



# Tenable OT Security 3.15 User Guide

---

Last Revised: November 07, 2023



# Table of Contents

<b>Introduction</b>	<b>12</b>
OT Security Technologies	14
Solution Architecture	15
Network Components	16
System Elements	16
Assets	17
Risk Assessment	18
Policies and Events	19
<b>OT Security Hardware Components</b>	<b>22</b>
OT Security Appliance	23
OT Security Sensor	25
<b>Firewall Considerations</b>	<b>28</b>
OT Security Core Platform	29
OT Security Sensors	31
Active Query	32
OT Security Integrations	33
<b>Installing the OT Security Appliance</b>	<b>33</b>
Step 1 – Setting up the OT Security Appliance	34
Step 2 – Connecting OT Security to the Network	35
Step 3 – Logging in to the Management Console	36
Step 4 – Setup Wizard	40
Step 5 – Licensing	46
Step 6 – Enabling the System	52



Step 7 – Connecting the Separate Management Port (for Port Separation Option) .....	54
<b>Installing OT Security Sensor .....</b>	<b>55</b>
Setting up the Sensor .....	60
Setting up a Rack Mount Sensor .....	61
Setting up a Configurable Sensor .....	64
Connecting the Sensor to the Network .....	68
Accessing the Sensor Setup Wizard .....	69
<b>Management Console UI Elements .....</b>	<b>71</b>
Main UI Elements .....	73
Turning On/Off Dark Mode .....	75
Checking Current Software Version .....	76
Main Screens .....	77
Working with Lists .....	78
Customizing the Column Display .....	79
Grouping .....	80
Sorting .....	82
Filtering .....	83
Searching .....	85
Exporting Data .....	86
Actions Menu .....	87
<b>Dashboards .....</b>	<b>87</b>
Risk Dashboard .....	89
Inventory Dashboard .....	90
Events and Policies Dashboard .....	91



Interacting with Dashboards .....	92
Graph mode .....	93
Table mode .....	95
Changing the Default Dashboard .....	96
Exporting the Dashboard .....	97
<b>Policies .....</b>	<b>97</b>
Policy Configuration .....	99
Policy Types .....	103
Turning Policies On and Off .....	110
Viewing Policies .....	111
Viewing Policy Details .....	114
Creating Policies .....	115
Creating Unauthorized Write Policies .....	122
Other Actions on Policies .....	123
Editing Policies .....	124
Duplicating Policies .....	128
Deleting Policies .....	130
Deleting Policy Exclusions .....	132
Groups .....	133
Asset Groups .....	135
Viewing Asset Groups .....	136
Creating Asset Groups .....	138
Network Segments .....	143
Viewing Network Segments .....	144





Creating Network Segments .....	145
Email Groups .....	148
Viewing Email Groups .....	149
Creating Email Groups .....	150
Port Groups .....	152
Viewing Port Groups .....	153
Creating Port Groups .....	154
Protocol Groups .....	156
Viewing Protocol Groups .....	157
Creating Protocol Groups .....	158
Schedule Group .....	160
Viewing Schedule Groups .....	161
Creating Schedule Groups .....	163
Tag Groups .....	168
Viewing Tag Groups .....	169
Creating Tag Groups .....	170
Rule Groups .....	172
Viewing Rule Groups .....	173
Creating Rule Groups .....	174
Actions on Groups .....	175
Viewing Group Details .....	176
Editing a Group .....	178
Duplicating a Group .....	180
Deleting a Group .....	182



<b>Inventory</b>	<b>182</b>
Viewing Assets	184
Asset Types	187
Viewing Asset Details	195
Header Pane	197
Details Tab	198
Code Revisions	199
Snapshot Details Pane	201
Version History Pane	202
Creating a Snapshot	204
IP Trail	205
Attack Vectors	206
Generating Attack Vectors	207
Viewing Attack Vectors	209
Open Ports	210
Additional Actions in the Open Ports Tab	211
Vulnerabilities	212
Events	213
Network Map	216
Device Ports	217
Editing Asset Details	218
Editing Asset Details through the UI	219
Editing Asset Details by Uploading a CSV	222
Hiding Assets	225



Performing an Asset-Specific Tenable Nessus Scan .....	226
Performing Resync .....	227
<b>Events .....</b>	<b>229</b>
Viewing Events .....	230
Viewing Event Details .....	234
Viewing Event Clusters .....	236
Resolving Events .....	237
Resolving Individual Events .....	238
Resolving All Events .....	240
Creating Policy Exclusions .....	242
Downloading Individual Capture Files .....	248
Downloading a PCAP File .....	249
Creating FortiGate Policies .....	250
<b>Network .....</b>	<b>252</b>
Network Summary .....	253
Setting the Time Frame .....	254
Traffic and Conversations over Time .....	256
Top 5 Sources .....	257
Top 5 Destinations .....	258
Protocols .....	259
Packet Captures .....	260
Packet Capture Parameters .....	261
Filtering Packet Capture Display .....	262
Activating/Deactivating Packet Captures .....	264



Downloading Files .....	265
Conversations .....	266
<b>Network Map .....</b>	<b>268</b>
Asset Groupings .....	270
Applying Filters to the Map Display .....	274
Viewing Asset Details .....	275
Setting a Network Baseline .....	276
<b>Vulnerabilities .....</b>	<b>277</b>
Vulnerabilities Screen .....	278
Plugin Details .....	280
Editing Vulnerability Details .....	281
<b>Local Settings .....</b>	<b>283</b>
Queries .....	286
All Controller Queries .....	287
Controller Query Functions Table .....	288
All Network Queries .....	289
Network Query Functions Table .....	290
Asset Discovery .....	293
Tenable Nessus Plugin Scans .....	296
System Configuration .....	299
Device .....	301
Ping Requests .....	303
Packet Captures .....	304
Auto Approve Sensor Pairing Requests .....	305



Enable Usage Statistics .....	306
Sensors .....	307
Port Configuration .....	311
Updates .....	312
Certificate .....	321
License .....	324
Updating the License .....	325
Registering a New License .....	326
Reinitializing the License .....	331
Licensing Calculation .....	333
Environment Configuration .....	333
Asset Settings .....	334
Event Clusters .....	336
PCAP Player .....	338
Uploading a PCAP File .....	339
Playing a PCAP File .....	340
Users and Roles .....	341
Local Users .....	341
Viewing Local Users .....	343
Adding Local Users .....	344
Additional Actions on User Accounts .....	345
Editing a User Account .....	346
Changing a User's Password .....	347
Deleting Local Users .....	348



User Groups .....	348
Viewing User Groups .....	349
Adding User Groups .....	350
Editing User Groups .....	352
Deleting User Groups .....	353
Authentication Servers .....	353
Active Directory .....	354
LDAP .....	359
SAML .....	364
Integrations .....	367
Tenable Products .....	368
Tenable Security Center .....	369
Tenable Vulnerability Management .....	370
Palo Alto Networks – Next Generation Firewall .....	371
Aruba – ClearPass Policy Manager .....	372
Servers .....	372
SMTP Servers .....	373
Syslog Servers .....	375
FortiGate Firewalls .....	377
System Log .....	379
Sending System Log to a Syslog Server .....	380
<b>Appendix 1 – Installing a Sensor (Version 3.13 and below) .....</b>	<b>380</b>
Step 1 Setting up the Sensor .....	381
Step 2 Connecting the Sensor to the Network .....	382



Step 3 Accessing the Sensor Setup Wizard .....	383
Step 4 – Sensor Setup Wizard .....	384
<b>Appendix 2 – SAML Integration for Microsoft Entra ID .....</b>	<b>386</b>
Setting up the Integration .....	387
Step 1 - Creating the Tenable Application in Azure .....	388
Step 2- Initial Configuration .....	389
Step 3 - Mapping Azure Users to Tenable Groups .....	396
Step 4 - Finalizing the Configuration in Azure .....	401
Step 5 - Activating the Integration .....	403
Signing in Using SSO .....	404
<b>Revision History .....</b>	<b>405</b>



---

# Introduction

---

## OT Security Functionality

OT Security 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, OT Security's ICS security capabilities maximize your operational environments visibility, security and control.

OT Security 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.

OT Security 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. OT Security 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** - OT Security 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, OT Security 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, OT Security 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** – OT Security 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.



## OT Security Technologies

The OT Security comprehensive solution comprises two core collection technologies:

- **Network Detection** – OT Security 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** – OT Security'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 OT Security'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.

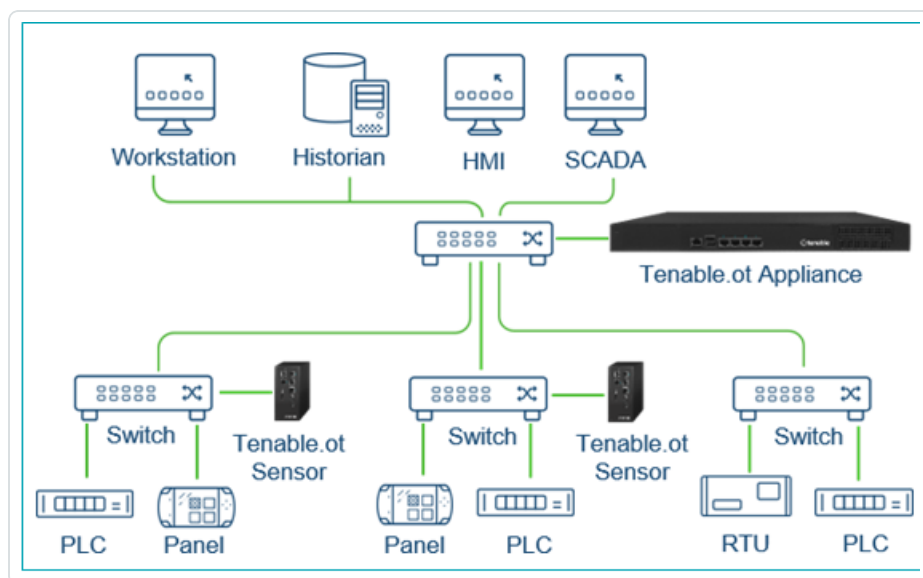


## Solution Architecture

### OT Security Platform Components

The OT Security solution is comprised of two components:

- **OT Security** – 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 OT Security Sensors. The OT Security appliance executes both the Network Detection and Active Query functions.
- **OT Security 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. OT Security sensors provide full visibility into these network segments by capturing all the traffic, analyzing it and then communicating the information to the OT Security 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 Components

OT Security supports interaction with the following network components:

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

**Note:** 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** – OT Security Event logs can be sent to a SIEM using Syslog protocol.
- **SMTP Server** – OT Security Event notifications can be sent by email to specific groups of employees via an SMTP server.
- **DNS Server** – DNS servers can be integrated into OT Security to help in resolving asset names.
- **Third party applications** – External applications can interact with OT Security using its REST API or access data using other specific integrations<sup>1</sup>.

<sup>1</sup>For example, OT Security supports integration with Palo Alto Networks Next Generation Firewall (NGFW) and Aruba ClearPass, enabling OT Security to share asset inventory info with these systems. OT Security can also integrate with other Tenable platforms such as Tenable Vulnerability Management and Tenable Security Center. Integrations are configured under **Local Settings > Integrations**, see [Integrations](#).

## System Elements



---

## Assets

---

Assets are the hardware components in your network such as controllers, engineering stations, servers etc. OT Security'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

OT Security applies sophisticated algorithms to assess the degree of risk posed to each asset on the network. A Risk Score (from 0 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).

**Note:** 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 OT Security, 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.

**Note:** 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 OT Security 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.

## **OT Security Hardware Components**

---

## OT Security Appliance



Component	Description
<b>Power Indicator</b>	Indicates when the OT Security appliance is turned on (Green) or off.
<b>Console Port</b>	Not in use
<b>USB Ports</b>	Not in use
<b>Ethernet Ports</b>	<p>Four GbE ports used to connect to management and operational networks as follows:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Port 4 – Reserved port, used by OT Security's Professional Services for remote or local support.</p>



## Rear Panel

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

## Package Contents

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

# OT Security Sensor

## Rack Mount Sensor

**Note:** 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

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

## Package Contents

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

## Configurable Sensor



**Note:** 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
<b>Power Indicator</b>	Indicates when the sensor is turned on (Green) or off.
<b>Console Port</b>	Not in use
<b>USB Ports</b>	Not in use
<b>Ethernet Ports</b>	Five GbE ports used to connect to management and operational networks as follows:



	<p>Port 1 – Management port – used for managing the device.</p> <p>Port 2 – Not in use.</p> <p>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.</p> <p>Port 4 – Not in use. Port 5 – Not in use.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Package Contents

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

## Firewall Considerations

In setting up your OT Security system, it is important to map out which ports should remain open so that the Tenable system can operate correctly. The following tables indicate which ports should be left open for use with the OT Security Core Platform and OT Security Sensors. There are also tables showing the ports needed for running Active Queries and for integration with Tenable Vulnerability Management and Tenable Security Center.





## OT Security Core Platform

The following ports should remain open for communication with the OT Security Core Platform.

Flow Direction	Port	Communicates With	Purpose
Inbound	TCP 443	Web interface for OT Security	Browser access to OT Security
Inbound	TCP 8000	Web interface for Tenable Core	Browser access to Tenable Core
Inbound	TCP 22	Sensors	Sensor Communication
Inbound	TCP 22	Appliance for SSH Access	Command line access to OS or appliance
Outbound	TCP 443	Tenable Security Center	Sends data for integration
Outbound*	TCP	cloud.tenable.com	Sends data for integration
Outbound*	Various Industrial protocols	PLCs/controllers	Active query
Outbound*	TCP 25	Email server for alerts	SMTP (alert emails, reports)
Outbound*	UDP 514	Syslog server	Syslog server
Outbound*	UDP 53	DNS server	Name Resolution
Outbound*	UDP 123	NTP server	Time service
Outbound*	TCP 636	AD server	AD LDAP authentication
Outbound*	TCP 443	SAML Provider	Single Sign On
Outbound*	UDP 161	SNMP Server	SNMP monitoring to Tenable Core



Outbound*	TCP\443	*.tenable.com	Automatic Plugin, Application and OS Updates <sup>1</sup>
-----------	---------	---------------	-----------------------------------------------------------

---

\*optional services



## OT Security Sensors

The following ports should remain open for communication with OT Security Sensors.

Flow Direction	Port	Communicates With	Purpose
Inbound	TCP 8000	Web interface	Browser access to user GUI
Outbound	TCP 22	OT Security appliance Sensor	Sensor Communication
Inbound	TCP 22	Appliance for SSH Access	Command line access to OS or appliance
Outbound*	TCP 25	Email server for alerts	SMTP (alert emails, reports)
Outbound*	UDP 53	DNS server	Name Resolution
Outbound*	UDP 123	NTP server	Time service
Outbound*	UDP 161	SNMP Server	SNMP monitoring to Tenable Core



## Active Query

The following ports should remain open in order to use the Active Query function.

Flow Direction	Port	Communicates With	Purpose
Outbound	TCP 80	OT Devices	HTTP fingerprinting
Outbound	TCP 102	OT Devices	S7/S7+ protocol
Outbound	TCP 443	OT Devices	HTTPS fingerprinting
Outbound	TCP 445	OT Devices	WMI queries
Outbound	TCP 502	OT Devices	Modbus protocol
Outbound	TCP 5432	OT Devices	PostgreSQL queries
Outbound	TCP 44818	OT Devices	CIP protocol <sup>2</sup>
Outbound	TCP/UDP 53	OT Devices	DNS
Outbound	ICMP	OT Devices	Asset Discovery
Outbound	UDP 161	OT Devices	SNMP queries
Outbound	UDP 137	OT Devices	NBNS queries
Outbound	UDP 138	OT Devices	NetBIOS queries



## OT Security Integrations

The following ports should remain open for communication with the Tenable Vulnerability Management and Tenable Security Center Integrations.

Flow Direction	Port	Communicates With	Purpose
Outbound	TCP 443	cloud.tenable.com	Tenable Vulnerability Management Integration
Outbound	TCP 443	Tenable Security Center	Tenable Security Center Integration

\*\*

offline procedure available

<sup>2</sup>used exclusively for the vendor. Depending on make and model of devices, other ports and protocols may be needed.

## Installing the OT Security Appliance



## Step 1 – Setting up the OT Security Appliance

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

### Rack Mounting

To mount the OT Security appliance on a standard (19-inch) rack:

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

**Note:** 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 OT Security appliance on a flat surface:

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

**Note:** 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 OT Security to the Network

---

OT Security 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 OT Security appliance to the network:

1. On the OT Security 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.

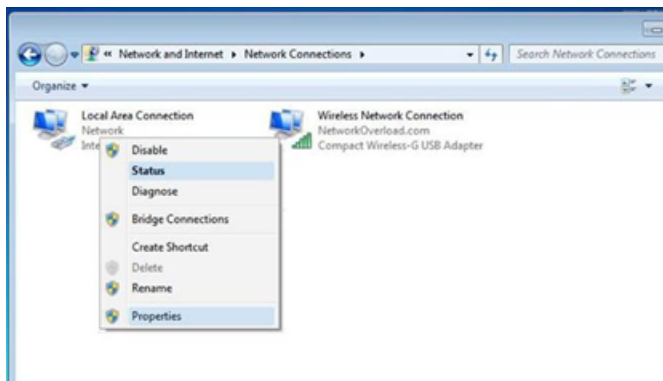


## Step 3 – Logging in to the Management Console

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 OT Security 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 OT Security 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 OT Security appliance):
  - a. Go to **Network and Internet > Network and Sharing Center > Change adapter settings**.

The Network Connections screen is displayed.

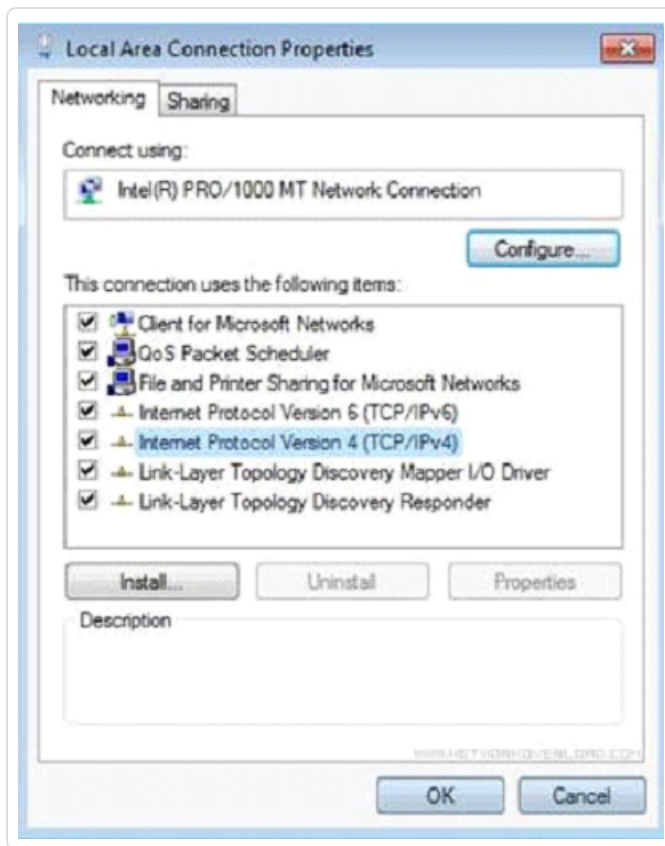


**Note:** Navigation may vary slightly for different versions of Windows.

- b. Right-click on **Local Area Connections** and select **Properties**.

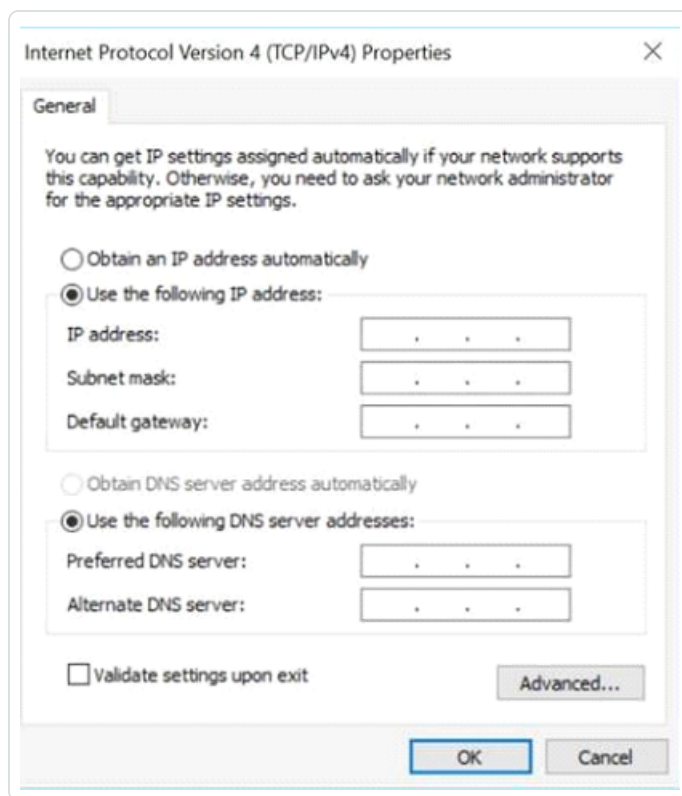
The **Local Area Connections** window appears.





- 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 <https://192.168.1.5>.

The Welcome screen of the setup wizard opens.



**Note:** 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 OT Security setup wizard takes you through the process of configuring the basic system settings.

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

### Screen 1 User Info

Setup Wizard

User Info   Device   System Time

Username

Username must be:

- ☐ Up to 12 characters
- ☐ Only lowercase letters and numbers
- ☐ Unique username

Retype Username

Full Name

Password

Retype Password

Next

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

**Note:** 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**.

**Note:** 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



## Setup Wizard

User Info

Device

System Time

**Device Name** ⓘ  
The name of the Tenable.ot core platform

**Port Configuration**  
It is possible to separate the Tenable.ot management port from the port used for active queries. After applying this change the management interface will be accessible through port #3 while the active queries through port #1.  
☐ Separate management from active queries

1 <input type="checkbox"/> Queries + Management	2 <input type="checkbox"/> Mirror Port	3 <input type="checkbox"/> Reserved	4 <input type="checkbox"/> Reserved
----------------------------------------------------------	----------------------------------------------	-------------------------------------------	-------------------------------------------

**IP** ⓘ  
The IP address for Management and active queries

**Subnet Mask** ⓘ

**Gateway**

☐ **Initial Asset Enrichment Active Query**  
First time classification queries are a group of queries aimed to classify assets once they are discovered. The queries will be executed only once per asset and includes: SNMP, minimal open ports verification, CIP/DCP, NetBIOS, backplane query, unicast identification, controller details, controller state

Back

Next

On the Device page, fill in the information about the OT Security platform as follows:

1. In the **Device Name** field, enter a unique identifier for the OT Security 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.



**Note:** 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 OT Security 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 OT Security platform. This becomes the OT Security 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.
- Note:** If you do not fill in this field then OT Security 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 OT Security 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

The screenshot shows a 'Setup Wizard' window with three steps: 'User info', 'Device', and 'System Time'. The 'System Time' step is active. It contains three input fields: 'Time Zone' with a dropdown menu showing 'Etc/UTC', 'Date' with a text field showing '10/1/2020' and a calendar icon, and 'Time' with a text field showing '07:10:46 AM' and a clock icon. At the bottom, there are two buttons: 'Back' and 'Complete and Restart'.

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

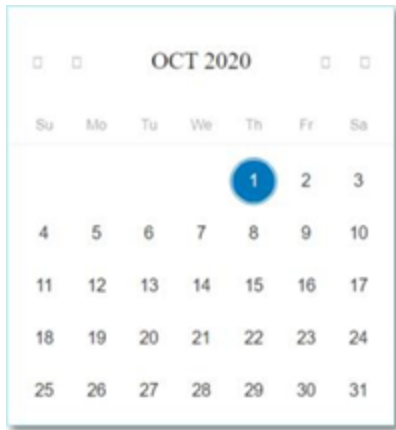
**Note:** Setting the correct date and time is essential for accurate recording of logs and alerts.

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.

**Note:** 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 OT Security license.

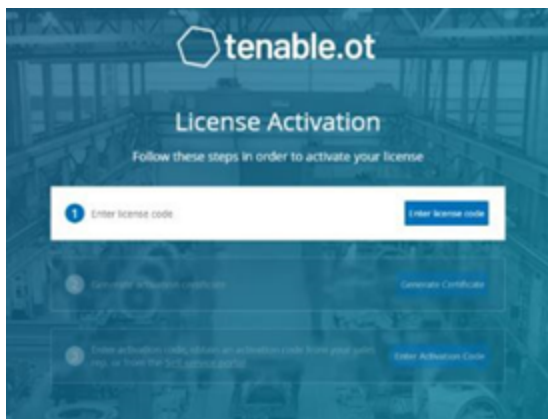
### Prerequisites

- 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 OT Security 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.

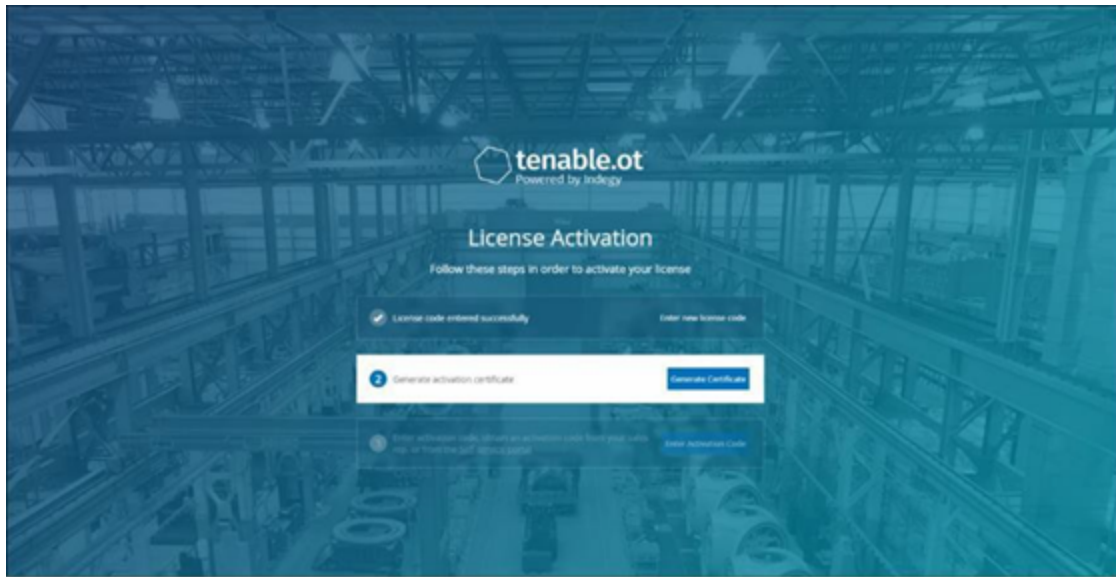
2. In the **License Code** field, enter your license code and click **Verify**.

The side panel closes.



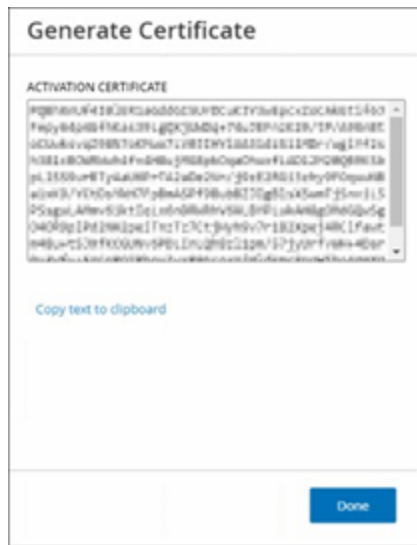
A dialog box titled "Enter license code" with a close button (X) in the top right corner. It contains a text input field labeled "LICENSE CODE" with a blue asterisk, containing the text "T988L20270LadK0u0m70L...J7L0". At the bottom, there are two buttons: "Cancel" and "Verify".

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



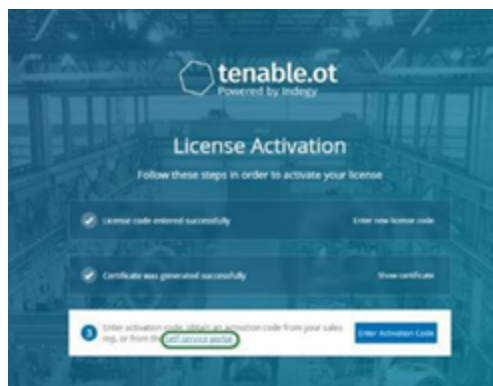
The **Generate Certificate** side panel is shown with the Activation Certificate.

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



The side panel closes.

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



The **Activate OT Security Offline** screen opens in a new tab.



**Activate Tenable.ot Offline**

**1 Activation Info**

**Offline Activation Details**

**Tenable.ot**  
Activation Certificate

License Code

Enter your Tenable.ot License Code

☐ I have read and understand the [Tenable Software License Agreement](#)

**2 Confirmation**

**Information**

Please copy / paste your Activation Certificate and click "Generate Activation Code"

[How Do I Generate a Tenable.ot Activation Certificate?](#)

[Tenable.sc Offline Activation](#)

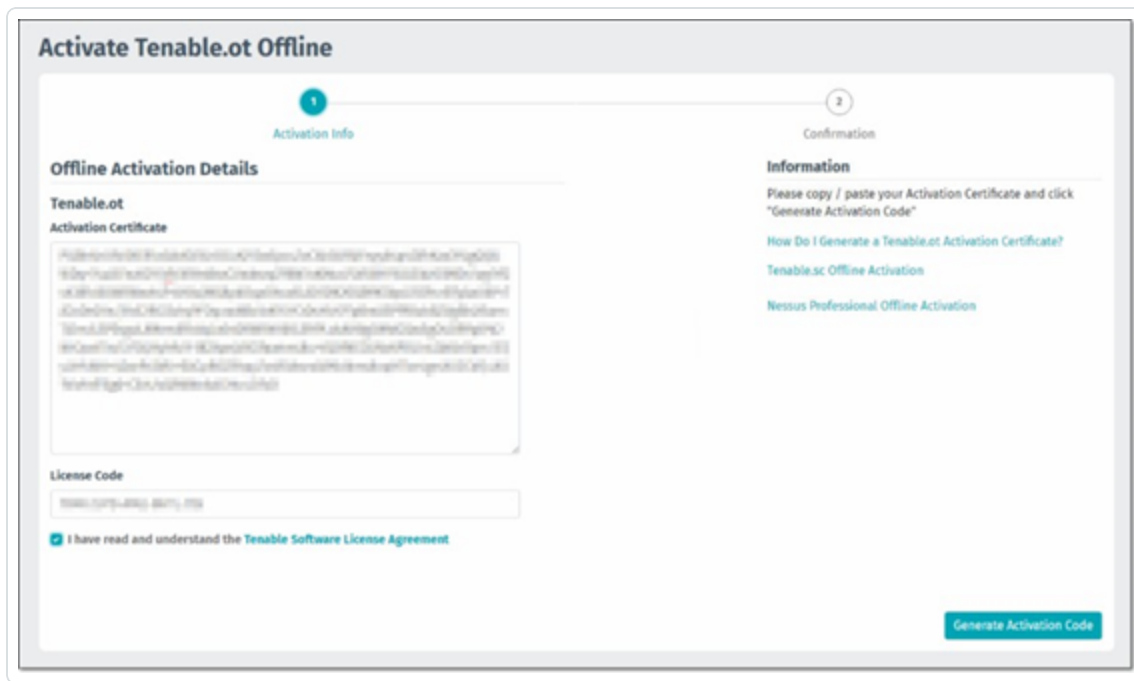
[Nessus Professional Offline Activation](#)

[Generate Activation Code](#)

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

**Note:** If you are not currently logged in to [tenable.com](https://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.

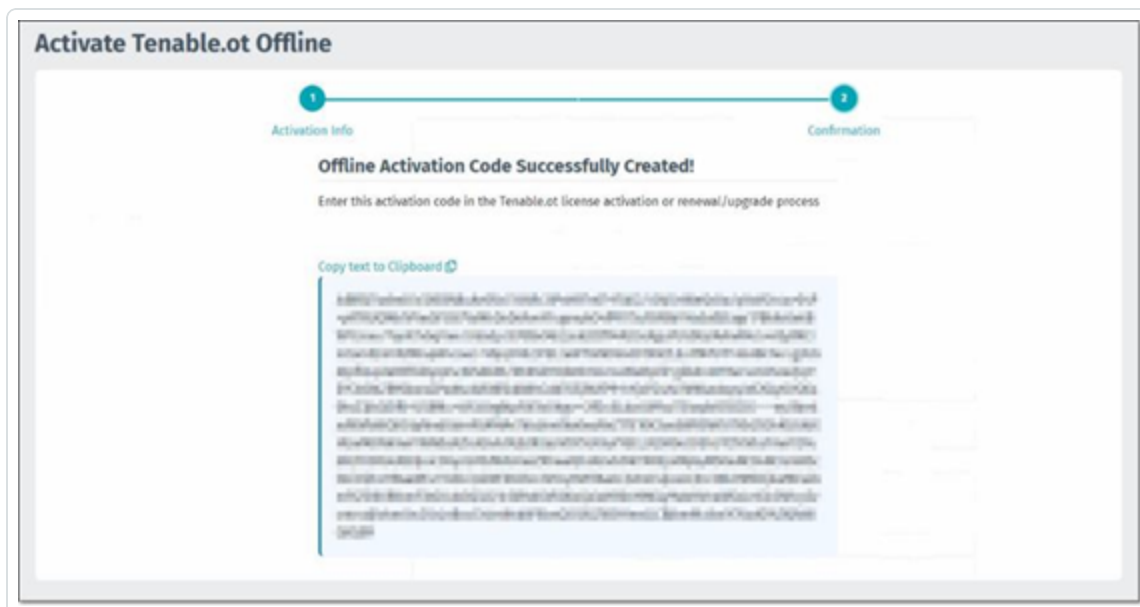
6. In the Activation Certificate field, enter the Activation Certificate.
7. In the **License Code** field, enter the same 20-character **license code** you entered in Step 2 of this procedure.
8. Click the I have read and understand the Tenable Software License Agreement checkbox.



**Note:** 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.

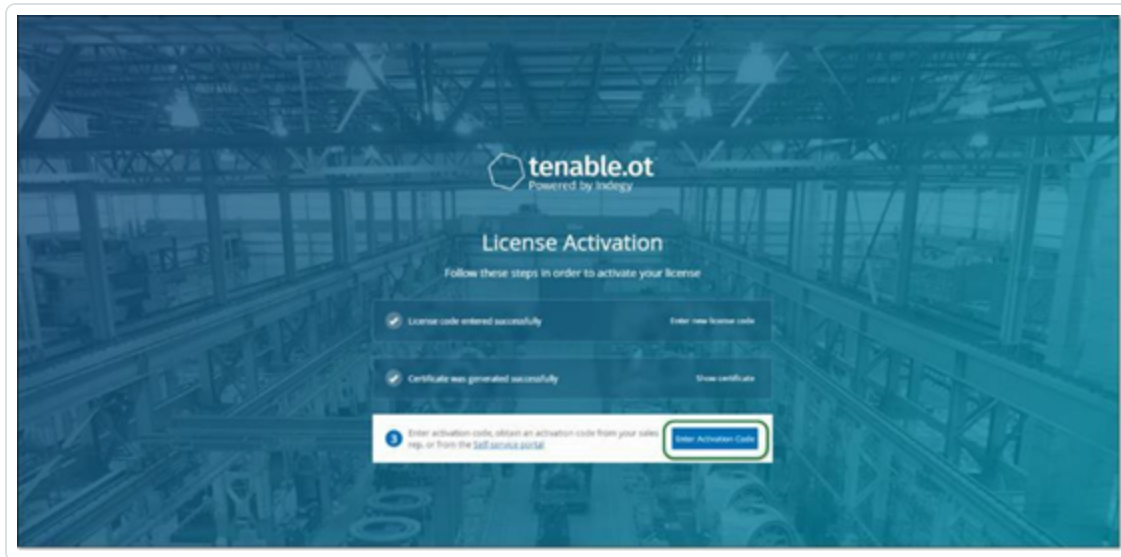


10. Click Copy text to Clipboard.

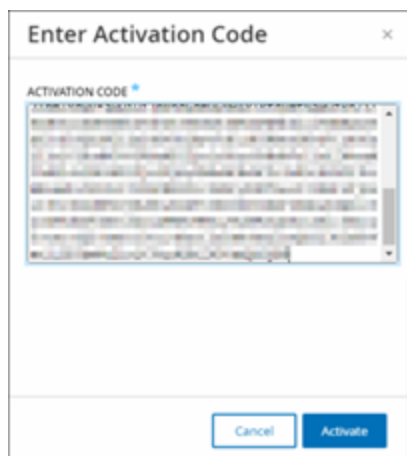


11. Navigate back to the **License Activation** screen on your OT Security device, and click the **Enter Activation Code** button.

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 OT Security home screen is shown. The Enable button is displayed.

**Note:** For information about updating your license, see [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).

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

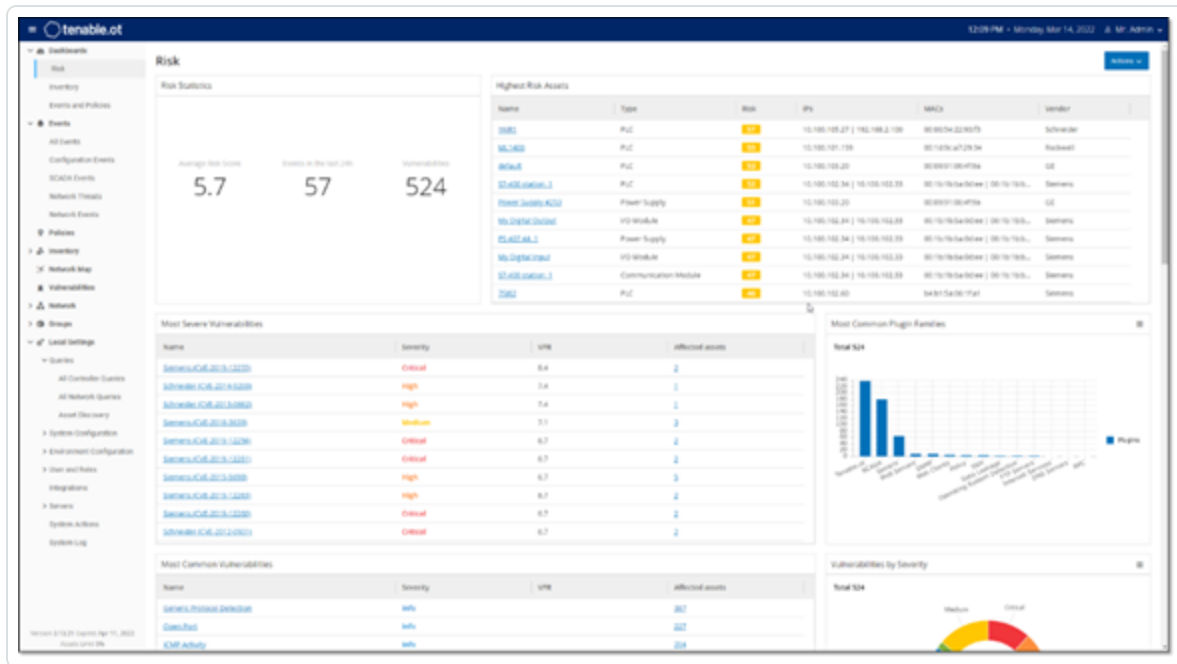
Additional functions such as Active Queries can be configured and activated on the **Local Settings** screen in the Management Console (UI), see [Queries](#).

To enable the system:

1. Click the **Enable** button.

The system is enabled. The UI opens, showing the **Dashboard > Risk** screen.





**Note:** 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 OT Security 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 OT Security appliance, connect an Ethernet cable (supplied) to Port 3.
2. Connect the cable to a port on a network switch.



---

## Installing OT Security 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 [Setting up the Sensor](#)).
- The Sensor is connected to your network switch (see [Connecting the Sensor to the Network](#)).
- The Sensor has its own static IPv4 address (see [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/tenable-core/OT-security/Content/TenableCore/Introduction\\_OT.htm](https://docs.tenable.com/tenable-core/OT-security/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**.

**Note:** 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** check box, and click **Log In**.




**Note:** 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 **OT Security Sensor**.



The **OT Security Sensor Pair** window is displayed.

**Note:** The **Tenable OT Security 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.

**Note:** 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.

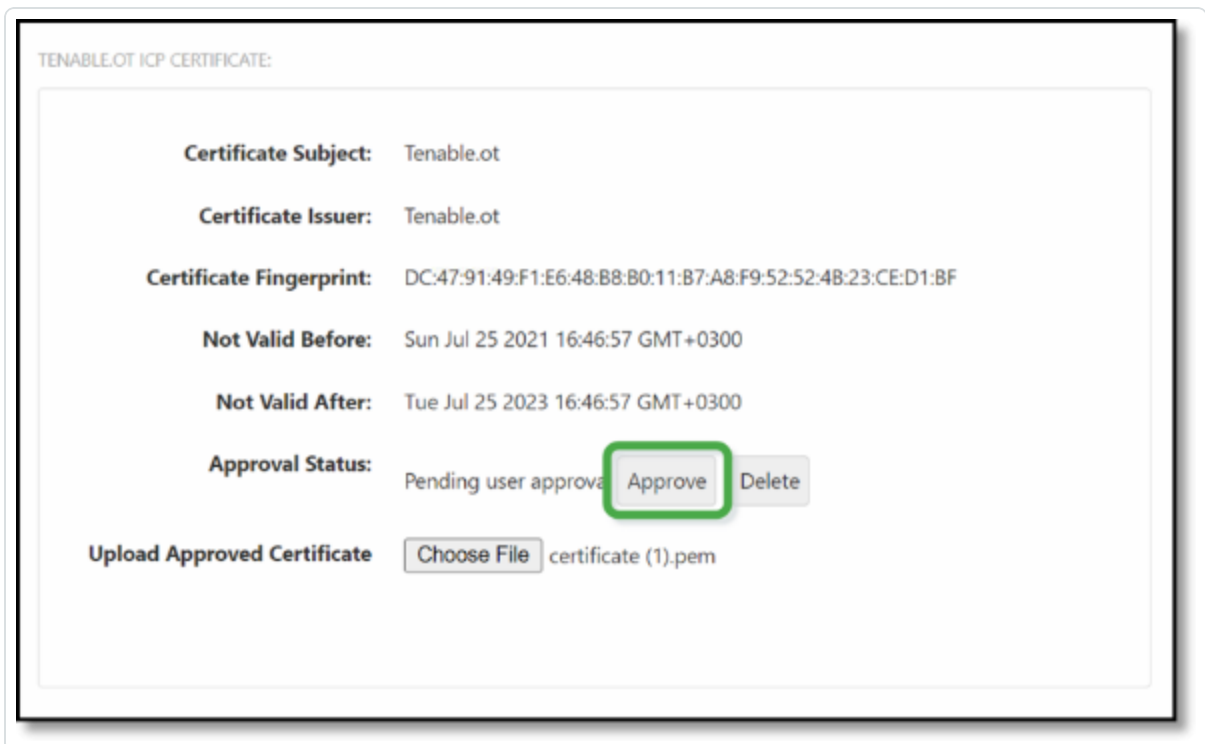
8. To authenticate the pairing, do one of the following:
  - Enter the ICP username in the **ICP User** field and the **ICP password** in the ICP Password field, OR
  - Enter an API Key for the ICP in the **ICP API Key** field.

**Note:** 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](#)).



**Note:** 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 Security Server Certificate** pop-up window, click **Accept This Certificate**.

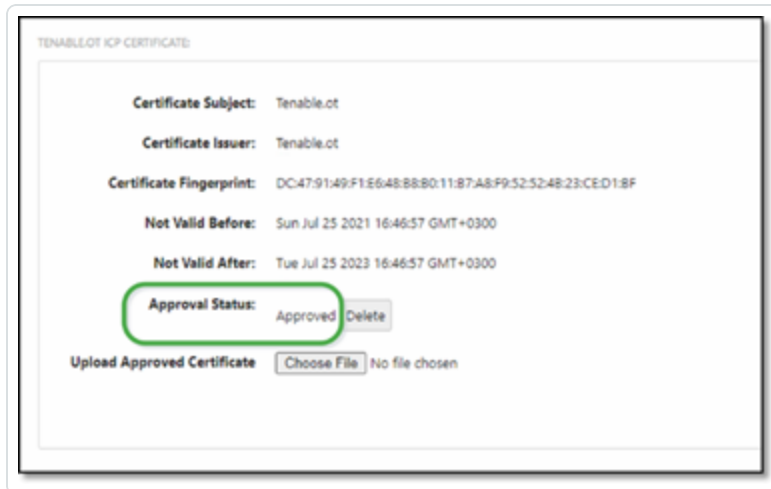
If you prefer to manually upload a Certificate:

- a. In the **Tenable ICP** console, follow the procedure described in [Generating an HTTPS Certificate](#).



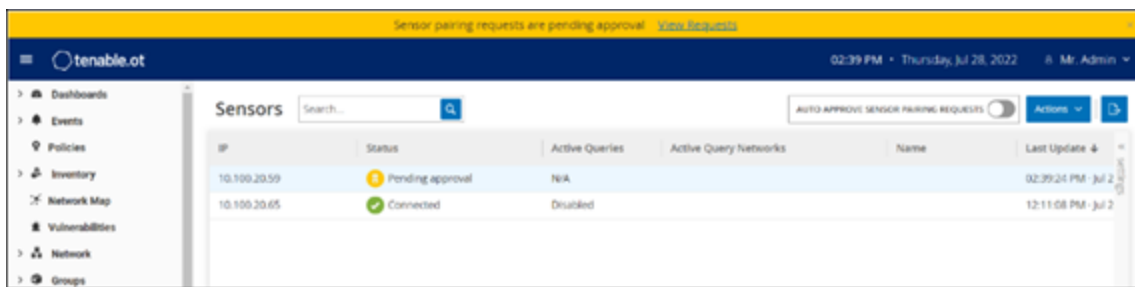
- b. In the **Tenable Core** console, in the **Tenable ICP Certificate** section, under **Upload Approved Certificate**, click **Choose File**.
- c. Navigate to the .pem Certificate file to upload.

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

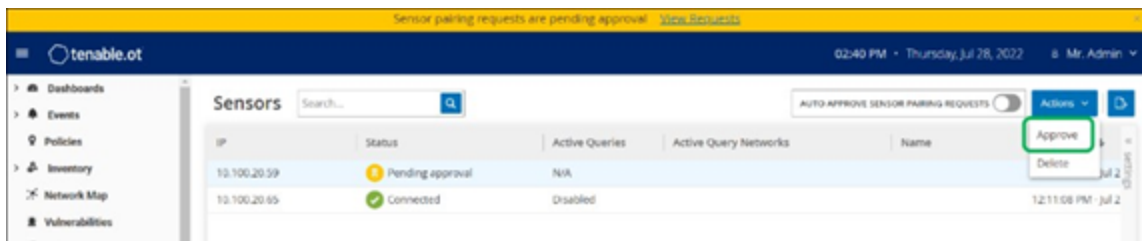


11. In the ICP UI, return to the **Local Settings > System Configuration > Sensors** screen.

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 Sensor, 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](#).

**Note:** 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.

## Setting up the Sensor

There are two models of the Sensor, the Rack Mount Sensor and the Configurable Sensor, as described in section OT Security 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

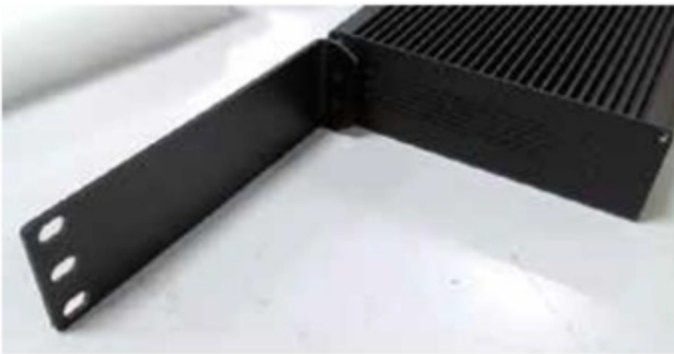
---

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 OT Security 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).



**Note:** 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 OT Security Sensor on a flat surface:

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

**Note:** 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

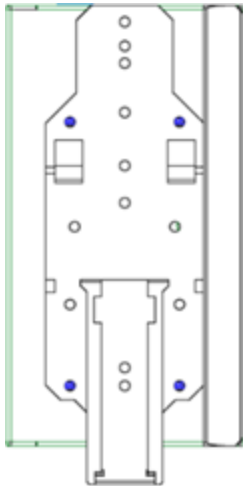
A Configurable Sensor can be mounted on a DIN rail or it can be mounted on a standard 19-inch mounting rack (using the “mounting ears” adapter kit).

### DIN Rail Mounting

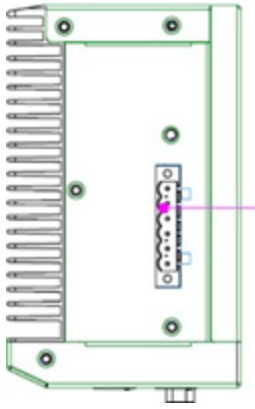
The Configurable Model can be mounted on a DIN Rail using the following procedure.

To mount the OT Security 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.

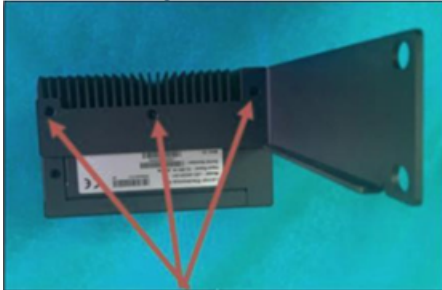
## Rack Mounting (for Configurable model)

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:



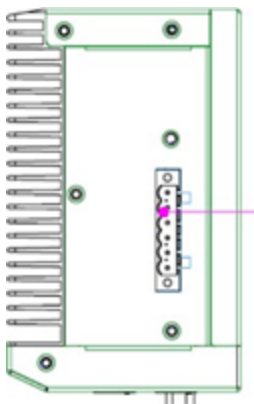
1. Prepare the unit for rack mounting, as follows:
  - a. Remove 3 screws from each side of the unit.
  - b. Attach the "mounting ears" on both sides of the unit, using new screws (provided).



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

**Note:** 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).
4. 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.



---

## Connecting the Sensor to the Network

---

OT Security Sensor is used to collect and forward network traffic to the OT Security 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 OT Security Rack Mount Sensor to the Network:

1. On the OT Security 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 OT Security Configurable Sensor to the Network:

1. On the OT Security 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.





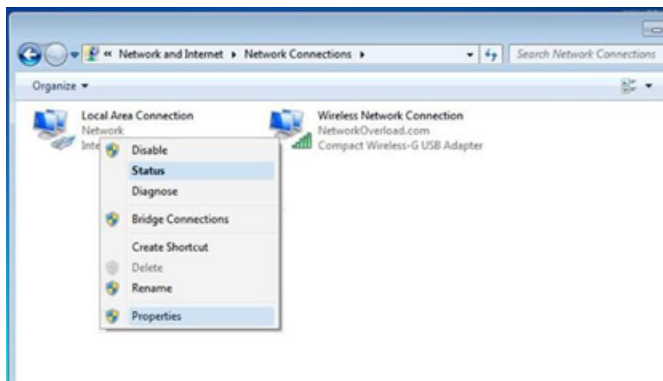
## Accessing the Sensor Setup Wizard

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 OT Security 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 OT Security 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 OT Security Sensor):
  - a. Go to **Network and Internet > Network and Sharing Center > Change adapter settings**.

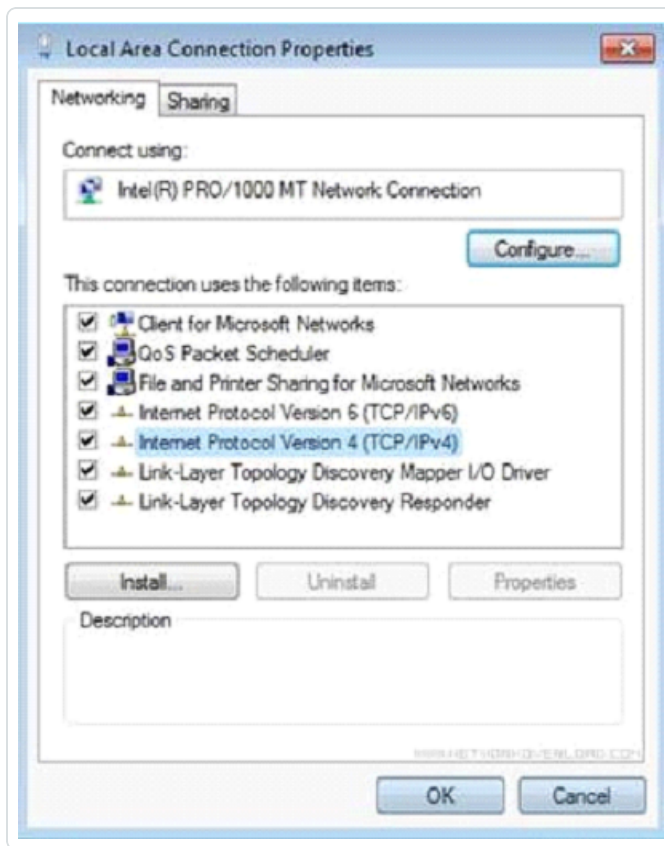
**Note:** Navigation may vary slightly for different versions of Windows.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

- 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 <https://192.168.1.5:8000>.

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

5. [Pair the sensor](#).

## Management Console UI Elements

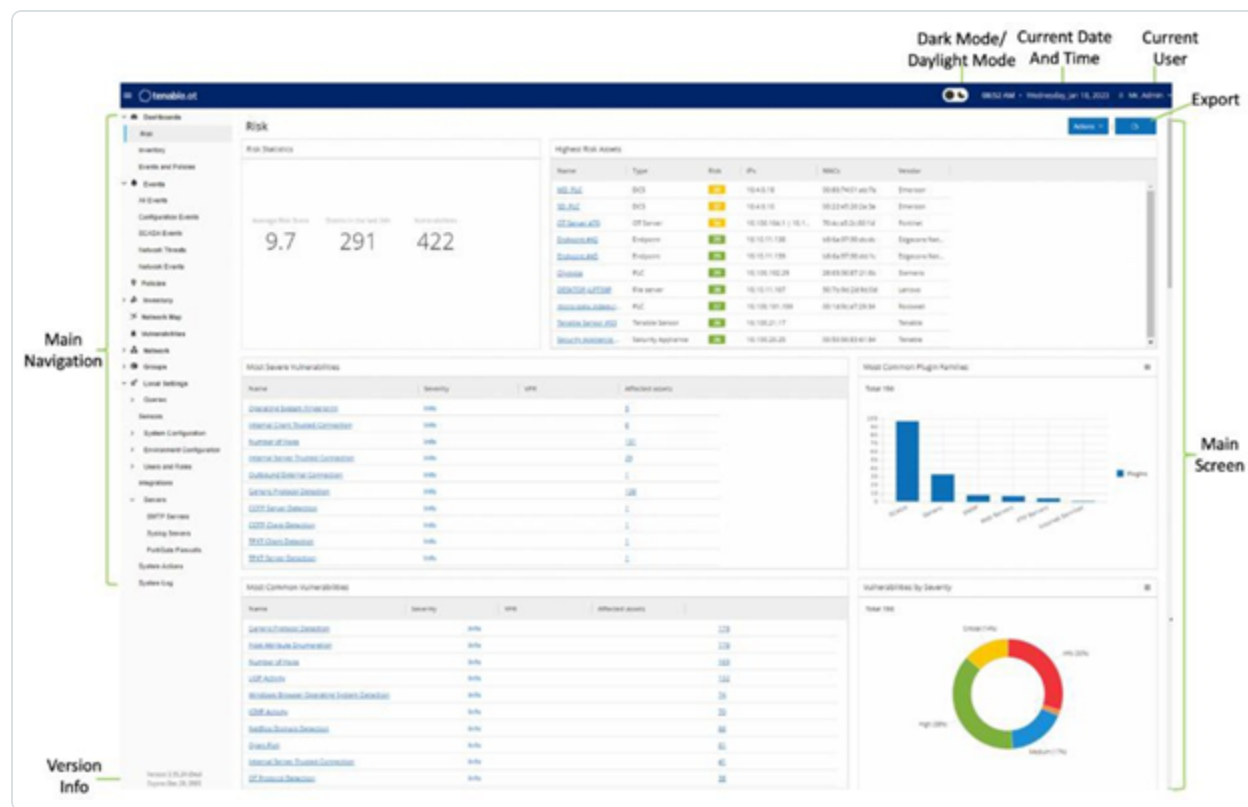
The Management Console UI provides easy access to important data discovered by OT Security relating to asset management, network activity and security events. You can use the UI to configure




the OT Security 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.

UIElement	Description
<b>Main Navigation</b>	Main navigation menu. Click on the  icon to show/hide the main navigation menu
<b>Current Date and Time</b>	Shows the current date and time as registered in the system.
<b>Current User Name</b>	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 (shows software info) or Logout.
<b>License Info</b>	Shows the OT Security software version and the license expiration date.
<b>Main Screen</b>	Displays the screen that was selected in the Main Navigation.



<b>Dark Mode/Daylight Mode</b>	Changes the display color scheme to Dark mode or Daylight mode.
<b>Export</b>	Downloads a PDF of the dashboard.





---

## Turning On/Off Dark Mode

---

The user may use the Dark Mode color scheme on all screens by toggling the Dark Mode switch.

To turn on/off Dark Mode:

1. Click the **Dark Mode** button  at the top of the screen to turn on Dark Mode.  
The setting is applied to all screens and the **Daylight Mode** button  is shown.
2. To restore the Daylight Mode setting, click the **Daylight Mode** button.



## Checking Current Software Version

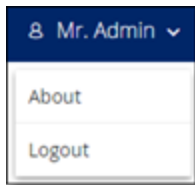
The user can check the version of his software using the username button in the top-right corner of the header bar.

To display the current software version:

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.







---

## 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 OT Security 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](#).

## Working with Lists

The various OT Security 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.

**Note:** 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**.



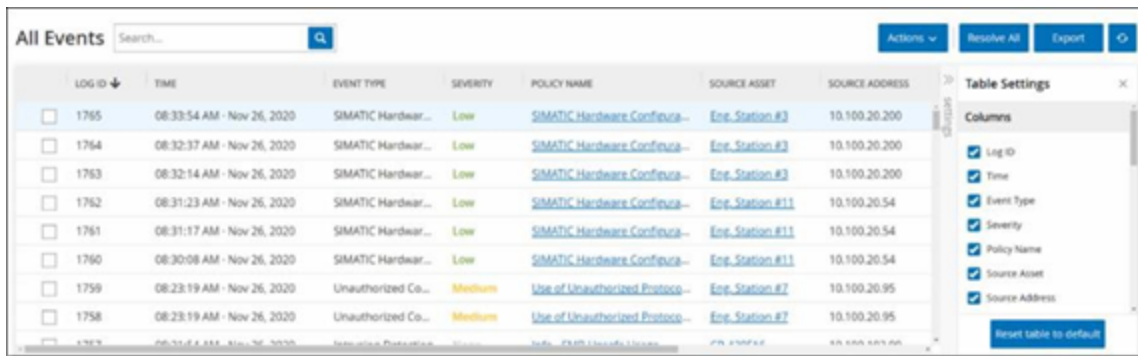
## Customizing the Column Display

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

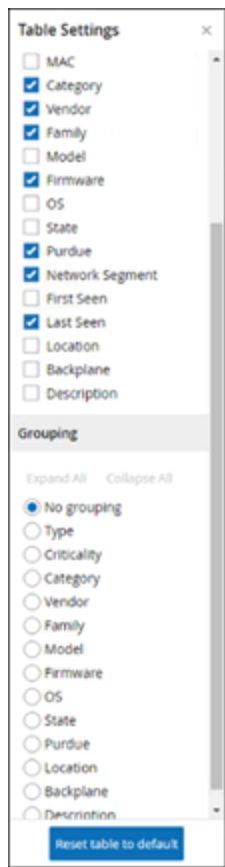
For each of the Inventory screens, you can group the lists by various parameters that are relevant to that particular screen.

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.



The screenshot shows the 'All Assets' interface. At the top, there is a search bar and a list of asset categories with counts: Camera(1), Controller(6), Communication Module(27), DCU(5), Engineering Station(26), HMI(1), Industrial Switch(3), I/O Module(10), Network Device(5), OI Device(27), OI Server(7), PLC(87), Power Supply(3), Printer(1), RTU(3), Serial Ethernet Bridge(1), Server(147), Switch(3), Endpoints(138), and Workstation(19). On the right, the 'Table Settings' sidebar is open, showing checkboxes for various attributes: Category, Vendor, Family, Model, Firmware, OS, State, Purview, Network Segment, First Seen, Last Seen, Location, Backplane, and Description. Below these, the 'Grouping' section shows 'Expand All' and 'Collapse All' buttons, and a list of attributes to group by: No grouping, Type, Criticality, Category, Vendor, Family, Model, Firmware, OS, State, Purview, Location, Backplane, and Description. A 'Reset table to default' button is at the bottom of the sidebar.

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.

The screenshot shows the 'All Assets' interface with the 'Communication Module' category expanded. The table displays the following data:

	Name	Type	Risk Score	Criticality	IP	Category	Vendor	Family
>	Camera(1)							
>	Controller(6)							
>	Communication Module(27)							
<input type="checkbox"/>	<a href="#">Comm_Adapter_#56</a>	Communication M...	25	High	10.100.101.151   10.100...	Controllers	Rockwell	
<input type="checkbox"/>	<a href="#">Comm_Adapter_#64</a>	Communication M...	25	High	10.100.101.151   10.100...	Controllers	Rockwell	
<input type="checkbox"/>	<a href="#">Comm_Adapter_#62</a>	Communication M...	25	High	10.100.101.151   10.100...	Controllers	Rockwell	
<input type="checkbox"/>	<a href="#">Comm_Adapter_#52</a>	Communication M...	25	High	10.100.101.151   10.100...	Controllers	Rockwell	
<input type="checkbox"/>	<a href="#">Comm_Adapter_#70</a>	Communication M...	25	High	10.100.105.24	Controllers	Schneider	
<input type="checkbox"/>	<a href="#">Comm_Adapter_#53</a>	Communication M...	25	High	10.100.101.151   10.100...	Controllers	Rockwell	
<input type="checkbox"/>	<a href="#">BMX_NOC001</a>	Communication M...	16	High	10.100.105.40	Controllers	Schneider	
<input type="checkbox"/>	<a href="#">QM_1142-1_1</a>	Communication M...	16	High	10.100.102.70   10.100.1...	Controllers	Siemens	
<input type="checkbox"/>	<a href="#">00300E22830C</a>	Communication M...	3	High	10.100.111.5	Controllers	Wago Corporation	
<input type="checkbox"/>	<a href="#">Comm_Adapter_#253</a>	Communication M...	6	High		Controllers	Rockwell	



## 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).



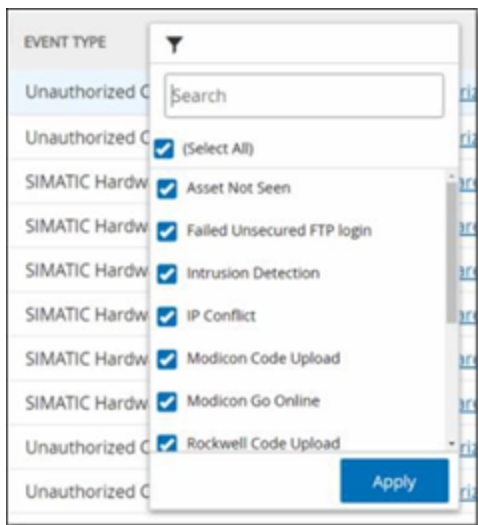
## Filtering

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.

**Note:** 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 OT Security UI (e.g. Events, Inventory etc.) as a CSV file.

**Note:** 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**.

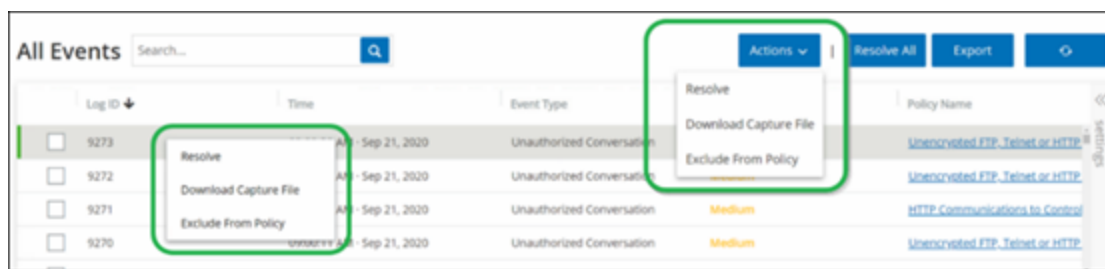


## Actions Menu

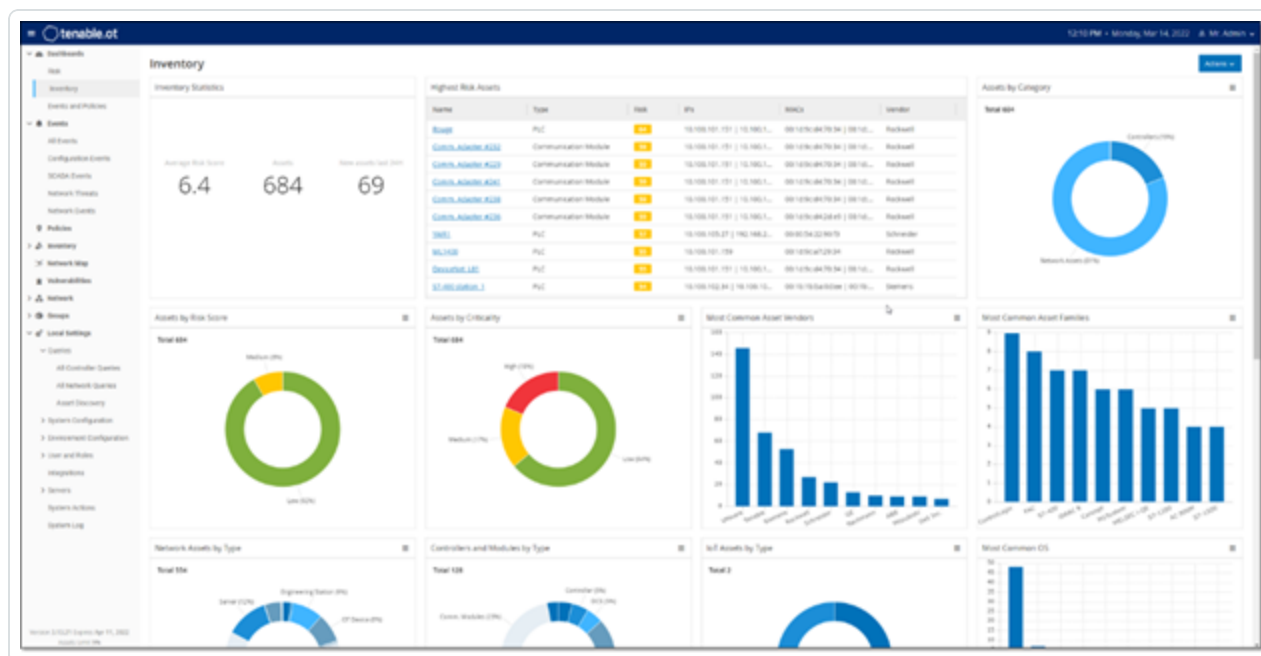
Each screen has a series of Actions that can be taken for the elements listed on that screen. For example, on the Policies screen you can *View*, *Edit*, *Duplicate* or *Delete* a Policy; on the Events screen, you can *Resolve* or *Download Capture File* for an Event etc.

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



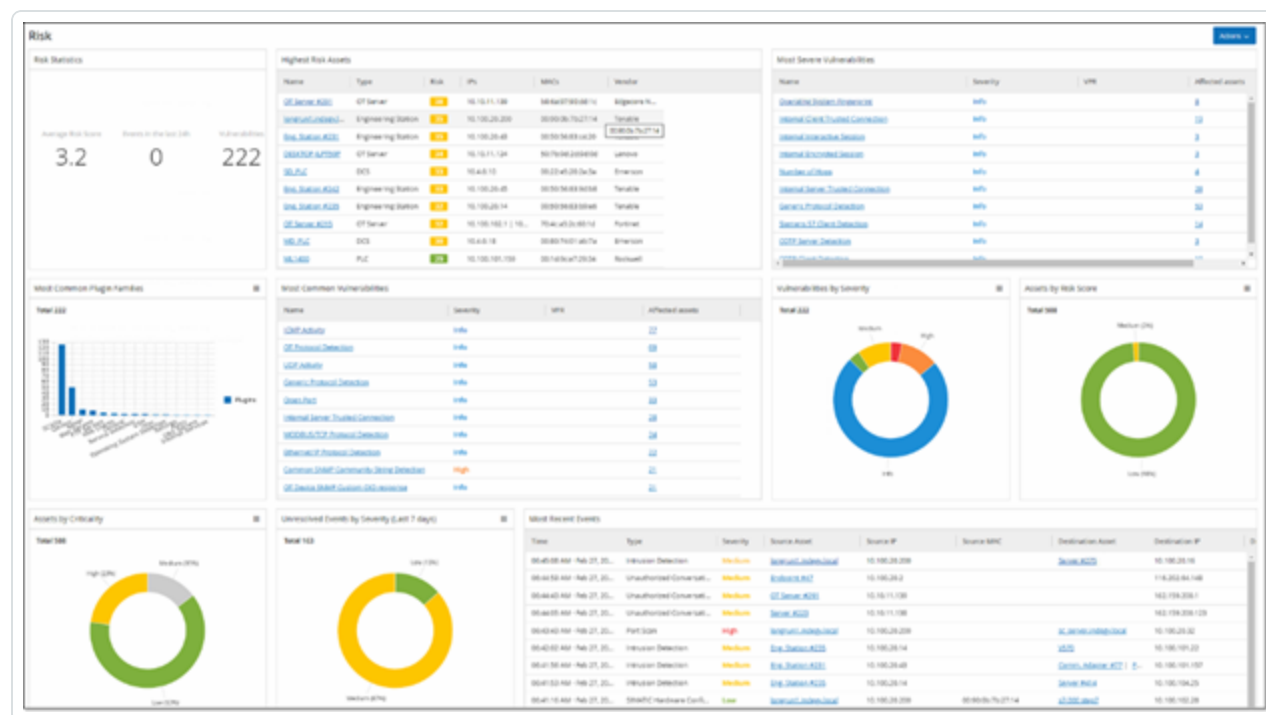


There are three dashboards: Risk, Inventory, and Events and Policies. The dashboards contain widgets that offer an at-a-glance view of your network's inventory and security posture. You can choose a dashboard from the Main Navigation or by clicking on the **Dashboards** button in the upper-right corner, 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](#).



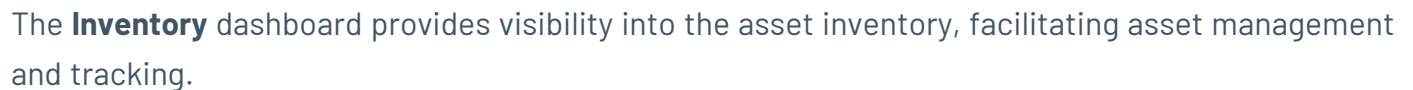
# Risk Dashboard



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.

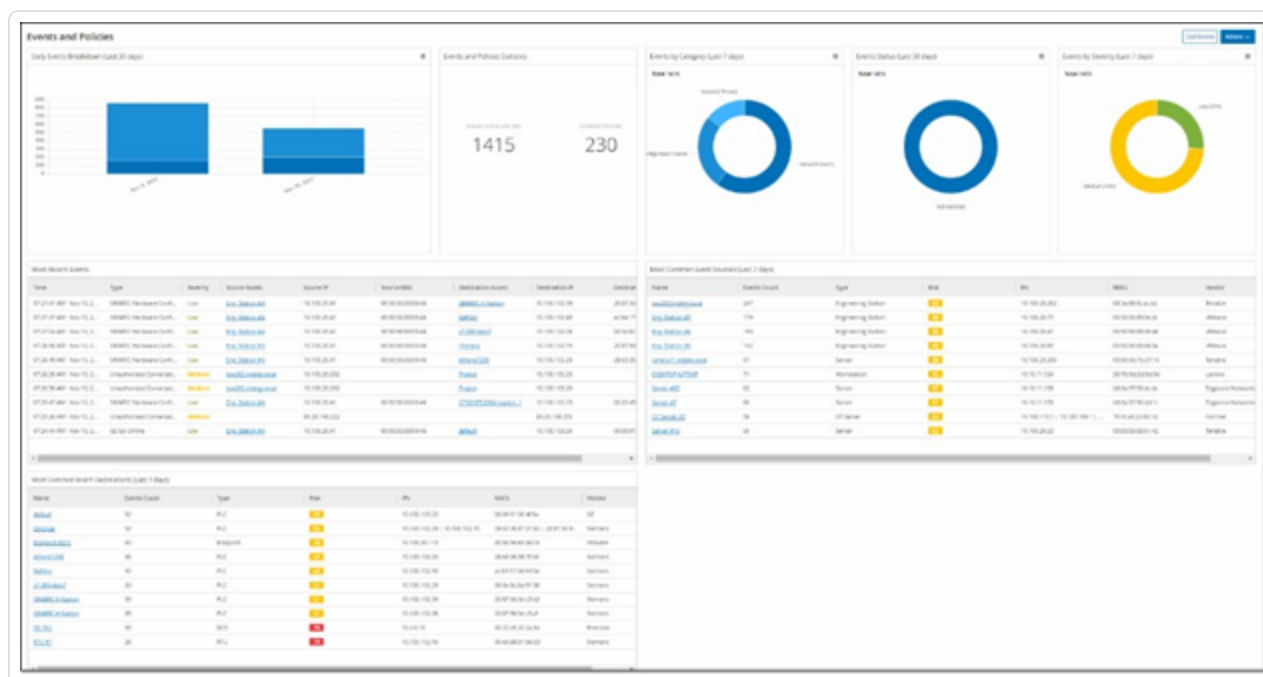
Clicking on an asset or Vulnerability link takes you to the corresponding element on the Inventory or Vulnerabilities screen, respectively.



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.

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





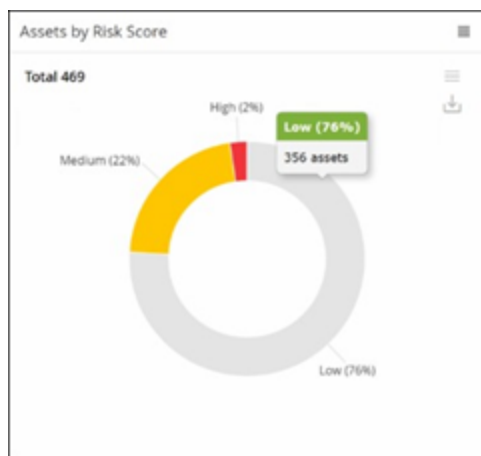
## Graph mode

Graph mode shows a graphic visualization of the widget data.

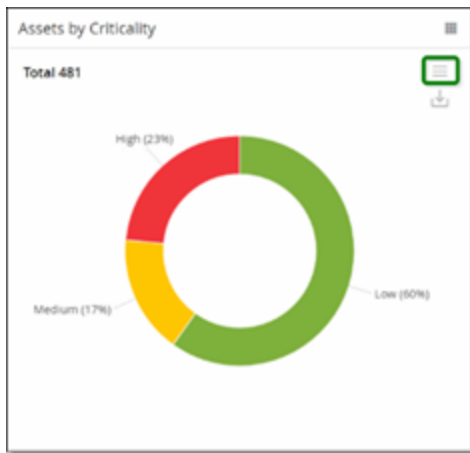


You can interact with the widgets in the following ways:

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



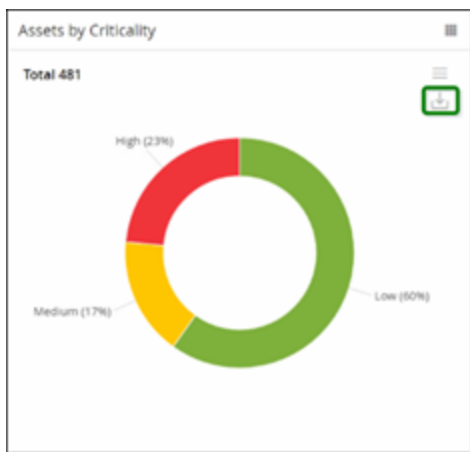
- You can adjust the type of chart used for the display by clicking on the **Settings** button in the top right corner.



- 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.

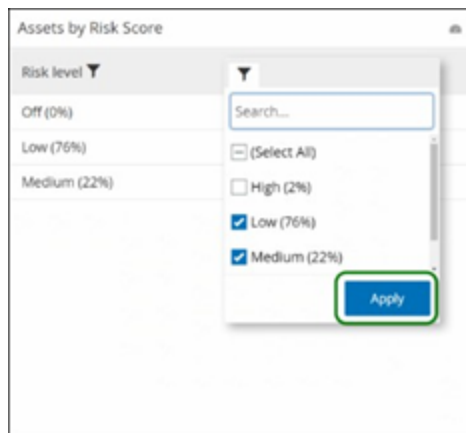




## Table mode

Risk level	Count
Off (0%)	0
Low (76%)	356
Medium (22%)	102
High (2%)	11

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.

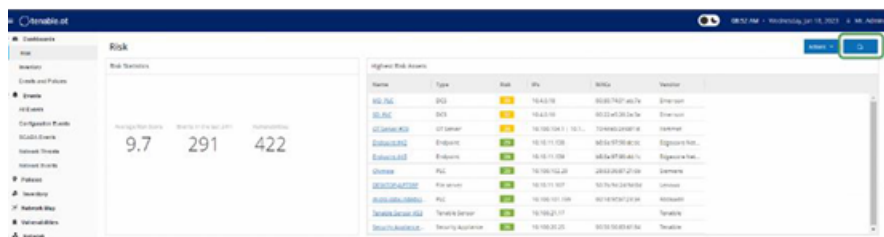


## Exporting the Dashboard

The Export button of the Dashboard screen exports a PDF with each Dashboard widget on a separate page.

To export the Dashboard:

1. In the top-right corner of the Dashboard, click the Export button ( ).



The PDF downloads automatically to the default download folder.

**Note:** Make sure to leave the Dashboard tab open in your browser while the PDF download is in progress (2-3 seconds).

2. After the file has downloaded, navigate to the file that was just downloaded to view or share it.

## 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.

- 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.

**Note:** By default, most policies are turned on. To turn Policies on/off see [Policies](#).



---

## 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 OT Security 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.

**Note:** 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 OT Security). For an explanation of how to interpret Syslog notifications see OT Security 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.

**Note:** 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	Affected Asset,	A change was made to the firmware running on the controller.



version	Schedule	
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.

**Note:** 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
<b>Asset not seen</b>	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.
<b>Change in USB configuration</b>	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.
<b>IP conflict</b>	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.
<b>Network Baseline Deviation</b>	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 <a href="#">SETTING A NETWORK BASELINE</a> . 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.
<b>New asset discovered</b>	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.
<b>Open port</b>	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.
<b>Spike in network traffic</b>	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.
<b>Spike in conversation</b>	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.
<b>RDP connection (authenticated)</b>	Source, Destination,	An RDP (Remote Desktop Connection) was made in the network using authentication credentials. The



	Schedule	Policy applies to asset in the Source Asset Group connecting to an asset in the Destination Asset Group during the specified time range.
<b>RDP connection (not authenticated)</b>	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.
<b>Unauthorized conversation</b>	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.
<b>Successful unsecured FTP login</b>	Source, Destination, Schedule	FTP is considered to be an unsecure protocol. This Policy detects successful logins using FTP.
<b>Failed unsecured FTP login</b>	Source, Destination, Schedule	FTP is considered to be an unsecure protocol. This Policy detects failed login attempts using FTP.
<b>Successful unsecured Telnet login</b>	Source, Destination, Schedule	Telnet is considered to be an unsecure protocol. This Policy detects successful logins using Telnet.
<b>Failed unsecured Telnet login</b>	Source, Destination, Schedule	Telnet is considered to be an unsecure protocol. This Policy detects failed login attempts using Telnet.
<b>Unsecured Telnet login attempt</b>	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.

**Note:** 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.
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.

**Note:** 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
<b>Modbus illegal data address</b>	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.
<b>Modbus illegal data value</b>	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.
<b>Modbus illegal function</b>	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.
<b>Unauthorized write</b>	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.
<b>ABB - Unauthorized write</b>	Source Asset, Destination Asset,	Detects write commands sent over MMS to ABB 800xA controllers that are out of the allowed range.





	Schedule	
<b>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)</b>	Source Asset, Destination Asset, Schedule	Detects specific commands sent to IEC-104 master or slave units that are considered to be risky.
<b>DNP3 Commands</b>	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.

**Note:** 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.

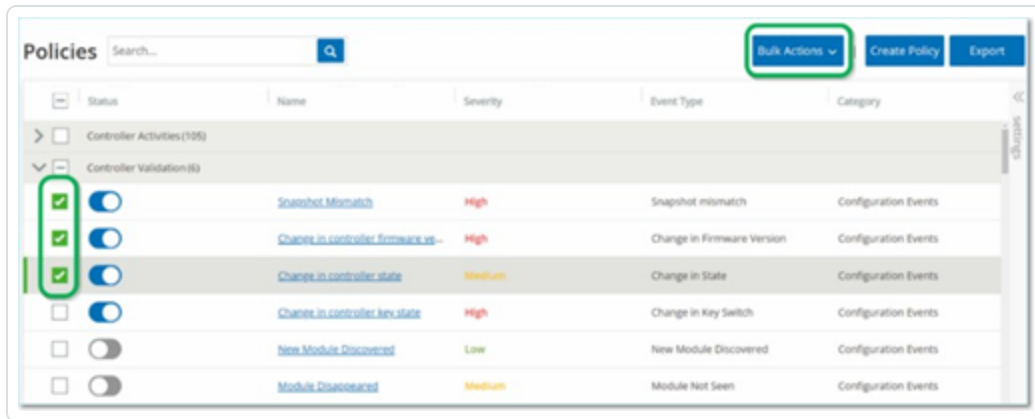
Status	Name	Severity	Event Type	Category
<input type="checkbox"/>	Controller Activities (185)			
<input checked="" type="checkbox"/>	Controller Validation (8)			
<input type="checkbox"/>	Snapshot Mismatch	High	Snapshot mismatch	Configuration Events
<input type="checkbox"/>	Change in controller firmware version	High	Change in Firmware Version	Configuration Events
<input type="checkbox"/>	Change in controller state	Medium	Change in State	Configuration Events
<input type="checkbox"/>	Change in controller key state	High	Change in Key Switch	Configuration Events
<input type="checkbox"/>	New Module Discovered	Low	New Module Discovered	Configuration Events
<input type="checkbox"/>	Module Disappeared	Medium	Module Not Seen	Configuration Events
<input checked="" type="checkbox"/>	Network Events (54)			
<input type="checkbox"/>	Asset Not Seen for 1 Hour	Low	Asset Not Seen	Network Events
<input type="checkbox"/>	Controller Not Seen for 1 Hour	Low	Asset Not Seen	Network Events
<input type="checkbox"/>	New Asset Discovered	Low	New asset discovered	Network Events

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 [Management Console UI Elements](#).

The Policy parameters are described in the following table.

Parameter	Description
-----------	-------------



<b>Status</b>	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.
<b>Policy ID</b>	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.).
<b>Name</b>	The name of the Policy.
<b>Severity</b>	The degree of severity of the Event. Possible values are: None, Low, Medium or High. See section <a href="#">Viewing Policies</a> for a description of the severity levels.
<b>Event Type</b>	The specific type of event that triggers this Event Policy.
<b>Category</b>	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 <a href="#">Viewing Policies</a> .
<b>Source</b>	A Policy condition. The source Asset Group/Network Segment (i.e. the asset that initiated the Activity) to which the Policy applies.
<b>Destination/ Affected Asset</b>	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.
<b>Schedule</b>	A Policy condition. The time range for which the Policy applies.
<b>Syslog</b>	The Syslog server (SIEM) where Events for this Policy are logged.
<b>Email</b>	The Email Group to which Event notifications for this Policy are sent.
<b>Sub Category</b>	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 <a href="#">Viewing Policies</a> .
<b>Number of Events per</b>	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



<b>Policy</b>	that had the most violations/events.
<b>Exclusions</b>	Lists the number of exclusions that were added to each policy. For more information, see <a href="#">Events</a> .

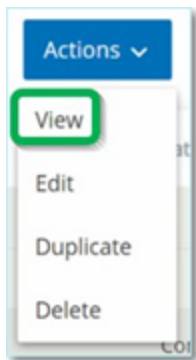


## Viewing Policy Details

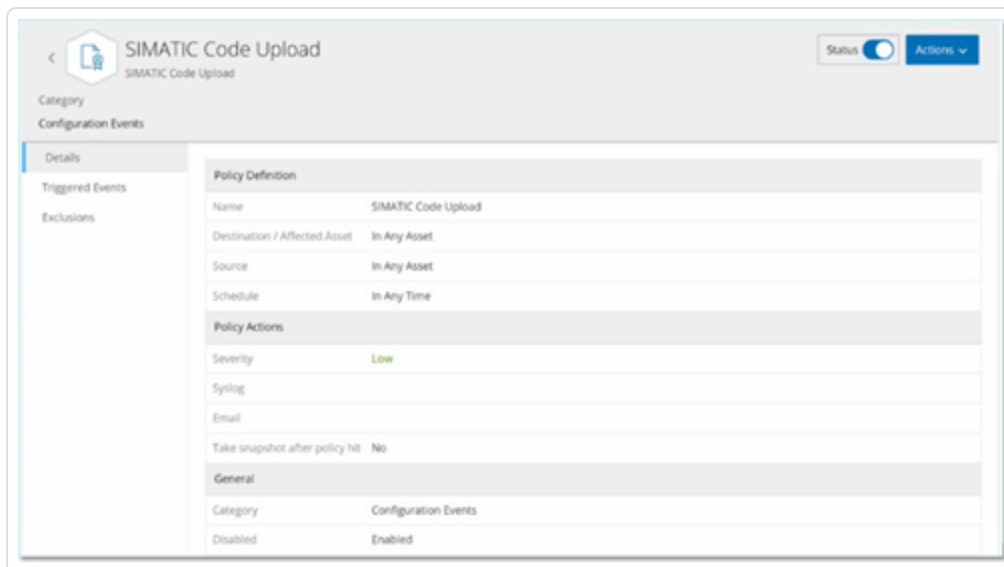
You can open the Policy Details screen for a Policy to view additional details about the Policy. This screen shows a complete listing of all Policy conditions. It also shows a listing of all Events triggered by the selected Policy.

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.



The Policy Details screen is shown for the selected Policy.



**Note:** Alternatively, you can access the Actions menu by right-clicking on the relevant 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 [Events](#). 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.



**Note:** 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 [Creating Policies](#).

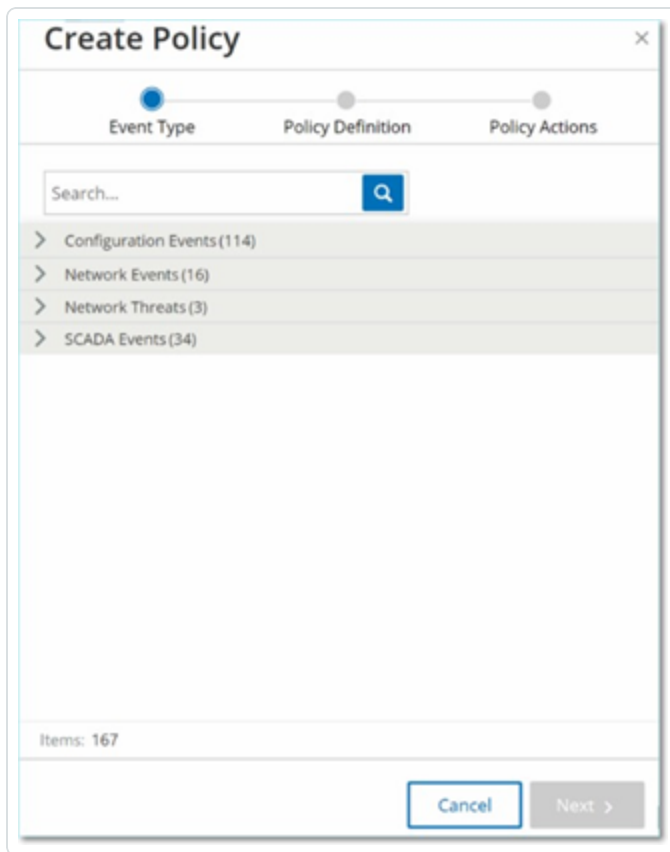
**Note:** If, after creating a Policy, you find that the Policy is generating Events for situations that don't require attention, you can exclude specific conditions from the Policy, see [Events](#).

To Create a New Policy:

1. On the **Policies** screen, click **Create Policy**.

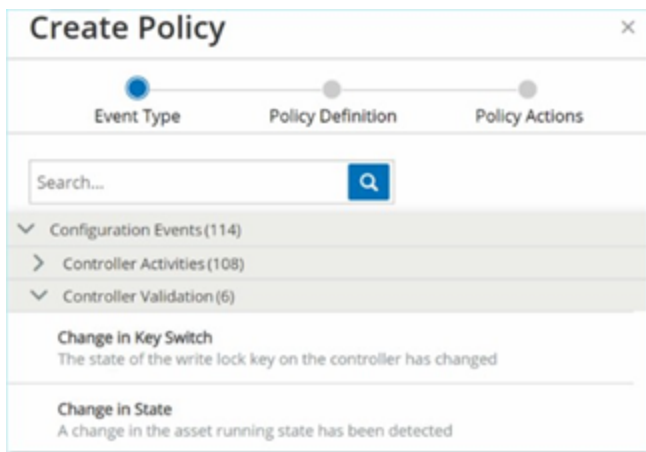
The **Create Policy** wizard opens.





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.

**Create Policy**

Event Type Policy Definition Policy Actions

Change in Firmware Version

Policy name \*

Affected Assets \*

In Select + Or

+ And

Schedule group \*

In Select

< Back Cancel Next >

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.

**Note:** 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:

- Where relevant, select **In** (default) to whitelist the selected element or Not in to blacklist the selected element.
- 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.

**Note:** 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 next to 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.

**Create Policy**

Event Type Policy Definition Policy Actions

Change in Firmware Version

**Severity** <sup>+</sup>

High Medium Low None

**Syslog**

Syslog servers are not configured

**Email group**

SMTP servers are not configured

< Back Cancel Create

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.

**Note:** To add a Syslog server, see [Syslog Servers](#).

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.

**Note:** To add an SMTP server, see [SMTP Servers](#).

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 desired 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.

**Note:** 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

---



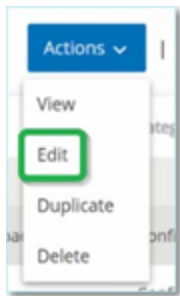
## Editing Policies

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.



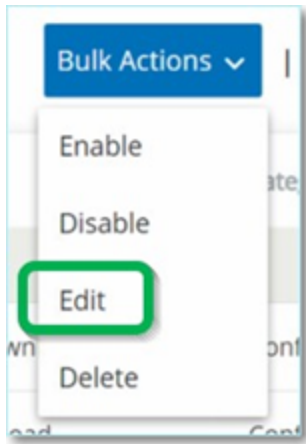


3. Adjust the *Policy Definition* parameters as desired.
4. Click **Next**.
5. Adjust the *Policy Actions* parameters as desired.
6. Click **Save**.

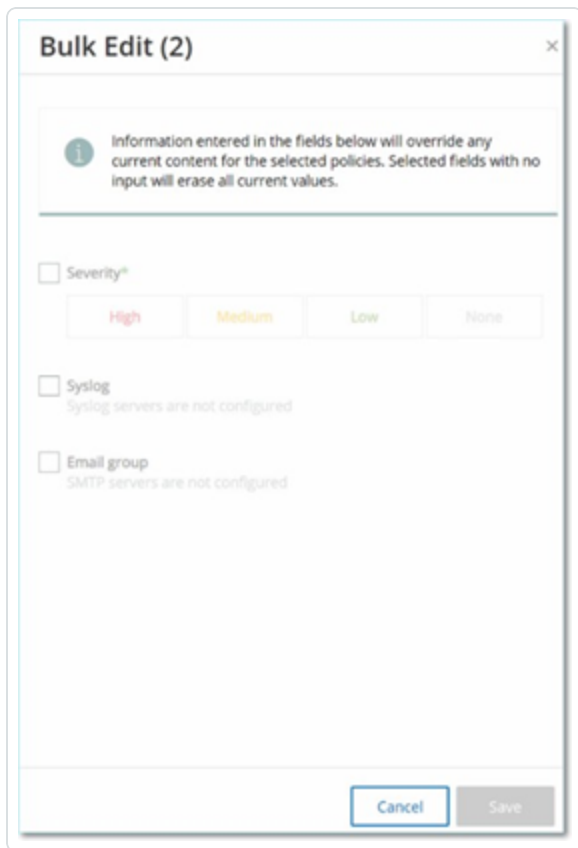
The Policy is saved with the new configuration.

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.



**Bulk Edit (2)**

Information entered in the fields below will override any current content for the selected policies. Selected fields with no input will erase all current values.

☐ Severity<sup>\*</sup>

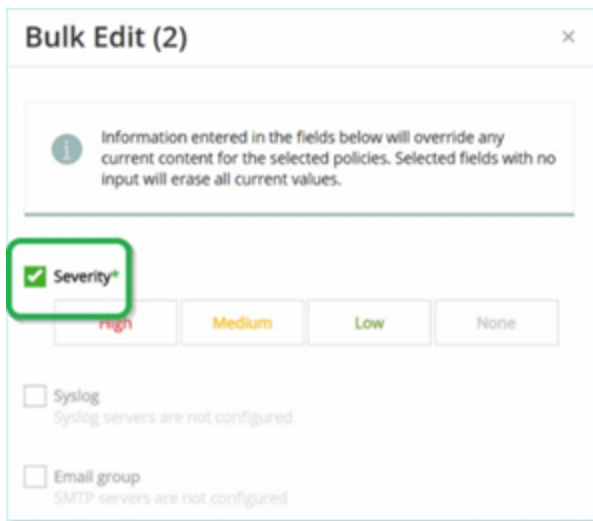
High Medium Low None

☐ Syslog  
Syslog servers are not configured

☐ Email group  
SMTP servers are not configured

Cancel Save

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



**Bulk Edit (2)**

Information entered in the fields below will override any current content for the selected policies. Selected fields with no input will erase all current values.

☒ Severity<sup>\*</sup>

High Medium Low None

☐ Syslog  
Syslog servers are not configured

☐ Email group  
SMTP servers are not configured

4. Set each parameter as desired.



**Note:** 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.

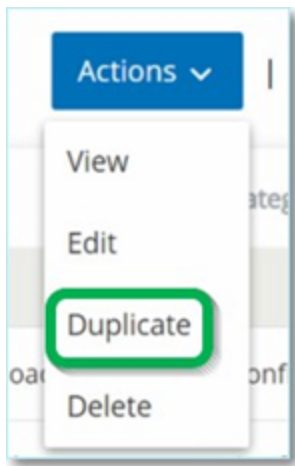


## Duplicating Policies

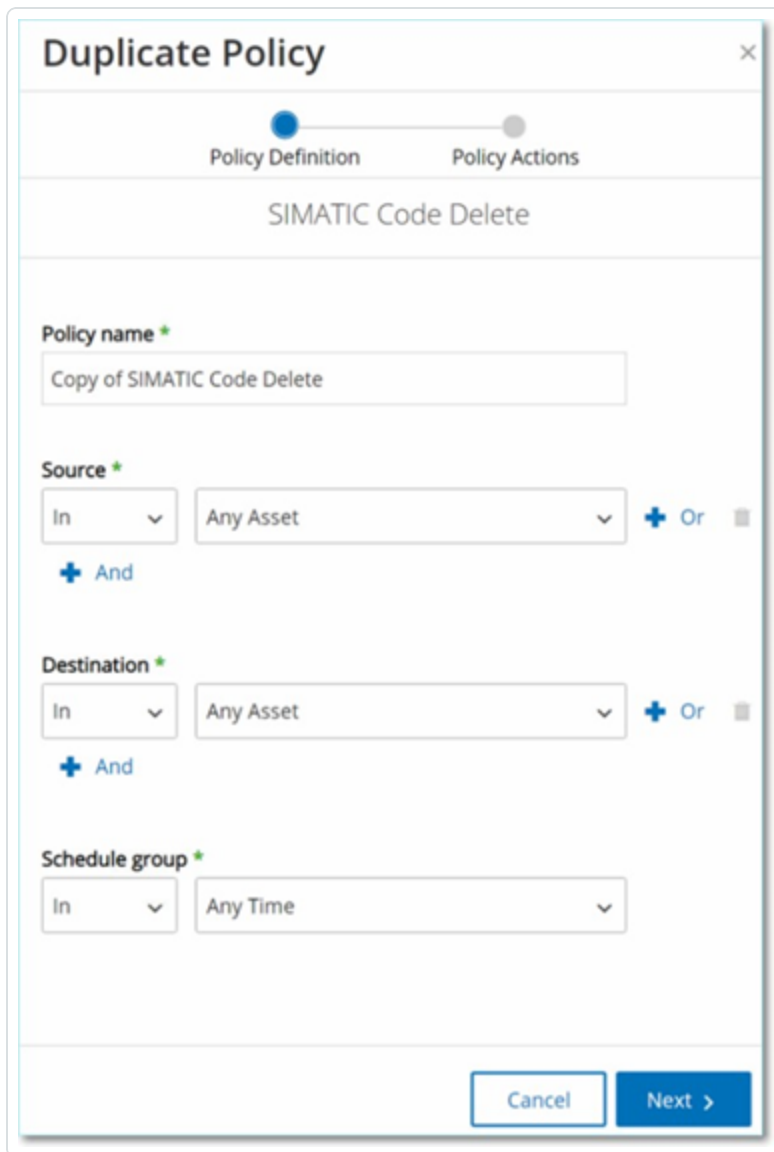
You can create a new Policy that is similar to an existing Policy by Duplicating the original Policy and making the desired adjustments. You can duplicate both predefined and user defined Policies (except for Intrusion Detection Policies).

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>".



The image shows a 'Duplicate Policy' dialog box with a close button (X) in the top right corner. At the top, there is a progress bar with two steps: 'Policy Definition' (active, indicated by a blue dot) and 'Policy Actions' (inactive, indicated by a grey dot). Below the progress bar, the title 'SIMATIC Code Delete' is displayed. The main content area contains three sections, each with a required field (marked with a green asterisk):

- Policy name \***: A text input field containing 'Copy of SIMATIC Code Delete'.
- Source \***: A section with two dropdown menus. The first dropdown is set to 'In' and the second to 'Any Asset'. To the right of these dropdowns are two buttons: a blue '+' button and an 'Or' button. Below the dropdowns is a blue '+' button labeled 'And'.
- Destination \***: A section with two dropdown menus. The first dropdown is set to 'In' and the second to 'Any Asset'. To the right of these dropdowns are two buttons: a blue '+' button and an 'Or' button. Below the dropdowns is a blue '+' button labeled 'And'.
- Schedule group \***: A section with two dropdown menus. The first dropdown is set to 'In' and the second to 'Any Time'.

At the bottom right of the dialog box, there are two buttons: 'Cancel' and 'Next >'.

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

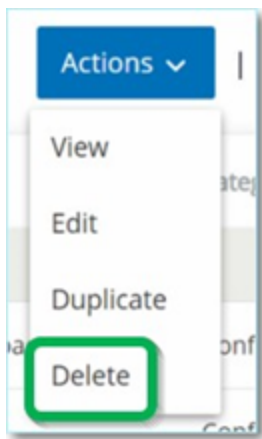
You can delete a Policy from the system. You can delete both predefined and user defined Policies (except for Intrusion Detection Policies which can't be deleted).

You can also delete multiple Policies in a bulk action.

**Note:** 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.



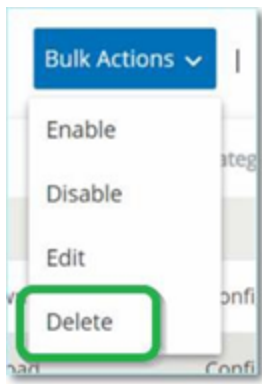
A confirmation window is displayed.

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.

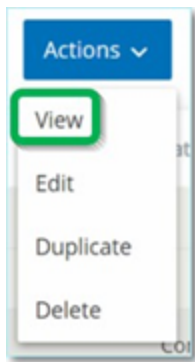


## Deleting Policy Exclusions

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

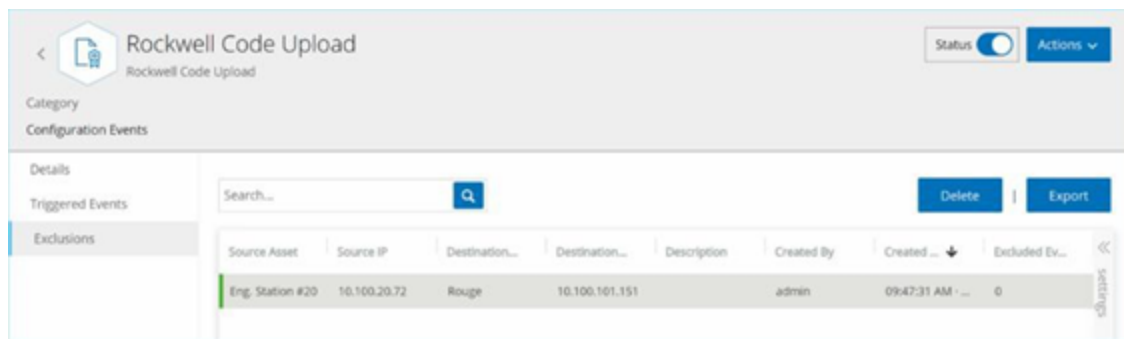
To delete a Policy Exclusion:

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



**Note:** 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.

**Note:** 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 screenshot shows the 'Asset Groups' interface. At the top, there is a search bar with the text 'Search...' and a magnifying glass icon. To the right of the search bar are two buttons: 'Create Asset Group' and 'Export'. Below the search bar is a table with the following columns: 'Name', 'Type', 'Members', and 'Used in Policies'. The table is filtered to show 'Predefined asset groups (92)'. The first row is '3D Printers' with 'Function Group' as the type. The second row is 'ABB 800X Controllers' with 'Function Group' as the type and 'Use of Unauthorized Protocols in ABB 800X Controllers | Use of Unauthorized ...' as the policy. The third row is 'ABB Masterbus300 Controllers' with 'Function Group' as the type. The fourth row is 'ABB TotalFlow Controllers' with 'Function Group' as the type. The fifth row is 'Actuators' with 'Function Group' as the type.

Name	Type	Members	Used in Policies
Predefined asset groups (92)			
3D Printers	Function Group		
ABB 800X Controllers	Function Group		Use of Unauthorized Protocols in ABB 800X Controllers   Use of Unauthorized ...
ABB Masterbus300 Controllers	Function Group		
ABB TotalFlow Controllers	Function Group		
Actuators	Function Group		

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
<b>Status</b>	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.
<b>Name</b>	The name of the Policy.
<b>Severity</b>	The degree of severity of the Event. Possible values are: None, Low, Medium or High. See section <a href="#">Severity Levels</a> for a description of the severity levels.
<b>Event Type</b>	The specific type of event that triggers this Event Policy.
<b>Category</b>	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 <a href="#">Policy Categories and Sub-Categories</a> .
<b>Source</b>	A Policy condition. The source Asset Group (i.e. the asset that initiated the Activity) to which the Policy applies.



<b>Name</b>	The name that is used to identify the Group.
<b>Type</b>	<p>Shows the type of Group. Options are:</p> <ul style="list-style-type: none"><li>• Function – A predefined Asset Group that was created to serve a particular function.</li><li>• Asset List – Specified assets are included in the Group.</li><li>• IP List – Assets with the specified IP Address.</li><li>• IP Range – Assets within the specified range of IP Addresses.</li></ul>
<b>Members</b>	<p>Shows the list of assets that are included in this Group. No value is shown for Function Groups.</p> <div><b>Note:</b> If there isn't room to display all assets in this row then click on <b>Table Actions &gt; View &gt; Members</b> tab.</div>
<b>Used in Policies</b>	<p>Shows the name of each Policy that uses this Asset Group in its configuration.</p> <div><b>Note:</b> To view more details about the Policies in which the Group is used, click on <b>Table Actions &gt; View &gt; Used in Policies</b> tab.</div>

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:

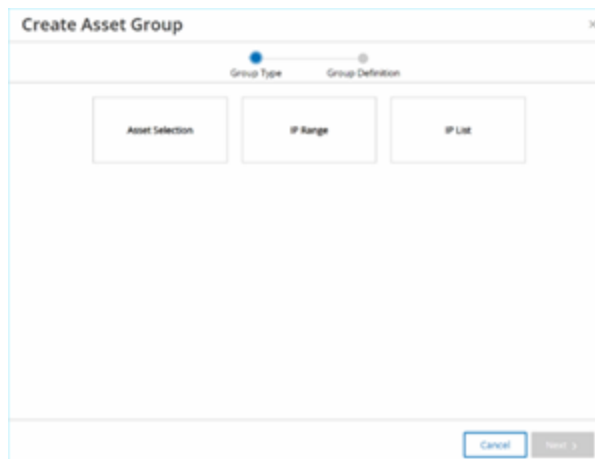
- **Asset List** – Specify the specific assets that are included in the Group.
- **IP List** – Specify the IP addresses of the Assets that are included in the Group.
- **IP Range** – Specify the range of IP addresses of the Assets that are included in the Group.

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

To Create an Asset Selection Type Asset Group:

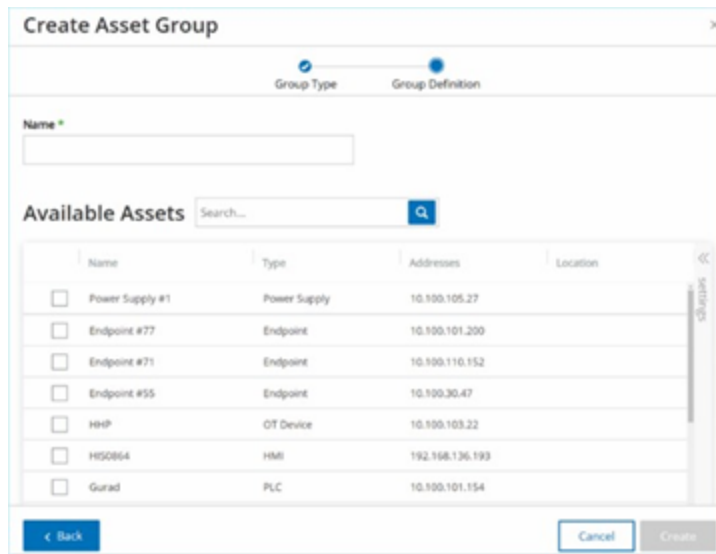
1. Under Groups, select Asset Groups.
2. Click **Create Asset Group**.

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



3. Click on Asset Selection.
4. Click **Next**.

The list of **Available Assets** is displayed.



The screenshot shows the 'Create Asset Group' wizard. At the top, there are two steps: 'Group Type' (selected) and 'Group Definition'. Below the steps is a 'Name' field with a green asterisk. Underneath is a section titled 'Available Assets' with a search bar. A table lists several assets with checkboxes for selection. The table has columns for Name, Type, Addresses, and Location. At the bottom, there are three buttons: '< Back', 'Cancel', and 'Create'.

Name	Type	Addresses	Location
<input type="checkbox"/> Power Supply #1	Power Supply	10.100.105.27	
<input type="checkbox"/> Endpoint #77	Endpoint	10.100.101.200	
<input type="checkbox"/> Endpoint #71	Endpoint	10.100.110.152	
<input type="checkbox"/> Endpoint #55	Endpoint	10.100.30.47	
<input type="checkbox"/> HWP	OT Device	10.100.103.22	
<input type="checkbox"/> H50854	HMI	192.168.136.193	
<input type="checkbox"/> Gurad	PLC	10.100.101.154	

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.

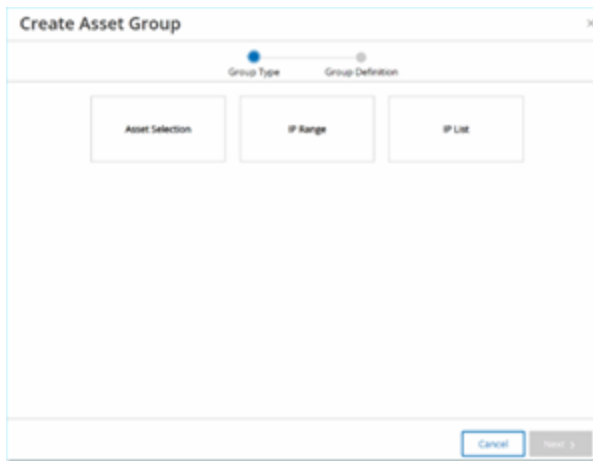
7. When you have finished making your selections, click **Create**.

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.

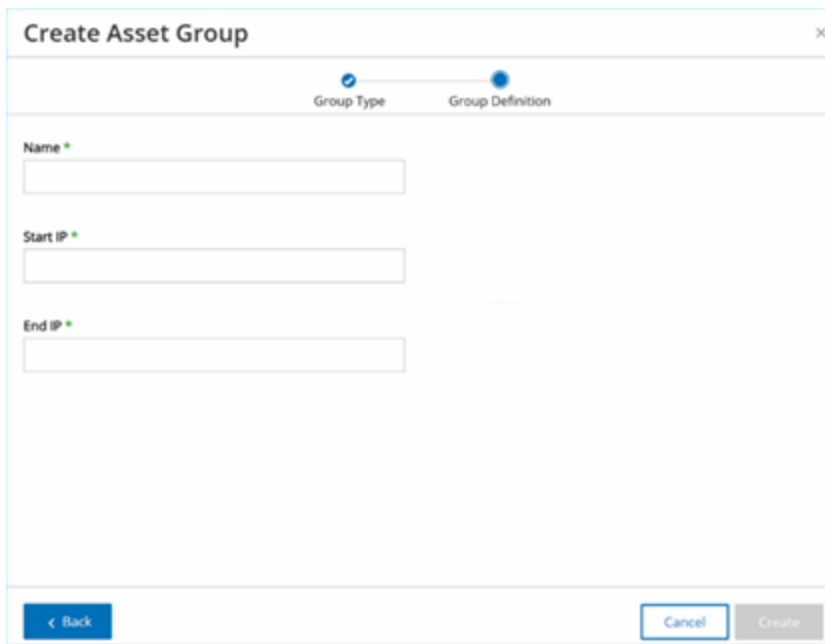
The Create Asset Group wizard is displayed.



The image shows a 'Create Asset Group' dialog box. At the top, there is a progress bar with two steps: 'Group Type' (which is currently selected, indicated by a blue dot) and 'Group Definition'. Below the progress bar, there are three buttons: 'Asset Selection', 'IP Range', and 'IP List'. The 'IP Range' button is highlighted. At the bottom right, there are two buttons: 'Cancel' and 'Next >'. The dialog box has a close button (X) in the top right corner.

3. Click on **IP Range**.
4. Click **Next**.

The IP Range selection parameters are displayed.



The image shows the 'Create Asset Group' dialog box in the 'Group Definition' step. The progress bar at the top now has two blue dots, one under 'Group Type' and one under 'Group Definition'. The 'Group Definition' section is active. It contains three text input fields: 'Name', 'Start IP', and 'End IP'. Each field has a green asterisk next to it, indicating it is required. At the bottom left, there is a blue button labeled '< Back'. At the bottom right, there are two buttons: 'Cancel' and 'Create'. The dialog box has a close button (X) in the top right corner.

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

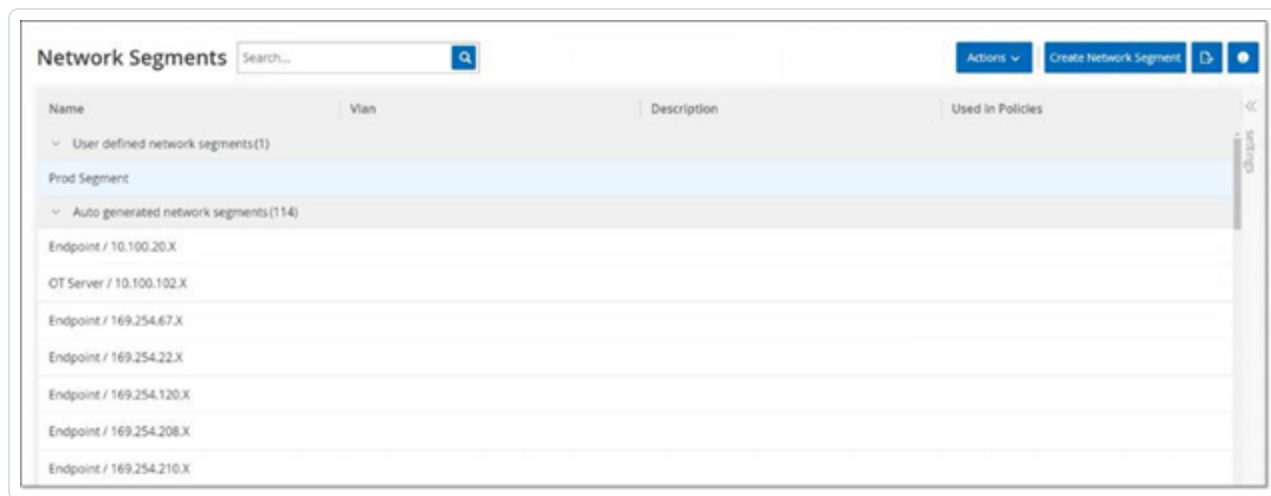
---

Network Segmentation is a method of creating groups of related network assets, assisting in the logical isolation of one group of assets from another. OT Security 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
<b>Name</b>	The name that is used to identify the Network Segment.
<b>VLAN</b>	The VLAN number of the Network Segment. (Optional)
<b>Description</b>	A description of the Network Segment. (Optional)
<b>Used in Policies</b>	Shows the names of the Policies that apply to this Network Segment. <div><b>Note:</b> To view more details about the Policies in which the Network Segment is used, click on <b>Table Actions &gt; View &gt; Used in Policies</b> tab.</div>

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.

The screenshot shows a dialog box titled "Create Network Segment" with a close button (X) in the top right corner. The dialog contains three input fields: "NAME" (with a required field asterisk), "VLAN", and "DESCRIPTION". The "NAME" field has a cursor and the letter "I" entered. The "VLAN" field is empty. The "DESCRIPTION" field is a larger text area, currently empty. At the bottom of the dialog are two buttons: "Cancel" and "Create".

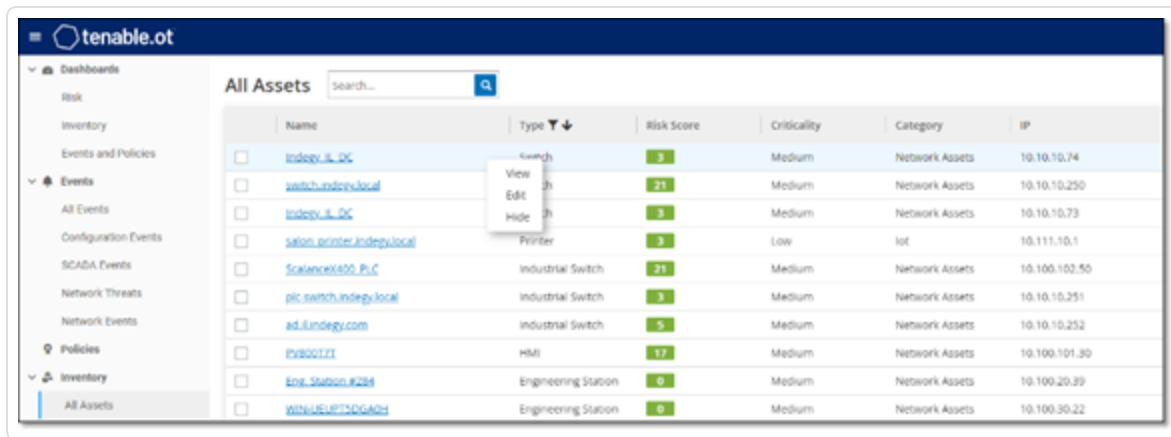
3. In the **Name** field, enter a name for the Network Segment.



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.



Edit Asset Details

TYPE

DCS

NAME

FCS0823

CRITICALITY

High

PURDUE LEVEL

Level 1

NETWORK SEGMENTS (192.168.8.47)

Server Room - 5

NETWORK SEGMENTS (192.168.136.47)

Controller / 192.168.136.X (System Default)

**Note:** 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

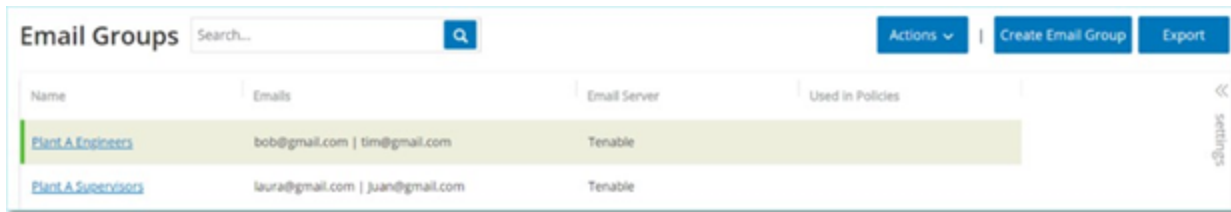
---

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



Name	Emails	Email Server	Used in Policies
<a href="#">Plant A Engineers</a>	bob@gmail.com   tim@gmail.com	Tenable	
<a href="#">Plant A Supervisors</a>	laura@gmail.com   juan@gmail.com	Tenable	

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:

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

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

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.

**Note:** 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.

The screenshot shows a dialog box titled "Create Email Group" with a close button (X) in the top right corner. The dialog contains three main sections: "Name" with a text input field, "SMTP server" with a dropdown menu showing "Select", and "Emails" with a text area labeled "One email per line". At the bottom of the dialog are two buttons: "Cancel" and "Create".

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.

**Note:** 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 Servers](#).

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 screenshot shows a web interface titled 'Port Groups'. At the top, there is a search bar with the placeholder text 'Search...' and a magnifying glass icon. To the right of the search bar are three buttons: 'Actions' with a dropdown arrow, 'Create Port Group', and 'Export'. Below the header, there is a table with three columns: 'Name', 'TCP Port', and 'Used in Policies'. The table is filtered to show 'Predefined port groups (39)'. The first row is highlighted in green and shows 'ABB Open Ports' with ports '80 | 102 | 44818 | 502' and the policy 'Use of Unauthorized Port in ABB 800X Controllers'. Other rows include 'Any Port', 'Apogee Open Ports', 'Bachmann M1 Open Ports', 'CIP', 'Commonly Exploited Ports', and 'DeltaV Open Ports'. A 'settings' icon is visible on the right side of the table.

Name	TCP Port	Used in Policies
Predefined port groups (39)		
ABB Open Ports	80   102   44818   502	Use of Unauthorized Port in ABB 800X Controllers
Any Port		
Apogee Open Ports	7   69   100   161 - 162   502   3001 - 3002   5441 - 5442   20 - 21   53   80	Use of Unauthorized Port in Apogee Controllers
Bachmann M1 Open Ports	21   80   443   445   502   3500	Use of Unauthorized Ports in Bachmann M1 Controllers
CIP	44818	
Commonly Exploited Ports	20 - 21   22   23   25   443   80   135   8080   513   3389	
DeltaV Open Ports	18508   18519   23   44818   502	Use of Unauthorized Port in DeltaV Controllers

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



## 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.

The screenshot shows a dialog box titled "Create Port Group" with a close button (X) in the top right corner. Inside the dialog, there is a "Name" field with a green asterisk, followed by an empty text input box. Below this is the "TCP Port" section, also with a green asterisk, and a subtitle "Port number or a range". Underneath the subtitle is a blue plus icon followed by the text "Add port". At the bottom of the dialog, there are two buttons: "Cancel" and "Create".

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.

OT Security 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

Name	Protocols
Predefined protocol groups(37)	
ABB Allowed Protocols	MMS   TCP1102   UDP2757   UDP2423   UDP1123   UDP2999   UDP1147   UDP3341   UDP24230   TCP180   TCP14818   MODBUS   TCP502
Any Protocol	TCP   UDP   MODBUS   UNITY   CONCEPT   PROFINET   CIP   PCCE   ETHIP   LLC   S7   S7Plus   P2   SRTT   BROWSER   DIGSI4   SICAM_PROFIBUS   IEC1850   IEC104   YOKOGAWA_CENTUM   BACNET   LLDP   MELSEC
Apogee Allowed Protocols	P2   TCP5033   TCP169   TCP100   TCP135   UDP161 - 162   TCP3001 - 3002   TCP5441 - 5442   UDP167 - 168
Bachmann M1 Allowed Protocols	PROFINET   MODBUS   DNP3   TCP21   TCP180   TCP1443   TCP1445   TCP502   UDP3000   TCP3500   IEC1
BACnet-IP	UDP147808   BACNET
Browser	BROWSER
CIP	CIP

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



## 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.

The screenshot shows a dialog box titled "Create Protocol Group" with a close button (X) in the top right corner. Inside the dialog, there is a "Name" field with a green asterisk, a "Protocols" dropdown menu with a green asterisk and the word "Select" inside, and a "Port" field with a green asterisk and the text "e.g 400 or 500-800". Below these fields is a link that says "Add Protocol" with a plus icon. At the bottom of the dialog are two buttons: "Cancel" and "Create".

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

Name	Type	Covers	Used in Policies
Predefined schedule groups(1)			
Any Time	Recurring		SIMATIC Code Download   SIMATIC Code Upload   ...
User defined schedule groups(1)			
Working Hours	Recurring	Monday to Friday 08:00 AM - 04:00 PM	

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
<b>Name</b>	The name that is used to identify the Group.
<b>Type</b>	<p>Shows the type of Group. Options are:</p> <ul style="list-style-type: none"><li>• Function – a predefined Schedule Group that was created to serve a particular function.</li><li>• 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.</li><li>• 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.</li></ul>
<b>Covers</b>	<p>A summary of the schedule settings.</p> <div><b>Note:</b> If there isn't room to display all members of the Group then click on <b>Table Actions &gt; View &gt; Members</b> tab.</div>



### 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:

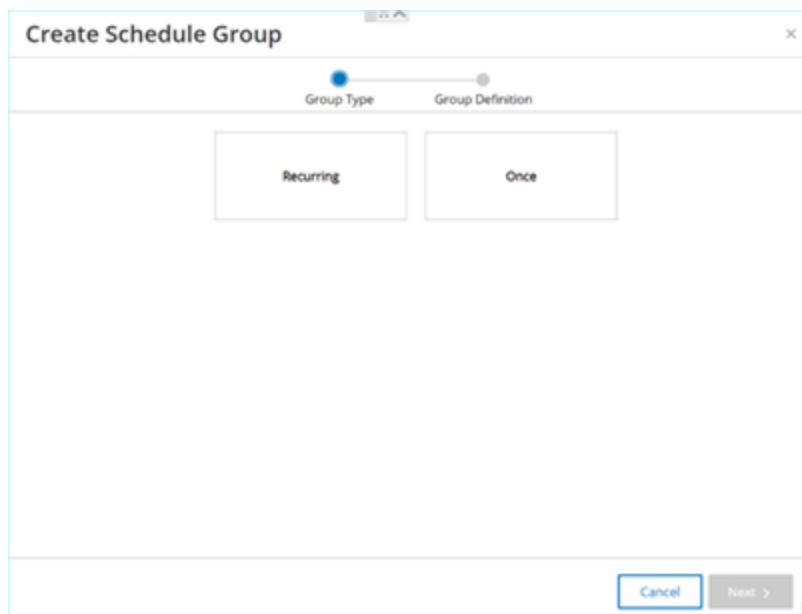
- **Recurring** – schedules that recur on a weekly basis. For example, a Work Hours schedule can be defined as Monday to Friday from 9am to 5pm.
- **Once** – schedules that occur on a specific date or range of dates. For example, a Plant Renovation schedule could be defined by the period from June 1 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.

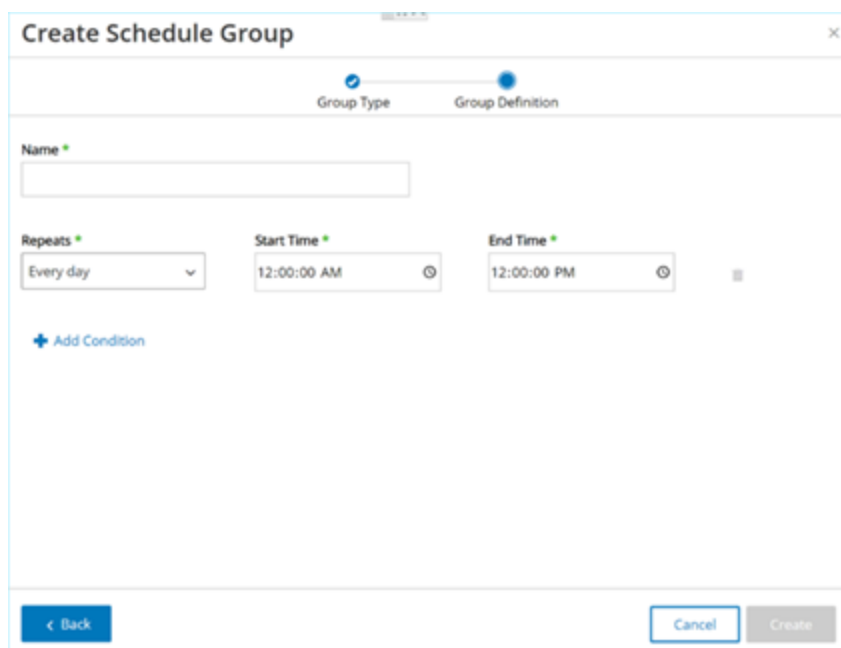


The dialog box is titled "Create Schedule Group". It features a progress bar at the top with two steps: "Group Type" (active, indicated by a blue dot) and "Group Definition" (inactive, indicated by a grey dot). Below the progress bar, there are two buttons: "Recurring" and "Once". The "Recurring" button is highlighted with a blue border. At the bottom right, there are two buttons: "Cancel" and "Next >".

4. Select **Recurring**.

5. Click **Next**.

The parameters for defining a Recurring Schedule group are shown.



The dialog box is titled "Create Schedule Group". It features a progress bar at the top with two steps: "Group Type" (inactive, indicated by a grey dot) and "Group Definition" (active, indicated by a blue dot). Below the progress bar, there is a "Name" field with a green asterisk and a text input box. Below the name field, there are three fields: "Repeats" with a dropdown menu showing "Every day", "Start Time" with a time picker showing "12:00:00 AM", and "End Time" with a time picker showing "12:00:00 PM". Below these fields, there is a blue plus icon and the text "Add Condition". At the bottom left, there is a blue button labeled "< Back". At the bottom right, there are two buttons: "Cancel" and "Create".

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.

**Note:** 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.

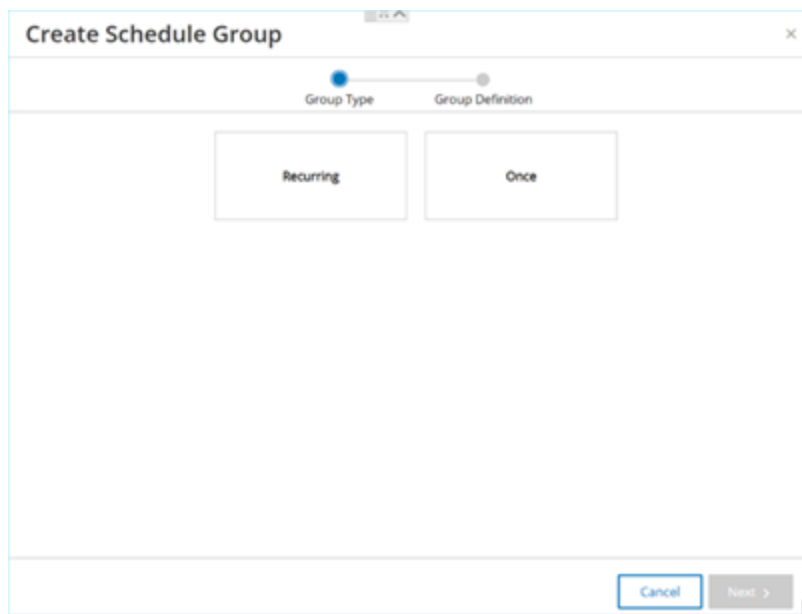
11. Click **Create**.

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:

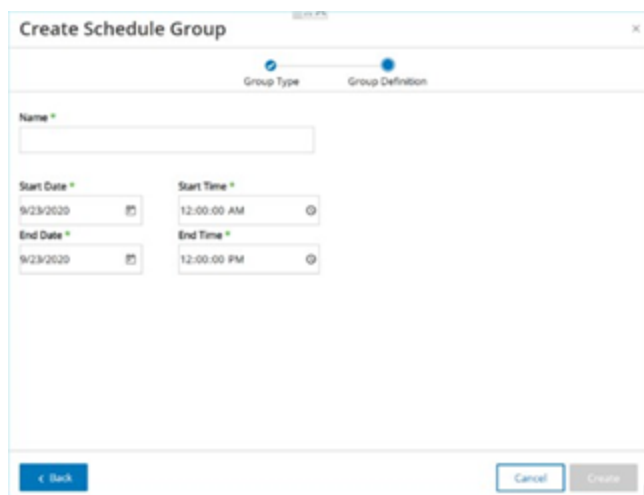
1. Under **Groups**, select **Schedule Groups**.
2. Click **Create Schedule Group**.

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



The dialog box is titled "Create Schedule Group". It features a progress bar at the top with two steps: "Group Type" (active, indicated by a blue dot) and "Group Definition" (inactive, indicated by a grey dot). Below the progress bar, there are two buttons: "Recurring" and "Once". The "Once" button is selected. At the bottom right, there are "Cancel" and "Next >" buttons.

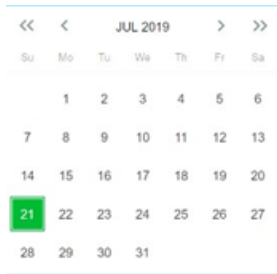
3. Select **Once**.
4. Click **Next**. The parameters for defining a one-time Schedule group are shown.



The dialog box is titled "Create Schedule Group". The progress bar now shows "Group Type" as inactive and "Group Definition" as active (indicated by a blue dot). The "Name" field is empty. Below it, there are four fields: "Start Date" (9/23/2020), "Start Time" (12:00:00 AM), "End Date" (9/23/2020), and "End Time" (12:00:00 PM). Each date and time field has a calendar icon to its right. At the bottom left, there is a "< Back" button. At the bottom right, there are "Cancel" and "Create" buttons.

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

Name ↑	Type	Controller	Tags	Used in Policies
User defined tag groups (2)				
Demo1	Bool	Rouge	Rouge - MainTask/MainProgram/Bit1(Bool)   Rouge - MainTask/MainProgram/Bit2(Bool)   Rouge - ...	
Demo2	Float	SIMATIC 300(1)	SIMATIC 300(1) - DB1/109(Float)   SIMATIC 300(1) - DB1/11(Float)   SIMATIC 300(1) - DB1/116(Float)   SIMATIC...	

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 OT Security 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.  <b>Note:</b> If there isn't room to display all Tags in this row then click on <b>Table Actions</b> > <b>View</b> > <b>Members</b> tab.
Used in Policies	Shows the Policy ID of each Policy that uses this Schedule Group in its configuration.  <b>Note:</b> To view additional details about the Policies in which this Group is used, click on <b>Table Actions</b> > <b>View</b> > <b>Used in Policies</b> 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:

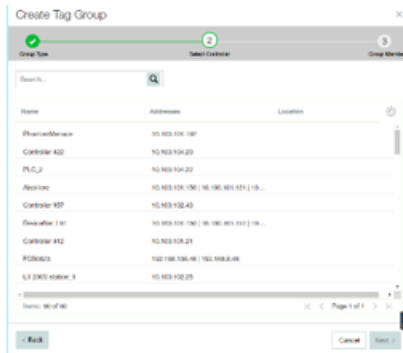
1. Under **Groups**, select **Tag Groups**.
2. Click **Create Tag Group**.

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



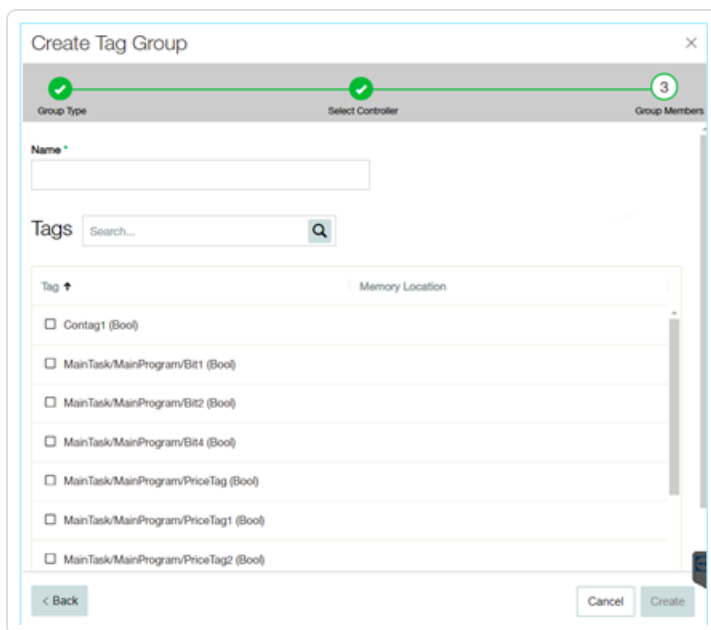
3. Select a Tag type. Options are: Bool, Dint, Float, Int, Long, Short or Any Type (which can include Tags of different Types)
4. Click **Next**.

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.

OT Security 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 screenshot shows the 'Rule Groups' management interface. At the top, there is a search bar and buttons for 'Actions', 'Create Rule Group', and 'Export'. Below the header, a table lists predefined rule groups. The table has three columns: 'Name', 'Number of Rules', and 'Used in Policies'. The first row is highlighted in green.

Name	Number of Rules	Used in Policies
Attacks - Heartbleed	6	Attacks - Heartbleed
Attacks - IOT	24	Attacks - IOT
Attacks - MS17-010 ETERNAL	13	Attacks - MS17-010 ETERNAL
Attacks - Magnitude	29	Attacks - Magnitude
Attacks - NETAPI	32	Attacks - NETAPI
Attacks - SMB Exploits	14	Attacks - SMB Exploits
Attacks - Spectre & Meltdown	8	Attacks - Spectre & Meltdown
Attacks - Splevo EK	6	Attacks - Splevo EK
Attacks - Sutra TDS	4	Attacks - Sutra TDS
Attacks - VNC	11	Attacks - VNC

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. <div><b>Note:</b> To view additional details about the Policies in which this Group is used, click on <b>Table Actions &gt; View &gt; Used in Policies</b> tab.</div>

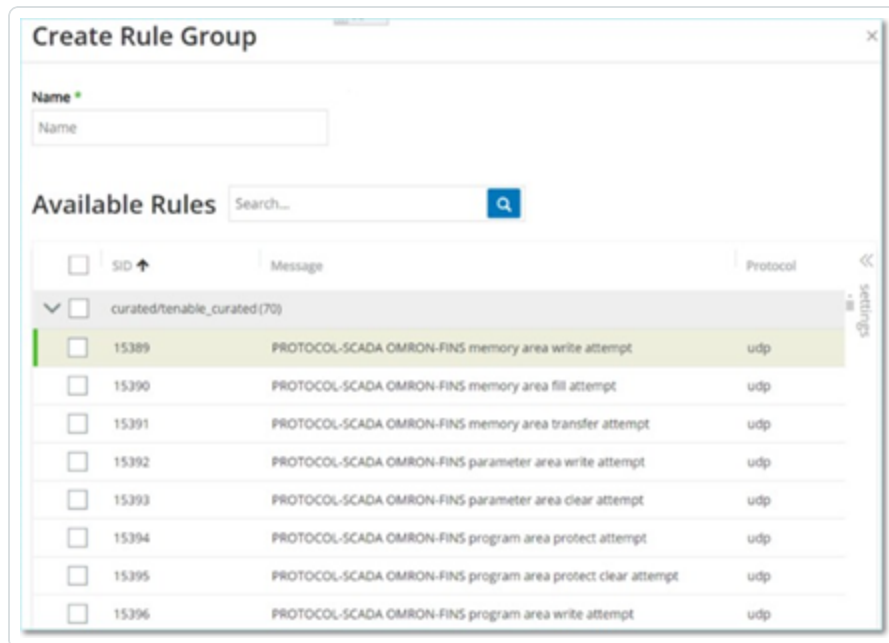


## Creating Rule Groups

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.

**Note:** 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:

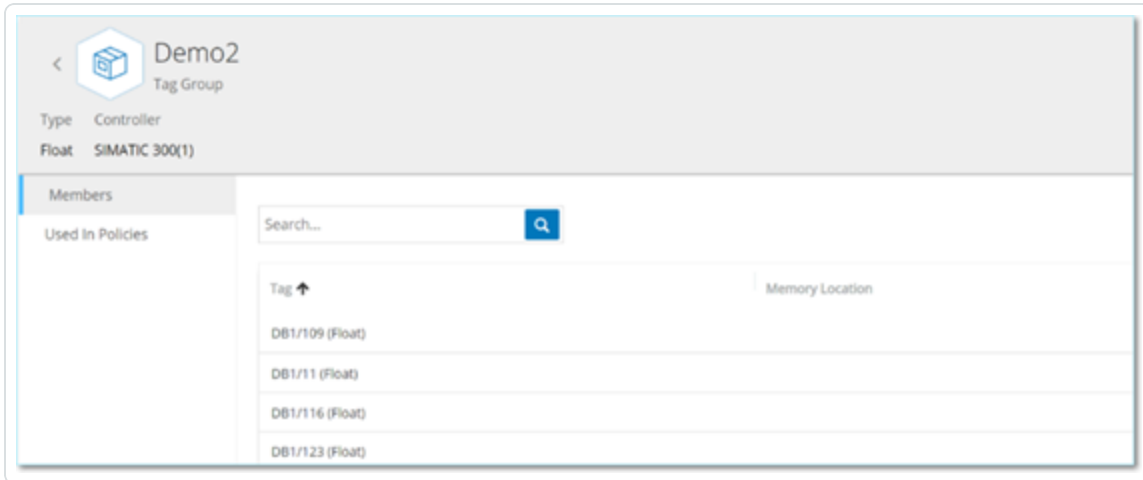
- **View** – shows details about the selected Group, such as which entities are included in the group and which Policies use the Group as a policy condition.
- **Edit** – edit details of the Group.
- **Duplicate** – create a new Group with similar configuration to the specified Group.
- **Delete** –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

**Note:** 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.



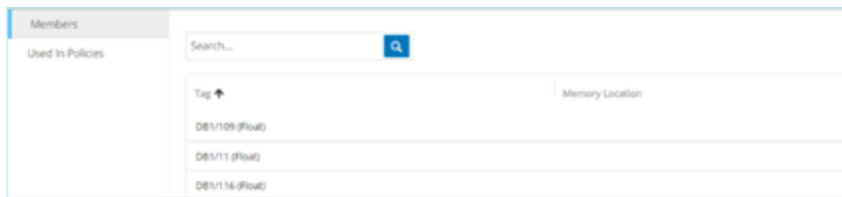
## Viewing Group Details

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:

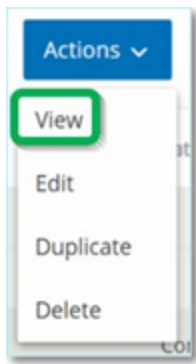
- **Members** – shows a list of all members of the Group.



- **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 [EXPORTING](#) the Dashboard.

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.

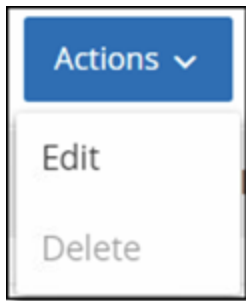


## Editing a Group

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.



### Edit Tag Group

**Name** \*  
Demo1

Search... 

 Tag 	Memory Location
<input checked="" type="checkbox"/> MainTask/MainProgram/Bit1 (Bool)	
<input checked="" type="checkbox"/> MainTask/MainProgram/Bit2 (Bool)	
<input checked="" type="checkbox"/> MainTask/MainProgram/Bit3 (Bool)	
<input type="checkbox"/> MainTask/MainProgram/Bit4 (Bool)	

Items: 4   Selected Items: 3   [\(Deselect all\)](#)

Cancel

Save

6. Make the desired changes.

7. Click **Save**.

The Group is saved with the new settings.

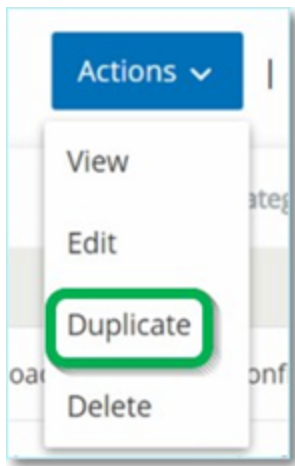


## Duplicating a Group

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.

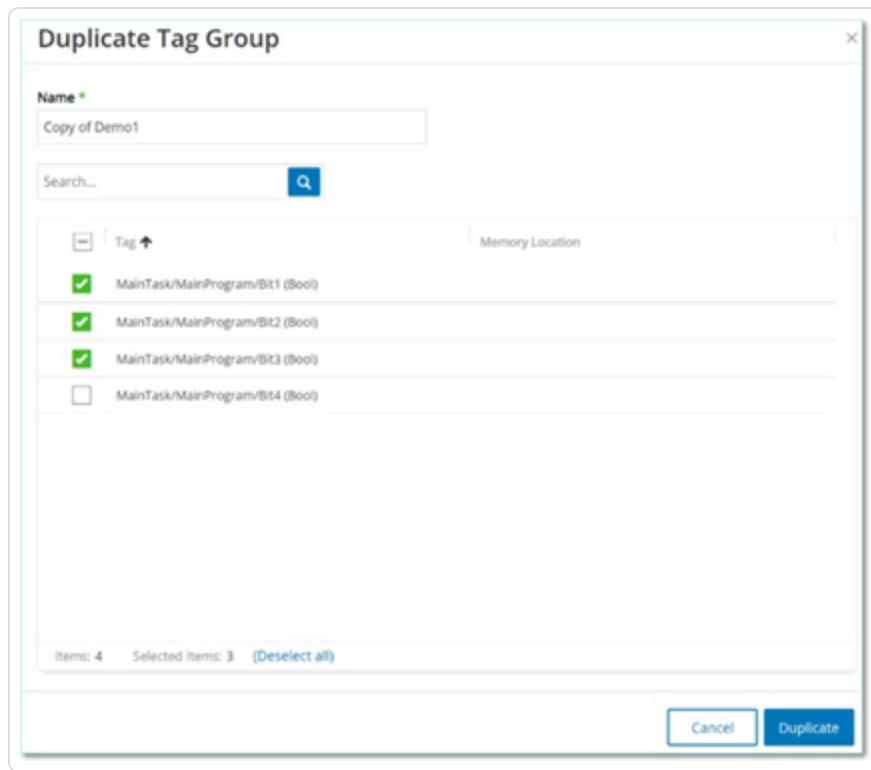
To Duplicate a Group:

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**.



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





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

The new Group is saved with the new settings, in addition to the existing Group.

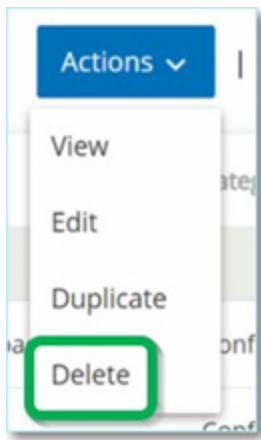


## Deleting a Group

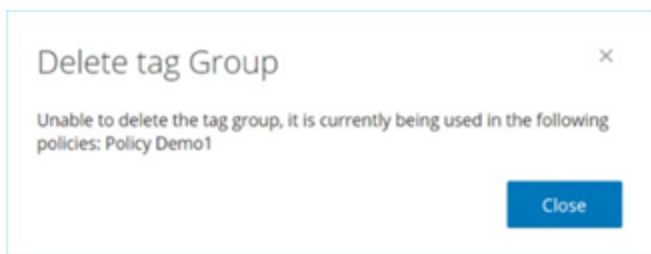
You can delete user defined Groups but not predefined Groups. Also, if a user defined Group is being used as a policy condition for one or more Policies it can't be deleted.

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**.



A confirmation window is displayed.



5. Click **Delete**.

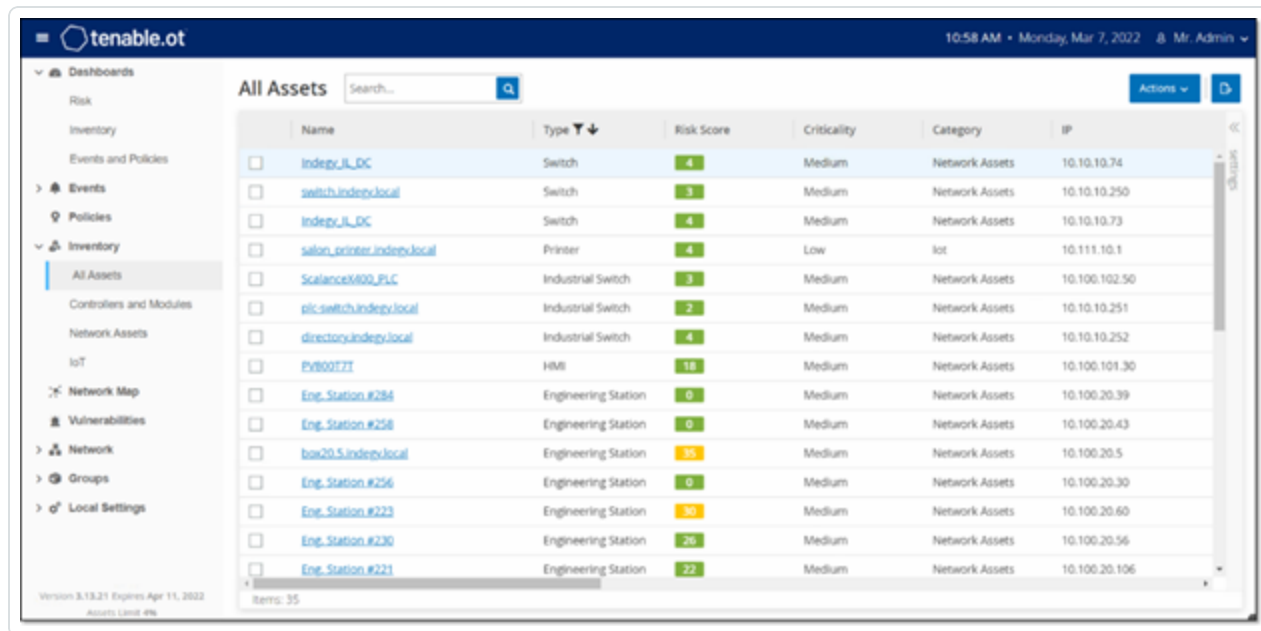
The Group is permanently deleted from the system.

## Inventory



OT Security'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



Name	Type	Risk Score	Criticality	Category	IP
Indegy_IL_DC	Switch	4	Medium	Network Assets	10.10.10.74
switch.indegy.local	Switch	3	Medium	Network Assets	10.10.10.250
Indegy_IL_DC	Switch	4	Medium	Network Assets	10.10.10.73
salon_printer.indegy.local	Printer	4	Low	IoT	10.111.10.1
ScalanceX800_PL_C	Industrial Switch	3	Medium	Network Assets	10.100.102.50
plc_switch.indegy.local	Industrial Switch	2	Medium	Network Assets	10.10.10.251
directory.indegy.local	Industrial Switch	4	Medium	Network Assets	10.10.10.252
PV800777	HMI	18	Medium	Network Assets	10.100.101.30
Eng_Station.#284	Engineering Station	0	Medium	Network Assets	10.100.20.39
Eng_Station.#258	Engineering Station	0	Medium	Network Assets	10.100.20.43
hsa20.5.indegy.local	Engineering Station	35	Medium	Network Assets	10.100.20.5
Eng_Station.#256	Engineering Station	0	Medium	Network Assets	10.100.20.30
Eng_Station.#223	Engineering Station	30	Medium	Network Assets	10.100.20.60
Eng_Station.#230	Engineering Station	26	Medium	Network Assets	10.100.20.56
Eng_Station.#221	Engineering Station	22	Medium	Network Assets	10.100.20.106

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 OT Security 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**.

**Note:** 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 [Management Console UI Elements](#).

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

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

Parameter	Description
-----------	-------------



<b>Name</b>	The name of the asset in the network. Click the name of the asset to view the Asset Details screen for that asset (See <a href="#">Inventory</a> .)
<b>IP</b>	<p>The IP address of the asset.</p> <div><b>Note:</b> An asset may have multiple IP addresses.</div> <div><b>Note:</b> IP addresses labeled as Direct are ones with which Tenable has established a direct connection. If there is no label, it means Tenable has discovered the IP without direct communication.</div> <div><b>Note:</b> Assets can be filtered by IP range. For more on filtering, see <a href="#">Management Console UI Elements</a>.</div>
<b>MAC</b>	The MAC address of the asset.
<b>Network Segment</b>	The Network Segment that the IP/s of this asset are assigned to.
<b>Type</b>	The type of asset, Controller, I/O or Communication, etc. see <a href="#">Asset Types</a> .
<b>Backplane*</b>	The backplane unit that the asset is connected to. Additional details about the backplane configuration are shown in the Asset Details screen.
<b>Slot*</b>	For assets that are on backplanes, shows the number of the slot to which the asset is attached.
<b>Vendor</b>	The asset vendor.
<b>Family*</b>	The family name of the product as defined by the asset vendor.
<b>Firmware</b>	The firmware version currently installed on the asset.
<b>Location</b>	The location of the asset as input by the user in the OT Security asset details. See <a href="#">Inventory</a> .
<b>Last Seen</b>	The time at which the device was last seen by OT Security. This is the last time that the device was connected to the network or performed an activity.
<b>OS</b>	The OS running on the asset.
<b>Model Name</b>	The model name of the asset.












<b>State*</b>	<p>The device state. Possible values:</p> <ul style="list-style-type: none"><li>• Backup – the controller is running as a backup to a primary controller.</li><li>• Fault – the controller is in fault mode.</li><li>• NoConfig – no configuration has been set for the controller.</li><li>• Running – the controller is running.</li><li>• Stopped – the controller is not running.</li><li>• Unknown – the state is unknown.</li></ul>
<b>Description</b>	<p>A brief description of the asset, as configured by the user in the OT Security asset details. See <a href="#">Inventory</a>.</p>
<b>Risk</b>	<p>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 <a href="#">Risk Assessment</a>.</p>
<b>Criticality</b>	<p>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.</p>
<b>Purdue Level</b>	<p>The Purdue level of the asset (0=Physical process, 1=Intelligent devices, 2=Control systems, 3=Manufacturing operations systems, 4=Business logistics systems).</p>
<b>Custom Field</b>	<p>You can create custom fields to tag your assets with relevant info. The custom field can be a link to an external resource.</p>














## Asset Types

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










Category	Default Criticality Level / Purdue Level	Description	Sub-Types	
Controllers	High / 1	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
				BMSController
				Robot
				Communication Module
				I/O Module
				CNC












				
				PowerSupply
				BackplaneModule
Field Devices	High / 1	An industrial device (e.g. sensor, actuator, electric motor) that uses industrial protocols to send information to ICS systems.		FieldDevice
				PowerMeter
				Remotel/O
				Relay
				Inverter
				IndustrialSensor
				Drive
				Actuator
OT Devices	Medium / 2	This category		OTDevice













		includes all types of OT devices.		
				IndustrialRouter
				IndustrialSwitch
				IndustrialGateway
				Industrial NetworkDevice
				IndustrialPrinter
OT Servers	Medium / 2	A computer/device that is used to access industrial data. This category includes all types of OT servers and their related components.		OTServer
				Historian
				HMI
				DataLogger












				
Network Devices	Medium / 3	A networking device (e.g. a switch or a router). This category includes all types of network devices and their related components.		NetworkDevice
				Router
				Switch
				Serial-EthernetBridge
				Gateway
				Hub
				Wireless AccessPoint
				Firewall













				Converter
				Repeater
				Radio
Workstations	Low / 3	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	Low / 3	This category includes various types of IT servers.		Server













				FileServer
				WebServer
				VirtualServer
				SecurityAppliance
				TenableICP
				TenableEM
				TenableSensor
				Domain Controller
				IoT
IoT	Low / 3	This category includes various		Camera



		type of interrelated devices.		
				Panel
				Projector
				VOIPDevice
				3DPrinter
				Printer
				UPS
				IP Phone
				SmartSensor
				BarcodeScanner



				Access ControlSystem
				LightingControl
				HVACModule
				SmartHub
				SmartTV
				MedicalDevice
				Tablet
				MobileDevice
				StorageDevice
Endpoints	Low / 3	An unidentified IP address in the network.		Endpoint



## Viewing Asset Details

Overview	
NAME	longrun1.local
PURDUE LEVEL	Level 3
STATE	Unknown
STATE UPDATE TIME	12:00:00 AM - Jan 1, 0001
DIRECT IP	10.100.20.200
DIRECT MAC	08:00:27:00:00:00
FAMILY	08:00:27
VENDOR	Tenable
MODEL NAME	08:00:27
LAST SEEN	08:36:12 AM - Mar 7, 2022
FIRST SEEN	09:17:08 AM - Mar 2, 2022
NETWORK SEGMENTS	Workstation / 10.100.20.X
RISK SCORE	36

The **Asset Details** screen shows comprehensive details about all data discovered by OT Security 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 OT Security '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.



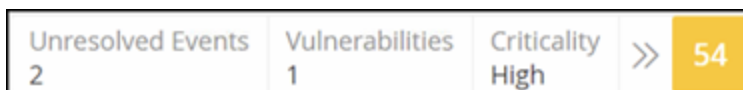


## Header Pane



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 Tenable Nessus scan.
- **Resync Button** – click on this button to manually run one or more of the queries that are available for this asset. See [Header Pane](#).



## Details Tab

The screenshot displays the 'Details' tab for the '140-NOE-771-01 Module'. The interface is divided into several sections:

- Header:** Shows the asset name '140-NOE-771-01 Module' and a 'Communication Module' icon. It includes a table with columns: IP, Vendor, Model, Last Seen, State, Family, and Firmware. The data row shows: 10.100.105.27, Schneider, 140-NOE-771-01, Mar 6, 2022 06:35:28 PM, Unknown, Concept, 393216.
- Left Sidebar:** Contains navigation links: Details, IP Trail, Attack Vectors, Open Ports, Vulnerabilities, Events, and Network Map.
- Overview Section:** A table of key attributes:

Attribute	Value
NAME	140-NOE-771-01 Module
DESCRIPTION	Schneider Quantum, Ethernet TCP/IP Communications Module
PURDUE LEVEL	Level 1
STATE	Unknown
STATE UPDATE TIME	12:00:00 AM - Jan 1, 0001
DIRECT IP	10.100.105.27
DIRECT MAC	00:00:54:22:90:f3
FAMILY	Concept
VENDOR	Schneider
MODEL NAME	140-NOE-771-01
LAST SEEN	06:35:28 PM - Mar 6, 2022
FIRST SEEN	09:17:41 AM - Mar 2, 2022
NETWORK SEGMENTS	Controller / 10.100.105.X
RISK SCORE	5.4
- General Section:** Shows the 'FIRMWARE VERSION' as 393216.
- Backplane View:** A diagram of 'Backplane #8' showing slots 0 through 4. Slot 1 is highlighted, showing 'Power Supply #324'. Slot 3 shows '140-NOE-771-01 M...'. Slot 4 shows 'I/O #324'.
- Power Supply Details Pop-up:** A detailed view of the selected power supply:

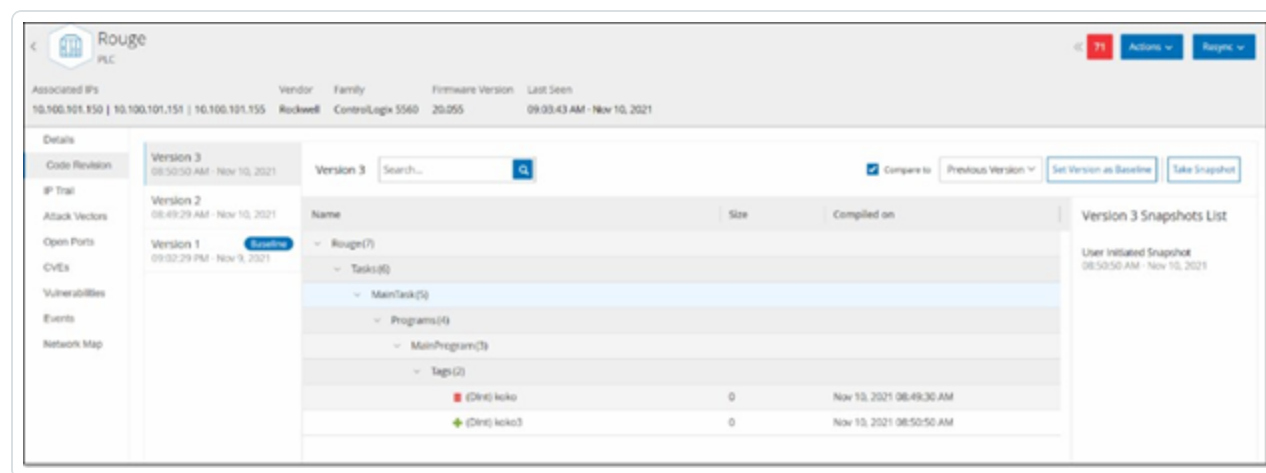
Attribute	Value
NAME	Power Supply #324
RISK SCORE	5.4
TYPE	Power Supply
DESCRIPTION	AC PS 115V/230 8A, CPS114-10 summable
MODEL	140-CPS-114-v0
VENDOR	Schneider

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 OT Security "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 Activities 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



<b>Version 3</b> 08:50:50 AM · Nov 10, 2021
<b>Version 2</b> 08:49:29 AM · Nov 10, 2021
<b>Version 1</b> 09:02:29 PM · Nov 9, 2021

Baseline

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

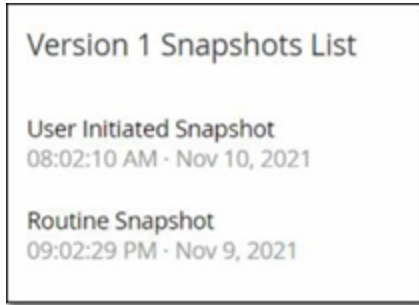
Version: 3 Search... ☐ Compare to Previous Version Set

Name	Size	Compiled on
Router(30)		
Tags(2)		
(Dint) RouterTag1	0	Nov 9, 2021 09:02:29 PM
(Bool) VAXTEXT	0	Nov 9, 2021 09:02:29 PM
Tasks(26)		
MainTask(23)		
Programs(22)		
MainProgram(21)		
Routines(2)		
(Ladder) Main_Routine	16	Nov 10, 2021 08:49:30 AM
(SFC) SFC1	432	Nov 9, 2021 09:02:29 PM
Tags(17)		
(Bool) MyBit	0	Nov 10, 2021 08:49:30 AM
(SFCStep) Step_000	0	Nov 9, 2021 09:02:29 PM
(SFCStep) Step_001	0	Nov 9, 2021 09:02:29 PM
(Bool) Tran_000	0	Nov 9, 2021 09:02:29 PM
(Bool) Tran_001	0	Nov 9, 2021 09:02:29 PM
(Dint) ...SL7162	0	Nov 9, 2021 09:02:29 PM

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.

The screenshot shows the 'Version 3' pane with a search bar and a 'Compare to' dropdown set to 'Previous Version'. The tree view shows a hierarchy: Rouge(7) > Tasks(6) > MainTask(5) > Programs(4) > MainProgram(3) > Tags(2). The table below shows two differences:

Name	Size	Compiled on
✖ (Dint) koko	0	Nov 10, 2021 08:49:30 AM
+ (Dint) koko3	0	Nov 10, 2021 08:50:50 AM

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.

**Note:** 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. In the field next to the Compare to checkbox, select Baseline Version from the dropdown menu.
7. 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

140-NOE-771-01 Module  
Communication Module

IP 10.100.105.27 Vendor Schneider Model 140-NOE-771-01 Last Seen Mar 6, 2022 06:35:28 PM State Unknown Family Concept Firmware 393216

Details  
IP Trail  
Attack Vectors  
Open Ports  
Vulnerabilities  
Events  
Network Map

Search...

IP	Start Date	End Date
140-NOE-771-01   Slot 3(1)		
10.100.105.27	Mar 2, 2022 09:17:08 AM	Active

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.



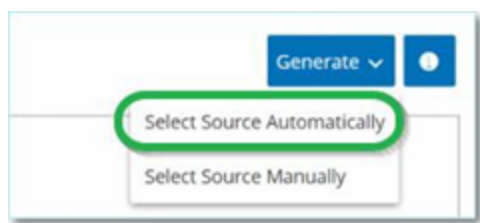
## Generating Attack Vectors

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

To generate an automatic Attack Vector:

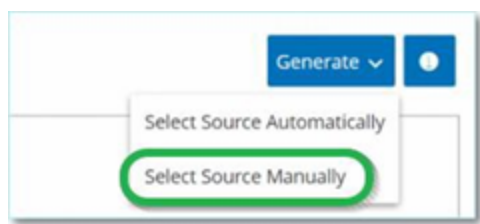
1. Navigate to the **Asset Details** page for the desired target asset and click on the **Attack Vector** tab.
2. Click **Generate** and then click **Select Source Automatically** from the dropdown list.



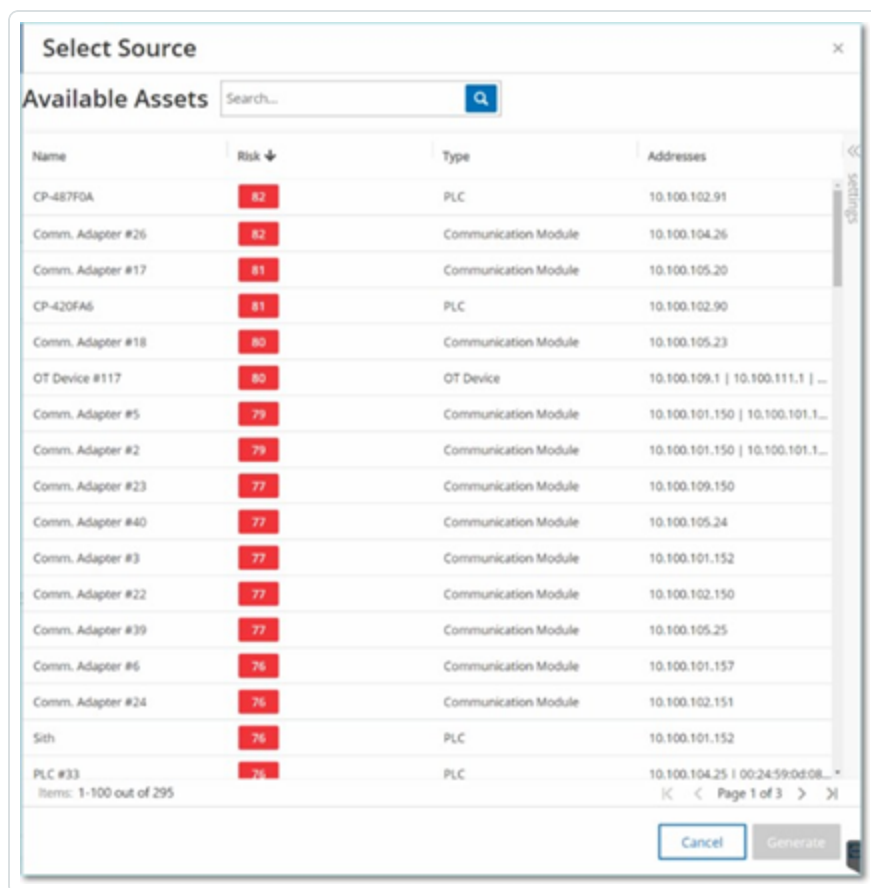
The Attack Vector is generated automatically and is displayed in the **Attack Vector** tab.

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.



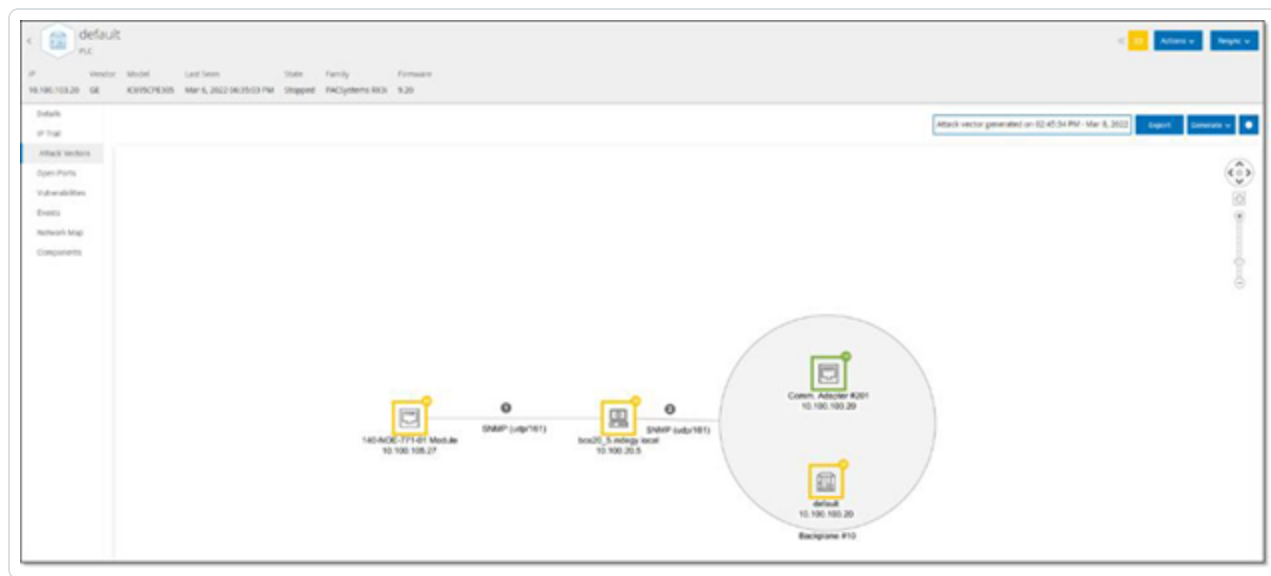
**Note:** By default, the source assets are sorted by Risk score. You can adjust the display settings or search for the desired asset.

3. Select the desired source asset.
4. Click **Generate**.

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



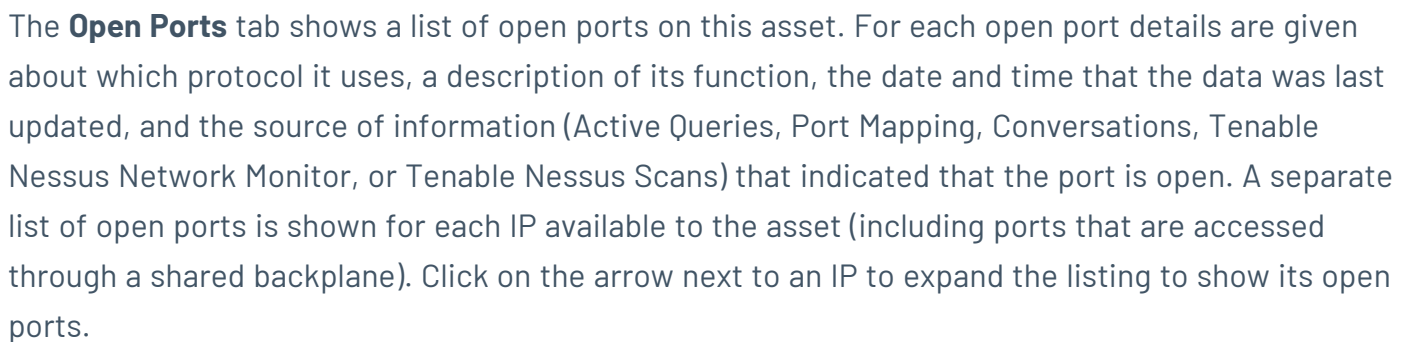
## Viewing Attack Vectors



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.

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



There is an automatic **Open Ports Age Out Period**, after which an open port listing will be automatically deleted from the list if no further indication has been received that the port is still open. The default period of time is two weeks. To adjust the length of the Open Ports Age Out Period, see [Device](#).

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**.

OT Security runs a scan on the selected port.

To view the asset's portal:

**Note:** 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 screenshot shows the 'Vulnerabilities' tab for an asset named 'YAIR1 PLC'. The asset details at the top include IP (10.100.105.27), Vendor (Schneider), Last Seen (Mar 6, 2022 06:35:28 PM), State (Unknown), and Family (Concept). The left sidebar lists various tabs: Details, Code Revision, IP Trail, Attack Vectors, Open Ports, Vulnerabilities (selected), Events, and Network Map. The main content area displays a table of vulnerabilities. The table has columns for Name, Severity, VPR, Affected a..., Plugin family, Plugin ID, and Source. One vulnerability is listed: 'Schneider (CVE-2014-0754)' with a 'Critical' severity, a VPR of 5.9, and a source of 'Tenable.ot'. The table also shows a search bar, a plugin set ID (202203060608), and a last update time (12:02:24 AM - Mar 7, 2022). Action buttons for 'Actions', 'Update plugins', and 'Refresh' are visible.

Name	Sev...	VPR	Affected a...	Plugin family	Plugin ID	Source
Schneider (CVE-2014-0754)	Critical	5.9		Tenable.ot	500039	Tot

The **Vulnerabilities** tab shows a list of all Vulnerabilities that affect the specified asset, as detected by OT Security 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

Log ID	Time	Event Type	Severity	Policy Name	Source Asset	Source Address	Destination Asset	Destination Address	Protocol
17842	09:02:09 AM - Mar 15, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.200	Eng.Station.#389	10.100.20.52	Tcp
10845	08:42:18 AM - Mar 15, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.5	Eng.Station.#389	10.100.20.52	Tcp
10860	05:41:28 AM - Mar 15, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.200	Eng.Station.#389	10.100.20.52	Tcp
14775	05:04:47 AM - Mar 15, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.5	Eng.Station.#389	10.100.20.52	Tcp
12881	01:25:09 AM - Mar 15, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.200	Eng.Station.#389	10.100.20.52	Tcp
12949	01:00:14 AM - Mar 15, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.5	Eng.Station.#389	10.100.20.52	Tcp
8968	09:58:08 PM - Mar 14, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.200	Eng.Station.#389	10.100.20.52	Tcp
8969	09:48:48 PM - Mar 14, 2022	Port Scan	High	20th Scan Detected	Sergent.Lindholm.local	10.100.20.5	Eng.Station.#389	10.100.20.52	Tcp
8976	09:00:58 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)
8929	09:00:04 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)
8987	09:00:04 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)
8985	09:00:13 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)
8990	09:00:52 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)
8978	09:00:58 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)
8998	09:00:49 PM - Mar 14, 2022	Rockwell Code Upload	Low	Rockwell Code Uploaded	Eng.Station.#389	10.100.20.52	Destination.LB1	10.100.101.152	DP (http)

**Event 34712** 08:27:47 AM - Mar 16, 2022 Port Scan High Not resolved

**Details**

A Port scan is a probe to reveal what ports are open and listening on a given asset.

**Source**  
SOURCE ASSET: Sergent.Lindholm.local  
SOURCE IP ADDRESS: 10.100.20.200

**Destination**  
DESTINATION ASSET: Eng.Station.#389  
DESTINATION IP ADDRESS: 10.100.20.52

**Policy**  
POLICY: 20th Scan Detected

**Scanned Ports**  
PROTOCOL: Tcp

**Why is this important?**  
Port scans are part of mapping communication channels to an asset. Some port scans are legitimate and done by monitoring devices in the network. However, such mapping may also be done in the early stages of an attack, in order to detect vulnerable and accessible ports for malicious communications.

**Suggested Mitigation**  
Make sure that you are familiar with the source of the port scan and that this port scan was expected. In case you are not familiar with the source check with the source asset owner to see whether this was a planned and expected port scan. If not, check which other assets have been scanned by the source asset and consider isolating the source asset to decrease network exposure while you investigate further.

The **Events** tab displays a detailed list of Events in the network involving the asset, as detected by OT Security 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 [Management Console UI Elements](#).

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
<b>Log ID</b>	The ID generated by the system to refer to the Event.
<b>Time</b>	The date and time that the Event occurred.
<b>Event Type</b>	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 <a href="#">Policy Types</a> .
<b>Severity</b>	<p>Shows the severity level of the Event. The following is an explanation of the possible values:</p> <ul style="list-style-type: none"><li>• None – No reason for concern.</li><li>• Info – No immediate reason for concern. Should be checked out when convenient.</li><li>• Warning – Moderate concern that potentially harmful activity has occurred. Should be dealt with when convenient.</li><li>• Critical – Severe concern that potentially harmful activity has occurred. Should be dealt with immediately.</li></ul>
<b>Policy Name</b>	The name of the Policy that generated the Event. The name is a link to the Policy listing.
<b>Source Asset</b>	The name of the asset that initiated the Event. This field is a link to the Asset listing.
<b>Source Address</b>	The IP or MAC of the asset that initiated the Event.
<b>Source Address</b>	The IP or MAC of the asset that initiated the Event.
<b>Destination Asset</b>	The name of the asset that was affected by the Event. This field is a link to the Asset listing.
<b>Destination Address</b>	The IP or MAC of the asset that was affected by the Event.



<b>Protocol</b>	When relevant, this shows the protocol used for the conversation that generated this Event.
<b>Event Category</b>	<p>Shows the general category of the Event.</p> <p>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.</p> <p>The following is a brief explanation of the Event categories (for a more detailed explanation see <a href="#">Policy Categories and Sub-Categories</a>):</p> <ul style="list-style-type: none"><li>• Configuration Events – this includes two sub-categories</li><li>• Controller Validation Events – These policies detect changes that take place in the controllers in the network.</li><li>• Controller Activity Events – Activity Policies relate to the Activities that occur in the network (i.e., the “commands” implemented between assets in the network).</li><li>• SCADA Events – policies that identify changes made to the data plane of controllers.</li><li>• Network Threats Events – these Policies identify network traffic that is indicative of intrusion threats.</li><li>• Network Events – Policies that relate to the assets in the network and the communication streams between assets.</li></ul>
<b>Status</b>	Shows whether or not the Event has been marked as resolved.
<b>Resolved By</b>	For resolved Events, shows which user marked the Event as resolved.
<b>Resolved On</b>	For resolved Events, shows when the Event was marked as resolved.
<b>Comment</b>	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

Details	Search...					
IP Trail						
Open Ports						
CVEs						
Events						
Asset Map						
Device Ports						
MAC	Name	Status	Alias	Description	Type	Time of Query
1c:4b:5d:48:05:31	G2/3/49	Down		GigabitEthernet2/3/49	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:93	G1/3/19	Down		GigabitEthernet1/3/19	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:35	G2/3/37	Down	Undronics	GigabitEthernet2/3/37	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:38	G2/3/40	Down	Valentin	GigabitEthernet2/3/40	Ethernetcomad	06:16:48 AM - May 11, 2020
00:a7:42:eb:85:a4	G3/3/36	Down		GigabitEthernet3/3/36	Ethernetcomad	06:16:48 AM - May 11, 2020
00:a7:42:eb:85:81	G3/3/1	Down		GigabitEthernet3/3/1	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:87	G1/3/7	Down		GigabitEthernet1/3/7	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:9c	G1/3/28	Down		GigabitEthernet1/3/28	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:9b	G1/3/27	Down		GigabitEthernet1/3/27	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:32	G2/3/32	Down	Sicam_Spinter	GigabitEthernet2/3/32	Ethernetcomad	06:16:48 AM - May 11, 2020
1c:4b:5d:48:05:30	G2/3/43	Down		GigabitEthernet2/3/43	Ethernetcomad	06:16:48 AM - May 11, 2020
00:a7:42:eb:85:8a	G3/3/10	Down	Beckoff	GigabitEthernet3/3/10	Ethernetcomad	06:16:48 AM - May 11, 2020
00:a7:42:eb:85:95	G3/3/21	Down		GigabitEthernet3/3/21	Ethernetcomad	06:16:48 AM - May 11, 2020
00:a7:42:eb:85:90	G3/3/48	Up	Cross_FSL_Pok...	GigabitEthernet3/3/48	Ethernetcomad	06:16:48 AM - May 11, 2020
Items: 168						

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.

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



---

## Editing Asset Details

---

OT Security 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.

**Edit Asset Details**

Type \*  
PLC

Name  
PLC #49

Criticality \*  
High

Purdue Level \*  
Level 1

Location

Description

Cancel Save

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 OT Security 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**.

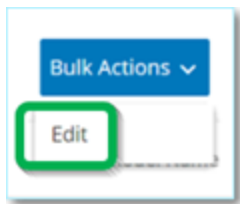
The edited details are saved for that asset.

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.

**Note:** 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).

**Note:** 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.





**Note:** 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.

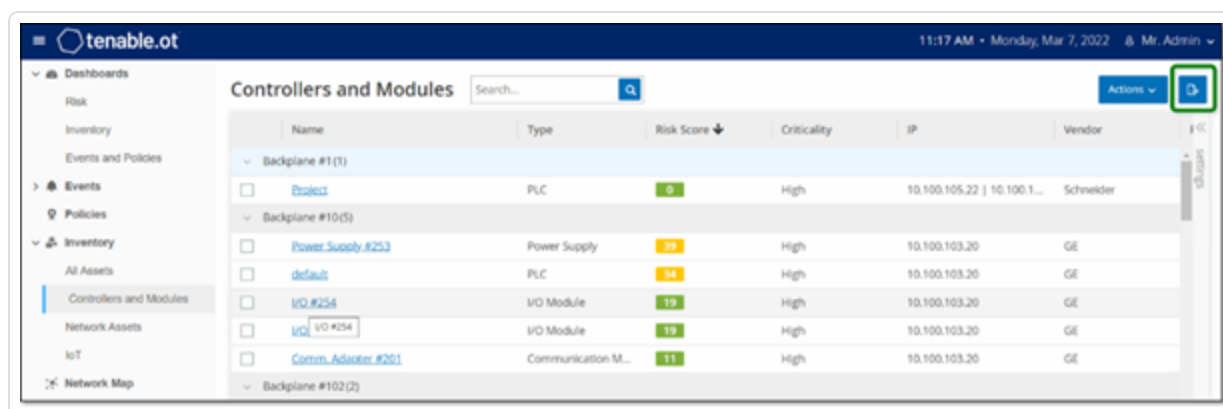


## Editing Asset Details by Uploading a CSV

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.

The screenshot shows a CSV file with columns A through S. The data includes asset details such as ID, Slot, Name, Type, Risk, Criticality, Addresses, Vendor, Family, Model, Firmware, State, Purdue, Last Seen, Location, Backplane, and Description.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description	
2	Q1Na2XQ6AHTA2MDE		DESKTOP-PLC	PLC	47	High-Critical	33.180.38	Beckhoff	C-Series	2.11.2305	Unknown	Level1	*****					
3	Q1Na2XQ6AHTA2MDE		SIMATIC H-PLC	PLC	32	High-Critical	33.180.38	Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	*****			Siemens, SIMATIC S7	
4	Q1Na2XQ6AHTA2MDE		Yairdeng	Communic	20	High-Critical	33.180.38	Helmholtz Netlink	NETLink Pi	2.7	Unknown	Level1	*****				700-884-MPI21	
5	Q1Na2XQ6AHTA2MDE		44aaa	Controller	20	High-Critical	33.180.38	Texas Instruments				Unknown	Level1	*****				
6	Q1Na2XQ6AHTA2MDE		BMX NOC	Communic	13	High-Critical	33.180.38	Schneider Modicon	FBMX NOC	2.5	Unknown	Level1	*****	lab			Schneider Electric M	
7	Q1Na2XQ6AHTA2MDE		bbab	PLC	74	High-Critical	33.180.38	Siemens	SIPROTEC	75182		Unknown	Level1	*****				
8	Q1Na2XQ6AHTA2MDE		ML1400	PLC	81	High-Critical	33.180.38	Rockwell	MicroLogix	1766-L328	2.015	Unknown	Level1	*****			Allen-Bradley 1766-L	
9	Q1Na2XQ6AHTA2MDE		cccc	DCS	72	High-Critical	33.180.38	Emerson	S-Series	SD Plus	13.3	Unknown	Level1	*****	Austin, Texas		DeltaV - SD Plus Soft	
10	Q1Na2XQ6AHTA2MDE		57300/ET2	Communic	61	High-Critical	33.180.38	Siemens	S7-300	CP 343-1	1.3.1.1	Unknown	Level1	*****			Siemens, SIMATIC NI	
11	Q1Na2XQ6AHTA2MDE		DCS #9	DCS	93	High-Critical	33.180.38	Tenable				Unknown	Level1	*****				
12	Q1Na2XQ6AHTA2MDE		7UT633 V1	PLC	76	High-Critical	33.180.38	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.)

**Note:** 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.

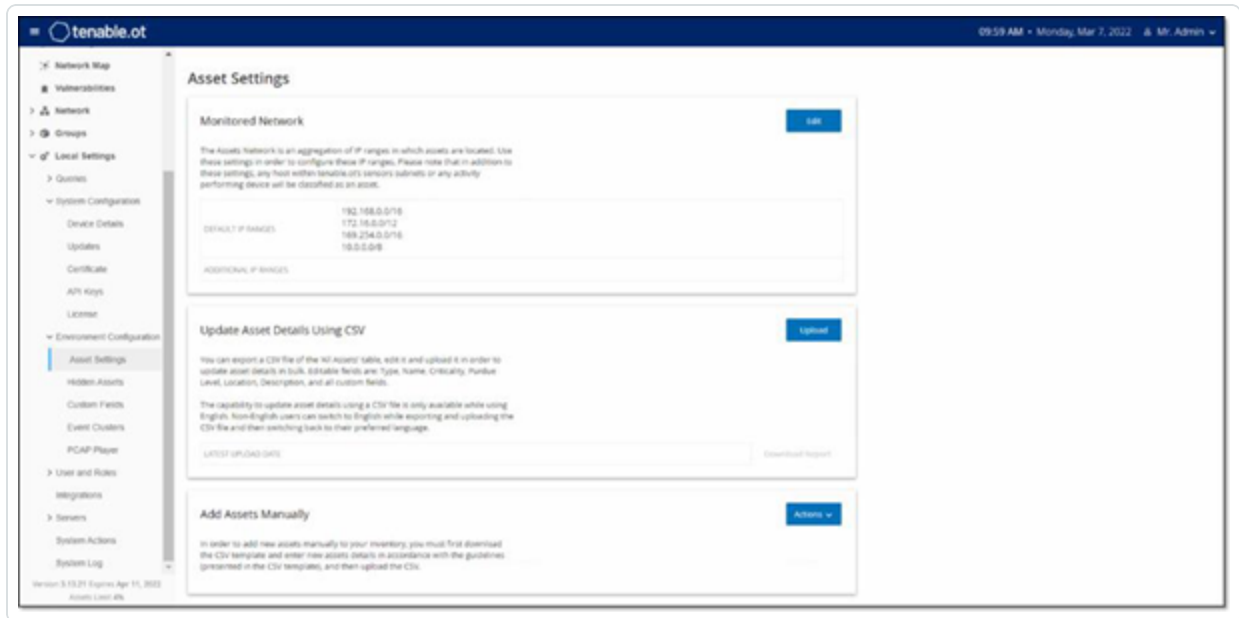
5. Save the file as a csv file type.



**Note:** 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.

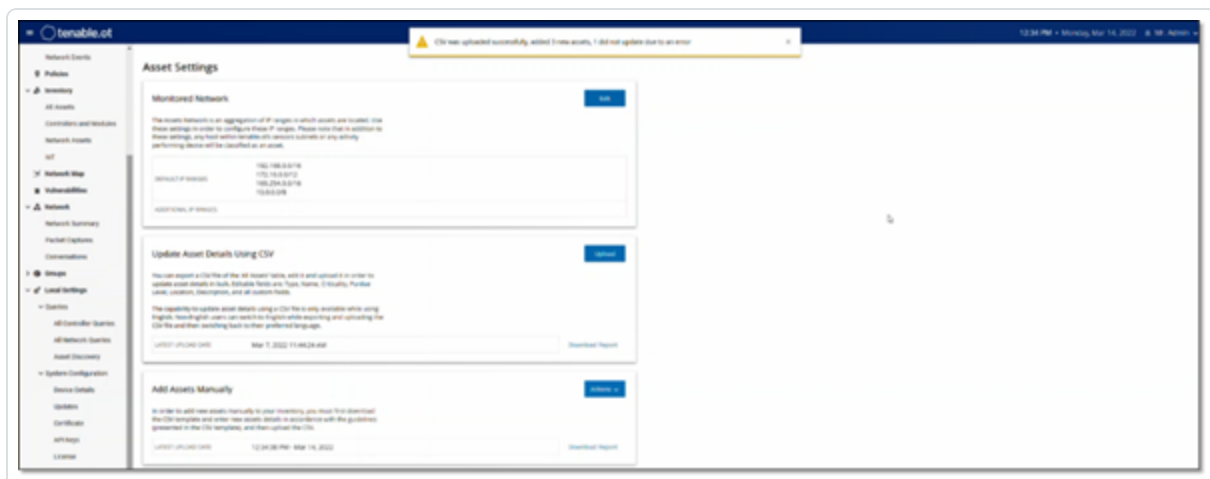
- Under **Local Settings**, go to **Environment Configuration > Asset Settings**.

The **Asset Settings** screen is shown.



- In the **Update asset details using CSV** section, click **Upload**.
- 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)

**Note:** 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 an Asset-Specific Tenable Nessus Scan

Tenable Nessus is a tool that scans IT devices to detect vulnerabilities. OT Security enables you to run the Tenable 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. You can also create customized scans to run a specific set of Tenable Nessus Plugins on a particular set of network assets, see [Tenable Nessus Plugin Scans](#).

**Note:** Tenable 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 Tenable 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 Tenable Nessus Scan is run.



---

## Performing Resync

---

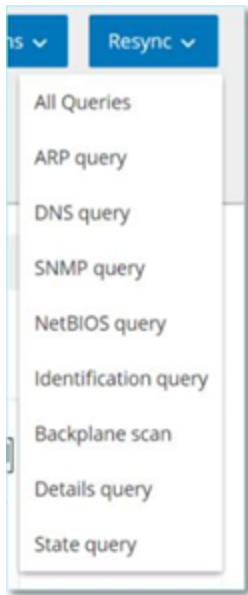
The Resync function initiates one or more Queries to the network and the controller in order to capture up-to-date information for this asset. You can run all available Queries or you can select specific Queries to run. The following, are the Queries available for “Resync”:

- **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.

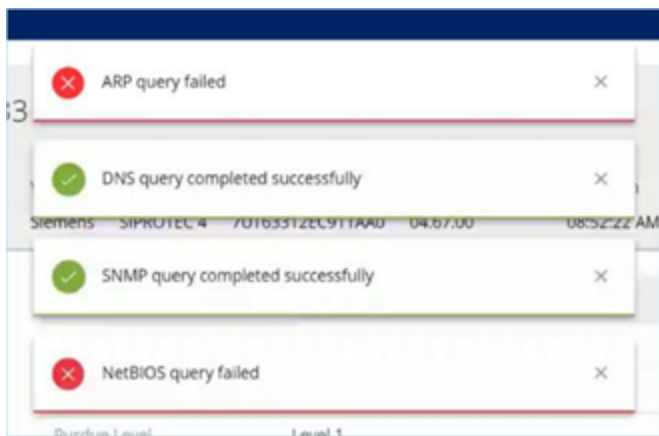
To run Resync asset data:

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

A dropdown list of queries is displayed.



2. Click on the query that you would like to run OR click on All Queries to run all available queries.
3. 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

Log ID	Time	Status	Event Type	Severity	Policy Name
1	09:16:49 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication to External...
4	09:17:29 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication to External...
5	09:17:29 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Conversation in a Commop...
2	09:17:33 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC
3	09:17:35 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC
6	09:17:36 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication from Exter...
7	09:17:41 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC
8	09:17:53 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC
9	09:17:54 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC

Items: 250

Event 1 09:16:49 AM - Mar 2, 2022 Unauthorized Conversation Medium Not resolved

**Details**

A conversation in an unauthorized protocol has been detected

**Source**

**Policy**

**Status**

**Why is this important?**

Conversations in unauthorized protocols may indicate suspicious traffic. Some assets are not expected to communicate in non-standard protocols and any deviation from the standard protocols may suggest a potential threat. In addition, some protocols are insecure and should...

**Suggested Mitigation**

Check if this communication is expected. If it is expected traffic, then adjust the Policy conditions so that Events aren't generated for similar communications in the future. If this communication is not expected, check the source asset to determine whether the source asset itself has been compromised. If this...

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 [Management Console UI Elements](#).

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.

**Note:** 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 [Network](#). The information shown for each Event listing is described in the following table:

Parameter	Description
<b>Name</b>	The name of the device in the network. Click the name of the asset to view the Asset Details Screen for that asset, see <a href="#">Inventory</a> .
<b>Addresses</b>	The IP and/or MAC address of the asset. <b>Note:</b> An asset may have multiple IP addresses.
<b>Type</b>	The asset type. See <a href="#">Asset Types</a> for an explanation of the various asset types.
<b>Backplane</b>	The backplane unit that the controller is connected to. Additional details about the backplane configuration are shown in the Asset Details screen.
<b>Slot</b>	For controllers that are on backplanes, shows the number of the slot to which the controller is attached.
<b>Vendor</b>	The asset vendor.
<b>Family</b>	The family name of the product as defined by the controller vendor.
<b>Firmware</b>	The firmware version currently installed on the controller.
<b>Location</b>	The location of the asset, as input by the user in the OT Security asset details. See <a href="#">Inventory</a> .
<b>Last Seen</b>	The time at which the device was last seen by OT Security. This is the last time that the device was connected to the network or performed an activity.
<b>OS</b>	The OS running on the asset.



<b>Log ID</b>	The ID generated by the system to refer to the Event.
<b>Time</b>	The date and time that the Event occurred.
<b>Event Type</b>	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 <a href="#">Policy Types</a> .
<b>Severity</b>	<p>Shows the severity level of the Event. The following is an explanation of the possible values:</p> <p>None – No reason for concern.</p> <p>Info – No immediate reason for concern. Should be checked out when convenient.</p> <p>Warning – Moderate concern that potentially harmful activity has occurred. Should be dealt with when convenient.</p> <p>Critical – Severe concern that potentially harmful activity has occurred. Should be dealt with immediately.</p>
<b>Policy Name</b>	The name of the Policy that generated the Event. The name is a link to the Policy listing.
<b>Source Asset</b>	The name of the asset that initiated the Event. This field is a link to the Asset listing.
<b>Source Address</b>	The IP or MAC of the asset that initiated the Event.
<b>Destination Asset</b>	The name of the asset that was affected by the Event. This field is a link to the Asset listing.
<b>Destination Address</b>	The IP or MAC of the asset that was affected by the Event.
<b>Protocol</b>	When relevant, this shows the protocol used for the conversation that generated this Event.
<b>Event</b>	Shows the general category of the Event.



<b>Category</b>	<div data-bbox="412 170 1477 283"><b>Note:</b> On the All Events screen, Events of all types are shown. Each of the specific Event screens shows only Events of the specified category.</div> <p>The following is a brief explanation of the Event categories (for a more detailed explanation see <a href="#">Policy Categories and Sub-Categories</a>):</p> <ul style="list-style-type: none"><li>• Configuration Events – this includes two sub-categories</li><li>• Controller Validation Events – These policies detect changes that take place in the controllers in the network.</li><li>• Controller Activity Events – Activity Policies relate to the Activities that occur in the network (i.e., the “commands” implemented between assets in the network).</li><li>• SCADA Events – policies that identify changes made to the data plane of controllers.</li><li>• Network Threats Events – these Policies identify network traffic that is indicative of intrusion threats.</li><li>• Network Events – Policies that relate to the assets in the network and the communication streams between assets.</li></ul>
<b>Status</b>	Shows whether or not the Event has been marked as resolved.
<b>Resolved By</b>	For resolved Events, shows which user marked the Event as resolved.
<b>Resolved On</b>	For resolved Events, shows when the Event was marked as resolved.
<b>Comment</b>	Shows any comments that were added when the Event was resolved.



## Viewing Event Details

Event 9717 11:02:45 AM · Sep 21, 2020 Snapshot mismatch **High** Not resolved

Details

Code

Affected Assets

Policy

Status

Source name [Rouge](#)

Source address 10.100.101.150 | 10.100.101.155 | 10.100.101.151

Backplane name **Backplane #52**

Code revision

Why is this important?

A change in the controller code was detected. Changes can occur over the network or via physical access to the controller.  
  
An attacker may use code changes to disrupt normal operations, to cause production losses or to create a security threat.

Suggested Mitigation

1) Check if the change was made as part of scheduled work.  
  
2) In the code revision tab, check if the code has changed. If it has changed, validate with an OT engineer that it matches the planned scope.  
  
3) If this was not part of a planned operation, check previous events involving the controller and examine if they affected the code.

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

The screenshot displays the 'All Events' interface. At the top, there is a search bar and buttons for 'Actions', 'Resolve All', and a refresh icon. Below this is a table with columns: Log ID, Time, Status, Event Type, Severity, and Policy Name. The table lists several event clusters, with Log IDs 1, 4, 68, 11, 5, 2, 3, 6, and 7. Log ID 4 is expanded, showing a cluster of events. Below the table, a detailed view for 'Event 4' is shown, including a title, a description, and a table of event details (Source Name, Source IP Address, Destination IP Address, Protocol, Port). To the right of the details table are two sections: 'Why is this important?' and 'Suggested Mitigation'.

Log ID	Time	Status	Event Type	Severity	Policy Name
1	09:16:49 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication to External...
4	09:17:29 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication to External...
68	09:17:30 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication to External...
11	09:18:03 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication to External...
5	09:17:29 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Conversation in a Common...
2	09:17:33 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC
3	09:17:35 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC
6	09:17:36 AM - Mar 2, 2022	Not resolved	Unauthorized Conversation	Medium	Communication from Inter...
7	09:17:41 AM - Mar 2, 2022	Not resolved	Intrusion Detection	Medium	Scans - VNC

Items: 266

Event 4 09:17:29 AM - Mar 2, 2022 Unauthorized Conversation Medium Not resolved

**Details**

A conversation in an unauthorized protocol has been detected

Source	Policy	Status
SOURCE NAME	DESKTOP-ILP15GP	
SOURCE IP ADDRESS	10.10.11.124	
DESTINATION IP ADDRESS	20.49.150.241	
PROTOCOL	HTTPS (tcp/443)	
PORT	443	

**Why is this important?**

Conversations in unauthorized protocols may indicate suspicious traffic. Some assets are not expected to communicate in non-standard protocols and any deviation from the standard protocols may suggest a potential threat. In addition, some protocols are insecure and should

**Suggested Mitigation**

Check if this communication is expected. If it is expected traffic, then adjust the Policy conditions so that Events aren't generated for similar communications in the future. If this communication is not expected, check the source asset to determine whether the source asset itself has been compromised. If this

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.

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

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 Configuration Events but not SCADA Events etc.) based on the filters that are currently applied to the display. For clustered Events, all Events in the cluster are marked as resolved.

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**.

The **Resolve All Events** window is displayed with the number of events to be resolved in the top right corner.



**Resolve all displayed events 20** ×

⚠ This action will resolve all displayed events, clustered events will be resolved automatically

COMMENT

Cancel Resolve All

2. In the **Comment** field, you can add a comment about the group of Events being resolved.  
(Optional field)

3. Click **Resolve**.

The warning message is displayed.

4. Click **Resolve**.

All Events in the current display are 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 [Policies](#).

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.

**Note:** 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".

**Exclude From Policy**

Future events that meet this condition will not affect asset risk score and will not appear in the events list. You will be able to delete this condition from the exclusions tab in the policy page.

**Policy Name**  
Snapshot Mismatch

**Exclude Conditions \***  
☒ Source asset is Rouge

**Exclusion Description**

Cancel Exclude

**Note:** 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
<b>Controller Activities</b>	Configuration Events (i.e. Activities)	<ul style="list-style-type: none"> <li>• Source asset</li> <li>• Source IP</li> <li>• Destination asset</li> <li>• Destination IP</li> </ul>
<b>Controller</b>	Change in Key State	Source asset



Validation		
	Change in Controller State	Source asset
	Change in FW Version	Source asset
	Module Not Seen	Source asset
	Snapshot Mismatch	Source asset
<b>Network</b>	Asset Not Seen	Source asset
	Change in USB Configuration	<ul style="list-style-type: none"><li>• Source asset</li><li>• USB Device ID</li></ul>
	IP Conflict	<ul style="list-style-type: none"><li>• MAC Addresses</li><li>• IP Address</li></ul>
	Network Baseline Deviation	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li><li>• Protocol</li></ul>
	Open Port	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Port</li></ul>
	RDP Connection	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li></ul>





		<ul style="list-style-type: none"><li>• Destination IP</li></ul>
	Unauthorized Conversation	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li><li>• Protocol</li></ul>
	FTP Log In (Failed and Successful)	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li></ul>
	Telnet Log In (Attempt, Failed and Successful)	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li></ul>
Network Threat	Intrusion Detection	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li><li>• SID</li></ul>
	ARP Scan	<ul style="list-style-type: none"><li>• Source asset</li></ul>



		<ul style="list-style-type: none"><li>• Source IP</li></ul>
	Port Scan	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li></ul>
SCADA	Modbus Illegal Data Address	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li></ul>
	Modbus Illegal Data Value	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li></ul>
	Modbus Illegal Function	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li></ul>
	Unauthorized Write	<ul style="list-style-type: none"><li>• Source asset</li><li>• Destination asset</li><li>• Tag Name</li></ul>
	IEC60870-5-104 StartDT IEC60870-5-104 StopDT	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li></ul>



		<ul style="list-style-type: none"><li>• Destination asset</li><li>• Destination IP</li></ul>
	IEC60870-5-104 function code based events	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li><li>• COT</li></ul>
	DNP3 events	<ul style="list-style-type: none"><li>• Source asset</li><li>• Source IP</li><li>• Destination asset</li><li>• Destination IP</li><li>• Source DNP3 address</li><li>• Destination DNP3 address</li></ul>



## Downloading Individual Capture Files

OT Security 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 [Network](#).

**Note:** 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 OT Security 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 OT Security 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 OT Security. See [FortiGate Firewalls](#).

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 OT Security Event already filled in.

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

Create Policy on FortiGate

SOURCE ADDRESS:

84.26.148.222

DESTINATION ADDRESS:

84.26.148.255

FORTIGATE SERVER:

FortiGate1

fortigateSTAS

Cancel

Create

5. Click **Create**.

The policy is created in FortiGate and the panel closes.

6. You can view the new policy in the FortiGate application.

A FortiGate administrator can adjust the settings as desired.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profile	Log	Rules
1	Tenbase-20190710	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10	Always	HTTP	Deny		Disabled	Log	10



## Network

---

OT Security monitors all activity in your 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.



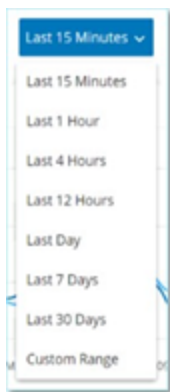
## Setting the Time Frame

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:

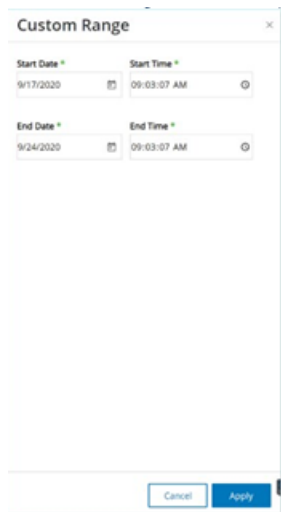
1. Click on **Time Frame Selection** in the header bar (default Last 15 Minutes).

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.



Custom Range

Start Date \* 9/17/2020 Start Time \* 09:03:07 AM

End Date \* 9/24/2020 End Time \* 09:03:07 AM

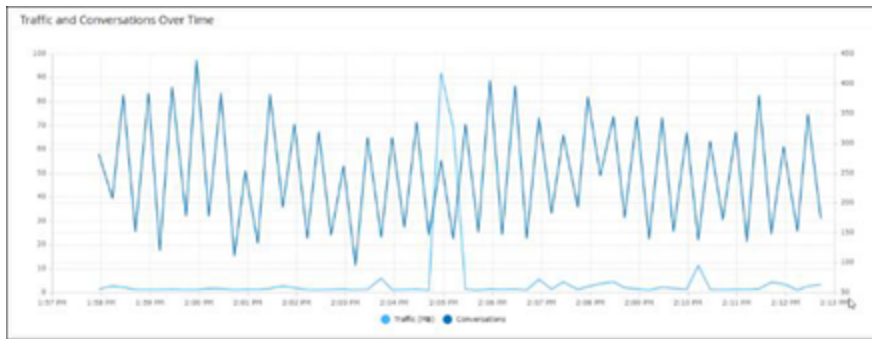
Cancel Apply

- 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 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.



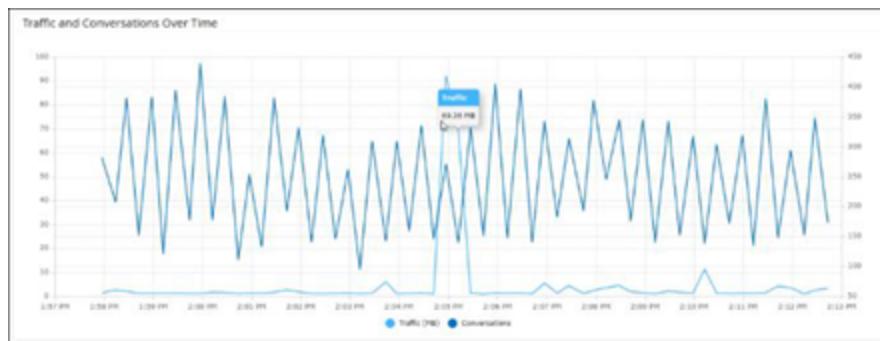
## Traffic and Conversations over Time



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:

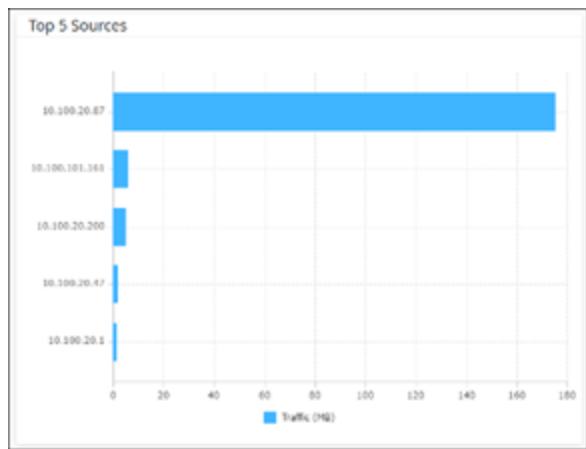
1. Hover over a point on the graph to display a pop-out window with specific data about the traffic and conversations that took place during that time segment.



**Note:** 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).



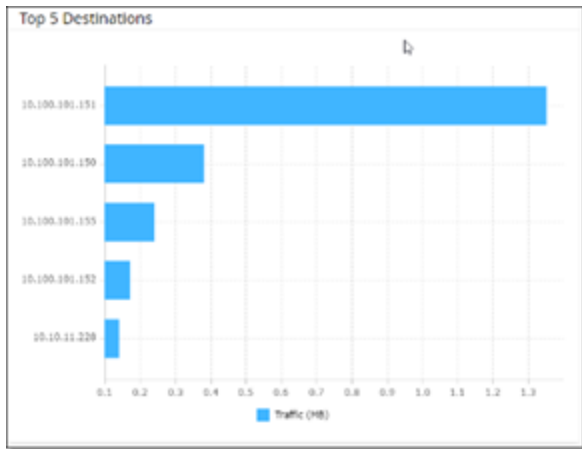
## Top 5 Sources



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.



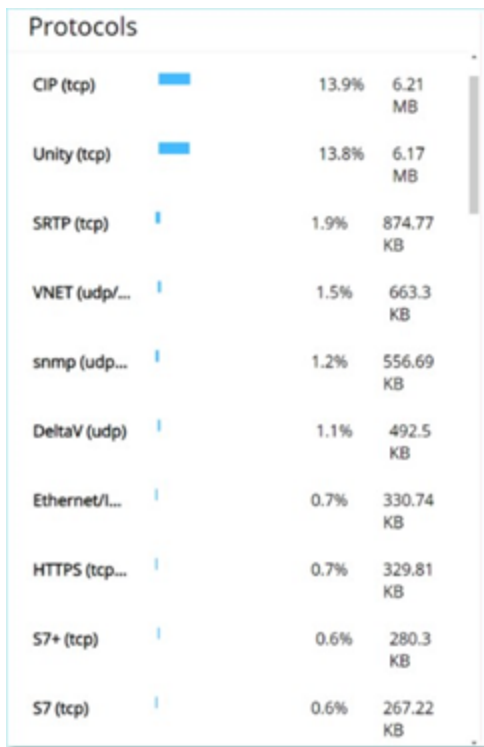
## Top 5 Destinations



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 [Management Console UI Elements](#).

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



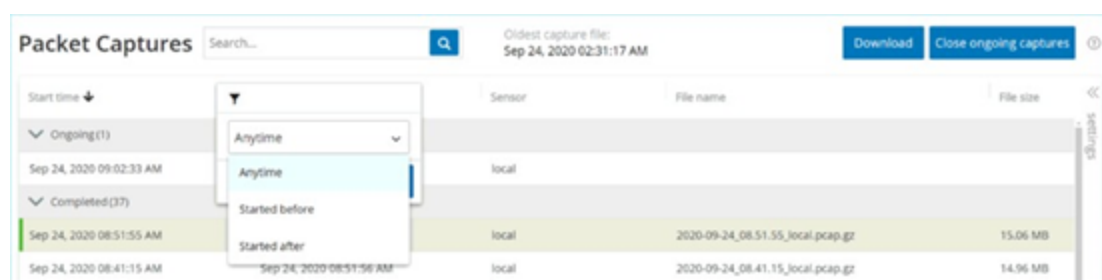
## Filtering Packet Capture Display

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 open 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 open with **Date** and **Time** fields allowing you to choose the desired date and time.
- c. Click **Apply**



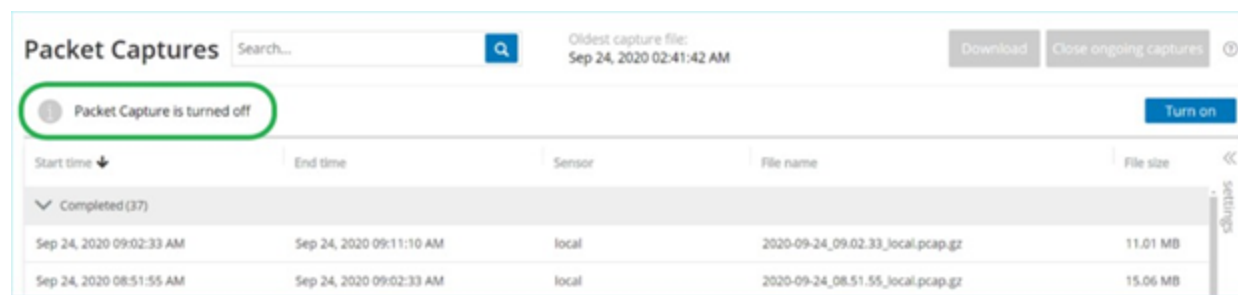
The filter is applied, and only the files generated within the selected time frame are displayed.



## Activating/Deactivating Packet Captures

Packet Capture can be activated/deactivated on the **Local Settings > Device Details** screen, see [Packet Captures](#).

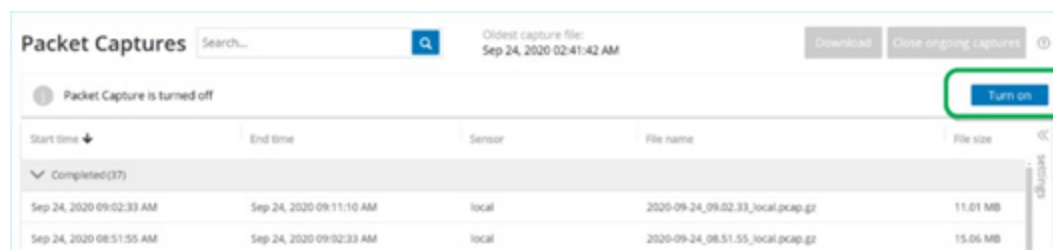
If the **Packet Capture** feature is turned off, then the **Packet Captures** screen shows a message informing you that it is turned off.



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.



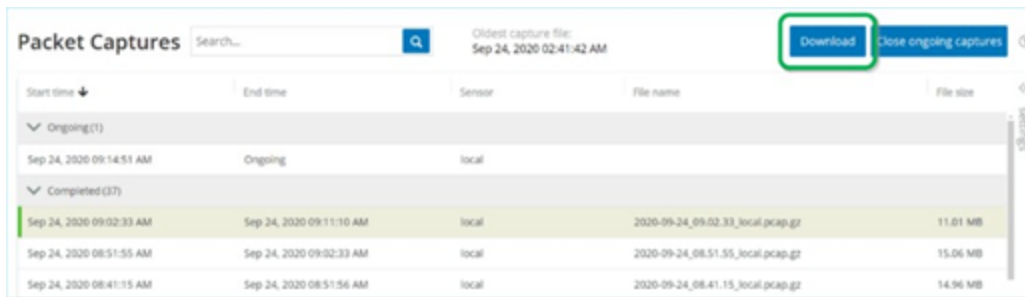
## Downloading Files

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:

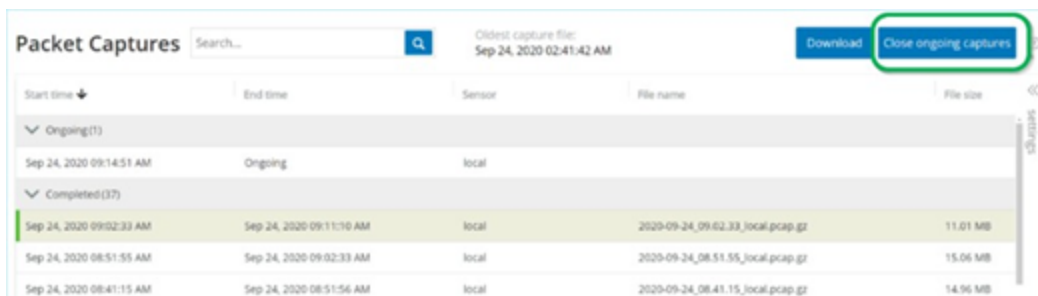
1. Under **Network**, select **Packet Captures**.
2. Select the desired file from the Packet Capture lists.
3. In the **Header** bar, click **Download**.



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 clicking **Export**.

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

The screenshot shows the 'Conversations' screen with a search bar and an 'Export' button. The table below represents the data shown in the screenshot.

START TIME	END TIME	DURATION	PACKETS	SOURCE ADDRESS	DESTINATION ADDRESS	PROTOCOL
Ongoing(56)						
Nov 26, 2020 08:10:05 AM	Ongoing	1 second	3	10.10.11.108	10.10.11.255	BROWSER (udp/138)
Nov 26, 2020 08:10:04 AM	Ongoing	1 second	1	10.100.111.28	10.100.111.255	cisco-net-mgmt (udp/1741)
Nov 26, 2020 08:10:04 AM	Ongoing	1 second	1	10.100.111.28	10.100.111.255	3Com-nsd (udp/1742)
Nov 26, 2020 08:10:04 AM	Ongoing	1 second	1	10.100.111.28	10.100.111.255	cinetgrfx-lm (udp/1743)
Nov 26, 2020 08:10:04 AM	Ongoing	1 second	1	10.100.111.28	10.100.111.255	encore (udp/1740)
Nov 26, 2020 08:10:01 AM	Ongoing	1 second	1	10.100.20.202	10.100.30.11	DNS (udp/53)
Nov 26, 2020 08:10:01 AM	Ongoing	1 second	11	10.100.20.31	10.100.20.202	SSH (tcp/22)
Nov 26, 2020 08:09:56 AM	Ongoing	1 second	16	10.100.111.151	10.100.111.255	BROWSER (udp/138)

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

Parameter	Description
<b>Start Time</b>	The time that the conversation began.
<b>End Time</b>	The time that the conversation ended. Shows Ongoing for conversations that are still in progress.
<b>Duration</b>	The amount of time that the conversation was in progress.
<b>Packets</b>	The number of data packets sent.
<b>Source</b>	The IP of the asset that sent the data.

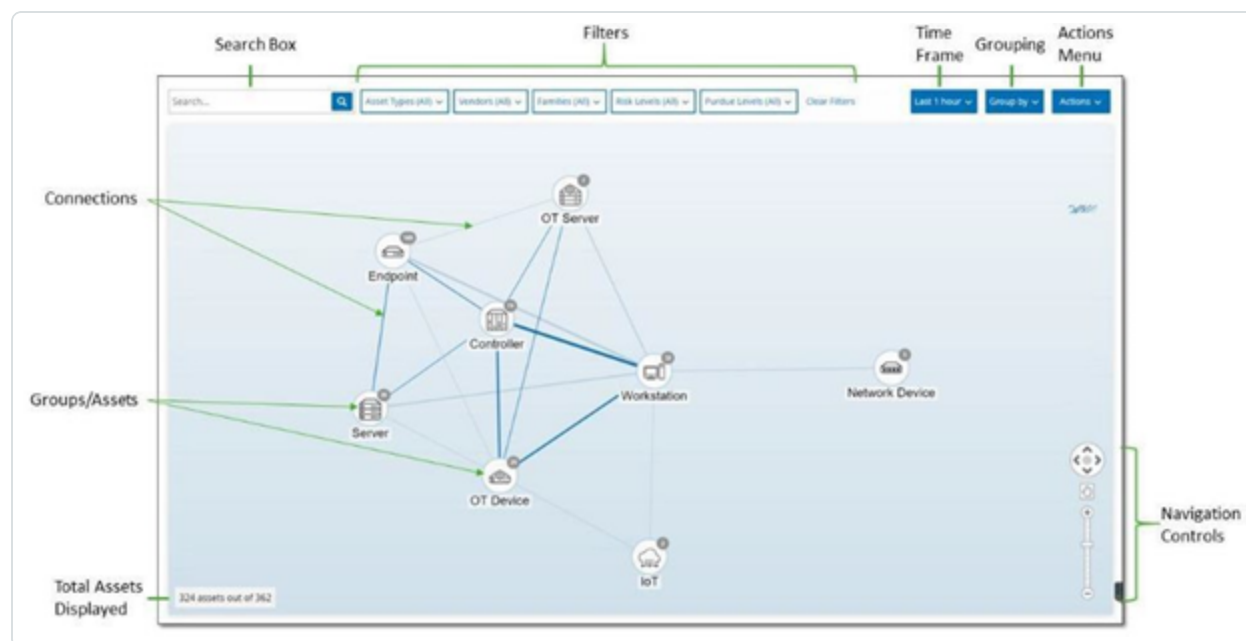


<b>Address</b>	
<b>Destination Address</b>	The IP of the asset that received the data.
<b>Protocol</b>	The protocol that was used for the communication.



## Network Map

The **Network Map** screen offers a visual representation of the network assets and their connections over time, as discovered by OT Security'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).
- Note:** 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. OT Security 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:

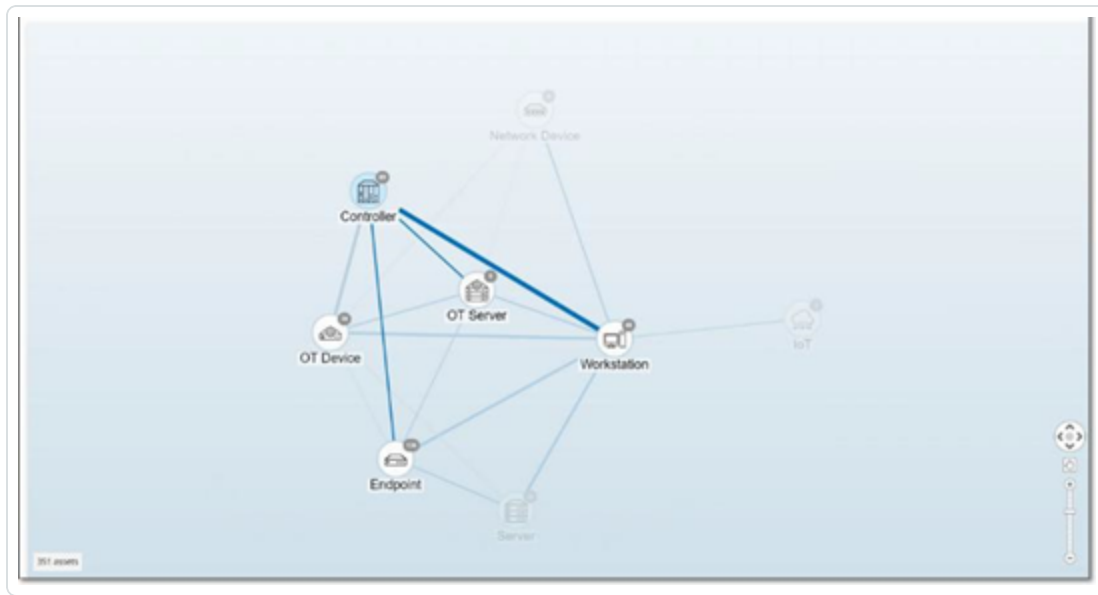
**Asset Type > Vendor > Family > Individual Asset.**

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.

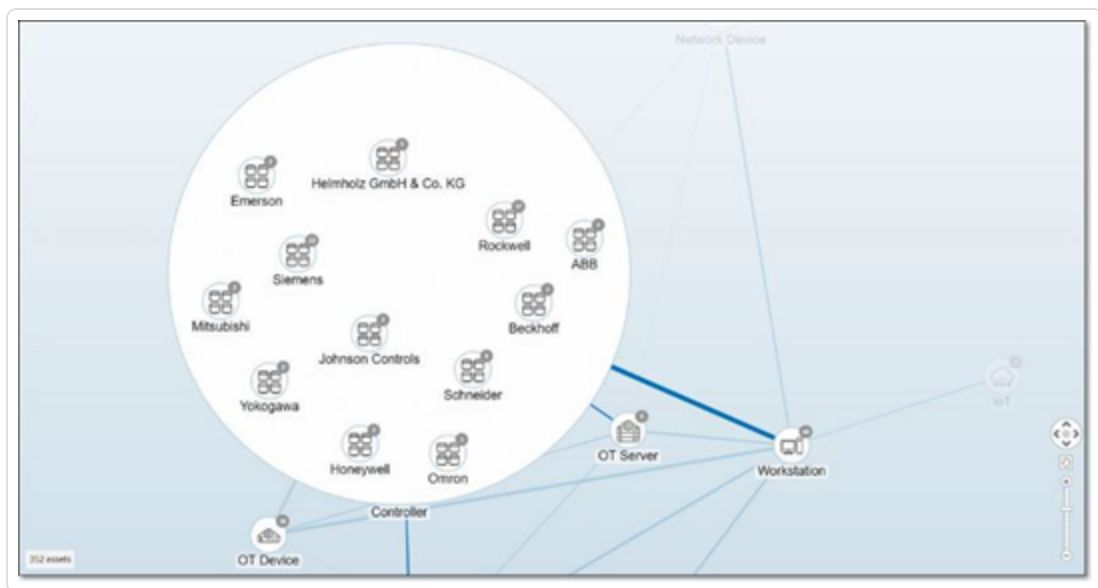
The following example shows how you can drill down into the display:

To drill down into an Asset Type Group:

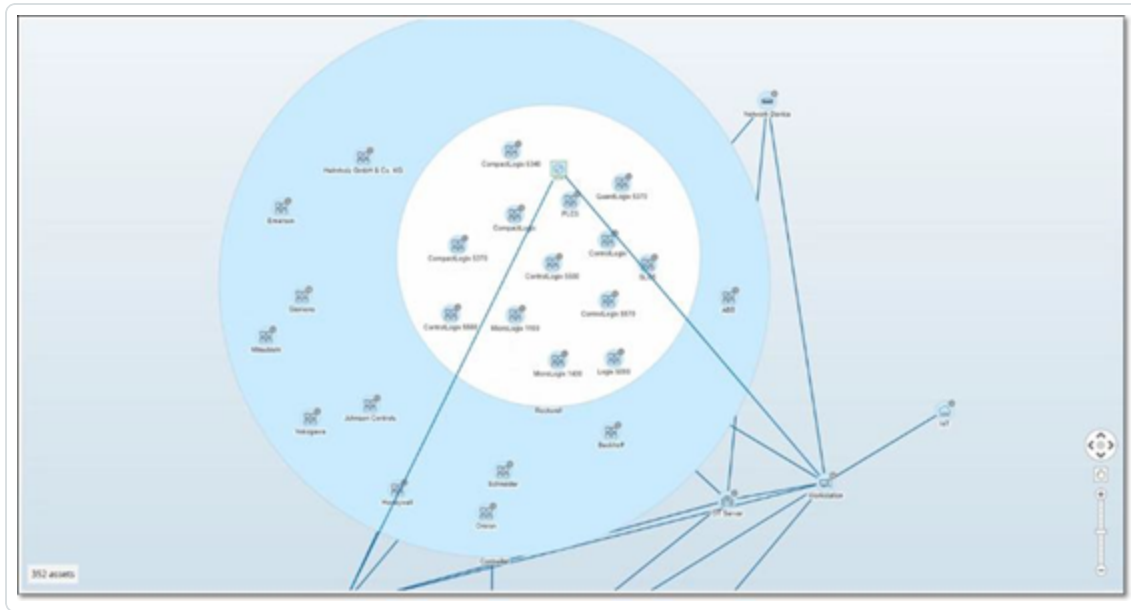
1. By default, when you open the Network Map screen it shows the assets grouped by Asset type.



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.

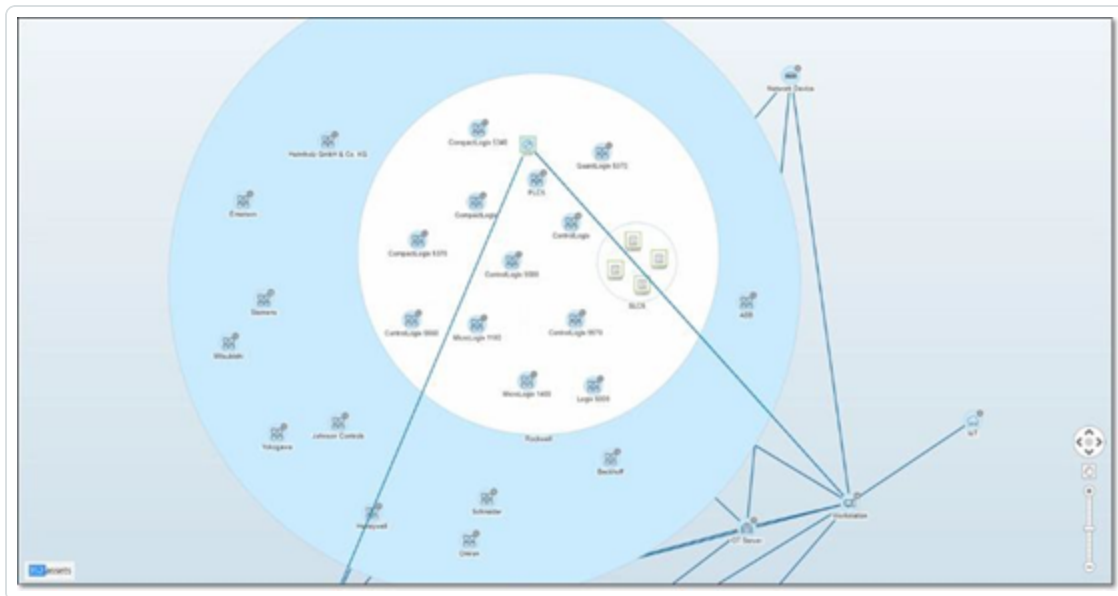


3. To drill down further, click on a Vendor group (e.g. Rockwell).



4. To drill down further, click on a Family group (e.g. SLC5).

The individual assets within that group are displayed.



5. You can now click on a specific asset to see details for that asset and its connections, see [Inventory](#).

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:

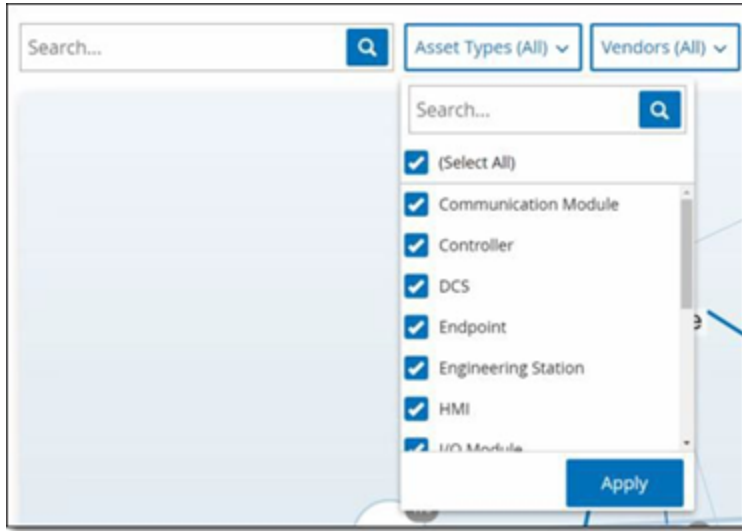
1. Click on the **Group by** button.
2. Select **No grouping**.

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.

**Note:** 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

---

OT Security 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 Tenable Nessus to detect them.

These programs are named Plugins, and are written in the Tenable 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 [Environment Configuration](#).



## 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 [Management Console UI Elements](#).

Name	Severity	VPR	Affected assets	Plugin family	Plugin ID	Source	Comment	Owner
<input type="checkbox"/> <a href="#">Excessive ICMP 2020-0800</a>	Critical	5.9	1	Tenable.cve	500052	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-2821</a>	Critical	6.7	2	Tenable.cve	500055	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-2736</a>	Critical	5.9	8	Tenable.cve	500059	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-0811</a>	Critical	5.9	1	Tenable.cve	500059	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-1220</a>	Critical	6.4	2	Tenable.cve	500065	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-0819</a>	Critical	5.2	2	Tenable.cve	500069	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-0808</a>	Critical	5.9	2	Tenable.cve	500071	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0468</a>	Critical	5.9	1	Tenable.cve	500075	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2009-3730</a>	Critical	5.9	2	Tenable.cve	500076	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0470</a>	Critical	5.9	1	Tenable.cve	500077	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0462</a>	Critical	5.9	1	Tenable.cve	500078	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0470</a>	Critical	5.9	1	Tenable.cve	500081	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-7000</a>	Critical	5.9	2	Tenable.cve	500084	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2018-8340</a>	Critical	6.5	2	Tenable.cve	500092	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0468</a>	Critical	5.9	1	Tenable.cve	500094	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0468</a>	Critical	5.9	1	Tenable.cve	500104	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0462</a>	Critical	5.9	2	Tenable.cve	500110	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2018-2842</a>	Critical	5.9	3	Tenable.cve	500122	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2018-2840</a>	Critical	5.9	3	Tenable.cve	500125	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0460</a>	Critical	5.9	2	Tenable.cve	500134	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2018-2829</a>	Critical	5.9	8	Tenable.cve	500170	Not		
<input type="checkbox"/> <a href="#">Excessive ICMP 2020-0801</a>	Critical	5.9	1	Tenable.cve	500187	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2019-10870</a>	Critical	5.9	2	Tenable.cve	500201	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-1220</a>	Critical	6.7	2	Tenable.cve	500208	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0468</a>	Critical	5.9	1	Tenable.cve	500207	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0467</a>	Critical	5.9	1	Tenable.cve	500208	Not		
<input type="checkbox"/> <a href="#">Schwabe CVE-2019-0819</a>	Critical	5.2	2	Tenable.cve	500209	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0470</a>	Critical	6.5	1	Tenable.cve	500213	Not		
<input type="checkbox"/> <a href="#">Redwatt CVE-2017-0470</a>	Critical	5.9	1	Tenable.cve	500214	Not		
<input type="checkbox"/> <a href="#">Excessive ICMP 2020-0800</a>	Critical	5.9	1	Tenable.cve	500216	Not		

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

Parameter	Description
<b>Name</b>	The Name of the Vulnerability. The Name is a link to show the full Vulnerability listing.
<b>Severity</b>	This score indicates the severity of the threat detected by this Plugin. Possible values: Info, Low, Medium or High.
<b>VPR</b>	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.
<b>Plugin ID</b>	The unique identifier of the Plugin.
<b>Affected Assets</b>	The number of assets in your network that are affected by this Vulnerability.
<b>Plugin family</b>	The family (group) with which this Plugin is associated.
<b>Comment</b>	You can add free text comments about this Plugin.



## Plugin Details

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

<

 **Network Interfaces List Detection (SNMP)**  
Vulnerability

Actions ▾

Severity

Affected assets

Plugin Family Name

Plugin ID

Medium

2

SNMP

1432

Details

Affected assets

Overview

NAME	Network Interfaces List Detection (SNMP)
SEVERITY	Medium
AFFECTED ASSETS	2
DESCRIPTION	The remote host is running an SNMPv1 agent. Using an SNMP get request, we can determine the list of network interfaces on the remote host. An attacker may use this information to gain more knowledge about the target host.
SOLUTION	Disable SNMP service on this host if you do not use it, or filter incoming UDP packets going to this port.

Plugin details

PLUGIN SOURCE	NNM
PLUGIN ID	1432
PLUGIN FAMILY NAME	SNMP

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.

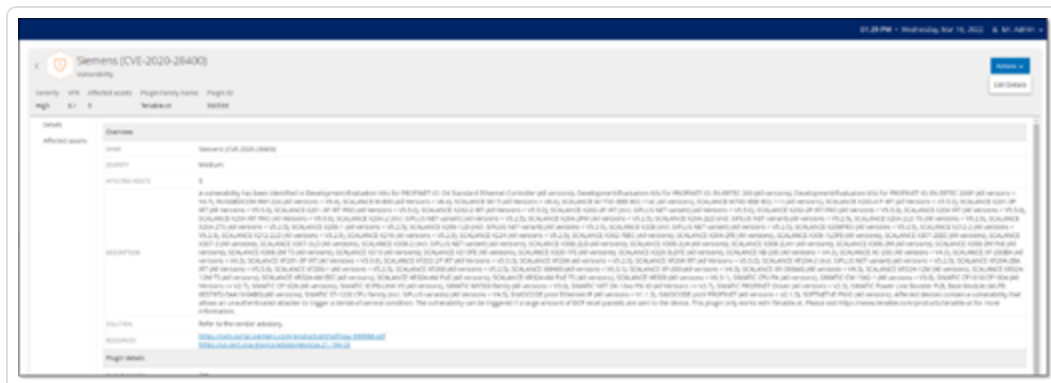


# Editing Vulnerability Details

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.

### Edit Vulnerability Details

COMMENT

OWNER

Cancel

Save

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 OT Security 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 OT Security 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.

**Note:** The max. number of IP ranges that can be sent to the Tenable Nessus Network Monitor is 128, therefore we recommend not exceeding this limit. In addition to the specified IP ranges, any host within the OT Security 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 [Inventory](#). 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 OT Security, 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 [Users and Roles](#).
- **User Groups** – An Admin user can view, edit, add and delete user groups. See [Users and Roles](#).
- **Authentication Servers** – 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 [Users and Roles](#).
- **Integrations** – set up integration with other platforms. OT Security currently supports integration with Palo Alto Networks Next Generation Firewall (NGFW) and Aruba ClearPass, as well as with other Tenable products (Tenable Security Center and Tenable Vulnerability Management). See [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 OT Security-FortiGate integration allows users to send firewall policy suggestions to a FortiGate firewall based on the OT Security 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 OT Security 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 OT Security will be unavailable to all users.
  - **Export Settings** – export OT Security 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 OT Security platform.
  - **Import Settings** – imports OT Security 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 OT Security platform and stores it on the local computer.
  - **Restart** – restarts the OT Security 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 OT Security platform. To power on, press the Power button on the OT Security 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 OT Security Queries screens enable you to configure and activate the queries features. For a general explanation of the Queries technology, see [OT Security 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.

**Note:** 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](#).

**Note:** 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.)
<b>All Controller Queries</b>	Activates all of the Query functions related to controllers, as described below.	n/a
<b>Periodic Snapshots</b>	Captures the current program deployed on each controller. By periodically taking snapshots, OT Security 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
<b>Policy Triggered Snapshots</b>	Enables the user to configure policies to trigger a snapshot when the conditions of a policy are met.	n/a
<b>Controllers Discovery</b>	A broadcast that searches for new controllers and assists in classifying unknown assets.	1/hr. – 1/6 weeks
<b>Controller State Query</b>	Detects the current PLC status (options are: Running, Stopped, Fault, No config. And Test).	1/5 min. – 1/hr.
<b>Diagnostic Buffer Query</b>	Queries for the Diagnostic Buffer event logs as defined in Siemens controllers.	1/day – 1/6 weeks
<b>Controller Details Query</b>	Retrieves the controller's hardware and firmware details.	1/hr. – 1/6 weeks
<b>Backplane Query</b>	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
<b>All Network Queries</b>	Activates all of the Query functions related to non-controller network assets, as described below.	n/a
<b>Port Mapping</b>	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.
<b>SNMP Query</b>	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
<b>DNS Query</b>	Searches for the DNS names of the assets in the network.	n/a
<b>ARP Query</b>	Retrieves the MAC address of new Ips detected in the network.	n/a
<b>NetBIOS</b>	This query sends a NetBIOS unicast	Frequency and Scheduling – 1/hr. – 1/6 weeks



	packet which is used to classify and detect Windows machines in the network.	
<b>Active Asset Tracking</b>	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
<b>WMI Query</b>	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.
<b>USB Connections Query</b>	Detects connection of USB/DoK devices to Windows PCs in the network.	Frequency and Scheduling – 1/day – 1/6 weeks
<b>Ripple20 Vulnerabilities</b>	This scan identifies CVEs	IP addresses or CIDRs



<b>Scan</b>	<p>related to the Ripple20 vulnerabilities. It uses a Tenable Nessus plugin.</p> <div><b>Note:</b> this scan must be run manually and it is only run on the assets within the specified IP addresses and/or CIDRs.</div>	
<b>Log4J Vulnerabilities Scan</b>	<p>This scan identifies CVEs related to the Log4J vulnerabilities. It uses a Tenable Nessus plugin.</p> <div><b>Note:</b> this scan must be run manually, and it is only run on the assets within the specified IP addresses and/or CIDRs.</div>	IP addresses or CIDRs





## Asset Discovery

OT Security automatically identifies assets in the network by detecting their interactions with other assets through the network. OT Security 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 the following queries to determine precise information about the asset: SNMP, Minimal Open Port Verification, CIP/DCP, NetBIOS, Backplane Query, Unicast Identification, Controller Details and Controller State.

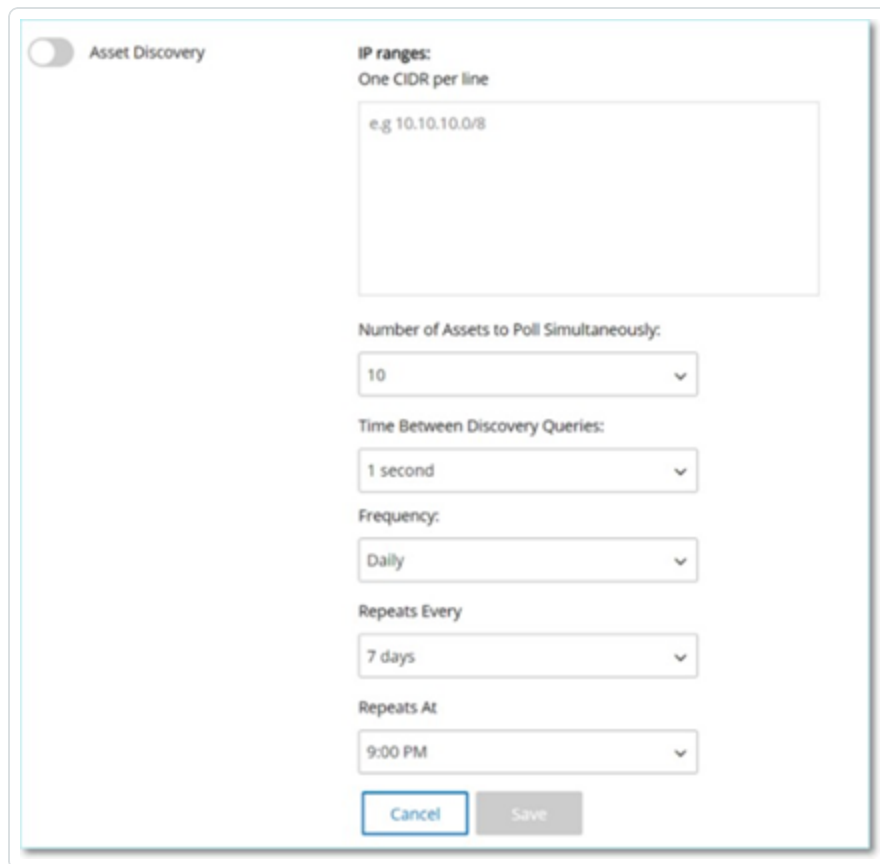
**Note:** Only IPs that are defined as Monitored Networks in the Asset Settings will be included in the scan.

**Note:** 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.



☒ Asset Discovery

**IP ranges:**  
One CIDR per line  
e.g 10.10.10.0/8

**Number of Assets to Poll Simultaneously:**  
10

**Time Between Discovery Queries:**  
1 second

**Frequency:**  
Daily

**Repeats Every**  
7 days

**Repeats At**  
9:00 PM

Cancel Save

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

**Note:** Segments of your network that are monitored by the mirror port do not need to be entered, and are automatically queried by OT Security. 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**.



## Tenable Nessus Plugin Scans

The Tenable Nessus plugin scan launches an advanced Tenable Nessus scan that executes a user-defined list of Plugins on the assets specified in the list of CIDRs and IP addresses.

The scan is executed on responsive assets within the designated CIDRs. However, in order to protect your OT devices, only confirmed network assets in the given range (non-PLCs) will be scanned. Assets of the type “Endpoint” won’t be scanned.

**Note:** Tenable 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 run a basic Tenable Nessus scan on any one asset, see [Inventory](#).

**Note:** The basic scan can be run on assets of type “Endpoint”.

To create a Nessus Plugin Scan:

1. Go to **Local Settings > Queries > Nessus Scans**.
2. Click on the **Create Scan** button.

The **Create Nessus Plugin List Scan** side panel is displayed.



The image shows a 'Create Nessus Plugin List Scan' dialog box. At the top, there is a title bar with a close button (X). Below the title bar, there is a progress indicator with two steps: 'IP Ranges' (selected, indicated by a blue dot) and 'Plugins' (indicated by a grey dot). A warning message is displayed: 'Nessus plugin list scan runs a user-defined list of plugins only on network assets within the specified IP ranges (CIDRs)'. Below the warning, there is a 'NAME' field with a blue asterisk, followed by a text input box. Below that, there is an 'IP RANGES' field with a blue asterisk, followed by a larger text input box. At the bottom, there are two buttons: 'Cancel' and 'Next >'. The 'Next >' button is disabled (greyed out).

### Create Nessus Plugin List Scan ×

IP Ranges ● Plugins ●

**⚠** Nessus plugin list scan runs a user-defined list of plugins only on network assets within the specified IP ranges (CIDRs).

NAME \*

IP RANGES \*

Cancel Next >

3. In the **Name** field, enter a name for the Tenable Nessus scan.
4. In the **IP Ranges** field, enter a range of IPs or CIDRs.
5. Click **Next**.

The **Plugins** pane is displayed.

**Create Nessus Plugin List Scan**

IP Ranges | **Plugins**

**Available Plugins** Search...

Plugin Family Name	Plugin Name	Plugin ID
<input checked="" type="checkbox"/> Settings (116)	<input checked="" type="checkbox"/> 3Com 3CServer/3CD...	16321
<input type="checkbox"/> Huawei Local Security Checks (7909)	<input type="checkbox"/> 3Com N8X ftpd CEL C...	11185
<input checked="" type="checkbox"/> NewStart CGSL Local Security Checks ...	<input checked="" type="checkbox"/> 3Com N8X ftpd CEL C...	11184
<input type="checkbox"/> Scientific Linux Local Security Checks ...	<input checked="" type="checkbox"/> 4D WebStar Pre-auth...	14195
<input checked="" type="checkbox"/> Mandriva Local Security Checks (3641)	<input checked="" type="checkbox"/> 4D WebSTAR SymLink...	14241
<input type="checkbox"/> Windows : Microsoft Bulletins (2712)	<input type="checkbox"/> Ability FTP Server Mu...	15628
<input type="checkbox"/> Red Hat Local Security Checks (9658)	<input type="checkbox"/> AIX FTPd libC Library ...	10009
<input checked="" type="checkbox"/> Solaris Local Security Checks (3784)	<input checked="" type="checkbox"/> Alcatel OmniSwitch D...	70210
<input checked="" type="checkbox"/> Denial of Service (110)	<input checked="" type="checkbox"/> Anonymous FTP Ena...	10079
<input checked="" type="checkbox"/> Palo Alto Local Security Checks (158)	<input checked="" type="checkbox"/> Anonymous FTP Writ...	10088
<input type="checkbox"/> RPC (39)	<input checked="" type="checkbox"/> Apache Log4Shell RC...	156115
<input type="checkbox"/> Firewalls (342)	<input checked="" type="checkbox"/> ArGoSoft FTP Server ...	15623
<input type="checkbox"/> Fedora Local Security Checks (16457)	<input checked="" type="checkbox"/> ArGoSoft FTP Server ...	16334
<input type="checkbox"/> Windows : User management (29)	<input checked="" type="checkbox"/> ArGoSoft FTP Server ...	17303
<input type="checkbox"/> PhotonOS Local Security Checks (1895)	<input checked="" type="checkbox"/> ArGoSoft FTP Server ...	21326
<input checked="" type="checkbox"/> Tenable.ot (653)	<input checked="" type="checkbox"/> ArGoSoft FTP Server ...	16094
<input type="checkbox"/> Ubuntu Local Security Checks (6406)	<input checked="" type="checkbox"/> ArGoSoft FTP Server ...	15439
<input checked="" type="checkbox"/> Gain a shell remotely (282)	<input checked="" type="checkbox"/> Ariel FTP Server Defa...	22870
<input checked="" type="checkbox"/> Misc. (2937)	<input type="checkbox"/> bftpd Multiple Comm...	10579
<input type="checkbox"/> Mobile Devices (140)	<input type="checkbox"/> bftpd NLST Comman...	10568
<input type="checkbox"/> CISCO (2206)	<input type="checkbox"/> BlackJumboDog FTP ...	14256
<input type="checkbox"/> Virtuozzo Local Security Checks (341)	<input checked="" type="checkbox"/> BlackMoon FTP Login...	11648
<input type="checkbox"/> Peer-To-Peer File Sharing (105)	<input type="checkbox"/> BlackMoon FTP Serve...	51585

Items: 56 Items: 261

**Back** **Cancel** **Save**

**Note:** The Plugins displayed are device-specific. Your license must be up-to-date in order to receive new Plugins. To update your license, see [Updating the License](#).

6. Select Plugin Families as desired in the left column to include them in the scan, and deselect individual Plugins as desired in the right column.

**Note:** For more information about Tenable Nessus Plugin Families, see <https://www.tenable.com/plugins/nessus/families>.

7. Click **Save**.

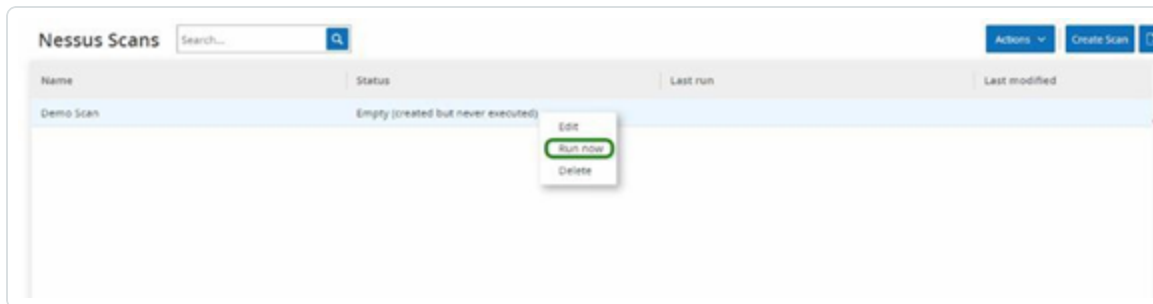


The new Tenable Nessus scan appears in the **Nessus Scans** screen.

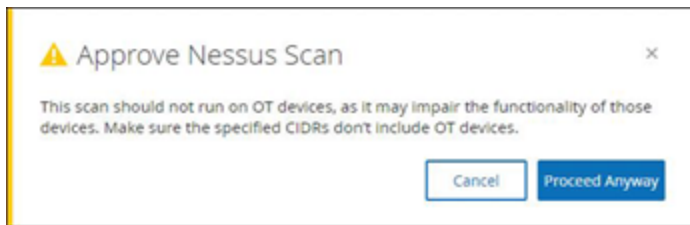
**Note:** To edit or delete an existing Tenable Nessus Scan, right-click on the desired Scan row and select **Edit** or **Delete**.

To run a Nessus Plugin Scan:

1. On the Nessus Scans screen, select the desired Scan row, right-click and select Run now, or click **Actions > Run now**.



The **Approve Nessus Scan** dialog appears.



2. If you know there are no OT devices included in the scan, click **Proceed Anyway**.

The dialog closes and the Scan is saved.

3. To run the Scan, right-click on the Scan row again and select **Run now**.

The **Approve Nessus Scan** dialog appears again.

4. Click **Proceed Anyway**.

The scan is now running. Scans may be paused/resumed, stopped, and killed, depending on their current status.

## System Configuration



The OT Security 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 OT Security configuration. You can view the info and edit the configuration on this screen.

Device

Device Name

The name of Terminix management system.

DEVICE NAME

T234

Save

Device URL

Device URL allows you to set the single URL from which the system can be accessed (PQDS). Adding it is a critical change. The new PQDS will not be generated again. Assume to make note of the exact string with make the URL responsive. Please make sure to verify the resolution before proceeding (Change requires restart).

Save

System Time

Determines the time of the Terminix system, system time, together with the time zone, determines the displayed time of alerts, activities, system log events and all other time related features (Change requires restart).

MANUAL SYSTEM TIME

Tue Jul 26 2022 11:42:58 GMT+0000

Save

Timezone

Determines the time zone for the Terminix system, Time zone, together with the system time, determines the displayed time of alerts, activities, system log events and all other time related features.

TIMEZONE

UTC+07:00

Save

DNS Servers

DNS servers are used by Terminix to assign DNS names to the alerts Terminix identifies. Server servers can be defined.

IP 1

10.100.00.11

Save

Automatic Logout

Determines the period after which logged in users will be logged out automatically and required to log in again (Requires restart).

LOGOUT AFTER

2 Weeks

Save

☒ Ping Requests

By default Terminix does not respond to ping requests in order to remain hidden from external scans. You can configure the system to respond to Ping requests in this section.

☐ Packet capture

Turning on the full packet capture capability will cause Terminix to record all traffic from all its sensors in a continuous growing file, as well as to delete older files upon reaching maximum storage capacity limit.

☐ Auto approve sensor pairing requests

☒ Enable Usage Statistics

The Enable Usage Statistics option specifies whether Terminix collects anonymous telemetry data about your Terminix deployment, other analytics. Terminix 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. Terminix uses the data to improve your user experience in future Terminix releases and for other reasonable business purposes. In accordance with the Terminix Master Agreement, you can disable this option at any time to stop sharing usage statistics with Terminix, after you enable or disable this option, all Terminix users must refresh their browser window for the changes to take effect.

The following info is shown:



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

**Note:** 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.

**Note:** 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 OT Security system to assign DNS names to the assets OT Security 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.
- **Open Ports Age Out Period** – determines the period after which Open Port listings will be removed from the individual Asset Details screen if no further indication is received that the port is still open. Default setting is two weeks. For more information, see [Inventory](#).



## Ping Requests

---

Turning on Ping Requests activates the OT Security 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 [Network](#).

To Activate Packet Captures:

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

**Note:** 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**.

**Note:** 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 OT Security 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 OT Security 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**.

**Note:** 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.

**Note:** 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.

IP	Status	Active Queries	Active Query Networks	Name	Last Update	Sensor Identifier	Version	Throughput
10.100.20.144	Pending approval	N/A			09:07:18 AM - Jul 26, 2022	9eb807d7-348c-40...	3.14.4	0 Bps
10.100.20.47	Connected (Unauthenticated)	N/A		remote10.100.20.47_...	05:43:03 AM - Jul 26, 2022	b4c9c5a-dc7f-4964...		181.66 Kbps

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

Parameter	Description
<b>IP</b>	The IPv4 address of the Sensor.
<b>Status</b>	The status of the Sensor: Connected, Connected (Unauthenticated), Pending approval, Disconnected or Paused.
<b>Active Queries</b>	The capacity of the Sensor to send Active Queries (Enabled, Disabled, N/A)
<b>Active Query Networks</b>	The network segments to which the Sensor is assigned.
<b>Name</b>	The name of the Sensor in the System.
<b>Last Update</b>	The date and time that the Sensor information was last updated.



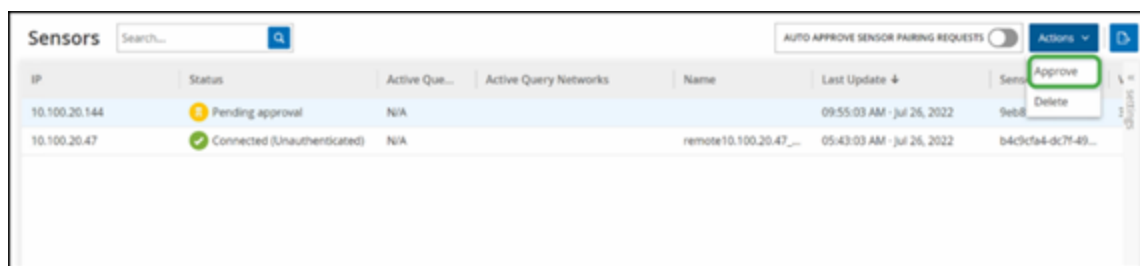
<b>Sensor Identifier</b>	The Sensor Universal Unique Identifier (UUID), a 128-bit value used to uniquely identify an object or entity on the internet.
<b>Version</b>	The Sensor version.
<b>Throughput</b>	A measure of how much data is streaming through the sensor (in kilobytes per second).

## 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.



**Note:** 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.

**Note:** 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.

**Edit Sensor**

NAME

Test3

Active Query Networks

ONE CIDR PER LINE

2.2.2.2/32  
192.168.0.0/24

☒ Sensor active queries

Cancel Save

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.

**Note:** 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.

8. 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 OT Security Appliance > Step 4 – Setup Wizard > SCREEN 2 – DEVICE](#).

### Port Configuration

Port Configuration

Edit

You can separate the Tenable.ot management interface from the Queries interface. (Change requires restart)

1  Queries + Management	2  Mirror Port	3  Reserved	4  Reserved
-------------------------------	----------------------	-------------------	-------------------

Queries IP configuration

IP	10.100.20.87
SUBNET MASK	255.255.255.0
GATEWAY	10.100.20.1



## Updates

Keeping Plugins and IDS Engine Ruleset 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.

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

**Note:** 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.

## Tenable Nessus Plugin Set Updates

### Cloud Updates

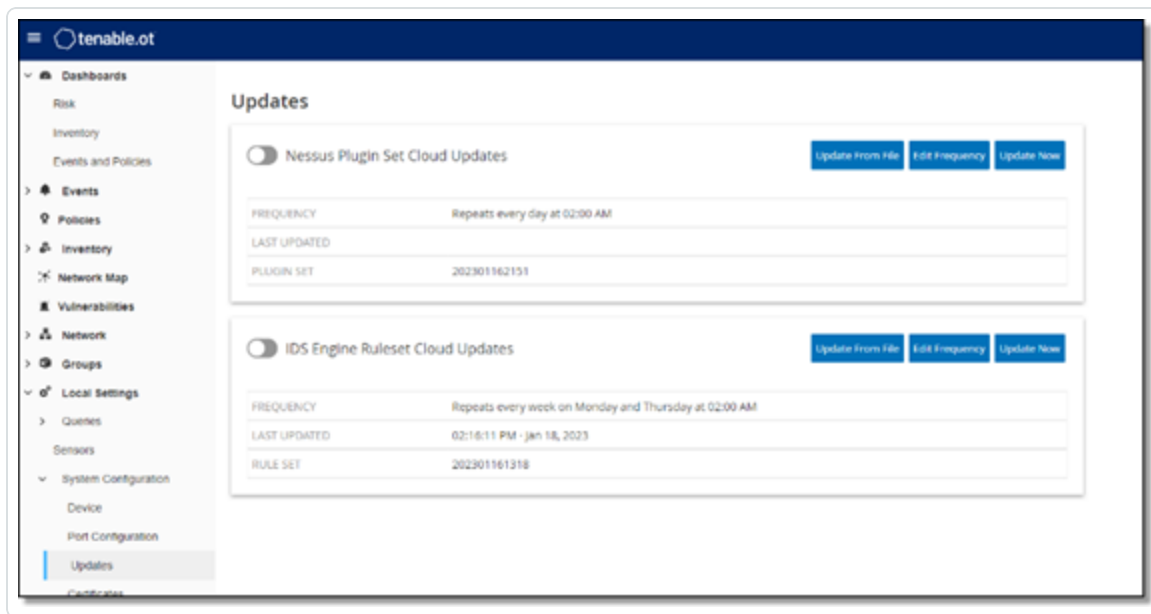
Users with an internet connection can update Plugins through the Cloud. When automatic updates are turned on, Plugins will update at the time and frequency set by the user (Default: daily at 02:00 AM).

### 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 with **Nessus Plugin Set Cloud Updates**, showing the number of your Plugin Set, when it was last updated and the update schedule.



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

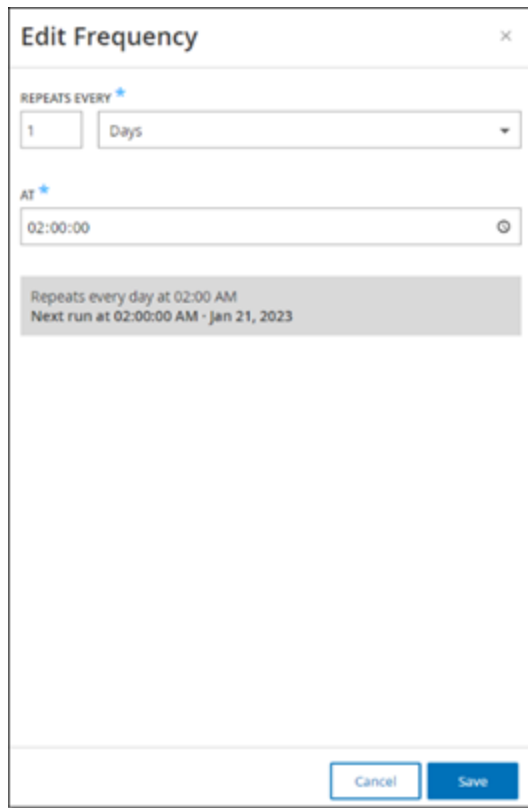
To edit the schedule of automatic updates of Plugins:

1. Under **Local Settings**, go to **System Configuration > Updates**.

The **Updates** screen is displayed with **Nessus Plugin Set Cloud Updates**, showing the number of your Plugin Set, when it was last updated and the update schedule.

2. Click on the **Edit Frequency** button.

The **Edit Frequency** side panel is displayed.



**Edit Frequency**

REPEATS EVERY <sup>\*</sup>

1 Days

AT <sup>\*</sup>

02:00:00

Repeats every day at 02:00 AM  
Next run at 02:00:00 AM - Jan 21, 2023

Cancel Save

3. Under **Repeats Every**, set the time interval at which you would like to update the Plugins by entering a number and selecting a unit of time (Days or Weeks) from the dropdown menu.
4. If you select **Weeks**, select which day(s) of the week you would like to perform a weekly update on the plugins.
5. Under **At**, set the time of day at which you would like to update the Plugins (in HH:MM:SS) by clicking on the clock icon and selecting the time, or by entering the time manually.
6. Click **Save**.

A dialog is displayed, letting you know that the frequency has been updated successfully.

## Performing Manual Cloud Updates of Plugins

To manually update Plugins:



1. Under **Local Settings**, go to **System Configuration > Updates**.

The **Updates** screen is displayed with **Nessus Plugin Set Cloud Updates**, showing the last updated version of your Plugin Set, when it was last updated and the update schedule.

2. Click on the **Update Now** button.

A dialog is displayed, letting you know that the update has started. When the update is completed, the **Plugin Set** field will display the number of the current Plugin Set.

**Note:** While the Plugin Set update is in progress, keep the browser window open and do not refresh the page.

## Offline Updates

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

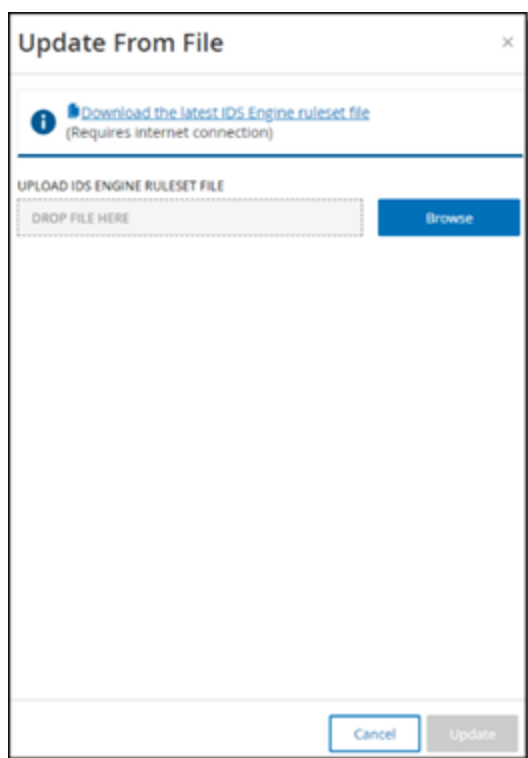
To update Plugins offline:

1. Under **Local Settings**, go to **System Configuration > Updates**.

The **Updates** screen is displayed with **Nessus Plugin Set Cloud Updates**, showing the number of your Plugin Set, when it was last updated and the update schedule.

2. Click on the **Update From File** button.

The **Update From File** window is displayed.



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

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

4. Click **Browse** and navigate to the Plugin set file you downloaded from the OT Security Customer portal.
5. Click **Update**.

## IDS Engine Ruleset Updates

### Cloud Updates

Users with an internet connection can update their IDS Engine Ruleset through the Cloud. When automatic updates are turned on, the IDS Engine Ruleset will update at the time and frequency set by the user (Default: Repeats every week on Monday and Thursday at 02:00 AM).

### Setting Automatic Cloud Updates of the IDS Engine Ruleset

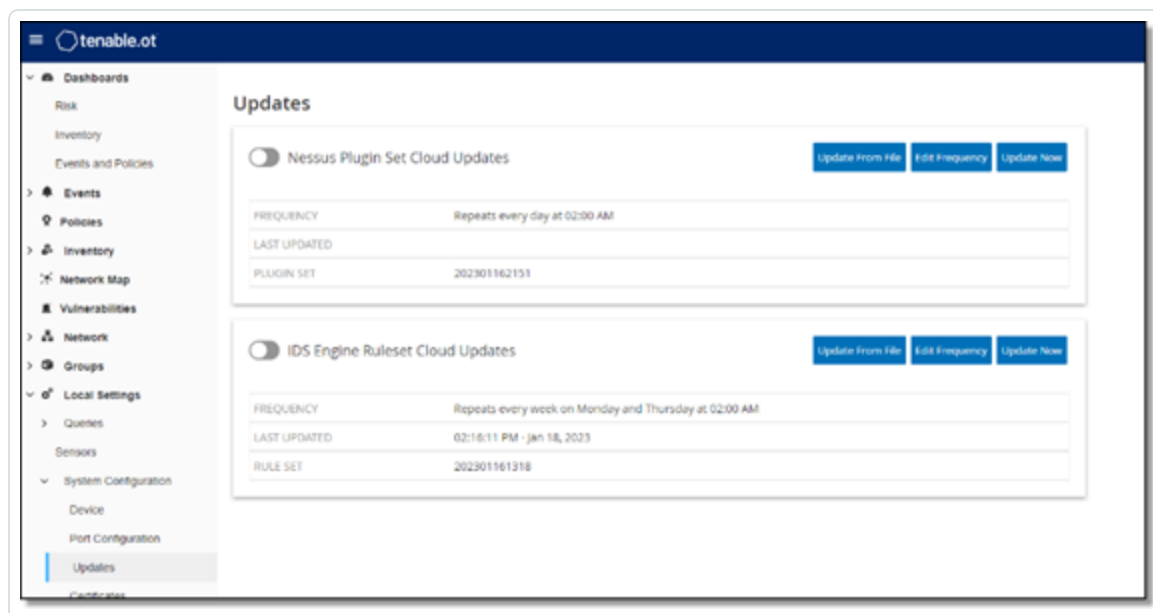




To enable automatic updates of the IDS Engine Ruleset:

1. Under **Local Settings**, go to **System Configuration > Updates**.

The **Updates** screen is displayed with **IDS Engine Ruleset Cloud Updates**, showing the number of your Rule Set, when it was last updated and the update schedule.



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

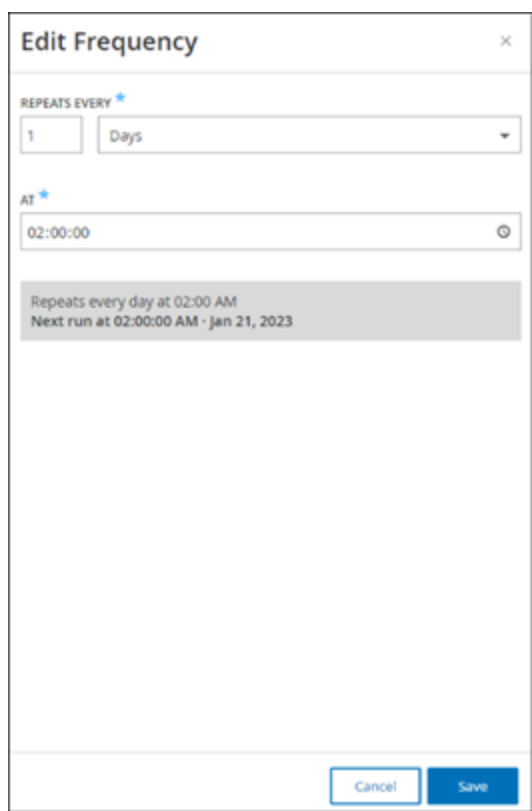
To edit the schedule of automatic updates of the IDS Engine Ruleset:

1. Under **Local Settings**, go to **System Configuration > Updates**.

The **Updates** screen is displayed with **IDS Engine Ruleset Cloud Updates**, showing the number of your Rule Set, when it was last updated and the update schedule.

2. Click on the **Edit Frequency** button.

The **Edit Frequency** side panel is displayed.



**Edit Frequency**

REPEATS EVERY <sup>\*</sup>

1 Days

AT <sup>\*</sup>

02:00:00

Repeats every day at 02:00 AM  
Next run at 02:00:00 AM - Jan 21, 2023

Cancel Save

3. Under **Repeats Every**, set the time interval at which you would like to update the Ruleset, by entering a number and selecting a unit of time (Days or Weeks) from the dropdown menu.
4. If you select **Weeks**, select which day(s) of the week you would like to perform a weekly update on the Ruleset.
5. Under **At**, set the time of day at which you would like to update the IDS Engine Ruleset (in HH:MM:SS) by clicking on the clock icon and selecting the time, or by entering the time manually.
6. Click **Save**.

A dialog is displayed, letting you know that the frequency has been updated successfully.

## Performing Manual Cloud Updates of the IDS Engine Ruleset

To manually update the IDS Engine Ruleset:



1. Under **Local Settings**, go to **System Configuration > Updates**.

The **Updates** screen is displayed with **IDS Engine Ruleset Cloud Updates**, showing the number of your Rule Set, when it was last updated and the update schedule.

2. Click on the **Update Now** button.

A dialog is displayed, letting you know that the update has started. When the update is completed, the **Ruleset** field will display the number of the current IDS Engine Ruleset.

## Offline Updates

Users without an internet connection on their OT Security device can manually update their IDS Engine Ruleset by downloading the latest Ruleset from the Tenable Customer Portal and uploading the file.

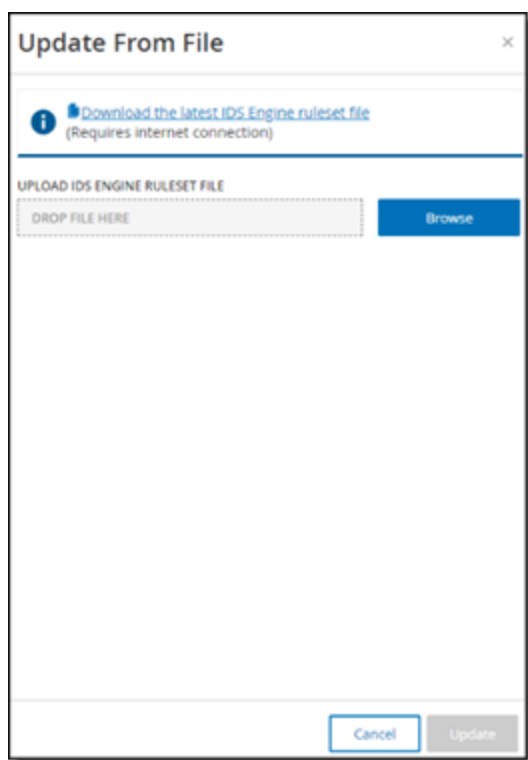
To update the IDS Engine Ruleset offline:

1. Under **Local Settings**, go to **System Configuration > Updates > IDS Engine Ruleset Cloud Updates**.

The **Updates** screen is displayed, showing the number of your Ruleset, when it was last updated and the update schedule.

2. Click on the **Update From File** button.

The **Update From File** window is displayed.



3. If you have not yet done so, click the link to download the latest IDS Engine ruleset file.

**Note:** Downloading the latest IDS Engine ruleset file from the link is only possible through an internet connection, such as with an internet-connected PC.

4. Click **Browse** and navigate to the IDS Engine ruleset set file you downloaded from the OT Security Customer portal.
5. Click **Update**.



# Certificate

## Generating an HTTPS Certificate

The HTTPS certificate ensures the system is using a secure connection to the OT Security 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.

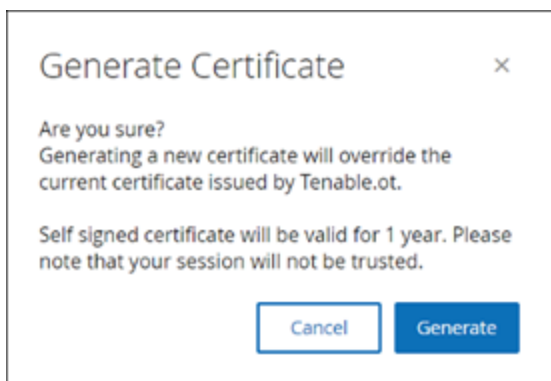
**Note:** Generating a new certificate will override the current certificate.

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**.

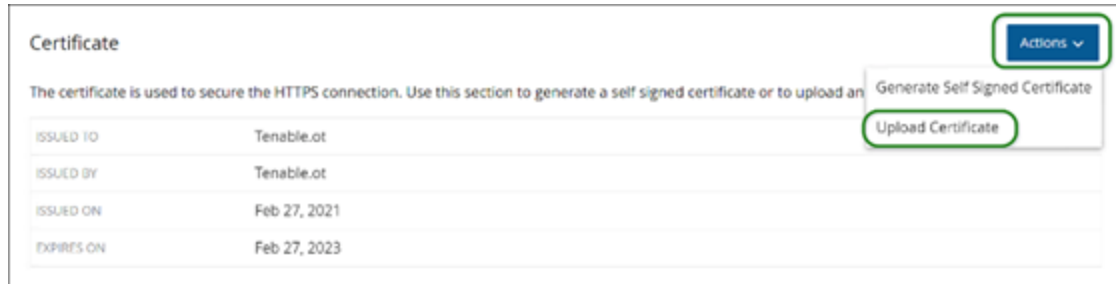
The self signed certificate is generated and can be viewed in the **Local Settings > System Configuration > Certificate** screen.



## Uploading an HTTPS Certificate

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.



**Upload Certificate** [X]

**CERTIFICATE FILE**  
PEM format only

DROP FILE HERE [Browse]

**PRIVATE KEY FILE**  
PEM format only

DROP FILE HERE [Browse]

**PRIVATE KEY PASSPHRASE**

[Cancel] [Upload]

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.

**Note:** 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 OT Security 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 OT Security 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.

The screenshot shows the 'License' screen with a table of license information and an 'Actions' button in the top right corner.

License	
LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	dummyActivationCode
COMPUTER ID	dummyUniqueId

2. Click on the **Actions** button and select **Update license**.

The **Generate Certificate** and **Enter Activation Code** steps are shown.

The screenshot shows the 'License' screen with the same table as before, followed by instructions to follow steps to update the license. Two steps are listed: '1 Generate activation certificate' and '2 Enter activation code, obtain an activation code from your sales rep. or from the Self-service portal'. Each step has a corresponding button: 'Generate Certificate' and 'Enter Activation Code'. A 'Cancel' button is also present at the bottom right.

Follow these steps in order to update your license

- 1 Generate activation certificate Generate Certificate
- 2 Enter activation code, obtain an activation code from your sales rep. or from the [Self-service portal](#) Enter Activation Code

Cancel

3. In the **(1) Generate activation certificate** field, click on the **Generate Certificate** button.

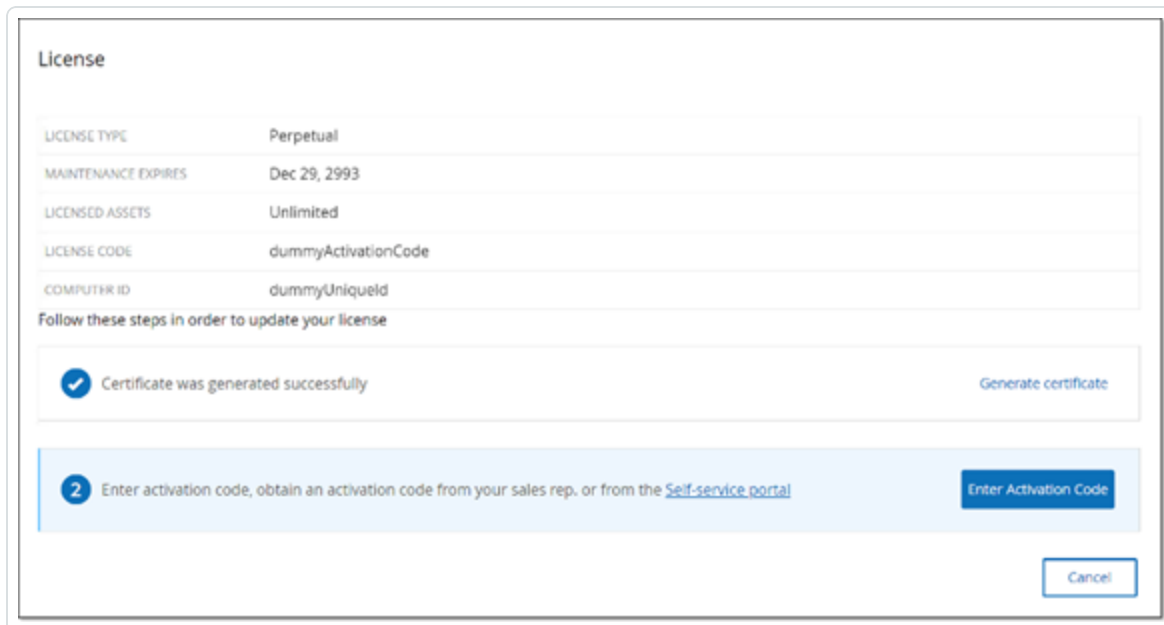
The **Generate Certificate** side panel is shown with the Activation Certificate.



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 OT Security Offline** screen opens in a new tab.



**Note:** You will need to access the Activate OT Security Offline screen from an Internet-connected device using the following URL: <https://provisioning.tenable.com/activate/offline/tenable-ot>.

**Note:** If you are not currently logged in to [tenable.com](https://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.



**Activate Tenable.ot Offline**

1 Activation Info

**Offline Activation Details**

**Tenable.ot**  
**Activation Certificate**

[Long alphanumeric string]

**License Code**

[Text input field]

☒ I have read and understand the Tenable Software License Agreement

**Generate Activation Code**

**Confirmation**

**Information**

Please copy / paste your Activation Certificate and click "Generate Activation Code"

[How Do I Generate a Tenable.ot Activation Certificate?](#)

[Tenable.sc Offline Activation](#)

[Nessus Professional Offline Activation](#)

**Note:** 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.

**Activate Tenable.ot Offline**

1 Activation Info

2 Confirmation

**Offline Activation Code Successfully Created!**

Enter this activation code in the Tenable.ot license activation or renewal/upgrade process

**Copy text to Clipboard**

[Long alphanumeric string]

**Confirmation**

Success

**Close**

10. Click **Copy text to Clipboard**.



11. Navigate back to the **License** tab, and click the **Enter Activation Code** button.

The screenshot shows a 'License' tab interface. At the top, it says 'License'. Below this is a table with the following details:

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	dummyActivationCode
COMPUTER ID	dummyUniqueld

Below the table, it says 'Follow these steps in order to update your license'. There are two steps:

1. Certificate was generated successfully. A 'Generate certificate' button is to the right.
2. Enter activation code, obtain an activation code from your sales rep. or from the [Self-service portal](#). An 'Enter Activation Code' button is to the right.

A 'Cancel' button is located at the bottom right of the panel.

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

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

The screenshot shows the 'Enter Activation Code' side panel. It has a title bar with a close button (X). Below the title bar is a text area labeled 'ACTIVATION CODE' with a blue asterisk. The text area contains a long, multi-line activation code. At the bottom of the panel are two buttons: 'Cancel' and 'Activate'.

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 OT Security 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**.

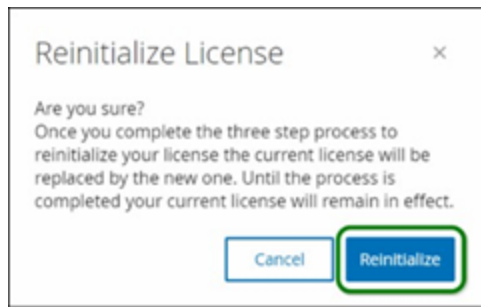
The screenshot shows a 'License' configuration page. At the top left is the title 'License'. At the top right is a blue button labeled 'Actions' with a downward arrow. Below these is a table with five rows, each representing a license attribute and its value.

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	dummyActivationCode
COMPUTER ID	dummyUniqueld

2. Click on the **Actions** button and select **Reinitialize license**.

A confirmation window is shown.

3. Click **Reinitialize**.



The License screen is shown with the three reinitialization steps.

A screenshot of the "License" screen. It displays license details in a table and a three-step reinitialization process. The table shows: LICENSE TYPE: Perpetual, MAINTENANCE EXPIRES: Dec 29, 2993, LICENSED ASSETS: Unlimited, LICENSE CODE: dummyActivationCode, and COMPUTER ID: dummyUniquelid. Below the table, it says "Follow these steps in order to reinitialize your license". The steps are: 1. Enter license code (with an "Enter license code" button), 2. Generate activation certificate (with a "Generate Certificate" button), and 3. Enter activation code, obtain an activation code from your sales rep. or from the [Self-service portal](#) (with an "Enter Activation Code" button). A "Cancel" button is at the bottom right.

4. 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 OT Security. 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.

**Note:** When assets are added manually, Events aren't detected for those Assets until OT Security 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	Descriptio	Result	Error
2	AAA	Plc	High	Critic	10.100.20.aa:bb:cc:dd	Siemens	S7300	2.3.1		Level1	Italy	Siemens,	Failure	IP 10.100.20.21 already exists
3	BBB	Server	Medium	C	10.200.30.30	VMware			Windows Server 2012				Success	
4	CCC	Switch			AA:bb:cd: Catalyst	C2960		12.3		Level3			Success	
5	DDD	Unknown	None	Criticality					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.



### Event Clusters

☐ Configuration Event Clusters Edit

MAXIMUM TIME BETWEEN CONSECUTIVE EVENTS	5 minutes
MAXIMUM TIME BETWEEN FIRST AND LAST EVENT	10 minutes

☒ SCADA Event Clusters Edit

MAXIMUM TIME BETWEEN CONSECUTIVE EVENTS	5 minutes
MAXIMUM TIME BETWEEN FIRST AND LAST EVENT	1 day

☒ Network Threat Event Clusters Edit

MAXIMUM TIME BETWEEN CONSECUTIVE EVENTS	5 minutes
MAXIMUM TIME BETWEEN FIRST AND LAST EVENT	1 day


☒ Network Event Clusters Edit

MAXIMUM TIME BETWEEN CONSECUTIVE EVENTS	5 minutes
MAXIMUM TIME BETWEEN FIRST AND LAST EVENT	1 day

- Click on the toggle to enable desired categories for clustering.
- To configure the time intervals for a category, click on the **Edit** button.

The **Edit Configuration** window is displayed.

- Enter the desired number value in the number field and adjust the unit of time using the drop-down list.

**Note:** For more information about clustering and time intervals, click on the  button.

- Click **Save**.



## PCAP Player

PCAP Player						<input type="text" value="Search..."/>		Actions	Upload PCAP File	Export
File Name	File Size	Uploaded At	Uploaded By	Last Played	Last Played By					
tag-write.pcap	15.57 MB	Sep 29, 2020 07:19:04 AM	admin	Never	Never					
full-download-nochange.pcap	16.48 MB	Sep 29, 2020 07:19:43 AM	admin	Never	Never					

OT Security enables you to upload a PCAP file containing recorded network activity and “play” it on OT Security. When you “play” a PCAP file, OT Security monitors the network traffic and records all information about detected assets, network activity and vulnerabilities as if the traffic had occurred within your 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 OT Security deployment (e.g. remote plants).

**Note:** 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 OT Security 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.

**Note:** 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.

**Note:** You cannot play another PCAP file while a file is still playing.





---

## Users and Roles

---

Access to the OT Security 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.
- **Authentication Servers** – Use your organization's authentication servers (e.g. Active Directory, LDAP) to authorize users to access the system. You can assign OT Security roles based on your existing groups in Active Directory.
- **SAML** – Set up an integration with your Identity Provider (e.g. Microsoft Entra ID) and assign users to your OT Security application.

[Local Users](#)

[Additional Actions on User Accounts](#)

[User Groups](#)

[Authentication Servers](#)

[SAML](#)

---

## 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.

**Note:** 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.

Full Name	Username ↑	User Groups
Mr. Admin	admin	Administrators
Bob Smith	bob	Site Operators   Read-Only Users

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.

The 'Add User' pane is a vertical form with a title bar at the top containing the text 'Add User' and a close button (X). Below the title bar are five input fields, each with a label and a required field indicator (blue asterisk):

- FULL NAME**: A text input field with the placeholder text 'Full Name'.
- USERNAME**: A text input field with the placeholder text 'Username'.
- PASSWORD**: A password input field with the placeholder text 'Password' and a toggle icon (eye) on the right.
- RETYPE NEW PASSWORD**: A password input field with the placeholder text 'Retype New Password' and a toggle icon (eye) on the right.
- USER GROUPS**: A dropdown menu with the placeholder text 'Select multiple' and a downward arrow icon.

At the bottom of the pane are two buttons: a blue 'Cancel' button and a grey 'Create' button.

3. In the Full Name field, enter the first and last name.

**Note:** 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.



**Note:** 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.

**Note:** 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 [Local Users](#).

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.

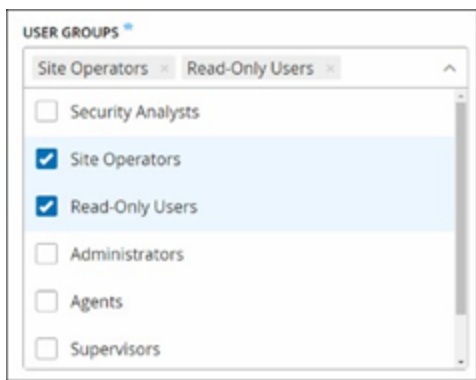
**Note:** Alternatively, you can select a user and then click on the **Actions** button > **Edit User**.

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

**Note:** 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.

**Note:** Alternatively, you can select a user and then click on the **Actions** button > **Reset Password**.

The Reset Password window is displayed.

**Reset Password** [X]

Reset password for Bob Smith.

**PASSWORD \***

Password [Eye Icon]

**RETYPE NEW PASSWORD \***

Retype New Password [Eye Icon]

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.

**Note:** Alternatively, you can select a user and then 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.

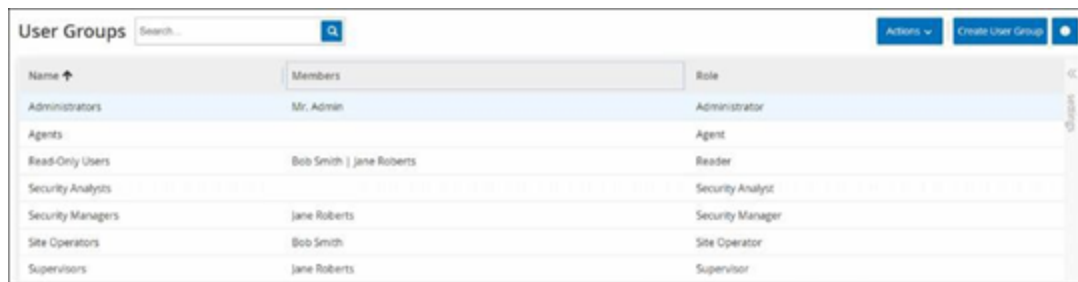
The system comes with a set of pre-defined User Groups, which correspond to each of the available roles, Administrators User Group > Administrator role, Site Operators User Group > Site Operator role etc. For an explanation of the available roles, see [User Groups](#).





## Viewing User Groups

The User Groups screen shows a list of all User Groups in the system.



The screenshot shows a web interface titled "User Groups". It features a search bar at the top left, a search icon at the top center, and two buttons at the top right: "Actions" and "Create User Group". Below the header, there is a table with three columns: "Name", "Members", and "Role". The table contains the following data:

Name	Members	Role
Administrators	Mr. Admin	Administrator
Agents		Agent
Read-Only Users	Bob Smith   Jane Roberts	Reader
Security Analysts		Security Analyst
Security Managers	Jane Roberts	Security Manager
Site Operators	Bob Smith	Site Operator
Supervisors	Jane Roberts	Supervisor

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

Parameter	Description
<b>Name</b>	The name of the User Group.
<b>Members</b>	A list of all members assigned to the group.
<b>Role</b>	The role given to this group. For an explanation of the permissions associated with each role, see <a href="#">User Groups</a> .



## 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.

The screenshot shows a 'Create User Group' dialog box with a title bar containing a close button (X). The dialog has three main sections: 'NAME' with a text input field containing the placeholder 'Name'; 'ROLE' with a dropdown menu showing 'Select'; and 'USERS' with a dropdown menu showing 'Select multiple'. At the bottom of the dialog are two buttons: 'Cancel' and 'Create'.

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.

**Note:** Alternatively, you can select a user and then click on the **Actions** button > **Delete User**.

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.

**Note:** Alternatively, you can select a user and then 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.

**Edit User Group**

**NAME** \*

Security Analysts

**ROLE** \*

Security Analyst

**USERS**

Bob Smith × Mr. Admin × +

5. Click **Save**.



## Deleting User Groups

**Note:** 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.

**Note:** 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.

## Authentication Servers

The Authentication Servers screen shows your existing integrations with authentication servers. Adding a server can be done by clicking on the **Add server** button.

Status	Name	Domain / Server	Status
Active Directory(1)			
<input checked="" type="checkbox"/>	Test1 AD	testad	Enabled
Ldap(1)			
<input checked="" type="checkbox"/>	Test LDAP 11	11	Enabled



## Active Directory

You can integrate OT Security with your organization's Active Directory. This enables users to log in to OT Security using their Active Directory credentials. The configuration involves setting up the integration and then mapping groups in your AD to User Groups in OT Security.

**Note:** 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 [Authentication Servers](#).

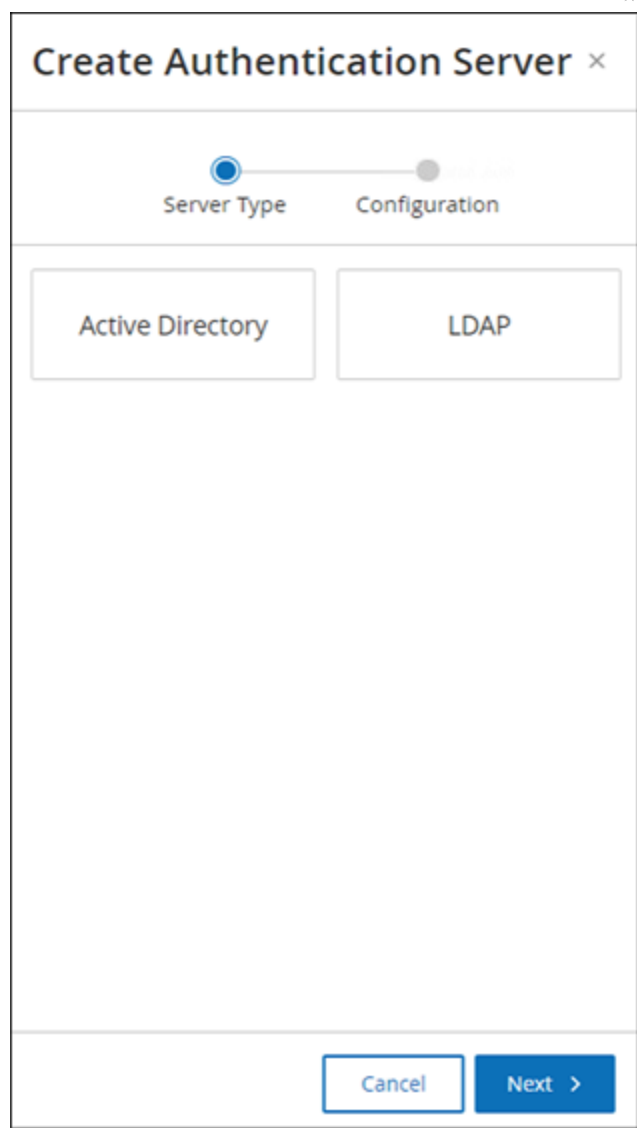
To configure Active Directory:

1. Optionally, you can obtain a CA Certificate from your organization's CA or Network Administrator and load it onto your local machine.

**Note:** 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 [Authentication Servers](#).

2. Under **Local Settings**, go to the **Users and Roles > Authentication Servers** screen.
3. Click **Add server**.

The **Create Authentication Server** side panel opens, with the **Server Type** pane displayed.



The image shows a 'Create Authentication Server' dialog box. At the top, there is a progress bar with two steps: 'Server Type' (which is currently selected and indicated by a blue dot) and 'Configuration' (indicated by a grey dot). Below the progress bar, there are two buttons: 'Active Directory' and 'LDAP'. The 'Active Directory' button is highlighted with a blue border. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Next >'. The 'Next >' button is highlighted in blue.

4. Click **Active Directory**.

The **Active Directory** configuration pane is displayed.

Create Authentication Server

Server Type

Configuration

Active Directory

You must enter at least one Group DN in order to proceed

NAME \*

DOMAIN \*

BASE DN \*

ADMINISTRATORS GROUP DN

READ-ONLY USERS GROUP DN

SECURITY ANALYSTS GROUP DN

SECURITY MANAGERS GROUP DN

SITE OPERATORS GROUP DN

SUPERVISORS GROUP DN

TRUSTED CA

PEM format only

DROP FILE HERE

Browse

< Back

Cancel

Save

5. In the **Name** field, enter the name to be used in the login screen.
6. In the **Domain Name** field, enter the FQDN of the organizational domain (e.g. company.com).

- 356 -





**Note:** 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.

7. 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).
8. For each of the Groups that you would like to map from an AD group to a OT Security 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.

**Note:** If you are not aware of the DN of the group that you would like to assign OT Security 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.

**Note:** 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.

9. 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)
10. Select the **Enable Active Directory** checkbox.
11. Click **Save**.

A pop-up window prompts you to restart the unit in order to activate the Active Directory.



Active directory changes are pending a restart

Restart

12. Click **Restart**.

The unit restarts. Upon reboot, the Active Directory settings will be activated. Any user assigned to the designated groups can access the OT Security platform using his/her organizational credentials.



**Note:** 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.



## LDAP

You can integrate OT Security with your organization's LDAP. This enables users to log in to OT Security using their LDAP credentials. The configuration involves setting up the integration and then mapping groups in your AD to User Groups in OT Security.

To configure LDAP:

1. Under Local Settings, go to the Users and Roles > **Authentication Servers** screen.
2. Click **Add Server**.

The **Add Authentication Server** side panel opens, with the **Server Type** pane displayed.

**Create Authentication Server** ×

Server Type Configuration

Active Directory LDAP

Cancel Next >



3. Select **LDAP**.

The **LDAP Configuration** pane is displayed.

Create Authentication Server

Server Type

Configuration

Active Directory

You must enter at least one Group DN in order to proceed

NAME \*

DOMAIN \*

BASE DN \*

ADMINISTRATORS GROUP DN

READ-ONLY USERS GROUP DN

SECURITY ANALYSTS GROUP DN

SECURITY MANAGERS GROUP DN

SITE OPERATORS GROUP DN

SUPERVISORS GROUP DN

TRUSTED CA

PEM format only

DROP FILE HERE

Browse

< Back

Cancel

Save

- In the **Name** field, enter the name to be used in the login screen.

- 361 -



**Note:** The login name should be distinctive and indicate that it is used for LDAP. In the event both LDAP and Active Directory are configured, only the login name will differentiate between the different configurations on the login screen.

5. In the **Server** field, enter the FQDN or the login address.

**Note:** If using a secure connection, it is recommended to use the FQDN and not an IP address to ensure that the secure Certificate provided will be verified.

**Note:** If a hostname is used, it must be in the list of DNS Servers in the OT Security system. See [System Configuration > DEVICE](#).

6. In the Port field, enter 389 to use a non-secure connection, or 636 to use a secure SSL connection.

**Note:** If Port 636 is chosen, a Certificate will be required to complete the integration.

7. In the **User DN** field, enter the DN with parameters in DN format (e.g. for a server name of AD\_1.qa.com, the user DN could be CN=Administrator,CN=Users,DC=qa,DC=com).

8. In the **Password** field, enter the password of the User DN.

**Note:** The OT Security configuration with LDAP will only continue to work as long as the User DN password is currently valid. Therefore, in the event that the User DN password changes or expires, the OT Security configuration must also be updated.

9. In the **User Base DN** field, enter the base domain name in DN format (e.g. DC=qa,DC=com).

10. In the **Group Base DN** field, enter the Group base domain name in DN format.

11. In the **Domain append** field, enter the default domain that will be appended to the authentication request in the event the user did not apply a domain they are a member of.

12. In the relevant group name fields, enter the Tenable group names for the user to use with the LDAP configuration.

13. If using Port 636 for the configuration, under **Trusted CA**, click **Browse**, and navigate to a valid PEM certificate file.

14. Click **Save**.



The Server is started in Disabled mode.

15. To apply the configuration, click the toggle switch to **ON**.

The **System Restart** dialog is displayed.

16. Click **Restart Now** to restart and apply the configuration immediately, or **Restart Later** to temporarily continue using the system without the new configuration.

**Note:** Enabling/disabling LDAP configuration will not be completed until the system is restarted. If you do not restart the system immediately, click the Restart button on the banner at the top of the screen when you are ready to restart.



---

## SAML

---

You can integrate OT Security 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 OT Security application within your identity provider, entering information about your created OT Security application and uploading your identity provider's Certificate to the OT Security **SAML** page, and then mapping groups from your identity provider to User Groups in OT Security. For a detailed tutorial for integrating OT Security with Microsoft Azure, see [Appendix 2 – SAML Integration for Microsoft Entra ID](#)

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.



**Configure SAML**

You must enter at least one group object ID in order to proceed

**IDP ID \***  
https://SAML\_Host.com

**IDP URL \***  
https://SAML\_host/saml-authresponse

**CERTIFICATE DATA \***  
PEM format only  
[Replace Current Certificate](#)

**USERNAME ATTRIBUTE \***  
NameID

**GROUPS ATTRIBUTE \***  
GroupsID

**DESCRIPTION**

**ADMINISTRATORS GROUP OBJECT ID**

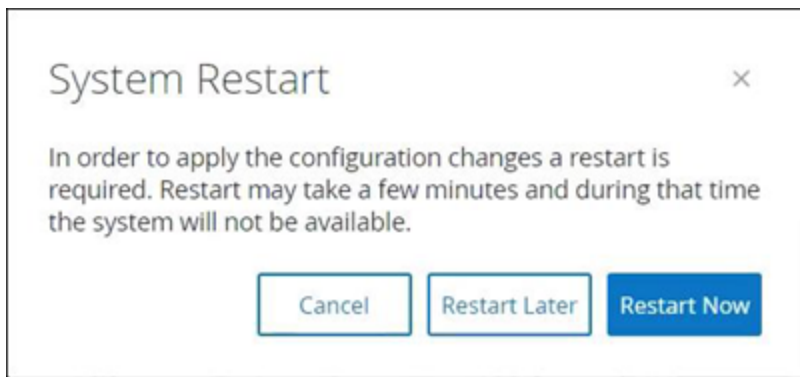
[Cancel](#) [Save](#)

3. In the **IDP ID** field, enter the Identity Provider's ID for the OT Security application.
4. In the **IDP URL** field, enter the Identity Provider's URL for the OT Security application.
5. Under **Certificate Data**, click **Replace Current Certificate**, navigate to the Identity Provider's Certificate file you downloaded for use with the OT Security application and open it.
6. In the **Username Attribute** field, enter the username attribute from the Identity Provider for the OT Security application.



7. In the **Groups Attribute** field, enter the groups attribute from the Identity Provider for the OT Security 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 OT Security 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 OT Security platform using their Identity Provider credentials.



## Integrations

---

You can set up integrations with other supported platforms in order to enable OT Security to sync with your other cyber security platforms.



## Tenable Products

You can integrate OT Security with Tenable Security Center and Tenable Vulnerability Management. This enables OT Security to share data with the other platforms. The synced data includes OT vulnerabilities as well as data discovered by IT-type Tenable Nessus scans initiated from OT Security.

**Note:** Data for Assets that have been “Hidden” in OT Security will not be sent to Tenable Security Center and Tenable Vulnerability Management via the integration.

**Note:** In order integrate the platforms, OT Security must be able to reach Tenable Security Center and/or Tenable Vulnerability Management via port 443. It is recommended to create a specific user on Tenable Security Center and/or Tenable Vulnerability Management to be used as the integration user to OT Security.



## Tenable Security Center

To integrate Tenable Security Center, create a new agent repository for OT Security data. Take note of the repo ID. In the OT Security, create a new integration, filling in IP or Hostname of your Tenable Security Center 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".

**Note:** It is recommended to create a specific user on Tenable Security Center that will be used to integrate with OT Security. The user should have the role of Security Manager/Security Analyst or Vulnerability Analyst and be assigned to the "Full Access" group.



## Tenable Vulnerability Management

To integrate with Tenable Vulnerability Management, enter your Access Key and Secret Key, and then set the sync frequency.

**Note:** You need to first generate an API key in the Tenable Vulnerability Management console (Settings > My Account > API Keys > Generate). You will be given an Access Key and a Secret Key which you enter in the OT Security console when configuring the integration.



---

## Palo Alto Networks – Next Generation Firewall

---

You can share asset inventory info discovered by OT Security with your Palo Alto system.

To integrate OT Security with your Palo Alto NGFW, fill in the IP or Hostname of your Palo Alto NGFW as well as the credentials for accessing your NGFW account.



---

## Aruba – ClearPass Policy Manager

---

You can share asset inventory info discovered by OT Security with your Aruba system.

To integrate OT Security 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 OT Security 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.

**SMTP Servers**

Tenable	Hostname / IP: 10.0.0.0.12	Edit	Delete
---------	----------------------------	------	--------

**Server Name \***  
Server Name

**Hostname / IP \***  
Hostname / IP

**Port \***  
25

**Sender Email Address \***  
Sender Email Address

**Username (Optional)**  
Username (Optional)

**Password (Optional)**  
Password (Optional)

Cancel Create Send Test Email

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 OT Security 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.

Syslog Servers

Server Name \*

Server Name

Hostname / IP \*

Hostname / IP

Port \*

514

Transport \*

Select

Send Test Message

Cancel Create

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.

**Add FortiGate Firewall** ×

The Tenable.ot-FortiGate integration allows the user to send firewall policy suggestions based on the Tenable.ot network events, to FortiGate

SERVER NAME \*

HOST/IP \*

API KEY \*

Test Server

Cancel Add

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.

**Note:** 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](https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token).



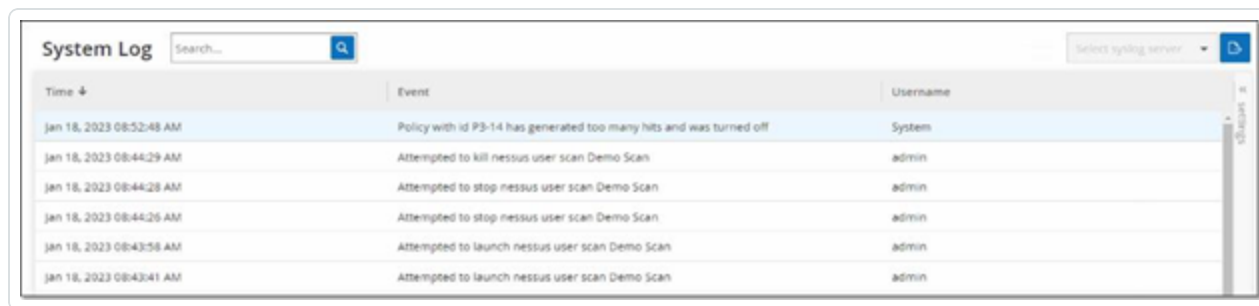
Please note: For the source address (which is needed to ensure the API token can only be used from trusted hosts), please use your OT Security unit IP address.

When creating an Administrator profile for OT Security, make sure to apply access permissions according to the following settings:

Access Control	Permissions
Security Fabric	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
FortiView	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
User & Device	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Firewall	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Log & Report	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
System	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
Security Profile	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
VPN	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
WAN Opt & Cache	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
WiFi & Switch	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write



## System Log



The screenshot shows the 'System Log' interface. At the top, there is a search bar with the placeholder text 'Search...' and a magnifying glass icon. To the right of the search bar is a dropdown menu labeled 'Select syslog server' with a blue button next to it. Below the header, there is a table with three columns: 'Time', 'Event', and 'Username'. The table contains six rows of log entries. The first row is highlighted in light blue. The table is scrollable, as indicated by a vertical scrollbar on the right side.

Time	Event	Username
Jan 18, 2023 08:52:48 AM	Policy with id P3-14 has generated too many hits and was turned off	System
Jan 18, 2023 08:44:29 AM	Attempted to kill nessus user scan Demo Scan	admin
Jan 18, 2023 08:44:28 AM	Attempted to stop nessus user scan Demo Scan	admin
Jan 18, 2023 08:44:26 AM	Attempted to stop nessus user scan Demo Scan	admin
Jan 18, 2023 08:43:58 AM	Attempted to launch nessus user scan Demo Scan	admin
Jan 18, 2023 08:43:41 AM	Attempted to launch nessus user scan Demo Scan	admin

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.

**Note:** To add a Syslog server, see [Syslog Servers](#).

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 of 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

---

Install the Sensor hardware. For instructions about setting up the sensor, see [Setting up the Sensor](#).



---

## Step 2 Connecting the Sensor to the Network

---

Connect the sensor to your network switch. For instructions about connecting the sensor to the network, see [Connecting the Sensor to the Network](#).



---

## Step 3 Accessing the Sensor Setup Wizard

---

Access the Sensor using its own static IPv4 address. For instructions about how to set up a static IP, see [Accessing the Sensor Setup Wizard](#).



## Step 4 – Sensor Setup Wizard

The OT Security setup wizard takes you through the process of configuring the basic system settings.

**Note:** 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.

Sensor Setup

Username \*  
yariv

Password \*

Sensor IP Address \*  
10.100.20.118

Subnet Mask \*  
255.255.255.0

Gateway  
10.100.20.1

Indegy Core Platform IP Address \*  
10.100.20.94

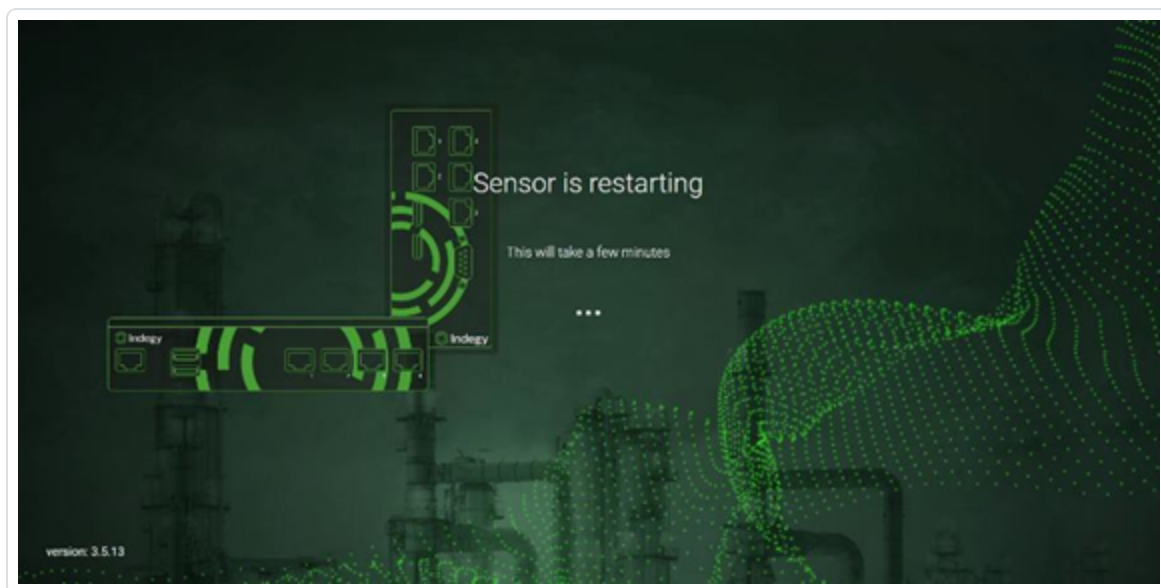
Save and Restart

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 OT Security 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 OT Security platform.
  9. Click **Save and Restart**.

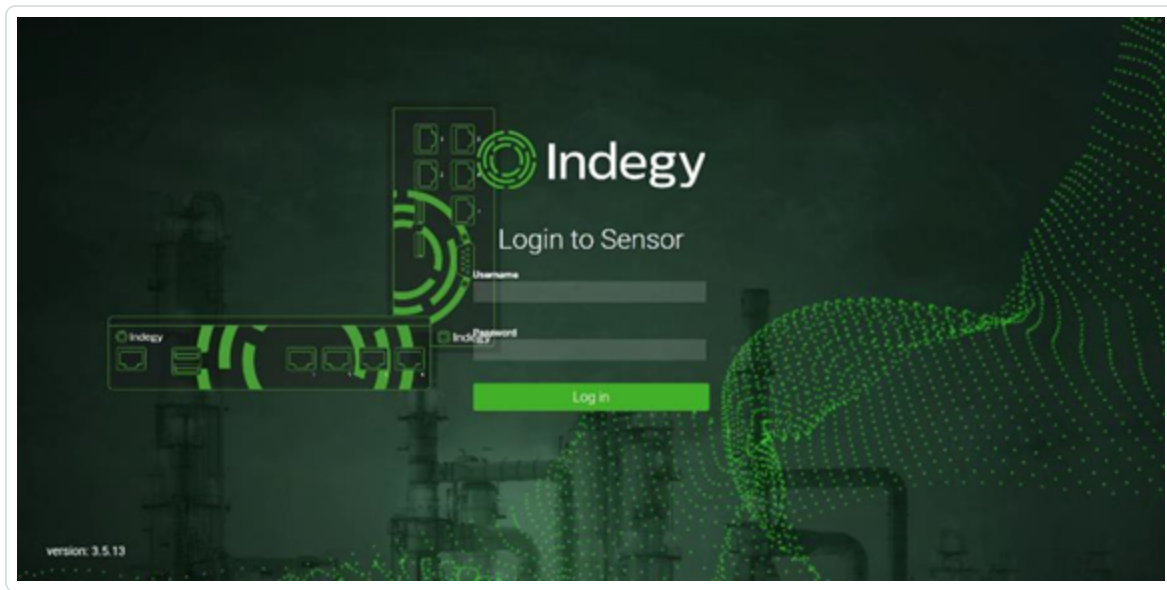
The sensor will perform a restart:



10. Following the restart process, the network traffic will be forwarded to the OT Security 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 Microsoft Entra ID

OT Security supports integration with Microsoft Entra ID via SAML protocol. This enables Azure users who were assigned to OT Security to log in to OT Security via SSO. You can use group mapping to assign roles in OT Security 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 OT Security with Microsoft Entra ID. The configuration involves setting up the integration by creating a OT Security application in Microsoft Entra ID, entering information about your created OT Security application and uploading your identity provider's Certificate to the OT Security SAML page, and then mapping groups from your identity provider to User Groups in OT Security.

To set up the configuration, you need to be logged in as an admin user in both Microsoft Entra ID and OT Security.



## Step 1 - Creating the Tenable Application in Azure

To create the Tenable application in Azure:

1. In Microsoft Entra ID go to **Microsoft Entra ID > Enterprise Applications**, click **+ New application** to display the **Browse Microsoft Entra ID Gallery**, and click **+ Create your own application**.

The **Create your own application** side panel is displayed.

**Create your own application** [X]

[Get feedback?](#)

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application

☐ Register an application to integrate with Azure AD (App you're developing)

☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

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 OT Security 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.

**Note:** 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 Entra ID** navigation menu, click **Single sign-on**, then selected SAML as the single sign on method.

The **SAML-based Sign-on** screen is displayed.

Microsoft Azure

Home > Tenable\_OT >

## Tenable\_OT | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Overview

Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting + Support

- Virtual assistant (Preview)

### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Tenable\_OT.

- #### Basic SAML Configuration

Identifier (Entity ID) **Required**

Reply URL (Assertion Consumer Service URL) **Required**

Sign on URL **Optional**

Relay State (Optional) **Optional**

Logout URL (Optional) **Optional**

[Edit](#)
- #### Attributes & Claims

⚠ Fill out required fields in Step 1

Attribute	Claim
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- #### SAML Certificates

Token signing certificate	
Status	Active
Thumbprint	D994292775296E30185D819A5C4265F255744CE2
Expiration	5/22/2027, 11:02:49 PM
Notification Email	ykrychenko@tenable.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/f116c1cc-9384-...">https://login.microsoftonline.com/f116c1cc-9384-...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

[Edit](#)



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://OT Security).

**Note:** 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 **Microsoft Entra ID Identifier**.

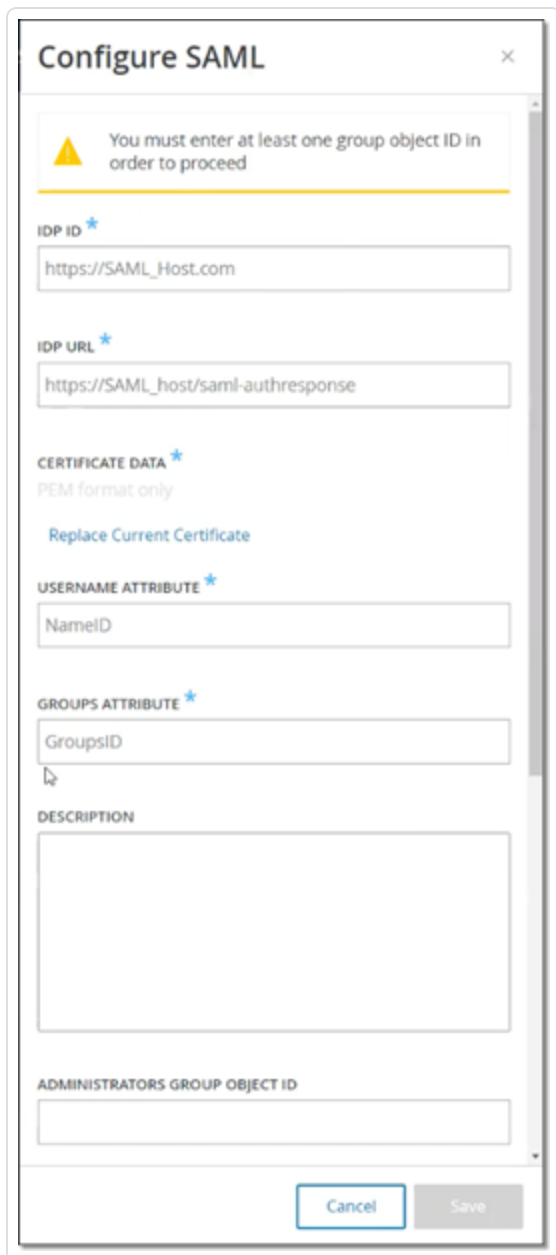


**4** Set up Tenable\_OT


You'll need to configure the application to link with Azure AD.

Login URL	<code>https://login.microsoftonline.com/f111</code>
Azure AD Identifier	<code>https://sts.windows.net/f111</code>
Logout URL	<code>https://login.microsoftonline.com/f111</code>

7. Switch to the OT Security 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.



**Configure SAML** [X]

 You must enter at least one group object ID in order to proceed

**IDP ID** \*

https://SAML\_Host.com

**IDP URL** \*

https://SAML\_host/saml-authresponse

**CERTIFICATE DATA** \*

PEM format only

[Replace Current Certificate](#)

**USERNAME ATTRIBUTE** \*

NameID

**GROUPS ATTRIBUTE** \*

GroupsID


**DESCRIPTION**

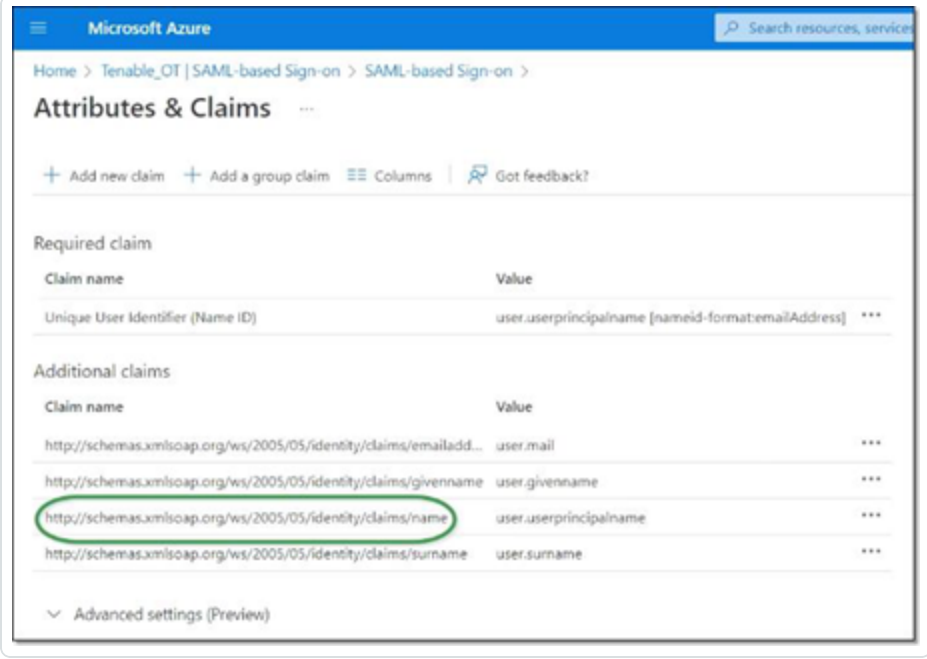
**ADMINISTRATORS GROUP OBJECT ID**

[Cancel](#) [Save](#)

9. In the **Azure** console, click the icon to copy the **Login URL**.
10. Return to the **OT Security** 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 **OT Security** 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**.

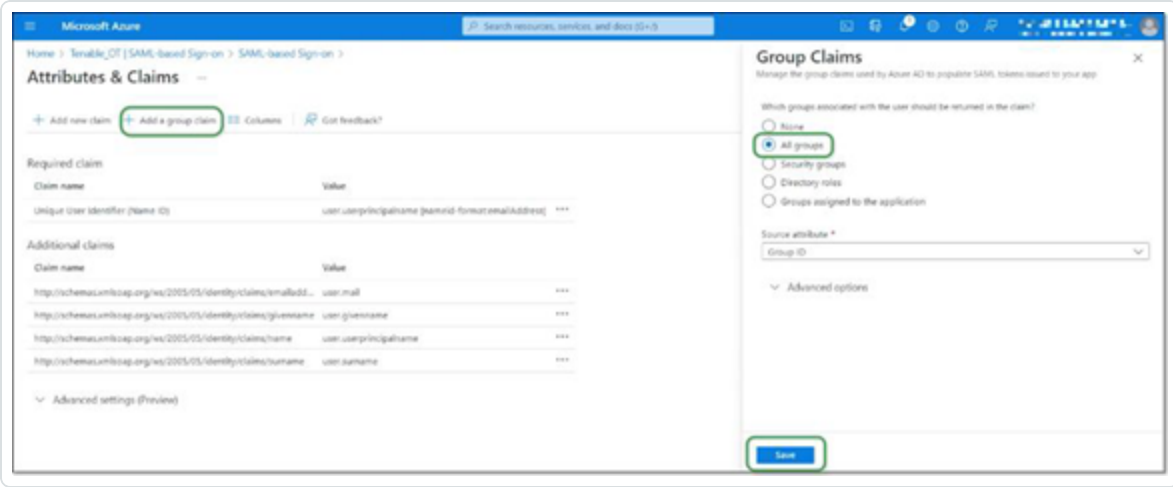


Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress] ***

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

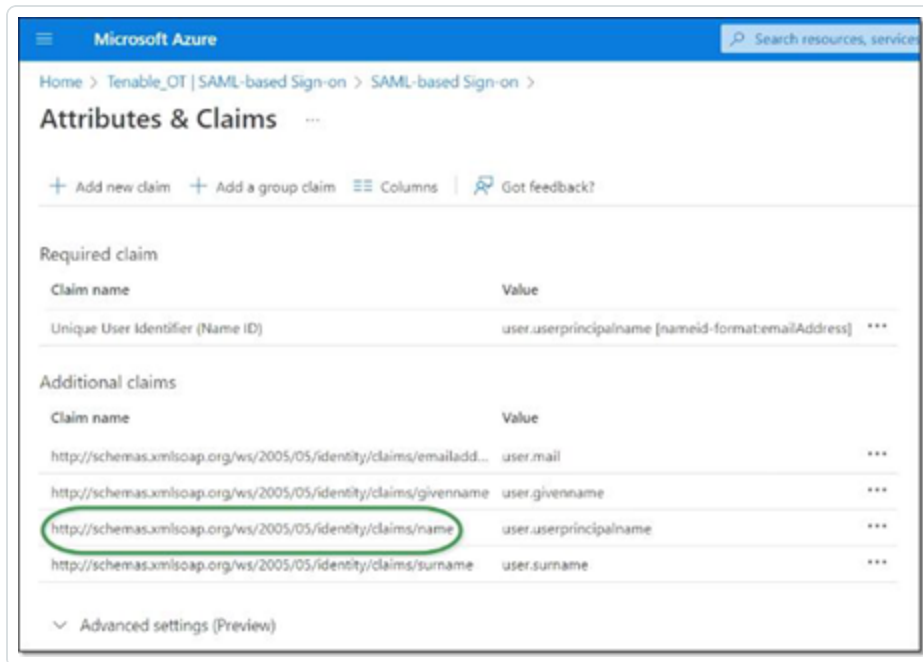
15. Return to the **Tenable** console and paste this URL in the **Username Attribute** field.
16. In the Azure console, click on **+ Add a group claim** to display the **Group Claims** side panel, and under **Which groups associated with the user should be returned in the claim?** Choose **All Groups** and click **Save**.





**Note:** 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.

- Under **Additional claims**, highlight and copy the **Claim name** URL associated with the Value user.groups [All].



- Return to the **Tenable** console and paste the copied URL in the **Groups Attribute** field.
- If you would like to add a description of the SAML configuration, enter it in the **Description** field.



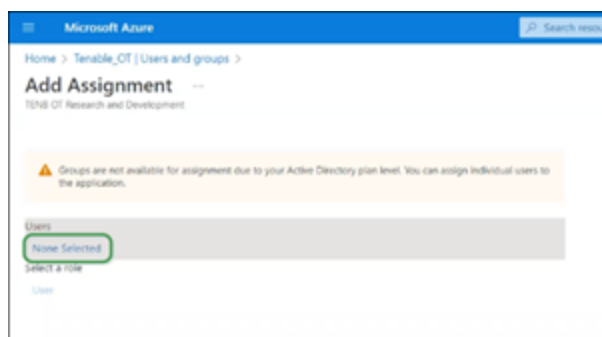
## Step 3 – Mapping Azure Users to Tenable Groups

In this step, Microsoft Entra ID users are assigned to the OT Security application. The permissions granted to each user are designated by mapping between the Azure groups to which they are assigned and a pre-defined OT Security User Group, which has an associated role and set of permissions. The OT Security pre-defined User Groups are: Administrators, Read-Only User, Security Analysts, Security Managers, Site Operators, and Supervisors. For more information, see [Users and Roles](#). Each Azure user must be assigned to at least one group that is mapped to a OT Security User Group.

**Note:** 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 OT Security:

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.

**Note:** 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.

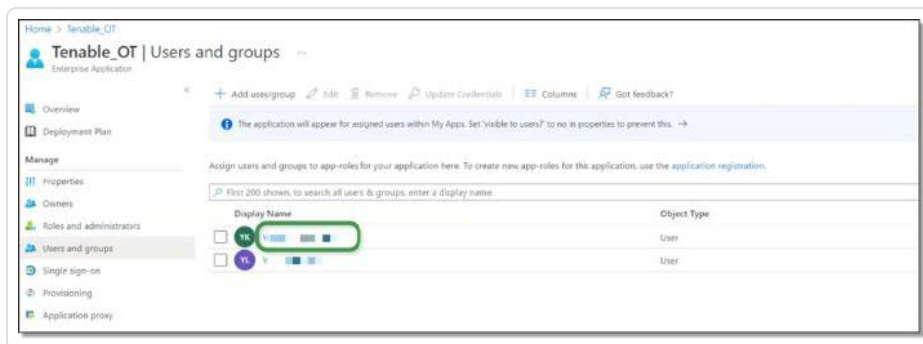
3. Search for and click on all desired users, then click **Select**, then click **Assign** to assign them to the application.



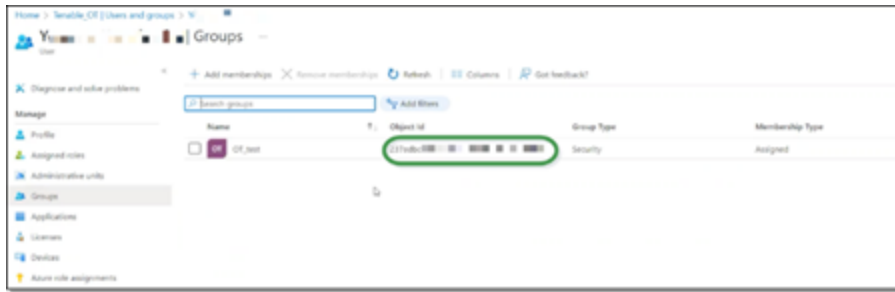


The **Users and groups** page is displayed.

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 **OT Security** 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 OT Security.
9. Click **Save** to save and close the side panel.

**Configure SAML**

GROUPS ATTRIBUTE

http://schemas.microsoft.com/w...

DESCRIPTION

ADMINISTRATORS GROUP OBJECT ID

237ed...

READ-ONLY USERS GROUP OBJECT ID

SECURITY ANALYSTS GROUP OBJECT ID

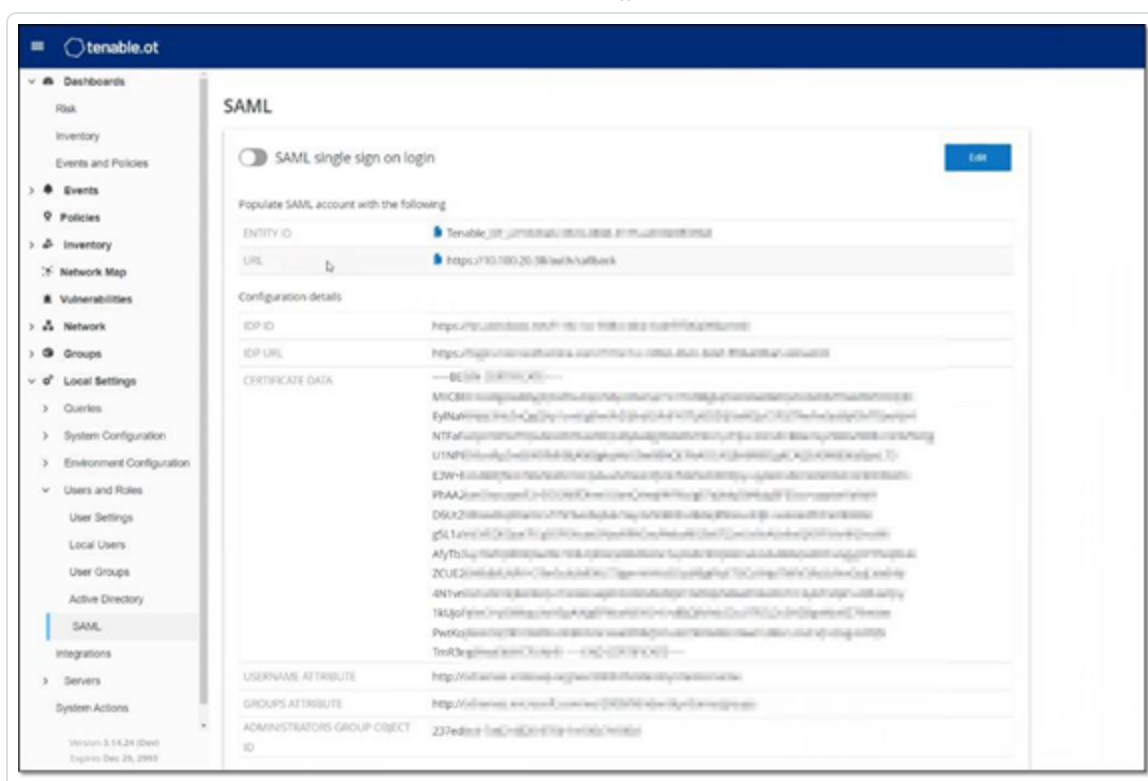
SECURITY MANAGERS GROUP OBJECT ID

SITE OPERATORS GROUP OBJECT ID

SUPERVISORS GROUP OBJECT ID

Cancel Save

The SAML screen is displayed in the OT Security console with the configured information.





## Step 4 - Finalizing the Configuration in Azure

To finalize the configuration in Azure:

1. In the OT Security **SAML** screen, under **Entity ID**, click the copy icon.

**SAML**


☒ SAML single sign on login Edit

Populate SAML account with the following

ENTITY ID	tenable_OT_e155
URL	https://10.101

Configuration details

IDP ID	https://sts.windows.net/...
IDP URL	https://login.microsoftonline.com/f116...
CERTIFICATE DATA	-----BEGIN CERTIFICATE----- MIK8DCCAdigAwIBAgIQZU6uDuUN6pH3vZvp1V11TANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDDQ...

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 Configuration**, click  **Edit**, and paste in the copied value in the **Identifier (Entity ID)** field, replacing the temporary value you previously entered.

**Tenable OT | SAML-based Sign-on**

Set up Single Sign-On with SAML

Read the configuration guide if you help integrating Tenable OT

1. Basic SAML Configuration Edit

Identifier (Entity ID)	tenable_OT_e155
Reply URL (Assertion Consumer Service URL)	https://10.101
Sign on URL (Optional)	
Relay State (Optional)	
Logout URL (Optional)	

2. Attributes & Claims Edit

Attribute	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.username
uniqueidentifier	user.uniqueidentifier
group	user.group

3. SAML Certificates Edit

Token signing certificate	Active
Status	7022708B8E1C280F40C8127804811370C21042
Expiration	5/14/2025, 19:20:31 AM

**Basic SAML Configuration**

Save Get feedback?

1. Want to know this process of the SAML Configuration experience? Click here to leave the provider.

Identifier (Entity ID) \*

The script ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

tenable\_OT\_e155 Edit

Reply URL (Assertion Consumer Service URL) \*

The reply URL is where the application expects to receive the authentication token. This is also referred to as the Assertion Consumer Service (ACS) in SAML.

https://10.101 Edit

Sign on URL (Optional)

Sign on URL is used if you need to perform service provider-initiated single sign-on. This value is the sign-on page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL ✓

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that is subsequent to a specific location within the application.

Enter a relay state ✓

4. Return to the OT Security **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.



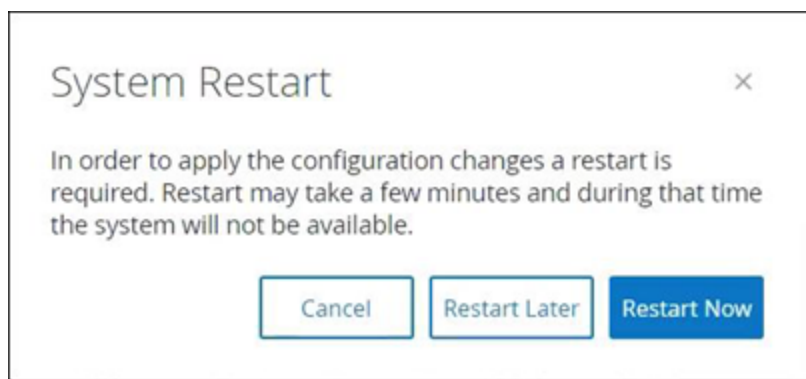
## Step 5 – Activating the Integration

To activate the SAML integration, OT Security must be restarted. The user may restart the system immediately or choose to restart it later.

To activate the integration:

1. In the OT Security 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 **OT Security** login window has a new **Sign in via SSO** link underneath the Log in button. Azure users who were assigned to OT Security can log in to OT Security using their Azure account.

To sign in using SSO:

1. On the **OT Security** login screen, click the **Sign in via SSO** link.



If you are already logged in to Azure, you are taken directly to the OT Security 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.





## Revision History

Product version: OT Security 3.15 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)



2.8	January 31, 2023	Updated for version 3.15
-----	------------------	--------------------------