of protocols (e.g. protocols that are used by controllers manufactured by a specific vendor), an Event is triggered. These policies can be limited to specific schedules and/or specific assets. Vendor specific protocols are organized by vendor for convenience, while any protocol can be used in a policy definition.
- SCADA Event Policies – these Policies detect changes in set-point values which can harm the industrial process. These changes may result from a cyber-attack or human error.
- Network Threats Policies – these Policies use signature-based OT and IT threat detection to identify network traffic that is indicative of intrusion threats. The detection is based on rules that have been catalogued in Suricata's Threats engine.

Policy Types

Within each Category and Sub-Category there are a series of different Types of Policies. The system comes with predefined Policies of each Type. You can also create your own custom Policies of each Type. The following tables explain the various Policy Types, grouped by Category.

Configuration Event – Controller Activities Event Types

Controller Activities relate to the Activities that occur in the network (i.e. the "commands" implemented between assets in the network). There are many different types of Controller Activity Events. Each Type is defined by the type of controller on which the Activity is done and the specific Activity that is identified (i.e. Rockwell PLC stop, SIMATIC code download, Modicon online session etc.).

The Policy Definition parameters (i.e. policy conditions) that apply to Controller Activity Events are *Source Asset*, *Destination Asset* and *Schedule*.

Configuration Event - Controller Validation Event Types

The following table describes the various types of Controller Validation Events.

Policy conditions relating to Affected Assets, Sources or Destinations can be specified by selecting either an *Asset Group* or a *Network Segment*.

Event Type	Policy Conditions	Description
Change in key switch	Affected Asset, Schedule	A change was made to the controller state by adjusting the physical key position. (Currently supported for Rockwell controllers only.)
Change in state	Affected Asset, Schedule	The controller changed from one operational state (e.g. running, stopped, test etc.) to another.
Change in firmware version	Affected Asset, Schedule	A change was made to the firmware running on the controller.
Module not seen	Affected Asset, Schedule	Detects a previously identified module that was removed from a backplane.
New module discovered	Affected Asset, Schedule	Detects a new module that is added to an existing backplane.
Snapshot mismatch	Affected Asset, Schedule	The most recent Snapshot (which captures the current state of the program deployed on a controller) of a controller was not identical to the previous Snapshot of that controller.

Network Event Types

The following table describes the various types of Network Events.

> Policy conditions relating to Affected Assets, Sources or Destinations can be specified by selecting either an *Asset Group* or a *Network Segment*.

Event Type	Policy Conditions	Description
Asset not seen	Not seen for, Affected Asset, Schedule	Detects previously identified assets in the *Affected Asset* Group that are removed from the network for the specified duration of time during the specified time range.
Change in USB configuration	Affected Assets, Schedule	Detects when a USB device is connected to or removed from a Windows based workstation. The Policy applies to changes to an asset in the Affected Asset Group during the specified time range.
IP conflict	Schedule	Detects multiple assets in the network using the same IP Address. This may indicate a cyber-attack or it may result from poor network management. The Policy applies to IP Conflicts discovered during the specified time range.
Network Baseline Deviation	Source, Destination, Protocol, Schedule	Detects new connections between assets that did not communicate with each other during the Network Baseline sampling. This option is only available once a Network Baseline has been set up in the system. To set the initial Network Baseline or to update the Network Baseline follow the procedures described in section **Setting a Network Baseline**. The Policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group using a Protocol from the Protocol Group during the specified time range.
New asset discovered	Affected Asset, Schedule	Detects new assets of the type specified in the *Source* Asset Group that appear in your network during the specified time range.

Event Type	Policy Conditions	Description
Open port	Affected Asset, Port	Detects new open ports in your network. Unused open ports can pose a security risk. The Policy applies to assets in the Affected Asset Group and to ports that are in the Port Group.
Spike in network traffic	Time window, Sensitivity level, Schedule	Detects anomalous spikes in the network traffic volume. The Policy applies to spikes relative to the specified time window and based on the specified sensitivity level. It is also limited to the specified time range.
Spike in conversation	Time window, Sensitivity level, Schedule	Detects anomalous spikes in the number of conversations in the network. The Policy applies to spikes relative to the specified time window and based on the specified sensitivity level. It is also limited to the specified time range.
RDP connection (authenticated)	Source, Destination, Schedule	An RDP (Remote Desktop Connection) was made in the network using authentication credentials. The Policy applies to asset in the *Source* Asset Group connecting to an asset in the *Destination* Asset Group during the specified time range.
RDP connection (not authenticated)	Source, Destination, Schedule	An RDP (Remote Desktop Connection) was made in the network without using authentication credentials. The Policy applies to asset in the *Source* Asset Group connecting to an asset in the *Destination* Asset Group during the specified time range.
Unauthorized conversation	Source, Destination, Protocol, Schedule	Detects communication sent between assets in the network. The Policy applies to communication sent from an asset in the *Source* Asset Group to an asset in the *Destination* Asset Group using a *Protocol* from the Protocol Group during the specified time range.
Successful unsecured FTP login	Source, Destination, Schedule	FTP is considered to be an unsecure protocol. This Policy detects successful logins using FTP.

Event Type	Policy Conditions	Description
Failed unsecured FTP login	Source, Destination, Schedule	FTP is considered to be an unsecure protocol. This Policy detects failed login attempts using FTP.
Successful unsecured Telnet login	Source, Destination, Schedule	Telnet is considered to be an unsecure protocol. This Policy detects successful logins using Telnet.
Failed unsecured Telnet login	Source, Destination, Schedule	Telnet is considered to be an unsecure protocol. This Policy detects failed login attempts using Telnet.
Unsecured Telnet login attempt	Source, Destination, Schedule	Telnet is considered to be an unsecure protocol. This Policy detects login attempts using Telnet (for which the result status was not detected).

Network Threat Event Types

The following table describes the various types of Network Threat Events.

Policy conditions relating to Affected Assets, Sources or Destinations can be specified by selecting either an *Asset Group* or a *Network Segment*.

Event Type	Policy Conditions	Description
Intrusion Detection	Source, Affected Asset, Rule Group, Schedule	Intrusion Detection Policies use signature-based OT and IT threat detection to identify network traffic that is indicative of intrusion threats. The detection is based on rules that have been catalogued in Suricata's Threats engine. The rules are grouped into categories (e.g. ICS Attacks, Denial of Service, Malware etc.) and sub-categories (e.g. ICS Attacks - Stuxnet, ICS Attacks – Black Energy etc.). The system comes with a series of Predefined groups of related rules. You can also configure your own custom groupings of various rules.

Event Type	Policy Conditions	Description
ARP scan	Affected Asset, Schedule	Detects ARP scans (network reconnaissance activity) that are run in the network. The Policy applies to scans that are broadcasted affect an in the *Affected* Asset Group during the specified time range.
Port scan	Source Asset, Destination Asset, Schedule	Detects SYN scans (network reconnaissance activity) that are run in the network to detect open (vulnerable) ports. The Policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group during the specified time range.

SCADA Event Types

The following table describes the various types of SCADA Event types.

Policy conditions relating to Affected Assets, Sources or Destinations can be specified by selecting either an *Asset Group* or a *Network Segment*.

Event Type	Policy Conditions	Description
Modbus illegal data address	Source Asset, Destination Asset, Schedule	Detects "illegal data address" error code in Modbus protocol. The Policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group during the specified time range.
Modbus illegal data value	Source Asset, Destination Asset, Schedule	Detects "illegal data value" error code in Modbus protocol. The Policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group during the specified time range.
Modbus illegal function	Source Asset, Destination Asset, Schedule	Detects "illegal function" error code in Modbus protocol. The Policy applies to communication from an asset in the Source Asset Group to an asset in the Destination Asset Group during the specified time range.

Event Type	Policy Conditions	Description
Unauthorized write	Source Asset, Tag Group, Tag value, Schedule	Detects unauthorized tag writes to the specified tag/s on a controller (currently supported for Rockwell and S7 controllers) in the specified Source Asset Group. The Policy can be configured to detect any new write, a change from a specified value or a value outside of a specified range. The Policy only applies during the specified time range.
ABB - Unauthorized write	Source Asset, Destination Asset, Schedule	Detects write commands sent over MMS to ABB 800xA controllers that are out of the allowed range.
IEC 60870-5-104 Commands (Start/Stop Data Transfer, Interrogation Command, Counter Interrogation Command, Clock Synchronization Command, Reset Process Command, Test Command with Time Tag)	Source Asset, Destination Asset, Schedule	Detects specific commands sent to IEC-104 master or slave units that are considered to be risky.
DNP3 Commands	Source Asset, Destination Asset, Schedule	Detects all main commands sent using DNP3 protocol, e.g. Select, Operate, Warm/Cold Restart etc. Also detects errors originating from internal indicators such as unsupported function codes and parameter errors.

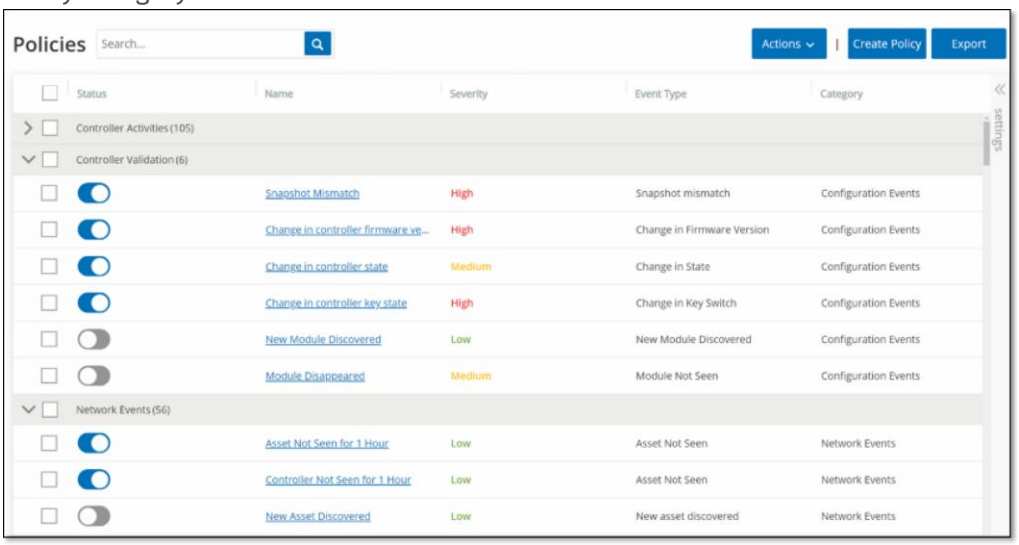
Turning Policies On and Off

Any Policy that is already configured in your system (both pre-configured and user defined) can easily be turned on or off. You can turn Policies on and off on an individual bases or you can select multiple Policies to turn on/off in a bulk process.

Many policies depend on using Queries to collect data. If some or all of the Query functions are disabled, then the related Policies won't be effective. Queries can be activated by going to **Local Settings** > **Queries**, see **QUERIES**.

To turn a Policy on/off:

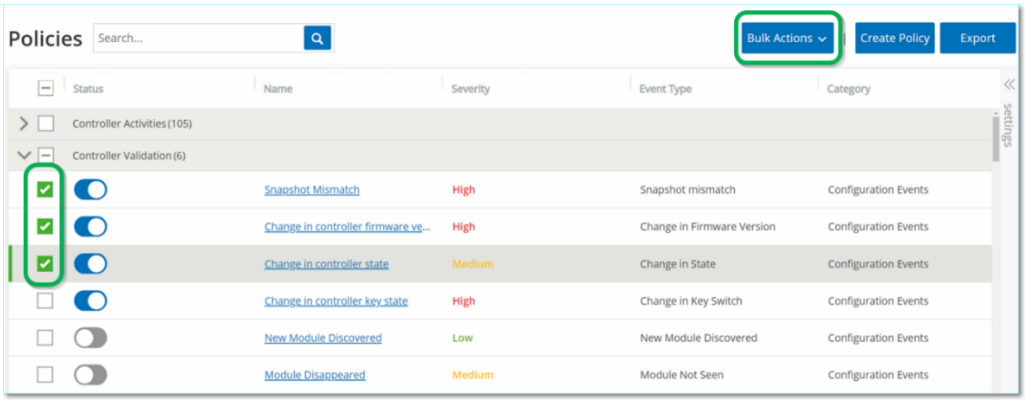
1. Go to the **Policies** screen.
   A list is shown for each Policy that is configured in the system. The Policy lists are grouped by Policy Category.



2. Toggle the **Status** switch next to the relevant Policy **ON/OFF**.

To turn on/off multiple Policies:

1. Go to the **Policies** screen.
   A list is shown for each Policy that is configured in the system. The Policy lists are grouped by Policy Category.



2. Select the checkbox next to each of the Policies that you would like to turn on/off. Use one of the following selection methods:
   - **Select individual Policies** – click the checkbox next to specific Policies.
   - **Select Policy Types** – click the checkbox next to a Policy Type heading.
   - **Select all Policies** – click the checkbox in the Title bar at the top of the table.
3. Click on the **Bulk Actions** button in the Header bar.
4. Select the desired action (**Enable** or **Disable**) from the dropdown list.
   All the selected Policies are turned on/off.

Viewing Policies

The **Policies** screen shows listing for each Policy that is configured in your system. The lists are grouped under separate tabs for each Policy Category. Both pre-configured Policies and user defined Policies are listed on this screen. The listing for each policy includes a toggle switch showing the current status of the Policy as well as several parameters indicating the Policy configuration.

You can show/hide columns and sort and filter the asset lists as well as searching for keywords. For an explanation of the customization features, see **Working with Lists**.

The Policy parameters are described in the following table.

Parameter	Description
Status	Shows if the Policy is turned on or off. If the Policy was automatically disabled by the system because it was generating too many Events, then a warning icon is displayed. Toggle the status switch to turn a Policy ON/OFF.
Policy ID	A unique identifier for the Policy in the system. Policy IDs are grouped by category, with a different prefix for each category (e.g. P1 for Controller Activities, P2 for Network Events etc.).
Name	The name of the Policy.
Severity	The degree of severity of the Event. Possible values are: None, Low, Medium or High. See section **Severity Levels** for a description of the severity levels.
Event Type	The specific type of event that triggers this Event Policy.
Category	The general category of the type event that triggers this Event Policy. Possible values are: Configuration, SCADA, Network Threats or Network Event. For an explanation of the various categories see **Policy Categories and Sub-Categories**.
Source	A Policy condition. The source Asset Group/Network Segment (i.e. the asset that initiated the Activity) to which the Policy applies.
Destination/ Affected Asset	A Policy condition. The destination Asset Group/Network Segment (i.e. the asset which receives the Activity) to which the Policy applies. For Policies that involve a single asset (no source and destination), this parameter shows the asset that was affected by the event.
Schedule	A Policy condition. The time range for which the Policy applies.
Syslog	The Syslog server (SIEM) where Events for this Policy are logged.
Email	The Email Group to which Event notifications for this Policy are sent.

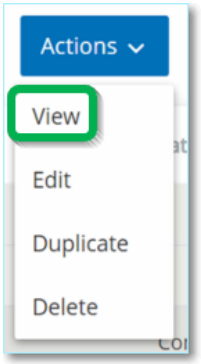
Parameter	Description
Sub Category	The sub-category classification of the Event. The category *Configuration Events* is made up of the sub-categories *Controller Activities* and *Controller Validation*. For an explanation of the different sub-categories, see **Policy Categories and Sub-Categories**.
Number of Events per Policy	Lists the number of events that were generated by every policy. By clicking the column, it is possible to sort the list in order to focus on the policies that had the most violations/events.
Exclusions	Lists the number of exclusions that were added to each policy. For more information, see **Creating Policy Exclusions**.

Viewing Policy Details

You can open the Policy Details screen for a Policy to view additional details about the Policy. This screen shows a complete listing of all Policy conditions. It also shows a listing of all Events triggered by the selected Policy.

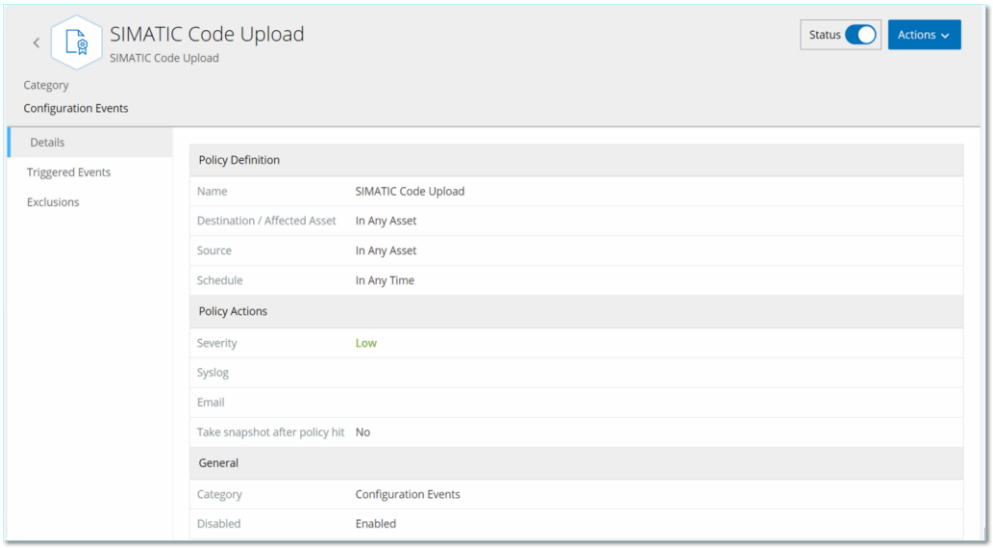
➡ **To open the Policy Details screen for a particular Policy:**

1. On the **Policies** screen, select the desired Policy.
2. Click on the **Actions** menu and select **View** from the dropdown list.



Alternatively, you can access the Actions menu by right-clicking on the relevant Policy.

The Policy Details screen is shown for the selected Policy.



The Policy Details screen contains the following elements:

- Header bar – shows the Name, Type and Category of the Policy. It also has a toggle switch to turn the Policy ON/OFF and a dropdown list of available Actions (Edit, Duplicate and Delete).
- Details tab – shows details about the Policy configuration in three sections:
  - Policy Definition – shows all Policy conditions. This includes all relevant fields according to the Type of Policy.
  - Policy Actions – shows the severity level as well as destination (Syslog, Email) of Event notifications. Also, shows whether the *Disable after first hit* feature is activated.
  - General – shows the category and status of the Policy.
- Triggered Events tab – shows a list of Events that were triggered by this Policy. For each Event, information is shown about the asset/s involved in the Event and the nature of the Event. The information shown in this tab is identical to the information shown on the Events screen except that only Events for the specified Policy are shown here. For an explanation of the Event information, see **Viewing Events**. Exclusions tab - If you find that a Policy is generating Events for specific conditions which don't pose a security threat, you can *Exclude* those conditions from the Policy (i.e. stop generating Events for those particular conditions). This is done on the Events screen, see **Creating Policy Exclusions**. The Exclusions tab shows all Exclusions that have been applied to this Policy. For each Exclusion, the specific conditions that have been excluded are displayed. From this tab you can delete an Exclusion (enabling the system to resume generating Events for the specified conditions).

Creating Policies

You can create custom Policies based on the specific considerations of your ICS network. You can determine precisely what type of events should be brought to the attention of your staff and how the notifications are delivered. You have complete flexibility in determining how specific or broad a definition you would like to give to each Policy.

Policies are defined by using Groups that have been configured in your system. If the dropdown list for a certain parameter doesn't show the specific grouping to which you would like the Policy to apply, then you can create a new Group according to your needs, see Groups.

When creating a new Policy, you start by selecting the *Category* and *Type* of Policy that you would like to create. The *Create Policy* wizard guides you through the setup process. Each Policy Type has its own set of relevant Policy condition parameters. The Create Policy wizard shows you the relevant Policy condition parameters for that selected Type of Policy.

For the *Source*, *Destination* and *Schedule* parameters, you can designate whether to whitelist or blacklist the specified Group.

- select In to whitelist the specified Group (i.e. include it in the Policy), OR
- select Not in to blacklist the specified Group (i.e. leave it out of the Policy).

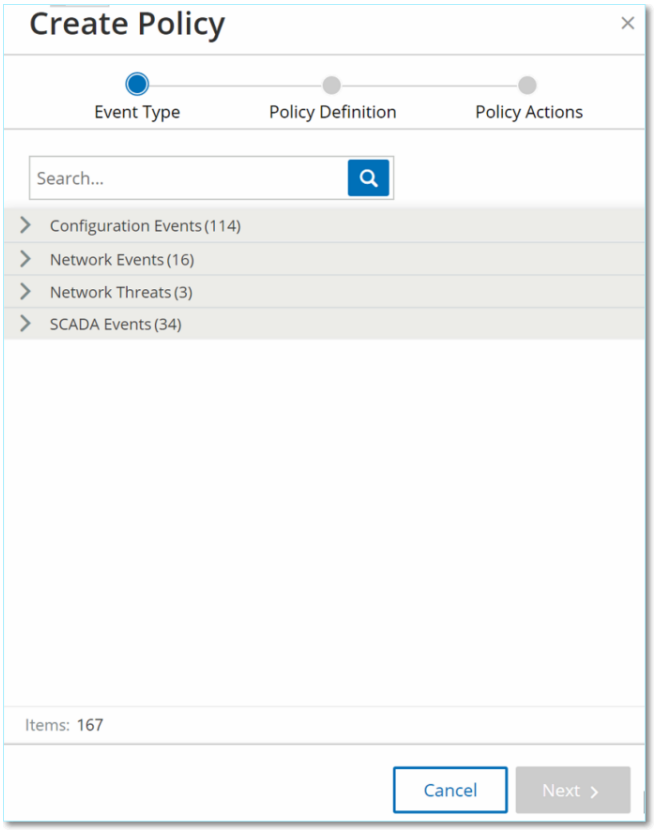
For Asset Group and Network Segment parameters (i.e. *Source, Destination* and *Affected Assets*) you can use logical operators (and/or) to apply the Policy to various combinations or subsets of your pre-defined Groups. For example, if you want a Policy to apply to any device that is either an *ICS Device* or an *ICS Server*, then select *ICS Devices* or *ICS Servers*. If you want a Policy to apply only to *Controllers* which are located in *Plant A*, then select *Controllers* and *Plant A Devices*.

If you would like to create a new Policy with similar parameters to an existing Policy, you can *Duplicate* the original Policy and make the necessary changes, see section **Duplicating Policies**.

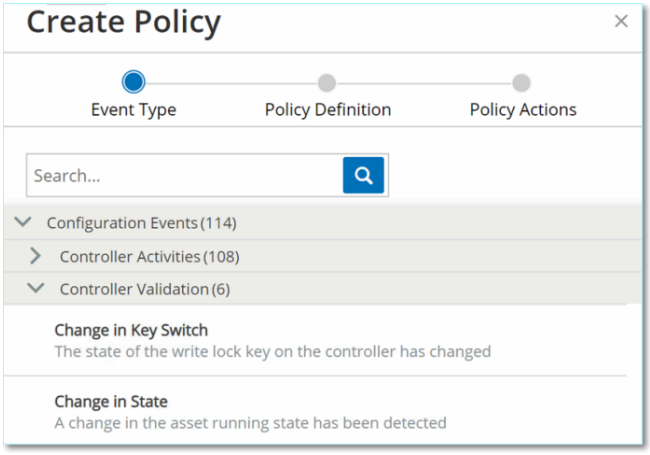
If, after creating a Policy, you find that the Policy is generating Events for situations that don't require attention, you can exclude specific conditions from the Policy, see **Creating Policy Exclusions**.

To Create a New Policy:

1. On the **Policies** screen, click **Create Policy**.
   The **Create Policy** wizard opens.

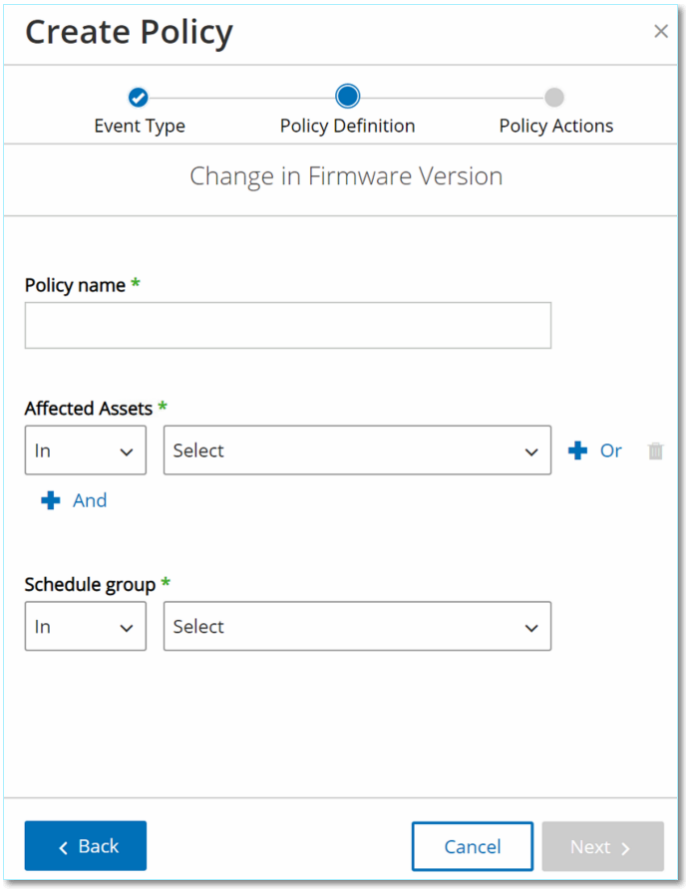


2. Click on a **Policy Category** to show the sub-categories and/or Policy Types.
   A list of all sub-categories and/or Types included in that category are displayed.



3. Select a Policy Type.
4. Click **Next**.
   A series of parameters for defining the Policy are displayed. This includes all relevant Policy

conditions for the selected Policy Type.

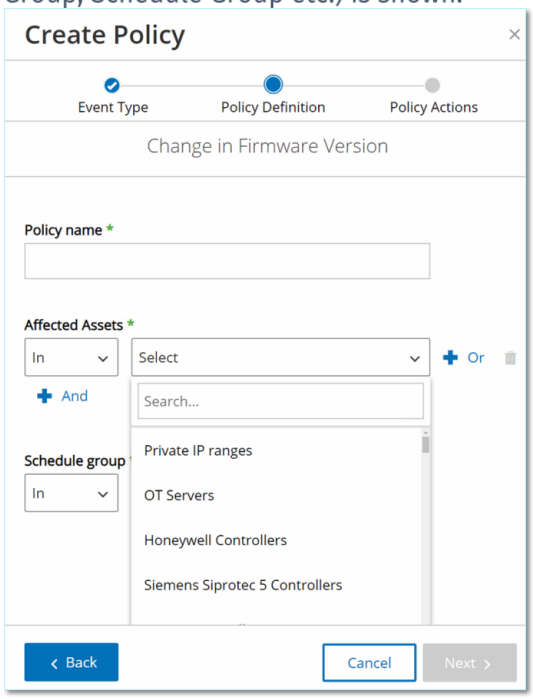


5. In the **Policy Name** field, enter a name for this Policy.

	Choose a name that describes the specific nature of the type of Event that the Policy is intended to detect.

6. For each parameter that is shown:
    a. Where relevant, select **In** (default) to whitelist the selected element or **Not in** to blacklist the selected element.

b. Click on **Select**.
A dropdown list of relevant elements (e.g. Asset Group, Network Segment, Port Group, Schedule Group etc.) is shown.



c. Select the desired element.

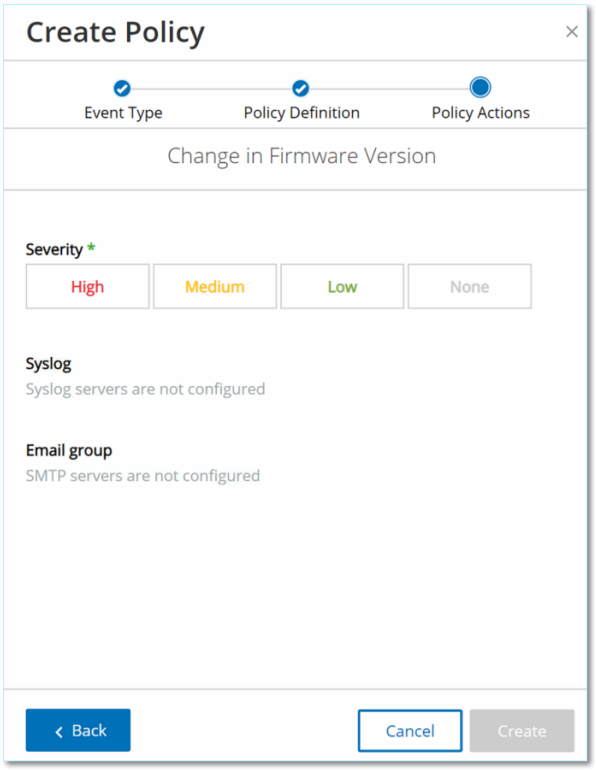
> If the precise grouping to which you would like to apply the Policy does not exist, then you can create a new Group according to your needs, see **GROUPS**.

d. For Asset parameters (i.e. *Source*, *Destination* and *Affected Assets*), if you would like to add an additional Asset Group/Network Segment with an "Or" condition, click on the blue **+ Or** button next to the field and select another Asset Group/Network Segment.

e. For Asset parameters (i.e. *Source*, *Destination* and *Affected Assets*), if you would like to add an additional Asset Group/Network Segment with an "And" condition, click on the blue **+ And** button below the field and select another Asset Group/Network Segment.

7. Once all fields have been filled in, click **Next**.
A series of Policy Action parameters (i.e. the actions taken by the system when a Policy hit

occurs) are shown.



8. In the **Severity** section, click on the desired severity level for this Policy.
9. If you would like to send Event logs to one or more Syslog servers, in the **Syslog** section, select the checkbox next to each server where you would like to send the Event logs.

> To add a Syslog server, see **Syslog Server**.

10. If you would like to send email notifications of Events, in the **Email group** field, select from the dropdown list the Email Group to be notified.

> To add an SMTP server, see **SMTP Server**.

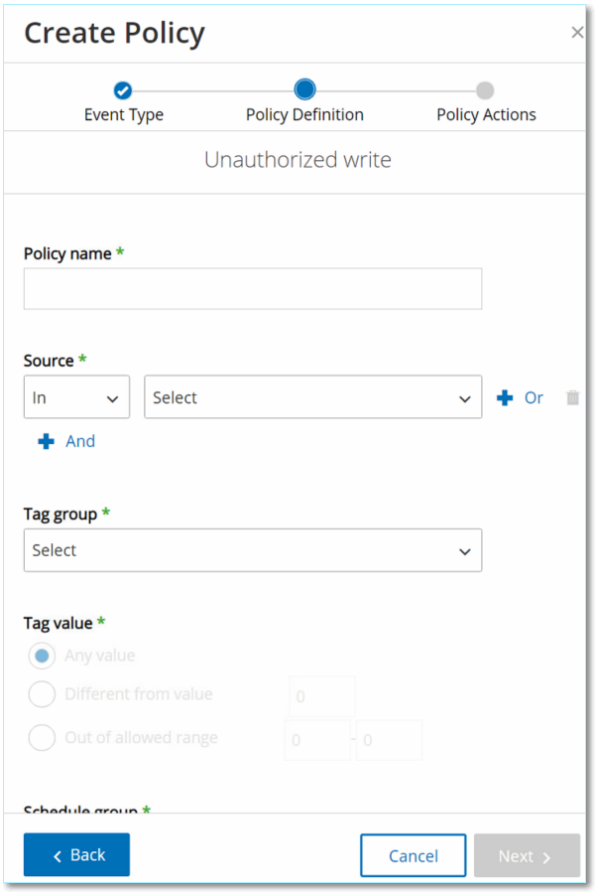
11. In the **Additional Actions** section, where the specified action is relevant:
    - If you would like to disable the Policy after the first time that a Policy hit occurs, select the **Disable policy after first hit** checkbox. (This action is relevant for some types of Network Event Policies and some types of SCADA Event Policies.)
    - If you would like to initiate an automatic snapshot of the affected asset whenever a Policy hit is detected, then select the **Take snapshot after policy hit** checkbox. (This action is relevant for some types of *Configuration Events* Policies.)
12. Once all fields have been filled in, click **Create**.
    The new Policy is created and automatically activate. The Policy is shown in the lists on the Policies screen.

Creating Unauthorized Write Policies

This type of Policy detects unauthorized writes to controller tags. The Policy Definition involves specifying the relevant Tag Groups and the type of write that generates a Policy hit.

➡ **To set the Policy Definition for an Unauthorized Write Policy:**

1. Create a new Unauthorized Write Policy as described in **CREATING POLICIES**.



2. In the Policy Definition section, in the **Tag Group** field, select the Tag Group to which this Policy applies.
3. In the **Tag value** section, select the desire option by clicking the radio button and filling in the required fields. Options are:
   - **Any value** – select this option to detect any change to the tag value.
   - **Different from value** – select this option to detect any value other than the specified value. Enter the specified value in the field next to this selection.
   - **Out of allowed range** – select this option to detect any value outside of the specified range. Enter the lower and upper limits of the allowed range in the respective fields next to this selection.

The *Different from value* and *Out of allowed range* options are only available for standard tag types (e.g. Integer, Boolean etc.) but not for customized tags or strings.

4. Complete the Policy creation procedures as described in **Creating Policies**.

Other Actions on Policies

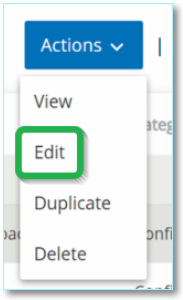
Editing Policies

You can edit the configuration of both predefined and user defined Policies. For most Policies you can adjust both the Policy Definition parameters (policy conditions) and the Policy Action parameters. For Intrusion Detection Policies you can only adjust the Policy Action parameters.

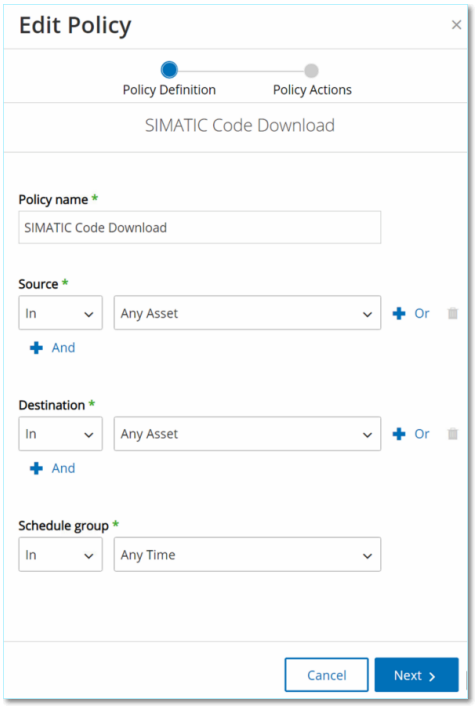
You can also edit the Policy Action parameters for multiple Policies in a bulk action.

➡ **To Edit a Policy:**

1. On the **Policies** screen, select the checkbox next to the desired Policy.
2. Click on the **Actions** menu and select **Edit** from the dropdown list.



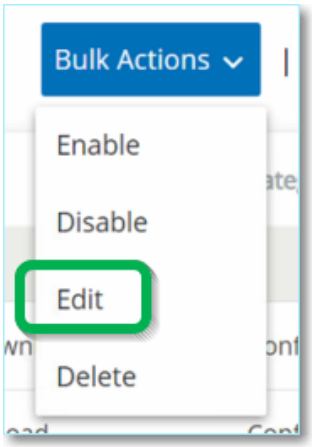
The **Edit Policy** screen is shown with the current configuration filled in.



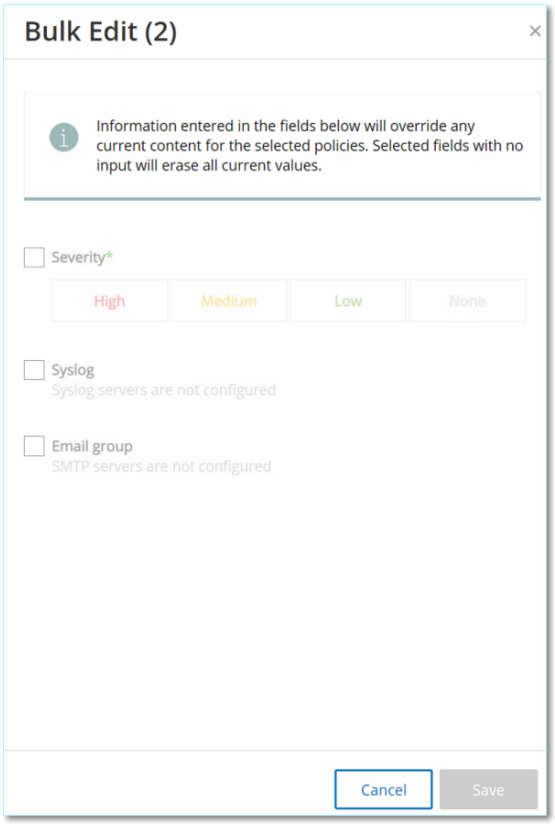
3. Adjust the *Policy Definition* parameters as desired.
4. Click **Next**.
5. Adjust the *Policy Actions* parameters as desired.
6. Click **Save**.
   The Policy is saved with the new configuration.

➡ **To Edit multiple Policies (bulk process):**

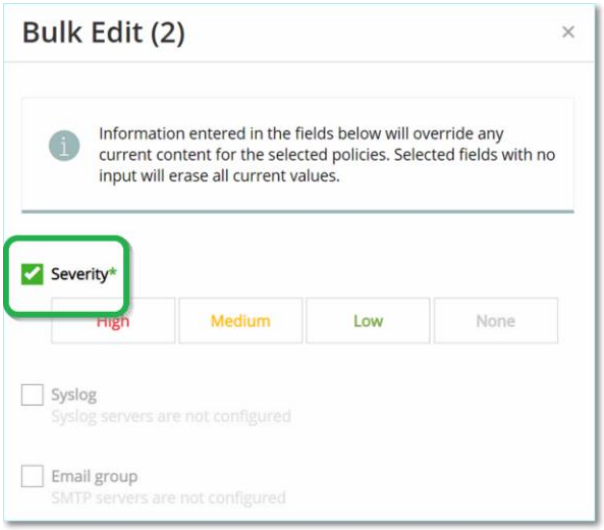
1. On the **Policies** screen, select the checkbox next to two or more Policies.
2. Click on the **Bulk Actions** menu and select **Edit** from the dropdown list.



The **Bulk Edit** screen is shown with the Policy Actions available for bulk editing.



3. Select the checkbox next to each of the parameters that you would like to edit (*Severity*, *Syslog*, *Email Group*).



4. Set each parameter as desired.

	Information entered in the Bulk Editing fields overrides any current content for the selected Policies. If you select the checkbox next to a parameter but do not enter a selection, then the current values for that parameter will be erased.

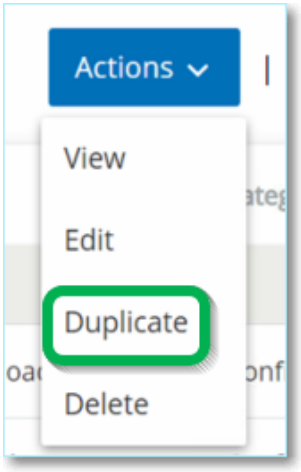
5. Click **Save**.
   The Policies are saved with the new configuration.

Duplicating Policies

You can create a new Policy that is similar to an existing Policy by *Duplicating* the original Policy and making the desired adjustments. You can duplicate both predefined and user defined Policies (except for Intrusion Detection Policies).

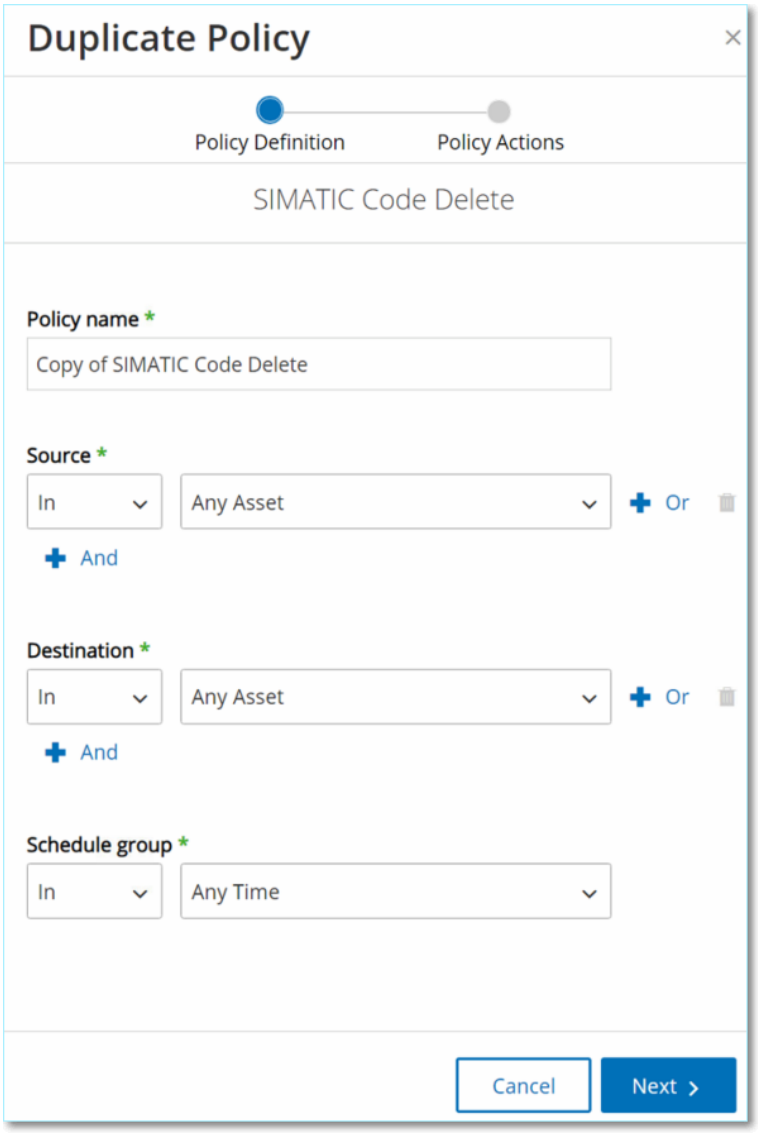
➡ **To Duplicate a Policy:**

1. On the **Policies** screen, select the checkbox next to the desired Policy.
2. Click on the **Actions** menu and select **Duplicate** from the dropdown list.



The **Duplicate Policy** screen is shown with the current configuration filled in and the name set

by default as "Copy of <Original Policy Name>".



3. Adjust the *Policy Definition* parameters as desired.
4. Click **Next**.
5. Adjust the *Policy Actions* parameters as desired.
6. Click **Save**.
   The Policy is saved with the new configuration.

Deleting Policies

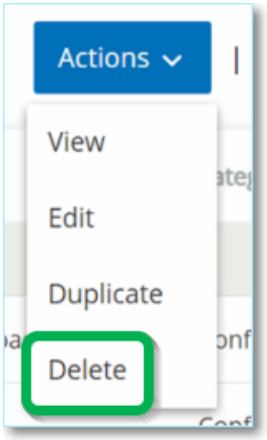
You can delete a Policy from the system. You can delete both predefined and user defined Policies (except for Intrusion Detection Policies which can't be deleted).

You can also delete multiple Policies in a bulk action.

> Once you delete a Policy from the system you won't be able to reactivate it. An alternative option is to toggle the status to OFF to deactivate it temporarily while reserving the option to reactivate it later.

To Delete a Policy:

1. On the **Policies** screen, select the checkbox next to the desired Policy.
2. Click on the **Actions** menu and select **Delete** from the dropdown list.

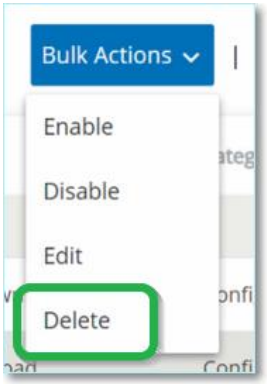


A confirmation window is displayed.

3. Click **Delete**.
   The Policy is deleted from the system.

To Delete multiple Policies (bulk action):

1. On the **Policies** screen, select the checkbox next each of the desired Policies.
2. Click on the **Bulk Actions** menu and select **Delete** from the dropdown list.



A confirmation window is displayed.

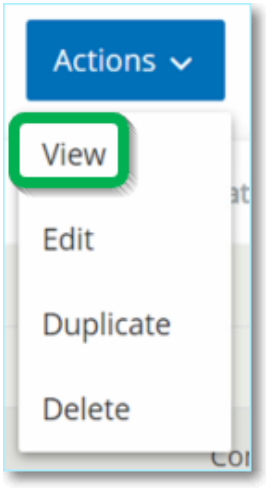
3. Click **Delete**.
   The Policies are deleted from the system.

Deleting Policy Exclusions

If you would like to delete an Exclusion that has been applied to a particular Policy, you can do so on the Policies screen.

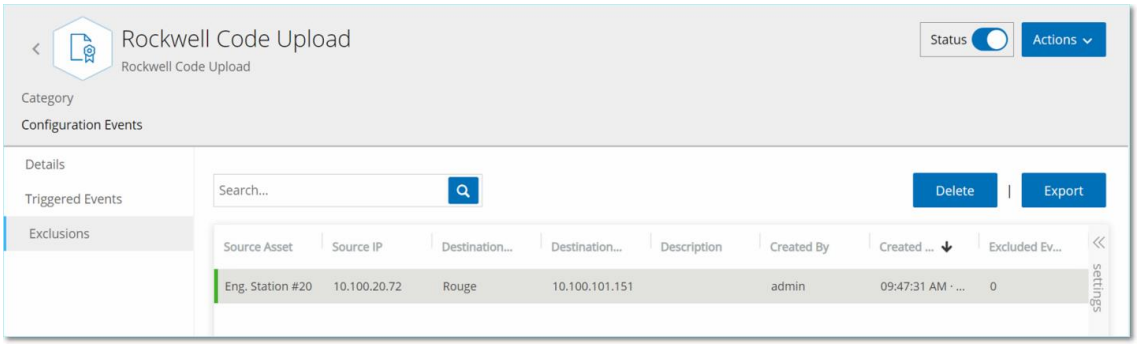
➡ **To delete a Policy Exclusion:**

1. On the **Policies** screen, select the desired policy.
2. Click on the **Actions** menu and select **View** from the dropdown list.



Alternatively, you can access the Actions menu by right-clicking on the relevant Policy.

3. Click on the **Exclusions** tab.



   A list of Exclusions is shown.
4. Select the Policy Exclusion you would like to delete.
5. Click on **Delete**.
   A confirmation window is displayed.
6. In the confirmation window, click on **Delete**.
   The Exclusion is deleted from the system.

Groups

Groups are the fundamental building blocks that are used to construct Policies. When configuring a Policy each of the policy conditions is set using Groups, as opposed to individual entities. The system comes with some predefined Groups. You can also create your own user defined Groups. Therefore, it is recommended to configure the Groups that you will need in advance to streamline the process of editing and creating Policies.

Policy parameters can only be set using Groups. If you want a Policy to apply to an individual entity you must configure a Group that includes only that entity.

Under Groups you can view all Groups that have been configured in your system. The Groups are divided into two categories:

- Predefined Groups – which come pre-configured in the system and can't be edited.
- User Defined Groups – which are created by the end-user and can be edited.

There are several different types of Groups, each of which is used for the configuration of various Policy types. Each Group type is shown on a separate screen under Groups. The Group types are:

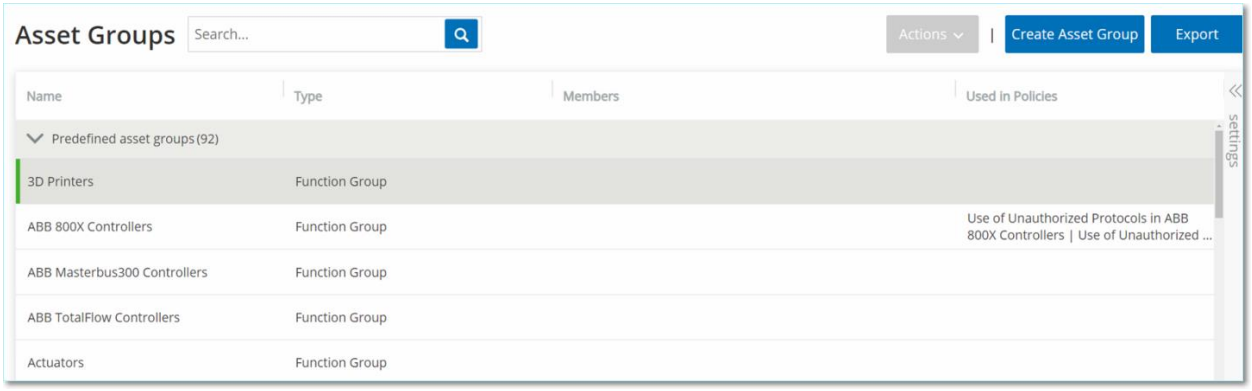
- Asset Groups – Assets are hardware entities in the network. Asset Groups are used as a Policy condition for a wide range of Policy types.
- Network Segments – Network Segmentation is a method of creating groups of related network assets, assisting in the logical isolation of one group of assets from another.
- Email Groups – Groups of emails that are notified when a Policy Event occurs. Used for all Policy types.
- Port Groups – Groups of Ports used by assets in the network. Used for Policies that identify open ports.
- Protocol Groups – Groups of Protocols by which conversations are conducted between assets in the network. Used as a Policy condition for Network Events.
- Schedule Groups – Schedule Groups are time ranges that are used to configure at what time the specified event must occur to fulfill the policy conditions.
- Tag Groups – Tags are parameters in controllers that contain specific operational data. Tag Groups are used as a Policy condition for SCADA Events.
- Rule Groups - Rule Groups are comprised of a group of related rules, which are identified by their Suricata Signature IDs (SIDs). These groups are used as a Policy condition for defining Intrusion Detection Policies.

The procedure for creating each type of Group is described in the following sections. In addition, you can View, Edit, Duplicate or Delete an existing Group, see **Actions on Groups**.

Asset Groups

Assets are hardware entities in the network. Grouping similar assets together enables you to create Policies that apply to all the assets in the Group. For example, you could use an Asset Group *Controllers* to create a Policy that alerts for firmware changes to any controller. Asset Groups are used as a Policy condition for a wide range of Policy types. Asset Groups can be used to specify the *Source* asset, the *Destination* asset or the *Affected Asset* for various Policy types.

Viewing Asset Groups



The **Asset Groups** screen shows all Asset Groups that are currently configured in the system. The *Predefined* tab includes Groups that are built into the system which can't be edited, duplicated or deleted. The *User defined* tab includes custom Groups that were created by the user. These Groups can be edited, duplicated or deleted.

The information shown on this screen is described in the following table.

Parameter	Description
Status	Shows if the Policy is turned on or off. If the Policy was automatically disabled by the system because it was generating too many Events, then a warning icon is displayed. Toggle the status switch to turn a Policy ON/OFF.
Name	The name of the Policy.
Severity	The degree of severity of the Event. Possible values are: None, Low, Medium or High. See section **Severity Levels** for a description of the severity levels.
Event Type	The specific type of event that triggers this Event Policy.
Category	The general category of the type event that triggers this Event Policy. Possible values are: Configuration, SCADA, Network Threats or Network Event. For an explanation of the various categories see **Policy Categories and Sub-Categories**.

Parameter	Description
Source	A Policy condition. The source Asset Group (i.e. the asset that initiated the Activity) to which the Policy applies.
Name	The name that is used to identify the Group.
Type	Shows the type of Group. Options are: • Function – A predefined Asset Group that was created to serve a particular function. • Asset List – Specified assets are included in the Group. • IP List – Assets with the specified IP Address. • IP Range - Assets within the specified range of IP Addresses.
Members	Shows the list of assets that are included in this Group. No value is shown for Function Groups. Note: If there isn't room to display all assets in this row then click on Table Actions > View > Members tab.
Used in Policies	Shows the name of each Policy that uses this Asset Group in its configuration. Note: To view more details about the Policies in which the Group is used, click on Table Actions > View > Used in Policies tab.

The procedures for creating various types of Asset Groups are described in the following section. In addition, you can View, Edit, Duplicate or Delete an existing Group, see **ACTIONS ON GROUPS**.

Creating Asset Groups

You can create custom Asset Groups to be used in the configuration of Policies. By grouping together similar assets you enable creation of Policies that apply to all assets in the Group.

There are three types of User Defined Asset Groups:

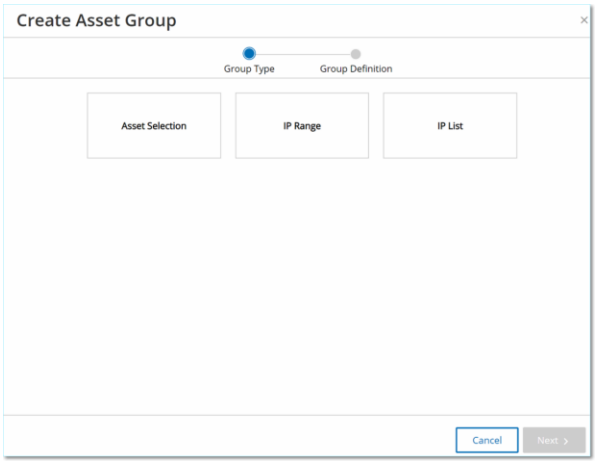
- Asset List – Specify the specific assets that are included in the Group.
- IP List – Specify the IP addresses of the Assets that are included in the Group.
- IP Range - Specify the range of IP addresses of the Assets that are included in the Group.

There are different procedures for creating each type of Asset Group.

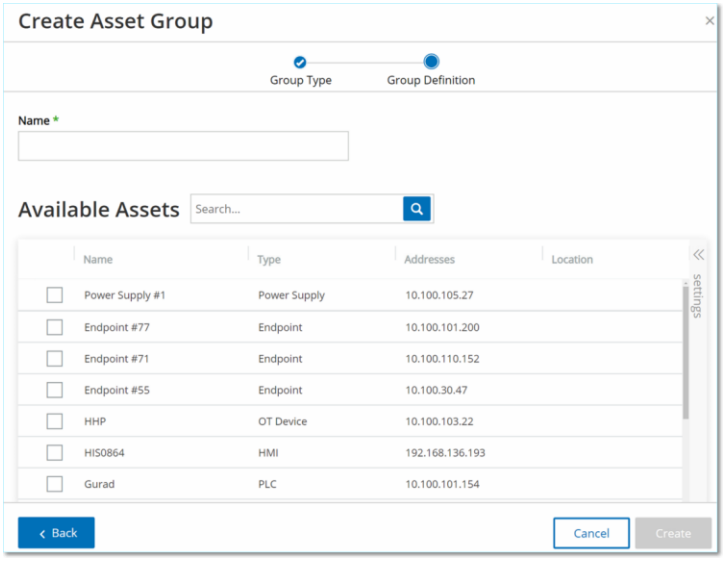
➡ **To Create an Asset Selection Type Asset Group:**

1. Under Groups, select Asset Groups.
2. Click Create Asset Group.

The **Create Asset Group** wizard is displayed.



3. Click on Asset Selection.
4. Click **Next**.
   The list of **Available Assets** is displayed.

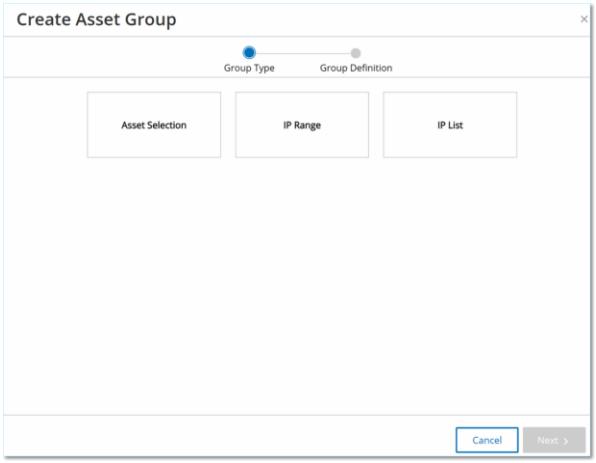


5. In the **Name** field, enter a name for the Group.
   Choose a name that describes a common element that categorizes the assets that are included in the Group.
6. Select the checkbox next to each Asset that you would like to include in the Group.
7. When you have finished making your selections, click **Create**.
   The new Asset Group is created and is shown on the Asset Groups screen. You can now use this Group when configuring Policies.

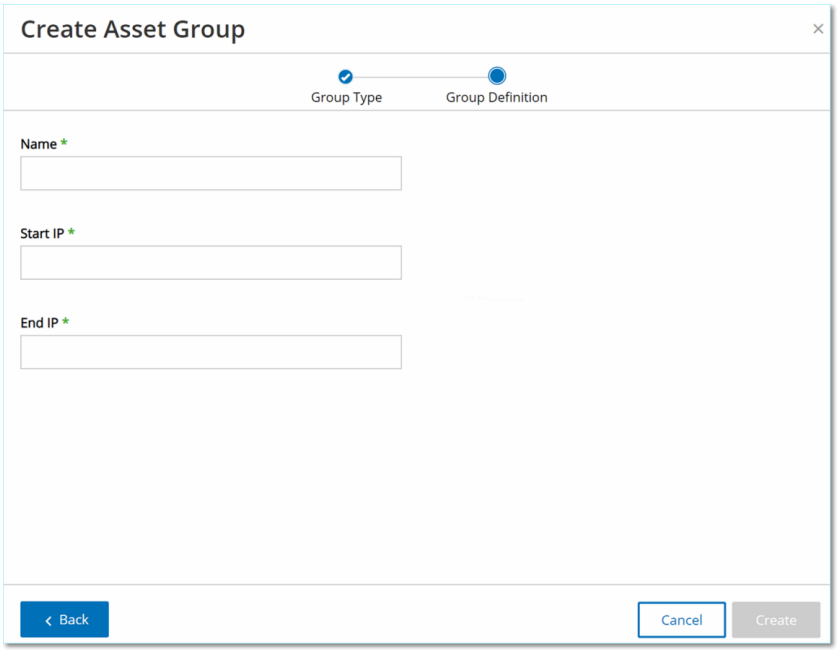
To Create an IP Range Type Asset Group:

1. Under Groups, select Asset Groups.

2. Click Create Asset Group.
   The Create Asset Group wizard is displayed.



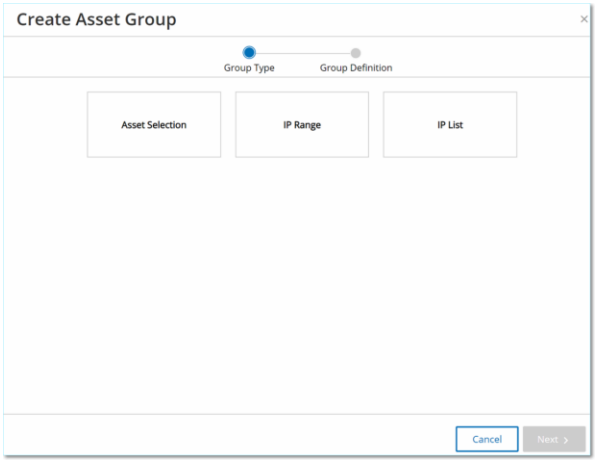
3. Click on **IP Range**.
4. Click **Next**.
   The IP Range selection parameters are displayed.



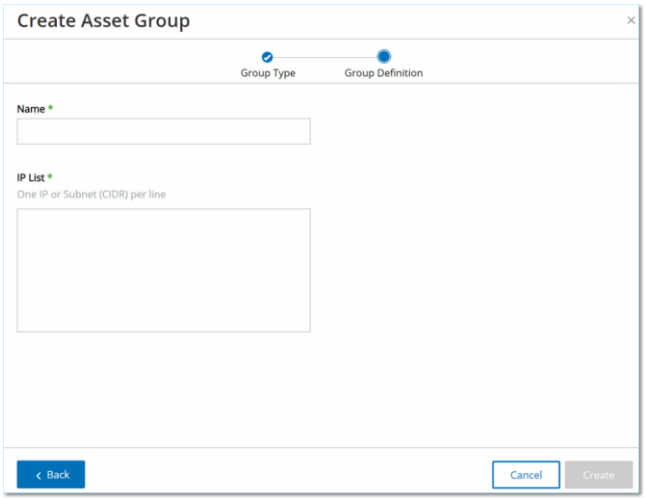
5. In the **Name** field, enter a name for the Group.
   Choose a name that describes a common element that categorizes the assets that are included in the Group.
6. In the **Start IP** field, enter the IP Address at the beginning of the range that you would like to include.
7. In the **End IP** field, enter the IP Address at the end of the range that you would like to include.
8. Click **Create**.
   The new Asset Group is created and is shown on the Asset Groups screen. You can now use this Group when configuring Policies.

To Create an IP List Type Asset Group:

1. Under Groups, select Asset Groups.
2. Click Create Asset Group.
   The Create Asset Group wizard is displayed.



3. Click on **IP List**.
4. Click **Next**.
   The IP List parameters are displayed.



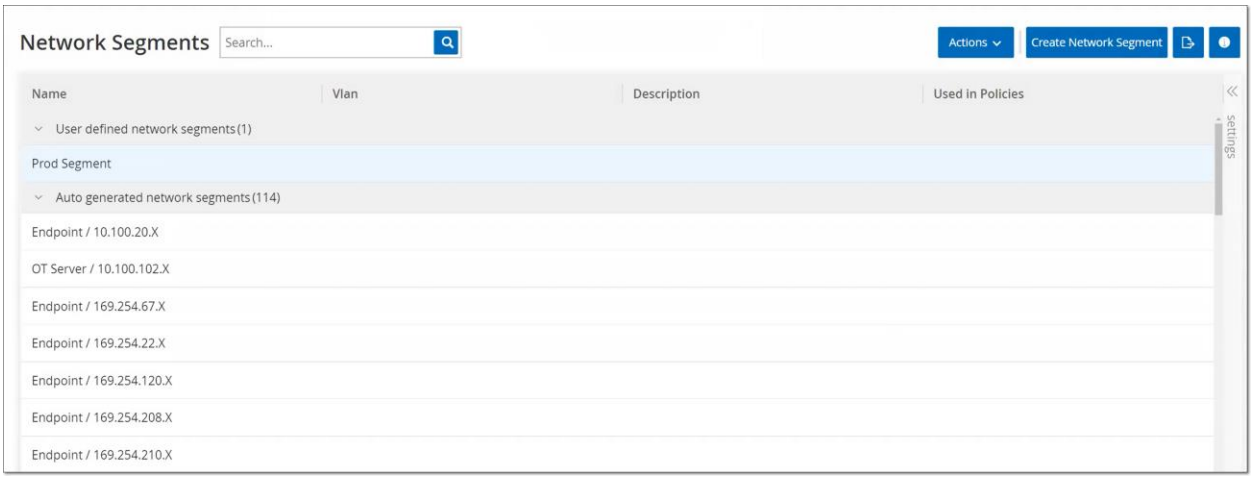
5. In the **Name** field, enter a name for the Group.
   Choose a name that describes a common element that categorizes the assets that are included in the Group.
6. In the **IP List** box, enter an IP Address or a Subnet to be included in the Group.
7. To add more assets to the Group, enter each additional IP address or Subnet on a separate line.
8. Click **Create**.
   The new Asset Group is created and is shown on the Asset Groups screen. You can now use this Group when configuring Policies.

Network Segments

Network Segmentation is a method of creating groups of related network assets, assisting in the logical isolation of one group of assets from another. Tenable.ot automatically assigns each IP address that is associated with an asset in your network to a Network Segment. (For assets with more than one IP address, each IP is associated with a Network Segment.) Each auto generated segment includes all Assets of a specific Category (Controller, OT Servers, Network Devices etc.) that have IPs with the same class C network address (i.e. the IPs have the same first 24 bits).

You can create user-defined Network Segments, and specify which assets are assigned to that segment. There is column on the Inventory screens showing the Network Segment for each asset, making it easy to sort and filter your assets by Network Segment.

Viewing Network Segments



The Network Segments screen shows all Network Segments that are currently configured in the system. The *Auto generated* tab includes Network Segments that are automatically generated by the system. The *User defined* tab includes custom Network Segments that were created by the user.

The information shown on this screen is described in the following table:

Parameter	Description
Name	The name that is used to identify the Network Segment.
VLAN	The VLAN number of the Network Segment. (Optional)
Description	A description of the Network Segment. (Optional)
Used in Policies	Shows the names of the Policies that apply to this Network Segment. Note: To view more details about the Policies in which the Network Segment is used, click on **Table Actions > View > Used in Policies** tab.

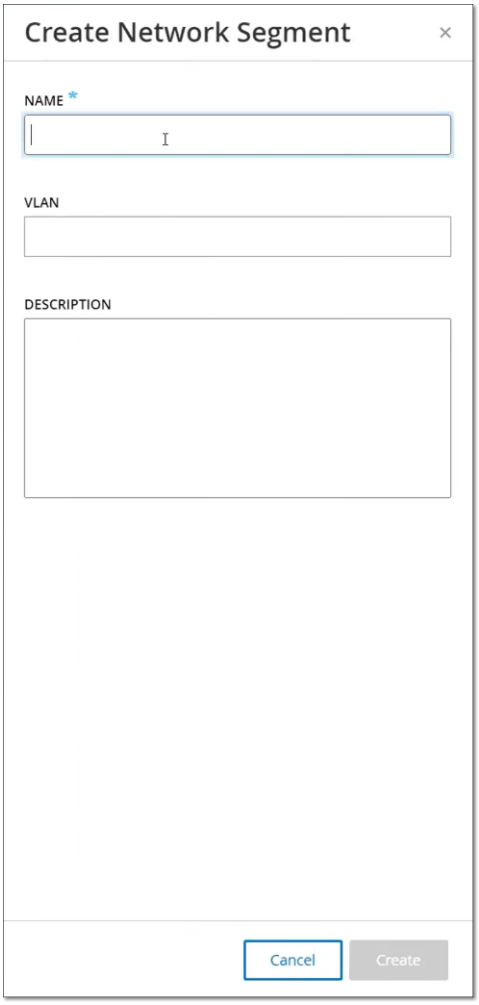
The procedure for creating a Network Segment is described in the following section. In addition, you can View, Edit, Duplicate or Delete an existing Network Segment, see **Actions on Groups**.

Creating Network Segments

You can create Network Segments to be used in the configuration of Policies. By grouping together related network assets you enable the creation of Policies that define acceptable network traffic for Asset in that segment.

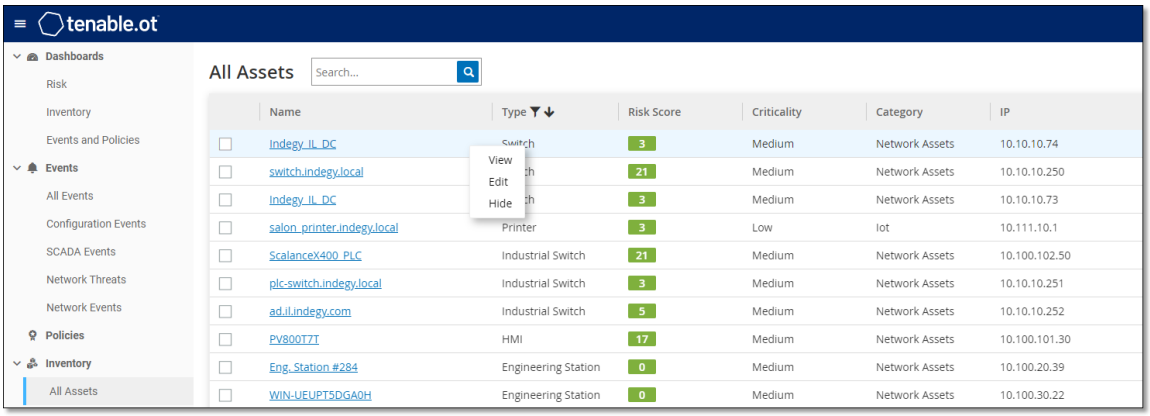
➡ **To Create a Network Segment:**

1. Under **Groups**, select **Network Segments**.
2. Click **Create Network Segment**.
   The **Create Network Segment** wizard is displayed.



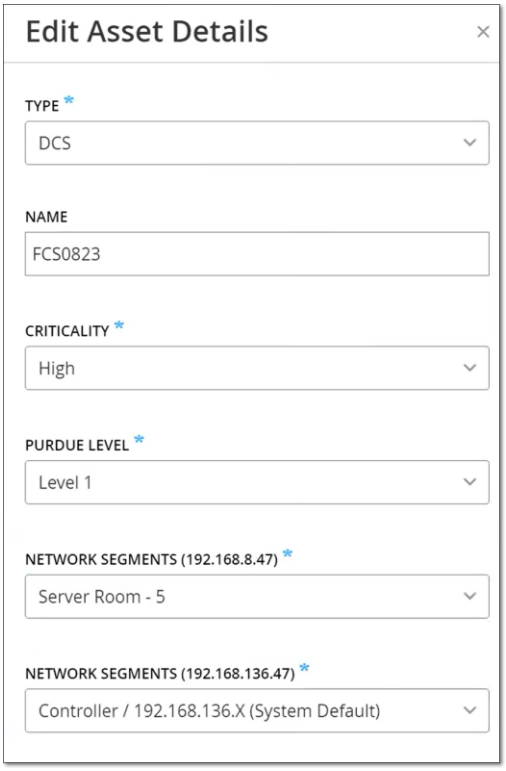
3. In the **Name** field, enter a name for the Network Segment.
4. In the **VLAN** field, enter a VLAN number for the Network Segment. (Optional)
5. In the **Description** field, enter a description of the Network Segment. (Optional)
6. Click **Create**.
   The new Network Segment is created and is shown in the list of Network Segments.
7. Under **Inventory**, select **All Assets**.

8. Right-click on the asset you wish to assign to the newly created Network Segment and select **Edit**.



The **Edit Asset Details** window opens.

9. In the **Network Segments** field, select the appropriate Network Segment from the dropdown list.



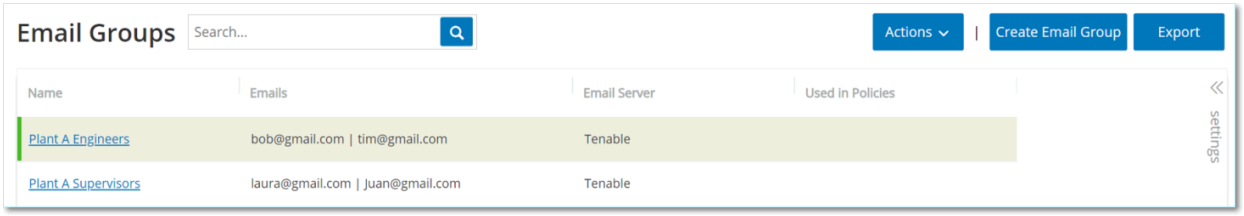
Some assets have more than one associated IP address, and you can select the appropriate Network Segment for each one.

The Network Segment is applied to the asset and is shown in the Network Segment column. You can now use this Network Segment when configuring Policies.

Email Groups

Emails Groups are groups of emails of relevant parties. Email Groups are used to specify recipients for Event notifications that are triggered by specific Policies. For example, grouping by role, department, etc. enables you to send the notifications for specific Policy Events to the relevant parties.

Viewing Email Groups



The Email Groups screen shows all Email Groups that are currently configured in the system.

The information shown on this screen is described in the following table:

You can view additional details about a specific Group by selecting the Group and clicking Table Actions > View.

Parameter	Description
Name	The name that is used to identify the Group.
Emails	The list of emails included in the Group. Note: If there isn't room to display all members of the Group then click on Table Actions > View > Members tab.
Email Server	The name assigned to the SMTP server that is used for sending out the emails to this Group.
Used in Policies	Shows the names of the Policies for which notifications are sent to this Group. Note: To view more details about the Policies in which the Group is used, click on Table Actions > View > Used in Policies tab.

The procedure for creating an Email Group is described in the following section. In addition, you can View, Edit, Duplicate or Delete an existing Group, see **Actions on Groups**.

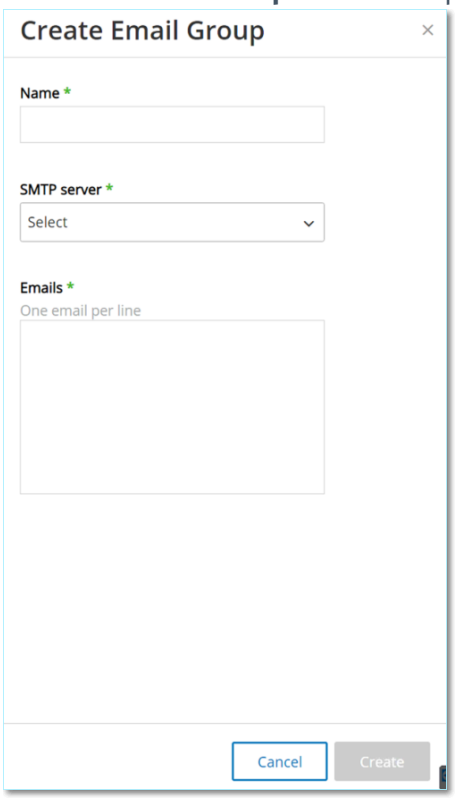
Creating Email Groups

You can create Email Groups to be used in the configuration of Policies. By grouping related emails, you set Policy Event notifications to be sent to all relevant personnel.

> You can only assign one Email Group to each Policy. Therefore, it is useful to create both broad, inclusive Groups as well as specific, limited Groups so that you can assign the appropriate Group to each Policy.

To Create an Email Group:

1. Under **Groups**, select **Email Groups**.
2. Click **Create Email Group**.
   The **Create Email Group** wizard is displayed.



3. In the **Name** field, enter a name for the Group.
4. In the **SMTP server** field, select from the dropdown list the server used for sending out the email notifications.

> If no SMTP server has been configured in the system, then you must first configure a server before you can create an Email Group, see **SMTP Server**.

5. In the **Emails** field, enter the email of each member of the Group on a separate line.
6. Click **Create**.
   The new Email Group is created and is shown on the Email Groups screen. You can now use this Group when configuring Policies.

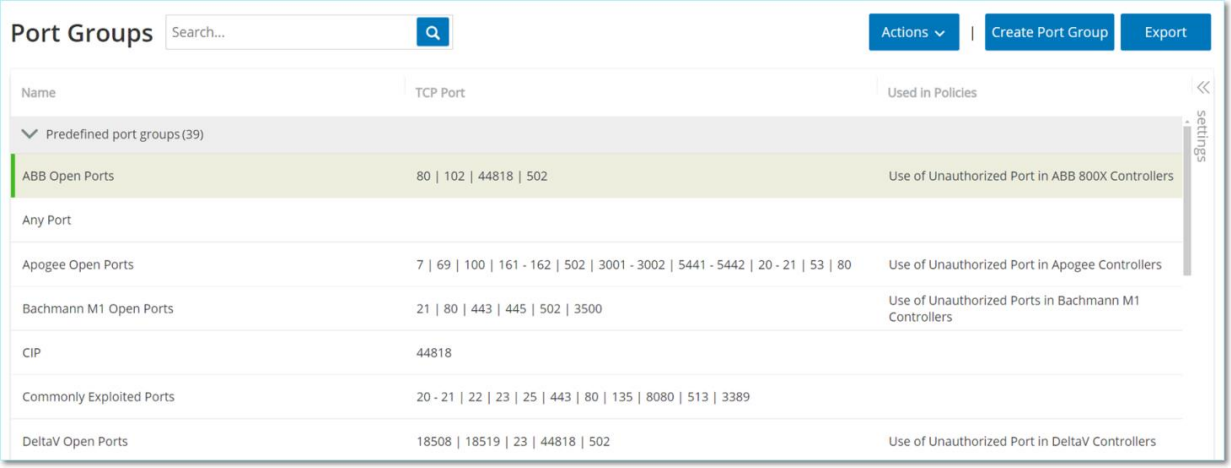
Port Groups

Port Groups are groups of ports used by assets in the network. Port Groups are used as a policy condition for defining **Open Port** Network Event Policies, which detect open ports in the network.

The *Predefined* tab shows the Port Groups that are predefined in the system. These Groups comprise ports that are expected to be Open on controllers from a specific vendor. For example, the Group Siemens PLC Open Ports includes: 20, 21, 80, 102, 443 and 502. This enables configuration of Policies that detect open ports that are not expected to be opened for controllers from that vendor. These Groups can't be edited or deleted but they can be duplicated.

The *User defined* tab includes custom Groups that were created by the user. These Groups can be edited, duplicated or deleted.

Viewing Port Groups



The information shown on this screen is described in the following table:

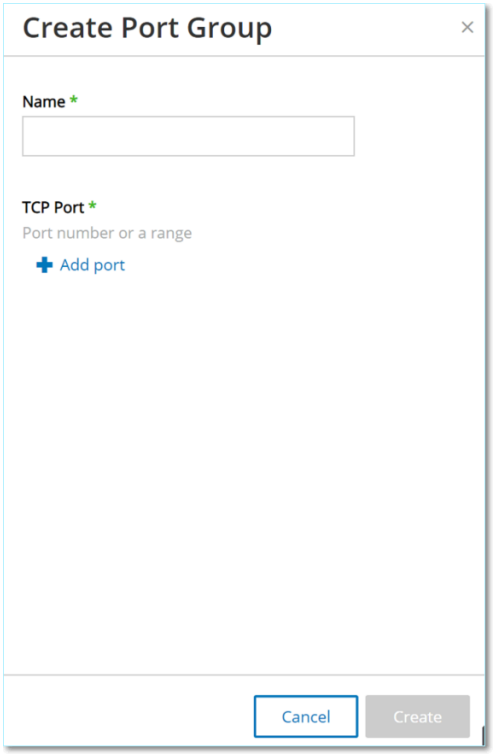
Parameter	Description
Name	The name that is used to identify the Group.
TCP Ports	The list of ports and/or ranges of ports that are included in the Group. Note: If there isn't room to display all members of the Group then click on **Table Actions > View > Members** tab.
Used in Policies	Shows the name of each Policy that uses this Port Group in its configuration. Note: To view additional info about the Policies in which this Group is used, click on **Table Actions > View > Used in Policies** tab.

Creating Port Groups

You can create user defined Port Groups to be used in the configuration of Policies. By grouping together similar ports you enable creation of Policies that alert for open ports that pose a particular security risk.

➡ **To Create a Port Group:**

1. Under **Groups**, select **Port Groups**.
2. Click **Create Port Group**.
   The **Create Port Group** wizard is displayed.



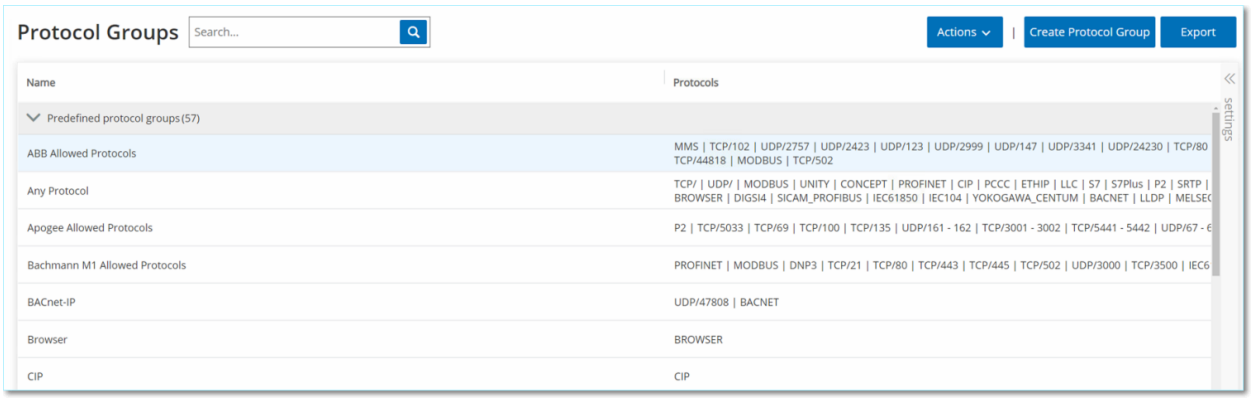
3. In the **Name** field, enter a name for the Group.
4. In the **TCP Port** field, enter a single port or a range of ports to be included in the Group.
5. If you would like to add additional Ports to the Group, use the following procedure for each additional Port.
   a. Click **+ Add Port**.
      A new Port Selection field is displayed.
   b. In the new **Port number** field, enter a single port or a range of ports to be included in the Group.
6. Click **Create**.
   The new Port Group is created and is shown in the list of Port Groups. You can now use this Group when configuring Policies.

Protocol Groups

Protocol Groups are groups of protocols with which conversations are conducted between assets in the network. Protocol Groups are used as a Policy condition for Network Policies, defining what Protocols being used between particular assets trigger a Policy.

Tenable.ot comes with a set of predefined Protocol Groups which comprise related protocols. These Groups are available for use in Policies. These Groups can't be edited or deleted. Protocols can be grouped by which protocols are allowed by a specific vendor. For example, Schneider allowed protocols include: 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). They can also be grouped by type of protocol (i.e. Modbus, PROFINET, CIP etc.). You can also create your own user defined Protocol Groups.

Viewing Protocol Groups



The **Protocol Groups** screen shows all Protocol Groups that are currently configured in the system. The *Predefined* tab shows Groups that are built into the system. These Groups can't be edited or deleted but they can be duplicated. The *User defined* tab shows custom Groups that were created by the user. These Groups can be edited, duplicated or deleted.

The information shown on this screen is described in the following table.

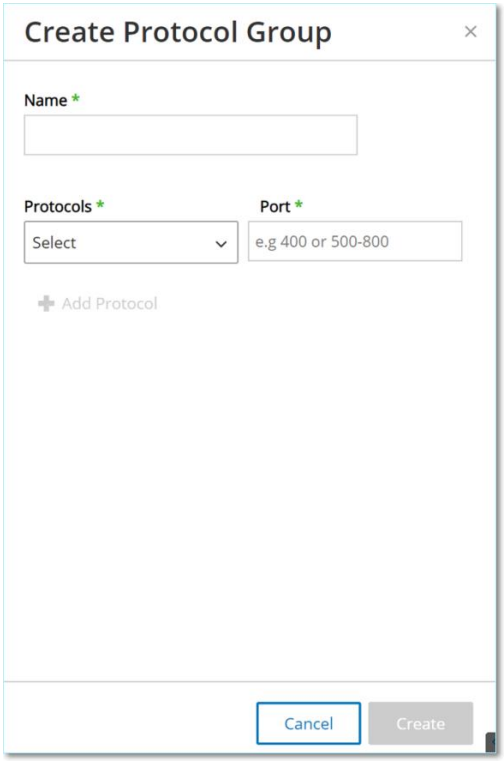
Parameter	Description
Name	The name that is used to identify the Group.
Protocols	The list of protocols that are included in the Group. Note: If there isn't room to display all members of the Group then click on **Table Actions > View > Members** tab.
Used in Policies	Shows the name of each Policy that uses this Protocol Group in its configuration. Note: To view additional details about the Policies in which this Group is used, click on **Table Actions > View > Used in Policies** tab.

Creating Protocol Groups

You can create custom Protocol Groups to be used in the configuration of Policies. By grouping together similar Protocols you enable creation of Policies that define which protocols are suspicious.

➡ **To Create a Protocol Group:**

1. Under **Groups**, select **Protocol Groups**.
2. Click **Create Protocol Group**.
   The **Create Protocol Group** wizard is displayed.

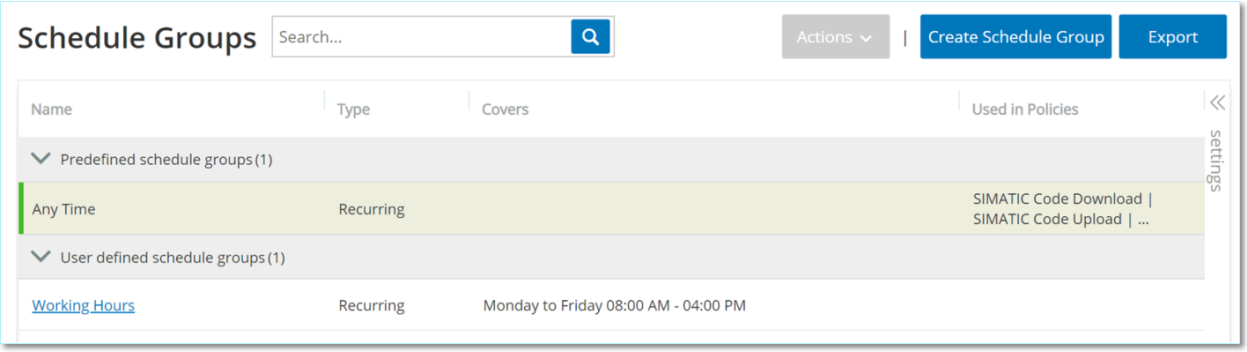


3. In the **Name** field, enter a name for the Group.
4. In the **Protocols** field, select from the dropdown menu a Protocol type.
5. If the selected Protocol is *TCP* or *UDP* then enter a Port number or range of Ports in the **Port** field. For other Protocol types no value is entered in the **Port** field.
6. If you would like to add additional Protocol/s to the Group, use the following procedure for each additional Protocol.
   a. Click **+ Add Protocol**.
      A new **Protocol Selection** field is displayed.
   b. Fill in the new Protocol Selection in the manner described in steps 4-5.
7. Click **Create**.
   The new Protocol Group is created and is shown in the list of Protocol Groups. You can now use this Group when configuring Policies.

Schedule Group

A Schedule Group defines a time range or group of time ranges that has particular characteristics that make activities that happen during that time period noteworthy. For example, certain activities are expected to occur during work hours while other activities are expected to occur during down-time.

Viewing Schedule Groups



The **Schedule Groups** screen shows all Schedule Groups that are currently configured in the system. The *Predefined* tab includes Groups that are built into the system. These Groups can't be edited, duplicated or deleted. The *User defined* tab shows the custom Groups that were created by the user. These Groups can be edited, duplicated or deleted.

The information shown on this screen is described in the following table.

Parameter	Description
Name	The name that is used to identify the Group.
Type	Shows the type of Group. Options are: • **Function** - a predefined Schedule Group that was created to serve a particular function. • **Recurring** – a schedule that recurs on a daily or weekly basis. For example, a Work Hours schedule can be defined as Monday to Friday from 9am to 5pm. • **Interval** – a schedule that occurs on a specific date or range of dates. For example, a Plant Renovation schedule could be defined by the period from June 1 to August 15.
Covers	A summary of the schedule settings. Note: If there isn't room to display all members of the Group then click on **Table Actions > View > Members** tab.
Used in Policies	Shows the Policy ID of each Policy that uses this Schedule Group in its configuration. Note: To view additional details about the Policies in which this Group is used, click on **Table Actions > View > Used in Policies** tab.

Creating Schedule Groups

You can create custom Schedule Groups to be used in the configuration of Policies. Designate a time range or group of time ranges that share characteristics that make events that happen during that time period noteworthy.

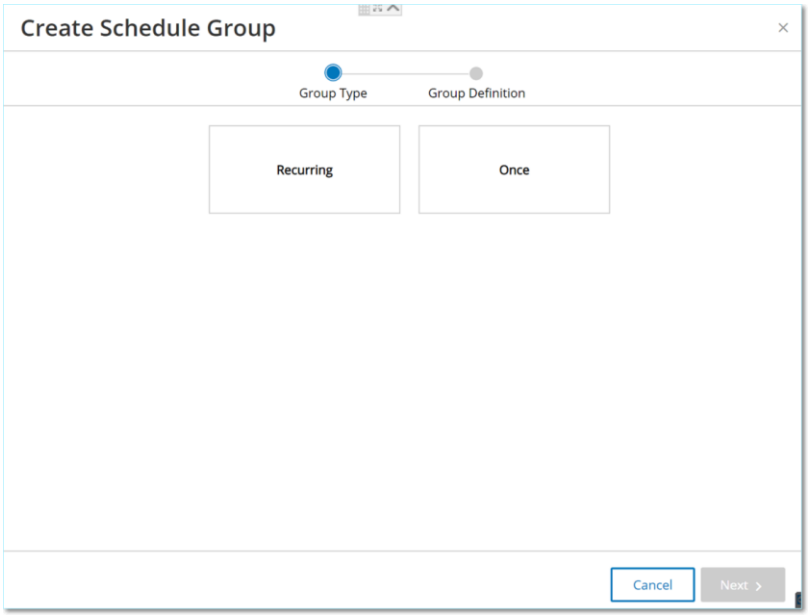
There are two types of Schedule Groups:

- Recurring – schedules that recur on a weekly basis. For example, a Work Hours schedule can be defined as Monday to Friday from 9am to 5pm.
- Once – schedules that occur on a specific date or range of dates. For example, a Plant Renovation schedule could be defined by the period from June 1 to August 15. There are different procedures for creating each type of Schedule Group.

There are different procedures for creating each type of Schedule Group.

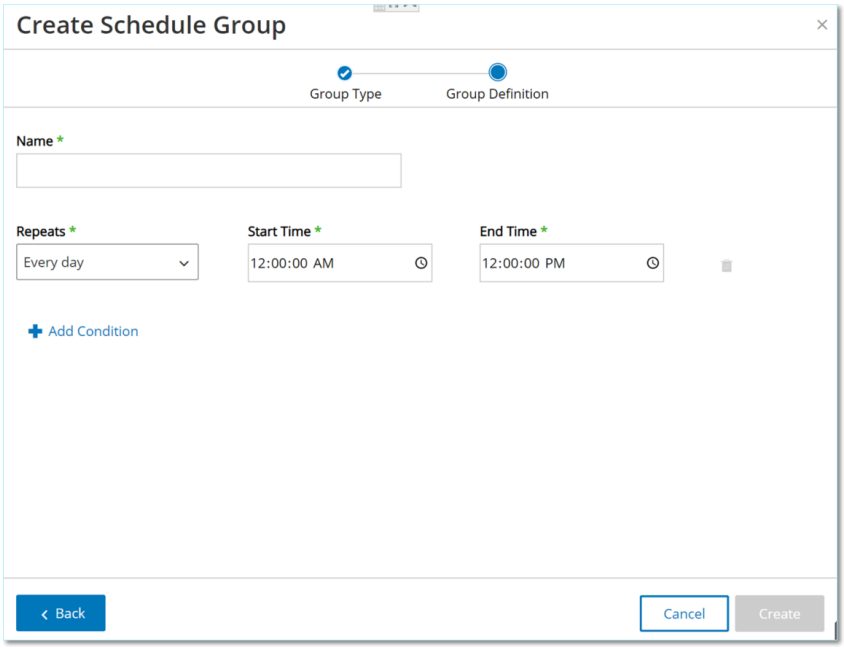
➡ **To Create a Recurring Type Schedule Group:**

1. Under **Groups**, select **Schedule Groups**.
2. Click **Create Schedule Group**.
3. On the **Schedule Groups screen**, click **Create Schedule Group**.
   The **Create Schedule Group** wizard is displayed.



4. Select **Recurring**.

5. Click **Next**.
   The parameters for defining a Recurring Schedule group are shown.



6. In the **Name** field, enter a name for the Group.
7. In the **Repeats** field, select which days of the week are included in the Schedule Group. Options are: *Every day*, *Monday to Friday* or a specific day of the week.

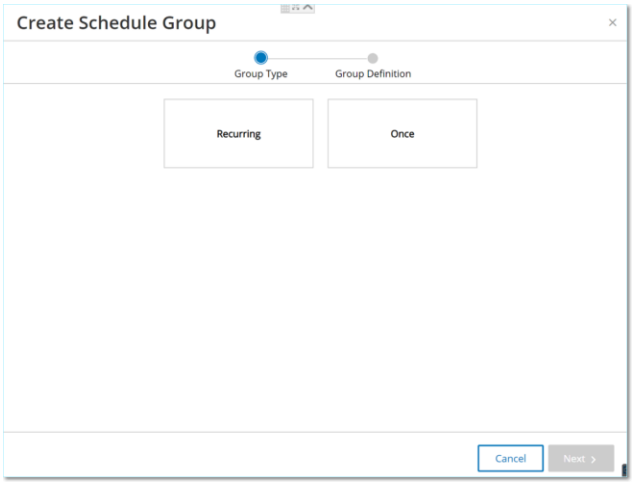
> If you would like to include particular days of the week, e.g. Monday and Wednesday, then you will need to add a separate condition for each day.

8. In the **Start Time** field, enter the time of day (HH:MM:SS AM/PM) of the beginning of the time range included in the Schedule Group.
9. In the **End Time** field, enter the time of day (HH:MM:SS AM/PM) of the end of the time range included in the Schedule Group.
10. If you would like to add additional Conditions (i.e. additional time ranges) to the Schedule Group, use the following procedure for each additional Condition.
    a. Click **+ Add Condition**.
       A new row of Schedule selection fields is displayed.
    b. Fill in the schedule fields as described above in step 5-7.
11. Click **Create**.
    The new Schedule Group is created and is shown in the list of Schedule Groups. You can now use this Group when configuring Policies.

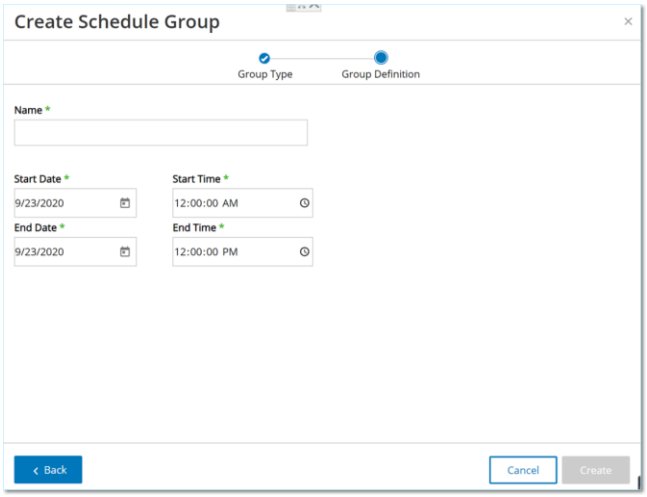
To Create a One Time Schedule Group:

1. Under **Groups**, select **Schedule Groups**.
2. Click **Create Schedule Group**.

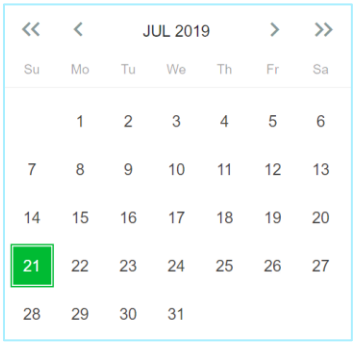
The **Create Schedule Group** wizard is displayed.



3. Select **Once**.
4. Click **Next**.
   The parameters for defining a one-time Schedule group are shown.



5. In the **Name** field, enter a name for the Group.
6. In the **Start Date** field, click on the calendar icon .
   A calendar window opens.



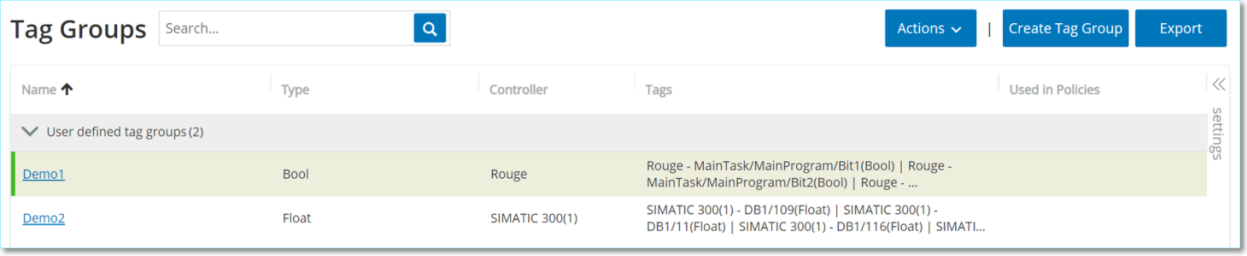
7. Select the date on which the Schedule Group begins. (Default: the current date)
8. In the **Start Time** field, enter the time of day (HH:MM:SS AM/PM) of the beginning of the time range included in the Schedule Group.

9. In the **End Date** field, click on the calendar icon .
   A calendar window opens.
10. Select the date on which the Schedule Group ends. (Default: the current date)
11. In the **End Time** field, enter the time of day (HH:MM:SS AM/PM) of the end of the time range included in the Schedule Group.
12. Click **Create**.
    The new Schedule Group is created and is shown in the list of Schedule Groups. You can now use this Group when configuring Policies.

Tag Groups

Tags are parameters in controllers that contain specific operational data. Tag Groups are used as a Policy condition for SCADA Events Policies. By grouping together Tags that play similar roles you can create Policies that detect suspicious changes to the specified parameter. For example, by grouping together Tags that control furnace temperature, you can create a Policy that detects temperature changes that could be harmful to the furnaces.

Viewing Tag Groups



The Tag Groups screen shows all Tag Groups that are currently configured in the system.

The information shown on this screen is described in the following table.

Parameter	Description
Name	The name that is used to identify the Group.
Type	The data type of the Tag. Possible values are: *Bool*, *Dint*, *Float*, *Int*, *Long*, *Short*, *Unknown* (for Tags of a type that Tenable.ot was unable to identify) or *Any Type* (which can include Tags of different Types)
Controller	The controller on which the Tag is being monitored.
Tags	Shows each Tag that is included in the Group as well as the name of the controller in which it is located. Note: If there isn't room to display all Tags in this row then click on Table Actions > View > Members tab.

Parameter	Description
Used in Policies	Shows the Policy ID of each Policy that uses this Schedule Group in its configuration. Note: To view additional details about the Policies in which this Group is used, click on **Table Actions > View > Used in Policies** tab.

The procedure for creating a Port Group is described in the following section. In addition, you can View, Edit, Duplicate or Delete an existing Group, see **ACTIONS ON GROUPS**.

Creating Tag Groups

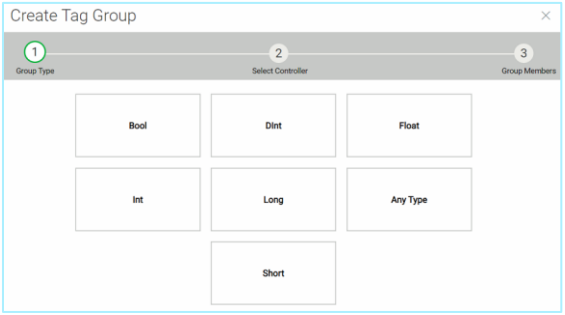
You can create custom Tag Groups for use in Policy configuration. By grouping together similar Tags you can create Policies that apply to all Tags in the Group. Select the Tags that are of a similar type and give them a name that represents the common element of the Tags.

You can also create Groups that include Tags of different types by selecting the *Any Type* option. In this case Policies that are applied to this Group can only detect changes to *Any Value* for the specified Tags but can't be set to detect specific values.

Tag Groups can be edited, duplicated or deleted.

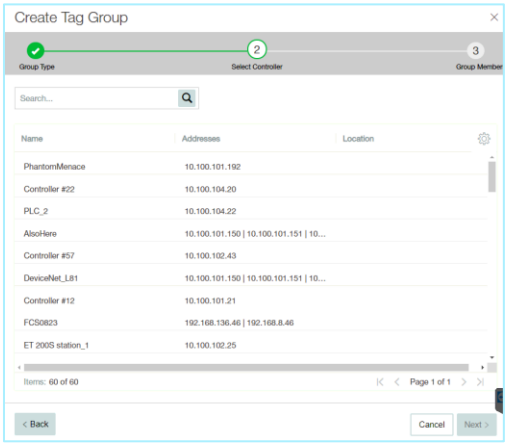
To Create a New Tag Group:

1. Under **Groups**, select **Tag Groups**.
2. Click **Create Tag Group**.
   The **Create Tag Group** wizard is displayed.

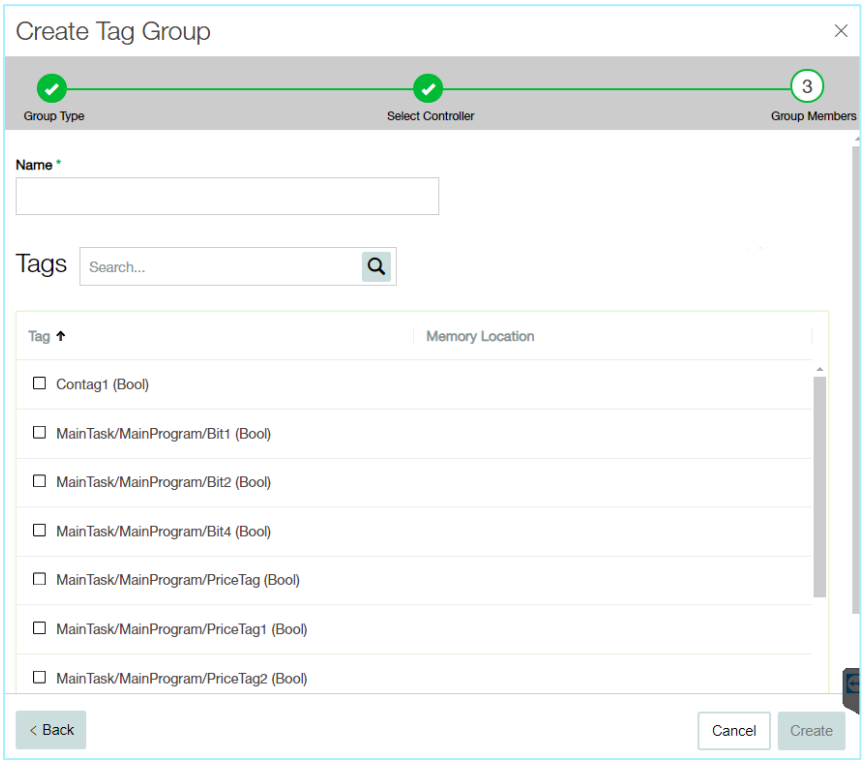


3. Select a Tag type. Options are: *Bool*, *Dint*, *Float*, *Int*, *Long*, *Short* or *Any Type* (which can include Tags of different Types)

4. Click **Next**.
   A list of controllers in your network is displayed.



5. Select a controller for which you would like include Tags in the Group.
6. Click **Next**.
   A list of Tags of the specified type on the specified controller are displayed.



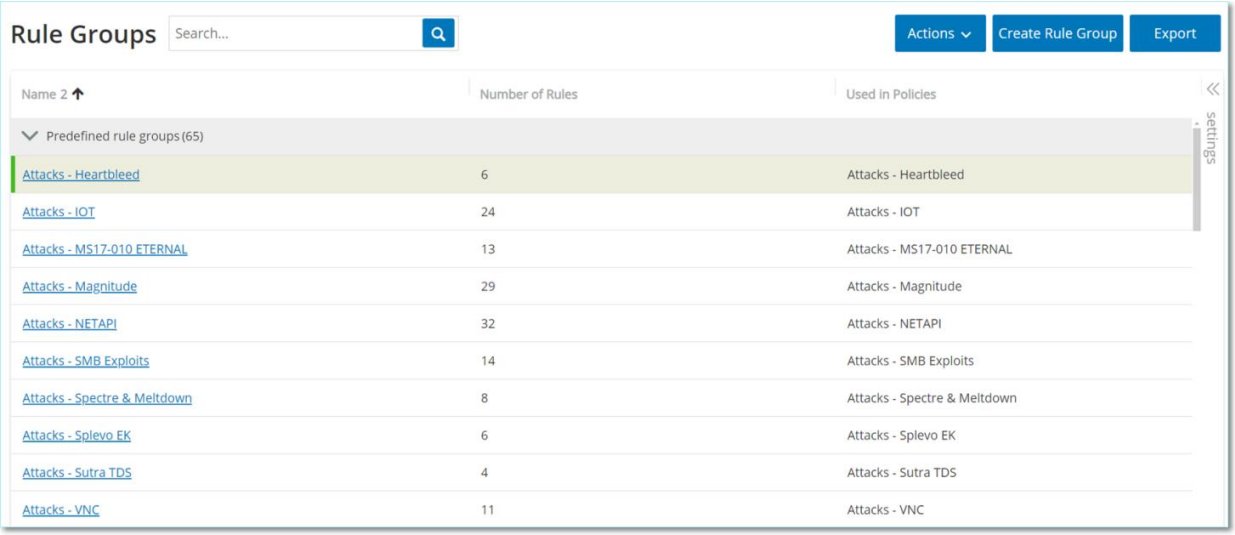
7. In the **Name** field, enter a name for the Group.
8. Select the checkbox next to each of the Tags that you would like to include in the Group.
9. Click **Create**.
   The new Tag Group is created and is shown in the list of Tag Groups. You can now use this Group when configuring SCADA Event Policies.

Rule Groups

Rule Groups are comprised of a group of related rules, which are identified by their Suricata Signature IDs (SIDs). These groups are used as a Policy condition for defining Intrusion Detection Policies.

Tenable.ot provides a set of predefined groups of related vulnerabilities. In addition, you can select individual rules from our repository of vulnerabilities and create your own custom Rule Groups.

Viewing Rule Groups



The **Rule Groups** screen shows all Rule Groups that are currently configured in the system. The *Predefined* tab includes Groups that are built into the system. These Groups can't be edited, duplicated or deleted. The *User defined* tab shows the custom Groups that were created by the user. These Groups can be edited, duplicated or deleted.

The information shown on this screen is described in the following table.

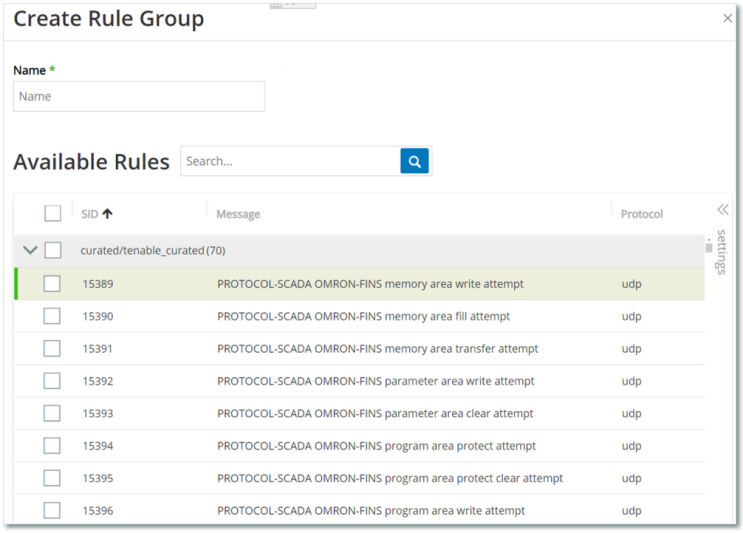
Parameter	Description
Name	The name that is used to identify the Group.
Number of Rules	The number of rules (SIDs) that comprise this Rule Group.
Used in Policies	Shows the Policy ID of each Policy that uses this Rule Group in its configuration. Note: To view additional details about the Policies in which this Group is used, click on **Table Actions** > **View** > **Used in Policies** tab.

Creating Rule Groups

➡ **To create a new Rule Group:**

1. Under **Groups**, select **Rule Groups**.

2. Click **Create Rule Group**.
   The **Create Rule Group** wizard is displayed.



3. In the **Name** field, enter a name for the group.
4. In the **Available Rules** section, select the checkbox next to each of the rules that you would like to include in the group.

> Use the search box to find the desired rules.

5. Click **Create**.
   The new Rule Group is created and is shown in the list of Rule Groups. You can now use this Group when configuring Intrusion Detection Policies.

Actions on Groups

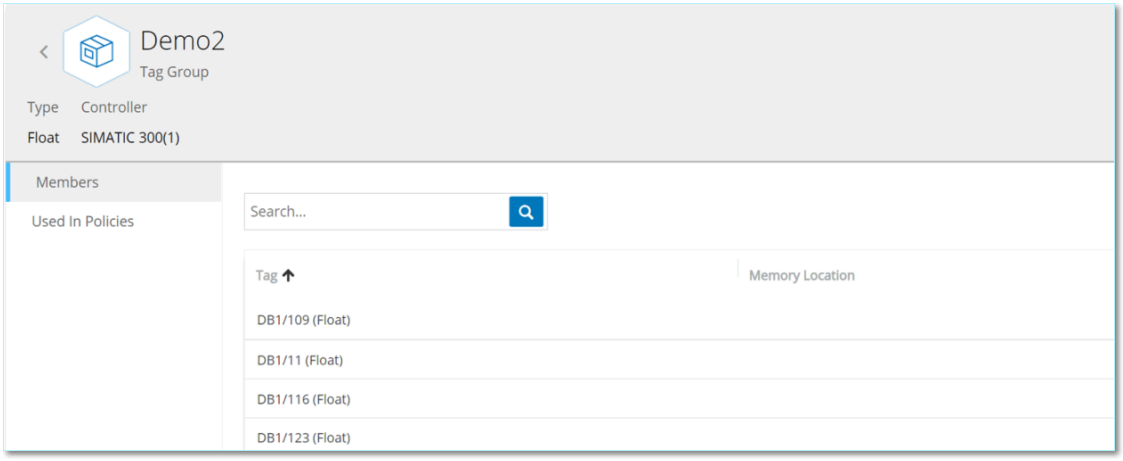
When you select a Group (on any of the Group screens), the Actions menu on the top of the screen enables you to take the following actions:

- View – shows details about the selected Group, such as which entities are included in the group and which Policies use the Group as a policy condition.
- Edit – edit details of the Group.
- Duplicate – create a new Group with similar configuration to the specified Group.
- Delete – delete the Group from the system.

> Predefined Groups can't be edited or deleted. Some predefined Groups also can't be duplicated.
>
> The actions menu can also be accessed by right-clicking on a Group.

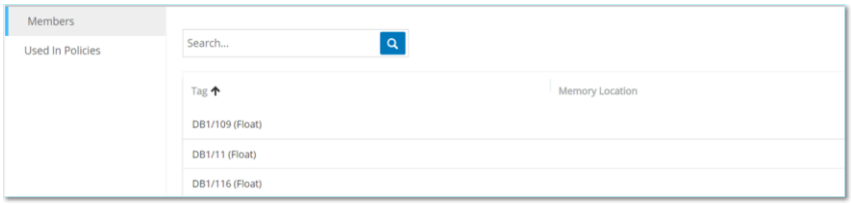
Viewing Group Details

When you select a group and click on **Actions > View** the *Group Details* screen is shown for the selected group.

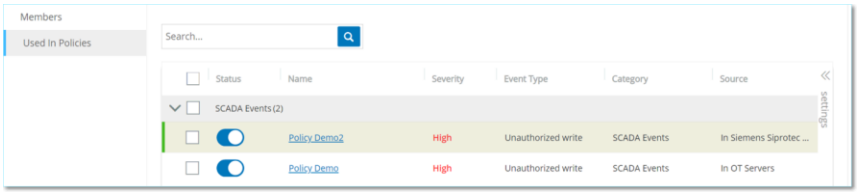


The Group Details screen has a header bar that shows the name and type of the Group. It also has two tabs:

- **Members** – shows a list of all members of the Group.



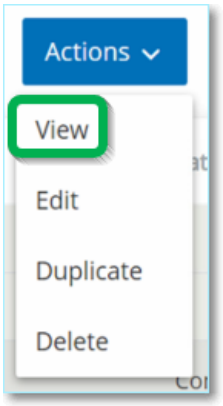
- **Used in Policies** – shows a listing for each Policy for which the specified Group is used as a policy condition. The Policy listing includes a toggle switch for turning the Policy On/Off. The info shown in the Policy lists is explained in the chapter on **POLICIES.**



➡ **To view details of a Group:**

1. Under **Groups**, select the desired type of Group.
2. Select the desired Group.
3. Click on **Actions** (or right-click on the Group).

4. From the dropdown menu, select **View**.



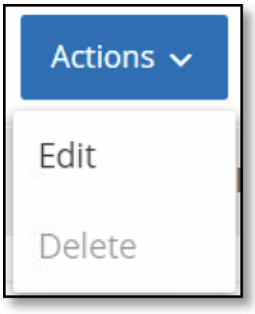
The Group details screen is displayed.

Editing a Group

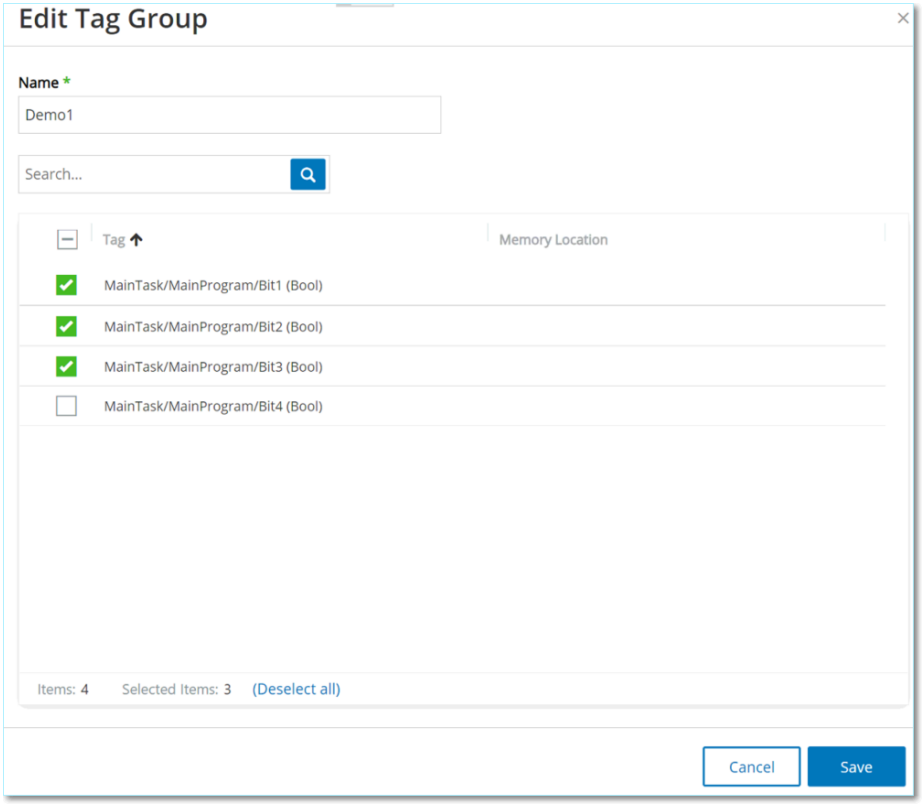
You can edit the details of an existing Group.

➡ **To edit details of a Group:**

1. Under **Groups**, select the desired type of Group.
2. Select the desired Group.
3. Click on **Actions** (or right-click on the Group).
4. From the dropdown menu, select **Edit**.



5. The **Edit Group** window is displayed, showing the relevant parameters for the specified Group type.



6. Make the desired changes.
7. Click **Save**.
   The Group is saved with the new settings.

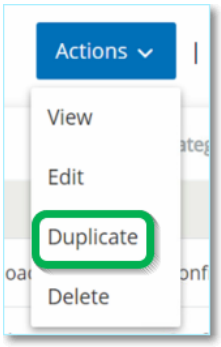
Duplicating a Group

If you would like to create a new Group with similar settings to an existing Group, you can "duplicate" the existing Group. When you duplicate a Group, the new Group is saved under a new name, in addition to the original Group.

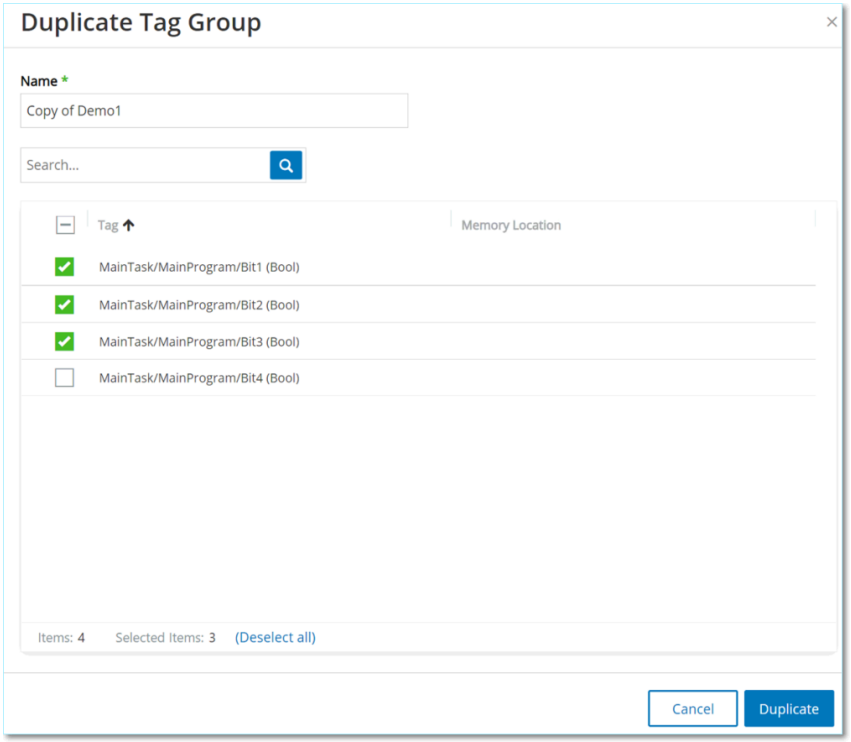
➡ **To Duplicate a Group:**

1. Under **Groups**, select the desired type of Group.
2. Select the existing Group on which you would like to base the new Group.
3. Click on **Actions** (or right-click on the Group).

4. From the dropdown menu, select **Duplicate**.



5. The **Duplicate Group** window is displayed, showing the relevant parameters for the specified Group type.



6. In the **Name** field, enter a name for the new Group. (By default, the new Group is named 'Copy of' the original Group name.)
7. Make the desired changes to the Group settings.
8. Click **Duplicate**.
   The new Group is saved with the new settings, in addition to the existing Group.

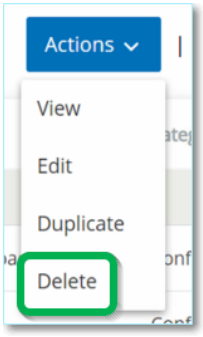
Deleting a Group

You can delete user defined Groups but not predefined Groups. Also, if a user defined Group is being used as a policy condition for one or more Policies it can't be deleted.

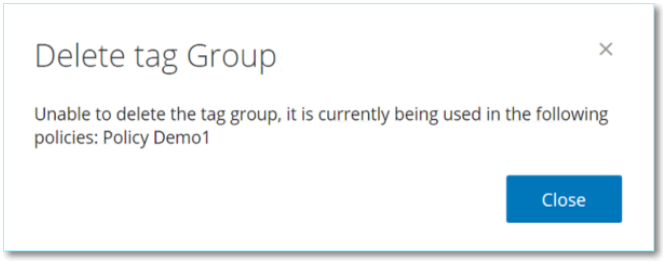
➡ **To Delete a Group:**

1. Under **Groups**, select the desired type of Group.
2. Select the Group that you would like to delete.

3. Click on **Actions** (or right-click on the Group).
4. From the dropdown menu, select **Delete**.



5. A confirmation window is displayed.

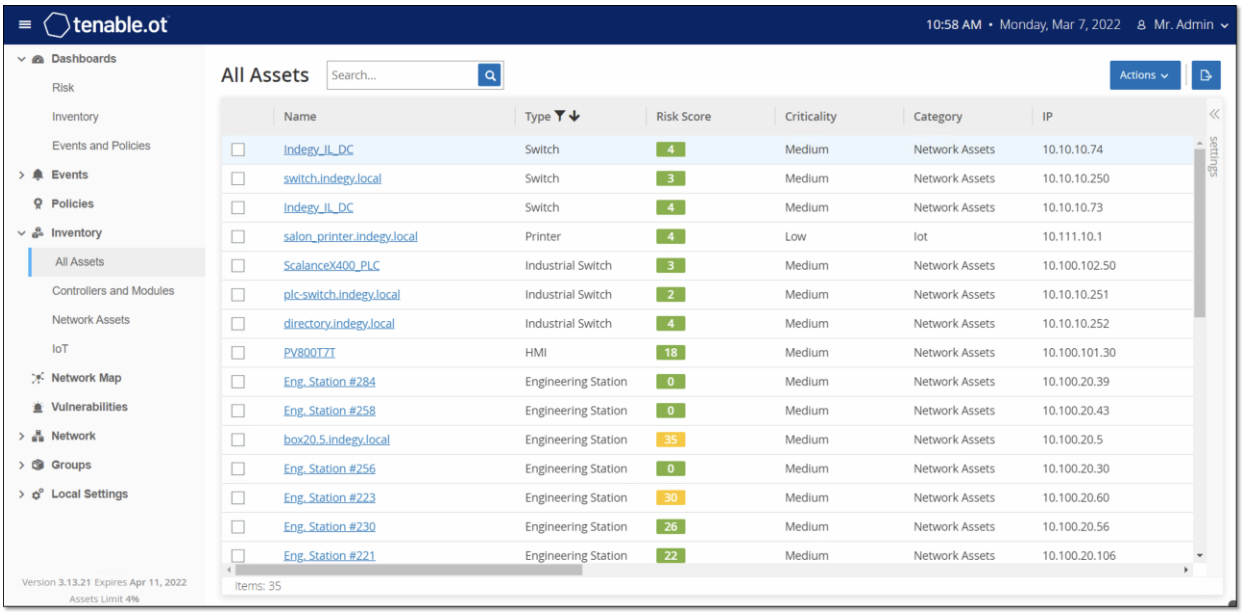


6. Click **Delete**.
   The Group is permanently deleted from the system.

Inventory

Tenable.ot's Automated Asset Discovery, Classification and Management provides an accurate, up-to-date asset inventory by continuously tracking all changes to devices. This simplifies sustaining of operational continuity, reliability and safety. It also plays a key role in planning maintenance projects, prioritizing upgrades, patch deployments, incident response and mitigation efforts.

Viewing Assets



All of the assets in the network are shown on the Inventory screens. Detailed data about each asset is shown, enabling comprehensive asset management as well as monitoring of the status of each asset and its related Events. The data shown in the Inventory screens is gathered using the Tenable.ot Network Detection and Active Query capabilities. The **All** screen shows data for all types of assets. In addition, specific subsets of the assets are shown on separate screens for each of the following asset types: **Controllers and Modules**, **Network Assets** and **IoT**.

The *Network Assets* screen includes all types of assets that aren't included in the *Controllers and Modules* or *IoT* screens.

For each of the asset screens (*All*, *Controllers and Modules*, *Network Assets* and *IoT*), you can customize the display settings by adjusting which columns are displayed and where each column is positioned. You can also sort and filter the Asset lists as well as perform a search. For an explanation of the customization features, see **WORKING WITH LISTS**.

The following table describes the parameters shown on the Inventory screens.

Parameters marked with an "*" are only shown on the *Controllers* screen.

Parameter	Description
Name	The name of the asset in the network. Click the name of the asset to view the Asset Details screen for that asset (See **VIEWING ASSET DETAILS**.)
IP	The IP address of the asset. Note: An asset may have multiple IP addresses.
MAC	The MAC address of the asset.
Network Segment	The Network Segment that the IP/s of this asset are assigned to.
Type	The type of asset, *Controller*, *I/O* or *Communication*, etc. see **ASSET TYPES**.
Backplane*	The backplane unit that the asset is connected to. Additional details about the backplane configuration are shown in the Asset Details screen.
Slot*	For assets that are on backplanes, shows the number of the slot to which the asset is attached.
Vendor	The asset vendor.
Family*	The family name of the product as defined by the asset vendor.
Firmware	The firmware version currently installed on the asset.
Location	The location of the asset as input by the user in the Tenable.ot asset details. See **EDITING ASSET DETAILS**.
Last Seen	The time at which the device was last seen by Tenable.ot. This is the last time that the device was connected to the network or performed an activity.
OS	The OS running on the asset.
Model Name	The model name of the asset.
State*	The device state. Possible values: • Backup – the controller is running as a backup to a primary controller. • Fault – the controller is in fault mode. • NoConfig – no configuration has been set for the controller. • Running – the controller is running. • Stopped – the controller is not running. • Unknown – the state is unknown.

Parameter	Description
Description	A brief description of the asset, as configured by the user in the Tenable.ot asset details. See **Editing Asset Details**.
Risk	A measure of the degree of risk related to this asset on a scale from 0 (no risk) to 100 (extremely high risk). For an explanation of how the Risk score is calculated, see **Risk Assessment**.
Criticality	A measure of the importance of this asset to the proper functioning of the system. A value is assigned automatically to each asset based on the asset type. You can manually adjust the value.
Purdue Level	The Purdue level of the asset (0=Physical process, 1=Intelligent devices, 2=Control systems, 3=Manufacturing operations systems, 4=Business logistics systems).
Custom Field	You can create custom fields to tag your assets with relevant info. The custom field can be a link to an external resource.

Asset Types

The following table describes the various types of assets identified by Tenable.ot. It also shows the icon by which each asset type is represented in the Tenable.ot Management Console (e.g. on the Network Map screen).

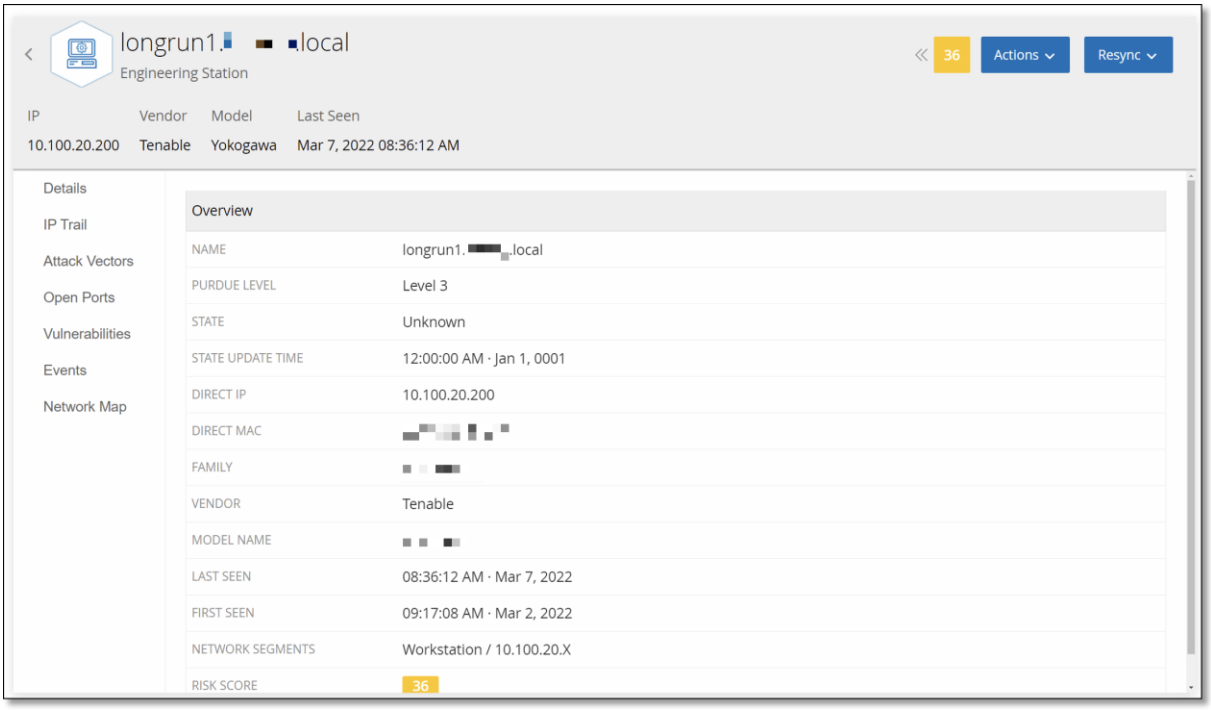
Category	Description	Sub-Types	
Controllers	An industrial computer control system that continuously monitors the state of input devices and makes decisions based upon a custom program to control the state of output devices. This category includes all types of controllers and their related components.		Controller
			PLC
			DCS
			IED
			RTU
			Communication Module
			I/O Module
			CNC

Category	Description	Sub-Types	
			Power Supply
Field Devices	An industrial device (e.g. sensor, actuator, electric motor) that uses industrial protocols to send information to ICS systems.		Field Device
			Actuator
			Smart Sensor
			Inverter
			Relay
			Remote I/O
			Power Meter
OT Devices	This category includes all types of OT devices.		OT Device
			Industrial Printer
OT Servers	A computer/device that is used to access industrial data. This category includes all types of OT servers and their related components.		OT Server
			Historian
			HMI
			Data Logger
Network Devices	A networking device (e.g. a switch or a router). This category includes all types of network devices and their related components.		Network Device
			Router
			Switch

Category	Description	Sub-Types	
			Hub
			Wireless Access Point
			Firewall
			Converter
			Radio
			Serial Ethernet Bridge
			Gateway
Workstations	A computer that is connected to the network and used to control the PLCs. This category includes all types of workstations and their related components.		Workstation
			OT Workstation
			Engineering Station
			Virtual Workstation
Servers	This category includes various types of IT servers.		Server
			File server
			Web Server
			Virtual Server
IoTs	This category includes various type of interrelated devices.		IoT
			Camera

Category	Description	Sub-Types	
			Panel
			Projector
			VOIP Device
			3D Printer
			Printer
			UPS
			IP Phone
			Storage Device
Endpoints	An unidentified IP address in the network.		Endpoint
			Mobile

Viewing Asset Details



The **Asset Details** screen shows comprehensive details about all data discovered by Tenable.ot for the selected asset. The details are shown in the Header bar as well as in a series of tabs and subsections. Some tabs and subsections are relevant only for specific Asset Types.

The Asset Details screen for a particular asset is accessed by clicking on the Name of the asset wherever it appears as a link in the Management Console (e.g. Inventory, Events, Network etc.) or by clicking **Actions** > **View** on the relevant **Inventory** screen.

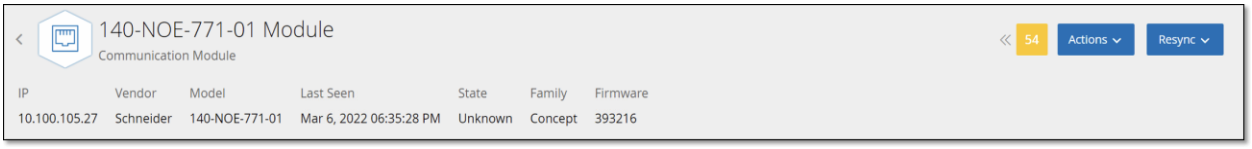
The following elements are included in the Asset Details screen (for relevant asset types):

- **Header Pane** – shows an overview of essential info about the asset and its current state. It also contains an *Actions* menu that enables you to edit the listing for that asset.
- **Details** – shows detailed information divided into subsection with specific data that is relevant to various asset types.
- **Code Revisions** (for controllers only) – shows information about current as well as previous code revisions as discovered by the Tenable.ot 'snapshot' function. This includes details of all the specific changes that were introduced to the code, i.e. the sections (code blocks/rungs) that were added, deleted or changed.
- **IP Trail** – shows all current and historical IPs that are related to the asset.
- **Attack Vectors** – shows vulnerable attack vectors, i.e. the routes that an attacker can use to gain access to this asset. You can generate an attack vector automatically, to show the most critical attack vector or you can manually generate attack vectors from specific assets.
- **Open Ports** – shows info about open ports on the asset.
- **Vulnerabilities –** shows the vulnerabilities the system identified for the selected asset, such as obsolete Windows operating systems, usage of vulnerable protocols and open communications

ports which are known to be risky or non-essential for specific types of devices, see **VULNERABILITIES**.

- Events – a list of Events in the network involving the asset.
- Network Map – shows a graphic visualization of the network connections of the asset.
- Device Ports (for network switches) – shows info about ports on the network switch.

Header Pane



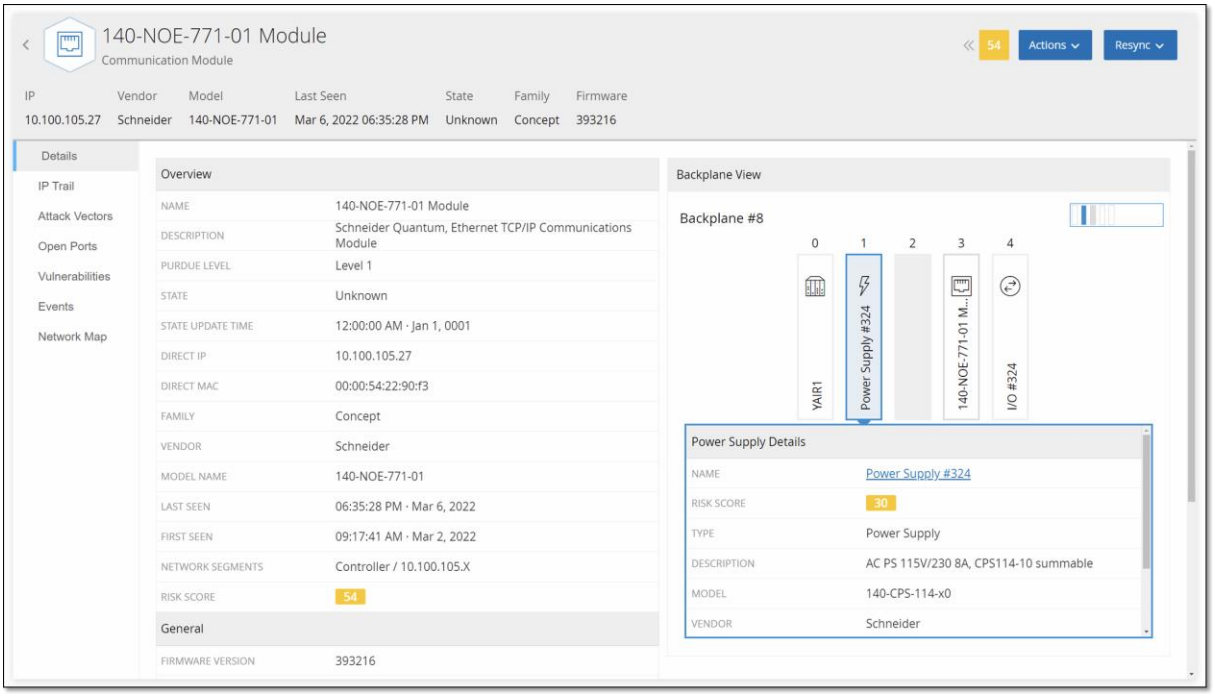
The Header Pane shows an overview of the current state of the asset. The display includes the following elements:

- Name – the name of the asset.
- Back (link) – sends you back to the screen from which you accessed this asset screen.
- Asset Type – shows icon and name of the asset type.
- Asset Overview – shows essential info about the asset, including IP/s, Vendor, Family, Model, Firmware and Last Seen (date and time).
- Risk Score Widget – shows the Risk score for the asset. The Risk score is an assessment (from 1 to 100) of the degree of threat posed to the asset. For an explanation of how the value is determined, see **RISK ASSESSMENT**. Click on the Risk Score indicator to show an expanded widget with a breakdown of the factors that contribute to assessing the Risk level (Unresolved Events, Vulnerabilities, and Criticality).

  Some of the elements are a link to the relevant screen that shows details about that element.
- Actions Menu – Allows you to edit the asset details or run a Nessus scan.
- Resync Button – click on this button to manually run one or more of the queries that are available for this asset. See **PERFORMING RESYNC**.

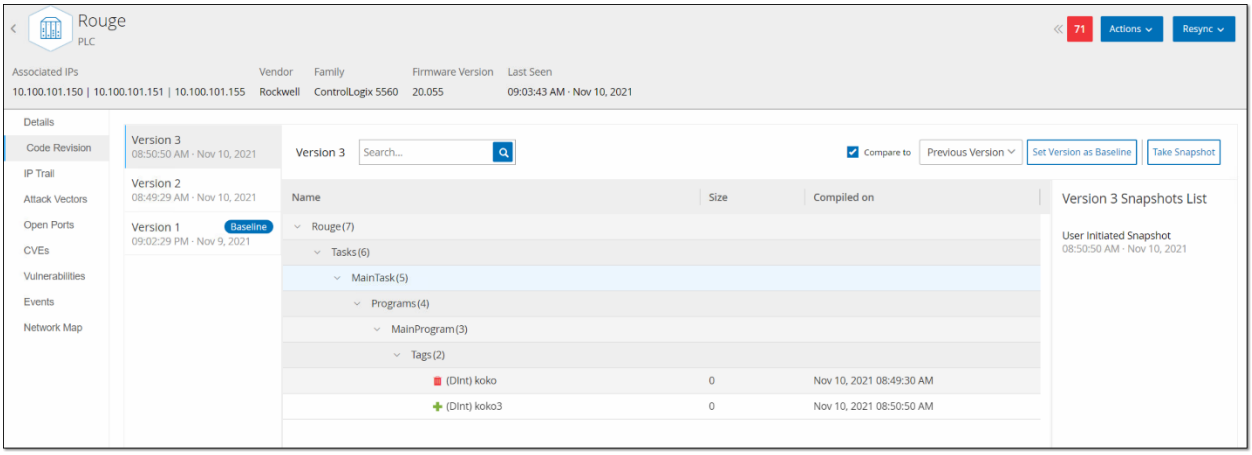
Details Tab



The **Details** tab shows additional details about the selected asset. The information is divided into sections showing various types of system and configuration data for the specified asset. Only sections that are relevant for the specified asset are shown. The following is a list of all of the section categories that may be shown for various types of assets: *Overview*, *General*, *Project*, *Memory*, *Ethernet*, *Profinet*, *OS*, *System*, *Hardware*, *Devices & Drives*, *USB Devices*, *Installed Software*, *IEC-61850*, and *Interface Status*.

For assets that are connected to a backplane, there is also a *Backplane View* section, which shows a graphic representation of the backplane configuration, including the slot position of each connected device. Select a device to show its details in the lower pane.

Code Revisions



The **Code Revision** tab (for Controllers only) shows the various versions of the controller's code that were captured by Tenable.ot "snapshots". Each "snapshot" version includes information about the code revision at the time that the "snapshot" was taken, including details about specific sections (code blocks/rungs) and tags. Whenever a "snapshot" isn't identical to the previous "snapshot" of that controller, a new *Version* of the code revision is created. You can compare between versions to see what changes were made to the controller code.

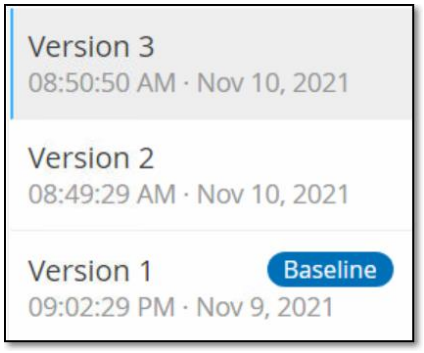
A snapshot can be triggered in the following ways:

- **Routine** – snapshots are taken at regular intervals, as set by the user in the system settings screen.
- **Activity Triggered** – the system triggers a snapshot when a particular code activity is detected (e.g. a code download).
- **User Initiated** – the user can manually trigger a snapshot by clicking the **Take Snapshot** button for a specific asset.

You can configure a "Snapshot Mismatch" Policy to detect additions, deletions or changes made to a controller's code, see **Configuration Event - Controller Validation Event Types**.

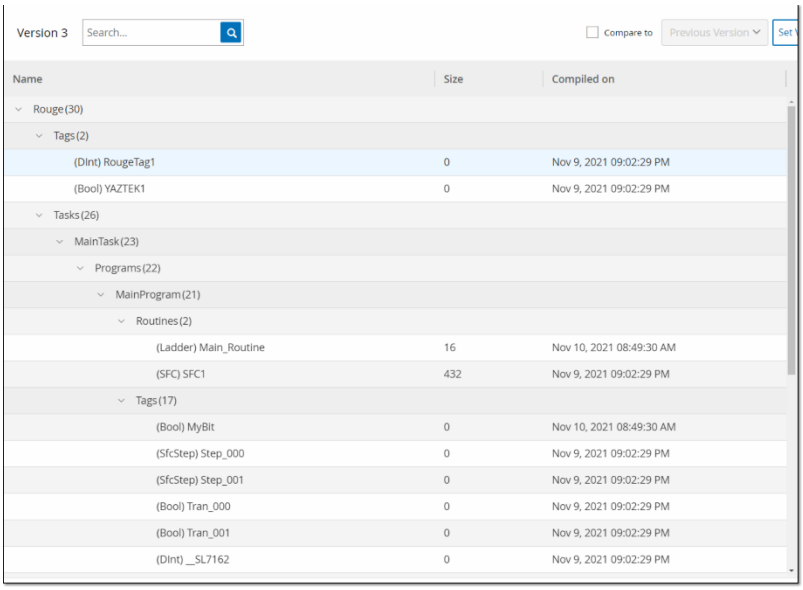
The following sections describe the various sections of the Code Revision display as well as how to compare different "snapshot" versions.

Version Selection Pane



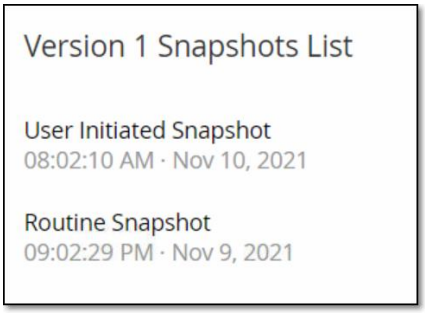
This pane shows a list of all available versions of the code revision for this controller. For each version the *Start* time that the version is known to have been in place is displayed. A new version is created each time that a change is detected from the previous "snapshot". The "Baseline" tag indicates which version is currently set as the baseline version for the purpose of comparison. Select a version to show its code revisions in the Snapshot Details pane.

Snapshot Details Pane



The details pane shows detailed information about the specific code blocks, rungs and tags for the selected snapshot version. The code elements are displayed in a tree structure with arrows for expanding/minimizing the details shown. For each element, the name, size, and date compiled are shown. You can compare the selected version to the previous version or to the "baseline" version to see what changes were made, see **Comparing Snapshot Versions**.

Version History Pane



This pane shows details about the "snapshot" that captured the selected version, including the method by which it was initiated as well as the date and time that it was captured.

If no changes were made between snapshots, then several snapshots are grouped together as a single version. All the identical snapshots are listed in the Snapshot History pane for that version.

Comparing Snapshot Versions

You can compare a Snapshot version either to the *previous* version or to the *baseline* version. Once a comparison has been run, the Snapshot Details pane shows the changes that were made to the controller's code between the two snapshots.

Changes are marked in the following manner:

Added – new code that was added in the selected version.

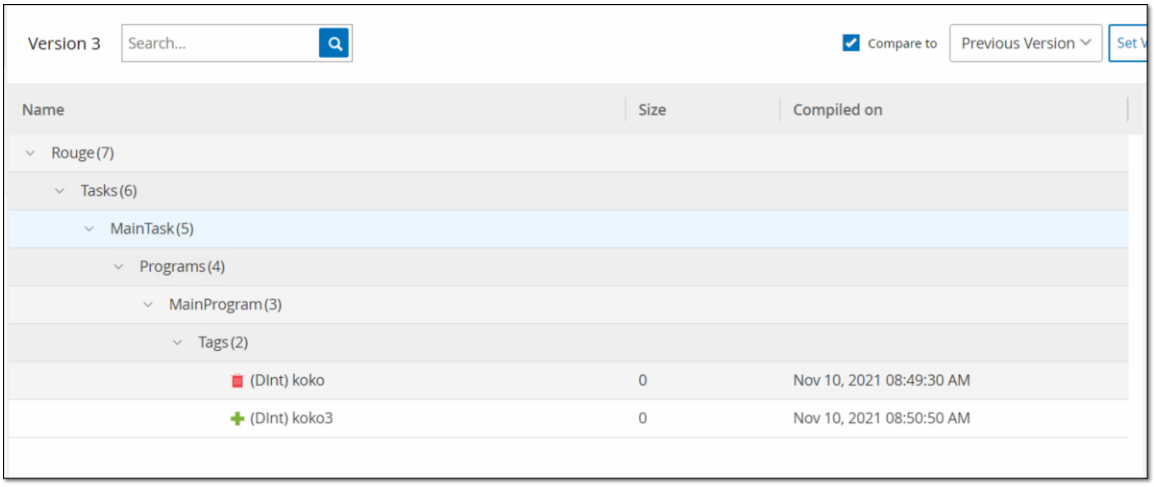
Deleted – code that was deleted from the selected version.

Edited – code that was edited in the selected version.

To compare a snapshot version to the previous version:

1. On the **Inventory** > **Controllers** screen, select the desired controller.
2. Click on the **Code Revision** tab.
3. In the **Version Selection** pane, select the version that you would like to analyze.
4. At the top of the **Snapshot Details** pane, in the comparison field, select **Previous Version** from the dropdown menu.
5. Click the **Compare to** checkbox.
   The Snapshot Details pane shows all differences between the two versions. For each change,

an icon indicates the type of change that occurred.



➡ **To compare a snapshot version to an earlier version (other than the previous version):**

1. On the **Inventory** > **Controllers** screen, select the desired controller.
2. Click on the **Code Revision** tab.
3. In the **Version Selection** pane, select the version that you would like to use as the baseline for comparison.
4. In the top of the **Snapshot Details** pane, click **Set Version as Baseline**.
   The **Baseline** tag is shown for the selected version, indicating that it is set as the baseline version.

Setting a version as the baseline affects only comparisons made using this screen. It does not affect Policies that check for *Snapshot Mismatch*.

5. In the **Version Selection** pane, select the version that you would like to compare to the baseline.
6. Click the **Compare to** checkbox.
7. In the field next to the Compare to checkbox, select **Baseline Version** from the dropdown menu.
   The Snapshot Details pane shows all differences between the two versions. For each change, an icon indicates the type of change that occurred.

Creating a Snapshot

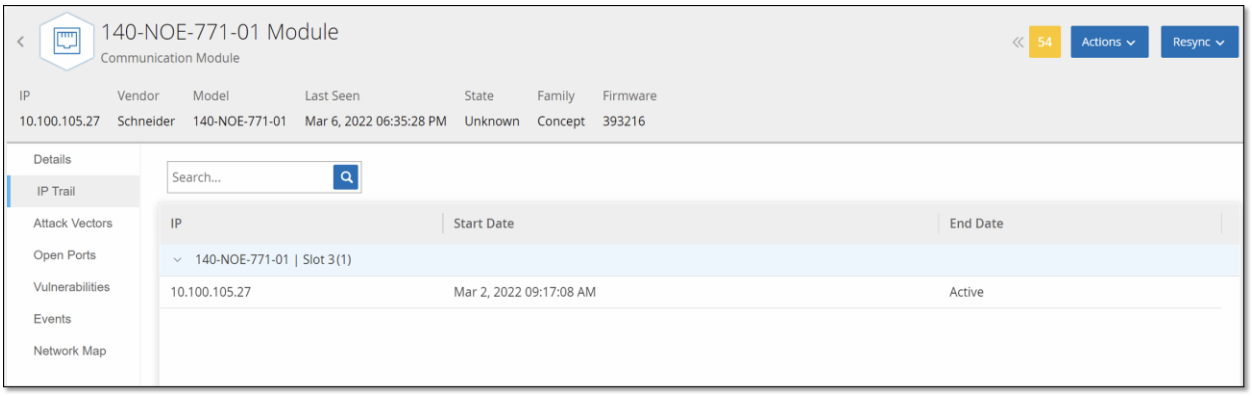
A snapshot can be initiated manually by the user. For example, it is recommended to perform a snapshot before and after a technician services a controller.

➡ **To create a snapshot of a controller:**

1. On the **Inventory** > **Controllers** screen, select the desired controller.
2. Click on the **Code Revision** tab.
3. In the upper right-hand corner of the **Snapshot Details** pane, click **Take Snapshot**.
   The User Initiated Snapshot is created.

4. If no changes are identified, then a new User Identified Snapshot is added to the Revision History pane for the latest version. If changes are identified, then a new version is created showing the code revision changes.

IP Trail



The **IP Trail** tab shows all IPs relevant to this asset. The Network Card column shows a listing of network cards used by this asset. Click on the arrow next to a network card to expand the listing to show the IPs of all assets connected to the shared backplane.

The lists include the Start and End Dates of the usage of the IP address. The options for End Date are:

- **Active** – the IP address is currently being used for this asset.
- **{date/time}** – the last date and time the IP address was active for this asset (if it has been active within the last 30 days).
- **{date/time} (Inactive)** – the last date and time the IP address was active for this asset (if it has been inactive for 30 days or more).
- **Inactive** – the IP address is being used by another asset.

Attack Vectors

An attacker can compromise a critical access by taking advantage of a vulnerable “weak link” in the network to gain access to the critical asset. The critical asset is the target (destination) of the attack, and the *Attack Vector* is the route the attacker uses to gain access to that asset.

How do we determine the attack vector?

Once the target asset is specified, the system calculates all of the potential attack vectors that could enable access to this asset and identify the path that has the highest risk potential for compromising this asset. The calculation factors in multiple parameters and uses a risk-based approach in order to identify the most critical attack vector. The parameters that are used include:

- Asset risk level
- Length of the path
- Asset to asset communication method
- External communication (Internet/Corporate) vs. internal communication

Recommended Mitigation Steps

In order to minimize the risk of a potential attack using the selected vector, the recommended mitigation steps include the following:

- Reducing the associated and individual risk scores of the assets which are included in the attack vector.
- Minimizing or removing network access to external networks (Internet or corporate networks)
- Examining the communication paths along the chain and validating their relevance to the process. In case they are not vital, they should be removed (e.g. Port closing or service removal) in order to eliminate the potential attack path.

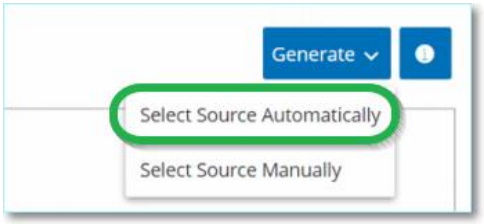
Generating Attack Vectors

Attack Vectors need to be generated manually for each relevant target asset. This is done on the Attack Vectors tab for the desired target asset. There are two methods for generating Attack Vectors:

- Automatic – Tenable.ot assesses all potential attack vectors and identifies the most vulnerable path.
- Manual – You specify a particular source asset and Tenable.ot shows you the potential path (if any) that can be used to access your target asset.

➡ **To generate an automatic Attack Vector:**

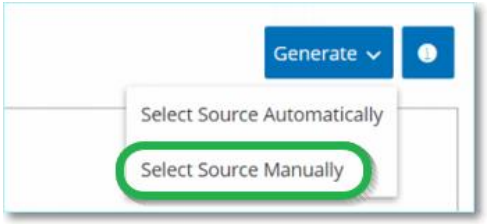
1. Navigate to the **Asset Details** page for the desired target asset and click on the **Attack Vector** tab.
2. Click **Generate** and then click **Select Source Automatically** from the dropdown list.



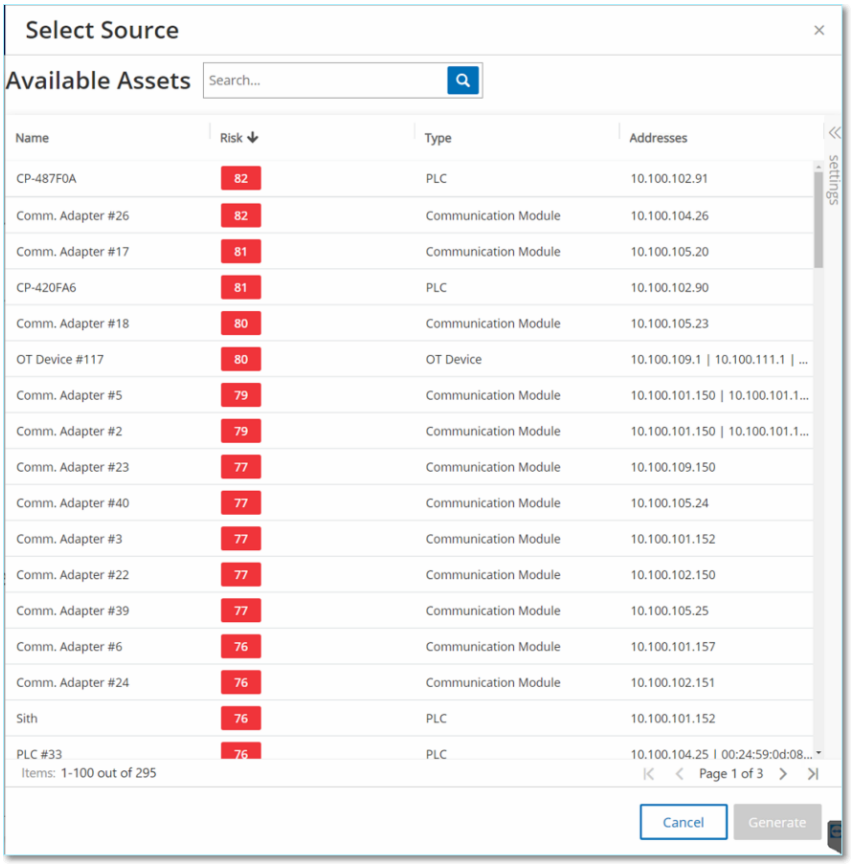
The Attack Vector is generated automatically and is displayed in the **Attack Vector** tab.

➡ **To generate a manual Attack Vector:**

1. Navigate to the **Asset Details** page for the desired target asset and click on the **Attack Vector** tab.
2. Click **Generate** and then click **Select Source Manually** from the dropdown list.



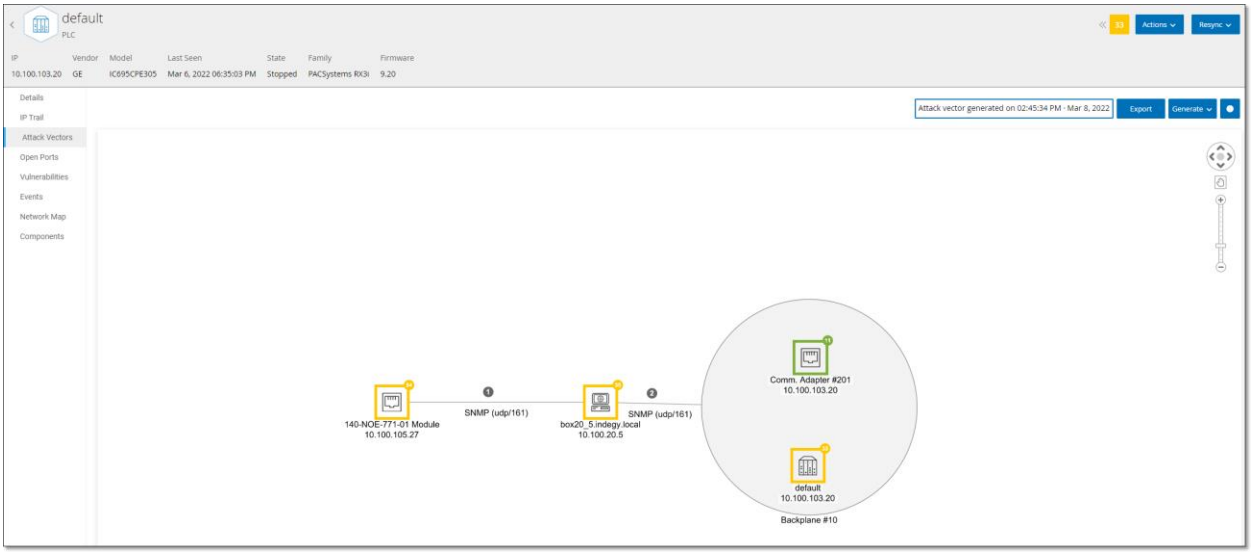
The **Select Source** window is displayed.



By default, the source assets are sorted by Risk score. You can adjust the display settings or search for the desired asset.

3. Select the desired source asset.
4. Click **Generate**.
   The Attack Vector is generated and is displayed in the **Attack Vector** tab.

Viewing Attack Vectors

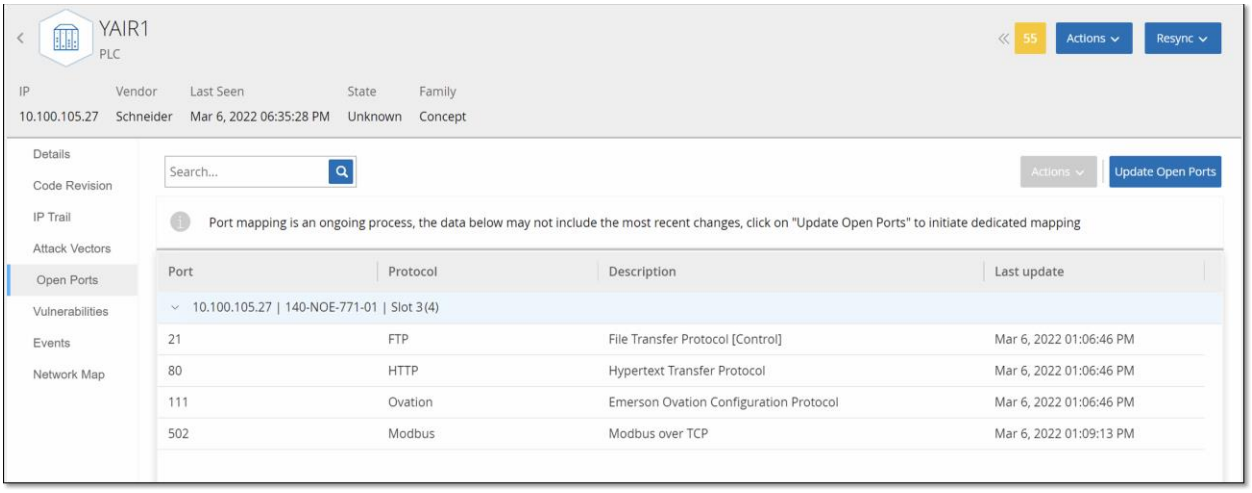


The Attack Vectors tab shows a diagram of the most recently generated Attack Vector for the specified target asset. The box next to the Generate button shows the date and time that the displayed Attack Vector was generated. The Attack Vector diagram includes the following elements:

- For each asset that is included in the Attack Vector, the risk level and IP addresses are shown. Click on an asset icon to show additional details about its risk factors.
- For each network connection, the communication protocol is shown.
- For assets that share a backplane, the assets are surrounded by a circle.

Click on the help button in the top right corner of the Attack Vectors tab for an explanation of the Attack Vector feature.

Open Ports



The Open Ports tab shows a list of open ports on this asset. For each open port details are given about which protocol it uses, a description of its function and the date and time that the data was last updated. A separate list of open ports is shown for each IP available to the asset (including ports that are accessed through a shared backplane). Click on the arrow next to an IP to expand the listing to show its open ports.

The open port scanning parameters are configured in the Local Settings tab, see **All Controller Queries**. You can also run a manual query of the selected asset to update the list of open ports.

➡ **To manually update the list of open ports:**

1. In the **Inventory > Controllers/Network Assets** screen, select the desired asset.
   The **Asset Details** screen is displayed.
2. Click on the **Open Ports** tab.
3. In the upper right-hand corner of the Open Ports pane, click **Update Open Ports**.
   A new scan is run, updating the open ports shown for this controller.

Additional Actions in the Open Ports Tab

In the Open Ports tab for a specific asset, you can take the following further actions for a specific open port.

- Scan – run a scan of the selected port.
- View – shows additional device details and diagnostics by accessing the web interface of the device.

➡ **To run a scan on a specific port:**

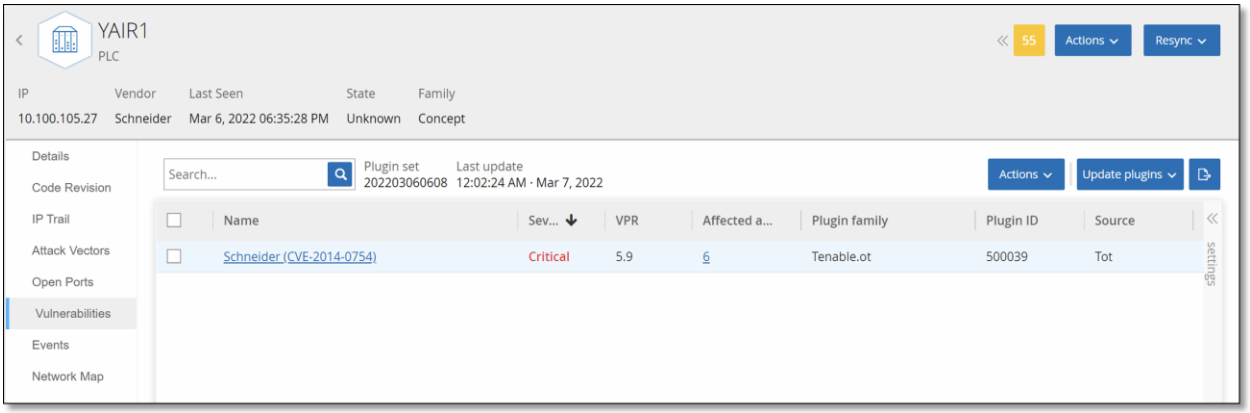
1. In the **Inventory > Controllers/Network Assets** screen, select the desired asset.
   The **Asset Details** screen is displayed.
2. Click on the **Open Ports** tab.
3. Select a specific port.
4. Click on the **Actions** menu.
5. From the drop-down menu, select **Scan**.
   Tenable.ot runs a scan on the selected port.

➡ **To view the asset's portal:**

This option is only available when port 80 (used for web-access) is one of the open ports.

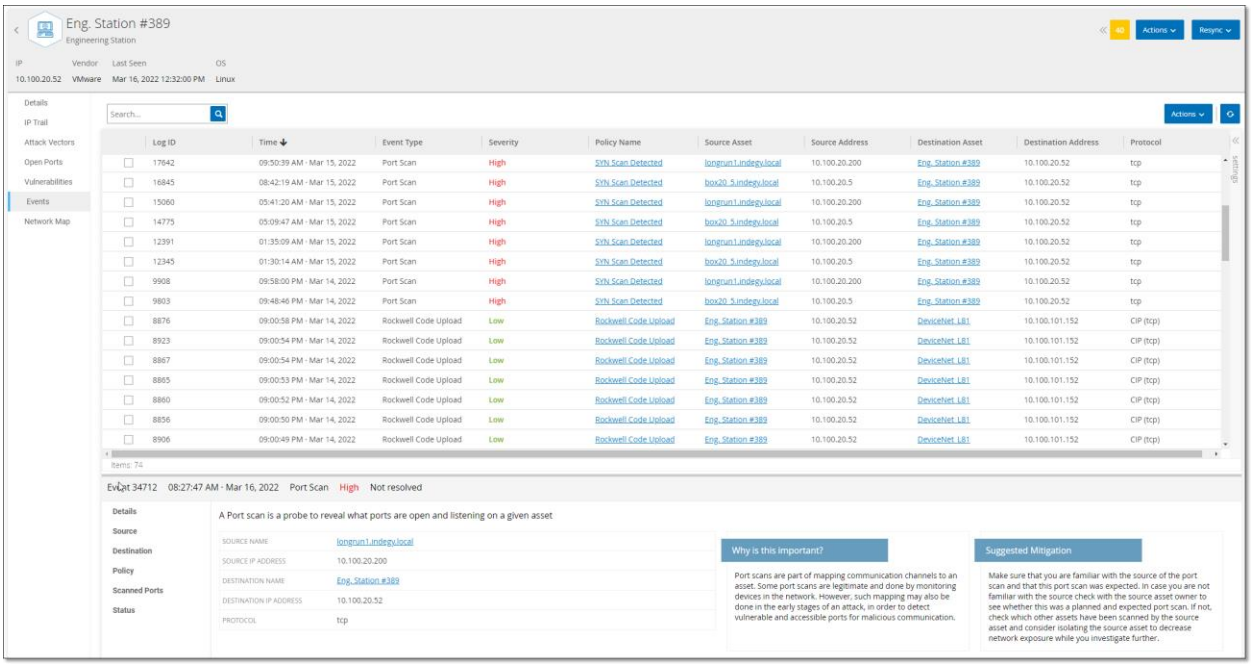
1. In the **Inventory > Controllers/Network Assets** screen, select the desired asset.
   The **Asset Details** screen is displayed.
2. Click on the **Open Ports** tab.
3. Select a specific port.
4. Click on the **Actions** menu.
5. From the drop-down menu, select **View**.
   A new browser tab opens showing the asset portal of that asset.

Vulnerabilities



The **Vulnerabilities** tab shows a list of all Vulnerabilities that affect the specified asset, as detected by Tenable.ot Plugins. The system identifies vulnerabilities such as obsolete Windows operating systems, usage of vulnerable protocols and open communications ports which are known to be risky or non-essential for specific types of devices. Each listing shows details about the nature of the threat and its severity. The information shown in this tab is **identical to the information shown on the Risk > Vulnerabilities screen**, except that only vulnerabilities relevant to the specified asset are shown here. For an explanation of the vulnerabilities information, see **VULNERABILITIES.**

Events



The **Events** tab displays a detailed list of Events in the network involving the asset, as detected by Tenable.ot Plugins. You can customize the display settings by adjusting which columns are displayed and where each column is positioned. The events can be grouped according to different categories (e.g.

Event type, Severity, Policy Name). You can also sort and filter the Event lists as well as searching for search text. For an explanation of the customization features, see **Working with Lists**.

The bottom of the screen shows detailed information about the selected Event, divided into tabs. Only tabs relevant to the Event type of the selected Event are shown. For more information about Events, see **Events**.

There is an Actions button at the top of the pane, which enables you to take the following Action on the selected Event/s:

- Resolve – Mark this Event as Resolved.
- Download PCAP – Download the PCAP file for this Event.
- Exclude – Create a Policy Exclusion for this Event.

Detailed information about these actions is given in the **Events** chapter.

The information shown for each Event listing is described in the following table:

Parameter	Description
Log ID	The ID generated by the system to refer to the Event.
Time	The date and time that the Event occurred.
Event Type	Describes the type of activity that triggered the Event. Events are generated by Policies that are set up in the system. For an explanation of the various types of Policies, see **Policy Types**.
Severity	Shows the severity level of the Event. The following is explanation of the possible values: None - No reason for concern. Info - No immediate reason for concern. Should be checked out when convenient. Warning - Moderate concern that potentially harmful activity has occurred. Should be dealt with when convenient. Critical - Severe concern that potentially harmful activity has occurred. Should be dealt with immediately.
Policy Name	The name of the Policy that generated the Event. The name is a link to the Policy listing.
Source Asset	The name of the asset that initiated the Event. This field is a link to the Asset listing.
Source Address	The IP or MAC of the asset that initiated the Event.
Destination Asset	The name of the asset that was affected by the Event. This field is a link to the Asset listing.
Destination Address	The IP or MAC of the asset that was affected by the Event.

Protocol	When relevant, this shows the protocol used for the conversation that generated this Event.
Event Category	Shows the general category of the Event. Note: On the All Events screen, Events of all types are shown. Each of the specific Event screens shows only Events of the specified category. The following is a brief explanation of the Event categories (for a more detailed explanation see **Policy Categories**): • Configuration Events – this includes two sub-categories • Controller Validation Events – These policies detect changes that take place in the controllers in the network. • Controller Activity Events – Activity Policies relate to the Activities that occur in the network (i.e., the "commands" implemented between assets in the network). • SCADA Events – policies that identify changes made to the data plane of controllers. • Network Threats Events – these Policies identify network traffic that is indicative of intrusion threats. • Network Events – Policies that relate to the assets in the network and the communication streams between assets.
Status	Shows whether or not the Event has been marked as resolved.
Resolved By	For resolved Events, shows which user marked the Event as resolved.
Resolved On	For resolved Events, shows when the Event was marked as resolved.
Comment	Shows any comments that were added when the Event was resolved.

Network Map

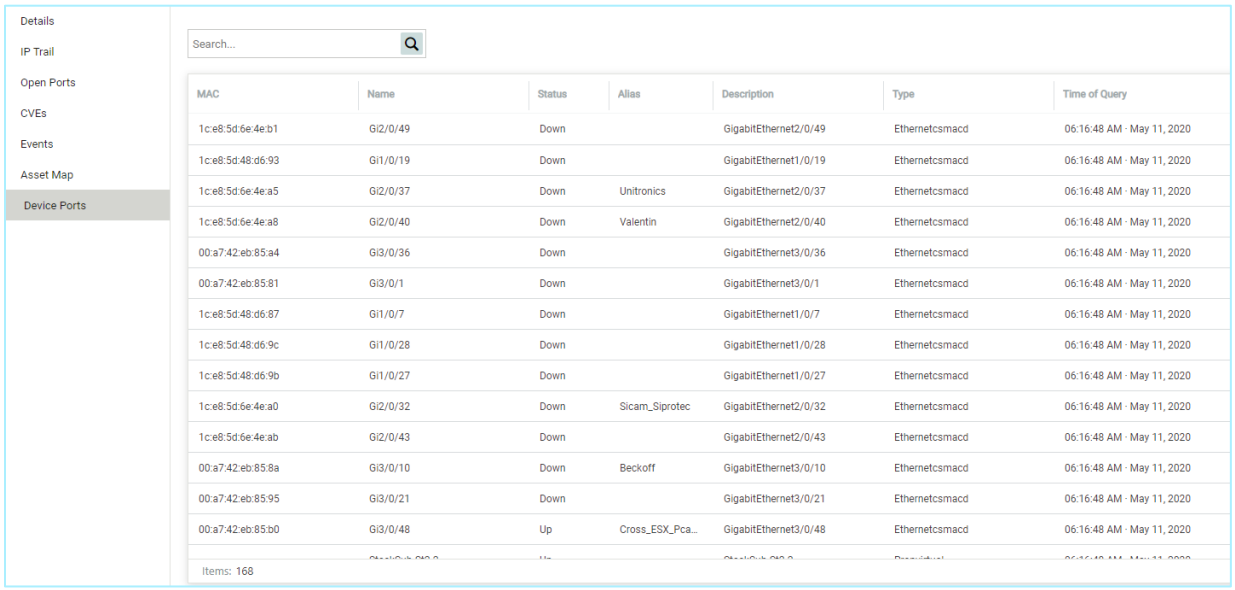
The **Network Map** tab shows a graphic visualization of the network connections of the asset. This view shows all of the connections that the selected asset made during the past 30 days.

The information shown in this tab is similar to the information shown on the **Network Map** screen, but it is limited to connections involving this specific asset. Also, this screen shows connections to individual assets and not to groups of assets as shown in the main Network Map screen. For an explanation of the information shown in this tab, see **NETWORK MAP**.

To view the Network Map for all assets, click the **Go to network map** button. When clicked, the Network Map will zoom in dynamically and focus on this asset and show its connections to other groups of assets.

Clicking on any of the connected assets on the map shows details of that asset, and clicking on the link in the asset's name takes you to the selected asset's Details screen.

Device Ports



The **Device Ports** tab is shown for network switches. It shows detailed information about the ports on the network switch. This data is collected by using SNMP queries to the switch. For each port, the following info is shown: the *MAC* address, *Name*, connection *Status* (up or down), *Alias* and *Description*.

> This tab is only available if it was activated for your account. To activate this feature, contact your Support agent.

Editing Asset Details

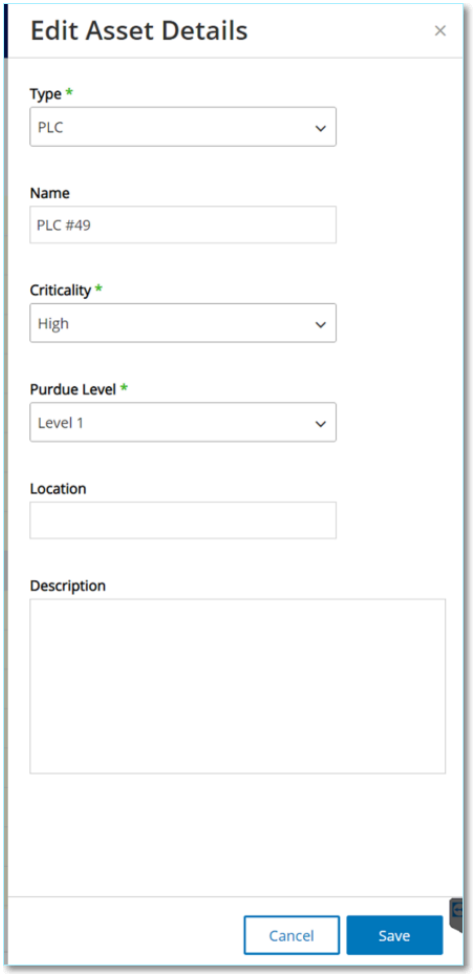
Tenable.ot automatically identifies the Asset Type and Name based on its internal data and based on its activity in the network. If the system couldn't gather this information or if you feel that the automatic identification is not accurate, you can edit these parameters either directly through the UI or by uploading a CSV file. You can also add a general description of the asset and a description of the location of the unit.

Editing Asset Details through the UI

➡ **To edit asset details for a single asset:**

1. Under **Inventory**, click on **Controllers** or **Network Assets**.
2. Select the desired asset.
3. In the Header bar, click on the **Actions** button.

4. From the drop-down list, select **Edit**.
   The **Edit Asset Details** window opens.



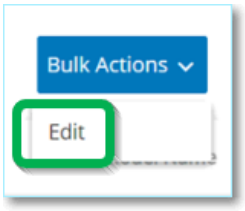
5. In the **Type** field, select the asset type from the dropdown list.
6. In the **Name** field, enter a name by which the asset will be identified in the Tenable.ot UI.
7. In the **Criticality** field, enter the level of criticality of this asset to the system.
8. In the **Purdue Level** field, enter the Purdue level based on the asset type.
9. In the **Backplane** field (for Controllers), enter the name of the backplane on which the asset is installed.
10. In the **Location** field, enter a description of the asset's location. This is an optional field. The data is shown in the assets table as well as on the Asset Details screen for this asset.
11. In the **Description** field, enter a description of the asset. This is an optional field. The data is shown on the Asset Details screen for this asset.
12. Click **Save**.
    The edited details are saved for that asset.

➡ **To Edit multiple assets (bulk process):**

1. Under **Inventory**, click on **Controllers** or **Network Assets**.
2. Select the checkbox next to each of the desired assets.

> Alternatively, you can select multiple assets by pressing the Shift key while clicking on each of the desired assets.

3. Click on the **Bulk Actions** menu and select **Edit** from the dropdown list.



The **Bulk Edit** screen is shown with the parameters that are available for bulk editing.

4. Select the checkbox next to each of the parameters that you would like to edit (*Type*, *Criticality*, *Purdue Level*, *Network Segments*, *Location* and *Description*).

> When bulk editing Network Segments, first filter your assets by Type, then select the assets you wish to bulk edit.
> Assets with multiple IP addresses can't be included in a bulk edit for Network Segments; you will need to edit each asset manually.

5. Set each of the parameters as desired.

> Information entered in the Bulk Editing fields overrides any current content for the selected asset. If you select the checkbox next to a parameter but do not enter a selection, then the current values for that parameter will be erased.

6. Click **Save**.
The assets are saved with the new configuration.

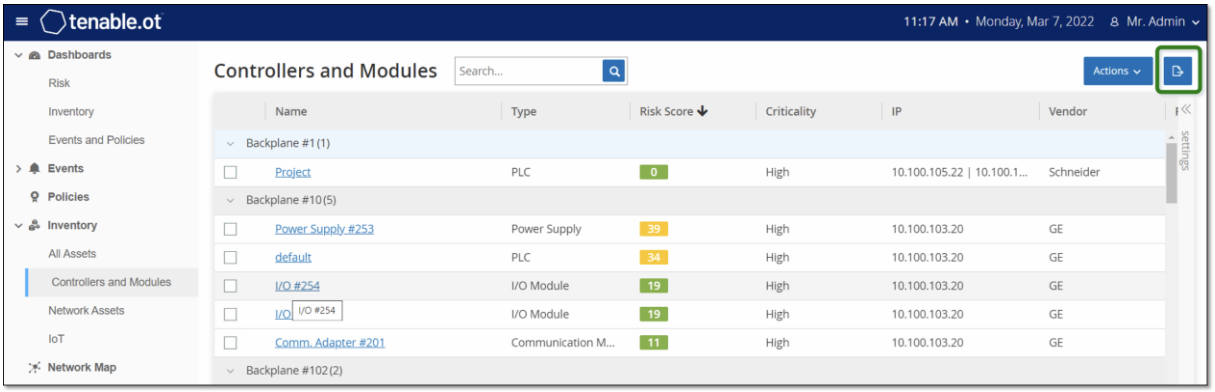
Editing Asset Details by Uploading a CSV

This method of editing asset details allows you to edit a large number of assets through a csv file instead of editing them manually in the UI. The following details can be edited using this method: *Type, Name, Criticality, Purdue Level, Location, Description* and custom fields.

➡ **To edit asset details through a CSV:**

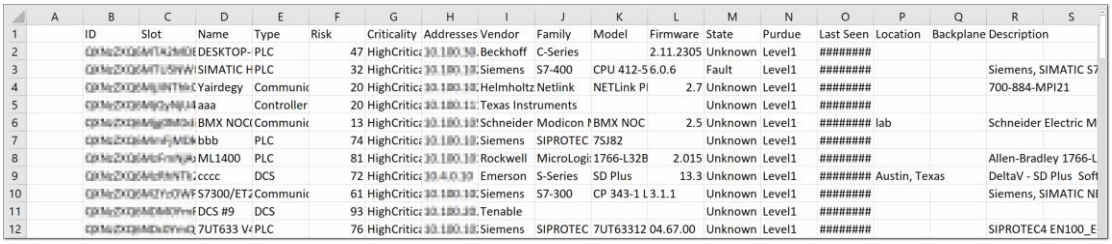
1. Under **Inventory**, click on **All Assets**, **Controllers** and **Modules**, or **Network Assets**.

2. Click the **Export** button.



A csv file of the inventory is downloaded.

3. Navigate to the file that was just downloaded and open it.



	ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description
2			DESKTOP-	PLC	47	HighCritic		Beckhoff	C-Series		2.11.2305	Unknown	Level1	########			
3			SIMATIC H	PLC	32	HighCritic		Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	########			Siemens, SIMATIC S7
4			Yairdegy	Communic	20	HighCritic		Helmholtz	Netlink	NETLink Pl	2.7	Unknown	Level1	########			700-884-MPI21
5			aaa	Controller	20	HighCritic		Texas Instruments				Unknown	Level1	########			
6			BMX NOC(	Communic	13	HighCritic		Schneider	Modicon I	BMX NOC	2.5	Unknown	Level1	########	lab		Schneider Electric M
7			bbb	PLC	74	HighCritic		Siemens	SIPROTEC	7SJ82		Unknown	Level1	########			
8			ML1400	PLC	81	HighCritic		Rockwell	MicroLogi	1766-L32B	2.015	Unknown	Level1	########			Allen-Bradley 1766-L
9			cccc	DCS	72	HighCritic		Emerson	S-Series	SD Plus	13.3	Unknown	Level1	########	Austin, Texas		DeltaV - SD Plus Soft
10			S7300/ET2	Communic	61	HighCritic		Siemens	S7-300	CP 343-1 L	3.1.1	Unknown	Level1	########			Siemens, SIMATIC NI
11			DCS #9	DCS	93	HighCritic		Tenable				Unknown	Level1	########			
12			7UT633 V4	PLC	76	HighCritic		Siemens	SIPROTEC	7UT63312	04.67.00	Unknown	Level1	########			SIPROTEC4 EN100_E

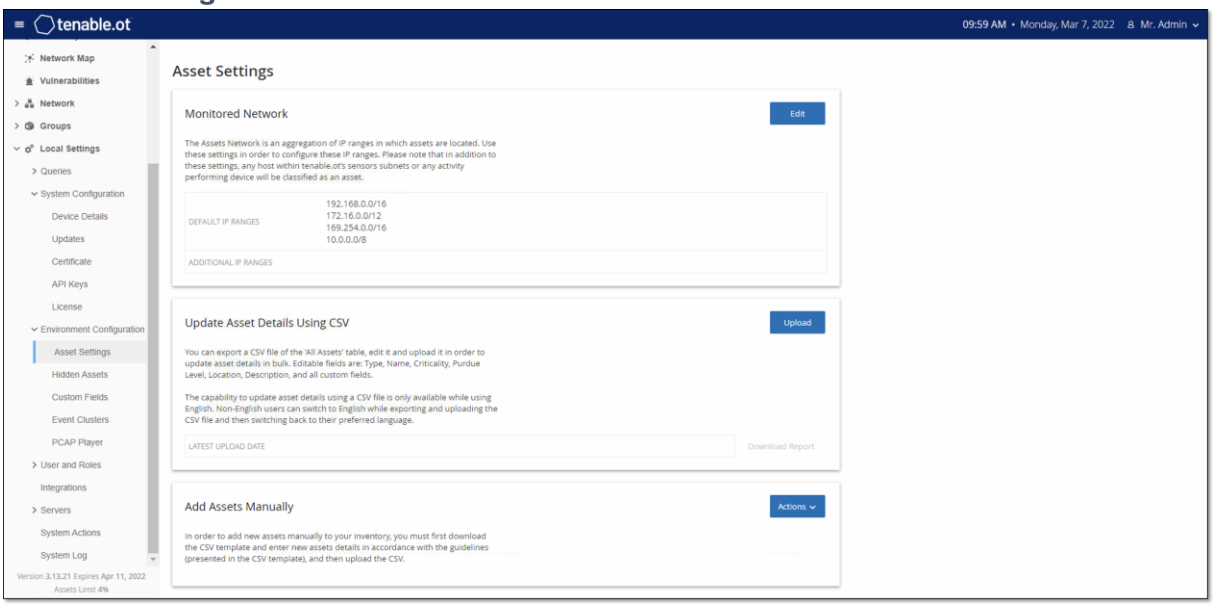
4. Edit the allowable parameters by changing the content of the cells. (Allowable parameters are: *Type, Name, Criticality, Purdue Level, Location, Description* and custom fields.)

You must enter valid data for parameters that require specific options (e.g. Type, Criticality, Purdue Level). Otherwise, the corresponding asset will fail to update.

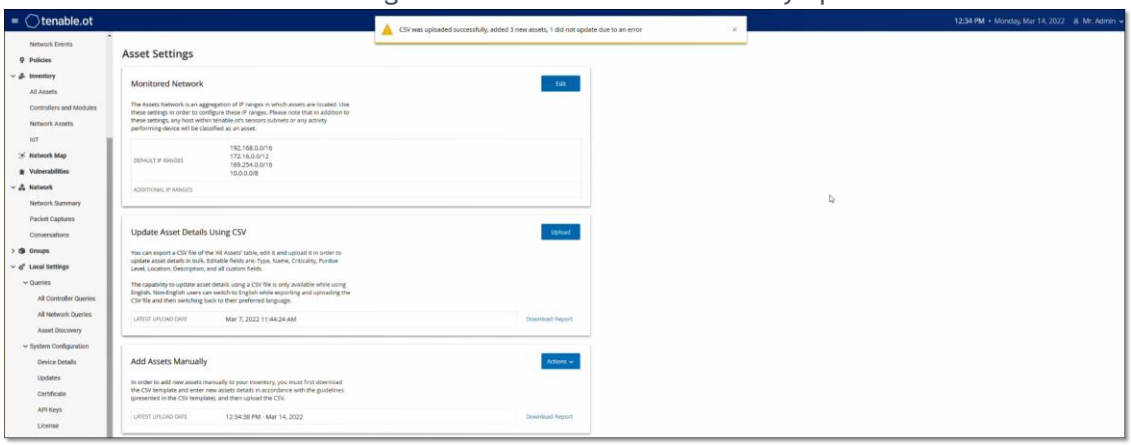
5. Save the file as a csv file type.

Only the assets that you modify will be updated in the system. Assets that are not included in the csv, or rows that you did not modify will remain unchanged in the system. It is not possible to delete assets using this method.

6. Under **Local Settings**, go to **Environment Configuration** > **Asset Settings**.
   The **Asset Settings** screen is shown.



7. In the **Update asset details using CSV** section, click **Upload**.
8. Follow your device's navigation prompts to upload the csv file that you just saved.
   A confirmation is shown indicating the number of rows successfully updated.



   The **Latest Upload Date** field in the Update asset details using CSV section is updated.
9. If you would like to see more info about the results of the upload, in the **Update asset details using CSV** section, click **Download Report**.
   A csv file is downloaded that details which Asset IDs were successfully updated and which ones failed.

Hiding Assets

You can hide one or more assets from the asset inventory. An asset that has been hidden isn't shown in the Inventory and it is removed from Groups. However, Events and network activity are still shown for the hidden asset.

An asset that was hidden can be restored from the Local Settings > Assets > Hidden Assets screen, see **LOCAL SETTINGS**.

➡ **To hide one or more assets:**

1. Under **Inventory**, click on **Controllers** or **Network Assets**.
2. Select the checkbox next to one or more assets that you would like to remove.
3. In the Header bar, click on the **Actions** button.
4. From the drop-down list, select **Hide Asset**.
   The **Hidden Assets** window opens.
5. In the **Comments** field, you can add free text comments about the asset/s. (Optional)

Comments are shown in the list of removed assets, on the Local Settings > Assets > Hidden Assets screen.

6. Click **Hide**.
   The asset/s are hidden from the Inventory and Groups.

Performing Nessus Scan

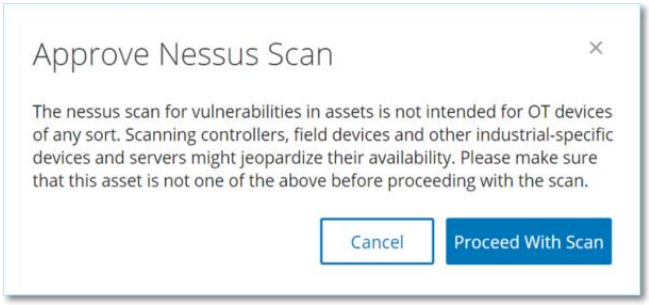
Nessus is a Tenable tool that scans IT devices to detect vulnerabilities. Tenable.ot enables you to run the Nessus "Basic Network Scan" on specific IT assets within your OT network. This is an active full system scan that gathers additional information about vulnerabilities on the servers and network devices. This scan will use the WMI and SNMP credentials if they were provided by the user. This action is only available for relevant PC based machines. The results of the scan are shown on the Vulnerabilities screen.

Nessus is an invasive tool which works best in IT environments. It is not recommended for use on OT devices, as it may interfere with their normal operation.

➡ **To manually run a Nessus Scan:**

1. Under **Inventory**, click on **Network Assets**.
2. Select the desired asset.
3. In the header bar, click on the **Actions** button.

4. From the drop-down list, select **Nessus Scan**.
   The **Approve Nessus Scan** confirmation window is displayed.



5. Click **Proceed with Scan**.
   The Nessus Scan is run.

Performing Resync

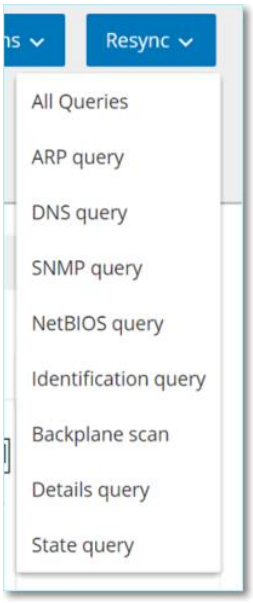
The Resync function initiates one or more Queries to the network and the controller in order to capture up-to-date information for this asset. You can run all available Queries or you can select specific Queries to run. The following, are the Queries available for "Resync":

- Backplane scan – Discovers modules and their specifications within a backplane.
- DNS scanning- Searches for the DNS names of the assets in the network.
- Details query – Retrieves the controller's hardware and firmware details. The result is displayed in the Firmware field, which is in the Assets > Controllers screen.
- Identification query – Uses multiple protocols to attempt to identify the asset.
- NetBIOS query - Sends a NetBIOS unicast packet which is used to classify and detect Windows machines in the network.
- SNMP query (for SNMP enabled assets) – Retrieves configuration details for SNMP-enabled assets.
- State – Detects the current status of the asset (i.e. Running, Stopped, Fault, No config. and Test).
- ARP - Retrieves the MAC address of new IPs detected in the network. The result is displayed in the MAC field, which is in the Details > Overview screen.

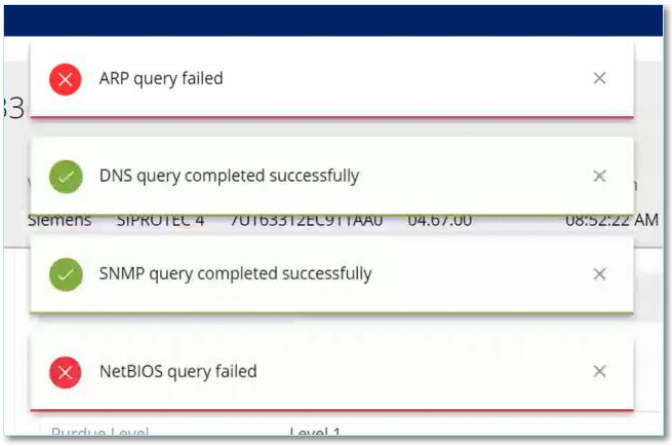
➡ **To run Resync asset data:**

1. On the **Asset Details** screen for the desired asset, click on the **Resync** button in the Header pane.

2. A dropdown list of queries is displayed.



3. Click on the query that you would like to run OR click on *All Queries* to run all available queries.
4. As each query runs, a pop-up notification shows the status of the query.



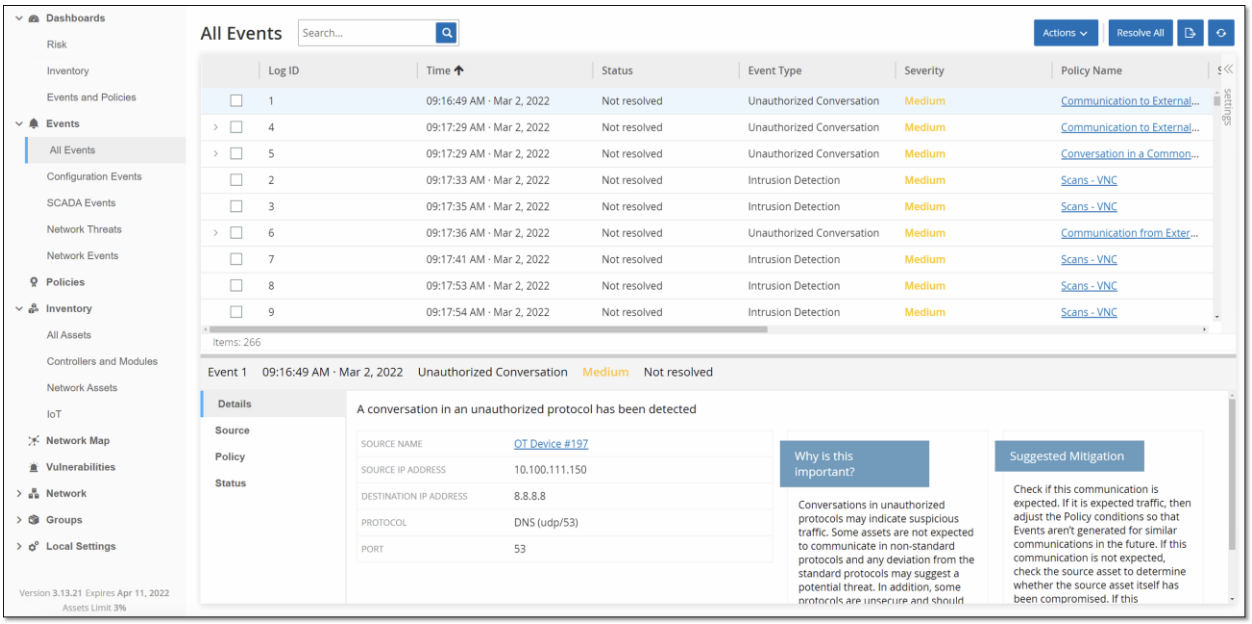
For each successfully run query, the system data for this asset is updated based on the new data.

Events

Events are notifications that have been generated in the system to call attention to potentially harmful activity in the network. Events are generated by Policies that are set up in the system in one of the following categories: *Configuration Events*, *SCADA Events*, *Network Threats* or *Network Events*. A Severity level is assigned to each Policy, indicating the severity of the Event.

Once a Policy has been activated, any event in the system that fits the Policy conditions will trigger an Event log. Multiple events with the same characteristics are clustered together into a single cluster.

Viewing Events



All Events that occurred in the system are shown on the **All Events** screen. Specific subsets of the Events are shown on separate screens for each of the following Event categories: **Configuration Events**, **SCADA Events**, **Network Threats** and **Network Events**.

The top of the screen shows a listing for each Event. For each of the Events screens (Configuration Events, SCADA Events, Network Threats and Network Events), you can customize the display settings by adjusting which columns are displayed and where each column is positioned. The events can be grouped according to different categories (e.g. Event type, Severity, Policy Name). You can also sort and filter the Event lists as well as searching for search text. For an explanation of the customization features, see **Working with Lists**.

There is an **Actions** button in the header bar, which enables you to take the following Action on the selected Event/s:

- Resolve – Mark this Event as Resolved.
- Download PCAP – Download the PCAP file for this Event.
- Exclude – Create a Policy Exclusion for this Event.

Detailed information about these actions is given in the following sections.

The bottom of the screen shows detailed information about the selected Event, divided into tabs. Only tabs relevant to the Event type of the selected Event are shown. The following tabs are shown for various types of Events: *Details*, *Code*, *Source*, *Destination*, *Policy*, *Ports Scanned* and *Status*.

You can drag the panel divider up or down to enlarge/reduce the bottom panel display.

You can download the packet capture file associated with each Event, see **Downloading Files**.

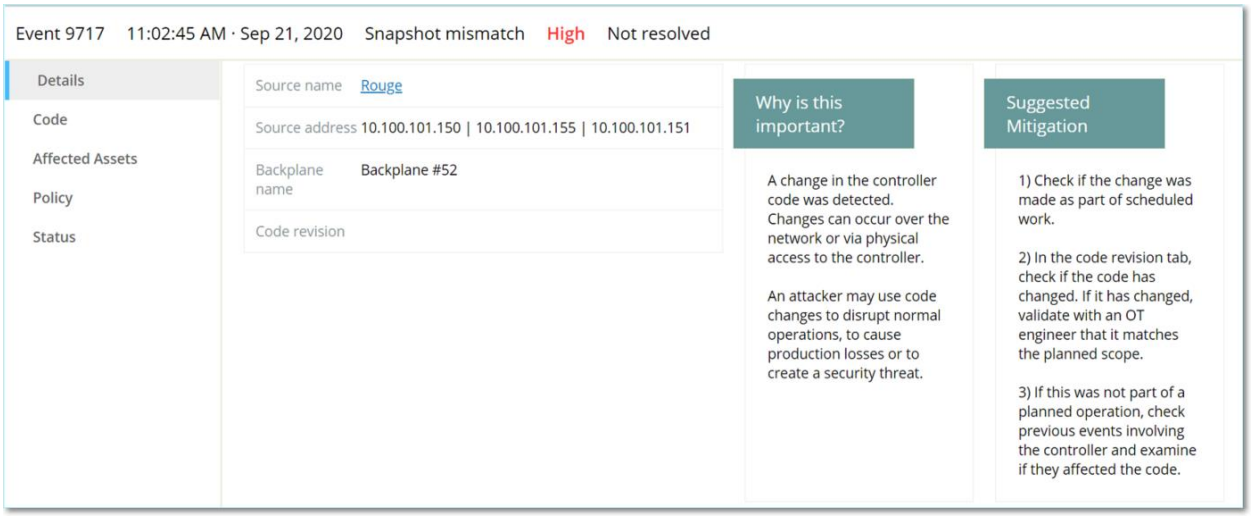
The information shown for each Event listing is described in the following table:

Parameter	Description
Name	The name of the device in the network. Click the name of the asset to view the Asset Details Screen for that asset, see **Viewing Asset Details**.
Addresses	The IP and/or MAC address of the asset. Note: An asset may have multiple IP addresses.
Type	The asset type. See **Asset Types** for an explanation of the various asset types.
Backplane	The backplane unit that the controller is connected to. Additional details about the backplane configuration are shown in the Asset Details screen.
Slot	For controllers that are on backplanes, shows the number of the slot to which the controller is attached.
Vendor	The asset vendor.
Family	The family name of the product as defined by the controller vendor.
Firmware	The firmware version currently installed on the controller.
Location	The location of the asset, as input by the user in the Tenable.ot asset details. See **Editing Asset Details**.
Last Seen	The time at which the device was last seen by Tenable.ot. This is the last time that the device was connected to the network or performed an activity.
OS	The OS running on the asset.
Log ID	The ID generated by the system to refer to the Event.
Time	The date and time that the Event occurred.
Event Type	Describes the type of activity that triggered the Event. Events are generated by Policies that are set up in the system. For an explanation of the various types of Policies, see **Policy Types**.

Severity	Shows the severity level of the Event. The following is explanation of the possible values: None - No reason for concern. Info - No immediate reason for concern. Should be checked out when convenient. Warning - Moderate concern that potentially harmful activity has occurred. Should be dealt with when convenient. Critical - Severe concern that potentially harmful activity has occurred. Should be dealt with immediately.
Policy Name	The name of the Policy that generated the Event. The name is a link to the Policy listing.
Source Asset	The name of the asset that initiated the Event. This field is a link to the Asset listing.
Source Address	The IP or MAC of the asset that initiated the Event.
Destination Asset	The name of the asset that was affected by the Event. This field is a link to the Asset listing.
Destination Address	The IP or MAC of the asset that was affected by the Event.
Protocol	When relevant, this shows the protocol used for the conversation that generated this Event.
Event Category	Shows the general category of the Event. Note: On the All Events screen, Events of all types are shown. Each of the specific Event screens shows only Events of the specified category. The following is a brief explanation of the Event categories (for a more detailed explanation see **Policy Categories**): • Configuration Events – this includes two sub-categories • Controller Validation Events – These policies detect changes that take place in the controllers in the network. • Controller Activity Events – Activity Policies relate to the Activities that occur in the network (i.e., the "commands" implemented between assets in the network). • SCADA Events – policies that identify changes made to the data plane of controllers. • Network Threats Events – these Policies identify network traffic that is indicative of intrusion threats. • Network Events – Policies that relate to the assets in the network and the communication streams between assets.
Status	Shows whether or not the Event has been marked as resolved.
Resolved By	For resolved Events, shows which user marked the Event as resolved.

Resolved On	For resolved Events, shows when the Event was marked as resolved.
Comment	Shows any comments that were added when the Event was resolved.

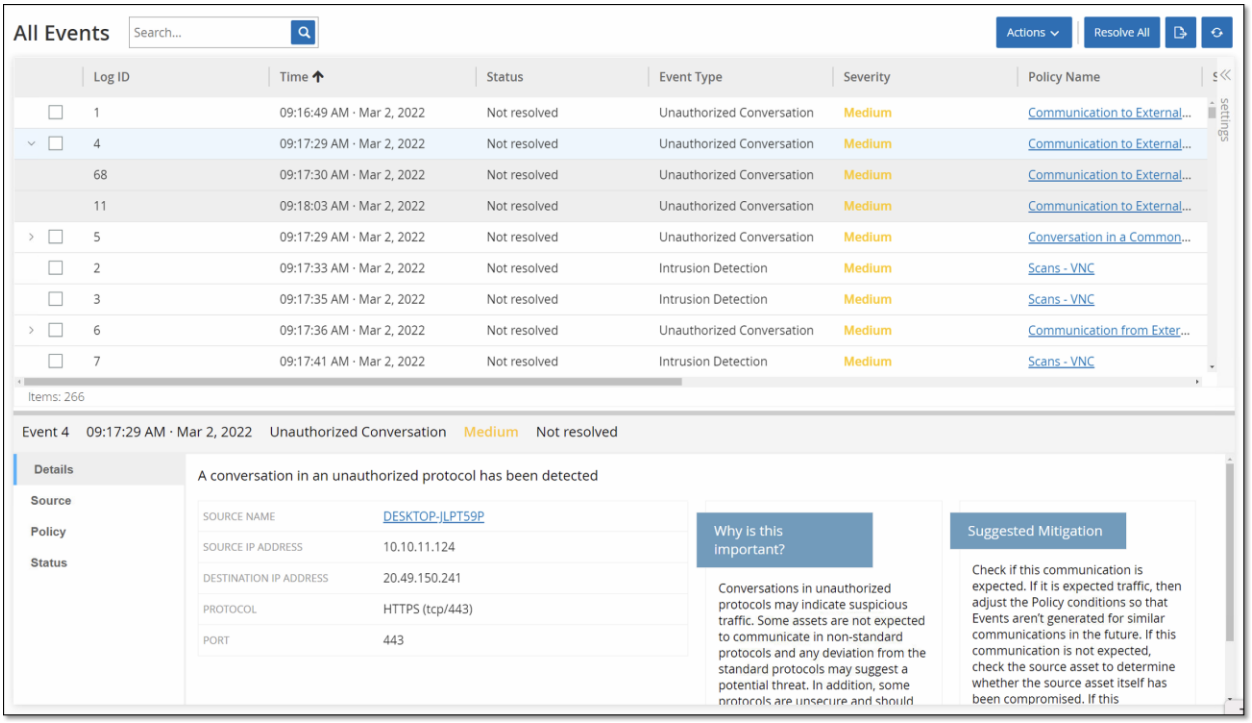
Viewing Event Details



The bottom of the Events screen shows additional details about the selected Event. The information is divided into tabs. Only tabs that are relevant for the selected Event are displayed. The detailed information includes links to additional information about the relevant entities (Source Asset, Destination Asset, Policy, Group, etc.)

- Header – shows an overview of essential info about the Event.
- Details – gives a brief description of the Event as well as an explanation of why this information is important and suggested steps that should be taken to mitigate the potential harm caused by the Event. In addition, it shows the source and destination assets that were involved in the Event.
- Rule Details (for Intrusion Detection Events) – shows information about the Suricata rule that applies to the Event.
- Code - This tab is shown for Controller activities such as code download and upload, HW configuration, and code deletion. It shows detailed information about the relevant code, including specific code blocks, rungs and tags. The code elements are displayed in a tree structure with arrows for expanding/minimizing the details shown.
- Source – shows detailed information about the Source Asset for this Event.
- Destination – shows detailed information about the Destination Asset for this Event.
- Affected Asset – shows detailed information about the Asset Affected by this Event.
- Scanned Ports (for Port Scan Events) – shows the ports that were scanned.
- Scanned Address (for ARP Scan Events) – shows the addresses that were scanned.
- Policy – shows detailed information about the Policy that triggered the Event.
- Status – shows whether or not the Event has been marked as resolved. For resolved Events, shows details about which user marked it as resolved and when it was resolved.

Viewing Event Clusters



To facilitate the monitoring of events, multiple events with the same characteristics are clustered together into a single cluster. The clustering is based on event type (i.e. share the same Policy), source and destination assets, and the time range in which the Events occur. For information on configuring Event Clusters, see **Event Clusters**.

Clustered Events are denoted with an arrow next to the Log ID. To view the individual Events in a Cluster, click on the record to expand the list.

Resolving Events

Once an authorized technician has assessed an Event and taken the necessary actions to address the problem or determined that there is no need to take action, then the Event should be marked as *Resolved*. When one event that is part of a cluster is resolved, all events in that cluster are marked as resolved. It is possible to select several Events to be marked as Resolved in a batch process. It is also possible to mark all Events (or all Events of a particular category) as Resolved at once.

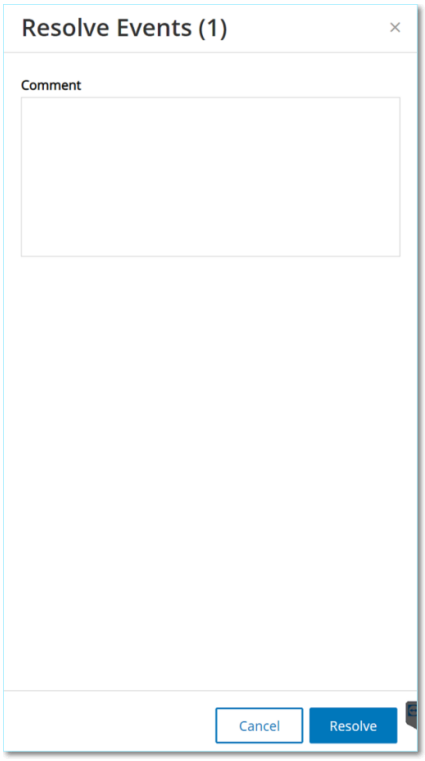
Resolving Individual Events

➡ **To mark specific Events as resolved:**

1. In the relevant **Events** screen (Configuration Events, SCADA Events, Network Threats or Network Events), select the checkbox next to one or more Events that you would like to mark as Resolved.
2. Click on the **Actions** button in the Header bar.

Even when you are marking multiple Events as Resolved, you must click on the *Resolve* button to resolve all Events based on the current user filter, and **not** on the *Resolve All* button. The *Resolve All* button is used to mark all Events, even those that are not selected, as Resolved.

3. In the dropdown menu, select **Resolve**.
   The **Resolve Event** window is displayed.



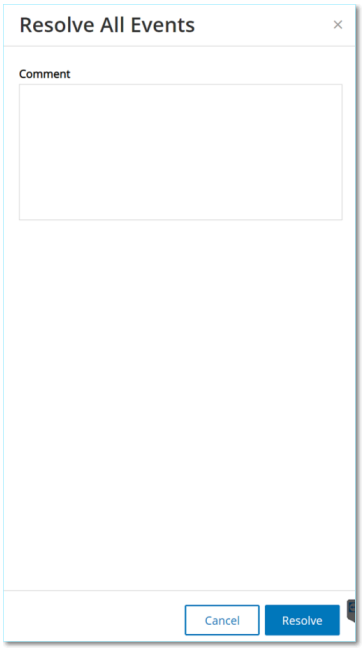
4. In the **Comment** field, you can add a comment describing the mitigation steps taken to resolve the issue/s. (Optional field)
5. Click **Resolve**.
   The status of the selected Event/s is marked as *Resolved*.

Resolving All Events

The *Resolve All* action applies to all Events on the current screen, i.e. if the Configuration Events screen is open, then *Resolve All* resolves all Configuration Events but not SCADA Events etc.

➡ **To mark all Events as resolved:**

1. In the relevant **Events** screen (Configuration Events, SCADA Events, Network Threats or Network Events), in the Header Bar, click on **Resolve All**.
2. The **Resolve All Events** window is displayed.



3. In the **Comment** field, you can add a comment about the group of Events being resolved. (Optional field)
4. Click **Resolve**.
5. The status of all Events is marked as *Resolved*.

Creating Policy Exclusions

If you find that a Policy is generating Events for specific conditions which don't pose a security threat, you can *Exclude* those conditions from the Policy (i.e. stop generating Events for those particular conditions). For example, if you have a Policy that detects changes in Controller State that occur during Workday hours, but you determine that for a particular controller it is normal for the State to change during those times, you can *Exclude* that controller from the Policy.

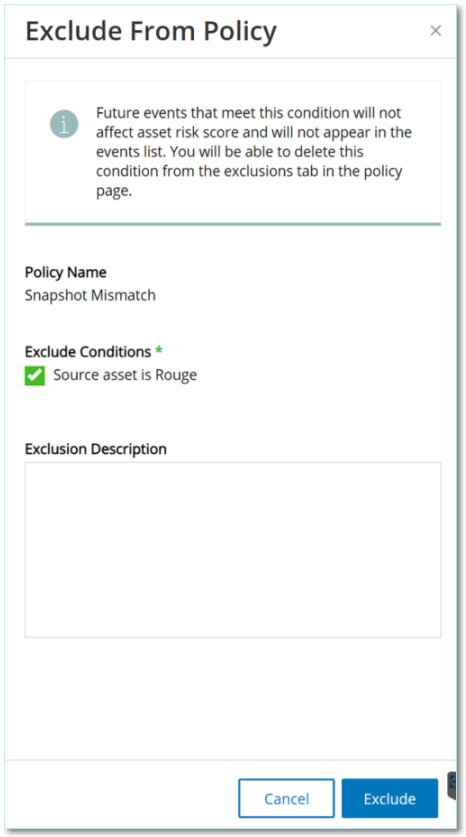
Exclusions are created from the Events screen, based on Events that were generated by your Policies. You can specify which conditions of a particular Event you would like to exclude from the Policy.

If you would like to resume generating Events for the specified conditions at a later time, you can delete the Exclusion, see **Deleting Policy Exclusions**.

➡ **To create a Policy Exclusion:**

1. In the relevant **Events** screen (Configuration Events, SCADA Events, Network Threats or Network Events), select the Event for which you would like to create an Exclusion.
2. Click on the **Actions** button in the Header bar (or right-click on the Event).
   The **Actions** menu is displayed.
3. Click on **Exclude from Policy**.
   The **Exclude from Policy** window opens.
4. In the **Exclude Condition** section, by default all conditions are selected (causing Events with *any* of the specified conditions to be excluded from the Policy). You can **deselect** the checkbox next to each condition for which you would like to continue generating Events.

For example, in the dialog shown below, if you would like to exclude the specified source and destination assets and IPs from this Policy, but you would like to continue applying this Policy to UDP conversations between other assets in the network, then you should deselect "Protocol is UDP".



The set of conditions that can be excluded differ depending on the type of Policy, see table below.

5. In the **Exclusion Description** field, you can add a comment about the Exclusion (optional).
6. Click on **Exclude**.
   The Exclusion is created.

The following table shows the conditions that can be excluded for each type of Event.

Policy Category	Event Type	Excludable Conditions
Controller Activities	Configuration Events (i.e. Activities)	• Source asset • Source IP • Destination asset • Destination IP
Controller Validation	Change in Key State	• Source asset
	Change in Controller State	• Source asset
	Change in FW Version	• Source asset
	Module Not Seen	• Source asset
	Snapshot Mismatch	• Source asset
Network	Asset Not Seen	• Source asset
	Change in USB Configuration	• Source asset • USB Device ID
	IP Conflict	• MAC Addresses • IP Address
	Network Baseline Deviation	• Source asset • Source IP • Destination asset • Destination IP • Protocol
	Open Port	• Source asset • Source IP • Port
	RDP Connection	• Source asset • Source IP • Destination asset

		• Destination IP
	Unauthorized Conversation	• Source asset • Source IP • Destination asset • Destination IP • Protocol
	FTP Log In (Failed and Successful)	• Source asset • Source IP • Destination asset • Destination IP
	Telnet Log In (Attempt, Failed and Successful)	• Source asset • Source IP • Destination asset • Destination IP
Network Threat	Intrusion Detection	• Source asset • Source IP • Destination asset • Destination IP • SID
	ARP Scan	• Source asset • Source IP
	Port Scan	• Source asset • Source IP
SCADA	Modbus Illegal Data Address	• Source asset • Source IP • Destination asset • Destination IP
	Modbus Illegal Data Value	• Source asset • Source IP • Destination asset • Destination IP
	Modbus Illegal Function	• Source asset • Source IP

		• Destination asset • Destination IP
	Unauthorized Write	• Source asset • Destination asset • Tag Name
	IEC60870-5-104 StartDT IEC60870-5-104 StopDT	• Source asset • Source IP • Destination asset • Destination IP
	IEC60870-5-104 function code based events	• Source asset • Source IP • Destination asset • Destination IP • COT
	DNP3 events	• Source asset • Source IP • Destination asset • Destination IP • Source DNP3 address • Destination DNP3 address

Downloading Individual Capture Files

Tenable.ot stores the packet capture data associated with each Event in the network. The data is stored as PCAP files which can be downloaded and analyzed using Network Protocol Analysis tools (e.g. Wireshark etc.). This section explains how to download the PCAP file associated with an individual Event. You can also download PCAP files for the entire network, see **PACKET CAPTURES**.

PCAP files are only available if the Packet Capture feature is activated. The Packet Capture feature can be activated from the Local Settings > System Configuration > Packet Captures screen, see **PACKET CAPTURES**.

PCAP files are only available for Events that relate to network activity, such as, Controller Activities, Network Threats, SCADA Events and some types of Network Events.

Downloading a PCAP File

➡ **To download a PCAP file:**

1. In the **Events** screen, select the checkbox next to the event for which you would like to download the PCAP file.
2. Click on the **Actions** button in the Header bar.
3. In the dropdown menu, select **Download Capture File**.
   The zipped PCAP file is downloaded to your local machine.

Creating FortiGate Policies

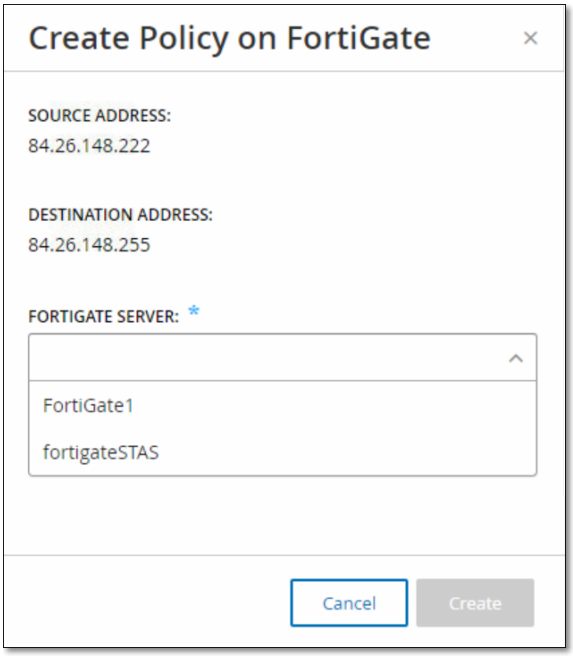
The FortiGate integration allows you to use certain Tenable.ot Events to create firewall policies/rules in the FortiGate Next Generation Firewall. The Event types that allow this capability (supported events) are *Baseline Deviation*, *Unauthorized Conversation*, *Intrusion Detection*, and *RDP Connection (authenticated and not authenticated)*. The FortiGate policy will automatically be set to apply to the source and destination Assets that were involved in the Tenable.ot Event. By default, the policy will cause FortiGate to deny (i.e. block) traffic of the specified type. A FortiGate administrator can adjust the policy settings in the FortiGate application.

Before being able to suggest FortiGate policies, you need to set up the integration for your FortiGate Firewall server with Tenable.ot. See **FORTIGATE FIREWALL**.

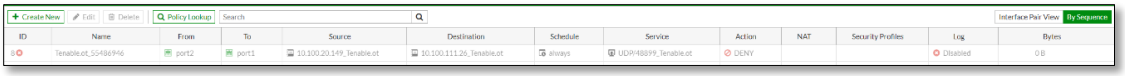
➡ **To Suggest a FortiGate Policy:**

1. In the relevant **Events** screen (*Configuration Events*, *SCADA Events*, *Network Threats* or *Network Events*), select the Event for which you would like to create a FortiGate policy.
2. Click on the **Actions** button in the Header bar (or right-click on the Event).
3. In the dropdown menu, select **Create FortiGate Policy**.
   The **Create Policy** on FortiGate panel opens, with the **Source Address** and **Destination Address** of the assets involved in the Tenable.ot Event already filled in.

4. In the **FortiGate Server** field dropdown menu, select the desired server.



5. Click **Create**.
   The policy is created in FortiGate and the panel closes.
6. You can view the new policy in the FortiGate application.



7. A FortiGate administrator can adjust the settings as desired.

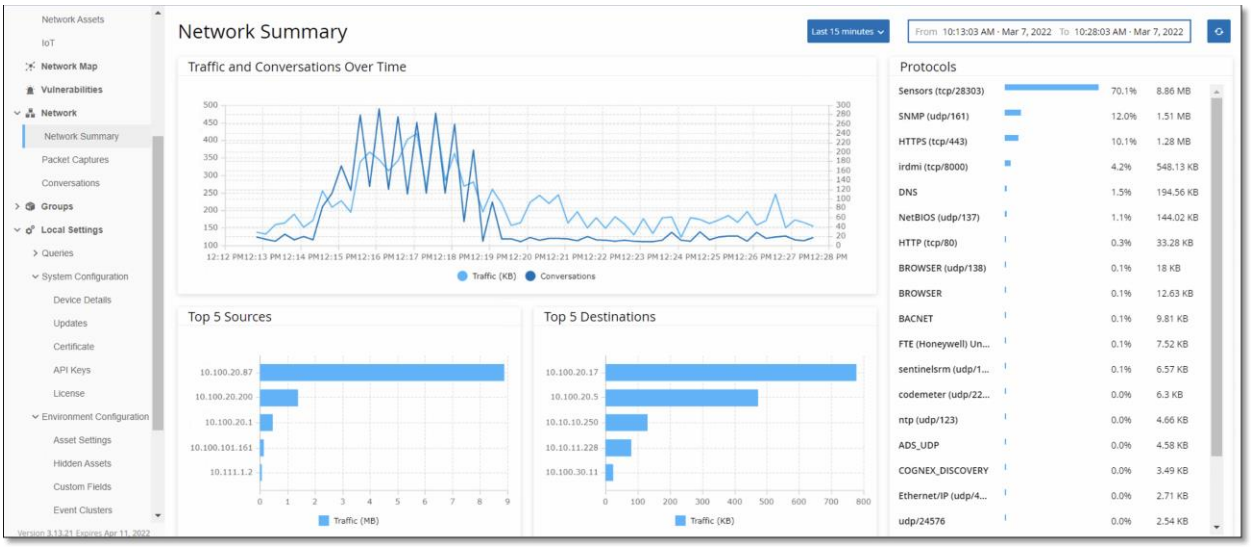
Network

Tenable.ot monitors all activity in you network. This information is displayed in the **Network** section of the UI.

The Network data is shown on three screens.

- **NETWORK SUMMARY** – shows an overview of the network activity.
- **PACKET CAPTURES** - shows a listing of the PCAP files captured by the system.
- **CONVERSATIONS** - shows a list of all conversations detected in the network, with details about the time that it occurred, involved assets etc.

Network Summary



The **Network Summary** screen shows visual graphs that summarize the network activity. You can set the time frame for which the data is displayed. You can also interact with the widgets to show additional details.

The screen includes four widgets:

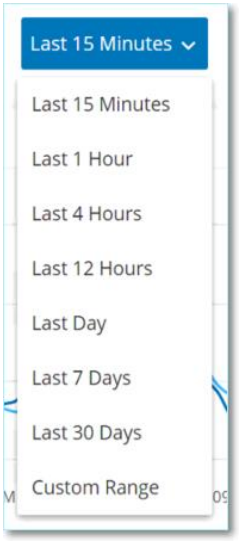
- **Traffic and Conversations over Time** – a graph displaying the amount of traffic in GB/MB and the number of conversations taking place in the network.
- **Top 5 sources** – a column bar graph displaying the five source assets that initiated the most network activity. For each source, the graph displays bars representing the amount of traffic. When you hover the cursor over the graph, the number of conversations is shown in a tooltip.
- **Top 5 destinations** - a column bar graph displaying the five destination assets that received the most network activity. For each destination, the graph displays bars representing the amount of incoming traffic. When you hover the cursor over the graph, the number of conversations is shown in a tooltip.
- **Protocols** – a bar graph displaying the communication protocols used in the network, ordered by frequency. For each protocol, the graph displays the rate at which it was used (as a percentage of the total traffic) and the volume of traffic.

Setting the Time Frame

All data displayed on the Network screen represents activity in the network during a specified time frame. The range of time for which data is currently displayed is shown in the header bar. The default time frame is set for the *Last 15 minutes*. The *Start* and *End* times of the selected time frame are displayed in the header bar.

➡ **To Set the Time Frame:**

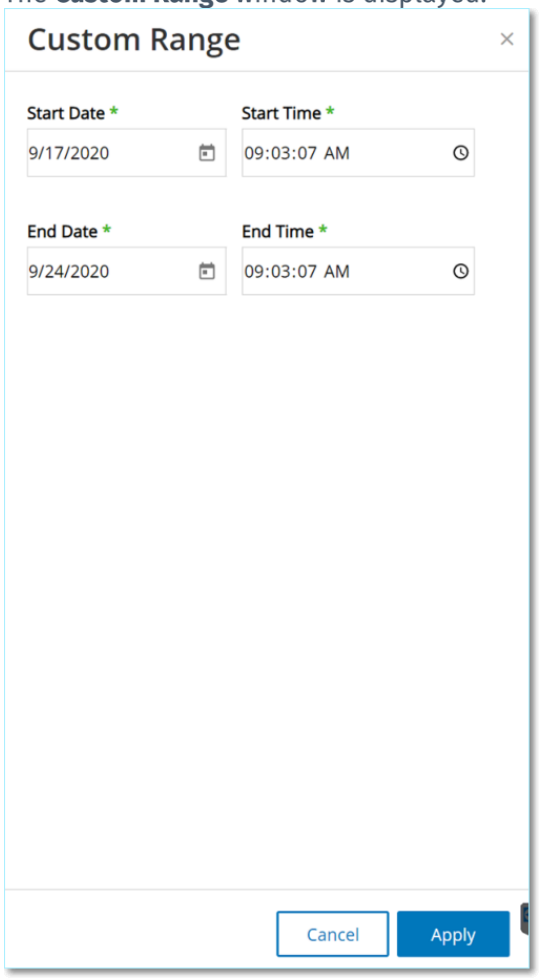
1. Click on **Time Frame Selection** in the header bar (default Last 15 Minutes).
   A dropdown menu with time frame options is displayed.



2. Select a time range using one of the following methods
   - Select a preset time range by clicking on the desired range (options are: Last 15 Minutes, Last 1 Hour, Last 4 Hours, Last 12 Hours, Last Day, Last 7 Days or Last 30 Days), OR

- Set a custom time range using the following procedure:

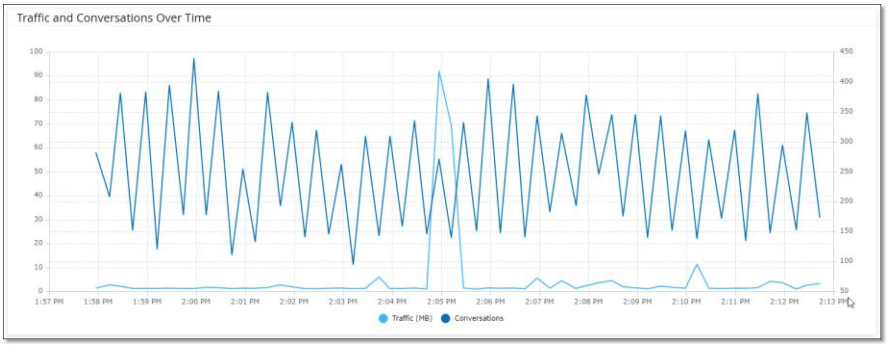
  a. Click **Custom Range**.
  The **Custom Range** window is displayed.



  b. Enter the **Start Date** and **Start Time** and the **End Date** and **End Time** in the appropriate fields.

  c. Click **Apply**.
  The time frame is set. The start date and time and end date and time are shown in the header bar next to the time frame selection. The screen is refreshed to show only data for the selected time frame.

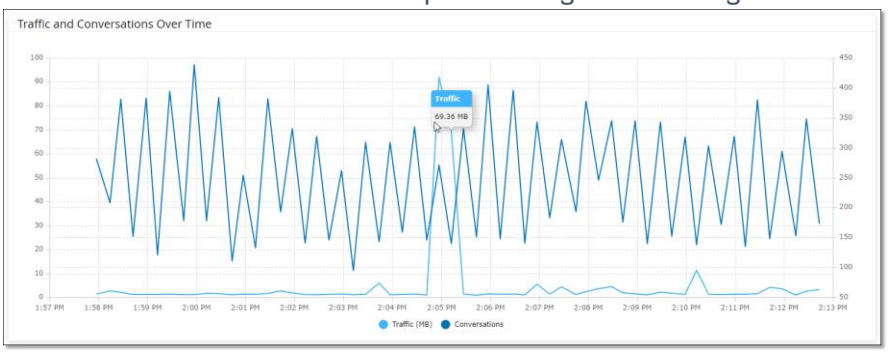
Traffic and Conversations over Time



A line graph displays the amount of traffic (measured in KB/MB/GB) and the number of conversations that took place in the network over time. The display key is shown on the top of the graph.

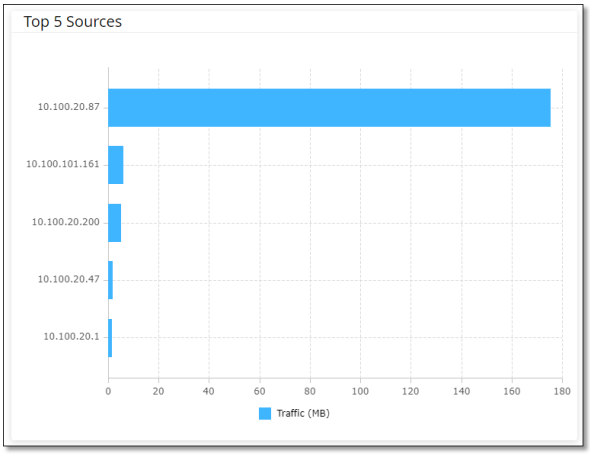
To Display Data for a specific time segment:

1. Hover over a point on the graph to display a pop-out window with specific data about the traffic and conversations that took place during that time segment.



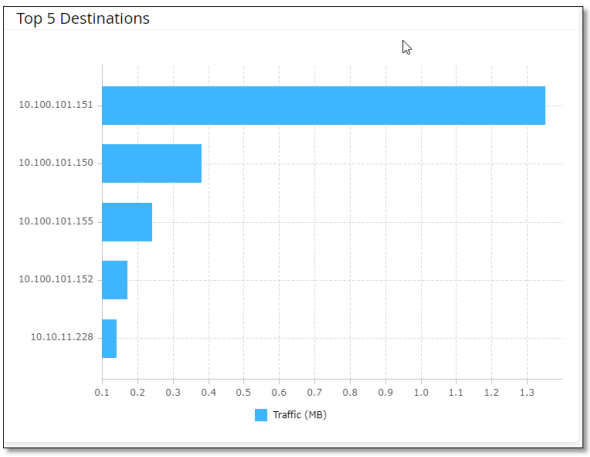
The length of the time segment shown is adjusted according to the time scale being displayed (e.g. for a 15-minute time frame data is shown for each minute separately but for a 30-day time frame it is shown for 6 hr. segments).

Top 5 Sources



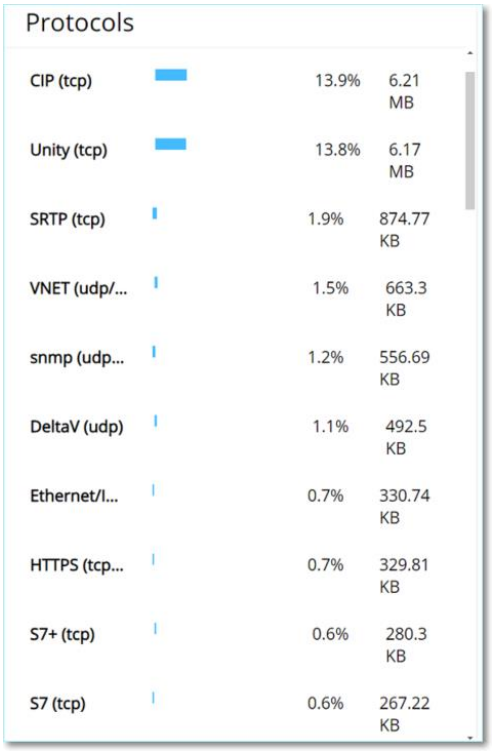
The **Top 5 Sources** pane shows the number of conversations and amount of traffic for each of the top 5 assets that sent communications through the network during the specified time frame. The source assets are identified by their IP addresses. Hovering over a bar graph shows the number of conversations and amount of traffic sent from that asset.

Top 5 Destinations



The **Top 5 Destinations** pane shows the number of conversations and amount of traffic for each of the top 5 assets that received communications through the network during the specified time frame. The destination assets are identified by their IP addresses. Hovering over a bar graph shows the number of conversations and amount of traffic received by that asset.

Protocols



The Protocols pane shows data about the usage of various protocols for communication within the network during the specified time frame. The protocols are listed from most used (on top) to least used (at the bottom). For each protocol the following information is displayed:

- A bar graph showing the rate of usage (with a full bar indicating the top usage and partial bars indicating the extent of usage relative to the top used protocol)
- The percentage of usage
- Total volume of communication

Packet Captures

The system stores files containing full network packet captures of activities in the network. The data is stored as PCAP files which can be analyzed using Network Protocol Analysis tools (e.g. Wireshark etc.). This enables in-depth forensic analysis of critical events. When the storage capacity of the system (1.8 TB) is exceeded, the system deletes older files.

The Packet Captures screen displays all of the Packet Capture files in the system. The *Completed tab* shows lists for each completed file that is available for download. The *Ongoing tab* shows details about the packet capture that is currently underway in the system.

The *Header bar* shows the oldest captured file that is still available in the system. It also contains a button for downloading files and for manually closing the current Packet Capture.

In the file lists table, you can show/hide columns and sort and filter the lists as well as searching for keywords. For an explanation of the customization features, see **Working with Lists**.

You can also download the PCAP file for an individual Event from the Events screen, see **DOWNLOADING FILES**.

Packet Capture Parameters

The following table describes the parameters shown for the Packet Capture lists.

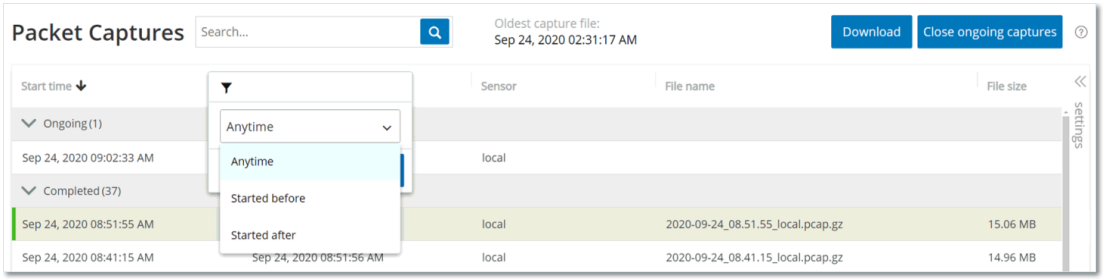
Parameter	Description
Start Time	The date and time that the Packet Capture began.
End Time	The date and time that the Packet Capture ended
Status	The status of the capture. Possible values: *Completed* or *Ongoing*.
Sensor	The Tenable.ot Sensor that captured the packet. For packets captured directly by the Tenable.ot appliance, the value is given as *local*.
File Name	The name of the file.
File Size	The size of the file, given in KB/MB.

Filtering Packet Capture Display

The Packet Captures display can be filtered to find a specific PCAP by entering the parameters for the start time and/or the end time.

To filter Packet Captures:

1. Under **Network**, select **Packet Captures**.
2. To filter by the start time, hover over **Start time** and click on the menu icon that appears. A drop-down menu opens.



   Set the filter as follows:
   a. Select from the drop-down list the filtering option. Options are: *Anytime* (default), *Started before* or *Started after*.
   b. If **Started before** or **Started after** were selected, a window opens with **Date** and **Time** fields, allowing you to choose the desired date and time.
   c. Click **Apply**.
3. To filter by end time, click on the **Filter** icon next to **End time**. A drop-down menu opens. Set the filter as follows:

a. Select from the drop-down list the filtering option. Options are: *Anytime* (default), *Started before* or *Started after*.

b. If **Started before** or **Started after** were selected, a window opens with **Date** and **Time** fields, allowing you to choose the desired date and time.

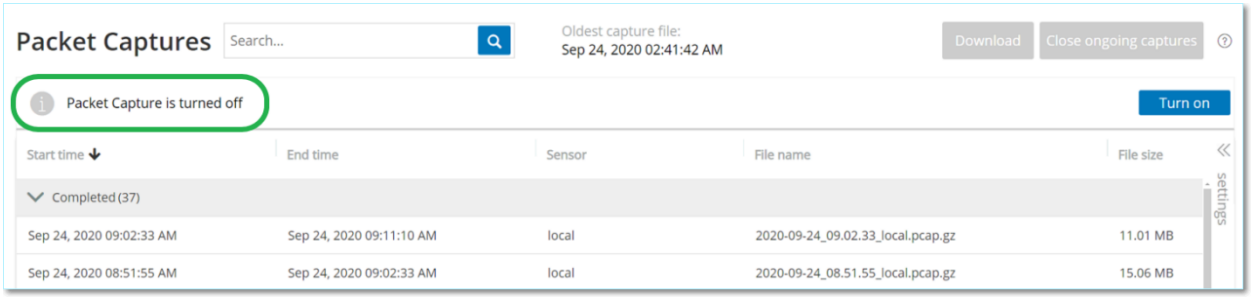
c. Click **Apply**.

The filter is applied, and only the files generated within the selected time frame are displayed.

Activating/Deactivating Packet Captures

Packet Capture can be activated/deactivated on the Local Settings > Device Details screen, see **PACKET CAPTURES**.

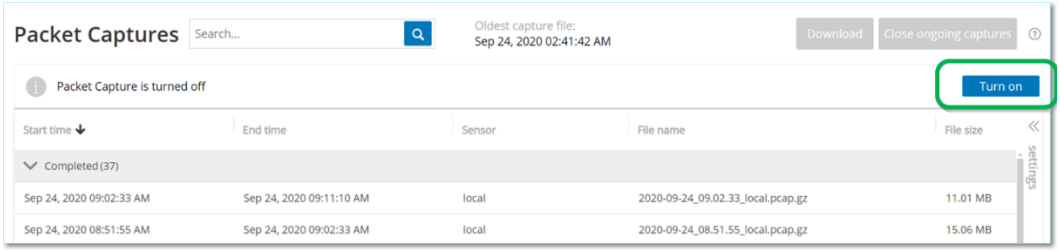
If the Packet Capture feature is turned off, then the Packet Captures screen shows a message informing you that it is turned off.



You can activate (but not deactivate) Packet Capture from the Network > Packet Capture screen.

➡ **To activate Packet Capture from the Packet Capture screen:**

1. Under **Network**, select **Packet Captures**.
2. In the **Header** bar, click **Turn on**.



The system begins Packet Capture.

Downloading Files

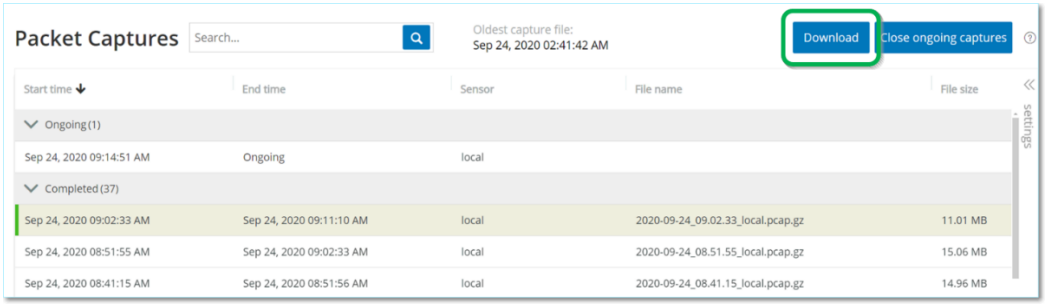
You can download any of the *Completed* PCAP files to your local machine. The PCAP files can then be analyzed using Network Protocol Analysis tools (e.g. Wireshark etc.).

File captures that are still ongoing are not yet available for download. You can manually close an ongoing capture in order to close the current file and begin capturing info for a new file.

➡ **To download a completed file:**

1. Under **Network**, select **Packet Captures**.

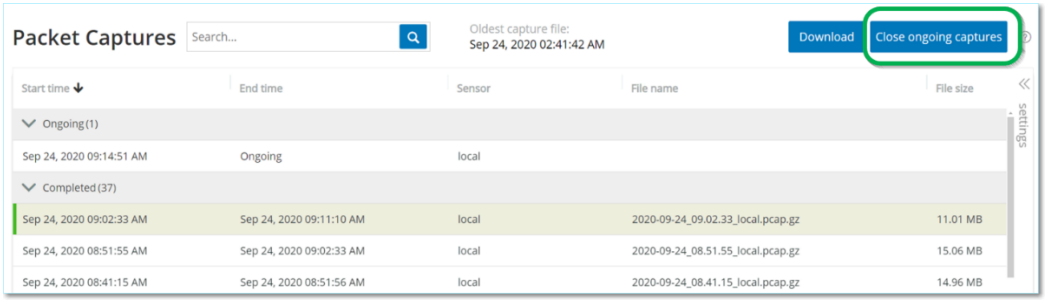
2. Select the desired file from the Packet Capture lists.
3. In the **Header** bar, click **Download**.



The zipped PCAP file is downloaded to your local machine.

➡ **To manually close the current Packet Capture:**

1. Under **Network**, select **Packet Captures**.
2. In the **Header** bar, click **Close ongoing capture**.



The current capture is stopped, and the file becomes available for download. A new Packet Capture is automatically started.

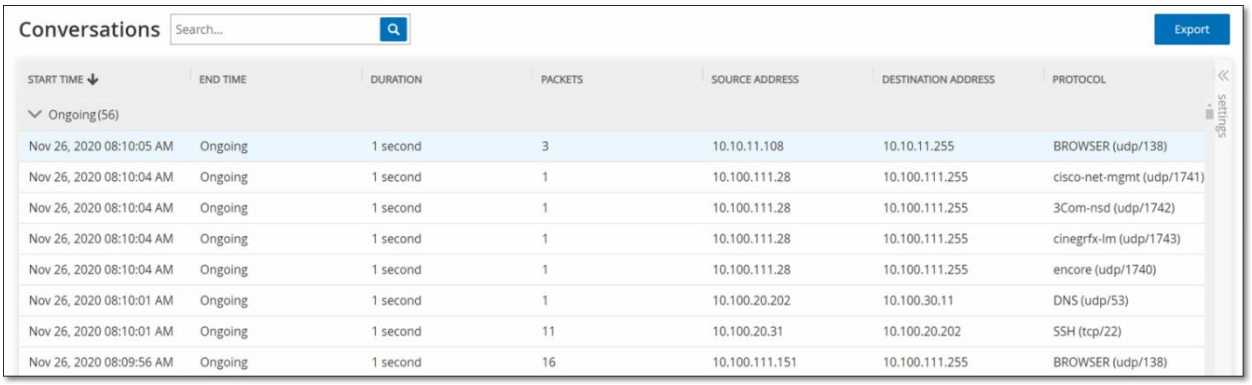
Conversations

Conversations are network communications between two assets – a source and a destination. For example, an interaction between an engineering workstation and a PLC, or between two servers. The Conversations screen displays a list of the current and past conversations, including the detailed information about the conversations.

The Conversations screen has the following additional functionalities:

- Search - search for specific conversations by entering identifying information into the Search box.
- Export – export all data from the Conversations tab onto your local machine as a .csv file by clinking Export.

	The Conversation table shows the last 10,000 network conversations.

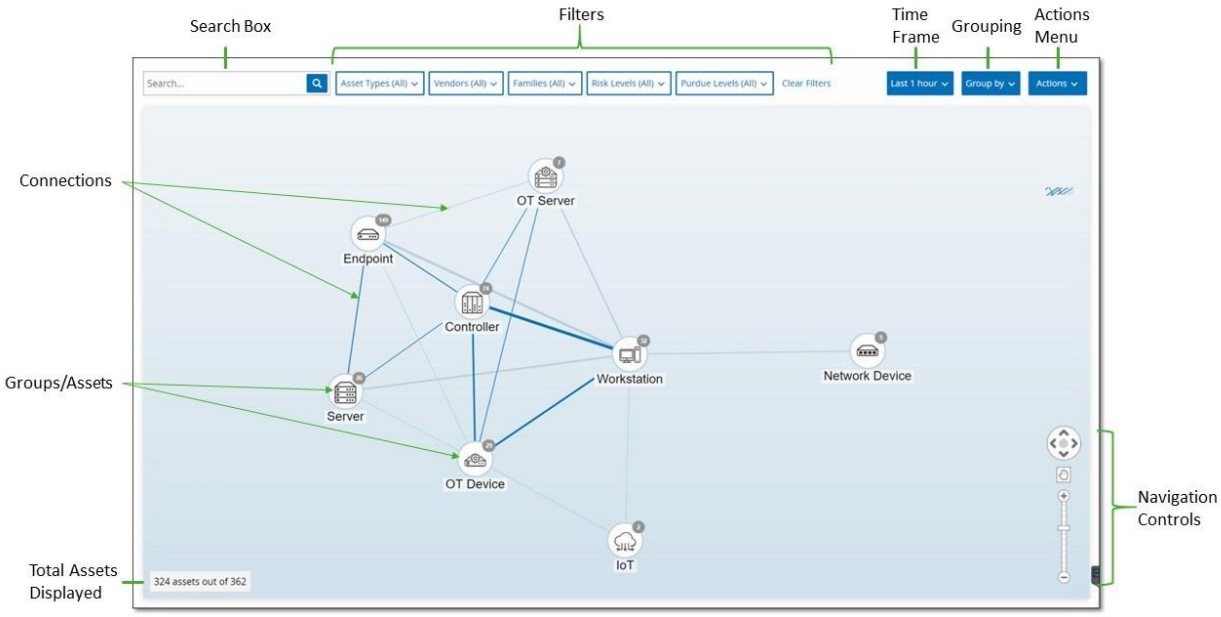


The information shown in the Conversations tab is described in the table below:

Parameter	Description
Start Time	The time that the conversation began.
End Time	The time that the conversation ended. Shows *Ongoing* for conversations that are still in progress.
Duration	The amount of time that the conversation was in progress.
Packets	The number of data packets sent.
Source Address	The IP of the asset that sent the data.
Destination Address	The IP of the asset that received the data.
Protocol	The protocol that was used for the communication.

Network Map

The **Network Map** screen offers a visual representation of the network assets and their connections over time, as discovered by Tenable.ot's Network Detection capabilities. Network Detection provides in-depth, real-time visibility into all activities performed over the operational network, with unique focus on control-plane engineering activities. For example, firmware downloads/uploads, code updates and configuration changes, performed over proprietary, vendor specific protocols. The assets can be shown by groups of related assets or as individual assets.



The Network Map displays all of the assets and connections that were discovered during the specified time frame.

The following is an explanation of the elements shown on the Network Map screen.

- **Search Box** - Enter search text to search for assets in the display. The search results are indicated by highlighting all groups in which a match was found for the search text. You can drill down into each group to see the relevant assets.
- **Filters** – You can filter the map display by one or more of the specified categories: *Asset Type*, *Vendors*, *Families*, *Risk Levels*, *Purdue Levels*. For an explanation of asset types, see **Asset Types**.
- **Time Frame** - The Network Map shows assets and network connections that were detected during the specified time frame. The default time frame is set for *Last 1 month*. Click the **Time Frame Selection** to select a different time frame from the dropdown menu.
- **Grouping** – You can specify the category by which the assets are grouped in the display. Options are: *Asset type*, *Purdue level*, *Risk level*, or *No grouping*. The *Collapse all groups* option, maintains the current grouping selection but collapses all groups that have been opened up.
- **Actions** – You can select the following actions from the dropdown menu:

  - Set as baseline - Set the baseline used for detecting anomalous network activity, see **SETTING A NETWORK BASELINE**.
  - Auto arrange – automatically optimize the map display for the entities currently being displayed.

- Groups/Assets – Each group of assets is represented by an icon on the map, with each asset type represented by a different icon (as described in **ASSET TYPES**). For groups, the number at the top of the icon indicates the number of assets included in that group. You can drill down to show separate icons for each sub-group until you get to the individual asset icons. For individual assets, the color of the frame around the asset indicates its risk level (red, yellow, green).

You can drag the groups and assets and reposition them to get a better view of the assets and their connections.

- Connections - Each communication between groups of assets and/or individual assets, according to the degree of granularity currently displayed in the map. The thickness of the line indicates the volume of communication through that connection.
- Total Assets Displayed – Shows the number of assets detected in the network (and displayed in the map) based on the specified time frame and asset filters. This number is shown relative to the total number of assets detected in your network.
- Navigation Controls – You can zoom in and out of the display and navigate to show the desired elements using the onscreen controls or by using standard mouse controls.

Asset Groupings

The Network Map can show assets grouped by various different categories. Connections are shown between groups of assets. You can click on an asset to drill-down into the elements included in that group. Multiple groups can be drilled-down simultaneously. Tenable.ot contains multiple layers of embedded groups, so that each time that you drill-down you get a more granular view of the included assets.

The following are the Groupings that can be applied to the main display and the drill-down options for that selection.

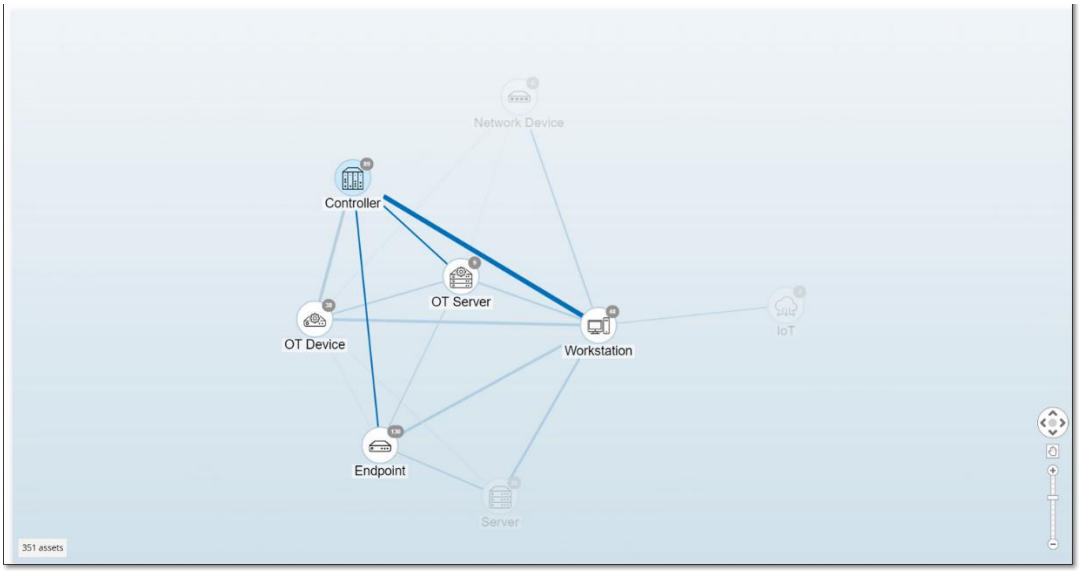
When the Map display is grouped by *Asset Type* (default), the drill-down hierarchy is as follows: Asset Type > Vendor > Family > Individual Asset.

When the Map display is grouped by *Risk Level* or *Purdue Level*, this adds an additional level *above* the Asset Type grouping, so that the hierarchy is: Purdue Level/Risk Level > Asset Type > Vendor > Family > Individual Asset. Every level is represented by a circle surrounding the included groups/assets.

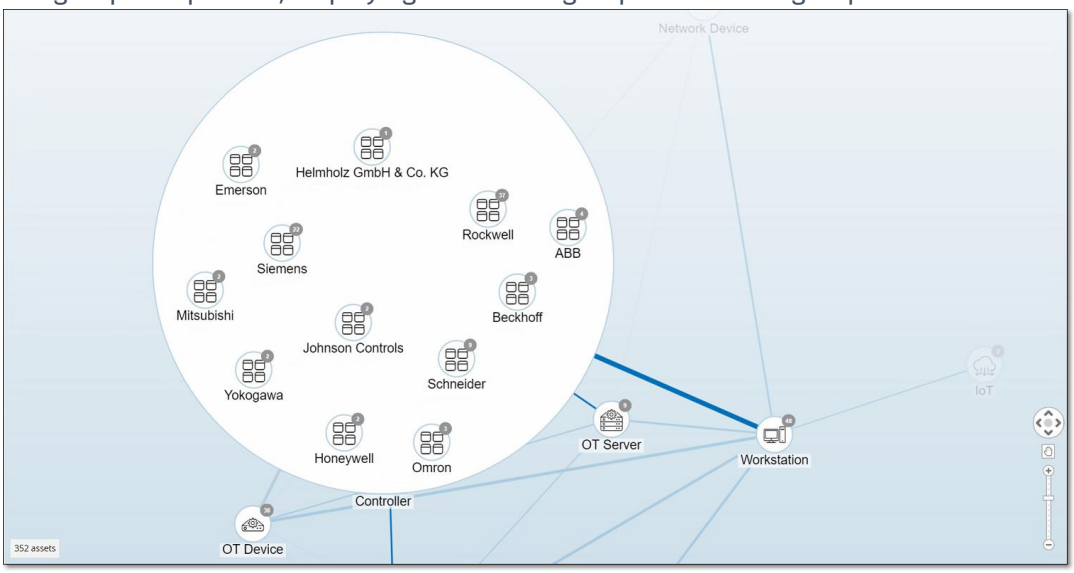
The following example shows how you can drill down into the display:

To drill down into an Asset Type Group:

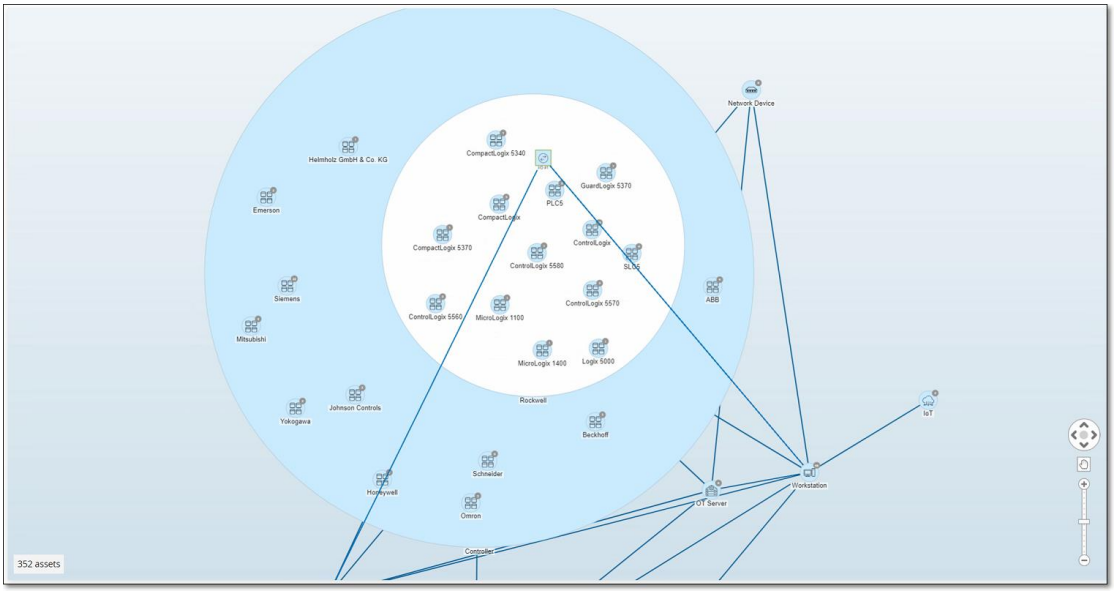
1. By default, when you open the **Network Map** screen it shows the assets grouped by *Asset type*.



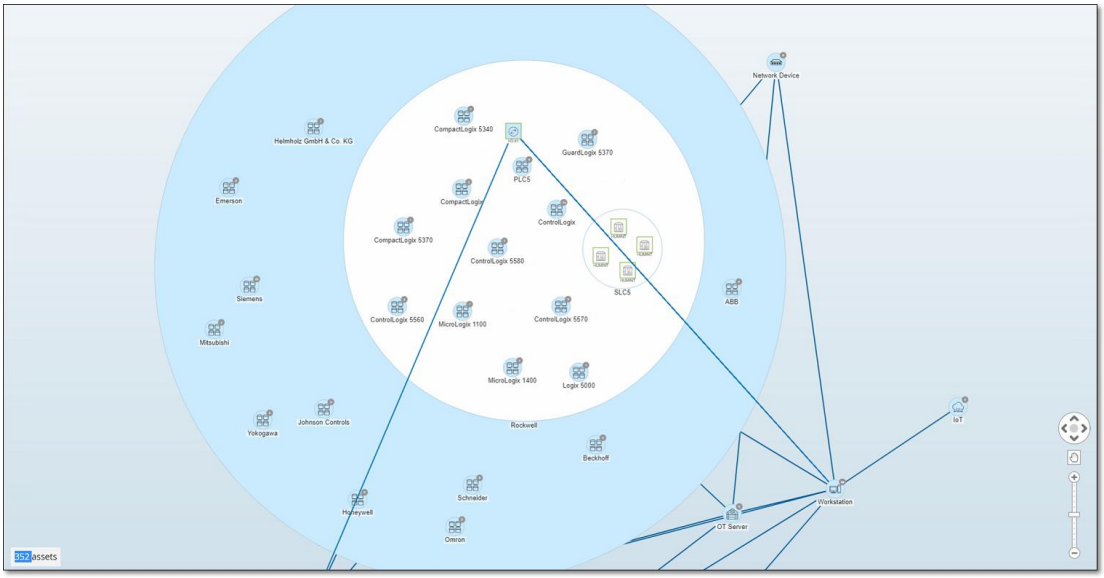
2. Double-click on the group icon that you would like to drill down into (e.g. **Controller**). The group is expanded, displaying the *Vendor* groups within that group.



3. To drill down further, click on a *Vendor* group (e.g. Rockwell).



4. To drill down further, click on a Family group (e.g. SLC5).
5. The individual assets within that group are displayed.



6. You can now click on a specific asset to see details for that asset and its connections, see **VIEWING ASSET DETAILS**.

➡ **To collapse the display:**

1. Click on **Group by**.
2. Click **Collapse all groups**.
   The display returns to showing the top-level groups.

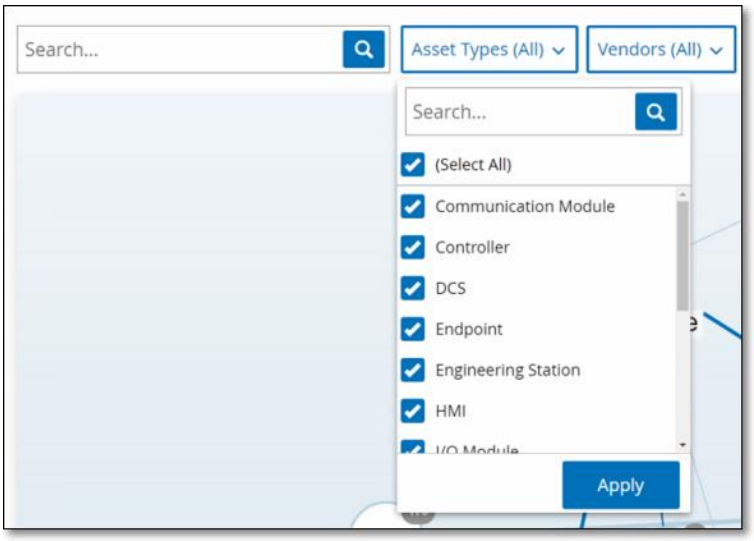
➡ **To remove all grouping:**

1. Click on the **Group by** button.

2. Select **No grouping**.
   The map shows all the single assets with no grouping applied.

Applying Filters to the Map Display

You can filter the map display by one or more of the specified categories: Asset Type, Vendors, Families, Risk Levels, Purdue Levels.



➡ **To apply filters to the Map:**

1. Click on the desired filter category.
2. Select/deselect the checkboxes for each element that you would like to include/exclude from the display.

> By default, all elements are included in the filter.

3. You can click on the **Select All** checkbox to deselect all the values, and then add the desired values.
4. You can perform a search in the filter search box to find a specific value in the filter window.
5. Repeat the process for each filter category, as needed.
6. Click **Apply**.
   Only the selected elements are displayed on the Map.

Viewing Asset Details

Click on a specific asset to display basic information about the asset and its network activities, including the risk level, IP address, asset type, vendor and family. The Map displays connections from the selected asset to all of the other assets that are communicating with it. You can then click on link in the asset name to go to the Asset Details screen where more detailed information about the asset is shown.

Setting a Network Baseline

A Network Baseline is a map of all conversations that took place between assets in the network during a specified time period. The Network Baseline is used in *Network Baseline Deviation* Policies, which alert for anomalous conversations in the network, see **Network Event Types.**

Each conversation between assets that did not interact during the Baseline sample triggers a Policy alert (assuming that it is within the scope of the specified Policy conditions). An initial Network Baseline must be created on the Network Map screen in order to enable creation of Network Baseline Deviation policies. The Network Baseline can be updated at any time by setting a new Network Baseline. You should set a new Network Baseline any time that new assets or connections are added to your network.

➡ **To Set a Network Baseline:**

1. On the **Network Map** screen, select the time range of the conversations that you would like to include in the Network Baseline using the **Time Frame Selection** at the top of the screen.
   The **Network Map** for the selected time frame is shown on the screen.
2. Click on **Actions** > **Set as baseline** at the top of the screen.
   The new Network Baseline is configured in the system and applied to all Network Baseline Deviation Policies.

Vulnerabilities

Tenable.ot identifies various types of threats that affect the assets in your network. As information about new vulnerabilities are discovered and released into the general public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them.

These programs are named *Plugins*, and are written in the Nessus proprietary scripting language, called *Nessus Attack Scripting Language* (NASL). Plugins detect CVEs as well as other threats that can affect assets in your network (e.g. obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, etc.)

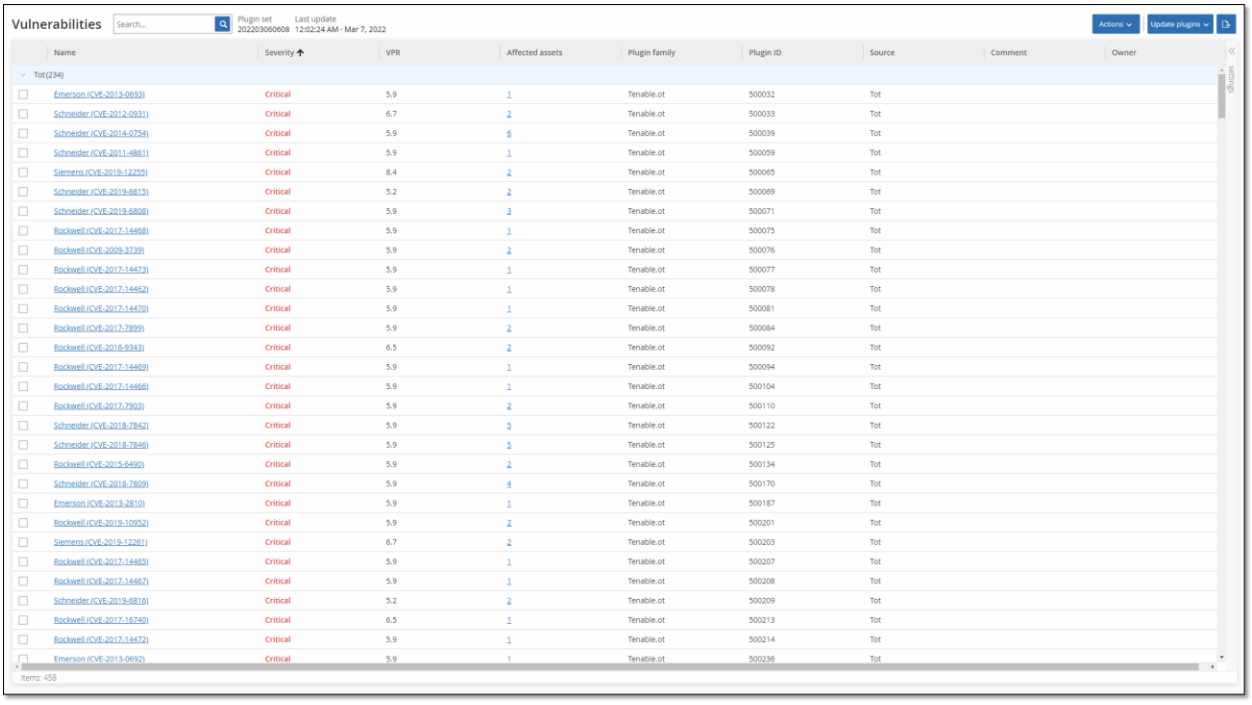
Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

For information about updating your Plugin set, see **Updates**.

Vulnerabilities Screen

The **Vulnerabilities** screen shows a list of all vulnerabilities detected by the Tenable Plugins that affect your network and assets.

You can customize the display settings by adjusting which columns are displayed and where each column is positioned. For an explanation of the customization features, see **Working with Lists**.



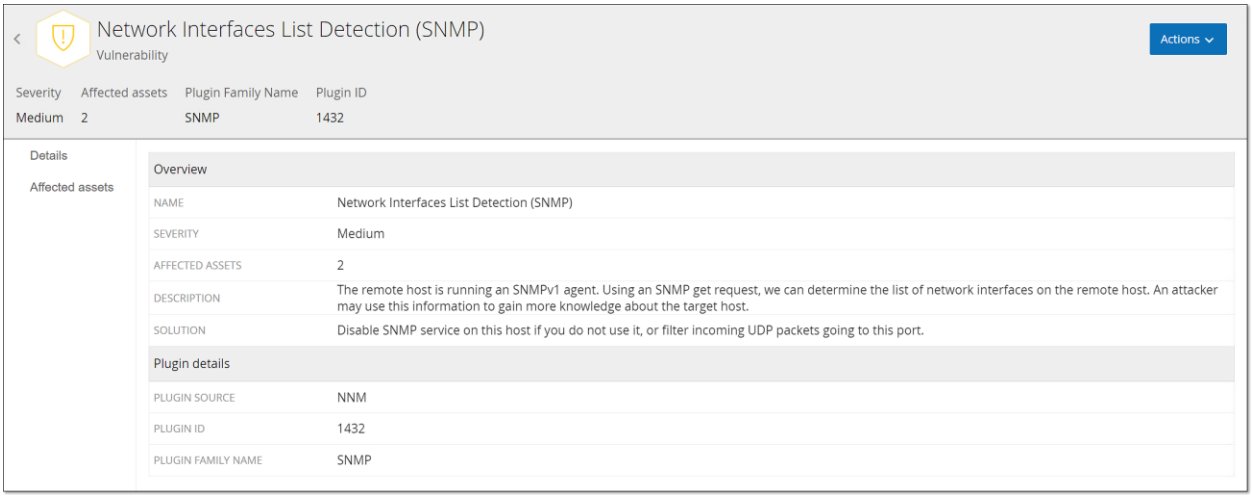
The information shown in the **Vulnerabilities** tab is described in the following table:

Parameter	Description
Name	The Name of the Vulnerability. The Name is a link to show the full Vulnerability listing.

Parameter	Description
Severity	This score indicates the severity of the threat detected by this Plugin. Possible values: *Info*, *Low*, *Medium* or *High*.
VPR	Vulnerability Priority Rating (VPR) is a dynamic indicator of the severity level, which is constantly updated based on the current exploitability of the vulnerability. This value is generated by Tenable as the output of Tenable Predictive Prioritization, which assess the technical impact and threat posed by the vulnerability. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploitation.
Plugin ID	The unique identifier of the Plugin.
Affected Assets	The number of assets in your network that are affected by this Vulnerability.
Plugin family	The family (group) with which this Plugin is associated.
Comment	You can add free text comments about this Plugin.

Plugin Details

Click on a Plugin Name to show detailed information about that Plugin.



This screen contains three elements:

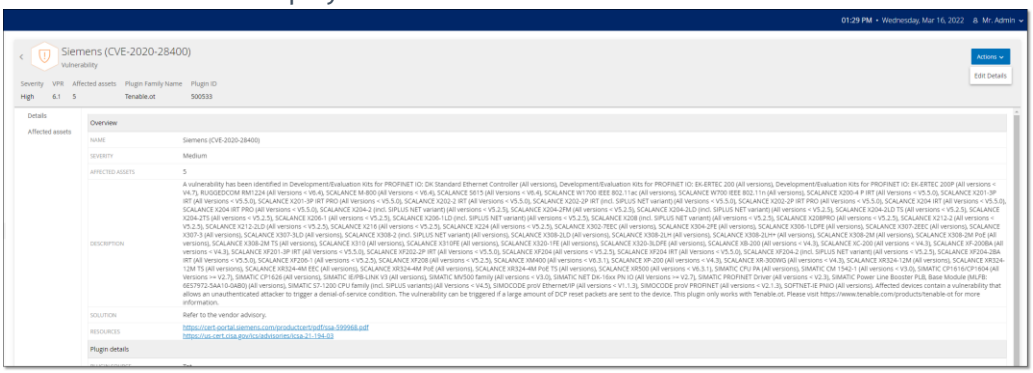
- Header bar - shows basic info about the specified Vulnerability, and contains the Actions button, which allows you to edit vulnerability details. See **Editing Vulnerability Details**.
- Details tab – shows the full description of the Vulnerability and gives links to relevant resources.

- Affected Assets tab – shows a listing of all assets that are affected by the specified Vulnerability. Each listing includes detailed information about the asset, as well as a link to view the Asset Details window for that asset.

Editing Vulnerability Details

➡ **To edit Vulnerability Details:**

1. In the relevant **Vulnerability Details** page, click on the **Actions** button at the top-right corner. The Actions menu is displayed.



2. In the **Actions** menu, click **Edit Details**.
   The **Edit Vulnerability Details** side panel is displayed.

3. In the **Comments field,** enter comments about the vulnerability.
4. In the **Owner** field, enter the name of the person assigned to address the vulnerability.
5. Click **Save**.

Local Settings

The various settings screens are listed under **Local Settings** in the Main Navigation.

The following is a brief description of the information shown and actions available in each of the tabs.

- **Queries** – activate/de-activate Query functions and adjust their frequency and settings. Queries are divided into separate screens for *Asset Discovery*, *Controller* and *Network*. See **QUERIES**
- System Configuration
    - **Device** – view and edit device details and network information (e.g. system time, DNS Servers, automatic logout (i.e. inactivity timeout)).
    - **Sensors** – view and manage Sensors, approve or delete incoming Sensor pairing requests, and configure Active Queries performed by Sensors. See **SENSORS**.
    - **Port Configuration** – view how the ports on the device are configured. For more information on Port Configuration, see **Installing the Tenable.ot Appliance** > **Step 4 - Setup Wizard** > **SCREEN 2 – DEVICE**.
    - **Updates** – perform updates of Plug-ins either automatically or manually through the cloud, or offline.
    - **Certificate** – view info about your HTTPS certificate and ensure a secure connection by either generating a new HTTPS certificate in the system or uploading your own. See **CERTIFICATE**.
    - **API Keys** – generate API keys to enable 3rd party apps to access Tenable.ot via API. All users can create API keys. The API key will have the same permissions as the user that created it. according to their role. An API key is shown once, when it is first generated; the user must save it in a secure location for later use.
    - **License** – view, update and renew your license. See **LICENSE**.
- Environment Configuration
    - **Asset Settings** –
        - **Monitored Network** – view and edit the aggregation of IP ranges in which the system classifies assets.
        - **Update Asset Details Using CSV** – Update the details of your assets using a CSV template.
        - **Add Assets Manually** – Add new assets to your assets list using a CSV template.

The max. number of IP ranges that can be sent to the NNM is 128, therefore we recommend not exceeding this limit.

In addition to the specified IP ranges, any host within the Tenable.ot platform's subnets or any Activity performing device will be classified as an asset.

    - **Hidden Assets** – view a list of assets that were hidden in the system (i.e. which the user chose to remove from the asset listings), see **HIDING ASSETS**. You can restore hidden assets from this screen.
    - **Custom Fields** - you can create custom fields to tag Assets with relevant info. The custom field can be plain text or it can be a link to an external resource.

- Event Clusters - enables you to cluster together multiple similar events that occur within a designated time range in order to facilitate monitoring them. See **EVENT CLUSTERS**.
- PCAP Player – enables you to upload a PCAP file containing recorded network activity and "play" it on Tenable.ot, loading the data into your system. See **PCAP PLAYER**.

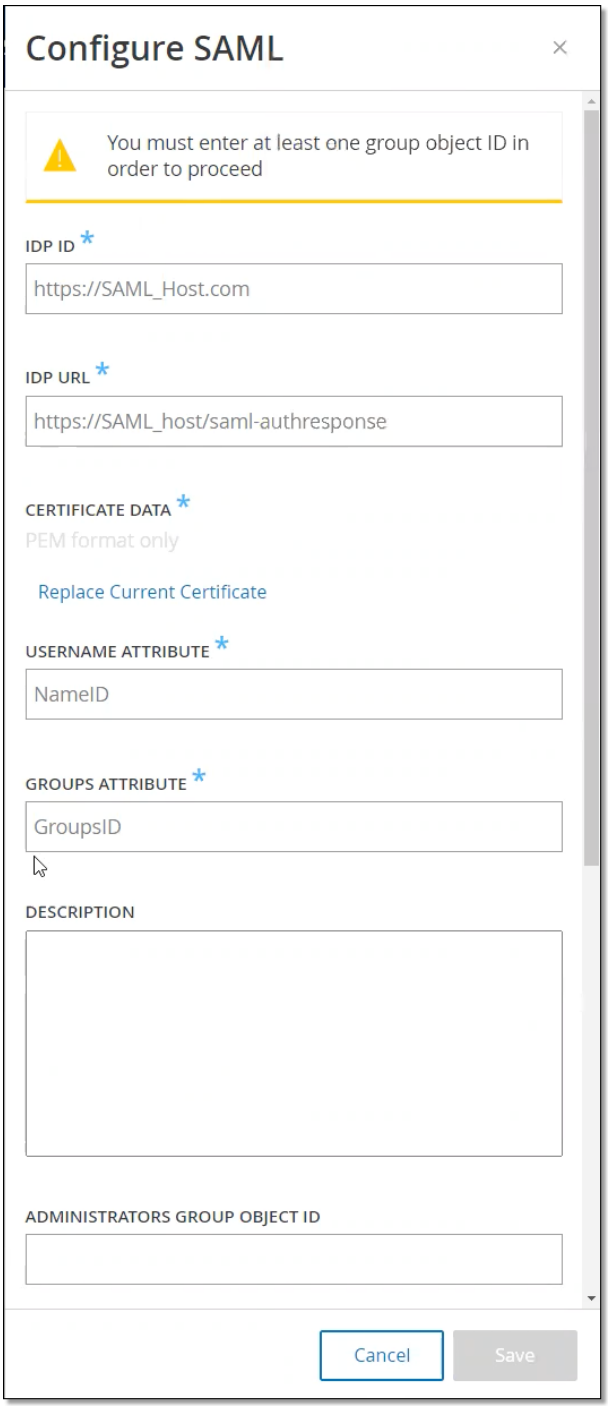
- Users and Roles – view, edit and export information about all user accounts.
  - User Settings – view and edit information about the User who is currently logged into the system (Full Name, Username and Password) and change the language used in the User Interface (English, Japanese, Chinese, French or German).
  - Local Users - An Admin user can create local user accounts for specific users and assign a Role to the account, see **LOCAL USERS**.
  - User Groups – An Admin user can view, edit, add and delete user groups. See **USER GROUPS**.
  - Active Directory - User credentials can optionally be assigned using an LDAP Server, such as Active Directory. In this case, user privileges are managed on the Active Directory. See **ACTIVE DIRECTORY**.
- Integrations – set up integration with other platforms. Tenable.ot currently supports integration with Palo Alto Networks Next Generation Firewall (NGFW) and Aruba ClearPass, as well as with other Tenable products (Tenable.sc and Tenable.io). See **SAML**

You can integrate Tenable.ot with your organization's identity provider (e.g. Microsoft Azure). This enables users to authenticate via their identity provider. The configuration involves setting up the integration by creating a Tenable.ot application within your identity provider, entering information about your created Tenable.ot application and uploading your identity provider's Certificate to the Tenable.ot SAML page, and then mapping groups from your identity provider to User Groups in Tenable.ot. For a detailed tutorial for integrating Tenable.ot with Microsoft Azure, see **APPENDIX 2 – SAML INTEGRATION FOR AZURE ACTIVE DIRECTORY**.

➡ **To configure SAML:**

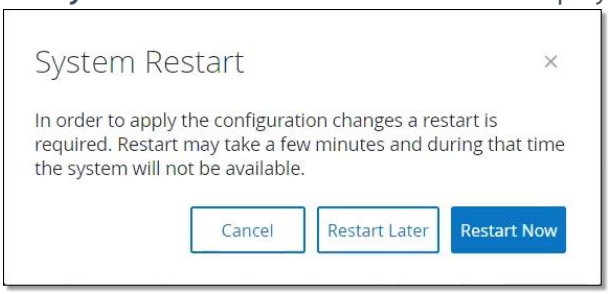
1. Under **Local Settings**, go to the **Users and Roles** > **SAML** screen.

2. Click **Configure.**
   The **Configure SAML** side panel is displayed.



3. In the **IDP ID** field, enter the Identity Provider's ID for the Tenable.ot application.
4. In the **IDP URL** field, enter the Identity Provider's URL for the Tenable.ot application.
5. Under **Certificate Data**, click **Replace Current Certificate**, navigate to the Identity Provider's Certificate file you downloaded for use with the Tenable.ot application and open it.

6. In the **Username Attribute** field, enter the username attribute from the Identity Provider for the Tenable.ot application.
7. In the **Groups Attribute** field, enter the groups attribute from the Identity Provider for the Tenable.ot application.
8. Enter a description in the **Description** field. (Optional)
9. For each group mapping that you would like to configure, access the Identity Provider's **Group Object ID** for a group of users and enter it into the desired **Group Object ID** field to map it to the desired Tenable.ot User Group.
10. Click **Save** to save and close the side panel.
11. On the **SAML** screen, click to toggle the **SAML single sign on login** button **ON**.
    The **System Restart** notification window is displayed.



12. Click **Restart Now** to restart the system and apply the SAML configuration immediately, or click **Restart Later** to delay the application of the SAML configuration the next time the system is restarted. If you choose to restart later, the following banner is shown until the restart is done:

    Upon reboot, the settings will be activated, and any user assigned to the designated groups can access the Tenable.ot platform using their Identity Provider credentials.

- Integrations.
- Servers – view, create and edit servers configured in your system. Separate screens are shown for:
    - SMTP Servers –SMTP servers enable Event notifications to be sent via email.
    - Syslog Servers - Syslog servers enable Event logs to be logged on an external SIEM.
    - FortiGate Firewalls - The Tenable.ot-FortiGate integration allows users to send firewall policy suggestions to a FortiGate firewall based on the Tenable.ot network events.
- System Actions – shows a sub-menu of system activities. The sub-menu includes the following options:
    - System Backup – enables you to back up your Tenable.ot appliance (except packet capture data). To restore the system from a backup file, please contact

https://www.tenable.com/products/tenable-ot. Please note that during the backup process Tenable.ot will be unavailable to all users.
  - Export Settings – export Tenable.ot platform configuration settings as an .ndg file to the local computer. This will serve as a backup in case of a system reset or to import to a new Tenable.ot platform.
  - Import Settings – imports Tenable.ot platform configuration settings that have been saved as an .ndg file on the local computer.
  - Download Diagnostic Data – creates a file with diagnostic data on the Tenable.ot platform and stores it on the local computer.
  - Restart – restarts the Tenable.ot platform. This is needed for activation of certain configuration changes.
  - Disable – disable all monitoring activities. You can reactivate the monitoring activities at any time.
  - Shut Down – shuts down the Tenable.ot platform. To power on, press the Power button on the Tenable.ot appliance.
  - Factory Reset – returns all settings to the factory default settings. Warning: this operation can't be undone and all data in the system will be lost.

- System Log – shows a log of all system events (e.g. Policy turned on, Policy edited, Event Resolved etc.) that occurred the system. You can export the log as a CSV file or send it to a Syslog server. See **SYSTEM LOG**.

Queries

The Tenable.ot Queries screens enable you to configure and activate the queries features. For a general explanation of the Queries technology, see **TENABLE.OT TECHNOLOGIES**. As part of the initial setup, it was recommended to activate all of the Query capabilities. At any time, you can activate/de-activate any of the Query functions. You can also adjust the settings for when and how the Queries are executed.

In addition to the automatic Queries that are run periodically, most queries can be initiated by the user on demand by clicking the Run Now button next to the Query.

The Log4J and Ripple20 Vulnerabilities Scans can only be run manually, not by a periodic schedule. They are activated from the Local Settings > Queries > Network screen, see **NETWORK QUERY FUNCTIONS TABLE**.

Turning the Queries off will prevent the system from detecting significant events in the network. This will cause many features to become unavailable.

The query activation and configuration are done under Local Settings > Queries. The queries are divided into three separate screens. The following sections explain the different types of Queries and gives procedures for activating and configuring each type of Query.

All Controller Queries

➡ **To activate Controller Queries:**

1. Under **Local Settings**, go to the **Queries** > **Controller** screen.
2. Toggle the switch for **All Controller Queries** to **ON**.
3. Activate/deactivate specific types of Queries by toggling the status **ON/OFF** for each type of query. For a description of the various type of Controller Queries, see **CONTROLLER QUERY FUNCTIONS TABLE**.
4. You can edit the settings for each Controller Query type using the following procedure:
    a. Click **Edit** next to the desired Query type.
    b. Adjust the frequency and scheduling of the queries (for an explanation of the available settings options see **CONTROLLER QUERY FUNCTIONS TABLE**).
    c. Click **Save**.

Controller Query Functions Table

Function	Description	Frequency (min.-max.)
All Controller Queries	Activates all of the Query functions related to controllers, as described below.	n/a
Periodic Snapshots	Captures the current program deployed on each controller. By periodically taking snapshots, Tenable.ot can detect changes that were made to a controller's program even if the changes were not sent through the network.	1/day - 1/6 weeks
Policy Triggered Snapshots	Enables the user to configure policies to trigger a snapshot when the conditions of a policy are met.	n/a
Controllers Discovery	A broadcast that searches for new controllers and assists in classifying unknown assets.	1/hr. - 1/6 weeks
Controller State Query	Detects the current PLC status (options are: *Running*, *Stopped*, *Fault*, *No config*. And *Test*).	1/5 min. – 1/hr.
Diagnostic Buffer Query	Queries for the Diagnostic Buffer event logs as defined in Siemens controllers.	1/day - 1/6 weeks
Controller Details Query	Retrieves the controller's hardware and firmware details.	1/hr. - 1/6 weeks
Backplane Query	Discovers modules and their specifications within a backplane. The query allows for quick identification of the entire backplane configuration.	1/15 min. – 1/week

All Network Queries

➡ **To activate Network Queries:**

1. Under **Local Settings**, go to the **Queries** > **Network** screen.
2. Toggle the switch for **All Network Queries** to **ON**.
3. Activate/deactivate specific types of Queries by toggling the status **ON/OFF** for each type of query that you would like to activate. For a description of the various Network Query capabilities, see **Network Query Functions Table**.
4. You can edit the settings for each Network Query type using the following procedure:
   a. Click **Edit** next to the desired Query type.
   b. Adjust the frequency and scheduling of the queries (for an explanation of the available settings options see **Network Query Functions Table**).
   c. Click **Save**.

Network Query Functions Table

Function	Description	Settings
All Network Queries	Activates all of the Query functions related to non-controller network assets, as described below.	n/a
Port Mapping	Identifies all open ports in network assets. This enables you to minimize security risks by closing off unused ports.	Mapping Range – set whether mapping is done for all ports or only for the 1,000 most frequently used ports. Mapping Rate – set the number of ports mapped per second by default and the maximum rate for mapping on demand.
SNMP Query	Collects configuration info from SNMP enabled assets in the network.	SNMP v2 Community Strings SNMP v3 Usernames Frequency and Scheduling - 1/day - 1/6 weeks
DNS Query	Searches for the DNS names of the assets in the network.	n/a
ARP Query	Retrieves the MAC address of new Ips detected in the network.	n/a
NetBIOS	This query sends a NetBIOS unicast packet which is used to classify and detect Windows machines in the network.	Frequency and Scheduling - 1/hr. - 1/6 weeks

Function	Description	Settings
Active Asset Tracking	Detects assets that are inactive in the network for the specified time period and polls them to verify if they are still active.	Frequency and Scheduling - 1/5 min. - 1/week
WMI Query	Collects info about Windows machines in the network.	WMI Username – provided by IT Password – provided by IT Frequency and Scheduling - 1/day - 1/6 weeks Test IP Address – You can test the WMI configuration by clicking Test IP address, entering the IP of a known Windows machine in your network and then clicking Test IP Address at the bottom of the screen. You can then open the Asset Details for that asset and check that the WMI info was added.
USB Connections Query	Detects connection of USB/DoK devices to Windows PCs in the network.	Frequency and Scheduling - 1/day - 1/6 weeks
Ripple20 Vulnerabilities Scan	This scan identifies CVEs related to the Ripple20 vulnerabilities. It uses a Nessus plugin. Note: this scan must be run **manually** and it is only run on the assets within the specified IP addresses and/or CIDRs.	IP addresses or CIDRs
Log4J Vulnerabilities Scan	This scan identifies CVEs related to the Log4J vulnerabilities. It uses a Nessus plugin. Note: this scan must be run manually, and it is only run on the assets within the specified IP addresses and/or CIDRs.	IP addresses or CIDRs

Asset Discovery

Tenable.ot automatically identifies assets in the network by detecting their interactions with other assets through the network. Tenable.ot has an additional capability of identifying assets that are not active in the network or that their communication streams are not captured by the mirroring ports using the **Asset Discovery** Query. You can configure the frequency that the query is run automatically. You can also manually run the query at any time from this screen.

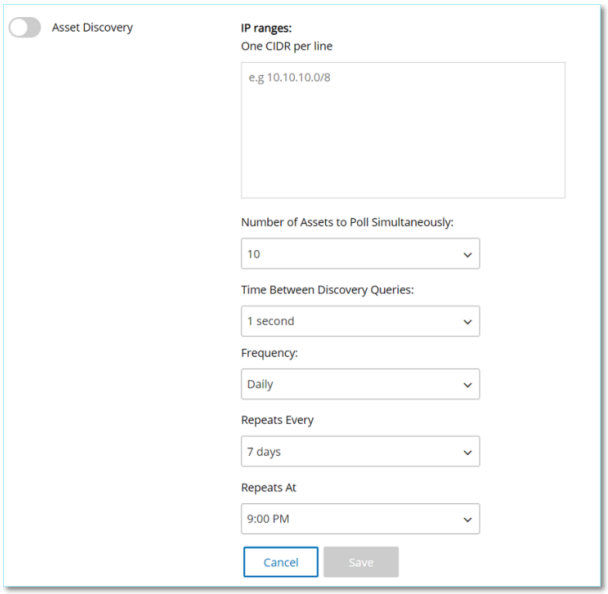
Once a new asset is discovered, the **Initial Asset Enrichment** feature runs a battery of queries to determine precise information about the asset.

	Only IPs that are defined as Monitored Networks in the **Asset Settings** will be included in the scan.

	Turning the Queries off will prevent the system from detecting significant events in the network. This will cause many features to become unavailable.

➡ **To activate the Asset Discovery Query:**

1. Under **Local Settings**, go to the **Queries** > **Asset Discovery** screen.
2. Click **Edit** in the **Asset Discovery** section.
   A series of configuration fields are shown.



3. In the **IP Ranges** box, enter one or more IP ranges (with each range on a separate line).

	Segments of your network that are monitored by the mirror port do not need to be entered, and are automatically queried by Tenable.ot. If you would like to run the Asset

	Discovery query on additional segments of your network that are not monitored by the mirror port, enter the range of IPs for those segments in this box.

4. You can adjust the following configuration settings (optional) by selecting a value from the dropdown menu.
   - **Number of Assets to Poll Simultaneously** (options: 10, 20, 30)
   - **Time Between Discovery Queries** (options: 1-3 seconds)
   - **Repeats** – set the type of interval used for setting the frequency of the query (daily or weekly)
   - **Repeats Every** – set the frequency of the query (Daily: 1-31 days, Weekly: 1-6 weeks)
   - **On** – for a weekly interval set the day of the week on which the query is run
   - **At** – set the time of day that the query is run
5. Click **Save**.
6. Toggle the **Asset Discovery** switch to **ON**.

➡ **To activate Initial Asset Enrichment:**

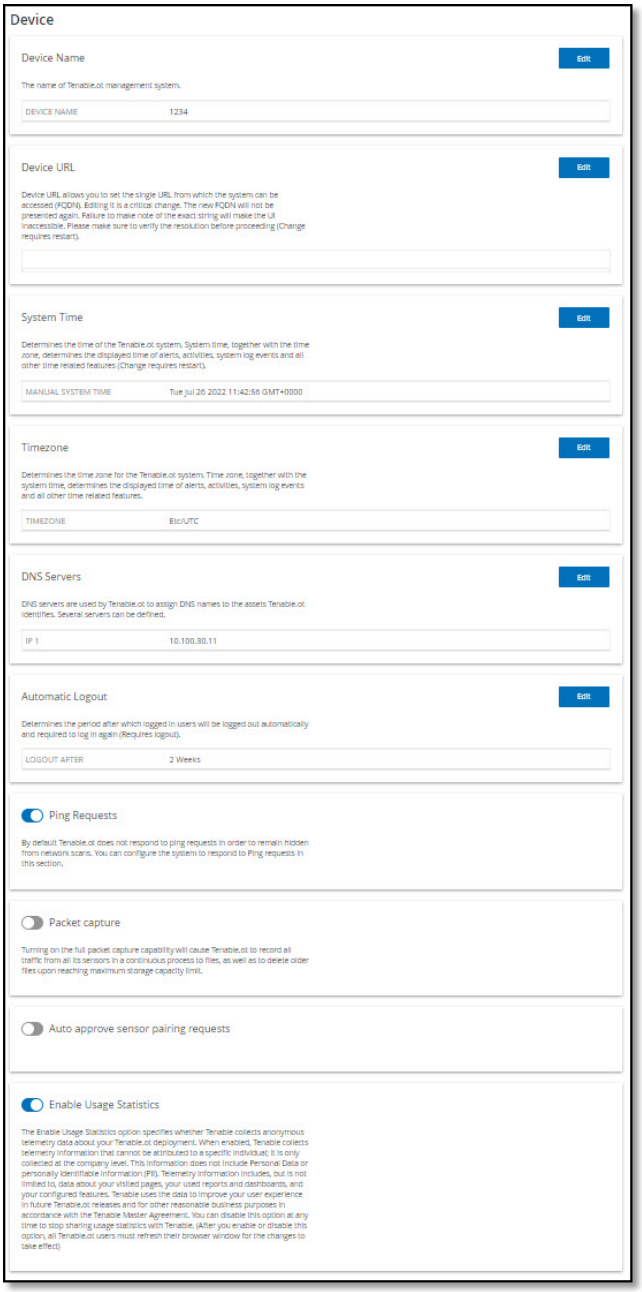
1. Under **Local Settings**, go to the **Queries** > **Asset Discovery** screen.
2. Toggle the switch for **Initial Asset Enrichment** to **ON**.

System Configuration

The Tenable.ot System Configuration screens enable you to automatically configure and manually perform Plugin updates, as well as view and update details regarding your device, HTTPS certificate, API Keys, and license.

Device

This screen shows detailed information about your Tenable.ot configuration. You can view the info and edit the configuration on this screen.



The following info is shown:

- **Device Name** – a unique identifier for the Tenable.ot appliance.
- **Device URL** – allows you to set the single URL from which the system can be accessed (FQDN).

> Editing the Device URL is a critical change. The new FQDN will not be presented again. Failure to make note of the exact string will make the UI inaccessible. Please make sure to verify the resolution before proceeding.

- System Time – the correct time and date are generally set automatically, but can be edited.

Setting the correct date and time is essential for accurate recording of logs and alerts.

- Timezone – select the local time zone at the site location from the dropdown list.
- DNS Servers – DNS servers are used by the Tenable.ot system to assign DNS names to the assets Tenable.ot identifies. Several servers can be identified.
- Automatic Logout – determines the period after which logged-in users will be logged out automatically and required to log in again.

Ping Requests

Turning on Ping Requests activates the Tenable.ot platform's automatic response to ping requests.

➡ **To Activate Ping Requests:**

1. Go to the **Local Settings** > **System Configuration** > **Device** screen.
2. Toggle the **Ping Requests** switch to **ON**.

Packet Captures

Turning on the full packet capture capability activates continuous recording of full-packet captures of all traffic in the network. This enables extensive troubleshooting and forensic investigation capabilities. When the storage capacity is exceeded (1.8 TB), the system deletes older files. You can view and download available files on the Network > Packet Captures screen, see section **PACKET CAPTURES**.

➡ **To Activate Packet Captures:**

1. Go to the **Local Settings** > **System Configuration** > **Device** screen.
2. Toggle the **Packet Capture** switch to **ON**.

You can stop the Packet Capture feature at any time by toggling the switch to OFF.

Auto Approve Sensor Pairing Requests

Enabling automatic approval of incoming Sensor pairing requests ensures all Sensor pairing requests are approved without any additional steps taken by the administrator. If this option is not selected, final manual approval is required for any new Sensors to connect to your network.

➡ **To Enable Auto Approval for Incoming Sensor Pairing Requests:**

1. Go to the **Local Settings** > **System Configuration** > **Device** screen.
2. Toggle the **Auto Approve Incoming Sensor Pairing Requests** switch to **ON**.

You can allow automatic approval of incoming Sensor pairing requests at any time by toggling the switch to OFF.

Enable Usage Statistics

The Enable Usage Statistics option specifies whether Tenable collects anonymous telemetry data about your Tenable.ot deployment. When enabled, Tenable collects telemetry information that cannot be attributed to a specific individual; it is only collected at the company level. This information does not include personal data or personally identifiable information (PII). Telemetry information includes, but is not limited to, data about your visited pages, your used reports and dashboards, and your configured features. Tenable uses the data to improve your user experience in future Tenable.ot releases and for other reasonable business purposes in accordance with the Tenable Master Agreement. This setting is enabled by default.

➡ **To enable Usage Statistics:**

1. Go to the **Local Settings** > **System Configuration** > **Device** screen.
2. Toggle the **Enable Usage Statistics** switch to **ON**.

You can disable sharing of usage statistics at any time by toggling the switch to OFF.

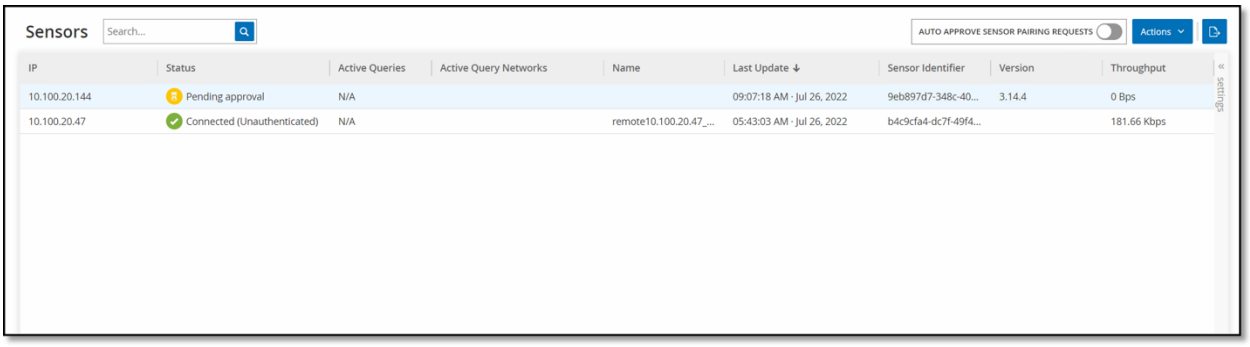
Sensors

After Sensors have been paired using the Tenable Core UI, you may approve new pairings, view and manage Sensors using the Edit, Pause and Delete functions in the Actions menu. You may also choose to enable automatic approval for Sensor pairing requests using the toggle switch.

Sensors models preceding version 2.214 will not appear in the ICP Sensors page. However, they still can be used in unauthenticated mode.

Viewing the Sensors Screen

The Sensors table shows a list of all Sensors v. 2.214 and above in the system.



The information shown on the screen is described in the following table:

Parameter	Description
IP	The IPv4 address of the Sensor.
Status	The status of the Sensor: *Connected, Connected (Unauthenticated), Pending approval, Disconnected* or *Paused*.
Active Queries	The capacity of the Sensor to send Active Queries (*Enabled, Disabled, N/A)*
Active Query Networks	The network segments to which the Sensor is assigned.
Name	The name of the Sensor in the System.
Last Update	The date and time that the Sensor information was last updated.
Sensor Identifier	The Sensor Universal Unique Identifier (UUID), a 128-bit value used to uniquely identify an object or entity on the internet.
Version	The Sensor version.
Throughput	A measure of how much data is streaming through the sensor (in kilobytes per second).

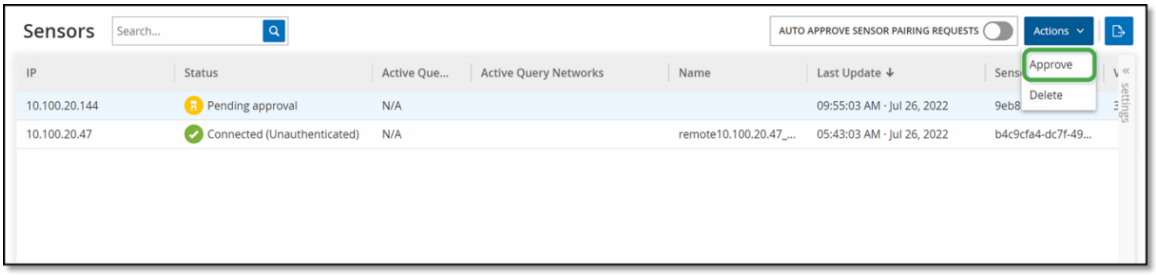
Manually Approving Incoming Sensor Pairing Requests

If the **Auto Approve Sensor Pairing Requests** setting is toggled to **OFF**, incoming sensor pairing requests must be manually approved before they are successfully connected.

➡ **To manually approve a Sensor pairing request:**

1. Go to the **Local Settings** > **System Configuration** > **Sensors screen**.
2. Click on a row in the table with a status of **Pending Approval**.

3. Click **Actions** > **Approve**, or right-click and select **Approve** from the right-click menu.



If you want to delete a Sensor, you may click Actions > Delete, or right-click and select Delete from the right-click menu.

Configuring Active Queries

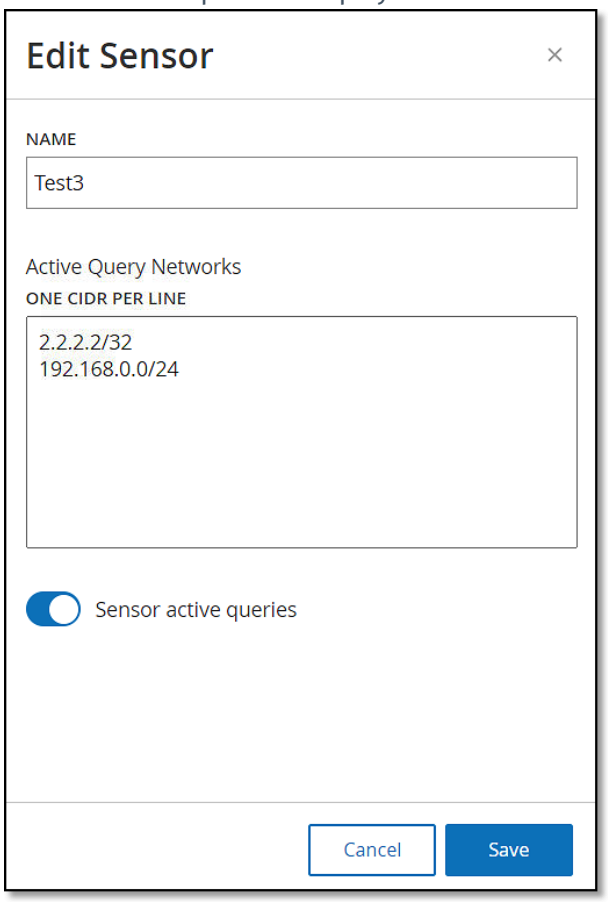
Once a Sensor is connected in *Authenticated* mode, it can be configured to perform Active Queries in the network segments to which it is assigned. You need to specify which network segments it will query.

Sensors will perform passive Network Detection on all available segments independent of this configuration.

To configure Active Queries:

1. Under **Local Settings**, go to **System Configuration** > **Sensors**.
2. Click on a row in the table with a status of **Connected**.

3. Click **Actions** > **Edit**, or right-click and select **Edit** from the right-click menu.
   The **Edit Sensor** panel is displayed.



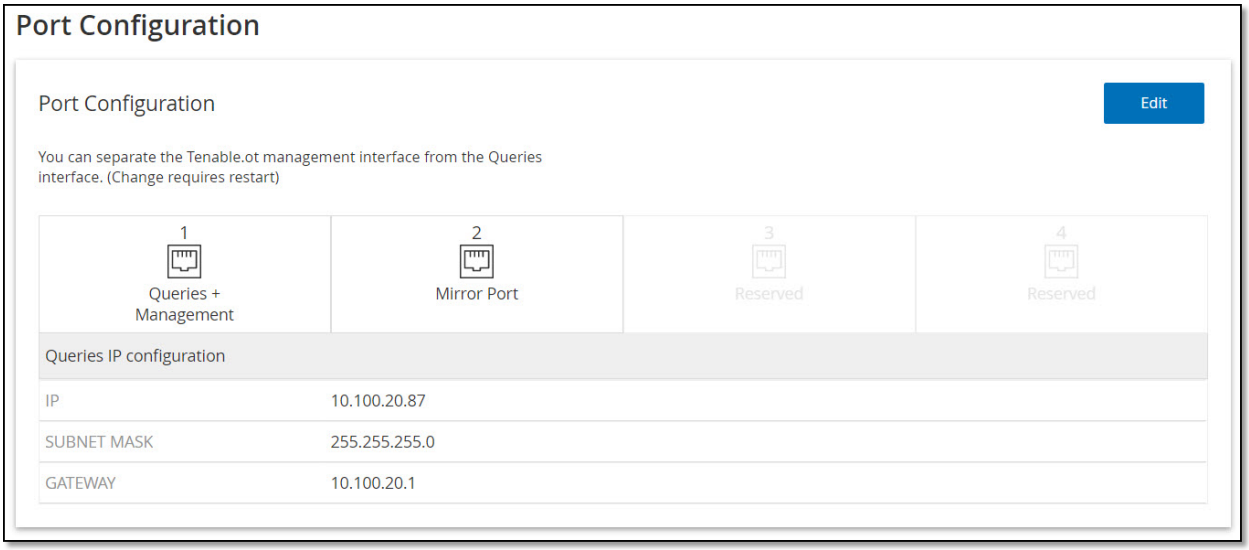
4. If you would like to rename the Sensor, edit the text in the **Name** field.
5. In the **Active Query** Networks field, add or edit relevant network segments to which the Sensor will send active queries, using CIDR notation and adding each subnetwork on a separate line.

> Queries can only be performed on CIDRs that are included in the monitored network ranges. Make sure to add only CIDRs that are accessible through this Sensor. Adding CIDRs that are not accessible may interfere with the ICP's ability to query those segments by other means.

6. Toggle the **Sensor active queries** switch to **ON** to enable active queries.
7. Click **Save**.
   The panel closes.
   In the **Sensors** table, under the **Active Queries** heading, the enabled Sensors will now display **Enabled**.

Port Configuration

The **Port Configuration** screen shows how the ports on the device are configured. For more information on Port Configuration, see **Installing the Tenable.ot Appliance** > **Step 4 – Setup Wizard** > **SCREEN 2 – DEVICE**.



Updates

Keeping Plugins up-to-date ensures that your assets are monitored for all of the latest known vulnerabilities. Updates can be performed through the cloud, both automatically and manually, and can be performed offline as well.

Updates can also be performed from the **Vulnerabilities** screen by clicking on the **Update plugins** button.

If the user license expires, the option to download new updates will be blocked, and the user will not be able to update their plugins.

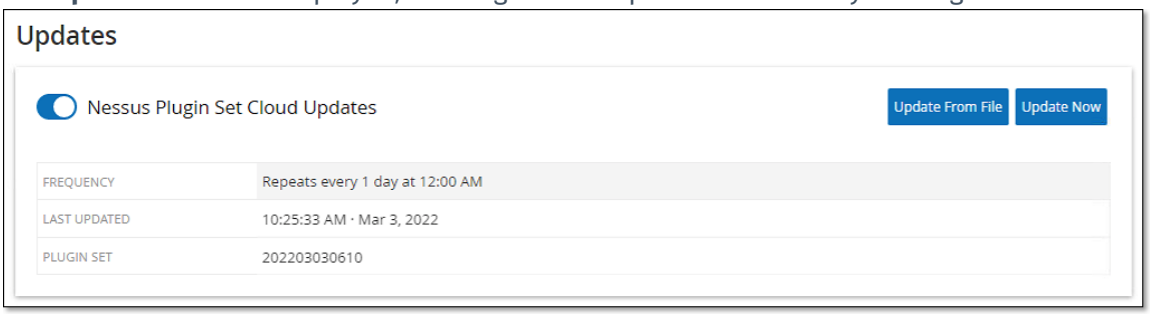
Cloud Updates

Users with an internet connection can update Plugins through the Cloud. When automatic updates are turned on, Plugins will update daily at 24:00:00.

Setting Automatic Cloud Updates of Plugins

➡ **To enable automatic updates of Plugins:**

1. Under **Local Settings**, go to **System Configuration** > **Updates**.
   The **Updates** screen is displayed, showing the last updated version of your Plugins.



2. If the toggle switch is not turned on, click on it to turn on automatic updates.

Performing Manual Cloud Updates of Plugins

➡ **To manually update Plugins:**

1. Under **Local Settings**, go to **System Configuration** > **Updates**.
   The **Updates** screen is displayed, showing the last updated version of your Plugins.
2. Click on the **Update Now** button.
   A dialog is displayed, letting you know that the update has started.

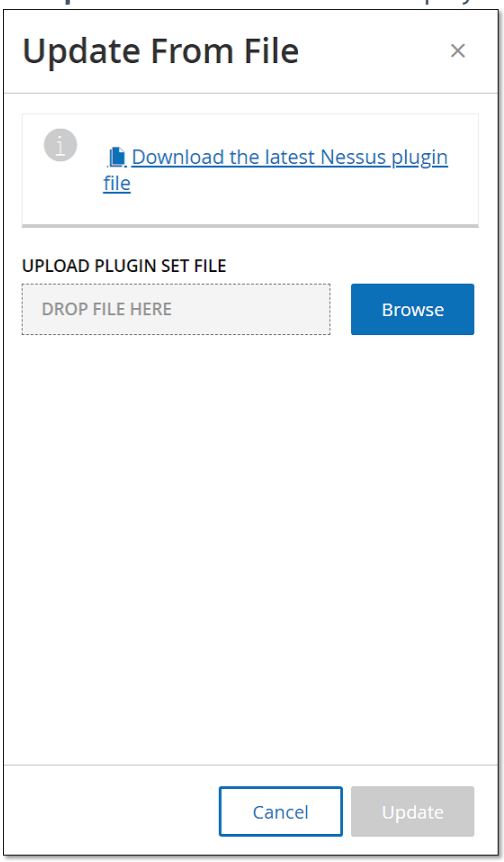
Offline Updates

Users without an internet connection on their Tenable.ot device can manually update their Plugins by downloading the latest Plugin set from the Tenable Customer Portal, and uploading the file.

➡ **To update Plugins offline:**

1. Under **Local Settings**, go to **System Configuration** > **Updates**.
2. The **Updates** screen is displayed, showing the last updated version of your Plugins.

3. Click on the **Update From File** button.
   The **Update From File** window is displayed.



4. If you have not yet done so, click the link to download the latest Plugin file, then return to the **Update From File** window.

> Downloading the latest Plugin file from the link is only possible through an internet connection, such as with an internet-connected PC.

5. Click **Browse**, and navigate to the Plugin set file you downloaded from the Tenable.ot Customer portal.
6. Click **Update**.

Certificate

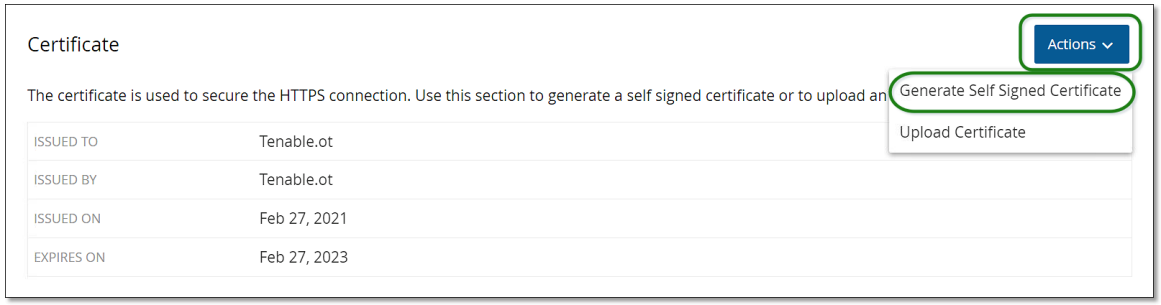
Generating an HTTPS Certificate

The HTTPS certificate ensures the system is using a secure connection to the Tenable.ot appliance and server. The initial certificate expires after two years. You can generate a new self signed certificate at any time. The new certificate is valid for one year.

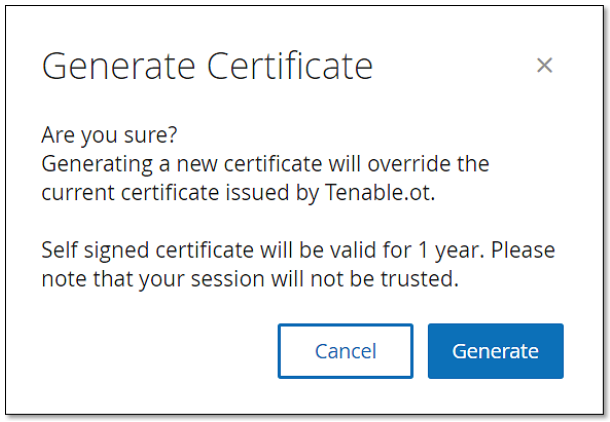
> Generating a new certificate will override the current certificate.

To generate a self signed certificate:

1. Under **Local Settings**, go to the **System Configuration** > **Certificate** screen.
2. Click on the **Actions** button, and select **Generate Self Signed Certificate**.



The Generate Certificate confirmation window is displayed.



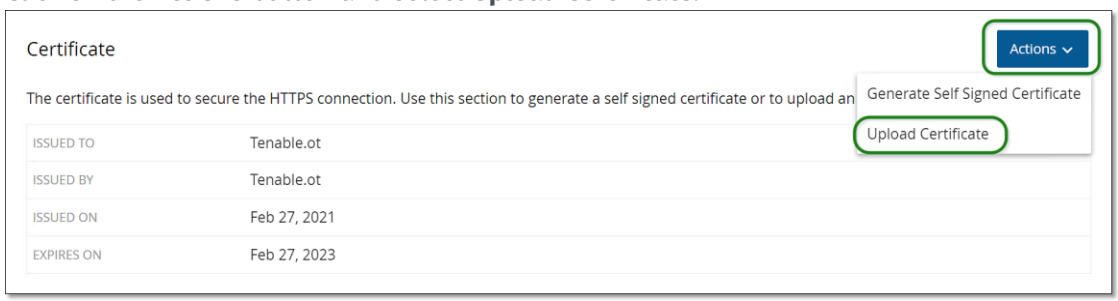
3. Click **Generate**.
   The self signed certificate is generated and can be viewed in the **Local Settings** > **System Configuration** > **Certificate** screen.

Uploading an HTTPS Certificate

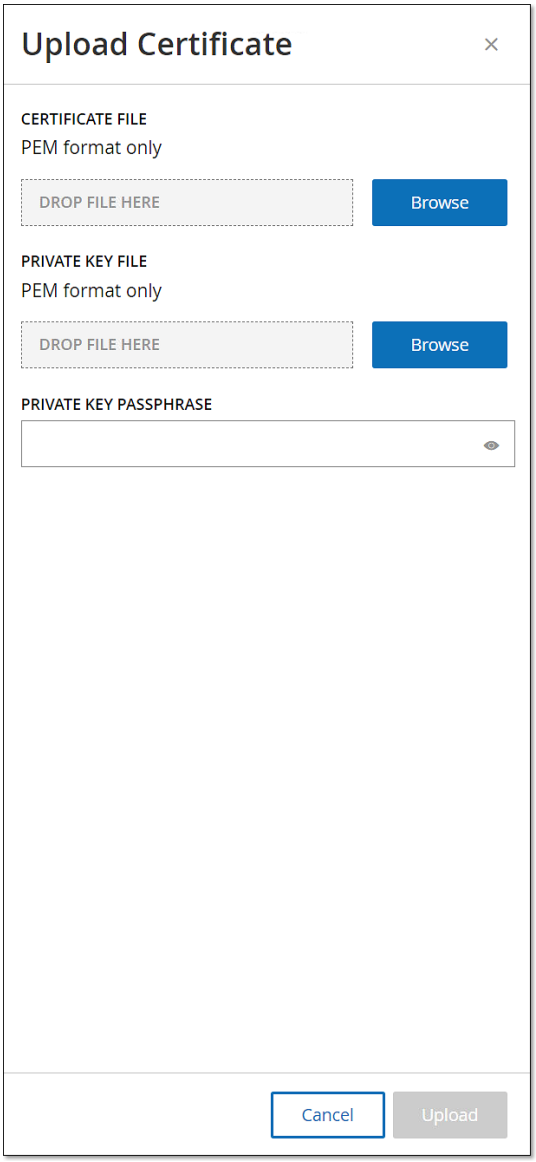
In addition to generating a self-signed HTTPS certificate, users can upload their own HTTPS certificate through the UI (Local Settings > System Configuration > Certificate). The certificate is used to secure the HTTPS connections to other devices, including your browser, between the ICP and the IM, etc.

To upload an HTTPS Certificate:

1. Under **Local Settings**, go to the **System Configuration** > **Certificate** screen.
2. Click on the **Actions** button and select **Upload Certificate.**



The **Upload Certificate** side panel is displayed.



3. Under **Certificate File** click on the **Browse** button and navigate to the Certificate file you wish to upload.
4. Under **Private Key File**, click on the **Browse** button, and navigate to the Private Key file you wish to upload.
5. Enter the private key passphrase in the **Private Key Passphrase** field.
6. Click on the **Upload** button to upload the files.
   The side panel closes.

After replacing the certificate, it is recommended to reload the browser tab to ensure the HTTP Certificate update was successful. If not, a warning notice will be displayed.

License

There may be times when you will need to update or reinitialize your Tenable.ot license. After reaching out to your Tenable account manager, you will need to follow one of the following procedures to update or reinitialize your license.

Updating the License

If you need to update your existing license (e.g. to increase your asset limit, extend your license period, or change your license type) follow the following procedure.

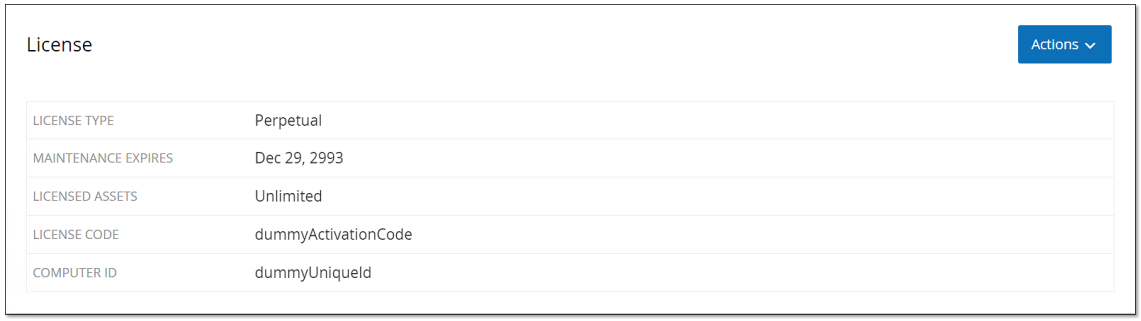
Prerequisites

- Your Tenable account manager must have already updated your license information in their system before you can register the new license.
- You need access to the Internet. If your Tenable.ot device is not connected to the Internet, you can register the license from any PC.

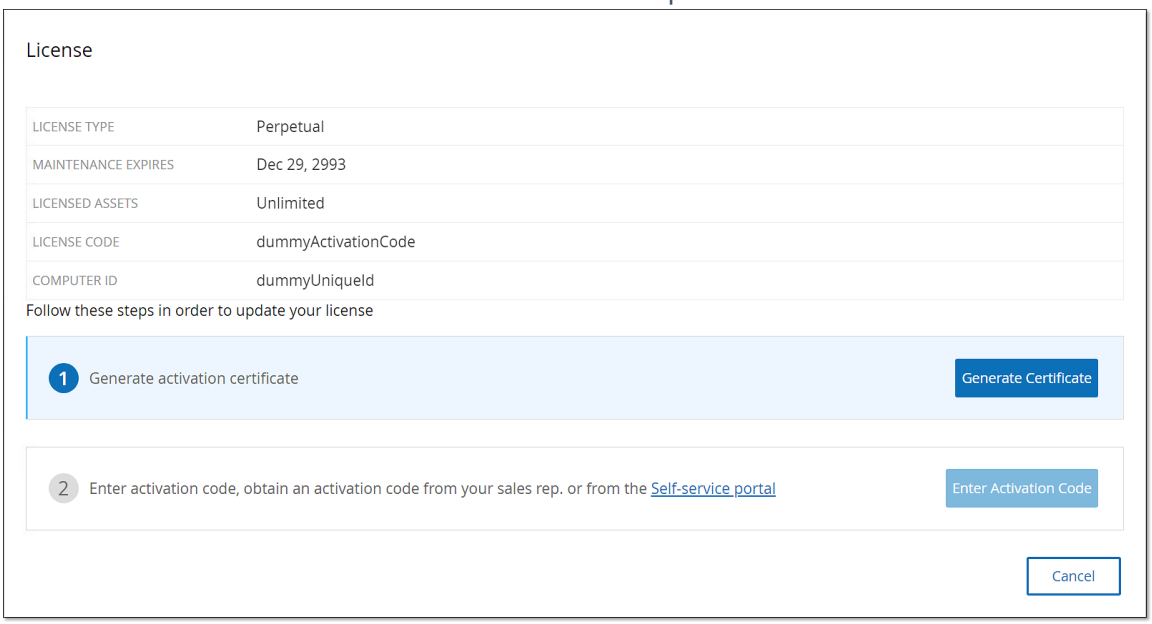
Registering a New License

➡ **To Register Your License:**

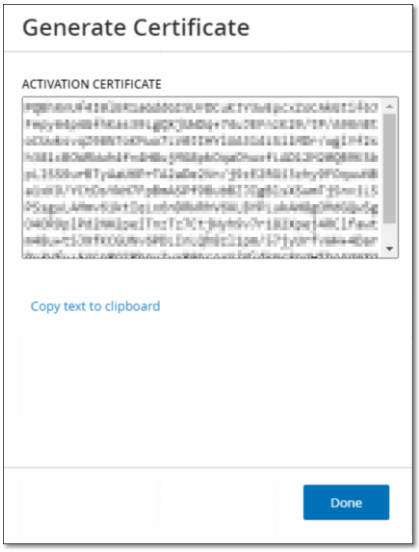
1. Under **Local Settings**, go to **System Configuration** > **License**.
   The **License** screen is displayed.



2. Click on the **Actions** button and select **Update license**.
   The **Generate Certificate** and **Enter Activation Code** steps are shown.

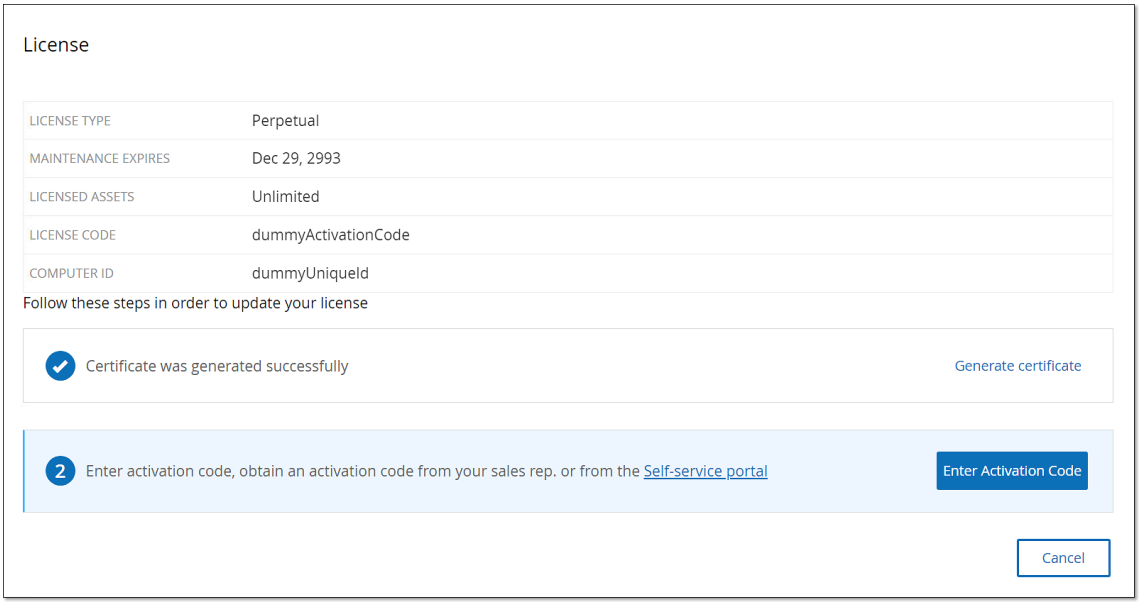


3. In the **(1) Generate activation certificate** field, click on the **Generate Certificate** button.
   The **Generate Certificate** side panel is shown with the Activation Certificate.

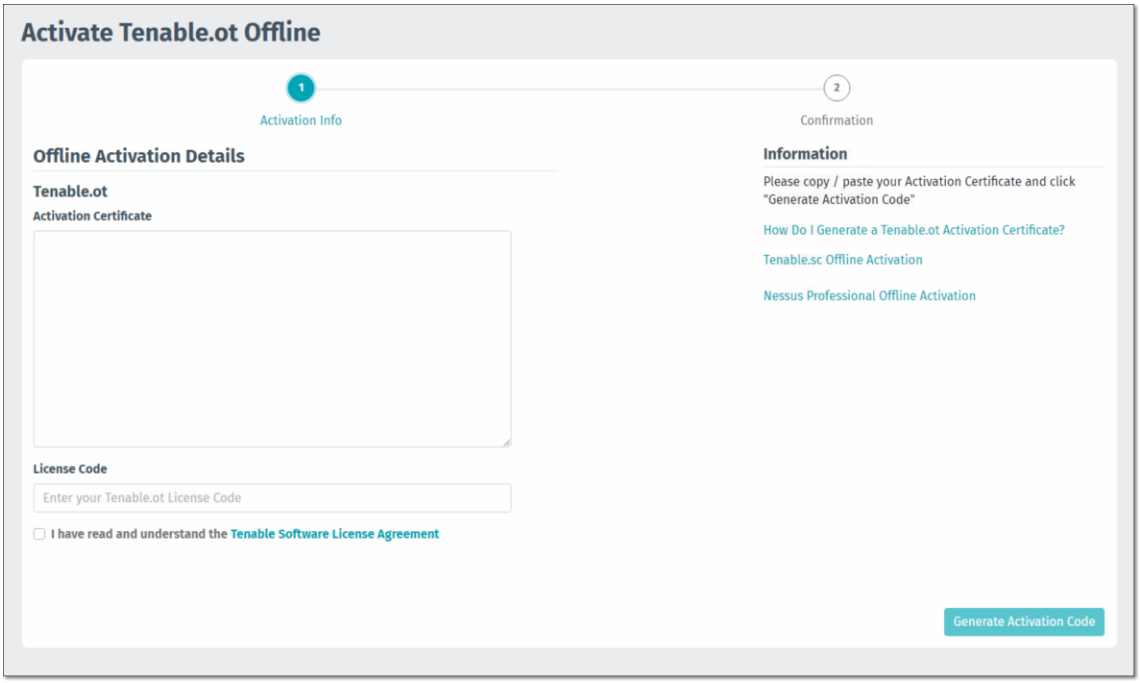


4. Click the **Copy text to clipboard** button, and then click **Done**.
   The side panel closes.

5. In the **(2) Enter activation code** field, click the Self-service portal link.



The **Activate Tenable.ot Offline** screen opens in a new tab.

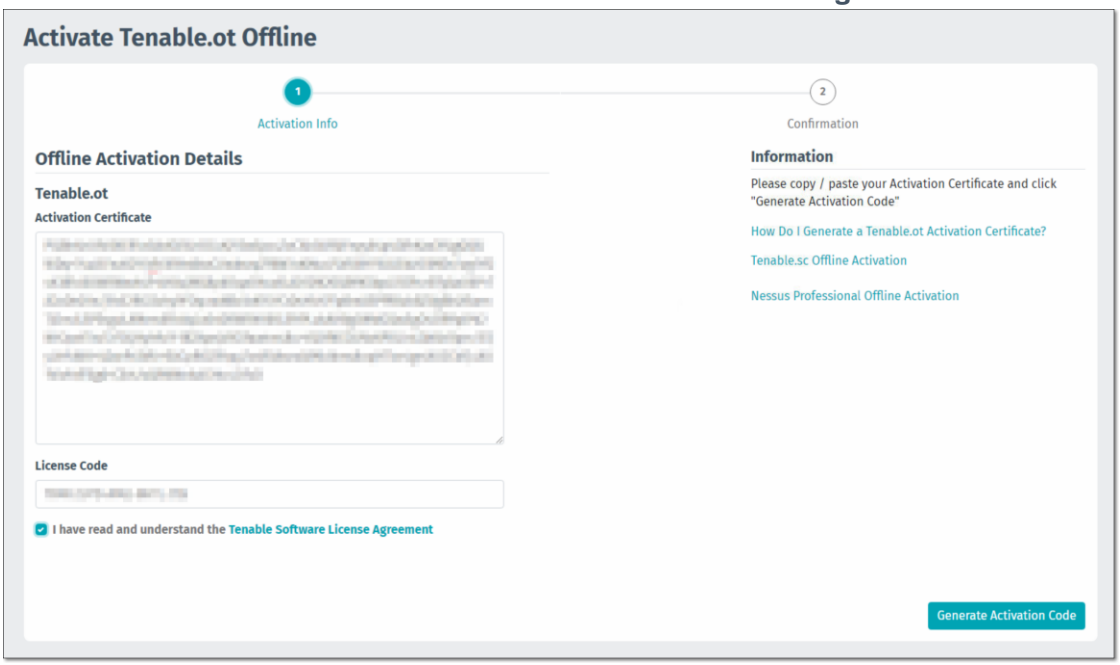


You will need to access the Activate Tenable.ot Offline screen from an Internet-connected device using the following URL: https://provisioning.tenable.com/activate/offline/tenable-ot.

If you are not currently logged in to tenable.com, you will need to log in using your email address and password. You must use the email account where you received your License

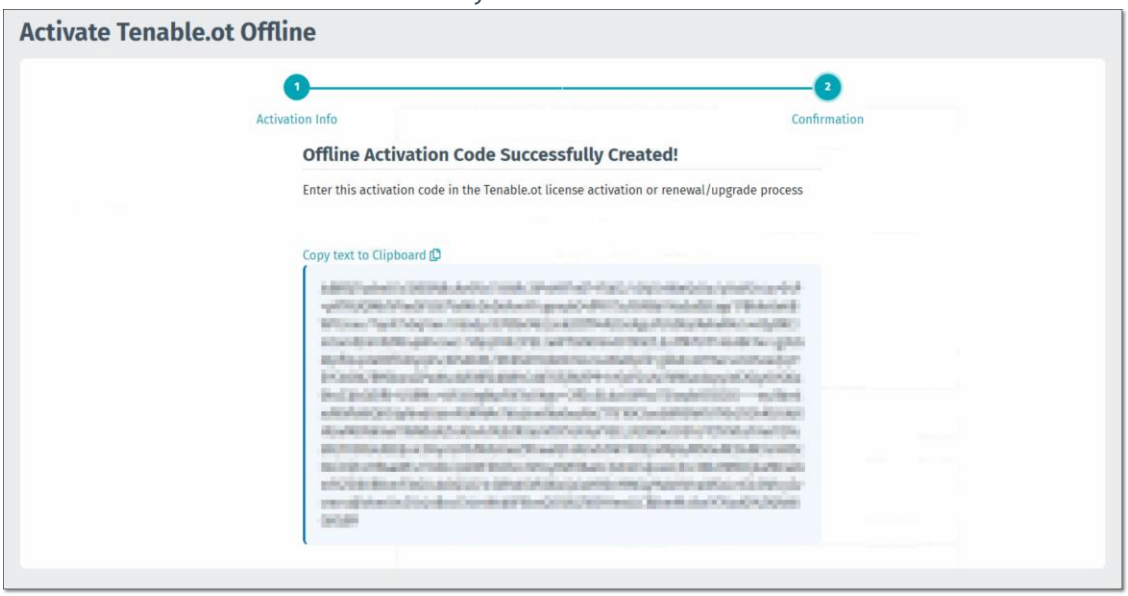
	Code. If you don't have login credentials, you can either click on **Don't remember your password** (and follow the prompts) or reach out to your Tenable account manager .

6. In the **Activation Certificate** field, enter the Activation Certificate.
7. In the **License Code** field, enter your 20-character **License Code** (which can be copied and pasted from the **License** screen).
8. Click the **I have read and understand the Tenable Software License Agreement** checkbox.

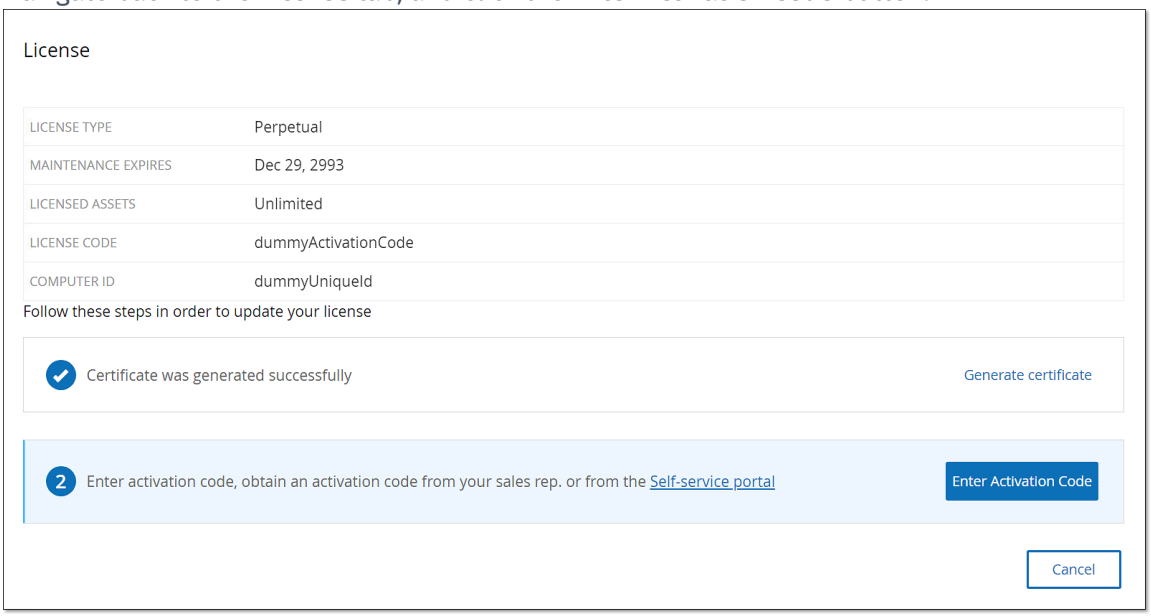


	To view the license agreement, click on the **Tenable Software License Agreement** link.

9. Click the **Generate Activation Code** button.
   The Offline Activation Code Successfully Created! screen is shown.

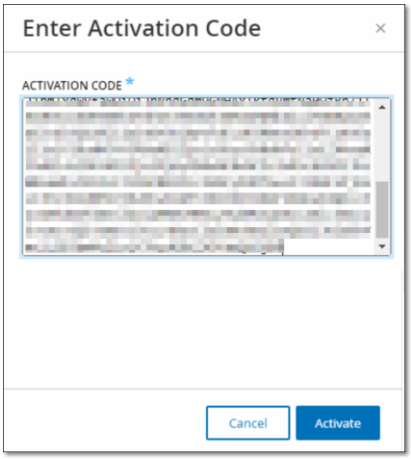


10. Click **Copy text to Clipboard**.
11. Navigate back to the **License** tab, and click the **Enter Activation Code** button.



The **Enter Activation Code** side panel is shown.

12. In the **Activation Code** field, paste your activation code and click the **Activate** button.



The side panel closes, and the license is updated.

Reinitializing the License

Reinitializing your license removes your current license from the system and activates a new license, similar to the license activation during your system startup. If you need to reinitialize your license (i.e., you have been issued a new license) use the following procedure.

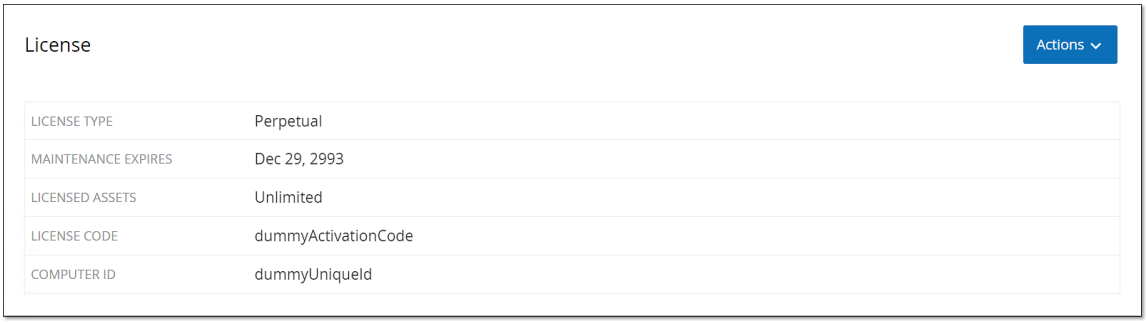
Prerequisites

- Your Tenable account manager must have already issued your new license in their system and provided you with a License Code (20 characters letter/numbers).
- You need access to the Internet. If your Tenable.ot device is not connected to the Internet, you can register the license from any PC.

Reinitializing a License

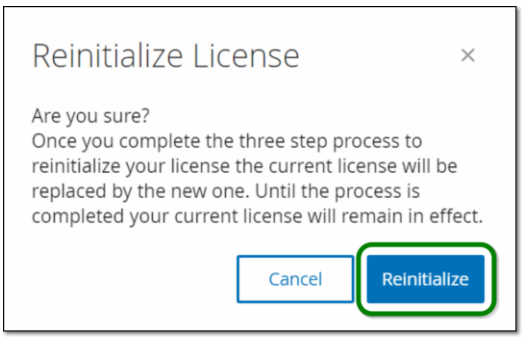
➡ **To Reinitialize Your License:**

1. Under **Local Settings**, go to **System Configuration** > **License**.

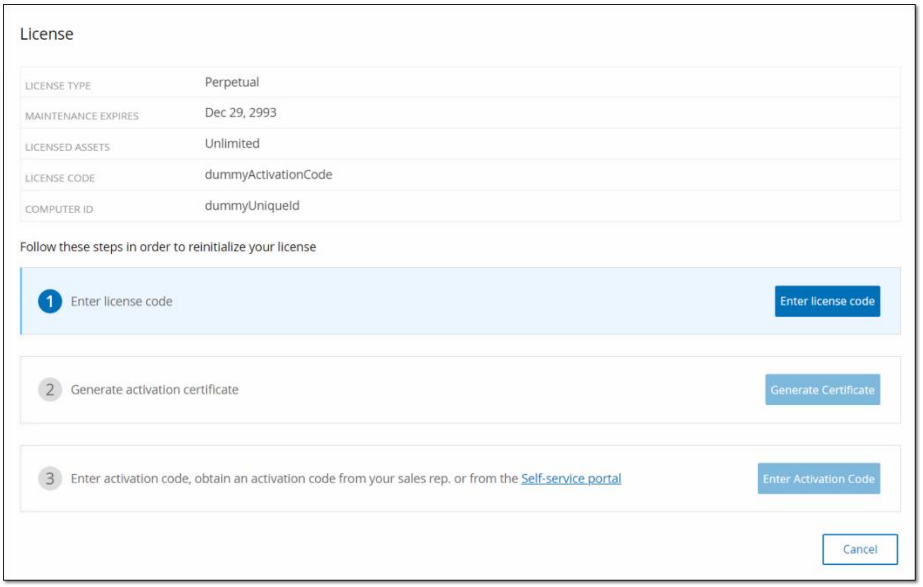


Click on the **Actions** button and select **Reinitialize license**.
A confirmation window is shown.

2. Click **Reinitialize**.



The **License** screen is shown with the three reinitialization steps.



3. Follow the system startup steps for activating your license. See **ACTIVATING YOUR LICENSE**. After entering your Activation Code, your current license will be replaced by your new license.

Licensing Calculation

Licenses for Tenable accounts are calculated based on the number of unique IPs in the system. Each IP requires a separate license. So, even if more than one device shares the same IPs (e.g., multiple devices connected to the same backplane that share the same three IPs), the licenses will still be based on the number of IPs, in this case 3 licenses, regardless of the number of devices.

Environment Configuration

Asset Settings

Adding Assets Manually

To better track your inventory, you may want to view some additional assets you possess, even though these assets were not yet detected by Tenable.ot. You can manually add these assets to your inventory by downloading and editing a CSV file, and then uploading the file to the system.

Users can only upload assets with IPs that are not already in use by an existing asset in the system. In the event that the system detects an asset communicating over the network with the same IP, it will use the information retrieved about the detected asset and overwrite the previously uploaded information. The system will begin handling the asset as a regular one when it is detected communicating in the network.

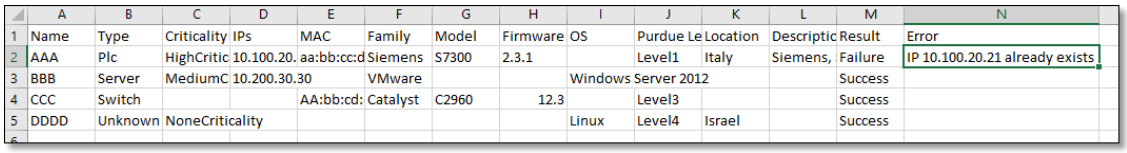
The IP addresses of uploaded assets are counted as part of the system licensing.

Uploaded assets will display a Risk score of 0 until they are detected by the system.

When assets are added manually, Events aren't detected for those Assets until Tenable.ot detects their communication in the network.

To add assets manually:

1. Under **Local Settings**, go to **Environment Configuration** > **Asset Settings**.
   The **Asset Settings** screen is displayed.
2. In **Add Assets Manually**, click on the **Actions** button and select **Download CSV template**.
3. The tot_Assets template document is downloaded.
4. Open the tot_Assets template document.
5. Edit the tot_Assets template precisely in accordance with the instructions found in the file, leaving only the column headers (Name, Type, etc.) and the values you enter.
6. Save the edited file.
7. Return to the **Assets Settings** screen.
8. Click on the **Actions** button, select **Upload CSV**, and navigate to and open the desired CSV file to upload it.
9. In **Add Assets Manually,** click **Download Report**.
   A CSV file with report is displayed, showing successes and failures in the Result column. Details of errors are shown in the Error column.



	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	

Event Clusters

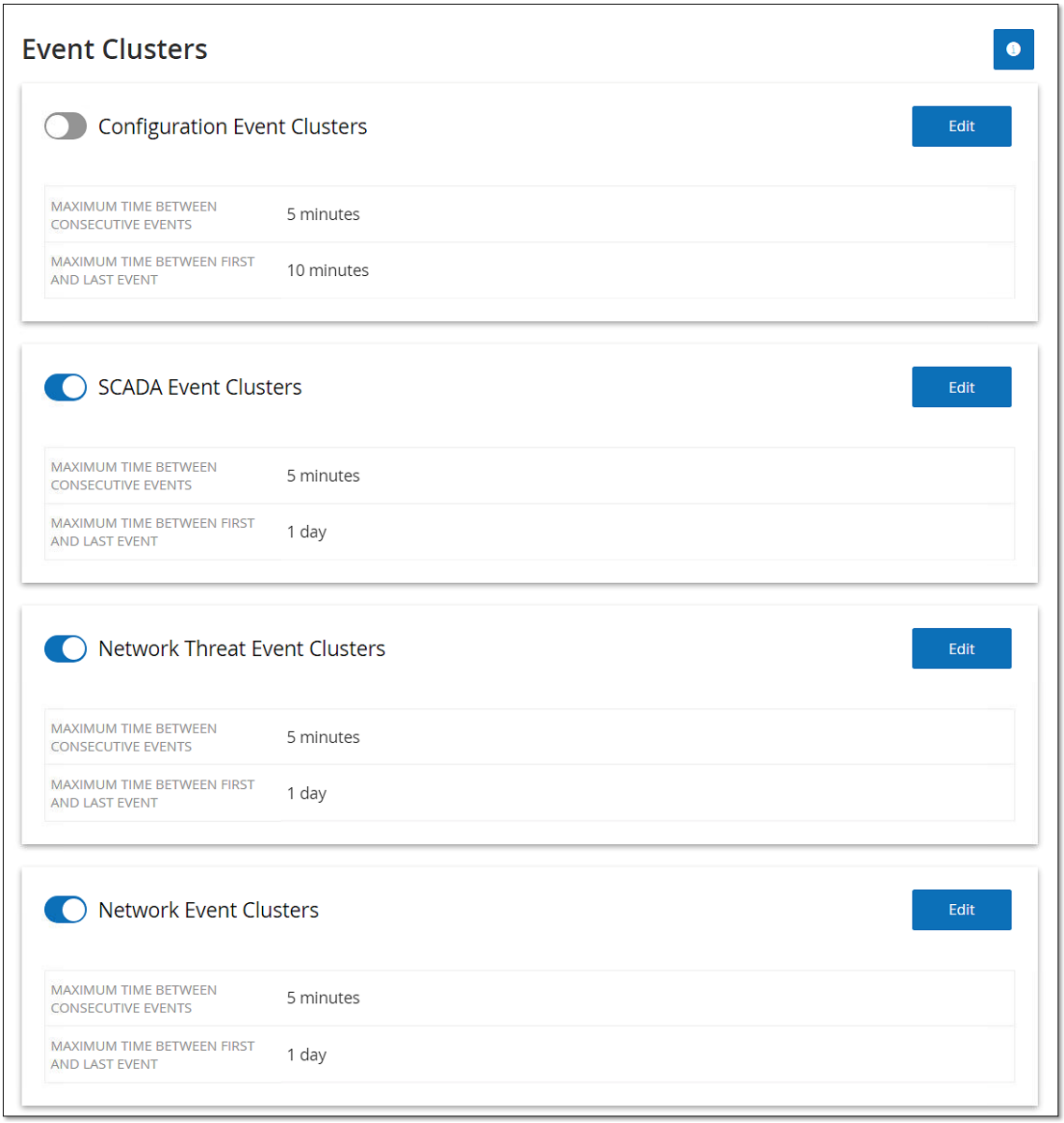
To facilitate the monitoring of events, multiple events with the same characteristics are clustered together into a single cluster. The clustering is based on event type (i.e., share the same policy), source and destination assets, etc.

For events to be clustered, they must be generated within the following configured time intervals:

- **Maximum time between consecutive events** - sets the maximal time interval between events. If this time passes, the consecutive events will not be clustered.
- **Maximum time between the first and last event** - sets the maximal time interval for all events to be shown as a cluster. An event that is generated after this time interval will not be part of the cluster.

To enable clustering:

1. Under **Local Settings**, go to **Environment Configuration** > **Event Clusters**.
   The **Event Clusters** screen is displayed.



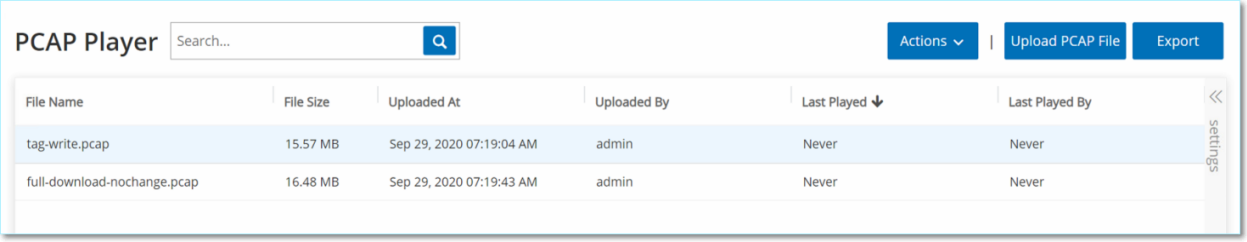
2. Click on the toggle to enable desired categories for clustering.
3. To configure the time intervals for a category, click on the **Edit** button.
   The **Edit Configuration** window is displayed.

4. Enter the desired number value in the number field and adjust the unit of time using the drop-down list.

> For more information about clustering and time intervals, click on the button.

5. Click **Save**.

PCAP Player



Tenable.ot enables you to upload a PCAP file containing recorded network activity and "play" it on Tenable.ot. When you "play" a PCAP file, Tenable.ot monitors the network traffic and records all information about detected assets, network activity and vulnerabilities as if the traffic had occurred within you network. This feature can be used for simulation purposes or in order to analyze traffic that occurs outside of the network that is monitored by your Tenable.ot deployment (e.g. remote plants).

> The following file types are supported for this feature: .pcap, .pcapng, .pcap.gz, .pcapng.gz. You can use files that were recorded by an instance of Tenable.ot or other network monitoring tools.

Uploading a PCAP File

To upload a PCAP file:

1. Under **Local Settings**, go to **Environment Configuration** > **PCAP Player**.
2. Click **Upload PCAP File**.
   The File Explorer opens.
3. Select the desired PCAP recording.
4. Click **Open**.
   The PCAP file is uploaded to the system.

Playing a PCAP File

To play a PCPAP file:

1. Under **Local Settings**, go to **Environment Configuration** > **PCAP Player**.
2. Select the PCAP recording you would like to play.
3. Click **Actions** > **Play**.
4. The **Play PCAP** wizard is displayed.
5. In the **Play Speed** field, select from the drop-down list the speed you would like the system to play the file. Options are: *1X*, *2X*, *4X*, *8X* or *16X*.

Playing a PCAP file injects data into the system, this operation cannot be undone or stopped once executed.

6. Click **Play**.
   The PCAP file is "played" in the system. All network activity in the PCAP file is registered in the system and assets identified by the system are added to the assets inventory.

You cannot play another PCAP file while a file is still playing.

Users and Roles

Access to the Tenable.ot Console (UI) is controlled by user accounts which designate the permissions that are available for that user. The user's permissions are determined by the User Group/s to which they are assigned. Each User Group is assigned a role which defines the set of permissions that will be available for its members. So, for example, if the *Site Operators* User Group has the role *Site Operator*, then all users assigned to that group will have the set of permissions associated with the *Site Operator* role.

The system comes with a set of pre-defined User Groups, which correspond to each of the available roles, *Administrators* User Group > *Administrator* role, *Site Operators* User Group > *Site Operator* role etc. You can also create custom User Groups and specify their roles.

There are three methods for creating users in the system:

- **Adding Local Users**– Create user accounts to authorize individual users to access the system. Assign users to User Groups which define their roles.
- **Active Directory** - Use your organization's Active Directory to authorize users to access the system. You can assign Tenable.ot roles based on your existing groups in Active Directory.
- **SAML** – Set up an integration with your Identity Provider (e.g. Azure Active Directory) and assign users to your Tenable.ot application.

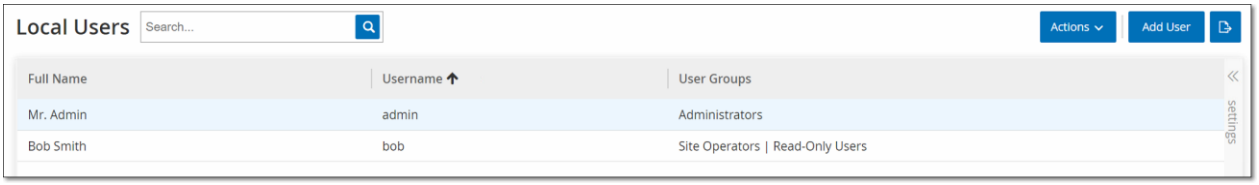
Local Users

An Admin user can create new user accounts and edit existing accounts. Each user is assigned to one or more User Groups which determines the role/s assigned to the user.

Users can be added to User Groups either during the creation/editing of the user's account or the User Group.

Viewing Local Users

The **Local Users** screen shows a list of all local users in the system.



The information shown on this screen is described in the following table:

Parameter	Description
Full Name	The full name of the user.
Username	The username of the user, used for login.
User Groups	The User Group/s to which the user is assigned.

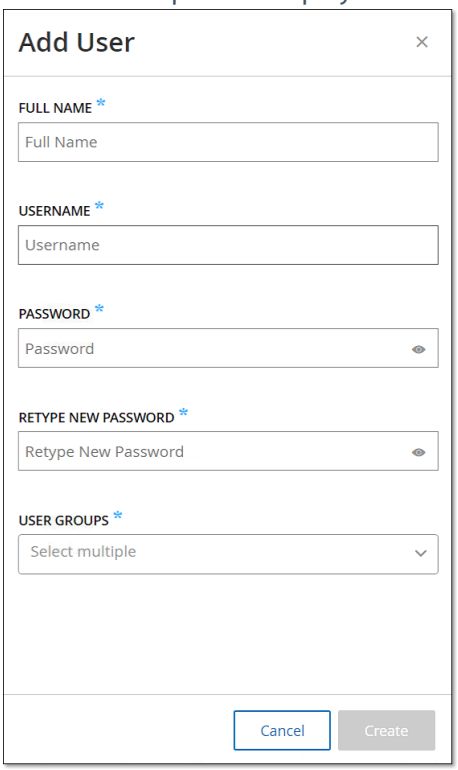
Adding Local Users

You can create user accounts to authorize individual users to access the system. Each user must be assigned to one or more User Groups.

➡ **To Create a User Account:**

1. Under **Local Settings**, go to the **User Management** > **Local Users** screen

2. Click on the **Add User** button.
   The **Add User** pane is displayed.



3. In the **Full Name** field, enter the first and last name.

> The name that you enter is displayed in the header bar when the user is signed in.

4. In the **Username** field, enter a user name to be used for logging in to the system.
5. In the **Password** field, enter a password.
6. In the **Retype Password** field, enter the identical password.

> This is the password that the user will use for the initial login. The user can change the password in the Settings screen after logging into the system.

7. Click on the **User Groups** field and select the checkbox for each User Group to which you would like to assign this user.

> The system comes with a set of pre-defined User Groups, which correspond to each of the available roles, *Administrators* User Group > *Administrator* role, *Site Operators* User Group > *Site Operator* role etc. For an explanation of the available roles, see **User Roles**.

8. Click **Create**.
   The new user account is created in the system and is added to the list of users shown in the **Local Users** tab.

Additional Actions on User Accounts

Editing a User Account

You can assign a user to additional User Groups or remove the user from a group.

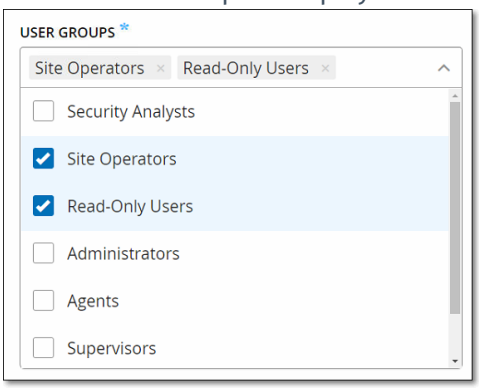
➡ **To change a user's User Groups:**

1. Under **Local Settings**, go to the **User Management** > **Local User** screen.
   The **Local Users** screen is displayed.
2. Right-click on the desired user and select **Edit User** from the menu.

> Alternatively, you can select a user and then click on the Actions button > Edit User.

3. The **Edit User** pane is displayed, showing the User Groups to which the user is assigned.

4. Click on the **User Groups** field.
   A list of User Groups is displayed.



5. Select/deselect the desired User Groups.
6. Click **Save**.

Changing a User's Password

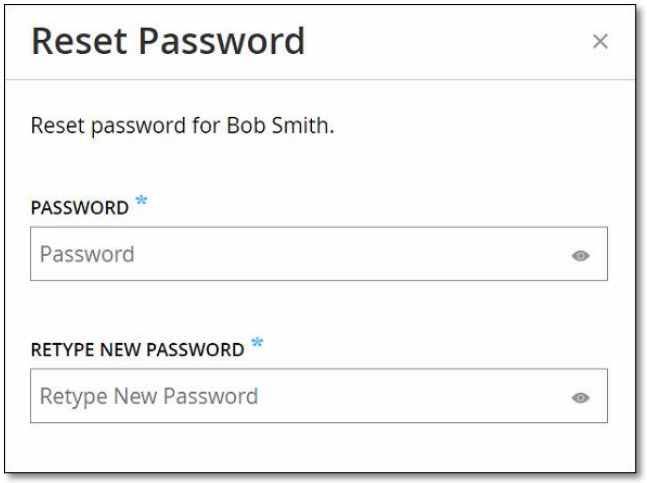
> The procedure described below is used by an admin user to change the password for any account in the system. Any user can change his/her own password by going to Local Settings > User.

To Change a User's Password:

1. Under **Local Settings**, go to the **User Management** > **Local User** screen.
   The **Local Users** screen is displayed.
2. Right-click on the desired user and select **Reset Password** from the menu.

> Alternatively, you can select a user and the click on the Actions button > Reset Password.

The **Reset Password** window is displayed.



3. In the **New Password** field, enter a new password.
4. In the **Retype New Password** field, re-enter the new password.
5. Click **Reset**.
   The new password is applied to the specified user account.

Deleting Local Users

To Delete a User Account:

1. Under **Local Settings**, go to the **User Management** > **Local User** screen.
   The **Local Users** screen is displayed.
2. Right-click on the desired user and select **Delete User** from the menu.

> Alternatively, you can select a user and the click on the Actions button > Delete User.

A confirmation window is displayed.

3. Click **Delete**.
   The user account is deleted from the system.

User Groups

An Admin user can create new User Groups and edit existing groups. Each user is assigned to one or more User Groups which determines the role/s assigned to the user.

The system comes with a set of pre-defined User Groups, which correspond to each of the available roles, *Administrators* User Group > *Administrator* role, *Site Operators* User Group > *Site Operator* role etc. For an explanation of the available roles, see **User Roles**.

Viewing User Groups

The User Groups screen shows a list of all User Groups in the system.

The information shown on this screen is described in the following table:

Parameter	Description
Name	The name of the User Group.
Members	A list of all members assigned to the group.
Role	The role given to this group. For an explanation of the permissions associated with each role, see **User Roles Table**.

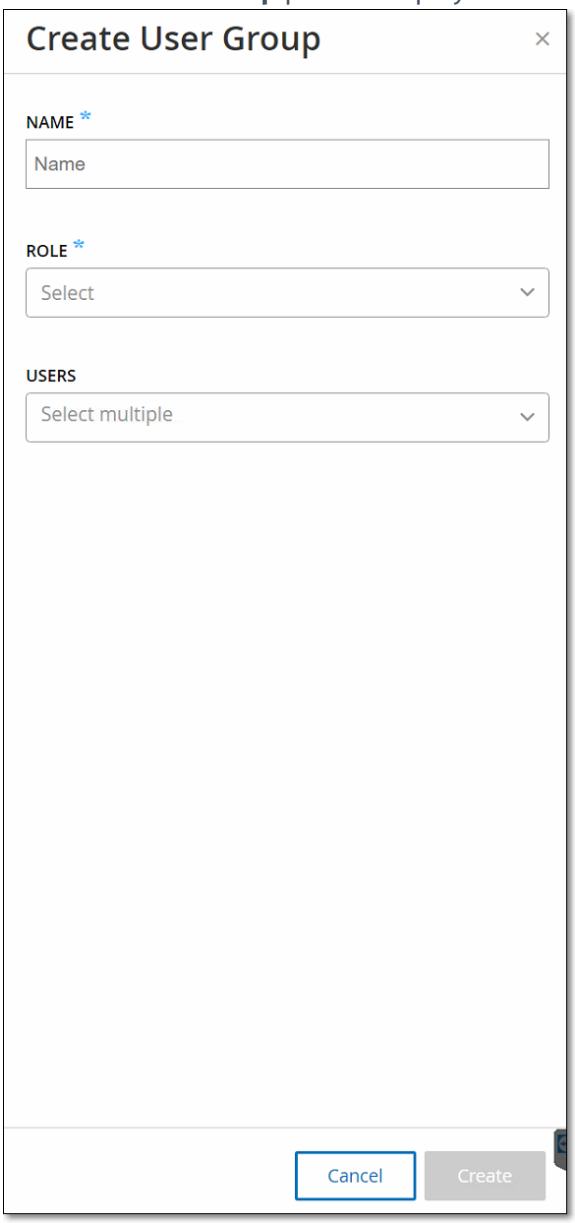
Adding User Groups

You can create new User Groups and assign users to that Group.

➡ **To Create a User Account:**

1. Under **Local Settings**, go to the **User Management** > **User Groups** screen.
   The **User Groups** screen is displayed.

2. Click on the **Create User Group** button.
   The **Create User Group** pane is displayed.



3. In the **Name** field, enter a name for the group.
4. In the **Role** field, select from the dropdown list the role that you would like to assign to this group.
5. In the **Users** field, select from the dropdown list one or more users that you would like to assign to this group.
6. Click **Create**.
   The new User Group is created in the system and is added to the list of groups shown in the **User Groups** screen.

Additional Actions on User Groups

Editing User Groups

You can edit the settings and add or remove members to an existing User Group by editing the Group.

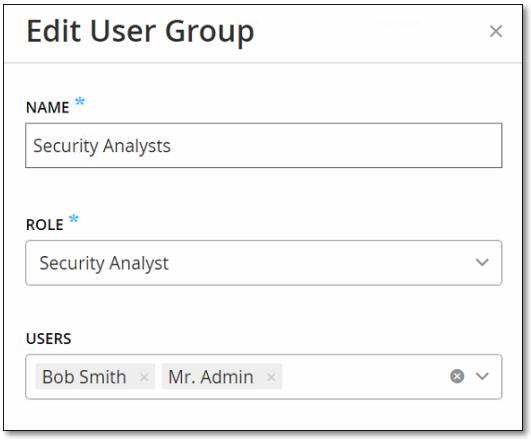
> Alternatively, you can add/remove an individual user to a User Groups by editing the user's profile.

To edit a User Group:

1. Under **Local Settings**, go to the **User Management** > **User Groups** screen.
   The **User Groups** screen is displayed.
2. Right-click on the desired user and select **Edit User Group** from the menu.

> Alternatively, you can select a user and the click on the Actions button > Edit User Group.

3. The **Edit User Groups** pane is displayed, showing the group's settings.
4. You can change the **Name** and **Role**. You can also select/deselect **Users** to add/remove Users to the group.



5. Click **Save**.

Deleting User Groups

> You can only delete a User Group that does not currently have users assigned to it. If users are assigned to a group, you will need to first remove the users from the group before you can delete the group.

To Delete a User Group:

1. Under **Local Settings**, go to the **User Management** > **User Groups** screen.
   The **User Groups** screen is displayed.

2. Right-click on the desired User Group and select **Delete User Group** from the menu.
A confirmation window is displayed.

> Alternatively, you can select a user and the click on the **Actions** button > **Delete User Group**.

3. Click **Delete**.
The User Group is deleted from the system.

User Roles

The following is a brief description of the available roles:

- **Administrator** – Has maximum privileges to do all operational as well as administrative tasks in the system, including creating new user accounts.
- **Read-Only** – Can view data (asset inventory, events, network traffic) but can't take action in the system.
- **Security Analyst** – Can view data in the system and resolve security events.
- **Security Manager** – Can manage security related capabilities, including configuring policies, viewing data in the system, and resolving events.
- **Site Operator** – Can view data in the system and manage the asset inventory.
- **Supervisor** – Has full privileges to do all operational tasks in the system as well as some limited administrative tasks (excluding creating new users and other sensitive activities).

User Roles Table

The following table gives a detailed breakdown of precisely which permissions are enabled for each role.

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Events							
View events	✓	✓	✓	✓	✓	✓	✓
Resolve	✓	✓	✓	✓	✓	X	X
Download capture file	✓	✓	✓	✓	✓	✓	✓
Exclude from policy	✓	✓	✓	✓	X	X	X
Resolve all	✓	✓	✓	✓	✓	X	X
Export	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Create Policy on FortiGate	✓	✓	✓	✓	X	X	X
Refresh	✓	✓	✓	✓	✓	✓	✓
Policies							
View policies	✓	✓	✓	✓	✓	✓	✓
Enable/Disable	✓	✓	✓	✓	X	X	X
View action	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✓	X	X	X
Duplicate	✓	✓	✓	✓	X	X	X
Delete	✓	✓	✓	✓	X	X	X
Create policy	✓	✓	✓	✓	X	X	X
Export	✓	✓	✓	✓	✓	✓	✓
Assets							
View assets	✓	✓	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	X	X	✓	X
Delete	✓	✓	✓	X	X	✓	X
Import (upload new assets by csv)	✓	✓	✓	X	X	✓	X
Hide	✓	✓	✓	X	X	✓	X
Export	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Resync	✓	✓	✓	✓	✓	✓	X
Nessus scan	✓	✓	✓	✓	✓	✓	X
Take snapshot (single asset)	✓	✓	✓	✓	✓	✓	X
Update open ports (single asset)	✓	✓	✓	✓	✓	X	X
Update port state (single asset)	✓	✓	✓	✓	✓	X	X
View in browser (single asset)	✓	✓	✓	✓	✓	✓	✓
View in main asset map (single asset)	✓	✓	✓	✓	✓	✓	✓
Generate attack vector (single asset)	✓	✓	✓	✓	✓	✓	✓
Vulnerabilities (Plugins)							
View plugin hits	✓	✓	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓	✓	✓
Edit comment	✓	✓	✓	✓	✓	X	X
Update plugin set	✓	✓	✓	✓	X	X	X
Export	✓	✓	✓	✓	✓	✓	✓
Network							
Turn on packet capture	✓	✓	✓	X	X	X	X

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Close ongoing captures	✓	✓	✓	✓	✓	✓	X
Download PCAP file	✓	✓	✓	✓	✓	✓	✓
Export conversations table	✓	✓	✓	✓	✓	✓	✓
Set as baseline	✓	✓	✓	✓	X	X	X
Generate map	✓	✓	✓	✓	✓	✓	✓
Refresh map	✓	✓	✓	✓	✓	✓	✓
Groups							
View groups	✓	✓	✓	✓	✓	✓	✓
View action	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✓	X	X	X
Duplicate	✓	✓	✓	✓	X	X	X
Delete	✓	✓	✓	✓	X	X	X
Create group	✓	✓	✓	✓	X	X	X
Export	✓	✓	✓	✓	✓	✓	✓
Report							
View reports	✓	✓	✓	✓	✓	✓	✓
Generate	✓	✓	✓	✓	✓	✓	✓
Download	✓	✓	✓	✓	✓	✓	✓
Export	✓	✓	✓	✓	✓	✓	✓

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
Network Segments							
View Network Segments	✓	✓	✓	✓	✓	✓	✓
Edit	✓	✓	✓	✓	X	X	X
Delete	✓	✓	✓	✓	X	X	X
Create	✓	✓	✓	✓	X	X	X
Export	✓	✓	✓	✓	✓	✓	✓
Learn More	✓	✓	✓	✓	✓	✓	✓
Local Settings							
Queries	✓	✓	✓	X	X	X	X
System Configuration - Device Details	✓	✓	✓	X	X	X	X
System Configuration - Sensors	✓	✓	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)	✓ (No Actions)
System Configuration – Port Configuration	✓	✓	✓	X	X	X	X
System Configuration - Updates	✓	✓	✓	X	X	X	X
System Configuration - Certificate (HTTPS)	✓	✓	X	X	X	X	X
System Configuration - API Keys	✓	X	✓ (Only Local Users)	✓ (Only Local Users)	✓ (Only Local Users)	✓ (Only Local Users)	✓ (Only Local Users)

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
System Configuration - License	✓	✓	X	X	X	X	X
Environment Configuration - Asset Settings	✓	✓	✓	X	X	X	X
Environment Configuration - Hidden Assets	✓	✓	✓	✔ - no restore	✔ - no restore	✓	✔ - no restore
Environment Configuration - Custom Fields	✓	✓	✓	X	X	X	X
Environment Configuration - Event Clusters	✓	✓	✓	X	X	X	X
Environment Configuration - PCAP Player	✓	✓	✓	X	X	X	X
Users and Roles - User Settings	✓	✓	✓	X	X	X	X
Users and Roles - Local Users	✓	X	X	X	X	X	X
Users and Roles - User Groups	✓	X	X	X	X	X	X
Users and Roles - Active Directory	✓	X	X	X	X	X	X
Integrations	✓	✓	X	X	X	X	X
Servers	✓	✓	✓	✔ (No Actions)	✔ (No Actions)	✔ (No Actions)	✔ (No Actions)
System Actions	✓	✔ - without factory reset	✔ - only backup	✔ - only diagnostics	X	X	X

Permission	Admin (Local)	Admin (External/AD)	Supervisor	Security Manager	Security Analyst	Site Operator	Read only
			and diagnostics				
System log	✓	✓	✓	✓	✓	✓	✔ - no syslog
Enable (on setup and after disable)	✓	✓	X	X	X	X	X
Delete Assets	✓	✓	✓	X	X	X	X

Active Directory

You can integrate Tenable.ot with your organization's Active Directory. This enables users to log in to Tenable.ot using their Active Directory credentials. The configuration involves setting up the integration and then mapping groups in your AD to User Groups in Tenable.ot.

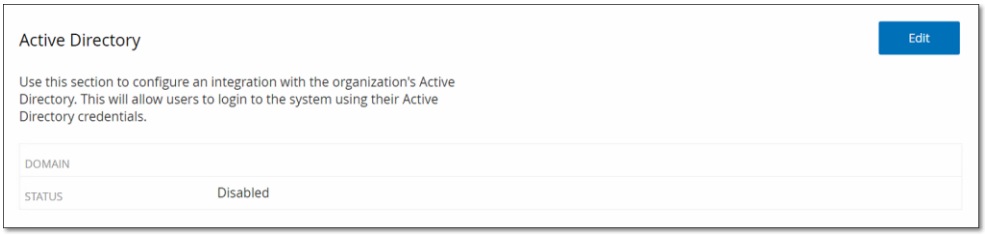
The system comes with a set of pre-defined User Groups, which correspond to each of the available roles, *Administrators* User Group > *Administrator* role, *Site Operators* User Group > *Site Operator* role etc. For an explanation of the available roles, see **User Roles**.

➡ **To configure Active Directory:**

1. **Optionally**, you can obtain a CA Certificate from your organization's CA or Network Administrator and load it onto your local machine.

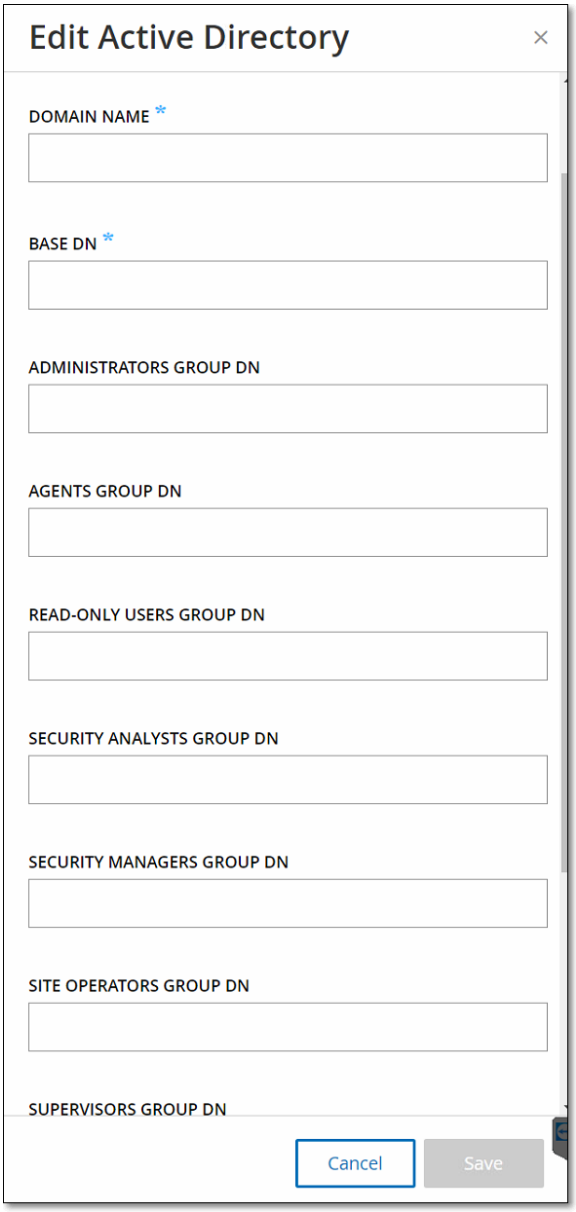
A certificate is not mandatory for this process.

2. Under **Local Settings**, go to the **User Management** > **Active Directory** screen.
The **Active Directory** screen is displayed.



3. Click **Edit**.

4. The **Edit Active Directory** pane is displayed.



5. In the **Domain Name** field, enter the FQDN of the organizational domain (e.g. company.com).

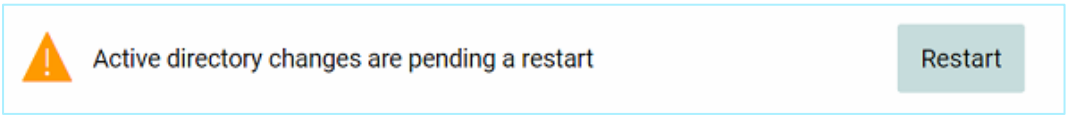
> If you are not aware of your Domain Name, you can find it by entering the command "set" in Windows CMD/Command Line. The value given for the "USERDNSDOMAIN" attribute is the Domain Name.

6. In the **Base DN** field, enter the distinguished name of the domain. The format for this value is 'DC={second-level domain},DC={top-level domain}' (e.g. DC=company,DC=com).
7. For each of the Groups that you would like to map from an AD group to a Tenable.ot User Group, enter the DN of the AD group in the appropriate field. For example, to assign a group of users to the Administrators User Group, enter the DN of the Active Directory group to which you would like to assign Admin privileges in the **Administrators Group DN** field.

If you are not aware of the DN of the group that you would like to assign Tenable.ot privileges, you can view a list of all groups configured in your Active Directory which contain users by entering the command “dsquery group -name Users*” in the Windows CMD/Command Line. The name of the group that you would like to assign should be entered into the field in the identical format in which it is shown (e.g. "CN=IT_Admins,OU=Groups,DC=Company,DC=Com"). The Base DN must be also be included at the end of each DN.

These fields are not mandatory. If a field is not filled in then no AD users will be assigned to that User Group. You can set up an integration with no groups mapped, but in that case no users will be able to access the system until you add at least one group mapping.

8. In the **Trusted CA** section, click **Browse** and navigate to the file that contains your organization's CA Certificate (which you obtained from you CA or Network Administrator). (Optional)
9. Select the **Enable Active Directory** checkbox.
10. Click **Save**.
    A pop-up window prompts you to restart the unit in order to activate the Active Directory.



11. Click **Restart**.
    The unit restarts. Upon reboot, the Active Directory settings will be activated. Any user assigned to the designated groups can access the Tenable.ot platform using his/her organizational credentials.

To log in using Active Directory, the User Principal Name (UPN) should be used on the login page. In some cases, this means simply adding @<domain>.com to the username.

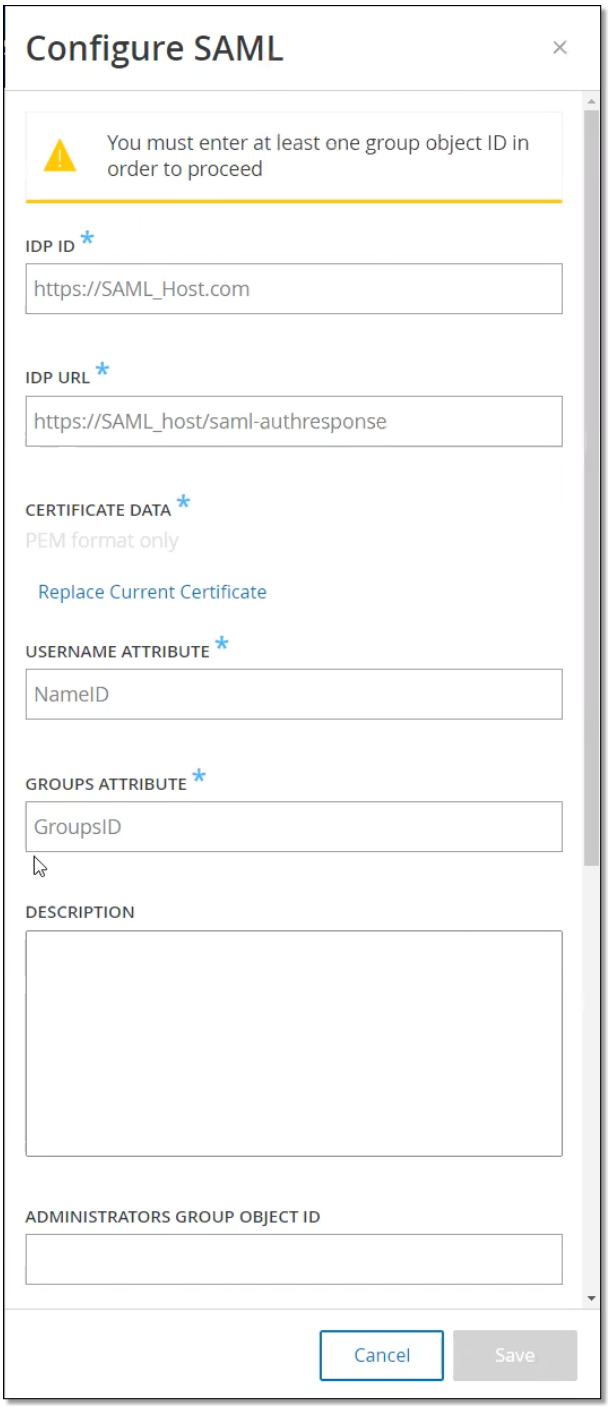
SAML

You can integrate Tenable.ot with your organization's identity provider (e.g. Microsoft Azure). This enables users to authenticate via their identity provider. The configuration involves setting up the integration by creating a Tenable.ot application within your identity provider, entering information about your created Tenable.ot application and uploading your identity provider’s Certificate to the Tenable.ot SAML page, and then mapping groups from your identity provider to User Groups in Tenable.ot. For a detailed tutorial for integrating Tenable.ot with Microsoft Azure, see **Appendix 2 – SAML Integration for Azure Active Directory**.

➡ **To configure SAML:**

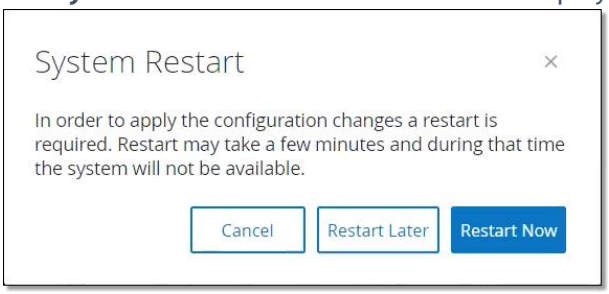
1. Under **Local Settings**, go to the **Users and Roles** > **SAML** screen.

2. Click **Configure.**
   The **Configure SAML** side panel is displayed.



3. In the **IDP ID** field, enter the Identity Provider's ID for the Tenable.ot application.
4. In the **IDP URL** field, enter the Identity Provider's URL for the Tenable.ot application.
5. Under **Certificate Data**, click **Replace Current Certificate**, navigate to the Identity Provider's Certificate file you downloaded for use with the Tenable.ot application and open it.

6. In the **Username Attribute** field, enter the username attribute from the Identity Provider for the Tenable.ot application.
7. In the **Groups Attribute** field, enter the groups attribute from the Identity Provider for the Tenable.ot application.
8. Enter a description in the **Description** field. (Optional)
9. For each group mapping that you would like to configure, access the Identity Provider's **Group Object ID** for a group of users and enter it into the desired **Group Object ID** field to map it to the desired Tenable.ot User Group.
10. Click **Save** to save and close the side panel.
11. On the **SAML** screen, click to toggle the **SAML single sign on login** button **ON**.
    The **System Restart** notification window is displayed.



12. Click **Restart Now** to restart the system and apply the SAML configuration immediately, or click **Restart Later** to delay the application of the SAML configuration the next time the system is restarted. If you choose to restart later, the following banner is shown until the restart is done:

    Upon reboot, the settings will be activated, and any user assigned to the designated groups can access the Tenable.ot platform using their Identity Provider credentials.

Integrations

You can set up integrations with other supported platforms in order to enable Tenable.ot to sync with your other cyber security platforms.

Tenable Products

You can integrate Tenable.ot with Tenable.sc and Tenable.io. This enables Tenable.ot to share data with the other platforms. The synced data includes OT vulnerabilities as well as data discovered by IT-type Nessus scans initiated from Tenable.ot.

	In order integrate the platforms, Tenable.ot must be able to reach Tenable.sc and/or Tenable.io via port 443. It is recommended to create a specific user on Tenable.sc and/or Tenable.io to be used as the integration user to Tenable.ot.

Tenable.sc

To integrate Tenable.sc, create a new agent repository for Tenable.ot data. Take note of the repo ID. In the Tenable.ot, create a new integration, filling in IP or Hostname of your Tenable.sc system as well as your account credentials and repository ID, and then set the sync frequency. Then, right-click on the newly added integration and hit "Sync".

It is recommended to create a specific user on Tenable.sc that will be used to integrate with Tenable.ot. The user should have the role of *Security Manager/Security Analyst* or *Vulnerability Analyst* and be assigned to the "Full Access" group.

Tenable.io

To integrate with Tenable.io, enter your Access Key and Secret Key, and then set the sync frequency.

You need to first generate an API key in the Tenable.io console (Settings > My Account > API Keys > Generate). You will be given an Access Key and a Secret Key which you enter in the Tenable.ot console when configuring the integration.

Palo Alto Networks - Next Generation Firewall

You can share asset inventory info discovered by Tenable.ot with your Palo Alto system.

To integrate Tenable.ot with your Palo Alto NGFW, fill in the IP or Hostname of your Palo Alto NGRW as well as the credentials for accessing your NGRW account.

Aruba - ClearPass Policy Manager

You can share asset inventory info discovered by Tenable.ot with your Aruba system.

To integrate Tenable.ot with your Aruba ClearPass system, fill in the IP or Hostname of your Aruba ClearPass system as well as the credentials for accessing your Aruba ClearPass account.

Servers

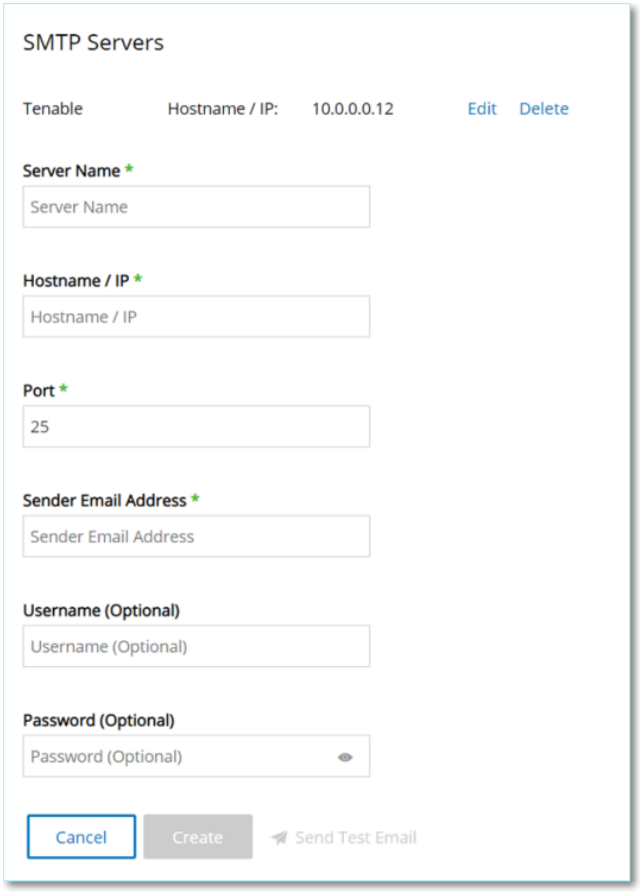
You can set up SMTP servers and Syslog servers in the system to enable Event notifications to be sent via email and/or logged on an SIEM. You can also set up FortiGate firewalls to send firewall policy suggestions to FortiGate based on the Tenable.ot network events.

SMTP Servers

In order to enable sending Event notifications via email to the relevant parties you will need to set up an *SMTP Server* in the system. If you do not set up an SMTP server, the Events generated by the system can't be sent out by email. Under any circumstances, all Events can be viewed in the Management Console (UI) on the Events screen.

To Set up an SMTP Server:

1. Under **Local Settings**, go to the **Servers** > **SMTP Servers** screen.
2. Click **Add SMTP Server**.
   The **SMTP Servers** configuration window is displayed.



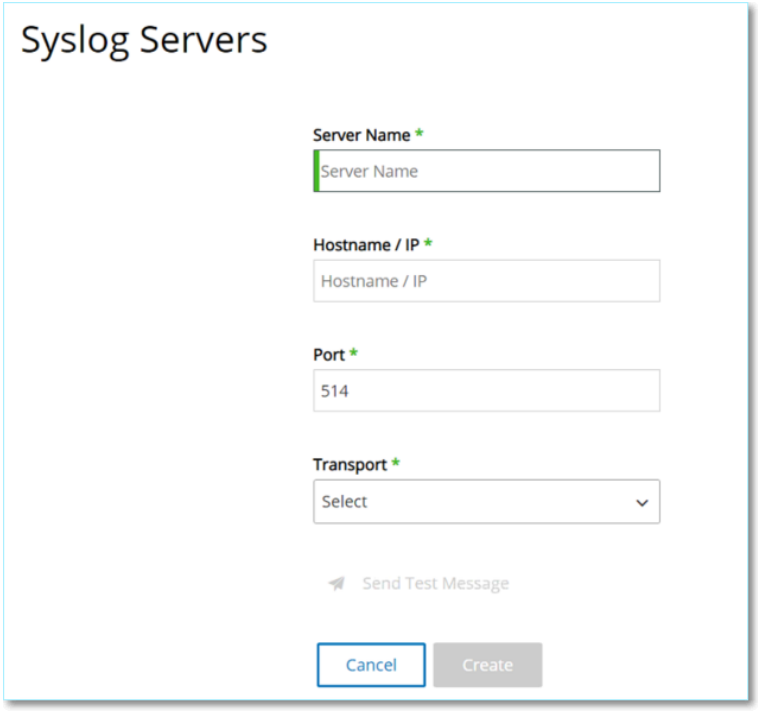
3. In the **Server Name** field, enter the name of an SMTP server to be used for email notifications.
4. In the **Hostname\IP** field, enter a host name or an IP address of the SMTP server.
5. In the **Port** field, enter the port number on which the SMTP server will listen for the Events (Default: 25).
6. In the **Sender Email Address** field, enter an email address that is shown as the sender of the Event notification email.
7. In the **User Name** and **Password** fields, enter a user name and password that will be used to access the SMTP server. These fields are optional.
8. At this point you can try to send a test email to verify that the configuration was successful. Click **Send Test Email**, then enter the email address to send to and check the inbox to see if the email arrived. If the email did not arrive, then troubleshoot to discover the cause of the problem and correct it.
9. Click **Save**.
   You can set up additional SMTP Servers by repeating the procedure described above.

Syslog Servers

In order to enable collection of log events on an external server you will need to set up a *Syslog Server* in the system. If you do not want to set up a Syslog Server, then the event logs will only be saved on the Tenable.ot platform.

To Set up a Syslog Server:

1. Under **Local Settings**, go to the **Servers** > **Syslog Servers** screen.
2. Click **+ Add Syslog Server**.
   The **Syslog Servers** configuration window is displayed.

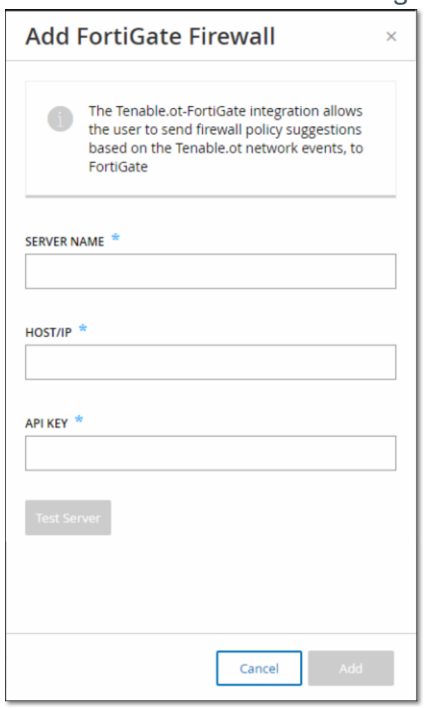


3. In the **Server Name** field, enter the name of a Syslog Server to be used for logging system events.
4. In the **Hostname\IP** field, enter a host name or an IP address of the Syslog server.
5. In the **Port** field, enter the port number on the Syslog server to which the events will be sent. (Default: 514)
6. In the **Transport** field, select from the dropdown list the transport protocol to be used. Options are *TCP* or *UDP*.
7. If you would like to send a test message to verify that the configuration was successful, click **Send Test Message**, and check if the message has arrived. If the message did not arrive, then troubleshoot to discover the cause of the problem and correct it.
8. Click **Save**.
   You can set up additional Syslog Servers by repeating the procedure described above.

FortiGate Firewalls

To Set up a FortiGate Server:

1. Under **Local Settings**, go to the **Servers** > **FortiGate Firewalls** screen.
2. Click the **Add Firewall** button.
   The **Add FortiGate Firewall** configuration window is displayed.



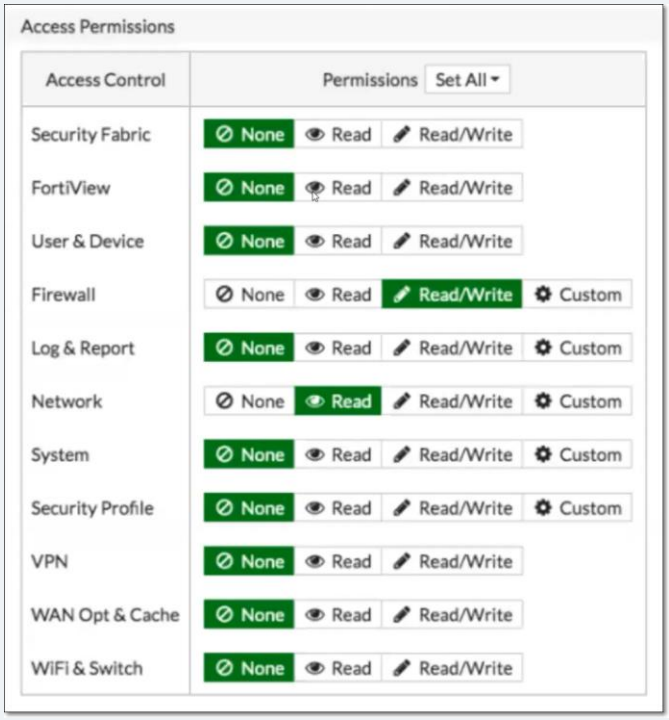
3. In the **Server Name** field, enter the name of a FortiGate Server to be used.
4. In the **Host/IP** field, enter a host name or an IP address of the FortiGate server.
5. In the **API Key** field, enter the **API token** you generated from FortiGate. For more information, see the note below.
6. Click **Add**.
   The FortiGate Firewall Server is created.

The instructions for generating a FortiGate API token can be found on the following page:
https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

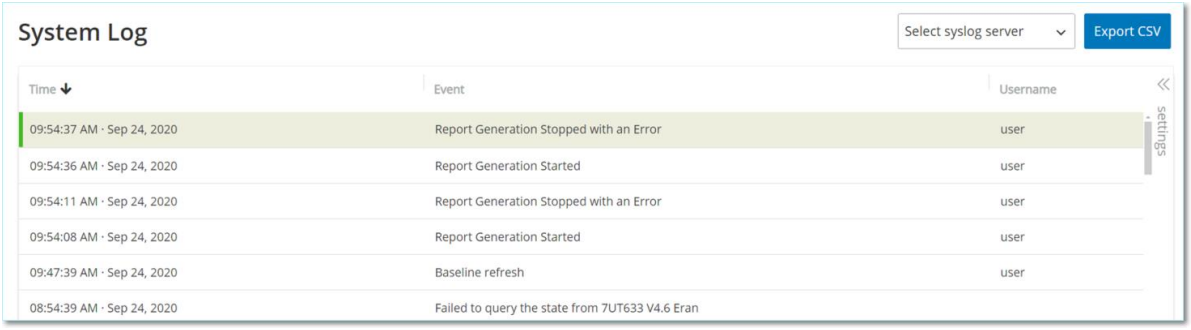
Please note:

- For the source address (which is needed to ensure the API token can only be used from trusted hosts), please use your Tenable.ot unit IP address.

- When creating an Administrator profile for Tenable.ot, make sure to apply access permissions according to the following settings:



System Log



The System Log screen shows a list of all system events (e.g. Policy turned on, Policy edited, Event Resolved etc.) that occurred in the system. This log includes both user-initiated events as well as automatically occurring system events (e.g. Policy turned off automatically because of too many hits). This log does not include Policy generated Events which are shown on the *Events* screen. The logs can be exported as a CSV file. You can also configure the system to send the System Log events to a Syslog server.

The information shown for each logged event is described in the following table:

Parameter	Description
Time	The time and date that the event occurred.
Event	A brief description of the event that occurred.
Username	The name of the user that initiated the event. For events that occur automatically, no username is given.

Sending System Log to a Syslog Server

➡ **To configure the system to send System Events to a Syslog server:**

1. Go to the **Local Settings** > **System Log** screen.
2. In the header bar, click on **Select syslog sever**.
   A dropdown list of servers is displayed.

To add a Syslog server, see **SYSLOG SERVER**.

3. Select the desired server.
   The System Log events will be sent to the specified Syslog server.

Appendix 1 – Installing a Sensor (Version 3.13 and Below)

The following procedure explains the complete flow for configuring a Sensor v. 3.13 and below. Some the initial steps are relevant also for newer sensors. However, the setup wizard has been replaced by the pairing procedure described in **PAIRING THE SENSOR.**

Step 1 - Setting up the Sensor

There are two models of the Sensor, the Rack Mount Sensor and the Configurable Sensor, as described in section **TENABLE.OT SENSOR**. The Rack Mount model can be mounted on a standard 19-inch rack or rested on top of a flat surface. The Configurable model can be installed in a DIN rail or mounted on a standard 19-inch rack (using the “mounting ears” adapter kit).

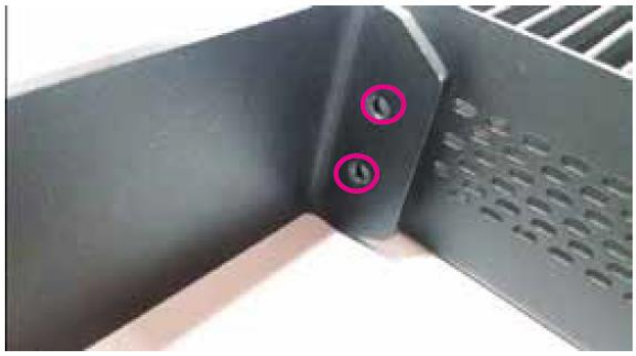
Setting up a Rack Mount Sensor

A Rack Mount Sensor can be mounted on a standard 19-inch rack, or simply rested on top of a flat surface (such as a desktop).

Rack Mounting (for Rack Mount model)

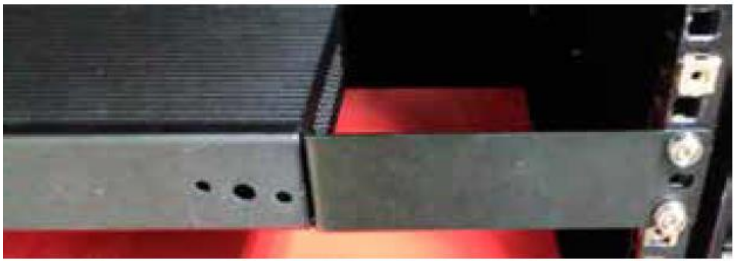
➡ **To mount the Tenable.ot sensor on a standard (19-inch) rack:**

1. Attach the L-shaped brackets to the screw holes on each side of the sensor, as indicated in the image below.



2. Insert two screws on each side and fasten them with a screwdriver to secure the brackets in place.
3. Insert the sensor with the brackets into an available 1U slot in the rack.

4. Secure the unit to the rack by fastening the rack-mount brackets (supplied) to the rack frame, using the appropriate screws for rack mounting (not supplied).



⚠	Make sure that the rack is electrically grounded. Make sure that the cooling fan air intake (located in the back panel) and the air ventilation holes (on the top panel) are not obstructed.

5. Plug in the AC power supply cable (supplied) to the power supply port in the rear panel, then plug the cable to the AC power supply (mains).

Flat Surface

➡ **To install the Tenable.ot sensor on a flat surface:**

1. Place the sensor on a dry, flat, leveled surface (such as a desktop).

⚠	Make sure that the tabletop is flat and dry. Make sure that the cooling fan air intake (located in the back panel) and the air ventilation holes (on the top panel) are not obstructed.

2. If the unit is placed within a stack of other electrical appliances, make sure there is ample space behind the cooling fan (located in the back panel) to allow proper ventilation and cooling.
3. Plug in the AC power supply cable (supplied) to the power supply port in the rear panel, then plug the cable to the AC power supply (mains).

Setting up a Configurable Sensor

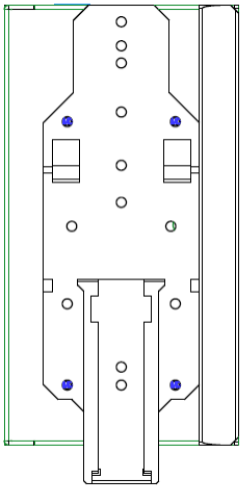
A Configurable Sensor can be mounted on a DIN rail or it can be mounted on a standard 19-inch mounting rack (using the "mounting ears" adapter kit).

DIN Rail Mounting

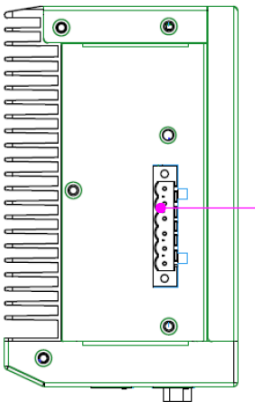
The Configurable Model can be mounted on a DIN Rail using the following procedure.

➡ **To mount the Tenable.ot Configurable Sensor on a standard DIN rail:**

1. Use the bracket, located on the back of the Sensor, to mount the Sensor on to a DIN rail.



2. Connect the power using one of the following methods:
   - **DC Power** - Connect the DC power chord to the Sensor by inserting the 12-36V DC 6-pin Phoenix Contact connector into the side of the Sensor unit and tightening the embedded screws at the top and bottom of the connector. Then, connect the other end of the chord to a DC power source.



   - **AC Power** - Connect the AC power supply to the Sensor by inserting the 12-36V DC 6-pin Phoenix Contact connector into the side of the Sensor unit and tightening the embedded screws at the top and bottom of the connector.

Then, insert the AC power supply cable (provided) into the power supply unit, and plug the other end into an AC outlet.

Rack Mounting (for Configurable model)

A Configurable Sensor can be attached to a mounting rack, using the "mounting ears" that are provided.

➡ **To mount the Configurable Sensor on a standard (19-inch) rack:**

1. Prepare the unit for rack mounting, as follows:
   a. Remove 3 screws from each side of the unit.
   b. Attach the "mounting ears" on both sides of the unit, using new screws (provided).

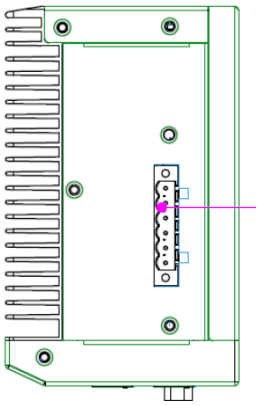
2. Insert the server unit into an available 1U slot in the rack.

⚠	Make sure that the rack is electrically grounded. Make sure that the cooling fan air intake (located in the back panel) and the air ventilation holes (on the top panel) are not obstructed.

3. Secure the unit to the rack by fastening the "mounting ears" to the rack frame using the mounting screws (provided).
3. Connect the power using one of the following methods:

   - **DC Power** - Connect the DC power chord to the Sensor by inserting the 12-36V DC 6-pin Phoenix Contact connector into the side of the Sensor unit and tightening the embedded screws at the top and bottom of the connector. Then, connect the other end of the chord

to a DC power source.



- **AC Power** - Connect the AC power supply to the Sensor by inserting the 12-36V DC 6-pin Phoenix Contact connector into the side of the Sensor unit and tightening the embedded screws at the top and bottom of the connector.

Then, insert the AC power supply cable (provided) into the power supply unit, and plug the other end into an AC outlet.

Step 2 – Connecting the Sensor to the Network

Tenable.ot Sensor is used to collect and forward network traffic to the Tenable.ot Appliance. To perform Network Monitoring, you will need to connect the unit to a mirroring port on the network switch, which is connected to the controllers/PLCs of interest.

To manage the sensor, you will need to connect the unit to a network (can be a different network than the one that is used to perform network monitoring).

➡ **To Connect the Tenable.ot Rack Mount Sensor to the Network:**

1. On the Tenable.ot sensor, connect the Ethernet cable (supplied) to **Port 1**.
2. Connect the cable to a regular port on the network switch.
3. On the unit, connect another Ethernet cable (supplied) to **Port 2**.
4. Connect the cable to a mirroring port on the network switch.

➡ **To Connect the Tenable.ot Configurable Sensor to the Network:**

1. On the Tenable.ot sensor, connect the Ethernet cable (supplied) to **Port 1**.
2. Connect the cable to a regular port on the network switch.
3. On the unit, connect another Ethernet cable (supplied) to **Port 3**.
4. Connect the cable to a mirroring port on the network switch.

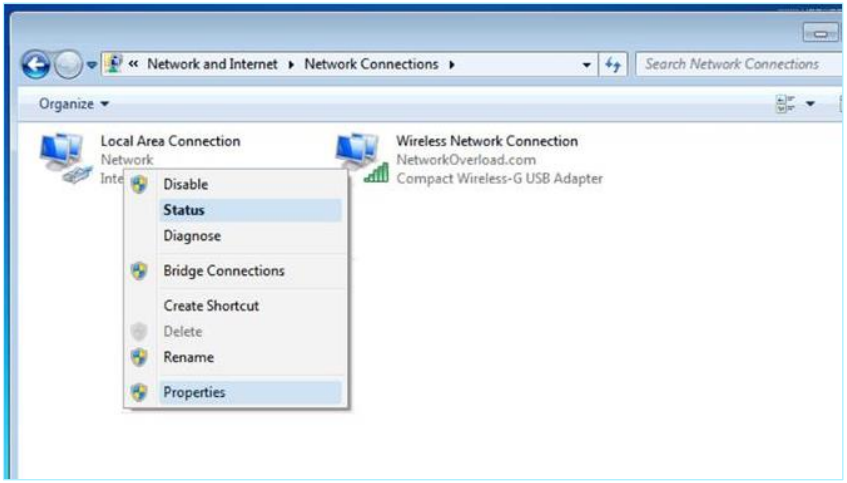
Step 3 – Accessing the Sensor Setup Wizard

➡ **To Log in to the Management Console.**

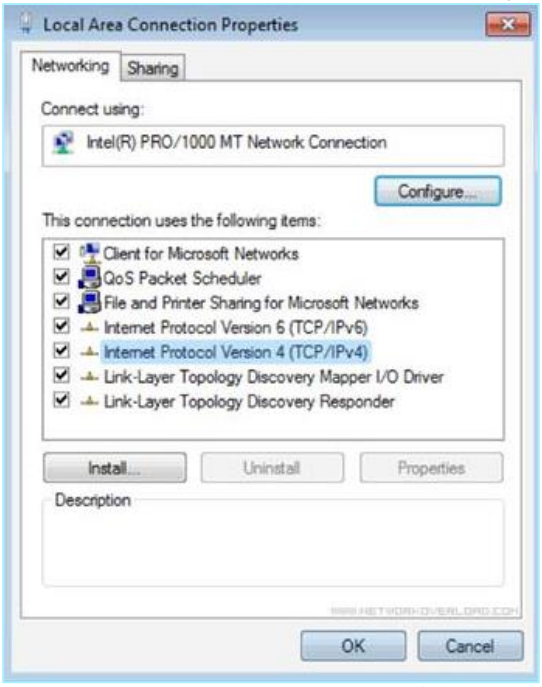
1. Do one of the following:
   - Connect the Management Console workstation (e.g. PC, laptop etc.) directly to Port 1 of the Tenable.ot sensor using the Ethernet cable, OR
   - Connect the Management Console workstation to the network switch.
2. Ensure that the Management Console workstation is part of the same subnet as the Tenable.ot sensor (which is 192.168.1.5) or is routable to the unit.
3. Use the following procedure to set up a static IP (you must set up a static IP in order to connect to the Tenable.ot sensor):
   a. Go to **Network and Internet** > **Network and Sharing Center** > **Change adapter settings**.

Navigation may vary slightly for different versions of Windows.

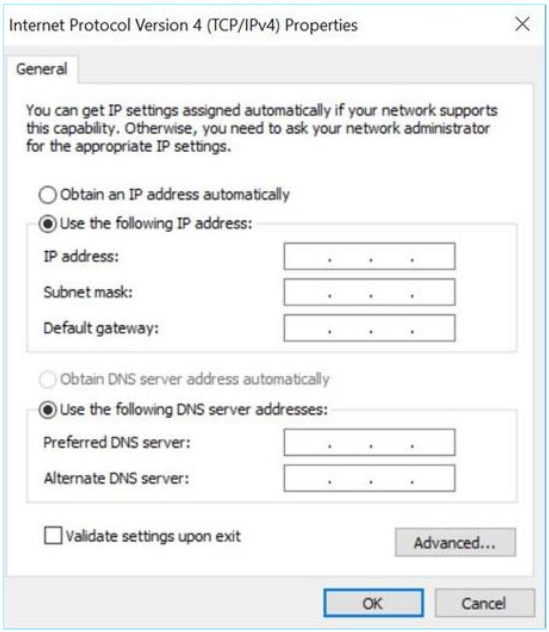
The Network Connections screen is displayed.



b. Right click on **Local Area Connections** and select **Properties**.
The **Local Area Connections** window is displayed.



c. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
The Internet Protocol Version 4 (TCP/IPv4) Properties window is displayed.

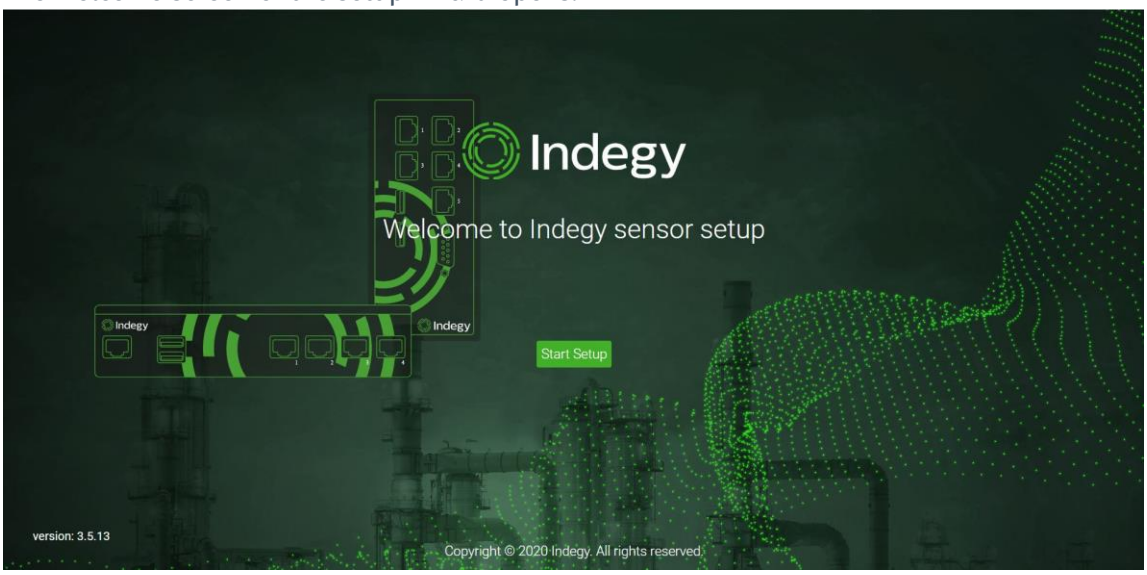


d. Select Use the Following IP address.
e. In the IP address field, enter *192.168.1.10*
f. In the Subnet mask field, enter *255.255.255.0*.
g. Click **OK**.
The new settings are applied.

4. From your Chrome web browser, navigate to 192.168.1.5.

> The UI can only be accessed from a Chrome browser. You also need to be using the latest version of Chrome.

The Welcome screen of the setup wizard opens.



5. Click **Start Setup Wizard**.
   The setup wizard opens, showing the **User Info** page.

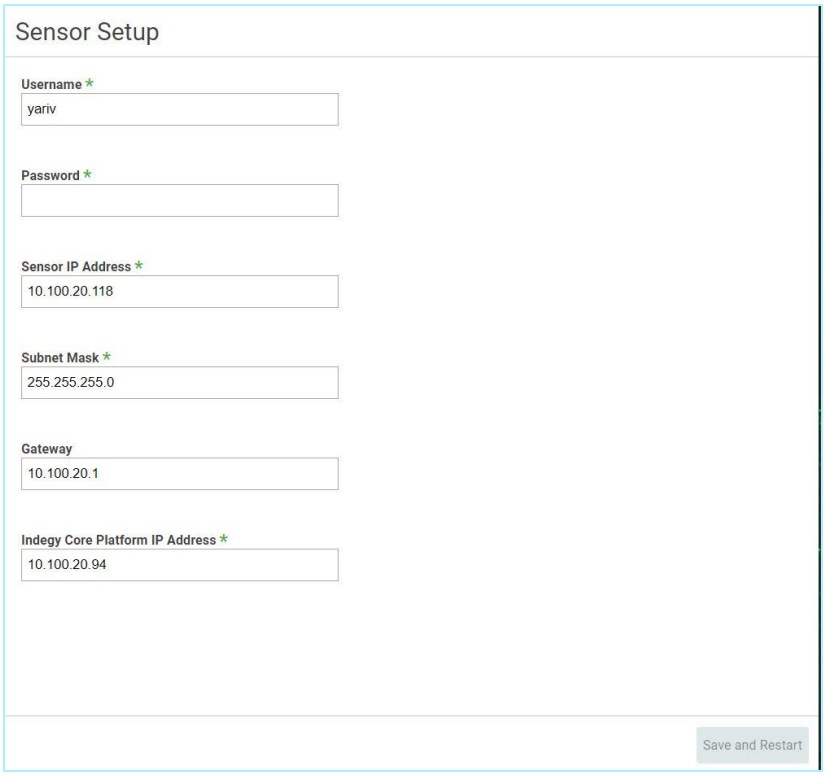
Step 4 – Sensor Setup Wizard

The Tenable.ot setup wizard takes you through the process of configuring the basic system settings.

> If you would like to change the configuration later, you will be able to do so on the Settings screen in the Management Console (UI).

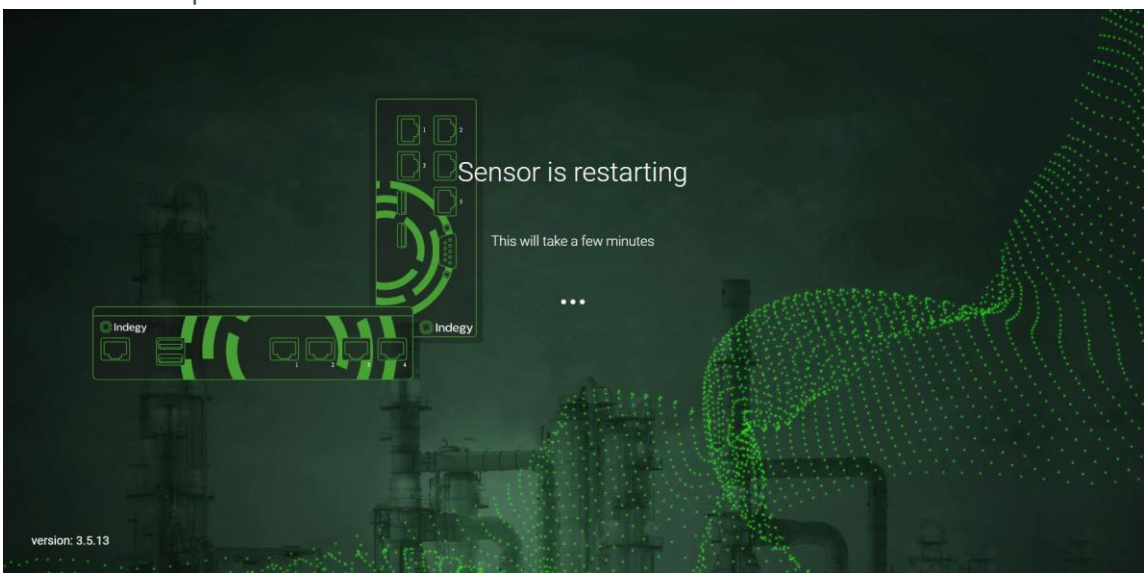
➡ **To set up the sensor:**

1. On the welcome screen, click **Start Setup**.
   The setup screen is displayed:

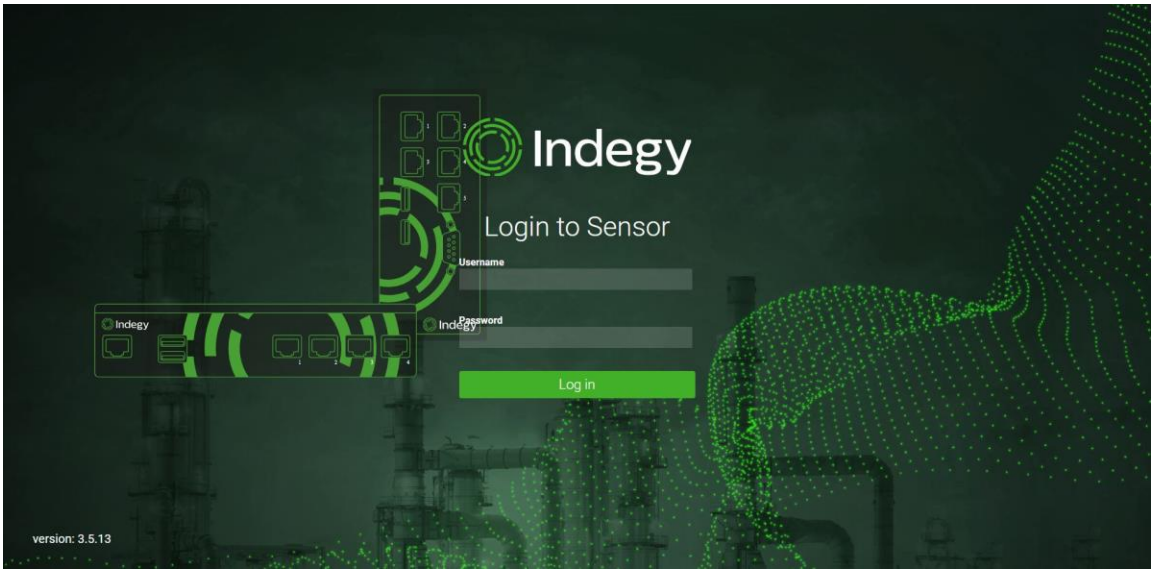


2. In the **Username** field, enter a username to be used for logging into the system. The username can have up to 12 characters and must include only lowercase letters and numbers.
3. In the **Password** field, enter a password to be used for logging into the system. The passwords must contain at least:
   - 12 characters
   - One uppercase letter
   - One lowercase letter
   - One digit
   - One special character
4. In the **Retype Password** field, re-enter the identical password.
5. In the **Sensor IP Address** field, enter an IP address (within the network subnet) to be applied to the Tenable.ot Sensor. It is strongly recommended to change the default IP address.
6. In the **Subnet Mask** field, enter the Subnet Mask of the network.
7. If you would like to set up a Gateway (optional), enter the Gateway IP for the network in the **Gateway** field.
8. In the **IP Address** field, enter the IP address of the Tenable.ot platform.

9. Click **Save and Restart**.
   The sensor will perform a restart:



10. Following the restart process, the network traffic will be forwarded to the Tenable.ot platform. If you want to modify the configuration, you will be able to login to the sensor using the configured IP address and the credentials that you have configured:



Appendix 2 – SAML Integration for Azure Active Directory

Tenable.ot supports integration with Microsoft Azure Active Directory via SAML protocol. This enables Azure users who were assigned to Tenable.ot to log in to Tenable.ot via SSO. You can use group mapping to assign roles in Tenable.ot according to the groups to which users are assigned in Azure.

Setting up the Integration

This section explains the complete flow for setting up a Single Sign-on (SSO) integration for Tenable.ot with Microsft Azure Active Directory. The configuration involves setting up the integration by creating a Tenable.ot application in Azure Active Directory, entering information about your created Tenable.ot application and uploading your identity provider's Certificate to the Tenable.ot SAML page, and then mapping groups from your identity provider to User Groups in Tenable.ot.

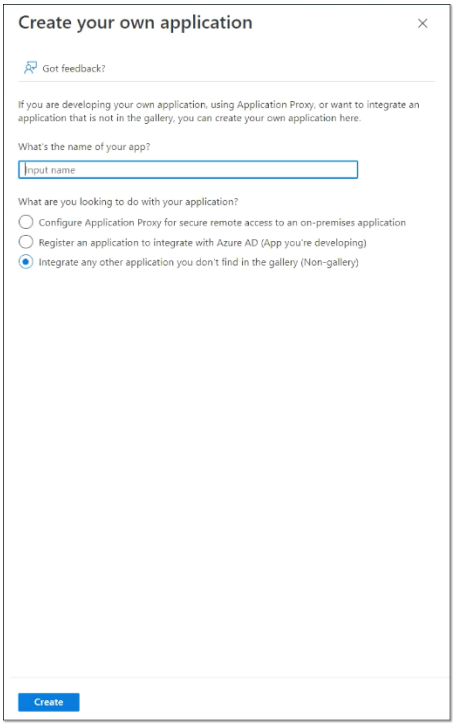
To set up the configuration, you need to be logged in as an admin user in both Azure Active Directory and Tenable.ot.

Step 1 - Creating the Tenable Application in Azure

➡ **To create the Tenable application in Azure:**

1. In **Microsoft Azure Active Directory** go to **Azure Active Directory** > **Enterprise Applications,** click **+ New application** to display the **Browse Azure AD Gallery**, and click **+ Create your own application.**

The **Create your own application** side panel is displayed.



2. In the **What's the name of your app?** field, enter a name for the application (e.g. Tenable_OT) and select **Integrate any other application you don't find in the gallery (Non-gallery)** (default selected), then click **Create** to add the application.

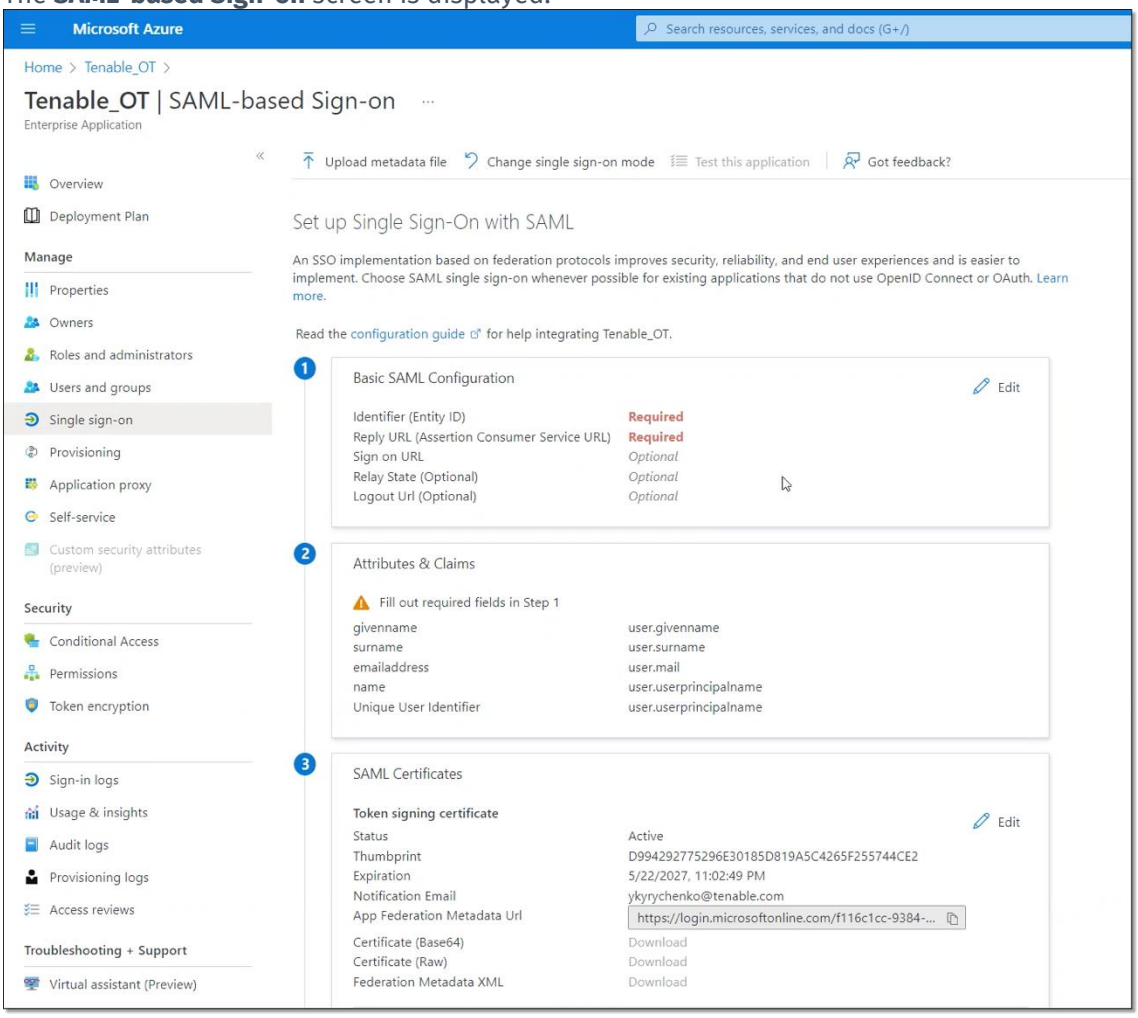
Step 2- Initial Configuration

This step is the initial configuration of the Tenable.ot application in Azure, consisting of creating temporary values for Basic SAML Configuration values Identifier and Reply URL, in order to enable download of the required Certificate.

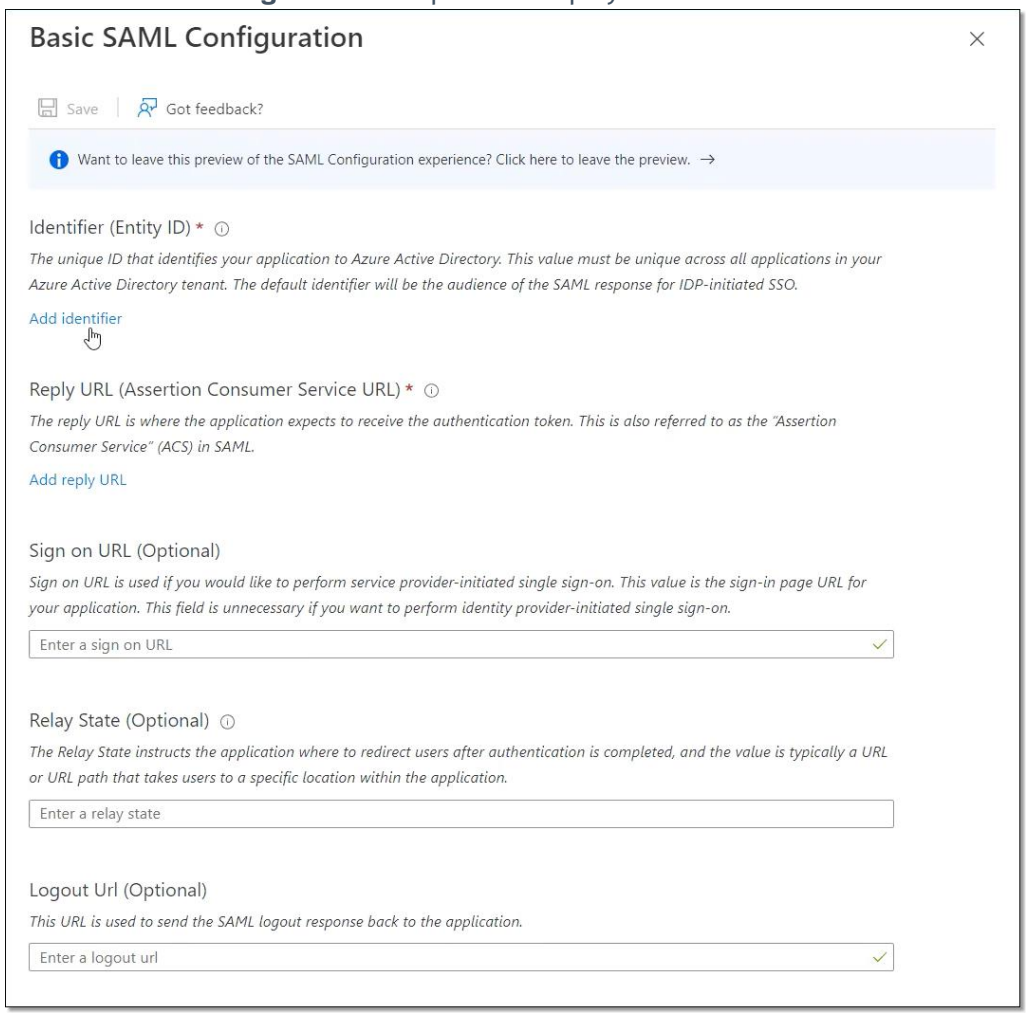
Only fields specified in this procedure must be configured. Other fields may be left with their default values.

To do initial configuration:

1. In the **Microsoft Azure Active Directory** navigation menu, click **Single sign-on,** then selected **SAML** as the single sign on method.
   The **SAML-based Sign-on** screen is displayed.



2. In section 1 – **Basic SAML Configuration**, click on Edit.
The **Basic SAML Configuration** side panel is displayed.

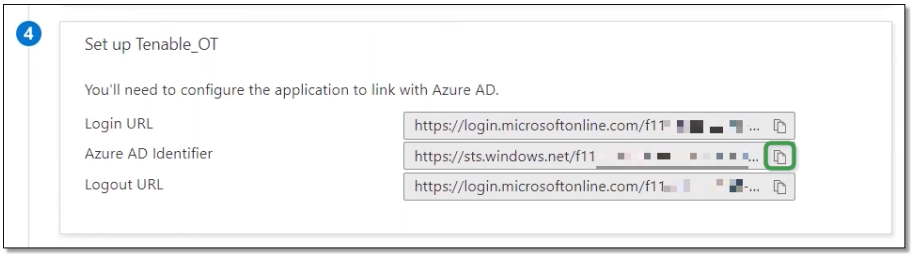


3. In the **Identifier (Entity ID)** field, enter a temporary ID for the Tenable application (e.g. tenable_ot).
4. In the **Reply URL (Assertion Consumer Service URL)** field, enter a valid URL (e.g. https://tenable.ot).

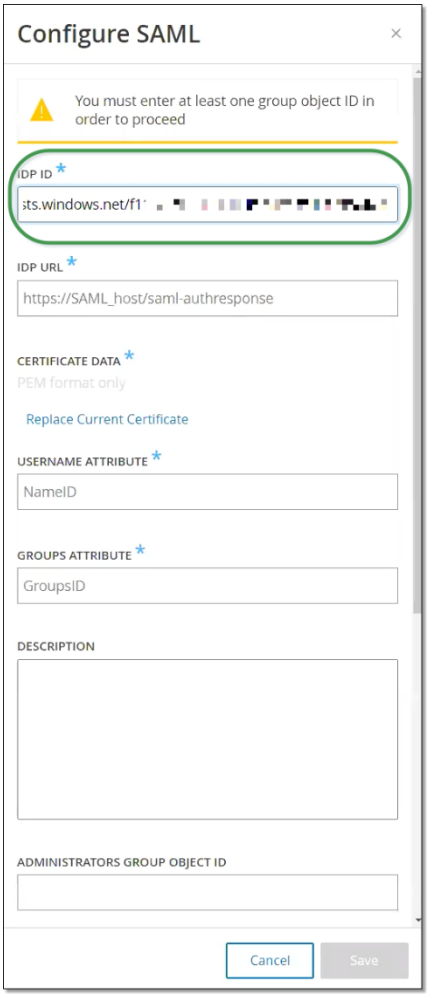
	Both the Identifier and Reply URL will be changed later in the configuration process.

5. Click **Save** to save the temporary values and close the **Basic SAML Configuration** side panel.

6. In section 4 - **Set up**, click the **copy** icon to copy the **Azure AD Identifier**.

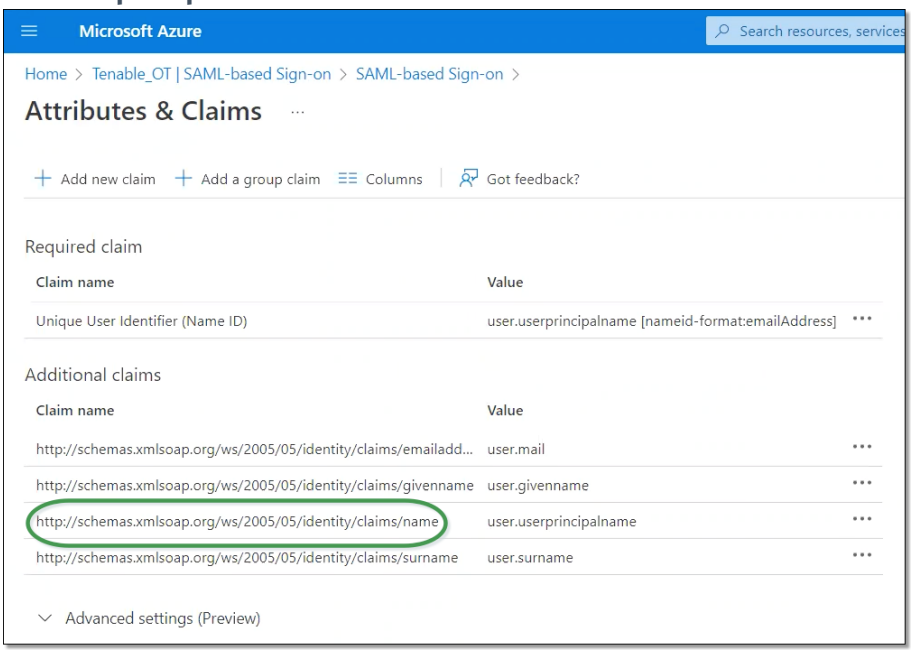


7. Switch to the **Tenable.ot** console, and go to **Users and Roles > SAML.**
8. Click **Configure** to display the **Configure SAML** side panel, and paste the copied value into the **IDP ID** field.

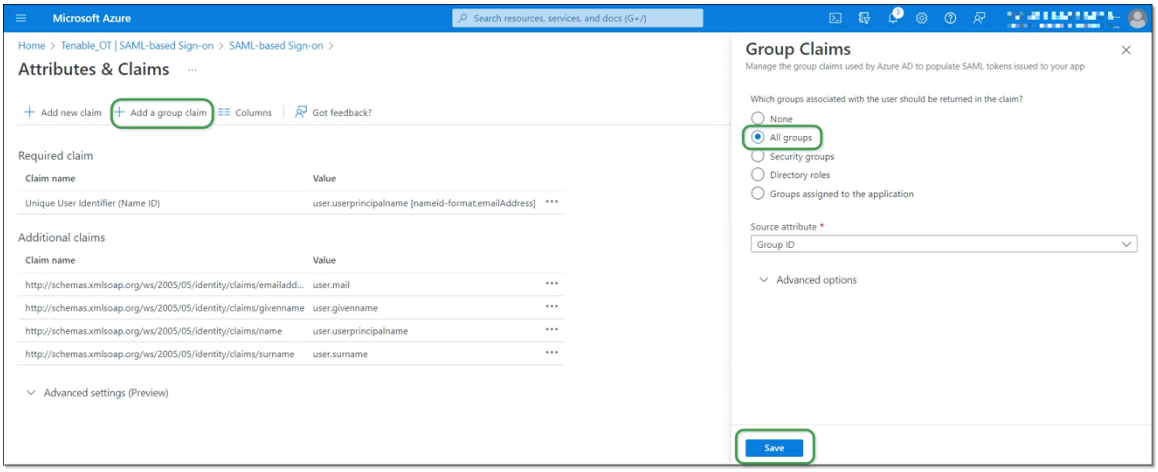


9. In the **Azure** console, click the icon to copy the **Login URL**.
10. Return to the **Tenable.ot** console and paste the copied value into the **IDP URL** field.
11. In the **Azure** console, in section 3 - **SAML Certificates**, for **Certificate (Base64)**, click **Download**.
12. Return to the **Tenable.ot** console, and under **Certificate Data**, click **Browse**, then navigate to the security certificate file and select it.
13. In the **Azure** console, in section 2 – **Attributes & Claims**, click **Edit.**

14. Under **Additional claims**, select and copy the **Claim name** URL corresponding to the Value **user.userprincipalname**.

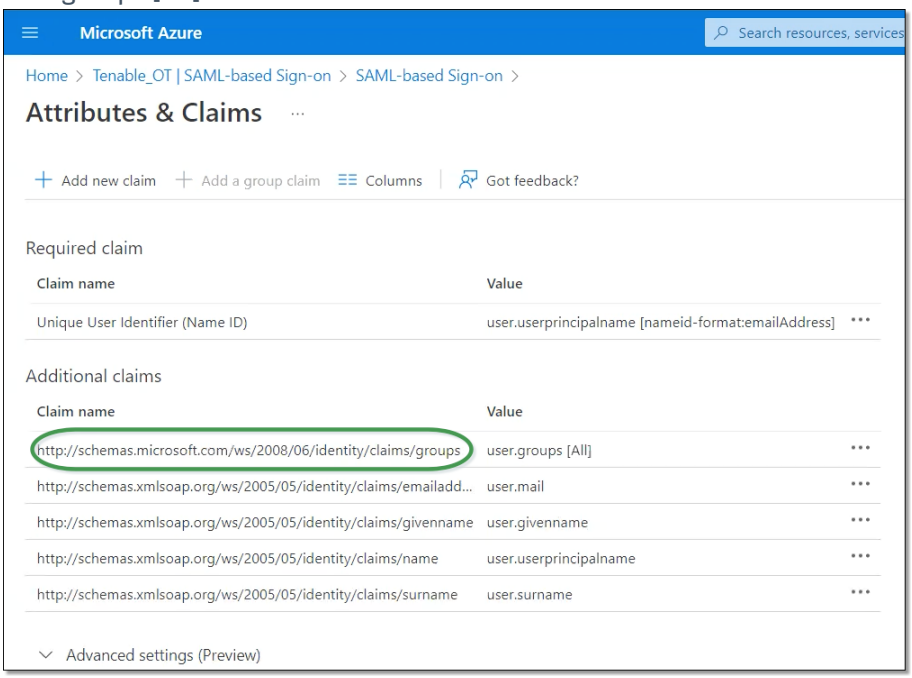


15. Return to the **Tenable** console and paste this URL in the **Username Attribute** field.
16. In the Azure console, click on **+ Add a group claim** to display the **Group Claims** side panel, and under **Which groups associated with the user should be returned in the claim?** Choose **All Groups** and click **Save**.



If you have groups setting enabled in Microsoft Azure, you may choose **Groups assigned to the application** instead of **All Groups,** and Azure will provide only the user groups that are assigned to the application.

17. Under **Additional claims**, highlight and copy the **Claim name** URL associated with the Value user.groups [All].



18. Return to the **Tenable** console and paste the copied URL in the **Groups Attribute** field.
19. If you would like to add a description of the SAML configuration, enter it in the **Description** field.

Step 3 - Mapping Azure Users to Tenable Groups

In this step, Azure Active Directory users are are assigned to the Tenable.ot application. The permissions granted to each user are designated by mapping between the Azure groups to which they are assigned and a pre-defined Tenable.ot User Group, which has an associated role and set of permissions. The Tenable.ot pre-defined User Groups are: *Administrators*, *Read-Only User*, *Security Analysts*, *Security Managers*, *Site Operators*, and *Supervisors*. For more information, see **USER GROUPS**. Each Azure user must be assigned to at least one group that is mapped to a Tenable.ot User Group.

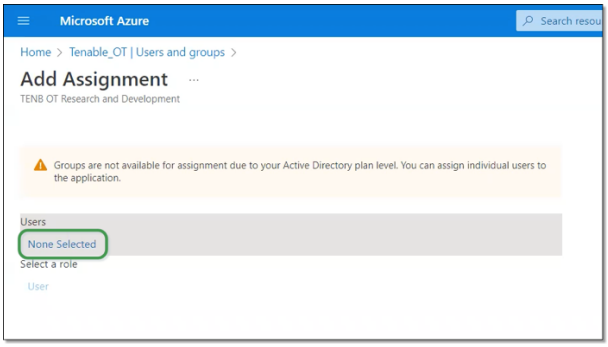
Admin users logged in via SAML are considered Admin (External) users, and are not granted all the privileges of local Admins.

Users assigned to multiple User Groups are granted the highest possible permissions from among their groups.

➡ **To map Azure users to Tenable.ot:**

1. In **Microsoft Azure**, navigate to the **Users and groups** page and click on **+ Add user/group**.

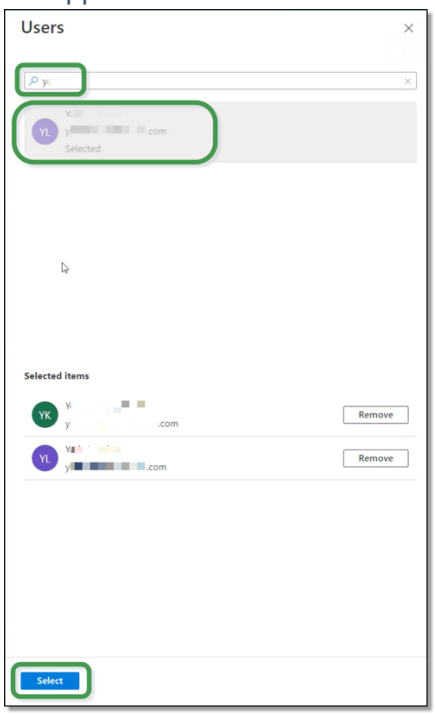
2. In the **Add Assignment** screen, under **Users**, click **None Selected**.



The **Users** side panel is displayed.

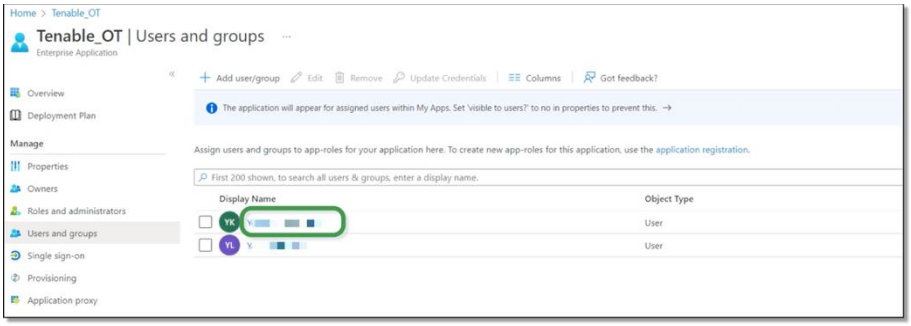
If you have groups setting enabled in Microsoft Azure and have previously selected **Groups assigned to the application** instead of All Groups, you may choose to assign groups instead of individual users.

3. Search for and click on all desired users, then click **Select**, then click **Assign** to assign them to the application.

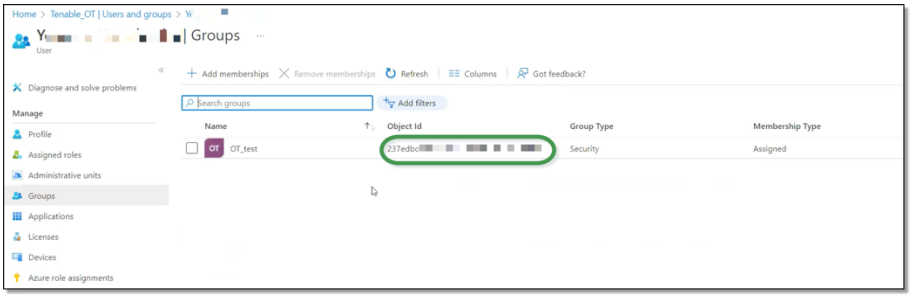


The **Users and groups** page is displayed.

4. Click on the **Display Name** of a user (or group) to display that user's (or group's) Profile.

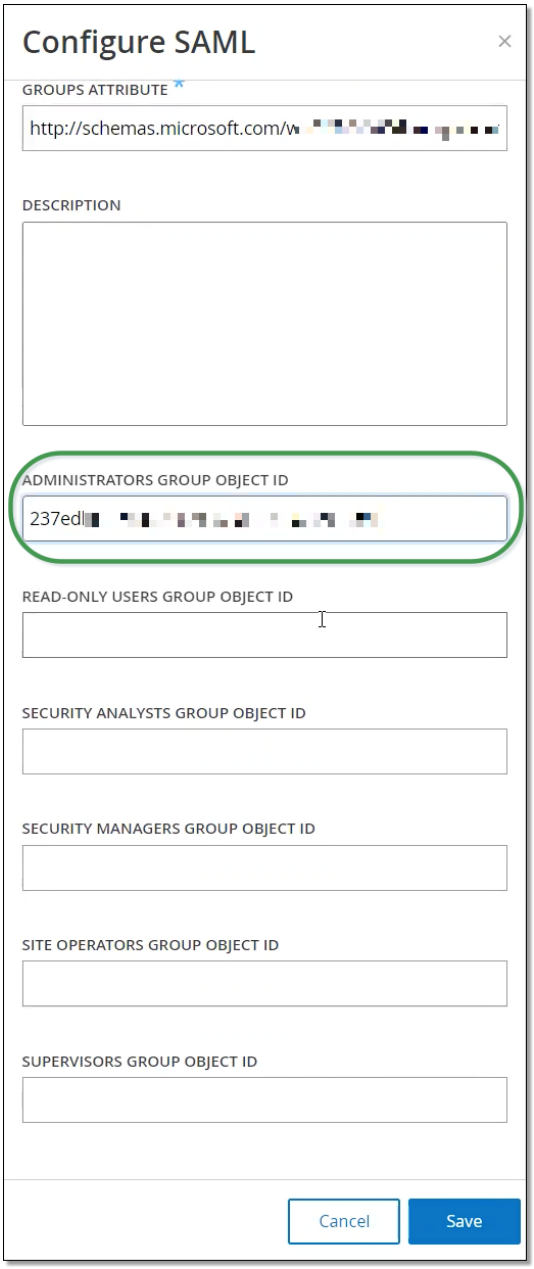


5. In the **Profile** screen, in the left-side navigation bar, select **Groups** to display the **Groups** screen.
6. Under **Object Id**, highlight and copy the value for the group that will be mapped to Tenable.

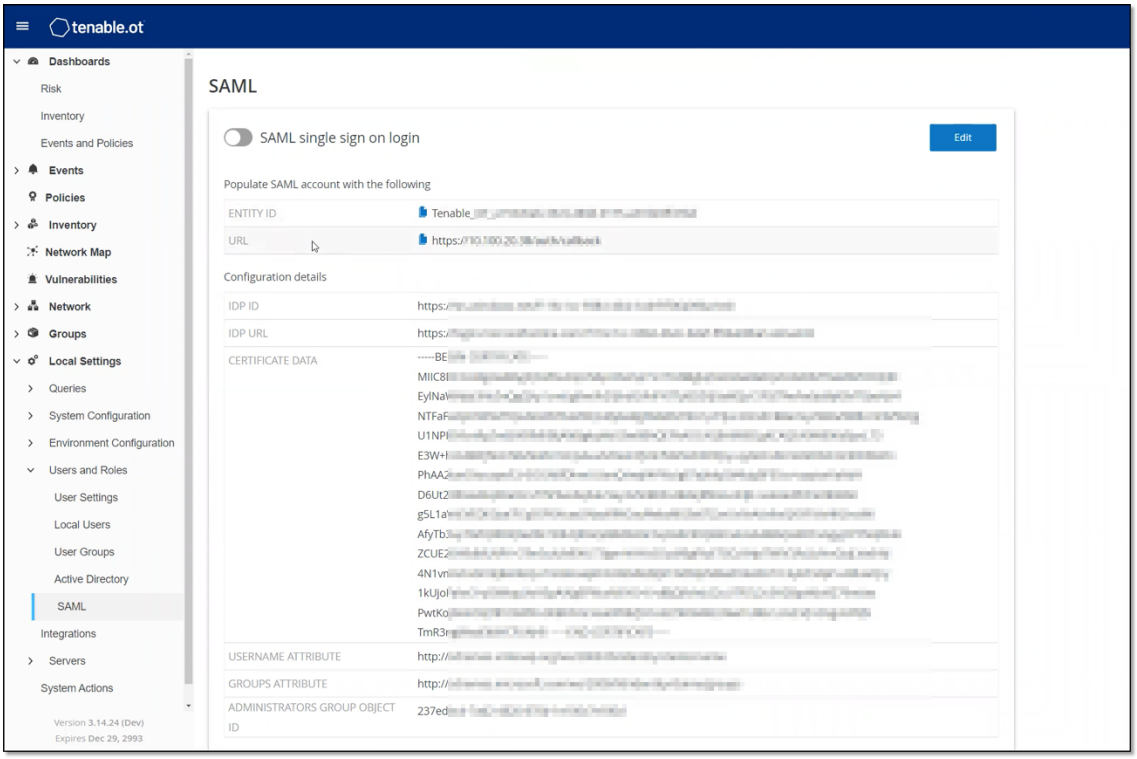


7. Return to the **Tenable.ot** console and paste the copied value in the desired **Group Object ID** field (e.g. Administrators Group Object ID).

8. Repeat steps 1-7 for each group that you would like to map to a distinct User Group in Tenable.ot.
9. Click **Save** to save and close the side panel.



The **SAML** screen is displayed in the Tenable.ot console with the configured information.



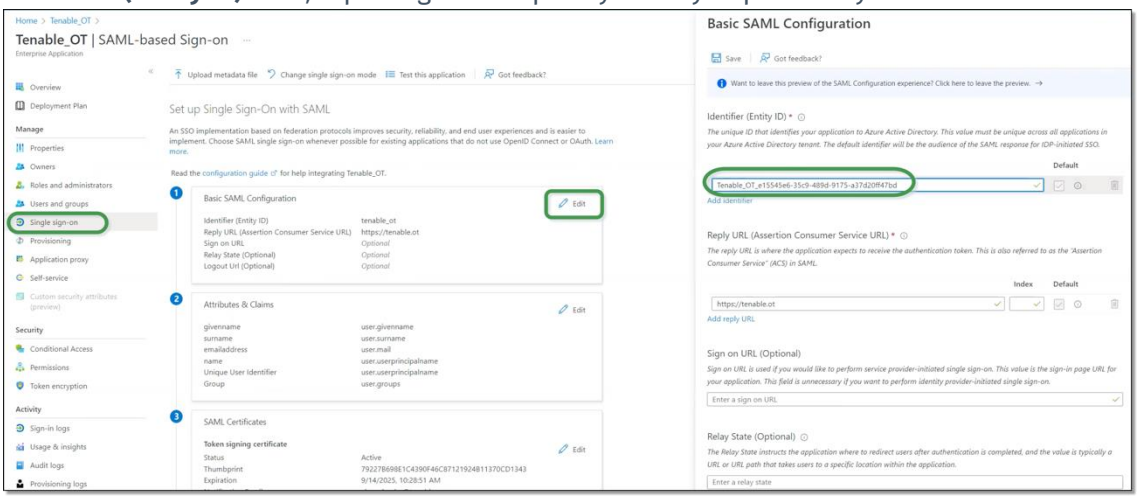
Step 4 - Finalizing the Configuration in Azure

➡ **To finalize the configuration in Azure:**

1. In the Tenable.ot **SAML** screen, under **Entity ID**, click the copy icon.

2. Switch to the **Azure** screen and click **Single sign-on** in the left-side navigation menu to open the **SAML-based Sign-on** page.

3. In section 1 - **Basic SAML Conifguration**, click **Edit**, and paste in the copied value in the **Identifier (Entity ID)** field, replacing the temporary value you previously entered.



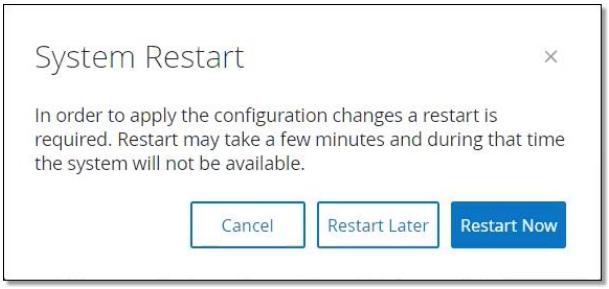
4. Return to the Tenable.ot **SAML** screen, and under **URL**, click the copy icon.
5. In the **Azure** console, and In the **Basic SAML Configuration** side panel, under **Reply URL (Assertion Consumer Service URL)**, paste the copied URL, replacing the temporary URL you previously entered.
6. Click **Save** to save the configuration, and close the side panel.
   The configuration is complete, and the connection is displayed on the **Azure Enterprise applications** screen.

Step 5 – Activating the Integration

To activate the SAML integration, Tenable.ot must be restarted. The user may restart the system immediately or choose to restart it later.

➡ **To activate the integration:**

1. In the Tenable.ot console, on the **SAML** screen, click to toggle the **SAML single sign on login** button **ON**.
   The **System Restart** notification window is displayed.



2. Click **Restart Now** to restart the system and apply the SAML configuration immediately, or click **Restart Later** to delay the application of the SAML configuration the next time the system is restarted. If you choose to restart later, the following banner is shown until the restart is done:

Signing in Using SSO

Upon restarting, the Tenable.ot login window has a new Sign in via SSO link underneath the Log in button. Azure users who were assigned to Tenable.ot can log in to Tenable.ot using their Azure account.

➡ **To sign in using SSO:**

1. On the **Tenable.ot** login screen, click the **Sign in via SSO** link.

If you are already logged in to Azure, you are taken directly to the Tenable.ot console, otherwise you are redirected to the Azure sign-in page.
Users with more than one account are redirected to the Microsoft **Pick an** account page, where they can select the desired account for login.